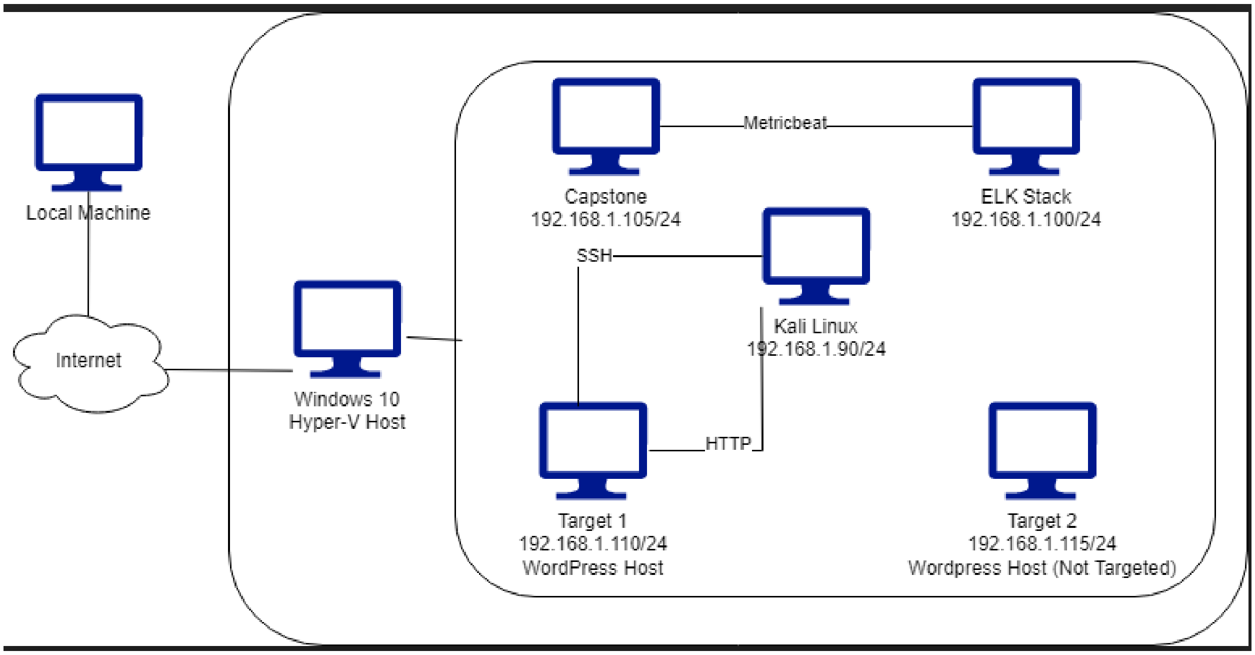
Blue Team: Summary of Operations

Table of Contents

Network Topology

TODO:



The following machines were identified on the network:

- Kali
  - **Operating** : Debian Kali 5.4.0
  - **Purpose**: Penetration Tester
  - **IP Address**: 192.168.1.90
- ELK
  - **Operating System**: Ubuntu 19.04
  - **Purpose**: The ELK Stack
  - **IP Address**: 192.168.1.100

- Capstone
  - **Operating:** Ubuntu 18.04
  - **Purpose:** The Vulnerable Web Server
  - **IP Address:** 192.168.1.105
- Target 1
  - **Operating:** Devian GNU/Linux
  - **Purpose:** The Vulnerable Web Server
  - **IP Address:** 192.168.1.110

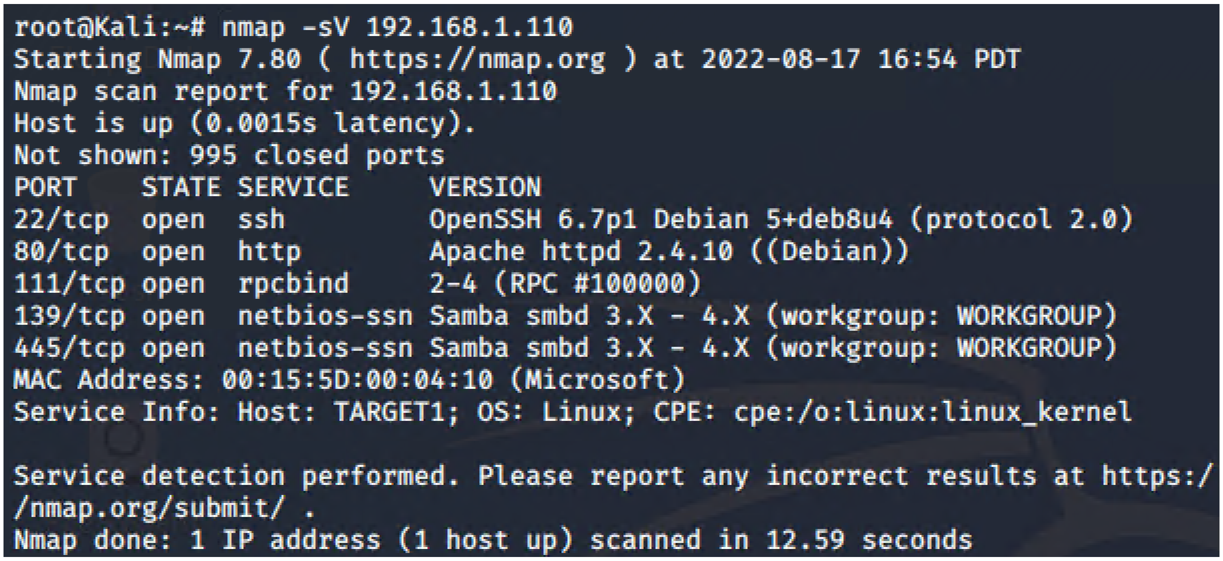
Description of Targets

- Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are ports of entry for attacks.
- We were able to exploit Target 1 (192.168.1.110)

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

HTTP Request

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:



```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-17 16:54 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0015s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.59 seconds
```

- **Metric**: WHEN count() GROUPED OVER top 5 ‘http.response.stats_code
- **Threshold**: IS ABOVE 400
- **Vulnerability Mitigated**: Enumeration/Brute Force
- **Reliability**: The alert is highly reliable. Measuring by error codes 400 and above should filter out any successful response. 400+ codes are client and servers errors which could be signs of a breach. Especially when in a high rate.

CPU Usage

Alert 2 is implemented as follows:

- **Metric**:When Max (). OF system.process.cpu.total.pct OVER all documents
- **Threshold**: IS ABOVE 0.5
- **Vulnerability Mitigated**: Malicious software, programs (malware or viruses) running taking up resources
- **Reliability**: Alert is highly reliable. Without malicious software this can still help monitor the CPU usage

Excessive HTTP Errors

Alert 3 is implemented as follows:

- **Metric**: When count () GROUPED OVER top 5 ‘http.response.status_code’ IS ABOVE 44 FOR THE LAST 5 minutes
- **Threshold**: Above 5 minutes
- **Vulnerability Mitigated**: Failed HTTP logins
- **Reliability**: Reliable showing how many failed HTTP logins within the past 5 minutes effective against brute attacks.