Week2: **Assignment 3:- HTB Academy: Introduction to Network Traffic Analysis**

Report by: **Aisha Khalifan, cs-cns04-23014**

Introduction

Log in to your Hack The Box academy account
on https://academy.hackthebox.com/course/preview/intro-to-network-traffic-analysis

In the Modules section, select the **"Intro to Network Traffic Analysis (Tier 0)" or use the following link: https://academy.hackthebox.com/module/details/81.** This module will explore principles of network traffic analysis and practically demonstrate the use of traffic analysis tools such as Wireshark and tcpdump.

Network Traffic Analysis (NTA) is the process of examining network traffic to better understand how your network is used and to identify potential threats. NTA can help security specialists to:

- Identify common ports and protocols: NTA can help you to identify the ports and protocols that are most commonly used in your network. This information can be used to establish a baseline for normal network behavior and to detect anomalies that may indicate a security threat.
- Establish a baseline: NTA can be used to establish a baseline for normal network traffic. This baseline can then be used to detect anomalies that may indicate a security threat.
- Detect and respond to threats: NTA can be used to detect a wide range of security threats, including malware, botnets, and denial-of-service attacks. Once a threat has been detected, NTA can be used to investigate the threat and to take steps to mitigate it.
- Gain visibility: NTA can provide security specialists with visibility into all of the traffic on their network. This visibility can be used to identify potential threats and to troubleshoot network problems.

NTA is an important tool for security specialists because it can help them to protect their networks from a wide range of threats.

To add to the above, NTA is particularly useful for detecting and responding to attacks that leverage legitimate credentials and tools. This is because NTA can monitor all of the traffic on the network, including traffic that is generated by legitimate users and applications. By monitoring all of the traffic, NTA can identify anomalies that may indicate a malicious attack, even if the attacker is using legitimate credentials and tools.

Overall, NTA is a powerful tool that can help security specialists to protect their networks from a wide range of threats, both old and new.

Answers to questions

Introduction

A. Networking Primer - Layers 1-4

a. How many layers does the OSI model have?
7

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

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

d. What addressing mechanism is used at the Link Layer of the TCP/IP model?
MAC-address

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

f. What addressing mechanism utilizes a 32-bit address?
IPv4

g. What Transport layer protocol is connection oriented?
TCP

h. What Transport Layer protocol is considered unreliable?
UDP

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

B. Networking Primer - Layers 5-7

It takes many different applications and services to maintain a network connection and ensure that data can be transferred between hosts.

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

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

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

d. SMB has moved to using what TCP port?
445

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

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

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

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

C. The Analysis Process

Network Traffic Analysis is a vital and dynamic process, adaptable based on available tools, organizational permissions, and network visibility. Its objective is to establish a repeatable analysis process. This involves dissecting network data, identifying irregularities that could indicate malicious activity, and understanding traffic trends against a baseline.

Traffic analysis offers essential insights for both proactive defense and daily operations troubleshooting. It can be performed actively or passively, depending on permissions and tools available, with key dependencies including permissions, capture tools, in-line placement, network tap or multiple NICs, and adequate storage and processing power.

Understanding daily traffic patterns through a baseline is crucial for efficient analysis and anomaly detection. This analysis is pivotal in swiftly identifying and mitigating potential network breaches

Traffic Capture Dependencies

They can be of two types: **Passive and active as shown in the table below:**

Dependencies	Type	Description
Permission	**Passive/ Active**	**Always ask for written permission from the right authority before capturing data, as it could be against the rules or laws in some organizations, especially in sensitive sectors like healthcare or banking. Stay legal and ethical, even if you consider yourself a hacker.**
Mirrored Port	**Passive**	**To capture data effectively, configure a switch or router interface to copy data to a specific port while enabling promiscuous mode on your NIC. This allows inspection of traffic not usually visible on other links.**
Capture Tool	**Passive/ Active**	**To process traffic, use tools like Wireshark on a capable computer. Be cautious as filtering large PCAP files can strain system resources. Ensure the host has sufficient power.**
In-line Placement	**Active**	**Placing a Tap in-line requires a topology change for the network you are working in. The source and destination hosts will not notice a difference in the traffic, but for the sake of routing and switching, it will be an invisible next hop the traffic passes through on its way to the destination.**
Network Tap or Host With Multiple NIC's	**Active**	**A computer with two NIC's, or a device such as a Network Tap is required to allow the data we are inspecting to flow still**
Storage and Processing Power	**Passive/ Active**	**You will need plenty of storage space and processing power for traffic capture off a tap.**

D. Analysis in Practice

In this section we go through the components of a network analysis

Workflow for Traffic Analysis:

a. **Descriptive Analysis:**
    1. Issue identification and scope definition.
b. **Diagnostic Analysis:**
    2. Capture network traffic and filter components.
    3. Understanding captured network traffic.
c. **Predictive Analysis:**
    4. Note-taking and mind mapping of results.
    5. Summary of analysis for decision-making.
d. **Prescriptive Analysis:**
    6. Actions and solutions based on the workflow.

Key Components of Effective Analysis:

i. Know your environment: Asset inventory and network maps.
ii. Placement is key: Ideal tool placement for capturing traffic.
iii. Persistence: Continuous drive to identify and solve issues.

Analysis Approach:

Start with standard protocols and progress to specific ones.
Look for patterns and unusual events in network traffic.
Don't hesitate to seek assistance for thorough analysis.

E. Tcpdump Fundamentals

i. Utilizing the output shown in question-1.png, who is the server in this communication? (IP Address) unzip question-1.zip open question-1.PNG
174.143.213.184
ii. Were **absolute** or **relative** sequence numbers used during the capture? (see question-1.zip to answer) - **relative**
iii. 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**
iv. 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
v. What TCPDump switch will increase the **verbosity** of our output? (Include the — with the proper switch) **-v**
vi. What built in terminal **help** reference can tell us more about TCPDump? man
vii. What TCPDump switch will let me **write** my output to a file? **-W**

F. Capturing with Tcpdump(Fundamentals Labs)

i. What TCPDump switch will allow us to **pipe the contents** of a pcap file out to another function such as 'grep'? **-l**
ii. True or False: The filter "port" looks at source and destination traffic. **True**
iii. If i wished to **filter out ICMP traffic** from out capture, what filter could we use? (word only, not symbol please.) **not icmp**
iv. What command will show you **where / if TCPDump is installed**? **which tcpdump**
v. How do you start a capture with TCPDump to **capture on eth0**? **tcpdump -i eth0**

vi. What switch will provide **more verbosity** in your output? **-v**
vii. What switch will **write** your capture output to a .pcap file? **-w**
viii. What switch will **read** a capture from a .pcap file? **-r**
ix. What switch will show the contents of a capture in **Hex and ASCII**? -X

G. Tcpdump Packet Filtering

i. 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**

ii. What filter will allow me to capture based on either of two options? **or**

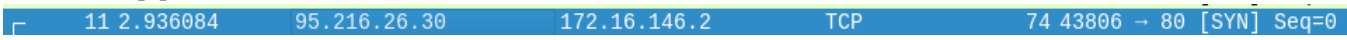
iii. True or False: TCPDump will resolve IPs to hostnames by default **True**

H. Interrogating Network Traffic with Capture and Display Filters

i. What are the **client** and **server port** numbers used in first full TCP three-way handshake? (low number first then high number)

wireshark

FILTER: tcp.port == 80



80 43806

ii. Based on the traffic seen in the pcap file, who is the **DNS** server in this network segment? (ip address)

Download: zeek

zeek -C -r TCPDump-lab-2.pcap

cat dns.log

172.16.146.1

I. Analysis with Wireshark

i. True or False: Wireshark can run on both Windows and Linux. **True**
ii. Which Pane allows a user to see a summary of each packet grabbed during the capture?
Packet List
iii. Which pane provides you insight into the traffic you captured and displays it in both ASCII and Hex?
Packet Bytes
iv. What switch is used with TShark to list possible interfaces to capture on? **-D**
v. What switch allows us to apply filters in TShark? **-f**
vi. Is a capture filter applied before the capture starts or after? (answer before or after) **before**

J. Familiarity With Wireshark

K. Wireshark Advanced Usage

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

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

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

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

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

L. Packet Inception, Dissecting Network Traffic With Wireshark

unzip Wireshark-lab-2.zip

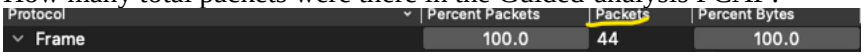
i. What was the filename of the image that contained a certain Transformer Leader? (name.filetype)
Rise-Up.jpg

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

M. Guided Lab: Traffic Analysis Workflow

i. What was the name of the new user created on Mr. Ben's host? **hacker**

ii. How many total packets were there in the Guided-analysis PCAP?



44

iii. What was the suspicious port that was being used?

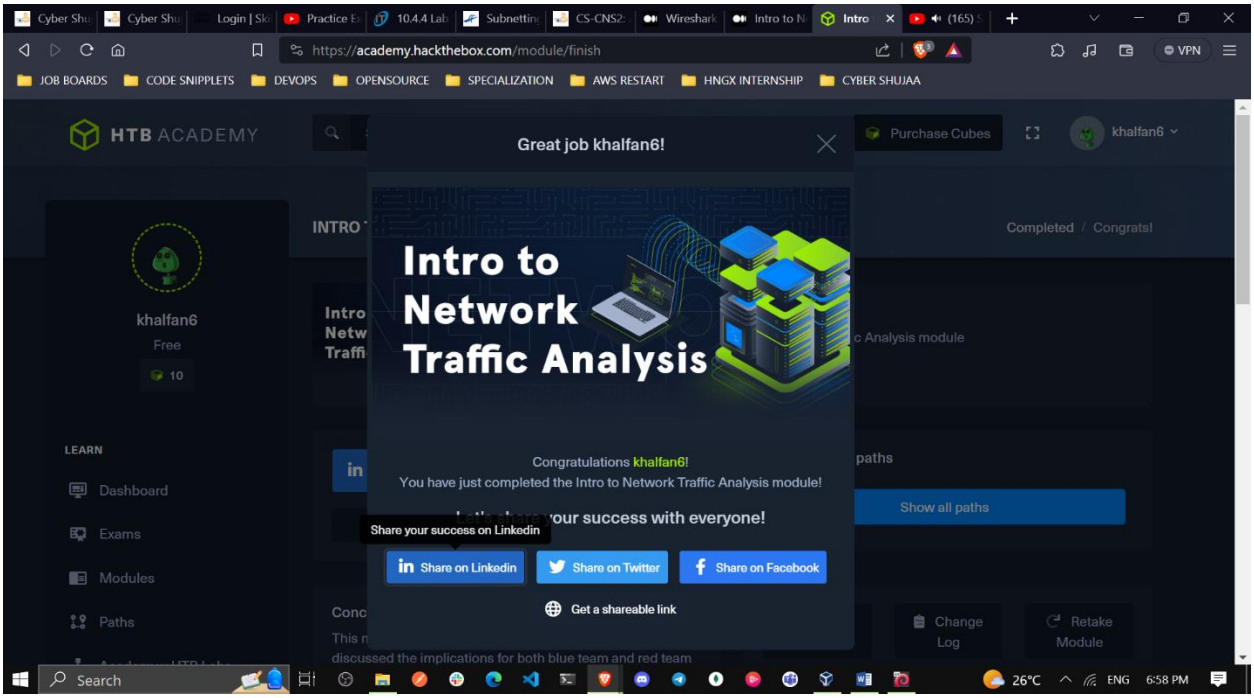
4444

N. Descripting RDP connections

i. What user account was used to initiate the RDP connection? bucky

Provide a shareable link : https://academy.hackthebox.com/achievement/785849/81

Conclusion


https://academy.hackthebox.com/module/finish
HTB ACADEMY
Purchase Cubes
khalfan6
Great job khalfan6!
Intro to Network Traffic Analysis
Congratulations khalfan6!
You have just completed the Intro to Network Traffic Analysis module!
Share your success on Linkedin
Share on Linkedin
Share on Twitter
Share on Facebook
Get a shareable link
Completed / Congrats!
LEARN
Dashboard
Exams
Modules
Paths
Show all paths
Change Log
Retake Module
Search
26°C
ENG
6:58 PM