C·O·L
CEMCA

Network Log Analysis and Forensics Tools

MODULE 10

Contents

Network Log Analysis And Forensics Tools

10.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Implement various techniques of capturing of network logs.
- Analyse network time stamps and data logs.
- Use various network tools used in forensics.
- Use various software tools used in forensics.

10.2 FORENSICS INFORMATION FROM NETWORK

Major information sources in network are: Host, router, fireworks, switches, and intrusion detection and prevention systems, network printers/copiers etc. wireless access points. An investigator needs to collect data from these sources. The categorization of these data as well as way these needs to be collected and analysed is of utmost importance.

Hosts: Generally, forensics makes use of agents (Software) to gather and send Host data to remote forensic server. The agents collect real time data stream passing through the network interface card (NIC) and send for analysis study.

Routers: Mostly router logs can be useful in many cases. Information of status details, errors, IP and MAC addresses getting resolved to other networks or hosts can be used to trace a suspect as well as can be helpful in getting to the chain of events while restructuring the crime.

Firewalls: Firewalls also very importantly maintain logs of every internet/ network access by the host user. These logs can be like dropped packets, un allowed application, filtered websites, recognised attacks, etc. at many times the logs of the host firewall or the network firewall is enough to trace the logs of the host firewall ir the network firewall is enough to trace links to a crime or suspicious activity.

Switch: Switches have a CAM (context addressable memory) which keeps information about mappings of MAC address to ports. Also, CAM is used to keep information about VLAN.

Two popular methods that are specifically designed to allow a network analyst to monitor traffic are [10]:

1. Port mirroring – the switch sends a copy of network packets to a monitoring network connection.
2. SMON – "Switch Monitoring" is described by RFC 2613 and is a protocol for controlling facilities such as port mirroring.

10.2.1 Intrusion detection/ prevention system

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.

Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. The logs generated by the IDS can be very useful for network forensics analysis.

Certain times network printers/copiers etc. also log the activities to some extent and can play vital role in network forensics. However, the logs maintained depend upon the manufacturer.

10.2.2 Wireless Access Points

At times WAP can also come into play as it also maintains logs of almost all routing type activities that it does like SSIDs and incoming connections etc. It is to be noted, looking at the amount of traffic that follows in and out of a network it is important to understand the storage aspects also. That is, how we will be storing these logs etc. for future analysis as well as evidence building.

The investigators can use one or more of the available bilk storage technologies like SAN (storage area network), network attached storage (NAS), direct attached storage (DAS) etc. for the purpose. Also, tape drives are in use since older days and still play a vital role in mass storages.

10.3 LOG ANALYSIS

The analysis of large volumes of data collected during IDPS is typically performed in a separate database system run by the analysis team. Live systems are usually not dimensioned to run extensive individual analysis without affecting the regular users. On the other hand, it is methodically preferable to analyse data copies on separate systems and protect the analysis teams against the accusation of altering original data.

Due to the nature of the data, the analysis focuses more often on the content of data than on the database it is contained in. If the database itself is of interest, then Database forensics are applied.

In order to analyse large structured data sets with the intention of detecting financial crime it takes at least three types of expertise in the team: A data analyst to perform the technical steps and write the queries, a team member with extensive experience of the processes and internal controls in the relevant area of the investigated company and a forensic scientist who is familiar with patterns of fraudulent behaviour.

After an initial analysis phase using methods of explorative data analysis the following phase is usually highly iterative. Starting with a hypothesis on how the perpetrator might have created a personal advantage the data is analysed for supporting evidence. Following that the hypothesis is refined or discarded.

The combination of different databases, in particular data from different systems or sources is highly effective. These data sources are either unknown to the perpetrator or he/she cannot manipulate them afterwards. Data Visualization is often used to display the results.

There are many tools that can be used to analyse the logs captured during above sources of information. However, still we need to understand how these analysis are done and how actually a criminal event can be re-created. Major activities during log analysis are:

a) Analysing time stamps
b) Analysing data

10.3.1 Analyzing time stamps

Time and its synchronization in network are very important. A smart criminal can use certain methodologies to put false time stamps in their communication. However, with advent of technologies like Network Time Protocol (NTP) this issue is more or less minimized. The investigator needs to find out whether the NTP has been incorporated or not before proceeding into the analysis. Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use. NTP was originally designed by David L. Mills of the University of Delaware, who still oversees its development. NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

10.3.2 Analyzing data

Data over network in Transmission Control Protocol/ Internet Protocol (TCP/IP) is broken into pieces which are further broken into smaller pieces called as packets to be transported over networks. The packets are re-assembled at the other end. Different packets of the same message might take different paths before reaching at other end. This adds to the complexity of reassembling the packets. To overcome this issue TCP/IP follows a mechanism of numbering each packet based on sequences. The receiver node sends acknowledgment based on these sequence numbers. The message is reconstructed and the sending host gets acknowledgement of all the packets sent over the network. The times stamps in these acknowledgement packets are in GMT (UTC) format and can give vital clues during analysis.

Other protocol which has to be understood are Address resolution protocol (ARP) which is used to map MAC address to an IP and vis-versa. This resolution protocols can help an investigator get vital traces into IP addresses and MAC addresses of any individual in a case. Other protocols/ technologies that need an overview are Internet control message protocol (ICMP), Internet protocol security (IPSec), BitTorrent, Domain name system (DNS), Dynamic host configuration protocol (DHCP), File transfer protocol (FTP), HyperText Transfer Protocol (HTTP), Internet message access protocol (IMAP), Network time protocol (NTP), Post office protocol version 3 (POP3), Secure shell (SSH), Simple mail transfer protocol (SMTP) etc.

10.4 FORENSICS TOOLS

Forensic tools that are used for forensic activities like seizure, capture, analysis etc. in network can be categorized in two forms:

a. Technology tools
b. Software tools

Technology tools are like methodologies to track, trace or identify hidden artefacts in any network system. The software tools are software solutions which can specifically assist forensic collection etc.

10.4.1 Network tools used for forensics

Network tap

A network tap is a hardware device which provides a way to access the data flowing across a computer network. In many cases, it is desirable for a third party to monitor the traffic between two points in the network. If the network between points A and B consists of a physical cable, a "network tap" may be the best way to accomplish this monitoring. The network tap has (at least) three ports: an A port, a B port, and a monitor port. A tap inserted between A and B passes all traffic through unimpeded, but also copies that same data to its monitor port, enabling a third party to listen.

Network taps are commonly used for network intrusion detection systems, VoIP recording, network probes, RMON probes, packet sniffers, and other monitoring and collection devices and software that require access to a network segment. Taps are used in security applications because they are non-obtrusive, are not detectable on the network (having no physical or logical address), can deal with full-duplex and non-shared networks, and will usually *pass through* traffic even if the tap stops working or loses power.

Once a network tap is in place, the network can be monitored without interfering with the network itself. Other network monitoring solutions require in-band changes to network devices, which meant that monitoring can impact the devices being monitored. Once a tap is in place, a monitoring device can be connected to it as-needed without impacting the monitored network.

Putting a network tap into place will disrupt the network being monitored for a short time. Even so, a short disruption is preferable to taking a network down multiple times to deploy a monitoring tool. Establishing good guidelines for the placement of network taps is recommended.

Port Mirroring

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port.

Promiscous mode

In computer networking, promiscuous mode (often shortened to "promisc mode" or "promisc. mode") is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive. This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a hub (instead of a switch) or one being part of a WLAN. Interfaces are placed into promiscuous mode by software bridges often used with hardware virtualization.

Promiscuous mode is often used to diagnose network connectivity issues. There are programs that make use of this feature to show the user all the data being transferred over the network. Some protocols like FTP and Telnet transfer data and passwords in clear text, without encryption, and network scanners can see this data. Therefore, computer users are encouraged to stay away from insecure protocols like telnet and use more secure ones such as SSH.

10.4.2 Software tools used for network forensics

Wire shark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues. Wireshark is cross-platform, using the GTK+ widget toolkit in current releases, and Qt in the development version, to implement its user interface, and using pcap to capture packets; it runs on Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public. Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options. Figure 4 depicts a typical wireshark gui.

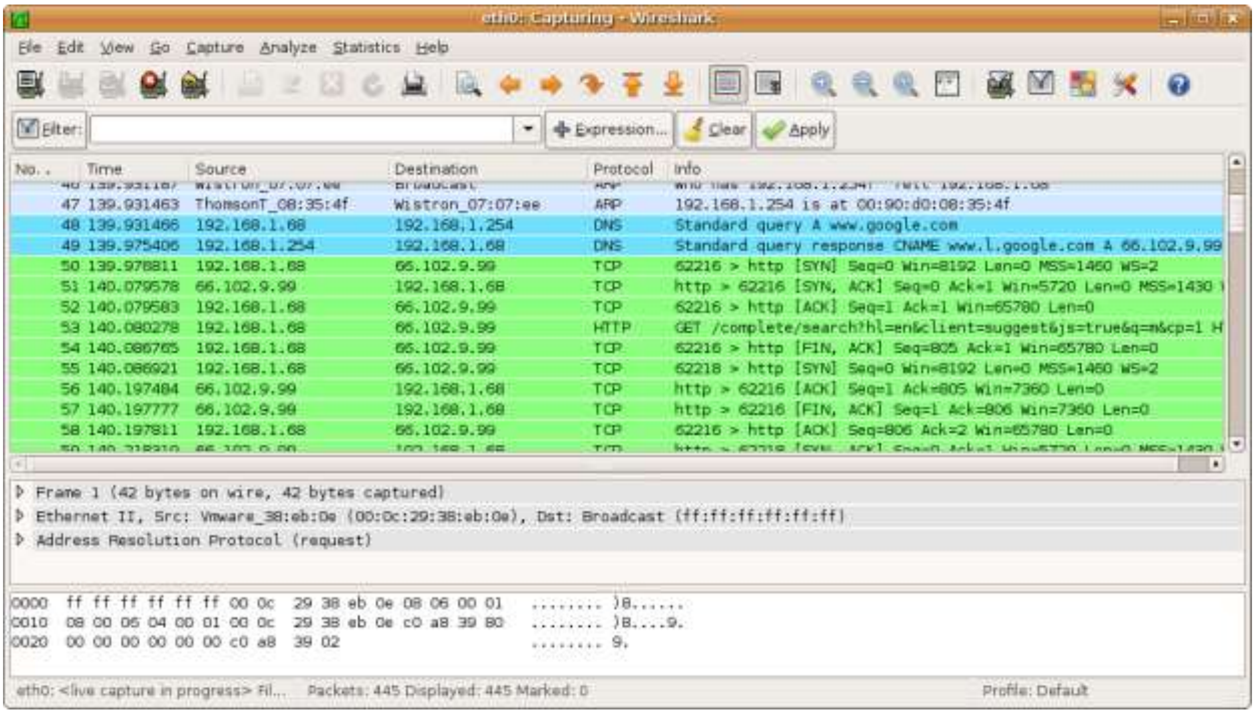
Wireshark lets the user put network interface controllers that support promiscuous mode into that mode, so they can see all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. However, when capturing with a packet analyser in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network.

VIDEO LECTURE

Wireshark is software that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from a number of types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.

Wireshark's native network trace file format is the libpcap format supported by libpcap and WinPcap, so it can exchange captured network traces with other applications that use the same format, including tcpdump and CA NetMaster. It can also read captures from other network analyzers, such as snoop, Network General's Sniffer, and Microsoft Network Monitor.


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source            Destination       Protocol  Info
    47 139.931463  ThomsonT_08:35:4f Wistron_07:07:ee  ARP       192.168.1.254 is at 00:90:d0:08:35:4f
    48 139.931466  192.168.1.68      192.168.1.254     DNS       Standard query A www.google.com
    49 139.975406  192.168.1.254     192.168.1.68      DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
    50 139.978811  192.168.1.68      66.102.9.99       TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    51 140.079578  66.102.9.99       192.168.1.68      TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
    52 140.079583  192.168.1.68      66.102.9.99       TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
    53 140.080278  192.168.1.68      66.102.9.99       HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
    54 140.086765  192.168.1.68      66.102.9.99       TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
    55 140.086921  192.168.1.68      66.102.9.99       TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    56 140.197484  66.102.9.99       192.168.1.68      TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
    57 140.197777  66.102.9.99       192.168.1.68      TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
    58 140.197811  192.168.1.68      66.102.9.99       TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.

eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0          Profile: Default
```

Figure 1: Wireshark GUI

TCPDUMP

VIDEO LECTURE

Tcpdump is a common packet analyser that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

Tcpdump works on most Unix-like operating systems: Linux, Solaris, BSD, OS X, HP-UX, Android and AIX among others. In those systems, tcpdump uses the libpcap library to capture packets. The port of tcpdump for Windows is called WinDump; it uses WinPcap, the Windows port of libpcap.

Tcpdump prints the contents of network packets. It can read packets from a network interface card or from a previously created saved packet file. Tcpdump can write packets to standard output or a file.

It is also possible to use tcpdump for the specific purpose of intercepting and displaying the communications of another user or computer. A user with the necessary privileges on a system acting as a router or gateway through which unencrypted traffic such as Telnet or HTTP passes can use tcpdump to view login IDs, passwords, the URLs and content of websites being viewed, or any other unencrypted information.

10.5 SUMMARY

.

1. In order to analyse large structured data sets with the intention of detecting financial crime it takes at least three types of expertise in the team: A data analyst to perform the technical steps and write the queries, a team member with extensive experience of the processes and internal controls in the relevant area of the investigated company and a forensic scientist who is familiar with patterns of fraudulent behaviour.
2. There are many tools that can be used to analyse the time stamps as well as data of the logs captured during Intrusion detection and prevention systems and monitoring above sources of information (components) in a network.
3. Technology tools are like methodologies to track, trace or identify hidden artefacts in any network system. The software tools are software solutions which can specifically assist forensic collection etc.
4. Tools can be used to do time line analysis, email re-construction, Metadata analysis, packet frame analysis or checksum on data exchanged.

10.6 CHECK YOUR PROGRESS

1. Fill in the blanks.

i. Applying forensic methods on the Ethernet layer is done by eavesdropping bit streams with tools called _____________.

ii. A switch sends a copy of network packets to a monitoring network connection is called as ___________.

iii. ______________________ are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.

2. State True or False

i. Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

10.7 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks.

a) monitoring tools or sniffers.
b) Port Mirroring.
c) Intrusion detection and prevention systems (IDPS).

2. State True or False

i. (T)

10.8 FURTHER READINGS

1. Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.
2. Investigating Hard Disks, File and Operating Systems: EC-Council | Press
3. Gary Palmer, A Road Map for Digital Forensic Research, Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, New York, August 7 – 8, 2001, Page(s) 27–30

10.9 MODEL QUESTIONS

1. State major features of wireshark tool.
2. What is promiscuous mode in networking?
3. What do you understand be network tapping and port mirroring?

References, Article Source & Contributors

[1] Computer network - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Computer_network

[2] Ethernet hub - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Ethernet_hub

[3] Forensic data analysis - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Forensic_data_analysis

[4] Host (network) - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Host_(network

[5] Intrusion detection system - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Intrusion_detection_system

[6] Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.

[7] Network forensics - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_forensics

[8] Network interface controller - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_interface_controller

[9] Network switch - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_switch

[10] Network tap - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_tap

[11] Network Time Protocol - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_Time_Protocol

[12] Node (networking) - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Node_(networking)

[13] OSI model - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/OSI_model

[14] Port mirroring - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Port_mirroring

[15] Promiscuous mode - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Promiscuous_mode

[16] Router (computing) - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Router_(computing)

[17] TCP/IP 4 layer model, http://www.planetlarg.net/tcpip-4-layer-model

[18] tcpdump - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Tcpdump

[19] Wireshark - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Wireshark

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar

This MOOC has been prepared with the support of

C·O·L

CEMCA