PRACTICAL :- 9

AIM: Exploiting with Metasploit (Kali Linux)

- Identify a vulnerable system and exploit it using Metasploit modules.
- Gain unauthorized access to the target system and execute commands or extract information.
- Understand the ethical considerations and legal implications of using Metasploit for penetration testing.

THEORY:

- The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
- Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.
- Other important sub-projects include the Opcode Database, shellcode archive and related research.
- The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework.
- Metasploit is pre-installed in the Kali Linux operating system.

METASPLOIT FRAMEWORK

The free version. It contains a command line interface, third-party import, manual exploitation and manual brute forcing. This free version of the Metasploit project also includes Zenmap, a well known ports-scanner and a compiler for Ruby, the language in which this version of Metasploit was written.

METASPLOIT MODULES:

PAYLOAD: When we use the show payloads command the msfconsole will return a list of compatible payloads for this exploit.

EXPLOIT: After vulnerability scanning and vulnerability validation, we have to run and test some scripts (called exploits) in order to gain access to a machine and do what we are planning to do.

RHOST: RHOST is the ip address of the target system.

LHOST: LHOST is the ip address of the system used to do the hacking**.**

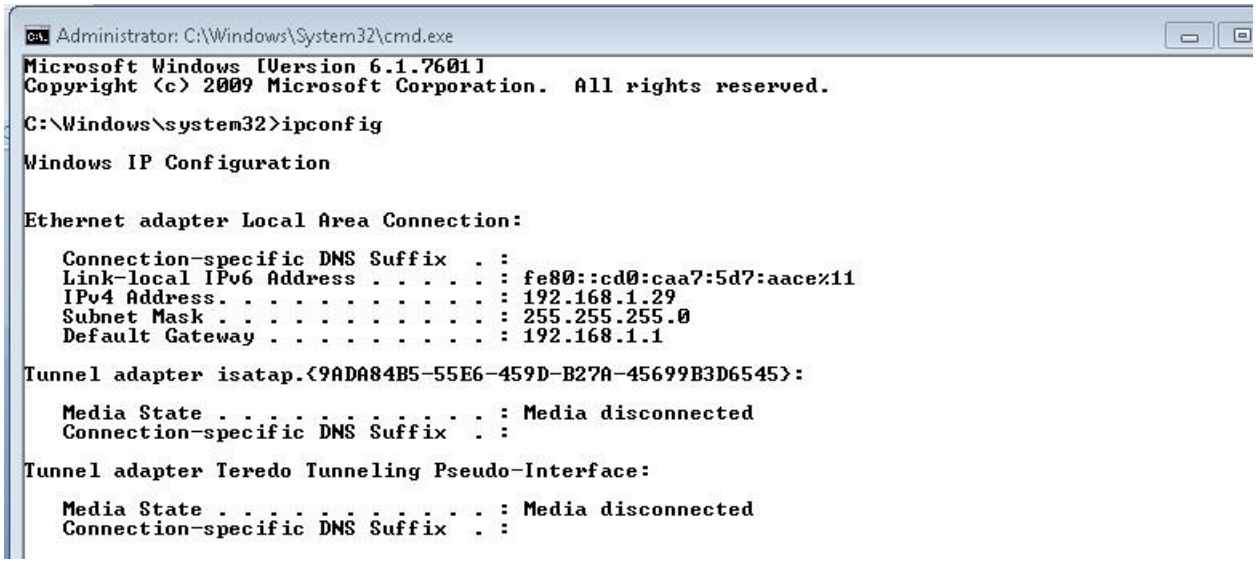
LPORT: LPORT is the local port used when opening a connection.

reverse_tcp: The php/meterpreter/reverse_tcp is a staged payload used to gain meterpreter access to a compromised system. This is a unique payload in the Metasploit Framework because this payload is one of the only payloads that are used in RFI vulnerabilities in web apps.

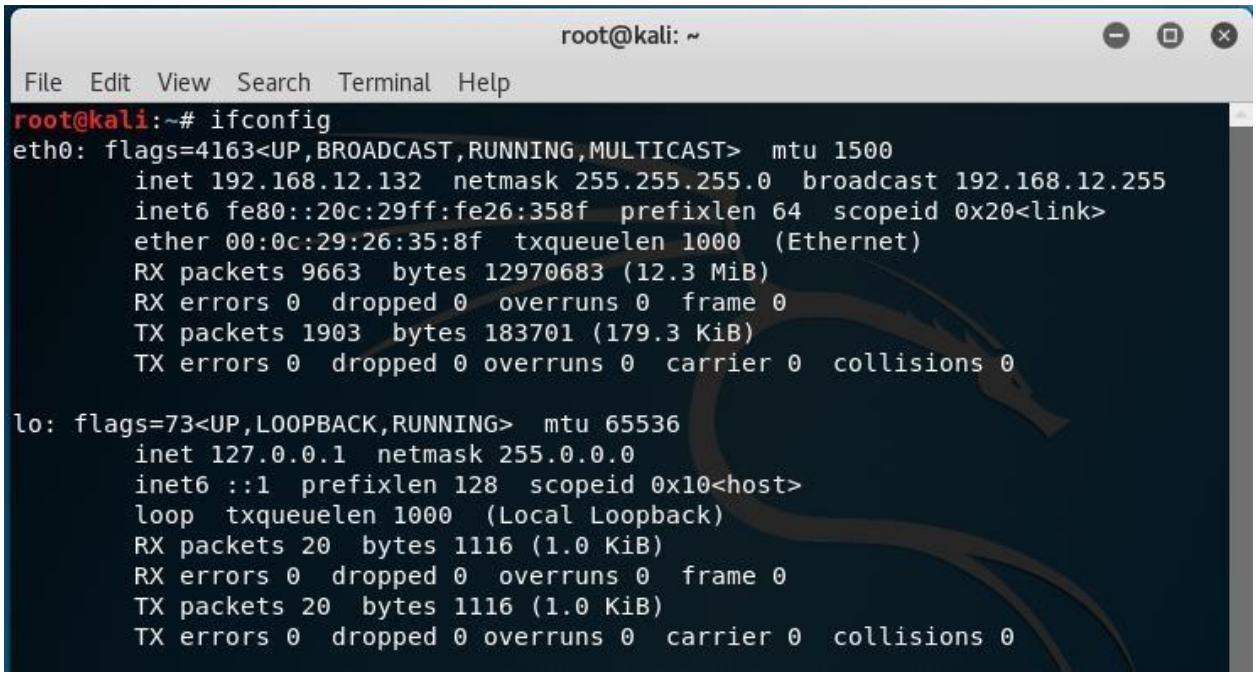
SMB: SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.

STEPS:

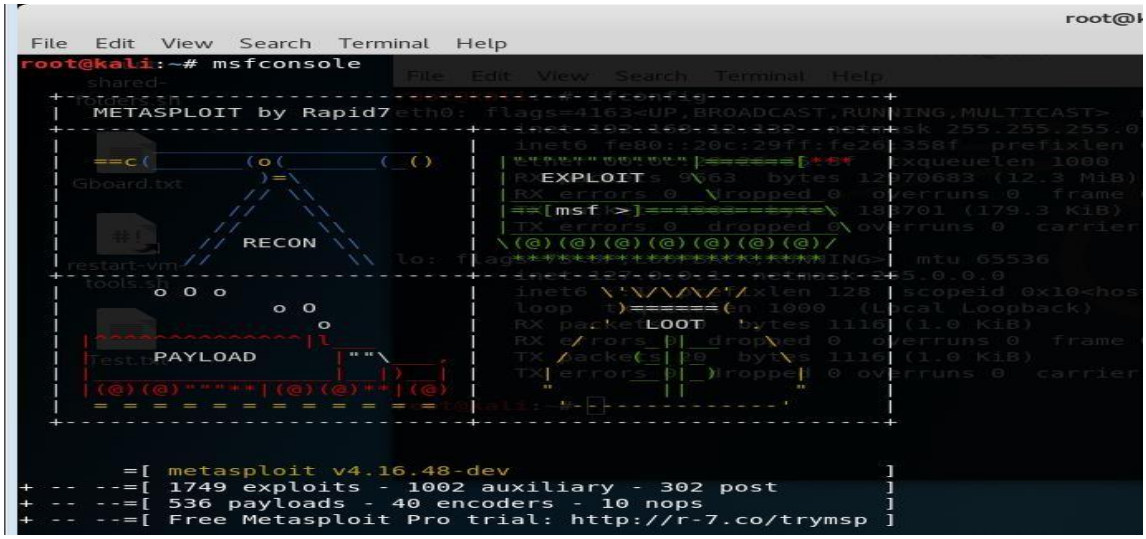
1. **Download and open Metasploit.**
2. **Use exploit to attack the host.**
3. **Create the exploit and add the exploit to the victim's PC.**
4. **Get the IP address of your windows operating system. By using ipconfig command on cmd.**

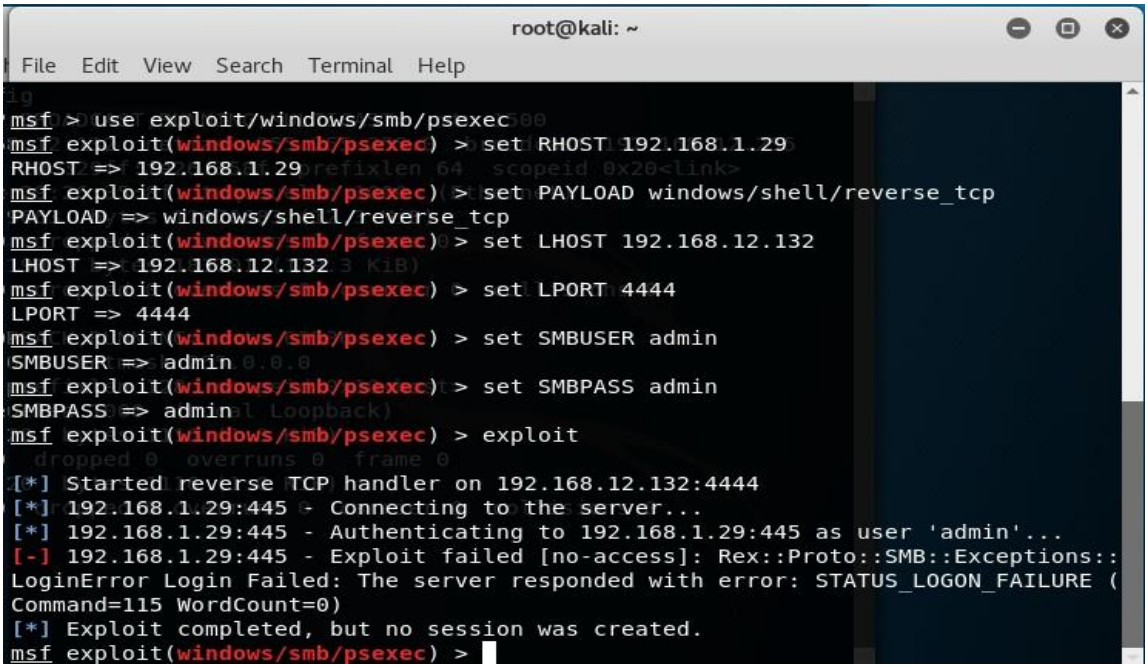


5. **Get the IP address of Linux Kali OS by using ifconfig command on terminal**



6. Enter the following code on terminal to get the output





CONCLUSION: Thus we have successfully exploited the Victims PC.