Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

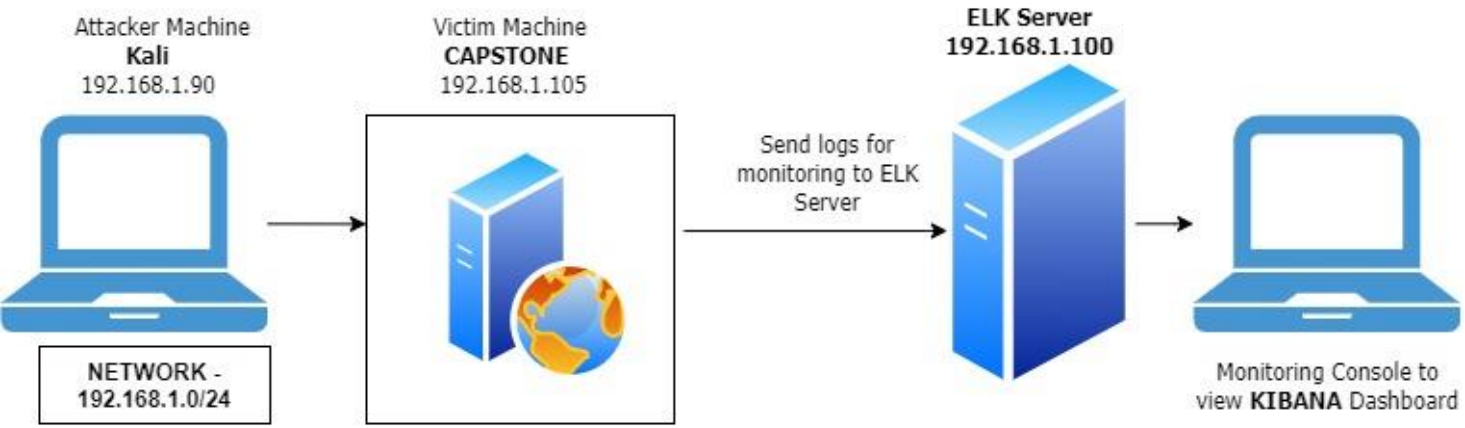
- Medha Parte

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask:255.255.255.255
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
Windows	192.168.1.1	It allows remote connections between internal systems on the network.
Elk	192.168.1.100	Elk Monitoring Server
Captsone	192.168.1.105	This system has Apache webserver running on it and is identified as target system to exploit the vulnerability.
Kali	192.168.1.90	This system is used to launch remote attack target system which is Capstone webserver.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure (SDE) OWASP Top 10 #3 || Critical	The secret folder which contains sensitive information intended for authorised users is publicly visible	An attacker can brute_force credentails required for accessing secret folder and get sensitive information using which he can further break into the web server
Unauthorized File Upload Critical	Users can upload arbitrary files to the web server	This vulnerability allows attackers to upload to php scripts to the server and open backdoor to the system
Remote Code Execution via Command Injection OWASP Top 10 #1 || Critical	Due to unauthorized file upload vulnerability, attacker can upload arbitrary shell scripts and achieve remote code execution on the web server	Using this vulnerability, an attacker can open reverse shell to the server

Exploitation: [Sensitive Data Exposure]

01

Tools & Processes

- Nmap – To scan network
- Browser – To navigate and explore
- Hydra – To perform brute force attack against secret folder and get password for user ashton

02

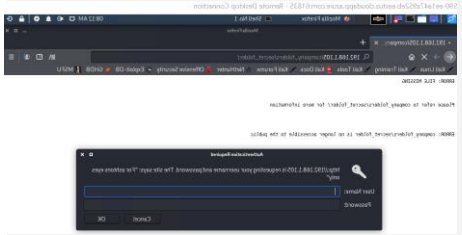
Achievements

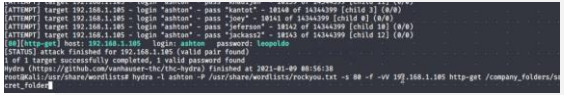
- Nmap scan revealed that capstone webserver is accessible via port 80
- Navigation to webserver url ip using browser highlighted secret folder on the server which is password protected but susceptible to brute_force
- Got password for user ashton by running hydra attack against secret directory

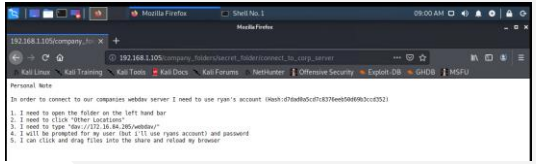
03

Exploitation

Accessed secret_folder and got sensitive information







Exploitation: [Unauthorized File Upload]

01

Tools & Processes:

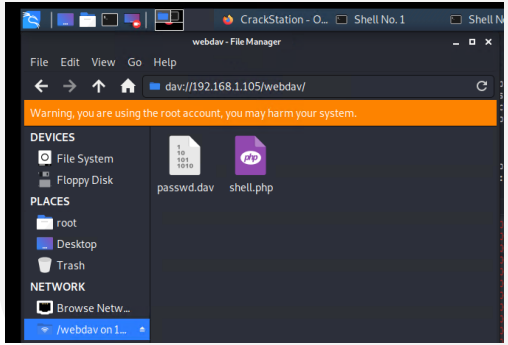
- **Crackstation** – To break the password hash
- **Msfvenom** – To create a custom payload to open a reverse shell to attacker
- Upload shell via WebDAV

02

Achievements:

Logged into WebDAV server using stolen credentails and uploaded payload (shell.php) into the share folder.

03



Exploitation: [Remote Code Execution]

01

Tools & Processes

Metasploit – To open meterpreter session to connect to target system once the uploaded payload is executed

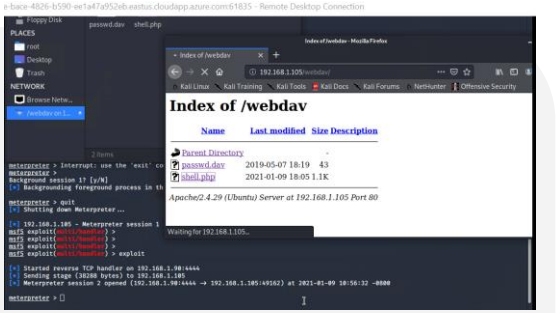
02

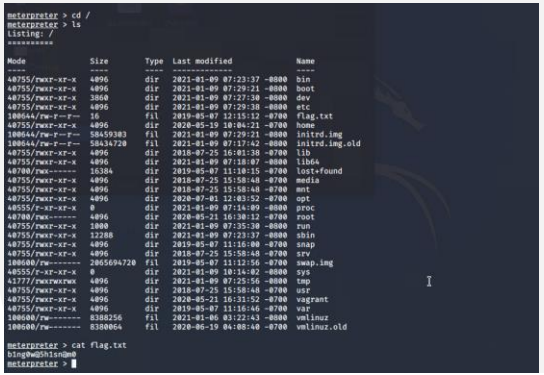
Achievements

Leveraging the RCE allows us to open a Meterpreter shell to the target

Achieving a shell on the target allows us to view all files and capture the flag

03





Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

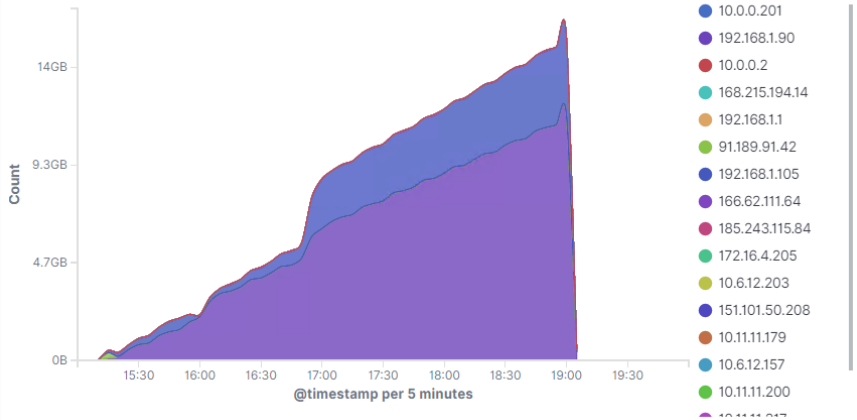
Network Traffic Between Hosts [Packetbeat Flows] ECS Jan 9, 2021 @ 15:00:00.000 to Jan 9, 2021 @ 20:00:00.000

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	278.2GB	5.9GB
192.168.1.90	192.168.1.105	53MB	94MB
192.168.1.90	192.168.1.1	704.4KB	2.5KB
192.168.1.90	192.168.1.90	351.9KB	328.1KB
192.168.1.90	172.253.115.99	286.2KB	5.9MB
192.168.1.105	192.168.1.100	86.2GB	4.4GB
192.168.1.105	91.189.88.152	325KB	288.3MB
192.168.1.105	91.189.91.43	257.4KB	164.8MB
192.168.1.105	91.189.91.42	211.7KB	80.7MB
192.168.1.105	91.189.88.142	186.3KB	43.8MB

Export: Raw Formatted

1 2 »

Top Hosts Creating Traffic [Packetbeat Flows] ECS Jan 9, 2021 @ 15:00:00.000 to Jan 9, 2021 @ 20:00:00.000

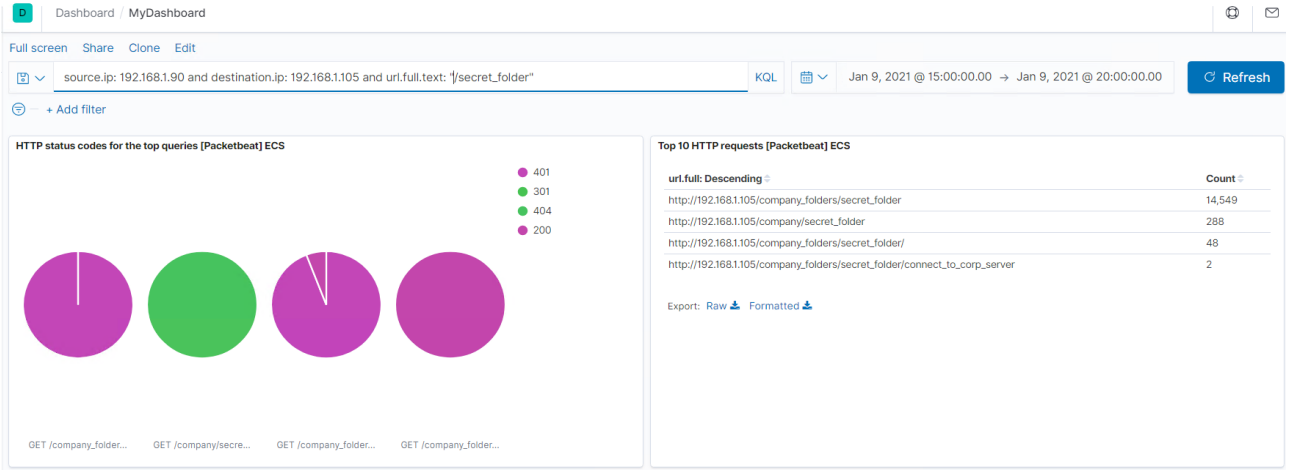


As seen in network traffic between hosts, spikes in traffice observed at 16:55 – 17:05. Source of the network traffic is source ip of attacking (kali) machine (192.168.1.90).

Response codes sent back by victim as 401, 301, 200 , 404 & 207 as seen in 'HTTP status codes for the top queries [packetbeat] ECS dashboard panel.

Response code of 401 indicates that unauthorized access attempt was made to secret_folder several times. 200 (OK), 301(Moved permanently), 404(Not Found) & 207(Multi-Status)

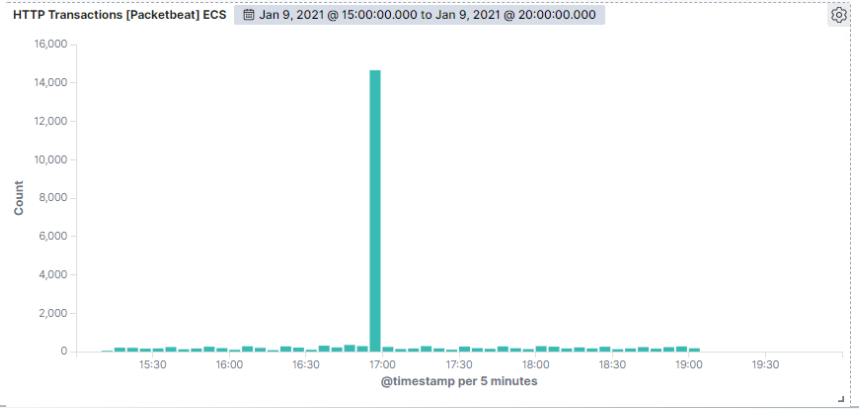
Analysis: Finding the Request for the Hidden Directory



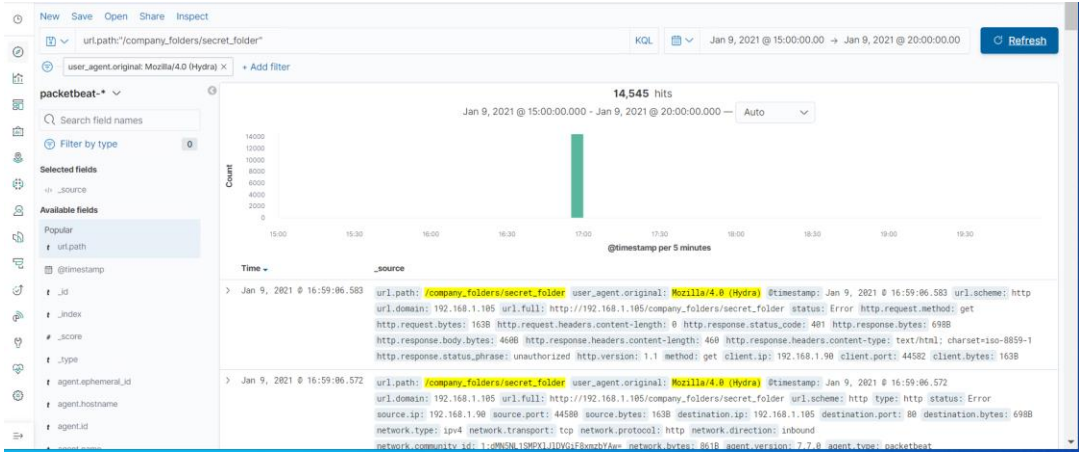
As seen in the Top HTTP requests dashboard, secret_folder was accessed 14,549 times from source ip address 192.168.1.90 which is attacker's machine.

File name 'connect_to_corp_server' from secret_folder was requested 2 times. This file has instructions on how to connect to the WebDAV directory, as well the user's username and hashed password.

HTTP Transactions shows that it occurred between 16:55 to 17:05.



Analysis: Uncovering the Brute Force Attack

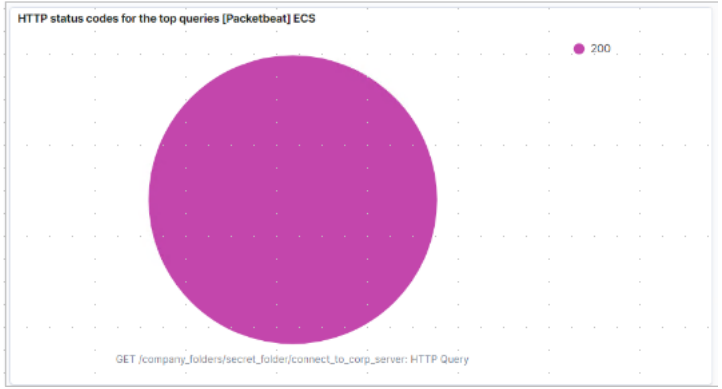


Top 10 HTTP requests [Packetbeat] ECS panel, contain evidence of large number of requests to sensitive secret_folder; but only 2 attempts were successful. This is a telltale signature of a brute-force attack.

Searching for url.path: ”/company_folders/secret_folder” shows the results from brute-forcing tool Hydra, which is identified by user_agent.original : Mozilla/4.0 (Hydra)

Top 10 HTTP requests [Packetbeat] ECS

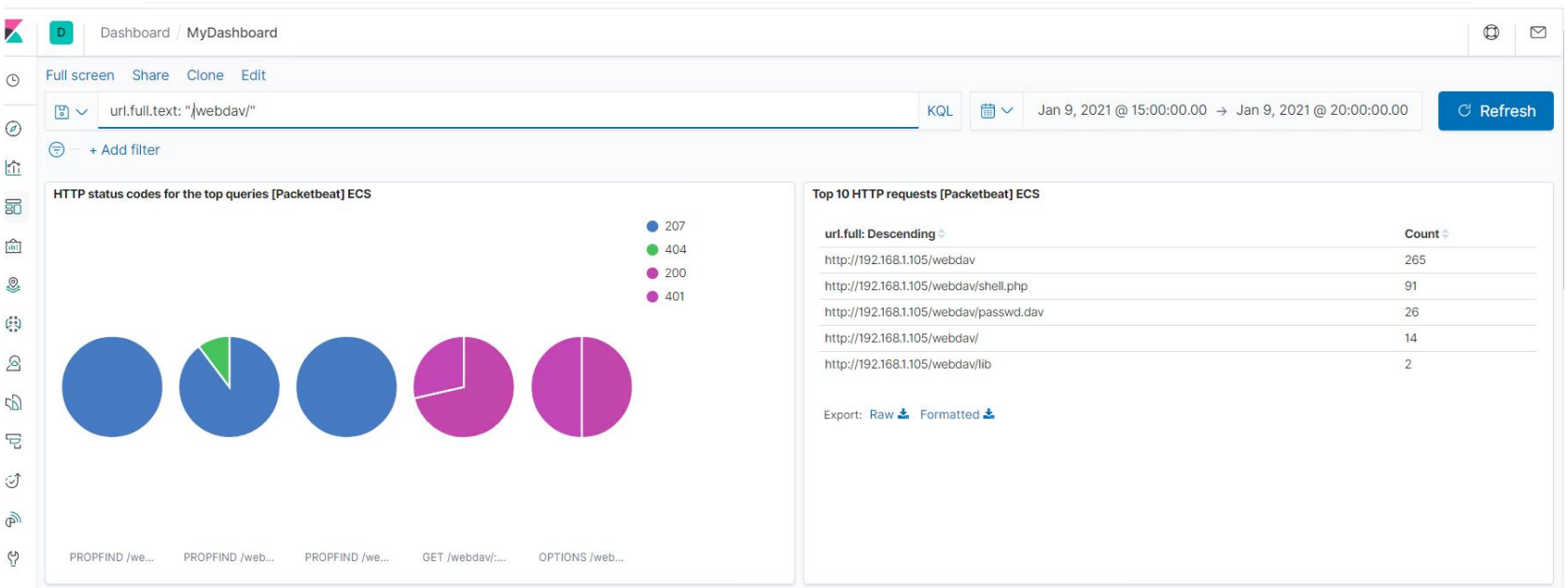
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	14,549
http://192.168.1.105/company/secret_folder	288
http://192.168.1.105/company_folders/secret_folder/	48
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2



Analysis: Finding the WebDAV Connection

Top 10 HTTP requests[packetbeat] ECS panel shows that attacker was able to access password protected webdav directory 265 times.

Shell.php inside webdav folder was accessed 91 times & passwd.dav was accessed 26 times.



url.full: Descending	Count
http://192.168.1.105/webdav	265
http://192.168.1.105/webdav/shell.php	91
http://192.168.1.105/webdav/passwd.dav	26
http://192.168.1.105/webdav/	14
http://192.168.1.105/webdav/lib	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?

- Alarm to monitor number of requests per second

What threshold would you set to activate this alarm?

- Alarms should be triggered if source IP address sends more than 25 requests per second for more than 5 seconds

System Hardening

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

- The local firewall can be used to throttle incoming connections
- ICMP traffic can be filtered
- An IP whitelist can be enabled
- Rate limiting traffic from single source in specified timeframe

Describe the solution. If possible, provide required command lines.
If client makes too many requests within a given time frame, HTTP servers can respond with status code 429: Too Many Requests.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Alarm should be triggered if unauthorized user attempt to access sensitive data.
- Alarm should be triggered if source of an access request is not from the permitted list of ip addresses allowed to access sensitive data.

What threshold would you set to activate this alarm?

- This is a binary alarm: It would be activated if the incoming IP is not whitelisted or user is not in permitted list of users.

System Hardening

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

- Secret_folder should be moved to system with strict access controls like key-based SSH access from whitelisted ip addresses
- Only authorized users should be able to access sensitive data
- In addition, inside file should be encrypted at rest.
- Filebeat should be configured to monitor and log access to secret_folder directory & its content.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Alarm for error code 401 (Unauthorized client)
- Excessive amount of bandwidth over the course of single session

What threshold would you set to activate this alarm?

- More than 100 responses per second for 5 seconds should trigger the alarm
- Sudden spike in BW consumption than the usual baseline should trigger the alarm for investigation.

System Hardening

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

- Configuring fail2ban or a similar utility would mitigate brute force attacks

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Access from source IP's other than whitelisted ip addresses
- Login failed events for webdav directory should be monitored
- Monitor access to webdav with Filebeat

What threshold would you set to activate this alarm?

- Access from source ips not listed in whitelisted ip addresses would trigger the alarm.
- More than 2 consecutive failed login attempts to webdav directory would lockout the account until enabled by administrator

System Hardening

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

- Administrators must install and configure Filebeat on the host.
- Deny access to RDP ports from external network

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alarms should trigger upon receipt of any POST request containing form or file data of a disallowed file type,

e.g., .php.

What threshold would you set to activate this alarm?

- The alarm should fire whenever users upload a forbidden file.

System Hardening

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

- Write permissions can be restricted on the host
- Uploads can be isolated into a dedicated storage partition.
- File uploads should require authentication
- Implement upload filter on server by disallowing users to upload files containing executable scripts codes

the End