



# **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

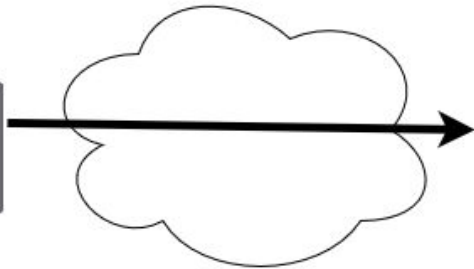
**Hardening:** Proposed Alarms and Mitigation Strategies

---

# Network Topology

# Network Topology

**Kali Box (Red Team)**  
192.168.1.8



**Capstone (Target)**  
192.168.1.105



**ELK stack Server**  
192.168.1.100

## Network

Address Range:  
192.168.1.0-255  
Netmask: 255.255.255.0  
Gateway: 0.0.0.0

## Machines

IPv4: 192.168.1.8  
OS: Linux 3.2-4.9  
Hostname: root

IPv4: 192.168.1.105  
OS: Linux 3.2-4.9  
Hostname: root

IPv4: 192.168.1.100  
OS: Linux 3.2-4.9  
Hostname: root

The background of the slide is a dark red, almost black, field filled with a complex, repeating geometric pattern of triangles and polygons in various shades of red and maroon, creating a textured, mosaic-like effect.

# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Windows machine	192.168.1.1	General purpose
ELK	192.168.1.100	ELK server (security monitoring)
Capstone	192.168.1.105	General purpose -- Apache server
Kali	192.168.1.8	Security -- Penetration testing

---

# Vulnerability Assessment

---

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port/service scanning	Enabled scanning of ports and active services.	Allows attackers to view potentially vulnerable services and vectors for exploitation.
Weak credentials	Credentials that are easily guessable or can be obtained through automation.	Allows for attackers to more quickly find login information to obtain info or perform other tasks.
Unlimited login attempts	No action taken by the SIEM to limit the number of failed logins.	Allows for brute force attacking by leaving user accounts open to multiple attempted logins.
Published administrative information to the public server	Information to log into the 'webdav' system folder along with user password has	Allows for direct access to modify server and/or obtain highly sensitive company information.

---

# Exploitation: Port scanning

---

01

## Tools & Processes

Simple pinging and NMAP scanning allowed for the discovery of vulnerable services, specifically the older version of Apache web server and website structure.

02

## Achievements

With this information, I was able to more easily traverse the website structure and find the vulnerable Apache software, leading me to place the reverse shell on the site.

03

See next slide for screenshot.



# Exploitation: Port scanning

```
root@kali:~# nmap -A 192.168.1.105
Starting Nmap 7.70 ( https://nmap.org ) at 2021-07-01 05:28 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00059s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256  c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256  b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29
|_ http-ls: Volume /
|   maxfiles limit reached (10)
|   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
|_
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Index of /
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.59 ms  192.168.1.105

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.41 seconds
```

# Exploitation: Weak credentials

---

01

## Tools & Processes

Using Hydra tool, I was able to brute force multiple login attempts with a simple wordlist for the 'ashton' user account.

02

## Achievements

Upon finding the successful password combination, I was able to get into the company "secret folder" containing important credential information for administrative access to the server (see also Exploitation 4).

03

See next slide for screenshot.

# Exploitation: Weak credentials

---

```
[80][http-get] host: 192.168.1.105  login: ashton  password: leopoldo  
[STATUS] attack finished for 192.168.1.105 (valid pair found)
```

# Exploitation: Unlimited login attempts

---

01

## Tools & Processes

Again, with the Hydra tool, the brute force attack was able to occur with over 10,000 login attempts without any impedance.

02

## Achievements

Able to access the the 'ashton' account which has access to the company "secret folder". However, theoretically I would be able to log into almost any account if the passwords were weak enough and/or I utilized a more complex wordlist.

03

See next slide for screenshot.

# Exploitation: Unlimited login attempts

---

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 5] (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 15] (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)
```

Note the number of login attempts before the password was found for the ashton account.

---

# Exploitation: Published administrative information to the public server

---

01

## Tools & Processes

Using crackstation, I was able to decrypt the hashed password of user account 'ryan' and gain access to the WebDAV folders for the server. Afterwards, MSFVenom and MSFConsole were used to establish a reverse shell on the server.

02

## Achievements

Upon logging into the WebDAV system, I was able to find a password to SSH into the server itself while also uploading a reverse shell script to the server.

03

See following slides for screenshots of process.


# Exploitation: Published administrative information to the public server

---

# Exploitation: Published administrative information to the public server

---





# **Blue Team**

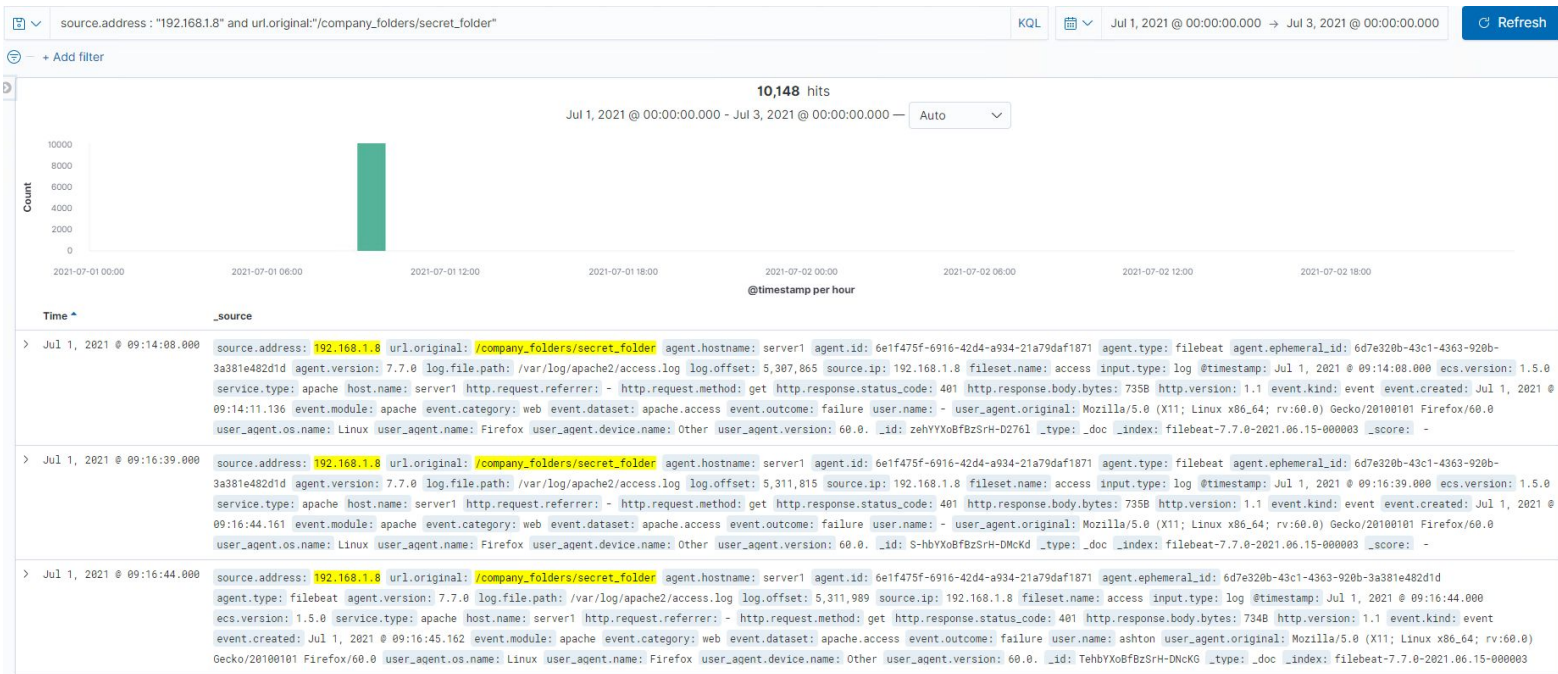
## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

Time	_source
> Jul 1, 2021 @ 08:59:26.000	source.address: 192.168.1.8 user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) agent.hostname: server1 agent.id: 6e1f475f-6916-42d4-a934-21a79daf1871 agent.type: filebeat agent.ephemeral_id: 6d7e320b-43c1-4363-920b-3a381e482d1d agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 1,765,343 source.ip: 192.168.1.8 fileset.name: access url.original: /sdk input.type: log @timestamp: Jul 1, 2021 @ 08:59:26.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: - http.request.method: post http.response.status_code: 404 http.response.body.bytes: 4608 http.version: 1.1 event.kind: event event.created: Jul 1, 2021 @ 08:59:27.706 event.module: apache event.category: web event.dataset: apache.access event.outcome: failure user.name: -
> Jul 1, 2021 @ 08:59:26.000	source.address: 192.168.1.8 user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) agent.hostname: server1 agent.id: 6e1f475f-6916-42d4-a934-21a79daf1871 agent.type: filebeat agent.ephemeral_id: 6d7e320b-43c1-4363-920b-3a381e482d1d agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 1,765,503 source.ip: 192.168.1.8 fileset.name: access url.original: /nmaplowercheck1625129966 input.type: log @timestamp: Jul 1, 2021 @ 08:59:26.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: - http.request.method: get http.response.status_code: 404 http.response.body.bytes: 481B http.version: 1.1 event.kind: event event.created: Jul 1, 2021 @ 08:59:27.706 event.module: apache event.category: web event.dataset: apache.access event.outcome: failure user.name: -
> Jul 1, 2021 @ 08:59:26.000	source.address: 192.168.1.8 user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) agent.hostname: server1 agent.id: 6e1f475f-6916-42d4-a934-21a79daf1871 agent.type: filebeat agent.ephemeral_id: 6d7e320b-43c1-4363-920b-3a381e482d1d agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 1,765,683 source.ip: 192.168.1.8 fileset.name: access url.original: / input.type: log @timestamp: Jul 1, 2021 @ 08:59:26.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: - http.request.method: post http.response.status_code: 404 http.response.body.bytes: 457B http.version: 1.1 event.kind: event event.created: Jul 1, 2021 @ 08:59:27.706 event.module: apache event.category: web event.dataset: apache.access event.outcome: failure user.name: -

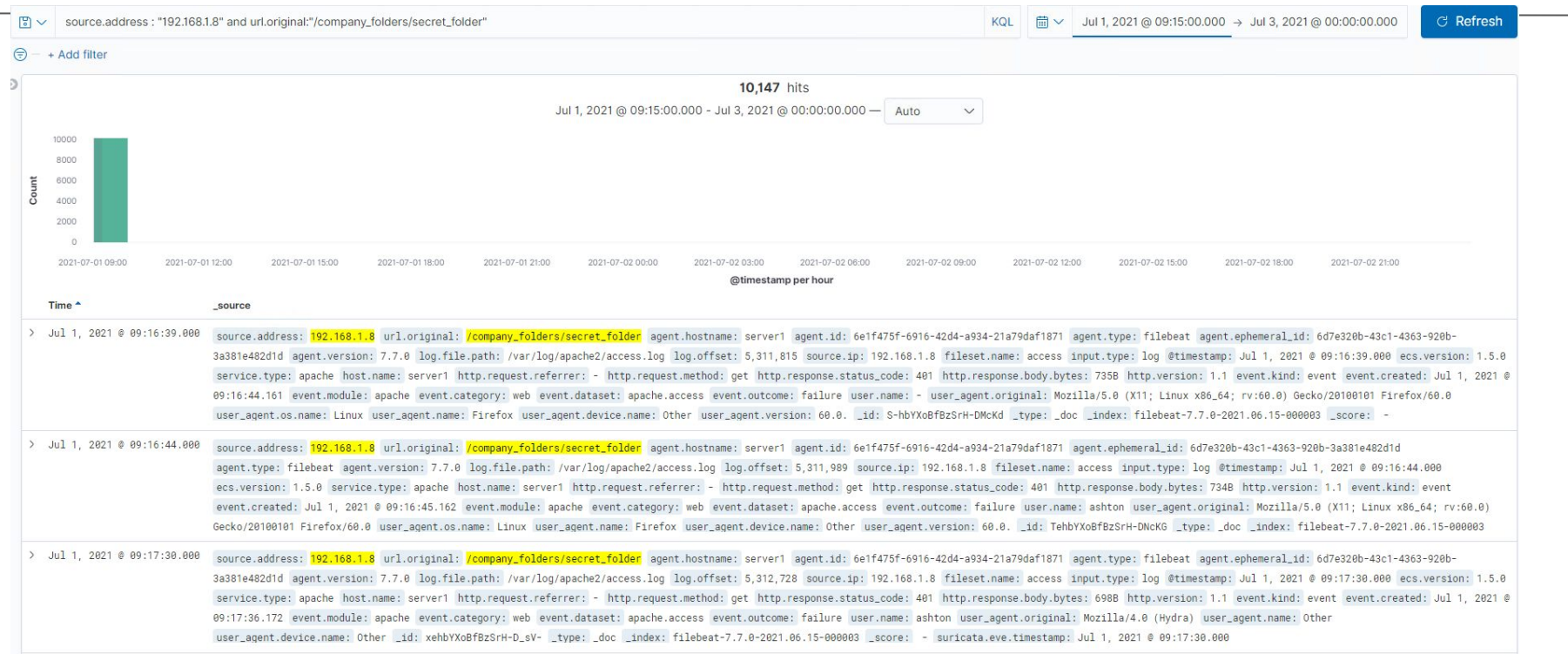
- The port scan began at 08:59 AM and ended at 09:03 on 7/1
- Approximately 33 packets were submitted from 192.168.1.8 (the IP of the Red Team system)
- Early user agents were listed as an NMAP Scripting Engine, which is a port scanning tool

# Analysis: Finding the Request for the Hidden Directory



- The request occurred at 09:14 with only one initial request made (more were done during the brute force attack)
- The only request was for access to the /company\_folders/secret\_folder directory. Because this leads to the login page for the server, this makes sense.

# Analysis: Uncovering the Brute Force Attack



- 10,147 requests were made during the attack
- 10,145 requests had failed based on the number of error responses (error code  $\geq 400$ )



# Analysis: Finding the WebDAV Connection

```
> Jul 1, 2021 @ 09:45:58.000 source.address: 192.168.1.8 user.name: ryan agent.hostname: server1 agent.id: 6elf475f-6916-42d4-a934-21a79daf1871 agent.type: filebeat agent.ephemeral_id: 6d7e320b-43c1-4363-920b-3a381e482d1d agent.version: 7.7.0
log.file.path: /var/log/apache2/access.log log.offset: 6,659,293 source.ip: 192.168.1.8 fileset.name: access url.original: /webdav/ input.type: log @timestamp: Jul 1, 2021 @ 09:45:58.000 ecs.version: 1.5.0
service.type: apache host.name: server1 http.request.referrer: - http.request.method: get http.response.status_code: 200 http.response.body.bytes: 743B http.version: 1.1 event.kind: event event.created: Jul 1, 2021 @ 09:45:59.752 event.module: apache event.category: web event.dataset: apache.access event.outcome: success user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
user_agent.os.name: Linux user_agent.name: Firefox user_agent.device.name: Other user_agent.version: 60.0 _id: sep1YXoBfBzSRH-D-Fa5 _type: _doc _index: filebeat-7.7.0-2021.06.15-000003 _score: -

> Jul 1, 2021 @ 09:48:42.000 source.address: 192.168.1.8 user.name: ryan agent.hostname: server1 agent.id: 6elf475f-6916-42d4-a934-21a79daf1871 agent.type: filebeat agent.ephemeral_id: 6d7e320b-43c1-4363-920b-3a381e482d1d agent.version: 7.7.0
log.file.path: /var/log/apache2/access.log log.offset: 6,661,914 source.ip: 192.168.1.8 fileset.name: access url.original: /webdav/passwd.dav input.type: log @timestamp: Jul 1, 2021 @ 09:48:42.000 ecs.version: 1.5.0
service.type: apache host.name: server1 http.request.referrer: http://192.168.1.105/webdav/ http.request.method: get http.response.status_code: 200 http.response.body.bytes: 301B http.version: 1.1 event.kind: event
event.created: Jul 1, 2021 @ 09:48:42.777 event.module: apache event.category: web event.dataset: apache.access event.outcome: success user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0 user_agent.os.name: Linux user_agent.name: Firefox user_agent.device.name: Other user_agent.version: 60.0 _id: Lup4YXoBfBzSRH-DeVRH _type: _doc _index: filebeat-7.7.0-2021.06.15-000003 _score: -

> Jul 1, 2021 @ 11:15:56.000 source.address: 192.168.1.8 user.name: ryan agent.hostname: server1 agent.id: 6elf475f-6916-42d4-a934-21a79daf1871 agent.type: filebeat agent.ephemeral_id: 6d7e320b-43c1-4363-920b-3a381e482d1d agent.version: 7.7.0
log.file.path: /var/log/apache2/access.log log.offset: 7,338,562 source.ip: 192.168.1.8 fileset.name: access url.original: /webdav/ input.type: log @timestamp: Jul 1, 2021 @ 11:15:56.000 ecs.version: 1.5.0
service.type: apache host.name: server1 http.request.referrer: - http.request.method: get http.response.status_code: 200 http.response.body.bytes: 710B http.version: 1.1 event.kind: event event.created: Jul 1, 2021 @ 11:15:57.279 event.module: apache event.category: web event.dataset: apache.access event.outcome: success user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
user_agent.os.name: Linux user_agent.name: Firefox user_agent.device.name: Other user_agent.version: 60.0 _id: DerIYXoBfBzSRH-DV-ko _type: _doc _index: filebeat-7.7.0-2021.06.15-000003 _score: -

> Jul 1, 2021 @ 11:44:41.000 source.address: 192.168.1.8 user.name: ryan agent.hostname: server1 agent.id: 6elf475f-6916-42d4-a934-21a79daf1871 agent.type: filebeat agent.ephemeral_id: 6d7e320b-43c1-4363-920b-3a381e482d1d agent.version: 7.7.0
log.file.path: /var/log/apache2/access.log log.offset: 7,358,753 source.ip: 192.168.1.8 fileset.name: access url.original: /webdav input.type: log @timestamp: Jul 1, 2021 @ 11:44:41.000 ecs.version: 1.5.0
service.type: apache host.name: server1 http.request.referrer: - http.request.method: options http.response.status_code: 200 http.response.body.bytes: 356B http.version: 1.1 event.kind: event event.created: Jul 1, 2021 @ 11:44:42.588 event.module: apache event.category: web event.dataset: apache.access event.outcome: success user_agent.original: gvfs/1.38.0 user_agent.name: Other user_agent.device.name: Other
_id: b0viYXoBfBzSRH-DrQw_ _type: _doc _index: filebeat-7.7.0-2021.06.15-000003 _score: - suricata.eve.timestamp: Jul 1, 2021 @ 11:44:41.000

> Jul 1, 2021 @ 11:51:05.000 source.address: 192.168.1.8 user.name: ryan agent.hostname: server1 agent.id: 6elf475f-6916-42d4-a934-21a79daf1871 agent.type: filebeat agent.ephemeral_id: 6d7e320b-43c1-4363-920b-3a381e482d1d agent.version: 7.7.0
log.file.path: /var/log/apache2/access.log log.offset: 7,364,438 source.ip: 192.168.1.8 fileset.name: access url.original: /webdav/shell.php input.type: log @timestamp: Jul 1, 2021 @ 11:51:05.000 ecs.version: 1.5.0
service.type: apache host.name: server1 http.request.referrer: - http.request.method: put http.response.status_code: 201 http.response.body.bytes: 533B http.version: 1.1 event.kind: event event.created: Jul 1, 2021 @ 11:51:05.654 event.module: apache event.category: web event.dataset: apache.access event.outcome: success user_agent.original: gvfs/1.38.0 user_agent.name: Other user_agent.device.name: Other _id: j-voYXoBfBzSRH-DhhSn _type: _doc _index: filebeat-7.7.0-2021.06.15-000003 _score: - suricata.eve.timestamp: Jul 1, 2021 @ 11:51:05.000
```

- 21 requests were made to the /webdav directory
- There was a request for the directory page itself, access to a file named “passwd.dav” and a put request for a “shell.php”



# **Blue Team**

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

---

## Alarm

Different types of alarms can be used to detect port scans.

- Filters for scanning tools (like NMAP)
  - This threshold can be set to 1 for instant detection
- Filters for uncommon ports
  - Depending on the usage of these uncommon ports, threshold can be very low (1-5) or moderate (~10)
- Filters for requests of multiple ports from the same IP in a certain timeframe
  - This threshold can be set to 10+ depending on the typical traffic the server receives

## System Hardening

- Firewalls can reduce visibility of open ports outside the network and can also be set up to detect and shut down port scans in progress
- Closing unnecessary ports on the router can prevent them from being accessed by scanners
- If the budget allows, set up a front facing server for the website and an internal server for the network that cannot be accessed from outside

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

- Access of the directory from an external IP (i.e. an address outside the company's IP range)
  - Threshold for this alert can be set to 1
- Attempted access by non-authorized users within the network can also be utilized for an alarm system
  - In case of unintended access, the threshold can be a little higher (~5)
- Depending on the frequency of access for authorized users, an alarm can also be triggered, but this will require monitoring of these authorized users for normal access times

## System Hardening

- Unwanted access can be easily mitigated by creating a network rule denying directory access from external IPs
- For authorized users within the network, redundancy systems like two-factor authentication can protect the directory from compromised accounts
- Placing this directory in a totally private, internal network can also prevent outside access



# Mitigation: Preventing Brute Force Attacks

---

## Alarm

- Brute force attacks can be easily monitored with an alert created based on failed login attempts beyond typical human error
  - A good threshold for this error can be around 5-10 failed attempts
- As with many other parts of this situation, creating alerts based on external IP access would also be wise
  - Alerts can be set to as low as 1, but as high as 10 depending on allowed external access to the network

## System Hardening

- Attacks like this can be mitigated by locking user accounts after a certain threshold of failed login attempts (like the alarm, 5-10 failed attempts is reasonable for human error)
- Mandating harder password policies will also help as increased complexity will greatly reduce the ability for systems to guess the passwords
- Two-factor authentication may also be helpful in the event of successful attack within the threshold

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

- Attempted access to this directory via non-authorized accounts could trigger an alarm
  - Threshold of 1 can be allowed for this as it is a high risk directory
- Access to the directory via external IP is also a good trigger to consider with a low threshold
- Depending on future usage of the directory, write access (put requests in this case) should also be for consideration for alarm, especially via external addresses

## System Hardening

- Depending on the developers' needs, the WebDAV directory could be placed in a private server with an unreadable and un-editable copy placed on the public server
- Changing the access to the directory to disallow both unauthorized users and external IP addresses would also prevent unwanted connection
- If possible, it may also be ideal to change software to a more stable/secure architecture

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

- An alarm can be set up to detect put requests beyond normal capacity for internal IPs
  - The threshold will vary based on the frequency of uploading to the server and certain directories
- An alarm should be set up for put requests for external IPs
  - This threshold can be set to 1 since it will likely be unauthorized access to the server in this instance
- Alarms can also be set to detect outbound internet traffic to certain IPs, but this threshold is dependent on typical business practices

## System Hardening

- Blocking all access of certain folders to external IP addresses would mitigate this threat by outside agents
- If all external access cannot be blocked, then changing http settings to deny put requests can suffice
- Reducing or limiting outbound internet traffic can also be helpful as it can prevent systems from communicating unintentionally with threat agents

*The  
End*