

Network Research Project

Command and Control

Unit: TMagen773631

Student code: s17

Student Name: Stanislav Kolbeshkin

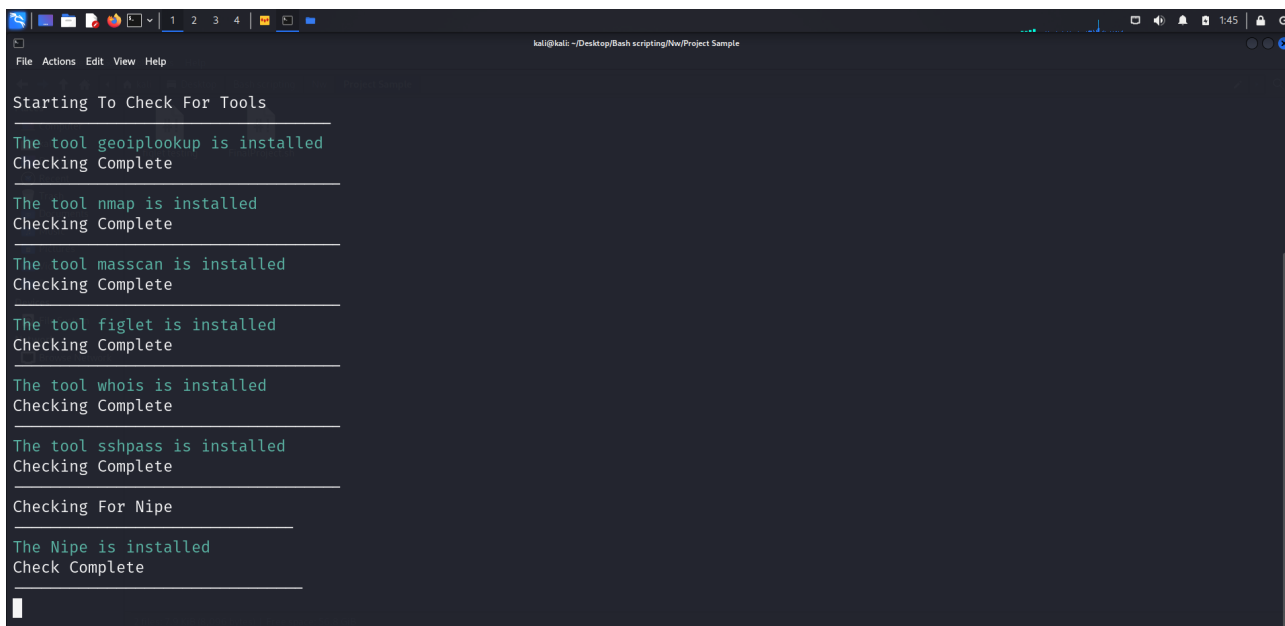
About the project:

As a student of cyber security I was tasked to build a script in kali Linux to take control of another machine using Ssh server and execute scans with different tools at different domains all while being anonymous.

In the beginning we were introduced to the tools that will help us guide us in the process of building the script, bash language and its usage, nipe.pl the tool that mask you through Tor web browser and acting like VPN and of course the sshpass tool which gives us remote control of ssh server which is running and his credentials are known.

The process itself was challenging but not impossible I took it to myself to build something that will guarantee the success of the task at hand. That's why I separated the project into 3 parts:

1st. Checking my machine on the tools I need for the mission and their correct work



A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~/Desktop/Bash scripting/No/Project Sample'. The terminal shows a script titled 'Starting To Check For Tools' that checks for the installation of several tools: geoipllookup, nmap, masscan, figlet, whois, and sshpass. Each tool is confirmed as installed. The script then checks for 'NiPe' and confirms it is also installed. The terminal output is as follows:

```
Starting To Check For Tools

The tool geoipllookup is installed
Checking Complete

The tool nmap is installed
Checking Complete

The tool masscan is installed
Checking Complete

The tool figlet is installed
Checking Complete

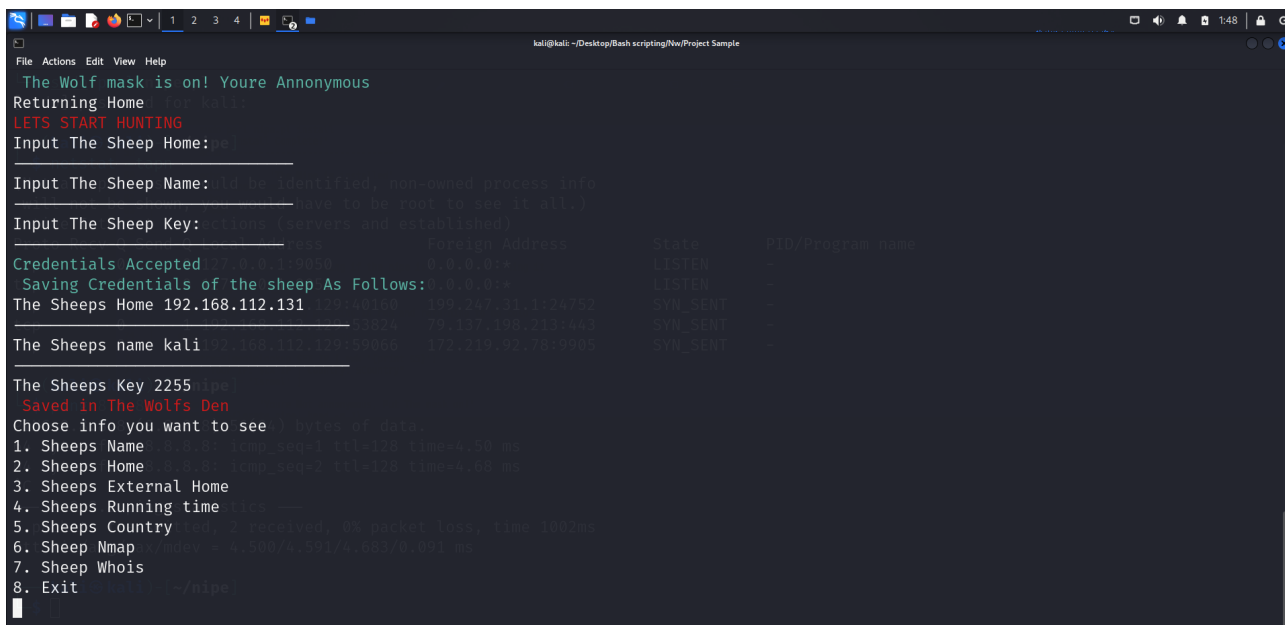
The tool whois is installed
Checking Complete

The tool sshpass is installed
Checking Complete

Checking For NiPe

The NiPe is installed
Check Complete
```

2nd. Checking my target credentials are correct and working



A screenshot of a Kali Linux terminal window showing a simulation. The window title is 'kali@kali: ~/Desktop/Bash scripting/No/Project Sample'. The simulation starts with a 'Wolf' character and a 'Sheep' character. The Wolf is on, and the Sheep is returning home. The Wolf starts hunting. The Sheep provides its home address (192.168.112.131) and key (2255). The Wolf accepts the credentials and saves them. The Wolf then chooses information to see from the Sheep, including its name, home, external home, running time, country, Nmap scan, whois, and exit. The terminal output is as follows:

```
The Wolf mask is on! You're Anonymous
Returning Home
LETS START HUNTING
Input The Sheep Home:192.168.112.131
Input The Sheep Name:192.168.112.131
Input The Sheep Key:2255
Credentials Accepted
Saving Credentials of the sheep As Follows:
The Sheeps Home 192.168.112.131
The Sheeps name kali
The Sheeps Key 2255
Saved in The Wolfs Den
Choose info you want to see
1. Sheeps Name
2. Sheeps Home
3. Sheeps External Home
4. Sheeps Running time
5. Sheeps Country
6. Sheep Nmap
7. Sheep Whois
8. Exit
```

3rd. Checking the victims machine have all the tools to successfully pass the scans of desired domains.

```
File Actions Edit View Help
3. Sheeps External Home
4. Sheeps Running time
5. Sheeps Country
6. Sheep Nmap --nmap
7. Sheep Whois
8. Exit
6. (If not be shown, you would have to be root to see it all.)

Checking For Nmap on Remote host
Foreign Address      State      PID/Program name
0.0.0.0*             LISTEN     -
0.0.0.0*             LISTEN     -
The tool nmapis installed 0.1.9001
Checking Complete 1 192.168.112.129:40160 199.247.31.1:24792 SYN_SENT -
192.168.112.129:40160 199.247.31.1:24792 SYN_SENT -
192.168.112.129:40160 199.247.31.1:24792 SYN_SENT -
Starting Nmap Scan, Enter desired destination: 192.92.78.9905 SYN_SENT -
192.168.112.131
Enter desired port: nmap
22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-04 01:49 EDT
Nmap scan report for 192.168.112.131 129 times=50 ms
Host is up (0.00011s latency). 129 times=60 ms

PORT      STATE SERVICE
22/tcp    open  ssh
1002ms
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

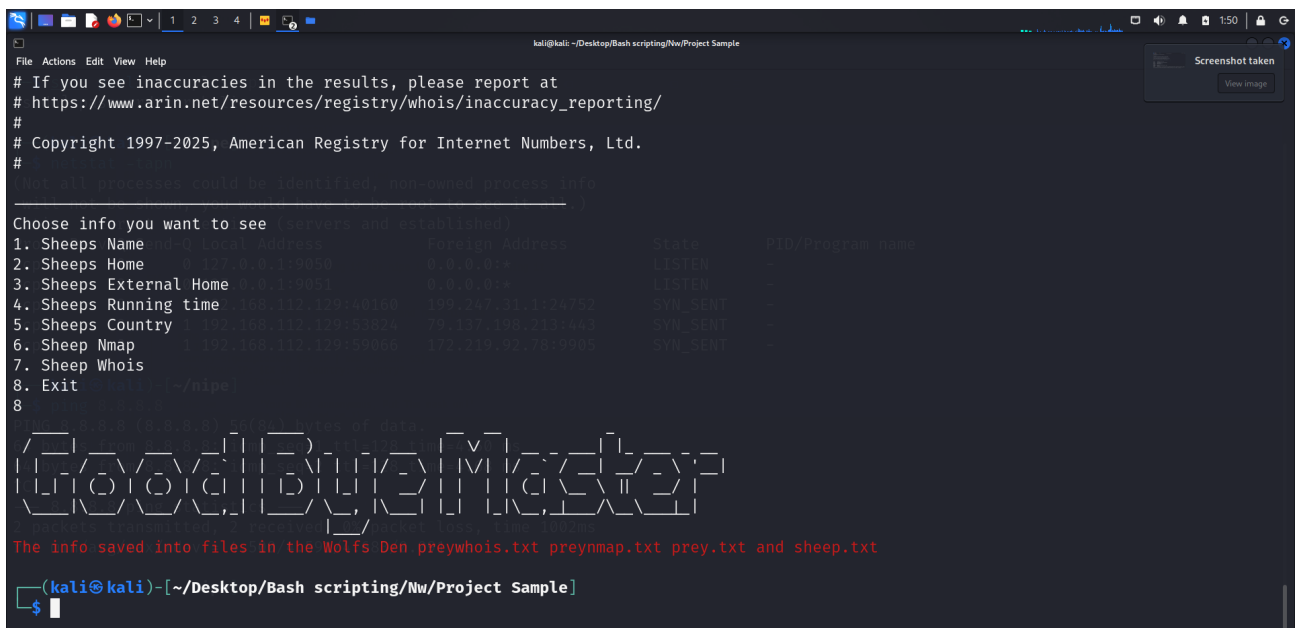
```
File Actions Edit View Help
Starting Whois Scan, Enter Desired Destination:
192.168.112.131
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# 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 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.
```

After each part was complete and properly tested I continued to the next part.

All that became at the end my first working script and project in this Course.

Thanks to Doron Zohar for guiding me through this process with advice and help.

Another tool that I used to help me around is Deepseek.com for correcting lines I had trouble with.



```
kali@kali: ~/Desktop/Bash scripting/Nw/Project Sample
File Actions Edit View Help
# 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.
#
Not all processes could be identified: non-owned process info
Choose info you want to see (servers and established)
1. Sheeps Name and 0 local Address      Foreign Address      State      PID/Program name
2. Sheeps Home      0 127.0.0.1:9950      0.0.0.0:*          LISTEN     -
3. Sheeps External Home 0.0.0.0:9950      0.0.0.0:*          LISTEN     -
4. Sheeps Running time 168.112.129.68168    199.247.31.174752   SYN_SENT    -
5. Sheeps Country 1 192.168.112.129:53074 79.137.198.213:443   SYN_SENT    -
6. Sheep Nmap      1 192.168.112.129:59066 172.219.32.78:9905   SYN_SENT    -
7. Sheep Whois
8. Exit      ~/nipe
8
Enter 0-9 or (0-9,0,8,0) if you want to see
Google BugMaster
The info saved into files in the Wolfs Den preywhois.txt preynmap.txt prey.txt and sheep.txt
(kali@kali)-[~/Desktop/Bash scripting/Nw/Project Sample]
$
```