# Ethical Hacking and Countermeasures

Version 6

## Module XVIII

## Web-based Password Cracking Techniques

abcNEWS

# 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

# Scenario

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.


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

# Module Objective

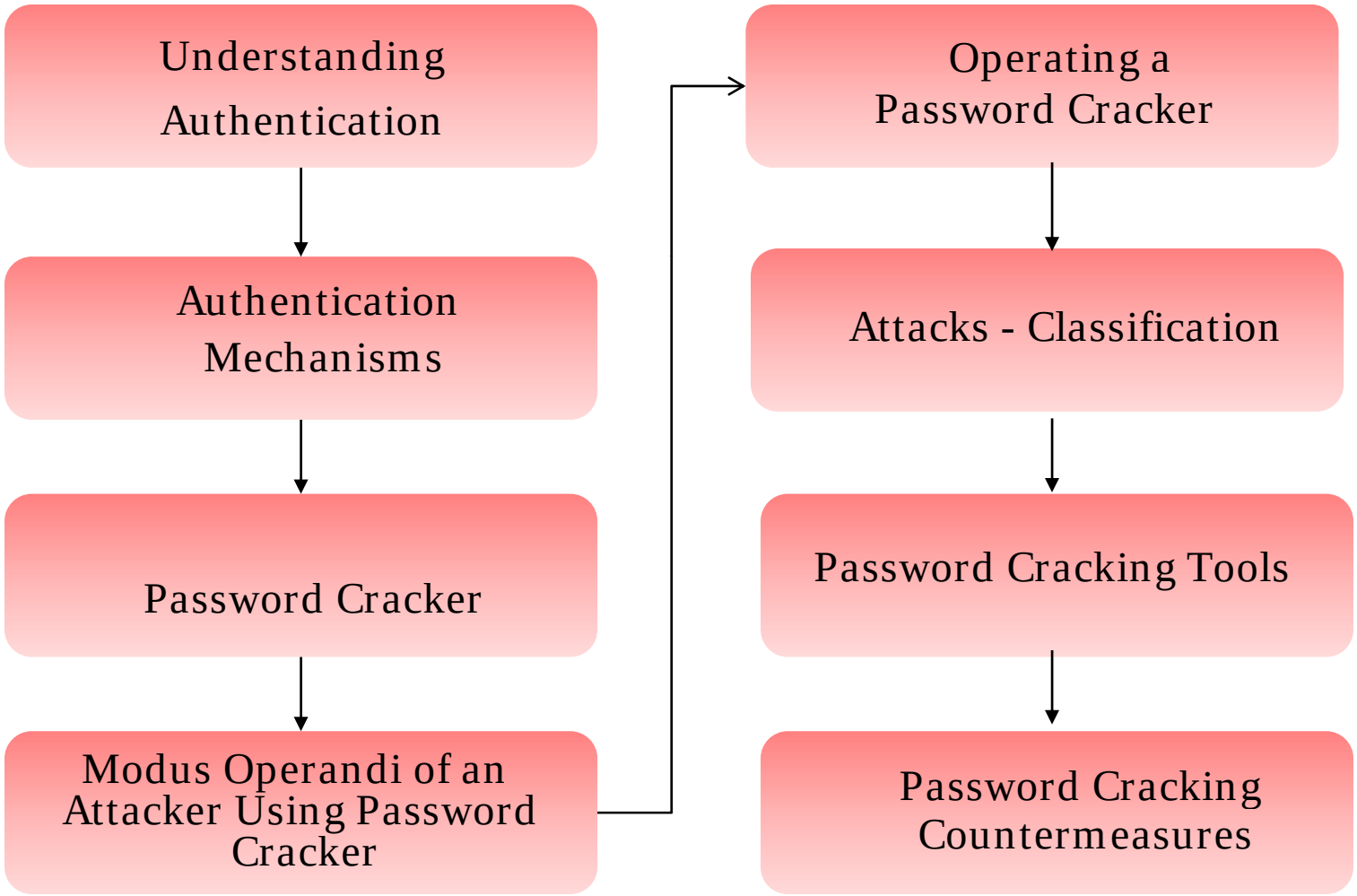
This module will familiarize you with :

- Authentication
- Authentication Mechanisms
- Password Cracker
- Modus Operandi of an Attacker Using Password Cracker
- Operation of a Password Cracker
- Classification of Attacks
- Password Cracking Tools
- Password Cracking Countermeasures



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

# Module Flow




EC-Council

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

# 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

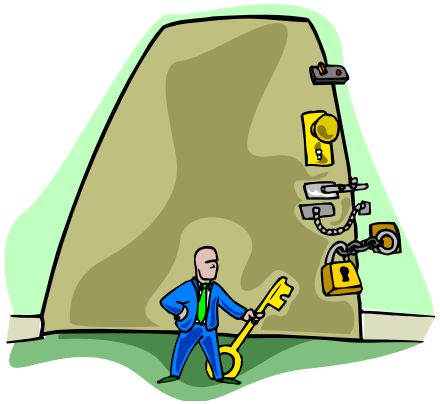
Passwords can often be stolen, accidentally revealed, or forgotten due to inherent loopholes in this type of authentication

EC-Council

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

# Authentication Mechanisms

- HTTP Authentication
  - Basic Authentication
  - Digest Authentication



- Integrated Windows (NTLM) Authentication
- Negotiate Authentication
- Certificate-based Authentication
- Forms-based Authentication
- RSA Secure Token
- Biometrics

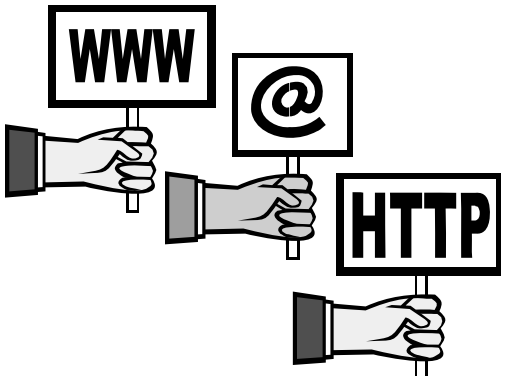
EC-Council

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

# HTTP Authentication

There are two techniques for HTTP authentication:

- Basic
- Digest



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

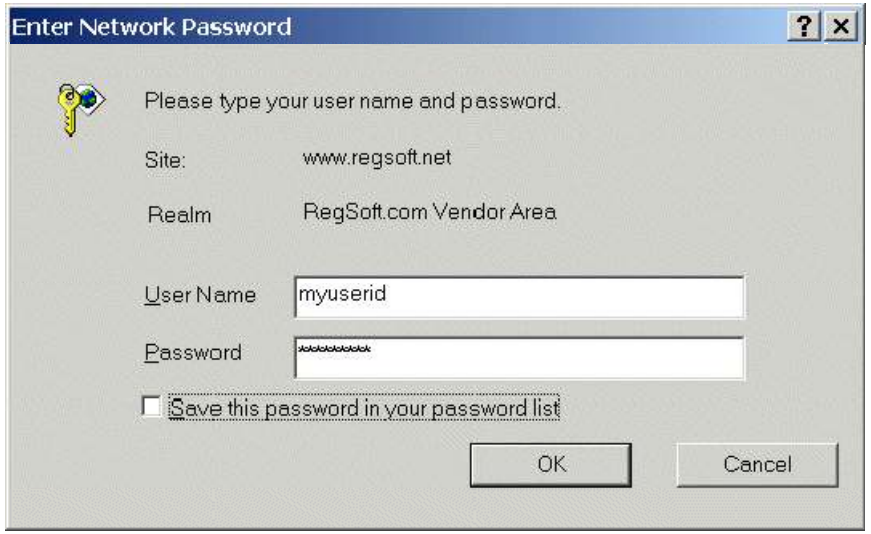
# Basic Authentication

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



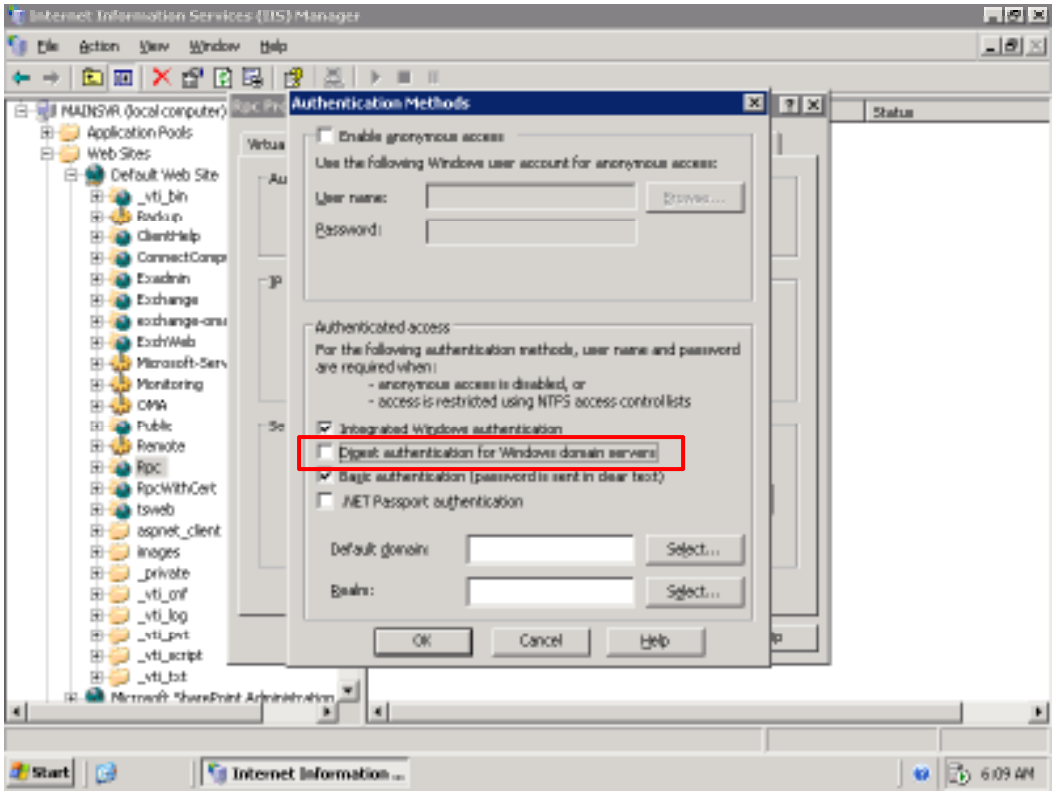
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Digest Authentication

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

It is based on the *challenge-response* authentication model

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






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

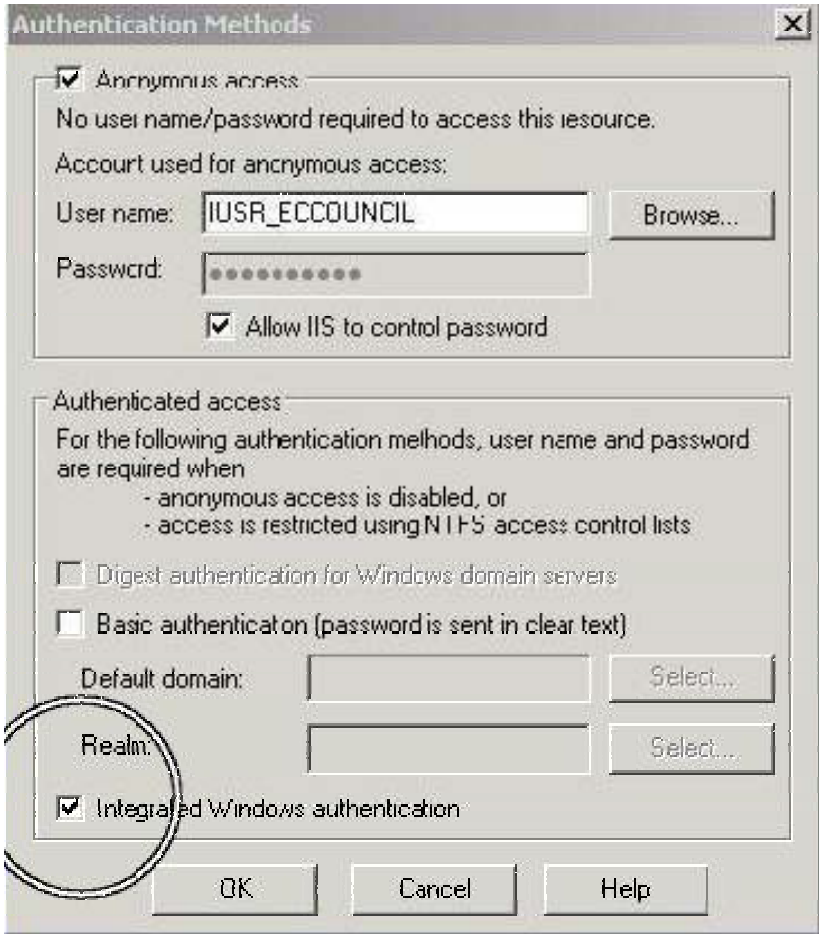
# Integrated Windows (NTLM) Authentication

It uses Microsoft's proprietary NT LAN Manager (NTLM) authentication program over HTTP

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






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

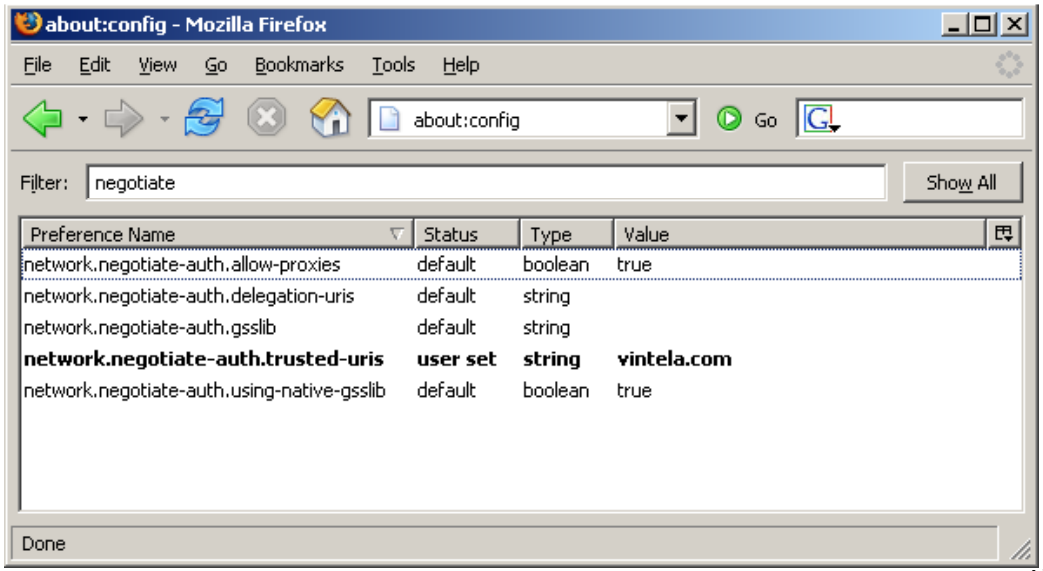
# Negotiate Authentication

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






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

# 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 two-factor 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

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

# Certificate-based Authentication (cont'd)

EC-Council

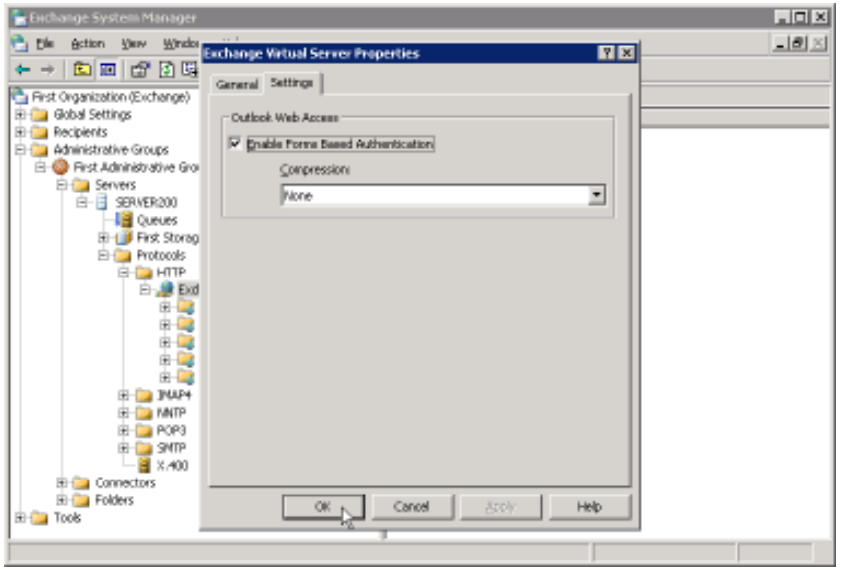
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# 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

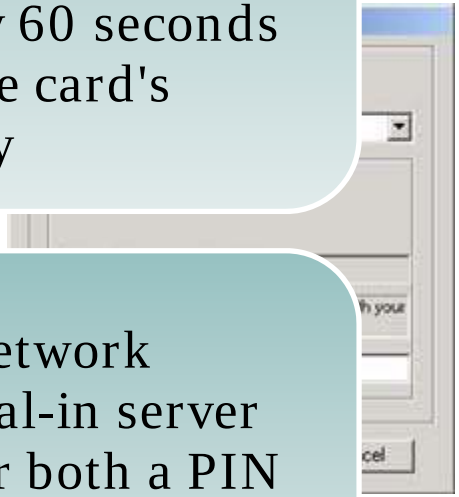





Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# RSA SecurID Token

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



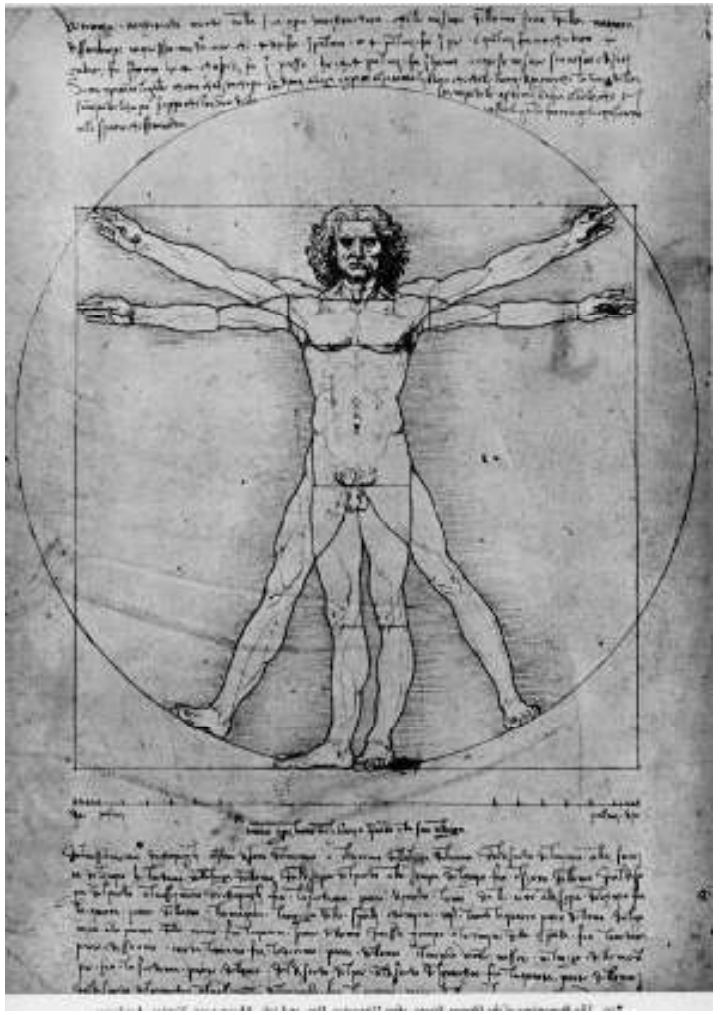
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Biometrics Authentication

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



EC-Council

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

# Biometrics Authentication (cont'd)

EC-Council

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

# Types of Biometrics Authentication

Face Recognition

Iris Scanning

Retina Scanning

Fingerprinting

Hand Geometry

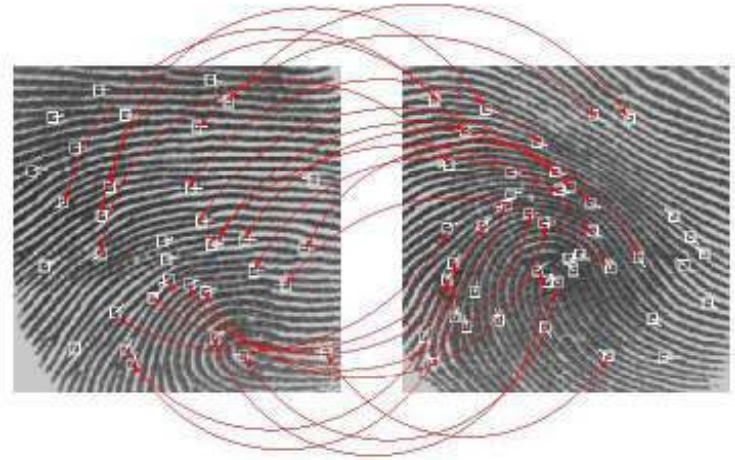
Voice Recognition

EC-Council

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

# 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

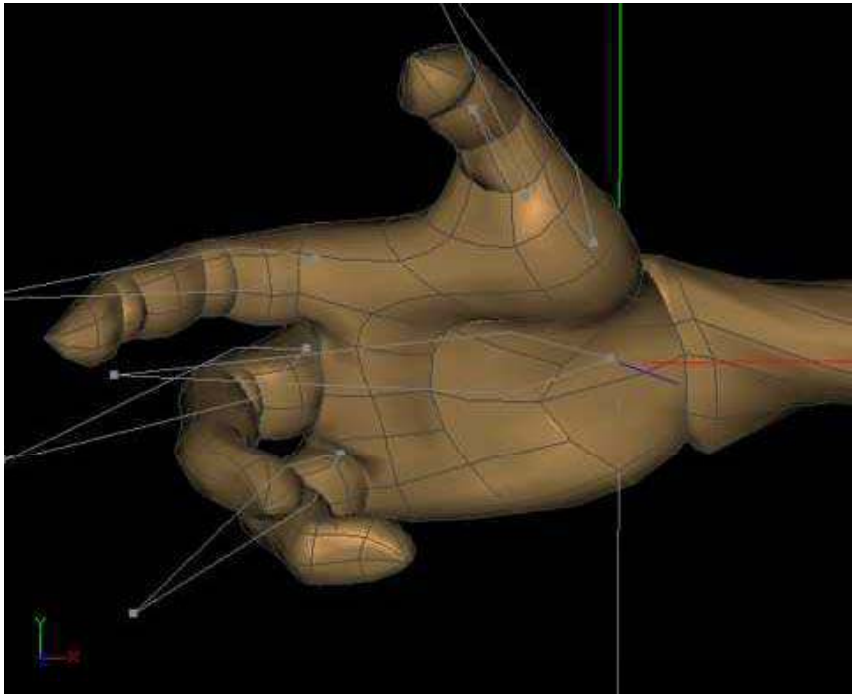




Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Hand Geometry-based Identification

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

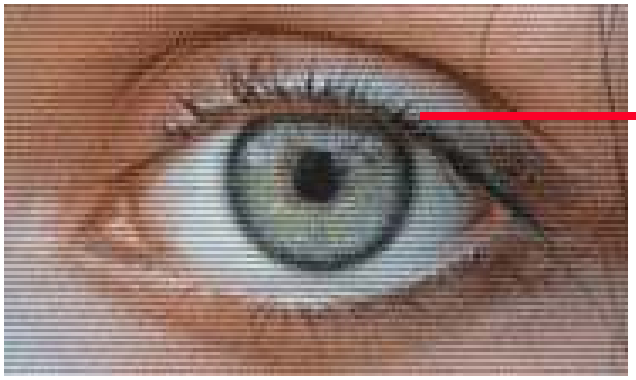


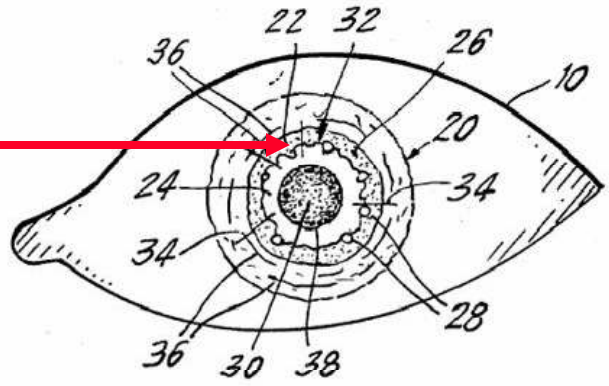
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Retina Scanning

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






EC-Council

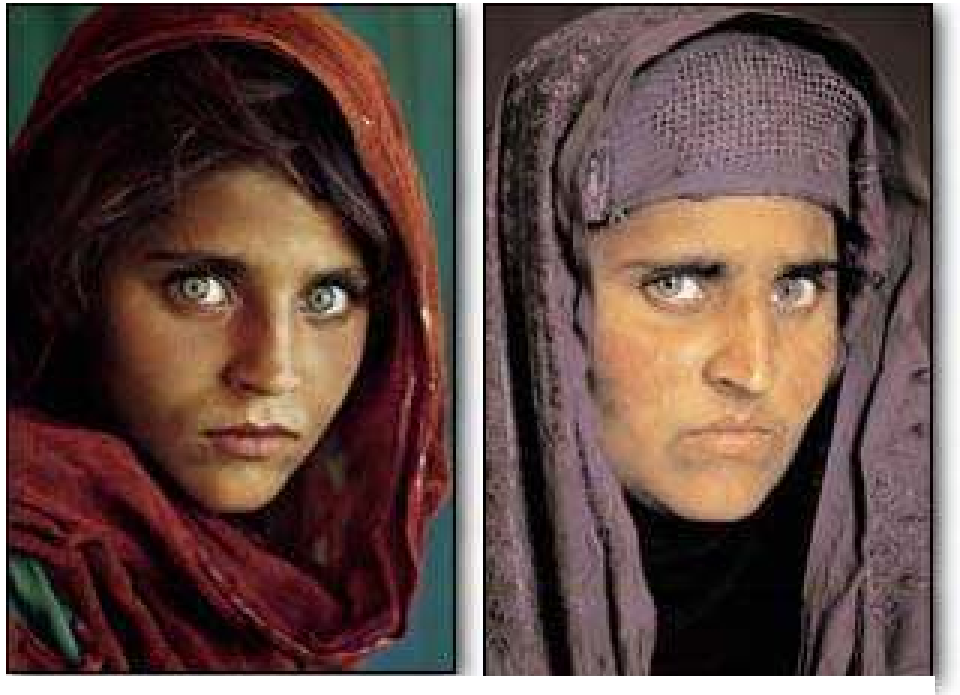
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# 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



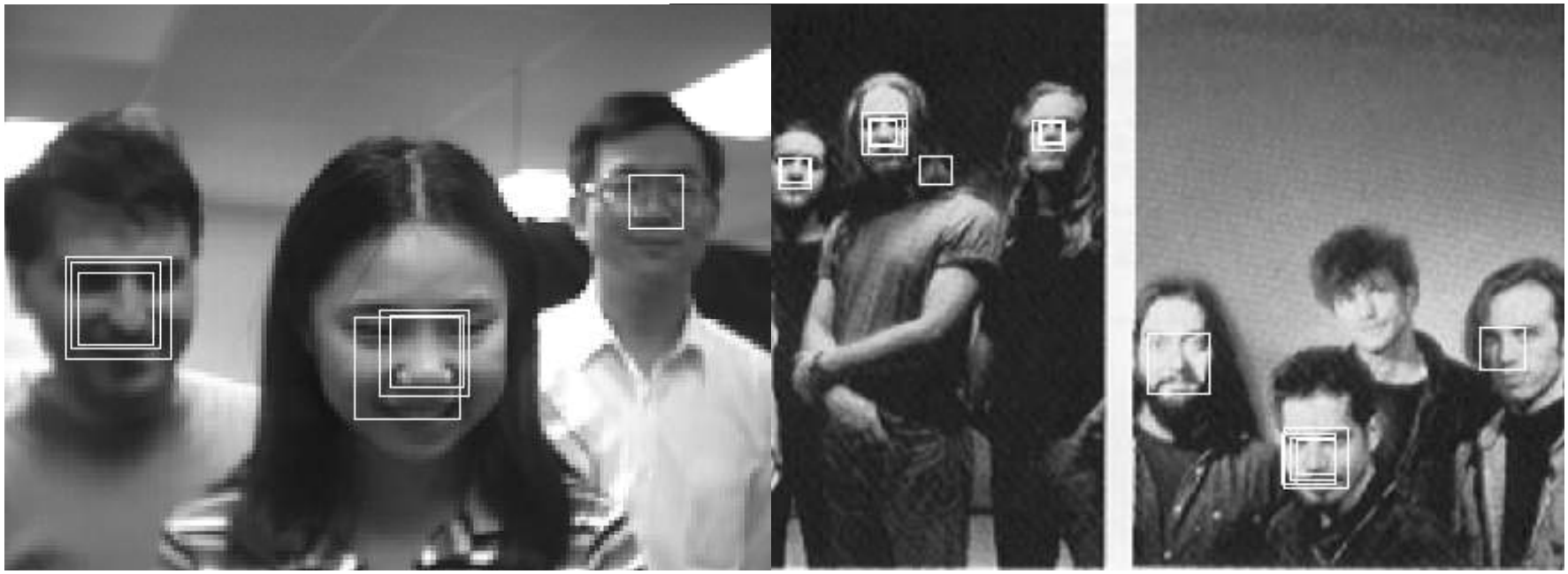
EC-Council

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

# Face Recognition

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

It is difficult to implement





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

# 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

EC-Council

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

# Facecode: Screenshot

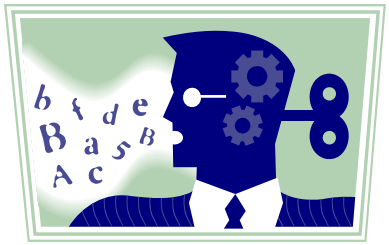
EC-Council

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

# 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. "

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



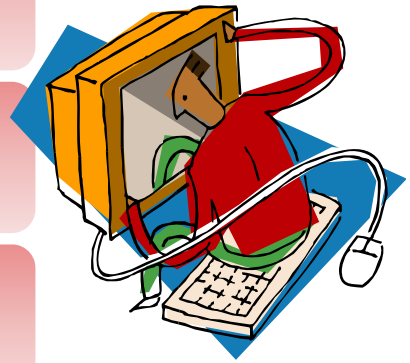
# Password Cracking



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

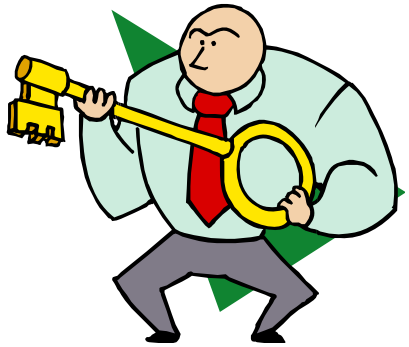




Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Things to Avoid in Passwords

- 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 **e** to **3**, **L** or **i** to **1**, **o** to **0**, as in "z3r0-10v3"





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

# Changing Your Password

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

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

# Protecting Your Password

- 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

EC-Council

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

# 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
- “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

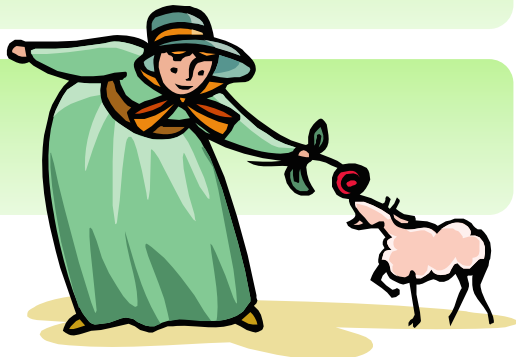
Consider a phrase: "*Mary had a little lamb. The lamb had white fleece.*"

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

- 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-letter 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 of words, 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"

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

# Windows XP: Remove Saved Passwords

1. Click Start and select ->Run
2. Type “rundll32.exe keymgr.dll, KRShowKeyMgr”, thestored usernames and passwords are visible
3. Select -> any of the entries -> Select Propertiesto view the existing information
4. Select-> any entries -> Select Remove, to remove a saved password
5. Then, click -> OK & thus, the account will be removed
6. After using the interface, click -> Close button

EC-Council

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

# 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

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

# Modus Operandi of an Attacker Using Password Cracker

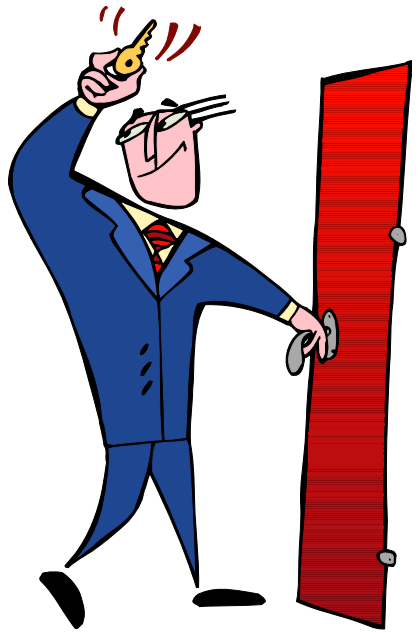
The aim of a password cracker is mostly to obtain the root/ administrator password of the target system

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



EC-Council

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

# How does a Password Cracker Work

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


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

# How does a Password Cracker Work (cont'd)

Distributed 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
All Rights Reserved. Reproduction is Strictly Prohibited

# Attacks – Classification

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

- Dictionary attack
- Hybrid attack
- Brute force attack

EC-Council

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

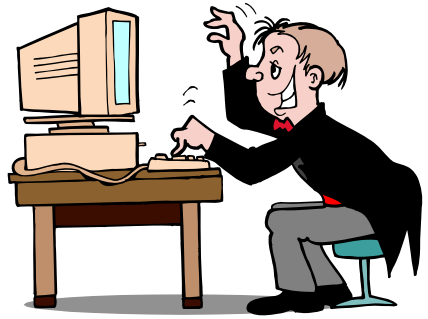
# Password Guessing

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]



EC-Council

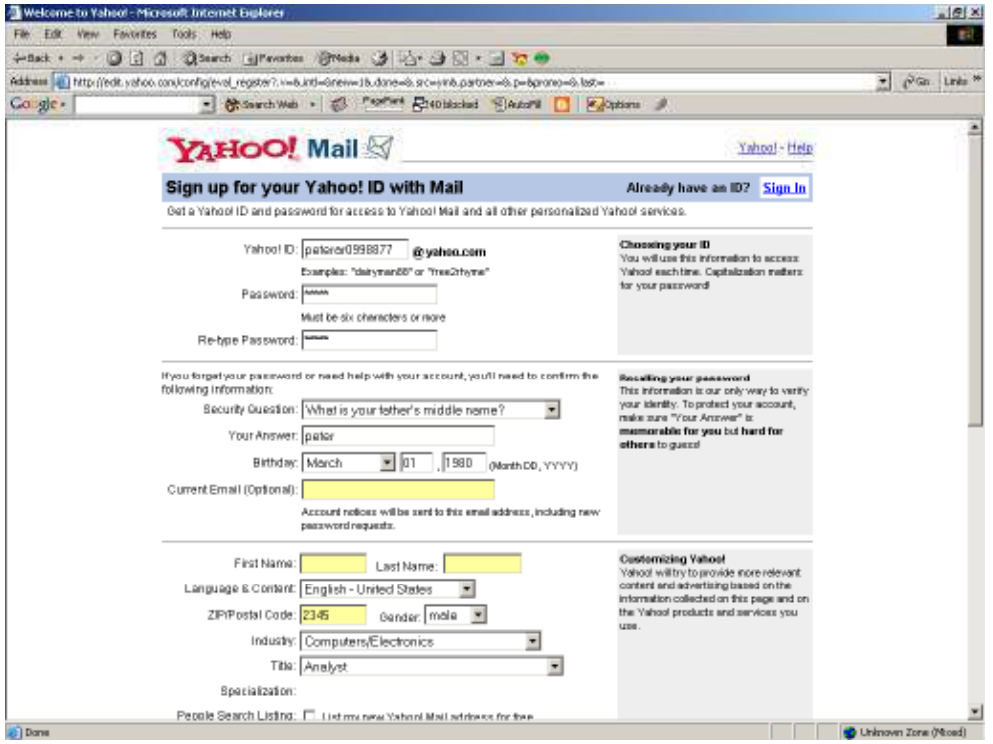
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# 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






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

# Query String

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

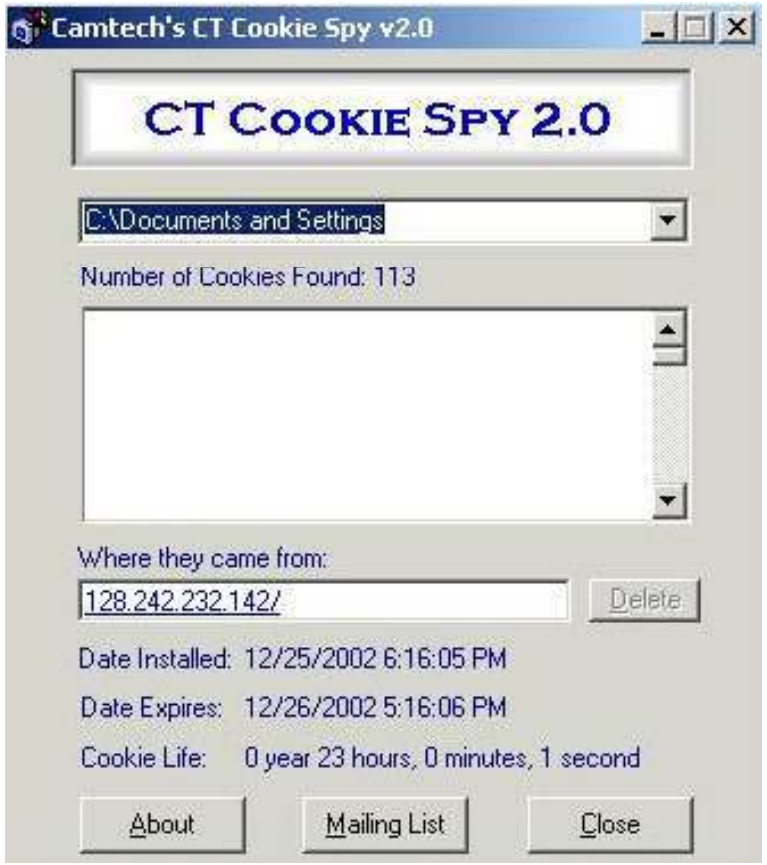
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Cookies

Cookies are a popular form of session management

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

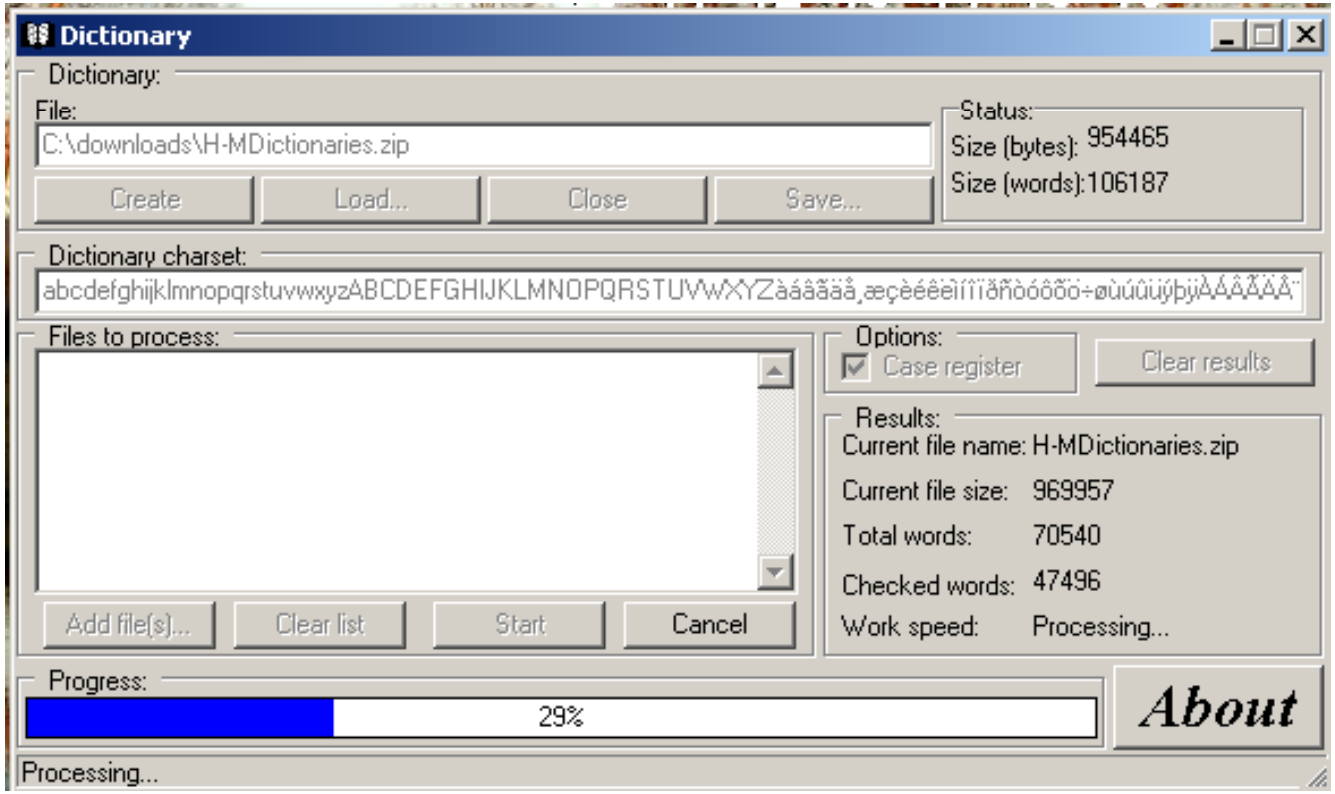
All the fields can be easily modified using a program like Cookie Spy






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

# Dictionary Maker




This tool can build your own dictionaries to create word lists

EC-Council

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

# 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

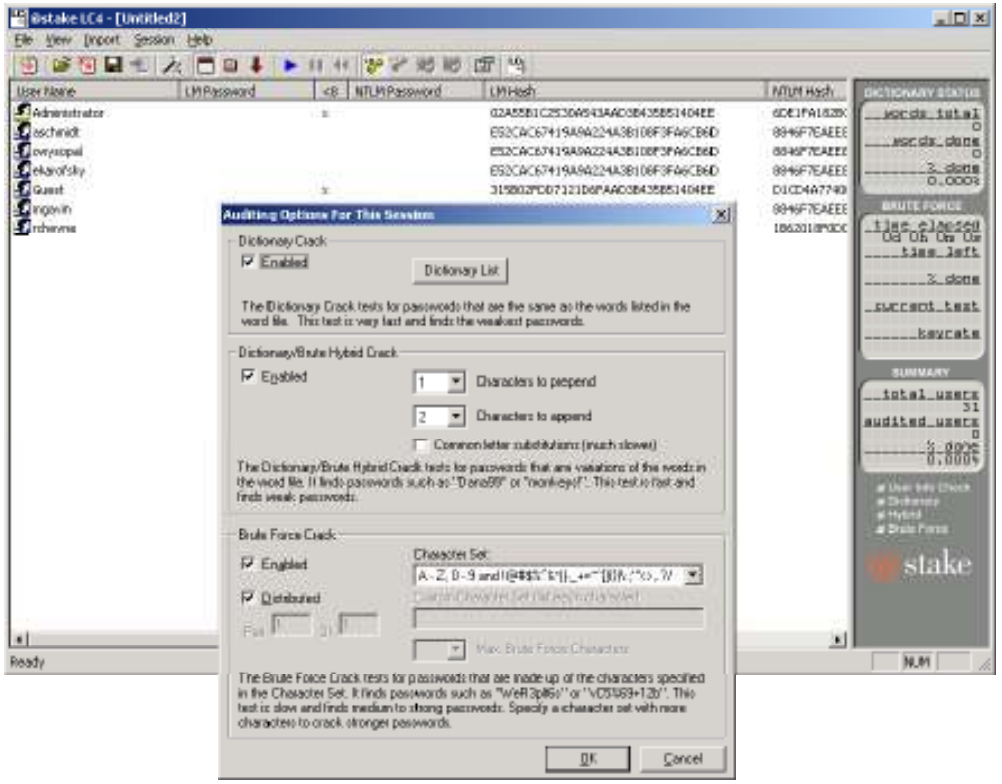
EC-Council

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



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

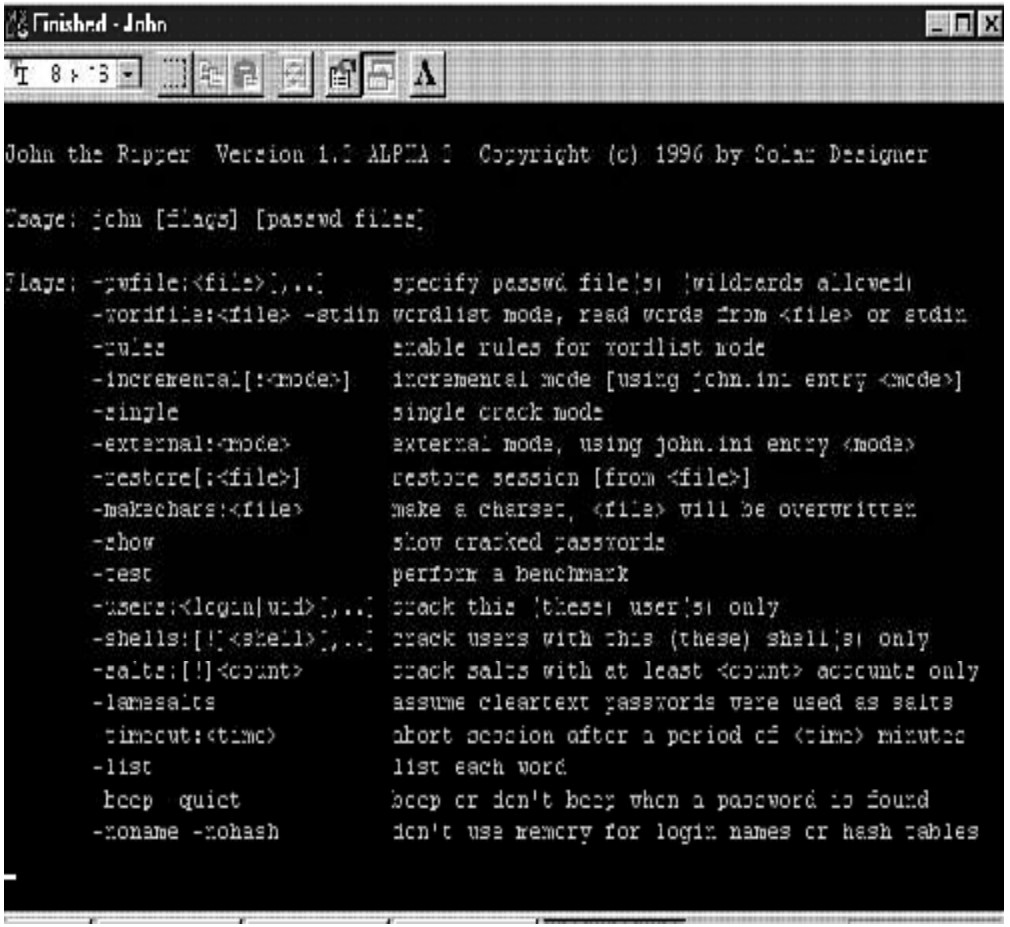
# John the Ripper

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 DES-based
- BSDI's extended DES-based
- FreeBSD's MD5-based
- OpenBSD's Blowfish-based






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

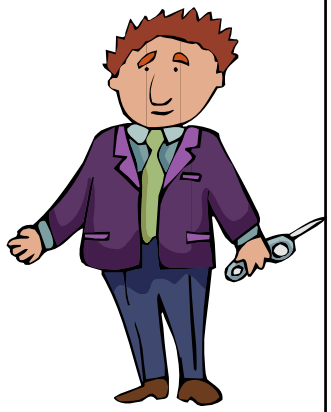
# Brutus

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:

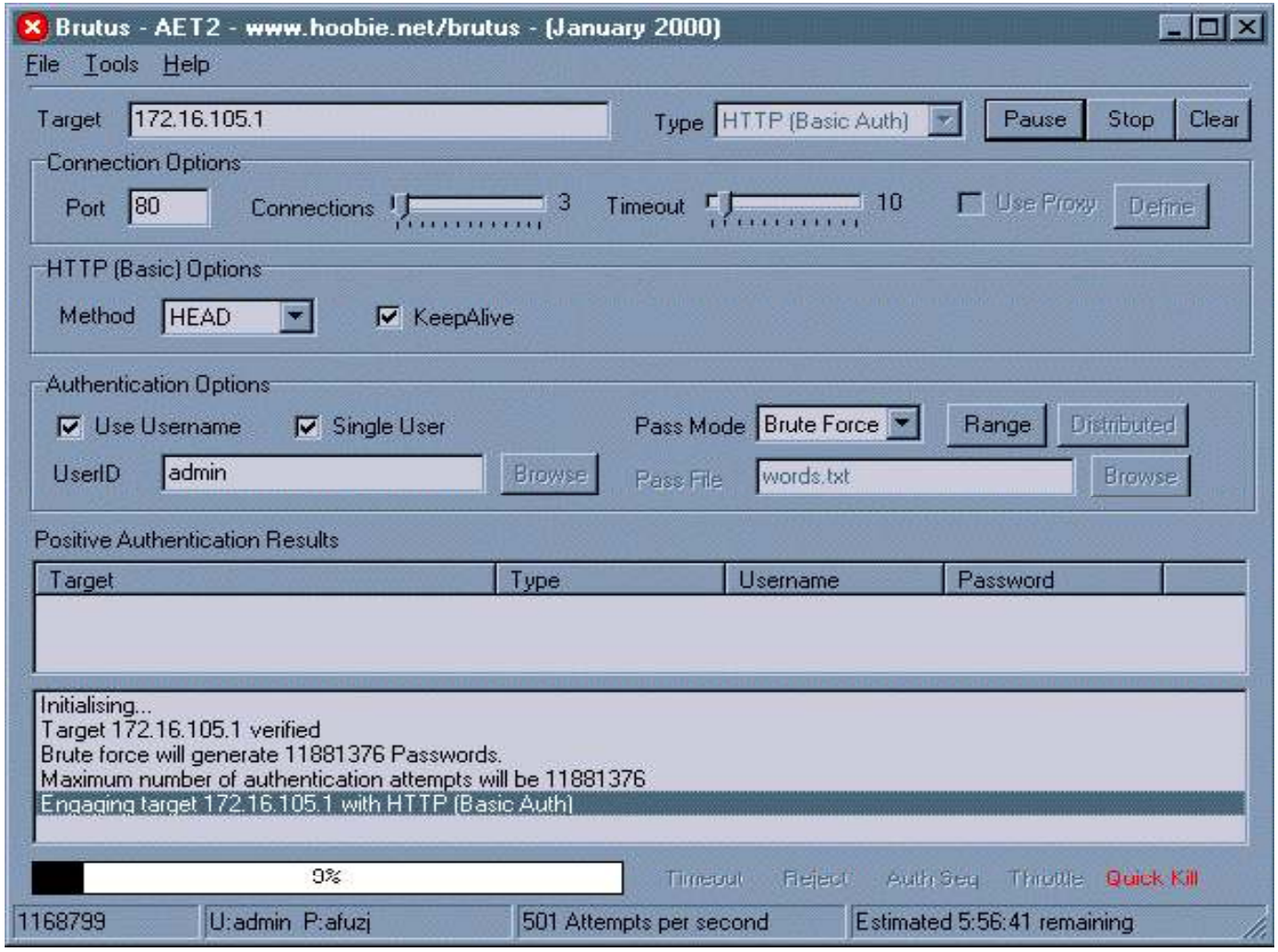
- Multi-stage authentication engine 60 simultaneous target connections
- No username, single username, and multiple username modes
- Password list, combo (user/password) list and configurable brute force modes
- Highly customizable authentication sequences
- It loads and resumes position
- Imports and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



EC-Council

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

# Brutus: Screenshot





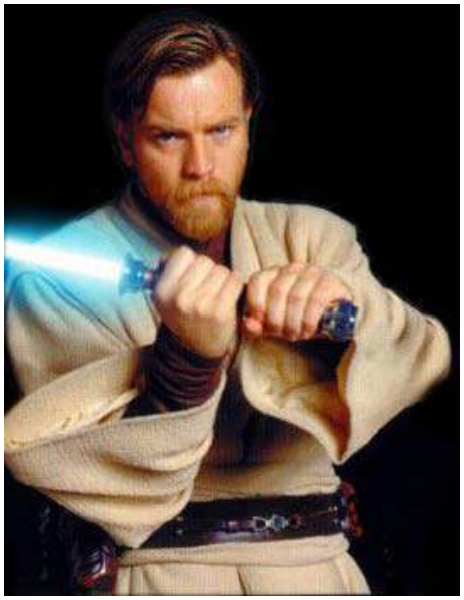

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Hacking Tool: Obiwan

Obiwan is based on the simple challenge-response 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



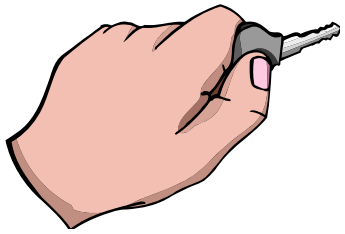
EC-Council

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

# Hacking Tool: Authforce

Authforce is an HTTP basic authentication brute forcer

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

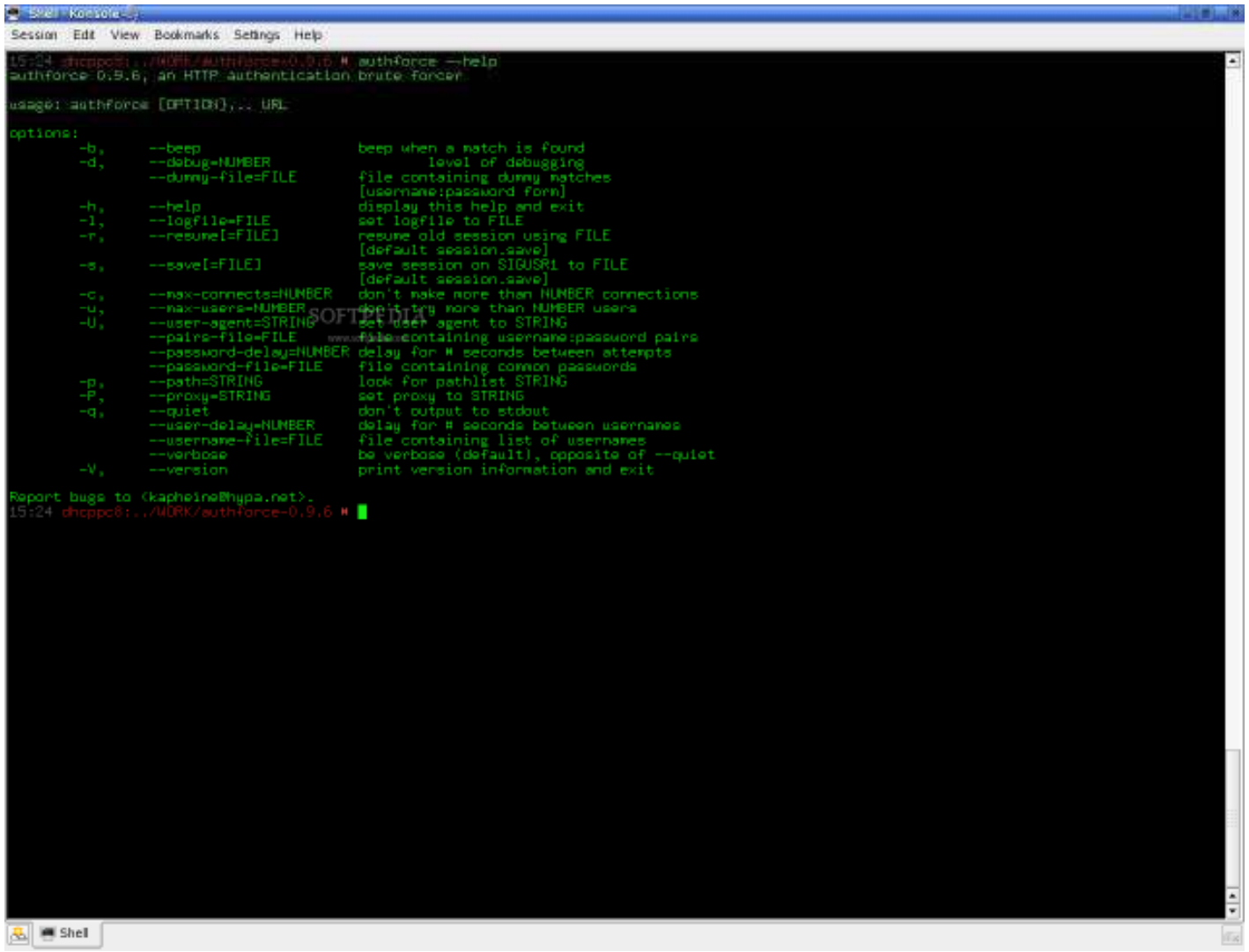


It is used to test both the security of a site and to prove the insecurity of HTTP basic authentication based on the fact that users usually do not choose good passwords



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

# Authforce: Screenshot




EC-Council

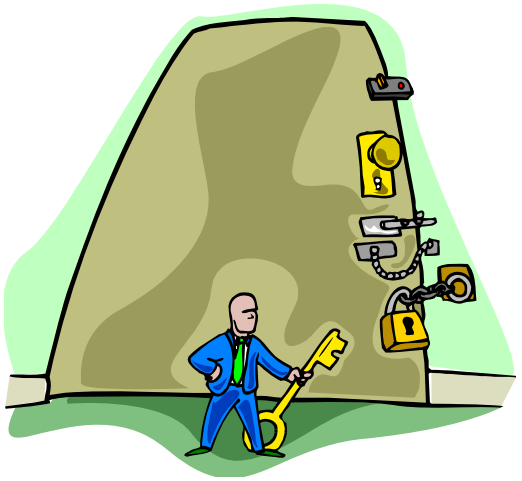
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Hacking Tool: Hydra

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

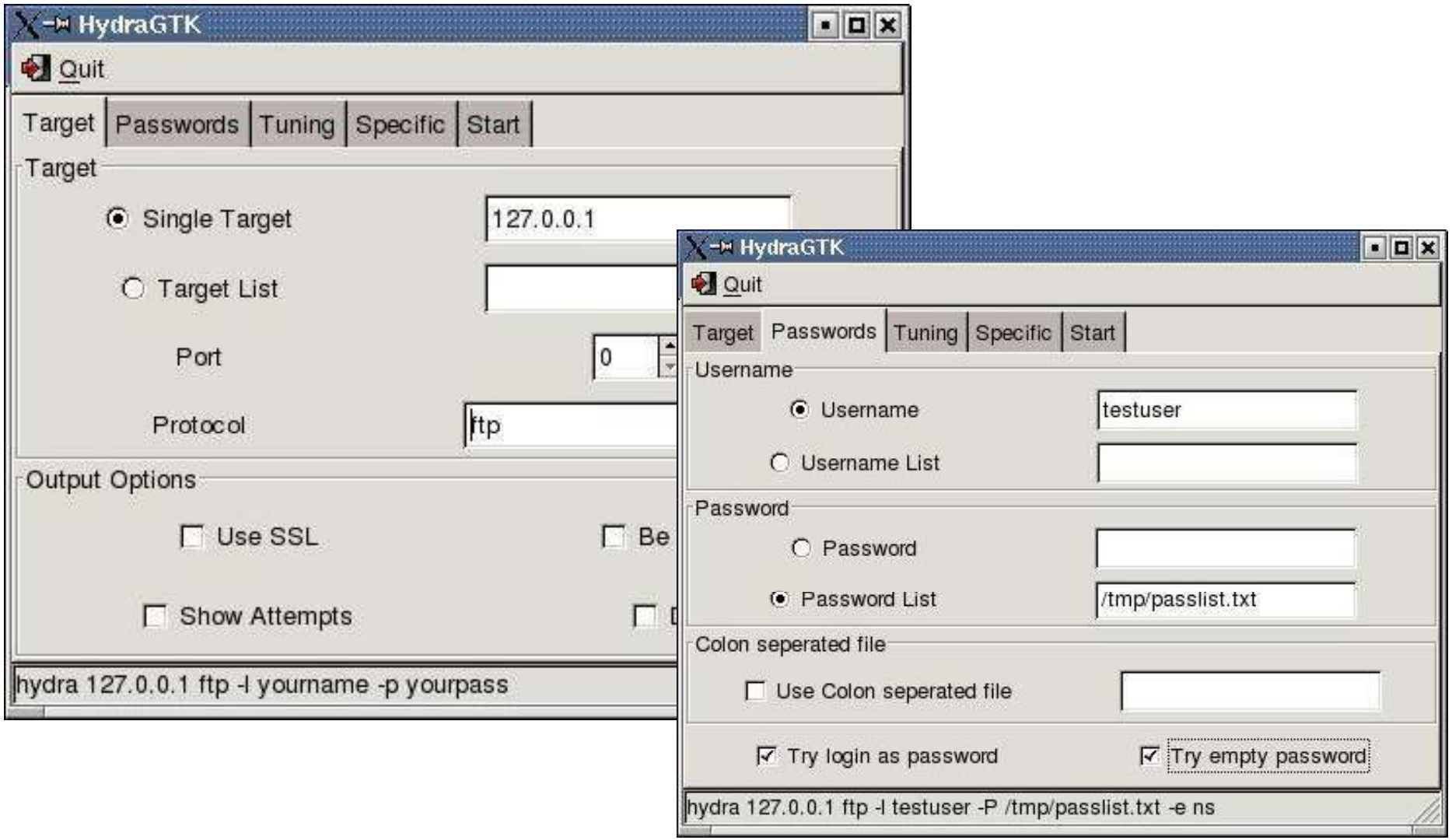
This tool allows for rapid dictionary attacks and includes SSL support





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

# Hydra: Screenshot



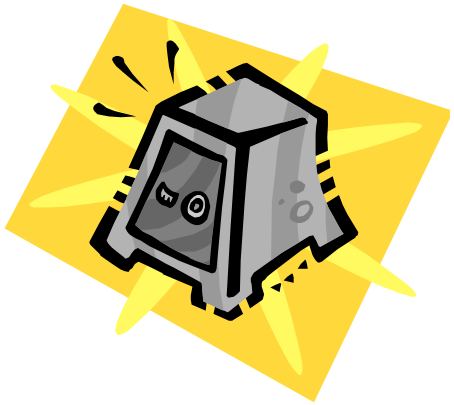



Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# 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

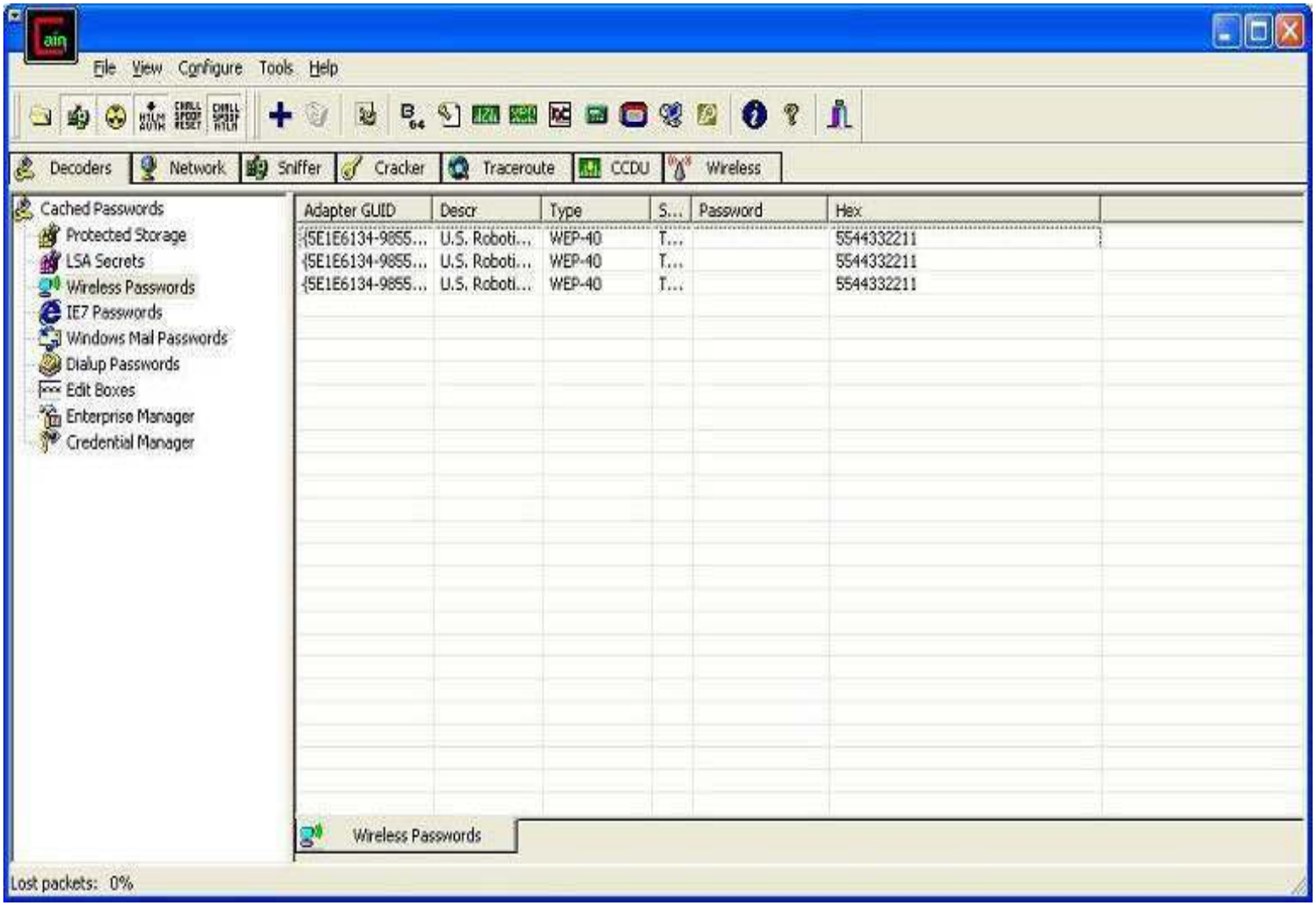


It contains a feature called APR (ARP Poison Routing), which enables sniffing on switched LANs by hijacking IP traffic of multiple hosts at the same time

EC-Council

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

# Cain & Abel: Screenshot




EC-Council

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

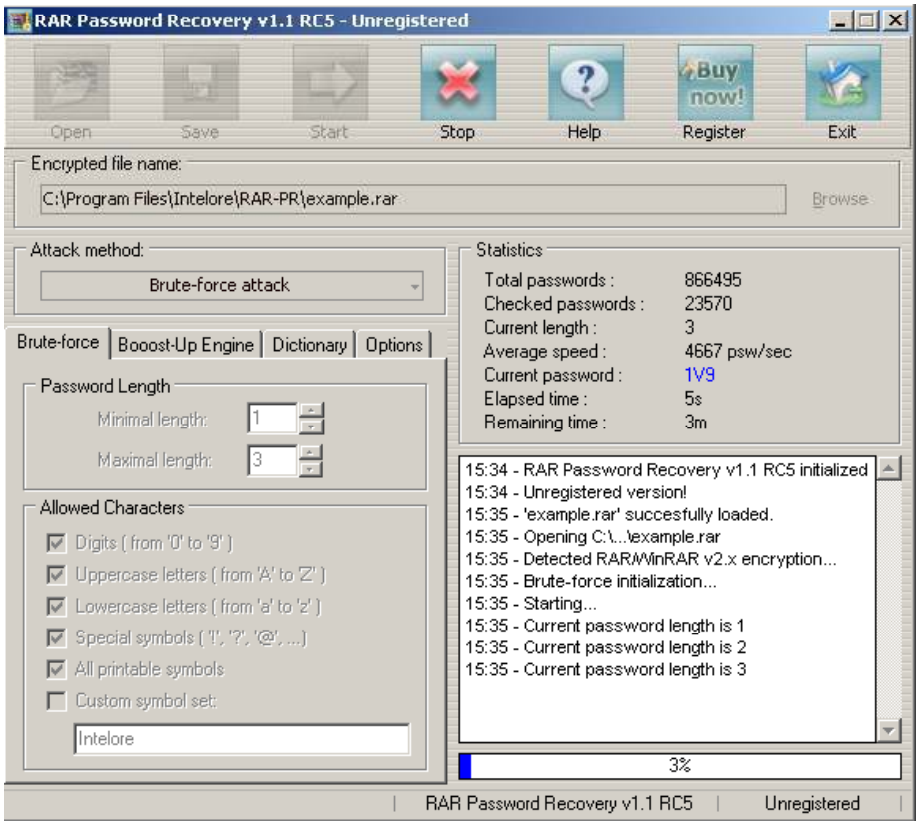
# Hacking Tool: RAR

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




EC-Council

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

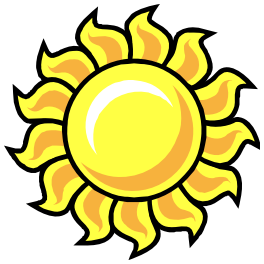
# Hacking Tool: Gammaprog

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



EC-Council

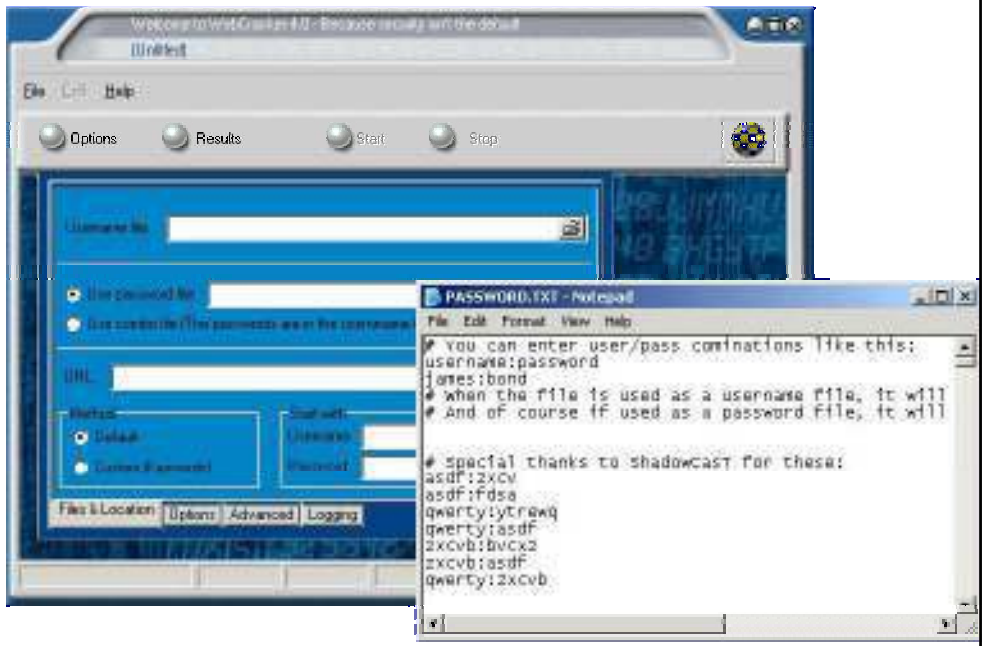
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# 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

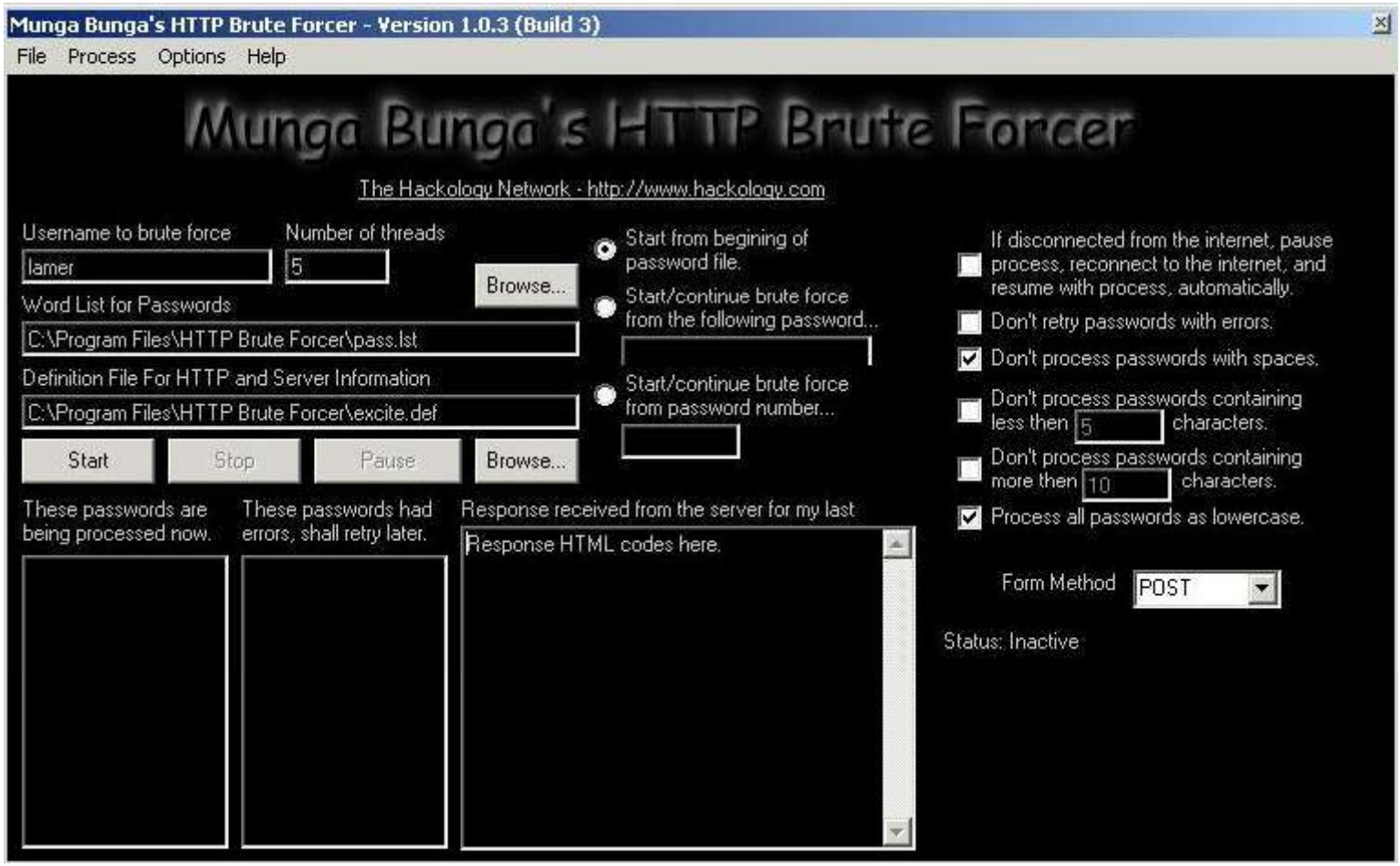
It will find all successful guesses given in a user name/password






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

# Hacking Tool: Munga Bunga



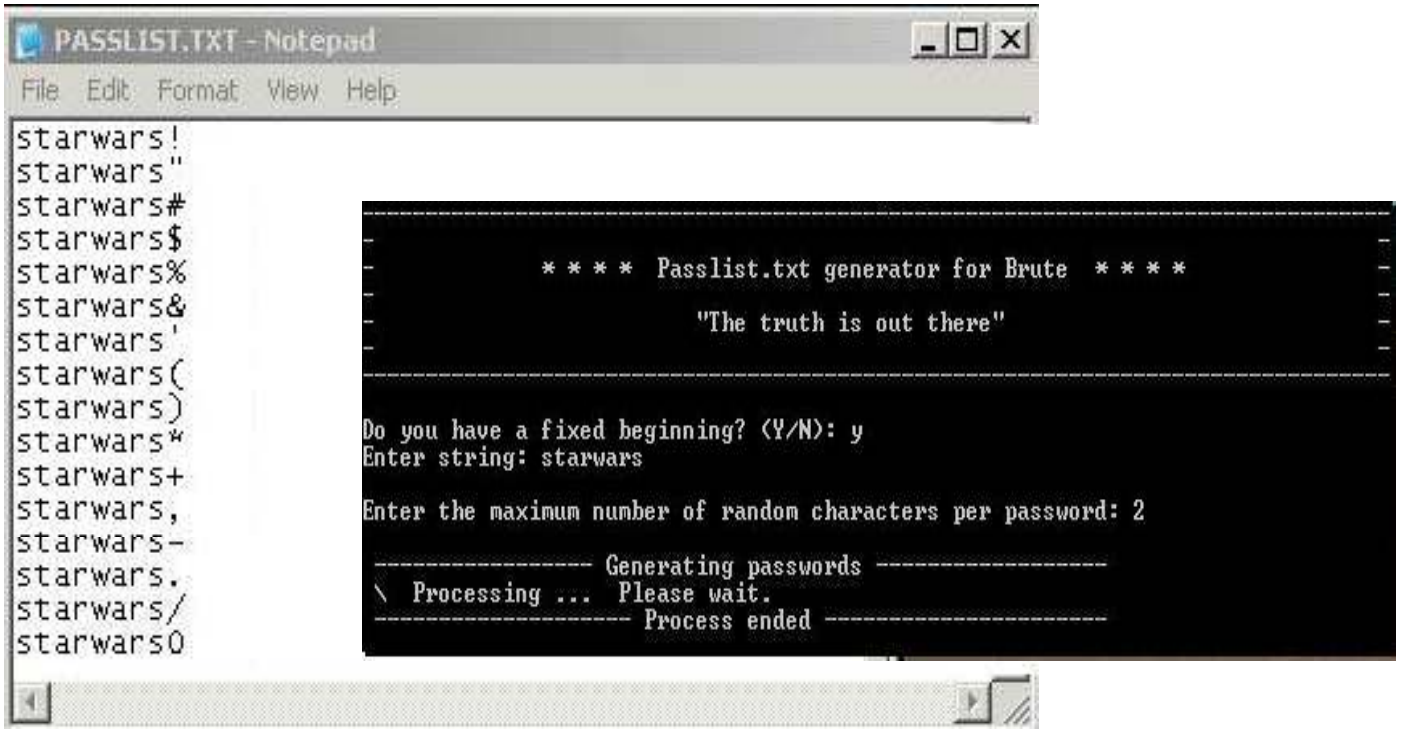

It's a brute forcer, which uses the HTTP protocol to establish its connections



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

# Hacking Tool: PassList

PassList is another character-based password generator



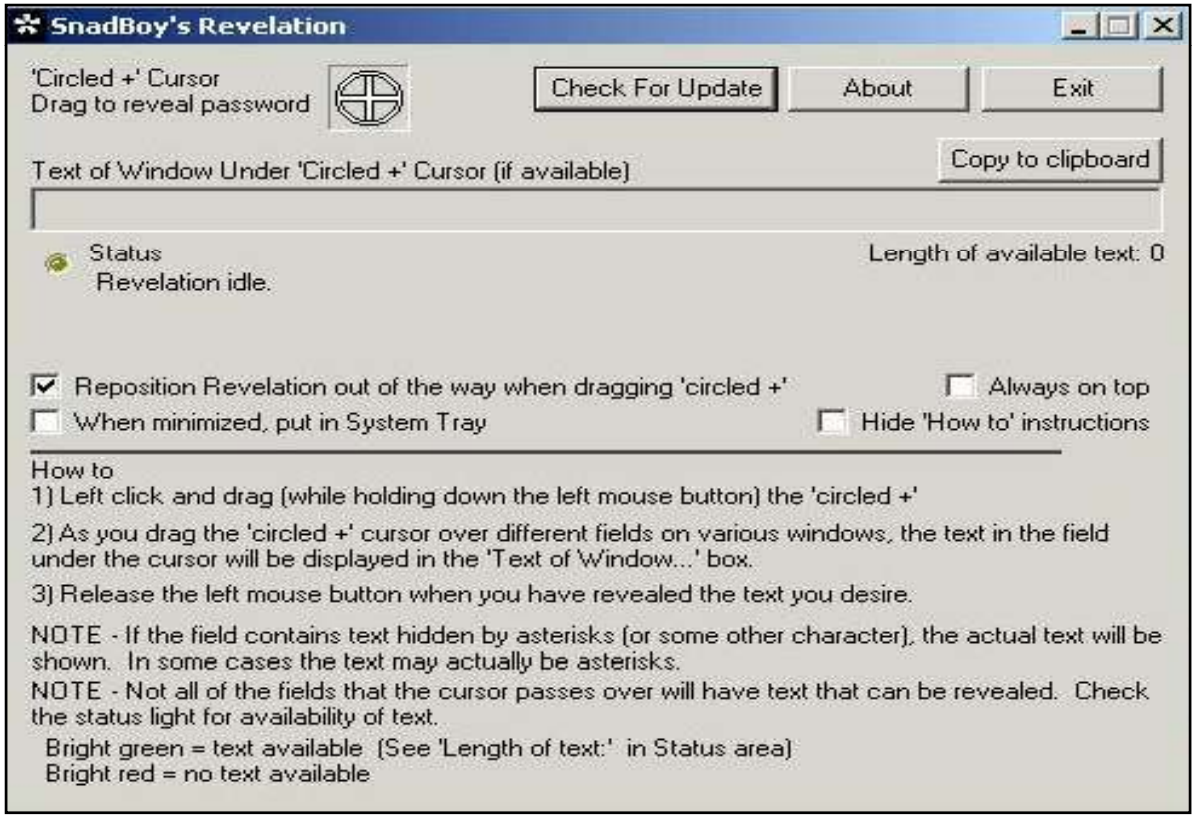



Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Hacking Tool: SnadBoy

http://www.snadboy.com

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



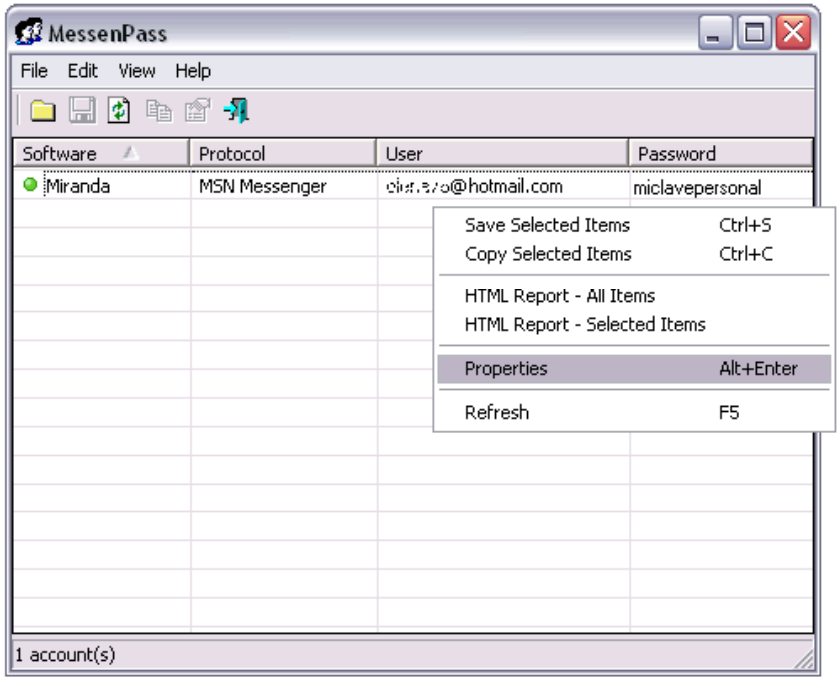


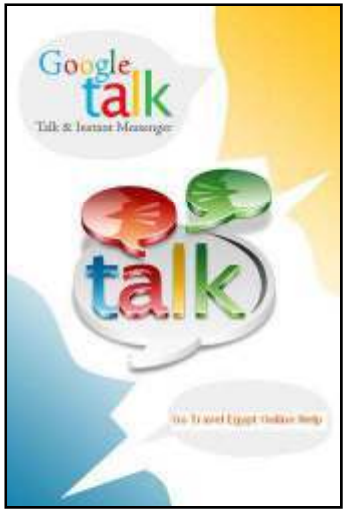

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Hacking Tool: MessenPass

MessenPass is a password recovery tool that reveals the passwords of instant messenger like:

- MSN Messenger
- Yahoo Messenger
- Google Talk

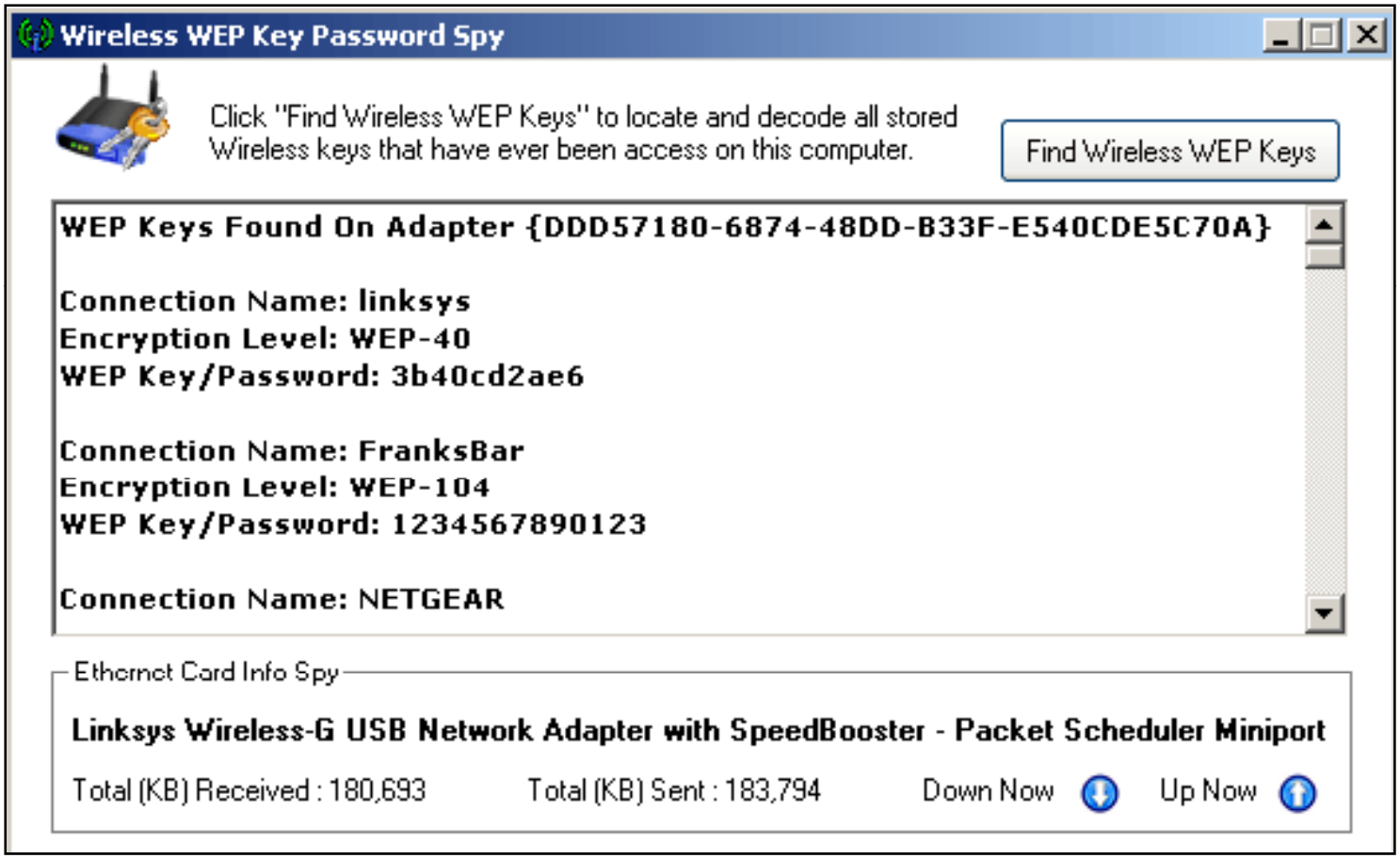





Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Hacking Tool: Wireless WEP Key Password Spy





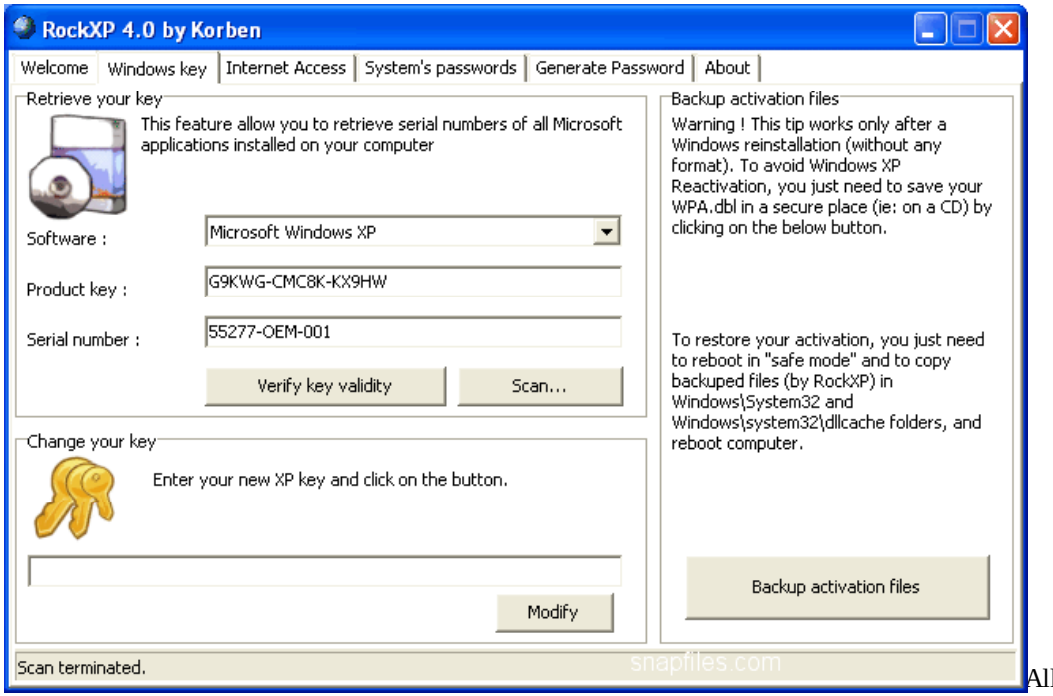

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Hacking Tool: RockXP

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

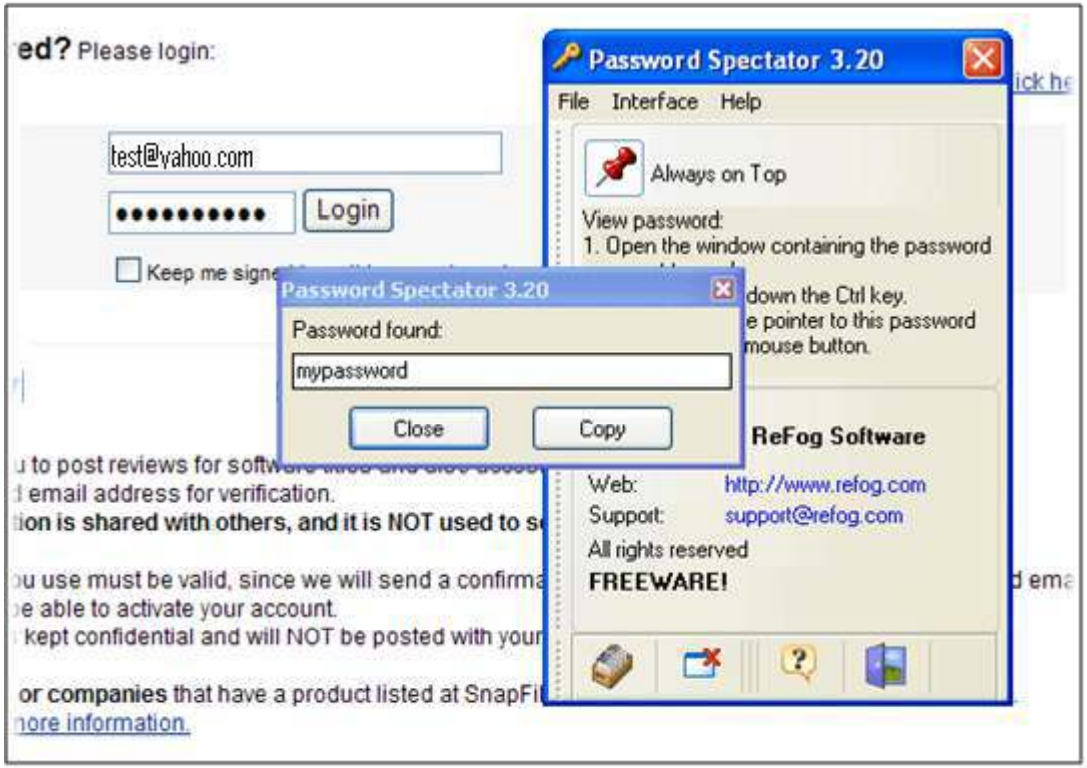
In addition, the program also lets you save the product activation to a file



Copyright © by EC-Council
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



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

# Tool: WWWhack

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

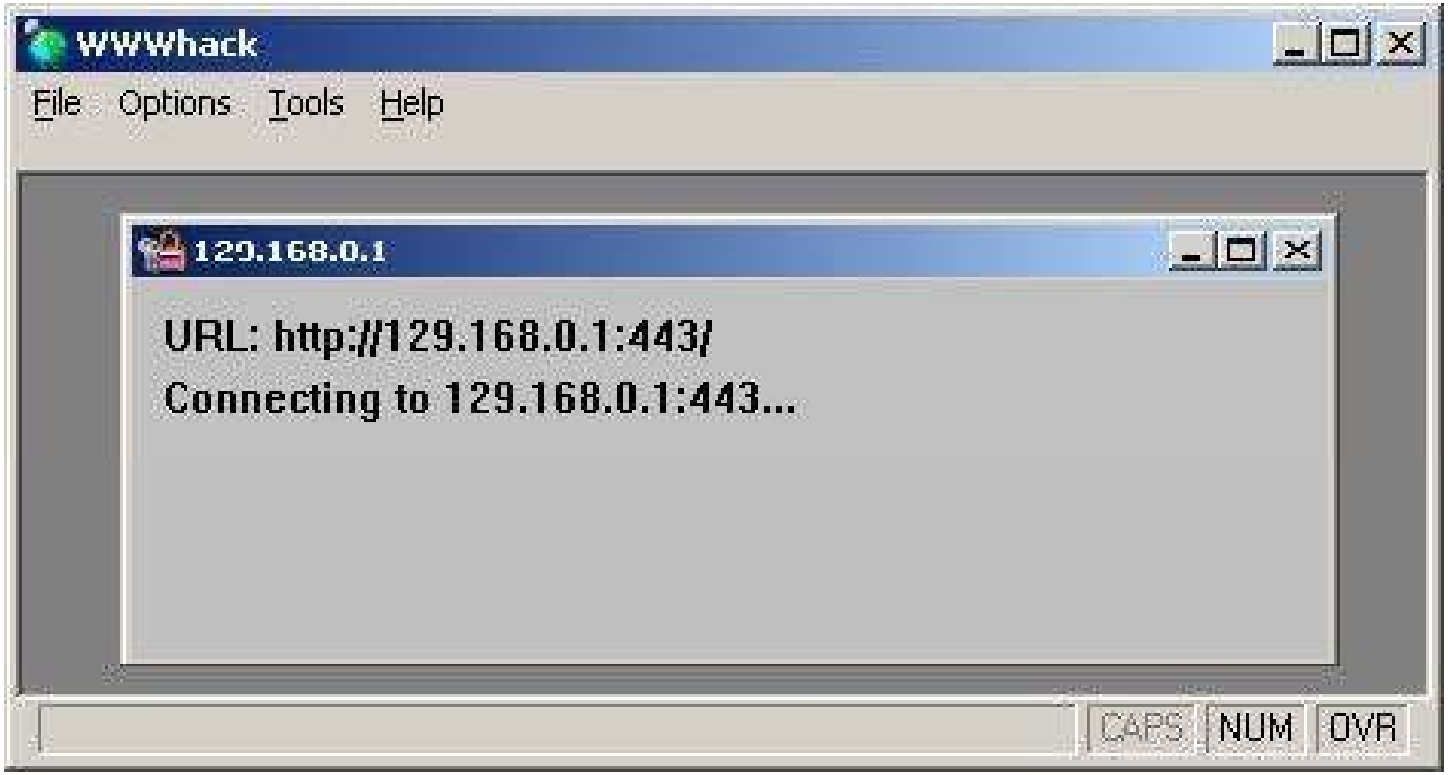
This utility can use a word file or try all possible combinations

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

EC-Council

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

# WWWhack: Screenshot






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

# Passwordstate

www.clickstudios.com.au

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

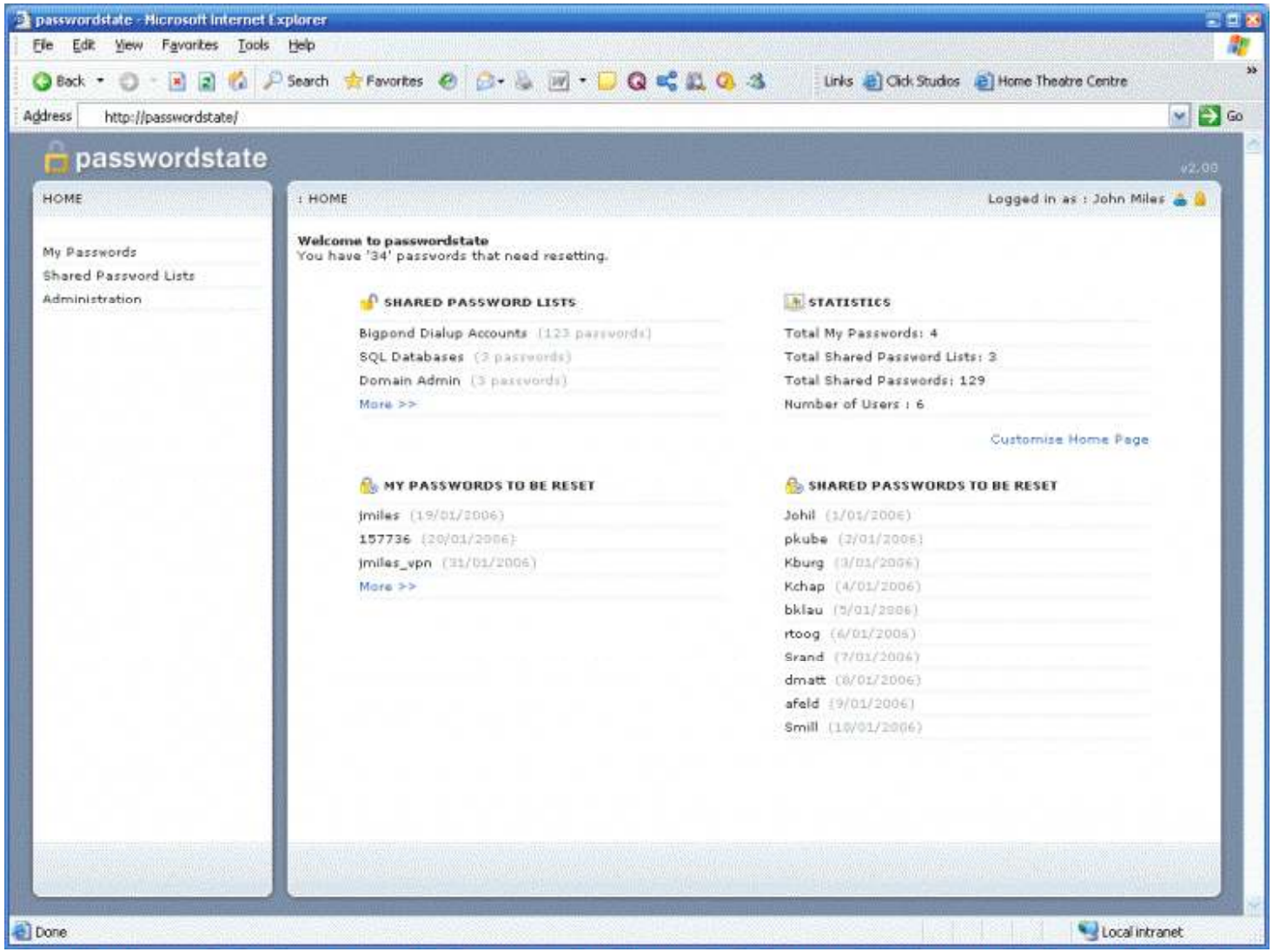
## Features:

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

EC-Council

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

# Passwordstate: Screenshot




EC-Council

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

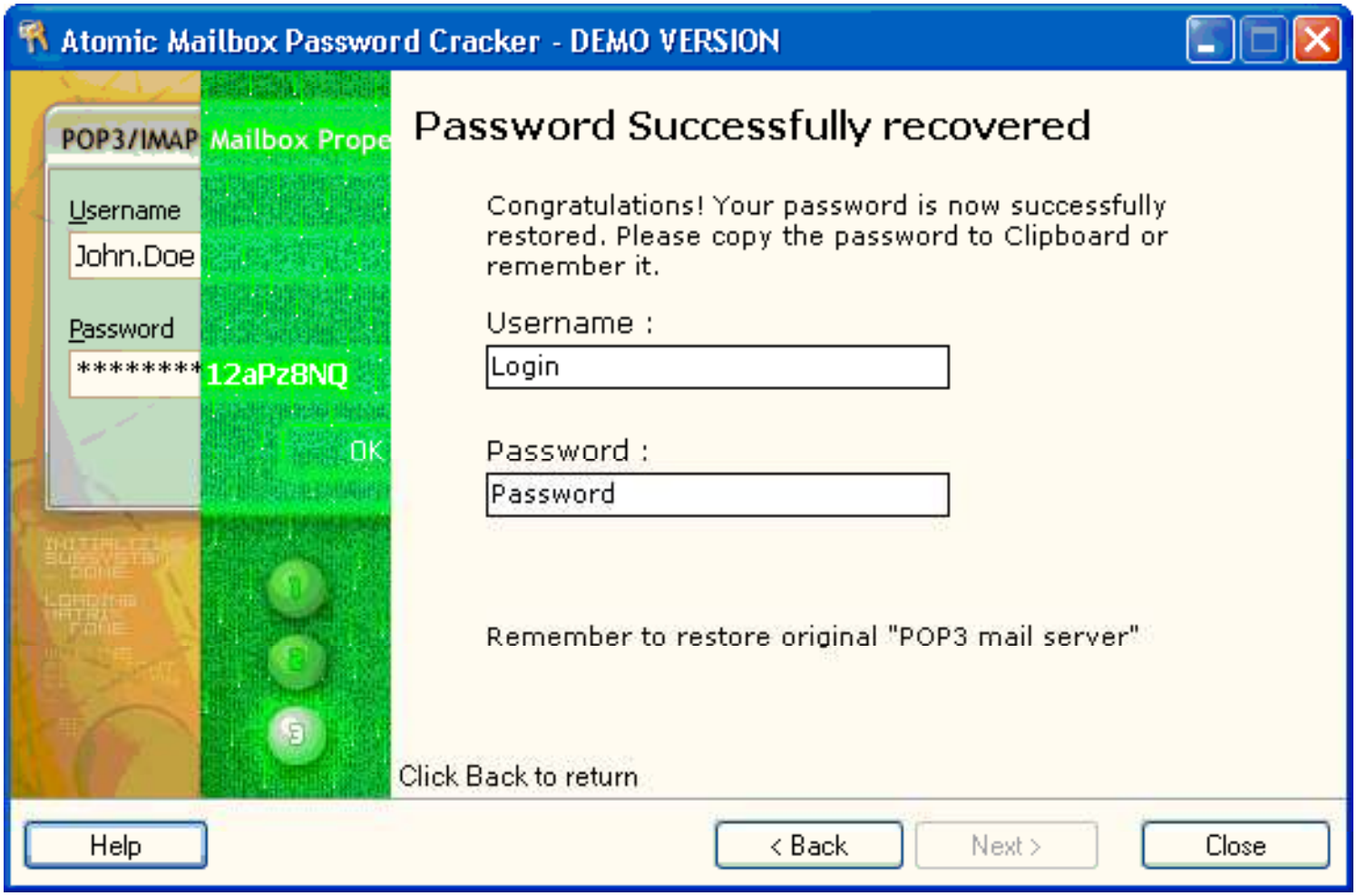
# Atomic Mailbox Password Cracker

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

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

# Atomic Mailbox Password Cracker: Screenshot






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

# Advanced Mailbox Password Recovery (AMBPR)

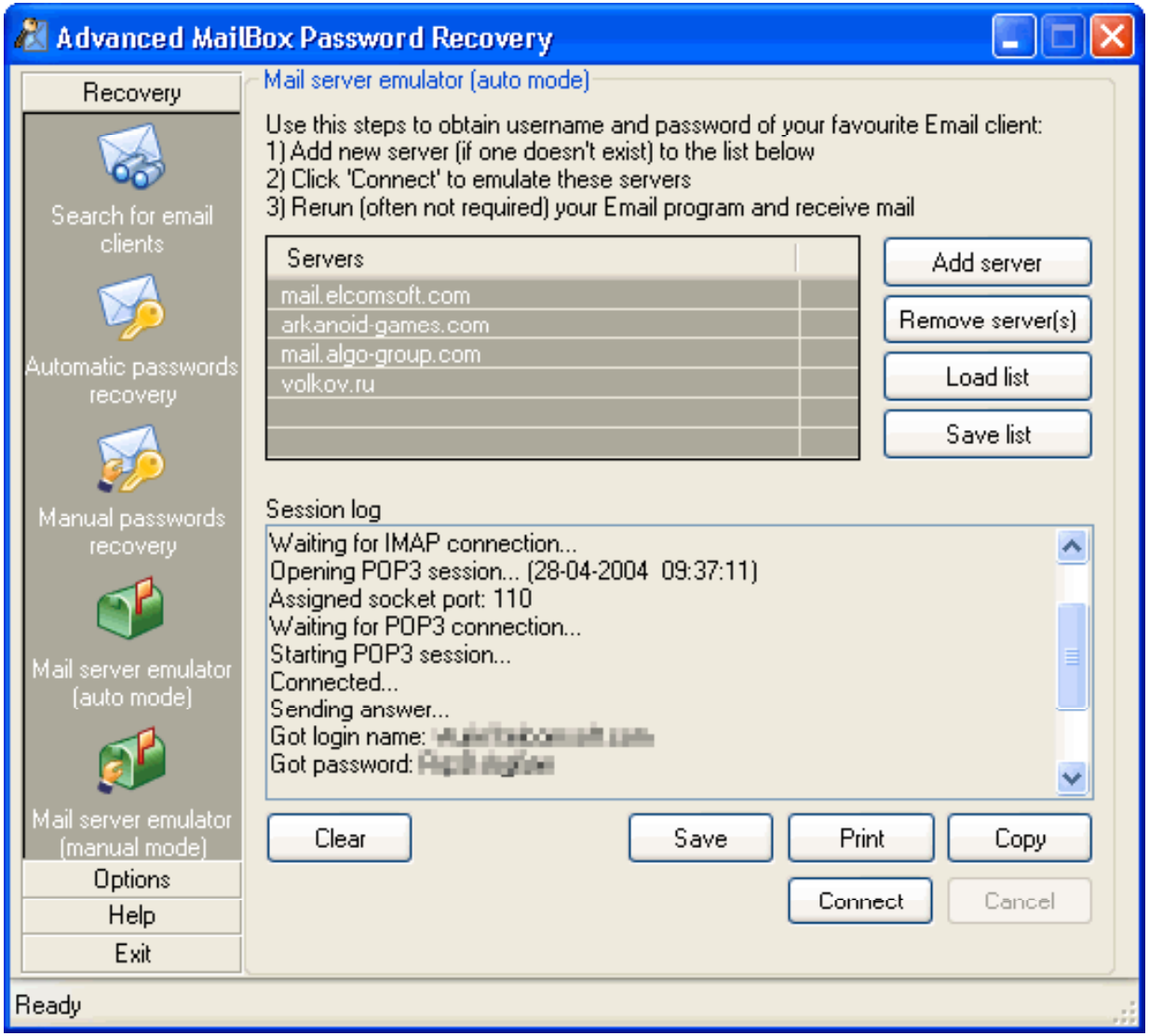
Advanced mailbox password recovery recovers login and password information for most popular email clients

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

EC-Council

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

# Advanced Mailbox Password Recovery (AMBPR): Screenshot




EC-Council

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

# Tool: Network Password Recovery

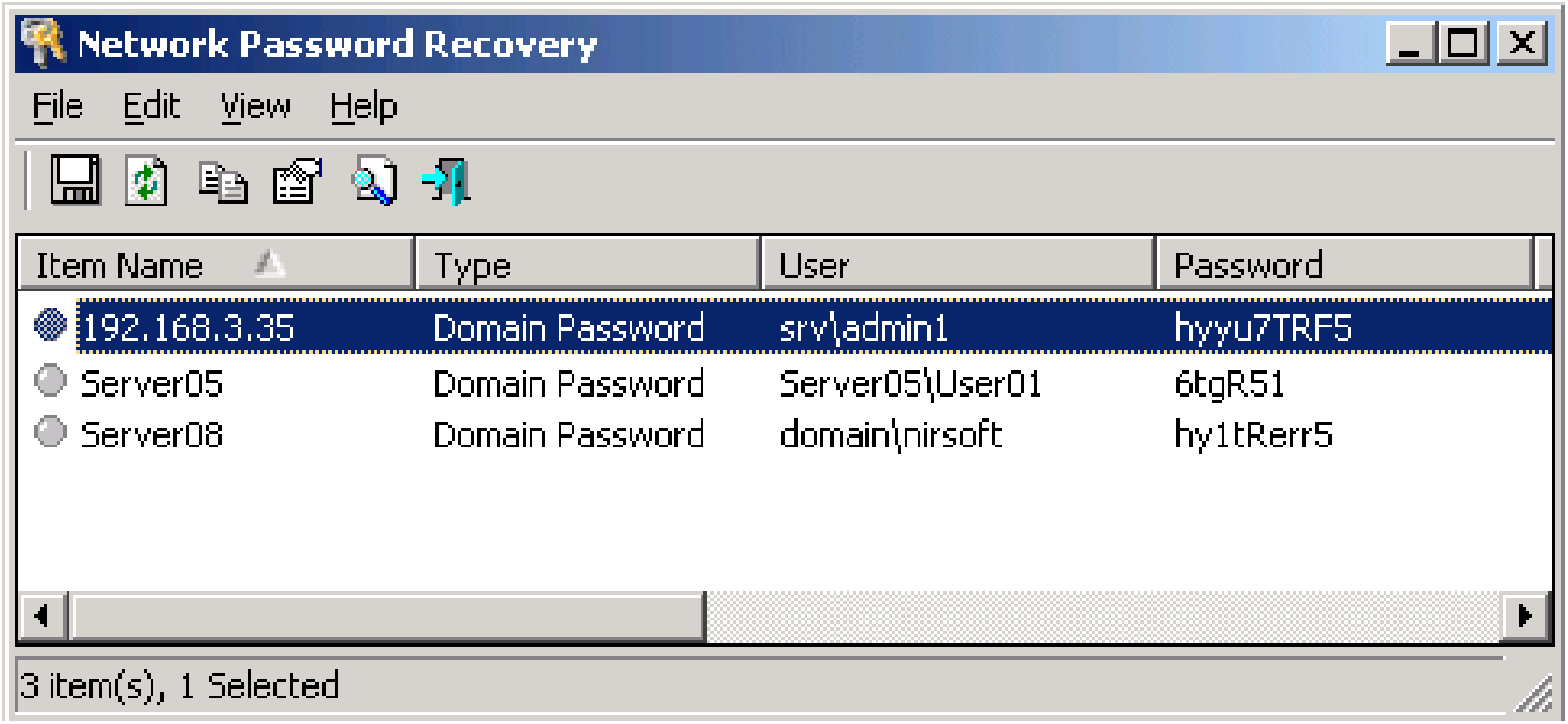
Network password recovery utility recovers all network passwords stored on the system for the current logged-on user

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
- Internet Explorer 7: Recovers passwords of password-protected Web sites

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

# Network Password Recovery: Screenshot






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

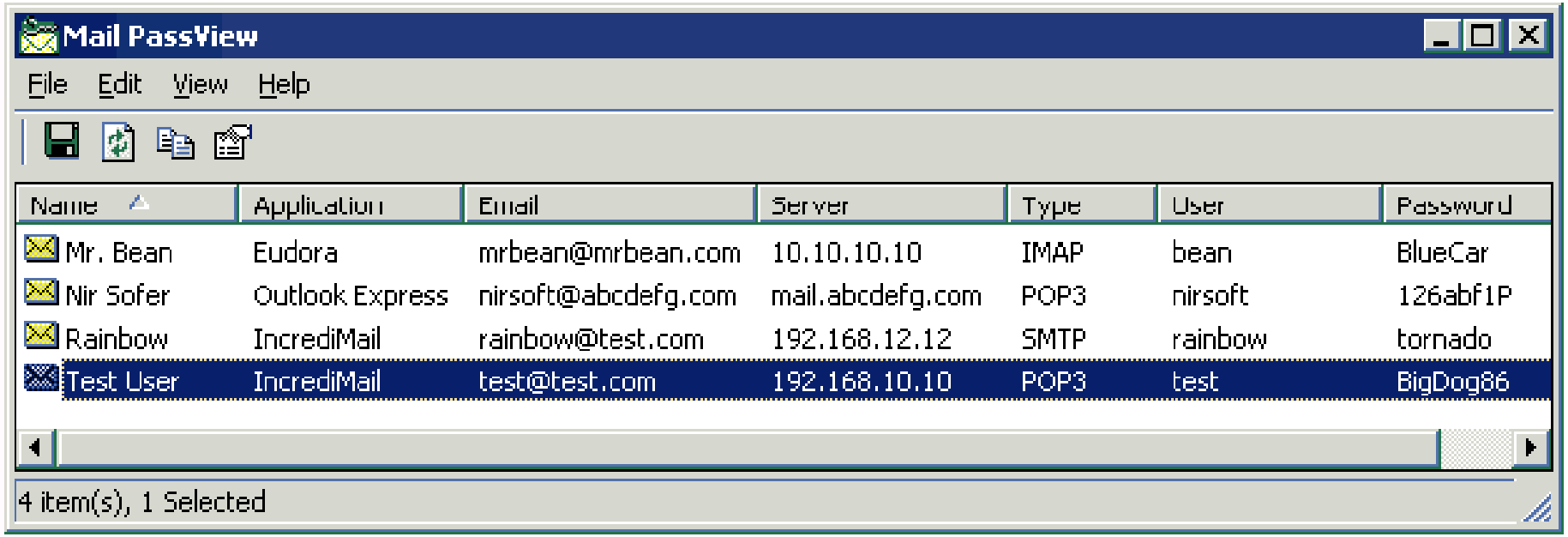
# Tool: Mail PassView

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 and SMTP 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 by Gmail Notifier application or by Google Talk

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

# Mail PassView: Screenshot

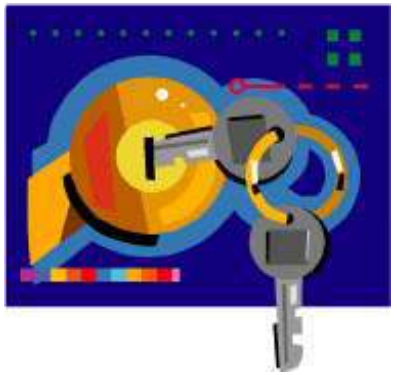





Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

# Tool: Messenger Key

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



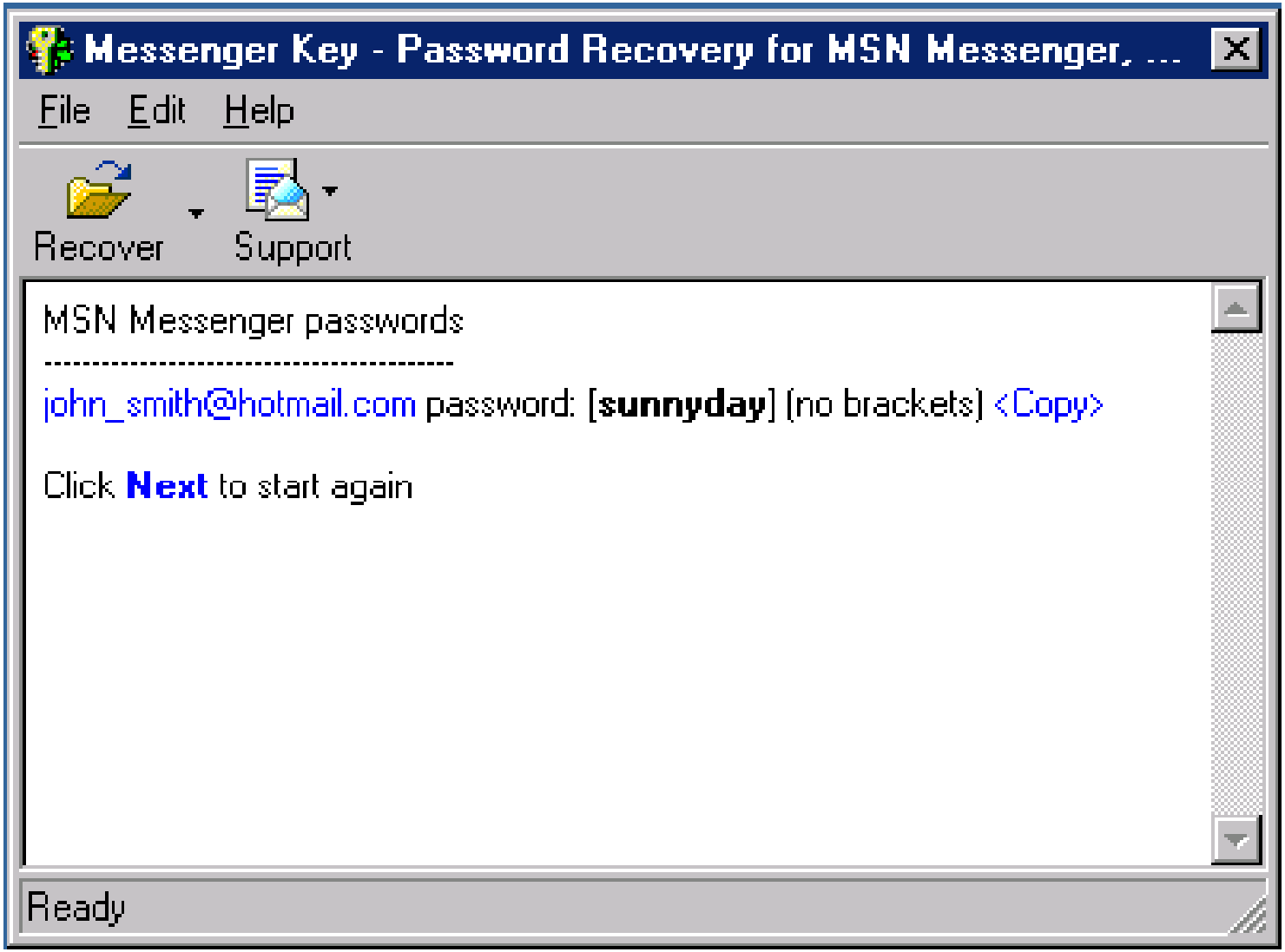
Features:

- 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 passwords are recovered instantly
- Supports multilingual passwords

EC-Council

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

# Messenger Key: Screenshot






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

# Tool: SniffPass

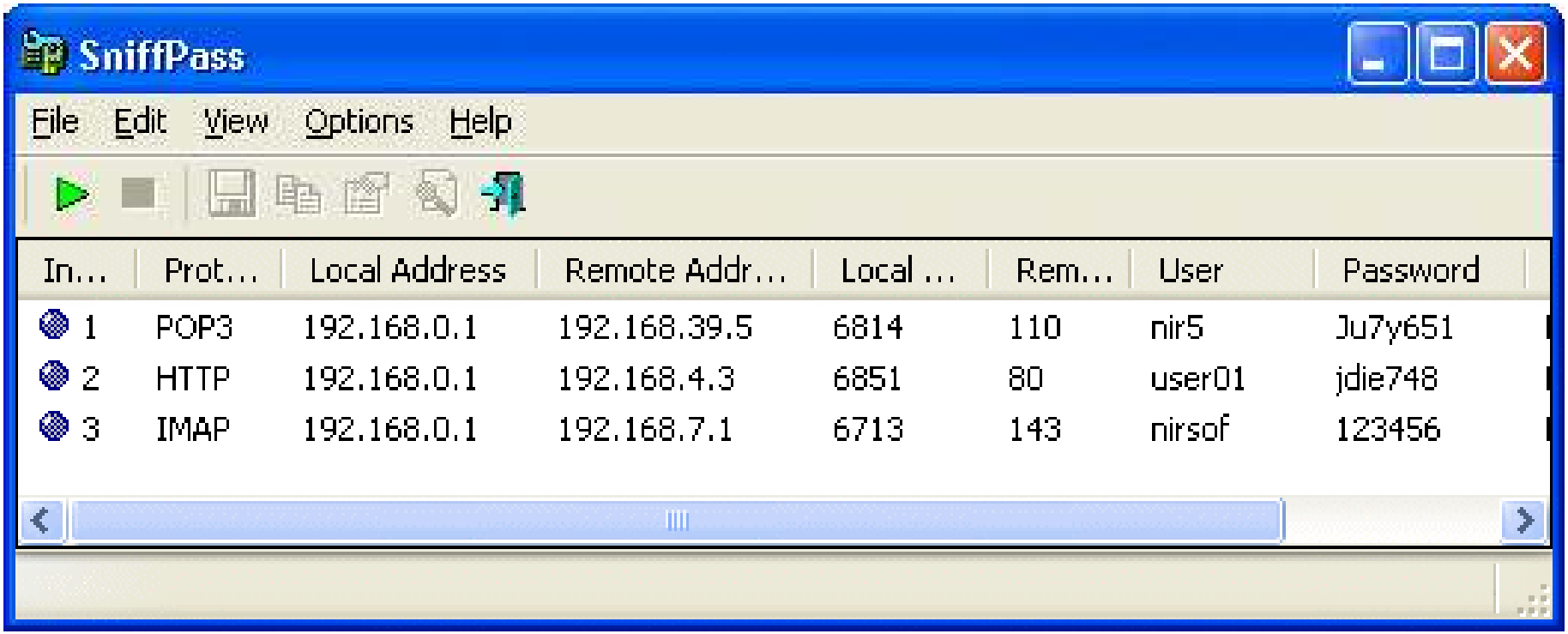
SniffPass is a tool that listens to your network, captures the passwords that pass through your network adapter, and displays them on the screen instantly

It captures the passwords of the following protocols:

- POP3
- IMAP4
- SMTP
- FTP
- HTTP

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

# SniffPass: Screenshot






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

# Security Tools



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

# WebPassword

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

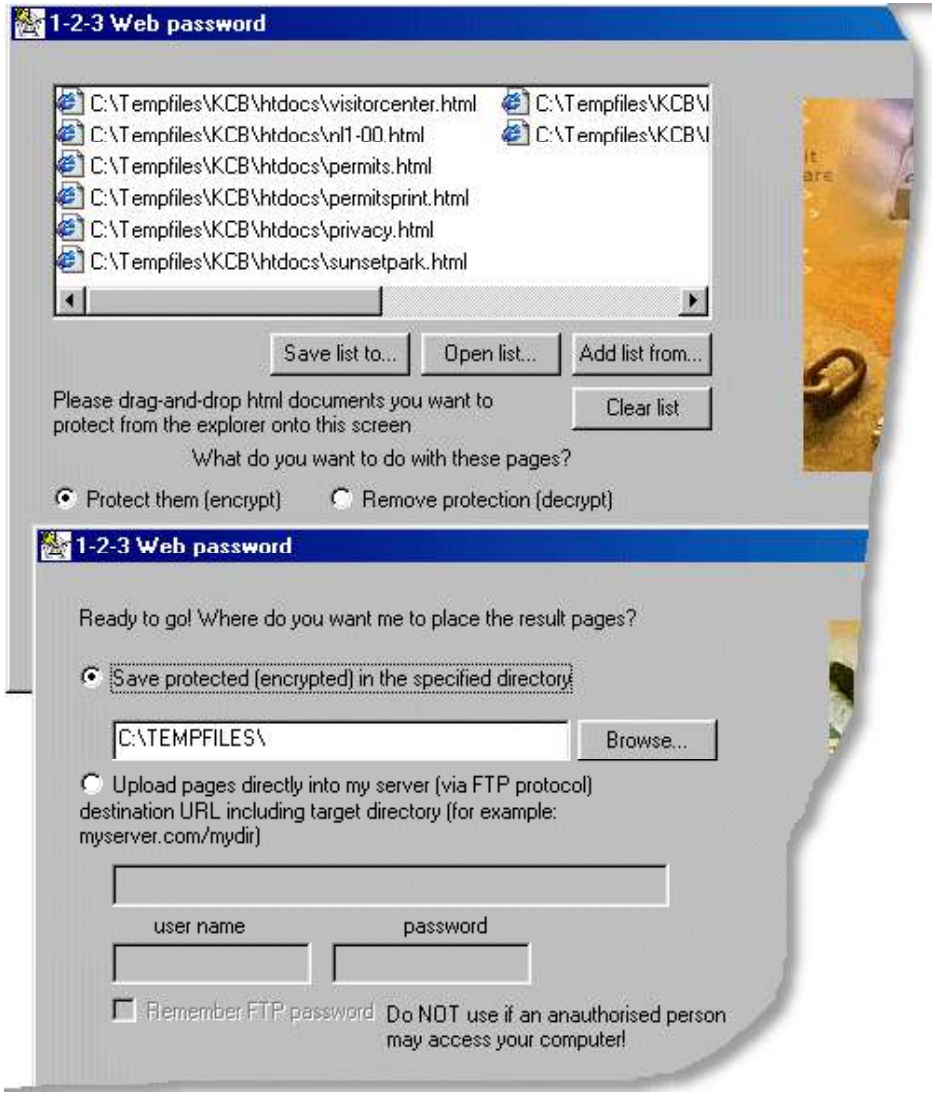
Unauthorized person will not be able to view its content without having a correct password, either in browser, or as an original HTML source

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


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

# WebPassword: Screenshot






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

# Password Administrator

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

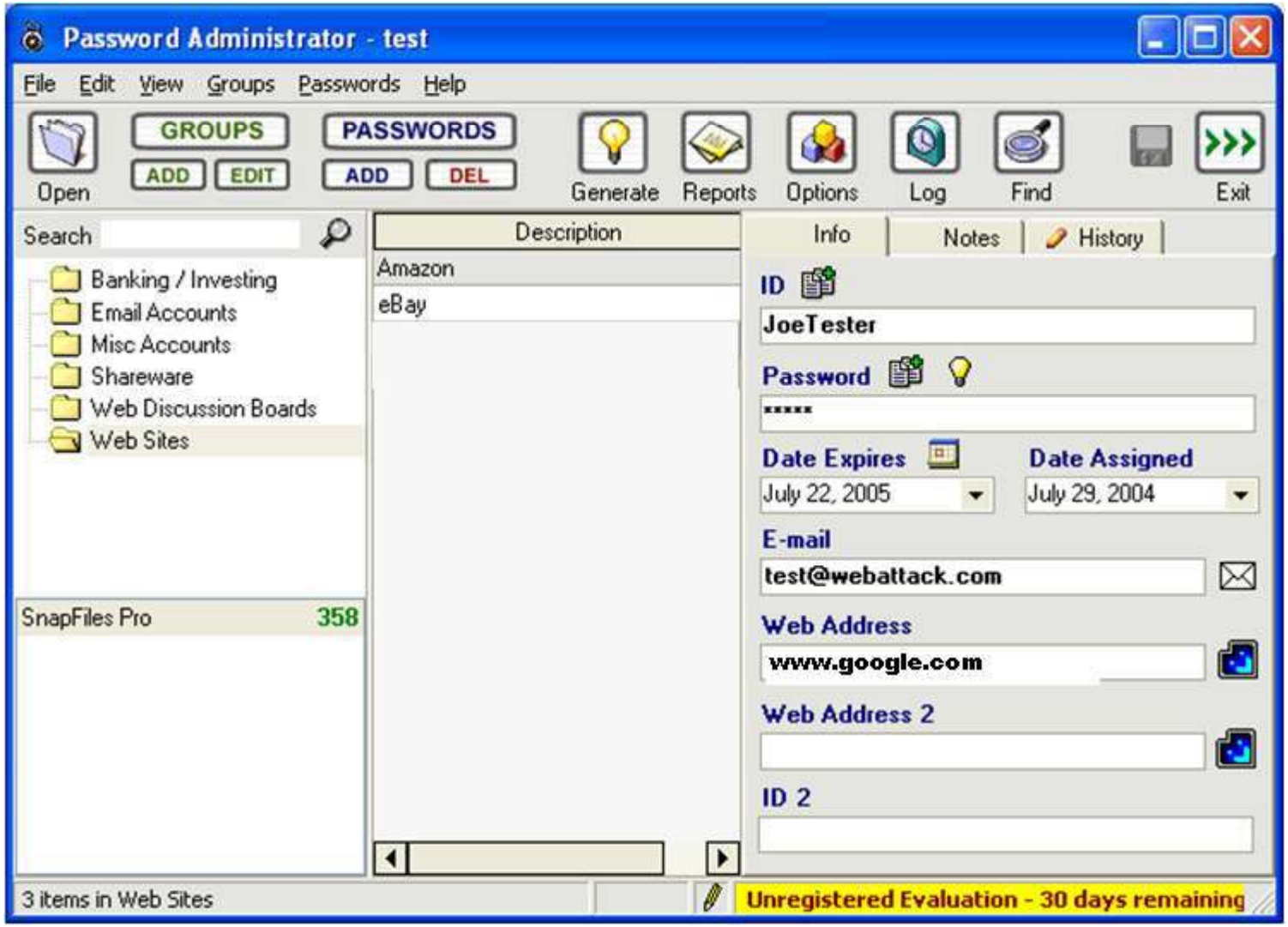
Features:

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

EC-Council

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

# Password Administrator: Screenshot




EC-Council

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

# Password Safe

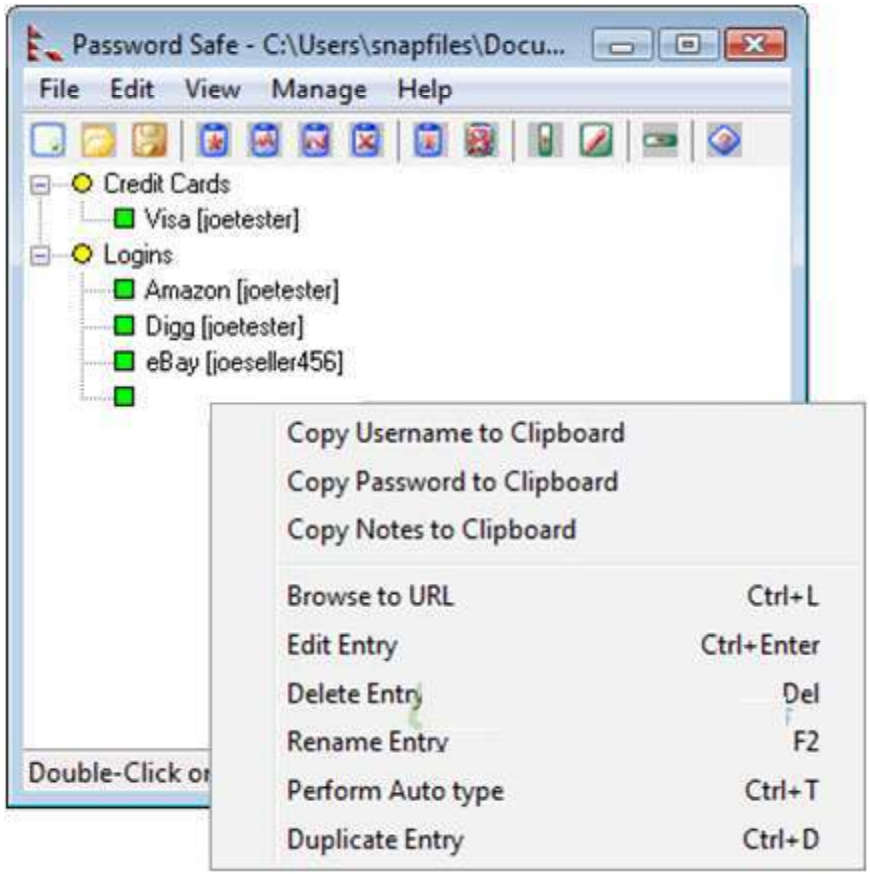
Password Safe is a password manager that protects your sensitive information with the TwoFish encryption algorithm

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

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

# Password Safe: Screenshot






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

# Easy Web Password

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

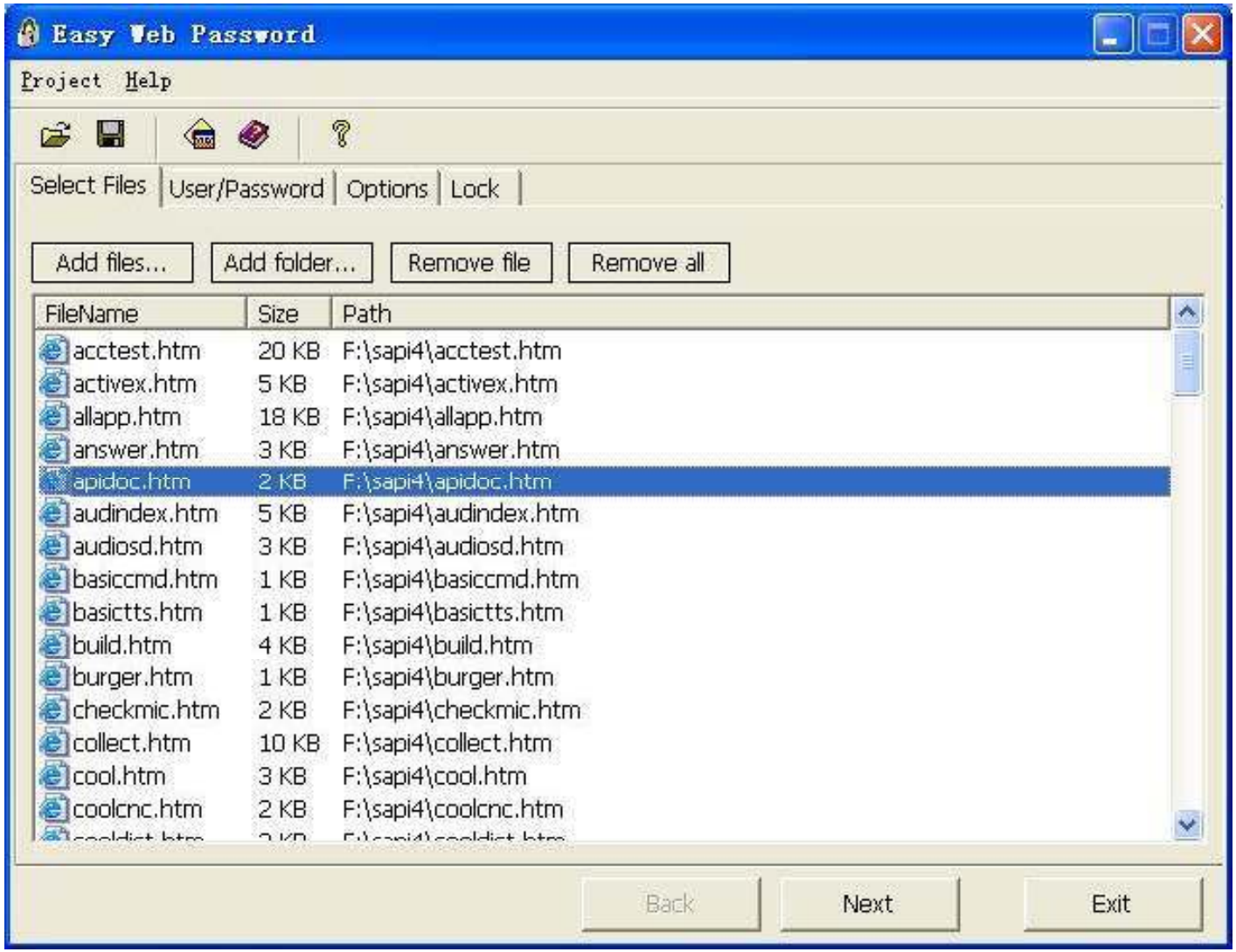
It can select the pages to the protected, set up user accounts and passwords, and generate password protected version of your HTML files

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



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

# Easy Web Password: Screenshot




EC-Council

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

# PassReminder

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

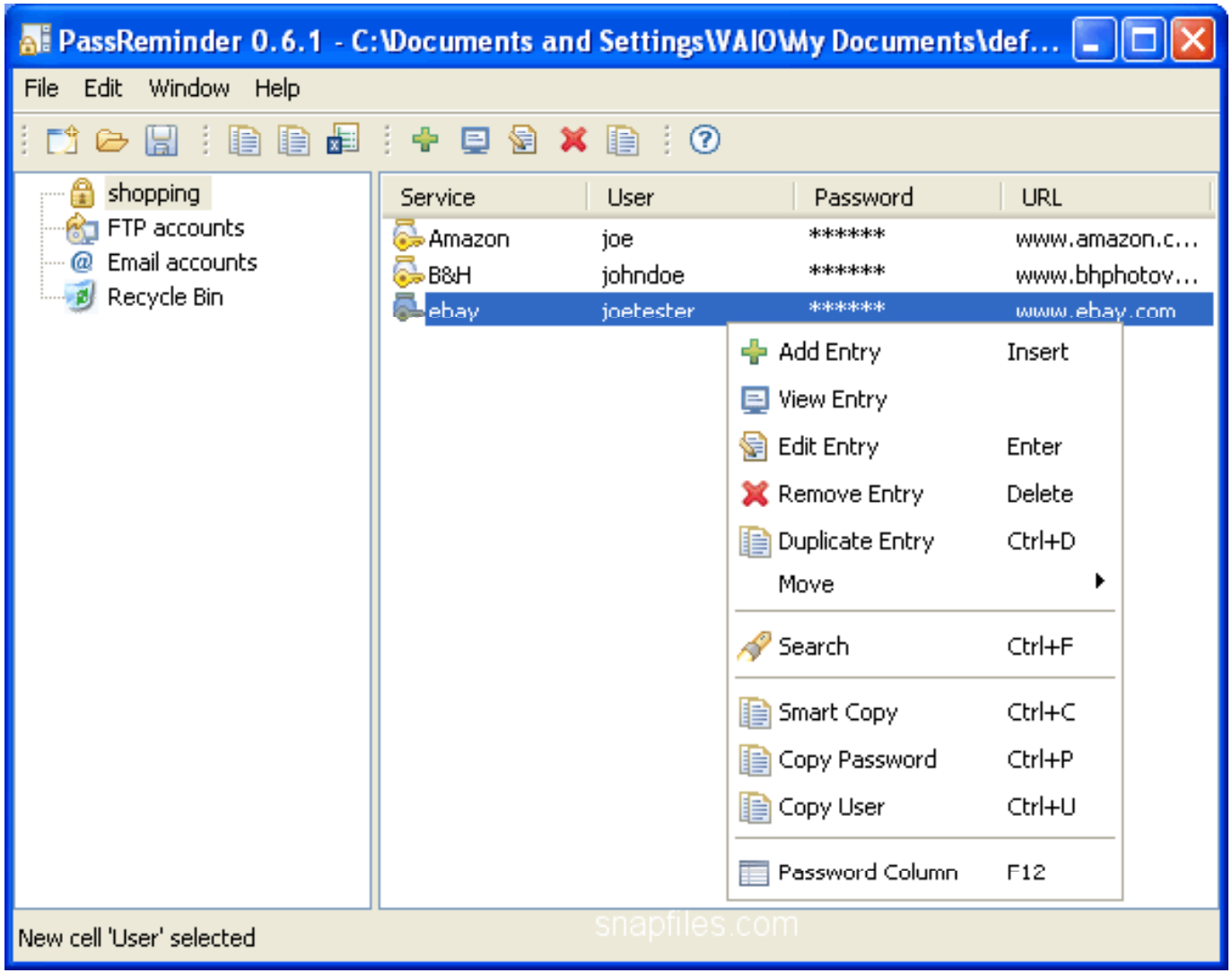
Features:

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



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

# PassReminder: Screenshot






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

# My Password Manager

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

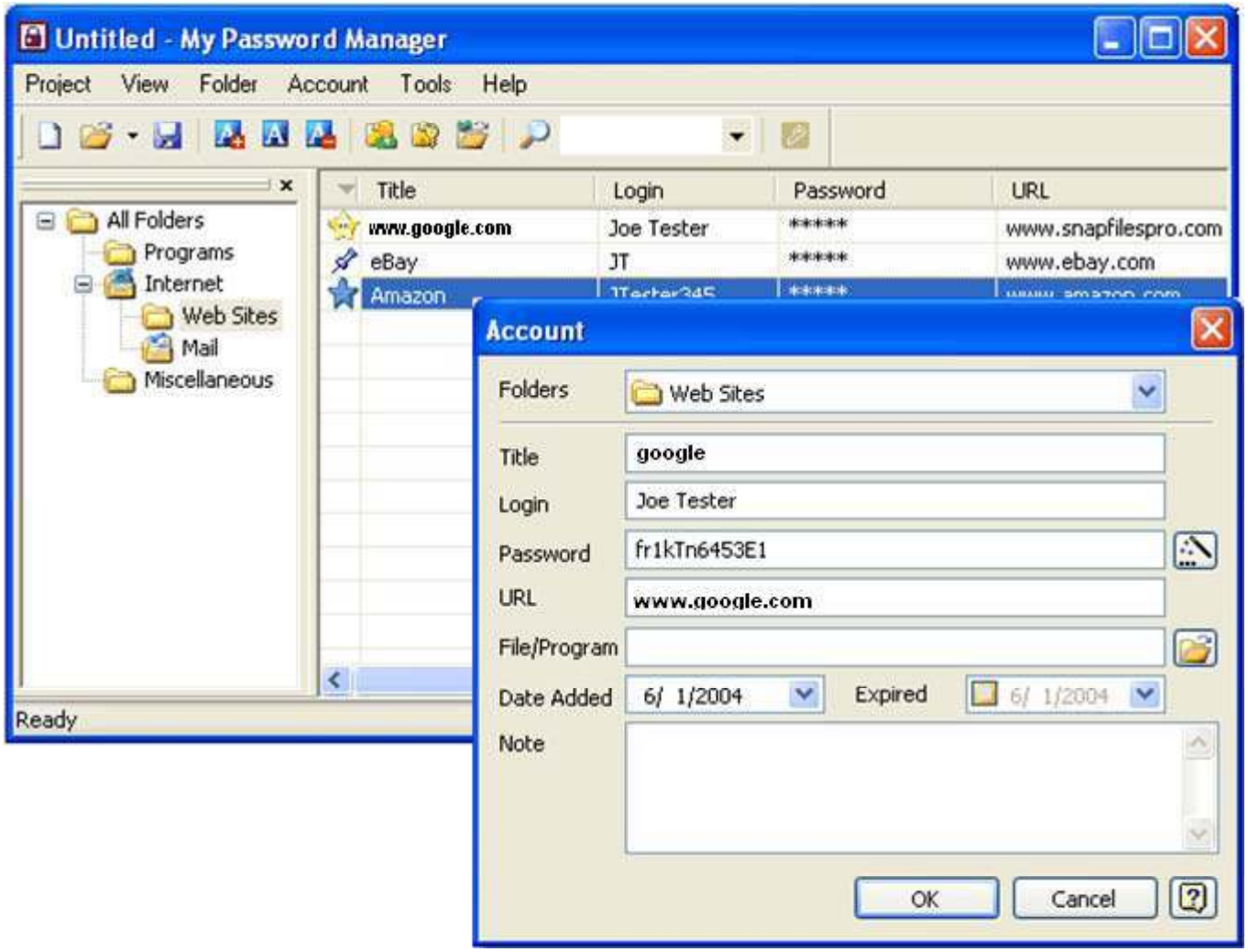
It supports custom categories, web links, and password expiration and has built-in password generator

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

EC-Council

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

# My Password Manager: Screenshot






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

# Countermeasures

- 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

# Countermeasures (cont'd)

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

EC-Council

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

# Countermeasures (cont'd)

The user can use the SRP protocol

- SRP is a secure password-based authentication andkey-exchange 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

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

# What Happened Next

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


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

# Summary

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

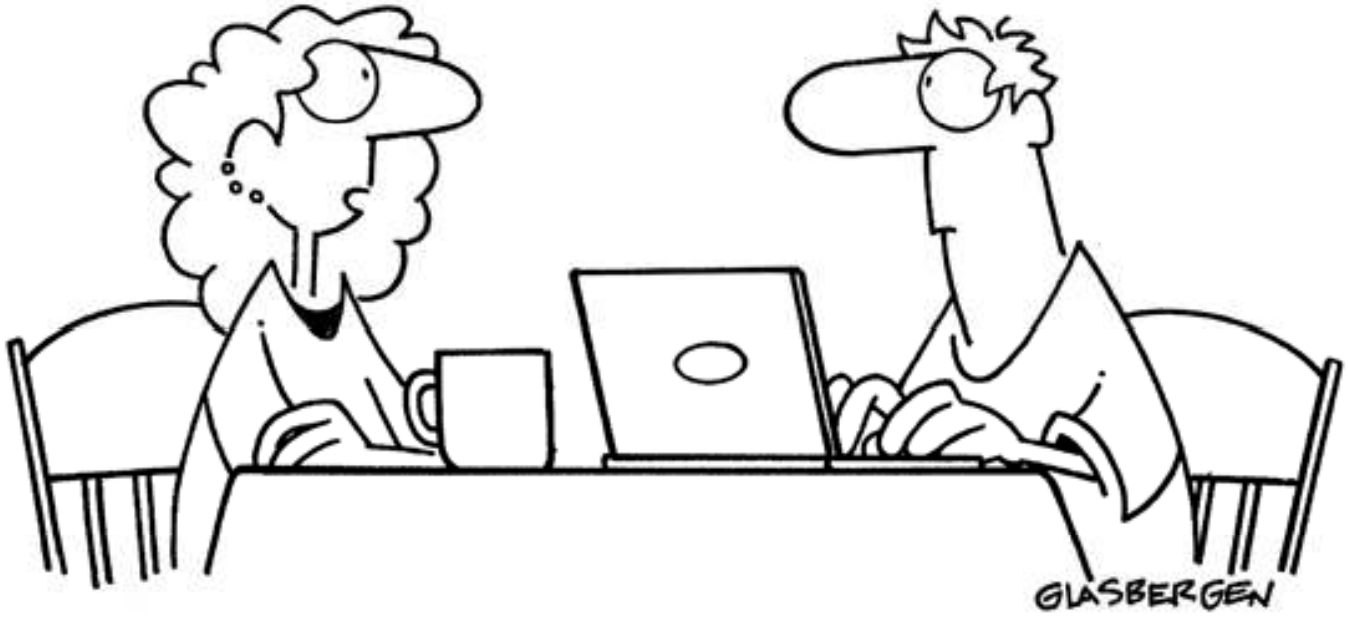
Password crackers use two primary methods to identify correct passwords: brute force and dictionary searches

LOphtcrack, John the Ripper, Brutus, Obiwan, etc. are some of the popular password-cracking 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'."**



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

**"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."



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