shai simchon

בשלב הראשון של הסקריפט נבצע התקנה של nipe:

inst script function:

```
#!/bin/bash


#here we going to install nipe in our system for anonymosity
inst()
{
echo -e '\e[36mfisrt thing we going to do is to install nipe progrem  on our system:\e[0m'
sudo perl nipe.pl install
}
```

inst script function output:

```
┌──(kali㉿kali)-[~/Desktop/cyber/nipe]
└─$ bash project
fisrt thing we going to do is to install nipe progrem  on our system:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.8-1).
tor is already the newest version (0.4.7.7-1).
The following packages were automatically installed and are no longer required:
  libpython3.9-dev libtbb2 oracle-instantclient-basic python3-llvmlite python3.9-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1077 not upgraded.

now we check our true ip:

[+] Status: disabled.
[+] Ip: 80.246.140.217

now we going to become anonymous:

[+] Status: activated.
[+] Ip: 104.244.74.97

our anonymous ip location is in: country: Europe/Luxembourg



now we performing nmap vulnerabilities script:

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-12 12:23 EDT
```

בשלב השני של הסקריפט נוודא את הip המקורי שלנו ואז נהפוך לאנונימים:

anon activation script function:

```
#here we check our original and true ip
anon()
{
echo ' '
echo -e '\e[36mnow we check our true ip:\e[0m'
sudo perl nipe.pl status
sleep 3
#here we start the nipe progrem for became anonymous
echo -e '\e[36mnow we going to become anonymous:\e[0m'
sudo perl nipe.pl start
sudo perl nipe.pl status
ip=$(curl -s https://ipinfo.io/timezone/)

#here we check from where server we will going to connect to our victim
echo -e our anonymous ip location is in: "\e[31mcountry: $ip\e[0m"
echo
echo
echo
}
```

anon activation script function output:

```
now we check our true ip:

[+] Status: disabled.
[+] Ip: 80.246.140.217

now we going to become anonymous:

[+] Status: activated.
[+] Ip: 104.244.74.97

our anonymous ip location is in: country: Europe/Luxembourg
```

בשלב השלישי נבצע התחברות למחשב מרוחק תחת ssh ונבצע nmap וwhois query:

vps script function:

```
vps()
{
sshpass -p 231231 ssh -o StrictHostKeyChecking=no shai2@192.168.152.128 echo -e $'\e[36mnow we connect to the victim and performing nmap vulnerabilities script:\e[0m';echo;
nmap -Pn -sV --script=vulners $(hostname -I);sleep 3;echo;echo -e $'\e[36mnow we performing whois query:\e[0m';echo; whois $(hostname -I)
}
```

vps script function output:

```
now we connect to the victim and performing nmap vulnerabilities script:

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-15 13:39 EDT
Nmap scan report for 192.168.152.132
Host is up (0.00022s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.7p1 Debian 4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.7p1:
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       CVE-2016-20012  4.3     https://vulners.com/cve/CVE-2016-20012
|_      CVE-2021-36368  2.6     https://vulners.com/cve/CVE-2021-36368
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds

now we performing whois query:
```

```
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:        2013-08-30
Comment:        These addresses are in use by many millions of independentl
ed in hundreds of millions of devices.  They are only intended for use with
Comment:
Comment:        These addresses can be used by anyone without any need to c
the source of activity you may see on logs or in e-mail records.  Please re
Comment:
Comment:        These addresses were assigned by the IETF, the organizatior
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0
```

```
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/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#
```

עכשיו נקרא לשלושת הפונקציות אחת אחרי השנייה בשביל להריץ את הסקריפט בצורה אוטומטית:

```
#here we install nipe progrem in our system
inst
#here we calling the nipe function that makes us anonymous
anon
#here wo calling the function that runs nmap vulnerability scan and whois query
vps
```

nipe install guide taken from:
https://www.geeksforgeeks.org/how-to-install-nipe-tool-in-kali-linux/