### **Command-Line File Searching Using a Windows Command Shell**

**Exercise 1: searching for keywords in files using find**: in the following exercise, you will use the Windows *find* command to search through files for specific keywords:

1. From a reverse shell, change into the c:\windows\ directory (only type what's in **bold**):

#### C:\>cd \windows\

2. Search for different keywords within various file types in the current directory (only type what's in **bold**):

### C:\WINDOWS\>find "setup" \*.log > c:\temp\find\_setup\_log.txt

Syntax breakdown: find: program name "setup": the string to search for \*.log: the file type to search > c:\temp\find\_setup\_log.txt: redirect the output to a file called find\_setup\_log.txt in the c:\temp directory

Open the c:\temp\find\_setup\_log.txt file by typing the following (only type what's in **bold**):

#### C:\WINDOWS\>type c:\temp\find\_setup\_log.txt

4. Repeat steps #2-3, experimenting with various text strings in various file types

**Exercise 2: searching for files using findstr**: in the following exercise, you will use the Windows *findstr* command to search for specific keywords in various file types in the current directory (and all subdirectories):

1. If you are not in the c:\windows directory, change into it (only type what's in **bold**):

#### C:\>cd \windows

2. Type (only type what's in **bold**, on one line):

### C:\WINDOWS\>findstr /S "license" \*.log > c:\temp\findstr\_license\_log.txt

Syntax breakdown: findstr: program name /S: program option to search for matching files in the current directory and all subdirectories "license": the string to search for

\*.log: the file type to search

> c:\temp\findstr\_license\_log.txt: redirect the output to a file called findstr\_license\_log.txt in the c:\temp directory

3. Open the c:\temp\findstr\_license\_log.txt file by typing the following (only type what's in **bold**):

## C:\WINDOWS\>type c:\temp\findstr\_license\_log.txt

4. Repeat steps #2-3, experimenting with various text strings in various file types

# **Erasing Windows Logs Using elsave**

**Exercise 1: clearing of the Security Log on the target system**: in the following exercise, you will use *elsave* from the command-line to erase the Security log file on a Windows-based target system:

- 1. RDP into the target system
- 2. Open the Event Viewer by clicking Start/Run and typing eventvwr
- 3. Hit RETURN
- 4. Select the Security log (left-hand window pane) by clicking on it one time. You should see entries in this log file
- 5. From your Windows attack system, establish an administrative connection to the target (only type what's in **bold**):

#### C:\>net use \\target\_IP\_address\ipc\$ password /u:Administrator

6. Then type the following (only type what's in **bold**):

#### C:\>elsave -s \\target\_IP\_address -I "Security" -C

Syntax breakdown:

elsave: program name

- -s \\target\_IP\_address: the IP address of the target system
- -I "Security": program option specifying the log file to clear as the Security log
- -C: program option to clear the specified log file
- 7. Go back to your target system and verify that the Security log file entries were deleted (you will need to refresh the Event Viewer by clicking Action/Refresh)
- 8. Close your RDP connection

### **Hiding Files Using attrib**

**Exercise 1: hiding a file on the target system**: in the following exercise, you will use the built-in Windows command *attrib* to hide a file you stashed on the target system:

5. From your Windows attack system, establish an administrative connection to the target (only type what's in **bold**):

#### C:\>net use \\target\_IP\_address\ipc\$ password /u:Administrator

6. Map a drive to the C\$ share on the target system (only type what's in **bold**):

#### C:\>net use z: \\target\_IP\_address\c\$

7. To hide a file called nc.exe on the target system, type the following (only type what's in **bold**):

#### C:\>attrib +h z:\windows\system32\nc.exe

Syntax breakdown: attrib: program name +h z:\windows\system32\nc.exe: program option to hide a file called nc.exe

**Exercise 2: hiding all the files in a directory**: in the following exercise, you will hide all the files in a directory on the target system:

1. To hide all the files in a directory called Temp on the target system, type the following (only type what's in **bold**):

C:\>attrib +h z:\temp\\*.\*

## **Hiding Files Using Alternate Data Streams**

**Exercise 1: hiding a file using an ADS**: in the following exercise, you will hide a file within another file using an ADS:

- 8. RDP into the Windows target system
- Open a command shell and change into the C:\>WINDOWS\system32 directory (only type what's in **bold**):

C:\Documents and Settings\Administrator.WIN2K3DC>cd \ C:\cd windows\system32

10. Next create a blank text file (only type what's in **bold**):

#### C:\WINDOWS\system32>notepad myfile.txt

11. Click Yes to create the new file called myfile.txt

Syntax breakdown: **notepad**: program name **myfile.txt**: name of file to create in Notepad

12. Type 10 lines worth of text into this file

13. Save the file and exit from Notepad

14. View the size of myfile.txt (only type what's in **bold**):

#### C:\WINDOWS\system32>**dir myfile.txt**

15. Record the file size:

16. Then type (only type what's in **bold**):

#### C:\WINDOWS\system32>notepad myfile.txt:hidden.txt

17. Click Yes to create the new file called *myfile.txt:hidden.txt* 

Syntax breakdown: **notepad**: program name **myfile.txt:hidden.txt**: hide myfile.txt into the stream called hidden.txt

- 18. Type 20 lines worth of text into this file
- 19. Save the file and exit from Notepad
- 20. View the size of myfile.txt (only type what's in **bold**):
- C:\WINDOWS\system32>dir myfile.txt
- 21. Record the file size:
- 22. Compare the file sizes in step #8 and step #14. They should be the same
- 23. The information you typed into the *myfile.txt:hidden.txt* file (20 lines worth of information) is hidden in *myfile.txt*
- 24. To view the hidden text again, type (only type what's in **bold**):

#### C:\WINDOWS\system32>notepad myfile.txt:hidden.txt

25. Leave your Windows command shell open for the next exercise

**Exercise 2: hiding nc.exe using an ADS**: in the following exercise, you will rename and hide the nc.exe on the victim Windows server within another file using an ADS:

1. View the size of calc.exe (only type what's in **bold**):

C:\WINDOWS\system32>dir calc.exe

- 2. Record the file size:
- 3. At your Windows command shell type (only type what's in **bold**, on one line):

C:\WINDOWS\system32>type nc.exe > calc.exe:svchost.exe

Syntax breakdown:

type: program name

**nc.exe > calc.exe:svchost.exe**: put nc.exe in calc.exe and change the file name from nc.exe to the more common process called svchost.exe (which may help in it being overlooked by an unsuspecting administrator)

4. View the size of calc.exe (only type what's in **bold**):

#### C:\WINDOWS\system32>**dir calc.exe**

- 5. Record the file size:
- 6. Compare the file sizes in step #2 and step #5. They should be the same
- 6. Open Windows Calculator to make sure the program has not been altered in any way (only type what's in **bold**):

### C:\WINDOWS\system32>calc.exe

7. Close Windows Calculator

# **ARP Poison Routing Using Cain**

The Cain tool for Microsoft operating systems does an excellent job of performing ARP Cache Poisoning attacks. It enables sniffing on switched networks and the hijacking of IP traffic between hosts. The name derives from the two steps needed to perform such unusual network sniffing: an ARP Poison Attack and routing packets to the correct destination.

What allows this attack to work is a weakness in how ARP handles out-of-band ARP replies. That is, an attacker can send an ARP reply to a host that never sent an ARP request. The receiving host happily updates its ARP cache with the bogus ARP reply entry. The attacker continues in this fashion for each host he wants to compromise:

**Step #1**: out-of-band ARP reply from attacker to FTP server with your IP address mapped to the attacker's MAC address

**Step #2**: out-of-band ARP reply from attacker to your PC with FTP server's IP address mapped to the attacker's MAC address

Step #3: ARP caches on both systems are poisoned

**Step#4**: watch for traffic of interest

**Exercise 1: ARP Poison Routing using Cain**: in this exercise, you will use Cain to perform an ARP Poison Routing attack:

1. Open Cain. The main Cain window appears:

dill						
File View C	onfigure Tools He	elp				
🖻 🏟 🕹 🕇	🥹 😼 B	8) 🚥 📟 🎌 🖪	🖬 🏧 🖬 🔁	à 😵 🧶 🖄	<b>i ? ()</b>	
💣 Protected Storage	🔮 Network 🛙	🎒 Sniffer 🏾 🎒 LSA S	Secrets 🥑 Cracke	r 🔯 Traceroute	🔣 🛄 CCDU 🕅 Wirele	ss
ress the + button on the	toolbar to dump the	Protected Storage				

2. Click on the Sniffer tab:

File Vie	ew Configure Tool	s Help										
🛛 🛥 🔹 💀 n												
\& Decoders 🖇	Decoders 🔮 Network 🏟 Sniffer 🥑 Cracker 🔕 Traceroute 🔝 CCDU 😵 Wireless 🚯 Query											
IP address	MAC address	OUI fingerprint		Host name		B31	B16 B	38 Gr	MO	M1	MЗ	
📃 Hosts 😽 AF	PR 🕂 Routing	🚯 Passwords	🔏 VoIP									
http://www.oxid.it												

3. Click the Start/Stop Sniffer icon (2<sup>nd</sup> from left in toolbar):

Ξ aíŋ							
File Vie	w Configure Too	ls Help					
🛛 🖻 🙀 😔 yi	CHALL CHALL LM SPODF SPODF JTH RESET NTLN	🖣 🦭 🐱 🖥	🔊 🚥 📟 🚾 📼 🤇	3 🙆 🚺 ?	1		
🔔 Decoders 💡	👌 Network 🛯 🏟 S	öniffer 🥑 Cracker	🔇 Traceroute 🔝 CCDU	🕅 Wireless 🚯 🤅	Query		
IP address	MAC address	OUI fingerprint	Host name	B31 B16	B8 Gr	M0 M1	M3
_		-					
📙 Hosts 🛛 😽 AF	PR 🕂 Routing	💦 Passwords	🔏 VoIP				
Lost packets: 0%							

- 4. Make sure the Hosts tab on the bottom-left of the Sniffer window is selected
- 5. Click the blue + sign (Add to list):

File View Configure Tools Help	
S 🔹 🕹 🚓 🎬 🛗 🕂 🕹 🐼 🛤	📟 🖻 🚍 🛠 💈 🊯 👔
🖉 📴 Decoders 🔮 Network 🏟 Sniffer 🥑 Cracker 🔕 T	MAC Address Scanner
IP address MAC address OUI fingerprint	Target B8 Gr M0 M1 M3   C Range Form Image: Construction of the state
📃 Hosts 🚱 APR 🕂 Routing 🕅 Passwords 🔏 VoIP Lost packets: 0%	

6. Click OK to build the list of all hosts in the LAN:

File Vie	w Configure Too	ls Help										
🛛 🛥 🐼 🐼 🕺	LM SPOOF SPOOF	• 🥡 😺 🖥	🔊 🌆 🔛	. 🛯 🖬	🥵 🙋 🛛	01	<b>ا</b>	Ī.				
Decoders	👌 Network 🛛 🏟 S	iniffer 🥑 Cracker	🛛 🔯 Tracer	oute 🔝 CCDU	👋 Wirele	ss	🏠 Qu	iery				
IP address	MAC address	OUI fingerprint		Host name		B31	B16	B8	Gr 🛛	M0 M1	M3	
172.30.30.2	000C292AED17	VMware, Inc.										
172.30.30.1	000C294DDF1D	VMware, Inc.										
		@	<i>Q</i>									
📇 Hosts 🛛 🔂 AF	'R 🕂 Routing	Passwords	🏈 VoIP									
Lost packets: 0%												

7. Click the ARP tab on the bottom-left of the Sniffer window:

File View Configu	ire Tools Help										
🔄 🏟 🚱 NTLM SPORT SP	if 🛛 🕂 🎯 🛛 🗄	🗟 📴 🚱 🐻	📟 🔀 🔤 🧲	9 🕵 💋	0 ? .	<u>n</u>					
🔔 Decoders 🔮 Network	🏂 Decoders 🔮 Network 🏟 Sniffer 🥑 Cracker 🙋 Traceroute 🛄 CCDU % Wireless 🚯 Query										
APR Cont	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address				
APR-Cert											
APR-SSH-1 (0)											
APR-HTTPS (U)											
APR-FTPS (0)											
APR-POP35 (0)											
APR-LDAPS (0)											
	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address				
	Configurati	on / Routed Packets									
			I								
Hosts 🔂 APR 🕂 Ro	outing 🎢 Passv	vords 🌠 🌠 VoIP									
Lost packets: 0%								1.			

- 8. Click in the empty white space in the top-right window pane
- 9. Click the blue + sign

10. Select one system on the left to hijack and a second on the right to hijack:

File View Configure Tools	Help										
🔄 🚳 📀 xữm được sựng 🖌											
🙈 Decoders 🔮 Network 🏟 Sni	iffer 🥑 Cracker 🔕 Tr	aceroute 🔝 CCDU 💖	Wireless 🚯 Q	uery							
APR Status	IP address	MAC address Packets	-> <- Packets	MAC address IF	P address						
APR-Cert											
APR-55H-1 (0)	New ARP Poison Routing										
APR-HTTPS (0)			RNING !!!								
APR-FTPS (0)	APR enables you to hijack I	P traffic between the selected H	nost on the left list an	d all selected hosts on th	ne right list in both						
APR-POP35 (0)	directions. If a selected host machine has not the same p	has routing capabilities WAN t erformance of a router you cou	affic will be intercept Id cause DoS if you :	ted as well. Please note I set APR between your D	that since your refault Gateway and						
APR-LDAPS (0)	all other hosts on your LAN.										
Status											
	IP address MAC	Hostname	IP address	MAC	Hostname						
	172.30.30.2 000C29 172.30.30.1 000C29	IZAED17	172.30.30.2	000C292AED17							
	172.30.30.1 000020	400110									
<u>.</u>	<		<		>						
📙 Hosts 👶 APR 🕂 Routing				OK	Cancel						
Lost packets: 0%						1.					

11. Click OK (this is pre-ARP Poison attack - notice the *Idle* status):

Ξ aíŋ											
File View Configu	ure Tools Help										
🔄 😰 🚱 MÌM REEF AN	H 🕂 🐨 🛙	B B 10 III	📟 🔀 🖬 🧲	3 🕵 💋	0 ?	1.					
Decoders 🔮 Network	🏂 Decoders 🔮 Network 🎒 Sniffer 🥑 Cracker 🙋 Traceroute 🔝 CCDU % Wireless 🔂 Query										
APR	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address				
- S APR-Cert - ♣ APR-CNS - ■ APR-SSH-1 (0) - ♣ APR-RDP (0) - ♣ APR-RDP (0) - ♣ APR-FUTS (0) - ♣ APR-POP35 (0) - ♣ APR-IMAPS (0) - ♣ APR-IMAPS (0)	ي الم	172.30.30.1	000C294DDF1D			000C292AED17	172.30.30.2				
APR-LUAPS (U)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address				
	😞 Configurati	on / Routed Packets									
📕 Hosts 😽 APR 🕂 R	, outing 💦 Passw	vords 🔏 VoIP									
Lost packets: 0%								la l			

12. Click the yellow nuclear icon (next to the Sniffer icon in main toolbar). The ARP Poison attack is under way):

Ζ										
File View Configu	ure Tools Help									
	li 🛛 🕂 🕑 🛛	8 B <sub>64</sub> 🕙 🛤	I 📟 🔀 📼 🧲	9 😻 💋	0 ?	1				
🎉 Decoders 🦉 Network 🏟 Sniffer 🥑 Cracker 🙋 Traceroute 🛄 CCDU 💖 Wireless 🔂 Query										
🔂 APR	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address			
APR-Cert	🖧 Poisoning	172.30.30.1	000C294DDF1D	36	36	000C292AED17	172.30.30.2			
APR-SSH-1 (0)										
APR-HTTPS (0)										
APR-FIPS (U)										
APR-IMAPS (0)										
APR-LDAPS (0)	l	1				1				
	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address			
						1	1			
	Configurati	on / Routed Packets								
📃 Hosts 🜏 APR 💠 Ri	outing 👫 Passv	vords 🔏 VoIP								
Lost packets: 0%								11		

13. After verifying that each host's ARP cache has been hijacked and the values have been replaced w/those of the attacker's MAC address, click the Passwords tab on the bottom-right of the Sniffer window:

αίη											
File View Configu	re Tools Help										
🙈 Decoders 🔮 Network	🙀 Sniffer 🥑 Cracke	r 🔕 Traceroute	🔜 CCDU  🎇	Wireless 🚯 Q	uery						
Resswords	Timestamp	SMB server	Client	Username	Domain	Password	AuthType	LM Hash			
- 🙅 FTP (0)											
BO LDAD (0)											
- DAF (0)											
Telnet (0)											
NNTP (0)											
(7) MSKerb5-PreAuth (0)											
- 📕 Radius-Keys (0)											
Radius-Users (0)											
SNMR (0)											
SIP (0)											
- 🖉 GRE/PPP (0)											
🗇 PPPoE (0)											
					)			2			
	side ZWB										
📕 Hosts 🚯 APR 💠 Ro	outing 👫 Passwords	🔏 VoIP									
Lost packets: 0%								1.			

14. Have *Your PC* user FTP into the *FTP server* (or a system of choice) and watch Cain grab the logon credentials:

File View Configu	re Tools Help				
	⊯ <b>│+</b>	. 🕙 🚥 📟 [		2 Ø ?	<u> </u>
😤 Decoders 🦉 Network	📲 Sniffer 🥑 Cracke	r 🔯 Traceroute	CCDU 🌋	Wireless 🚯 🤇	Query
Reasswords	Timestamp	FTP server	Client	Username	Password
→   →     →   HTAP (0)     →   POP3 (0)     →   POP3 (0)     →   SM8 (0)     →   Tehet (0)     →   Toba (0)     →   Radius-Keys (0)     →   Toba (0)     →   Toba (0)     →   Toba (0)     →   SIMP (0)     →   SIP (0)     →   SRE/PPP (0)     →   PPPoE (0)	12/05/2009 - 20:04:52			anonymous	thisispasswords
📕 Hosts 🛛 APR 🕂 Ro Lost packets: 0%	puting 💦 Passwords	🏀 VoIP			

15. To clean up and have the ARP cache entries on the victim system's restored to their correct values, click the yellow nuclear icon (next to the Sniffer icon in the

main toolbar) to stop the ARP Poison attack and click the Sniffer icon to stop sniffing traffic on the LAN

16. Go to hosts and verify they have the correct IP-to-MAC address mappings