Capstone Engagement

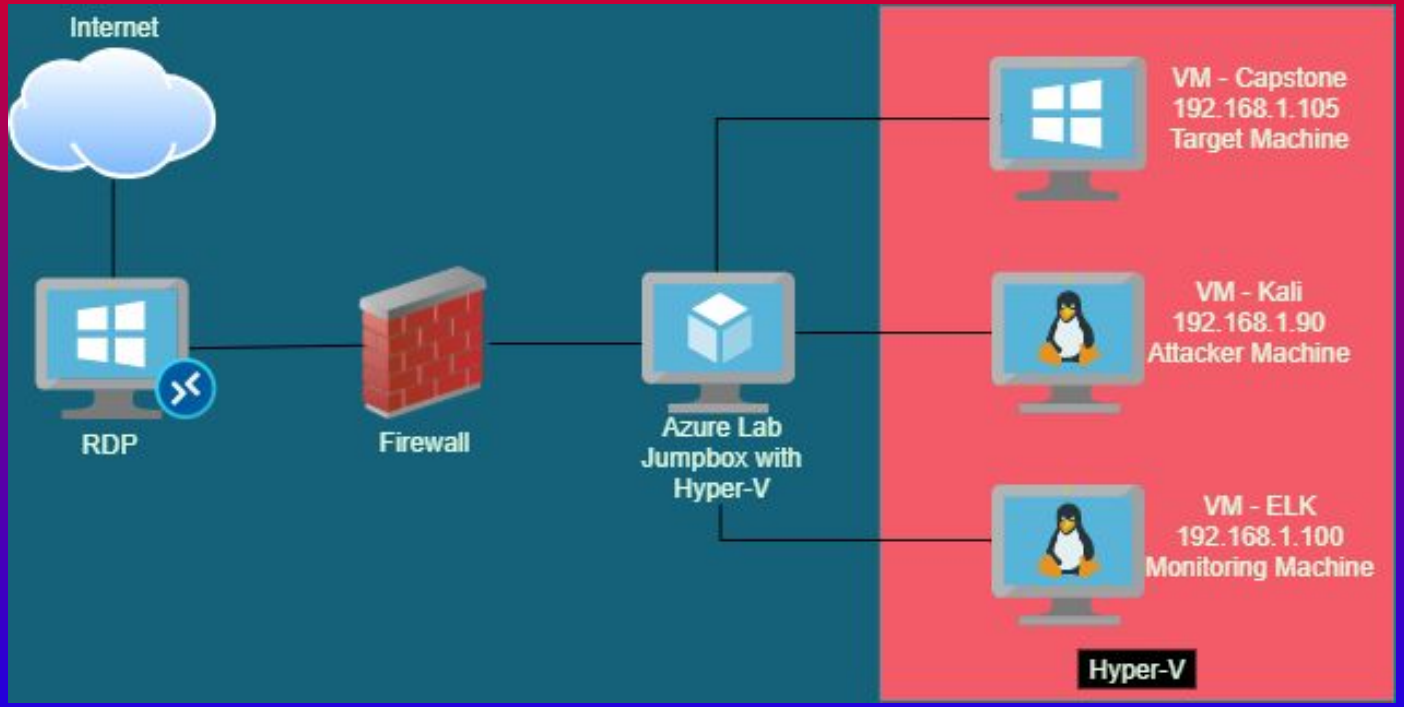
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network

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

Machines

IPv4: 192.168.1.105
OS: Windows
Hostname: Capstone

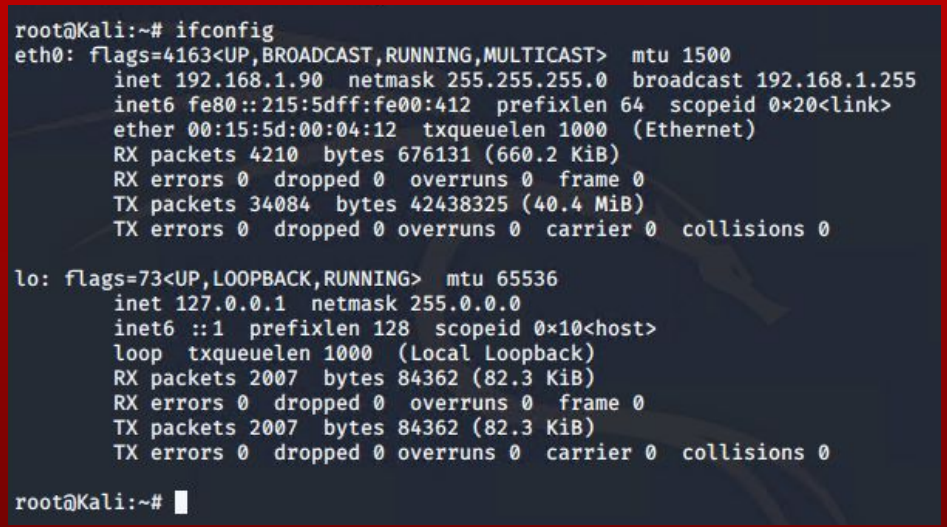
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

Red Team
Security Assessment

Recon: Network Discovery

- Our goal here is to gather information that will help us begin our attack.
- By running **ifconfig** on our Kali machine we will discover our ip address on the network along with the subnet.
- Using this information we can run various **Nmap scans** to determine other machines on the network, the services they are running, and the OS they are using.



Recon: Network Discovery

```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-10 16:51 PST
Nmap scan report for 192.168.1.1
Host is up (0.00049s 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 (0.0055s 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 (0.00058s 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 6.75 seconds
root@Kali:~#
```

```
root@Kali:~# nmap -sV 192.168.1.1-105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-16 15:09 PST
Nmap scan report for 192.168.1.1
Host is up (0.00044s 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)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00055s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00054s 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

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 105 IP addresses (4 hosts up) scanned in 29.68 seconds
root@Kali:~#
```

Recon: Identifying the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-REFVM-684427	192.168.1.1	Gateway
Capstone	192.168.1.105	Target Machine
Kali	192.168.1.90	Attacker Machine
ELK	192.168.1.100	Monitor Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Identification and Authentication Failure	There were no limitations on logins and weak passwords were used. Admin user ryan's password hash was exposed in a text file. Access to paths for login pages.	This vulnerability allowed for a brute force attack to crack the password for the given two admin level users
Unauthorized File Upload	There were no limitations on being able to upload arbitrary files on the server regardless of size or file type	This permitted external php scripts to be uploaded on the server
Remote Code Execution	The uploaded php script can be used to execute arbitrary shell commands	This vulnerability resulted in the attacker opening a reverse shell to the server
Browsable Web Directory	The web directory was found to be browsable which means anyone can view it's contents. Admin username 'ashton' openly exposed.	This vulnerability made it easy to narrow down which username to use for a brute force as well as revealing the path to admin folders

Exploitation: Identification and Authentication Failure

01

Tools & Processes

- Cracked password for admin user ashton using *hydra*
- Cracked hash for admin user ryan using crackstation.net

02

Achievements

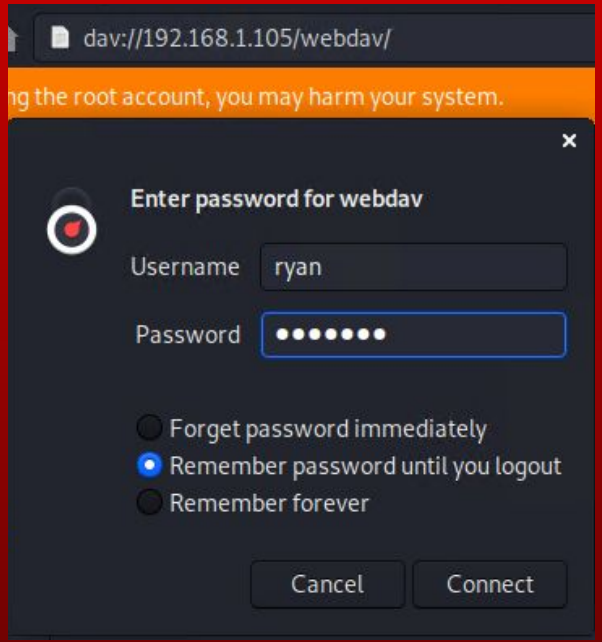
- Admin user ‘ryan’ password hash used to access target machine server via WebDav directory
- Admin user ‘ashton’ password cracked to access secret folder on web directory

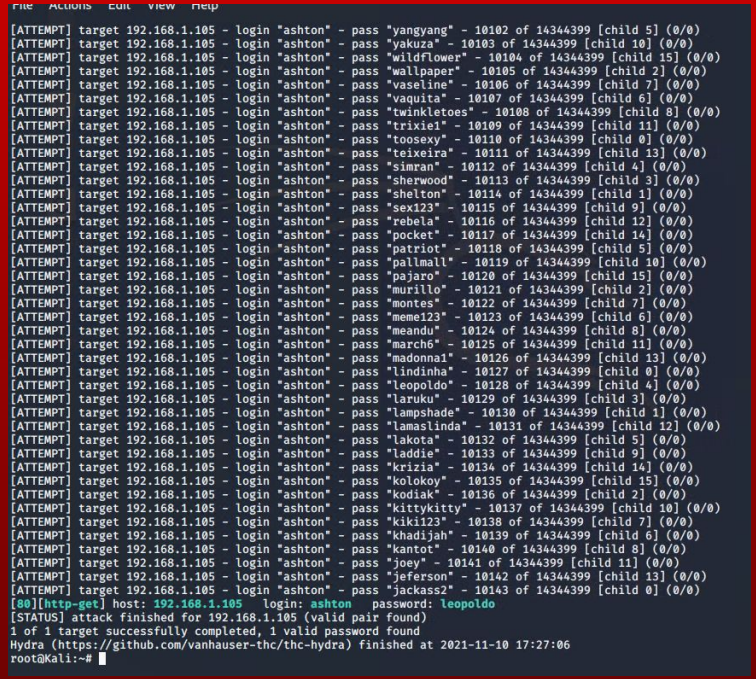
03

Screenshots

- Hydra
- Crackstation password hash cracking
- WebDav login

Screenshots: Identification and Authentication Failure





Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Exploitation: Unauthorized File Upload

01

Tools & Processes

- Hash crack credentials used to connect via WebDav
- Generated custom shell using msfvenom command
- Uploaded generated shell via WebDav

02

Achievements

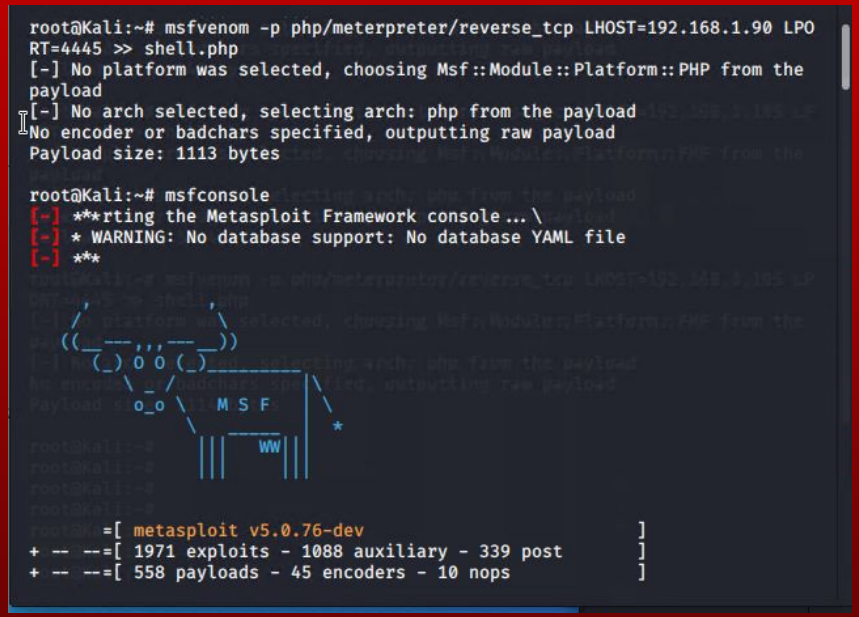
- Successfully uploaded shell as a means to gain access to executing arbitrary commands on the target machine

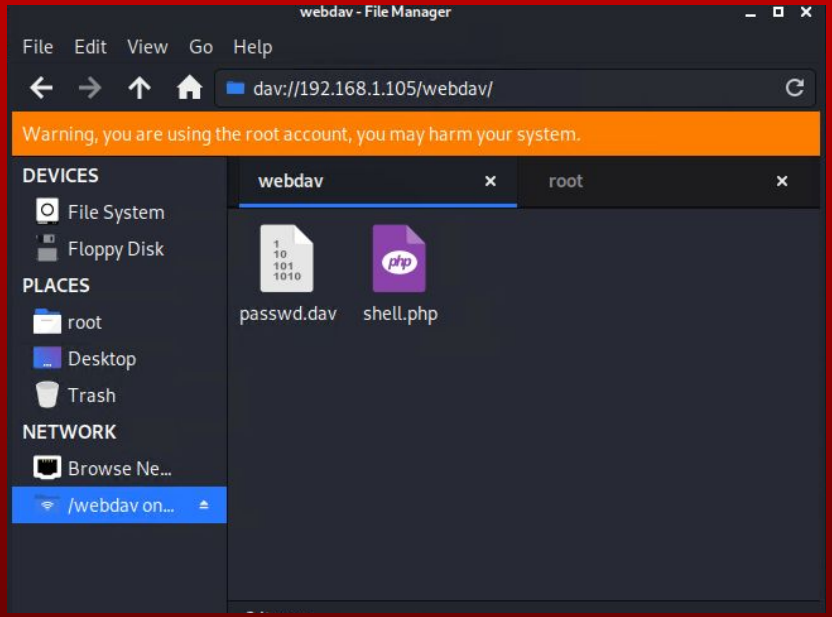
03

Screenshots

- Shell created using msfvenom
- Reverse shell upload

Screenshots: Unauthorized File Upload





Exploitation: Remote Code Execution

01

Tools & Processes

- Set up meterpreter listener using msfconsole
- Meterpreter used to connect to web shell that was uploaded
- Shell used to gain access to target machine and compromise data

02

Achievements

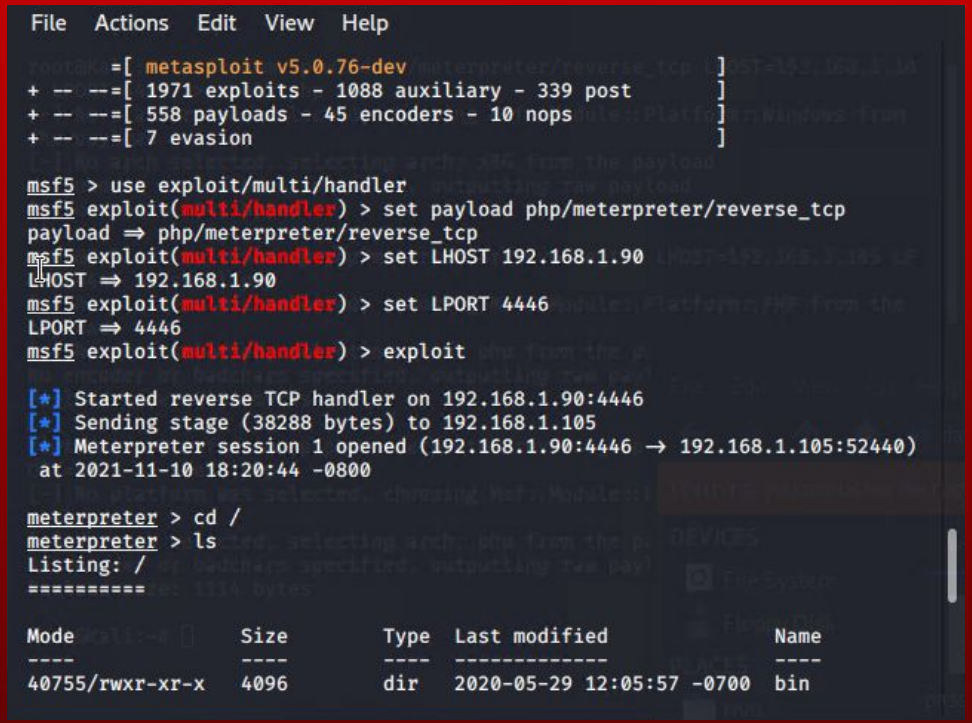
- Successfully executed reverse shell to target machine
- Gained access to full file system on target machine

03

Screenshot

- Meterpreter setup and successful session opened using reverse shell exploit

Screenshots: Remote Code Execution



Exploitation: Browsable Web Directory

01

Tools & Processes

- Web browser used to navigate
- Narrowed password cracking to just one user (ashton)
- Used browsable web directories to discover the secret_folder hidden directory

02

Achievements

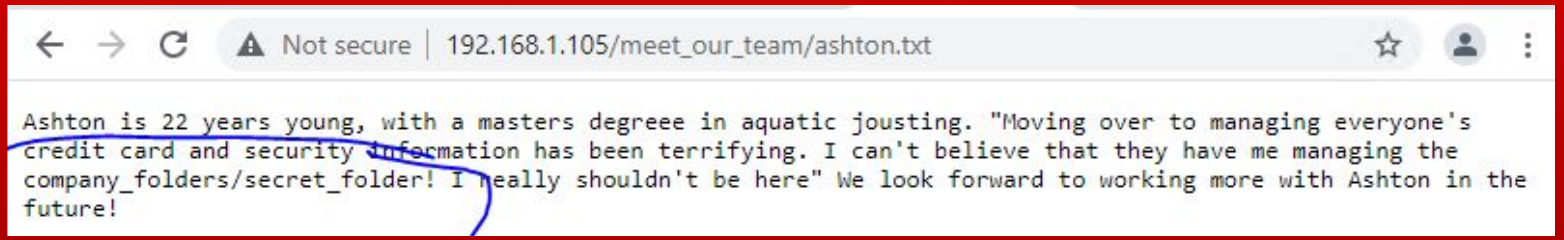
- Open paths to secret_folder and WebDav
- Easily identified paths to admin folders for file upload
- Directory paths openly listed on web server
- Admin ‘ashton’ username exposed

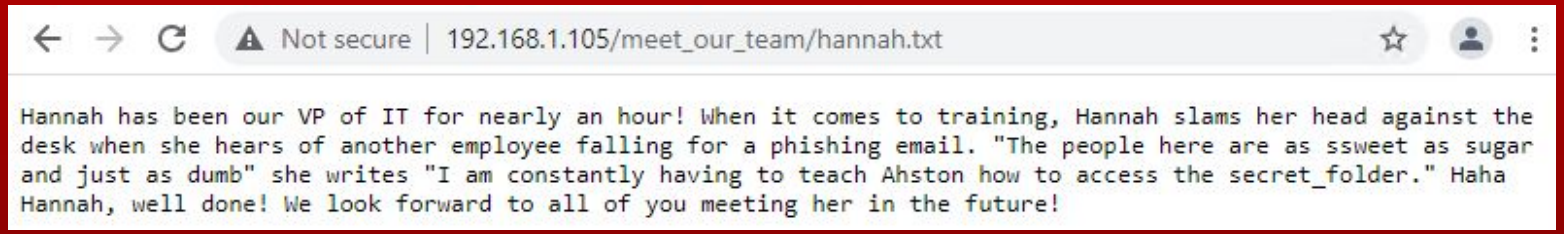
03

Screenshots

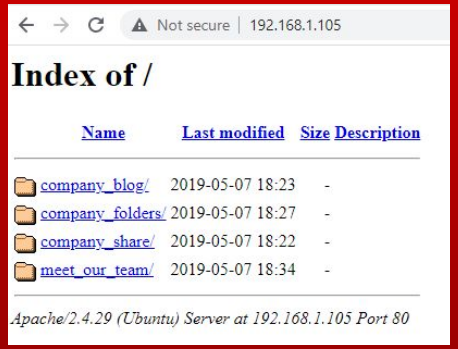
- Web server directory
- Secret_folder discussion
- Access to secret_folder
- Secret_folder contents

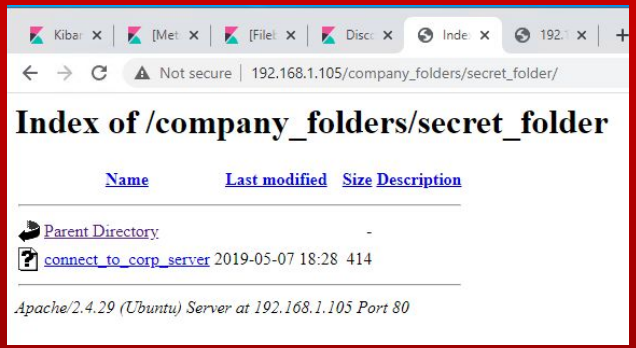
Screenshots: Browsable Web Directories

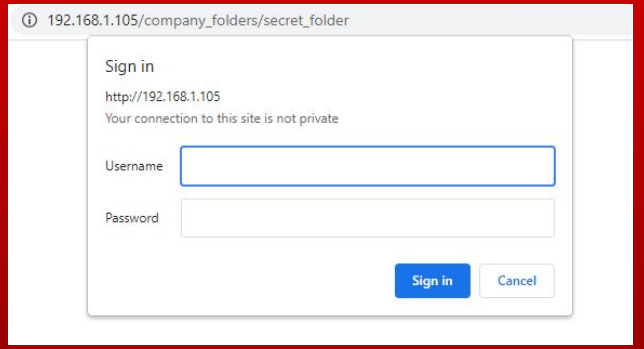


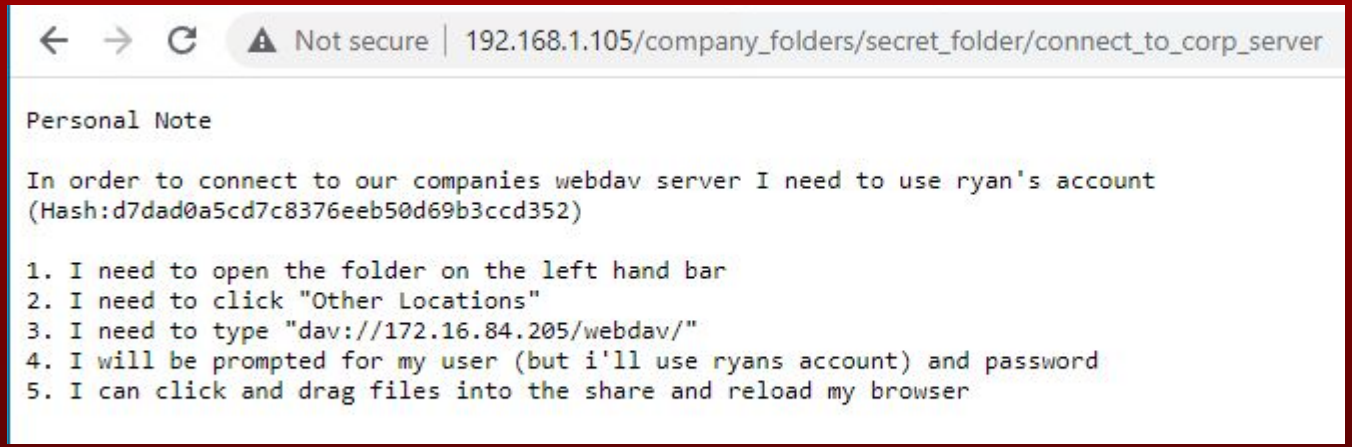


Screenshots: Browsable Web Directories







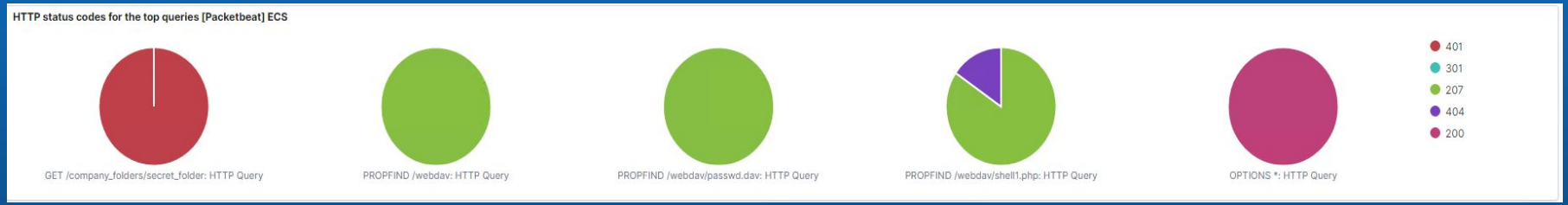


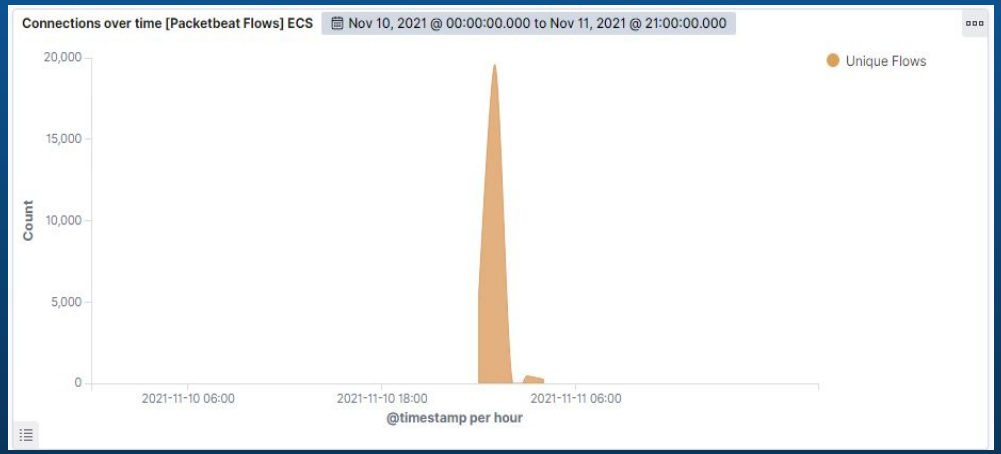
Blue Team

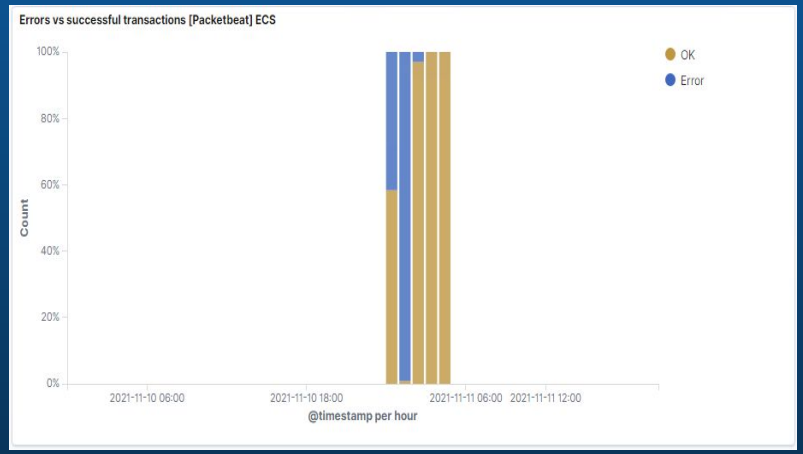
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur? *1:00 pm*
- How many packets were sent, and from which IP? *19,584 packets sent from the IP address 192.168.1.90*
- What indicates that this was a port scan? *The large volume of packets being sent to the network along with the HTTP status codes.*







Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? 1:05 pm
- How many requests were made? *15,621 requests were made for /company_folders/secret_folder directory from the IP address 192.168.1.90*
- Which files were requested? *We can see that the /webdav and /webdav/passwd.dav directories were also requested numerous times.*
- What did they contain? *These directories and the files inside them contained confidential data along with documentation of highly sensitive information involving company secrets. The information gathered in these directories played a huge role in the attack on the server.*

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,621
http://192.168.1.105/webdav	442
http://192.168.1.105/webdav/shell1.php	36
http://192.168.1.105/webdav/passwd.dav	33
http://192.168.1.105/	6

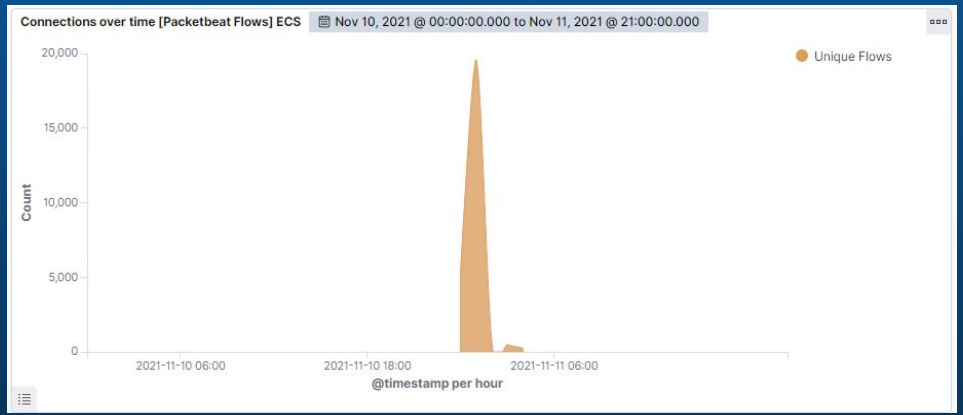
Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? *We can see that the password protected secret_folder was requested 15,621 times, but the file inside that directory was only requested 3 times. So, out of 15,621 requests, only 3 were successful.*
- How many requests had been made before the attacker discovered the password? *15,618 requests had been made using hydra before the password was discovered. As you can see below the large spike in connections from the hydra attack*

http://192.168.1.105/company_folders/secret_folder	15,621

http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	3

server.ip	192.168.1.105
server.port	80
source.bytes	163B
source.ip	192.168.1.90
source.port	42000
status	Error
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder
url.path	/company_folders/secret_folder
url.scheme	http
user_agent.original	Mozilla/4.0 (Hydra)



Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 442 requests were made for the /webdav directory.

- Which files were requested? *We can see the passwd.dav file was requested as well as a file named shell1.php.*

  In this case the /webdav/shell1.php happens to be the reverse shell we uploaded to the server during the attack.

http://192.168.1.105/webdav	442
http://192.168.1.105/webdav/shell1.php	36
http://192.168.1.105/webdav/passwd.dav	33
http://192.168.1.105/	6

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- An alarm can be set to notify the security analyst when numerous ports are scanned from the same IP address in a short period of time
- An example of an appropriate threshold could be 10 requests per second for more than 5 seconds. Also, 4 or more ports scanned over 200 seconds.

System Hardening

- A firewall may be set to keep ports closed when they are not in use and whitelist certain IP addresses on the network
- Port forwarding can be used to redirect open ports to a new port or empty host, which makes the scanning process more difficult for the attacker

Mitigation: Finding the Request for the Hidden Directory

Alarm

- An alarm that notifies the security analyst when the path to the secret_folder directory is accessed from an IP address that does not have authorized access.
- An example of an appropriate threshold could be any occurrence greater than 0 from an external IP address

System Hardening

- Remove the information about how to access the secret_folder directory. Changing the name of the directory so it is less obvious and installing a proper html index page will be beneficial as well.
- Modify which IPs can access the secret_folder directory via the /var/www/ folder on the network

Mitigation: Preventing Brute Force Attacks

Alarm

- Notify security analyst any time ‘hydra’ command is used and there are multiple failed login attempts
- An example of an appropriate threshold could be if set to notify on any attempts greater than 5 logins in one minute. Also notify when an external or non-trusted IP address has a success code (200)

System Hardening

- Implement a strong password policy and add incremental delays on logins following every failed attempt
- Utilize a CAPTCHA to filter out ‘bot’ activity
- Implement 2 factor authentication

Mitigation: Detecting the WebDAV Connection

Alarm

- Notify security analyst when an external IP address attempts to access Webdav (>0 attempts)
- Splunk advanced machine learning capabilities can be used to detect out-of-ordinary patterns and trigger an alert based on previous ‘normal’ activities

System Hardening

- Limiting access can be done by restricting access to only select admin IP addresses and blocking all other external IPs. Utilize authentication for each login. Also, configure filebeat on the host
- Enforce a strong password policy and use SSH keys for connection authentication. Install filebeat.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Notify the security analyst for any ‘post’ request that is made that is made from an external non-trusted IP address (>0).
- Alarm should fire for any upload of a forbidden file (eg. .php) greater than 0 occurrences.

System Hardening

- Restrict permissions to admins only.
- Install and configure filebeat
- Limit write privileges to admins only
- Modify allowed IPs in /var/www for a target folder (eg. webdav).


The End