NETCAT

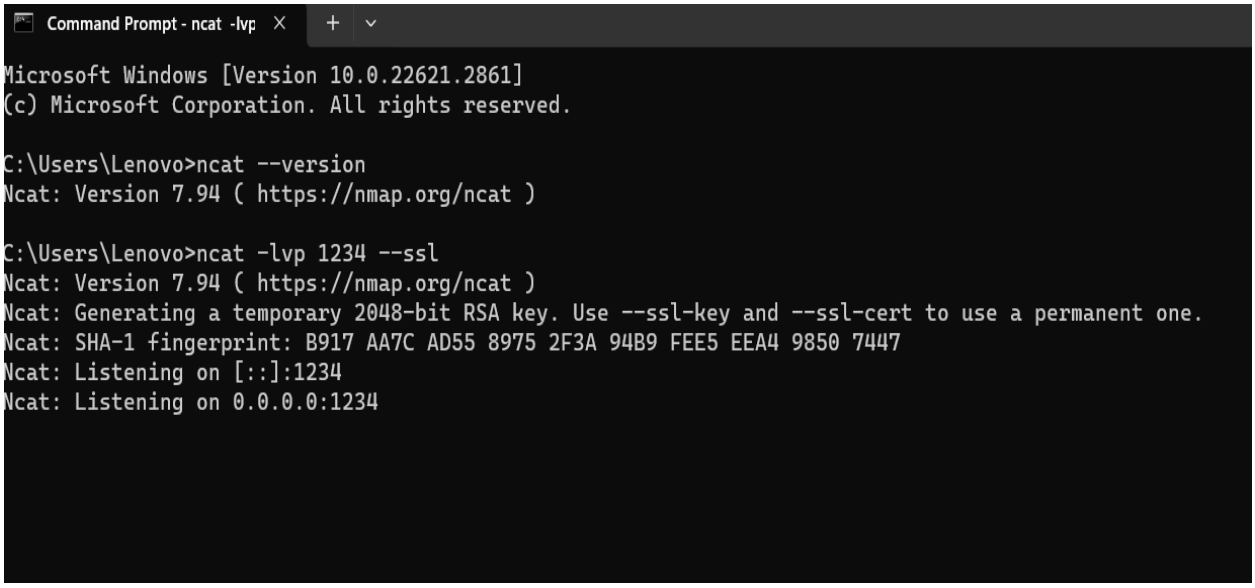
NETCAT is a command-line or shell application that can be used for a variety of uses including transferring files, establishing remote shells, chat, and more!

Features of NATCAT:

- **Port Scan**
- **Send File**
- **Receive File**
- **Execute Remote Script**
- **Encrypted Chat (NCAT)**
- **Banner Grab**
- **Shells/Reverse Shells**

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:ff80:1009:52:d2e1:a770:8ea6:a09f
   Temporary IPv6 Address. . . . . . : 2401:ff80:1009:52:5df7:b8d1:c222:2058
   Link-local IPv6 Address . . . . . : fe80::6a28:fb59:bd06:b7db%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.116
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::16eb:b6ff:fe5b:74d7%11
                                       192.168.0.1
PS C:\Users\Lenovo>
```

Netcat will start listening on port 1234 and any data sent to this port will be received by Netcat. The SSL encryption ensures that the data is encrypted during transmission. This is particularly useful for secure data transfers or for setting up secure communication channels.

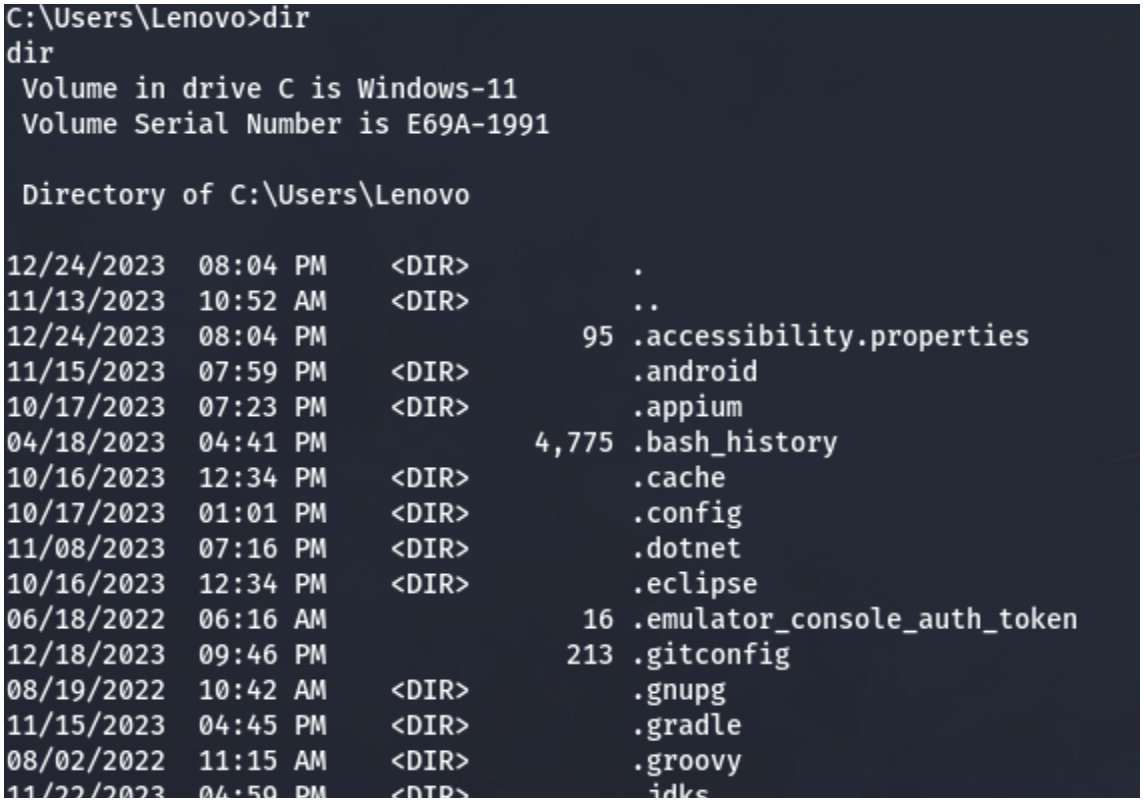


```
C:\Users\Lenovo>ncat -lvp 1234 --ssl
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Generating a temporary 2048-bit RSA key. Use --ssl-key and --ssl-cert t
Ncat: SHA-1 fingerprint: B917 AA7C AD55 8975 2F3A 94B9 FEE5 EEA4 9850 7447
Ncat: Listening on [::]:1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.0.118:39028.
hello
hi
hello dear
```

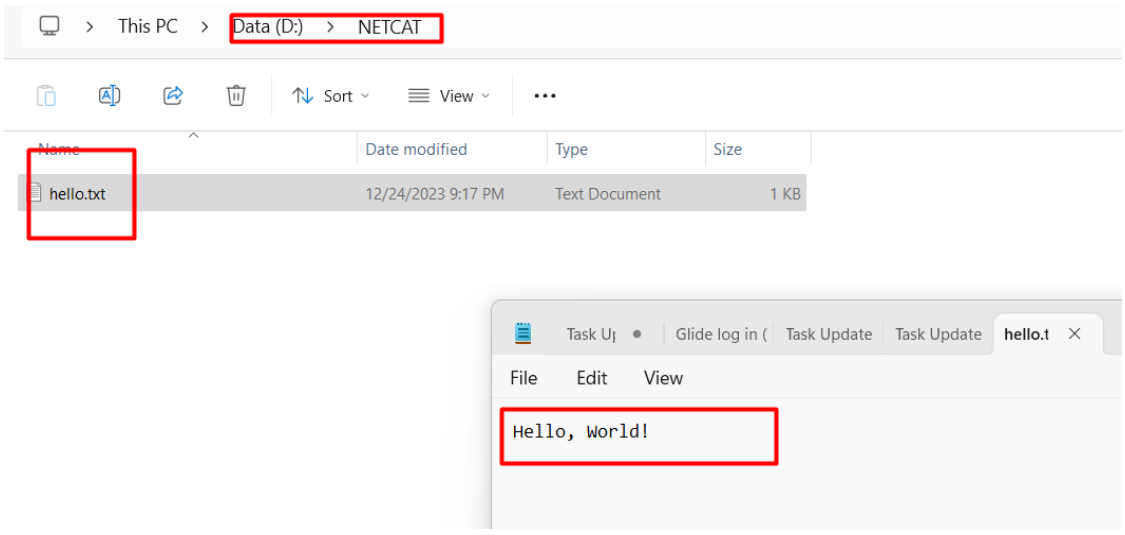
Netcat will listen on port 1234 and, upon receiving a connection, will execute `cmd.exe`, effectively giving the remote user access to a command prompt on your machine. This can be extremely dangerous as it could allow an unauthorized user to gain control over your computer.

```
C:\Users\Lenovo>ncat -lvp 1234 --ssl -e cmd.exe
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Generating a temporary 2048-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: 6993 B2C2 574E 2204 8176 01A9 54E8 E3AC B0DE 73EB
Ncat: Listening on [::]:1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.0.118:36908.
```

create a file remotely involves a simple data transfer process between two machines. Here's a basic guide on how to do it, but keep in mind that you should only perform such actions in a controlled environment, like a lab setup, and only on systems where you have permission to do so. Unauthorized access to systems can be illegal and unethical.



```
02/28/2023  11:29 AM    <DIR>          Saved Games
02/28/2023  11:29 AM    <DIR>          Searches
10/18/2023  03:41 PM    <DIR>          source
12/21/2023  03:43 PM    <DIR>          Videos
              13 File(s)        304,046 bytes
              47 Dir(s)  47,651,336,192 bytes free

C:\Users\Lenovo>d:
d:

D:\>cd NETCAT
cd NETCAT

D:\NETCAT>Hello.txt
Hello.txt

D:\NETCAT>echo Hello, World! > hello.txt
echo Hello, World! > hello.txt

D:\NETCAT>
```



Open a Port to Listen: On the remote machine, use Netcat to listen on a specific port. This machine will receive the data and create a file from it. For example:

ncat -lvp 1234 > output.txt

Send the File: On your local machine, use Netcat to send the file to the remote machine's IP address and the port they are listening on.

ncat [remote IP address] 1234 < input.txt