Microsoft

# Windows forensic Commands

# Windows forensic post exploit command

## network discovery:

net view /all

net view

net view \\HOSTNAME

net share

net session

wmic volume list brief

wmic share get

wmic logicladisk get

## scan:

nbtstat -A indirizzoip

for /L %I in (1,1,254) do ping -w 30 -n 1 192.168.1.%I | find "Reply" >> nomefile.txt

nbtstat -c

for /L %I in (1,1,254) do nbtstat -An 192.168.1.%I

vedere le connessioni wifi salvate:

netsh wlan show profile

vedere le pssword salvate:

netsh wlan show profile nomedelprofilo key=clear

## network:

netstat -e

netstat -nr

netstat -naob

netstst -S

netstat -vb

route print

arp -a

ipconfig /all

netsh wlan show interfaces

netsh wlan show all

# start/stop firewall:

netsh advfirewall show rule name=all

netsh advfirewall set allprofile state off

netsh advfirewall set allprofile state on

netsh advfirewall set publicprofile state on

netsh advfirewall set privateprofile state on

netsh advfirewall set domainprofile state on

netsh advfirewall firewall add rule name="Open Port 80" dir=in action=allow protocol=TCP localport=80

netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes

## Utenti:

creo l'utente:

net user /add nomeutente password

lo aggiungo al gruppo amministratori:

net localgroup administrators nomeutente /add

visualizzo i dettagli dell'utente:

net user nomeutente

cambio password:

net user nomeutente nuvapassword

## vari:

net users

net localgroup administrators

net group administrators

wmic rdtoggle list

wmic useraccount list

wmic group list

wmic netlogin get name,lastlogin,badpasswordcount

wmic netclient list brief

wmic nicconfig get

wmic netuse get

show content of file:

type file.txt

## servizi:

at

tasklist

tasklist /svc

schtask

net start

sc query

wmic service list brief | findstr "Running"

wmic service list brief | findstr "Stopped"

wmic service list config

wmic service list brief

wmic service list status

wmic service list memory

wmic job list brief

start/stop service:

sc config "nome servizio" start= disable

sc stop "nome servizio"

wmic service where name='nome servizio' call ChangeStartMode Disabled

autorun an autoload:

wmic startup list full

wmic ntdomain list brief

## leggere voci di registro:

reg query "HKCU\Control Panel\Desktop"

enable/disable rdesktop:

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

enable remote assistance:

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fAllowToGetHelp /t REG_DWORD /d 1 /f

## mainlista shadows files:

vssadmin List ShadowStorage

vssadmin List Shadow

net start VSS

polycy, patch:

set

gpresult /r

systeminfo

wmic qfe

## reboot:

shutdown.exe /r

## check settings of security log:

wevtutil gl Security

## check settings of audit policies:

auditpool /get /category:*

## system info:

echo %DATE% %TIME%

hostname

systeminfo

wmic csproduct get name

wmic bios get serialnumber

wmic computersystem list brief