Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

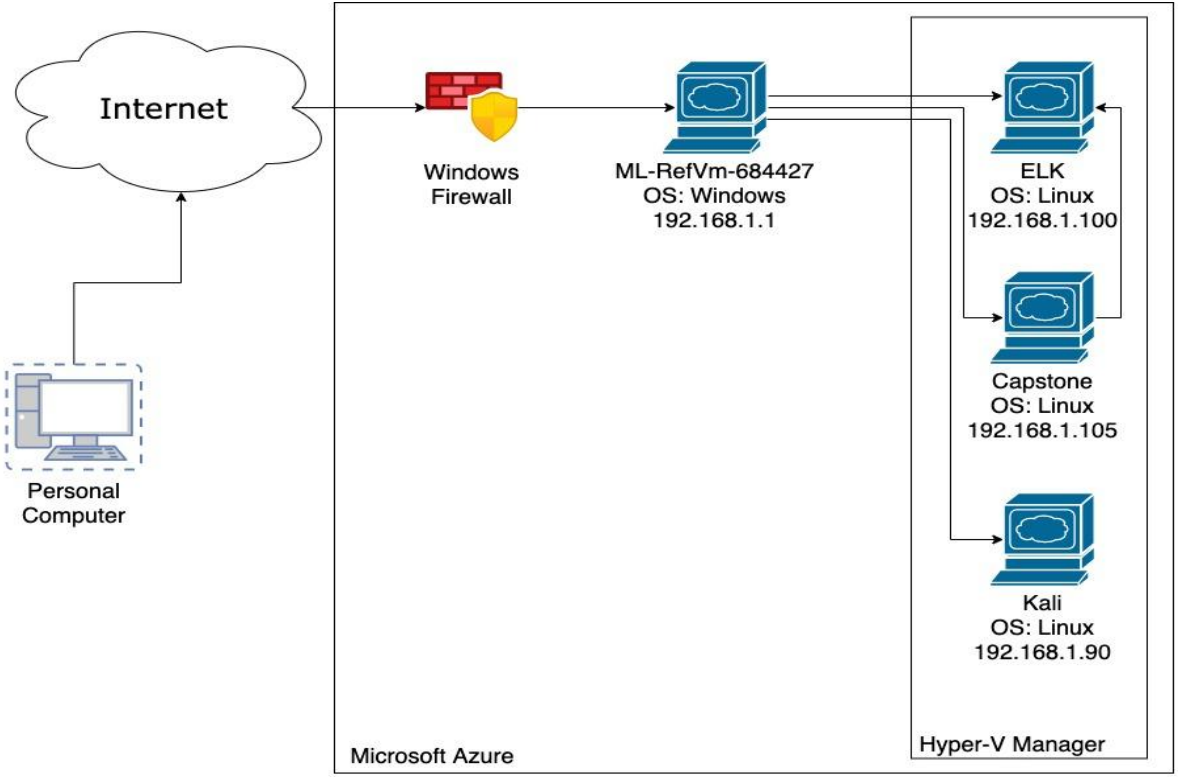
Created by Jared Knighten

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Network: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Host: ML-RefVm-684427

IPv4: 192.68.1.100
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
ML-REFVM-684427	192.168.1.1	Virtual Machine Host
Capstone	192.168.1.105	Web Server
ELK	192.168.1.100	SIEM
Kali	192.168.1.90	Pentest Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability (In Order Of Execution)	Description	Impact
Sensitive Data Exposure	Sensitive data was found within directories of the web server.	Leaves sensitive information exposed and accessible, the location of this information: /company_folders/secret_folder/
Brute Force	Was allowed a password field within a protected directory, which allowed me to launch a brute force attack. This indicates having a faulty security configuration within the web server	Once the attack was completed, it allowed access to /company_folders/secret_folder/ & within this “secret_folder” it had a password hash for the user named “Ryan”, as well as detailed instructions how to access webdav (IP: 192.168.1.105)
Unauthorized File Upload	An attack script was able to be uploaded to the web server using WebDAV.	The attack script gained access to a remote backdoor shell to (also known as reverse tcp shell) access the web server.

Exploitation: Sensitive Data Exposure

01

Tools & Processes
This data is obtainable two different ways:

Way One: Run “wget -r 192.168.1.105” within the terminal & then use the “cat” command on “ashton.txt”

Way Two: Navigate throughout web server directory

02

Achievements
Created a file with all directory and file locations from the web server

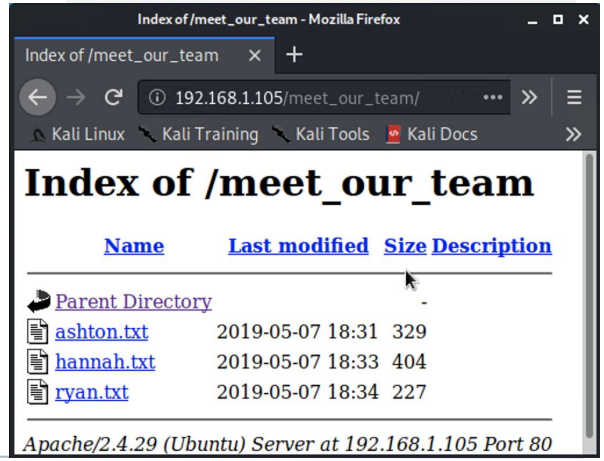
Files revealed location of /company_files/secret_folder

Determined Ashton is the admin for the /secret_folder directory based on the information within the text file

03

```
File  Actions  Edit  View  Help
root@Kali:~# wget -r 192.168.1.105
```

```
root@Kali:~/192.168.1.105/meet_our_team# cat ash
ton.txt
Ashton is 22 years young, with a masters degreee
 in aquatic jousting. "Moving over to managing e
veryone's credit card and security information h
as been terrifying. I can't believe that they ha
ve me managing the company_folders/secret_folder
! I really shouldn't be here" We look forward to
 working more with Ashton in the future!
```



Exploitation: Brute Force Vulnerability

01

Tools & Processes

The tool used was called Hydra, we can use this to brute force attack Ashton's password field for the directory "/secret_folder"

02

Achievements

Within the "rockyou.txt" file Ashton's password was found

Once the password is obtained, it gives access to the secret_folder which contains more sensitive information

With more digging the password hash for admin "Ryan" was found & with this, it gives more system access

03

```
root@Kali:/usr/share/wordlists# hydra -l ashton
-P rockyou.txt -s 80 -f -vV 192.168.1.105 http-g
et /company_folders/secret_folder/
```

```
[ATTEMPT] target 192.168.1.105 - login "ashton"
- pass "jeferson" - 10142 of 14344399 [child 7]
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton"
- pass "jackass2" - 10143 of 14344399 [child 9]
(0/0)
[80][http-get] host: 192.168.1.105   login: asht
on   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (vali
d pair found)
1 of 1 target successfully completed, 1 valid pa
ssword found
Hydra (https://github.com/vanhauser-thc/thc-hydr
a) finished at 2021-04-03 22:00:04
root@Kali:/usr/share/wordlists#
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

Uploaded an attack payload through WebDAV

Tools that were used:

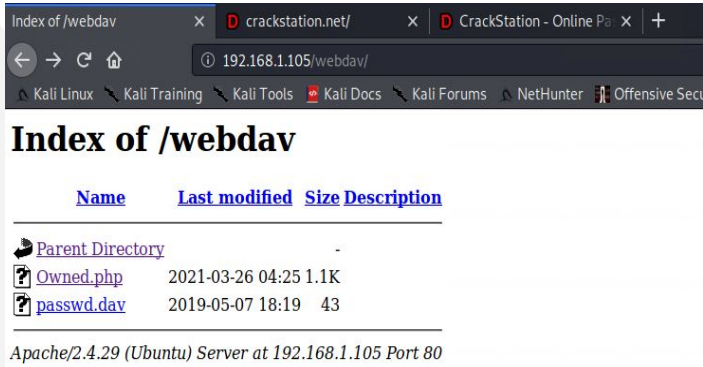
- Msfvenom
- Metasploit

02

Achievements

This payload creates a reverse shell that allows backdoor access to the web server

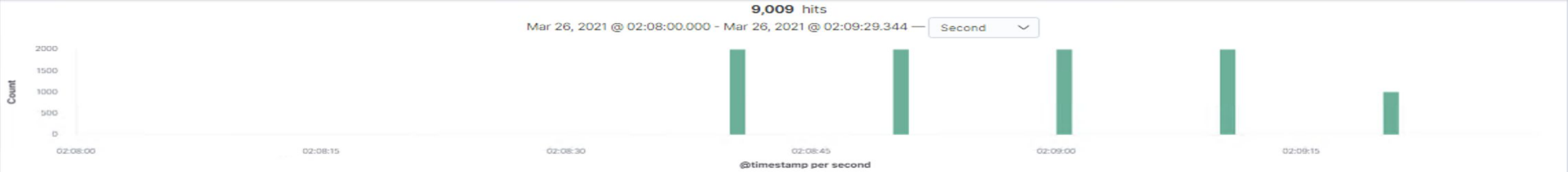
03



Blue Team

Log Analysis and Attack Characterization

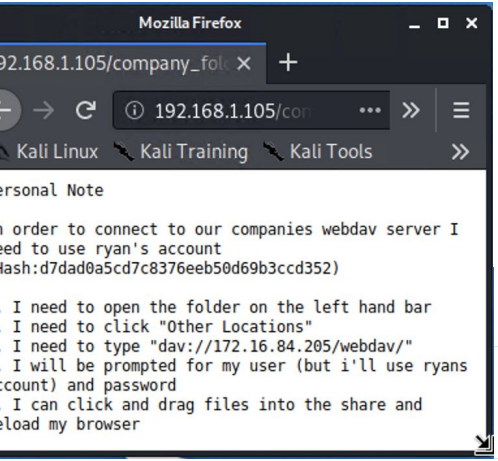
Analysis: Identifying the Port Scan



	Time	source.ip	destination.port
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	1
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	3
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	4
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	6
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	7
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	9
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	13
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	17
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	19
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	20
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	21
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	22
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	23
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	24
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	25
>	Mar 26, 2021 @ 02:08:40.000	192.168.1.90	26

- 9,009 packets were sent from IP 192.168.1.90
- The rapid number of scans indicate this was a port scan.
- The scanner sent 9 packets to the 1,000 most used ports.

Analysis: Finding the Request for the Hidden Directory



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,444
http://192.168.1.105/webdav/Owned.php	174
http://192.168.1.105/webdav/passwd.dav	54
http://192.168.1.105/webdav/lib	6
http://192.168.1.105/webdav/	5
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Mar 26, 2021 @ 02:46:18.006 url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Mar 26, 2021 @ 02:46:18.006 type: http user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:LabIPCEH9WPZuOhjFDW45tBOZS0= network.bytes: 1.1KB ecs.version: 1.5.0 host.name: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 8ff7925e-fb4e-4d28-aec6-b774560facb5 agent.hostname: server1 client.ip: 192.168.1.90 client.port: 49516 client.bytes: 470B source.port: 49516 source.bytes: 470B source.ip: 192.168.1.90 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 674B event.start: Mar 26, 2021 @ 02:46:18.006 event.end: Mar 26, 2021 @ 02:46:18.015 event.kind: event event.category: network_traffic event.dataset: http event.duration: 8.9 server.ip: 192.168.1.105

- The requests began at 02:43:14 on 26 March 2021. 16,444 requests were made, most during the brute force attack.
- The “/company_folders/secret_folder/connect_to_corp_server” file was accessed at 02:46:18.
- The file contained instructions to access WebDAV, the username and the user’s password hash.

Analysis: Uncovering the Brute Force Attack

> Mar 26, 2021 @ 02:44:22.896 user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Mar 26, 2021 @ 02:44:22.896 server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B
url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder/ network.bytes: 862B network.type: ipv4
network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:qz3kKxfjzSMFaCpEpvc3Ay5DUG8= event.end: Mar 26, 2021 @ 02:44:22.898 event.kind: event
event.category: network_traffic event.dataset: http event.duration: 1.6 event.start: Mar 26, 2021 @ 02:44:22.896 client.port: 49494 client.bytes: 164B client.ip: 192.168.1.90 method: get
http.request.bytes: 164B http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-

Time	user_agent.original	http.response.status_code
> Mar 26, 2021 @ 02:44:22.831	Mozilla/4.0 (Hydra)	200

p 10 HTTP requests [Packetbeat] ECS

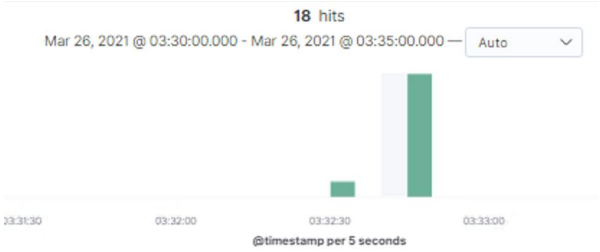
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,444
http://192.168.1.105/webdav/Owned.php	174
http://192.168.1.105/webdav/passwd.dav	54
http://192.168.1.105/webdav/lib	6
http://192.168.1.105/webdav/	5
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

- A total of 16,444 requests were made in the brute force attack (16,444 errors and 2 successful)
- The successful request was made at 02:44:22 on 26 March 2021.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,444
http://192.168.1.105/webdav/Owned.php	174
http://192.168.1.105/webdav/passwd.dav	54
http://192.168.1.105/webdav/lib	6
http://192.168.1.105/webdav/	5
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2



- The “/webdav” directory had 5 requests throughout the attack.
- The file “owned.php” was uploaded to the webdav directory.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- To detect port scans, it is advocated for an alarm to be configured for when the web server (in this case 192.168.1.105) is accessed by other ports that ARE NOT 443 & 80

- Threshold: An example of a good alert would be when a source IP sends more than 3 requests per second to any ports other than 443 or 80

System Hardening

- A good firewall configuration would be to close all ports other than 443 & 80
- To block out unwanted port scans you can use something called IPtables, an example of IPtables would be:
  1. iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 80,443 -j DROP (this blocks all ports other than 443 & 80)
  2. iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT (this is a rejection if

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Whitelisting certain IP that are authorized can mitigate unwanted access from untrusted users
- An alert that should be created would be to send an alert if any untrusted IPs (not on the whitelist) access a protected directory

System Hardening

- Always encrypt sensitive data
- Whitelisting trusted IPs
- Modifying the httpd.config to include only trusted IPs. Example below:

```
“<Directory /var/www/company_folders/secret_folder/>
Order allow,deny
Allow from *authorized IP*
Allow from *authorized IP*
Deny from all
</Directory>”
```

Mitigation: Preventing Brute Force Attacks

Alarm

- A good rule of thumb to preventing brute force attacks is creating an alarm that recognizes multiple failed requests

- Threshold: Alert when 3 failed attempts are made from the same source IP within a second

System Hardening

- Temporarily block access if the same source IP has more than 3 failed login attempts

- Use multi-factor authentication

- Have the firewall delay responses to slow down attacks & have a better chance to mitigate the attack before it gets too big

- Have a strong password policy to make sure users do have have passwords found on established

Mitigation: Detecting the WebDAV Connection

Alarm

- Whitelisting authorized IP address to be the only ones that are allowed access
- Alert if any IP accesses directory not on the whitelist

System Hardening

- Encrypt sensitive data
- Block access from all IPs not on the whitelist
- As seen on a previous slide configuring & modifying the httpd.conf file to allow only authorized IP address

Mitigation: Identifying Reverse Shell Uploads

Alarm

- An alarm should be configured if any POST & PUT requests attempt to upload an uncertified file type
- Threshold: Alert if any unauthorized file type is attempted

System Hardening

- Only allow specific file extensions
- Only allow authorized and authenticated users to upload files
- Execute content checking on any files that are uploaded
- Uploaded directories should not have executable permission from unauthorized users

the End