

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

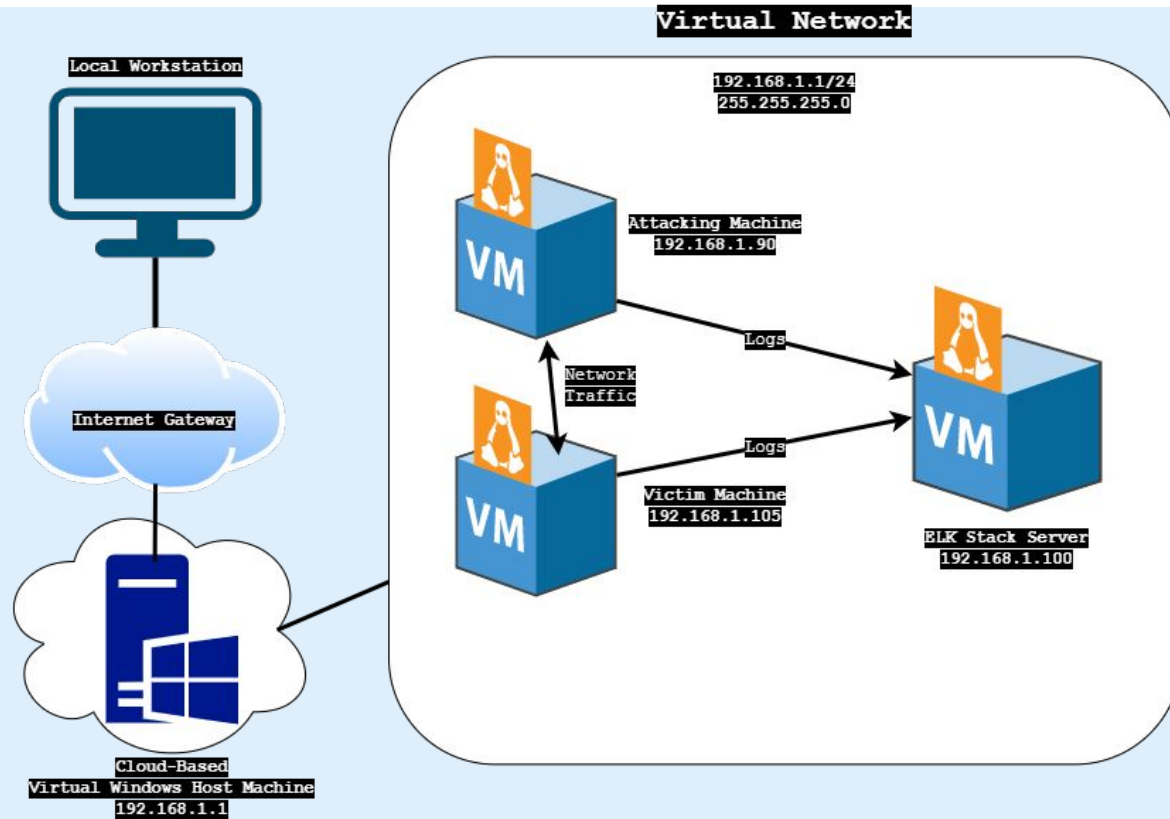
Blue Team: Log Analysis and Attack Characterization

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: 192.168.1.1

Machines

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

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

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
Red vs. Blue	192.168.1.1	Virtual Machine Host
ELK	192.168.1.100	ELK Stack Server
Capstone	192.168.1.105	Target Server
Kali	192.168.1.90	Attacker Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Use the CVE number if it exists. Otherwise, use the common name.</i>	<i>Describe the vulnerability.</i>	<i>Describe what this vulnerability allows the attacker to do.</i>
Sensitive Data Exposure (OWASP Top 10 #3)	The /secret_folder/ directory is accessible and contains credential data that can be maliciously exploited	An attacker can use this information to gain access to the web server.
Unrestricted File Upload	Users have no restrictions on uploading files to sensitive directories	Users can upload malicious files to critical directories on the server.
Reverse Shell Code Injection via php_handler exploit CVE-2015-3330	The php_handler function can be exploited to run arbitrary instructions.	An attacker can execute this in order to gain command and control of a target machine.

Exploitation: [Sensitive Data Exposure]

01

Tools & Processes

- nmap was used to scan for open ports.
- Once port 80 was confirmed to be open, a browser was used for additional reconaissance.

02

Achievements

- Exploring the public files revealed the existence of a /secret_directory/ folder
- Though requiring login credentials, a valid username was uncovered

03

Impact

- The aforementioned username was discovered to be 'ashton'.
- This can be used to execute any number of password cracking attacks to gain elevated access.

Exploitation: [Unrestricted File Upload]

01

Tools & Processes

- hydra was used to crack the password of 'ashton'
- A web browser was used to explore the contents of the /secret_folder/ directory
- john was used to obtain a password from the unencrypted hash stored in plaintext.
- msfconsole was used to create a reverse shell file
- WebDAV was used to upload the file

02

Achievements

- The steps followed in this process places a file on the server that enables the execution of malicious shell code.

03

Impact

- The ability to operate a shell on this server allows an attacker to connect directly to their target.

Exploitation: [Reverse Shell Code Injection]

01

Tools & Processes

- Meterpreter was used to connect to the target remotely via the previously uploaded shell script.
- The shell was used to gain root access to the target.

02

Achievements

- Successful execution of this reverse shell script allows a Meterpreter shell to be opened directly on the target machine.
- Once done, a user can freely navigate through the target machine's filesystem.


03

Impact

- Red Team was able to parse through system files and obtain the flag.

```
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:35484)
at 2021-02-03 19:43:13 -0800

meterpreter > shell
Process 1603 created.
Channel 0 created.
whoami
www-data
locate -i "*flag.txt*"
/flag.txt
cat /flag.txt
bing0w@5h1sn@m0
```



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- What time did the port scan occur?
 - 30 Jan 2021 09:00hrs
- How many packets were sent, and from which IP?
 - 6 packets from 192.168.1.90
- What indicates that this was a port scan?
 - Packets were sent to destination port 80 indicating a tcp scan

Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/secret_folder	15,985
http://192.168.1.105/webdav/	14
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/company_folders/customer_info/	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Export: [Raw](#)  [Formatted](#) 

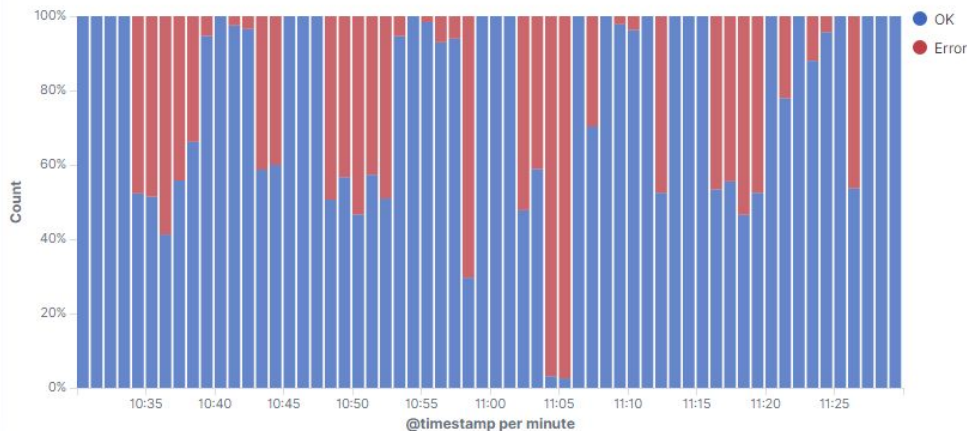
- At approximately 11:05AM, 15,985 requests to access the secret_folder were made. All of these requests came from the IP address 192.168.1.90.
 - We've concluded that the attackers were after the connect_to_corp_server file, which contains instructions on how to access the companies WebDAV server
-

Analysis: Uncovering the Brute Force Attack

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,985
http://192.168.1.105/webdav/	14
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/company_folders/customer_info/	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Errors vs successful transactions [Packetbeat] ECS



- As previously stated, there were 15,985 requests made for this directory, however the file inside was only successfully accessed twice. Approximately 97% of all traffic during this short window of time generated an error.
- This many errors in a very short time is often the sign of a brute force attack.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾	Count ▾
http://192.168.1.105/webdav	30
http://192.168.1.105/webdav/	14
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/webdav/passwd.dav	4

Export: [Raw](#)  [Formatted](#) 

- In total, there were 44 requests made to access this directory.
- Both the passwd.dav file and shell.php file were requested multiple times.



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?

Set an alarm triggered by large numbers of requests that occur in a short period of time and setting a limit for the number of requested ports for each source IP address.

What threshold would you set to activate this alarm?

About 10+ port scans in less than a minute.

System Hardening

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

Enable only traffic required to access internal hosts and deny everything else. Also, configure firewalls to look for potentially malicious behavior and set rules to terminate attacks if a pre-specified threshold is reached.

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

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

An alarm can be set to send an alert anytime a non-whitelisted IP attempts to access the hidden directory, either successfully or unsuccessfully.

What threshold would you set to activate this alarm?

This alarm will be set to send an alert if even a single unauthorized IP address attempts to access this directory.

System Hardening

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

A firewall can be configured to block unauthorized IPs from remotely connecting to the host machine. Additionally, access to the Hidden Directory can be restricted to specific users so that if an attacker somehow bypasses the firewall, they are still prevented from gaining access.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Set up an alarm if 401 unauthorized code is returned from any server over a certain preset threshold that would filter out failures due to forgotten passwords. Another alarm could be set if the "user_agent.original" value includes Hydra in the name.

What threshold would you set to activate this alarm? 4 or more failed attempts within 30 minutes.

System Hardening

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

After a server has returned the threshold number of unauthorized access codes, the server can be set to drop traffic for a specified time from the attacking IP address that is making the multiple failed requests

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

Lock out IP addresses with multiple failed logins.

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alarm can be set to trigger when a read request is initiated on any file in the WebDAV directory.

What threshold would you set to activate this alarm?

The alarm should be triggered when a non-whitelisted IP attempts to read a file in the WebDAV directory.

System Hardening

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

Access to the company's WebDAV server should be removed from the company's public facing website entirely, and access should be restricted to only those who need it on the company's internal network.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

An alert can be set to trigger anytime someone attempts to access port 4444. Additionally, another alert can be set to trigger if any non-whitelisted IP attempts to upload a file.

What threshold would you set to activate this alarm?

This alarm will be set to send an alert if even a single unauthorized IP address attempts to upload a file

System Hardening

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

Write permissions can be restricted to specific users on the host machine. Additionally, file uploads can be restricted to a dedicated logical storage partition.

*The
End*