

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 Capabilities:

1. Installations and Anonymity Check

1.1 Install the needed applications.

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

```
[sudo] password for kali:
figlet is already the newest version (2.2.5-3+b2).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 324
```

Abstract

```
[*] Checking local dependencies ...
sshpas is installed on remote host.
git is installed on remote host.
curl is installed on remote host.
geoiip-bin is installed on remote host.
cpanminus is installed on remote host.
tor is installed on remote host.
nmap is installed on remote host.
[*] NIPE already installed.
```

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.

```
[*] Starting NIPE ...
[+] You are anonymous. Spoofed Country: Poland
```

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

```
[*] Enter the IP address to scan: 8.8.8.8
[*] Enter remote username: kali
[*] Enter remote IP: 192.168.223.133
[*] Enter remote password:
```

Variable save:

```
[*] Generating WHOIS results and NMAP open port scan through the remote server for the ip target: 192.168.223.130
[*] SSH connection success - remote directory created
```

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).

```
Generating WHOIS results and NMAP open port scan through the remote server for the ip target: 192.168.223.130
[*] SSH connection success - remote directory created
Remote Server Info:
IP: 77.125.83.30 | Country: Israel | Uptime: 13:48:34 up 10:27, 2 users, load average: 0.02, 0.02, 0.00
```

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

```
Generating WHOIS results and NMAP open port scan through the remote server for the ip target: 192.168.223.130
[!] SSH connection failed. Could not create remote directory.

(kali@kali) [~ /Desktop]
```

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

WHOAMI scan finished

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

```

WHOAMI scan finished
[*] Choose scan type for Nmap:
1) Full scan (all ports)
2) Normal scan (default 1000 ports)
3) Fast scan (top 100 ports)
4) Custom port(s)
Enter your choice (1/2/3/4): 1
[*] Stopping NIPE...
[*] Done! Results saved in /home/kali/Desktop/Network_Project and all traces was deleted from the remote machine disk
[*] Nmap -p- scan saved on: /home/kali/Desktop/Network_Project nmap_result.txt
[*] WHOIS check saved on: /home/kali/Desktop/Network_Project whois_result.txt

```

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

```

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 324

[+] You are anonymous. Spoofed Country: Sweden
[*] Enter the IP address to scan: 192.168.223.130
[*] Enter remote username: kali
[*] Enter remote IP: 192.168.223.133
[*] Enter remote password:
Generating WHOIS results and NMAP open port scan through the remote server for the ip target: 192.168.223.130
[*] SSH connection success - remote directory created
Remote Server Info:
IP: 77.125.83.30 | Country: Israel | Uptime: 14:26:12 up 11:04, 2 users, load average: 0.08, 0.03, 0.01
WHOAMI scan finished
[*] Choose scan type for Nmap:
1) Full scan (all ports)
2) Normal scan (default 1000 ports)
3) Fast scan (top 100 ports)
4) Custom port(s)
Enter your choice (1/2/3/4): 1
[*] Stopping NIPE...
[*] Done! Results saved in /home/kali/Desktop/Network_Project and all traces was deleted from the remote machine disk
[*] Nmap -p- scan saved on: /home/kali/Desktop/Network_Project nmap_result.txt
[*] WHOIS check saved on: /home/kali/Desktop/Network_Project whois_result.txt

```

```

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 324

[+] You are anonymous. Spoofed Country: Sweden
[*] Enter the IP address to scan: 192.168.223.130
[*] Enter remote username: kali
[*] Enter remote IP: 192.168.223.133
[*] Enter remote password:
Generating WHOIS results and NMAP open port scan through the remote server for the ip target: 192.168.223.130
[*] SSH connection success - remote directory created
Remote Server Info:
IP: 77.125.83.30 | Country: Israel | Uptime: 14:38:01 up 11:16, 2 users, load average: 0.10, 0.04, 0.01
WHOAMI scan finished
[*] Choose scan type for Nmap:
1) Full scan (all ports)
2) Normal scan (default 1000 ports)
3) Fast scan (top 100 ports)
4) Custom port(s)
Enter your choice (1/2/3/4): 2
[*] Stopping NIPE...
[*] Done! Results saved in /home/kali/Desktop/Network_Project and all traces was deleted from the remote machine disk
[*] Nmap scan saved on: /home/kali/Desktop/Network_Project nmap_result.txt
[*] WHOIS check saved on: /home/kali/Desktop/Network_Project whois_result.txt

```

```

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 324

[*] Checking local dependencies...
sshpas is installed on remote host.
git is installed on remote host.
curl is installed on remote host.
geoi-bin is installed on remote host.
cpanminus is installed on remote host.
tor is installed on remote host.
nmap is installed on remote host.
[*] NIPE already installed.
[*] Starting NIPE ...
[+] You are anonymous. Spoofed Country: Sweden
[*] Enter the IP address to scan: 192.168.223.130
[*] Enter remote username: kali
[*] Enter remote IP: 192.168.223.133
[*] Enter remote password:
Generating WHOIS results and NMAP open port scan through the remote server for the ip target: 192.168.223.130
[*] SSH connection success - remote directory created
Remote Server Info:
IP: 77.125.83.30 | Country: Israel | Uptime: 14:38:48 up 11:17, 2 users, load average: 0.12, 0.05, 0.01
WHOAMI scan finished
[*] Choose scan type for Nmap:
1) Full scan (all ports)
2) Normal scan (default 1000 ports)
3) Fast scan (top 100 ports)
4) Custom port(s)
Enter your choice (1/2/3/4): 3
[*] Stopping NIPE ...
[*] Done! Results saved in /home/kali/Desktop/Network_Project and all traces was deleted from the remote machine disk
[*] Nmap -F scan saved on: /home/kali/Desktop/Network_Project nmap_result.txt

```

```

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 324

[*] Checking local dependencies...
sshpas is installed on remote host.
git is installed on remote host.
curl is installed on remote host.
geoi-bin is installed on remote host.
cpanminus is installed on remote host.
tor is installed on remote host.
nmap is installed on remote host.
[*] NIPE already installed.
[*] Starting NIPE ...
[+] You are anonymous. Spoofed Country: Netherlands
[*] Enter the IP address to scan: 192.168.223.130
[*] Enter remote username: kali
[*] Enter remote IP: 192.168.223.133
[*] Enter remote password:
Generating WHOIS results and NMAP open port scan through the remote server for the ip target: 192.168.223.130
[*] SSH connection success - remote directory created
Remote Server Info:
IP: 77.125.83.30 | Country: Israel | Uptime: 14:40:27 up 11:19, 2 users, load average: 0.02, 0.03, 0.00
WHOAMI scan finished
[*] Choose scan type for Nmap:
1) Full scan (all ports)
2) Normal scan (default 1000 ports)
3) Fast scan (top 100 ports)
4) Custom port(s)
Enter your choice (1/2/3/4): 4
Enter costume port 23
[*] Stopping NIPE ...
[*] Done! Results saved in /home/kali/Desktop/Network_Project and all traces was deleted from the remote machine disk
[*] Nmap -p 23 scan saved on: /home/kali/Desktop/Network_Project nmap_result.txt

```

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

```

[*] Choose scan type for Nmap:
1) Full scan (all ports)
2) Normal scan (default 1000 ports)
3) Fast scan (top 100 ports)
4) Custom port(s)
Enter your choice (1/2/3/4): 6
[!] Invalid choice. Please enter 1, 2, 3, or 4. Script exit

```

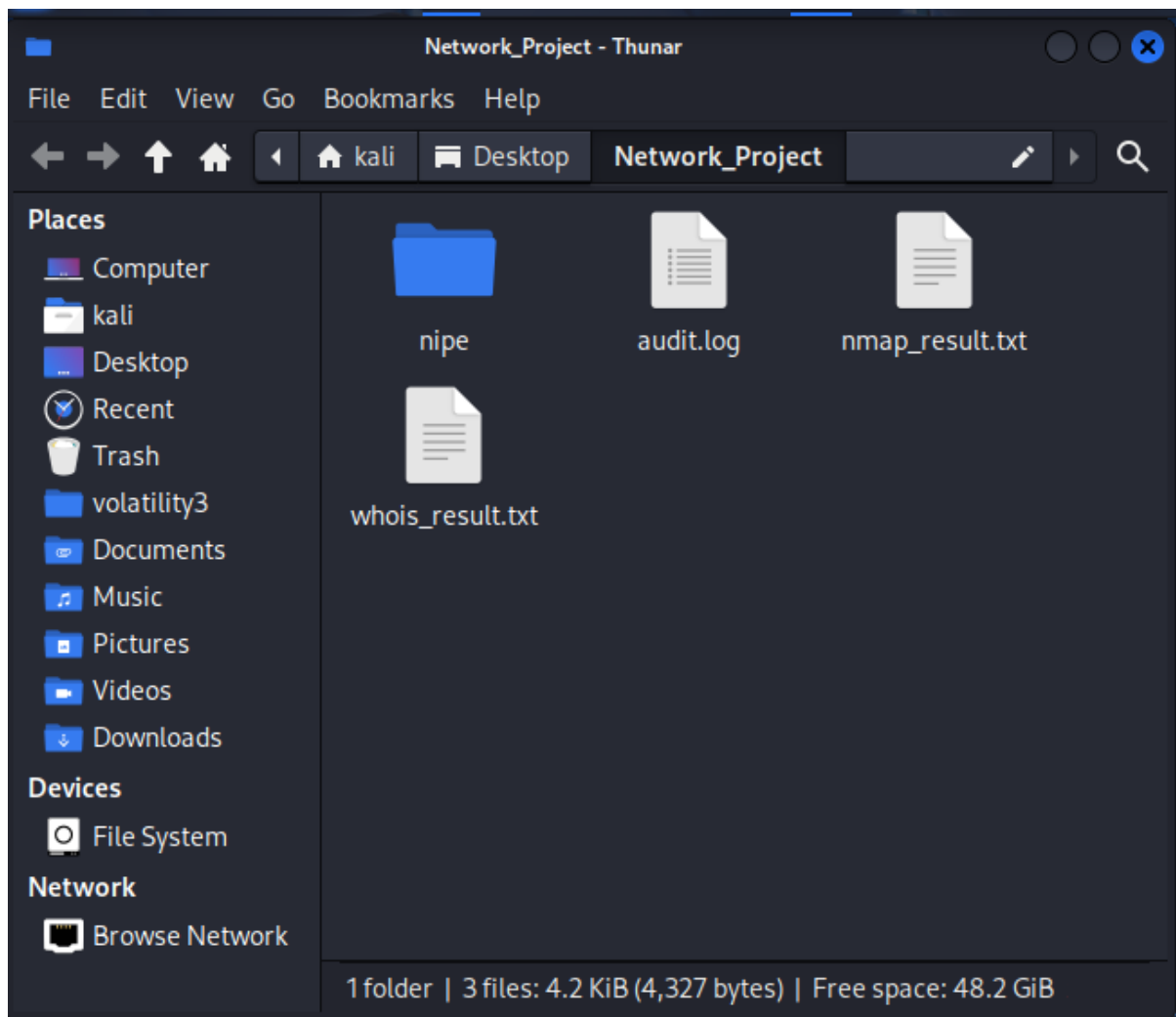
3. Results

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.

```
1 #
2 #
3 # ARIN WHOIS data and services are subject to the Terms of Use
4 # available at: https://www.arin.net/resources/registry/whois/tou/
5 #
6 # If you see inaccuracies in the results, please report at
7 # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
8 #
9 # Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
10 #
11
12
13 NetRange: 192.168.0.0 - 192.168.255.255
14 CIDR: 192.168.0.0/16
15 NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
16 NetHandle: NET-192-168-0-0-1
17 Parent: NET192 (NET-192-0-0-0-0)
18 NetType: IANA Special Use
19 OriginAS:
20 Organization: Internet Assigned Numbers Authority (IANA)
21 RegDate: 1994-03-15
22 Updated: 2024-05-24
23 Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to
24 Comment:
25 Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses
26 Comment:
27 Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC
28 Comment: http://datatracker.ietf.org/doc/rfc1918
29 Ref: https://rdap.arin.net/registry/ip/192.168.0.0
30
```

```
shadow x merged.txt x Project.sh x NR_nipe(l).sh x ssh_pass.sh x Project0.sh x nmap_result.txt x whois_result.txt x Project99.sh x audit.log
1 # 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
2 Nmap scan report for 192.168.223.130
3 Host is up (0.0028s latency).
4 Not shown: 65505 closed tcp ports (reset)
5 PORT      STATE SERVICE
6 21/tcp    open  ftp
7 22/tcp    open  ssh
8 23/tcp    open  telnet
9 25/tcp    open  smtp
10 53/tcp    open  domain
11 80/tcp    open  http
12 111/tcp   open  rpcbind
13 139/tcp   open  netbios-ssn
14 445/tcp   open  microsoft-ds
15 512/tcp   open  exec
16 513/tcp   open  login
17 514/tcp   open  shell
18 1099/tcp  open  rmiregistry
19 1524/tcp  open  ingreslock
20 2049/tcp  open  nfs
21 2121/tcp  open  ccproxy-ftp
22 3306/tcp  open  mysql
23 3632/tcp  open  distccd
24 5432/tcp  open  postgresql
25 5900/tcp  open  vnc
26 6000/tcp  open  X11
27 6667/tcp  open  irc
28 6697/tcp  open  ircs-u
29 8009/tcp  open  ajp13
30 8180/tcp  open  unknown
31 8767/tcp  open  #66666666
```



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:

Scanning options.

Closing Nipe

Deleting traces.

Ssh connection test.