ASSIGNMENT 3: INTRODUCTION TO NETWORK TRAFFIC ANALYSIS WRITEUP

Introduction

In this module, we introduced ourselves into the principles of network traffic analysis and explored its significance for both blue team defenders and red team attackers. We focused on the usage of two powerful tools, Wireshark and tcpdump, to capture and analyze network packets. Additionally, we examined the broader implications of network traffic analysis, highlighting the criticality of visibility into network activity for effective security measures. Throughout this module, we acquired key takeaways, including the importance of network traffic analysis, the utilization of Wireshark and tcpdump, and techniques for detecting sensitive data within network traffic.

Networking Layer 1-4

In this section, we went through the basic concepts driving networking behavior for example the standard protocols and many different Protocol Data Units (PDU). We then looked at the addressing mechanisms that enable the delivery of our packets to the correct hosts in which were MAC addressing and IP addressing in which MAC addressing operates at the Data Link Layer where it assigns a unique identifier to network interface controllers (NICs) on devices. They facilitate local communication within a LAN by allowing switches to forward packets directly to the intended device based on the MAC address table.

On the other hand, IP addressing is a logical addressing mechanism operating at the Network Layer. IP addresses are hierarchical and assigned to devices participating in an IP-based network. IPv4 addresses, the most used, consist of 32 bits expressed in four groups of decimal numbers. IPv6 addresses use 128 bits and are represented in eight groups of hexadecimal digits. IP addresses enable global communication by routing packets across different networks. Routers use IP addresses to determine the best path for forwarding packets based on the routing table.

Finally, we examined the TCP and UDP transport mechanism in which TCP is a connection-oriented protocol that ensures reliable and ordered delivery of data by establishing a logical connection, implementing flow control, error detection, and packet sequencing while UDP is a connectionless protocol that offers a lightweight, low-overhead transport mechanism. It does not provide reliability or ordering guarantees but allows for fast and efficient transmission.

Questions

How many layers does the OSI model have? 7

How many layers are there in the TCP/IP model? 4

True or False: Routers operate at layer 2 of the OSI model? False

What addressing mechanism is used at the Link Layer of the TCP/IP model? Mac-Address

At what layer of the OSI model is a PDU encapsulated into a packet? (the number) 3

What addressing mechanism utilizes a 32-bit address? IPv4

What Transport layer protocol is connection oriented? TCP

What Transport Layer protocol is considered unreliable? UDP

TCP's three-way handshake consists of 3 packets: 1.Syn, 2.Syn & ACK, 3. _? What is the final packet of the handshake? ACK

Networking Layer 5-7

In this section, we looked at the upper layer protocols that handle our applications. Firstly, we looked at HTTP and HTTPS protocols which are protocols used for communication between web browsers and web servers. HTTP that transmits data in plain text, making it susceptible to eavesdropping and tampering. It operates over port 80 and is widely used for regular web browsing and data transfer. On the other hand, HTTPS is a secure version of HTTP that incorporates encryption through SSL/TLS protocols. HTTPS uses port 443 and encrypts the data exchanged between the browser and server, ensuring confidentiality and integrity.

We then looked at FTP (File Transfer Protocol) which is a standard network protocol used for transferring files between a client and a server on a computer network. It's capable of running in two different modes, active or passive. We also looked at basic FTP commands like User, Pass, Pasv and many more.

Finally, we looked at SMB (Server Message Block) which is a protocol most widely seen in Windows enterprise environments that enables sharing resources between hosts over common networking architectures. It uses TCP as its transport mechanism, it will perform standard functions like the three-way handshake and acknowledging received packets.

Questions

What is the default operational mode method used by FTP? active

FTP utilizes what two ports for command and data transfer? (seperate the two numbers with a space) 20 21

Does SMB utilize TCP or UDP as its transport layer protocol? TCP

SMB has moved to using what TCP port? 445

Hypertext Transfer Protocol uses what well known TCP port number? 80

What HTTP method is used to request information and content from the webserver? GET

What web-based protocol uses TLS as a security measure? HTTPS

True or False: when utilizing HTTPS, all data sent across the session will appear as TLS Application data?True

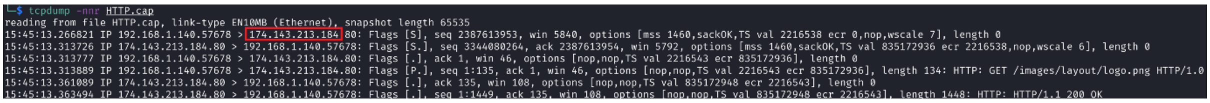
TcpDump Fundamentals

In this section, we learned about tcpdump which is a command-line packet capture utility used for network traffic analysis. It allows users to capture and analyze packets flowing through a network interface in real-time or from saved capture files. By specifying filters and options.

Questions

Utilizing the output shown in question-1.png, who is the server in this communication? (IP Address)

unzip question-1.zip



```
└─$ tcpdump -nnr HTTP.cap
reading from file HTTP.cap, link-type EN10MB (Ethernet), snapshot length 65535
15:45:13.266821 IP 192.168.1.140.57678 > 174.143.213.184 80: Flags [S], seq 2387613953, win 5840, options [mss 1460,sackOK,TS val 2216538 ecr 0,nop,wscale 7], length 0
15:45:13.313726 IP 174.143.213.184.80 > 192.168.1.140.57678: Flags [S.], seq 3344080264, ack 2387613954, win 5792, options [mss 1460,sackOK,TS val 835172936 ecr 2216538,nop,wscale 6], length 0
15:45:13.313777 IP 192.168.1.140.57678 > 174.143.213.184.80: Flags [.], ack 1, win 46, options [nop,nop,TS val 2216543 ecr 835172936], length 0
15:45:13.313889 IP 192.168.1.140.57678 > 174.143.213.184.80: Flags [P.], seq 1:135, ack 1, win 46, options [nop,nop,TS val 2216543 ecr 835172936], length 134: HTTP: GET /images/layout/logo.png HTTP/1.0
15:45:13.361089 IP 174.143.213.184.80 > 192.168.1.140.57678: Flags [.], ack 135, win 108, options [nop,nop,TS val 835172948 ecr 2216543], length 0
15:45:13.363494 IP 174.143.213.184.80 > 192.168.1.140.57678: Flags [.], seq 1:1449, ack 135, win 108, options [nop,nop,TS val 835172948 ecr 2216543], length 1448: HTTP: HTTP/1.1 200 OK
```

174.143.213.184

Were **absolute** or **relative** sequence numbers used during the capture? (see question-1.zip to answer)

relative

If I wish to start a capture without **hostname** resolution, **verbose** output, showing contents in **ASCII and hex**, and **grab the first 100 packets**; what are the switches used? please answer in the order the switches are asked for in the question.

-nvXc 100

Given the **capture file at /tmp/capture.pcap**, what **tcpdump command** will enable you to **read** from the capture and show the output contents in **Hex and ASCII?** (Please use best practices when using switches)

sudo tcpdump -Xr /tmp/capture.pcap

What TCPDump switch will increase the **verbosity** of our output? (Include the — with the proper switch)

-v

What built in terminal **help** reference can tell us more about TCPDump?

man

What TCPDump switch will let me **write** my output to a file?

-w

Tcpdump Lab

In this section, we practiced the various tcpdump basics such as reading from and writing to files, utilizing basic switches, and locating files in the terminal. Tasks were also done in this section like validating Tcpdump is installed on our machine by using the which command, starting a capture with tcpdump -i interfacename -vx , how to save and read a capture.

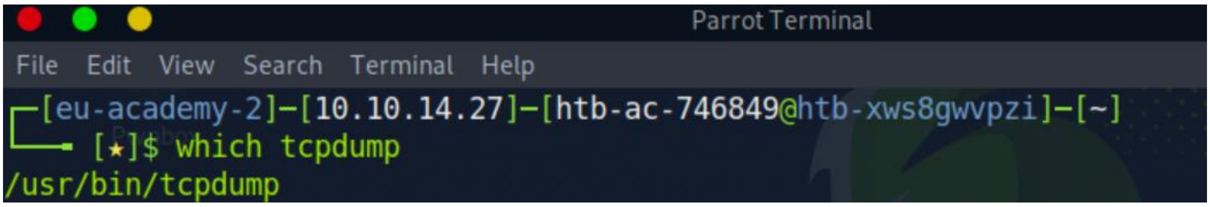
Questions

What TCPDump switch will allow us to **pipe the contents** of a pcap file out to another function such as ‘grep’? -l

True or False: The filter “port” looks at source and destination traffic. True

If i wished to **filter out ICMP traffic** from out capture, what filter could we use? (word only, not symbol please.) not icmp

What command will show you **where / if TCPDump is installed**? which tcpdump



```
┌─[eu-academy-2]─[10.10.14.27]─[htb-ac-746849@htb-xws8gwvpzi]─[~]
└──╼ [★]$ which tcpdump
/usr/bin/tcpdump
```

How do you start a capture with TCPDump to **capture on eth0**?

tcpdump -i eth0

What switch will provide **more verbosity** in your output? -v

What switch will **write** your capture output to a .pcap file? -w

What switch will **read** a capture from a .pcap file? -r

What switch will show the contents of a capture in **Hex and ASCII**? -X

Tcpdump Packet filtering

Tcpdump provides a robust and efficient way to parse the data included in our captures via packet filters. This section will examine those filters and get a glimpse at how it modifies the output from our capture. Some of the TCPDump filters examined were host in which is used to examine a specific host or server , scr/dest which allows us to work with the direction of communication , protocol number filter to know how a protocol functions and many more.

Questions

What filter will allow me to see traffic coming from or **destined to the host** with an **ip of 10.10.20.**1? host 10.10.20.1

What filter will allow me to capture based on either of two options? the or filter

True or False: TCPDump will resolve IPs to hostnames by default True

Wireshark

In this part of the module, we examined wireshark for network traffic analysis. In the first section we covered the basic familiarity of wireshark to perform traffic captures and did a couple of tasks like Validate Wireshark is installed, then open Wireshark and familiarize yourself with the GUI windows and toolbars and creating a capture filter.

We then moved to the next section whereas some advanced usage with Wireshark were covered. Different plugins such as Statistics tab and Analyze tab were explored.

Questions

Which plugin tab can provide us with a way to view conversation metadata and even protocol breakdowns for the entire PCAP file? Statistics

What plugin tab will allow me to accomplish tasks such as applying filters, following streams, and viewing expert info? Analyze

What stream oriented Transport protocol enables us to follow and rebuild conversations and the included data? tcp

True or False: Wireshark can extract files from HTTP traffic. True

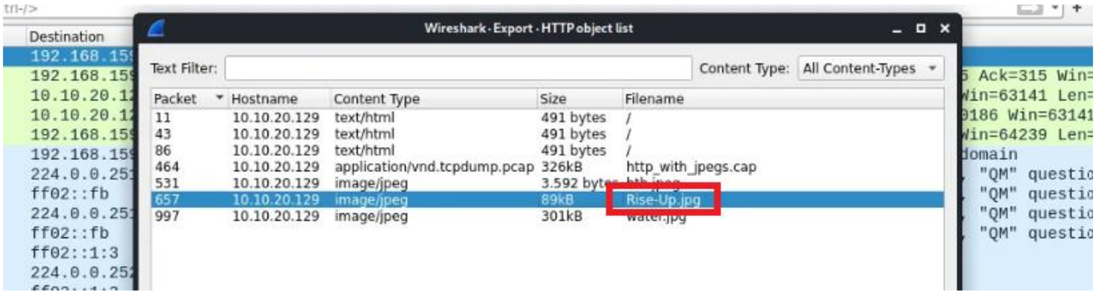
True or False: The ftp-data filter will show us any data sent over TCP port 21. False

We then explored how to dissect network traffic with Wireshark by undergoing a lab where we were able to open previously captured .pcap files, apply display filters, follow streams, and extract items from the capture file. Experiment with ways to capture new traffic and applying filters to find specific traffic.

Questions

What was the filename of the image that contained a certain Transformer Leader? (name.filetype)

Rise-Up.jpg



Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
11	10.10.20.129	text/html	491 bytes	/
43	10.10.20.129	text/html	491 bytes	/
86	10.10.20.129	text/html	491 bytes	/
464	10.10.20.129	application/vnd.tcpdump.pcap	326kB	http_with_jpegs.cap
531	10.10.20.129	image/jpeg	3.592 byt	htb.jpeg
657	10.10.20.129	image/jpeg	89kB	Rise-Up.jpg
997	10.10.20.129	image/jpeg	301kB	water.jpg

Which employee is suspected of performing potentially malicious actions in the live environment?

Bob

Finally, we then did a guided lab to utilize the concepts from the Analysis Process sections to complete an analysis.

Conclusion

In conclusion, this module on network traffic analysis provided me with essential knowledge and skills to understand and analyze network activity. We explored the significance of network traffic analysis for both defensive and offensive purposes, recognizing its role in identifying vulnerabilities and detecting potential threats. By using powerful tools like Wireshark and tcpdump, I gained the ability to capture and dissect network packets, enabling us to uncover sensitive data and assess the security of a network. It was interesting to see what one can do with simple tools such as wireshark and tcpdump.

Link:- https://academy.hackthebox.com/achievement/746849/81

Congratulations IsabellaAbuor!
You have just completed the Intro to Network Traffic Analysis module!