Capstone Engagement

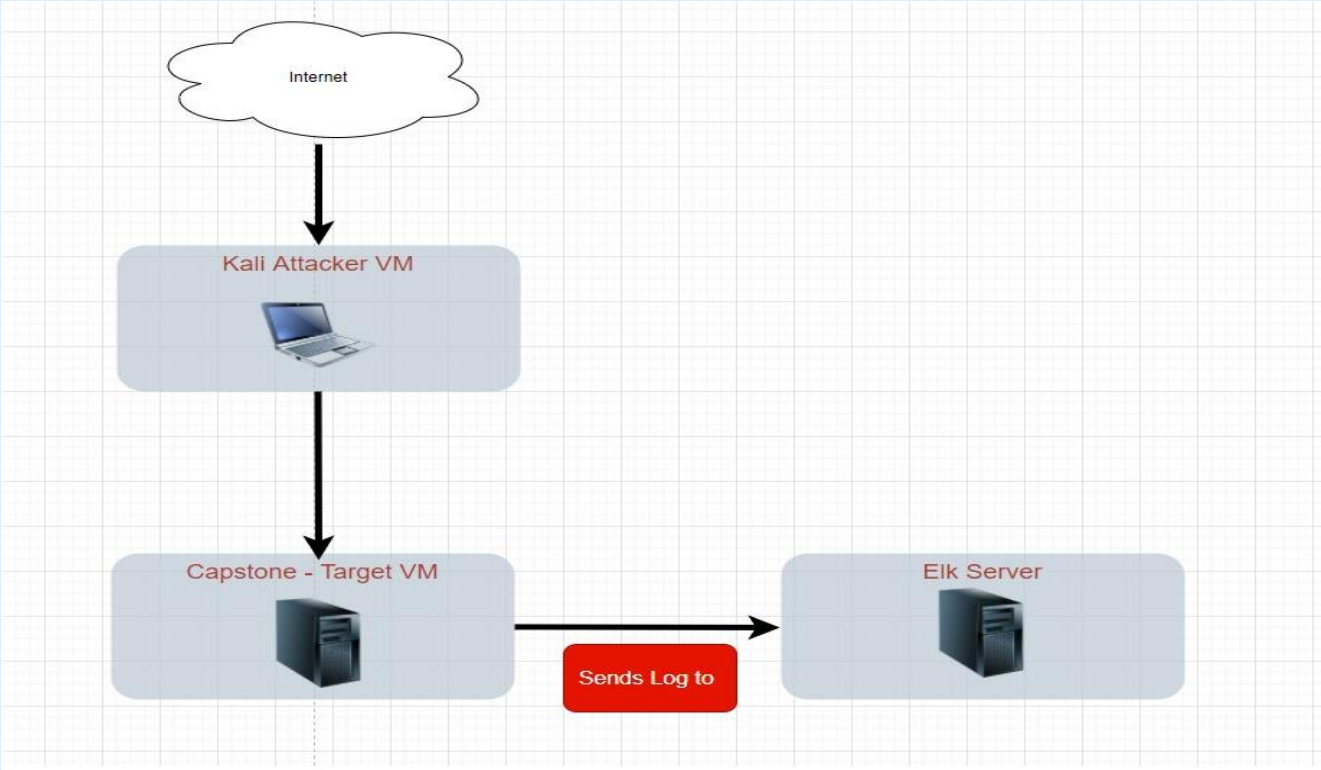
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
IP 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: 192.168.1.100
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
➢ Host	➢ 192.168.1.1	➢ Gateway
➢ ELK	➢ 192.168.1.100	➢ Monitor Machine <Kibana>
➢ Linux – Kali	➢ 192.168.1.90	➢ Hacker Machine (Attack)
➢ Capstone	➢ 192.168.1105	➢ Victim Machine

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 || A3:2017 - **CWE-200**	The secret_folder is publicly accessible, but contains sensitive data intended only for authorized personnel.	*The exposure compromises credentials that attackers can use to break into the web server. (Port 80)*
Unauthorized File Upload - Brute Force Attack	an attacker may use to access a dictionary (file/folder) on web.	This vulnerability allows attackers to upload PHP scripts to the server.
Remote Code Execution via Command Injection OWASP Top #1 ||A1:2017-Injection **CWE-94**	Attackers can use PHP scripts to execute arbitrary shell commands.	Vulnerability allows attackers to open a reverse shell to the web server. (shell.php)

Exploitation: Sensitive Data Exposure

01

Tools & Processes

- `nmap` discovering hosts that are available and the services they offer, finding open ports and detecting security risks.
- `dirb` comes with a set of preconfigured attack wordlists for easy usage.
- Browser to explore tools for accessing the Internet port 80 (http)

02

Achievements

- The exploit revealed a 192.168.1.105/company_folders/secret_folders/connectocorp_server directory.
- Hydra run to find password on ashton (victim). Attacker did access a company folder (secret_folders).

03

Exploitation

- The login prompt reveals that the user is `ashton` and password is `leopoldo` from Hydra ran.
- Hydra command ran with rockyou.txt resulted.

```
[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
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-08-09 18:46:43
root@Kali:/#
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

- CrackStation.net credentials to connect via WebDAV
- Upload shell via WebDAV
- msfvenom

02

Achievements

- Hash allows you to quickly identify types of hashes used to encrypt passwords
- A web shell allows us to execute arbitrary shell commands on the target
- msfvenom is used to make payload to penetrate the victim machine.

03

Aftermath

- User is ryan and password is linux4u to access on WebDAV site and displayed a passwd.dav file.
- Uploaded shell.php script via WebDav
- Run php code via meterpreter reverse tcp location 192.168.1.90 port 4444 to writing via php file for shell code.

Exploitation: Remote Code Execution

01

Tools & Processes

- Msfconsole used interface to work with Metasploit framework.
- Meterpreter to connect to uploaded web shell.
- Use shell to explore and compromise target.

02

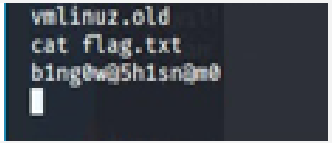
Achievements

- allows us to open a Meterpreter shell to the target
- shell that is initiated from a victim's server to connect with attacker's computer.
- Metasploit attack payload that provides an interactive shell.

03

Aftermath

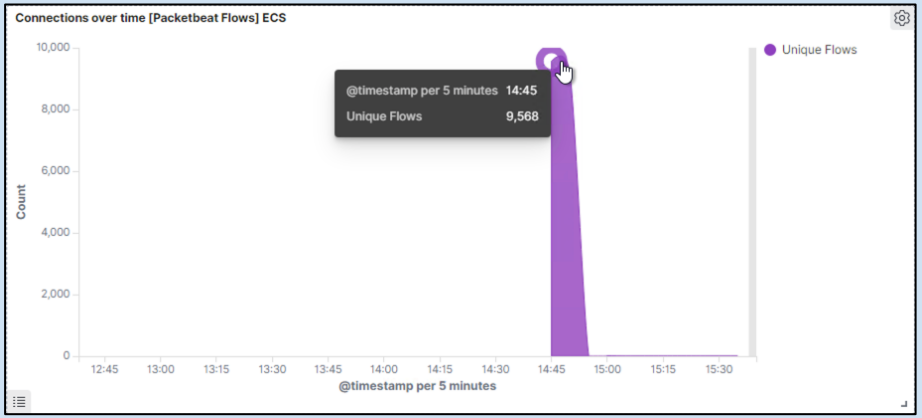
- Achieved a shell on the target allows us to display all files and capture the flag.
- uploaded PHP web shell in a web server
- Found the flag file.
- Ran flag.txt

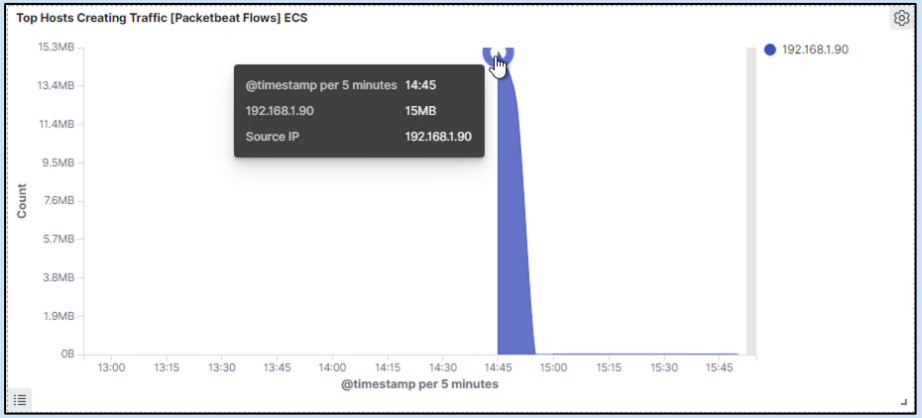


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





What time did the port scan occur?

- 2:45

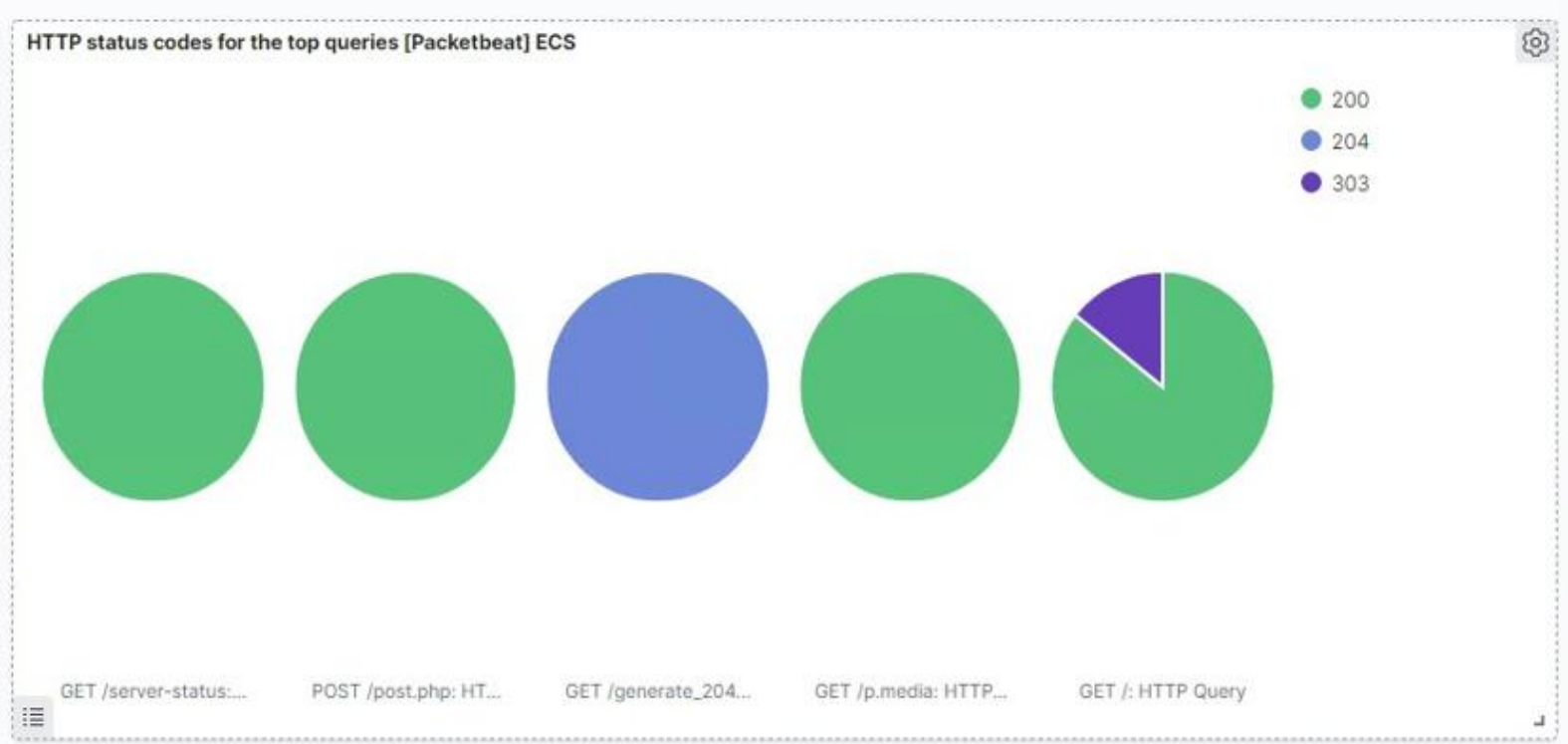
How groups of many packets were sent and from which IP?

- Resting the courser at the top of the arc, we can observe **9,568.** In the second chart we can observe it's the IP address **192.168.1.90**.

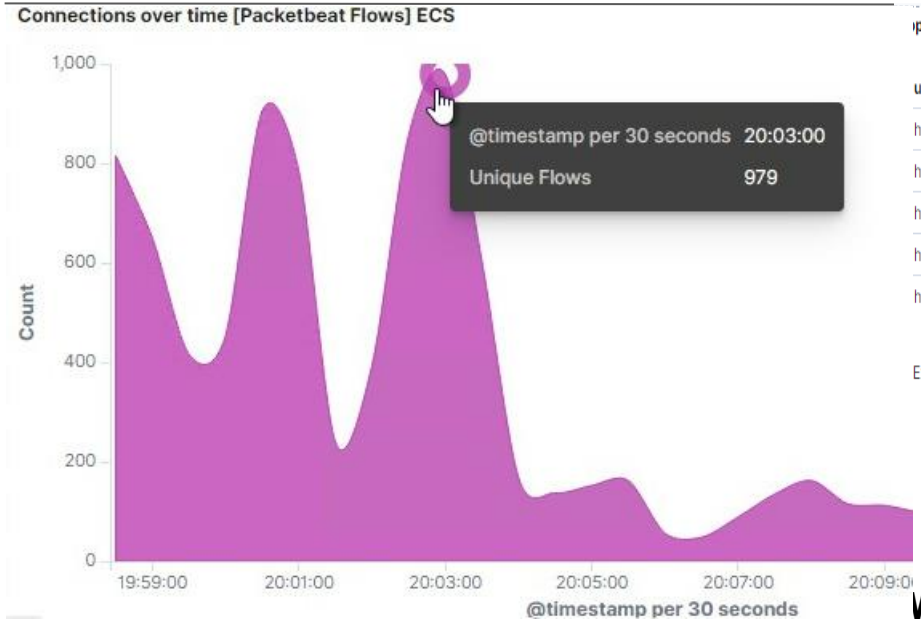
We can observe that the victim responded back with 401 (Unauthorized), 207 (Multi-Status), 200 (OK), and 404 (Not found) responses.

Analysis: Identifying the Port Scan (cont.)

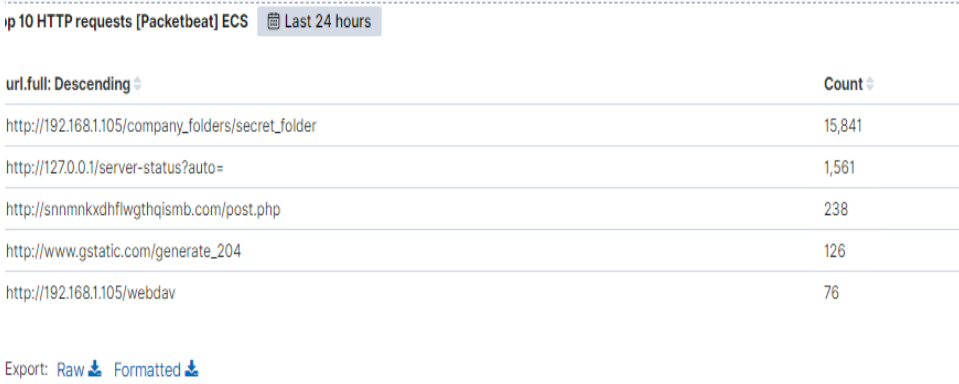
What responses did the victim respond back with?



Analysis: Finding the Request for the Hidden Directory



- In the first screenshot we can observe that the attack started at **8:03** with 979 requests.



url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,841
http://127.0.0.1/server-status?auto=	1,561
http://snnmnkxdhflwgthqismb.com/post.php	238
http://www.gstatic.com/generate_204	126
http://192.168.1.105/webdav	76

Which files were requested? What did they contain?

The top three hits for directories and files that were requested were:

- `http://192.168.1.105/company_folder/secret_folder`
- `http://192.168.1.105/company_folder/webdav`
- `http://192.168.1.105/webdav/shell.php`

Analysis: Finding the WebDAV Connection

The `secret_folder` directory was requested **6,961 times**.

The `shell.php` file was requested **6 times**.

Top 10 HTTP requests [Packetbeat] ECS Last 24 hours

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,841
http://127.0.0.1/server-status?auto=	1,561
http://snnmnkxdhflwgthqismb.com/post.php	238
http://www.gstatic.com/generate_204	126
http://192.168.1.105/webdav	76

Export: Raw Formatted

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	6,961
http://192.168.1.105/webdav	14
http://192.168.1.105/webdav/	8
http://192.168.1.105/webdav/shell.php	6
http://192.168.1.105/company_folders/secret_folder/	5

Export: Raw Formatted

server.ip	192.168.1.105
server.port	80
source.bytes	163B
source.ip	192.168.1.90
source.port	42000
status	Error
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder
url.path	/company_folders/secret_folder
url.scheme	http
user_agent.original	Mozilla/4.0 (Hydra)

The logs contain evidence of a large number of requests for the sensitive data. Only 5 requests were successful. This is a telltale signature of a brute-force attack.

- Specifically, the password protected `secret_folder` was requested 6961 times, but the file inside that directory was only requested 5 times. Out of 6209 requests, only 5 were successful.

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?

- NMAP is a tool of choice for penetration testers when an alert comes to port scanning.

What threshold would you set to activate this alarm?

- 15 Ports within 5000 milliseconds

System Hardening

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

- Block unused ports in the firewall.
- IDSs log an alarm entery into network. Most IDSs are located where they can see as much traffic
- You can change it in script. After that attacker will not to be able to open access anything.
- Keep Current on all security patches.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- HTTP GET request

What threshold would you set to activate this alarm?

- This is a **binary** alarm: If the incoming IP is *not* allowed, it fires. Otherwise, it does not.

System Hardening

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

- Access to the sensitive file can be locally restricted to a specific user.
- This way, someone who gets a shell as, e.g., www-data will not be able to read it.
- In addition, the file should be encrypted at rest.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- **# of Requests per Second**

What threshold would you set to activate this alarm?

- More than 100 requests per second for 5 seconds should trigger the alarm

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?

- Monitor access to `webdav` with Filebeat
- Fire an alarm on any read performed on files within `webdav`

What threshold would you set to activate this alarm?

- Simply fire the alarm whenever someone accesses the `webdav` directory.
- Ideally, allow valid IP addresses.

System Hardening

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

- Administrators must install and configure Filebeat on the host.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alarms should fire 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?

- Keep Current on all Security Patches.
- Detect and Respond to Intrusions Quickly.
- Implement Principle of Least Privilege (Minimize Data Access).
- Use Multi-Factor Authentication.
- Implement IP Whitelisting.
- Encrypt Network Traffic Inside the System.
- The attacking IP address will be blacklisted for 24 hours.

the End