Capstone Engagement

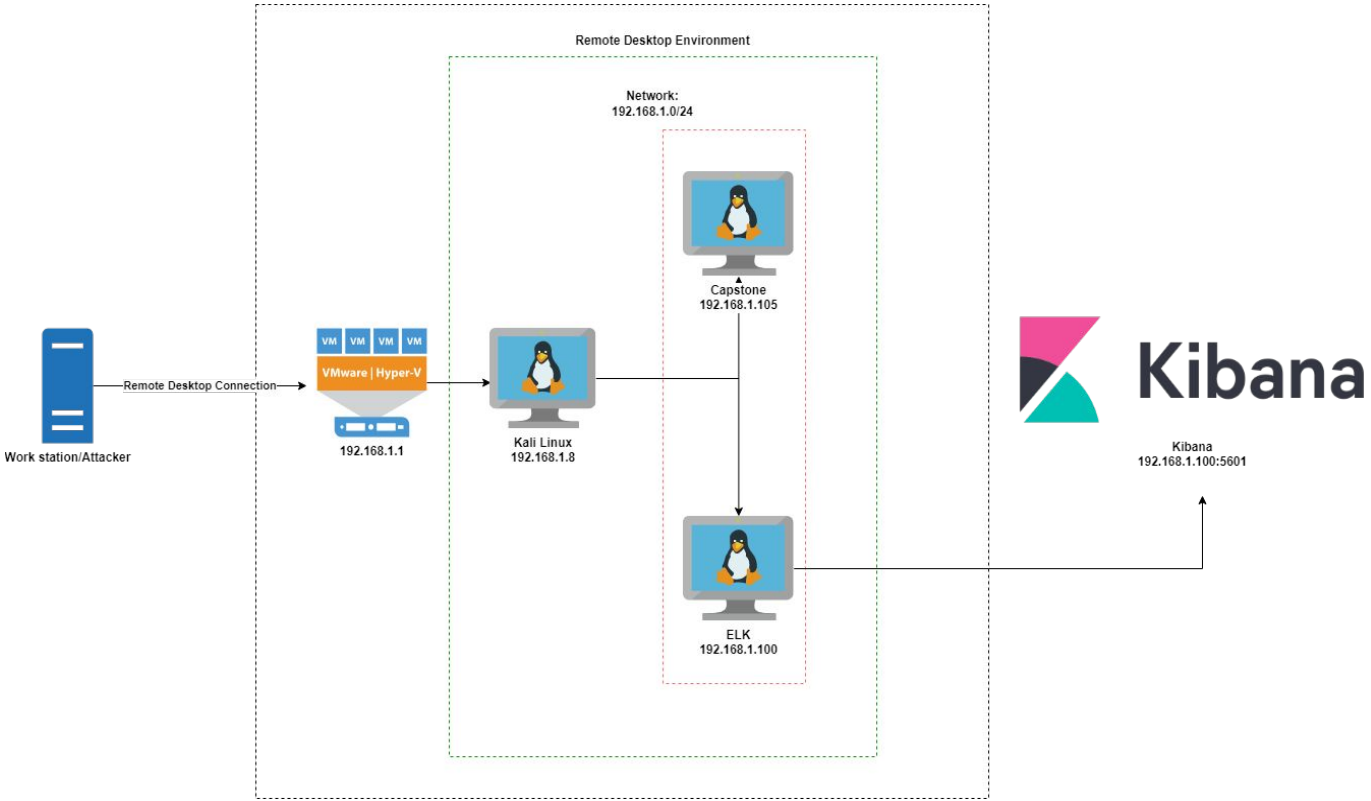
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.1.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows 10
Hostname: HyperV Gateway

IPv4: 192.168.1.8
OS: Linux
Hostname: Kali Linux

IPv4: 192.168.1.105
OS: Linux Ubuntu
Hostname: Capstone

IPv4: 192.168.1.105
OS: Linux Ubuntu
Hostname: ELK

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
HyperV (Azure) ml-lab-8f4ec878-1f4c-4e81-8714-9a6606cede64.eastus2.cloudapp.azure.com:55942	192.168.1.1	Host virtual cloud machine.
Kali	192.168.1.8	Attacker Machine
ELK	192.168.1.100	Monitoring Machine/ Kibana/ Logstash/ Elastic Search
Capstone	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 has exposed to the public	Port 80 is an unsecured http which allow anyone to follow up with the traffic	Allow public access via a web browser. An attacker can discover a hidden directory that stored sensitive information.
Directory open to public	The site has a /secret_folder directory open to public	Allow public to access the unintended access folder that may stored a critical information or by using LFI(Local file inclusion)
Weak passwords	Using of the weak passwords that have a short combination.	Password can be easily guess or brute-forcing using a simple wordlists.
Weak hashes	Using of weak hashed such as a md5	Md5 hashes can be decoded using the online resource in a short amount of time.

Exploitation: Opened TCP port 80

01

Tools & Processes

Enumerating the opened and unsecured port 80 using a common tool, nmap and dirb

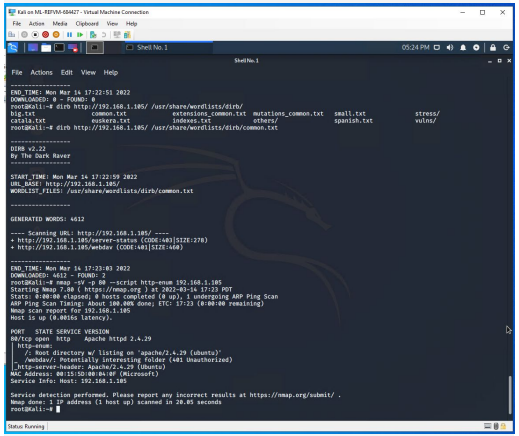
Command used: nmap -sV -p 80 –script http-enum 192.168.1.105

02

Achievements

We are able to gather the information such as an opened service and some sensitive folder that may have a confidential information inside.

03



Exploitation: Directory Opened to public

01

Tools & Processes

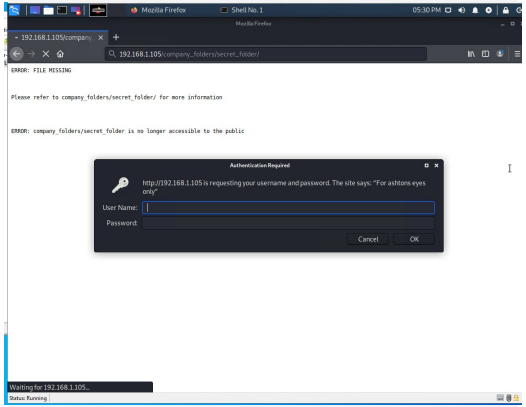
The secret folder can be discover by browsing the directory and found inside the text file mentioned the secret folder path.

02

Achievements

We were able to discover the hidden folder, but it seems that it is protected by a password, which we will need to approach in the next step.

03



Exploitation: Weak Password

01

Tools & Processes

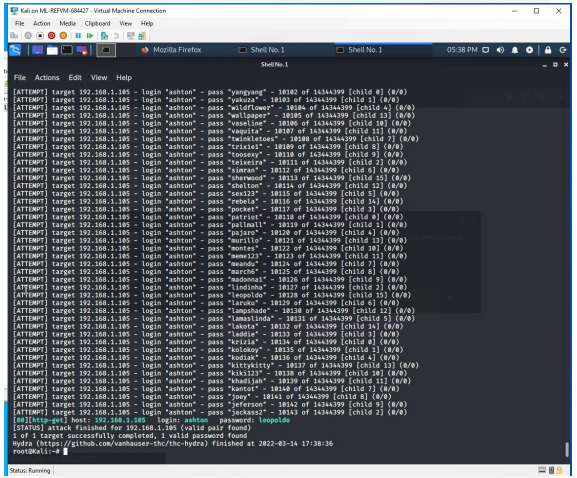
Continuing on from the previous stage, we've discovered the hidden folder and are now using hydra to brute-force the protected folder.
Command: hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get “/company_folders/secret_folder”

02

Achievements

We are able to break into the secret_folder using the password retrieve from hydra tool. With the use of a weak password which is **leopoldo** we are able to brute force it in a short amount of time.

03



Blue Team
Log Analysis and Attack Characterization

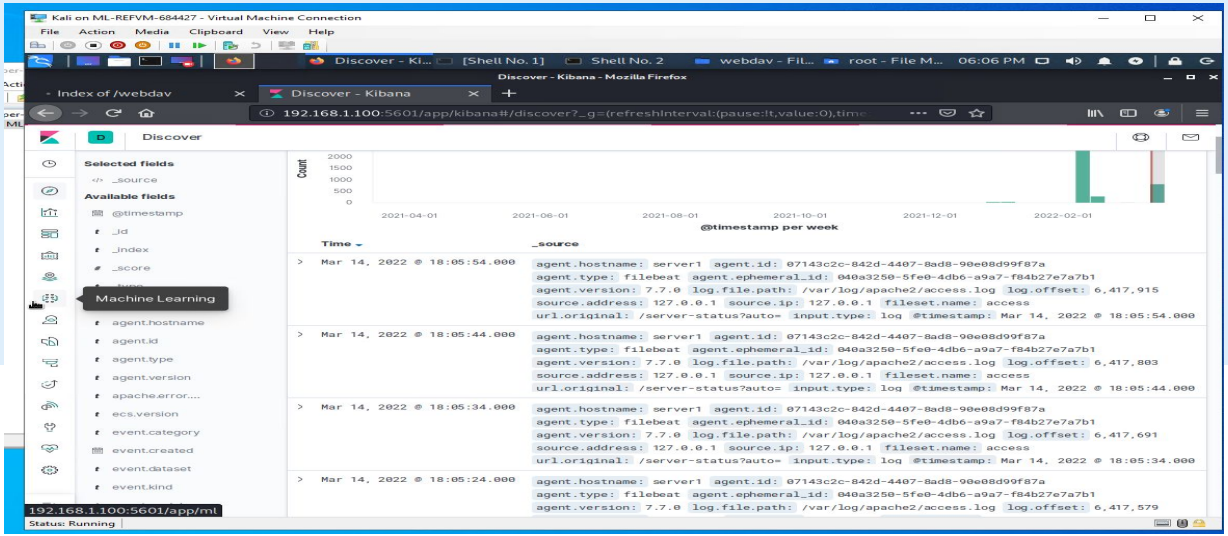
Analysis: Identifying the Port Scan

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?: Mar 14, 2022 @ 17:54:13
- How many packets were sent, and from which IP?

  7000 packets sent from 192.168.1.90
- What indicates that this was a port scan?

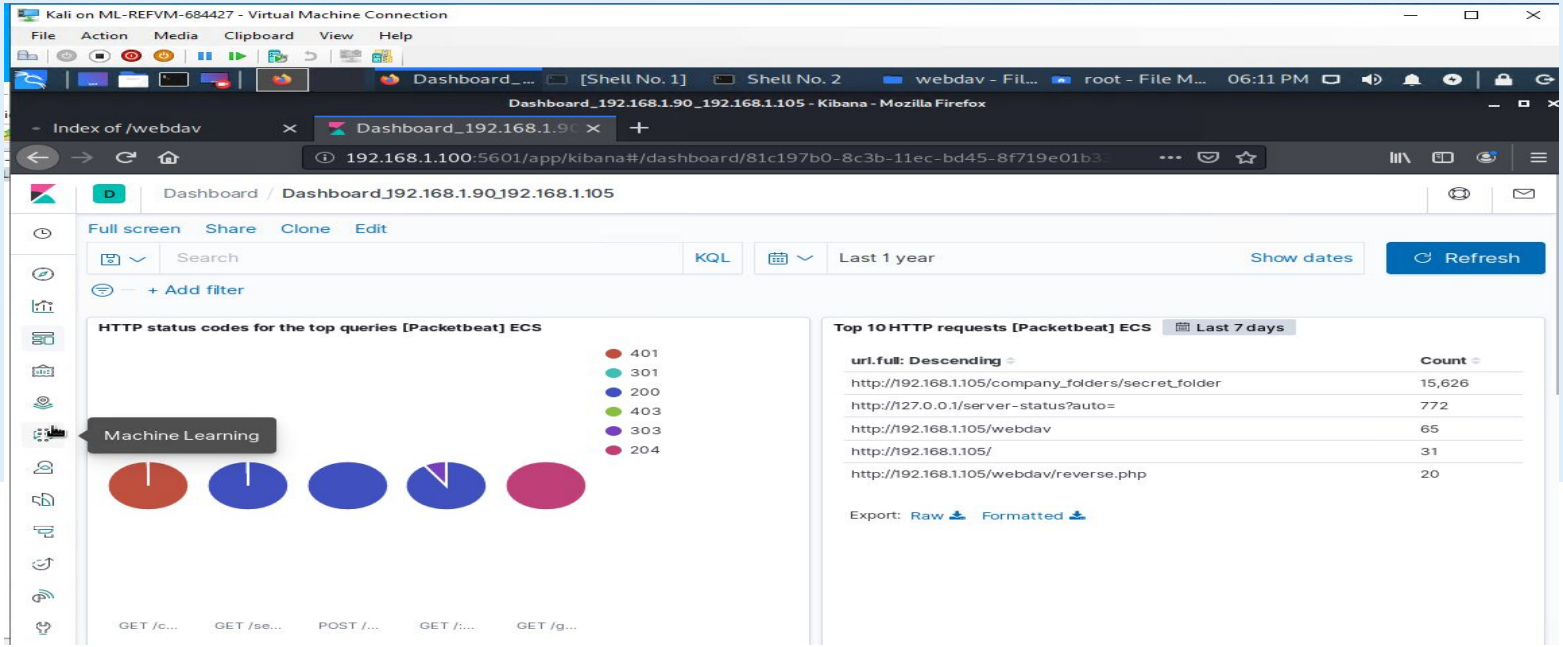
  “Destination.ip: 192.168.1.105



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.

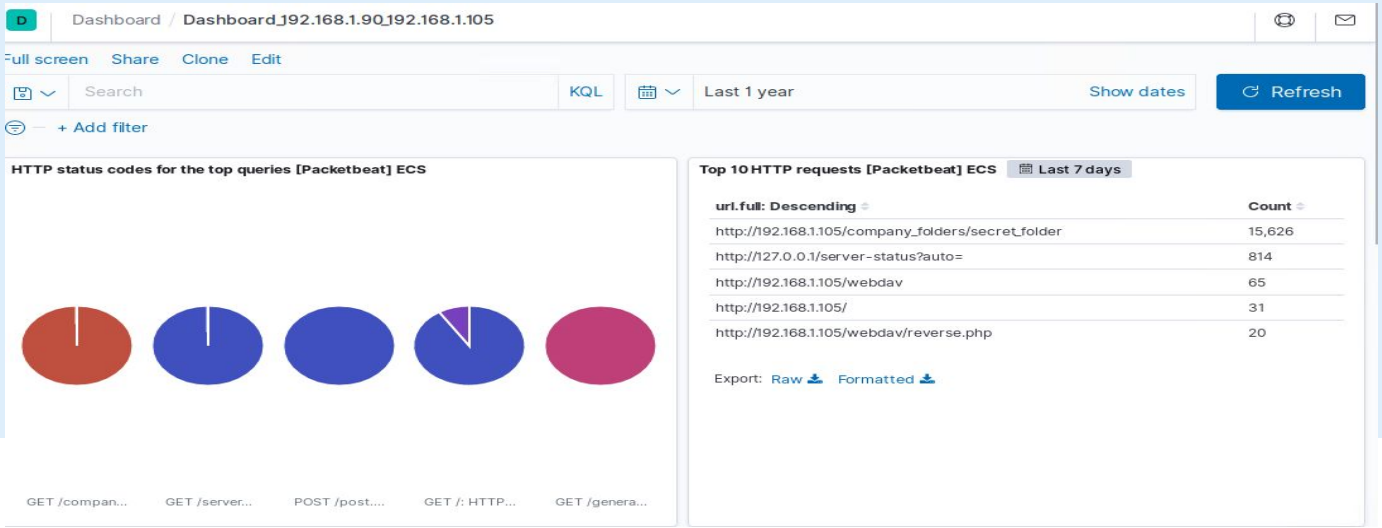
- The request occurred on Mar 14, 2022 with the request of 15,626 packets
- “Connect_to_the_corp_server” and contains the instruction on how to connect to the company server webdav.



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.

- 15,626 request we made before password was cracked.



Analysis: Finding the WebDAV Connection

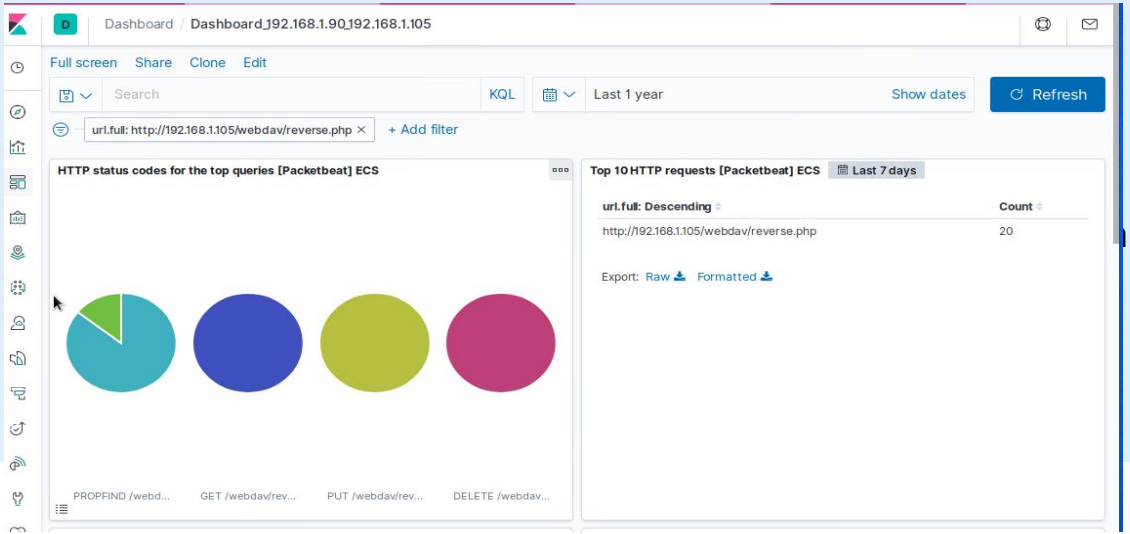
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory?

  20 requests

- Which files were requested?

  reverse.php



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 a low-level warning for any port scanning that exceeds a threshold of 10, and a serious alert for anything that exceeds 100.
- Set up notifications for every time Nmap is used.
- Set up a critical alert for scans that are too aggressive.

System Hardening

Allow just the traffic required to connect to internal hosts, and block anything else. TCP 80 for HTTP and ICMP for ping requests are among the typical ports. Create and configure IPtables for port blocking and scanning on the firewall. An IDS like Kibana or SPLUNK can notify you to port scan activity right away, allowing you to respond quickly to any risks.

Mitigation: Finding the Request for the Hidden Directory

Alarm

If a request for the concealed directories is made from outside the company's internal network, an alarm should be set to go off. The hidden folders are exclusively for internal usage and should not be accessible from the outside. The threshold for collected requests from a single IP address should be set at more than 0. When it's activated by an unknown IP, send an email to the SOC Analyst.

System Hardening

Users with access to the hidden folders must use stronger usernames and passwords. Disable the listing of folders in Apache. Encrypt the contents of the hidden directories, as well as the contents of the hidden directories.
Make a whitelist of IP addresses that are allowed to access your network. Change the permissions on the folder to make it private. Protect data in sensitive folders by encrypting it.

Mitigation: Preventing Brute Force Attacks

Alarm

If a specified amount of requests are sent to the server from a single IP address, an alert should be configured to go off, particularly if the requests return HTTP 401 (Unauthorized) answers. Because a brute force assault requires a large number of queries, this traffic might be stopped before the password is obtained. A threshold of more than 10 queries from an IP address in 30 minutes should be specified.

System Hardening

Every three months, increase the password strength requirements and the expiration date. To prevent brute forcing, set account timeout and lockout rules for unsuccessful password attempts.
After three password failures, a 30-minute countdown is started, which grows with each subsequent password failure until it reaches ten, at which point the user account is locked, a password expiration is triggered, and a critical alert is issued to the security team.

Mitigation: Detecting the WebDAV Connection

Alarm

If any access to the WebDAV directory is done from outside the company's internal network, an alert should be configured to go off.
If the WebDAV directory is visited, or if any files are uploaded to the directory, a single incident will raise an alert.

System Hardening

By default, the host should block WebDAV uploads and only allow uploads from a certain IP address.
The Apache configuration files may be used to do this. Ensure that all software patches are current. Disable WebDAV or double-check if it's set up properly.
For monitoring, install Filebeat on the host system.
iptables -A INPUT iptables -A INPUT iptables - —dports 80,443 -j ACCEPT -s [IP address] –p tcp –m multiport!

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alerts from anti-virus/anti-malware software should be set up to monitor all incoming uploads.
Create a file alert for questionable code/scripts/file extensions.
Any traffic trying to reach port 4444 may be alerted to. It is issued when one or more attempts are made to send the alert.
How to set up an alert for new files in the /webDAV folder? It is issued when one or more attempts are made to send the alert.

System Hardening

Make sure you have a safe anti-virus/anti-malware program installed that checks all incoming files and updates itself on a regular basis.
Firewall rules should be updated.
Limit the file types that may be uploaded, including php, for security reasons.
Make certain that just the most essential ports are open. You may prevent payloads from being uploaded by restricting access to the /webDAV folder to read-only permissions.


The End