**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 anomally 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- Alot 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 number **(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 **firewal**l logs and **syslog** should be checked and reviewed.

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

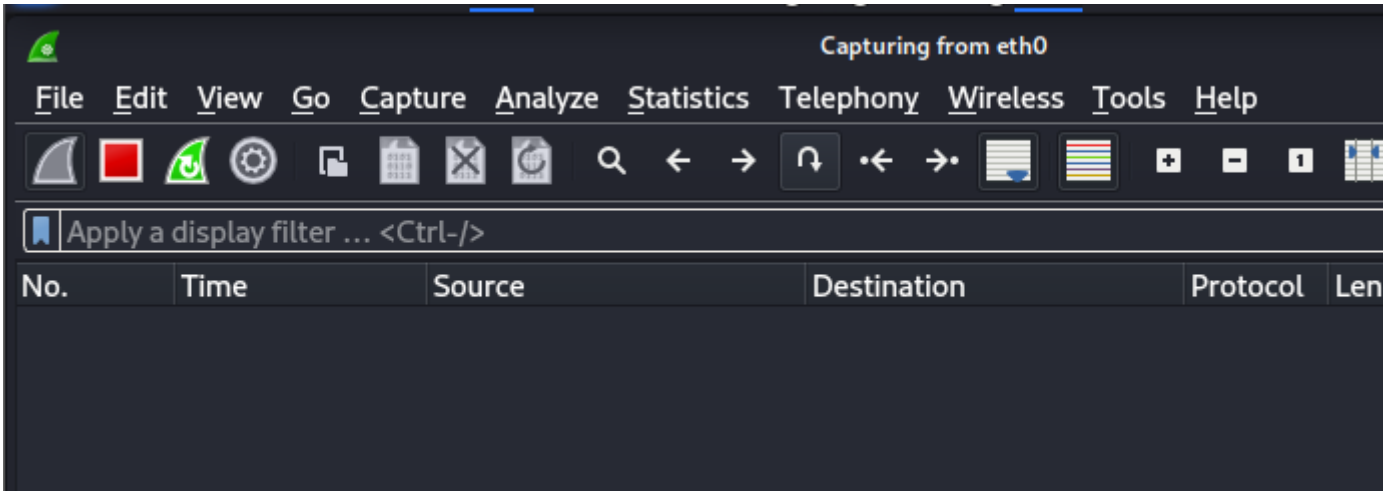
Capture network traffic using Wireshark. Analyze the traffic to identify signs of a potential attack, such as port scanning, abnormal DNS queries, or unexpected outbound traffic. Document your findings and propose mitigation steps.

ANSWER

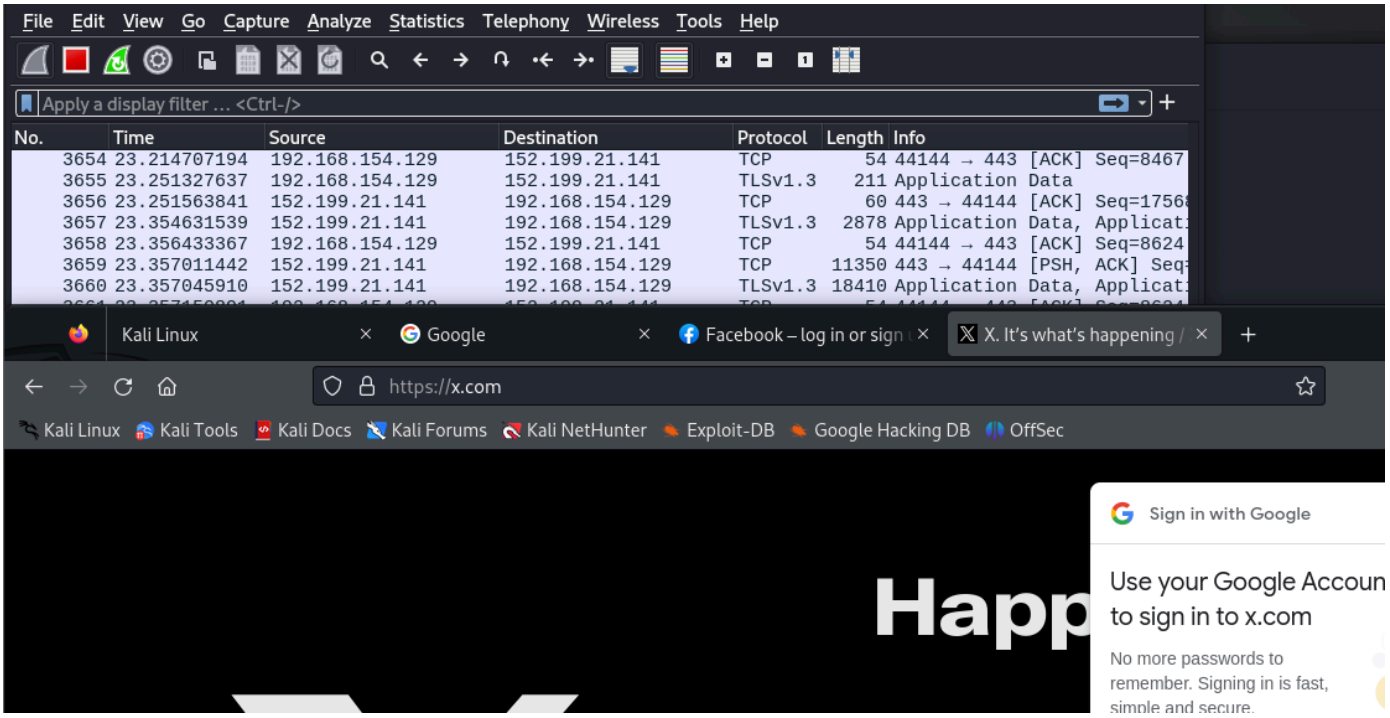
-I used the wireshark on my kali linux

-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 , faceebook.com and also twitter.com)

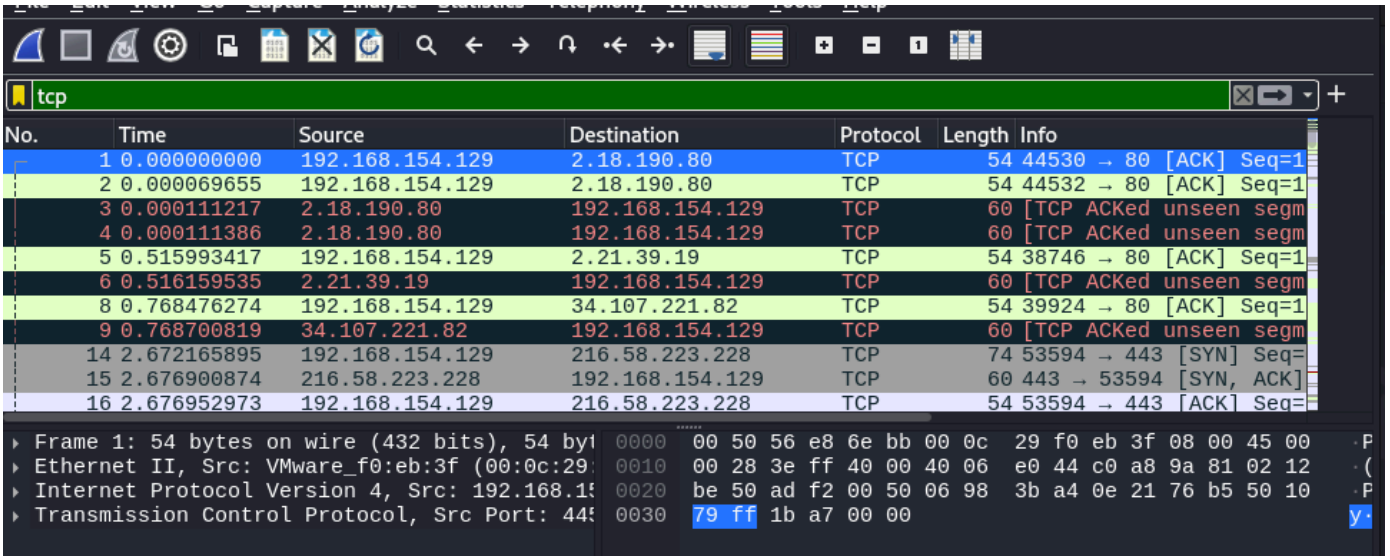
-my results and screenshots are displayed below



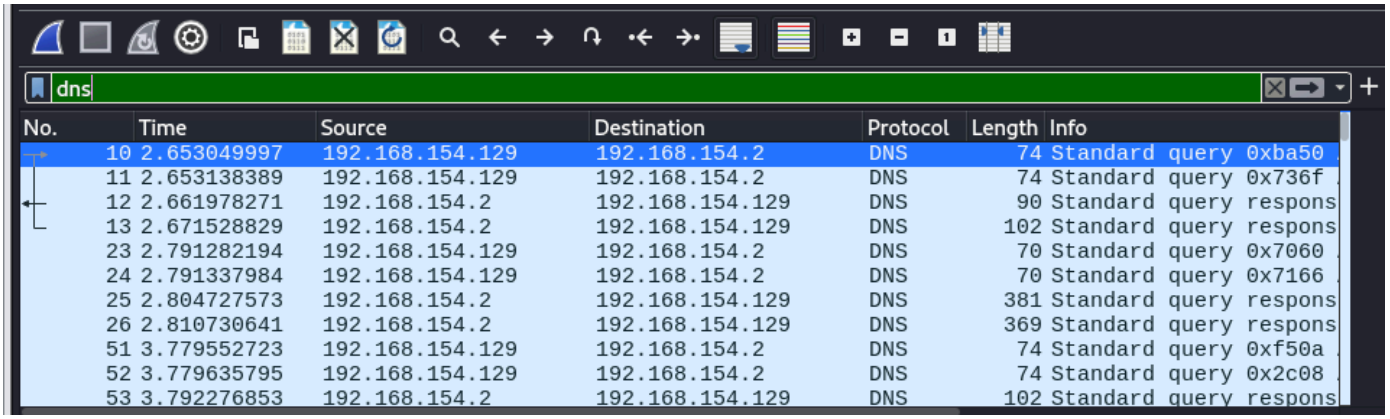
After visiting the website



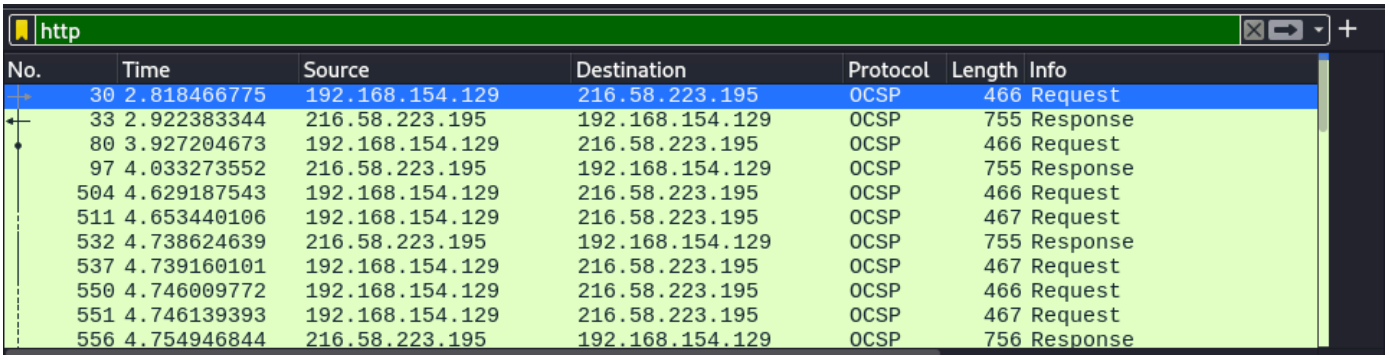
I inputed tcp in the filter button so as to see network traffic on the tcp protocol



I also filtered DNS traffic



I filtered HTTP traffic also



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

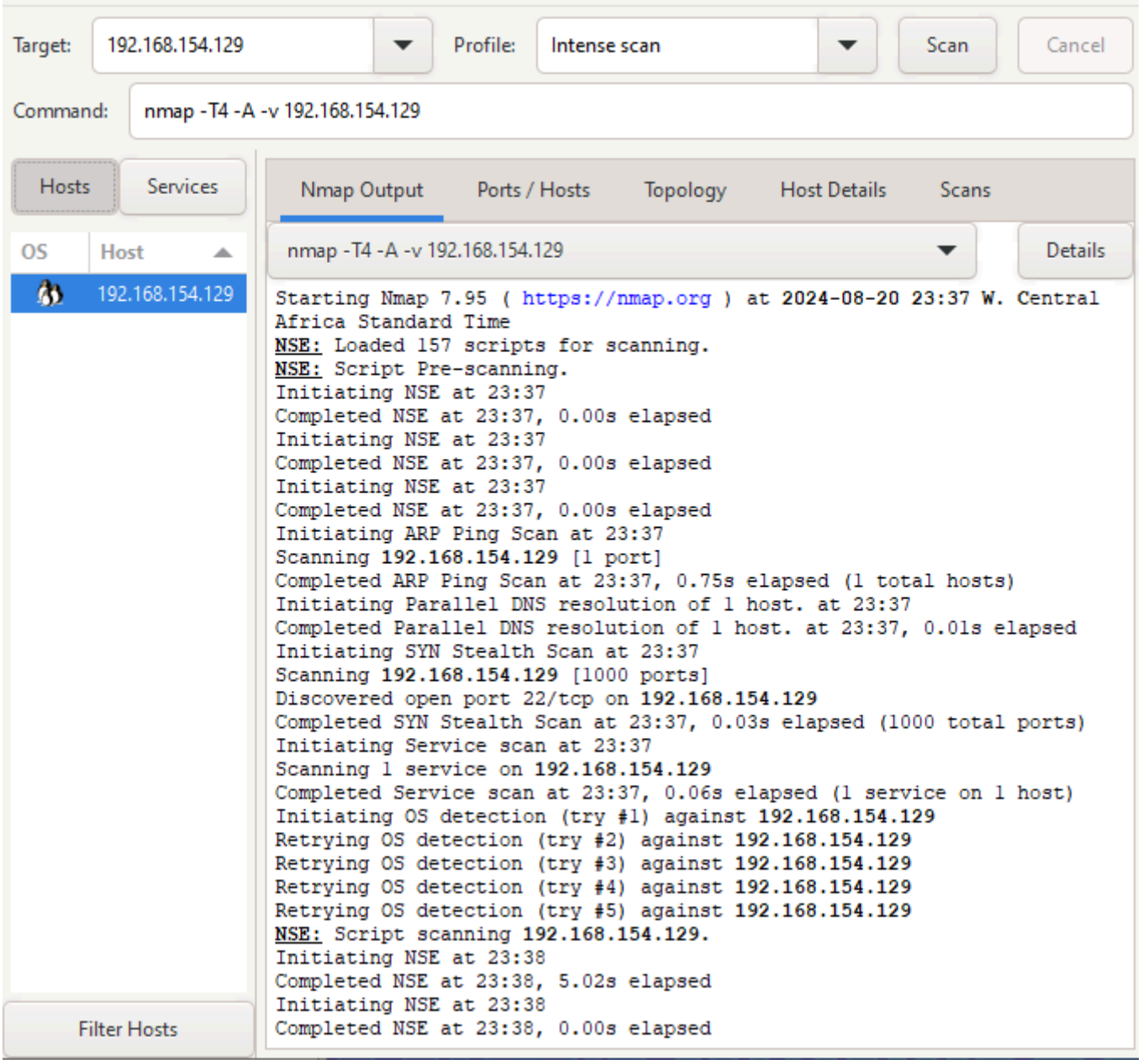
-DNS MONITORING- enable DNS logging so as to monitor suspicious DNS queries.

-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

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.154.129 Details

```
OS:=M5B4NN5NW7%CC=1%Q=)T1(R=1%DF=1%I=40%S=O%A=S+
%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