Cain and Able A disturbing Tutorial



Questions? <u>muts@mutsonline.com</u> <u>http://mutsonline.com</u>

Cain and Able – The Terror begins

DESCRIPTION

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary & Brute-Force attacks, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

It also has ARP poisoning and spoofing capabilities, making it into an <u>extremely</u> powerful hacking or auditing tool. The ARP spoofing feature works in a similar way as described in the "ARP Spoofing" tutorial. Indeed it would be wise to read that tutorial before attempting to use Cain.

Environment

 Install and run Cain. Immediately when it opens you can see the first disturbing scene. All the cached passwords are shown in the "Protected Storage" tab. These include passwords from IE, Outlook or other HTTP transactions.

File View Configure Tools Help			
🔹 🕹 🕇 😜 🗟 🗇 😤 💠	≓ ₽ ₆₄ 🕙 🔤	🚾 🖚 (- C 0 i
📸 Protected Storage 🔮 Network 🎲 Sniffe	er 🥑 Cracker (🧕 Traceroute	
Resource	Username	Password	Туре
Rain.inter.net.il	muts		Outlook Express POP3 Account
🕗 http://192.168.1.22/	muts		Internet Explorer Form Autocomplete
http://192.168.1.22/error.php	muts		Internet Explorer Form Autocomplete
🕗 http://192.168.1.22/index.php	muts		Internet Explorer Form Autocomplete
🕗 http://192.168.1.22/test/html/index.php	muts +		Internet Explorer Form Autocomplete
🕗 http://192.168.1.22/user.php	muts		Internet Explorer Form Autocomplete
🕗 http://goldmail.zahav.net.il/	muts		Internet Explorer Form Autocomplete
🐔 http://gonext.pelephone.co.il/pelefun/login.asp 👘			Internet Explorer Form Autocomplete

2. The "Network" tab is a scaled enumeration system, able of enumerating all Windows computers it can find on the local network.

File View Configure Tools He	lp		<u> </u>					
🎒 Protected Storage 🔮 Network 🙀 Sniffer 🦪 Cracker 🔕 Traceroute								
🔮 Entire Network 📃	Group	Comment	SID					
icrosoft Windows Network المحمد الم	M None	Ordinary users	5-1-5-21-1644491937-1960408961					
	Administrators	Administrators have	5-1-5-32-544					
All Computers	Backup Oper	Backup Operators c	5-1-5-32-551					
ADSERVER	🚾 Guests	Guests have the sa	5-1-5-32-546					
	🚾 Power Users	Power Users posses	5-1-5-32-547					
	2 Replicator	Supports file replica	S-1-5-32-552					
Browsers	🗳 Users	Users are prevente	S-1-5-32-545					
Dial-In Servers								
Domain Controllers								
- 👰 Novell Servers								
Printer Servers								
- 🔂 SQL Servers								
Time Servers								
All Computers								
Services								
Shares								
🖸 Users								

 The most interesting (IMHO) feature of Cain is in the "Sniffer" Tab. Cain allows you to ARPSpoof, Sniff and Brute force passwords all via one interface. Notice that the "Sniffer Tab" has 5 sub-tabs - Hosts, APR, DNS Spoofer, Routing and Passwords.

📃 Hosts 🛛 🔂 APR	2 DNS Spoofer	🕂 Routing	🚯 Passwords
-----------------	---------------	-----------	-------------

We will discuss Cain's functionality as an ARP-Spoofer only.

File Vie	w Configure Tool	s Help		_ 🗆	×			
 ♠ ↔ +	🔹 🕹 🕂 🦭 🗟 🥪 롲 💠 🛱 🧞 🐑 🚥 🚾 🚾 🗂 🧿 🗘							
💣 Protected Stor	rage 🧕 🔮 Netwo	rk 🙀 Sniffer 🥑 Cracker	🔇 Traceroute					
IP address	MAC address	OUI fingerprint	Host name	B31	B1			
192.168.1.1 192.168.1.22	0020188A1278 0002B38E307F	CIS TECHNOLOGY INC. Intel Corporation						
192.168.1.32	000629256047	IBM CORPORATION						
192.168.1.138	0090D023D4E6	ALCATEL BELL						
•	1				F			
📃 Hosts 😽 AF	PR 🚉 DNS Spoo	fer 🕂 Routing 👫 Passw	vords					
Cain v2.5 beta26 by	mao				1			

- 4. To start ARP Spoofing, you need to activate the sniffing daemon and the APR daemon. You do this by clicking on both the "Sniff" and "APR" buttons at the top of the window ().
- 5. Make sure you are in the "Sniffer" tab, and right click anywhere inside the tab. You should see a "Scan MAC addresses" option. Click it.

File Vie	w Configure Tools Help	
💣 Protected Stor	rage 💡 Network 🏟 Sniffer 🥑 Cracker	🔯 Tracerou
IP address	MAC address OUI fingerprint	Host name
	Scan MAC Addresses	
	Resolve Host Name	
	Remove Delete	
	Clear Promiscuous-Mode Results	
	Export	

6. Choose the appropriate IP range that suits your local network and click "Ok".

MAC Address Scanner	×
_ Target	
C All hosts in my subnet	
Range	
From	
192 . 168 . 1 . 1	
То	
192 . 168 . 1 . 254	
Promiscuous-Mode Scanner ARP Test (Broadcast 31-bit) ARP Test (Broadcast 16-bit) ARP Test (Broadcast 8-bit) ARP Test (Group bit) ARP Test (Group bit) ARP Test (Multicast group 0) ARP Test (Multicast group 1) ARP Test (Multicast group 3) All Tests	
OK Cancel	

7. A quick scan should occur, giving you all the MAC addresses present in that subnet.

File Vie	w Configure Too	ls Help		
🕼 😔 🕇 🕇	I .	╤ � ☴ ¤, ∿ ₪	M 💷 🚾 🏧 🔲	0 1
💣 🛛 Protected Stor	rage 🔮 Netwo	rk 🙀 Sniffer 🥑 Cracker	🔇 Traceroute	
IP address	MAC address	OUI fingerprint	Host name	B31
192.168.1.1	0020188A1278	CIS TECHNOLOGY INC.		
192.168.1.22	0002B38E307F	Intel Corporation		
192.168.1.32	000629256047	IBM CORPORATION		
192.168.1.97	000255686172	IBM Corporation		
192.168.1.138	0090D023D4E6	ALCATEL BELL		
	So	anning MAC addresses [74	%]	
		Current Host:		-
	I	192.168.1.187		
				Iancel
		1		

- Once the scan is complete, move to the APR sub-tab at the bottom of the window (APR). This is the window in which you choose the computers you want to attack. Now click on the blue "plus" sign at the top of the windows to add hosts to attack.
- 9. You should get the following screen:

Ne	w ARP Poison Routing							
	WARNING !!!							
	APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted also. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.							
	IP address	MAC		IP address	MAC			
	192.168.1.1 0020188A1278 192.168.1.32 000629256047							
	192.168.1.22 0002B38E307F 192.168.1.22 0002B38E307F							
	192.168.1.132	000623236047 0090D023D4E6		132.100.1.1	UUZU100A1278			

Here you choose the hosts which you want to route traffic through your computer. A default Gateway, or a Domain controller are good endpoints to choose between the attacked host. 10. Now we wait for the attacked host to enter password data to services such as FTP, HTTP, POP3, IMAP, and lots of others. In the following screenshot, an FTP password was intercepted.

File	View Configure T	ools Help				_ 🗆 >
🔹 📀 🛛 -	• 🕲 😼 🤇	ୖ │ ⊋│ ₽	B ₆₄ 🐑	alifa. Ialifa. 🚾	*** 🖬 🗖	0 i
🕉 Protected S	Storage 🛛 🔮 Net	work 🙀 Sniffer	🥑 Cracker	🔯 Tracero	ute	
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.1.138	0090D023D4E6			000629256047	192.168.1.32
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.1.32	000629256047	8	7	0090D023D4E6	194.90.1.6
🖳 Hosts 🛛 🕰	APR 🚉 DNS Sc	poofer 🔂 Routin	g 🚯 Pass	words		
est packets: 0%	, 1		- 1			

11. We can see that the FTP session between 192.168.1.32 (Attacked Computer) and 194.90.1.6 (Netvision's FTP server) was router via our computer. Now click on the "Passwords" Passwords)and you will see the captured passwords.

File View Configu	ire Tools Help				
 🚱 + 🗞 R		B ₆₄ 🐑 🌆 🖩		d 🧿 🗖	
💣 Protected Storage 🔮	Network 🙀 Sniffer 🍯	🖌 Cracker [🔕	Traceroute		
💦 Passwords	Timestamp	FTP server	Client	Username	Password
Passwords	Timestamp 25/02/2003 - 17:50:34	FTP server 194.90.1.6	Client 192.168.1.32	Username myuser	Password mypassword
Passwords Provide FTP (1) Provide HTTP (0)	Timestamp 25/02/2003 - 17:50:34	FTP server 194.90.1.6	Client 192.168.1.32	Username myuser	Password mypassword
Passwords PIP (1) PIP (1) P	Timestamp 25/02/2003 - 17:50:34	FTP server 194.90.1.6	Client 192.168.1.32	Username myuser	Password mypassword
Passwords PTP (1) HTTP (0) IMAP (0) POP3 (0)	Timestamp 25/02/2003 - 17:50:34	FTP server 194.90.1.6	Client 192.168.1.32	Username myuser	Password mypassword

12. For encrypted passwords such as SMB (NTLM in it's various flavours) you can send the password to a Brute Force session.

File View Configu	ire Tools He	lp					
😰 🕹 🕂 😵 🐼 菜 💠 ☴ 🧏 🐿 🚥 🚥 🖻 📼 🚺 🚺							
💣 Protected Storage 🔮	Network 📓	🔋 Sniffer 🥑	Cracker 🔯	Traceroute	•		
💦 Passwords	SMB server	Client	Username	Password	AuthType	LM Hash	
- 😋 FTP (1)	192.168.1.1	192.168.1.32	iris		LM & NTLMv1 (NTLMSSP)	B5EA94B	
	192.168.1.1	192.168.1.32	administrator		I M & NITI MUL (NITI MSSD)	DA0FA65	
					Send to Cracker		
• POP3 (0)					Send All to Cracker		
5MB (2)					Remove		
Telpet (0)					Remove All		

13. After sending the password to the cracker, click on the "Cracker" tab and start the required attack.

File View Configure Tools Help Image: Solution of the state o				
Creater	Network	Cracker 🔯 In		[
	User Name	Lanman Pass	< 8 NI Password	Lanman Hash
IM & NT Hashes	MUTSONLINE\administrator			LDA0FA65DDFB
NTLMv2 Hashes	Start Dictionary Attack			
🖳 🧟 PWL files		Start Brute-Force Attack		
Cisco IOS-MD5 Hast				
Cisco PIX-MD5 Hast		Drop Attack		
		Test nassword		
		Delete regume info		
OSPF-MD5 Hashes		Add to list	Insert	
RIPv2-MD5 Hashes		Demous	Delote	
VRRP-HMAC Hashes		Remove	Delete	,
VNC 3DES		Remove All		
MD2 Hashes	1	Evport		
MD4 Hashes		Export		
· ·				

This was a quick tutorial about Cain's ARP Spoofing ability. Apart from ARP Spoofing Cain can do lots of other wonderful things, just take time to *carefully* learn the application.

Scary eh? 😳