Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

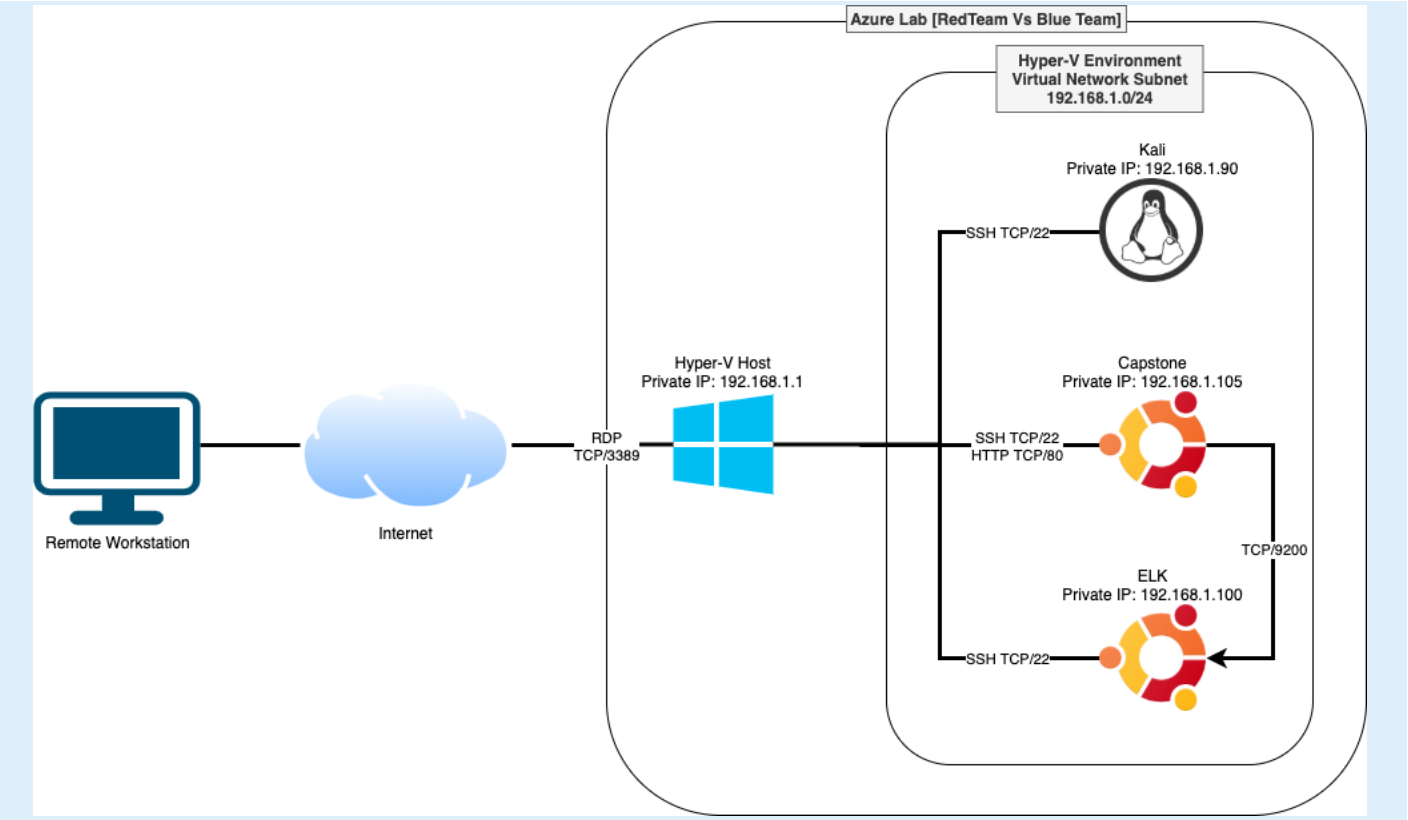
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address Range:
192.168..1.1 ~
192.168.1.254
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux 2020.1
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04 LTS
Hostname: capstone
(server1)

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Gateway	192.168.1.1	Gateway, Hyper-V Host
Kali	192.168.1.90	Pentester
ELK	192.168.1.100	SIEM
Capstone (Server1)	192.168.1.105	Webserver, Vulnerable Target)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Network vulnerable to port scan	Finding an active port on a host and exploit a known vulnerability of that service	Able to locate the active port of Capstone and obtain webserver directory listing and structure.
Hidden folder vulnerable to unauthorized access	Website contains confidential accessing information to the public.	Able to obtain webserver secret folder location is vulnerable to brute force attack
Password vulnerable to brute force attack	Gain access to a restricted resource by using the most commonly used usernames and passwords	Able to retrieve Ashton's password by using Hydra
WebDAV vulnerable to reverse shell attack	Let the attacker's machine run shell script on the target's machine	Able to upload paul.php to WebDav and open remote session to run shell commands locally

Exploitation: [Network Port Scan]

01

Tools & Processes

Tools: nmap

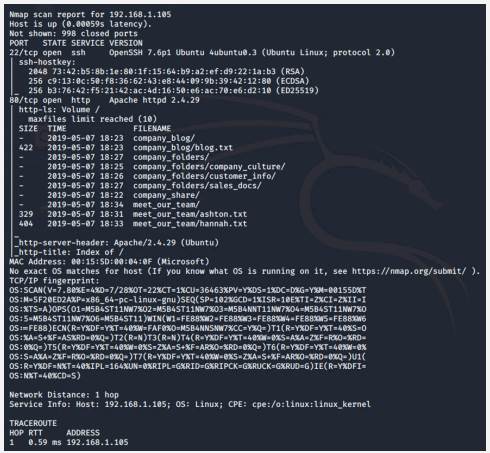
Command:
nmap -A 192.168.1.1/24

02

Achievements

Able to obtain capstone's active ports and web directory listings

03



Exploitation: [Hidden Folder unauthorized access]

01

Tools & Processes

Tools: Web Browser, Hydra, Crackstation
Use web browser to obtain information from files within /meet_our_team/ and shows there is a secret_folder that can be access by Ashton
Use Hydra to obtain the password of Ashton
Use Crackstation to obtain Ryan's password from hashes inside secret folder

02

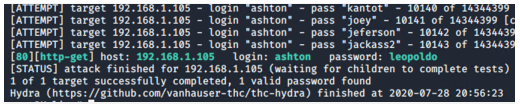
Achievements

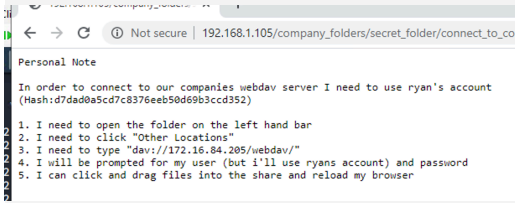
Able to reveal there is a hidden folder inside company_folders and then

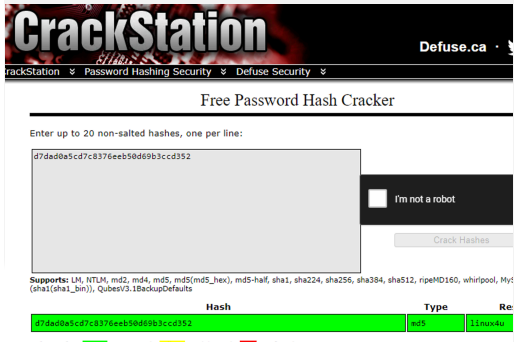
Obtain Ashton's password of Ashton and get access to the secret_folder

Obtain Ryan's password and reveal the access information of WebDav folder

03







Exploitation: [WebDav Reverse Shell Attack]

01

Tools & Processes

msfvenom: create a custom script for the reverse shell attack

cadaver: Use to upload customed php script to webdav folder

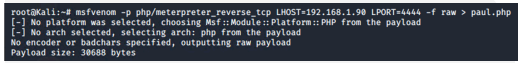
msfconsole: Perform a reverse shell attack

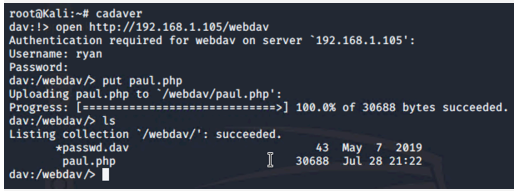
02

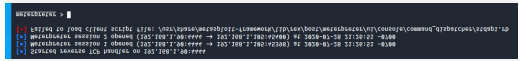
Achievements

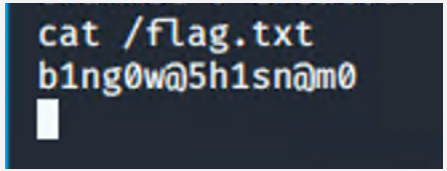
Able to run customized script paul.php and let the pentester run meterpreter script to locate and obtain the flag.txt from root folder

03



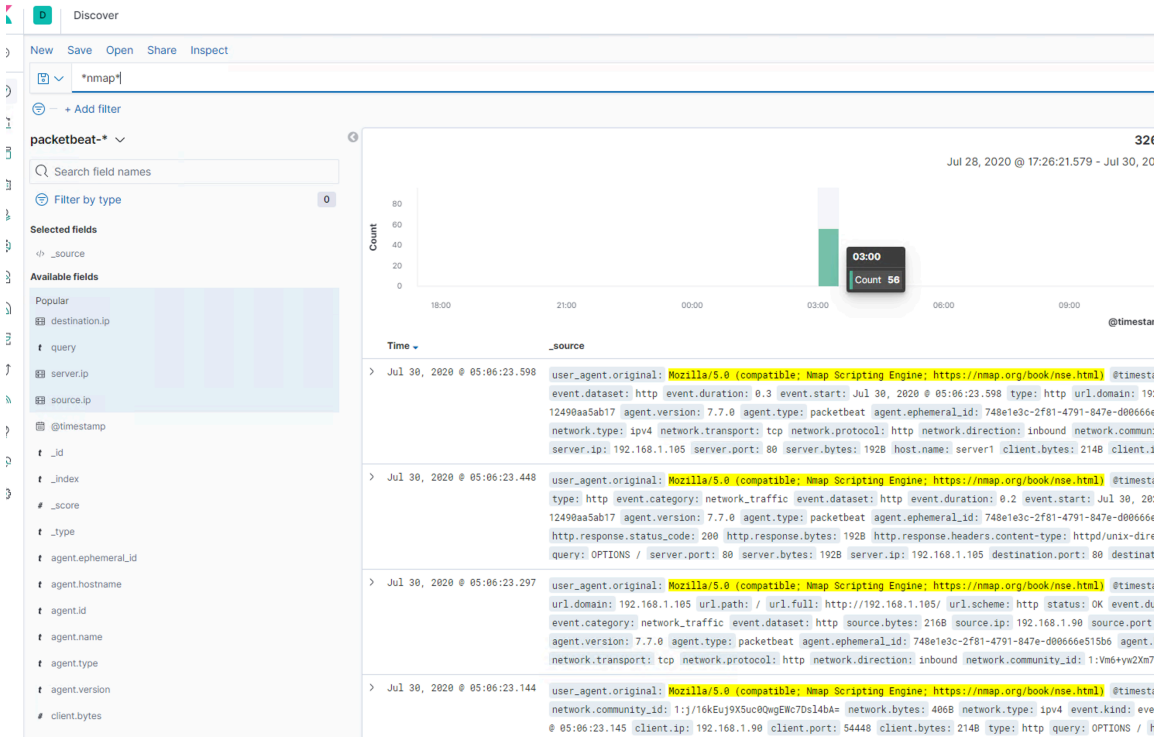






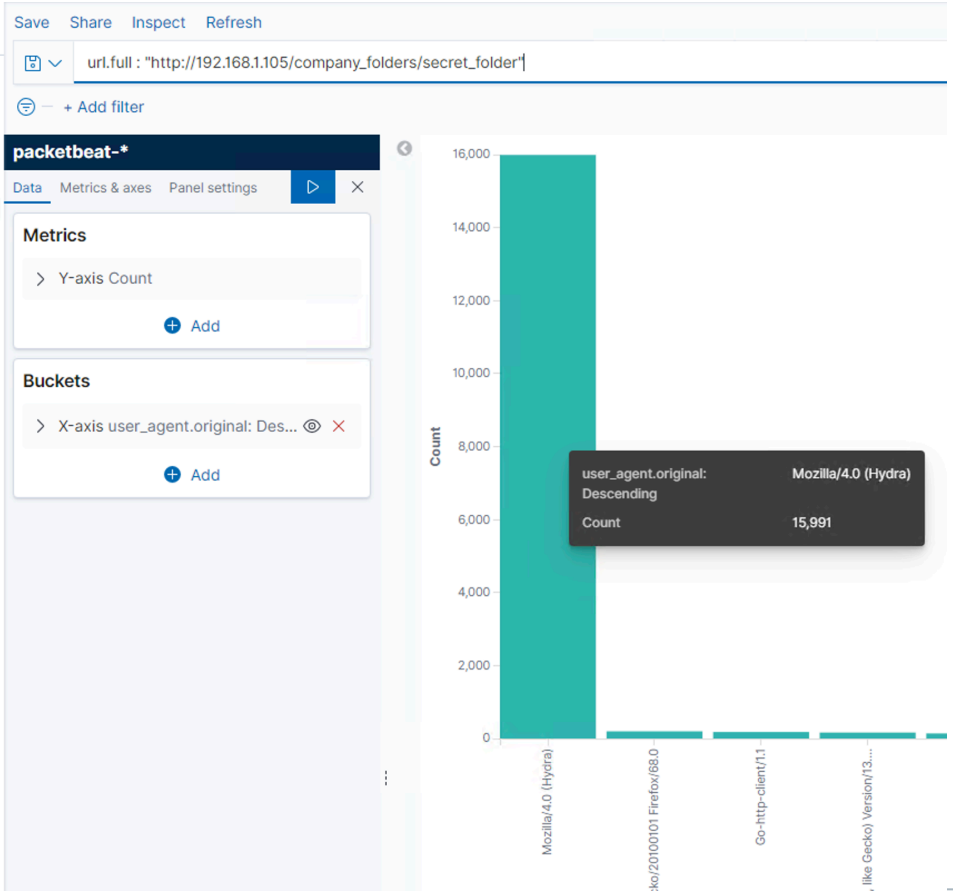
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



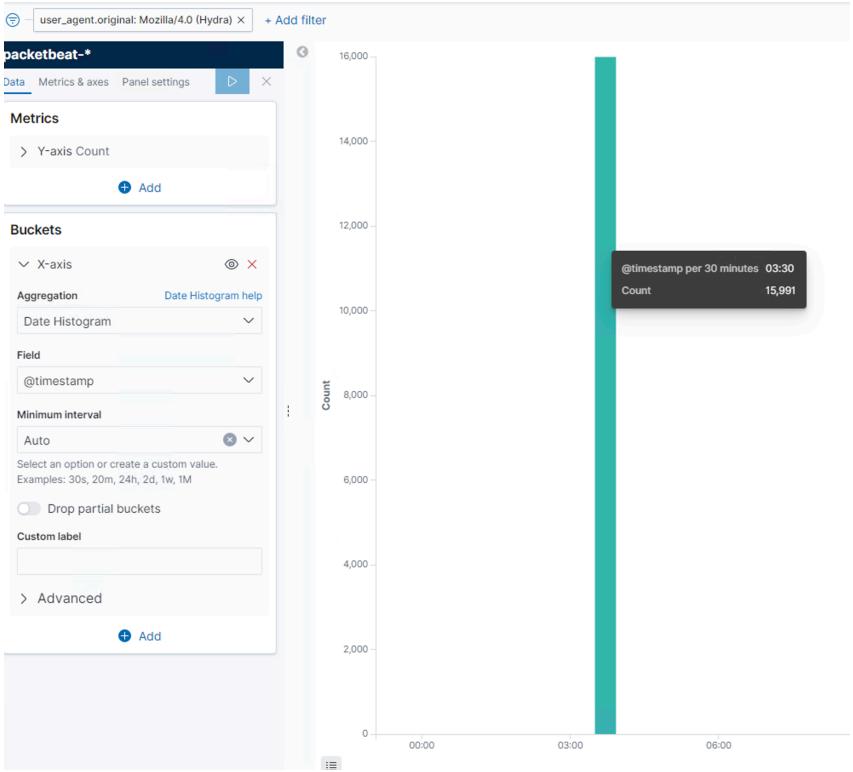
- The port scan occurred at 3:29 am on 7/29/2020
- There were 56 packets were sent, and from 192.168.1.90
- The user agent shows it is from nmap

Analysis: Finding the Request for the Hidden Directory



- The request occurred at 22:26 PM on July 29, 2020. And there are 15991 requests are made.
- It was requesting connect_to_corp_server file inside the secret_folder

Analysis: Uncovering the Brute Force Attack



- There were 15991 requests were made in the attack.
- There were 15990 requests had been made before the attacker discovered the password.

Analysis: Finding the WebDAV Connection

Time	_source
Jul 29, 2020 @ 04:09:50.756	url.full: http://192.168.1.105/webdav/ @timestamp: Jul 29, 2020 @ 04:09:50.756 user_agent.original: cadaver/0.23.3 neon/0.30.2 http.request.headers.content-length: 0 http.request.method: options http.request.bytes: 146B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 720B http.response.body.bytes: 460B http.version: 1.1 status: Error ecs.version: 1.5.0 agent.type: packetbeat agent.ephemeral_id: e218da9a-a018-41ba-8f8e-0681c4455fdd agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 destination.port: 80 destination.bytes: 720B destination.ip: 192.168.1.105 source.bytes: 146B source.ip: 192.168.1.90 source.port: 49692 server.ip: 192.168.1.105 server.port: 80
Jul 29, 2020 @ 04:09:50.682	url.full: http://192.168.1.105/webdav/ @timestamp: Jul 29, 2020 @ 04:09:50.682 source.ip: 192.168.1.90 source.port: 49692 source.bytes: 146B network.bytes: 866B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound network.community_id: 1:wQ3z7YwKaNow8rmQvoh8ElxaZ2A= url.domain: 192.168.1.105 url.path: /webdav/ url.scheme: http http.version: 1.1 http.request.method: options http.request.bytes: 146B http.request.headers.content-length: 0 http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 720B http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 status: Error method: options query: OPTIONS /webdav/ client.ip: 192.168.1.90 client.port: 49692 client.bytes: 146B agent.type: packetbeat agent.version: 7.8.0

- There were 2 requests were made to this directory.
- It was requested the paul.php which is the reverse shell php inside the webdav folder

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?

Detect Nmap user agent

What threshold would you set to activate this alarm?

Any source ip with nmap user agent detected more than 1000 times in 30 mins

System Hardening

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

Firewall rules to detect user agent

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

url path = hidden directory besides whitelisted ip

What threshold would you set to activate this alarm?

Any ip is not whitelisted ip AND
URL path is hidden directory
More than 2000 times in 30 minutes

System Hardening

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

Set allow ip address for specific folder access

Mitigation: Preventing Brute Force Attacks

Alarm

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

Detect user agent original is Hydra

What threshold would you set to activate this alarm?

Any source ip with user agent is Hydra

System Hardening

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

- Use of user certificate
- Captcha
- Multiple user authentication

Mitigation: Detecting the WebDAV Connection

Alarm

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

Detect URL path is WebDav AND
IP address is not whitelisted ip

What threshold would you set to activate this alarm?

If URL path contains webdav and source up is not whitelisted ip

System Hardening

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

- Use of SSL certificate
- Multiple Factor Authentication
- Use of IP and domain filtering
- Prevent File execution
- Use Request filtering to block certain type of file extension
- Use of stateful firewall

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

When http method is PUT and source ip is unknown ip addresses.

What threshold would you set to activate this alarm?

System Hardening

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

- impose strict control of outgoing connections


The End