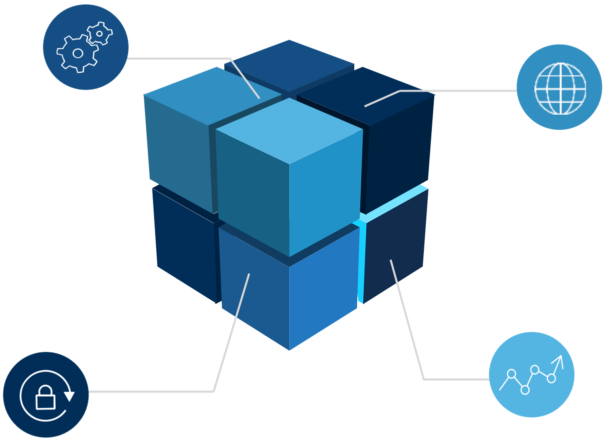
CYBERIUM ARENA
SIMULATOR

PROJECT: REMOTE CONTROL | NETWORK RESEARCH

OPERATION ORDER

During attacks on the enemy's server, we waste valuable time typing wrong commands due to stress and are even exposed because the source addresses are exposed.



1. VISION

Cyber units operating in an automated way.

2. MISSION

Communicating with a remote server and executing automatic tasks anonymously.

3. STRATEGY

Creating automation that would let cyber units execute commands on their local devices but would be executed by the remote server.

4. OBJECTIVES

- Connecting to the remote server should be automated.
- Automations on the remote server should include:
  I. Scanning targets

  II. Getting information (Whois)

Score Structure

1. Installations and Anonymity Check (50 Points)

    1.1 Install the needed applications – (5 Points)
    1.2 If the applications are already installed, don't install them again – (15 Points)
    1.3 Check if the network connection is anonymous; if not, alert the user and exit – (10 Points)
    1.4 If the network connection is anonymous, display the spoofed country name – (15 Points)
    1.5 Allow the user to specify the address to scan via remote server; save into a variable – (5 Points)

2. Automatically Connect and Execute Commands on the Remote Server via SSH (30 Points)

    2.1 Display the details of the remote server (country, IP, and Uptime) – (10 Points)
    2.2 Get the remote server to check the Whois of the given address – (10 Points)
    2.3 Get the remote server to scan for open ports on the given address – (10 Points)

3. Results (15 Points)

    3.1 Save the Whois and Nmap data into files on the local computer – (10 Points)
    3.2 Create a log and audit your data collecting – (5 Points)

4. Creativity (5 Points)

General

- Suggested tools: Sshpass, Nipe, Torify, Nmap, Whois.
- Everything other than the user input should be automated.
- Usage of functions adds 5 points.

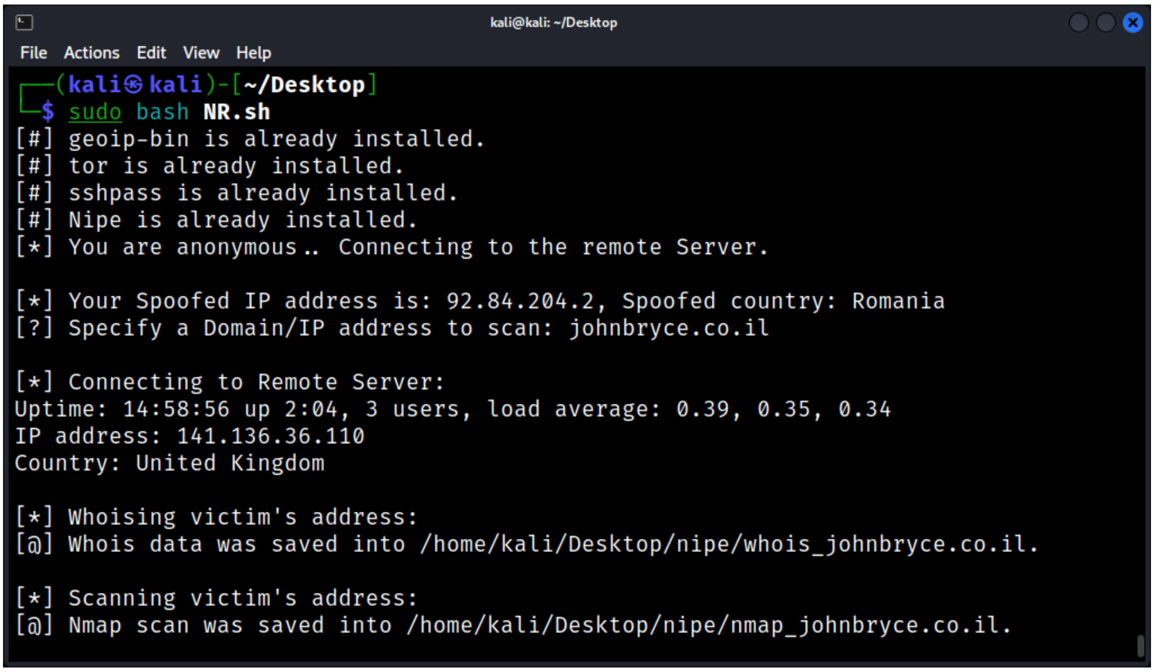
Comments

Use comments in your code to explain what you did.
If you are using code from the internet, add credit and links.
In the script, write the student's name and code, the class code, and the lecturer's name.

Submitting

Submit the source code (.sh) and a pdf file with screenshots proving the functions work.
Send the project to the trainer's email.
In the email subject type **project: Remote Control <student name>**.

Project Output



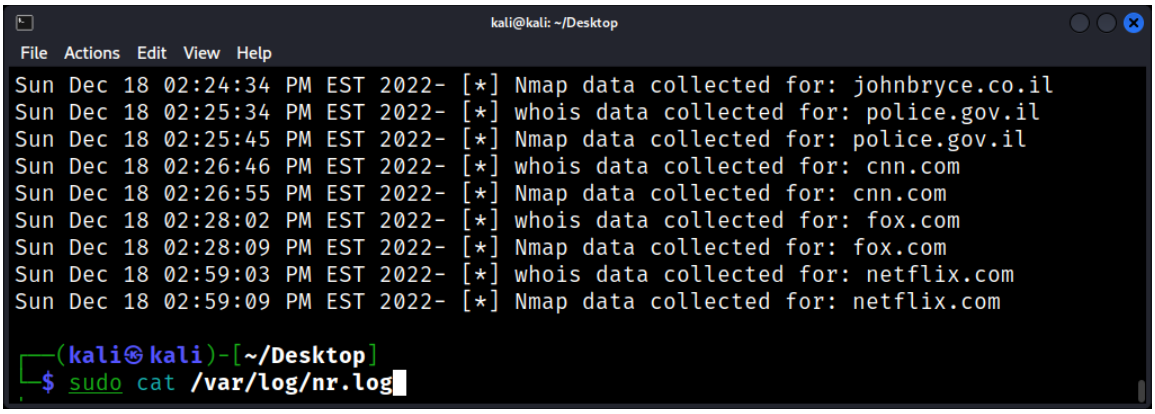
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo bash NR.sh
[#] geoip-bin is already installed.
[#] tor is already installed.
[#] sshpass is already installed.
[#] Nipe is already installed.
[*] You are anonymous.. Connecting to the remote Server.

[*] Your Spoofed IP address is: 92.84.204.2, Spoofed country: Romania
[?] Specify a Domain/IP address to scan: johnbryce.co.il

[*] Connecting to Remote Server:
Uptime: 14:58:56 up 2:04, 3 users, load average: 0.39, 0.35, 0.34
IP address: 141.136.36.110
Country: United Kingdom

[*] Whoising victim's address:
[@] Whois data was saved into /home/kali/Desktop/nipe/whois_johnbryce.co.il.

[*] Scanning victim's address:
[@] Nmap scan was saved into /home/kali/Desktop/nipe/nmap_johnbryce.co.il.
```



```
Sun Dec 18 02:24:34 PM EST 2022- [*] Nmap data collected for: johnbryce.co.il
Sun Dec 18 02:25:34 PM EST 2022- [*] whois data collected for: police.gov.il
Sun Dec 18 02:25:45 PM EST 2022- [*] Nmap data collected for: police.gov.il
Sun Dec 18 02:26:46 PM EST 2022- [*] whois data collected for: cnn.com
Sun Dec 18 02:26:55 PM EST 2022- [*] Nmap data collected for: cnn.com
Sun Dec 18 02:28:02 PM EST 2022- [*] whois data collected for: fox.com
Sun Dec 18 02:28:09 PM EST 2022- [*] Nmap data collected for: fox.com
Sun Dec 18 02:59:03 PM EST 2022- [*] whois data collected for: netflix.com
Sun Dec 18 02:59:09 PM EST 2022- [*] Nmap data collected for: netflix.com

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo cat /var/log/nr.log
```