

CYBERIUM PROJECT

Name: MUGISHA Pascal

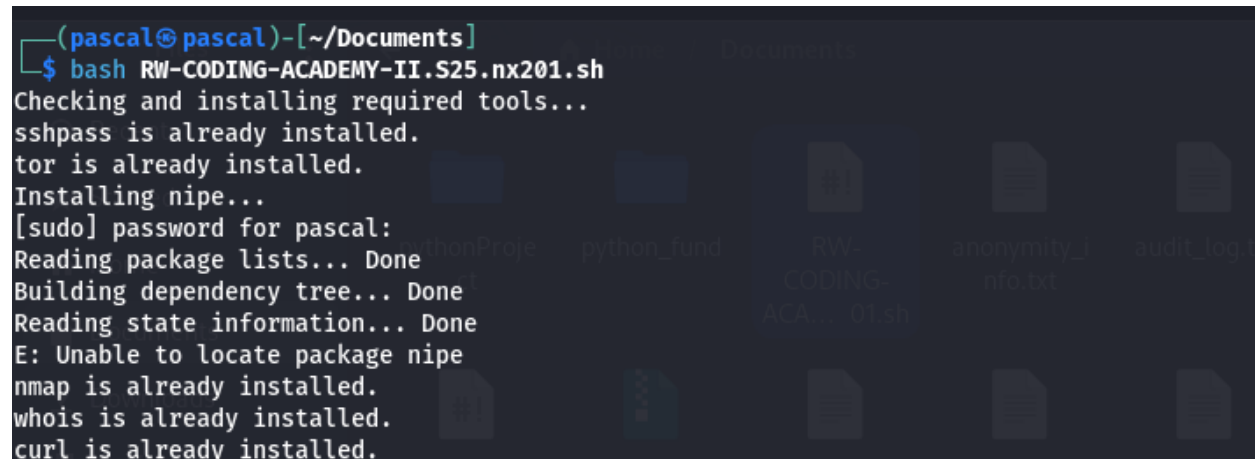
Student: S25

Unit: RW-CODING-ACADEMY-II

Remote Control

1.Installing applications

Here Once App is installed can't be re-Installed it jumps to the next part.
Look the logs after checking if they are installed



```
(pascal@pascal)-[~/Documents]
$ bash RW-CODING-ACADEMY-II.S25.nx201.sh
Checking and installing required tools...
sshpas is already installed.
tor is already installed.
Installing nipe...
[sudo] password for pascal:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package nipe
nmap is already installed.
whois is already installed.
curl is already installed.
```

2. we prompt you to enter you the address to spoof

```
Enter the IP address to check its anonymity: 10.12.74.235
Checking network anonymity for IP: 10.12.74.235...
The network is anonymous. Current IP: 154.68.72.188 (Spoofed country: RW)
Enter the address to scan: 10.12.74.235
Enter remote server IP: 10.12.74.235
Enter SSH username: rubuto-yvan
Enter SSH password:
Connecting to remote server at 10.12.74.235...
```

3. Printing the logs for the data being fetched from whois and iplookup

```
Pseudo-terminal will not be allocated because stdin is not a terminal.
Warning: Permanently added '10.12.74.235' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

18 updates can be applied immediately.
10 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

10 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Remote Server Details:
Country: RW
IP: 10.0.2.15
Uptime: 11:07:13 up 57 min, 1 user, load average: 0.16, 0.10, 0.15
```

4. After all data is saved to the local computer

```
Performing Whois lookup for 10.12.74.235...
Whois results saved to whois_10.12.74.235.txt
Scanning for open ports on 10.12.74.235...
Nmap results saved to nmap_10.12.74.235.txt
Saving results from remote server to local computer...
Creating audit log...
All tasks completed. Results saved locally.
```

5. Here is the screenshot for the logs in the whois_result.txt

```
#
# 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:      10.0.0.0 - 10.255.255.255
CIDR:          10.0.0.0/8
NetName:       PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:     NET-10-0-0-1
Parent:        ()
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:
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 a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within 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 traffic from 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. Please refer 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 Practice document,
                RFC 1918 which can be found at:
                http://datatracker.ietf.org/doc/rfc1918
Comment:
Ref:           https://rdap.arin.net/registry/ip/10.0.0.0

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
# 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/
```

6. Here is the screenshot for the logs in the nmap_result.txt

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 11:07 CAT
Nmap scan report for rubuto-yvan (10.12.74.235)
Host is up (0.00013s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Summary : overall operation

(pascal@pascal)-[~/Documents]

\$ bash RW-CODING-ACADEMY-II.S25.nx201.sh

Checking and installing required tools...

sshpas is already installed.

tor is already installed.

Installing nipe...

[sudo] password for pascal:

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

E: Unable to locate package nipe

nmap is already installed.

whois is already installed.

curl is already installed.

Enter the IP address to check its anonymity: 10.12.74.235

Checking network anonymity for IP: 10.12.74.235...

The network is anonymous. Current IP: 154.68.72.188 (Spoofed country: RW)

Enter the address to scan: 10.12.74.235

Enter remote server IP: 10.12.74.235

Enter SSH username: rubuto-yvan

Enter SSH password:

Connecting to remote server at 10.12.74.235...

Pseudo-terminal will not be allocated because stdin is not a terminal.

Warning: Permanently added '10.12.74.235' (ED25519) to the list of known hosts.

Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

Other Locations

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/pro>

Expanded Security Maintenance for Applications is not enabled.

18 updates can be applied immediately.

10 of these updates are standard security updates.

To see these additional updates run: apt list --upgradable

10 additional security updates can be applied with ESM Apps.

Learn more about enabling ESM Apps service at <https://ubuntu.com/esm>

Remote Server Details: to '154.68.72.0 - 154.68.73.255'

Country: RW

IP: 10.0.2.15

Uptime: 11:07:13 up 57 min, 1 user, load average: 0.16, 0.10, 0.15

Performing Whois lookup for 10.12.74.235...

Whois results saved to whois_10.12.74.235.txt

Scanning for open ports on 10.12.74.235...

Nmap results saved to nmap_10.12.74.235.txt

Saving results from remote server to local computer...

Creating audit log...

All tasks completed. Results saved locally.