Capstone Engagement

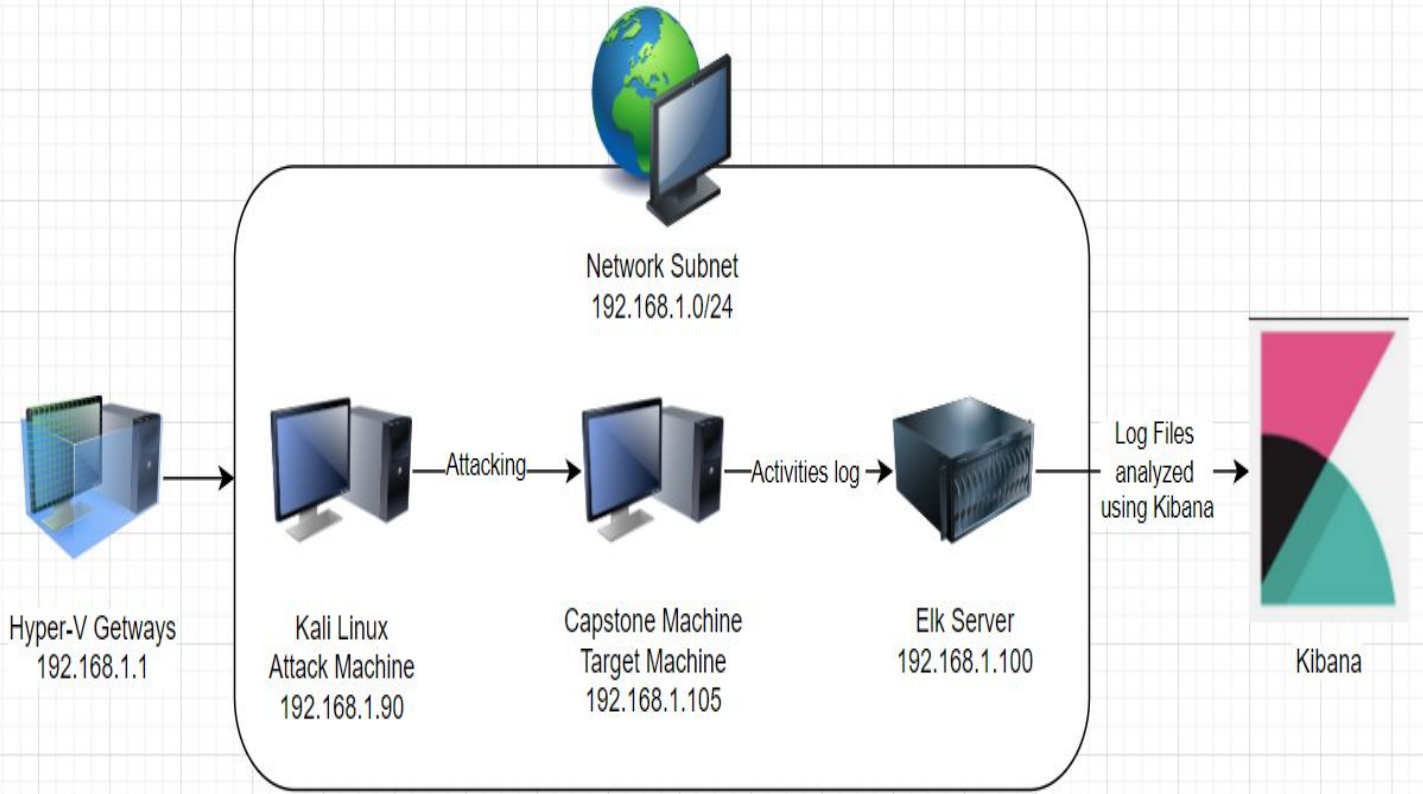
Assessment, Analysis, and Hardening of a Vulnerable System

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: 10.0.0.76

Machines
IPv4:192.168.1.1
OS: Window 10
Hostname: Azure Hyper-V

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali Linux

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk-Stack

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
Kali	192.168.1.90	Attacking machine
Elk	192.168.1.100	Network machine running Kibana
Capstone	192.168.1.105	Target machine
Azure Hyper-V Getways	192.168.1.1	Host machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
WebDav	Exploit WebDav on a server and Shell access is possible	If WebDav is not configured properly, it can allow hackers to remotely modify website content.
Weak Passwords	Commonly used passwords that is easy to guess. Short, lack of complexity such as: numbers, special characters, and capitals letters.	Create a weak link that hackers can easily crack to get access to systems.
Port 80 with public access	Open and unsecured access to anyone attempting entry using Port 80	Sensitive/ secret files and folders can be exposed to hackers with access to the internet.
Hashed Passwords	If a password is not salted it can be cracked with online tools such as crackstation.net	Once the password is cracked, and the hackers already know the user name, they can access system file.

Exploitation: Discover Open Port to Public Access

01

Tools & Processes

- nmap to scan open ports on the target machine.

02

Achievements

-found 4 hosts are up

-Port 22 and 80 are interested of brute forcing

03

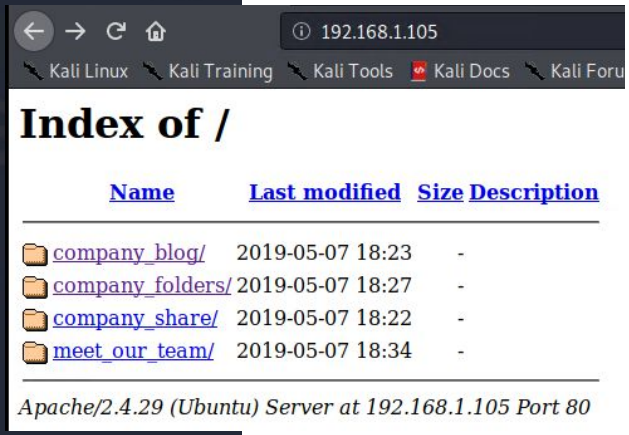
```
File  Actions  Edit  View  Help
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-26 19:20 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00052s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00058s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.90 seconds
root@Kali:~/Desktop#
```



Exploitation: Brute Force the Password

01

Tools & Processes

- Using Hydra command to crack the user password
- Command: $hydra -l ashton -P rockyou.txt -s 80 -f -vV192.164.1.105 http-get /company_folders/secret_folder/

02

Achievements

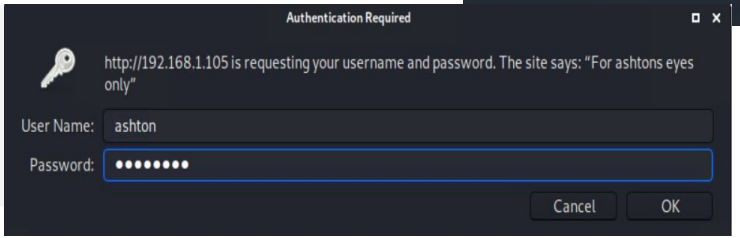
- The exploit provided the password of user 'ashton'

03

```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.164.1.105 http-get /company_folders/secret_folder/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-26 19:44:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.164.1.105:80/company_folders/secret_folder/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.164.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.164.1.105 - login "ashton" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.164.1.105 - login "ashton" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.164.1.105 - login "ashton" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.164.1.105 - login "ashton" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.164.1.105 - login "ashton" - pass "princess" - 6 of 14344399 [child 5] (0/0)
```

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 7] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-26 19:46:11
root@Kali:/#
::1             ff02::2         ip6-allrouters  ip6-loopback    localhost
ff02::1         ip6-allnodes    ip6-localhost   Kali
root@Kali:/#
```



Exploitation: Hashed Passwords

01

Tools & Processes

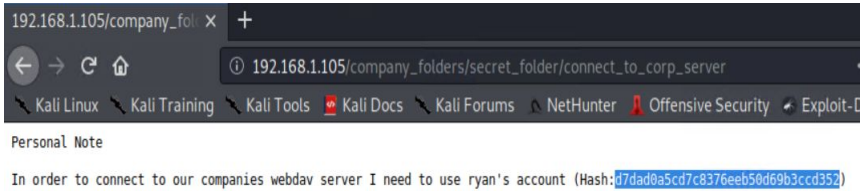
- Using the website crackstation.com to crack the hashed password.

02

Achievements

- The password ‘linux4u’ was used in conjunction with username ‘Ryan’ to access the ‘webdav’

03

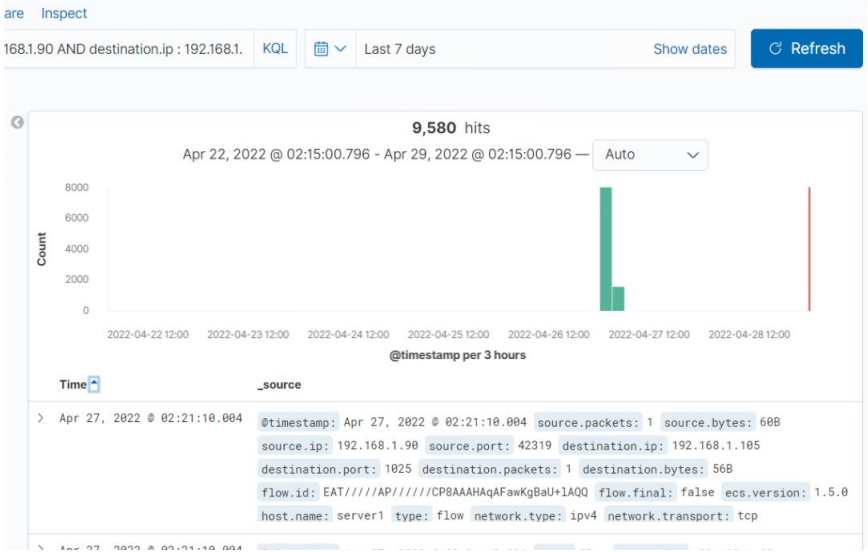


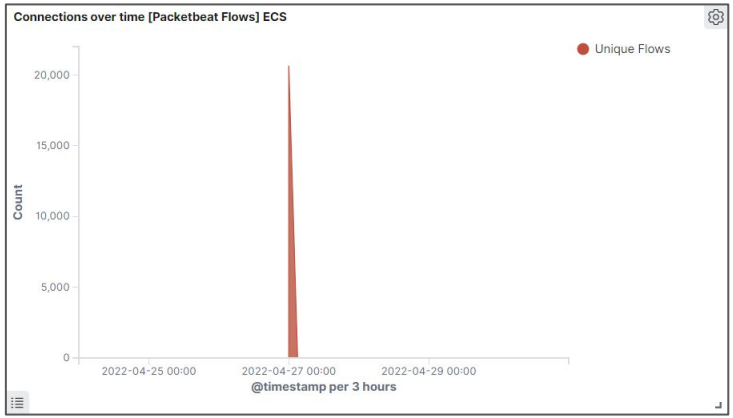
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur?
  - The port scan occurred on April 27, 2022.
- How many packets were sent, and from which IP?
  - The packets were sent from the IP 192.168.1.90, yielding over 20 thousand packets



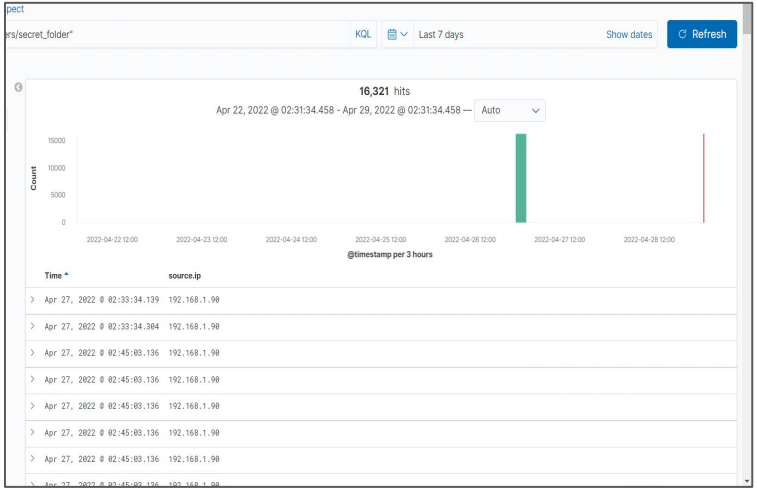


Analysis: Finding the Request for the Hidden Directory

- What time did the request occur?
  - The attack started at 2:33
- Which files were requested? What did they contain?

  The top three hits for directories and files that were requested were:

  - http://192.168.1.105/company_folder/secret_folder
  - http://192.168.1.105/company_folder/webdav/passwd.dav
  - http://192.168.1.105/webdav



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,321
http://192.168.1.105/webdav/passwd.dav	136
http://192.168.1.105/webdav	120
http://192.168.1.105/webdav/.passwd.dav.swp	38
http://192.168.1.105/webdav/shell.php	36

Export: Raw Formatted

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory?
  - The secret_folder directory was requested 16,321 times.
- Which files were requested?
  - The shell.php file was requested only 36 times in comparison.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,321
http://192.168.1.105/webdav/passwd.dav	136
http://192.168.1.105/webdav	120
http://192.168.1.105/webdav/.passwd.dav.swp	38
http://192.168.1.105/webdav/shell.php	36

Export: Raw Formatted

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Setup a low-level alert for any port scanning, with a threshold of 10 and the number of requests per second

System Hardening

- Whitelisting must know the IPs and have firewall to block unauthorised IPs from scanning

Mitigation: Finding the Request for the Hidden Directory

Alarm

Must Create 2 alerts

- A low-level alert for more than 3 password failures
- Create a critical alert for more than 10 failures

System Hardening

- Highly confidential folders/files should not be share for public access.
- Rename folders/files containing sensitive/private/company critical data.
- Review IP addresses that cause alerts to be sent: either whitelist or block the IP addresses.

Mitigation: Preventing Brute Force Attacks

Alarm

- Setup alerts for 3 or more failed attempts to login webserver and SSH, and critical alerts for 10 failed attempts.

System Hardening

- Create a policy that locks out accounts for 30 minutes after 3 unsuccessful attempts.
- Create passwords policy that requires password complexity.
- Create a list of blocked IP addresses based on IP that have many unsuccessful attempts in 3 months.If the IP address happens to be a staff member, re-education may be required

Mitigation: Detecting the WebDAV Connection

Alarm

- Create alerts for non-whitelisted IPs connecting to webDAV and from non secure locations.

System Hardening

- Limit user access to WebDAV.
- Harden authentication to WebDAV-password requirements, whitelisting IPs.
- Scanning all incoming traffic with anti-virus/anti-malware.
- Update and upgrade secure application regularly

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Monitor all incoming uploads and setup an alert for anything triggered by anti-virus/ anti-malware.

System Hardening

- Setup anti-virus/ anti-malware to secure application that screens all incoming files and automatically updates daily.
- Update firewall rules.
- Limit file types that can be uploaded, including restricting php.

the End