Capstone Engagement

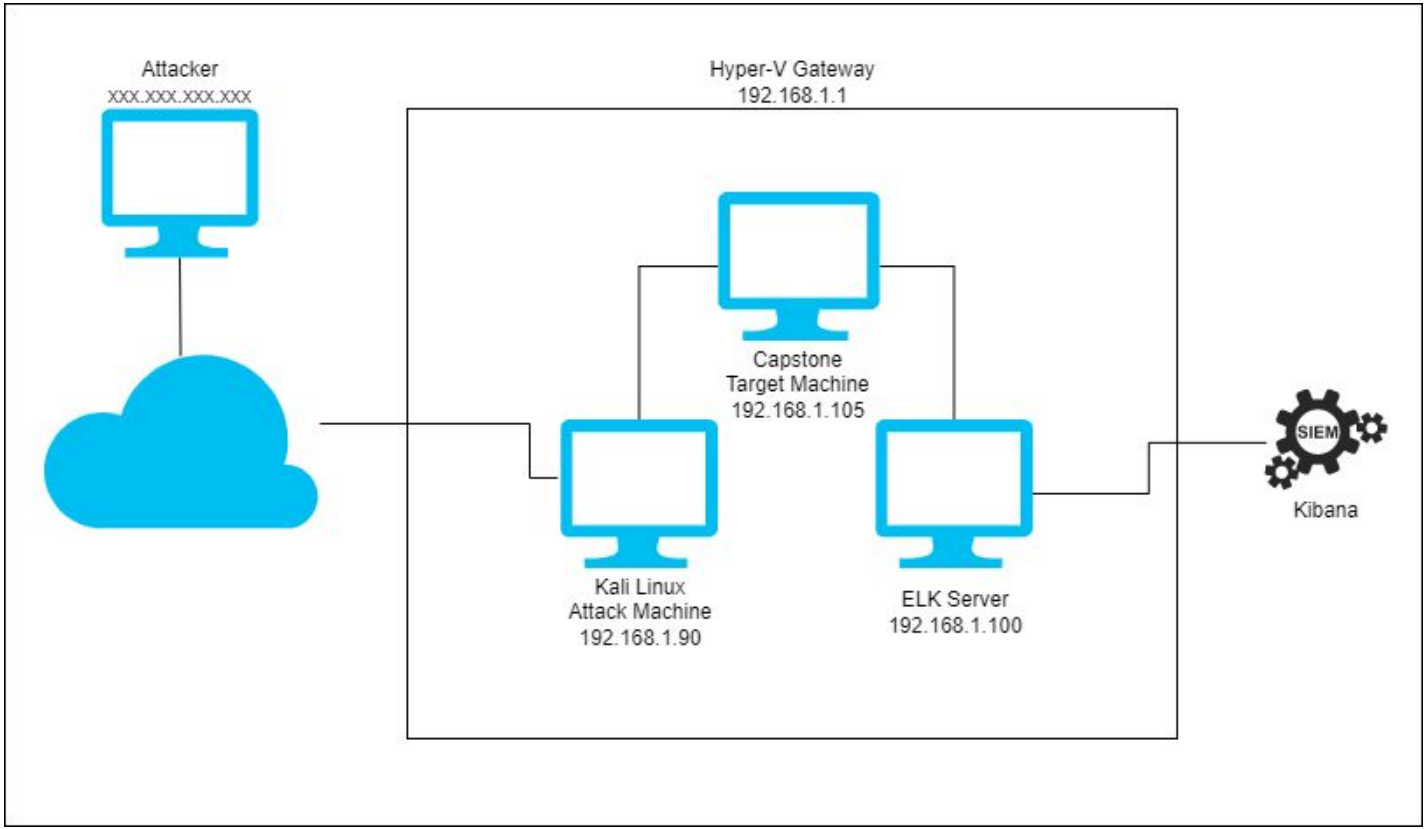
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 102.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.76

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

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 1892.168.1.100
OS: Linux
Hostname: ELK

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 Gateway	192.168.1.1	Cloud Based Host Machine
Kali	192.168.1.90	Attacking Machine
ELK	192.168.1.100	Network Monitoring Machine running Kibana
Target	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Cryptographic Failure	On OWASP list of top 10 vulnerabilities. Exposure of sensitive data in one of the companies hidden folders.	Led to discovery of credentials to gain Web DAV access.
Brute Force	System vulnerable to numerous username and password combinations to access the system.	System is easy to access through common password lists and programs like Hydra and John the ripper.
Data Security Failure	User credentials were saved on an unsecured plaintext file within another user's machine.	Sensitive data is easily gathered. This enabled further access to organizational systems.

Exploitation: Cryptographic Failures

01

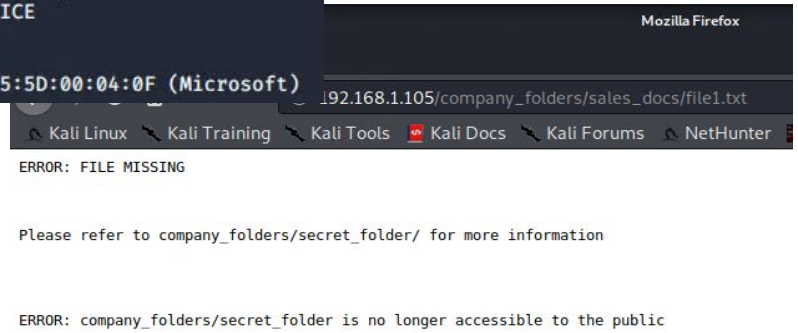
Tools & Processes
Performing nmap scan revealed port 22 and 80 as open and vulnerable. Connected to vulnerable machine 192.168.1.105 and researched viewable contents for additional information.

02

Achievements
Open port 80 allowed for HTTP connection and viewing of unsecured data. Further research exposed unlisted folders with additional unsecured data.

03

```
Nmap scan report for 192.168.1.105
Host is up (0.00081s 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)
```



Exploitation: Brute Force

01

Tools & Processes

Using Hydra on the Kali machine, I was able to run a command to attempt to break into one of the organizations locked directories.

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 vulnerability allowed me to gather Aston's password and gain access to the secret folder.

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of 14344399 [child 9] (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
```

Exploitation: Data Security Failure

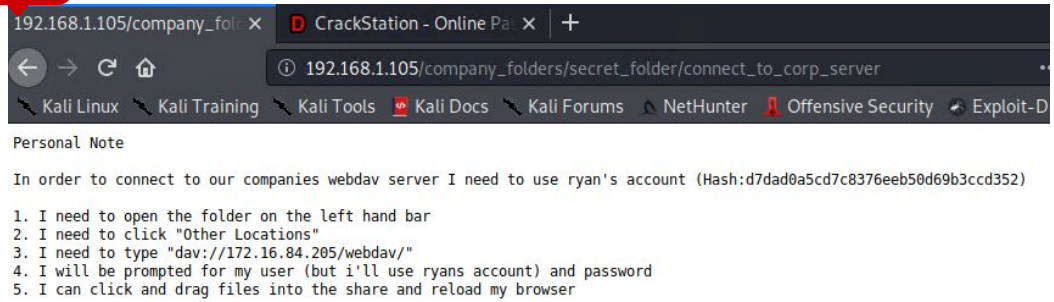
01

Tools & Processes
User credentials and information leading to the organizations Web DAV directory were exposed in a plain text file. Used CrackStation to crack the hashed password.

02

Achievements
The cracked hashed password lead to access of the Web DAV directory to plant malicious software.

03

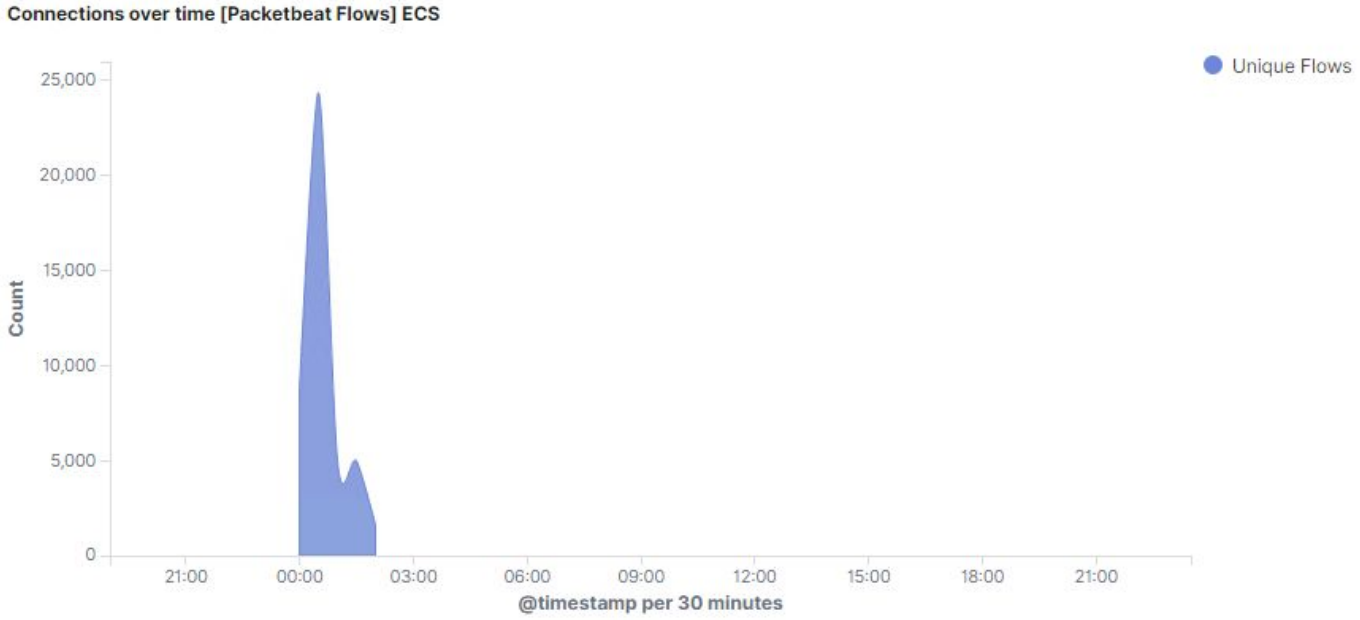


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- A port scan occurred at approximately 00:00 on May 9th.
- Saw a peak of 24,368 connections during the scan originating from IP 192.168.1.90
- The sudden peak in network traffic indicates this could be a port scan



Analysis: Finding the Request for the Hidden Directory

- At approximately 00:00 on May 9th, 17,271 request were made fo the */secret_folder* directory.
- The secret folder contained a plain text document with an employee's name and their hashed password.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,271
http://127.0.0.1/server-status?auto=	660
http://192.168.1.105/webdav	118
http://snnmnkxdhflwgthqismb.com/post.php	97
http://www.gstatic.com/generate_204	56

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

- A total of 17,271 requests were made for the */secret_folder* directory.
- Of those requests, 3 were successful.

```
user_agent.original: "Mozilla/4.0 (Hydra)" and not http.response.status_phrase:"unauthorized"
```

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	3

Export: Raw Formatted

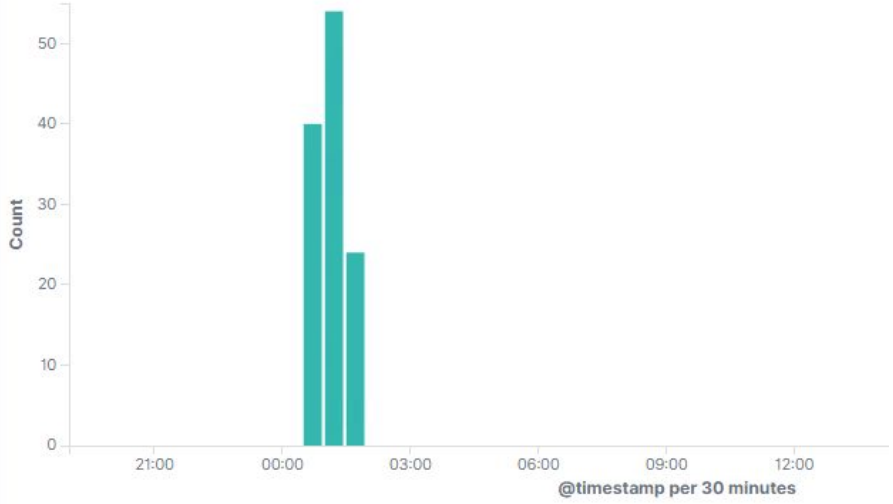
Analysis: Finding the WebDAV Connection

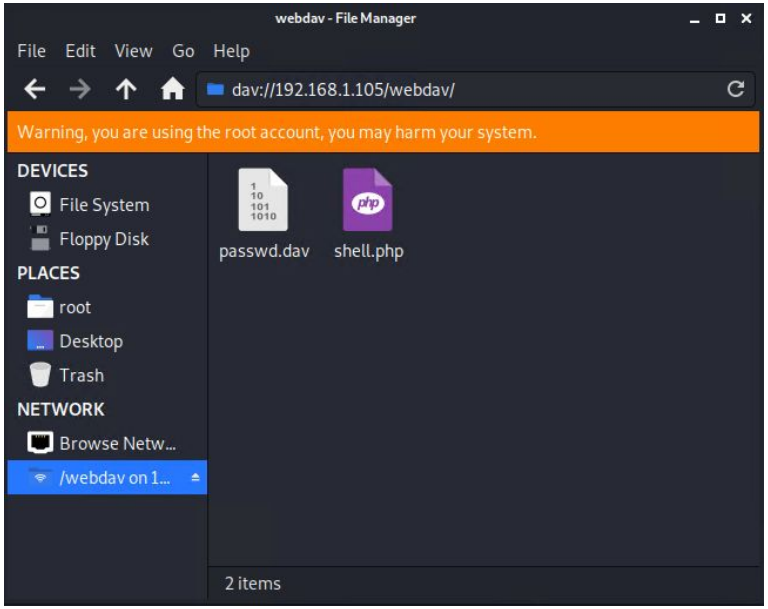
- A total of 118 request were made.
- The primary requests were for the *passwd.dav* and *shell.php* files.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	118

HTTP Transactions [Packetbeat] ECS





Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Implement a low-level alert for any port scanning with a threshold of 10, and a severe-alert for anything above 100.

System Hardening

Whitelist known IPs and block unauthorized IPs.

Schedule regular security checks on all ports. Close any that do not need to be open.

Implement rate-limit blocks to automatically blacklist anything over 1000.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Create a low-level alert for more than 3 password failures and a severe-alert for more than 10 failures.
Create an alert for non-whitelisted IPs attempting to access directories.

System Hardening

Increase password strength requirements (ie minimum length, upper and lower case letters, special characters, etc.).
Implement directory permissions to further limit access.

Mitigation: Preventing Brute Force Attacks

Alarm

Create low-level alert for 3 failed login attempts, and a critical alert for more than 10 failed login attempts.

System Hardening

Implement account timeout and lockout rules for failed login attempts.
Increase password strength requirements.

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alert for non-whitelisted IPs attempting to connect to WebDAV.

System Hardening

Implement WebDAV user access limits.
Regularly update WebDAV.
Limit connection to WebDAV through secure connections like an organization's VPN.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Monitor all incoming uploads using anti-virus and anti-malware detection.
Create alerts for any suspicious uploads.

System Hardening

Implement a secure anti-virus and malware detection software to review any uploaded file.
Implement file type restrictions to include blocking *.php* files.

the End