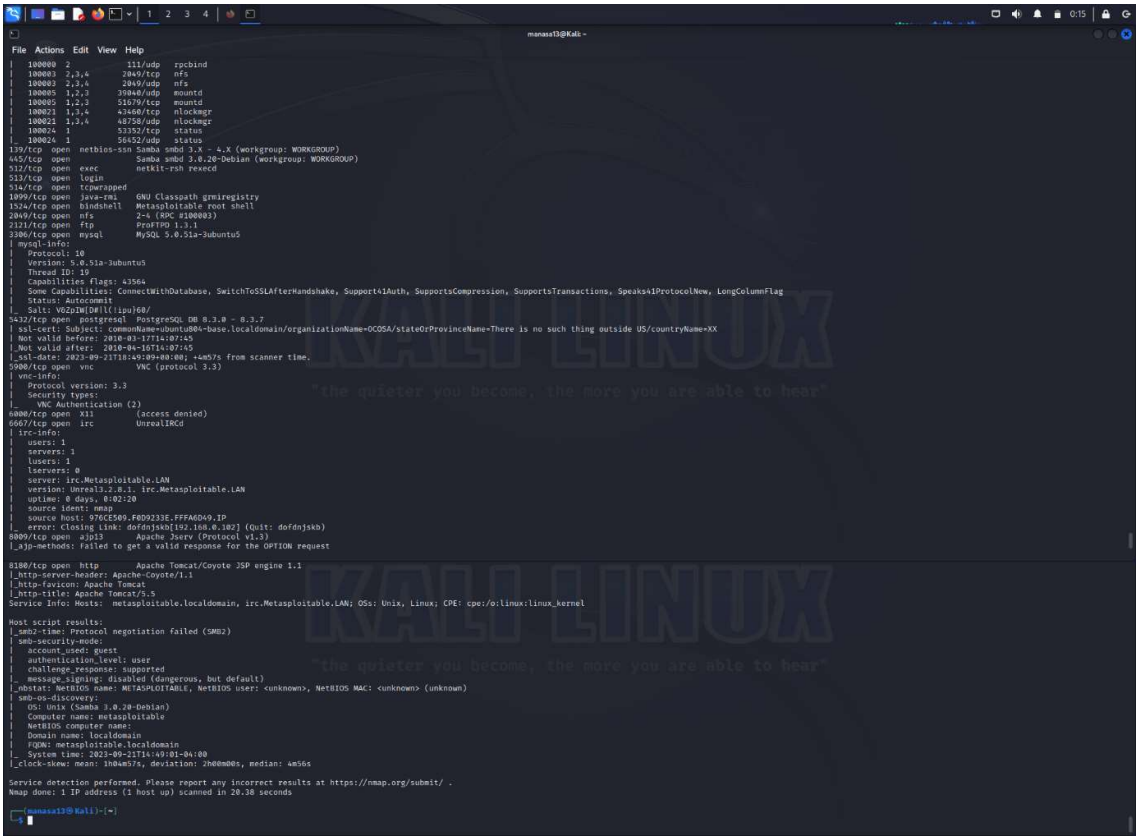
AI FOR WEB SECURITY WITH IBM QRADAR

Name: J. Manasa

Task-15: Any 3 vulnerabilities information from a particular ip address

First of all, **nmap -A <ip> command** is run where the aggressive scan of a particular ip address is performed where all the details related to that ip address such as types of ports used, open ports etc are displayed.

Information about the ip address:

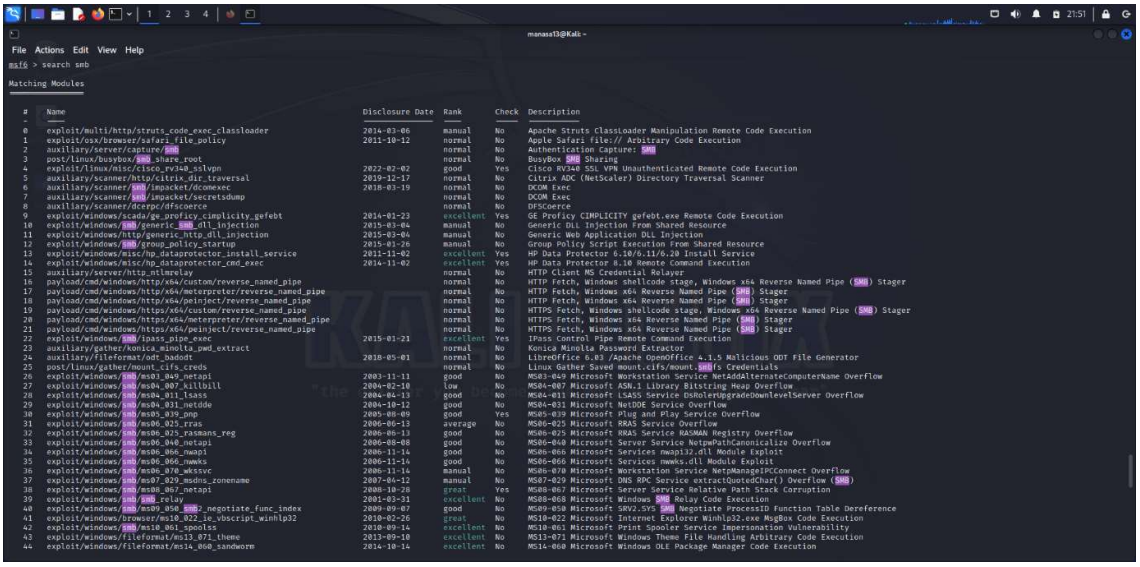


Commands used:

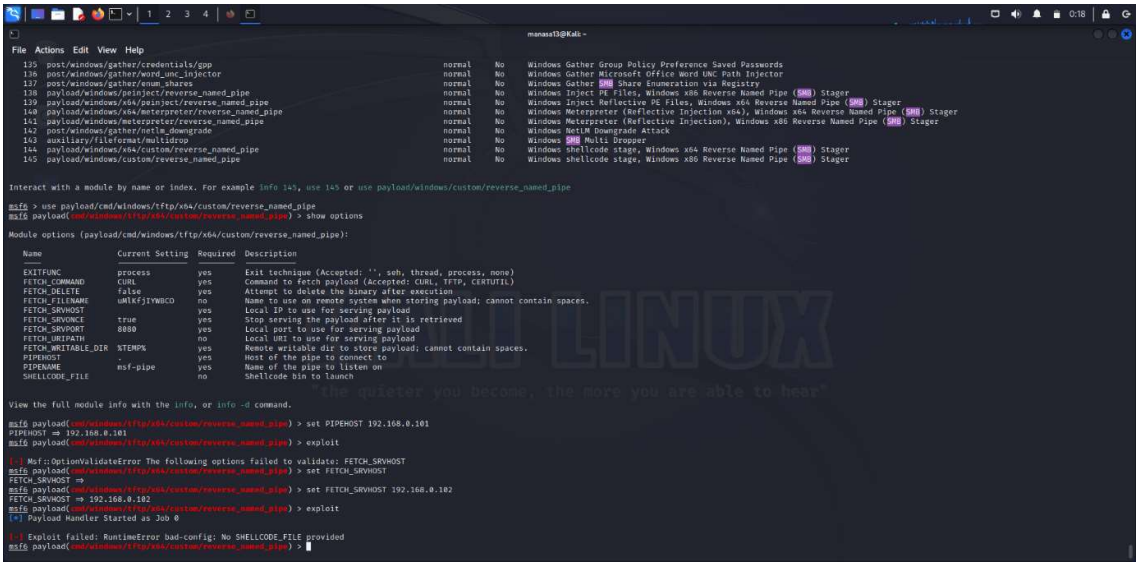
1. search smb
2. use <exploit name or module number>
3. show options
4. set <option name, value>
5. exploit

Vulnerabilities:

All these vulnerabilities were scanned using Metasploitable2. Metasploitable2 is a vulnerable virtual machine which runs on Linux. It is used to test common vulnerabilities.



1.



The above module is a payload module.

payload(cmd/windows/tftp/x64/custom/reverse_named_pipe):

Target Platform: Windows 64-bit.

Payload Function: Custom payload with reverse named pipe.

Purpose: This module is designed for 64-bit Windows systems and provides a custom payload that uses a reverse named pipe for communication. The "cmd/windows" prefix suggests that this payload may be intended to execute arbitrary Windows shell commands on the compromised system, providing the attacker with control over the system.

2.

The above module is a payload module.

windows/x64/meterpreter/reverse_named_pipe

Payload Name: "meterpreter/reverse_named_pipe"

Payload Platform: Windows

Payload Function: Reverse Meterpreter Payload Over Named Pipe

Purpose:

The purpose of this payload is to facilitate remote control and exploitation of a Windows x64 systems through a reverse Meterpreter session over a named pipe, especially in ethical hacking and penetration testing.

3.

The above module is an exploit module.

exploit(windows/browser/java_ws_vmargs):

Exploit Type: This is an exploit module.

Target Platform: Windows.

Exploit Target: Browsers with Java Web Start (JWS) applications running.

Purpose: This module is designed to exploit vulnerabilities in Java Web Start applications that run within web browsers on Windows systems. Java Web Start allows users to launch and manage Java applications from their web browsers. If a vulnerability exists in a JWS application, this module can be used to exploit it and gain control over the target system.