Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

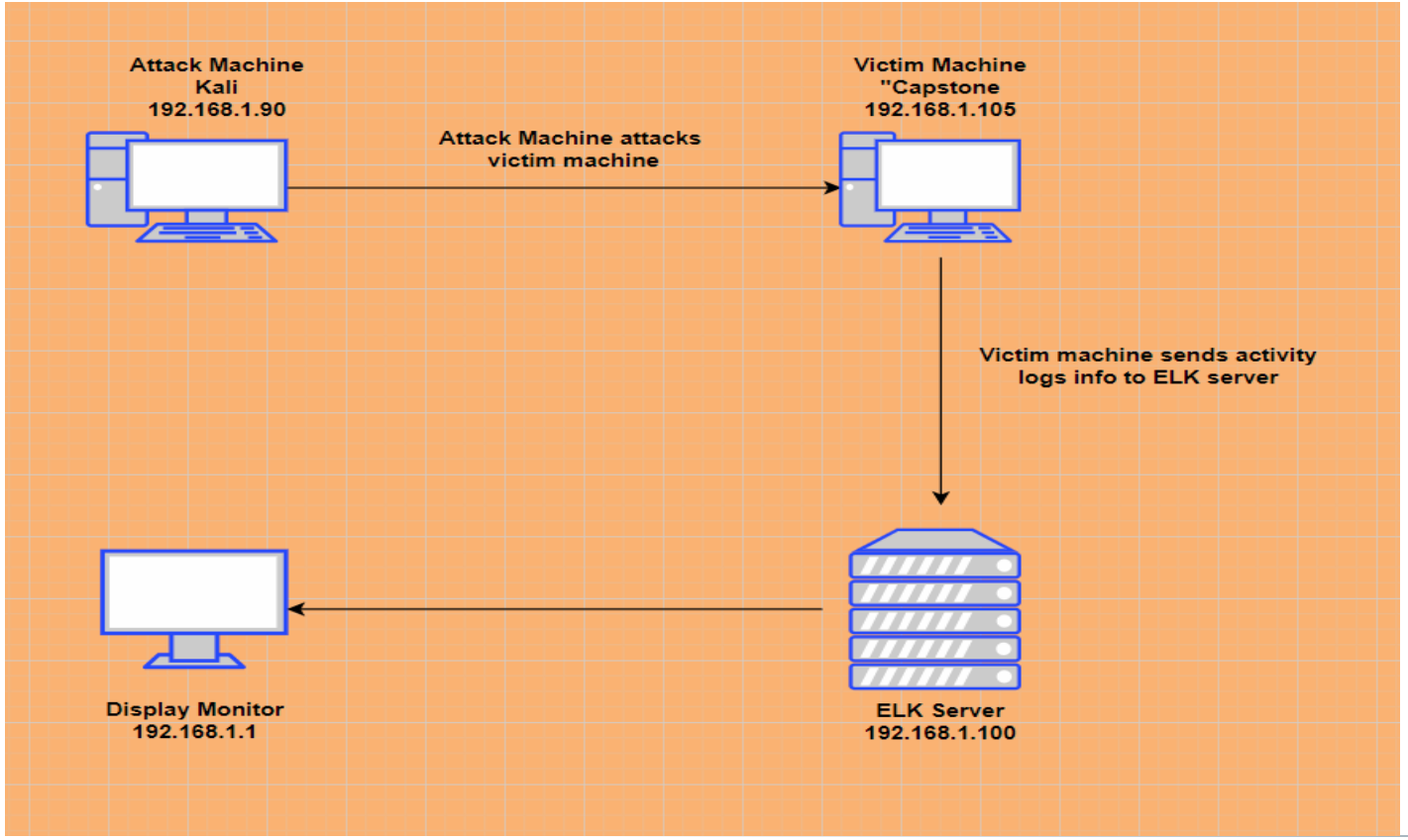
Felix Amenumey

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network

Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
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

IPv4: 192.168.1.1
OS: Windows
Hostname:ML-REfVm-0684427

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVM-684427	192.168.1.1	Host Machine
Kali	192.168.1.90	Attacker Machine
Server 1 (Capstone)	192.168.1.105	Victim Machine
ELK	192.168.1.100	Monitoring Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute force	Allowed unlimited attempt to break user logins and passwords	It led us to gain access to credentials by using tools such as hydra
WebDAV software (sensitive data exposed)	Allowed accessing shared folder from any machine	It led to upload php shell
Reverse shell payload	Allows attacker to execute arbitrary code	It could lease to escalating privilege to compromise the system. Attacker can install delete

Exploitation: Accessible Folders

01

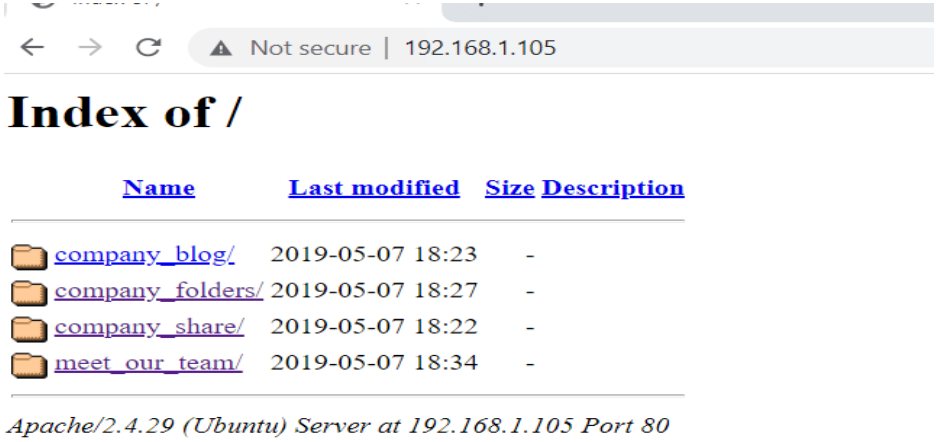
Tools & Processes

Port 80 was used to open a web browser to seek vital information

02

Achievements

Accessing the files gave us Intel on which users had access to what and where their secret files were located.



Exploitation: Brute Force Attack

01

Tools & Processes

We used the too Hydra to brute force Ashton's password using the username: ashton.

```
root@Kali:~# hydra -l ashton -P ./rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders
/secret_folder/
```

```
ild 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [chil
d 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [
child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [
child 2] (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
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-25 11:47:16
root@Kali:~#
```

02

Achievement

The exploit granted us user shell access into the victim machine so we could navigate to the secret files

Exploitation: Remote Code Execution

01

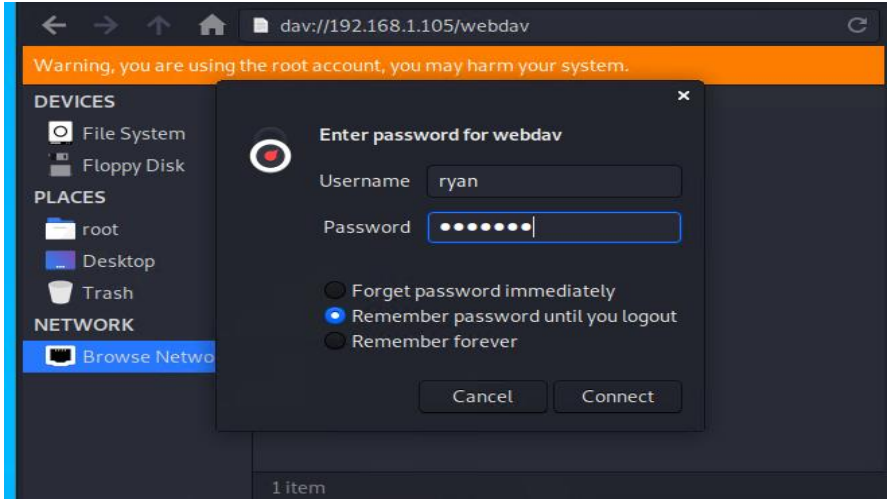
Tools & Processes

Shell was uploaded through WebDAV

02

Achievement

Web shell was uploaded to allow execution of arbitrary commands on the target.

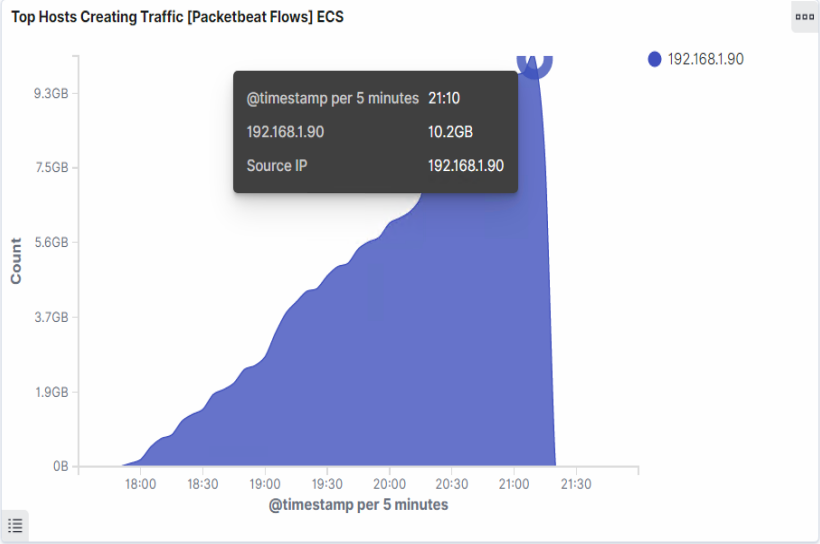


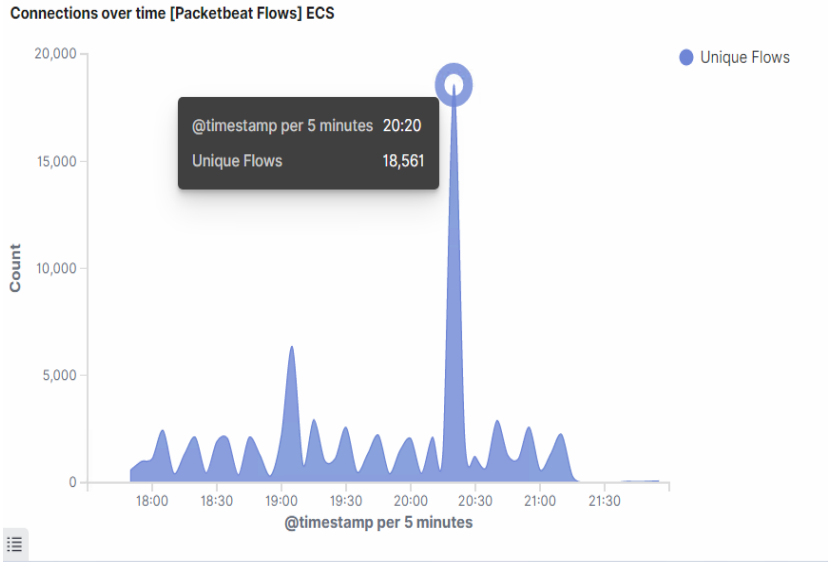
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

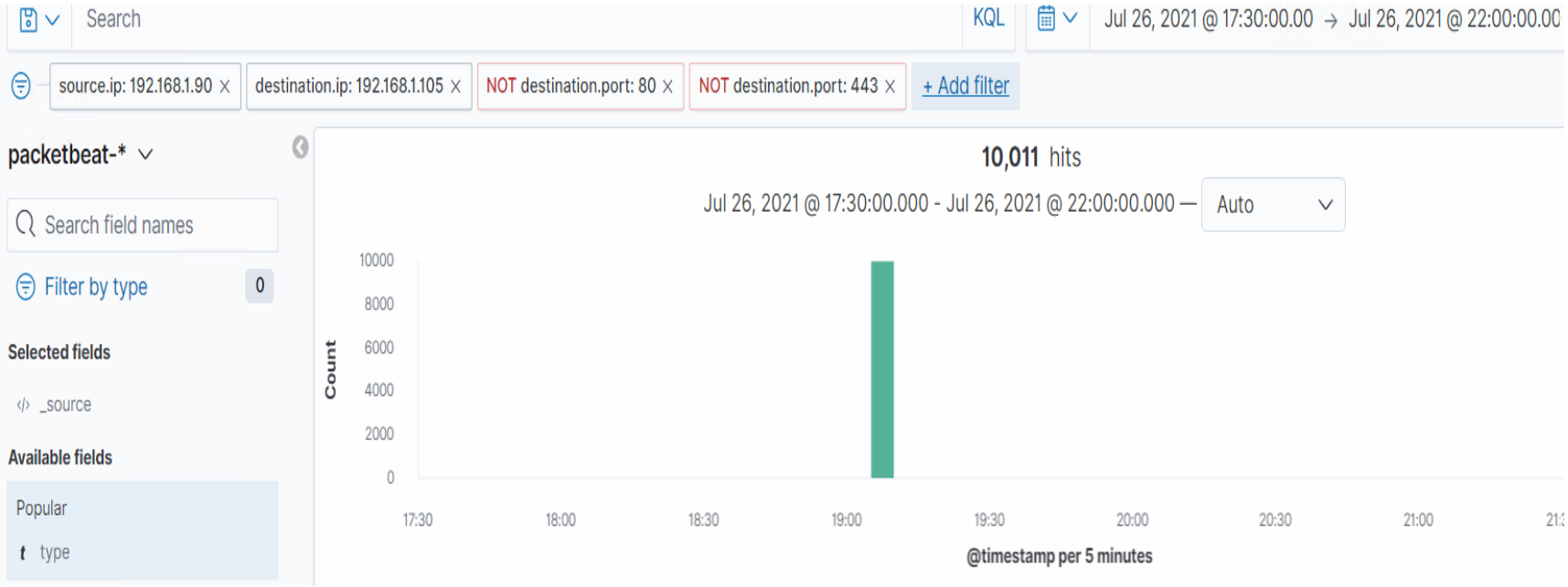
- 20:20
- 18,561 packets were send from IP address 192.168.1.90





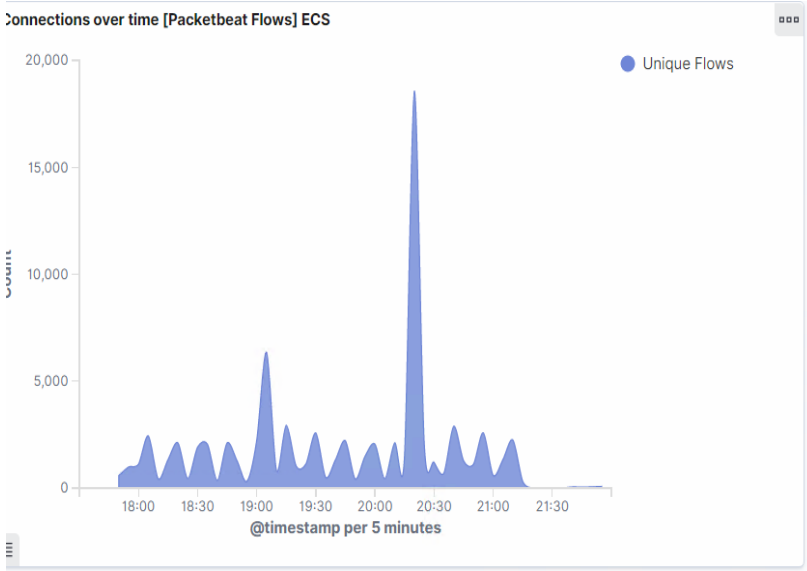
Analysis: Identifying the Port Scan (Cont.)

- port 80 and 443 were not scanned, but other ports were scanned 10.011 times



Analysis: Finding the Request for the Hidden Directory

- The request occurred at 20:20 and 18,561requests were made.
- The file requested were:
  - http://192.168.1.105/company_folder/secret_folder
  - http://192.168.1.105/webdav
  - http://192.168.1.105/webdav/shell.php



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	14,991
http://192.168.1.105/webdav	95
http://192.168.1.105/webdav/shell.php	22
http://192.168.1.105/webdav/passwd.dav	14
http://192.168.1.105/	8

Analysis: Uncovering the Brute Force Attack

- The logs contain evidence of a large number of request for sensitive data. Only 3 requests were successful. This is an indication of Brute force attack.
- Specifically, the password protected “secret_folder” was Requested 14,991 tines, but the file inside the directory Was only requested 22 times. Out of **14,991** requests, Only **3** were successful.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	14,987
http://192.168.1.105/webdav	4

Export: Raw Formatted

Top 10 HTTP requests [Packetbeat] ECS

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

t url.domain	192.168.1.105
t url.full	http://192.168.1.105/company_folders/secret_folder/
t url.path	/company_folders/secret_folder/
t url.scheme	http
t user_agent.original	Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection

- The secret_folder directory was requested **14,991 times.**
- The shell.php file was requested **22 times.**

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	14,991
http://192.168.1.105/webdav	95
http://192.168.1.105/webdav/shell.php	22
http://192.168.1.105/webdav/passwd.dav	14
http://192.168.1.105/	8

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?
- **Set alarm for a number of port scans per minutes**

What threshold would you set to activate this alarm?
- Alarm should go off if a given IP address sends more than 20 requests per minutes for more than 10 minutes

System Hardening

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

- **Firewall should be set to enable only traffic that could access internal host, and deny all other ones.**
- **ICMP traffic can be filtered**

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Alarm should go off if any unauthorized IP address attempts to connect

What threshold would you set to activate this alarm?

- The treshhold should be more than 1 attempt

System Hardening

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

- **Making sure that only specific users could have access vital or vert sensitive files**
- **Also, 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?

- Alarm will be set for unauthorized requests

What threshold would you set to activate this alarm?
- More than 90 requests per seconds for 5 seconds should set off an alarm

System Hardening

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

Set up at lockout for IP addresses that receive 401 response.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
- Set up an alarm on Filebeat for any unauthorized read performed on webdav

The threshold should be more than one attempt

System Hardening

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

_ Administrators should install and configure Filebeat on the host machine.
- Also, connections to the folder should not be accessed from the web interface.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alarm should go off for any authorized file data upload, such as '.php' to the server

What threshold would you set to activate this alarm?

- **The alarm should go off whenever unauthorized file data is uploaded.**

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.
- Filebeat should be enabled and configured.

the End