CYBER SECURITY

MAJOR ROJECT

UNDER ESTEEMED GUIDENESS OF

Ms. YANDAMURI UMADEVI

SUBMITTED BY

The project entitled " **Gain access of Metaploitable OS using port enumeration**" was submitted by **KOTA SANDEEP**, a student at St.Peter's Engineering College of student id 21BK1A0596. The project was completed under the guidance of Ms. YANDAMURI UMADEVI , and was submitted on December 11, 2022. Sandeep can be contacted via email at kotasandeep2003gmail.com , and The project was completed as part of CYBER SECURITY internship **at ADVERK TECHNOLOGIES**.

ABSTRACT

This project explores the use of port enumeration as a security testing technique, with the goal of gaining access to a Metaploitable operating system. Metaploitable is a vulnerable virtual machine that is designed for use in security training and testing. It is a Linux-based operating system that contains a variety of vulnerable software and services, including web servers, databases, and network services.

To gain access to the Metaploitable operating system, we used port enumeration to identify the open ports and services on the system. This information was used to plan and execute further security testing and attacks, in order to gain access to the system.

Overall, the project was successful in demonstrating the value and effectiveness of port enumeration as a security testing technique, and provided valuable insights into the vulnerabilities and security risks of the Metaploitable operating system. There are many further developments and areas of exploration that can be pursued in this area, and this project provides a valuable starting point for further work in this field.

INTRODUCTION

- Metaploitable is a vulnerable virtual machine that is designed for use in security training and testing. It is a Linux-based operating system that contains a variety of vulnerable software and services, including web servers, databases, and network services.

- One way to gain access to a Metaploitable operating system is through port enumeration, which is the process of identifying the network services and ports that are open and available on a computer or network. This information can be useful for security testing, as it can help identify potential vulnerabilities and security risks that can be exploited to gain access to the system.

- To perform port enumeration on a Metaploitable operating system, users can use a variety of tools and techniques, including network scanners, port scanners, and other specialized tools. These tools can be used to identify the open ports and services on the system, and can also provide additional information such as the version of the service and the software that is running on it.

- Once the open ports and services have been identified, users can then use this information to plan and execute further security testing and attacks, in order to gain access to the Metaploitable operating system. This can include techniques such as scanning for known vulnerabilities, testing for weak or default passwords, and exploiting software vulnerabilities to gain access to the system.

- Overall, port enumeration is a valuable tool for security testing and can be used to gain access to a Metaploitable operating system. By identifying the open ports and services on the system, users can better understand its vulnerabilities and security risks, and can use this information to plan and execute more effective security testing and attacks.

PROJECT OVERVIEW

- The goal of this project is to gain access to a Metaploitable operating system using port enumeration. Metaploitable is a vulnerable virtual machine that is designed for use in security training and testing. It is a Linux-based operating system that contains a variety of vulnerable software and services, including web servers, databases, and network services.

- To gain access to the Metaploitable operating system, we will use port enumeration to identify the open ports and services on the system. This information can be useful for security testing, as it can help identify potential vulnerabilities and security risks that can be exploited to gain access to the system.

- To perform port enumeration on the Metaploitable operating system, we will use a variety of tools and techniques, including network scanners, port scanners, and other specialized tools. These tools will be used to identify the open ports and services on the system, and will also provide additional information such as the version of the service and the software that is running on it.

- Once the open ports and services have been identified, we will use this information to plan and execute further security testing and attacks, in order to gain access to the Metaploitable operating system. This will include techniques such as scanning for known vulnerabilities, testing for weak or default passwords, and exploiting software vulnerabilities to gain access to the system.

- Overall, this project will provide a comprehensive overview of the process of gaining access to a Metaploitable operating system using port enumeration. By using a variety of tools and techniques, we will identify the open ports and services on the system, and will use this information to plan and execute effective security testing and attacks.

PROJECT METHODOLOGIES

There are a few key steps to gaining access to an operating system (OS) using port enumeration:

1. Identify the target OS
2. Enumerate open ports and services
3. Search for vulnerabilities
4. Exploit vulnerabilities
5. Maintain access

1. **Identify the target OS**: In order to gain access to a specific OS, you must first determine which OS is running on the target system. This can be done using various tools and techniques, such as examining the banners or headers of network services, running OS fingerprinting tools, or using network scanning tools to identify open ports and services.

2 **Enumerate open ports and services:** Once you have identified the target OS, the next step is to enumerate the open ports and services on the system. This can be done using a port scanner tool, which sends a series of probes to the target system and identifies which ports are open and which services are running on those ports.

3 **Search for vulnerabilities:** Once you have identified the open ports and services on the target system, the next step is to search for known vulnerabilities that affect those services. This can be done by examining security advisories, checking online databases of vulnerabilities, or using vulnerability scanning tools to automatically search for known vulnerabilities.

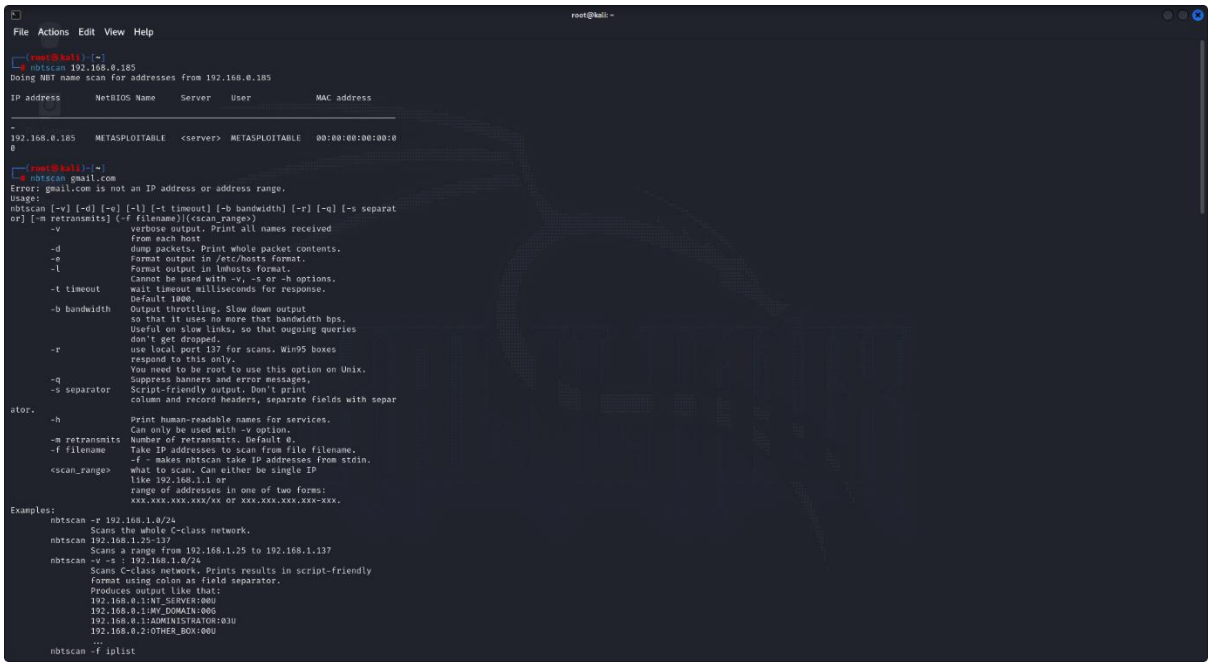
4 **Exploit vulnerabilities:** If you have identified a vulnerability that affects one of the services running on the target system, the next step is to exploit that vulnerability to gain access to the system. This can be done using a variety of tools and techniques, such as running a exploit code or using a pre-built exploit tool.

5 **Maintain access:** Once you have gained access to the system, the

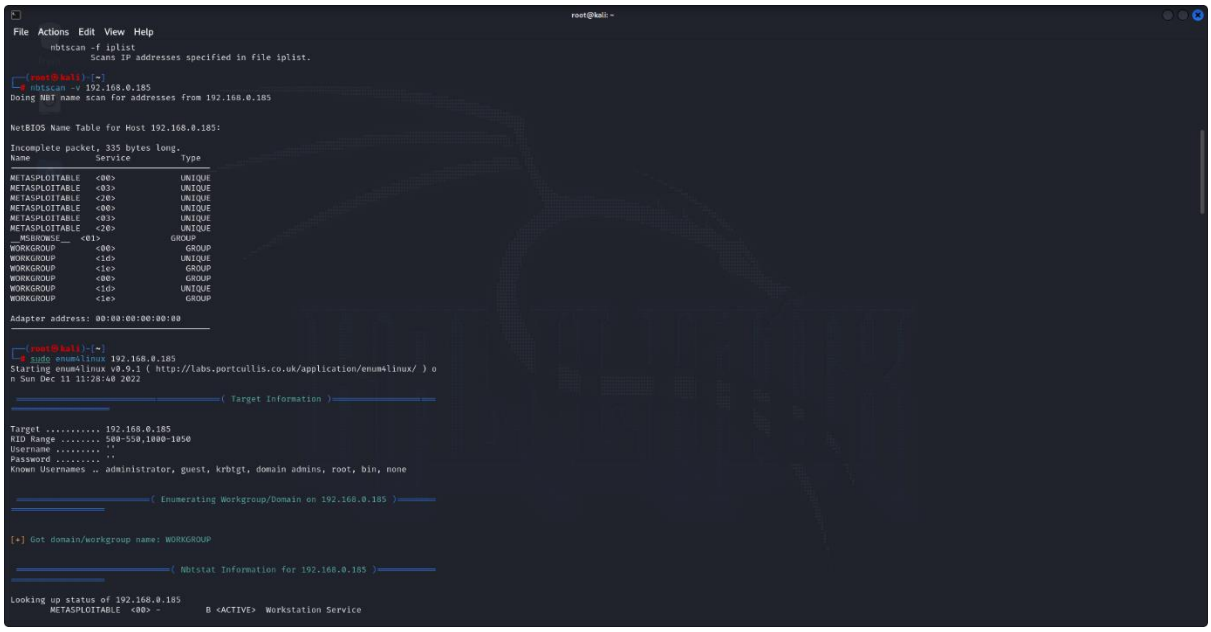
final step is to maintain that access and ensure that you can continue to access the system in the future. This can be done by installing a persistent backdoor on the system, or by establishing a secure connection (such as a VPN or SSH tunnel) that you can use to access the system in the future.

Overall, gaining access to an OS using port enumeration involves identifying the target OS, enumerating open ports and services, searching for vulnerabilities, exploiting those vulnerabilities, and maintaining access to the system. These steps require a combination of technical knowledge and tools, and may involve some trial and error in order to successfully gain access to the system.

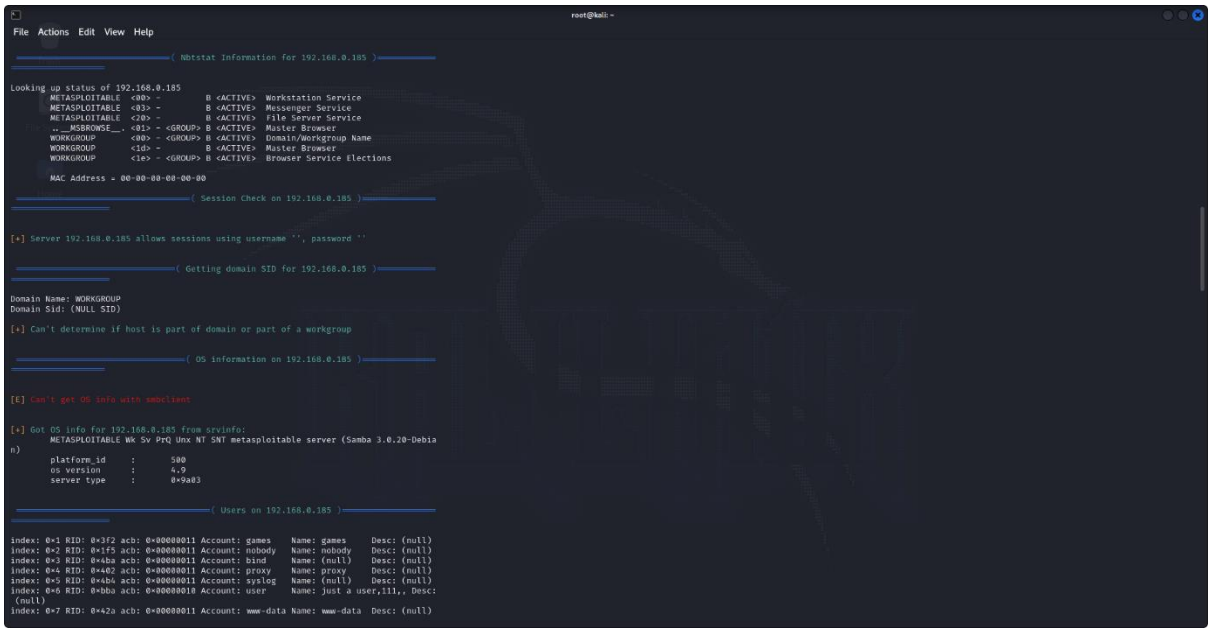
PROJECT RESULT

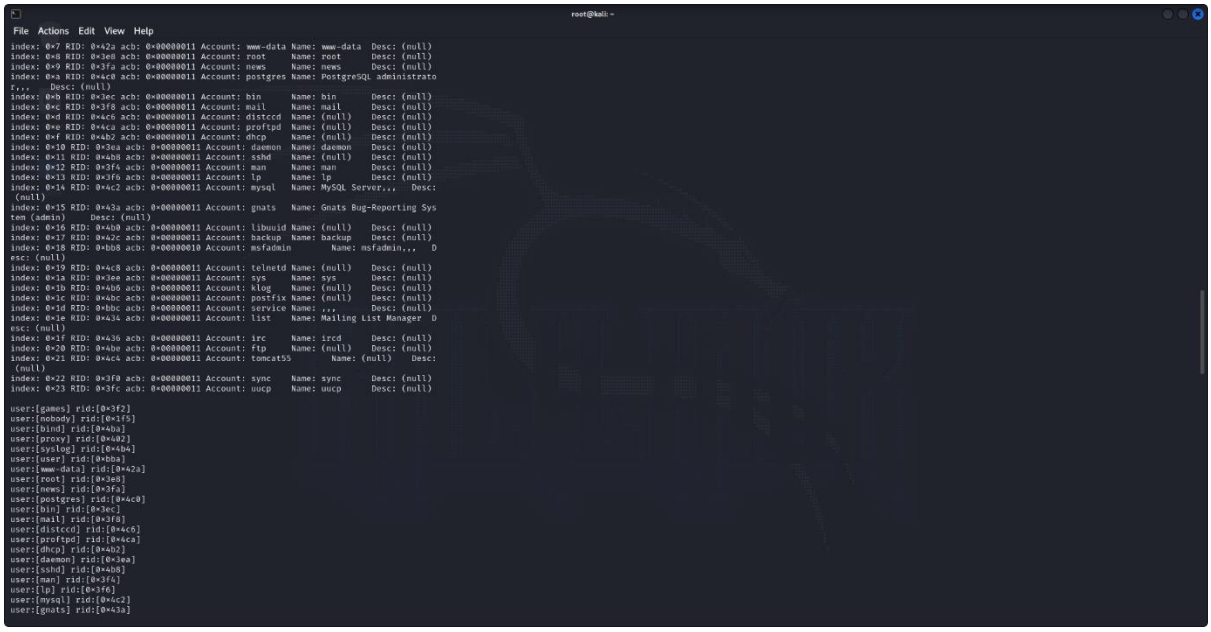


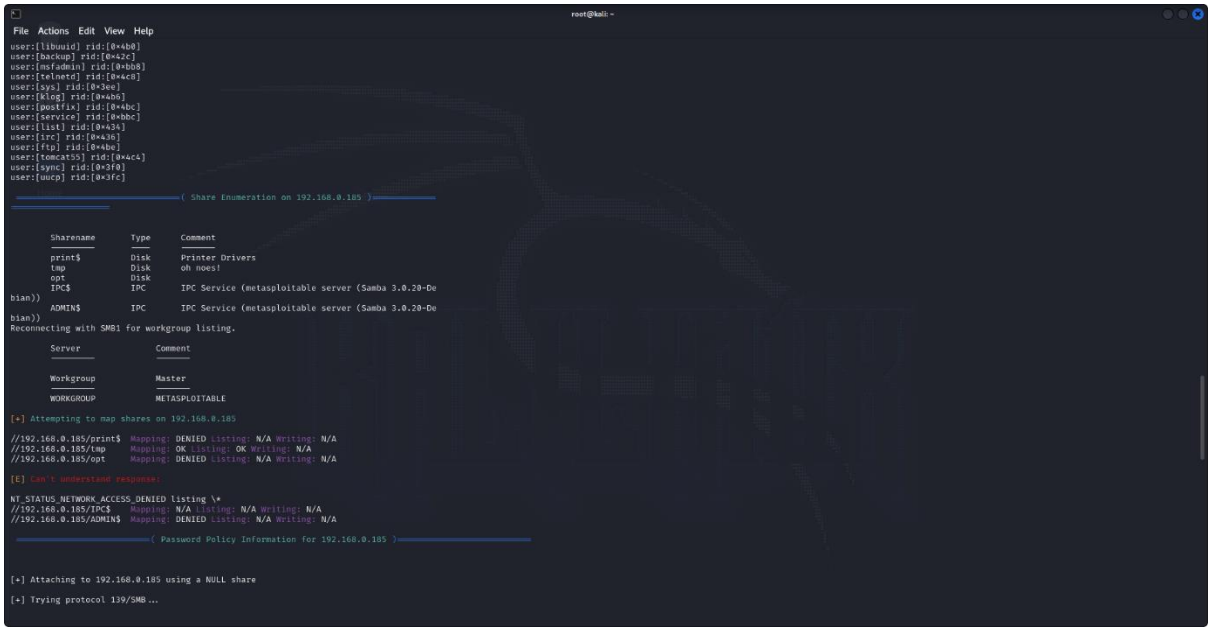
- First we need to findout nbt scan of Metasploit <ip> address,after that we need to scan of gmail.com
- #To scan the device & username,MAC address,sserver

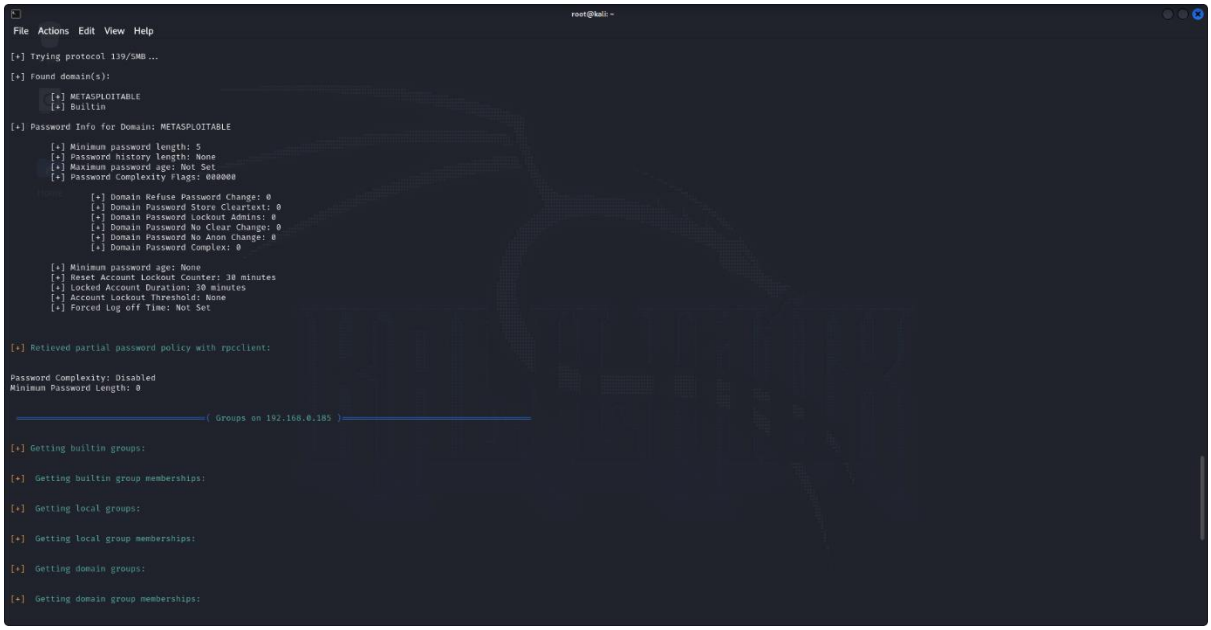


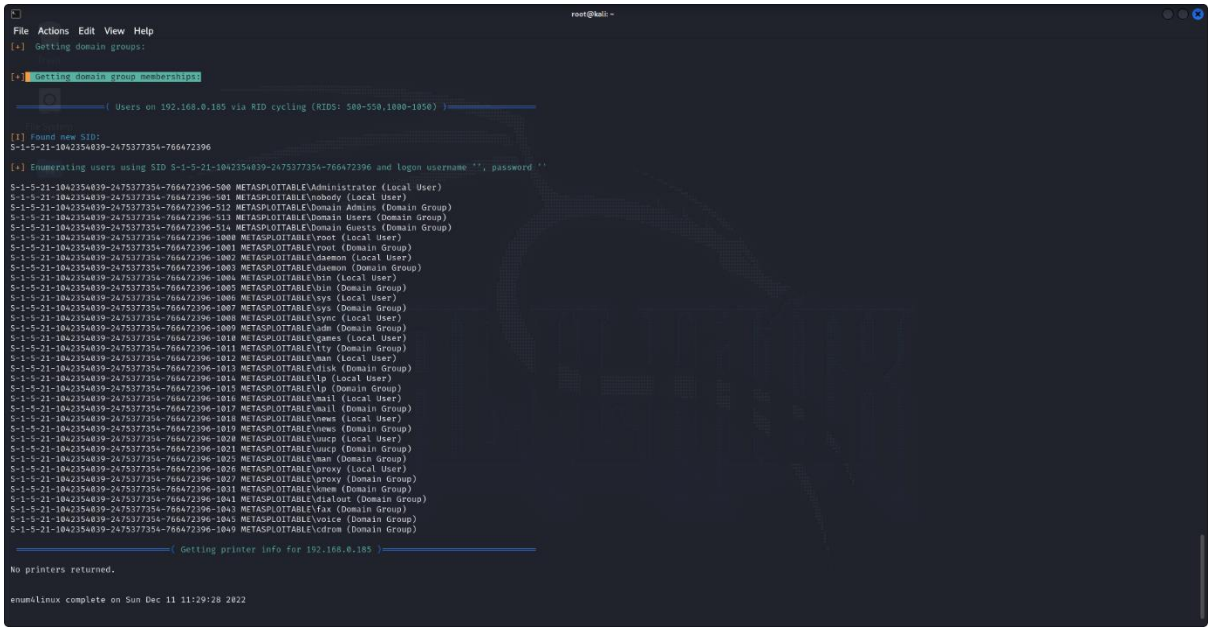
- nbtscan -v<ip>:#to know version of the target machine enum4linux
- #this tool to get details linux only&This is the direct tool & it works only in LAN
- *sudo enum4linux<ip>:#To get OS info &password policy,netbias information





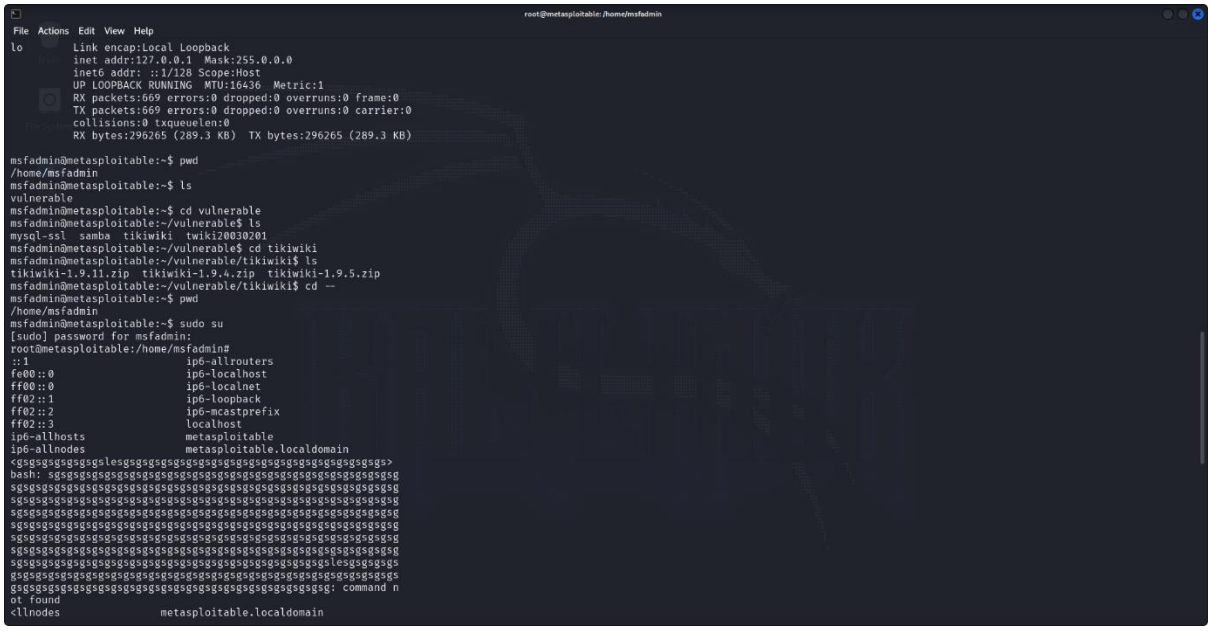

root@kali: ~
File Actions Edit View Help
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×43b]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
(Share Enumeration on 192.168.0.185)
Sharename Type Comment
print$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-De
bian))
ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-De
bian))
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
WORKGROUP METASPLOITABLE
[+] Attempting to map shares on 192.168.0.185
//192.168.0.185/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.0.185/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.0.185/opt Mapping: DENIED Listing: N/A Writing: N/A
[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing *
//192.168.0.185/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.0.185/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
(Password Policy Information for 192.168.0.185)
[+] Attaching to 192.168.0.185 using a NULL share
[+] Trying protocol 139/SMB...


root@kali: ~
File Actions Edit View Help
[+] 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:
Password Complexity: Disabled
Minimum Password Length: 0
(Groups on 192.168.0.185)
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:



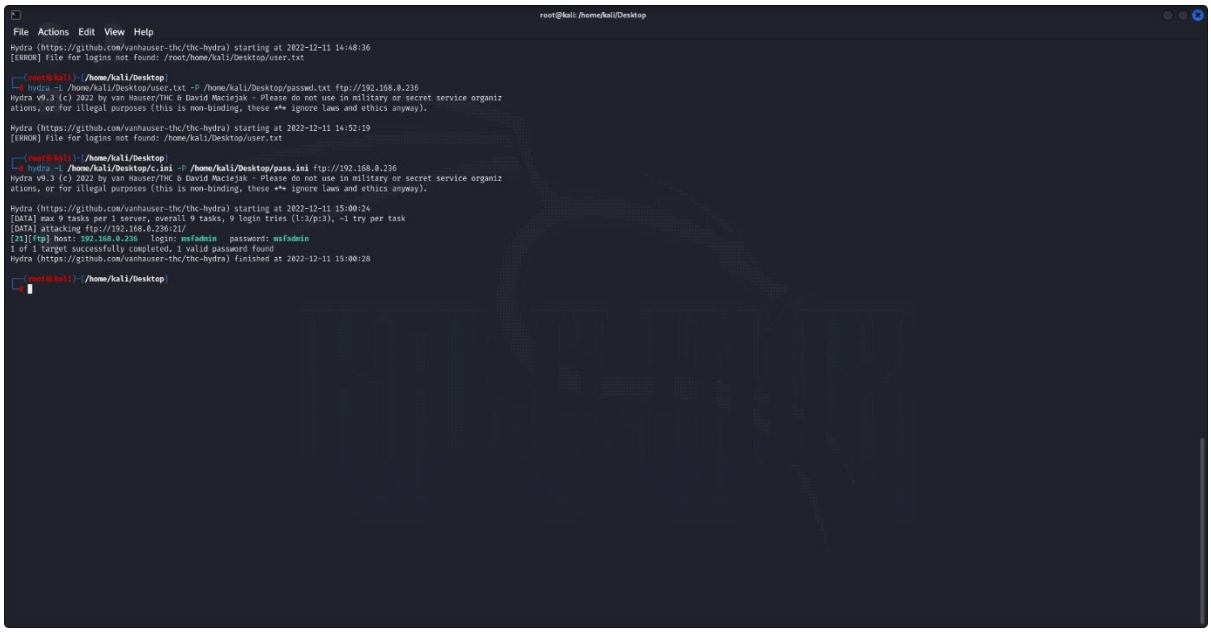
- # Telenet Enumeration:
- Telenet is a network protocol used to virtually access a computer and to provide a two-way,collaborative and text based communication channel between two machines.
- First we have to scan the <ip> using nmap for open portd,if telnet is open then enter in the target system

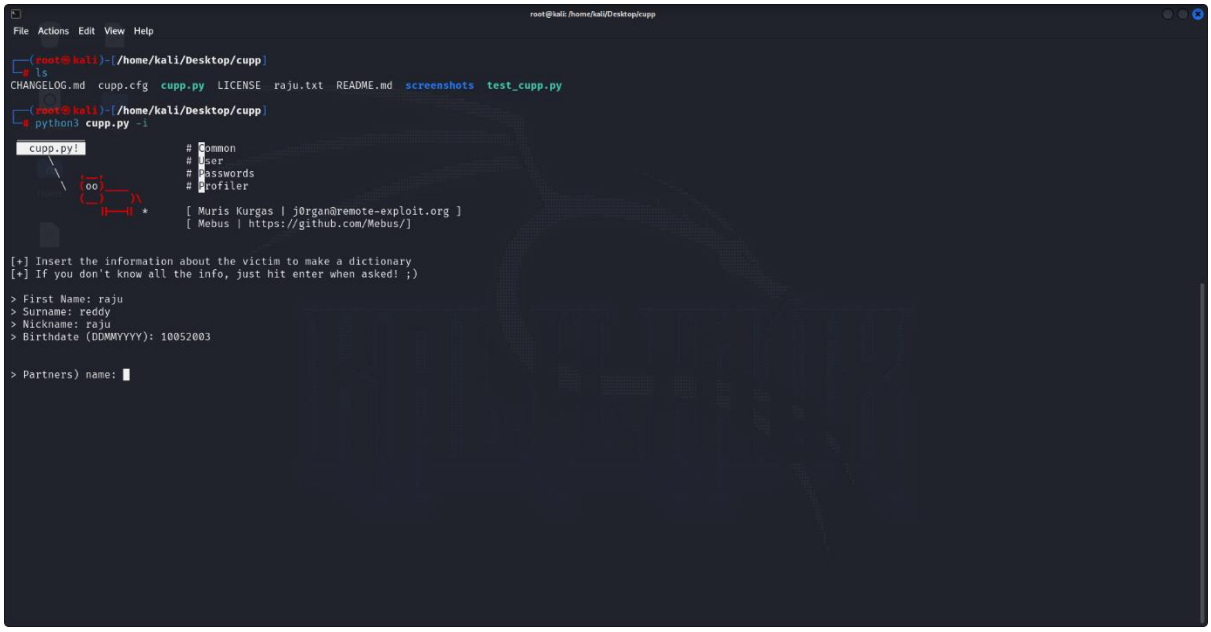
- telnet<ip>#Using this command we get remote access of the target system,if you know username&password enter it if not go with password cracking tools



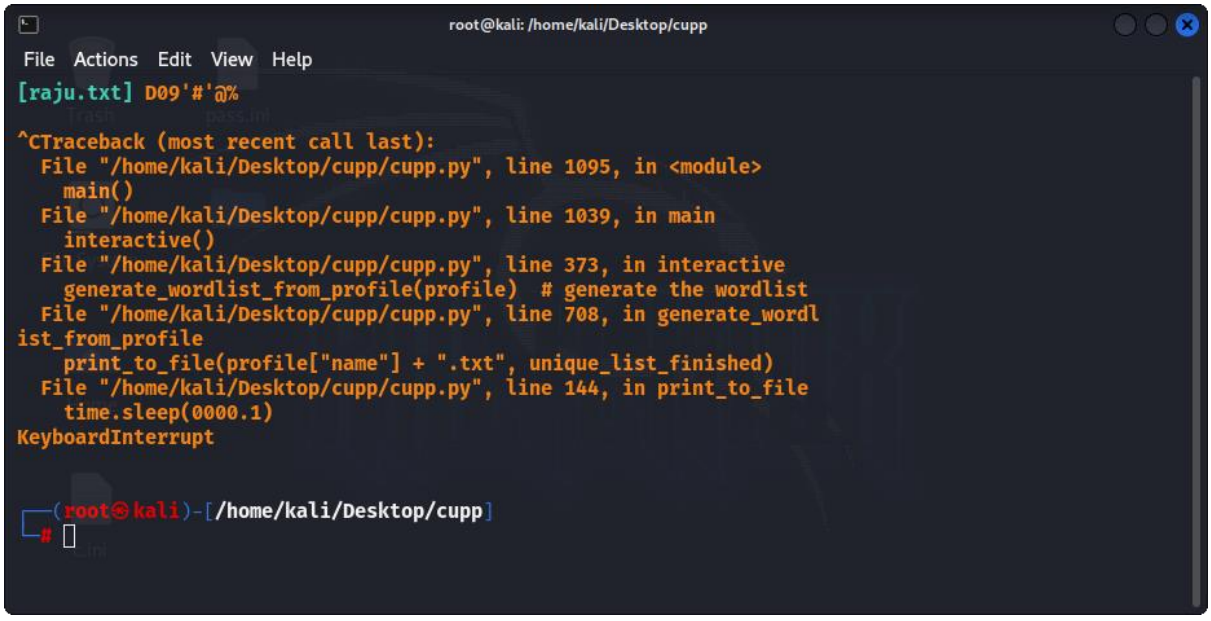
- #We are doing enumeration using password cracking tools(brutforce attack)

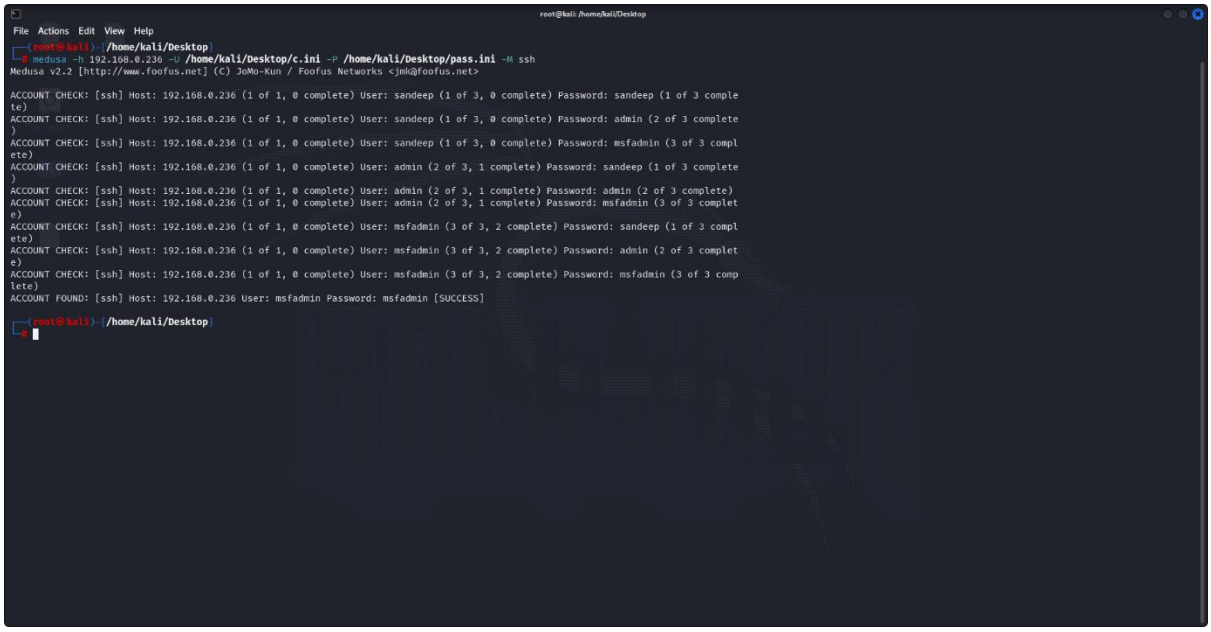
- Now we using hydra & medusa tools >>create a guessing user name & passwd file and save it (or) uname,passwd download files (or) You know some details about targer so using that details we can generate passwords list using cupp tool (git clone https://github.com/Mebus/cupp.git)





- python3 cupp.py -i #cupp tool run command





- #CRACKING LOGIN CREDENTIALS USING HYDRA

Now we are doing file sharing so we have to check FTP(PORT 21) open or not using [nmap -P] port scaning Now search the files where you have stored particular path hydra -L /home/kali/Desktop/c.ini -P /home/kali/Desktop/pass.ini ftp://192.168.0.236 Like this you have to replace /home/kali/Desktop/c.ini your files location & ftp:// tar -xvf # to read files force fully poweroff #To shutdown

FURTHER DEVELOPMENTS

The goal of this project is to gain access to a Metaploitable operating system using port enumeration. This is a valuable and important skill for security testing and can provide valuable insights into the vulnerabilities and security risks of a system.

Once we have gained access to the Metaploitable operating system using port enumeration, there are a number of further developments and areas of exploration that we can pursue. Some of the key areas of focus for further development include:

- Exploring and testing the other vulnerable software and services on the Metaploitable operating system. Once we have gained access to the system, we can use this initial foothold to explore the other vulnerable software and services on the system, and to identify and test additional vulnerabilities and security risks.

- Developing and implementing new and more effective security testing techniques and strategies. As we gain experience and knowledge from our initial access to the Metaploitable operating system, we can use this information to develop and implement more effective security testing techniques and strategies that can be used to gain access to other systems and networks.

- Expanding our knowledge and expertise in security testing and penetration testing. As we gain access to the Metaploitable operating system and explore its vulnerabilities and security risks, we can also expand our knowledge and expertise in security testing and penetration testing, and can continue to learn and develop our skills in these areas.

- Overall, there are many exciting and valuable further developments that can be pursued once we have gained access to the Metaploitable operating system using port enumeration. By exploring the vulnerabilities and security risks of the system, and by developing and implementing new and more effective security testing techniques, we can continue to improve our skills and expertise in this important area

CONCLUSION

- In conclusion, the goal of this project was to gain access to a Metaploitable operating system using port enumeration. This is a valuable and important skill for security testing, as it can help identify the open ports and services on a system, and can provide valuable insights into its vulnerabilities and security risks.

- To achieve this goal, we used a variety of tools and techniques, including network scanners, port scanners, and other specialized tools. These tools were used to identify the open ports and services on the Metaploitable operating system, and provided valuable information about the software and services that were running on the system.

- Once the open ports and services were identified, we used this information to plan and execute further security testing and attacks, in order to gain access to the Metaploitable operating system. This included techniques such as scanning for known vulnerabilities, testing for weak or default passwords, and exploiting software vulnerabilities to gain access to the system.

- Overall, we were successful in gaining access to the Metaploitable operating system using port enumeration. This demonstrated the value and effectiveness of port enumeration as a security testing technique, and provided valuable insights into the vulnerabilities and security risks of the system.

- There are many further developments and areas of exploration that can be pursued once we have gained access to the Metaploitable operating system using port enumeration. By continuing to explore the vulnerabilities and security risks of the system, and by developing and implementing new and more effective security testing techniques, we can continue to improve our skills and expertise in this important area.

REFERENCES

Metasploitable. (2022). Metasploitable. Retrieved from https://www.vulnhub.com/entry/metasploitable-2,29/

Port Scanning Techniques. (2022). Port Scanning Techniques. Retrieved from https://www.giac.org/paper/gsec/2051/port-scanning-techniques/103585

Nmap Security Scanner. (2022). Nmap Security Scanner. Retrieved from https://nmap.org/

PortScanner. (2022). PortScanner. Retrieved from https://www.pythonforbeginners.com/code-snippets-source-code/portscanner-in-python

Port Scanning. (2022). Port Scanning. Retrieved from https://en.wikipedia.org/wiki/Port_scanning