Executive Post Graduate Certification in Cyber Security and Ethical Hacking

Project

Nmap Network Reconnaissance:

To identify open ports, active services, and OS details, we performed an **Nmap scan** with the following command: nmap -sS -sV -O -p- <target-IP> and our target IP is 192.168.27.131.

Command executed:

nmap -sS -sV -O -p- 192.168.27.131

Nmap Scan Results:

Target IP: 192.168.27.131
Host Status: Up (0.0017s latency):

Identified Open Ports and Services:

Port	State	Service	Version
21/tcp	open	FTP	vsftpd 2.3.4
22/tcp	open	SSH	OpenSSH 4.7p1 Debian 8ubuntu1
23/tcp	open	Telnet	Linux telnetd
25/tcp	open	SMTP	Postfix smtpd
53/tcp	open	DNS	ISC BIND 9.4.2
80/tcp	open	HTTP	Apache 2.2.8
139/tcp	open	NetBIOS-SSN	Samba smbd 3.X - 4.X
445/tcp	open	SMB	Samba smbd 3.X - 4.X
2049/tcp	open	NFS	2-4 (RPC #100003)
3306/tcp	open	MySQL	MySQL 5.0.51a-3ubuntu5
5900/tcp	open	VNC	VNC (protocol 3.3)
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

Operating System: Linux 2.6.X

Device Type: General-purpose

Service Info: Unix, Linux, metasploitable.localdomain

SMB Enumeration:

Enumerating SMB Shares with smbclient

Command : smbclient -L \\192.168.27.131 --no-pass

Command executed:

Findings:

Anonymous login successful.

Shared resources identified on the target system.

Possible misconfigured permissions.

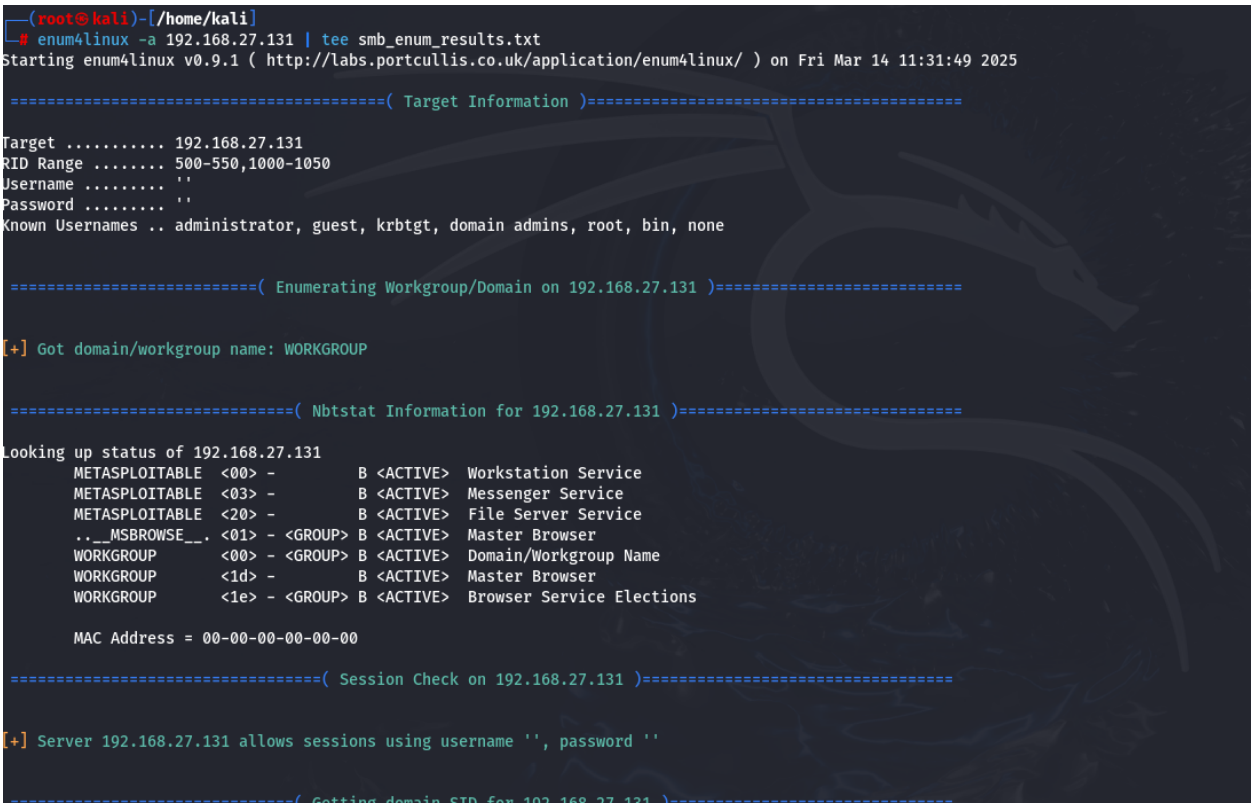
Sharename	Type	Comment
print$	Disk	Printer Drivers
tmp	Disk	oh noes!
opt	Disk	
IPC$	IPC	IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$	IPC	IPC Service (metasploitable server (Samba 3.0.20-Debian))

Workgroup & Server Details:

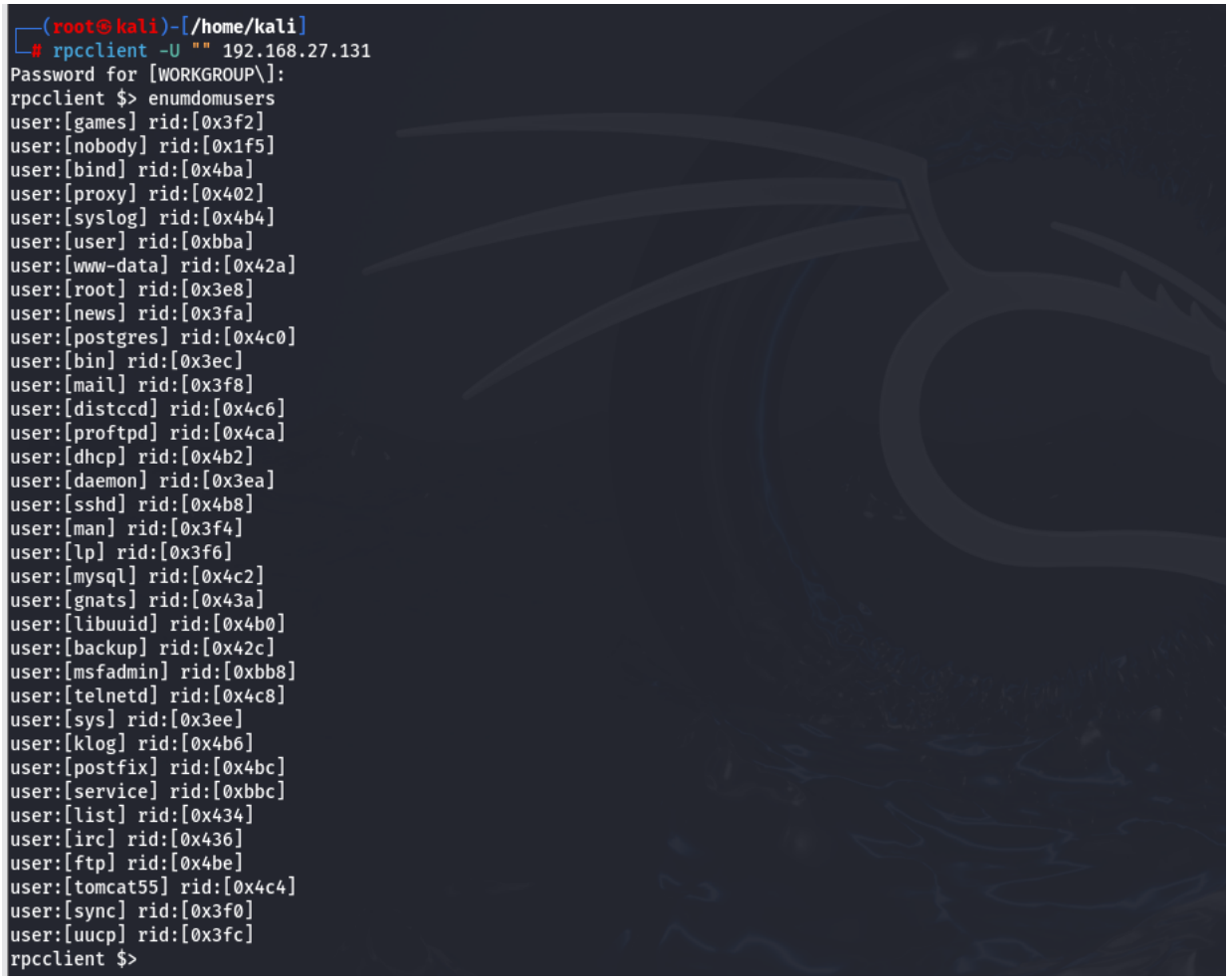
Workgroup	Master
WORKGROUP	METASPLOITABLE

Enumerate SMB with enum4linux

enum4linux -a 192.168.27.131 | tee smb_enum_results.txt



rpcclient -U "" 192.168.27.131



This project involved various reconnaissance and enumeration techniques to identify vulnerabilities in a target system (192.168.27.131). Using Nmap, we identified open ports, active services, and OS details, revealing that the system is running Linux 2.6.X with multiple exposed services.

Further, SMB enumeration using smbclient and enum4linux indicated potential misconfigurations, including anonymous login access and shared resources, which could be exploited by attackers. These findings highlight the importance of securing network services, implementing proper access controls, and regularly monitoring for misconfigurations to prevent unauthorized access.

The project demonstrates the effectiveness of ethical hacking methodologies in identifying security gaps, reinforcing the need for proactive security measures in an organizational environment.