# Cain & Abel v 2.5

Password Cracking Via ARP Cache Poisoning Attacks

v.1

File View Cor	ifigure Tools Help		s) 🕅 🖬 🛲 📾 🦱 🗞 🕫 3	
Protected Storage	🖉 Network 🙀	+ →   64 ) Sniffer 🚮 LSA	A Secrets 🧭 Cracker 🔯 Traceroute	CCDU Wireless
Resource	Username	Password	Туре	
n v2.5 beta56 by mao				

2004

# Objective:

At the end of this lab students will be able to use the password auditing and ARP Poison Routing (APR) features of Cain & Abel.

# Background Information:

The Cain & Abel password recovery tool for Microsoft Operating Systems allows recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force, Cryptanalysis attacks, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. There is a version for Windows 98 and a NT2000/XP version with more features that will be used in this lab.

Where Cain is the main analysis tool, the Abel NT service provides a remote console on the target machine, which can dump user hashes from the remote SAM even if it was encrypted using the "Syskey" utility and other features like the LSA Secrets dumper, the route table manager and the TCP/UDP Table Viewer.

An interesting feature of Cain & Abel is APR (ARP Poison Routing) which enables sniffing on switched LANs by hijacking IP traffic of multiple hosts at the same time. The sniffer can also analyze encrypted protocols such as SSH-1 and HTTPS if used with APR and a Man-in-the-middle situation. Cain also comes with routing protocol authentication monitors, route extractors, crackers for all common hashing algorithms and for other various specific authentications, password calculators (Cisco PIX Hashes, RSA SecurID Tokens), decoders (Access Databases, Base64, Cisco Type-7, Enterprise Manager, Dialup, Remote Desktop) Cisco Config Downloader/Uploader, SiD-Scanner, LSA Secrets Dumper, Protected Storage Passwords Viewer, NT Hash-Dumper, Abel Remote Console, MAC Scanner, Promiscuous-Mode Scanner, Wireless Scanner, and TCP/UDP/ICMP Traceroute + DNS Resolver + Netmask Discovery + WHOIS resolver.

The current version of Cain & Abel is limited to use on the same physical network segment. Switched segments work fine, however remote sniffing is not enabled at this time. It will work on wireless networks as well with select supported NIC's. WEP cracking is in progress but not completed as of 8/15/04.

Network administrators as well as hackers will find uses for this software. A network administrator might use the password cracking feature to audit a

system for weak or non-existent passwords. By the same token, a hacker could gain illicit entry into a system this way. The remote control features of Cain & Abel allow for activities such as these to be carried out from a different location on the network. APR could be used to examine traffic to and from a remote computer on a switched network for auditing or nefarious purposes. Other features are available, but these are but a few of the possible good and bad uses of Cain & Abel. At the least, security personal should have a working knowledge of what this package does and how it can be used.

Oxid.it is the website for Massimiliano Montoro (<u>mao@oxid.it</u>) <u>http://www.oxid.it.</u> He has many free software tools available, including Cain & Abel.

For this lab, you will install Cain & Abel and the packet capture driver WinPcap, utilize the Windows password cracking feature of Cain & Abel, utilize MAC address discovery feature, and implement APR on a selected MAC address that was discovered on the network. Lastly, you will examine traffic from the target machine with Ethereal, a protocol analyzer.

## Student Preparation:

The student will have completed required reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

## Instructor Preparation:

Before class, the instructor or a lab assistant will ensure that Cain & Abel 2.5 or newer, WinPcap, Ethereal .10.5a or newer, and tcpdump are installed and operational on the Windows 2000 or higher workstations and targets. Each student will need a workstation and target machine on the same switched LAN. Students will need administrator rights on both machines.

During class the instructor will discuss the function of Cain & Abel utility for password analysis and APR via ARP cache poisioning. Students will then demonstrate use of both features individually.

## Warnings:

Use of the APR capability could cause Denial of Service on some networks, so as such this feature should be used on non-production networks only! Also, care must be exercised when auditing passwords as some may view this as illegal activity and frown on its use. As such, these are powerful, professional tools and such be used as a professional.

# Estimated Completion Time

90 minutes

# Password auditing and recovery and ARP Poison Routing lab

# Cain & Abel 2.5

Cain & Abel is a password auditing and recovery tool that offers ease of installation and use. It is also very powerful and as such is a tool any IT professional would want in there repertoire.

# To install:

- 1) Download and install Cain & Abel from <a href="http://www.oxid.it/cain.html">http://www.oxid.it/cain.html</a>
- 2) Install software and WinPcap packet capture driver
- 3) Reboot computer.
- 4) Download and install Ethereal from <a href="http://www.ethereal.com/">http://www.ethereal.com/</a>
- 5) Reboot computer.

Use: To find protected storage information/passwords that have been saved in the system registry such as from Outlook, Outlook Express, MSN, Internet Explorer (IE), autocomplete and form information, ebay username and password, etc. Note: autocomplete must be enabled and passwords must be saved via IE.

Starting with version 4.0, Microsoft's Internet Explorer may save everything that you ever type into a form. When you use a similarly named field on another form, it automatically provides you with a selection of previous data. This is stored in the registry and is based on a unique security identifier (SID).

- 1) Start Cain
- 2) Click blue + icon on the upper left, note username (ID) and Password and URL of resource it was saved for on the Protected Storage tab.

File View Con	ifigure Tools Help			
	😼 🥥 롲		🔊 🚾 🚾 Free 📾 💼 🐞 🧐 🔌	
Resource	Username	Password	Type	
www.waldenu.edu/Fa	smith123 smith123	mypasswd12 mypasswd12	Internet Explorer Protected Sites Internet Explorer Protected Sites	

3) To save information from any of the Protected Storage sites:

- a. Click on one of the resources
- b. Right click and select Export
- c. Key in name such as resc1.txt
- d. Now, open file using notepad or similar text editor

4) To delete entry, left click on item, select either Remove or Remove All.

To find Windows login ID and passwords on a local machine.

- Create three users on your local machine. Make the accounts as follows: user1 with password of password, user2 with password of 1password1, and user 2 with password of 123xyz321. Now proceed to #1 below. With the different passwords selected, you will be able to examine how password difficulty affects auditing and cracking techniques.
- 1) Click on Cracker tab
- 2) Click on LM & NTLM Hashes
- 3) Click on + sign icon on toolbar then Dump NT Hashes from Local machine. \* Note, if you have a SAM file from an NT/win2k/XP machine you can also use the import option to import from that. \*See bottom of lab on remote installation of Abel to see how you might gain access to a SAM file from a remote PC.
- 4) Click Next
- 5) On Guest id, right click and select dictionary attack NTLM. Select Add, then browse to where cain is installed (possibly in c:\program\files\cain) Then select wordlists folder and wordlist.txt. Then click Start.
- 6) Note options such as As is Password, etc. Also note that you could use a Brute force attack if you had no luck on a dictionary word from a list file. However, this would take much longer.

Ele View Configu Sele View Configu Sele View Configu Protected Storage	ure Tools Help 실 :	🔓 🕥 🛲 🚾	F*** 📾 💽 🏠 🤇 7 Cracker 🔯 Trace	🕄 🧶 🚺 🧘	
Cracker	User Name	LM Password	< 8 NT Password	LM Hash	NT Hash
INTLMV2 Hashes (0)           WL files (0)           Image: Cisco IOS-MD5 Hashes           Image: Cisco PIX-MD5 Hashes <t< td=""><td>Guest HelpAssistant LNSS_MONITOR_USR SUPPORT_388945a0</td><td>* empty * * empty *</td><td></td><td>E52CAC67419A 2CF081EFA79E AAD3B435B514 AAD3B435B514</td><td>8846F7EAEE8F 475D90691DDB FCB359C5BBA2 671B05D602D4</td></t<>	Guest HelpAssistant LNSS_MONITOR_USR SUPPORT_388945a0	* empty * * empty *		E52CAC67419A 2CF081EFA79E AAD3B435B514 AAD3B435B514	8846F7EAEE8F 475D90691DDB FCB359C5BBA2 671B05D602D4
<ul> <li>SHA-1 Hashes (0)</li> <li>RIPEMD-160 Hashes (0)</li> <li>Kerb5 PreAuth Hashes (0)</li> <li>IKE-PSK Hashes (0)</li> <li>MSSQL Hashes (0)</li> <li>MySQL Hashes (0)</li> </ul>	LM & NTLM Hashes				

Using APR - ARP Poison Routing.

**Theory** -- On an Ethernet/IP network, when host A wants to send a packet to host B, it must know the MAC or physical address of the machine and IP address. It also needs to know the application layer protocol (IP) address, but the physical MAC is required for construction of the Ethernet frame. Review the OSI model if you are unclear on these concepts. In short we have to have both.

Once it knows the MAC's of the machines on the network, it keeps them stored in an ARP cache table. However, before it can "know" it has to query the network to find out the addresses. A host does this by sending out an ARP request on broadcast to FFFFFFFFF. Only the station with the specified IP will reply in unicast with an ARP reply packet to the requesting station with it's MAC. Now host A has an updated table entry for host B and it will communicate now in unicast directly to it by using the MAC of B in the Ethernet frame. ARP request and reply packets are only sent if the host doesn't know the destination machines MAC. Again, once it is learned the cache is used....this is a key point to why APR works. How APR works - ARP Poison Routing uses the stored cache as a way to reroute or re-direct packets from a target, to an intermediary machine, then forward to the host, thus the middle machine "sees" all traffic between target and host, even if on a switched LAN. First the target MAC address must be established, then the APR feature "poisons" the cache of the target by forcing a cache update with the path re-routed so that the middle machine forwards traffic to and from host and target. The middle machine can now examine packets with a sniffer such as Ethereal, Nmap, or others.

## Instructions to use APR:

<u>\*\* Before you try this, you must make sure that WinPcap is properly bound to</u> <u>your NIC. Select Configure and make sure you see your adapter(s) listed</u>. See illustration *c1*.

- 🕑 😼 🚽	Configuration Dialog			
torage 👰 Neti	Sniffer APR ( Arp Poison Routin	ng)   Traceroute	1	
MAC address	Adapter	IP address	Subnet Mas 🔨	B
	Device\NPF_{4FDBD3	0.0.0	255.0.0.0	1
	Device\NPF_{01FF6A5	192.168.123.121	255.255.25!	
	Device\NPF_{475A90F	192.168.123.157	255.255.25!	
	<		>	
	\Device\NPF_GenericNdisW	'an Adapter		
	WARNING !!! Only e	ethemet adapters sup	ported	
	Options			-
	Start Sniffer on startup			
	Start APR on startup			
	Password Collectors	> Filters		-
	Routing Protocols Analysis	8	-	
	No.			

C1.

At main screen, select Configure, then click your your network adapter, then Apply and Ok.

1) Click to enable both Sniffer and APR (Left of the + ). See Illustration c2.



С2.

- 3) Click on +, then Range. Range for your network (based on adapter you chose) is displayed. Click OK to start scanning.
- 4) After 100% you will see IP address, MAC, and OUI fingerprint of devices in range.
- 5) Now click on APR icon to enable it.
- 6) Click on + and select IP address to poison, then OK
- 7) Now you should see it change from Idle to Poisoning. See C3.

Protected St	torage 👰 Netwo	ork	LSA Secr	ets 🥑 Cr	acker 🔯 Tracer	oute	Wireless
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
Poisoning	192, 168, 123, 101	0002E3020804	0	0	005018051A96	192. 168. 123. 254	
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
Half-routing	192, 168, 123, 101	0002E3020804	1	0	005018051A96	24.20.196.101	(
Half-routing	192.168.123.101	0002E3020804	1	0	005018051A96	24.210.164.52	
Full-routing	192.168.123.101	0002E3020804	1	2	005018051A96	196.31, 185, 224	
Half-routing	192.168.123.101	0002E3020804	1	0	005018051A96	66.74.184.171	
Half-routing	192, 168, 123, 101	0002E3020804	1	0	005018051A96	81.76.110.219	
Full-routing	68.75.91.129	005018051A96	16	8	0002E3020804	192.168.123.101	
Full-routing	192, 168, 123, 101	0002E3020804	5	4	005018051A96	67.175.20.179	

C3.

- 8) IP connections should appear from target and spoofing computer(your computer).
- 9) So, what we have now, looking at C3, is the target IP on the left, where they were going on the right. All of this passing harmlessly through the middle PC.
- 10) For better analysis of this traffic, and perhaps text strings that have been sent from the target, etc. (e.g. They connected to Google, but what did they search for?) We will run a sniffer on the middle computer.
- 11) Start Ethereal, select Capture, then select the same interface adapter you selected in Cain. Then select OK. You are trying to capture the packets being forwarded to and from your machine via ARP session.
- 12) Stop the capture after connecting to google and searching for items such as "vacation villas", or "cheap air fare". Your machine is now analyzing the traffic from a target as all of its traffic is rerouted through yours. Note in Figure C4 we see all traffic listed in the top window of Ethereal (examine that we see our connection to Google).

	0,				
Eile	<u>E</u> dit <u>Vi</u> ew <u>G</u> o <u>C</u> a	apture <u>A</u> nalyze <u>S</u> tatistics <u>H</u>	elp		
	🗀 🗔 🗙	re 🔁 🔄 🗢	🗣   🍄 🏹 👱   🤆		, 🕪 🗓 🖽 💥 🔯
Ð	ilter:		•	Expression	💩 <u>C</u> lear 🖋 <u>А</u> рріу
No, .	Time	Source	Destination	Protocol	Info
	1 0.000000	192.168.123.254	192.168.123.157	ARP	192.168.123.254 is at 00:50:18:05:1a:96
	2 0.000184	192.168.123.157	24.25.35.64	DNS	Standard query AAAA www.google.com
	3 0.025369	24.25.35.64	192.168.123.157	DNS	Standard query response CNAME www.google.akadns
	4 0.200055	192.168.123.157	24.25.35.64	DNS	Standard query A www.google.com
	5 0.216859	24.25.35.64	192.168.123.157	DNS	Standard query response CNAME www.google.akadns
	6 0.222616	192.168.123.157	216.239.41.104	TCP	4974 > http [SYN] Seq=0 Ack=0 Win=64240 Len=0 M
	7 0.265420	216.239.41.104	192.168.123.157	TCP	http > 4974 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len
	8 0.265815	192.168.123.157	216.239.41.104	TCP	4974 > http [ACK] Seq=1 Ack=1 Win=64896 Len=0
	9 0.266668	192.168.123.157	216.239.41.104	HTTP	GET / HTTP/1.1
	10 0.313124	216.239.41.104	192.168.123.157	HTTP	HTTP/1.1 200 OK (text/html)
	<b>~</b> /				

Figure C4.

13)Click the Protocol field to organize the list, then scroll down to HTTP and look for GET /search? Here we see in Figure C5 that the user was searching on vacation villas (vacation+villa).

D	Eilter:			Expression	💩 <u>C</u> lear 🛛 Apply	
No.	Time	Source	Destination	Protocol -	Info	
and the second second	26 0.592209	216.239.41.104	192.168.123.157	HTTP	Continuation	
	28 0.905968	192.168.123.157	216.239.41.104	HTTP	GET /favicon.ico HTTP/1.1	
	31 0.957416	216.239.41.104	192.168.123.157	HTTP	HTTP/1.1 200 OK (image/x-icon)	
	32 0.957849	216.239.41.104	192.168.123.157	HTTP	Continuation	
	34 8.713636	192.168.123.157	216.239.41.104	HTTP	GET /search?hl=en&ie=UTF-8&g=vacation+villas&btn	
	37 8.747618	216.239.41.104	192.168.123.157	HTTP	HTTP/1.1 200 OK[Unreassemb]ed Packet]	
	38 8.748038	216.239.41.104	192.168.123.157	HTTP	Continuation	
	42 0 000413	103 160 133 157	216 220 41 104	UTTO	CET /impace/loss on oif UTTD/1 1	
<b>Г</b> :.	aura CE					

Figure C5.

14) When finished select Tools, Disconnect, Disconnect All.

## What is Abel? How can I install it ?

Abel is an NT service composed by two files: "Abel.exe" and "Abel.dll". These files are copied by the installation package into the program's directory but the service IS NOT automatically installed. Abel can be installed locally or remotely (using Cain), anyway you need Administrator privileges to do that.

LOCAL INSTALLATION:

 Copy the files Abel.exe and Abel.dll into the %WINNT% directory (ES: C:\WINNT)

2) Launch Abel.exe to install the service (not automatically started)

3) Start the service using the Service Manager

REMOTE INSTALLATION (most reliable on wired network):

1) Use the "Network TAB" in Cain and choose the remote computer where Abel will be installed

2) Right click on the computer icon in the tree and select "Connect As"



4) Provide Administrator credentials for the remote machine.

5) Once connected right click on the "Services" icon and select "Install Abel"

File View Configure Tools Help					
	→ <u></u> = <mark>B</mark> <sub>64</sub> §	🕅 🔀 🏧 🖬 🗖 🏹	à 🕵 🧶 🕯	0 i	
📸 Protected Storage 🔮 Network 📓 Sr	iffer 📸 LSA Sec	rets 🥑 Cracker 🔕 T	raceroute	CCDU %	Wireless
👰 Entire Network	Service Name	Display Name	Status	Start Type	Filename
Microsoft Windows Network	Alerter	Alerter	Running	Auto	C: WINNTS
	AppMgmt	Application Management	Stopped	Manual	C: WINNTS
E All Computers	AvgServ	AVG6 Service	Running	Auto	C: PROGRA
BTS-SERVER1	BINLSVC	Boot Information Negotiat	Stopped	Manual	C: WINNTS
	Browser	Computer Browser	Running	Auto	C:\WINNTS
Services	Cisvc	Indexing Service	Running	Auto	C: WINNTS
Share Install Abel	ClipSrv	ClipBook	Stopped	Manual	C: WINNTSU
🖸 Users	Dfs	Distributed File System	Running	Auto	C: WINNTS
🛁 麊 Apple File Servers	Dhcp	DHCP Client	Running	Auto	C: WINNTS
Browsers	DHCPServer	DHCP Server	Running	Auto	C: WINNTS
Dial-In Servers	dmadmin	Logical Disk Manager Admi	Stopped	Manual	C: WINNTS
Domain Controllers	dmserver	Logical Disk Manager	Running	Auto	C: WINNTS
Printer Servers	DNS	DNS Server	Running	Auto	C: WINNTS
SQL Servers	Dnscache	DNS Client	Running	Auto	C: WINNTS
Terminal Servers	Eventlog	Event Log	Running	Auto	C: WINNTS
Time Servers	EventSystem	COM+ Event System	Running	Manual	C: WINNTS
uick List 🕹 🕹 🗠	Fax	Fax Service	Stopped	Manual	C: WINNTS
E E 192, 168, 123, 101	Groveler	Single Instance Storage G	Stopped	Manual	C: WINNTS
JBBLAPTOP \administrator	IAS	Internet Authentication S	Running	Auto	C: WINNTS
Groups	IISADMIN	IIS Admin Service	Running	Auto	C: WINNTS
Shares	Serv IsmServ	Intersite Messaging	Stopped	Disabled	C: WINNTS
G Users	📲 kdc	Kerberos Key Distribution	Stopped	Disabled	C: WINNTS
192, 168, 123, 121	anmanserver	Server	Running	Auto	C: WINNTS
<b>192</b> , 168, 123, 121	anmanworkst	Workstation	Running	Auto	C: WINNTS
<b>1</b> 92 168 123 121	ż.	I tanana I anatan Anatan		A	e humanite

- 5) The two files "Abel.exe" and "Abel.dll" will be copied into the remote machine, the service will be installed and started automatically.
- 6) Once installed on the remote computer, note that among other things, you can bring up a console prompt on the remote machine, examine password Hashes, etc.

📸 Protected Storage 🔮 Network 📱	🕼 Sniffer 🍏 LSA Secrets 🥑	Cracker 🙋 Traceroute 🛄 CCDU %
Entire Network	12/07/1999 08:00a	189,986 c_1361.nls
	12/07/1999 08:00a	180,258 c_20000.nls
E All Computers	12/07/1999 08:00a	186,402 c_20001.nls
E BTS-SERVER 1	12/07/1999 08:00a	173,602 c_20002.nls
- Abel	12/07/1999 08:00a	185,378 c_20003.nls
1 Hashes	12/07/1999 08:00a	180,258 c_20004.nls
🖓 Lsa Secrets	12/07/1999 08:00a	187,938 c_20005.nls
Routes	12/07/1999 08:00a	66,082 c_20105.nls
	12/07/1999 08:00a	66,082 c_20106.nls
	1 10/07/1000 00 00	00.000 00407 1

# Analysis

- 1) APR could be used by network administrators for what purpose?
- 2) After working with these utilities, what about Cain & Abel do you feel you should study further? Why?
- 3) How can network administrators protect against APR?
- 4) Why would someone (not with criminal intent) want to crack passwords on a system?
- 5) Putting on a criminal hat, what are the best bad uses of Cain & Abel?
- 6) How might someone design a system to passively record data from a target machine, then have it easily searchable via a database such as MySQL?

#### Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analysis as a group. Share your experiences and knowledge with the class.

#### If You Want To Learn More:

Ethereal is a great sniffer. Try <u>http://www.insecure.org/</u> which is home of NMAP, another great network sniffer.

Visit: <u>http://nirsoft.mirrorz.com/</u> and examine the utilities that are available. Are any different or similar? Would some of these tools be helpful?

MySQL is available for free at <a href="http://www.mysql.org">http://www.mysql.org</a>

Look on google or another search engine for: *how to detect ARP poison routing*.

Read Intro to ARP Spoofing (attached) by Sean Whalen. Also available by searching the web.

## Appendix

This lab was testing with cain 2.5b Download and install from <u>http://www.oxid.it</u> You will also need to install WinPcap with is part of the Cain install. Then reboot.

Install Ethereal .10.5a from <a href="http://www.ethereal.com">http://www.ethereal.com</a>

These labs were tested on wired and wireless networks.

Wired: 100baseT with 3Com 4 port switched

Wireless: 802.11b Netgear PCMCIA card, 3Com router/switch

Testing on XP Professional with current service packs from Microsoft as of 8/15/04 Windows 2000 Server with service packs as of 8/15/04. It was not tested with Windows 9x nor XP Home.

Tested with M.S. Internet Explorer and Mozilla Firefox 0.9.1