Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Taney Aaron Paul
Red VS Blue Project

Table of Contents

This document contains the following sections:

01 **Network Topology**

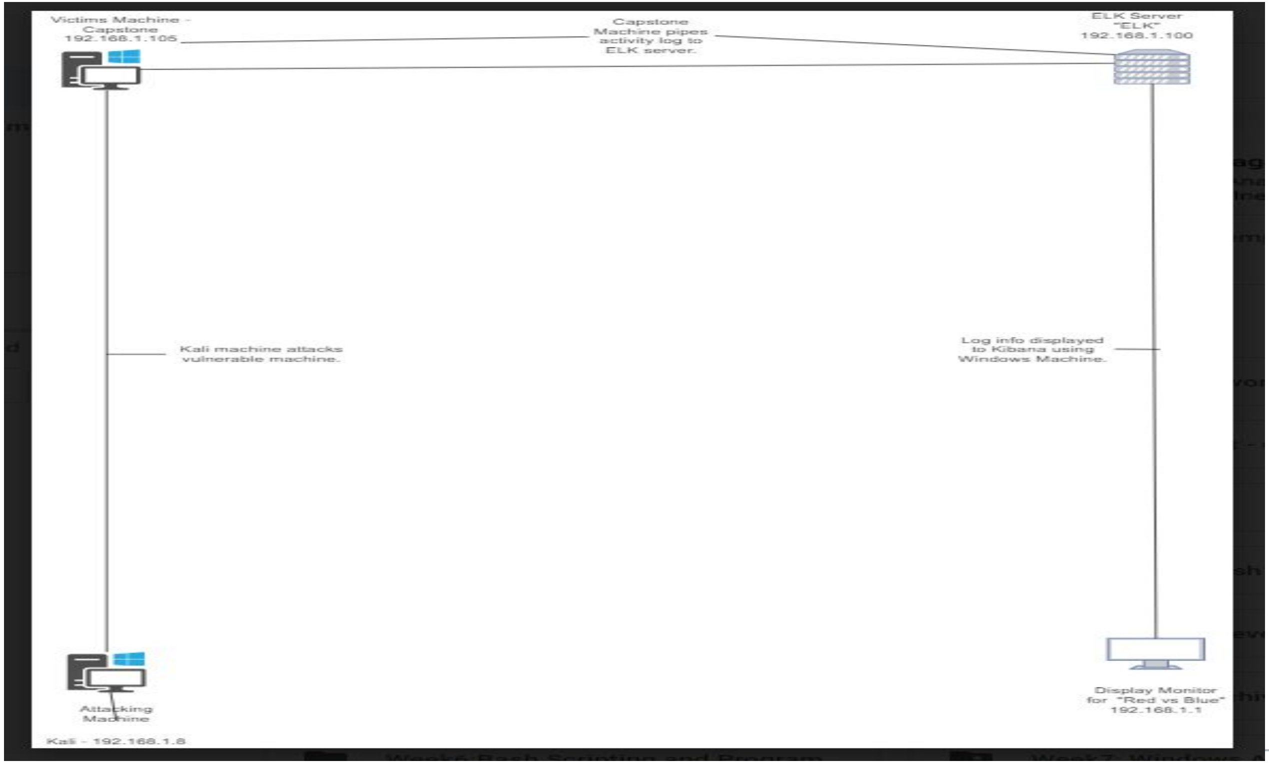
02 **Red Team**: Security Assessment

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
IPv4:192.168.1.8
OS:Linux ver 4.18.0
Hostname:Kali

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

IPv4:192.168.1.100
OS:Linux
Hostname:ELK

IPv4:192.168.1.1
OS:WIndows
Hostname:Red VS Blue

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red VS Blue	192.168.1.1	Virtual machine which was where we viewed the log data from.
Kali	192.168.1.8	Attacking Machine
ELK	192.168.1.100	Machine which logs activity data from Capstone machine.
Capstone	192.168.1.105	Vulnerable victim machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80	*An open port can allow an attacker on 80 gain access to information that would potentially be private.*	*It let the red team find files with useful info on the blue team database.*
Accessible Files	Accessible files can give access to the root user.	Red team was able to access company IP on port 80 thru the web browser. This gave them the chance to get ahold of user names and access to hidden sub-directories.
Brute Force Password	If a password can be guessed easily one could use a wordlist such as rockyou.txt to hack the password.	It let us on red team brute force the password with Hydra for user Ashton, the password leopoldo allowed us access hidden files.
Hashed Password	The hashed password was cracked thru the use of the Crackstation website.	Red team was able to use crackstation to identify the password for Ryan and the

01

Tools & Processes
Red team used NMAP to scan for open port on the companies IP.

02

Achievements
It allowed us to access the company IP @ 192.168.1.105 on port 80 which also allowed access to see a hidden directory that had sensitive information.

03

NMAP screenshot below...

Exploitation: Accessible Files

01

Tools & Processes
We used open port 80 to view important info with the web browser.

02

Achievements
Access to these files gave us ability to see which users would have privileged info and access to the secret_folder.

03

Screenshots above and below.

01

Tools & Processes
We used the Hydra tool to brute force Ashton’s password.

02

Achievements
The exploit gave us access to secret_folder on the targets database and revealed a hash for Ryans password.

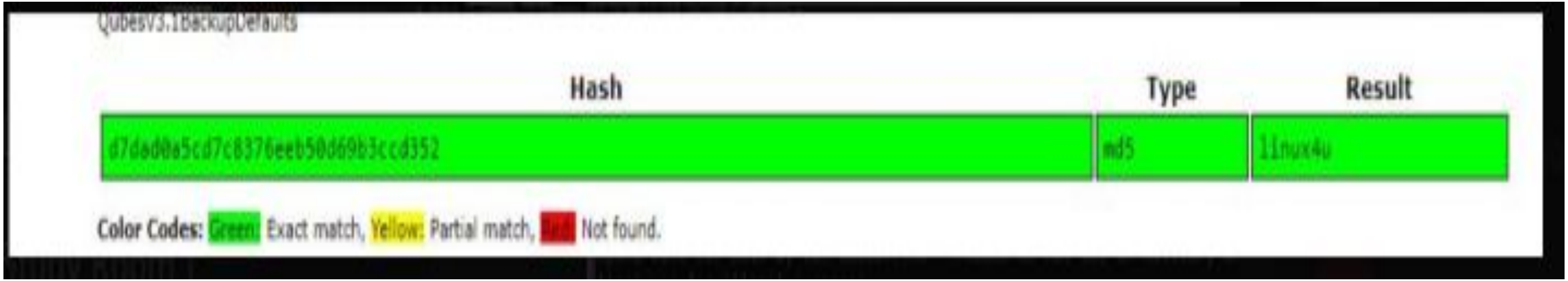
03

The screenshots are above and below.

Exploitation: Hashed Password

01

Tools & Processes:
We used the website Crackstation to find the text of the hashed password for Ryan.



QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

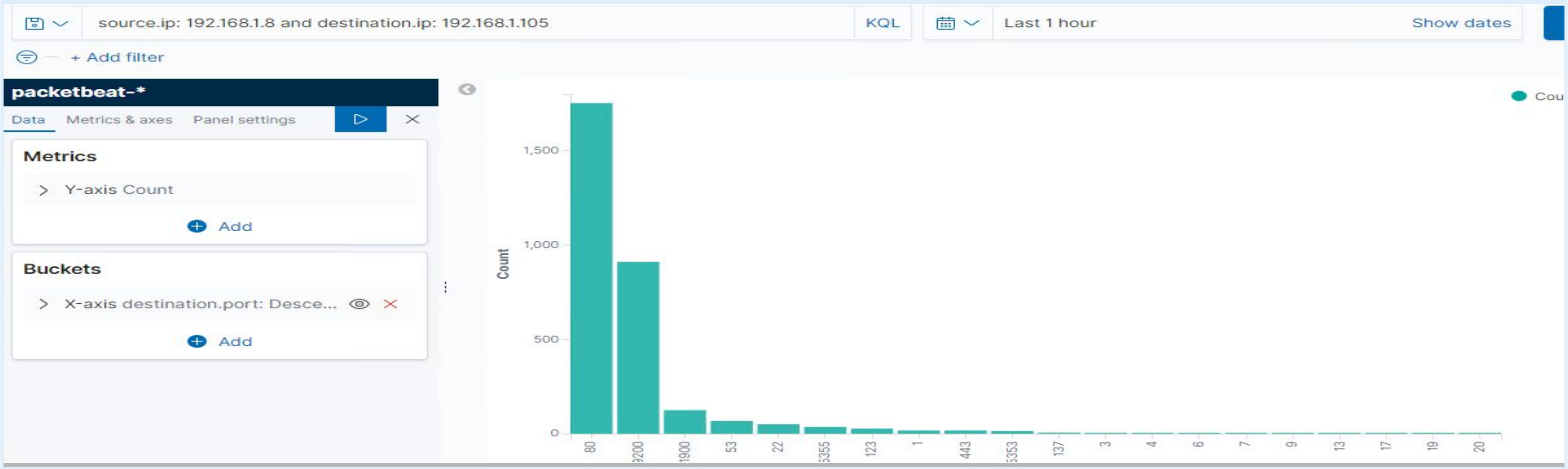
Blue Team

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?



source.ip: 192.168.1.8 and destination.ip: 192.168.1.105

Last 1 hour

packetbeat-*

Metrics

Y-axis Count

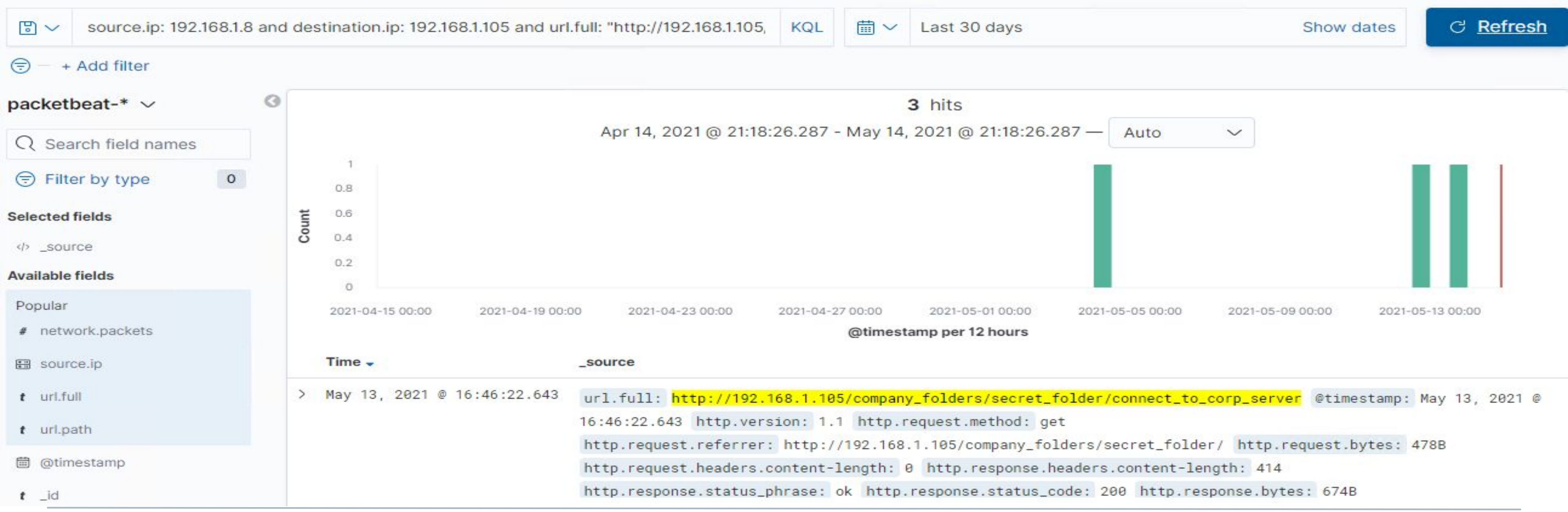
Buckets

X-axis destination.port: Desce...

- The port scan occurred @ 19:00 hours
- Eleven packets were sent from IP 192.168.1.8
- The field showing that multiple ports were scanned in almost a consecutive order and they were hit at the same time.

Analysis: Finding the Request for the Hidden Directory

May 13th @ 16:46 requests for the hidden directory occurred. One file was accessed containing the info on how to access the hidden folder and it also had the hash for Ryans password.



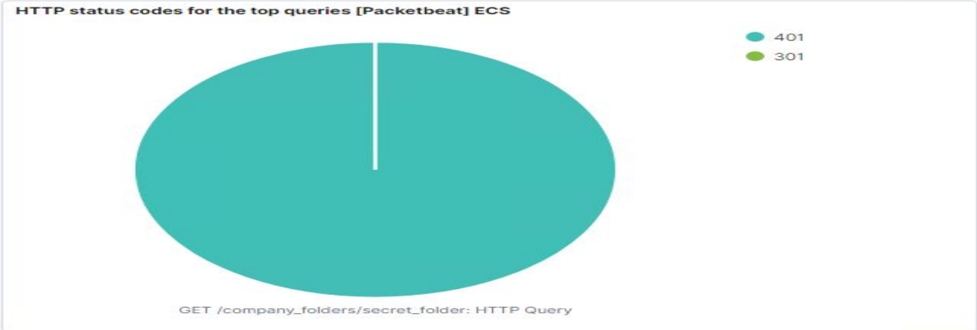
```
source.ip: 192.168.1.8 and destination.ip: 192.168.1.105 and url.full: "http://192.168.1.105,
```

```
May 13, 2021 @ 16:46:22.643   url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server @timestamp: May 13, 2021 @
                              16:46:22.643 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 http.response.headers.content-length: 414
                              http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 674B
```

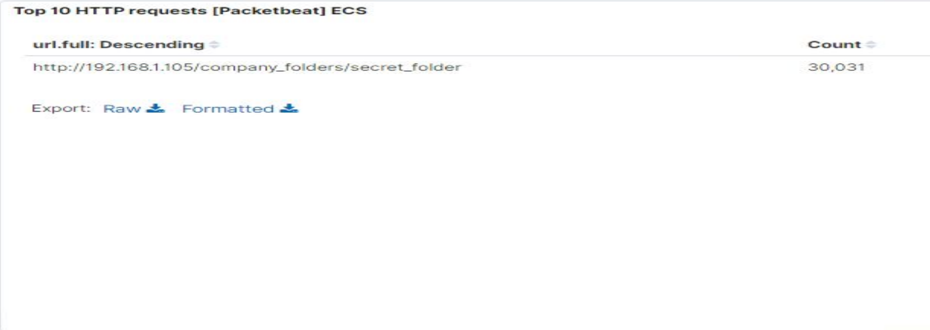
Analysis: Uncovering the Brute Force Attack

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

- 30,031 requests were made in the attack.

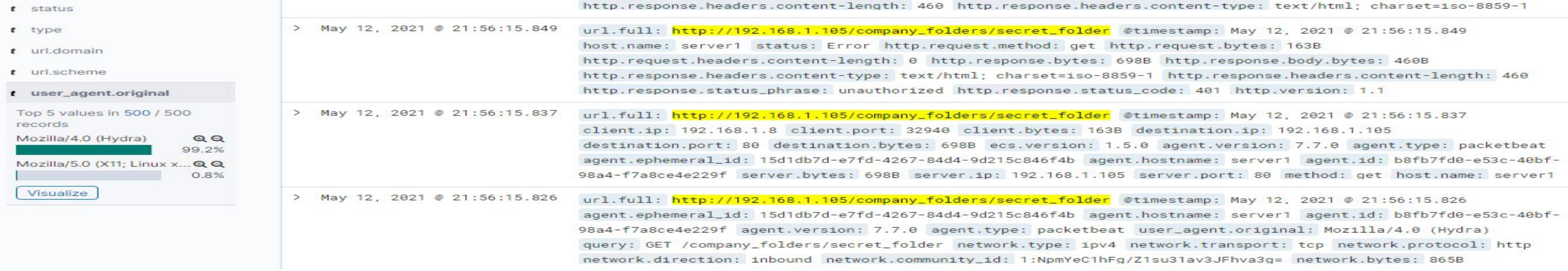


HTTP status codes for the top queries [Packetbeat] ECS



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	30,031



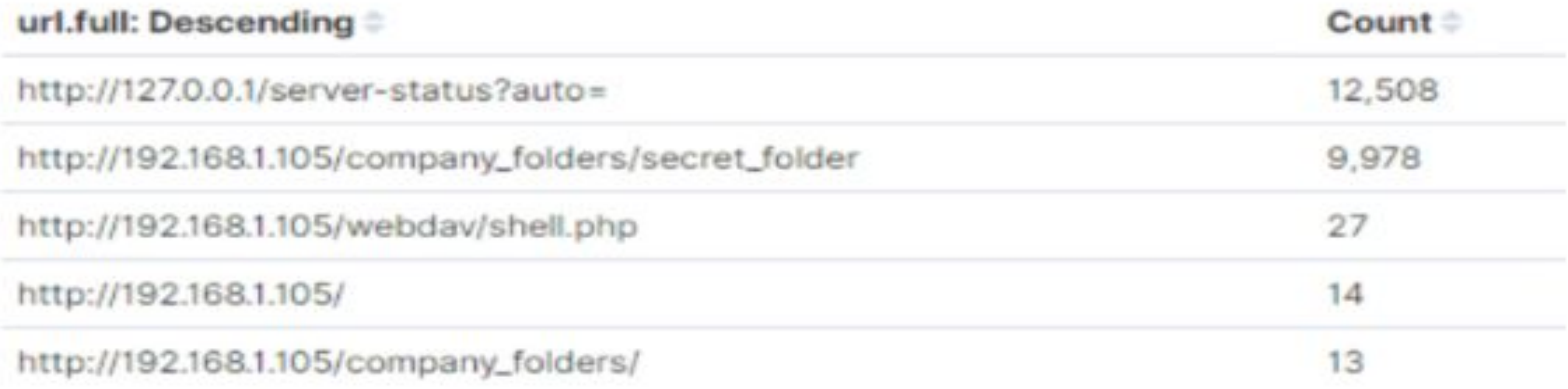
Mozilla/4.0 (Hydra)	99.2%
Mozilla/5.0 (X11; Linux x...	0.8%

```
  http.response.headers.content-length: 460  http.response.headers.content-type: text/html; charset=iso-8859-1

> May 12, 2021 @ 21:56:15.849   url.full: http://192.168.1.105/company_folders/secret_folder  @timestamp: May 12, 2021 @ 21:56:15.849
                                host.name: server1  status: Error  http.request.method: get  http.request.bytes: 163B
                                http.request.headers.content-length: 0  http.response.bytes: 698B  http.response.body.bytes: 460B
                                http.response.headers.content-type: text/html; charset=iso-8859-1  http.response.headers.content-length: 460
                                http.response.status_phrase: unauthorized  http.response.status_code: 401  http.version: 1.1

> May 12, 2021 @ 21:56:15.837   url.full: http://192.168.1.105/company_folders/secret_folder  @timestamp: May 12, 2021 @ 21:56:15.837
                                client.ip: 192.168.1.8  client.port: 32940  client.bytes: 163B  destination.ip: 192.168.1.105
                                destination.port: 80  destination.bytes: 698B  ecs.version: 1.5.0  agent.version: 7.7.0  agent.type: packetbeat
                                agent.ephemeral_id: 15d1db7d-e7fd-4267-84d4-9d215c846f4b  agent.hostname: server1  agent.id: b8fb7fd0-e53c-40bf-
                               98a4-f7a8ce4e229f  server.bytes: 698B  server.ip: 192.168.1.105  server.port: 80  method: get  host.name: server1

> May 12, 2021 @ 21:56:15.826   url.full: http://192.168.1.105/company_folders/secret_folder  @timestamp: May 12, 2021 @ 21:56:15.826
                                agent.ephemeral_id: 15d1db7d-e7fd-4267-84d4-9d215c846f4b  agent.hostname: server1  agent.id: b8fb7fd0-e53c-40bf-
                               98a4-f7a8ce4e229f  agent.version: 7.7.0  agent.type: packetbeat  user_agent.original: Mozilla/4.0 (Hydra)
                                query: GET /company_folders/secret_folder  network.type: ipv4  network.transport: tcp  network.protocol: http
                                network.direction: inbound  network.community_id: 1:NpmYeC1hFg/Z1su31av3JFhva3g=  network.bytes: 865B
```

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.

- 27 requests were made to this directory.
- The shell.php file was requested and this is their direct attempt to upload a reverse shell to the target machine to start a listener.



url.full: Descending	Count
http://127.0.0.1/server-status?auto=	12,508
http://192.168.1.105/company_folders/secret_folder	9,978
http://192.168.1.105/webdav/shell.php	27
http://192.168.1.105/	14
http://192.168.1.105/company_folders/	13

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 that triggers for any traffic requested on anything other than port 80.**

What threshold would you set to activate this alarm?**The ports other than 80 would need a single request to trigger the alarm response.**

System Hardening

What configurations can be set on the host to mitigate port scans?
Eliminate server responses to requests on anything but port 80.

Describe the solution. If possible, provide required command lines. **Request port blocking on all ports except 80.**

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Block any kind of remote traffic to company directories on port 80.

What threshold would you set to activate this alarm?
Any kind of successful external access to directories would trigger and alert for security team.

System Hardening

What configuration can be set on the host to block unwanted access?
Blocking any kind of remote access to company folders not critical for basic port 80 operations.

Describe the solution. If possible, provide required command lines. **Remove access to specific directories excluding those with specific security approved IP address or those that have been whitelisted.**

Mitigation: Preventing Brute Force Attacks

Alarm

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

An alarm indicating multiple login attempts from the same IP in a small amount of time.

What threshold would you set to activate this alarm? **An alarm that would activate if more than 10 failed login attempts were performed in less than 10 seconds.**

System Hardening

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

Use of CAPTCHA and the requirement to answer a security question upon multiple attempts.

Dual authentication and also account lockout upon more than 5 login attempts in 5 minutes.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Create an alert that anytime this machine is accessed by a machine other than the ones intended to have permission to do so, For example employ the usage if Whitelisting IP addresses.

What threshold would you set to activate this alarm?

The threshold would be no more than one

System Hardening

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

Inhibit access to this folder from IP's other than internal company IP's.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads? **Setting up an alert for traffic on port 4444.**

Setting up an alert for any .php file thats uploaded.

What threshold would you set to activate this alarm? **The threshold will be more than 1 attempt.**

System Hardening

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

Inhibit access to the shared folder from the web interface.

Take away the option to upload files to this directory on web browser.

The End