

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

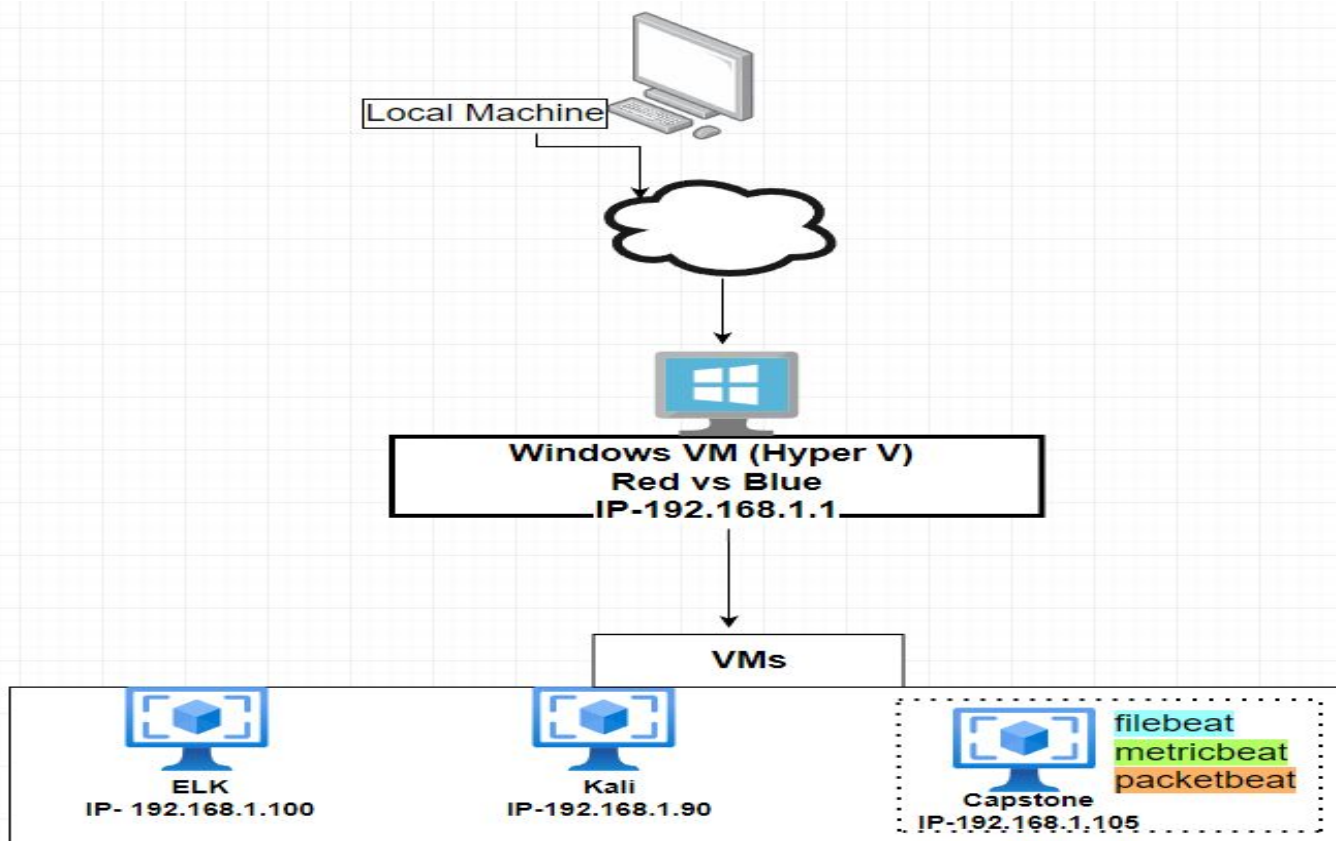
Blue Team: Log Analysis and Attack Characterization

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
OS:Linux
Hostname:Red vs Blue

IPv4:192.168.1.100
OS:Linux
Hostname:Elk

IPv4:192.168.1.90
OS:Kali Linux
Hostname:Kali

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

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, crystalline effect.

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 using Apache Web Server |
| Kali | 192.168.1.90 | Attacking machine running on Kali Linux |
| Elk | 192.168.1.100 | Logging service capturing data and server activity. |
| Hyper V Manager | 192.168.1.1 | Software that contains and visualizes multiple virtual machines. |

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---------------------------------|---|--|
| Out of date software | Old version of Apache was being used without being patched. | Leaves vulnerabilities open to attackers to connect to the network. |
| Lack of password complexity | Users on the network lacked complex passwords ex.(numbers, characters, capitalization) | Created a weak point for the attacker to easily crack password to access confidential information. |
| Vulnerable ports open to public | Port 80 and port 22 showed as open to any source on an Nmap scan | Allowed the attacked to connect directly from the internet on their machine. |

Exploitation: Open Vulnerable Ports

01

Tools & Processes

Ran an Nmap scan on the servers network.

02

Achievements

Showed port 80 and port 22 were open that allows any source to connect to the network.

03

```
root@kali:~# nmap 172.16.84.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-30 04:14:14
Nmap scan report for 172.16.84.1
Host is up (0.0017s latency).
Not shown: 908 closed ports, 91 filtered ports
PORT      STATE SERVICE
631/tcp    open  ipp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.16.84.2
Host is up (0.00070s latency).
All 1000 scanned ports on 172.16.84.2 are closed
MAC Address: 00:50:56:F9:EB:07 (VMware)

Nmap scan report for 172.16.84.205
Host is up (0.00068s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:1C:28:DC (VMware)
```



Exploitation: Lack of Password Complexity

01

Tools & Processes

Hydra was used to brute force attack the password for ashton

02

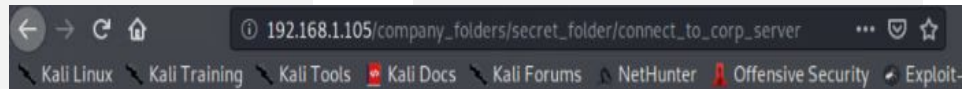
Achievements

Accessed

/company_folders/secret_folder directory from the server.

03

```
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "joey" - 10141 of 14344399 [ch
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jeferson" - 10142 of 14344399
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jackass2" - 10143 of 14344399
[80][http-get] host: 172.16.84.205 login: ashton password: leopoldo
[STATUS] attack finished for 172.16.84.205 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-04-30 13:08:56
root@kali:/#
```



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

Exploitation: Out of Date Software

01

Tools & Processes

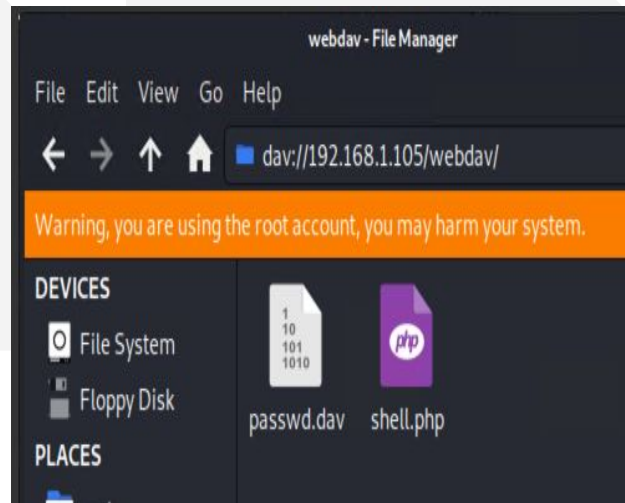
Created a reverse shell with msfvenom. From there a listener was set up in Metasploit by creating a payload.


02

Achievements

Successful upload and activated a PHP reverse shell script to the WebDav directory.

03





Blue Team

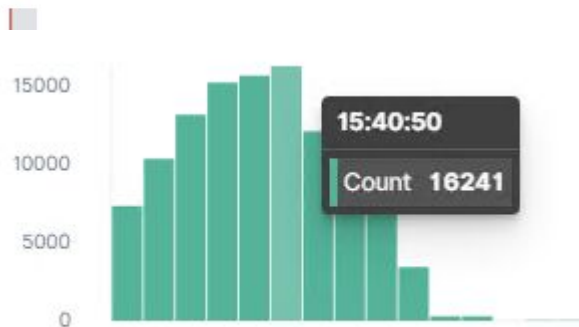
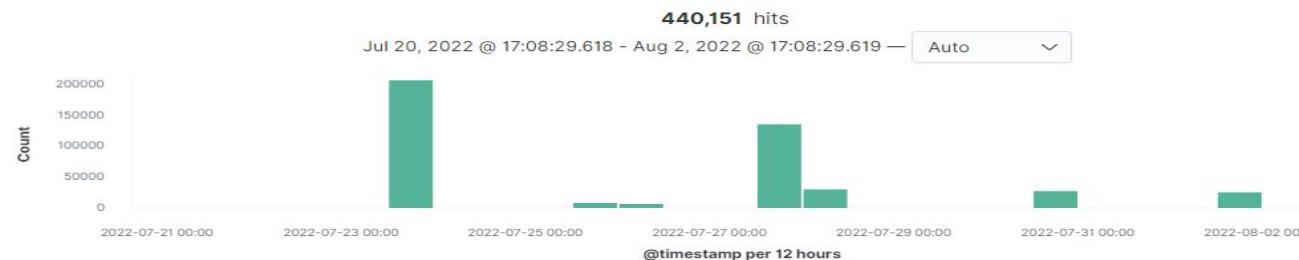
Log Analysis and Attack Characterization

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? 3:40pm
- How many packets were sent, and from which IP? 11 packets from IP: 192.168.1.90
- What indicates that this was a port scan? The HTTP request through port 80.



```
> Aug 2, 2022 @ 17:08:24.040 @timestamp: Aug 2, 2022 @ 17:08:24.040 url.full: http://127.0.0.1/server-status?auto= url.scheme: http
url.domain: 127.0.0.1 url.path: /server-status url.query: auto= client.port: 36260 client.bytes: 1098
client.ip: 127.0.0.1 host.name: server1 status: OK query: GET /server-status source.ip: 127.0.0.1
source.port: 36260 source.bytes: 1098 type: http ecs.version: 1.5.0 method: get destination.bytes: 50
```

```
> Jul 23, 2022 @ 15:40:50.004 @timestamp: Jul 23, 2022 @ 15:40:50.004 type: flow network.type: ipv4 network.transport: tcp
network.community_id: 1:zNEA2DfFs2xUI41K7sJwWVYy9mw= network.bytes: 1.6KB network.packets: 11 ecs.version: 1.5.0
agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: ca074e14-e3fa-4407-9d20-
7b9dfa226521 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali source.port: 48786 source.packets: 6
source.bytes: 580B source.ip: 192.168.1.90 destination.ip: 192.168.1.105 destination.port: 80
```

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? July 23rd 2022 @ 3:43 pm
- How many requests were made? 16,352
- Which files were requested? /company_folders/secret_folder/
- What did they contain? The secret folder contained a password hash for the user Ryan.

Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|---|--------|
| http://192.168.1.105/company_folders/secret_folder/ | 16,352 |
| http://192.168.1.105/webdav | 174 |
| http://192.168.1.105/webdav/passwd.dav | 30 |
| http://192.168.1.105/webdav/normalfile.exe | 16 |
| http://192.168.1.105/company_folders/ | 14 |

Export: Raw Formatted

```
> Jul 23, 2022 @ 15:43:20.223 url.path: /company_folders/secret_folder/ @timestamp: Jul 23, 2022 @ 15:43:20.223 destination.ip: 192.168.1.105
destination.port: 80 destination.bytes: 733B user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0)
Gecko/20100101 Firefox/68.0 status: OK http.version: 1.1 http.request.headers.content-length: 0
http.request.method: get http.request.bytes: 386B http.response.body.bytes: 482B http.response.headers.content-length: 482 http.response.headers.content-type: text/html;charset=UTF-8 http.response.status_phrase: ok

> Jul 23, 2022 @ 15:43:19.900 url.path: /company_folders/secret_folder/ @timestamp: Jul 23, 2022 @ 15:43:19.900 status: OK host.name: Kali
event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.7 event.start: Jul 23, 2022 @ 15:43:19.900 event.end: Jul 23, 2022 @ 15:43:19.901 destination.ip: 192.168.1.105 destination.port: 80
destination.bytes: 733B url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http
url.domain: 192.168.1.105 query: GET /company_folders/secret_folder/ agent.version: 7.8.0 agent.hostname: Kali

> Jul 23, 2022 @ 15:42:45.155 url.path: /company_folders/secret_folder/ @timestamp: Jul 23, 2022 @ 15:42:45.155 destination.ip: 192.168.1.105
destination.port: 80 destination.bytes: 735B event.category: network_traffic event.dataset: http
event.duration: 0.3 event.start: Jul 23, 2022 @ 15:42:45.155 event.end: Jul 23, 2022 @ 15:42:45.156
event.kind: event source.ip: 192.168.1.90 source.port: 36298 source.bytes: 343B query: GET
/company_folders/secret_folder/ host.name: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17
```

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.



- The file was requested 3,207 times before the attacker successfully requested the file 1 time July 23rd 2022 @ 3:40pm.

3,207 hits

Jul 23, 2022 @ 15:40:00.000 - Jul 23, 2022 @ 15:40:10.000 —

1 hit

Jul 23, 2022 @ 15:40:00.000 - Jul 23, 2022 @ 15:40:10.000 — Auto ▾



15:40:03.000 15:40:04.000 15:40:05.000 15:40:06.000 15:40:07.000 15:40:08.000

@timestamp per 200 milliseconds

Time ▾

_source

```
> Jul 23, 2022 @ 15:40:08.000 event.outcome: success agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: fa647d40-aae5-443f-b482-0285cde11cac
agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 566,954 source.address: 127.0.0.1 source.ip: 127.0.0.1 fileset.name: access url.original: /server-
status?auto= input.type: log @timestamp: Jul 23, 2022 @ 15:40:08.000 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: 596B http.version: 1.1 event.kind: event event.created: Jul 23, 2022 @ 15:40:09.588
event.module: apache event.category: web event.dataset: apache.access user.name: - user_agent.original: Go-http-client/1.1 user_agent.name: Go-http-client
```

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? 174 requests
- Which files were requested? HTTP query for GET /company_folders/secret_folder/

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending

Count

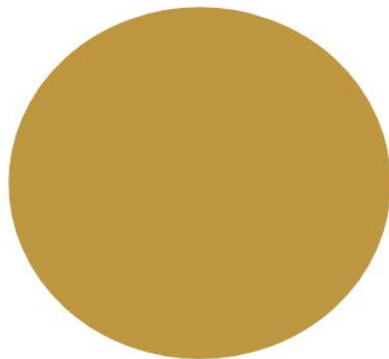
http://192.168.1.105/webdav

174

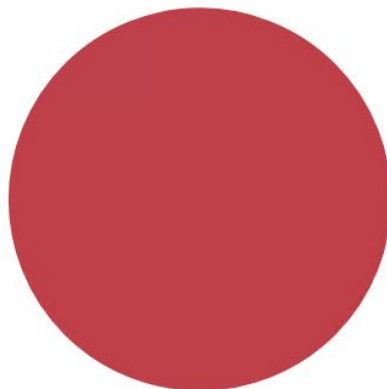
Export: Raw Formatted

HTTP status codes for the top queries [Packetbeat] ECS

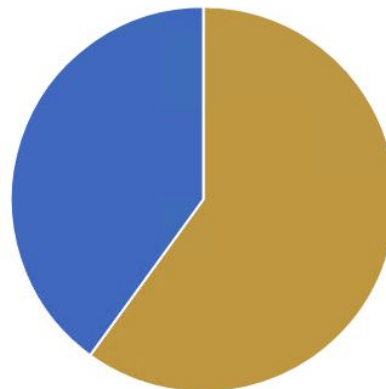
401



GET /company_folders/secret_folder/: HTTP Query



PROPFIND /webdav: HTTP Query



OPTIONS /webdav: HTTP Query



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?

- Setting an alert for scan and sweep filters to capture high levels of port scans from a single IP.

What threshold would you set to activate this alarm?

- Placing a threshold value determined off of baseline activity for connection attempts from a specific IP. Once the threshold is met the alert is sent.

System Hardening

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

- Deploying adaptive firewalls.
- Also setting up filters to block port scans.

Describe the solution. If possible, provide required command lines.

- Adaptive firewalls block ports when malicious IPs are trying to scan them.
- Filters for 7000-7003 (TCP / UDP port scan / host sweeps), as well as 7004 and 7016 (ICMP & ICMPv6 host sweep).

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alert can be put in place for any IP address that's not authorized to access this file / directory.

What threshold would you set to activate this alarm?

- The threshold would be 1, met by any machine IP not whitelisted for this directory.

System Hardening

What configuration can be set on the host to block unwanted access?

- Only allowing this directory to be accessed by certain IPs.

Describe the solution. If possible, provide required command lines.

- Open Apache Configuration File.
- Restrict Access by IP. Once you have opened the appropriate configuration file, look for <Directory> tag.
- Restart Apache web server

Mitigation: Preventing Brute Force Attacks

Alarm

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

- A 401 Unauthorized alert can be created for the server.

What threshold would you set to activate this alarm?

- When a baseline of 5 over a 1 hour period is met, the alert would then be triggered.

System Hardening

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

- Allowing only a certain amount of failed login attempts.
- Using MFA (Multi Factor Authentication)

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

- Alter account policies for logins on the server.
- Implement a multi factor authentication process for user logins.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Setting an alert when any attempt is made to access this directory outside of the whitelisted IPs.

What threshold would you set to activate this alarm?

- Creating a range for accepted IPs.
- Setting a threshold of 1 attempt for any unauthorized IPs.

System Hardening

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

- Creating a firewall rule to protect this directory.
- Not allowing access to this directory from the web, especially from a non-local source.

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

- Blacklisting all IPs outside of Whitelisted IPs.
 - Blocking port 80 and 443.
-

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Setting up an alert for .php files uploaded to the server, as well as an alert for the firewall including traffic going through port 80, 443, and 4444.

What threshold would you set to activate this alarm?

- The threshold would be for any .php files, and any traffic moving through / trying to connect to port 80, 443, and 4444, triggering the set alarm.

System Hardening

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

- Taking away the ability to upload any type of files from the web, and only allowing uploads from a local source.

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

- Block port 80, 443, and 4444.

*The
End*