Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

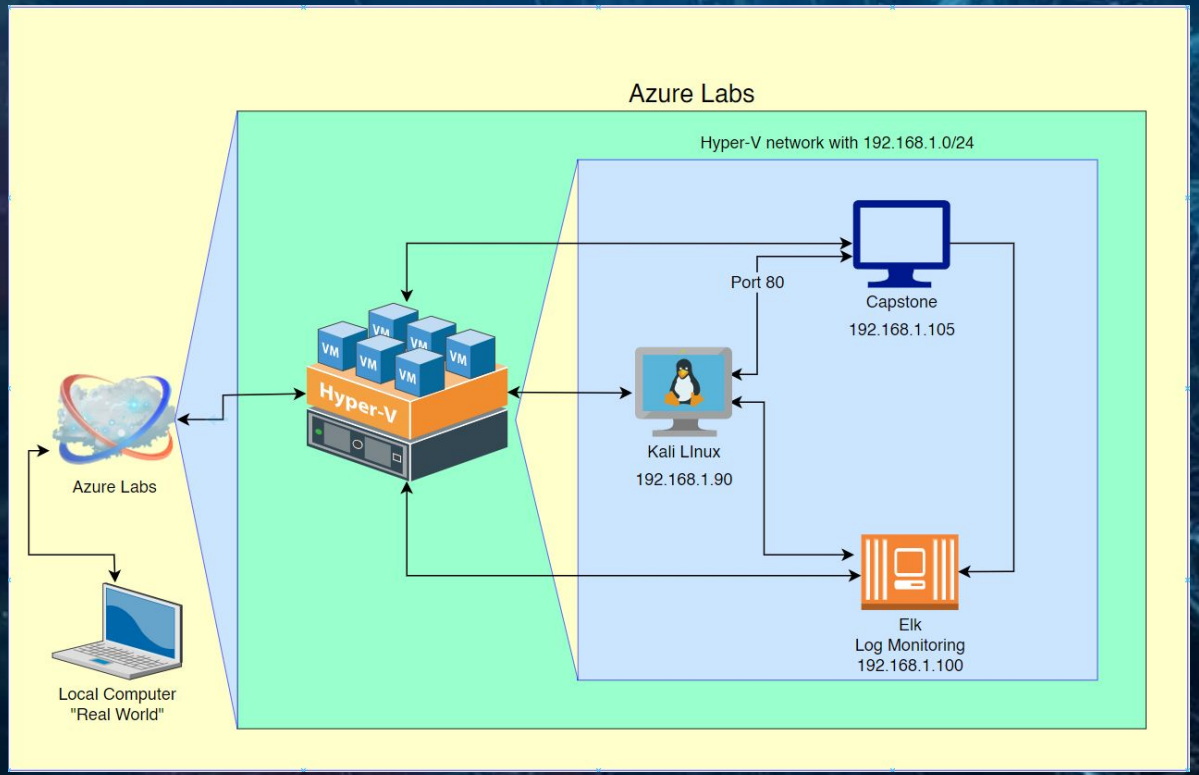
Background: Google image Search in Google Docs

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: 192.168.1.1
OS: MS 10.0.19041.1
Hostname: Hyper-V

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali Linux

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4
Hostname: Elk

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V	192.168.1.1	This is a container for all the Virtual Machines
Kali Linux	192.168.1.90	This is a Virtual Machine that is used for reconnaissance or to attack another machine
Elk	192.168.1.100	This is a LIstener device to retrieve data from a target machine to sort and parse the information
Capstone	192.168.1.105	This is the target machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Insufficient Logging and Monitoring	No alerts are configured to be sent for active attacks in real or close to real time.	Security personnel not alerted to breach in real time that allows attackers to penetrate further.
Bruteforce Attack Vulnerability *CVE-2020-14494*	Able to gain access to web application using brute force.	A bruteforce attack vulnerability allows attackers to gain unauthorized access to sensitive data.
Sensitive Data Exposure	The sensitive data present in secret_folder is accessible to the public	The attacked is able to use this data to cause further harm.
Unrestricted File Upload	Insufficient controls on who can upload files to the server.	Unauthorized users can upload potentially malicious files, such as a reverse shell, to the server.

Exploitation: Brute Force

01

Tools & Processes
Hydra:
a fast online password cracking tool

02

Achievements
Obtained the password to remote computer
Obtained access to other information

03

Exploitation: Password Hash

01

Tools & Processes
Crack Station, an online tool used to crack password hashes

02

Achievements
Obtained the password from the md5/sha1 hash discovered

Obtained access to other information

03

Exploitation: Unrestricted File Upload

01

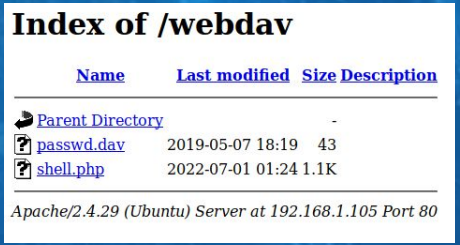
Tools & Processes

reverse_tcp, a handler payload that provides more information from a remote victim computer by placing a shell.php on the remote computer.

02

Achievements

Obtained ability to find hidden data from the remote computer



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2022-07-01 01:24	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

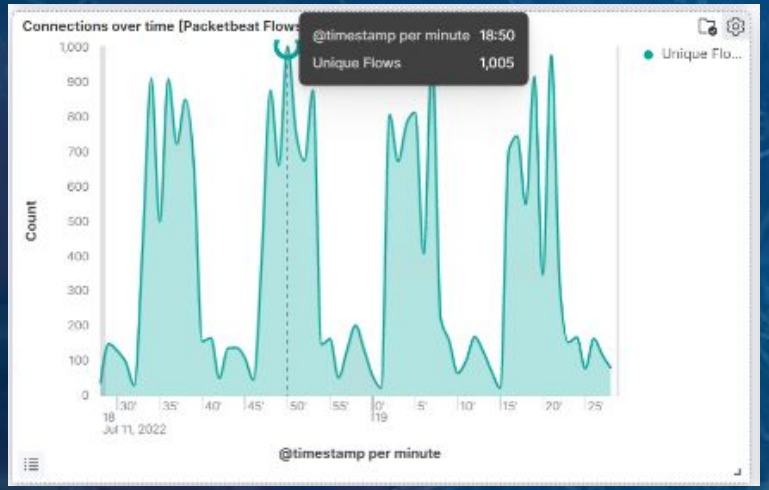
03

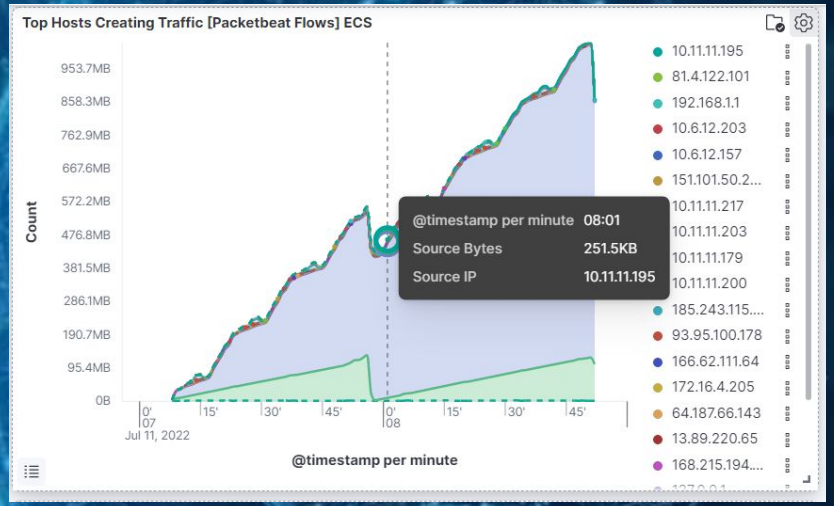
```
meterpreter > shell
Process 2194 created.
Channel 1 created.
pwd
/var/www/webdav
cd /
find flag.txt
flag.txt
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





- A port scan occurred at 18:50
- 1005 packets were sent from the ip address:
- A large number of connections at start of interactions between the two machines

Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://192.168.1.105/company_folders/se...	17,051
http://192.168.1.105/company_folders/se...	6
http://192.168.1.105/	2
http://192.168.1.105/company_folders/	2
http://192.168.1.105/icons/folder.gif	2

- The request occurred at 17:54
- 17,051 requests were made
- Files were requested from secret_folder
- This folder contained a password hash

Analysis: Uncovering the Brute Force Attack

KQL | Jul 11, 2022 @ 17:27:27.196 → Jul 11, 2022 @ 17:52:58.956

Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	152
http://snnmnkxdhflwgthqismb.com/post.php	14
http://www.gstatic.com/generate_204	14
http://ocsp.godaddy.com	6
http://169.254.169.254/2014-02-25/dynamic/instance-identity/do...	4

KQL | Jul 11, 2022 @ 17:53:02.759 → Jul 11, 2022 @ 17:55:33.092

Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,051
http://127.0.0.1/server-status?auto=	13
http://snnmnkxdhflwgthqismb.com/post.php	13
http://cdn1.friendbuy.com/widgets/configs/site-c34415b4-vinylmep...	2
http://djnf6e5yyirys.cloudfront.net/js/friendbuy.min.js	2

- 17,501 requests were made in the attack
- About 150 requests had been made before the attacker discovered the password

Analysis: Finding the WebDAV Connection

KQL | Jul 11, 2022 @ 17:10:35.294 → Jul 11, 2022 @ 22:58:49.411

Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	19,352
http://127.0.0.1/server-status?auto=	1,853
http://snnmnkxdhflwgthqismb.com/post.php	293
http://www.gstatic.com/generate_204	146
http://192.168.1.105/webdav	122

KQL | Jul 11, 2022 @ 17:10:35.294 → Jul 11, 2022 @ 22:58:49.411

Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	19,352
http://127.0.0.1/server-status?auto=	1,853
http://snnmnkxdhflwgthqismb.com/post.php	293
http://www.gstatic.com/generate_204	146
http://192.168.1.105/webdav	122

- 122 requests were made to this directory
- Files from from the directory ../secret_folder were requested

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alarm that can detect the number of requests per second can be set to detect future port scans

Normally about 1-2 scans p/s were detected, but when attacked, more than 15 scan happened p/s, so the threshold is set to anything above 5 requests per second produces an alert

System Hardening

Specific IP(s) may be blacklisted to mitigate port scans

To blacklist an ip, use: sudo firewall-cmd --zone=work --add-rich-rule='rule family="ipv4" source address="192.168.1.90" reject'

Change the ip to 192.168.1.0/24 to blacklist an entire range

Mitigation: Finding the Request for the Hidden Directory

Alarm

An Alarm that detects IP's that are on the blacklist can be set to detect unauthorized access.

If the number of blacklisted ips reaches 5 send an alert

System Hardening

To block unwanted access:

- Use better, stronger passwords
- Require password be changed after 30 days
- Multi-factor authentication

Mitigation: Preventing Brute Force Attacks

Alarm

Limit number or requests before lockout to detect future brute force attacks

Once the maximum of 5 attempts is reached, lockout occurs and an alert is sent

System Hardening

To block brute force attacks:

Use a 2 factor authentication, especially for off site locations:

- sudo apt install libpam-google-authenticator
- run Google Authenticator (answer Y to all options)
- nano /etc/pam.d/sshd
- For the rest, go to https://linuxhint.com/linux-two-factor-authentication/

Mitigation: Detecting the WebDAV Connection

Alarm

Monitor access to webdav and send an alert any time a file in webdav is read

Any access by unknown ip addresses would send an alert

System Hardening

Form a whitelist for ip addresses that are accepted and grant them access

Different methods to do this are available for whitelisting on different machines

Mitigation: Identifying Reverse Shell Uploads

Alarm

Only allow safe and critical extensions for business functionality.
Any others would sent an alert to admin

Set an absolute rule. No file uploads without admin authorization

System Hardening

Whitelist specific machines or app updates

The End