Capstone Engagement

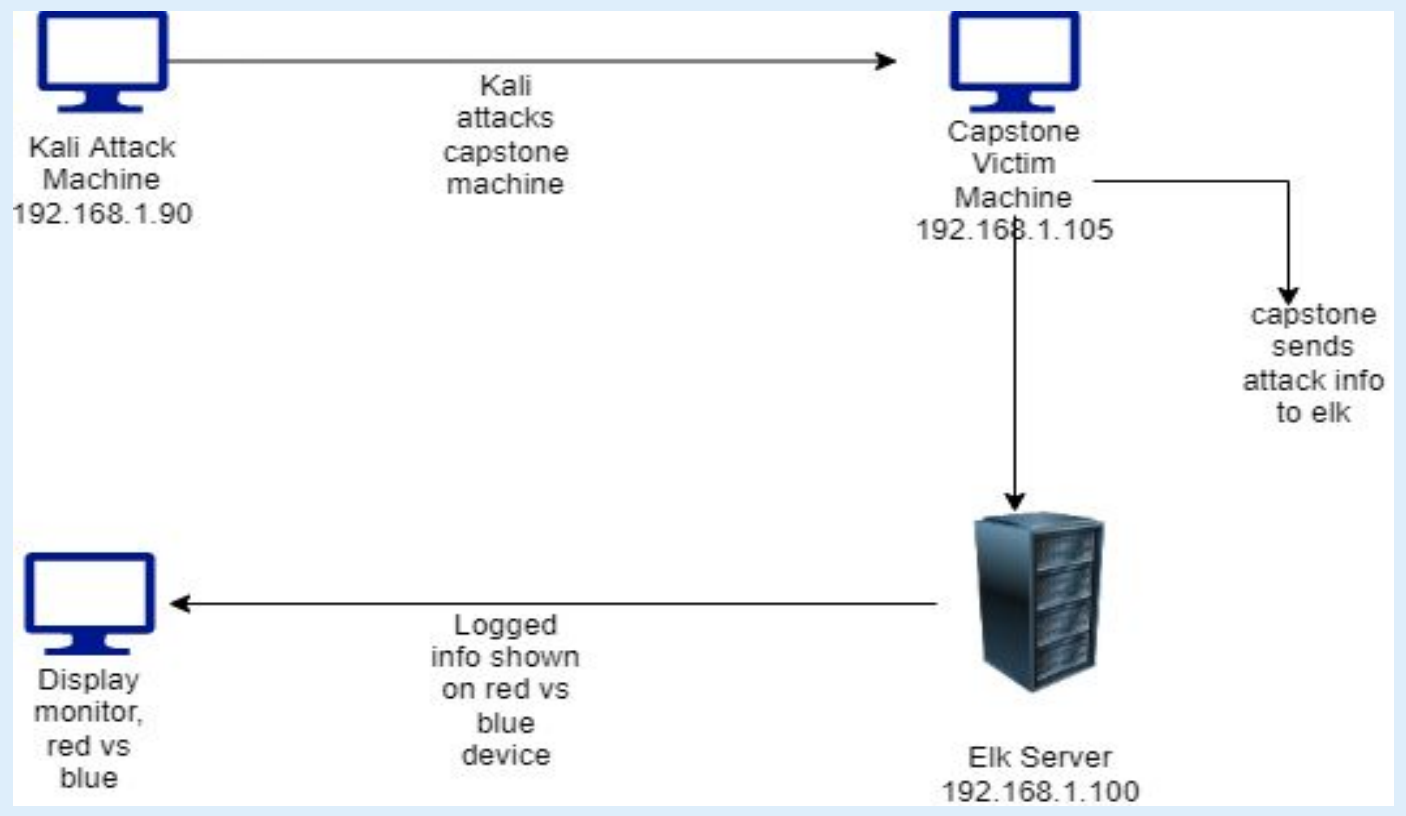
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk Machine

IPv4: 192.168.1.1
OS: windows
Hostname: Red vs Blue monitoring machine

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone Machine	192.168.1.105	Hosts the company server and webdav
Elk Server	192.168.1.100	Contains and Elk stack to log all traffic data and sends to Kibana for analyzing
RvB monitoring machine	192.168.1.1	
Kali	192.168.1.90	

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute Force	Password can be checked against a wordlist to “force” entry with common passwords.	Attackers can guess passwords for high ranking employees, access secret files and perform privilege escalation attacks
Accessible Folders/files	Folders and files are stored directly under root with unrequited access to everyone on the web server	Attackers are able to see root folders and contents within once forcing entry through port 80.
Port 80 open	Open ports can allow unwanted access to a network and increase attack platform as well as allow certain types of data transmission (in this case http)	Attackers are able to utilize open ports to gain access into a network and wreak havoc

Exploitation: Brute Force

01

Hydra's wordlist was used to check against ashton's password to allow unauthorized access.

02

Achievements
This allowed attackers not only access to the web server but elevated access with the ability to exfiltrate secret data.

03

Exploitation: Accessible Files

01

Tools & Processes

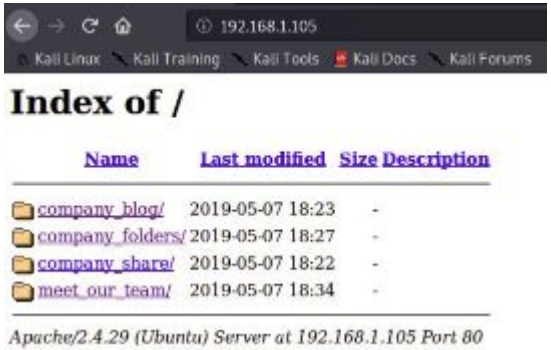
Once inside the network with correct credentials attackers were able to see all folder and file paths.

02

Achievements

With the knowledge of file and folder paths attackers were able to find instructions on how to access confidential data

03



Exploitation: Port 80

01

Tools & Processes

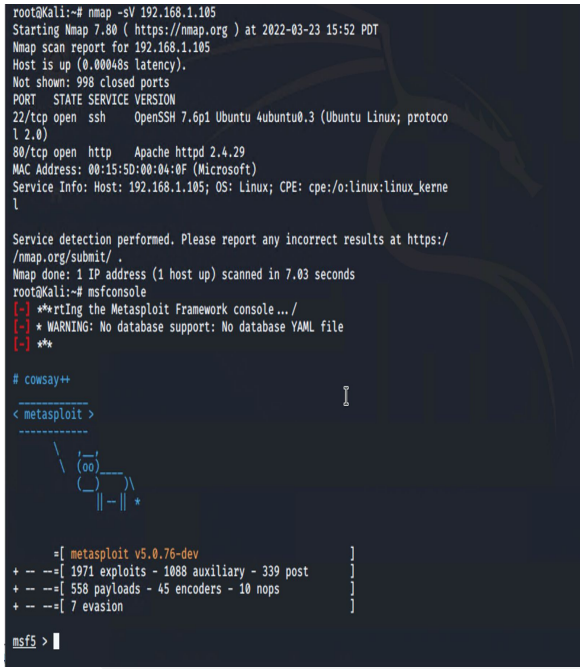
Nmap was used for a full network scan to identify IPs and open ports.

02

Achievements

Nmap came back with two open ports, 22 and 80 along with all IPs in the network

03

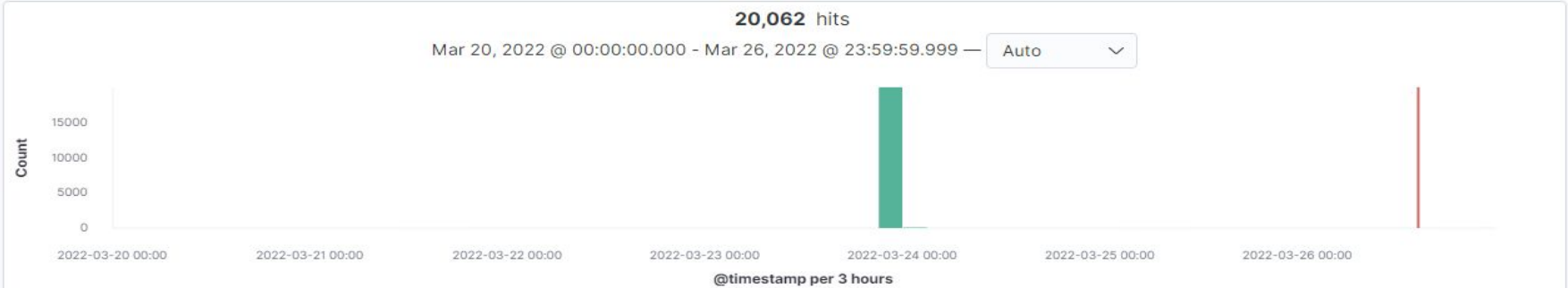


Blue Team
Log Analysis and Attack Characterization

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.

- Port scan occurred around 6pm est
- About 20k packets were transmitted from 192.168.1.90
- Nmap sends requests through port 443



Time	_source
Mar 24, 2022 @ 01:36:10.000	@timestamp: Mar 24, 2022 @ 01:36:10.000 event.start: Mar 24, 2022 @ 01:34:47.310 event.end: Mar 24, 2022 @ 01:35:29.806 event.duration: 42496.2 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow type: flow source.ip: 192.168.1.90 source.port: 4444 source.packets: 8 source.bytes: 1KB ecs.version: 1.5.0 host.name: server1 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRNuo flow.final: true network.packets: 13 network.type: ipv4 network.transport: tcp network.community_id: 1:tiQ/Zw2NWAsHeAsjaHAUmIhINR4= network.bytes: 1.8KB destination.port: 59958 destination.packets: 5
Mar 24, 2022 @ 01:36:00.003	@timestamp: Mar 24, 2022 @ 01:36:00.003 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Mar 24, 2022 @ 01:34:46.914 event.end: Mar 24, 2022 @ 01:35:29.921 event.duration: 43007.5 type: flow host.name: Kali agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: b131840c-9c5c-4fa2-ba8e-80d7c191748d flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRNuo flow.final: true network.packets: 13 network.type: ipv4 network.transport: tcp network.community_id: 1:tiQ/Zw2NWAsHeAsjaHAUmIhINR4= network.bytes: 1.8KB
Mar 24, 2022 @ 01:36:00.000	@timestamp: Mar 24, 2022 @ 01:36:00.000 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRNuo flow.final: false ecs.version: 1.5.0 host.name: server1 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat

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.

- Around 6:30 pm 18 requests were made for the secret directory
- The files requested were the secret files which contained instructions how to ssh onto the target machine

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/sales_docs/file1.txt	96
http://192.168.1.105/	28
http://192.168.1.105/company_folders/secret_folder/	18
http://192.168.1.105/webdav/	18
http://192.168.1.105/company_folders/	10

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.

- A little more than 21,500 attempts were made
- 95 failed attempts before the correct password was found on the 96th trv

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.

- 18 requests were made to this directory
- Shell.php was requested which allowed a reverse shell connection for attackers

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/sales_docs/file1.txt	96
http://192.168.1.105/	28
http://192.168.1.105/company_folders/secret_folder/	18
http://192.168.1.105/webdav/	18
http://192.168.1.105/company_folders/	10

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm that detects port scans that are aggressive or for when nmap is used at all.

Set an alarm for when a rarely used port is scanned (7,9,19)

Scans of rarely used ports of a few or more should trigger an alarm.

System Hardening

To mitigate port scans you could allow only local network access and deny external traffic.

Redirect to a honeypot.

Iptables to set up a honeypot and create logs to highlight the intrusion on a monitoring dashboard.

Mitigation: Finding the Request for the Hidden Directory

Alarm

We can set alarms to trigger when sensitive directory is accessed more than a number of times in a given period of time.

Threshold will be 3x within 10 minutes

System Hardening

Remove the directory from main file server to remove from public view
“rm -r ../company_files”
Do not allow everyone access to this directory, use most restrictive practices.
Don't announce the path to secret folder in any documents.
Firewalld Configurations:
“sudo firewalld-cmd --permanent--new-zone=encrypted”
Add verified IP address
“sudo firewall-cmd --zone=drop --permanent --add-source=<IP>”

Mitigation: Preventing Brute Force Attacks

Alarm

A critical alarm can be set if there are more than 10 attempts on the same user account trying to be accessed. While also setting low level alarms for more than 3 failed attempts. Also, alert triggers can be based on established trends of each user.

Follow windows server lockout policy (something like Local Group Policy Editor GPE)

System Hardening

Direct Brute Force Attackers to a Honeypot

Create a blacklist of malicious IPs based on attempts in the past 6 months and can lead to training measures if an employee is involved

Password complexity requirement
MFA
CAPCHAs
account lockouts
account timeouts

Mitigation: Detecting the WebDAV Connection

Alarm

Create and alert any time directory is accessed by a user other than the user with proper clearance
Create a whitelist of trusted ip and review every 6 months, set alerts for any non-whitelisted IP trying to connect to WebDAV
On HTTP GET request, set an alarm that activates on an ip address that tries to access webdav

Threshold can be set to one attempt

System Hardening

Limit user access to webdav
Harden webdav authentication
Scanning incoming traffic with anti virus software
Update regularly
Upgrade to more secure applications
Only use webdav with internal access within the company

Mitigation: Identifying Reverse Shell Uploads

Alarm

Set an alarm for anything using port 4444

Set an alarm for use of any suspicious file extension or scripts. in the server

Set an alarm for anything triggered by an anti-virus software.

Threshold should be set at 1 attempt

System Hardening

Remove ability to upload files to this directory through the web interface

Disabling HTTP PUT method to prevent file uploading.

Setup secure anti-virus application to screen all incoming files with daily automatic update.

Update firewall rules bi-monthly


The End