Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

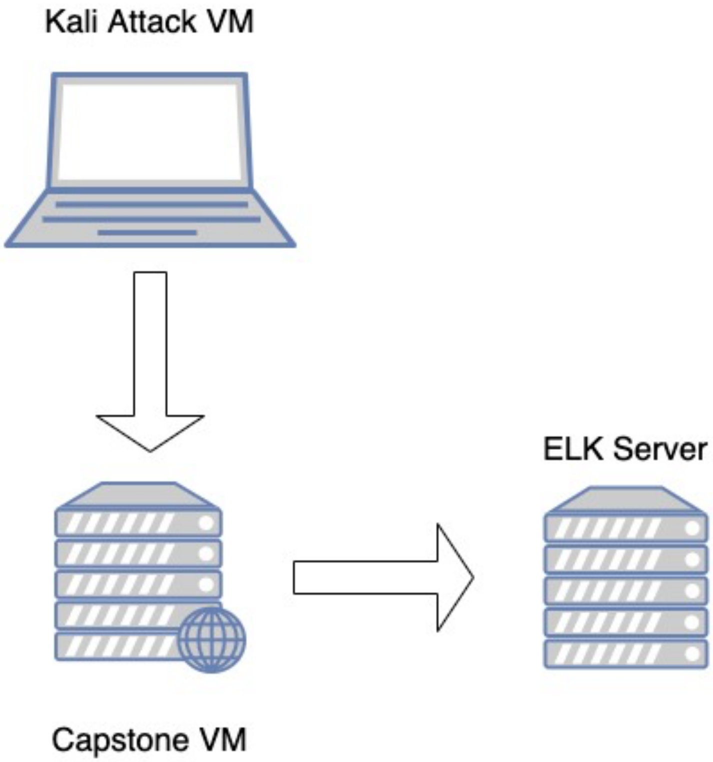
02 **Red Team**: Security Assessment

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: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.100
OS: Linux
Hostname: ELK

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Intel Corporate	192.168.1.100	Stores the logs for the corporate server.
Microsoft	192.168.1.105	Machine on the corporate network.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Sensitive Data Exposure OWASP Top 10 #3 Critical	The secret_folder can be accessed by a public web page, but contains information for authorized users only.	This compromises login credentials that an attacker can use to gain access to the web server.
Unauthorized Uploads Critical	Users can upload anything they want to the web server.	This allows hackers to upload a PHP script to the server.
Injection OWASP Top 10 #1 Critical	Hackers can use PHP scripts to execute shell commands.	This vulnerability allows hackers to open a reverse shell to the server.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

- nmap to scan network
- Browser to explore
- hydra to brute force login credentials.

02

Achievements

- Found there is a secret_folder directory.
- This directory is password protected but susceptible to a brute force attack on the login credentials.
- Found out the login credentials are:

U: ashton P: leopoldo

03

Exploitation

- The login window reveals that the user is ashton.
- This info was used to run a brute force attack to obtain login credentials.
- Brute force syntax:

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

Exploitation: Unauthorized Uploads

01

Tools & Processes

- Using the cracked login info, found the folder containing the WebDAV connection instructions.
- Used crackstation to obtain login for the provided hash and user ryan.
- msfconsole to create custom web shell.
- meterpreter to open connection to target.

02

Achievements

- Uploaded a custom web shell containing a PHP script.

03

Exploitation

- Logged in to the secret folder directory and ran the PHP script I uploaded. This opened a bash shell.

Exploitation: [Name of Third Vulnerability]

01

Tools & Processes

- Used meterpreter to connect to my uploaded web shell.
- Used this shell to explore the target.

02

Achievements

- Once connected to the target using meterpreter, I have access to the full file system.

03

Aftermath

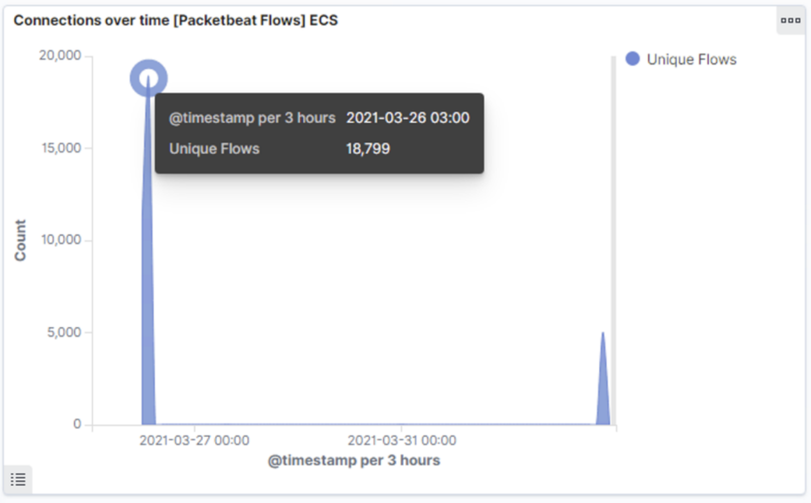
- Using this bash shell to get into the target allowed me to look through the file system and capture the flag.
- The flag was found in the root directory.

Blue Team

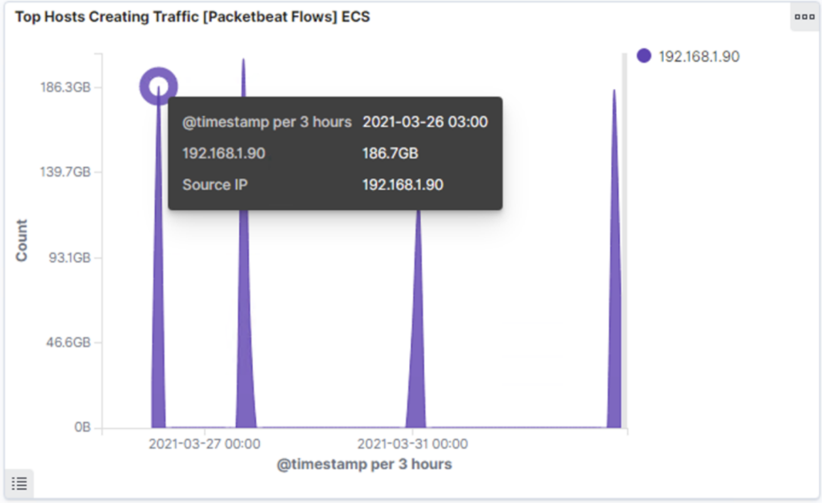
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur? **3:00**
- How many packets were sent, and from which IP? **In the first chart we see that 18,799 packets were sent. In the second chart we can see that the IP address is 192.168.1.90**
- What indicates that this was a port scan? **The amount of packets that were sent.**



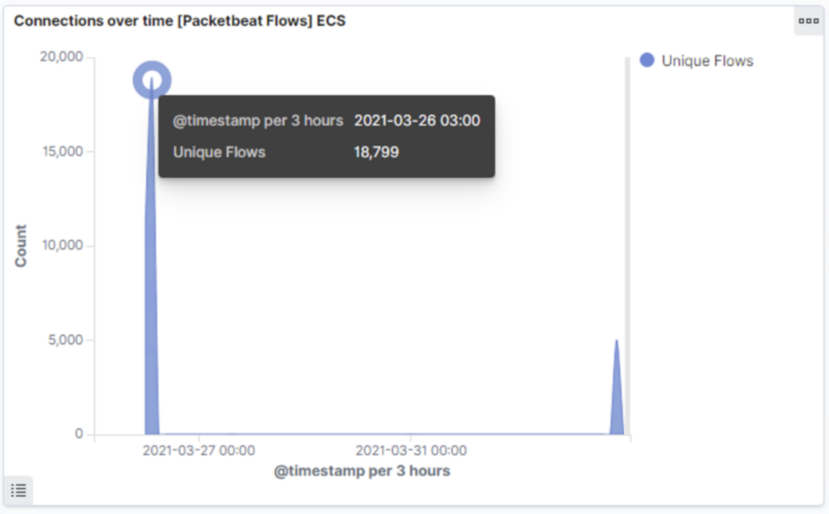
@timestamp per 3 hours 2021-03-26 03:00
Unique Flows 18,799

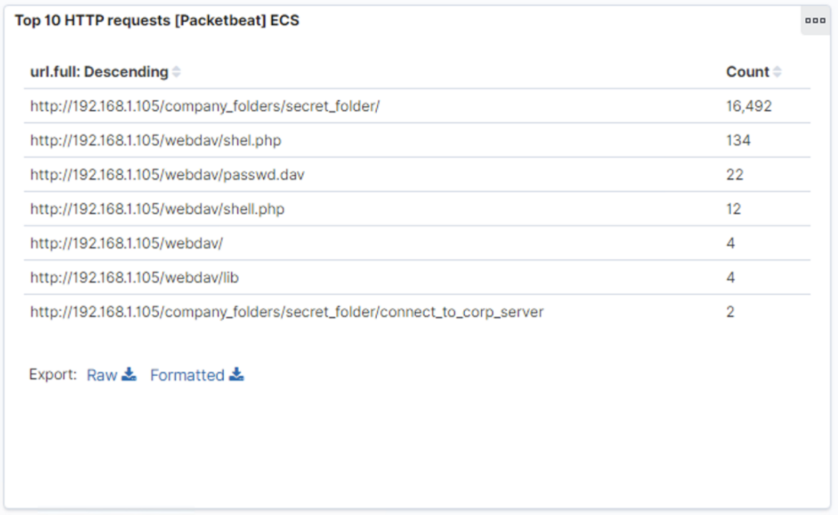


@timestamp per 3 hours 2021-03-26 03:00
192.168.1.90 186.7GB
Source IP 192.168.1.90

Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? How many requests were made? **In the first chart we can see the attack started at 3:00 with 18,799 requests.**
- Which files were requested? What did they contain? **In the second chart we can see which files were requested and what they contained.**





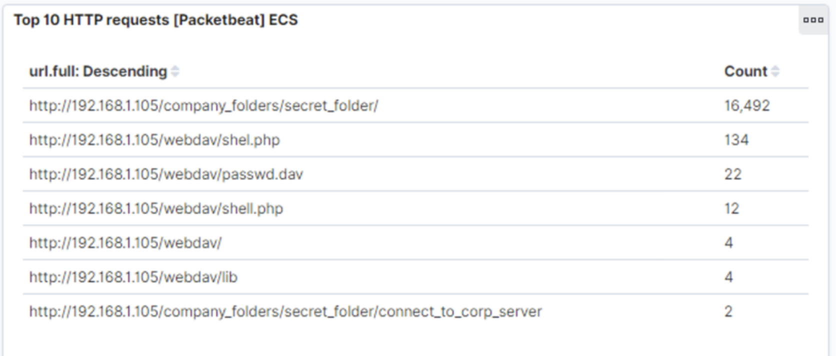
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,492
http://192.168.1.105/webdav/shel.php	134
http://192.168.1.105/webdav/passwd.dav	22
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/webdav/	4
http://192.168.1.105/webdav/lib	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Export: Raw Formatted

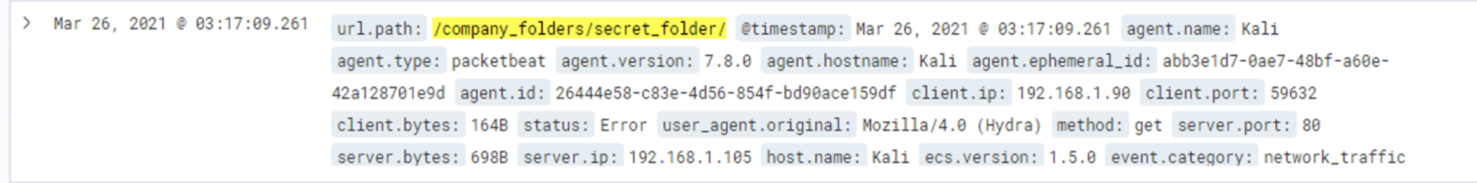
Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? **In the first chart we see that 16,492 requests were made on the secret_folder.**
- How many requests had been made before the attacker discovered the password? **Inside of the secret_folder directory there were only 2 requests, so out 16,492 requests only 2 were successful.**



Top 10 HTTP requests [Packetbeat] ECS

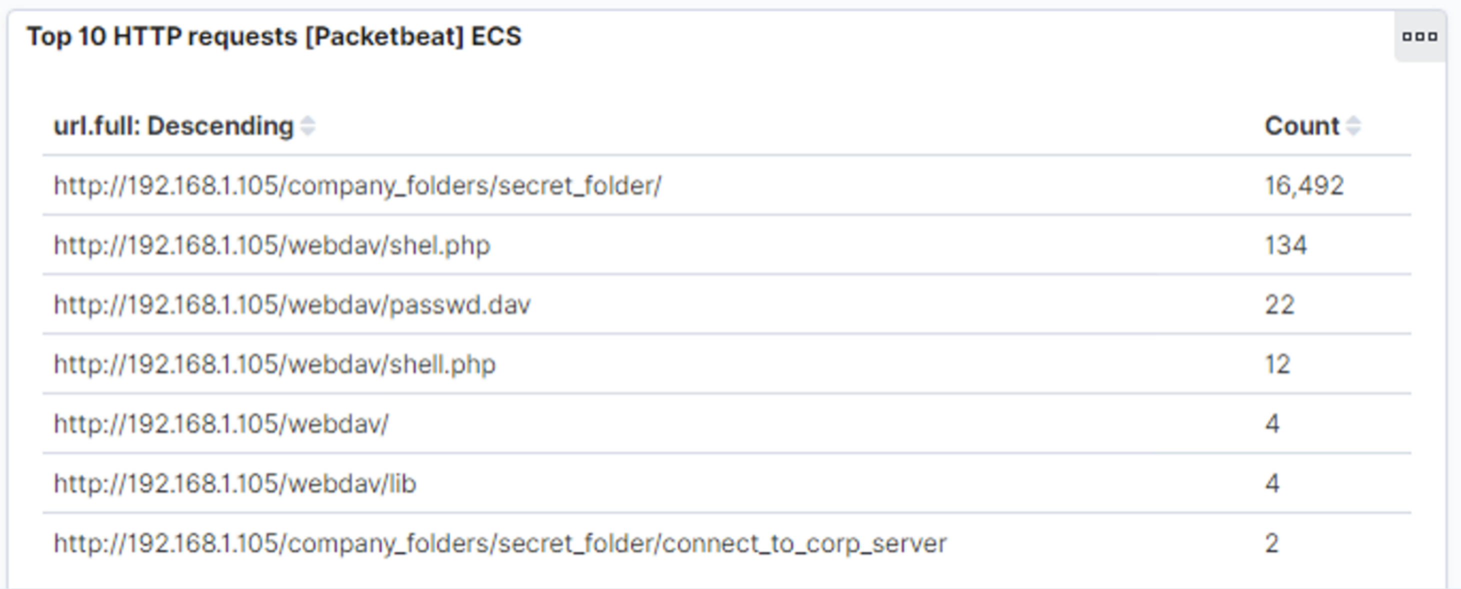
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,492
http://192.168.1.105/webdav/shel.php	134
http://192.168.1.105/webdav/passwd.dav	22
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/webdav/	4
http://192.168.1.105/webdav/lib	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2



```
> Mar 26, 2021 @ 03:17:09.261   url.path: /company_folders/secret_folder/ @timestamp: Mar 26, 2021 @ 03:17:09.261 agent.name: Kali
                                agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: abb3e1d7-0ae7-48bf-a60e-
                                42a128701e9d agent.id: 26444e58-c83e-4d56-854f-bd90ace159df client.ip: 192.168.1.90 client.port: 59632
                                client.bytes: 164B status: Error user_agent.original: Mozilla/4.0 (Hydra) method: get server.port: 80
                                server.bytes: 698B server.ip: 192.168.1.105 host.name: Kali ecs.version: 1.5.0 event.category: network_traffic
```

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? **There were 4 requests made to the webdav connection.**
- Which files were requested? **The successful shell.php file was requested 12 times.**



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,492
http://192.168.1.105/webdav/shel.php	134
http://192.168.1.105/webdav/passwd.dav	22
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/webdav/	4
http://192.168.1.105/webdav/lib	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

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? **We can set an alarm for the number of requests per second.**

What threshold would you set to activate this alarm? **The alarm should go off if we see more than 10 requests per second from a single IP address.**

System Hardening

What configurations can be set on the host to mitigate port scans? **A list of allowed IP address should be created. Also, a local firewall can be used to block incoming connections.**

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? **An alarm that is triggered when an IP address that is not on the allowed list tries to connect.**

What threshold would you set to activate this alarm? **If the IP is allowed it won't trigger, if the IP is NOT allowed it will go off.**

System Hardening

What configuration can be set on the host to block unwanted access? **A file with classified info should not be kept on the web server where it can be accessed by a public web page. At minimum the file should be encrypted.**

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? **An alarm that triggers after a certain number of requests per second.**

What threshold would you set to activate this alarm? **It should be set to go off when more than 50 requests per second is exceeded.**

System Hardening

What configuration can be set on the host to block brute force attacks? **You can use two factor authentication and you could limit the number of failed login attempts.**

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory? **You can set an alarm to go off if an unauthorized user or IP tries to access this directory. You can monitor access to this directory with Filebeat.**

What threshold would you set to activate this alarm? **If the user or IP is unauthorized, it goes off.**

System Hardening

What configuration can be set on the host to control access? **An admin must install filebeat on the host.**

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads? **You can set an alarm to go off if a forbidden file type is uploaded to this directory. For example a .php file like the one used in this attack.**

What threshold would you set to activate this alarm? **The alarm would trigger whenever a forbidden file type is uploaded.**

System Hardening

What configuration can be set on the host to block file uploads? **Permissions on the host can be restricted. Filebeat needs to be enabled and configured.**

The End