

Ethical Hacking and Countermeasures

Version 6



Module XVIII

Web-based Password Cracking Techniques





Password-Cracking Chip Causes Security Concerns

By ANDREW BRANDT

Oct. 24, 2007 -

A technique for cracking computer passwords using inexpensive off-the-shelf computer graphics hardware is causing a stir in the computer security community.

Elcomsoft, a software company based in Moscow, Russia, has filed a US patent for the technique. It takes advantage of the "massively parallel processing" capabilities of a graphics processing unit (GPU) - the processor normally used to produce realistic graphics for video games.

Using an \$800 graphics card from nVidia called the GeForce 8800 Ultra, Elcomsoft increased the speed of its password cracking by a factor of 25, according to the company's CEO, Vladimir Katalov.

The toughest passwords, including those used to log in to a Windows Vista computer, would normally take months of continuous computer processing time to crack using a computer's central processing unit (CPU). By harnessing a \$150 GPU - less powerful than the nVidia 8800 card - Elcomsoft says they can cracked in just three to five days. Less complex passwords can be retrieved in minutes, rather than hours or days.

It is the way a GPU processes data that provides the speed increase. NVidia spokesman Andrew Humber describes the process using the analogy of searching for words in a book. "A [normal computer processor] would read the book, starting at page 1 and finishing at page 500," he says. "A GPU would take the book, tear it into a 100,000 pieces, and read all of those pieces at the same time."

Benjamin Jun, of Cryptography Research based in San Francisco, US, says massively parallel processing is ideally suited to the task of breaking passwords. And, while concerned about the development, Jun also pays tribute to the achievement: "A number of us have been following advances in those platforms, and there's a lot of elegant, intelligent design."

Source: http://www.abcnews.go.com/

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



Ron, a strong supporter of peace and harmony in war-torn regions is also a computer hacker by profession. He trades his service at one of the IRC channels. Defacing websites, cracking software licenses, reverse engineering applications are few of the services that Ron offers to his clients on the IRC channel.

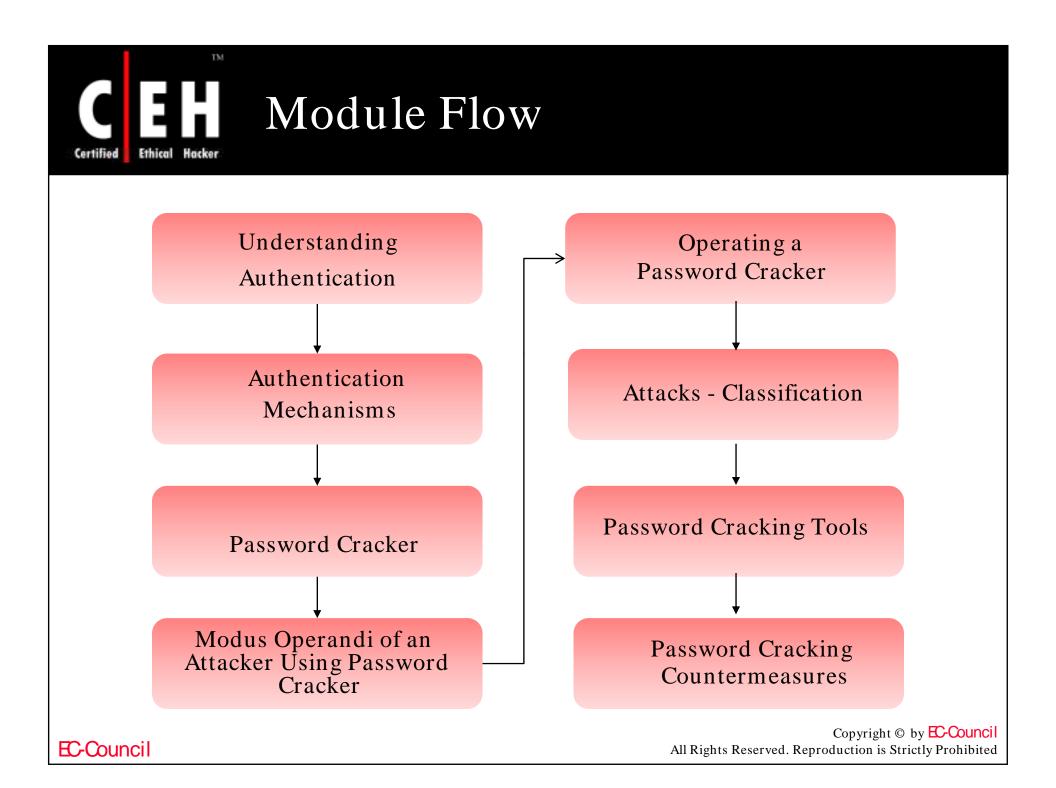
Depressed by the hindrances in the way to peace in the Asian region, he plans to voice his concern by targeting website of one of the Not-for-Profit government organizations.

While searching for target websites, Ron stumbles on the website of a Government body. *XChildrelief4u Welfare Organization* is a body dedicated to abolish child labor in the region.

Ron runs an FTP brute force tool and cracks the admin password for the website. With the cracked admin password he logs on to the website and changes the Index.htm file. He posts "*Stop War We Need Peace*", deletes log file and logs out.

Visitors at the website of *XChildrelief4u Welfare Organization* were quite amused to read the message.

| Ethical | Hacker |
|---------|------------------------------------------------------|
| | |
| | his module will familiarize you with : |
| | |
| | |
| • | Authentication |
| ٠ | Authentication Mechanisms |
| • | Password Cracker |
| • | Modus Operandi of an Attacker Using Password Cracker |
| ٠ | Operation of a Password Cracker |
| • | Classification of Attacks |
| • | Password Cracking Tools |
| • | Password Cracking Countermeasures |







Authentication

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



Authentication – Definition

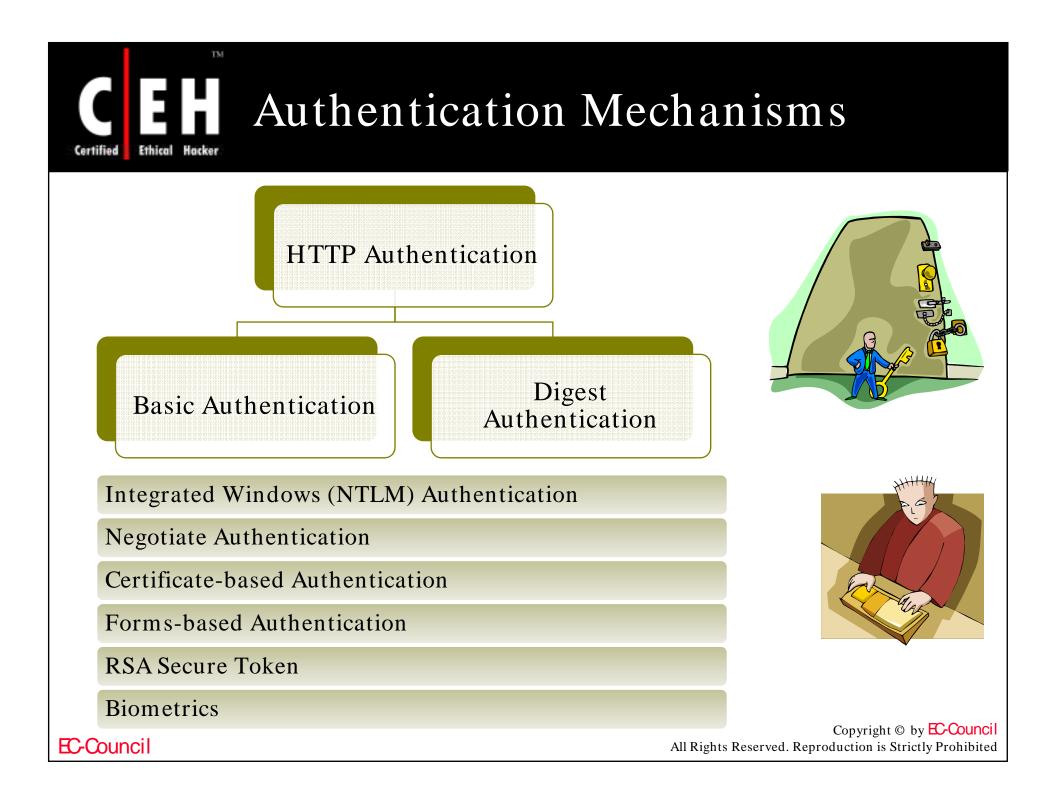
Authentication is the process of determining the user's identity

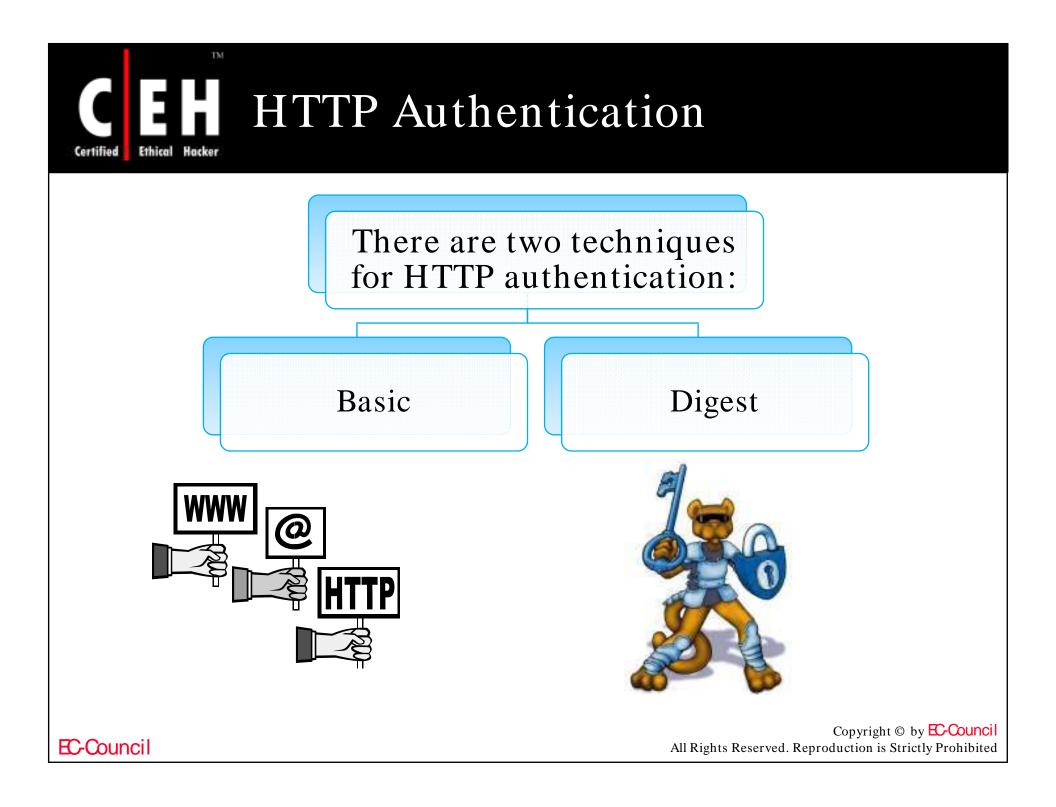
In private and public computer networks, authentication is commonly done through the use of login IDs and passwords

Knowledge of the password is assumed to guarantee that the user is authentic

Passwords can often be stolen, accidentally revealed, or forgotten due to inherent loopholes in this type of authentication









Basic Authentication

Basic authentication is the most basic form of authentication available to web applications

It begins with a client making a request to the web server for a protected resource without any authentication credentials

The limitation of this protocol is that it is wide open to eavesdropping attacks

The use of 128-bit SSL encryption can thwart these attacks

| nter Net | work Passwor | rd | ? × |
|----------|-------------------|-------------------------------|------|
| ? | Please type y | /our user name and password. | |
| 4 | Site: | www.regsoft.net | |
| | Realm | RegSoft.com Vendor Area | |
| | <u>U</u> ser Name | myuserid | |
| | <u>P</u> assword | - | |
| | □ Save this p | assword in your password list | Şeri |
| | | OK Cancel | |
| | | | |



Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited

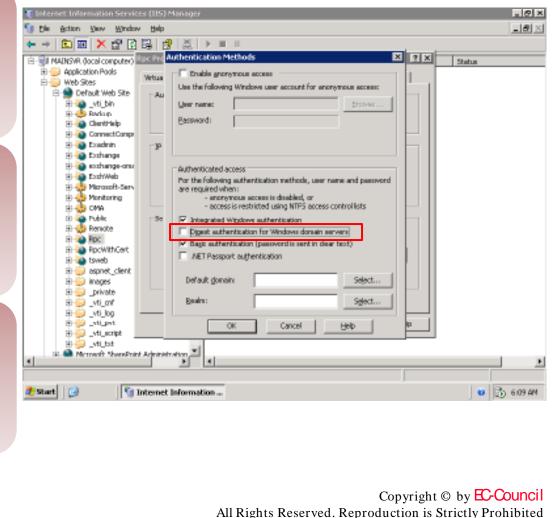


Digest Authentication

Digest authentication is designed to provide a higher level of security vis-à-vis Basic authentication

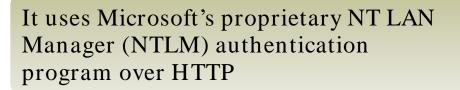
It is based on the *challengeresponse* authentication model

It is a significant improvement over basic authentication as it does not send the user's cleartext password over the network





Integrated Windows (NTLM) Authentication



It only works with Microsoft's Internet Explorer browser and IIS web servers

Integrated Windows authentication is more suitable for intranet deployment

In this type of authentication, no version of the user's password ever crosses the wire

| | ne/password required to acc ed for ancnymous access; | | | | |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|--|--|--|
| Jser name: | IUSR_ECCOUNCIL | Browse | | | |
| Password: | | | | | |
| | Allow IIS to control password | | | | |
| For the follow are required - an - ac | wing authentication melhods when ionymous access is disabled icess is restricted using NTF! | , or 5 access control lists | | | |
| For the follow are required - an - ac Digest a | wing authentication methods when ionymous access is disabled icess is restricted using NTF uthentication for Windows d | , or 5 access control lists omain servers | | | |
| For the follow are required - an - ac Digest a | wing authentication melhods when ionymous access is disabled icess is restricted using NTF! | , or 5 access control lists omain servers | | | |
| are required - an - ac Digest a | wing authentication methods when ionymous access is disabled icess is restricted using NTF uthentication for Windows d ithenticaton (password is se | , or 5 access control lists omain servers | | | |
| For the follow are required - an - ac Digest a Basic au | wing authentication methods when ionymous access is disabled icess is restricted using NTF uthentication for Windows d ithenticaton (password is se | , or 5 access control lists omain servers nt in clear text) | | | |



Negotiate authentication is an extension of NTLM authentication

It provides Kerberos-based authentication

It uses a negotiation process to decide on the level of security to be used

This configuration is fairly restrictive and uncommon except on corporate intranets

| | 🕲 about:config - Mozilla Firefox | | | | _ 🗆 🗡 | |
|------------|--------------------------------------------------------|----------|---------|-------------|------------------|---------------------------------------------------------|
| | <u>Eile Edit View Go Bookmarks I</u> ools <u>H</u> elp | | | | | |
| | | | | | | |
| | Fijlter: negotiate | | | | Sho <u>w</u> All | |
| | Preference Name | 7 Status | Туре | Value | E | |
| | network.negotiate-auth.allow-proxies | default | boolean | true | | |
| | network.negotiate-auth.delegation-uris | default | string | | | |
| | network.negotiate-auth.gsslib | default | string | | | |
| | network.negotiate-auth.trusted-uris | user set | string | vintela.com | | |
| | network.negotiate-auth.using-native-gsslib | default | boolean | true | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | J | | | | | |
| | Done | | | | | Copyright © by EC-Counc |
| EC-Council | | | | | A | All Rights Reserved. Reproduction is Strictly Prohibite |



Certificate-based Authentication

Certificate-based authentication uses public key cryptography and a digital certificate to authenticate a user

It is considered as an implementation of twofactor authentication



In addition to the information known by the user, for e.g.: (his password), he must authenticate with a certificate

A user can be tricked into accepting a spoofed certificate or a fake certificate

Few hacking tools currently support client certificates





Certificate-based Authentication (cont'd)



EC-Council

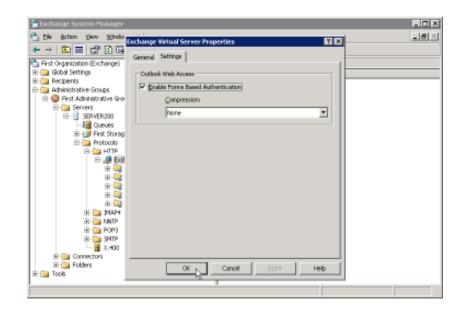


Forms-based Authentication

Forms-based authentication does not rely on features supported by the basic web protocols like HTTP and SSL

It is a customizable authentication mechanism that uses a form, usually composed of HTML

It is the most popular authentication technique deployed on the Internet







The SecurID authentication mechanism consists of a "token," a piece of hardware assigned to a user that generates an authentication code in every 60 seconds using a built-in clock and the card's factory-encoded random key

A user authenticating to a network resource – for example, a dial-in server or a firewall – needs to enter both a PIN and the number being displayed at that moment in time on his SecurID token



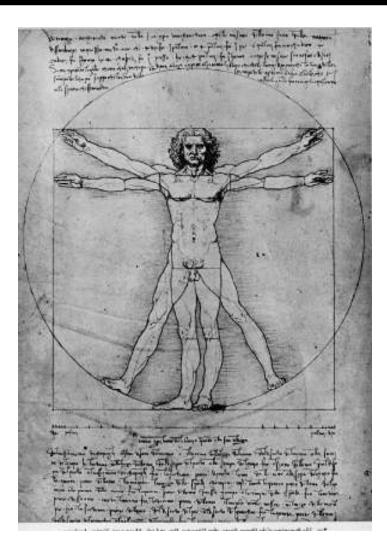
h you



A biometric system is essentially a pattern recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user

This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- The person to be identified is required to be physically present at the point of identification
- Identification based on biometric techniques obviates the need to remember a password or carry a token





Biometrics Authentication (cont'd)













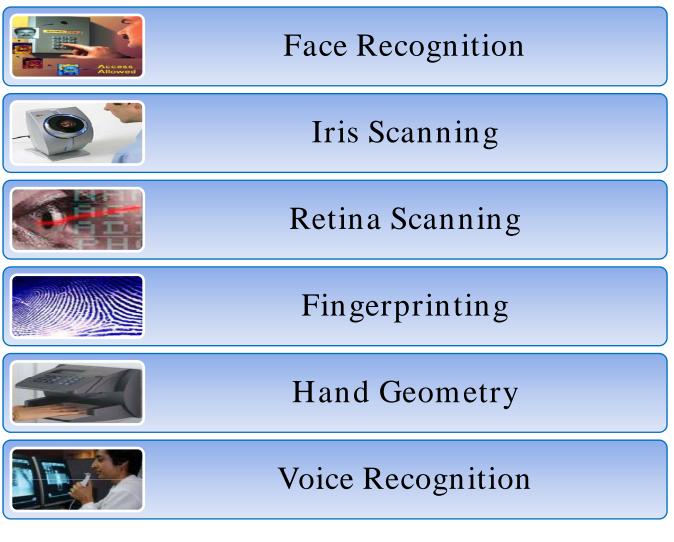






Certified Ethical Hacker

Types of Biometrics Authentication



EC-Council



Fingerprint-based Identification

It is a known fact that everyone has a unique and immutable fingerprints

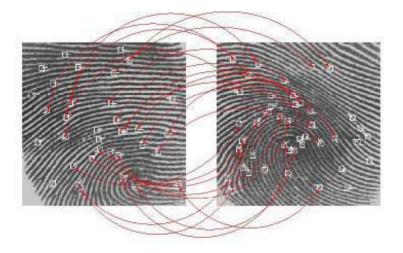
A fingerprint is made of a series of ridges and furrows on the surface of the finger

The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points

US Immigration uses this type of authentication at airports



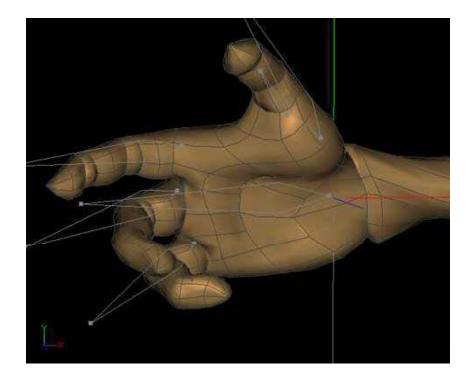




Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



This approach uses the geometric shape of the hand for authenticating a user's identity

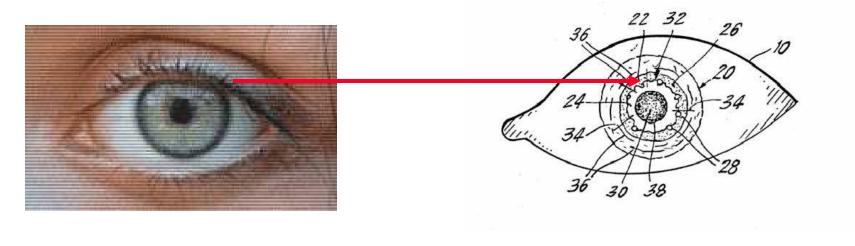






Retina is recognized by means of scanning blood vessel patterns of the retina and the pattern of flecks on the iris

A retinal scan is difficult to fake because no technology exists that allows the forgery of a human retina, and the retina of a deceased person decays too fast to be used to fraudulently bypass a retinal scan





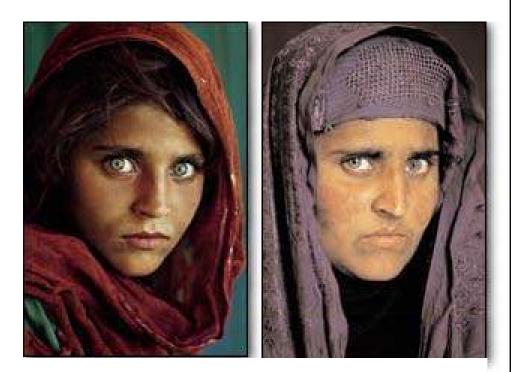


Afghan Woman Recognized After 17 Years

An Afghan woman, Sharbat Gula, was photographed in 1984 at a refugee camp in Pakistan

She was found by the original photographer in the beginning of 2002

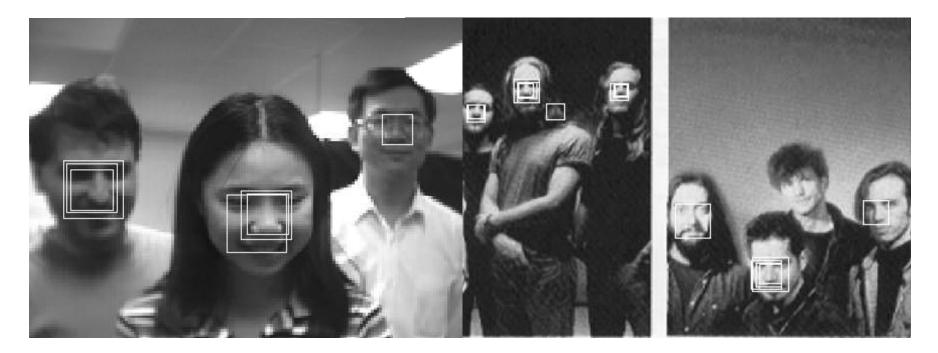
Her identity was confirmed by iris analysis





Face recognition is a type of authentication that uses facial recognition to identify a person

It is difficult to implement





Face Code: WebCam Based Biometrics Authentication System

FaceCode with face recognition technologies uses your existing web camera to authenticate and access your PC

FaceCode password bank provides you with easy to use password management tool, using face recognition as automatic logon to secure websites and application access

By creating a FaceCode password bank account, you can protect all your access codes in a digitally encrypted safe where your face is your key

You do not need to use user name and password at all, just show your face to the web camera for authentication

Download the tool from http://www.eccouncil.org/cehtools/facecodce.zip









Bill Gates at the RSA Conference 2006

"Another weak link is in authentication. Today, we're using password systems, and password systems simply won't cut it; in fact, they're very quickly becoming the weak link. This year, there was a significant rise in phishing attacks where sites that pretended to be legitimate would get somebody to enter their password and then be able to use that to create exploitive financial transactions. And so we need to move to multifactor authentication. A lot of that will be a smart-card-type approach where you have challenge/response, you don't have a single secret that you're passing to the other person so they can actually have that and reuse it. It's a significant change and that needs to be built down into the system itself."







Password Cracking

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



How to Select a Good Password

Use at least eight characters – 15 is better

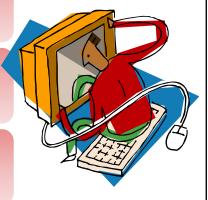
Use a random mixture of characters – upper and lower case letters, numbers, punctuation, spaces, and symbols

Do not use a word found in a dictionary whether it is English or foreign

Never use the same password twice

Choose a password that you can remember

Choose a password that you can type quickly – this reduces shoulder surfing



Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited



Do not add a single digit or symbol before or after a word – for example, "microsoft1"

Do not double up a single word – for example, "msoftmsoft"

Do not simply reverse a word – for example, "tfosorcim"

Do not remove the vowels - for example, "io"

Key sequences that can easily be repeated – for example, "qwerty," "asdf," etc.

Do not garble letters – for example, converting \mathbf{e} to $\mathbf{3}$, \mathbf{L} or \mathbf{i} to $\mathbf{1}$, \mathbf{o} to $\mathbf{0}$, as in "z3r0-10v3"





Change your password regularly, such as once a month

Change your password after you return from a trip

You should also change your password whenever you suspect that somebody knows it or even that they may guess it – for example, if someone stood behind you while you typed it







Do not store your password on your computer, except in an encrypted form

Password cache that comes with windows (.pwl files) is NOT secure; so, whenever windows prompts you to "Save password," don't

Do not tell anyone your password, not even your system administrator

Never send your password via email or other unsecured channels

Write your password in a piece of paper, but do not leave the paper lying around; lock the paper away somewhere

Be careful when you are entering your password with somebody else in the same room

Examples of Bad Passwords

"james8" - Based on the user's name, it is too short also

"samatha" - The name of the user's girlfriend; easy to guess

"harpo" - The user's name (Oprah) backwards

"superstitious" - Listed in a dictionary

" sUperStiTIous " - Just adding random capitalization does not make it safe

"kadhal - Listed in a Tamil foreign language dictionary

"obiwan" - Listed in word lists

TM

Ethical

"spicer" - Listed in a geological dictionary

"qwertyuiop" - Listed in word lists



Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited



The "Mary Had A Little Lamb" Formula

Consider a phrase: "Mary had a little lamb. The lamb had white fleece."

Consider the first letter of each word, i.e.: MHALLTLHWF

Every second letter of the abbreviation can be put in the lower case, i.e. MhAlLtLhWf

Replace "A" with "@" and "L" with "!". Thus, a new alphanumeric password with more than eight characters will be formed

New Password: Mh@l!t!hWf



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited

How Hackers get hold of Passwords

Steal it

TM

- Shoulder surfing watching while you type the password
- Retrieving the paper in which you wrote the password

Guess it

- Simply guess the password
- Psychologists say that most men use four-etter obscenities as passwords, and most women use the names of their boyfriends, husbands, or children

A brute force attack

• A brute force attack refers to the act of using every possible combination of letters, numbers, and symbols being in an attempt to guess the password. While this is a labor-intensive task with fast, modern processors, and software tools, this method should not be underestimated

A dictionary attack

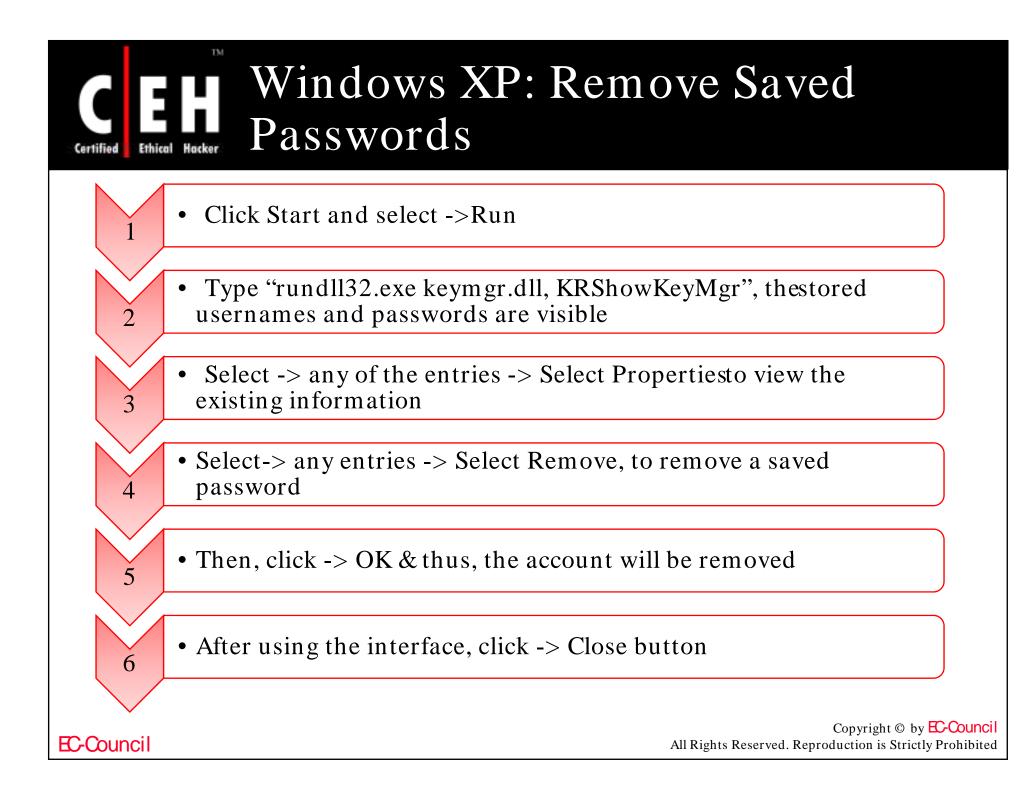
• Dictionaries with hundreds of thousands ofwords, as well as specialist, technical, and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords, such as "qwerty" and "abcdef"













What is a Password Cracker

According to maximum security definition, "A password cracker is any program that can decrypt passwords or otherwise disable password protection"

Password crackers use two primary methods to identify correct passwords: brute force and dictionary searches



A password cracker may also be able to identify encrypted passwords. After retrieving the password from the computer's memory, the program may be able to decrypt it

Modus Operandi of an Attacker Using Password Cracker

The aim of a password cracker is mostly to obtain the root/administrator password of the target system

The administrator right gives the attacker access to files and applications and can install a backdoor, such as a Trojan, for future access to the system

The attacker can also install a network sniffer to sniff the internal network traffic so that he will have most of the information passed around the network

After gaining root access, the attacker escalates privileges to that of the administrator

In order to crack passwords efficiently, the attacker should use a system that has a greater computing power



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited

Certified Ethical Hacker Hocker Hocker

To understand how a password cracker works, it is better to understand how a password generator works

Most of them use some form of cryptography

- Crypto stems from the Greek word kryptos
- *Kryptos* was used to describe anything that was hidden, obscured, veiled, secret, or mysterious
- Graph is derived from graphia, which means writing

Cryptography is concerned with the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers, and other methods, so that only certain people can see the real message

Image: Second Cracker How does a Password Cracker Image: Second Cracker Work (cont'd) Image: Second Cracking is where the cracker runs the cracking program in parallel,

on separate processors. The common way to do this: Break the password file into pieces and crack those pieces on separate machines The wordlist is sent through the encryption process, generally one word at a time Rules are applied to the word and, after each application, the word is again compared to the target password (which is also encrypted) If no match occurs, the next word is sent through the process In the final stage, if a match occurs, the password is then deemed *cracked* The plain-text word is then piped to a file Copyright © by EC-Council EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



The various types of attacks that a hacker performs to crack a password are as follows:

- Dictionary attack
- Hybrid attack
- Brute force attack





Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited





Password Guessing

Password guessing attacks can be carried out manually or via automated tools

Conducting social engineering on the victim may also sometimes reveal passwords

Password guessing can be performed against all types of web authentication

The common passwords used are as follows: root, administrator, admin, operator, demo, test, webmaster, backup, guest, trial, member, private, beta, [company_name] or [known_username]





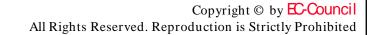
Password Guessing (cont'd)

Most users assign passwords that are related to their personal life, such as their father's middle name, as shown in the screenshot

An attacker can easily fill out the form for forgotten passwords and retrieve the same

This is one of the simplest ways of password guessing

| The Advertise of the Ad | ole Minosoft Internet Bulloren Finontes Tools Help | | 1912 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------|
| Back + -+ - @ |)]] Qtart (fronte Briefs) [] -] [] -] 🛪 😁 | | |
| Address 💽 http://ed | it, vahoo, condiconfigieval, register?, v=8, krtl=Grew=18, dane=6, src=vn8, partner=6, p=8prono=6, last= | 6. K | · Pan Links * |
| Go gle - | - Staarch Web - 😸 Peoplark - Statisticked - Statist | | and the second second |
| | YAHOO! Mail | Yahool - Help | 1 |
| | Sign up for your Yahoo! ID with Mail | Already have an ID? Sign In | |
| | Get a Yahool ID and password for access to Yahool Mail and all other personalized Y | ahool services. | |
| | Yahoo! D: pateror0998877 @yahoo.com Example:: "detymor66" or "treachtyme" | Choosing your ID You will use this information to access Yahool each time. Capitalization matters | |
| | Piessword: Must be six characters or more | for your password | |
| | Re-type Password: | | |
| | Hyou forget your password or need help with your account, you'll need to confirm the following information: | Recalling your personned This information is our only way to verify your identity. To protect your account, | |
| | Security Question: Whet is your tether's middle name? Your Answer: pater | your correct, to provide your account, make ours "Your Accover" is memorable for you but hard for | |
| | Bittiday: March 💌 💷 (Manth DD, YYYY) | others to guess | |
| | Current Email (Optional): | | |
| | Account notices will be sent to this enail address, including new password nequests. | | |
| | First Name: Last Name: | Customizing Vahool Yahool will try to provide more relevant. | |
| | Language & Contant: English - United States | content and advertising based on the intermetion collected on this page and on | |
| | ZIPIPostal Code: 2345 Gender: male | the Valvool products and services you use. | |
| | Industry: Computers/Electronics | | |
| | Specialization: | | |
| | People Search Listing: 🔲 Listing new Yahani Mail address for the | | |
| 🗊 Dane | | | Unknown Zone (Nood) |





The query string is the extra bit of data in the URL after the question mark (?) that is used to pass variables

The query string is used to transfer data between client and server, example:

http://www.mail.com/mail.asp?mailbox=sue&company=abc%20c omSue's mailbox can be changed by changing the URL to: http://www.mail.com/mail.asp?mailbox=joe&company=abc%20c om





EC-Council







Cookies are a popular form of session management

Cookies are often used to store important fields, such as user names and account numbers

All the fields can be easily modified using a program like Cookie Spy

| C:\Documen | ts and Settings | • |
|--------------------------------------|--------------------------------------------------------|------|
| Number of Co | ookies Found: 113 | |
| | | - |
| | | |
| | | |
| | | |
| | | - |
| Where they c | ame from: | • |
| | | |
| 128.242.232 | | |
| <u>128.242.232</u> Date Installed | 142/ | |
| | 142/ 12/25/2002 6:16:05 PM 12/26/2002 5:16:06 PM | |



Dictionary Maker

| ile: D:\downloads\H-MDictionaries.zip | | | Status: Size (bytes): 954465 |
|------------------------------------------------------|----------|-----------|------------------------------------|
| Create Load | Close | Save | Size (words):106187 |
| abodefghijklmnopqrstuvwxyzABCDE Files to process: | | Option: | s: Clear results |
| | | | ile name: H-MDictionaries.zip |
| | | Current f | |
| Add file(s) Clear list | Start Ca | Checked | d words: 47496 weed: Processing |
| Progress: | | | Abou |

This tool can build your own dictionaries to create word lists





Password Cracking Tools

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



Password Crackers Available

LOphtcrack

John The Ripper

Brutus

Obiwan

Authforce

Hydra

Cain And Abel

RAR

Gammaprog

WebCracker

Munga Bunga

PassList

RockXP

SnadBoy

WWWhack

Passwordstate

Atomic Mailbox Password Cracker

Advanced Mailbox Password Recovery

Network Password Recovery

Mail PassView

Messenger Key

MessenPass

Password Spectator Pro

SniffPass

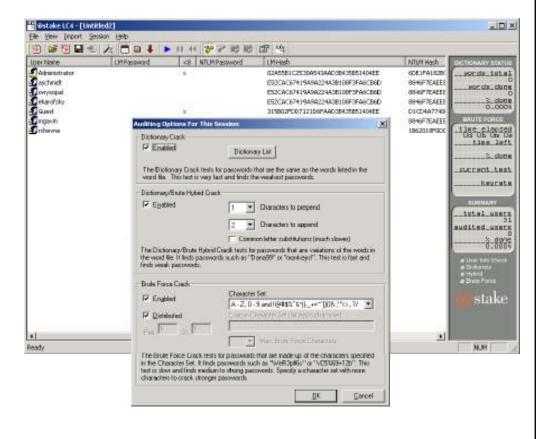
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited

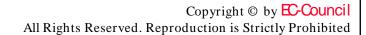


L0phtcrack (LC4)

LC 4 is one of the most popular password crackers available

It recovers Windows user account passwords to access accounts whose passwords are lost or to streamline migration of users to other authentication systems









John the Ripper

浅Fi 竹

Joh

3a

71a;

John the Ripper is a password cracker for UNIX

It combines several cracking modes in one program and is fully configurable

John can crack the following password ciphers:

- Standard and double-length DESbased
- BSDI's extended DES-based
- FreeBSD's MD5-based
- OpenBSD's Blowfish-based

| inished - John | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8. · · · · · · · · · · · · · · · · · · · | Δ |
| n the Ripper Version 1.5 Å | APEA 5 Copyright (c) 1996 by Solar Designer |
| ge: john [flags] [passwd fi. | Lac ¹ |
| <pre>-vorifile:<file> -stiin -tules -incremental[:<mode>] -single -external:<mode> -testcre[:<file>] -makechars:<file> -thow -test -users:<login[uid>],]</login[uid></file></file></mode></mode></file></pre> | <pre>specify passwd file(s) (wildbards allowed) wordlist mode, read words from <file> or stdin enable rules for wordlist mode incremental mode [using [chn.in1 entry <mode>] single crack mode external mode, using john.in1 entry <mode> restore session [from <file>] make a charset, <file> uill be overuritten show cracked passwords perform a benchmark prack this (these) user(s) only crack users with this (these) shell(s) only</file></file></mode></mode></file></pre> |
| -salts:[!] <count> -lamesalts timecut:<time> -list heep quiet -noname -nohash</time></count> | brack salts with at least <count> accounts only assume cleartext passwords were used as salts abort section after a period of (time) minutes list each word beep or don't beep when a paseword is found ion't use memory for login names or hash tables</count> |



Brutus

Brutus is an online or remote password cracker

It is used to recover valid access tokens (usually a user name and password) for a given target system

Features:

- Multi-stage authentication engine 60 simultaneous target connections
- No username, single username, and multiple username modes
- Password list, combo (user/password) list and confgurable brute force modes
- Highly customizable authentication sequences
- It loads and resumes position
- Imports and exports custom authentication types asBAD files seamlessly
- SOCKS proxy support for all authentication types
- HTML Form/CGI authentication types

Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited



EC-Council

Brutus: Screenshot

| e <u>T</u> ools | Help | | |
|-----------------|--------------------------------------------------------------|------------------------|----------------------------------|
| arget 17 | 2.16.105.1 | Type HTTP (B. | asic Auth) 🔽 Pause Stop Cl |
| Connection | | | |
| Port 80 | Connections 1 | 3 Timeout | 10 🗖 Use Proxy Define |
| HTTP (Bas | ic) Options | | |
| Method | | epAlive | |
| | | | |
| | tion Options | | |
| 🔽 Use U | sername 🔽 Single Use | r Pass Mode Brute | Force Range Distributed |
| UserID | admin | Browse Rass File word: | s.txt Browse. |
| ositive Autł | nentication Results | | |
| Target | | Type Usernar | me Password |
| | | | |
| | | | |
| nitialising | | | |
| | 16.105.1 verified will generate 11881376 Pas: | words. | |
| łaximum nu | umber of authentication atter arget 172.16.105.1 with HTT | npts will be 11881376 | |
| | | - (GENEREUM) | |
| 100 | | | eor AuthGeg Throttle Quick Kill |
| | 9% | Timeout Rie | iect AuthSeq Throttle Quick Kill |



Obiwan is based on the simple challengeresponse authentication mechanism

This mechanism does not provide for intruder lockout or impose delay time for wrong passwords

Obiwan uses wordlists and alternations of numeric or alphanumeric characters as possible passwords



Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited



Authforce is an HTTP basic authentication brute forcer

Using various methods, it attempts to brute force user name and password pairs for a site

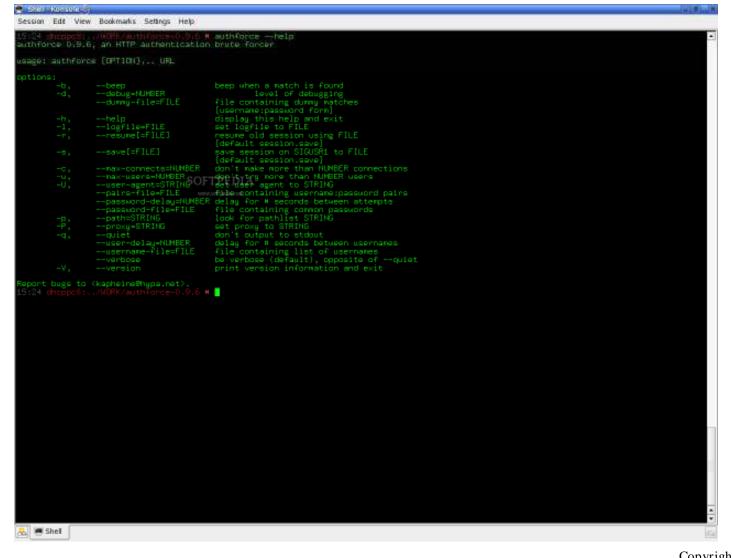
It is used to test both the security of a site and to prove the insecurity of HTTP basic authentication based on the fact that users usually do not choose good passwords





Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited





EC-Council



Hydra supports several protocols like TELNET, FTP, HTTP, HTTPS, LDAP, SMB, SMBNT, MYSQL, REXEC, SOCKS5, VNC, POP3,IMAP, NNTP, PCNFS, ICQ, Cisco auth, Cisco enable, Cisco AAA

Through the paralyzing feature, this password cracker tool can be fast depending on the protocol

This tool allows for rapid dictionary attacks and includes SSL support



Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited



| X-⊨ HydraGTK | | • • × | |
|------------------------------------------------------------------------------------------------------------------|-----------|------------------------------------------------------|-----------------------|
| 🛃 <u>Q</u> uit | | | |
| Target Passwords Tuning Specifi | c Start | | |
| Target | | | |
| Single Target | 127.0.0.1 | | |
| O Target List | | <mark>X-</mark> ⊨ HydraGTK ∲] <u>Q</u> uit | |
| O raiger List | 1 | | |
| Port | 0 | Target Passwords Tuning Specific | Start |
| Protocol | ftp | Username | testuser |
| Output Options | | O Username List | |
| and the second | | Password | |
| Use SSL | ∏ B€ | C Password | |
| Show Attempts | Г | Password List | /tmp/passlist.txt |
| | 5.03 | Colon seperated file | |
| iydra 127.0.0.1 ftp -l yourname -p yo | urpass | Use Colon seperated file | |
| | | I Try login as password | Try empty password |
| | | hydra 127.0.0.1 ftp -I testuser -P /tmp/p | passlist.txt -e ns |
| | | | Copyright © by EC-Cou |

EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited



Hacking Tool: Cain & Abel

Cain & Abel is a password cracking 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 and so on

It contains a feature called APR (ARP Poison Routing), which enables sniffing on switched LANs by hijacking IP traffic of multiple hosts at the same time





| Decoders 👰 Network 🗐 | Sniffer 🥑 Cracker | 🔯 Tracerou | ite 🔝 CCDU | Nº | Wireless | | 201 |
|-----------------------------------------------------------------------------------------|----------------------------------------------------|-------------|------------|-------------|----------|----------------------------------------|-----|
| iched Passwords | Adapter GUID | Descr | Туре | S | Password | Hex | |
| Protected Storage LSA Secrets Wireless Passwords IE7 Passwords | {5E1E6134-9855 {5E1E6134-9855 {5E1E6134-9855 | U.S. Roboti | WEP-40 | T T T | | 5544332211 5544332211 5544332211 | |
| 3 Windows Mal Passwords 2 Edit Boxes 3 Enterprise Manager 4 Credential Manager | | | | | | | |
| | | | | | | | |

EC-Council



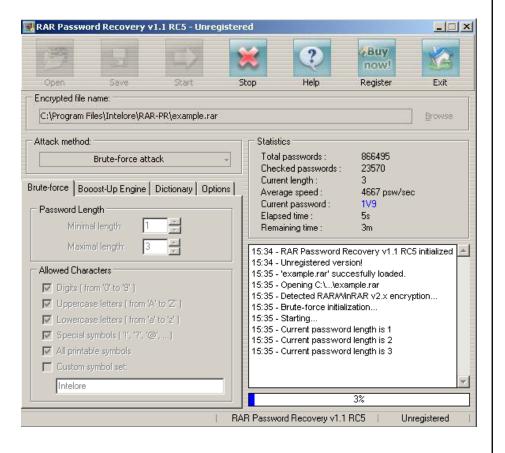
Hacking Tool: RAR

RAR program is intended to recover lost passwords for RAR/WinRAR archives of versions 2.xx and 3.xx

The program cracks passwords by brute force method, wordlist, or dictionary method

The program is able to save the current state

Estimated time calculator allows the user to configure the program more carefully





Gammaprog is a brute force password cracker for web-based email addresses

It supports POP3 cracking as well

It provides for piping support. If the wordlist name is *stdin*, the program will read from *stdin* rather than from a file

It consists of Wingate support for POP3 cracking



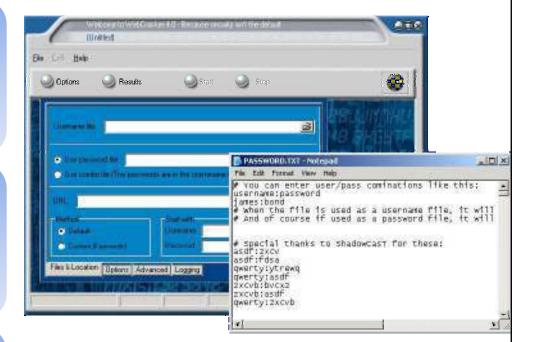
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



Hacking Tool: WebCracker

WebCracker is a simple tool that takes text lists of user names and passwords and uses them as dictionaries to implement basic authentication password guessing

It keys on the "HTTP 302 Object Moved" response to indicate successful guesses



It will find all successful guesses given in a user name/password



| Munga Bunga's HTTP File Process Options | Brute Forcer - Version Help | 1.0.3 (Build | 3) | <u>×</u> |
|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|--------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username to brute force lamer Word List for Passwords C:\Program Files\HTTP Definition File For HTTP | <u>The Hack</u> Number of threads 5 Brute Forcer\pass.lst | | Start/continue brute force Start/continue brute force Start/continue brute force | If disconnected from the internet, pause process, reconnect to the internet, and resume with process, automatically. Don't retry passwords with errors. Onn't process passwords with spaces. |
| | P Brute Forcer\excite.def top Pause These passwords had errors, shall retry later. | | from password number | Don't process passwords containing less then 5 characters. Don't process passwords containing more then 10 characters. Process all passwords as lowercase. Form Method POST Status: Inactive |
| | | | × | |

It's a brute forcer, which uses the HTTP protocol to establish its connections



PassList is another character-based password generator

| PASSLIST.TXT - Not File Edit Format View | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| starwars! starwars" starwars# starwars\$ starwars% starwars% starwars(starwars) starwars; starwars+ starwars, starwars, starwars, starwars, starwars, starwars, | A Help **** Passlist.txt generator for Brute **** "The truth is out there" Do you have a fixed beginning? (Y/N): y Enter string: starwars Enter the maximum number of random characters per password: 2 Yerocessing Processing Process ended |



http://www.snadboy.com

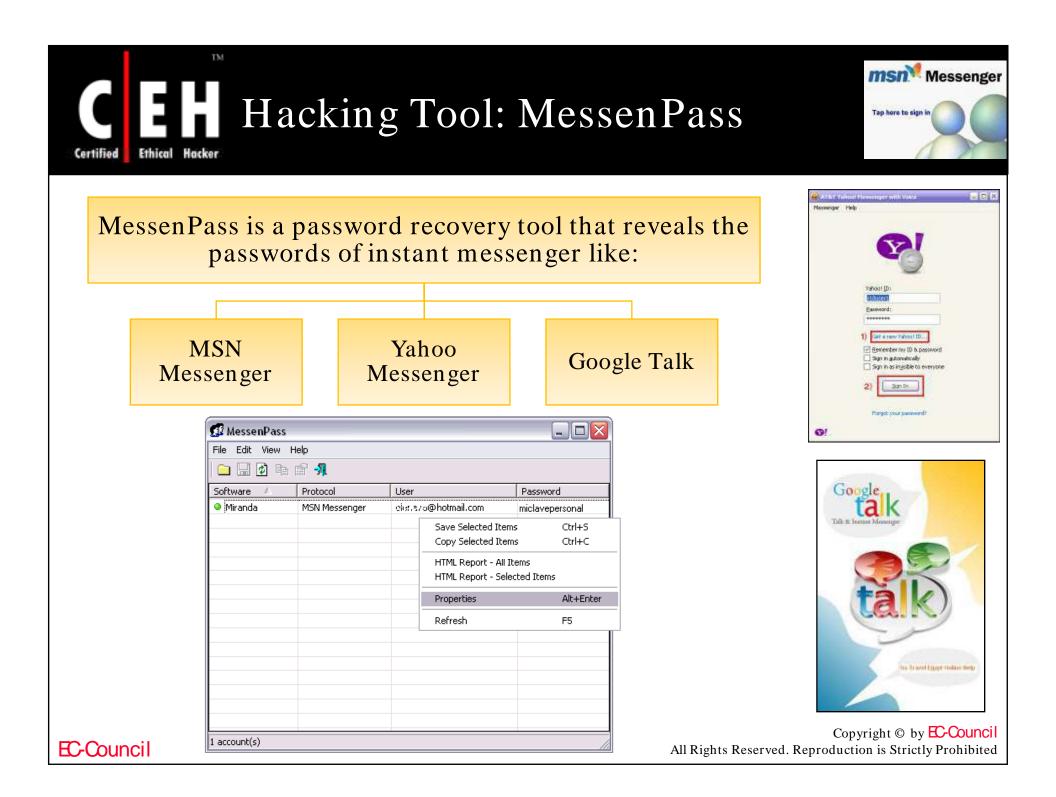
EC-Council

"Snadboy Revelation" turns back the asterisk in password fields to plain text passwords

| Circled +' Cursor Drag to reveal password | Check For Update | About | Exit |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|-----------------------------------|
| Fext of Window Under 'Circled +' Curs | or (if available) | Co | py to clipboard |
| Status Revelation idle. | | Length of | available text: 0 |
| | | - | |
| | 이 집에 가장 이 것이 아주 집에 집에 집에 가장 아주지 않는 것 | I Hide 'How | Always on top |
| Reposition Revelation out of the w When minimized, put in System Transformed How to | 이 집에 가장 이 것이 아주 집에 집에 집에 가장 아주지 않는 것 | I I Hide 'How | Always on top to' instructions |
| When minimized, put in System Tra How to | ay | | |
| When minimized, put in System Tra | ay own the left mouse button) the er different fields on various w | 'circled +' | to' instructions |
| When minimized, put in System Tra How to 1) Left click and drag (while holding do 2) As you drag the 'circled +' cursor ov | bwn the left mouse button) the er different fields on various w e 'Text of Window' box. | 'circled +' ndows, the text | to' instructions |
| When minimized, put in System Tra How to 1) Left click and drag (while holding do 2) As you drag the 'circled +' cursor ov under the cursor will be displayed in th | bwn the left mouse button) the rer different fields on various w e 'Text of Window' box. In you have revealed the text yo n by asterisks (or some other c ctually be asterisks. | 'circled +' ndows, the text ou desire. haracter), the a | to' instructions |

Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited



Hacking Tool: Wireless WEP Key Password Spy

| Wireless WI | P Key Password S | py | | > |
|------------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------|-------------------|-----------------|
| | | 'EP Keys'' to locate and decode all s e ever been access on this compute | | eless WEP Keys |
| Connectio Encryptio | Found On Adapt n Name: linksys n Level: WEP-40 Password: 3b40; | er {DDD57180-6874-48DD |)-B33F-E540CD | DE5C70A} |
| Encryption | n Name: Franksl n Level: WEP-10 Password: 1234 | 4 | | |
| Connectio | n Name: NETGE# | NR | | • |
| - Ethernet Car | d Info Spy | | | |
| Linksys Wi | reless-G USB Net | work Adapter with SpeedBoos | ter - Packet Sche | eduler Miniport |
| | | | | |

Ethical

Certified



RockXP allows you to retrieve your XP product key that you used when you installed Windows XP, as well as keys for other Microsoft products

This can come in very handy if you need to reinstall but have misplaced or lost the CD cover with the serial sticker

In addition, the program also lets you save the product activation to a file

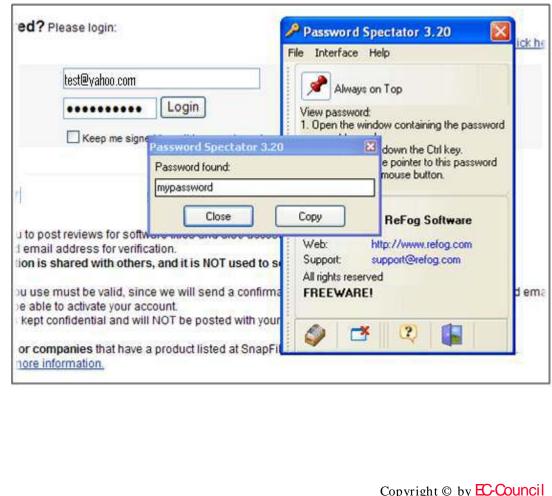
| | RockXP 4.0 by Korben | | |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| | Welcome Windows key Internet Access System's passwords Generate Pass Retrieve your key This feature allow you to retrieve serial numbers of all Microsoft applications installed on your computer Microsoft Windows XP Image: Comparison of the series of th | word About Backup activation files Warning ! This tip works only after a Windows reinstallation (without any format). To avoid Windows XP Reactivation, you just need to save your WPA.dbl in a secure place (ie: on a CD) by clicking on the below button. To restore your activation, you just need to reboot in "safe mode" and to copy backuped files (by RockXP) in Windows\System32 and Windows\system32\dlicache folders, and reboot computer. | |
| | Modify | Backup activation files | |
| -Council | Scan terminated. Si | napfiles.com | Copyright © by <mark>EC-Counci</mark> All Rights Reserved. Reproduction is Strictly Prohibited |



Tool: Password Spectator Pro

Password Spectator is a software that views the actual password behind the asterisks

It works with application passwords, as well as with web site passwords





WWWhack is a brute force utility that tries to crack web sites guarded by a web access password



This utility can use a word file or try all possible combinations

It attempts to find a combination of username/password that is accepted by the web server





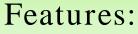
EH WWWhack: Screenshot

| e WWWhack | |
|----------------------------------------|---------------|
| ile Options <u>T</u> ools <u>H</u> elp | |
| 129.168.0.1 | -o× |
| URL: http://129.168.0.1:443/ | |
| Connecting to 129.168.0.1:443 | |
| | |
| | |
| | CAPS (NUM OVR |

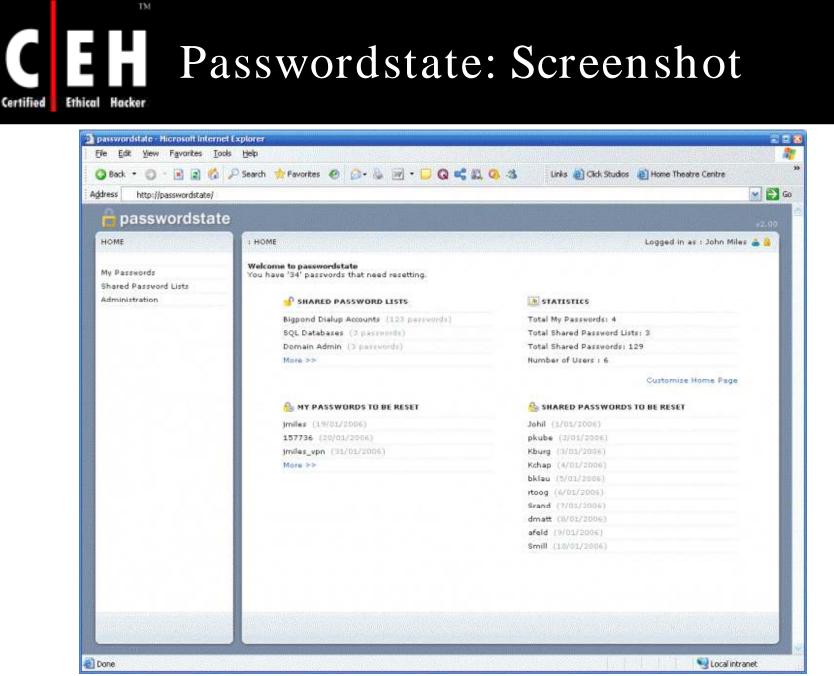


Passwordstate www.clickstudios.com.au

Passwordstate is a web-based solution for tracking both personal passwords for individuals and shared password lists for teams



- Tracks personal and shared password lists
- Encrypts all passwords within the database
- Has reminders for password resets
- Imports and exports password lists



EC-Council



Atomic Mailbox Password Cracker is capable of recovering lost or forgotten mailbox passwords for the e-mail clients that work with mail servers using POP3 and IMAP4 protocols

It recovers the password from the most popular e-mail programs such as Outlook and Outlook Express





Atomic Mailbox Password Cracker: Screenshot

Ethical

Certified

EC-Council

| Atomic Mailbox Passwor | d Cracker - DEMO VERSION 🛛 🔚 🗖 🔀 |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| POP3/IMAP Mailbox Prope | Password Successfully recovered |
| Username John.Doe | Congratulations! Your password is now successfully restored. Please copy the password to Clipboard or remember it. |
| Password | Username : |
| ************************************** | Login |
| | Password : Password |
| | Remember to restore original "POP3 mail server" |
| | Click Back to return |
| Help | < Back Next > Close |

Advanced Mailbox Password Recovery (AMBPR)

Advanced mailbox password recovery recovers login and password information for most popular email clients



It includes POP3 and IMAP server emulator that allows to get POP3/IMAP password from any email client



Advanced Mailbox Password Recovery (AMBPR): Screenshot

| 鸄 Advanced Mail | Box Password Recovery |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recovery | Mail server emulator (auto mode) Use this steps to obtain username and password of your favourite Email client: 1) Add new server (if one doesn't exist) to the list below 2) Click 'Connect' to emulate these servers 3) Rerun (often not required) your Email program and receive mail |
| clients | Servers Add server mail.elcomsoft.com Remove server(s) |
| Automatic passwords recovery | mail.algo-group.com volkov.ru Load list |
| | Save list |
| Manual passwords recovery Mail server emulator (auto mode) | Session log Waiting for IMAP connection Opening POP3 session (28-04-2004 09:37:11) Assigned socket port: 110 Waiting for POP3 connection Starting POP3 session Connected Sending answer Got login name: Got password: |
| Mail server emulator (manual mode) Options | Clear Save Print Copy Connect Cancel |
| Help Exit | |
| Ready | |

Certified

EC-Council

Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited

| Certified Ethical Hacker Tool: Network Password Recovery | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Network password recovery utility recovers all network pass on the system for the current logged-on user | words stored |
| Features: | |
| Recovers login passwords of remote computers on your LAN Recovers passwords of mail accounts on exchange server (stored by Outlook 2003) Recovers password of MSN Messenger account InternetExplorer 7: Recovers passwords of password-protected Web sites | |

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited

Network Password Recovery: Screenshot

Certified

Ethica

| Network Password | Recovery | | |
|------------------------------------------------------|------------------------------------|-----------------------------------|----------------------------------------------------------------------|
| <u>File E</u> dit <u>V</u> iew <u>H</u> elp | | | |
| 🔜 🐼 🗈 😭 🔕 | -71. | | |
| Item Name 🔺 | Туре | User | Password |
| | Domain Password | srv\admin1 | hyyu7TRF5 |
| Server05 Server08 | Domain Password Domain Password | Server05\User01 domain\nirsoft | 6tgR51 hy1tRerr5 |
| ▲ 3 item(s), 1 Selected | | | |
| -Council | | All Rights Res | Copyright © by EC-Counc served. Reproduction is Strictly Prohibit |



Tool: Mail PassView

Mail PassView is a password-recovery tool that reveals the passwords and other account details for the following email clients:

- Outlook Express
- Microsoft Outlook 2000 (POP3 and SMTP Accounts only)
- Microsoft Outlook 2002/2003 (POP3, IMAP, HTTP andSMTP Accounts)
- IncrediMail
- Eudora
- Netscape 6.x/7.x
- Mozilla Thunderbird
- Group Mail Free
- Yahoo! Mail If the password is saved in Yahoo! Messenger application
- Hotmail/MSN mail If the password is saved in MSN Messenger application
- Gmail If the password is saved byGmail Notifier application or by Google Talk

Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited



Mail PassView: Screenshot

| 👸 Mail PassVie | w | | | | | | |
|--------------------------------|-----------------|---------------------|------------------|------|---------|----------|--|
| <u>Eile E</u> dit <u>V</u> iew | <u>H</u> elp | | | | | | |
| | | | | | | | |
| Name 🛆 | Application | Email | Server | Туре | User | Password | |
| 🖾 Mr. Bean | Eudora | mrbean@mrbean.com | 10.10.10.10 | IMAP | bean | BlueCar | |
| 🖾 Nir Sofer | Outlook Express | nirsoft@abcdefg.com | mail.abcdefg.com | POP3 | nirsoft | 126abf1P | |
| 🖾 Rainbow | IncrediMail | rainbow@test.com | 192.168.12.12 | SMTP | rainbow | tornado | |
| 🚟 Test User | IncrediMail | test@test.com | 192.168.10.10 | POP3 | test | BigDog86 | |
| • | | | | | | | |
| 4 item(s), 1 Select | ed . | | | | | | |



Tool: Messenger Key

Messenger key program recovers passwords for ICQ, MSN, Google Talk, and Yahoo! instant messengers

Features:

- Supports all versions of Mirabilis ICQ starting with ICQ 99
- Supports Mirabilis ICQ Lite
- Supports MSN Messenger and Yahoo! Messenger
- Supports Google Talk
- Has password recovery engine through which all paswords are recovered instantly
- Supports multilingual passwords







EC-Council



SniffPass is a tool that listens to your network, captures the passwords that pass through your network adapter, and displays them on the screen instantly

It captures the passwords of the following protocols:

- POP3
- IMAP4
- SMTP
- FTP
- HTTP





SniffPass: Screenshot

| | | h 🕜 🖏 👖 | | | | | |
|----|------|---------------|--------------|-------|-----|--------|----------|
| [n | Prot | Local Address | Remote Addr | Local | Rem | User | Password |
| 1 | POP3 | 192.168.0.1 | 192.168.39.5 | 6814 | 110 | nir5 | Ju7y651 |
| 2 | HTTP | 192.168.0.1 | 192.168.4.3 | 6851 | 80 | user01 | jdie748 |
| 3 | IMAP | 192.168.0.1 | 192.168.7.1 | 6713 | 143 | nirsof | 123456 |
| | | | 111 | | | | |
| | | | | | | | |
| | | | | | | | |





Security Tools





WebPassword

WebPassword is a program that protects your web pages with password (HTML password protector)

Unauthorized person will not be able to view its content without having a correct password, either in browser, or as an original HTML source

Features:

- Uses strong crypto algorithm
- Protected pages could be placed on a web server, CD/ DVD, or hard disk
- E-book compiler allows to create password-protected e-books



WebPassword: Screenshot

| C:\Tempfiles\KCB\htdocs\nl1-00.html C:\Tempfiles\KCB\htdocs\permits.html | | | iti are | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------|--|
| C:\Tempfiles\KCB\htdocs\permitsprint. | | | - <u>1</u> | |
| C:\Tempfiles\KCB\htdocs\sunsetpark. | | i i i i i i i i i i i i i i i i i i i | | |
| • | | <u> </u> | | |
| Save list to | Open list Add lis | st from | ~ | |
| ۔ لیسیسیسی Please drag-and-drop html documents you v | want to | ar list | 51 | |
| protect from the explorer onto this screen | 1775 | | | |
| | th these pages? | | and the second | |
| What do you want to do wit | | | | |
| Protect them (encrypt) C Remove | e protection (decrypt) | | | |
| | | | | |
| Protect them (encrypt) C Remove 1-2-3 Web password | e protection (decrypt) | | | |
| Protect them (encrypt) C Remove | e protection (decrypt) | | | |
| Protect them (encrypt) C Remove 1-2-3 Web password | e protection (decrypt) place the result pages? | | | |
| Protect them (encrypt) Remove 1-2-3 Web password Ready to gol Where do you want me to gol Save protected (encrypted) in the specific section of the specific | e protection (decrypt) place the result pages? <u>ecified directory</u> | | | |
| Protect them (encrypt) Remove 1-2-3 Web password Ready to gol Where do you want me to gol Save protected (encrypted) in the sp C:\TEMPFILES\ | e protection (decrypt) place the result pages? ecified directory Bro | wse | | |
| Protect them (encrypt) Remove 1-2-3 Web password Ready to gol Where do you want me to Save protected (encrypted) in the sp C:\TEMPFILES\ Upload pages directly into my server destination URL including target director | e protection (decrypt) place the result pages? ecified directory Bro (via FTP protocol) | | | |
| Protect them (encrypt) Remove 1-2-3 Web password Ready to gol Where do you want me to go Save protected (encrypted) in the sp C:\TEMPFILES\ Upload pages directly into my server | e protection (decrypt) place the result pages? ecified directory Bro (via FTP protocol) | | | |
| Protect them (encrypt) Remove 1-2-3 Web password Ready to gol Where do you want me to Save protected (encrypted) in the sp C:\TEMPFILES\ Upload pages directly into my server destination URL including target director | e protection (decrypt) place the result pages? ecified directory Bro (via FTP protocol) | | | |
| Protect them (encrypt) Removes 1-2-3 Web password Ready to gol Where do you want me to a second second | e protection (decrypt) place the result pages? ecified directory Bro (via FTP protocol) | | | |
| Protect them (encrypt) Removes 1-2-3 Web password Ready to gol Where do you want me to a second second | e protection (decrypt) place the result pages? ecified directory Bro (via FTP protocol) y (for example: | | | |

EC-Council



Password Administrator is a secure password and account manager that enables you to store all your sensitive logins and account information in an encrypted database

Features:

- Database search
- Login reports
- Import/export
- Password expiration
- Built-in password generator





Password Administrator: Screenshot

| Password Administra | tor - test | | | | | | | |
|-----------------------------------------|------------|-----|----------|---------|--------------|------------|---------------|----------------|
| <u>Eile Edit View Groups Pa</u> | sswords H | elp | | | | | | |
| Open GROUPS ADD EDIT | PASSWO | DEL | Generate | Reports | s Options | Log | Find | Exit |
| Search | Q 🗌 | Des | cription | | Info | Note | s 📔 🥜 Histo | ory |
| - 📋 Banking / Investing | Amazo | on | | | ID 💕 | | | |
| - C Email Accounts - C Misc Accounts | eBay | | | | JoeTester | ł | | |
| - C Shareware | | | | | Password | | | |
| - 🗋 Web Discussion Boards | | | | | **** | | | |
| - 🔄 Web Sites | | | | | Date Expi | res 🛄 | Date As | signed |
| | | | | | July 22, 200 | 5 👻 | July 29, 2 | 004 💌 |
| | | | | | E-mail | | | |
| | | | | | test@web | attack.co | n | |
| SnapFiles Pro | 358 | | | | Web Addr | ess | | |
| | | | | | www.goo | ogle.com | (- | |
| | | | | | Web Addr | ess 2 | | |
| | | | | | Aller and | | | |
| | | | | | ID 2 | | | |
| | • | | | | | | | |
| 3 items in Web Sites | | | | | Unregistere | d Evaluati | ion - 30 day: | s remaining // |

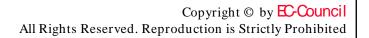
EC-Council



Password Safe is a password manager that protects your sensitive information with the TwoFish encryption algorithm

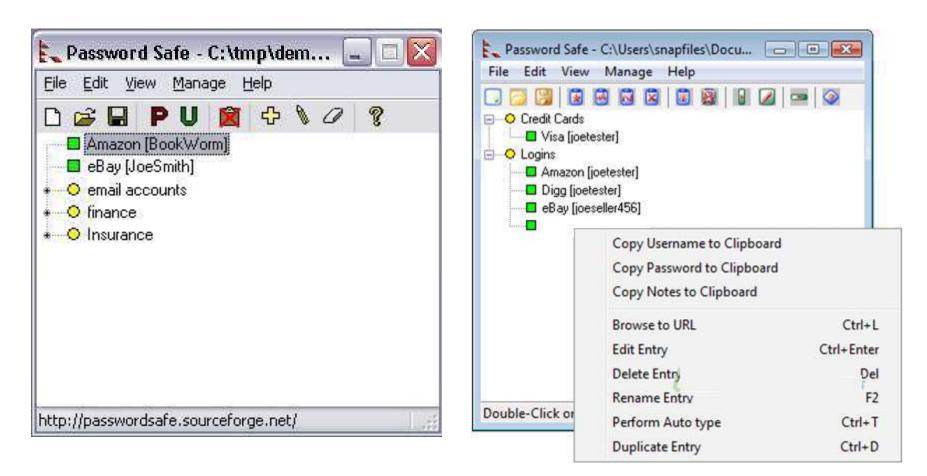
> It enables you to store all your passwords in one or more encrypted databases and accesses them with a master password

> > It allows you to manage your old passwords and to easily and quickly generate, store, organize, retrieve, and use complex new passwords





Password Safe: Screenshot





Easy web password enables you to password protect your web pages without the need for any server side software or scripting



It can select the pages to the protected, set up user accounts and passwords, and generate password protected version of your HTML files

> It works with HTML and text file and is compatible with all modern web browsers

CEH Easy Web Password: Screenshot

Ethical Hacker Certified

TM

| Easy Veb Pas | sword | | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------|-------------|------|----------|
| roject <u>H</u> elp | | | | | |
| 🗃 🔛 🛛 🍙 🛛 | 0 | 7 | | | |
| Select Files User/P | | Continue Linety L | | | |
| Delect Tiles USER/P | asswuru | | | | |
| Add files | dd folder | r Remove file | Remove all | | |
| | uu iuluei | | Kentove all | | |
| FileName | Size | Path | | | <u>^</u> |
| 🕘 acctest.htm | 20 KB | F:\sapi4\acctest.htm | | | |
| ど activex.htm | 5 KB | F:\sapi4\activex.htm | | | |
| 🕘 allapp.htm | 18 KB | F:\sapi4\allapp.htm | | | |
| 🕘 answer.htm | 3 KB | F:\sapi4\answer.htm | | | |
| 📱 apidoc.htm | 2 KB | F:\sapi4\apidoc.htm | | | |
| 🕘 audindex.htm | 5 KB | F:\sapi4\audindex.htm | | | |
| 🕘 audiosd.htm | 3 KB | F:\sapi4\audiosd.htm | | | |
| 🕘 basiccmd.htm | 1 KB | F:\sapi4\basiccmd.htm | | | |
| 🙆 basictts.htm | 1 KB | F:\sapi4\basictts.htm | | | |
| 🔄 build.htm | 4 KB | F:\sapi4\build.htm | | | |
| 🕘 burger.htm | 1 KB | F:\sapi4\burger.htm | | | |
| 🗟 checkmic.htm | 2 KB | F:\sapi4\checkmic.htm | | | |
| 🕘 collect.htm | 10 KB | F:\sapi4\collect.htm | | | |
| 🕘 cool.htm | З КВ | F:\sapi4\cool.htm | | | |
| 🕘 coolcnc.htm | 2 KB | F:\sapi4\coolcnc.htm | | | ~ |
| and the second s | ם אי ר | Filennial cooldist htm | | | <u> </u> |
| | | | step IV. | 1. | 1 |
| | | | Back | Next | Exit |
| | | | | - | Cop |



All Rights Reserved. Reproduction is Strictly Prohibited



PassReminder is a secure password manager that allows you to maintain an encrypted database, containing all your passwords and login information

Features:

- Include import/export options
- Clipboard security
- Password generator





| 🚮 PassReminder 0.6.1 - C | Documents and | d Settings\\ | AIO\My Documents | def 🔳 🗖 🚺 | × |
|-------------------------------------------------------|---------------|--------------|-------------------|--------------|---|
| File Edit Window Help | | | | | |
| : 📬 🗁 🔛 : 🖻 🖻 🖥 | i 🕂 📃 🗟 🗯 | 1 | | | |
| shopping | Service | User | Password | URL | |
| @ Email accounts @ Email accounts @ Recycle Bin | 🧟 Amazon | joe | **** | www.amazon.c | |
| | ises B&H | johndoe | **** | www.bhphotov | |
| | 🛼 ebay | joetester | **** | www.ebay.com | |
| | | | 💠 Add Entry | Insert | |
| | | | 📃 View Entry | | |
| | | | 😪 Edit Entry | Enter | |
| | | | 💢 Remove Entry | Delete | |
| | | | 📄 Duplicate Entry | Ctrl+D | |
| | | | Move | • | |
| | | | 🔗 Search | Ctrl+F | |
| | | | 📄 Smart Copy | Ctrl+C | |
| | | | 📄 Copy Password | Ctrl+P | |
| | | | Copy User | Ctrl+U | |
| | | | Password Column | F12 | |
| New cell 'User' selected | | snapfiles | .com | | |



My Password Manager

My Password Manager allows you to store all your passwords and logins in a 256 bit AES encrypted database

> It supports custom categories, web links, and password expiration and has built-in password generator

> > It creates backup copies of your database, enhances security by wiping the clipboard at exit, and auto-locks the interface after a period of time



Certified Ethical Hacker My Password Manager: Screenshot

| 🙆 Untitled - My Passwor | d Manager | | | | | | |
|--------------------------------------------------------------------------------|-------------|--------------|--------------------------------|------------------------|---------|--------------------------------|---|
| Project View Folder Ac | count Tools | Help | | | | | |
|) D 🧉 • 🖬 🗛 🛛 I | 1 🗷 🗠 🕹 | 3 P | • | 2 | | | |
| | Title | 1. | Login | Pas | sword | URL | |
| All Folders Programs Programs Meb Sites Mail Miscellaneous | 🖋 eBay 🔰 | | Joe Tester JT 1Tester345 | - Atalenka Atalenka | e# | www.snapfilesp www.ebay.com | |
| | 😭 Amazon | Account | ll offer (a) | | | Lunun smaton re | |
| | | Folders | 🗀 Web Sites | 🛅 Web Sites 💌 | | | |
| | | Title | google | | | | |
| | | Login | Joe Tester | | | | |
| | | Password | fr1kTn6453E1 | | | | |
| | | URL | www.google. | .com | | | |
| | (14) | File/Program | n | | | | |
| l Ready | < | Date Added | 6/ 1/2004 | ~ | Expired | 6/ 1/2004 💌 |] |
| | | Note | | | | | 0 |
| | | | | | | | 3 |
| | | | | | ОК | Cancel | 0 |



Choose passwords that have at least eight characters

Passwords should have a combination of lower- and upper-case letters, numbers, special characters, etc.

Do not use words that can be easily found in a dictionary as passwords

Do not use public information, such as social security number, credit card number, and ATM card number as passwords

Never use personal information as passwords

User names and passwords should be different

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



Managers and administrators can enhance the security of their networks by setting strong password policies. Password requirements should be built into organizational security policies

Systems administrators should implement safeguards to ensure that people on their systems are using adequately strong passwords

When installing new systems, make sure default passwords are changed immediately



The user can use the SRP protocol

- SRP is a secure password-based authentication andkeyexchange protocol
- It solves the problem of authenticating clients toservers securely, where the user of the client software is required to memorize a small secret (like a password) and carries no other secret information





It took 5 minutes for Ron to run 200000 words to brute force the ftp password.

Jason Springfield, an Ethical Hacker was called in by *XChildrelief4u Welfare Organization*. Jason inspects the log file of the web server and finds a last entry which shows that log file was deleted. Jason was sure that the attacker had escalated the administrative privilege.

Jason tries different kinds of attacks such as Dictionary attack, guessing, brute force attack.

Based on the result obtained from the above attacks, Jason recommends the following:

- Integration of strong password requirement into the Organization's security policy
- Ensuring that SRP protocol and key-exchange protocol are implemented
- Ensuring that no personal and easily guessed phrases are set as passwords



Authentication is the process of checking the identity of the person claiming to be the legitimate user

HTTP, NTLM, egotiate, Certificate-based, Forms-based, and Microsoft Passport are the different types 0f authentications

Password crackers use two primary methods to identify correct passwords: brute force and dictionary searches

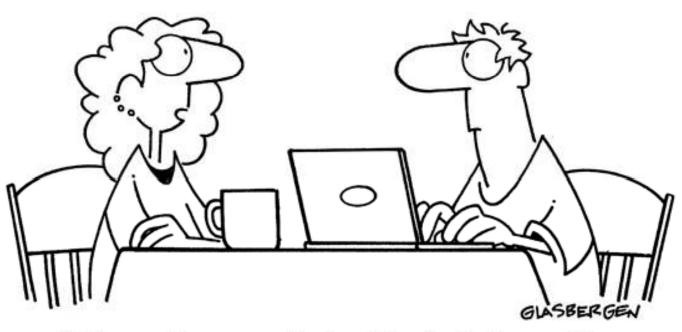
LOphtcrack, John the Ripper, Brutus, Obiwan, etc. are some of the popular passwordcracking tools available today

The best technique to prevent the cracking of passwords is to have passwords that are more than eight characters long and to incorporate upper- and lower-case alphanumeric, as well as special characters into them

Copyright © by **EC-Council** All Rights Reserved. Reproduction is Strictly Prohibited



Copyright 2005 by Randy Glasbergen. www.glasbergen.com



"Information security is a big deal at my office so sometimes we have to communicate in code. We have 37 different symbols for the word 'jerk'."





"Sorry about the odor. I have all my passwords tattooed between my toes."

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



Copyright 2004 by Randy Glasbergen. www.glasbergen.com



"I shut my eyes when I need to remember one of my passwords. I have them tattooed inside my eyelids."

EC-Council