

# THINK CYBER CYBERIUM ARENA SIMULATOR TRAINING

## NX201 - NETWORK RESEARCH

### PROJECT TITLE: REMOTE CONTROL

#### (OLALEKAN ILORI – S4)

```
#!/bin/bash
```

**TITLE: --A bash script to automatically execute commands on a remote server anonymously from my local system**

```
#-----#
#STUDENT NAME;      Olalekan Ilori
#STUDENT CODE;      s4
#CLASS CODE;        Unit 0722
#LECTURER'S NAME;   David Shiffman
#-----#
#Code for Checking if my system is anonymous
echo "$(geoiplookup $(curl -s ifconfig.me))" > myIPadd #checks the geolocation of systems ipaddress
cat myIPadd|awk '{print $5}' > myCountry

for i in $(cat myCountry)                                #takes ip in the
do
echo "Your Ip address is from $i "
done
if [ "$i" == "Nigeria" ]                                #checks if my ip
still from Nigeria
then
    cd /home/kali/nipe                                    #if ip
still Nigeria, it changes directory to Nipe folder to access Nipe tool
    perl nipe.pl restart                                    #starts the nipe
tool to make ip anonymous
    cd /home/kali
    #changes directory back to current directory
    echo "You're Not Anonymous, relaunch this script to become anonymous..."
    echo "$(cat myCountry)"
else
    echo "You're in Anonymous State Already....."
fi
```

#2---In section below, after achieving anonymous IP, script Automatically connect to a remote VPS server (156.67.208.189) via ssh and executing commands to a Target server

#---the one-liner script below Enables bypassing fingerprint with "sshpass -p" and Stores the result locally into the file NRproject.tst in current directory

```
sshpass -p MjsbBaU30OtuzEH ssh -o StrictHostKeyChecking=off root@156.67.208.189 'whois
boilecon.com && nmap -F boilecon.com' > NRproject.tst
```

```
echo " [+] The result of your scan has been stored in the file NRproject.tst inside current directory"
```

```
File Actions Edit View Help
(root@kali)-[/home/kali/CyberPT]
# ./NR-Project.sh
Your Ip address is from Nigeria
You're Not Anonymous, relaunch this script to become anonymous...
cat: myCountry: No such file or directory

[+] The result of your scan has been stored in the file NRproject.tst inside current directory

(root@kali)-[/home/kali/CyberPT]
# ls
myCountry  myIPadd  NR-Project.sh

(root@kali)-[/home/kali/CyberPT]
# cat myCountry
Nigeria

(root@kali)-[/home/kali/CyberPT]
# ./NR-Project.sh
Your Ip address is from Romania
You're in Anonymous State Already.....
[+] The result of your scan has been stored in the file NRproject.tst inside current directory

(root@kali)-[/home/kali/CyberPT]
# ls
myCountry  myIPadd  NR-Project.sh  NRproject.tst

(root@kali)-[/home/kali/CyberPT]
# cat NRproject.tst
Domain Name: BOILECON.COM
Registry Domain ID: 1887083758_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.resellercamp.com
Registrar URL: http://www.idwebhost.com
Updated Date: 2022-10-16T17:05:32Z
Creation Date: 2014-11-25T09:48:27Z
Registry Expiry Date: 2023-11-25T09:48:27Z
Registrar: CV. JOGJACAMP
Registrar IANA ID: 1478
Registrar Abuse Contact Email: abuse@resellercamp.com
Registrar Abuse Contact Phone: +62 813 2900 4500
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS00AI.STACKPATHDNS.NET
Name Server: NS07CI.STACKPATHDNS.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-10-28T08:51:53Z <<<

For more information on Whois status codes, please visit https://icann.org/epp/

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: BOILECON.COM
Registry Domain ID: 1887083758_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.resellercamp.com
Registrar URL: http://resellercamp.com/
Updated Date: 2022-10-16T17:05:33Z
Creation Date: 2014-11-25T09:48:27Z
Registrar Registration Expiration Date: 2023-11-25T09:48:27Z
Registrar: CV. Jogjacamp
Registrar IANA ID: 1478
Registrar Abuse Contact Email: abuse@resellercamp.com
Registrar Abuse Contact Phone: +62.82141570000
Domain Status: clientTransferProhibited (http://icann.org/epp#clientTransferProhibited)
Registrant Organization: Bank of Industry, Nigeria
Registrant State/Province: Lagos
Registrant Country: NG
Name Server: ns00ai.stackpathdns.net
Name Server: ns07ci.stackpathdns.net
DNSSEC: Unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>>Last update of WHOIS database: 2022-10-28T08:37:11Z<<<

For more information on Whois status codes, please visit https://icann.org/epp

Registration Service Provided By: THE GOLIVE DIGITAL SOLUTIONS COMPANY LTD

The data in this whois database is provided to you for information purposes
only, that is, to assist you in obtaining information about or related to a
domain name registration record. We make this information available "as is",
and do not guarantee its accuracy. By submitting a whois query, you agree
that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to:
(1) enable high volume, automated, electronic processes that stress or load
this whois database system providing you this information; or
(2) allow, enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via direct mail, electronic mail, or
by telephone.
The compilation, repackaging, dissemination or other use of this data is
expressly prohibited without prior written consent from us. The Registrar of
record is CV. Jogjacamp.
We reserve the right to modify these terms at any time.
By submitting this query, you agree to abide by these terms.
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-28 08:52 UTC
Nmap scan report for boilecon.com (151.139.128.10)
Host is up (0.00069s latency).
rDNS record for 151.139.128.10: map3.hwcdn.net
```

```

Registrar URL: http://resellercamp.com/
Updated Date: 2022-10-16T17:05:33Z
Creation Date: 2014-11-25T09:48:27Z
Registrar Registration Expiration Date: 2023-11-25T09:48:27Z
Registrar: CV. Jogjacamp
Registrar IANA ID: 1478
Registrar Abuse Contact Email: abuse@resellercamp.com
Registrar Abuse Contact Phone: +62.82141570000
Domain Status: clientTransferProhibited (http://icann.org/epp#clientTransferProhibited)
Registrant Organization: Bank of Industry, Nigeria
Registrant State/Province: Lagos
Registrant Country: NG
Name Server: ns00ai.stackpathdns.net
Name Server: ns07ci.stackpathdns.net
DNSSEC: Unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>>Last update of WHOIS database: 2022-10-28T08:37:11Z<<<

For more information on Whois status codes, please visit https://icann.org/epp#status:OnlineP

Registration Service Provided By: THE GOLIVE DIGITAL SOLUTIONS COMPANY LTD

The data in this whois database is provided to you for information purposes
only, that is, to assist you in obtaining information about or related to a
domain name registration record. We make this information available "as is",
and do not guarantee its accuracy. By submitting a whois query, you agree
that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to:
(1) enable high volume, automated, electronic processes that stress or load
this whois database system providing you this information; or
(2) allow, enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via direct mail, electronic mail, or
by telephone.
The compilation, repackaging, dissemination or other use of this data is
expressly prohibited without prior written consent from us. The Registrar of
record is CV. Jogjacamp.
We reserve the right to modify these terms at any time.
By submitting this query, you agree to abide by these terms.
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-28 08:52 UTC
Nmap scan report for boilecon.com (151.139.128.10)
Host is up (0.00069s latency).
rDNS record for 151.139.128.10: map3.hwcdn.net
Not shown: 98 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 2.71 seconds

(root@kali)-[/home/kali/CyberPT]

```

```

NR-Project.sh x NR-Project.sh x
1  #!/bin/bash
2
3  #TITLE:--A bash script to automatically execute commands on a remote server anonymously from my local system
4  #-----#
5  #STUDENT NAME ;      Olalekan Ilori
6  #STUDENT CODE ;      s4
7  #CLASS CODE ;      Unit 0722
8  #LECTURER'S NAME;    David Shiffman
9  #-----#
10
11 #Code for Checking if my system is anonymous
12 echo "$(geopiplookup $(curl -s ifconfig.me))" > myIPadd #checks the geolocation of systems ipaddress
13 cat myIPadd|awk '{print $5}'> myCountry
14
15 for i in $(cat myCountry)
16 do
17   echo "Your Ip address is from $i"
18 done
19 if [ "$i" == "Nigeria" ]
20 then
21   cd /home/kali/nipe
22   perl nipe.pl restart
23   cd /home/kali
24   echo "You're Not Anonymous, relaunch this script to become anonymous..."
25   echo "$(cat myCountry)"
26 else
27   echo "You're in Anonymous State Already....."
28 fi
29
30 #2---In section below, After achieving anonymous IP, script Automatically connect to a remote VPS server(156.67.208.189) via ssh and executing commands to a Target server
31 #---the one-liner script below Enables bypassing fingerprint with "sshpass -p" and Stores the result locally into the file NRproject.tst in current directory
32 sshpass -p MjsbBaU300tuZEh ssh -o StrictHostKeyChecking=off root@156.67.208.189 'whois boilecon.com && nmap -F boilecon.com' > NRproject.tst
33
34 echo " [*] The result of your scan has been stored in the file NRproject.tst inside current directory"
35
36
37
38
39
40

```