

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

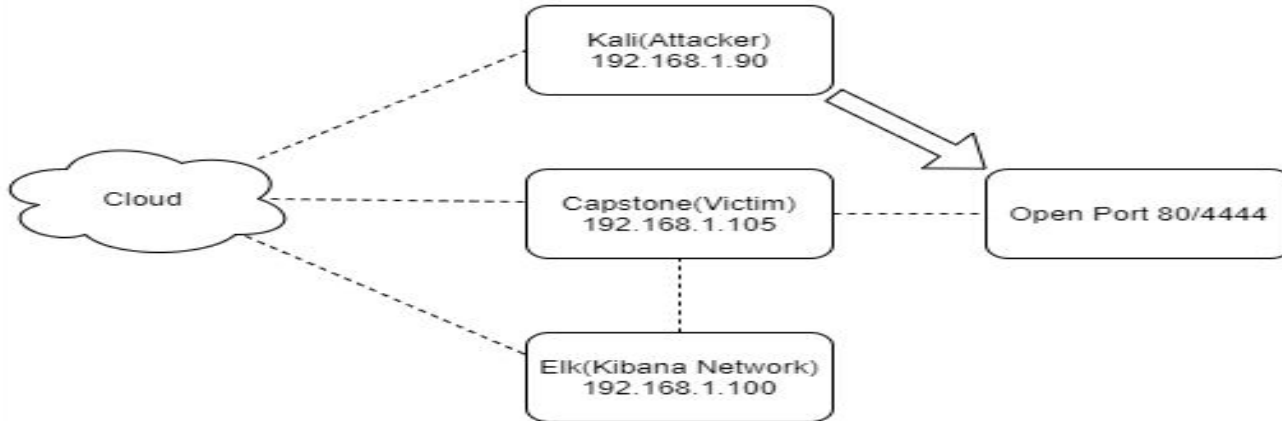
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network 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: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: Elk

IPv4: 192.168.1.1
OS: Windows Cloud
Hostname: Azure

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Victim Machine
Kali	192.168.1.90	Attacking Machine
ElkStack Kibana	192.168.1.100	Network Monitoring Logs
Azure	192.168.1.1	Cloud Server Host

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open HTTP port 80 with public access.	Unsecured public access to the HTTP server and directory accessible.	With path traversal attackers can find secret directories on the system and work their way in.
Server susceptible to Brute Force attacks.	Attacker will input many Username/Password combinations to gain access.	Once inside the network they have access to private company files.
WebDav Plain Text Credentials	Blank text that provides a framework for users to create, change, and move documents on a server.	Allows an attacker to gain privilege escalation by changing or creating documents.

Exploitation: [Open HTTP]

01

Tools & Processes

Used Nmap scan on the server to determine that port 80 was open.

02

Achievements

Granted access to the server directory. Where we used Path Traversal to move around through the system and find hidden files to access the server.

03

Ifconfig

```
nmap -sV -sC -O  
192.168.1.0/24
```


Exploitation: [Brute Force Attack]

01

Tools & Processes

Brute Force attack using
Hydra

02

Achievements

Access to an admin user
account.

03

```
hydra -l ashton -P  
/usr/share/wordlists/rockyou  
.txt -s 80 -f -vV 192.168.1.90  
http-get  
/company_folders/secret_fol  
der
```

Exploitation: [WebDav]

01

Tools & Processes

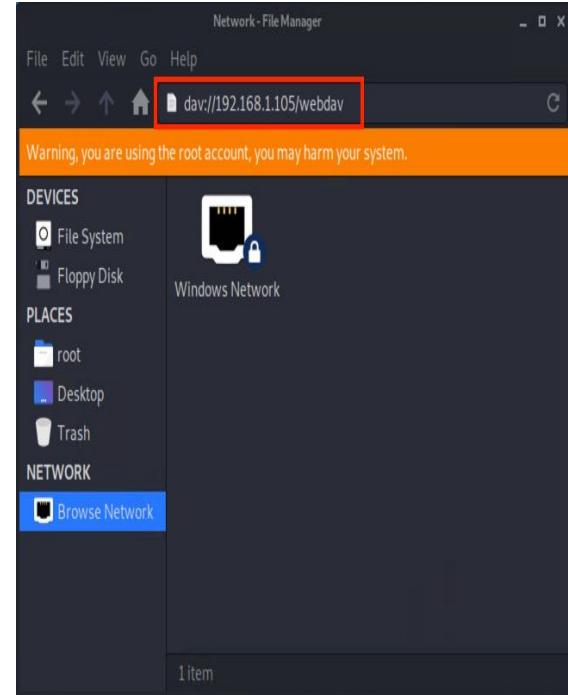
Once gaining access to an admin account, we found the password hash to access the WebDav.


02

Achievements

It granted us access to upload a shell script to be run to gain full access to the server.

03





Blue Team

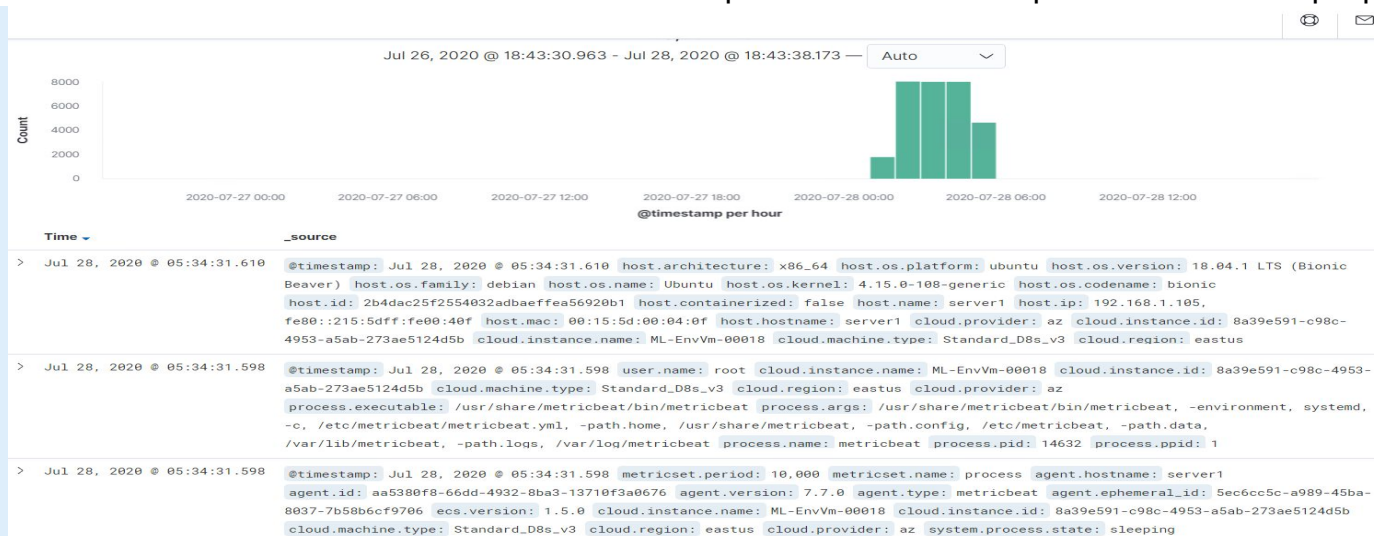
Log Analysis and Attack Characterization

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? 1:30PM-2:50PM
- How many packets were sent, and from which IP? About 1800 requests were sent from 192.168.1.90
- What indicates that this was a port scan? Multiple requests from and to a specific IP over multiple ports



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?

There were about 16000 requests between 2:30 and 2:45.

- Which files were requested? What did they contain?

/secret_folder - Log in information to the server.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending


http://192.168.1.105/company_folders/secret_folder

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? 6,209
- How many requests had been made before the attacker discovered the password? 6,208

Top 10 HTTP requests [Packetbeat] ECS 

url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/secret_folder	6,209

Export: Raw  Formatted 

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? 28
- Which files were requested? Shell.php, passwd.dav, and connect_to_corp_server

<code>http://192.168.1.105/webdav</code>	28
<code>http://192.168.1.105/webdav/shell.php</code>	24
<code>http://192.168.1.105/webdav/passwd.dav</code>	4
<code>http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server</code>	3



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?

- Primary alarm/method of detection for port scans is through an IDS(Intrusion Detection System) or IPS(Intrusion Prevention System)

What threshold would you set to activate this alarm?

- An Example, a machine trying to create 1000 connections using multiple ports with a server is not normal.

System Hardening

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

- IDS/IPS monitor the system.

Describe the solution. If possible, provide required command lines.

- Configure the IDS to recognize a scanning attempt, IPS to either alert or block the offending IP address of an attacker.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Set an alert for whenever someone tries to access this directory.
- Set an alert for unauthorized access for this directory at a specific time.

What threshold would you set to activate this alarm?

- Alert whenever someone tries to get access to this directory.
- Unusual/Off Times. Like unusual hours and closed times.

System Hardening

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

- The whole directory and file should be removed from the server.

Describe the solution. If possible, provide required command lines.

- Remove the whole directory and files and should be placed on a whole other server.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Set alert for failed user account login/logon attempts.

What threshold would you set to activate this alarm?

- Baseline threshold for failed user account login/logon attempts.

System Hardening

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

- Multi-factor authentication
- Required Password change after a number of failed logins.

Describe the solution. If possible, provide the required command line(s).

- Set up 2-factor authentication for everyone.
- Force required password change after a set number of failed logins.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Set an alert for any unauthorized machines/IPs/MAC address trying to access the vulnerable machine.

What threshold would you set to activate this alarm?

- Threshold would be set to have an alert go off whenever an IP that is not authorized attempts to connect to the machine.

System Hardening

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

- Connections to this shared folder should be restricted and web interface connection should not be allowed.

Describe the solution. If possible, provide the required command line(s).

- Set up a firewall rule to restrict connections to this shared folder.
- Block connection access to this shared folder from the web interface.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alarm for any traffic moving over port 4444.
- Alarm for any .php file that is uploaded to the server.

What threshold would you set to activate this alarm?

- Any traffic moving over port 4444.
- Any file that is uploaded to the server.

System Hardening

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

- Remove the ability to upload files to this directory over the web interface.

Describe the solution. If possible, provide the required command line.

- Use file and group permissions to prevent unauthorized access and changes.

*The
End*