Dor Amihai – John Bryce- class 7736.37 -lecturer's name Erel Regev.

Network Research through a remote while local host in NIPe mode Script (Project) – Summary

This Bash script automates the whole remote-recon workflow on Kali:

1. **Environment setup** – it creates a clean working directory under `~/Desktop/Network_Project`, then checks/installs the must-have tools (`sshpass`, `curl`, `geoip-bin`, `nmap`, `tor`, etc.). `INSTALL_NIPE` function is there to check if the user is TOR-based IP masking with NIPE. If not script stop and exit.

2. **User input** – the script asks user for three things:

* the **target IP** the user wants to probe,

* the **remote server's IP/hostname**,

* and the **SSH credentials** (user + password) for the remote server.

3. Extra: another input from user to decide which port scan he like to do.

3. **Remote connection** – using `sshpass`, it logs into the remote server with no interactive prompts.

4. **Recon phase** – on the remote machine it runs a `whois` lookup and an `nmap` open-port **full** scan against the target IP the user supplies. All output is dropped into a single results folder.

5. **Pull & **cleanup**** – once the scans finish, the script copies the results folder back to the user local workspace, verifies the copy, and then wipes the folder on the remote host (`rm -rf`) so no leftovers stay behind.

The end result: the user get a neat local snapshot of the recon data, the remote server stays clean, and the user didn't have to type the same commands over and over.

The script creates a log who document all important activity.

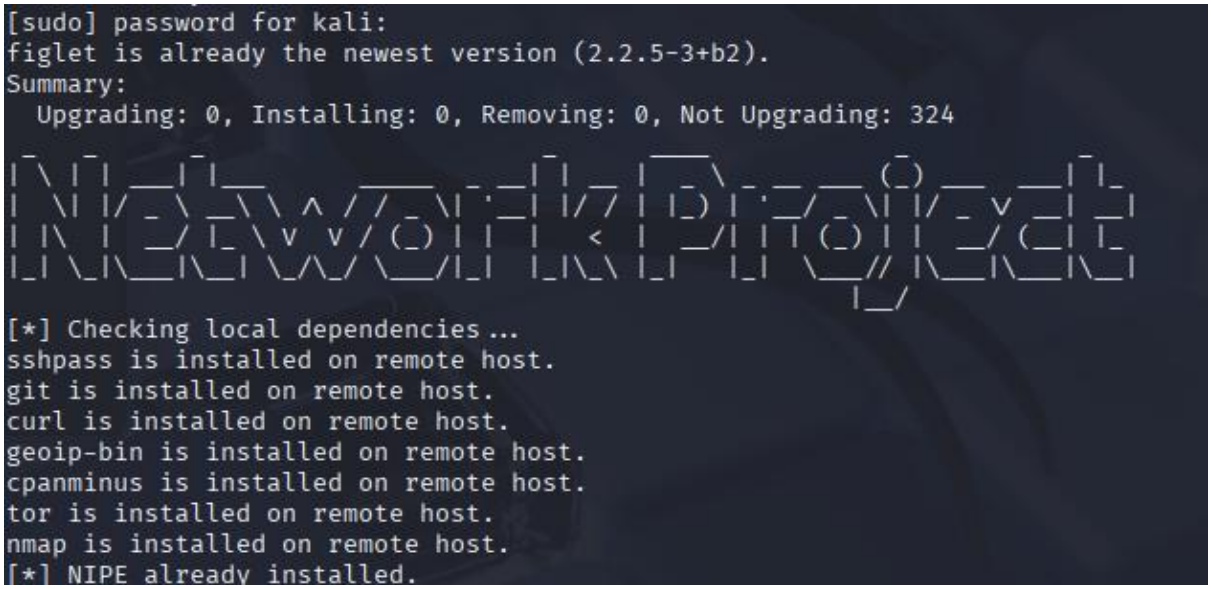
This zip file contains: The script called TMagen773637.s23.nx201.sh and this PDF file.

Features and Capabillitys:

1.Installations and Anonymity Check

1.1 Install the needed applications.

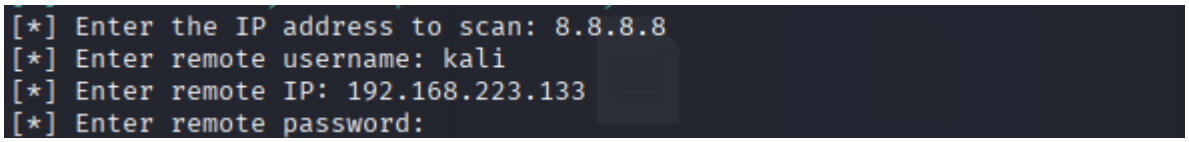
1.2 If the applications are already installed, don't install them again.



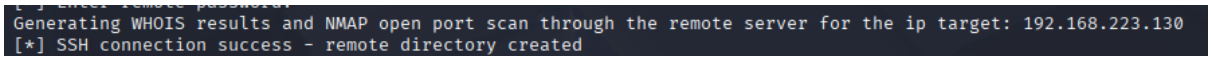
1.3 Check if the network connection is anonymous; if not, alert the user and exit.

1.4 If the network connection is anonymous, display the spoofed country name.

1.5 Allow the user to specify the address to scn via remote server; save into a variable.

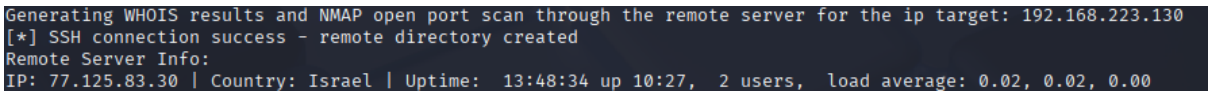


Variable save:

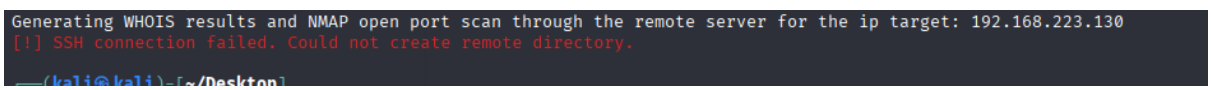


2. Automatically Connect and Execute Commands on the Remote Server via SSH

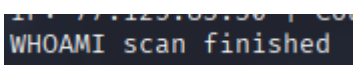
2.1 Display the details of the remote server (country, IP, and Uptime).



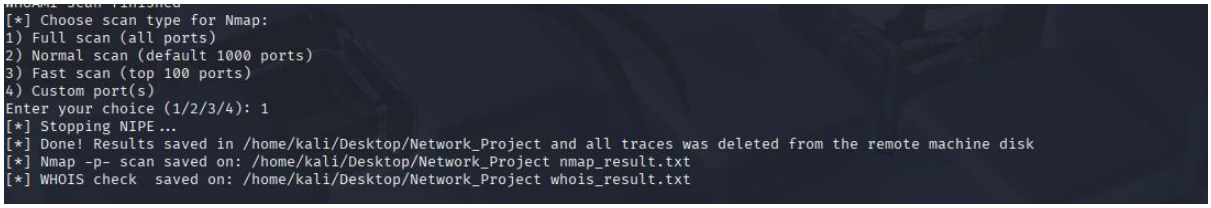
Extra: if connection don't work – tell the user and stop the script.



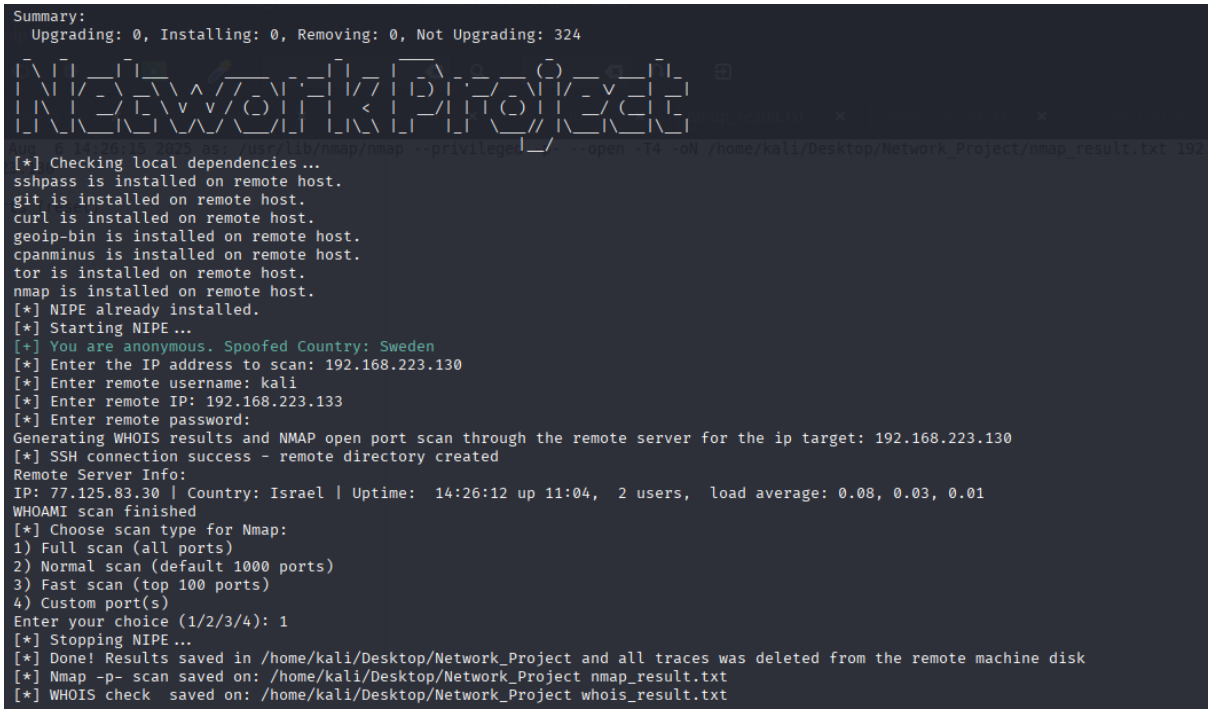
2.2 Get the remote server to check the Whois of the given address.

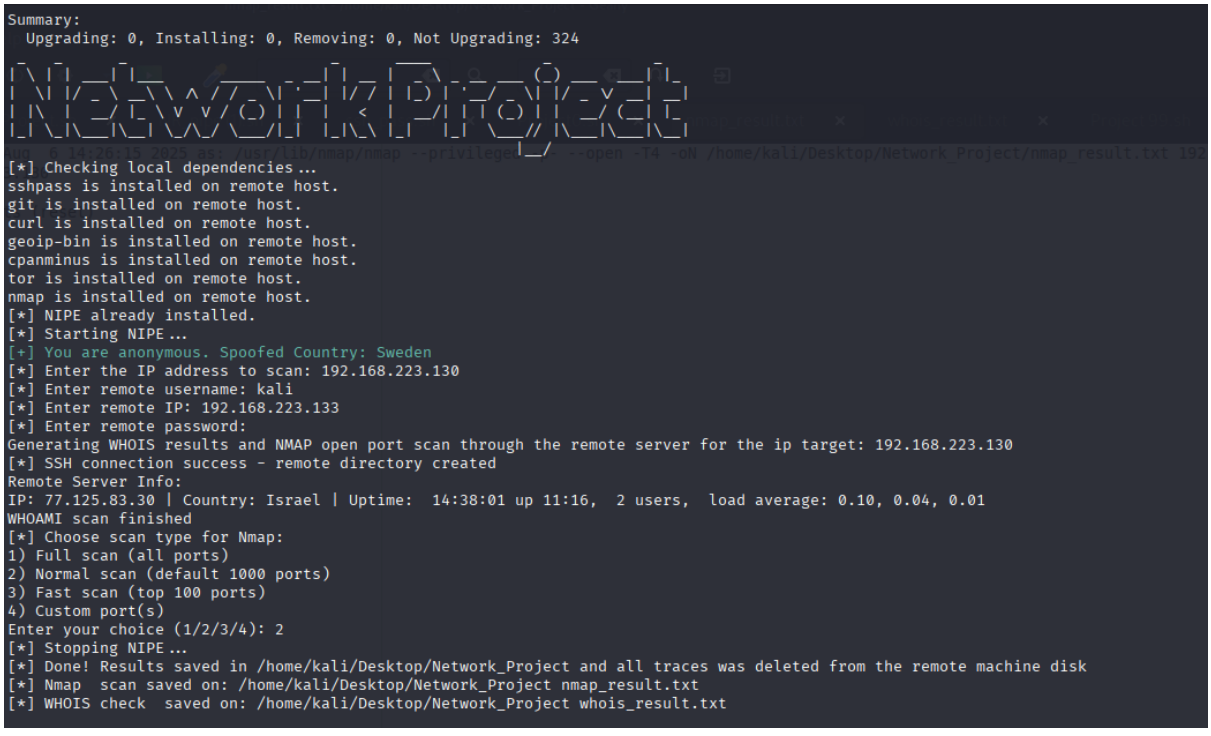


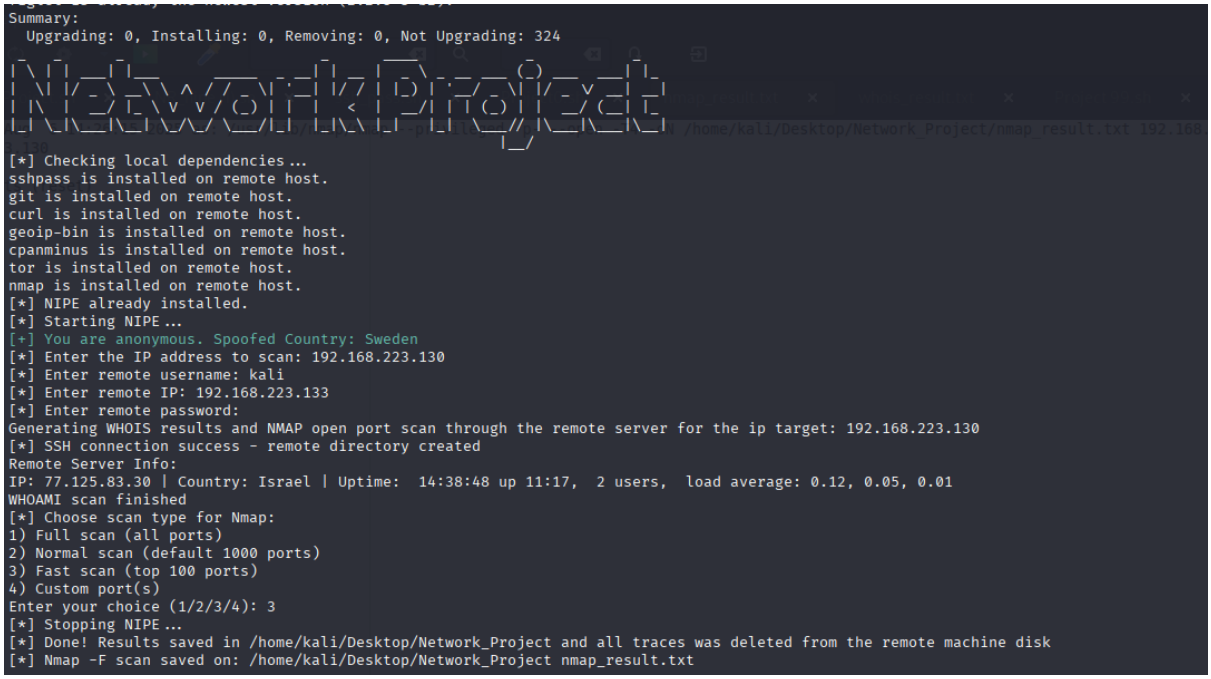
2.3 Get the remote server to scan for open ports on the given address.

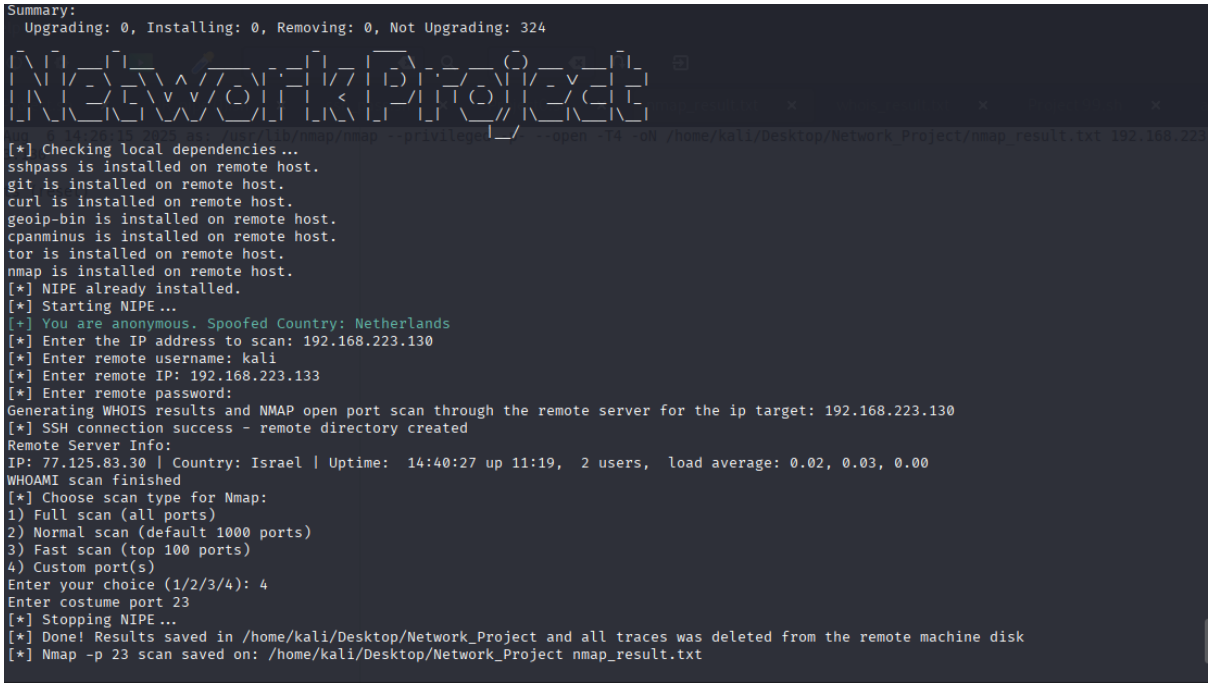


I had an extra to choose between 4 different scan. They all work.

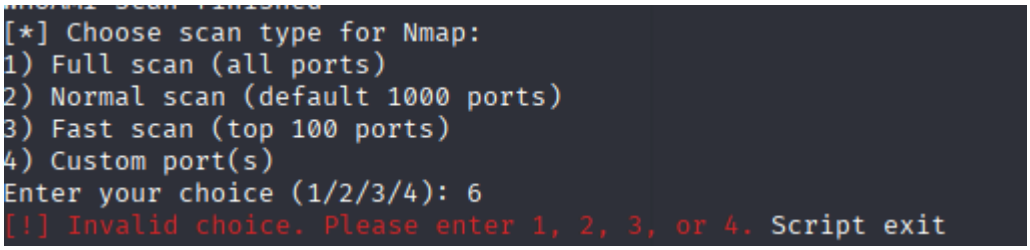








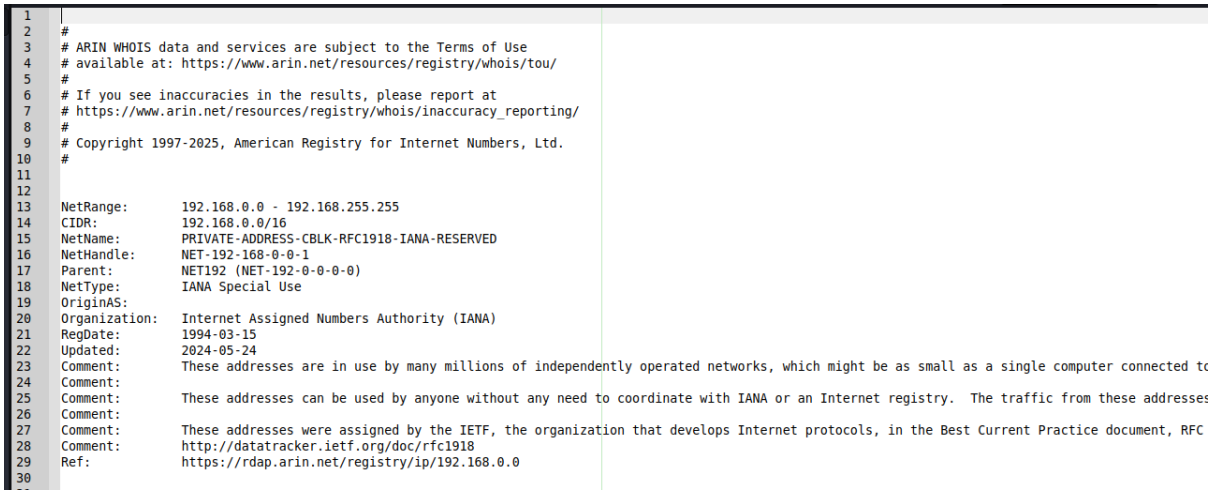
If you choose anything other than 4 options the script tells you and stop.



3. Results

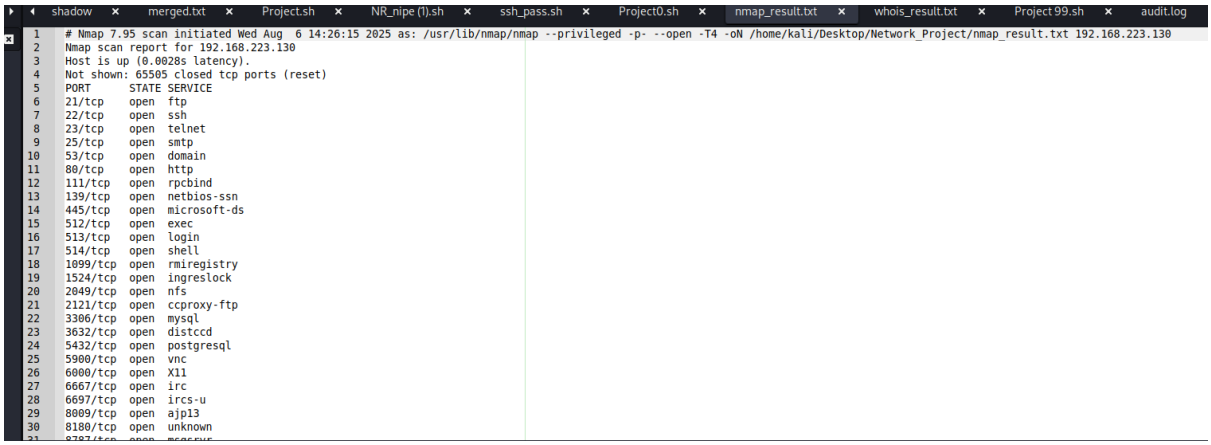
Results being saved on the remote machine. Copied to local machine and remove all traces in the remote machine – by deleting the dir who contains the log files.

3.1 Save the Whois and Nmap data into files on the local computer.



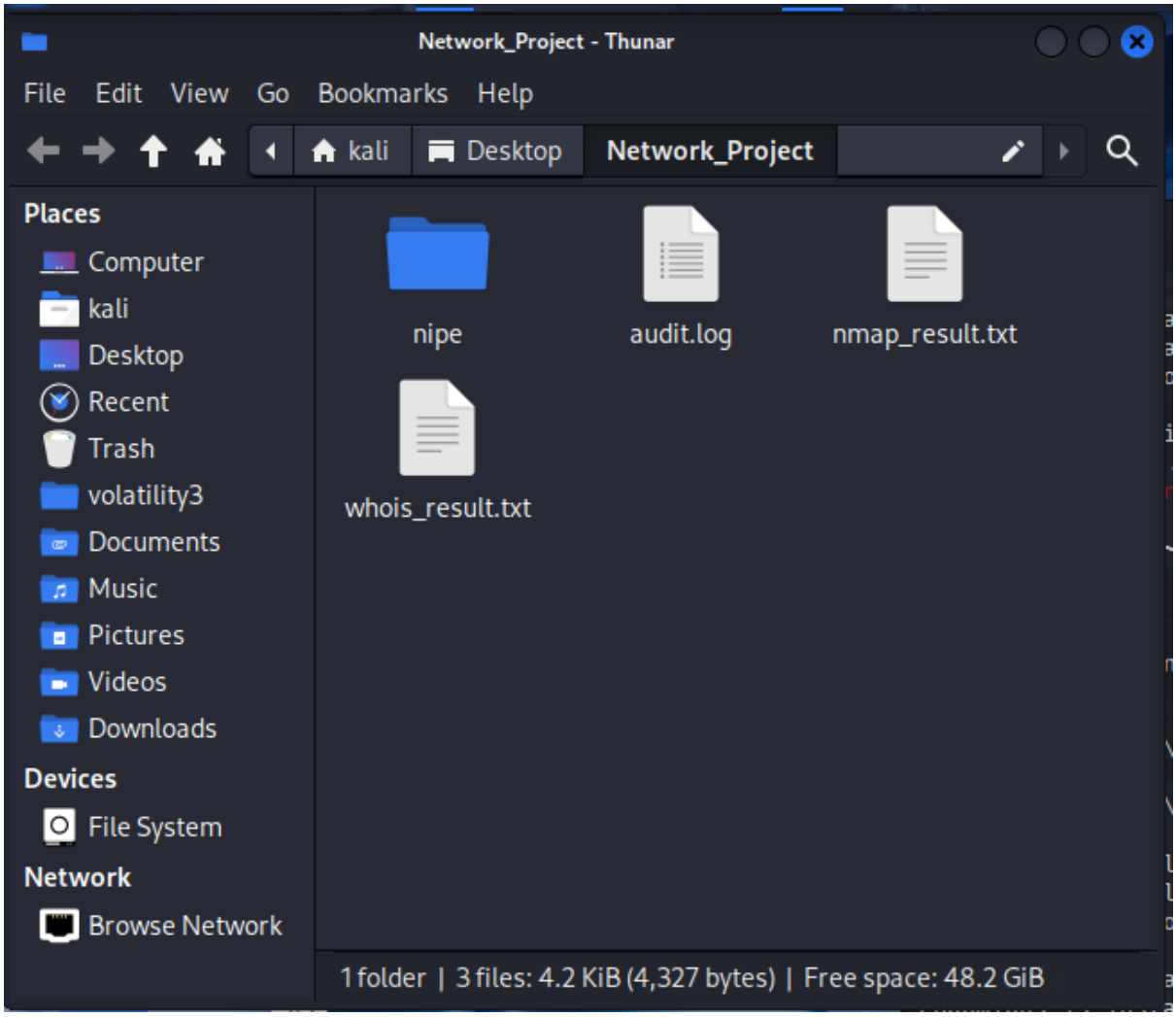
```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American 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 single computer connected to
Comment:
Comment:        These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry.  The traffic from these addresses
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0
```



shadow × merged.txt × Project.sh × NR_nipe (1).sh × ssh_pass.sh × Project0.sh × nmap_result.txt × whois_result.txt × Project 99.sh × audit.log

```
# Nmap 7.95 scan initiated Wed Aug  6 14:26:15 2025 as: /usr/lib/nmap/nmap --privileged -p- --open -T4 -oN /home/kali/Desktop/Network_Project/nmap_result.txt 192.168.223.130
Nmap scan report for 192.168.223.130
Host is up (0.0028s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
```



3.2 Create a log and audit your data collecting.

```
1  [Wed Aug  6 02:25:35 PM EDT 2025] Script started.
2  [Wed Aug  6 02:25:51 PM EDT 2025] Anonymity OK. IP: 158.174.210.51 (Sweden)
3  [Wed Aug  6 02:26:12 PM EDT 2025] WHOAMI scan finished
4  [Wed Aug  6 02:26:20 PM EDT 2025] Nmap scan (-p-) finished on 192.168.223.130
5  [Wed Aug  6 02:26:20 PM EDT 2025] Port scan of -p- Scan completed on target: 192.168.223.130
6  [Wed Aug  6 02:26:20 PM EDT 2025] Script completed.
7
```

Creativity:

Scaning options.

Closing Nipe

Deleting traces.

Ssh connection test.