Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Mary Yang, Cameo Reindl, Christina LeBaron, Rob Myers,

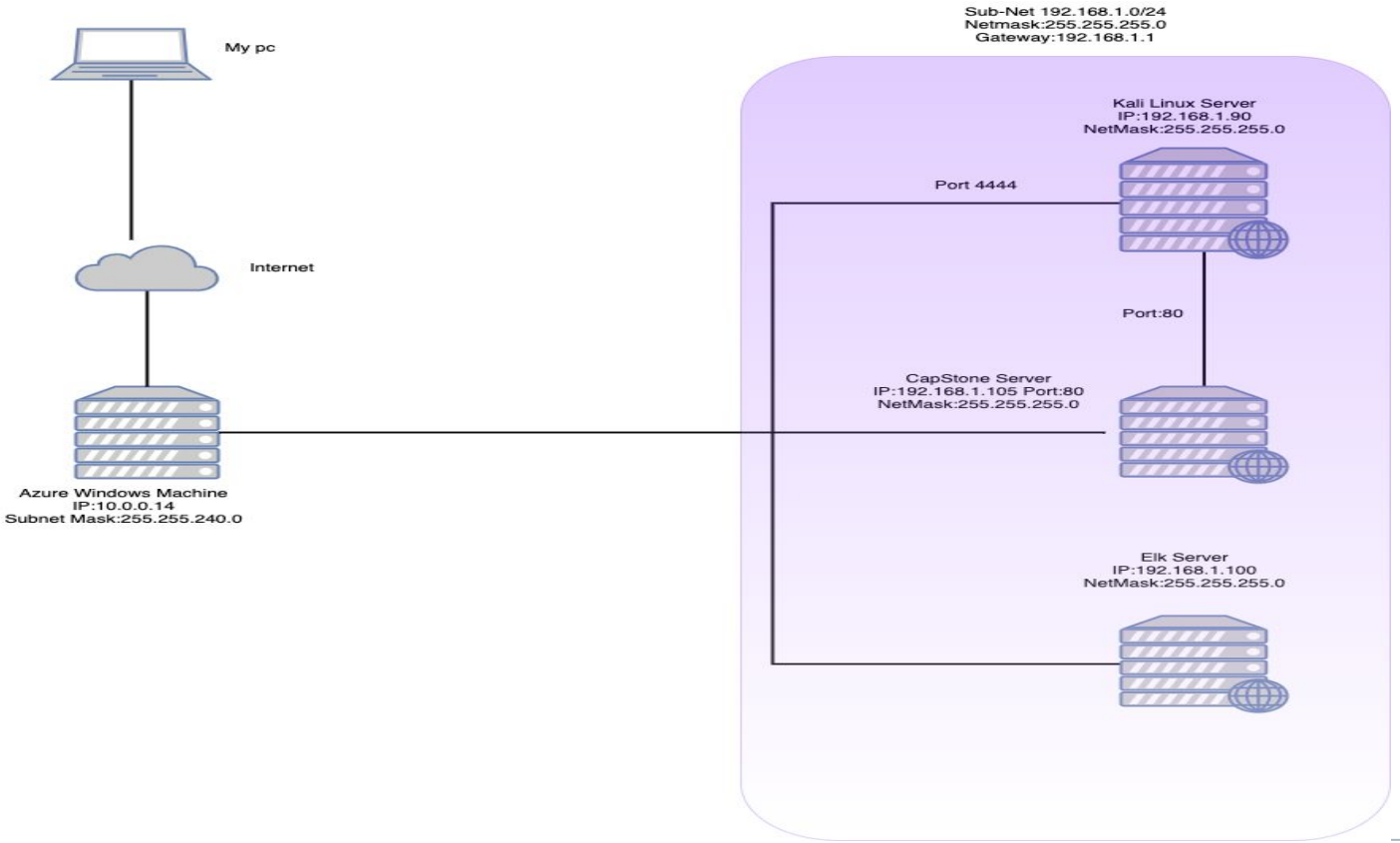
Phillip Snell, Georges Avenie

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-684424 **AZURE**
:

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper V (Manager)	192.168.1.1	Host of virtual machines used to attack, defend, and monitor activity.
Kali	192.168.1.90	Attacker Machine (Kali Linux)
Capstone	192.168.1.105	Victim Machine
ELK	192.168.1.100	Collect logs from server and application, to analyze

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 opened	Open ports are dangerous and has poor network security rules. This vulnerability makes sensitive data more publicly accessible	We (attackers) were able to access sensitive files.
Local File inclusion Vulnerability	LFI allows access into confidential files on a site. This is a web vulnerability on the programming side that a hacker can exploit to add malicious executable files.	We exploited this web vulnerability by adding a reverse shell script file to the website that when clicked, allowed us access to the victim's machine.

Exploitation: [Nmap scan]

01

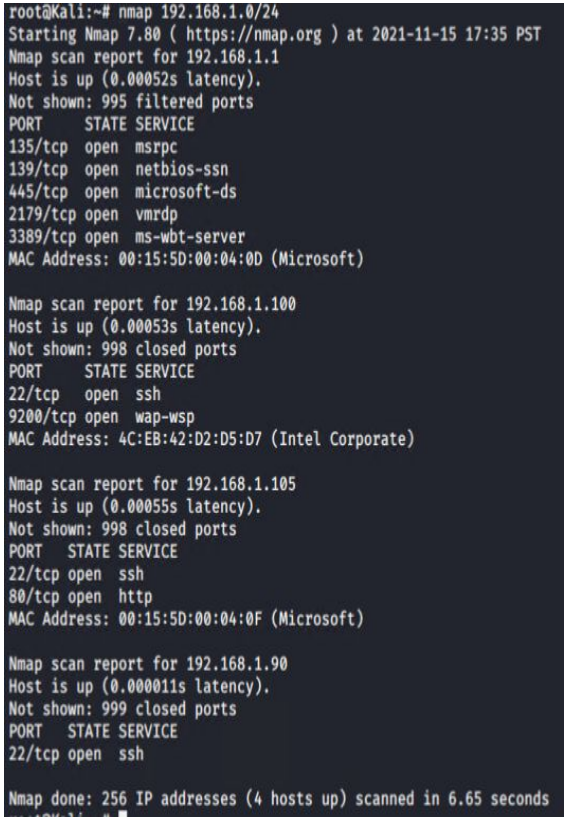
Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

To find this vulnerability we used nmap to discover which ports are open and which services are being used.

02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

We discovered that our target machine with IP 192.168.1.105 had port 80 open. Through this port we were able to access the website's directory and find sensitive file data.



Exploitation: [Brute Force:]

01

Tools & Processes
Hyrdra- used against directory to find secret folder and brute force into Capstone (victim's) machine

02

Achievements:
User: Ashton
Pw: leopoldo
With this information we were able to access system

```
[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 2021-11-15 18:38:52
root@Kali:~#
```

Exploitation: [Php Script]

01

Tools & Processes

Using open port 80, we accessed the target IP address in a web browser to view the vulnerable directories.

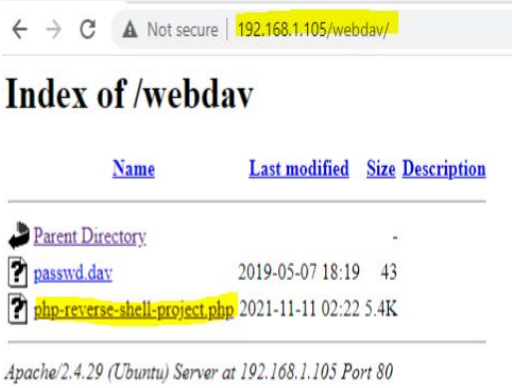
02

Achievements

This allowed us to find confidential login information and identify where important files were located.

Because the website has an LFI vulnerability, we are able to write a malicious executable file into the website's directory.

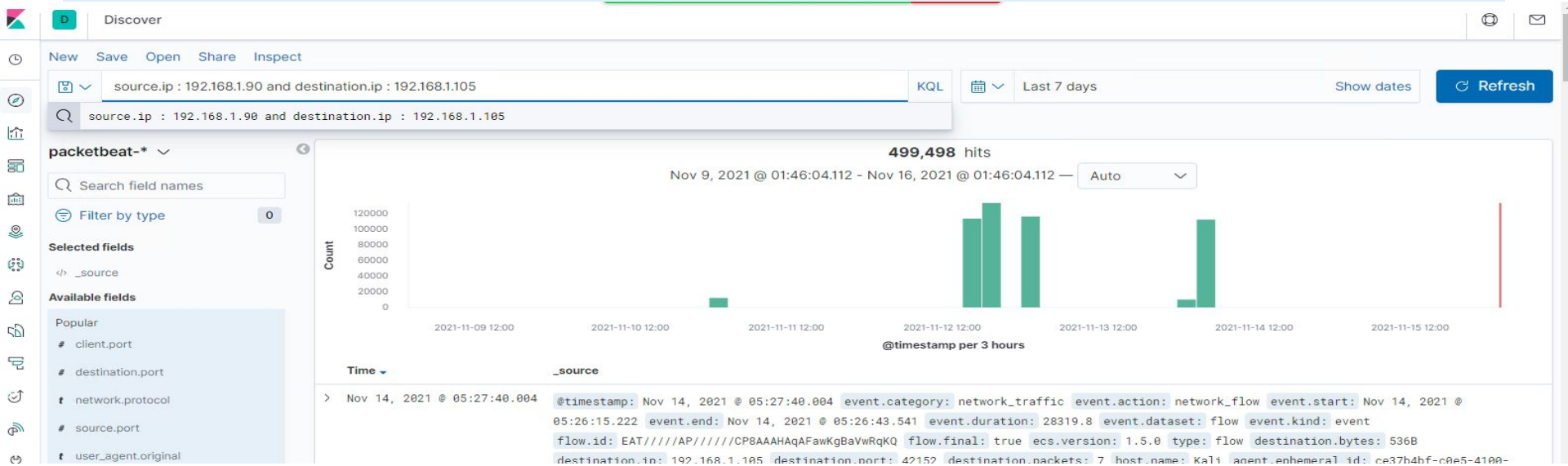
03



Blue Team
Log Analysis and Attack Characterization

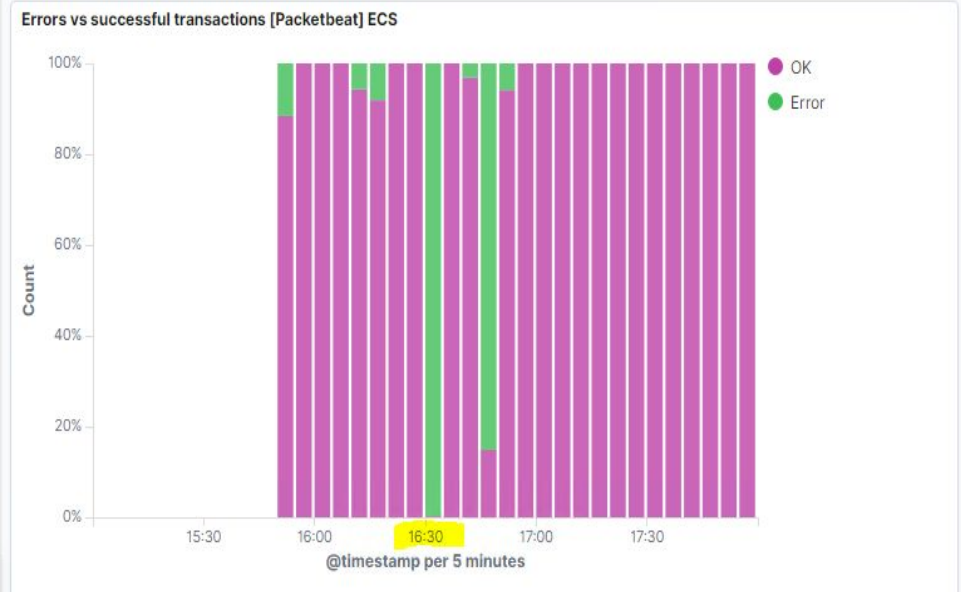
Analysis: Identifying the Port Scan

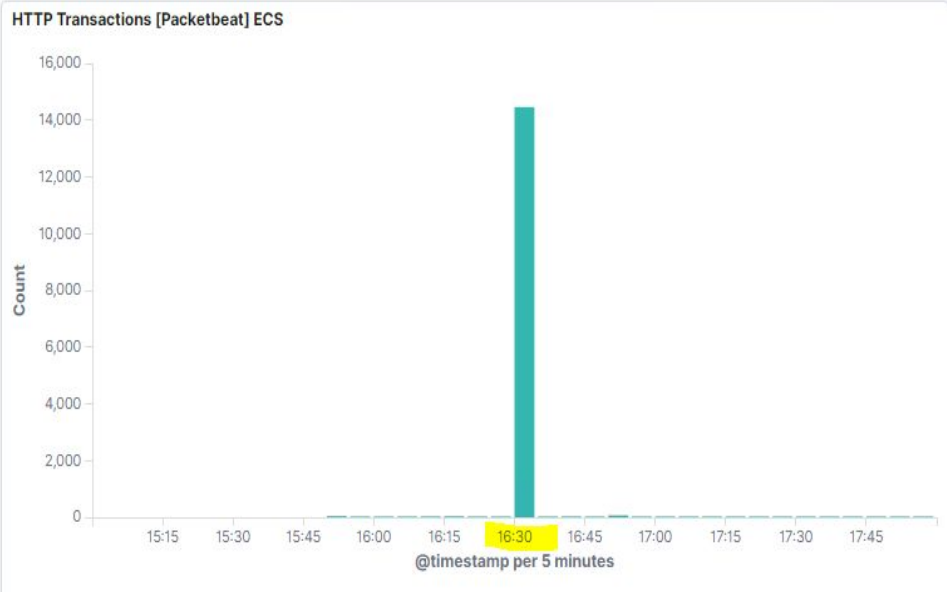
- What time did the port scan occur? Dashboard indicates the time as 6:00pm
- How many packets were sent, and from which IP? 499,498 hits from IP: 192.168.1.105
- What indicates that this was a port scan? Using scan source.ip : 192.168.1.90 and destination.port : 4444 demonstrates the port scan



Analysis: Finding the Request for the Hidden Directory

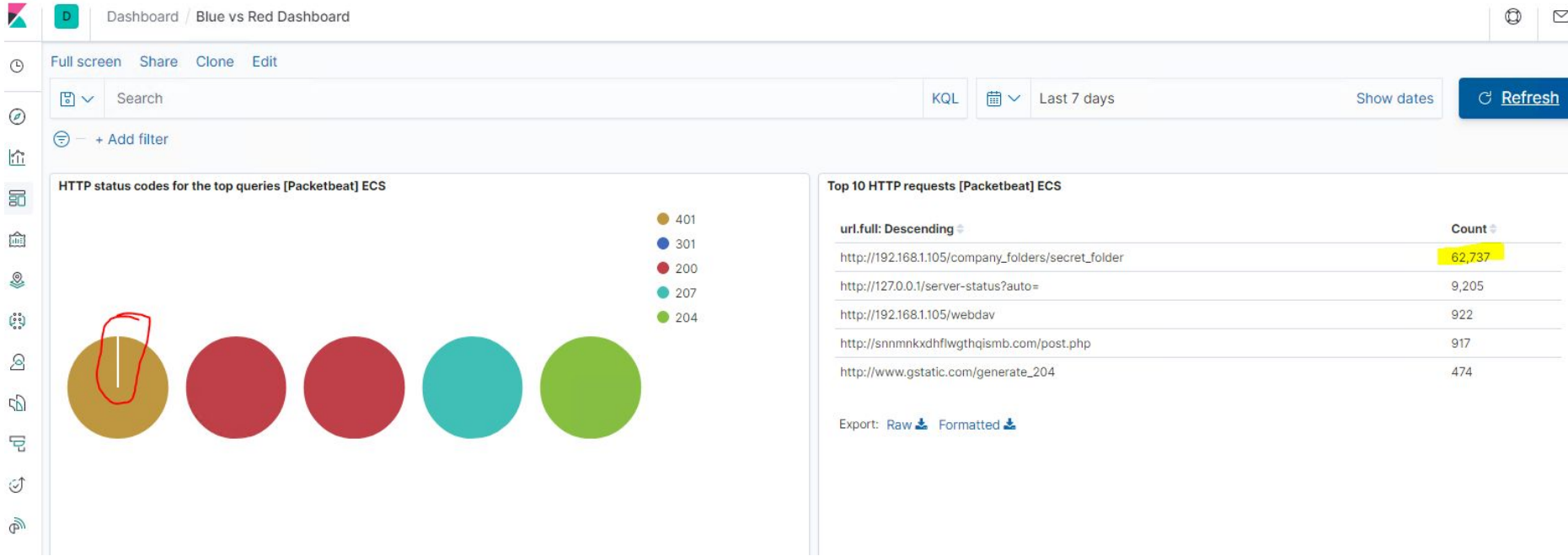
- What time did the request occur?4:30pm
- How many requests were made? 14423
- Which files were requested? http://192.168.1.105/company_folders/secret_folder
- What did they contain? The Secret Folder contained the HASH for Ryans Password





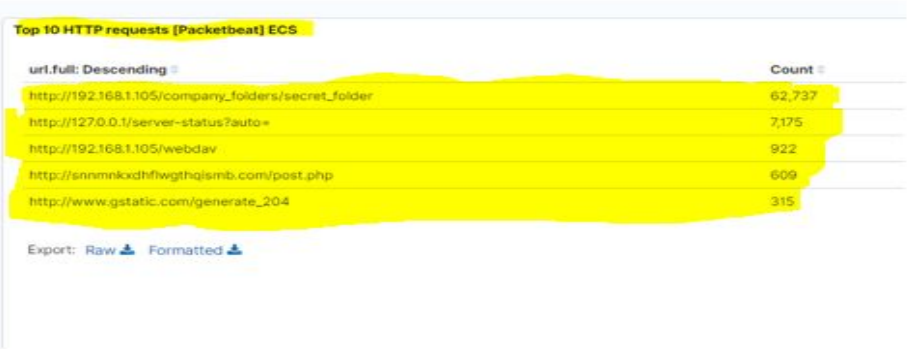
Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 14423
- How many requests had been made before the attacker discovered the password? 62737 total requests and only 1 user got through



Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? http://192.198.1.105/webdav count was 922
- Which files were requested? post.php



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?

- Establish an Alarm anytime there are more than 16,000 400 Error Requests in FIVE minutes

System Hardening

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

- Enable only the traffic needed to access internal hosts and deny everything else.
- Configure Fire Wall Rules to cut off attacks if a certain threshold is reached, such as 10 port scans in one minute.

Describe the solution. If possible, provide required command lines.

- Use your IDS like Kibana or SPLUNK for immediate alerting inorder to initiate the rapid response team

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Implement a strong password policy that locks out a user for 15 minutes after three unsuccessful login's as well as completely locking out the user after six unsuccessful login's
- Recomend implementing a multi-authentication procedure when resetting passwords

System Hardening

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

- Create a rule that locks out a user after a password threshold has been met

Describe the solution. If possible, provide required command lines.

- When a user enters three wrong passwords the user is locked out for 15 minutes

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Establish an Alarm when the user-agent.original indicates: Mozilla/4.0 (Hydra)
- Set the threshold to: ZERO

System Hardening

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

- Set rule to state: Block user-agent.original indicates: Mozilla/4.0 (Hydra)

Describe the solution. If possible, provide the required command line(s).

- When the Hydra user agent is detected block that traffic

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Create Alert anytime the IDS detects any webdav, PHP, or remote access connection

What threshold would you set to activate this alarm?

- Threshold is Zero

System Hardening

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

- Establish a rule that blocks: webdav, PHP, or remote access connection

Describe the solution. If possible, provide the required command line(s).

- Any remote access connection is unauthorized and requires immediate response

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Establish alarm anytime a file is uploaded from outside the internal network

What threshold would you set to activate this alarm?

- Threshold is Zero

System Hardening

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

- Establish a rule that blocks all file uploads from outside the internal network.
- Establish rules that restrict users from uploading files with out permission


The End