Capstone Engagement

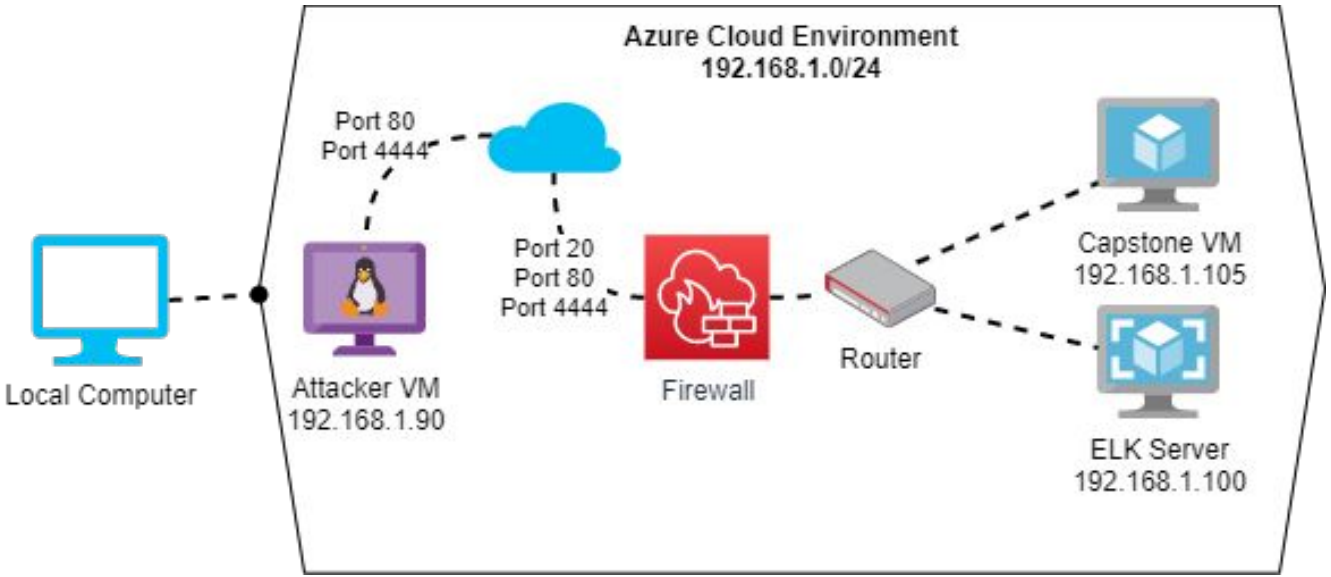
Assessment, Analysis, and Hardening of a Vulnerable System

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: 10.0.0.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Azure cloud

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

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	Azure Cloud Environment
Kali Linux	192.168.1.90	Red Team : Offensive Machine
ELK Server	192.168.1.100	Blue Team : Defensive Machine
Capstone VM	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute-Force Attack	Force method using a list of possible passwords.	Attacker able to query the server if the username is available. Attacker able to access sensitive information and able to take control of a system.
Credential stored in web file	Credential to user's account with administrative privileges are stored on web server.	Easily achievable credentials on web server that able to exploit, inject script and loss of sensitive data.
Gain-privilege script injection	Open to script injection for user who shouldn't able to upload and execute files.	Vulnerable to data leak, stolen and loss of control.

Exploitation: [Brute-Force Attack]

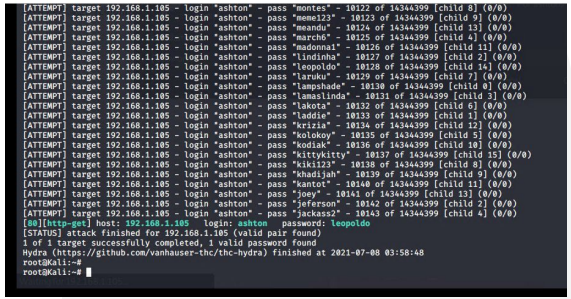
01

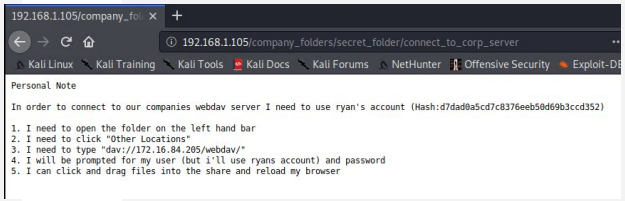
Tools & Processes
Nmap and Hydra

02

Achievements
Credential Access to sensitive information

03





Exploitation: [Credential Web App]

01

Tools & Processes
crackstation.net

Decode Ryan’s password hash.

02

Achievements
Username and password to webdav.

Lateral movement.

03

Exploitation: [Name of Third Vulnerability]

01

Tools & Processes

Metasploit

- MSFvenom

Payload generator.

- Meterpreter

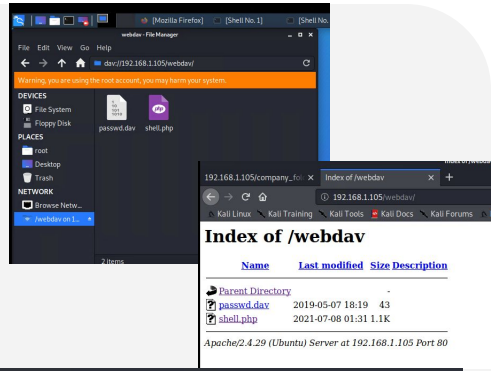
The payload that provides a reverse shell.

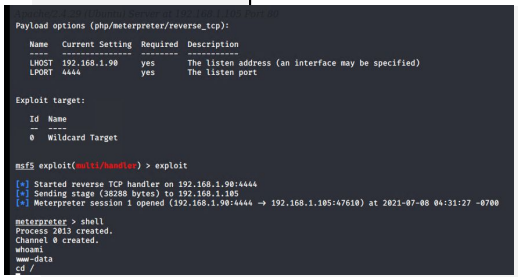
02

Achievements

Execution and remote control the target's machine.

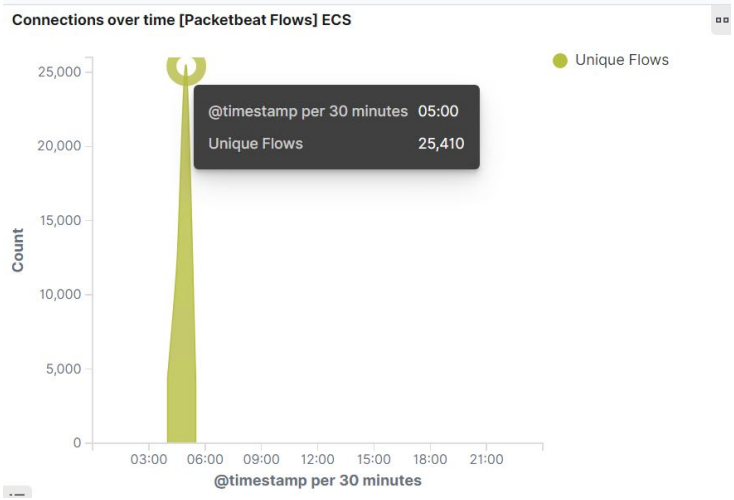
03





Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

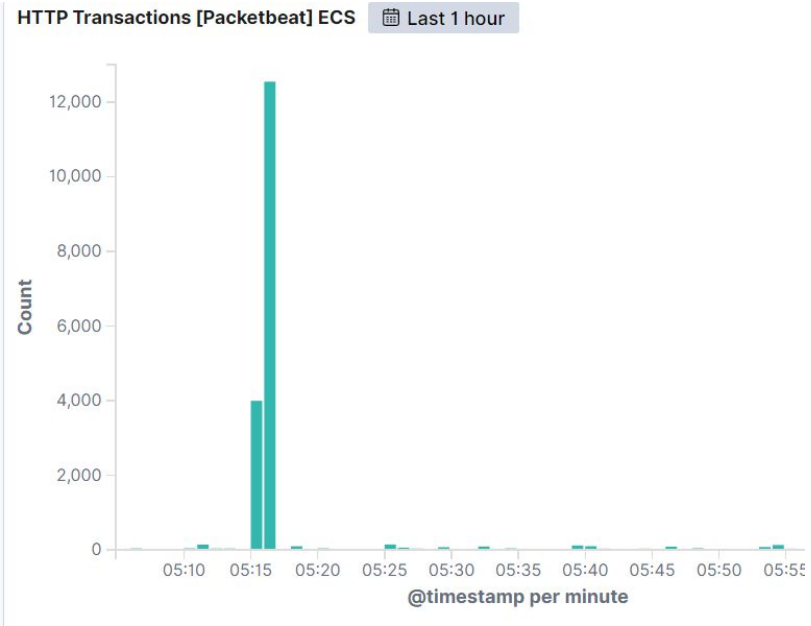


Network Traffic Between Hosts [Packetbeat Flows] ECS

192.168.1.90	192.168.1.105	52.7MB	94MB
192.168.1.90	192.168.1.1	587.5KB	2.3KB
192.168.1.90	192.168.1.90	586.5KB	546.9KB
192.168.1.90	172.217.2.106	87.5KB	26.7MB
192.168.1.105	192.168.1.100	21.6GB	917.6MB
192.168.1.105	91.189.88.142	170.9KB	44.9MB
192.168.1.105	169.254.169.254	30.6KB	75.2KB
192.168.1.105	91.189.92.41	28.4KB	14.7KB
192.168.1.105	91.189.92.38	25.1KB	4.8MB

- What time did the port scan occur?
  - Jul 18, 2021 @ 05:17:30.004
- How many packets were sent, and from which IP?
  - 25,410 from 192.168.1.90
- What indicates that this was a port scan?
  - Port scan is identified by the broadcast address 192.168.1.105

Analysis: Finding the Request for the Hidden Directory

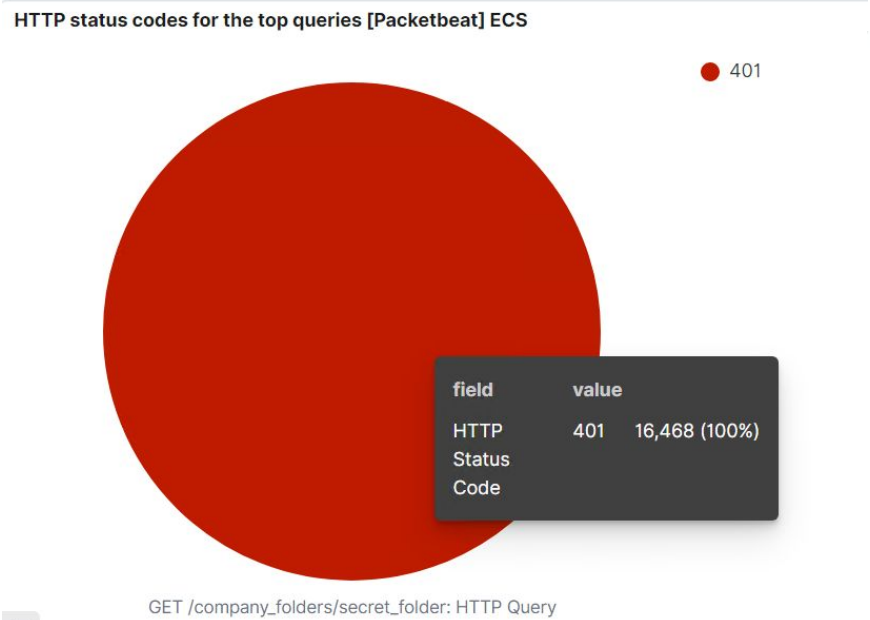


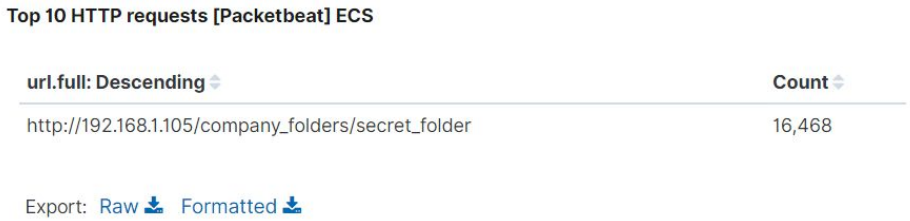
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,476
http://127.0.0.1/server-status?auto=	635
http://snnmnkxdhflwgthqismb.com/post.php	98
http://www.gstatic.com/generate_204	49
http://ocsp.godaddy.com	24

- What time did the request occur? How many requests were made?
  - 05:15
  - 16,475
- Which files were requested? What did they contain?
  - http://192.168.1.105/company_folders/secret_folder
  - How to connect to company's server.

Analysis: Uncovering the Brute Force Attack





- How many requests were made in the attack?
  - 16,468 requests were made during the attack
- How many requests had been made before the attacker discovered the password?
  - 16,465 request had been made before the attacker discover the password.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,476
http://127.0.0.1/server-status?auto=	990
http://snnmnkxdhflwgthqismb.com/post.php	140
http://www.gstatic.com/generate_204	76
http://192.168.1.105/webdav	38

- How many requests were made to this directory?
  - 38
- Which files were requested?
  - http://192.168.1.105/webdav

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- An Intrusion Detection System can arranged to recognize a scan attempt.
- An Intrusion Prevention System can alert or block the suspicious IP address from the attacker.
- Setup an alarm when IPS request to attempts at TCP connections over various ports. Kibana able to detect and show there is a port scan occurring and then we able to block before any further steps are taken by an attacker.

System Hardening

- Logging of TCP connection attempts
- Firewall configurations
- Deployment of IDS/IPS systems
  - Alerts for unusual port scans.
  - Block port scans

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Set alarm for any connection made to http://192.169.1.105/company_folders/secret_folder

System Hardening

- Creating a white-list to limit IPs that able to access into company's files and directories.
- Remove sensitive data (such as password, and how to get into company's webdav) from server.

Mitigation: Preventing Brute Force Attacks

Alarm

- Set alarm to detect status code 401 when login requests are made more than four times.
- Detect any IP that notice Hydra in <user_agent.original>

System Hardening

- Use Multi-factor authentications
- Send alert and lock account after fourth time failed to login.
- Block any IPs that <user_agent.original> noticed Hydra.

Mitigation: Detecting the WebDAV Connection

Alarm

- Set alarm in any connection to http://192.168.1.105/webdav

System Hardening

- Creating Whitelist of limited IPs that able to access to Webdav
- Set two-factor authentication.
- Don’t allow storage of passwords and credentials for network authentication.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set alarm:
  - When there are traffic over port 4444 because it's Meterpreter's default port.
  - When there are files uploaded to server

System Hardening

- Creating Whitelist for limited IPs that able to upload files and directories.
- Block all outgoing traffic by default on the WAN connection.
- Run chmod 700
  - This command allow only owner to read,write, and execute.


The End