Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

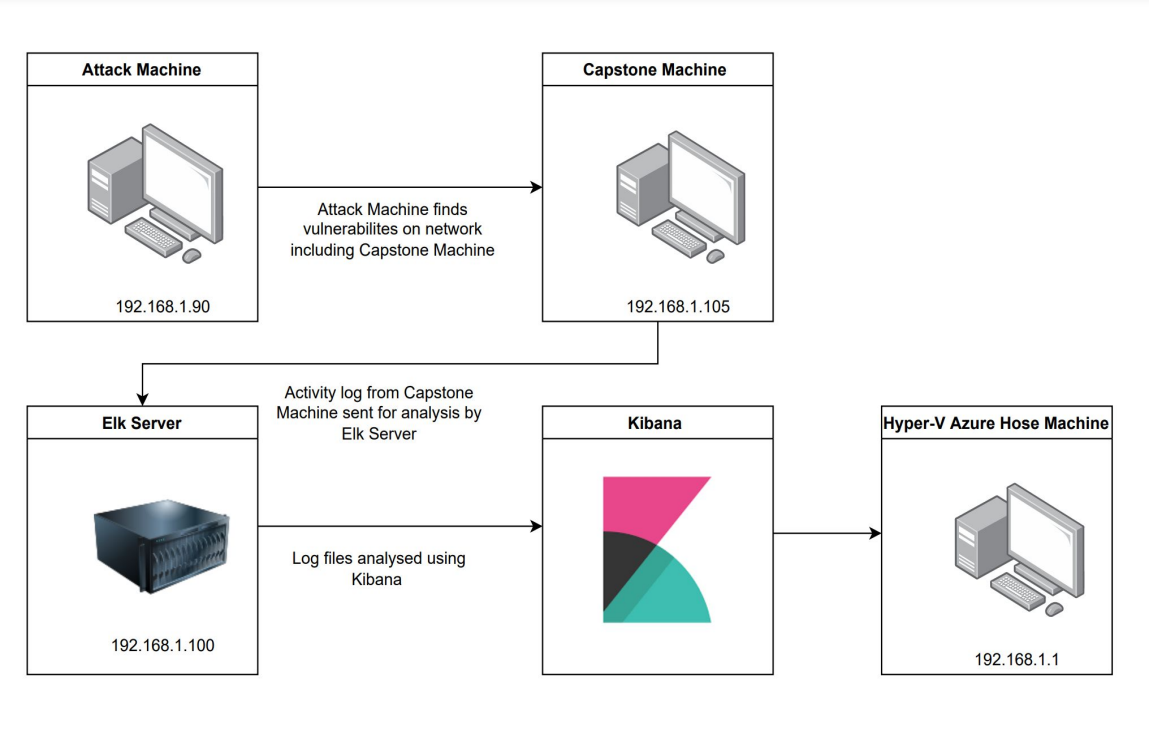
Report Prepared By Hanna Kalantar

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: 19.168.1.1
OS: Windows 10
Hostname: Azure Hyper-V-ML-REFVM-684427

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

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:

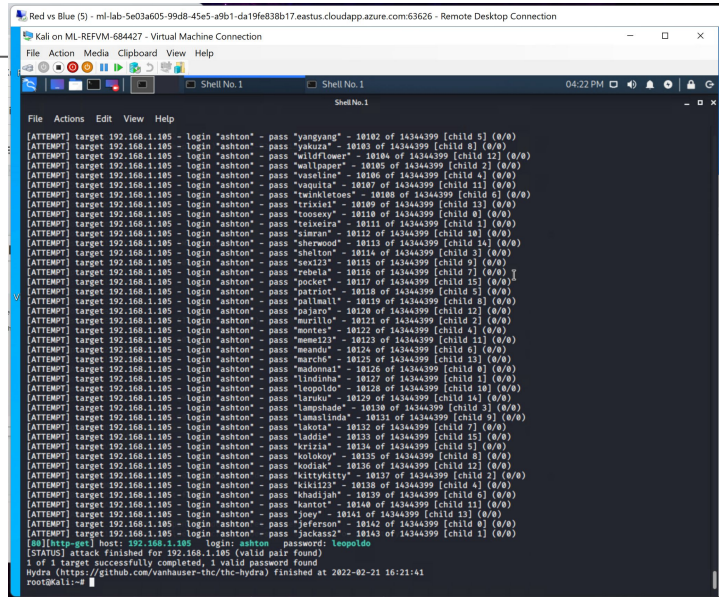
Hostname	IP Address	Role on Network
Hyper-V Azure Machine ML-REFVM-684427	192.168.1.1	Host Machine Cloud Based
Kali	192.168.1.90	Attacking Machine
Elk Stack	192.168.1.100	Network Monitoring Machine Running Kibana
Capstone	192.168.1.105	Target Machine Replicating a Vulnerable Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 open with public access CVE-2019-6579	Open and unsecured access to anyone attempting entry using Port 80	Files and Folders are readily accessible. Sensitive files and folders can be found
Root accessibility	Authorization to execute and command, and access any resource on the vulnerable device	Vulnerabilities can be leveraged. Extensive potential impact to any connected network
Simplistic Username	First name, short name, or similar information can be easily socially engineered	Names like “ryan” and “ashton” are all predictable names that can be discovered by social engineering. In conjunction with a simple/weak password, file/folder access can be attained
Weak Passwords	Commonly used passwords such as simple words, and the lack of password complexity, such as the inclusion of symbols, numbers, and capitals	System access could be discovered by social engineering.

Exploitation: Brute Force Password



01

Tools & Processes

I used Hydra attack which is already pre installed on Kali Linux. I also required password list, in this case I used rockyou.txt

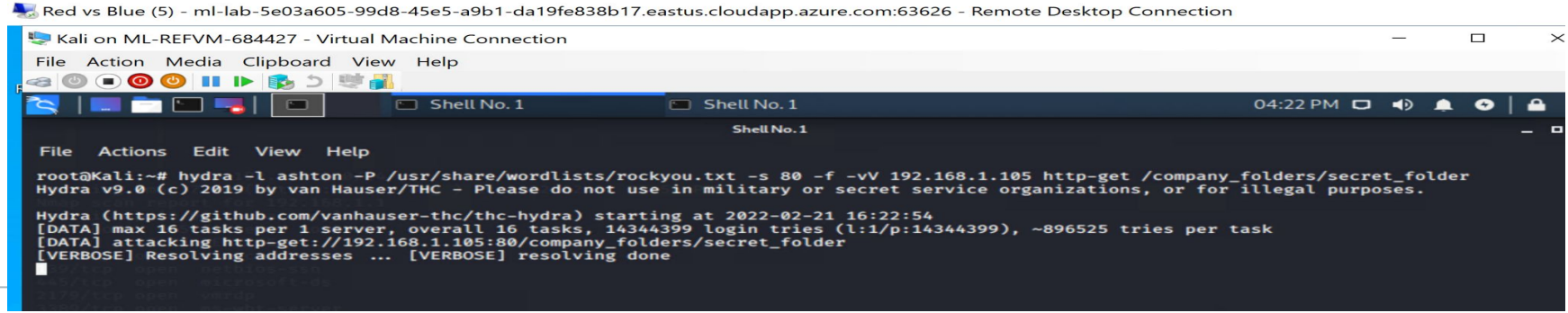
Command: ` hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder`

02

Achievements

The exploit provided me the confirmation of the login name “ashton”, as well as, the password “leopoldo”

03



Exploitation: Port 80 Open to Public Access

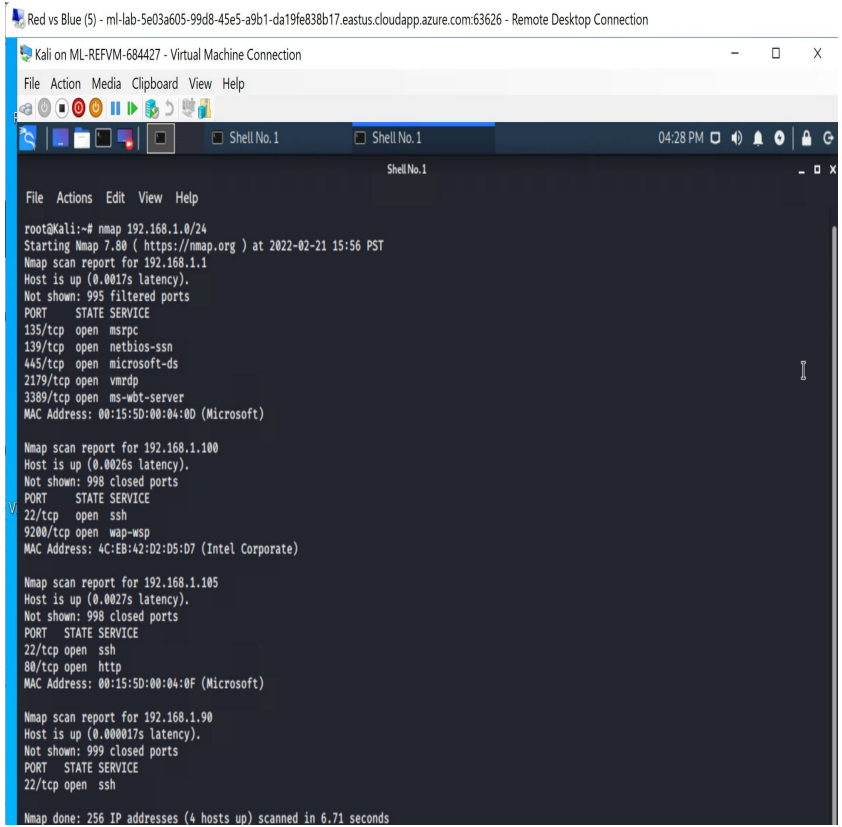
01

Tools & Processes
I used nmap to scan for open ports on the target machine

02

Achievements
Nmap scanned 256 IP addresses. I ended up finding 4 hosts up and Port 22 and 80 open.

03



Exploitation: Hashed Passwords

01

Tools & Processes

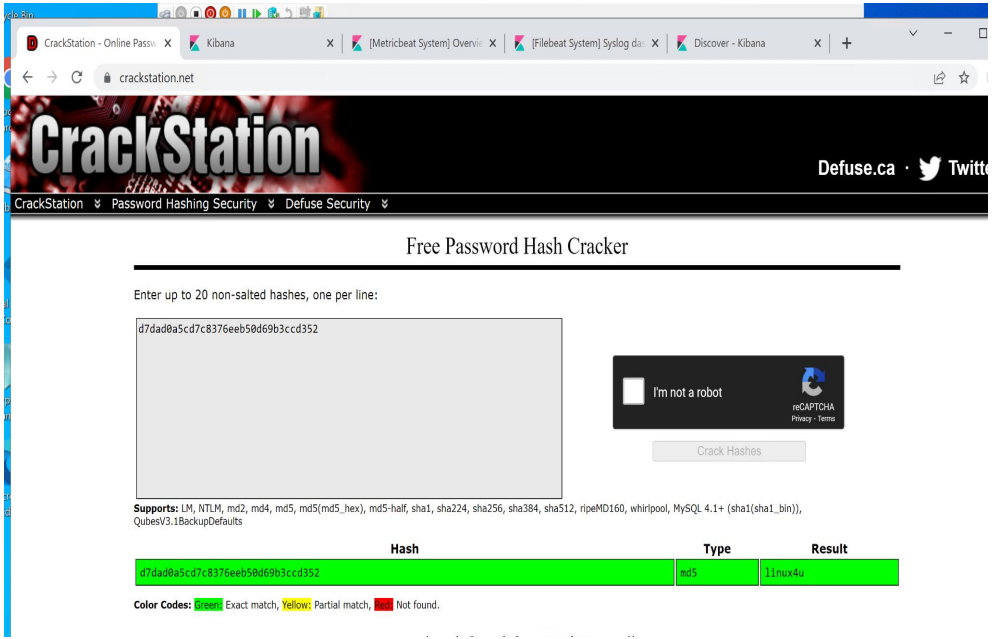
I used the website: crackstation.net to crack the hashed password.

02

Achievements

The password “linux4u” was used in conjunction with username “ryan” to access the /webdav folder.

03

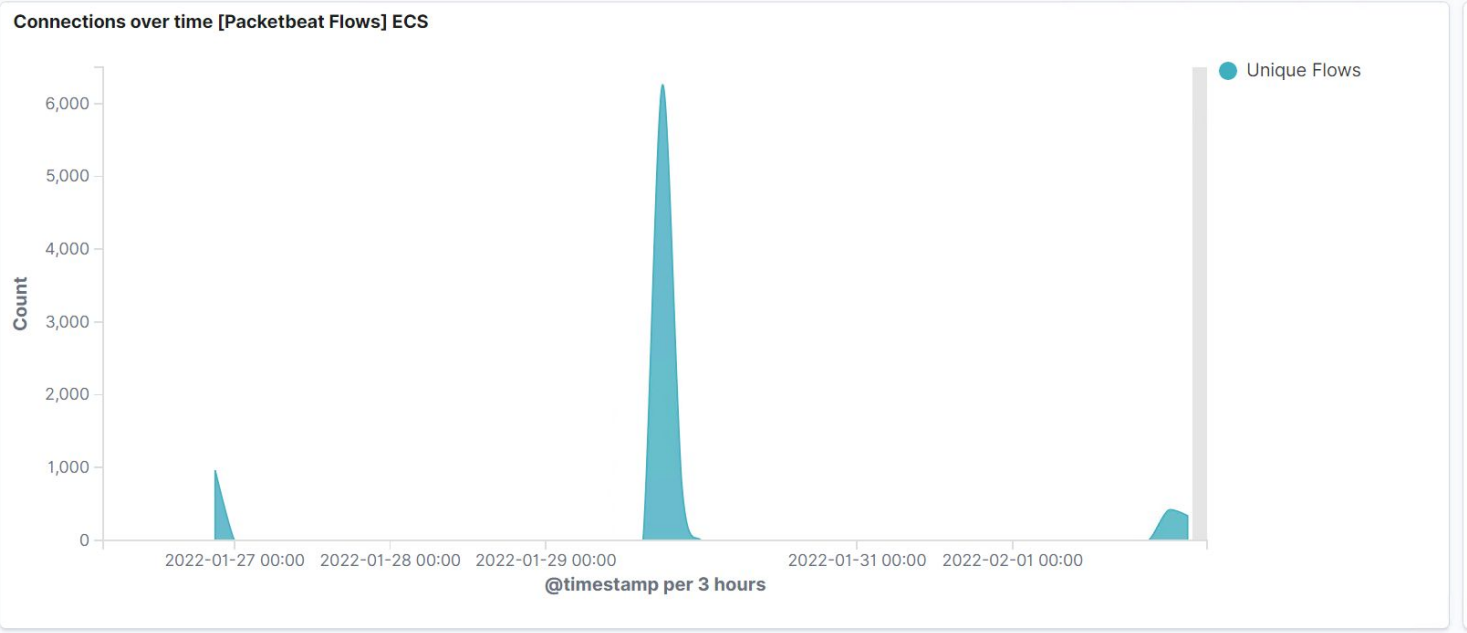


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan started on January 27, 2022 at approximately 0100hrs.
- 6,789 connections occurred at the peak, the source IP was 192.168.1.90.
- The sudden peaks in network traffic indicate that this was a port scan.



Analysis: Finding the Request for the Hidden Directory

- The request started January 27, 2022. 1,893 requests were made to access the /secret_folder.
- The /secret_folder contained a hash that I could use to access the system using another employee's credentials (ryan). The /secret_folder also allowed me to upload a payload, thus exploiting other vulnerabilities.

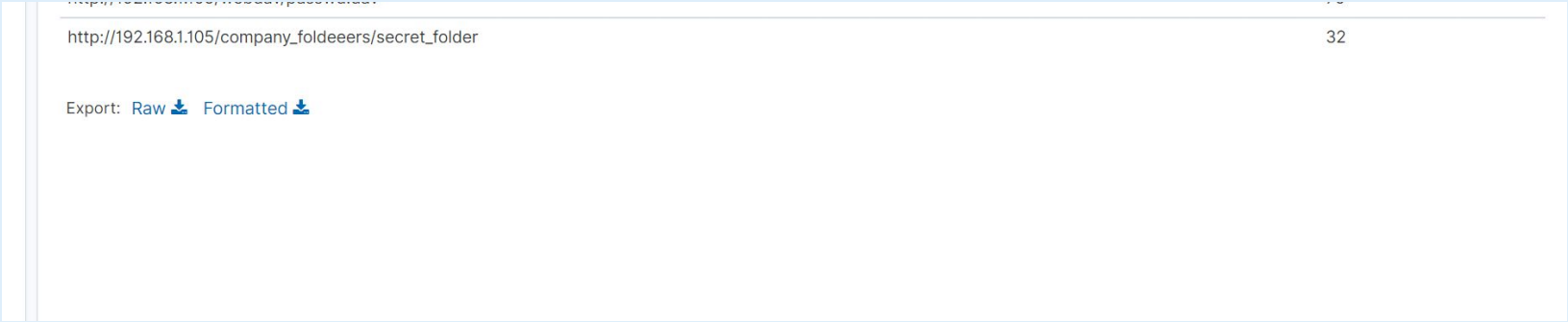
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	1,893
http://192.168.1.105/webdav	304
http://192.168.1.105/webdav/shell.php	106
http://192.168.1.105/webdav/passwd.dav	70
http://192.168.1.105/company_foldeeers/secret_folder	32

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

- 1,893 requests were made in the attack to access the /secret_folder.
- 32 attacks were successful. 100% of these attacks returned a 301 HTTP status code “Moved Permanently”.



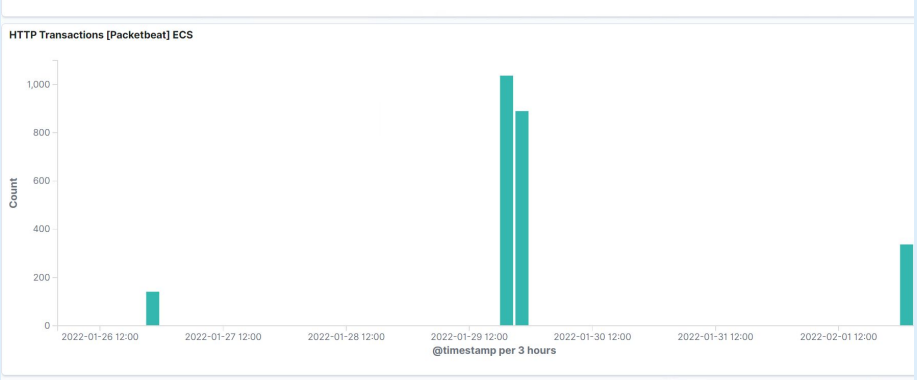
Analysis: Finding the WebDAV Connection

- 304 requests were made to access the /webdav directory
- The primary requests were for the passwd.dav and shell.php files.

http://192.168.1.105/webdav	304
http://192.168.1.105/webdav/shell.php	106

```
40555/r-xr-xr-x   0        dir   2022-01-29 10:45:33 -0800  sys
41777/rwxrwxrwx   4096     dir   2022-01-29 10:46:16 -0800  tmp
40755/rwxr-xr-x   4096     dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096     dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096     dir   2019-05-07 11:16:46 -0700  var
100600/rw------  8380064   fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw------  8380064   fil   2020-06-04 03:29:12 -0700  vmlinuz.old

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- I recommend an alert be sent once 1000 connections occur in an hour.

System Hardening

- Regularly run a system port scan to proactively detect and audit any open ports.
- Set server iptables to drop packet traffic when thresholds are exceeded.
- Ensure the firewall is regularly patched to minimise new zero-day attacks.
- Ensure the firewall detects and cuts off the scan attempt in real time .

Mitigation: Finding the Request for the Hidden Directory

Alarm

- To detect unauthorized access requests for hidden folders and files, I would set an alert when these requests occur.
- I would recommend a threshold of maximum 5 attempts per hour that would trigger an alert to be sent.

System Hardening

- Highly confidential folders should not be shared for public access.
- Rename folders containing sensitive/private/company critical data.
- Encrypt data contained within confidential folders.
- Review IP addresses that cause an alert to be sent: either whitelist or block the IP addresses.

Mitigation: Preventing Brute Force Attacks

Alarm

- A HTTP 401 Unauthorized client error indicates that the request has been applied because it lacks valid authentication credentials for the target resource.
- I would detect future brute force attacks by setting an alarm that alerts if a 401 error is returned.
- The threshold I would set to activate this alarm would be when 10 errors are returned

System Hardening

- I would create a policy that locks out accounts for 30 minutes after 3 unsuccessful attempts.
- I would create a password policy that requires password complexity. I would compare the passwords to common password lists, and prevent users from reusing historial passwords.
- I would create a list of blocked IP addresses based on IP addresses that have 30 unsuccessful attempts in 6 months. If the IP address happens to be a staff member, re-education may be required.

Mitigation: Detecting the WebDAV Connection

Alarm

- First, I would create a Whitelist of trusted IP Addresses. Then I would review this list every 6 months to see if I think it's necessary for them to have access.
- On **HTTP GET r**equest, I would set an alarm that activates on any IP address trying to access the webDAV directory outside of those trusted IP addresses.
- The threshold I would set to activate this alarm would be when any **HTTP PUT** request is made.

System Hardening

- Creating a whitelist of trusted IP addresses and ensuring my firewall security policy prevents all other access.
- Assuming my IP address is 192.168.1.1, within Ubuntu I would run the following command: $ iptables -I INPUT -s 192.168.1.1 -p tcp -m multiport -- dports 80,443 -j ACCEPT
- In conjunction with other mitigation strategies, I would ensure that any access to the WebDAV folder is only permitted by users with complex usernames and passwords.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- I recommend that an alert be set for any traffic attempting to access port 4444. The threshold for the alert to be sent is when one or more attempt is made.
- I recommend setting an alert for any files being uploaded into the /webDAV folder. The threshold for the alert to be sent is when one or more attempt is made.

System Hardening

- Block all IP addresses other than whitelisted IP addresses (because reverse shells can be created over DNS, this action will only limit the risk of reverse shell connections, not eliminate the risk).
- Set access to the /webDAV folder to read only to prevent payloads from being uploaded.
- Ensure only necessary ports are open.

the End