PROJECT--1
(INFORMATION GATHERING TOOL)

ABSTRACTION:(Information gathering tool)

-->The purpose is to collect the efficient information for cybersecurity professionals by using the tools.

-->The tool will focus on the network reconnaissance, using the NSE scripts.

-->Effective information gathering is crucial for identifying vulnerabilities and assessing security risks.

OBJECTIVE:

-->The goal is to develop a versatile tool that automates the reconnaissance tasks.

-->In this we utilize the Nmap Scripting Engine (NSE) scripts for the targets.

-->We use Auxiliary Modules (Metasploit) for additional scanning.

-->We have to obtain the proper authentication and do not cross the privacy.

INTRODUCTION:

-->The information can be gathered in two ways. They are

1)Active {automated - directly interacts with the target}
2)Passive {manual - not interacting with the target}

-->All the hackers and the cyber security professionals need the accurate and detailed information about the target systems.

-->Manual / Passive reconnaissance is time-consuming and it is not accurate.

-->So, the automated / active reconnaissance provides the valuable information in less time.

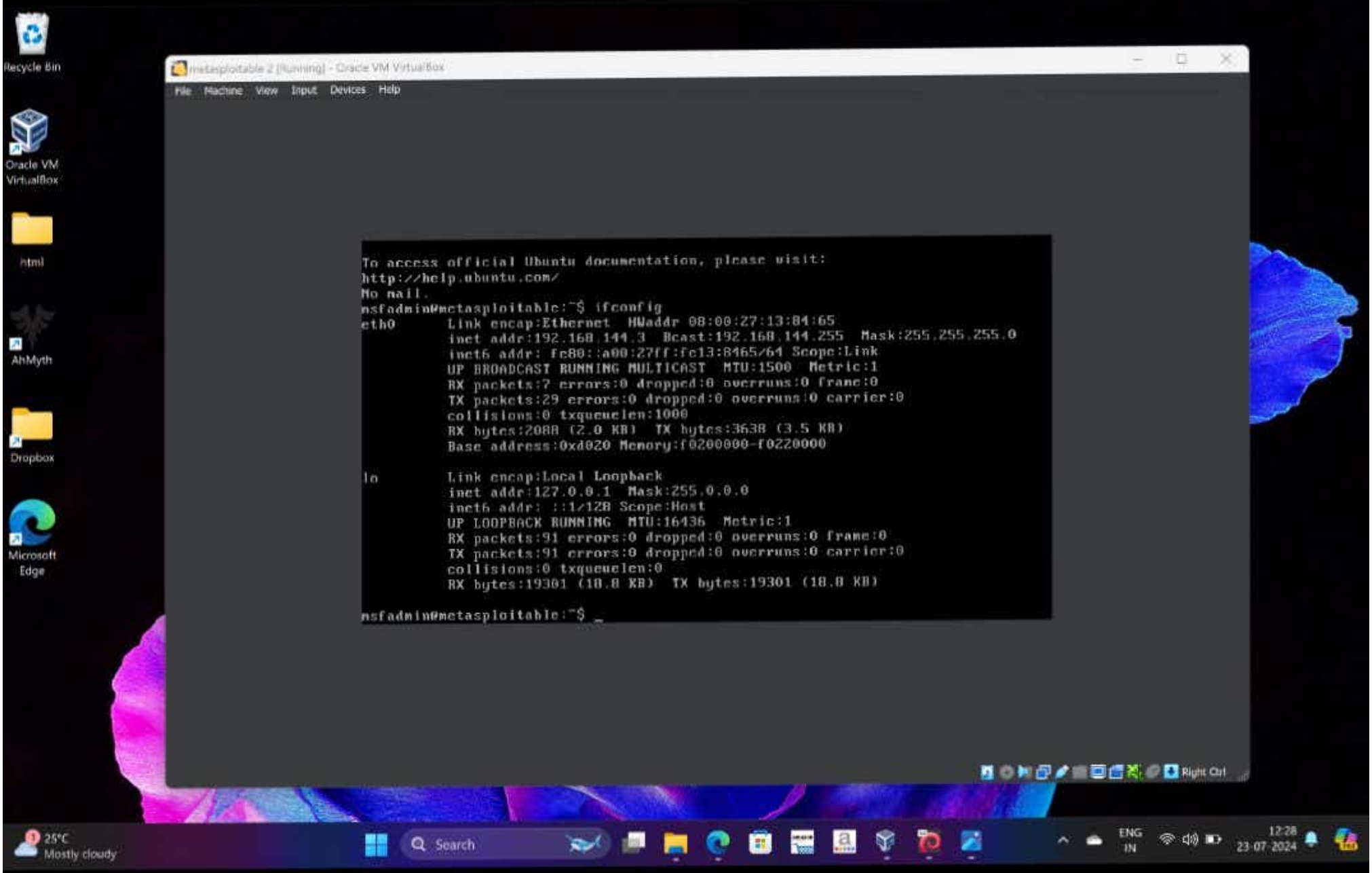
METHODOLOGY:

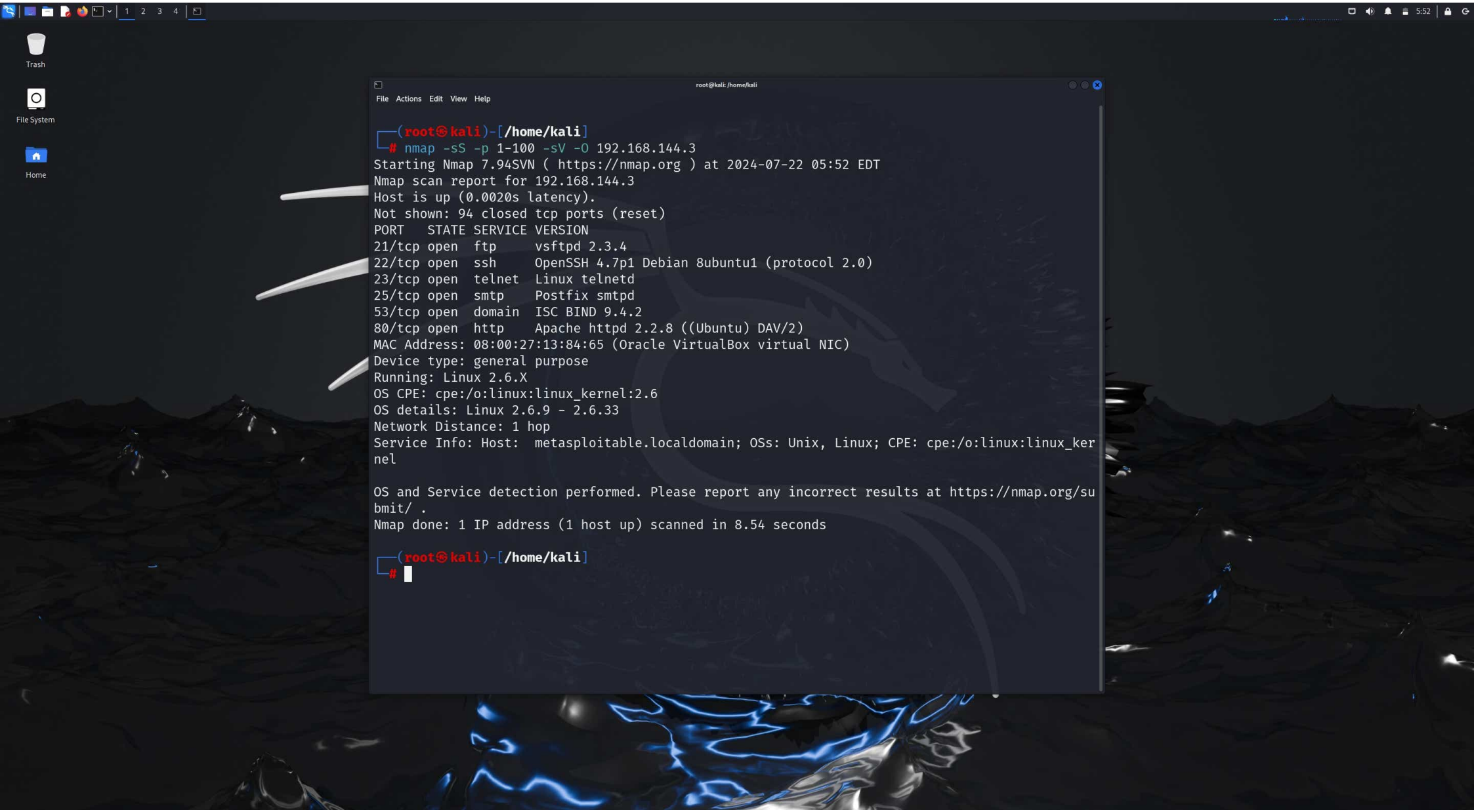
-->NSE (Nmap Scripting Engine) Scripts:

<>NSE scripts increases the Nmap's capabilities by automating the tasks during the scans.
=>Some of the information using Nmap tool (attacking on metasploitable2)

COMMAND => nmap -sS -p (port number/range) -sV -O <target ip address>

Where, -sS: sync scanning [-sF, -sA, -sX, -F, -A, -sT, -sU]
-p: represents port
-sV: scan fo version details
-O: operating system details


Recycle Bin
Oracle VM VirtualBox
html
AhMyth
Dropbox
Microsoft Edge
metasploitable 2 [Running] - Oracle VM 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 08:00:27:13:84:65
inet addr:192.168.144.3 Bcast:192.168.144.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe13:8465/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7 errors:0 dropped:0 overruns:0 frame:0
TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2088 (2.0 KB) TX bytes:3638 (3.5 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:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
msfadmin@metasploitable:~$ _
Right Ctrl
25°C
Mostly cloudy
Search
ENG
IN
12:28
23-07-2024


1 2 3 4
5:52
Trash
File System
Home
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 1-100 -sV -O 192.168.144.3
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-22 05:52 EDT
Nmap scan report for 192.168.144.3
Host is up (0.0020s latency).
Not shown: 94 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)
MAC Address: 08:00:27:13:84:65 (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
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
┌──(root㉿kali)-[/home/kali]
└─#

-->WHOIS:

<>This 'whois' command provides the information about the domain names,IP addresses, and the network.

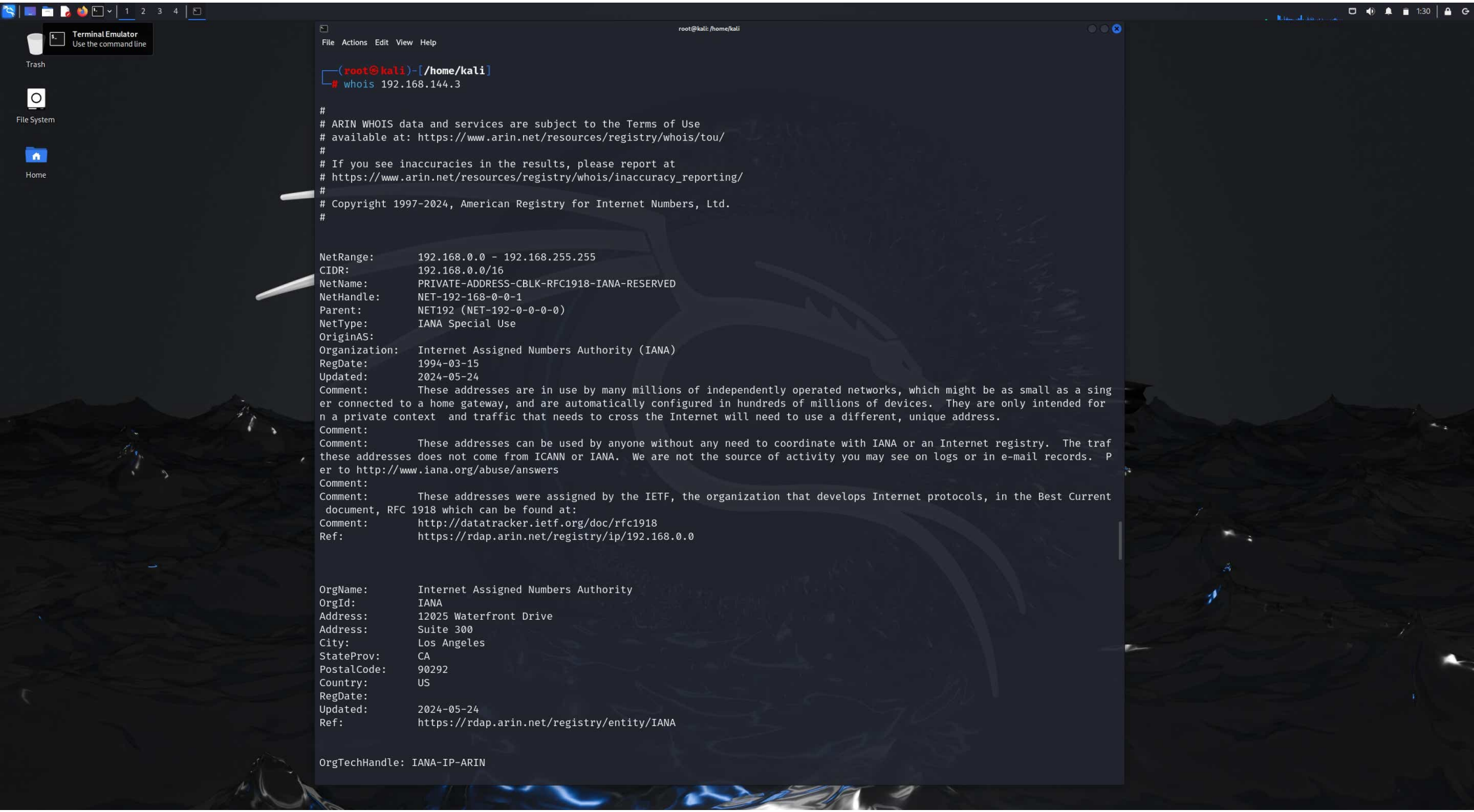
<>It gathers the details like contacts,mail servers, and registration dates.

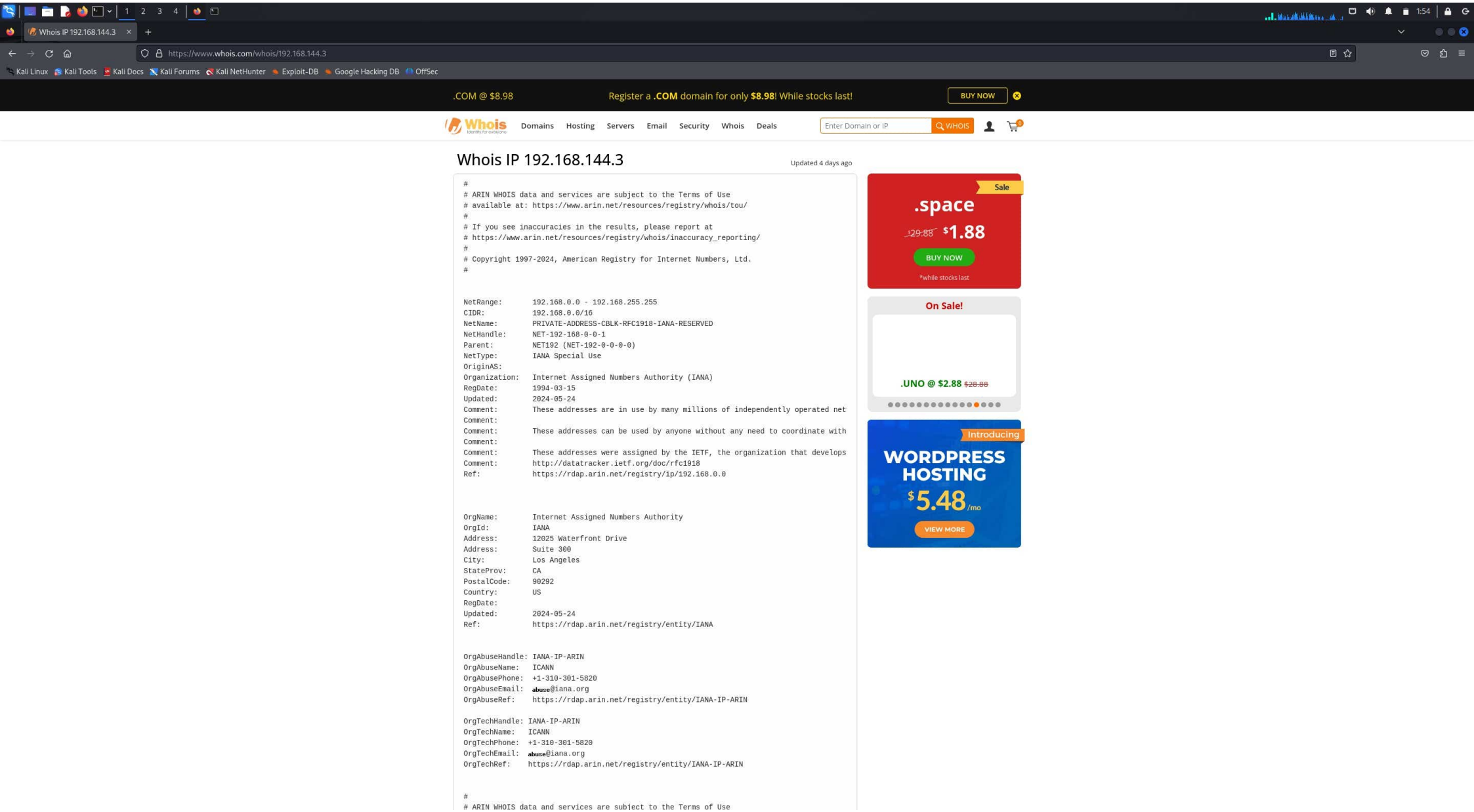
<>The 'whois' database contains records of registered domains.

<>Commands like

->whois <target ip address>

->whois <target domain name>


1 2 3 4
1:30
Terminal Emulator
Use the command line
Trash
File System
Home
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# whois 192.168.144.3
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a sing
er connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for
n a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traf
these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. P
er to http://www.iana.org/abuse/answers
Comment:
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current
document, RFC 1918 which can be found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Updated: 2024-05-24
Ref: https://rdap.arin.net/registry/entity/IANA
OrgTechHandle: IANA-IP-ARIN


Whois IP 192.168.144.3
https://www.whois.com/whois/192.168.144.3
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
.COM @ $8.98
Register a .COM domain for only $8.98! While stocks last!
BUY NOW
Whois
Domains Hosting Servers Email Security Whois Deals
Enter Domain or IP
WHOIS
Whois IP 192.168.144.3
Updated 4 days ago
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated net
Comment:
Comment: These addresses can be used by anyone without any need to coordinate with
Comment:
Comment: These addresses were assigned by the IETF, the organization that develops
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Updated: 2024-05-24
Ref: https://rdap.arin.net/registry/entity/IANA
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
ARIN WHOIS data and services are subject to the Terms of Use
Sale
.space
$29.88 $1.88
BUY NOW
*while stocks last
On Sale!
.UNO @ $2.88 $28.88
Introducing
WORDPRESS HOSTING
$5.48/mo
VIEW MORE

Project Conclusion:

-->In this project, we explored various information gathering tools commonly used in ethical hacking and the penetration testing.

-->Nmap, a powerful network scanner, helps to discover the hosts, open ports, and the various network services.

-->The whois command retrieves the information about the domain owner and the IP address.

-->Finally, it is responsible to use of these tools and it is crucial.

-->Information gathering sets the path for the successful security assessments.