MSFrop a11y.text MSFrop Please note: This command is deprecated in the current version of Metasploit Searching Code Vulnerabilities with MSFrop a11y.text Searching Code Vulnerabilities with MSFrop As you develop exploits for newer versions of the Windows operation systems, you will find that they now have Data Execution Prevention (DEP) enabled by default. DEP prevents shellcode from being executed on the stack and has forced exploit developers to find a way around this mitigation and the so-called Return Oriented Programming (ROP) was developed. A ROP payload in created by using pre-existing sets of instructions from non-ASLR enabled binaries to make your shellcode executable. Each set of instructions needs to end in a RETN instruction to carry on the ROP-chain with each set of instructions commonly referred to as a gadget . The msfrop tool in Metasploit will search a given binary and return the usable gadgets. root@kali:# msfrop -h

Options:

-d, --depth [size] Number of maximum bytes to backwards disassemble from return instructions

-s, --search [regex] Search for gadgets matching a regex, match intel syntax or raw bytes

-n, --nocolor Disable color. Useful for piping to other tools like the less and more commands

-x, --export [filename] Export gadgets to CSV format

-i, --import [filename] Import gadgets from previous collections

-v, --verbose Output very verbosely

-h, --help Show this message Running msfrop with the -v switch will return all of the found gadgets directly to the console: root@kali:/tmp# msfrop -v metsrv.dll

Collecting gadgets from metsrv.dll

Found 4829 gadgets

metsrv.dll gadget: 0x10001057

0x10001057: leave

0x10001058: ret

metsrv.dll gadget: 0x10001241

0x10001241: leave

0x10001242: ret

metsrv.dll gadget: 0x1000132e

0x1000132e: leave

0x1000132f: ret

metsrv.dll gadget: 0x1000138c

0x1000138c: leave

0x1000138d: ret

...snip... The verbose msfrop output is not particularly helpful when a binary contains thousands of gadgets, so a far more useful switch isÂ -x Â whichÂ allows you to output the gadgets into a CSV file that you can then search later. root@kali:/tmp# msfrop -x metsrv_gadgets metsrv.dll

Collecting gadgets from metsrv.dll

Found 4829 gadgets

Found 4829 gadgets total

Exporting 4829 gadgets to metsrv_gadgets

Success! gadgets exported to metsrv_gadgets

root@kali:/tmp# head -n 10 metsrv_gadgets

Address,Raw,Disassembly

"0x10001098","5ec20c00","0x10001098: pop esi | 0x10001099: ret 0ch | "

"0x100010f7","5ec20800","0x100010f7: pop esi | 0x100010f8: ret 8 | "

"0x1000113d","5dc21800","0x1000113d: pop ebp | 0x1000113e: ret 18h | "

"0x1000117a","5dc21c00","0x1000117a: pop ebp | 0x1000117b: ret 1ch | "

"0x100011c3","5dc22800","0x100011c3: pop ebp | 0x100011c4: ret 28h | "

"0x100018b5","5dc20c00","0x100018b5: pop ebp | 0x100018b6: ret 0ch | "

"0x10002cb4","c00f9fc28d54","0x10002cb4: ror byte ptr [edi], 9fh | 0x10002cb7: ret 548dh | "

"0x10002df8","0483c20483","0x10002df8: add al, -7dh | 0x10002dfa: ret 8304h | "

"0x10002e6e","080bc20fb6","0x10002e6e: or [ebx], cl | 0x10002e70: ret 0b60fh | "

root@kali:/tmp# Next Writing an Exploit Prev Alphanumeric Shellcode