Password Cracking Using Cain & Abel

0

Ahmed Mohamed January 25, 2013 Hacking

Introduction

According to the official website, 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 and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

The latest version is faster and contains a lot of new features like APR (ARP Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS and contains filters to capture credentials from a wide range of authentication mechanisms. The new version also ships routing protocols authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders and some not so common utilities related to network and system security.

OTHER ARTICLES BY AHMED MOHAMED

- Dictionary Attack Using Burp Suite
- Pharming Attack
- Phishing and Social Engineering Techniques 3.0
- Phishing and Social Engineering Techniques 2.0
- PHP Email Injection Example
- Phishing and Social Engineering Techniques
- Webscarab – An Overview
- Graphical Network Simulator Usage
- Manual Packet Analysis
- SQL Injection
- Complete File Upload Vulnerabilities

LIKE US ON FACEBOOK == STAY UP TO DATE

Who Should Use This Tool?

Cain & Abel is a tool that will be quite useful for network administrators, teachers, professional penetration testers, security consultants/professionals, forensic staff and security software vendors.

Requirements

The system requirements needed to successfully setup Cain & Abel are:

– At least 10MB hard disk space

– Microsoft Windows 2000/XP/2003/Vista OS

– Winpcap Packet Driver (v2.3 or above).

– Airpcap Packet Driver (for passive wireless sniffer / WEP cracker).

Installation

First we need to download Cain & Abel, so go to the download page www.oxid.it/cain.html.

After downloading it,just run the Self-Installing executable package and follow the installation instructions.

Cain’s Features

Here’s a list of all of Cain’s features that make it a great tool for network penetration testing:

Protected Storage Password Manager
LSA Secrets Dumper
Service Manager
Route Table Manager
SID Scanner
Sniffer
Full RDP sessions sniffer for APR
Full HTTPS sessions sniffer for APR
Full POP3S sessions sniffer for APR
Full LDAPS sessions sniffer for APR
MAC Address Scanner with OUI fingerprint
Wireless Scanner

Credential Manager Password Decoder
Dialup Password Decoder
APR (ARP Poison Routing)
Network Enumerator
Remote Registry
Routing Protocol Monitors
Full SSH-1 sessions sniffer for APR
Full FTPS sessions sniffer for APR
Full IMAPS sessions sniffer for APR
Certificates Collector
Promiscuous-mode Scanner
PWL Cached Password Decoder

802.11 Capture Files Decoder
Access (9x/2000/XP) Database Passwords Decoder
Base64 Password Decoder
Cisco Type-7 Password Decoder
Cisco VPN Client Password Decoder
RSA SecurID Token Calculator
TCP/UDP Table Viewer
Cisco Config Downloader/Uploader (SNMP/TFTP)
Wireless Zero Configuration Password Dumper
MSCACHE Hashes Dumper
Microsoft SQL Server 2000 Password Extractor
VNC Password Decoder
Password Crackers
Cryptanalysis attacks
WEP Cracker
Rainbowcrack-online client
Enterprise Manager Password Decoder
Hash Calculator
TCP/UDP/ICMP Traceroute
Box Revealer
Remote Desktop Password Decoder
MySQL Password Extractor
Oracle Password Extractor
Syskey Decoder

Related Definitions:

MAC: (from Wikipedia) “A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the OSI reference model.

MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card’s read-only memory, or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer’s registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. A network node may have multiple NICs and will then have one unique MAC address per NIC.”

Sniffing: (fromWikipedia) “A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet’s raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.”

ARP(from Wikipedia) “Address Resolution Protocol (ARP) is a telecommunications protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks. ARP was defined by RFC 826 in 1982. It is Internet Standard STD 37. It is also the name of the program for manipulating these addresses in most operating systems.”

Usage

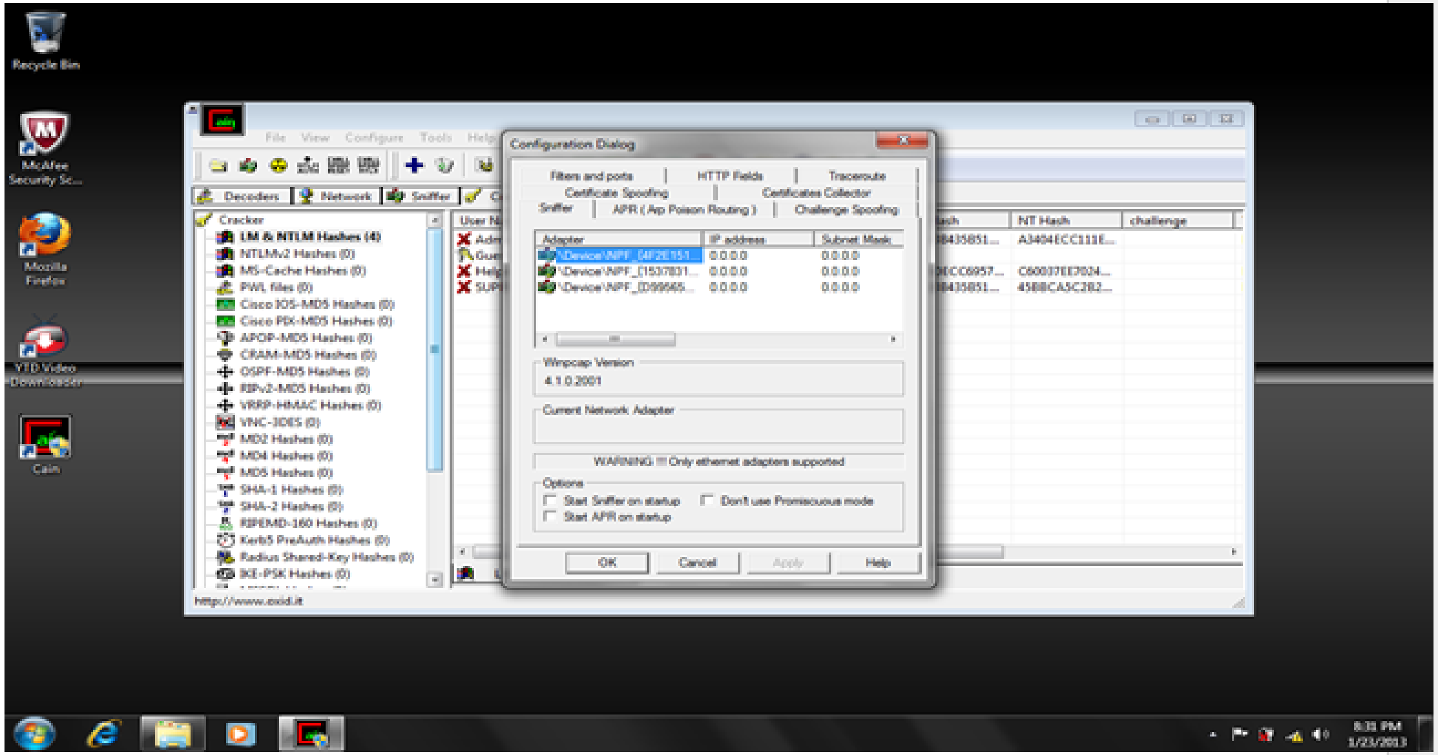
Now after launching the application, we have to configure it to use appropriate network card.If you have multiple network cards, it's better to know the MAC address of the network card that you will use for the sniffer.To get the MAC address of your network interface card, do the following:

1- Open CMD prompt.
/p>

2- Write the following command "ipconfig /all".

3- Determine the MAC address of the desired Ethernet adapters, write it on Notepad,and then use this information to help determine which NIC to select in the Cain application.

Now clickConfigure on the main menu. It will open the configuration dialog box where you can select the desired network interface card.



Adapter	IP address	Subnet Mask
\Device\NPF_{4F2E151...	0.0.0.0	0.0.0.0
\Device\NPF_{1537831...	0.0.0.0	0.0.0.0
\Device\NPF_{D99565...	0.0.0.0	0.0.0.0

Winpcap Version
4.1.0.2001

Current Network Adapter

WARNING !!! Only ethernet adapters supported

Options
□ Start Sniffer on startup □ Don't use Promiscuous mode
□ Start APR on startup

Now let’s go through the configuration dialog tabs and take a brief look at most of them:

Sniffer Tab:

This tab allows us to specify which Ethernet interface card we will use for sniffing.

ARP Tab:

This tab allows us to configure ARP poison routing to perform ARP poisoning attack, which tricks the victim’s computer by impersonating other devices to get all traffic that belongs to that device, which is usually the router or an important server.

Filters and Ports Tab:

This tab has the most standard services with their default port running on.You can change the port by right-clicking on the service whose port you want to change and then enabling or disabling it.

Cain’s sniffer filters and application protocol TCP/UDP port.

HTTP Fields Tab:

There are some features of Cain that parse information from web pages viewed by the victim such as LSA Secrets dumper, HTTP Sniffer and ARP-HTTPS,so the more fields you add to the username and passwords fields, the more you capture HTTP usernames and passwords from HTTP and HTTPS requests. Here is an example:

The following cookie uses the fields “logonusername=” and “userpassword=” for authentication purposes. If you don’t include these two fields in the list, the sniffer will not extract relative credentials.

```
GET /mail/Login?domain=xxxxxx.xx&style=default&plain=0 HTTP/1.1

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*

Referer: http://xxx.xxxxxxx.xx/xxxxx/xxxx
```

```
Accept-Language: it
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; (R1 1.3); .NET CLR 1.1.4322)
Host: xxx.xxxxxx.xx
Connection: Keep-Alive
Cookie: ss=1; logonusername=user@xxxxxx.xx; ss=1; srclng=it; srcdmn=it; srctrg=_blank; srcbld=y; srcauto=on; srcclp=on; srcsct=web; userpassword=password; video=c1; TEMPLATE=default;
```

Traceroute Tab:

Traceroute is a technique to determine the path between two points by simply counting how many hops the packet will take from the source machine to reach the destination machine. Cain also adds more functionality that allows hostname resolution, Net mask resolution, and Whois information gathering.

Certificate Spoofing Tab:

This tab will allow Certificate spoofing.From Wikipedia:

“In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document that uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users (“endorsements”). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.”

We can simply think of it as some sort of data (cipher suites & Public key and some other information about the owner of the certificate) that has information about the destination server and is encrypted by trusted companies (CA) that are authorized for creating these types of data.The server sends its own certificate to the client application to make sure it's talking to the right server.

Certificate Collector Tab:

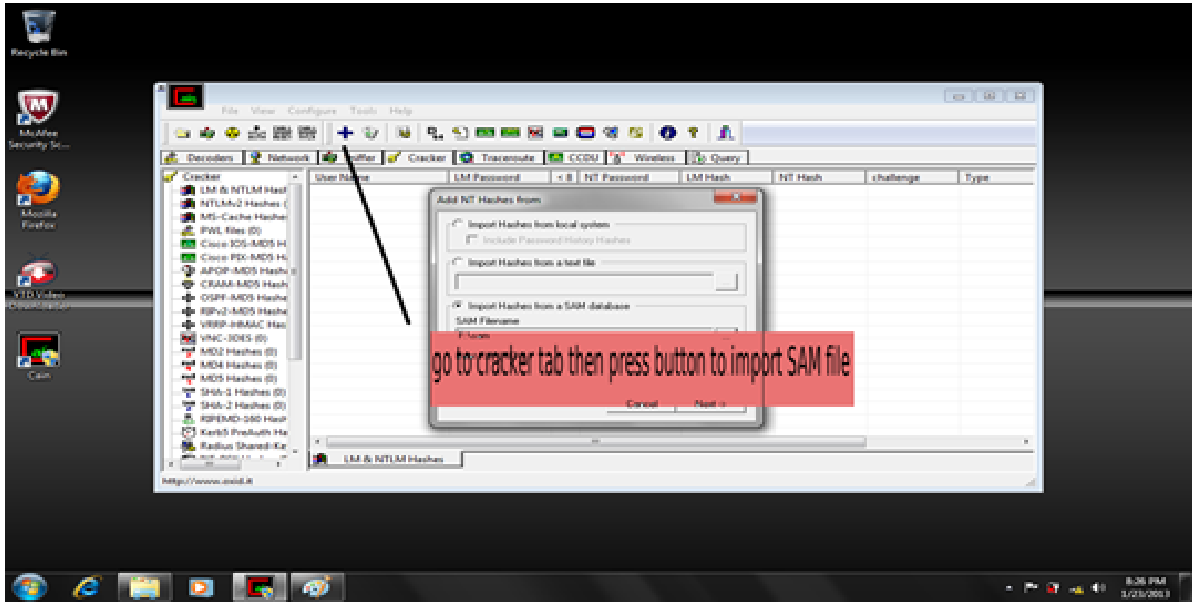
This tab will collect all certificates back and forth between servers and clients by setting proxy IPs and ports that listen to it.

Challenge Spoofing Tab:

Here you can set the custom challenge value to rewrite into NTLM authentications packets. This feature can be enabled quickly from Cain's toolbar and must be used with APR. A fixed challenge enables cracking of NTLM hashes captured on the network by means of Rainbow Tables.

Password Cracking

Now it's time to speak about the cracker tab,the most important feature of Cain.When Cain captures some LM and NTLM hashes or any kind of passwords for any supported protocols, Cain sends them automatically to the Cracker tab.We will import a local SAM file just for demonstration purposes to illustrate this point.Here is how to import the SAM file:

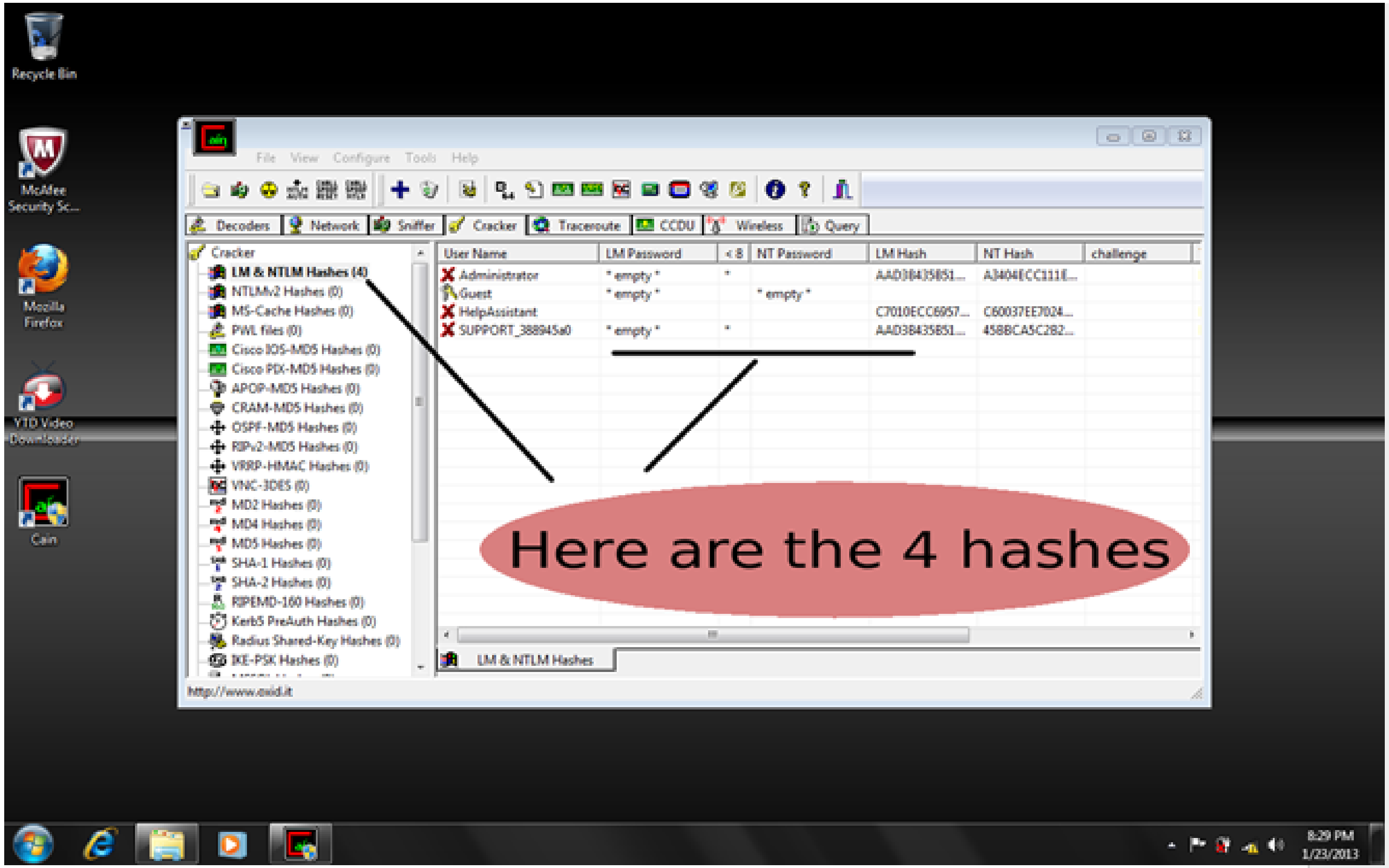


Add NT Hashes from

○ Import Hashes from local system
□ Include Password History Hashes
○ Import Hashes from a text file
● Import Hashes from a SAM database
SAM Filename
Cancel
Next >

go to cracker tab then press button to import SAM file

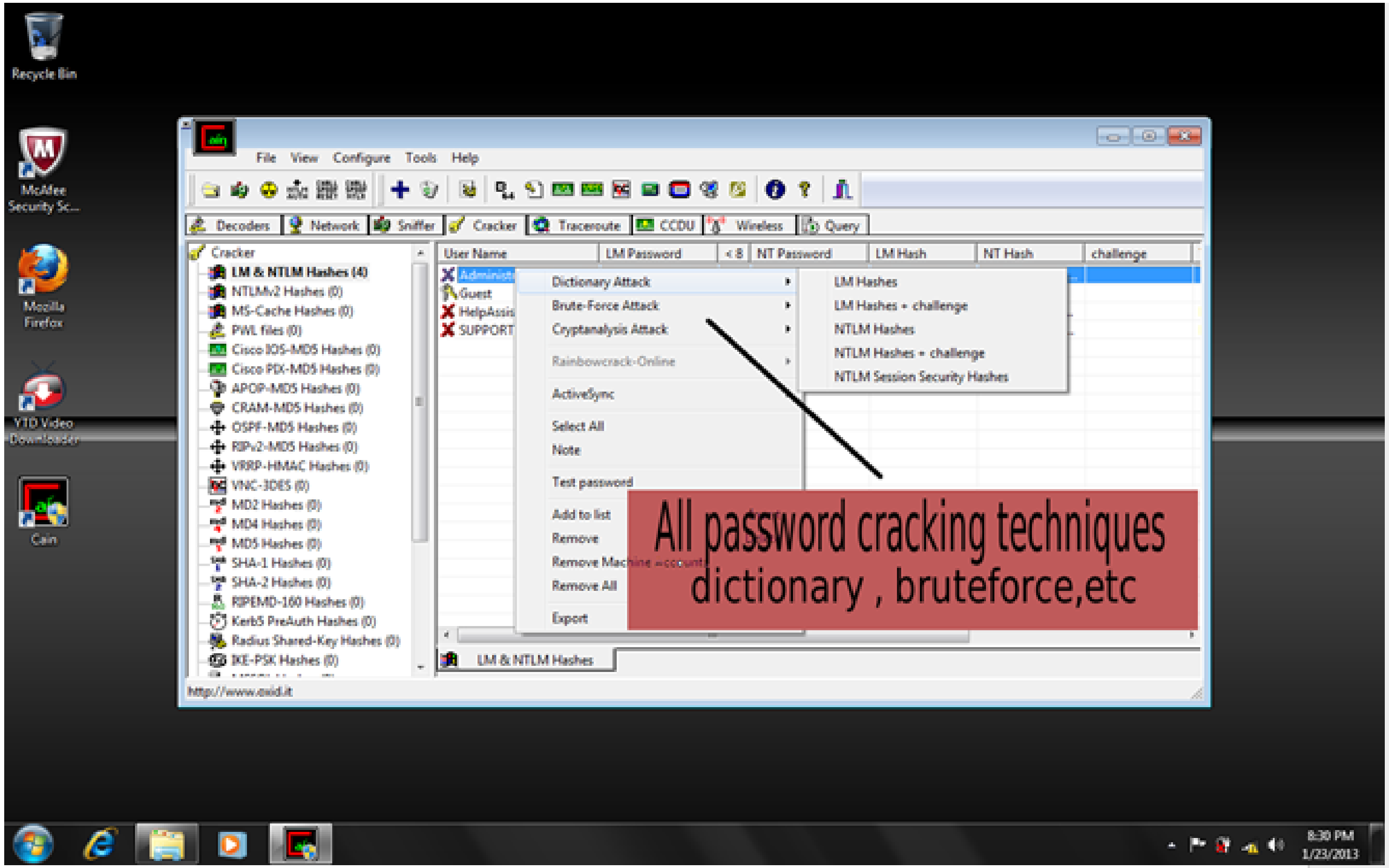
Here are the 4 NTLM and LM hashes which will appear like the following image:



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge
Administrator	* empty *	*		AAD3B435B51...	A3404ECC111E...	
Guest	* empty *		* empty *			
HelpAssistant				C7010ECC6957...	C60037EE7024...	
SUPPORT_388945a0	* empty *	*		AAD3B435B51...	45BBCA5C2B2...	

Here are the 4 hashes

And here you will find all possible password techniques in the following image:



All password cracking techniques
dictionary , bruteforce,etc

As you can see from the previous image, there are various types of techniques that are very effective in password cracking.We will look at each of their definitions.

Dictionary attack:

From Wikipedia: “A dictionary attack uses a targeted technique of successively trying all the words in an exhaustive list called a dictionary (from a pre-arranged list of values). In contrast with a brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a dictionary (hence the phrase dictionary attack). Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries or simple, easily predicted variations on words, such as appending a digit. However these are easy to defeat. Adding a single random character in the middle can make dictionary attacks untenable.”

Brute forcing attack:

From Wikipedia: “In cryptography, a brute-force attack, or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be utilized when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space.

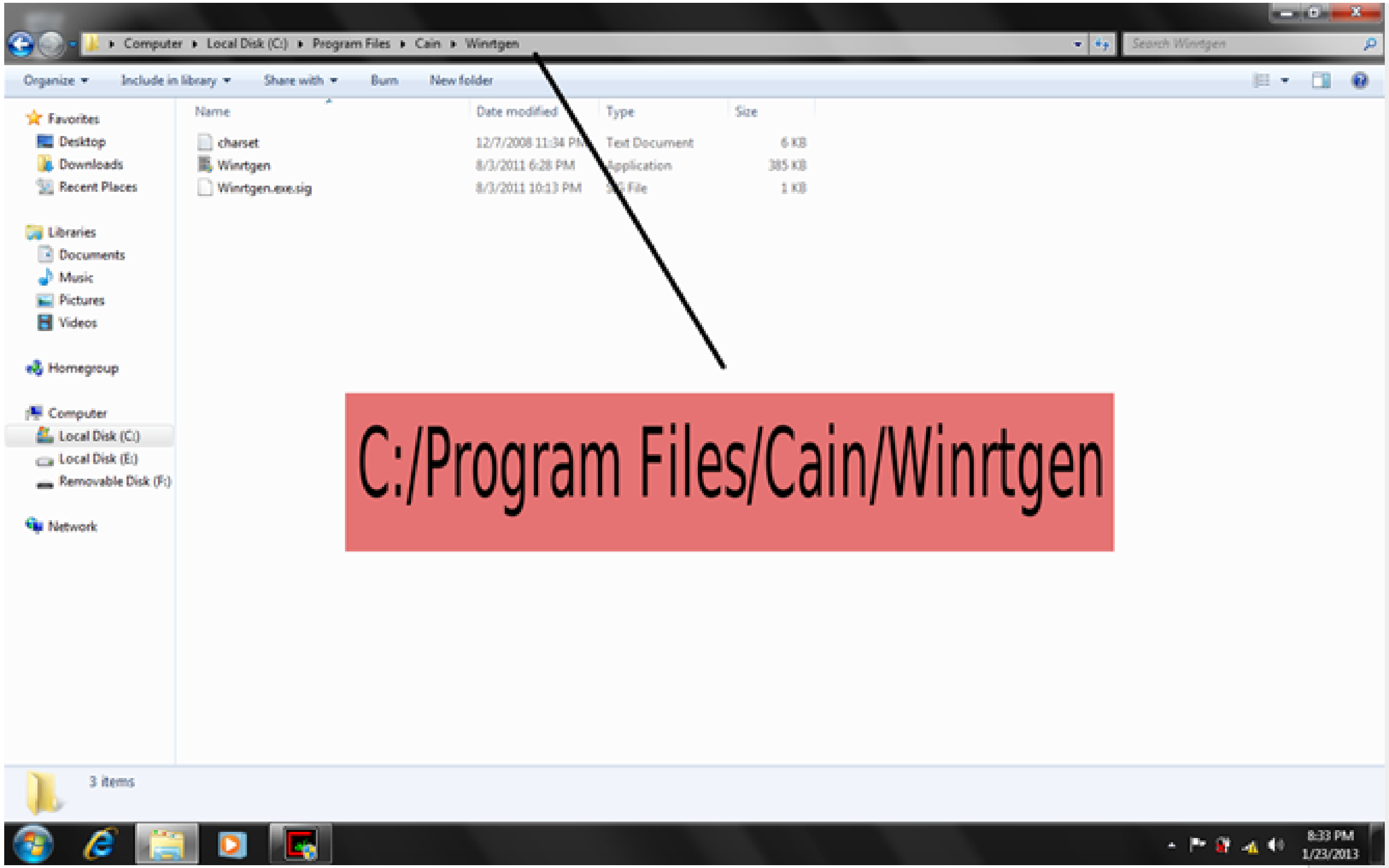
The key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. A cipher with a key length of N bits can be broken in a worst-case time proportional to 2N and an average time of half that. Brute-force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when he/she has cracked the code. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it.”

Cryptanalysis attack (Using Rainbow Table):

From Wikipedia: “A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering the plain text password, up to a certain length consisting of a limited set of characters. It is a practical example of a space-time tradeoff, using more computer processing time at the cost of less storage when calculating a hash on every attempt, or less processing time and more storage when compared to a simple lookup table with one entry per hash. Use of a key derivation function that employ a salt makes this attack infeasible. Rainbow tables are a refinement of an earlier, simpler algorithm by Martin Hellman.”

How To Make A Rainbow Table?

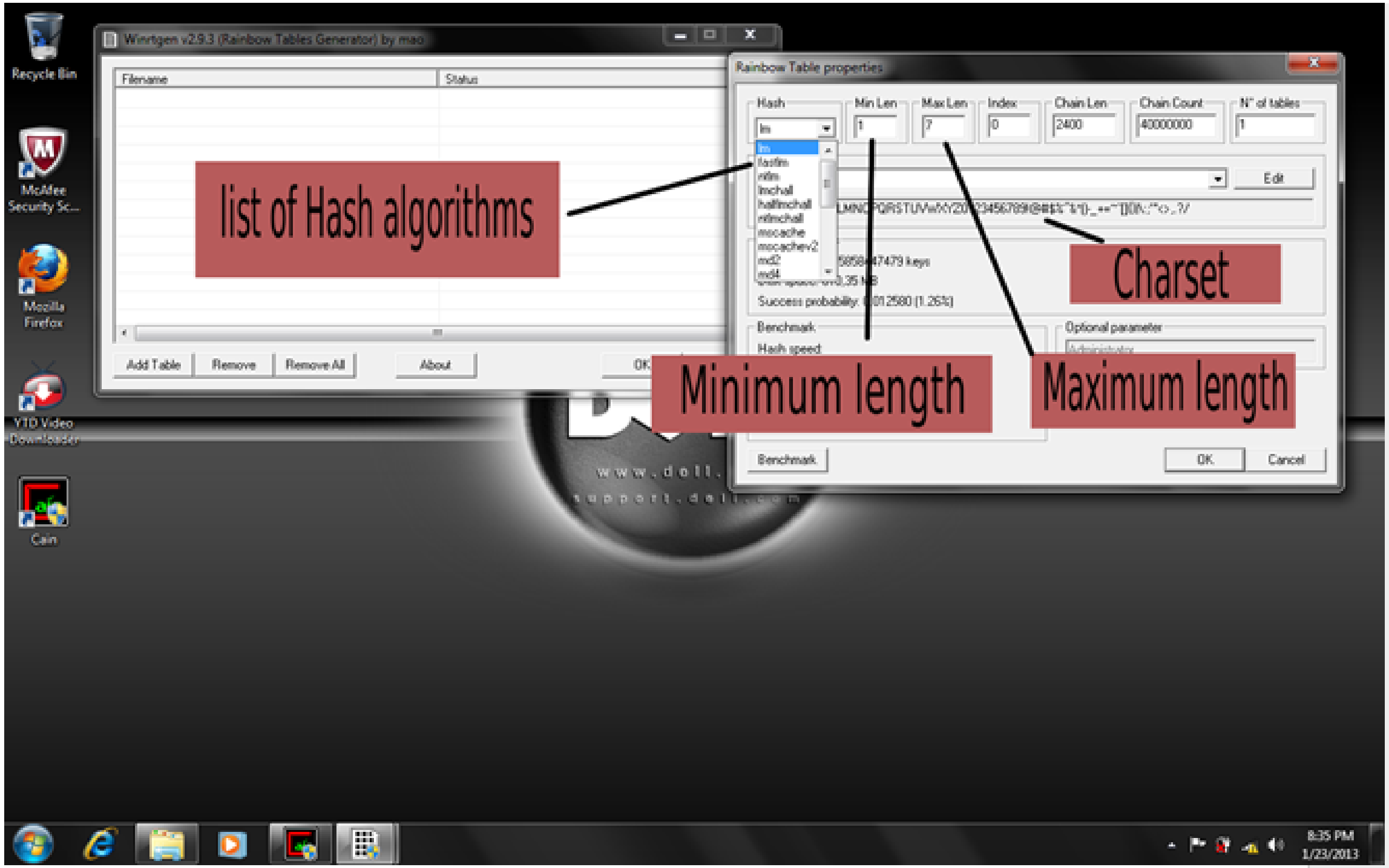
There are many tools that create a rainbow table and there are many rainbow tables already available on the internet.Fortunately, Cain comes with a tool called winrtgen, which is located in its own folder in the installation.



Name	Date modified	Type	Size
charset	12/7/2008 11:34 PM	Text Document	6 KB
Winrtgen	8/3/2011 6:28 PM	Application	385 KB
Winrtgen.exe.sig	8/3/2011 10:13 PM	SIG File	1 KB

C:/Program Files/Cain/Winrtgen

You will need to choose ahash algorithm, minimum andmaximum length of password, and finally the charset that the password will use.Then press OK.



Hash: lm
Min Len: 1
Max Len: 7
Index: 0
Chain Len: 2400
Chain Count: 40000000
N° of tables: 1

LMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/

5858447479 keys

Success probability: 0.012580 (1.26%)

Conclusion

Cain and Abel is a powerful tool that does a great job in password cracking. It can crack almost all kinds of passwords, and it's usually just a matter of time before you get it.

References

1- www.wikipedia.org

2- www.oxid.it

3- www.thehackerslibrary.com

Incoming search terms:

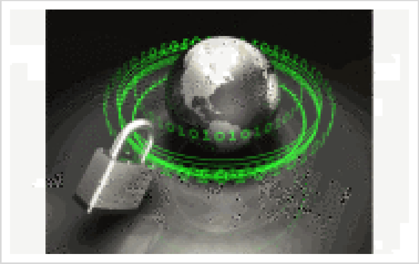
- how to use cain and abel
- using Cain and Abel
- how to use cain
- cain and abel password cracker
- using cain and able
- cain and abel https
- how to use cain and abel to get passwords
- how to use cain and abel to crack passwords
- cain abel https password
- cain and abel ssl passwords

cain & abel feature password recovery tool

About the Author

Ahmed Elhady Mohamed is a researcher at InfoSec Institute and an information security professional and author. He focuses mainly in the areas of exploitation,reverse engineering and web security. He's the webmaster of www.ITsec4all.com

Related Posts



Leave A Response

Name (required)

Email (required)

Website

Comment

Post Comment

ARCHIVE

- September 2013 (36)
- August 2013 (42)

RECENT POSTS

- Web Services Penetration Testing Part 1
- Ajax Security Issues

CATEGORIES

- Application Security (140)
- Exploit Development (48)

- July 2013 (44)
- June 2013 (38)
- May 2013 (42)
- April 2013 (56)
- March 2013 (68)
- February 2013 (65)
- January 2013 (65)
- December 2012 (51)
- November 2012 (45)
- October 2012 (59)
- September 2012 (56)
- August 2012 (35)
- July 2012 (21)
- June 2012 (31)
- May 2012 (11)
- April 2012 (16)
- March 2012 (12)
- February 2012 (24)
- January 2012 (22)
- December 2011 (15)
- November 2011 (12)
- October 2011 (12)
- September 2011 (1)
- August 2011 (2)
- July 2011 (7)
- June 2011 (22)

- Windows Phone digital forensics
- Enterprise Security Management
- Fixing CSRF vulnerability in PHP Applications
- Linux Kernel Development Process
- Windows Systems and Artifacts in Digital Forensics, Part I: Registry
- IOS Application Security Part 18 – Detecting custom signatures with Introspy
- Social Engineering: A Hacking Story
- Patching .NET Binary Code with CFF Explorer
- Conditional Complexity of Risk Models
- Backup Media Encryption

POPULAR COMMENTS TAGS

Antivirus Evasion: The Making of a Full, Undetectable USB Dropper / Spreader

September 20, 2012

45

- Forensics (62)
- General Security (193)
- Hacking (310)
- Interviews (33)
- IT Certifications (65)
- CCNA (2)
- CEH (5)
- CISA (16)
- CISM (10)
- CISSP (33)
- MCITP (2)
- Malware Analysis (2)
- Management, Compliance, & Auditing (48)
- Meta (2)
- Other (79)
- Reverse Engineering (119)
- SCADA (5)
- Virtualization Security (6)
- Wireless Security (10)

POPULAR SEARCH TERMS

iphone, i phone, backtrack 5 r3 tutorial, resources infosecinstitute com, diarmf, network security engineer, w3af tutorial, backtrack 5 r3 tutorial pdf, Backtrack 5, Application Controls, iphone 1, maltego

May 2011 (30)

April 2011 (33)

March 2011 (24)

February 2011 (7)

January 2011 (2)

December 2010 (3)

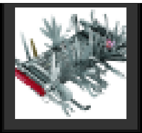
November 2010 (7)

October 2010 (1)

September 2010 (1)

August 2010 (4)

July 2010 (2)



Ideal Skill Set For the Penetration Testing

August 27, 2010 44

SLAAC Attack – 0day Windows Network Interception Configuration Vulnerability

April 04, 2011 39

Demystifying Dot NET Reverse Engineering, Part 1: Big Introduction

October 24, 2012 39

Back