

## Project requirements:

### 1. Installations and Anonymity Check

#### 1.1 Install the needed applications.

```
[Checking local dependencies]
[✓] curl is already installed
[✓] jq is already installed
[✓] git is already installed
[✓] sshpass is already installed
[✓] nmap is already installed
[✓] tar is already installed
[x] whois not found - installing...
[✓] whois installed successfully
[TOR] Checking Tor service...
[✓] Tor is already running.
```

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

```
[Checking local dependencies]
[✓] curl is already installed
[✓] jq is already installed
[✓] git is already installed
[✓] sshpass is already installed
[✓] nmap is already installed
[✓] tar is already installed
[✓] whois is already installed
[TOR] Checking Tor service ...
[✓] Tor is already running.
```

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

```
# Check anonymity
if [[ "$COUNTRY" != "IL" ]]; then
    echo -e "${GREEN}[NIPE] Anonymity verified.${RESET}"
    echo -e "${GREEN}Exit IP: $EXIT_IP ($COUNTRY)${RESET}"
    return 0
fi

echo -e "${RED}[NIPE] Still IL exit ($EXIT_IP). Retrying...${RESET}"
((ATTEMPT++))
sleep 3
done
```

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

```
[NIPE] Restarting anonymization (Attempt 1/5) ...
[NIPE] Anonymity verified.
Exit IP: 204.137.14.106 (NL)
```

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

```

1) Scan a single remote IP
2) Scan the remote network
0) Exit
Choose: 1
Target IP: 192.168.72.165

```

```
read -rp "Target IP: " TARGET
```

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

### SSH connection

```

[SSH SETUP]
Attempt 1 of 3
Remote SSH username: kali
Remote IP/hostname: 192.168.72.163
Remote port [22]:
Password (for SSH login):
[*] Testing SSH connection to kali@192.168.72.163:22 ...
[✓] SSH connection successful!

```

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

```

[REMOTE] Gathering remote system information ...

===== REMOTE SERVER INFO =====
Public IP: 176.230.76.92
Country: The Netherlands
Uptime: up 2 hours, 10 minutes
=====

```

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

```

#####
# 4.5 WHOIS lookup (remote server)
#####
sshpass -p "$SSH_PASS" ssh -o StrictHostKeyChecking=no -p "$REMOTE_PORT" \
"$REMOTE_USER@$REMOTE_HOST" \
"echo \"$SSH_PASS\" | sudo -S whois $TARGET > $REMOTE_DIR/whois_$TARGET.txt 2>/dev/null"

```

Target whois saved to file to clean terminal

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

```

#####
Target IP: 192.168.72.165
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 06:26 EST
Nmap scan report for 192.168.72.165
Host is up (0.00076s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:8F:E4:D2 (VMware)

```

```

#####
# 2. FAST PORT DISCOVERY SCAN
# (-p- only, NO service detection, save as fast.gnmap)
#####
sshpass -p "$SSH_PASS" ssh -o StrictHostKeyChecking=no -p "$REMOTE_PORT" \
"$REMOTE_USER@$REMOTE_HOST" \
"echo \"$SSH_PASS\" | sudo -S nmap -Pn -p- -T3 \
--max-retries 1 --min-rate 300 --host-timeout 45s \
-oG $REMOTE_DIR/fast_$TARGET.gnmap $TARGET 2>/dev/null"

```

First run fast open port scan then re-run deep scan for vuln on the found open ports > save to file

### 3. Results

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

All files created by script are taken back to main machine then runs cleanup after.

```
#####
# 6. Download entire scan folder silently
#####
sshpass -p "$SSH_PASS" scp -r -o StrictHostKeyChecking=no -P "$REMOTE_PORT" \
"$REMOTE_USER@$REMOTE_HOST:$REMOTE_DIR" "$LOCAL_DIR/" >/dev/null 2>&1

#####
# 7. Cleanup remote
#####
sshpass -p "$SSH_PASS" ssh -o StrictHostKeyChecking=no -p "$REMOTE_PORT" \
"$REMOTE_USER@$REMOTE_HOST" \
"echo \"$SSH_PASS\" | sudo -S rm -rf $REMOTE_DIR 2>/dev/null"

log "Single IP scan saved in: $LOCAL_DIR"
```

3.2 Create a log and audit your data collecting.

```
[REPORT] Building S10 Security Report...
[REPORT] S10 Report Created:
- /home/kali/Desktop/nipe_tool/Sessions/scan_22.11.2025_06-19/report.md
- /home/kali/Desktop/nipe_tool/Sessions/scan_22.11.2025_06-19/report.txt
```

### 4. Creativity

4.1 cleanup - if script fails or exits before completion clean files created.

4.2 REMOTE\_SCAN\_NETWORK – optional auto detect range and run nmap on the found ip in range.