

# **\*\*PRATICAL**

## **VERSION NUMBER 4\***

---

### **PRATICAL VERSION NUMBER 4**

#### **NETWORK TRAFFIC ANALYSIS**

##### **QUESTION**

1. How can you detect suspicious network traffic that might indicate a cyber attack?

##### **ANSWER**

--->There are several ways to detect suspicious network traffic that might indicate a cyber attack which includes

**The NIDS(network intrusion detection system) and NIPS(network intrusion prevention system)**

<1>- Signature-based detection--This simply means detecting of attacks by looking for a specific pattern which include known malicious instructions used by malware, network patterns researched by threat hunters, and also bite sequences in network traffic.. In this signature-based detection, the network database is stored with attack patterns or signatures, if the network traffic matches the database pattern or signature, such traffic is detected. The problem a SOC analyst will encounter while using this type of detection is that it is difficult to detect new attacks because no pattern is available.

<2>-Behavior-based detection-This is also known as the heuristic detection or anomaly based detection. It differs from the signature based detection because the behavior based detection are used to detect unknown attacks while the signature based are used for known attacks. **As the name anomaly it simply means abnormality.** The approach is to use machine learning algorithms to identify patterns and anomalies that may show an attack.

**Note:The difference between the NIDS and NIPS is that the NIDS can detect suspicious activity but cant prevent while the NIPS can prevent detected threats. D for detection and P for prevention**

<3>-Unusual traffic pattern--This can either be as a result of increase in the traffic volume or traffic coming from unknown sources or segmented system. Any unexpected increase in the traffic volume which leads to resource consumption can be as a result of a DDoS attack\*\*(Distributed Denial of Service\*\*) Attack. Large amount of traffic coming from an unfamiliar location is also considered suspicious and might indicate a cyber attack.

Example: A company situated in Lagos and has 10 workers working from home in Lagos suddenly gets a request from Ghana is considered suspicious and might indicate a cyber attack or a network that consumes 2mb per sec starts consuming 25mb per sec is considered suspicious

<4>- Too many failed login attempts: On this category, we have the brute force attack and password spraying..

brute force attack- A lot of failed login attempts from a particular IP address or from different accounts could be considered suspicious

password spraying: using a single password to break into multiple accounts.

<5> Port scanning: Scanning for open ports can also help detect suspicious network traffic that may indicate cyber threats and there are some common port numbers (**HTTP-80 ,HTTPS(secured version of HTTP)-443,telnet-23,SSH-22,**)

<6>-Log analysis-Reviewing of logs regularly for unusual patterns or errors will help detect suspicious network traffic and this is done with the help of the **SIEM(security information and event management)** and **firewall** logs and **syslog** should be checked and reviewed.

<7>Traffic analysis: Have a baseline of what the traffic for your network looks like considering protocols and types of traffic. The baseline configuration will help detect suspicious activities.

<8>--Network security devices such as **firewalls ,web application firewalls(WAF) ,NGFW(next generation firewalls) and network access control(NAC)** should be used. The firewalls will be configured to filter malicious traffic and should **deny on default**. The WAF is used to prevent web applications from SQL injections and cross site scripting(XSS). The NAC is also important as it creates policy for the security requirements of devices.

Other ways to detect suspicious behavior include deep packet inspection with the help of the Wireshark, monitoring of indicators which most definitely indicates data exfiltration on the outbound traffic

## QUESTION

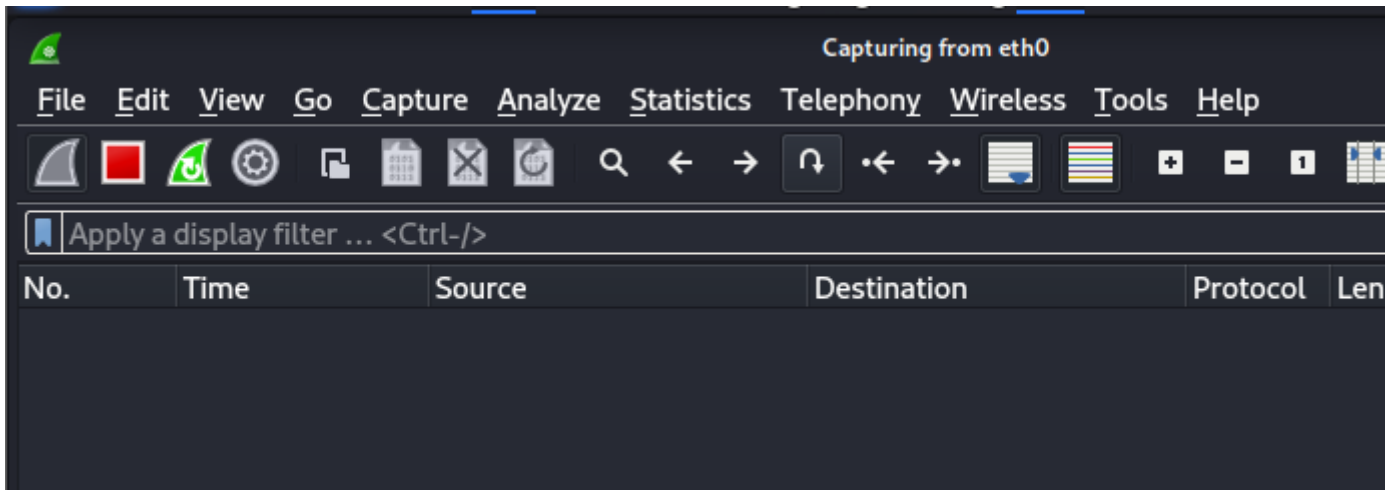
Capture network traffic using Wireshark. Analyze the traffic to identify signs of a potential attack, such as port scanning, abnormal DNS queries, or unexpected outbound traffic. Document your findings and propose mitigation steps.

## ANSWER

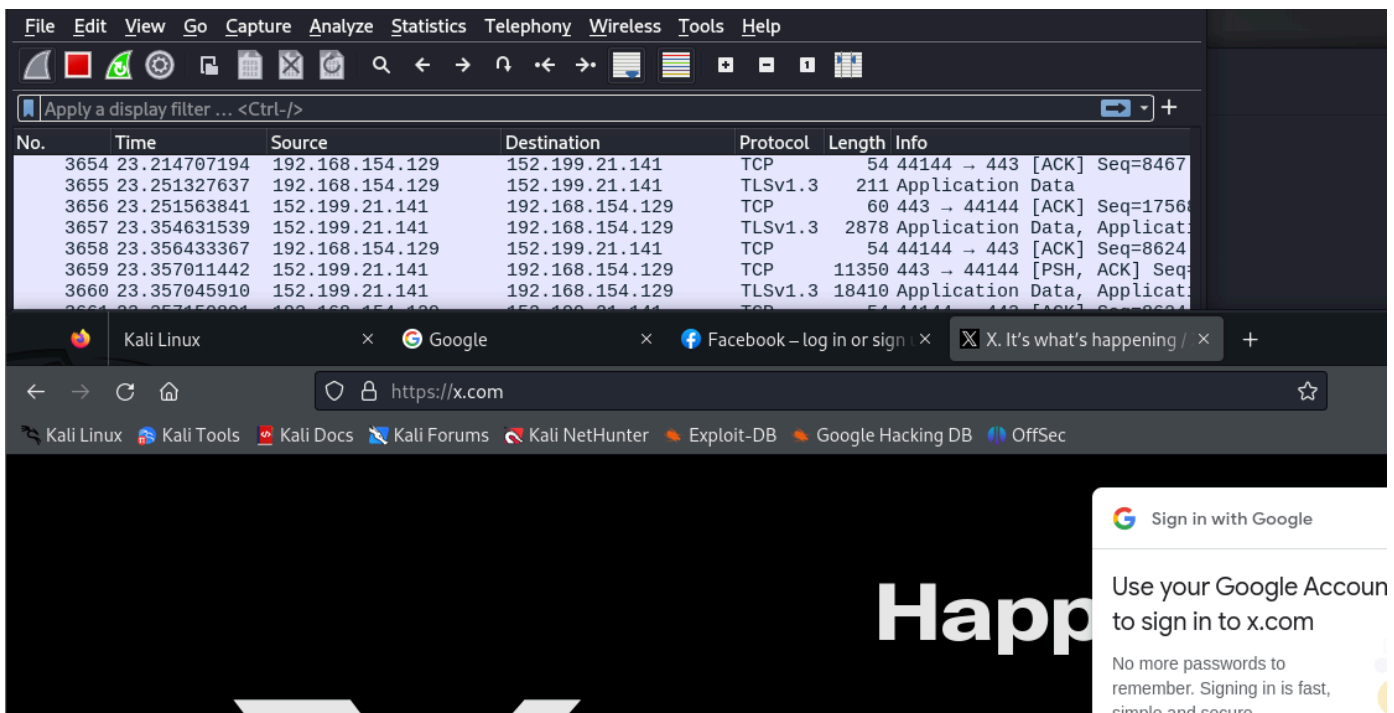
-I used the Wireshark on my Kali Linux

-I visited the following website on my web browser so as to have a lot of activities before i stop capturing (google.com (5TIMES consecutively , facebook.com and also twitter.com)

-my results and screenshots are displayed below



After visiting the website



I inputed tcp in the filter button so as to see network traffic on the tcp protocol

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.154.129	2.18.190.80	TCP	54	44530 → 80 [ACK] Seq=1
2	0.000069655	192.168.154.129	2.18.190.80	TCP	54	44532 → 80 [ACK] Seq=1
3	0.000111217	2.18.190.80	192.168.154.129	TCP	60	[TCP ACKed unseen segm
4	0.000111386	2.18.190.80	192.168.154.129	TCP	60	[TCP ACKed unseen segm
5	0.515993417	192.168.154.129	2.21.39.19	TCP	54	38746 → 80 [ACK] Seq=1
6	0.516159535	2.21.39.19	192.168.154.129	TCP	60	[TCP ACKed unseen segm
8	0.768476274	192.168.154.129	34.107.221.82	TCP	54	39924 → 80 [ACK] Seq=1
9	0.768700819	34.107.221.82	192.168.154.129	TCP	60	[TCP ACKed unseen segm
14	2.672165895	192.168.154.129	216.58.223.228	TCP	74	53594 → 443 [SYN] Seq=
15	2.676900874	216.58.223.228	192.168.154.129	TCP	60	443 → 53594 [SYN, ACK]
16	2.676952973	192.168.154.129	216.58.223.228	TCP	54	53594 → 443 [ACK] Seq=

▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 ▶ Ethernet II, Src: VMware\_f0:eb:3f (00:0c:29:00:00:00), Dst: 00:0c:29:00:00:00  
 ▶ Internet Protocol Version 4, Src: 192.168.154.129, Dst: 2.18.190.80  
 ▶ Transmission Control Protocol, Src Port: 44530, Dst Port: 80

I also filtered DNS traffic

No.	Time	Source	Destination	Protocol	Length	Info
10	2.653049997	192.168.154.129	192.168.154.2	DNS	74	Standard query 0xba50
11	2.653138389	192.168.154.129	192.168.154.2	DNS	74	Standard query 0x736f
12	2.661978271	192.168.154.2	192.168.154.129	DNS	90	Standard query response
13	2.671528829	192.168.154.2	192.168.154.129	DNS	102	Standard query response
23	2.791282194	192.168.154.129	192.168.154.2	DNS	70	Standard query 0x7060
24	2.791337984	192.168.154.129	192.168.154.2	DNS	70	Standard query 0x7166
25	2.804727573	192.168.154.2	192.168.154.129	DNS	381	Standard query response
26	2.810730641	192.168.154.2	192.168.154.129	DNS	369	Standard query response
51	3.779552723	192.168.154.129	192.168.154.2	DNS	74	Standard query 0xf50a
52	3.779635795	192.168.154.129	192.168.154.2	DNS	74	Standard query 0x2c08
53	3.792276853	192.168.154.2	192.168.154.129	DNS	102	Standard query response

I filtered HTTP traffic also

No.	Time	Source	Destination	Protocol	Length	Info
30	2.818466775	192.168.154.129	216.58.223.195	OCSP	466	Request
33	2.922383344	216.58.223.195	192.168.154.129	OCSP	755	Response
80	3.927204673	192.168.154.129	216.58.223.195	OCSP	466	Request
97	4.033273552	216.58.223.195	192.168.154.129	OCSP	755	Response
504	4.629187543	192.168.154.129	216.58.223.195	OCSP	466	Request
511	4.653440106	192.168.154.129	216.58.223.195	OCSP	467	Request
532	4.738624639	216.58.223.195	192.168.154.129	OCSP	755	Response
537	4.739160101	192.168.154.129	216.58.223.195	OCSP	467	Request
550	4.746009772	192.168.154.129	216.58.223.195	OCSP	466	Request
551	4.746139393	192.168.154.129	216.58.223.195	OCSP	467	Request
556	4.754946844	216.58.223.195	192.168.154.129	OCSP	756	Response

## FINDINGS

\*\*--\*\*i noticed multiple packets being detected from IP address (192.168.154.2 192.168.154.129) respectively targeting ports 22,80 which shows a port scan attempt

## MITIGATION OR PREVENTION

**-DNS MONITORING-** enable DNS logging so as to monitor suspicious DNS queries.

**-PORT SCANNING-** use an intrusion detection system to detect port scanning attempts.

**OUTBOUND TRAFFIC** - communications to familiar IP address should be limited and traffic to unknown IP address should be blocked and firewalls is configured to block repeated attempts from an IP address as i did visit google.com 5 times repeatedly.

USING NMAP which is now zenmap

The results are shown below

Target: 192.168.154.129

Profile: Intense scan

Scan

Cancel

Command: nmap -T4 -A -v 192.168.154.129

Hosts

Services

OS

Host

192.168.154.129

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

nmap -T4 -A -v 192.168.154.129

Details

Starting Nmap 7.95 ( <https://nmap.org> ) at 2024-08-20 23:37 W. Central Africa Standard Time  
**NSE:** Loaded 157 scripts for scanning.  
**NSE:** Script Pre-scanning.  
Initiating NSE at 23:37  
Completed NSE at 23:37, 0.00s elapsed  
Initiating NSE at 23:37  
Completed NSE at 23:37, 0.00s elapsed  
Initiating NSE at 23:37  
Completed NSE at 23:37, 0.00s elapsed  
Initiating ARP Ping Scan at 23:37  
Scanning 192.168.154.129 [1 port]  
Completed ARP Ping Scan at 23:37, 0.75s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 23:37  
Completed Parallel DNS resolution of 1 host. at 23:37, 0.01s elapsed  
Initiating SYN Stealth Scan at 23:37  
Scanning 192.168.154.129 [1000 ports]  
Discovered open port 22/tcp on 192.168.154.129  
Completed SYN Stealth Scan at 23:37, 0.03s elapsed (1000 total ports)  
Initiating Service scan at 23:37  
Scanning 1 service on 192.168.154.129  
Completed Service scan at 23:37, 0.06s elapsed (1 service on 1 host)  
Initiating OS detection (try #1) against 192.168.154.129  
Retrying OS detection (try #2) against 192.168.154.129  
Retrying OS detection (try #3) against 192.168.154.129  
Retrying OS detection (try #4) against 192.168.154.129  
Retrying OS detection (try #5) against 192.168.154.129  
**NSE:** Script scanning 192.168.154.129.  
Initiating NSE at 23:38  
Completed NSE at 23:38, 5.02s elapsed  
Initiating NSE at 23:38  
Completed NSE at 23:38, 0.00s elapsed


Filter Hosts

Target:
192.168.154.129
Profile:
Intense scan
Scan
Cancel

Command:
nmap -T4 -A -v 192.168.154.129

Hosts

Services

OS	Host
	192.168.154.129

Filter Hosts

Nmap Output
Ports / Hosts
Topology
Host Details
Scans

nmap -T4 -A -v 192.168.154.129
Details

```

OS: =MDD4NNNNW / %U=1%Q=) 11 (K=1%DF=1%1=40%O=U%A=O+
%F=AS%RD=0%Q=) T2 (R=N) T3 (R=N
OS:) T4 (R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=) T5 (R=Y%DF=Y%T=40%W=0%S=Z
OS:S+
%F=AR%O=%RD=0%Q=) T6 (R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=) T7 (R=Y%DF
OS:=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=) U1 (R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE (R=Y%DFI=N%T=40%CD=S)

Uptime guess: 27.931 days (since Wed Jul 24 01:17:46 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.69 ms 192.168.154.129

NSE: Script Post-scanning.
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
Read data files from: C:\Users\User\Nmap
OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.57 seconds
Raw packets sent: 1111 (52.918KB) | Rcvd: 1147 (50.666KB)

```

DONE