Password Cracking Penetration Testing

Module 17

Designed by Security Auditors. Presented by Professionals.

ECSA™

EC-Council Certified Security Analyst

Module Objectives

- Importance of Passwords
- Common Password Vulnerabilities
- Types of Password Attacks
- How Are Passwords Stored in Windows?
- How Are Passwords Stored in Linux?
- Steps for Password Cracking Penetration Testing

- Perform Non-Electronic Attacks
- Perform Brute Force and Dictionary Attacks
- Perform Man-in-the-Middle Attack to Collect Passwords
- Perform Hash Injection Attack
- Password Cracking Using Distributed Network Attack

Password - Terminology

Secret Characters

A password is a secret series of characters that **enables** a **user to access** a file, computer, or a program

A Unique String

It contains a unique string of characters used to **restrict access** to computers and sensitive files

Passwords may contain:

- Only letters **POTHMYDE**
- Only numbers **23698217**
- Only special characters **&*#@!(%)**
- Letters and numbers **meet123**
- Only letters and special characters **bob@&ba**
- Only special characters and numbers **123@$45**
- Letters, special characters, and numbers **ap1@52**

Importance of Passwords

1. Passwords protect a computer's resources and files from unauthorized access by malicious users (attackers)

2. Companies protect their resources by using combinations of user IDs and passwords

3. Attackers can brute force or guess the passwords of the web applications

4. Some system software products use weak or no encryption to store and/or transmit their user IDs and passwords from the client to the server

5. One of the leading causes of network compromises is the use of guessable or decipherable passwords

Password Types

Cleartext Passwords

- A cleartext password is sent over the wire (and wirelessly) or stored on some media as it is typed, without any alteration

Obfuscated Passwords

- Passwords stored or communicated after a transformation
- The transformation is reversible: after applying an algorithm the password becomes unreadable, and after applying the reverse algorithm it returns cleartext. This process is called obfuscation

Hashed Passwords

- Hashed passwords seem similar to obfuscated passwords, but the latter are reversible
- Passwords are transformed using a non-reversible (hashing) algorithm for hashed passwords

Common Password Vulnerabilities

Password Vulnerabilities

Organizational Password Vulnerabilities

- **Weak passwords**
  - **Guessable**, e.g., pet names, car number, family member's name, etc.
  - Composed of **common vocabulary** words
- **Improper handling of strong passwords**
  - Involves the need for the user to **write down** the password in an insecure location

Technical Password Vulnerabilities

- Weak password **encryption** schemes
- **Security software** which stores passwords in memory
- End-user applications that show **passwords on the screen** while typing

Password Cracking Techniques

Dictionary Attacks

A dictionary file is loaded into the cracking application that runs against user accounts. These attacks **compare a set of words** against a password database

Brute Forcing Attacks

The program tries every **combination of characters** until the password is broken

Hybrid Attack

It works like a dictionary attack, but **adds some numbers and symbols** to the words from the dictionary and tries to crack the password

Syllable Attack

It is the combination of the **brute force** attack and the **dictionary** attack

Rule-based Attack

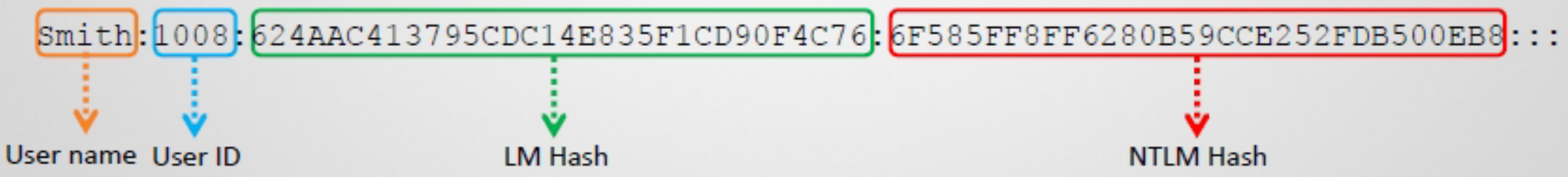
This attack is used when the attacker gets some **information** about the password

Types of Password Attacks

How Are Passwords Stored in Windows?

- Windows stores user passwords in the **Security Accounts Manager** database (SAM), or in the **Active Directory** database in domains
- Passwords are never stored in clear text; **passwords are hashed** and the results are stored in the SAM
- **NTLM** and **LM** authentication protocols are used to **securely store a user's password** in the SAM database using different hashing methods
- Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM
- The SAM file is located at `c:\windows\system32\config\SAM`

Password hash using LM/NTLM



Note: LM hash has been disabled in Windows Vista and Windows 7; LM will be blank in those systems

LM Authentication

LM hash or **LAN Manager** hash is one of the formats that Microsoft LAN Manager and Microsoft Windows use to **store user passwords** that are less than 15 characters long

When this password is **encrypted with the LM algorithm**, all the letters are converted to uppercase: 123456QWERTY

LM Hash

Before encrypting this password, the **14-character string is split in half**: 123456Q and WERTY_; each string is individually encrypted and the results concatenated:

```
123456Q = 6BF11E04AFAB197F
WERTY_  = F1E9FFDCC75575B15
```

The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15

The password is **padded with null** (blank) **characters** to make it 14 characters in length: 123456QWERTY_

Note: LM hash has been disabled in Windows Vista and Windows 7

LM Authentication (Cont'd)

1

2

3

4

The **first 8 bytes** are derived **from** the **first 7 characters** of the password and the **second 8** bytes are derived **from** characters **8 through 14** of the password

If the password is **less than 7 characters**, the second half will always be 0xAAD3B435B51404EE

Suppose, for this example, the user's password has an **LM hash** of **0xC23413A8A1E7665f AAD3B435B51404EE**

L0phtCrack 6 cracks the password as "**WELCOME**"

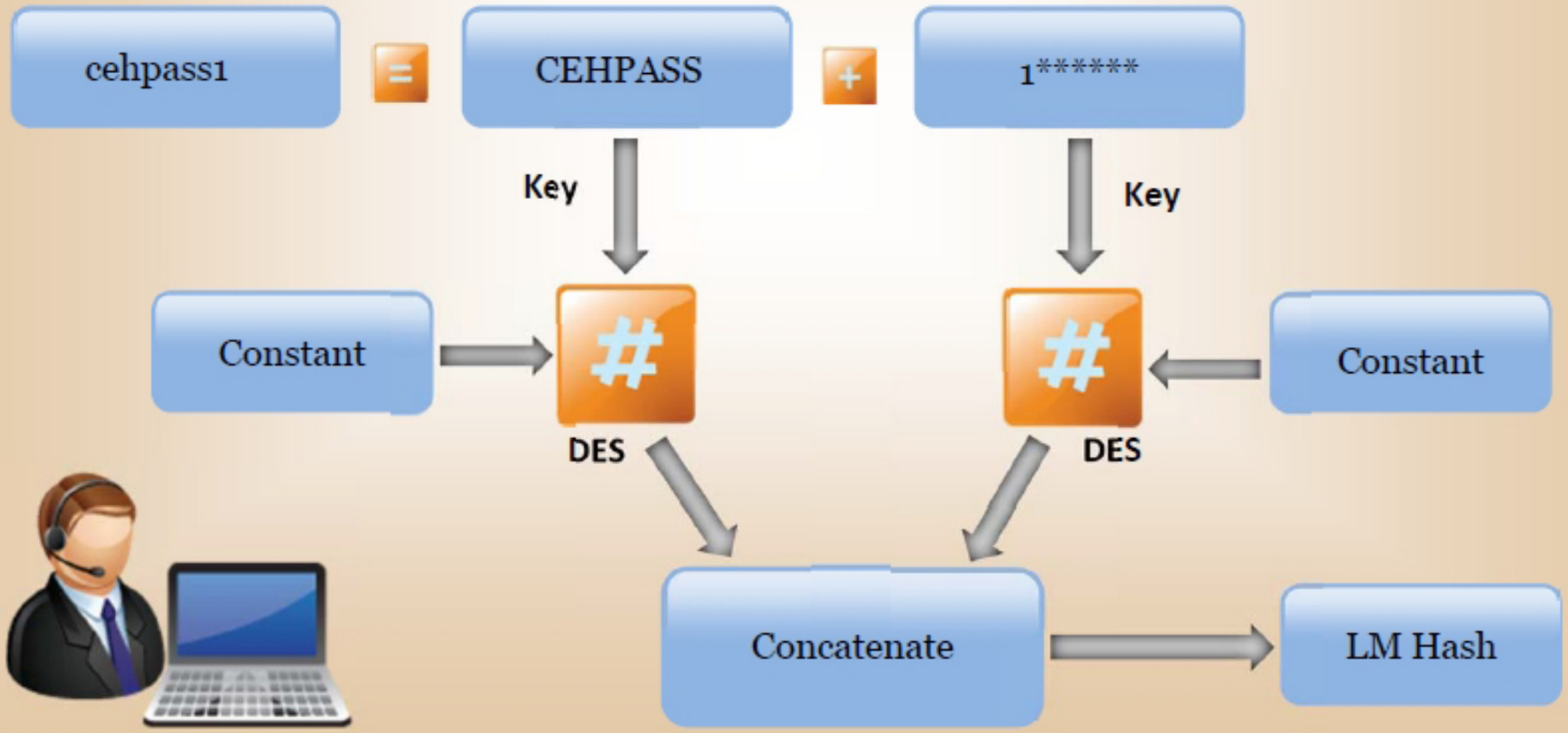
Note: **NTLMv2** is a challenge/response authentication protocol, that offers improved security over the obsolete LM protocol

LM Authentication (Cont'd)

Padded with NULL to 14 characters

Converted to the uppercase

Separated into two 7-character strings



NTLM Authentication

Client Computer

User types **password** into logon window

1 Martin
****

Hash Algorithm

Windows runs password through **hash algorithm**

2 `Martin:1008:624AAC413795CDC14 E835F1CD90F4C76:6F585FF8FF628 0B59CCE252FDB500EB8:::`

3 Computer sends logon request to DC

4 DC sends logon challenge

5 `Aa r8 ppq kgj89 pqr`

Computer sends response to challenge

Windows Domain Controller

Domain controller has a **stored copy** of the user's **hashed password**

`Martin:1008:624AAC413795CDC14 E835F1CD90F4C76:6F585FF8FF628 0B59CCE252FDB500EB8:::`

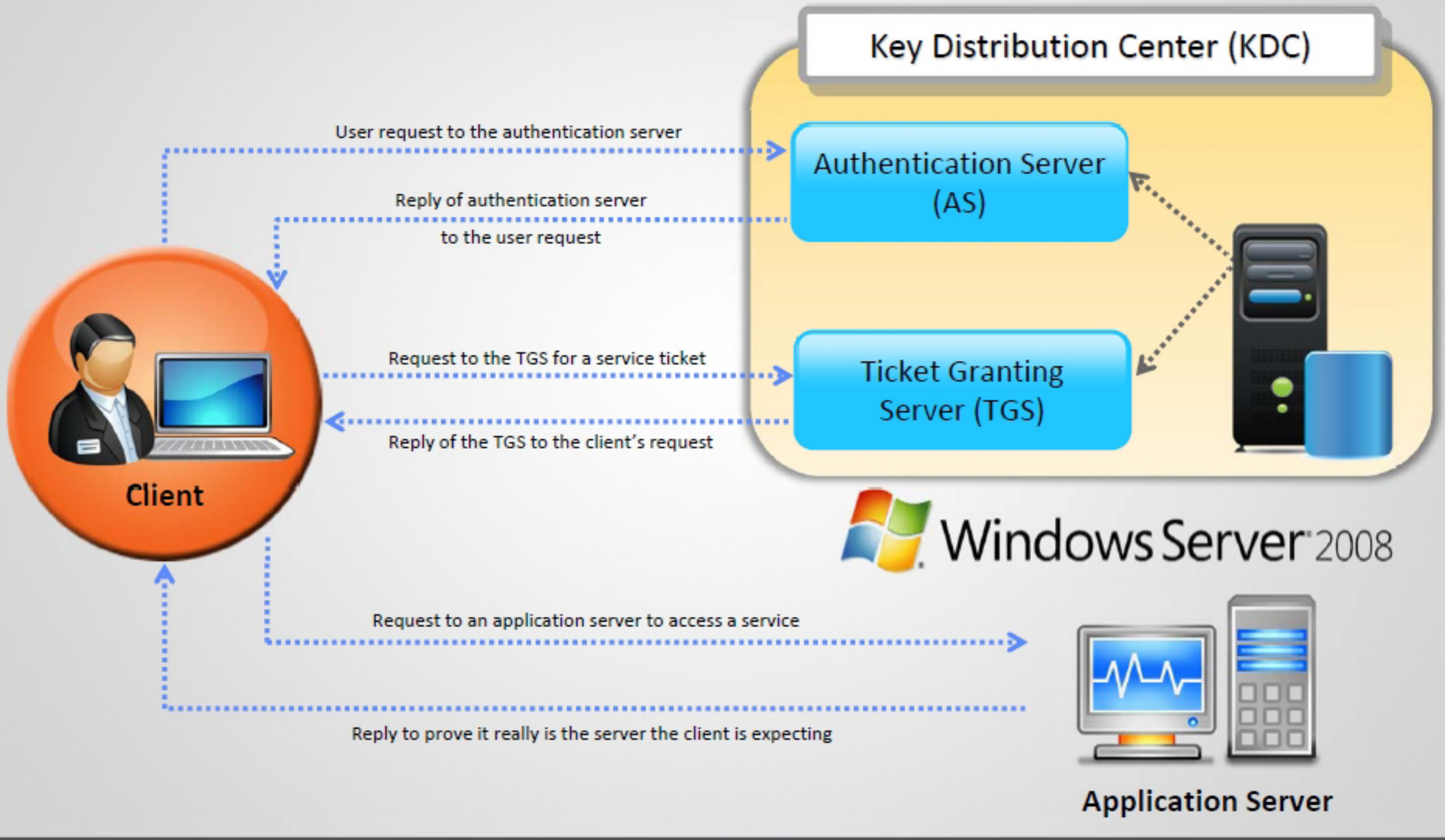
DC **compares computer's response** with the response it created with its own hash

If they **match**, the **logon is a success**

6 `Aa r8 ppq kgj89 pqr`

Note: Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM

Kerberos Authentication



LM, NTLMv1, and NTLMv2

Attribute	LM	NTLMv1	NTLMv2	
Password Case Sensitive	No	YES	YES	✓
Hash Key Length	56bit + 56bit	-	-	✓
Password Hash Algorithm	DES (ECB mode)	MD4	MD5	✓
Hash Value Length	64bit + 64bit	128bit	128bit	✓
C/R Key Length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit	✓
C/R Algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5	✓
C/R Value Length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit	✓

How Are Passwords Stored in Linux?

1

LOCAL passwords are stored in one of two places: `/etc/passwd`, or `/etc/shadow`

2

Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called "`/etc/passwd`"

3

`/etc/passwd` file is readable to all users

4

In shadow password format, Linux stores account information in the `/etc/passwd` file in a compatible format; however, the password is stored as a single "x" character and a second file, called "`/etc/shadow`", contains the encrypted password as well as other information such as account or password expiration values, etc.

5

The `/etc/shadow` file is readable only by the root account and is therefore less of a security risk

Steps for Password Cracking Penetration Testing

Step 1	Identify the target person's personal profile
Step 2	**Perform non-electronic attacks**
Step 3	Build a dictionary of word lists
Step 4	**Attempt to guess passwords**
Step 5	Perform brute-force and dictionary attacks
Step 6	**Perform wire sniffing to capture passwords**
Step 7	Perform man-in-the-middle attack to collect passwords
Step 8	**Perform replay attack to collect passwords**

Steps for Password Cracking Penetration Testing (Cont'd)

Step 9	Extract SAM file in Windows machines
Step 10	**Perform hash injection (pass-the-hash) attack**
Step 11	Perform rainbow attack (perform password attack using pre-computed hashes)
Step 12	**Extract cleartext passwords from an encrypted LM hash**
Step 13	Perform password cracking using Distributed Network Attack
Step 14	**Extract `/etc/passwd` and `/etc/shadow` files in Linux systems**
Step 15	Use automated password crackers to break password-protected files
Step 16	**Use a Trojan/spyware/keyloggers to capture passwords**

Step 1: Identify the Target Person's Personal Profile

- Use dice.com, Monster, and other job sites to **look for the target person's personal information**
- Use **people search online services** to collect the information
- Collect the **personal information from social networking sites** such as LinkedIn, Facebook, Twitter, Orkut, MySpace, etc.

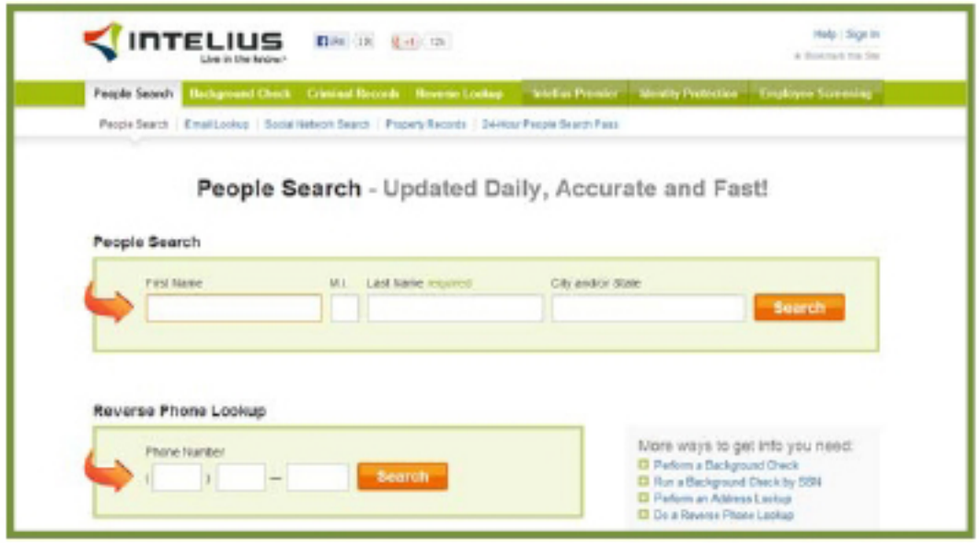
Find out the following information about the target person's:

- Residential addresses, contact number, email address, and favorite car
- Birthday, anniversary day, and other special occasions
- Movies, music, sports, drama, and arts
- Education, cartoon characters, novelists
- Parents, relatives, kids' names
- Country, city, holiday resorts, etc.

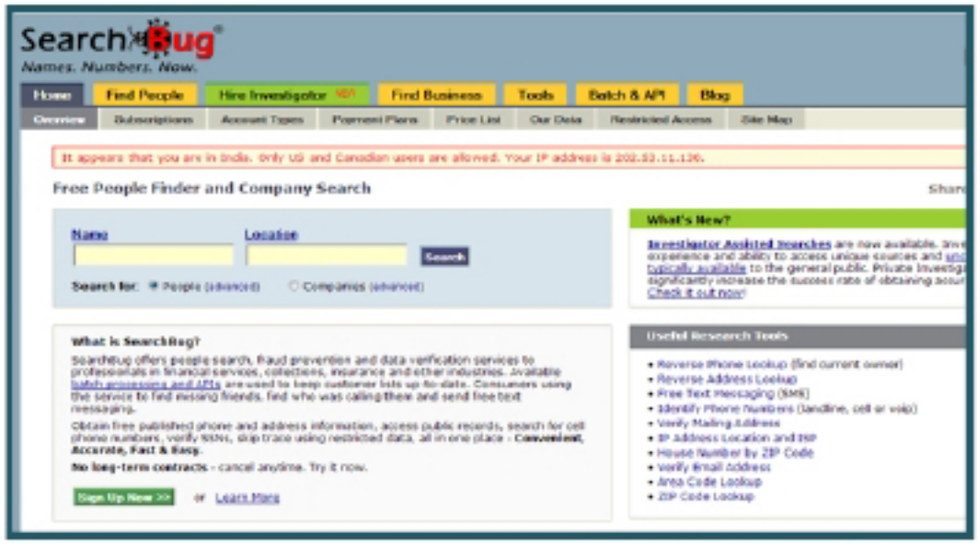
People Search Using http://pipl.com

- Pipl uses a technique known as **"the deep web"** to extract information about people
- The term **"deep web"** refers to a vast repository of underlying content, such as documents in online databases that general-purpose **web crawlers** cannot reach

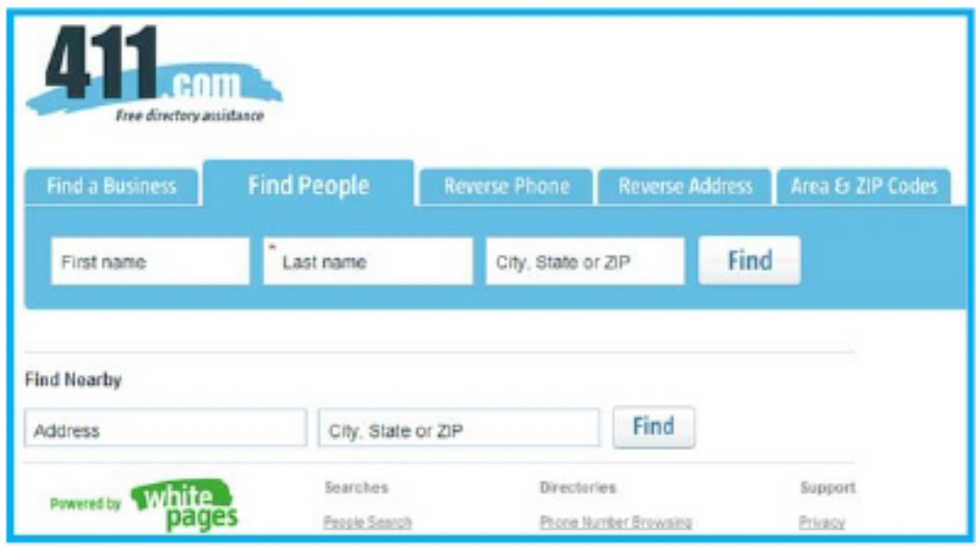
People Search on Online Services



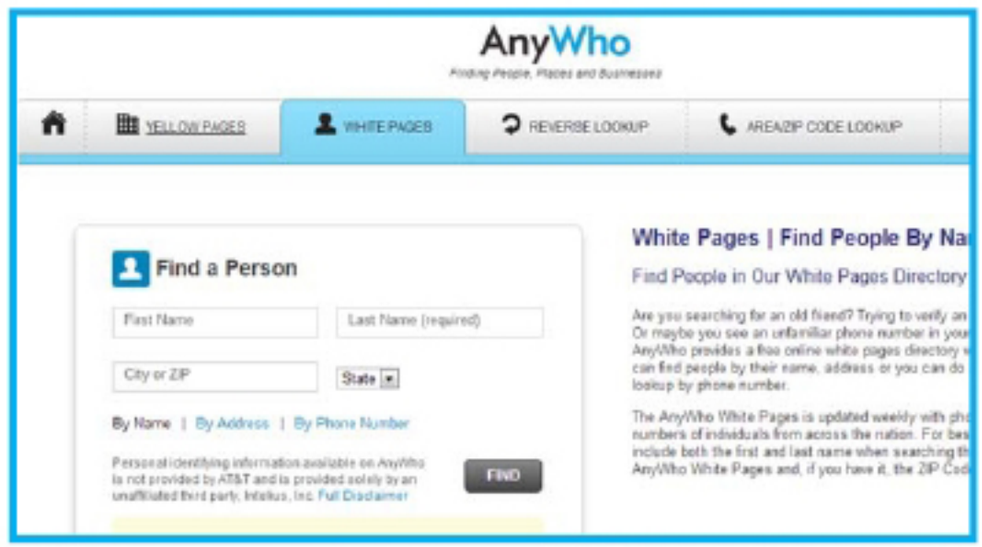
http://www.intelius.com



http://www.searchbug.com



http://www.411.com



http://www.anywho.com

People Search Online Services

Yahoo People Search
http://people.yahoo.com

Address.com
http://www.address.com

123 People Search
http://www.123people.com

Zaba Search
http://www.zabasearch.com

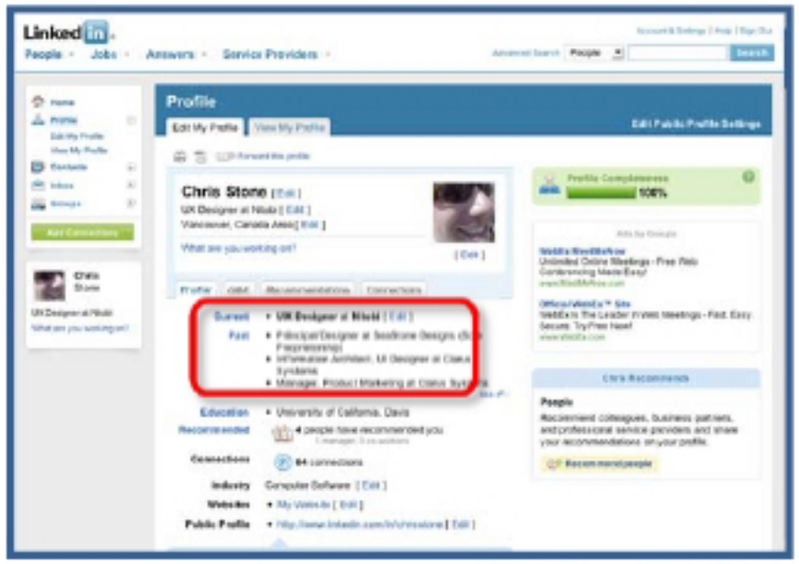
Wink People Search
http://wink.com

Public People Finder
http://www.publicpeoplefinder.com

People Finders
http://www.peoplefinders.com

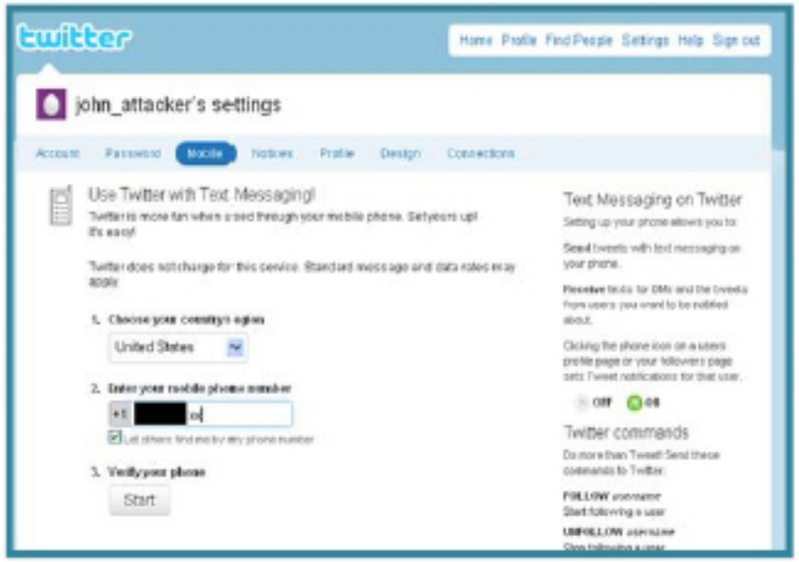
People Lookup
https://www.peoplelookup.com

People Search on Social Networking Services

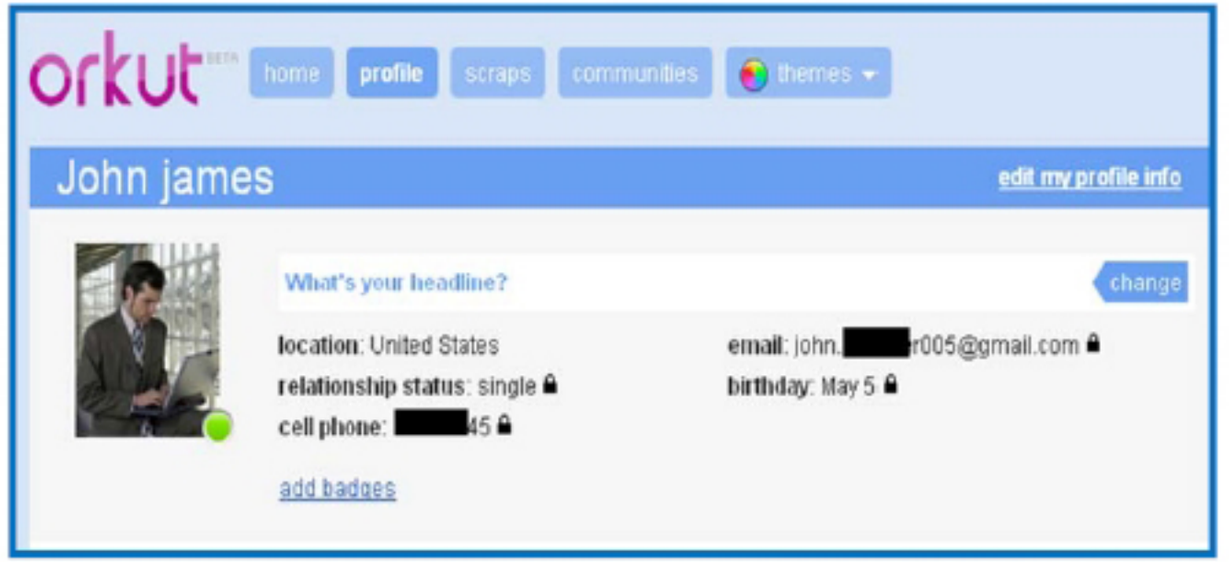


http://www.linkedin.com

http://www.facebook.com



http://twitter.com



http://www.orkut.com

People Search on Job Sites

- Gather a **company's infrastructure details** from job postings
- **Look for this information:**
  - Job requirements
  - Employee's profile
  - Hardware information
  - Software information

Job ID
17123.6554670.6
42319173004

Location
Boca Raton, FL 33487

Job Status
IT/Software Development

Apply Now

Become a Fan on facebook

Network Administrator, Active Directory, Citrix, Exchange

Job Description:

- Design and implement technical solutions on the Windows platform to support business requirements.
- Support existing Windows Infrastructure including: Active Directory 2003, SMS, SUS, Citrix Metaframe, SQL Server, SQL Clusters, Exchange 5.5, Exchange 2003, VM Ware, Veritas backup software, Account and server security, Disaster Recovery services, RAID technologies, and Fibre/SAN disk solutions.

Job Experience:

- 5 or more years experience working in IT implementing and supporting a global business
- Prior experience in supporting a global Windows server and Domain Infrastructure
- Experience implementing and supporting Active Directory, Citrix Metaframe, SQL Server, SQL Cluster, DNS, DHCP, WINS, and Exchange 2003 in an Enterprise environment
- Very strong systems troubleshooting skills
- Experience in providing 24-hour support to a global enterprise as part of an on-call rotation
- Effective interpersonal skills with the ability to be persuasive
- Other skills: Building Effective Teams, Action Oriented Peer Relationships, Customer Focus, Priority Setting, Problem Solving, and Business Acumen
- Bachelorâ€™s Degree or equivalent experience
- MCSE (2003) certification a plus, Citrix Certification a plus

Step 2: Perform Non-Electronic Attacks

Shoulder Surfing

- **Look** at either the **user's keyboard** or **screen** while he/she is logging in
- **Gaze into someone's password** or PIN code with the help of binoculars or a low-power telescope

Dumpster Diving

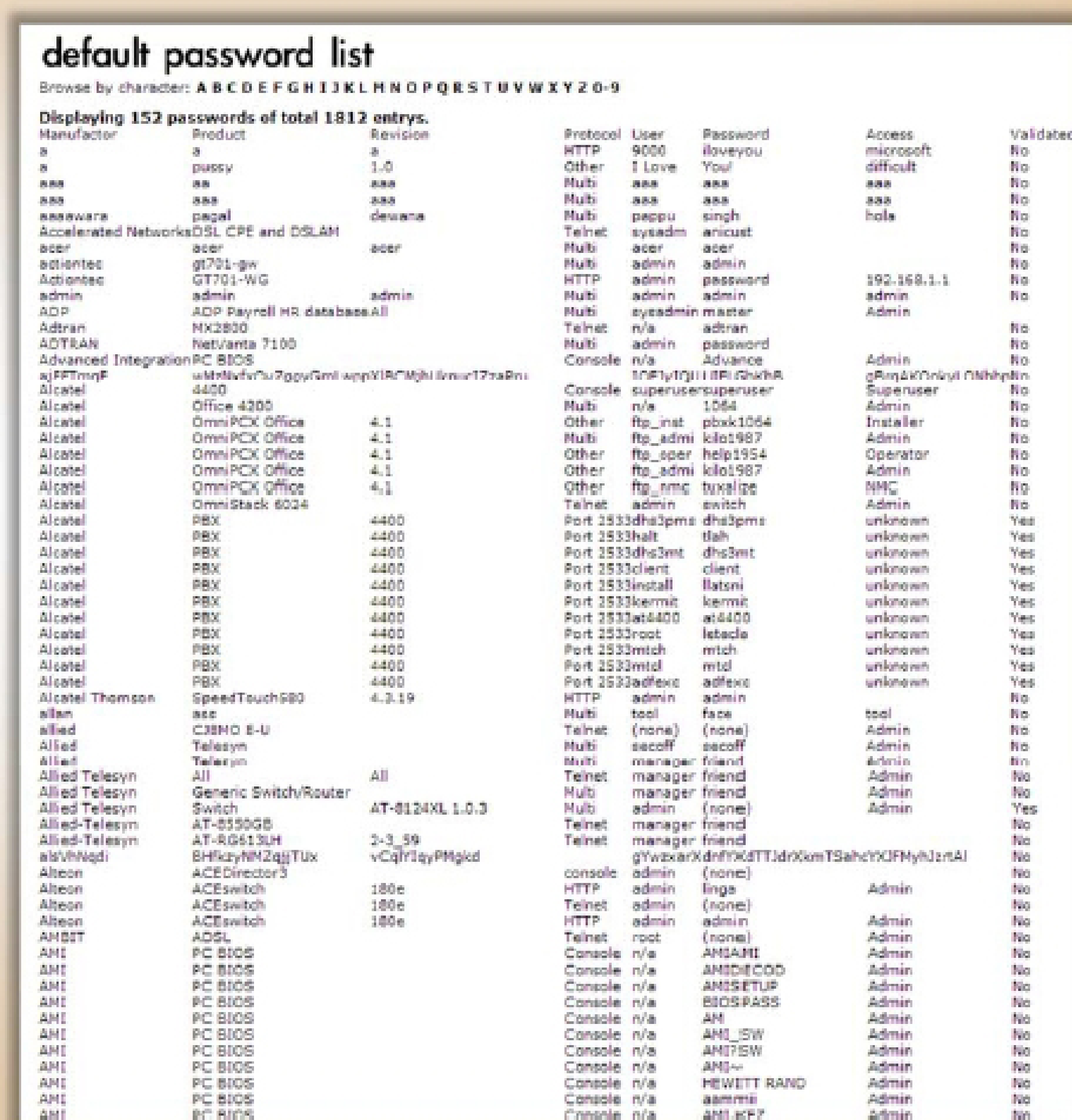
- Search for **sensitive information** in the user's trashbins, printer trash bins, and at the user's desk for sticky notes

Social Engineering

- **Convince** the target person to **reveal the confidential information**
- Call the target person and **ask questions** that reveal sensitive information

Step 3: Build a Dictionary of Word Lists

- **Note down the information** gathered from step 1 and step 2 into the text file
- Use a dictionary maker tool to **create a word list**
- Try to **find a default password** supplied by the manufacturer with new equipment
- Online tools that can be used to search default passwords:
  - http://www.defaultpassword.com
  - http://default-password.info
  - http://www.defaultpassword.us
  - http://www.passwordsdatabase.com



default password list

Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9

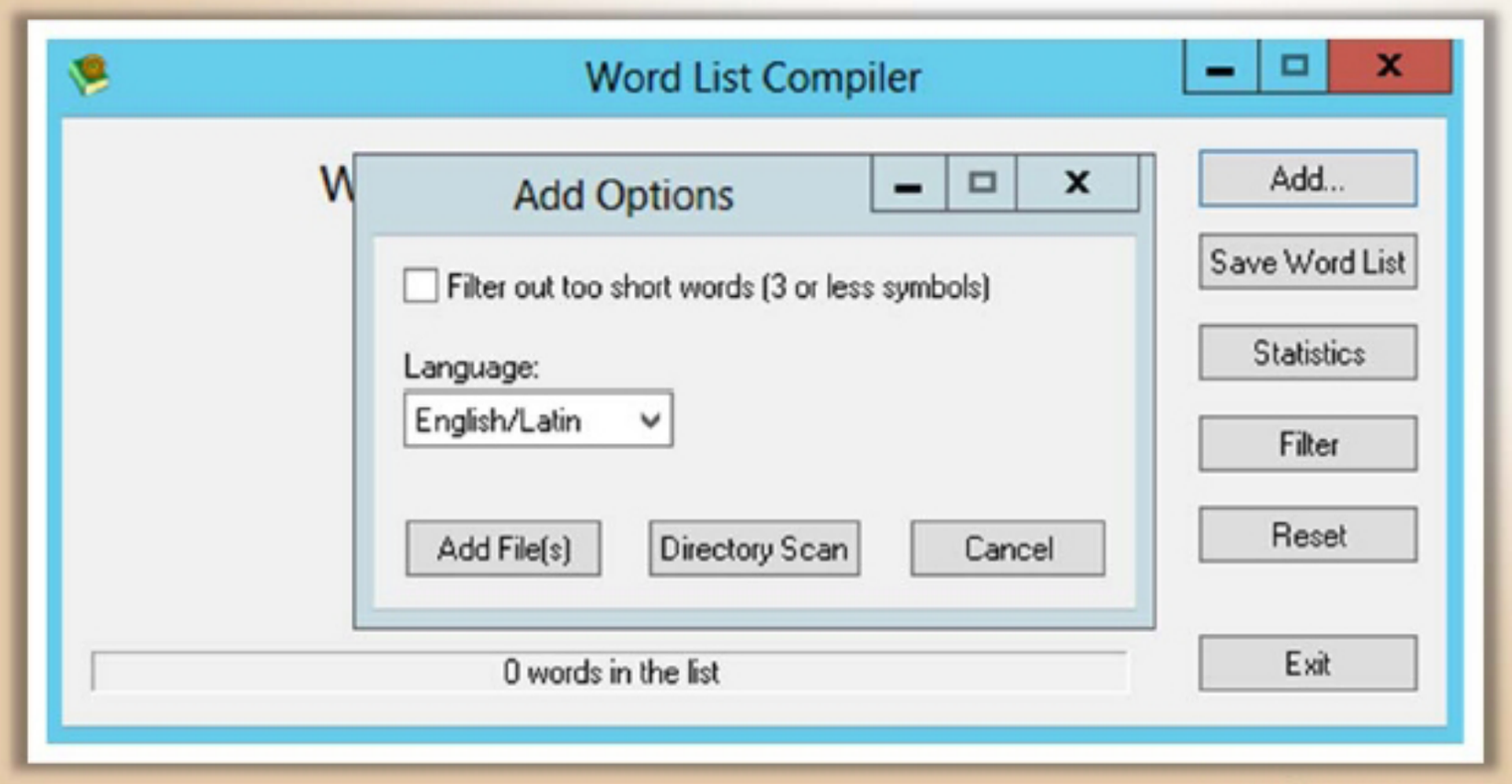
Displaying 152 passwords of total 1812 entrys.

Manufactor	Product	Revision	Protocol	User	Password	Access	Validated
a	a	a	HTTP	9000	iloveyou	microsoft	No
a	pussy	1.0	Other	I Love	You!	difficult	No
aaa	aa	aaa	Multi	aaa	aaa	aaa	No
aaa	aaa	aaa	Multi	aaa	aaa	aaa	No
aaaaware	pagal	dewana	Multi	pappu	singh	hola	No
Accelerated Networks	DSL CPE and DSLAM		Telnet	sysadm	anicust		No
acer	acer	acer	Multi	acer	acer		No
actiontec	gt701-gw		Multi	admin	admin		No
Actiontec	GT701-WG		HTTP	admin	password	192.168.1.1	No
admin	admin	admin	Multi	admin	admin	admin	No
ADP	ADP Payroll HR database	All	Multi	sysadmin	master	Admin	
Adtran	MX2800		Telnet	n/a	adtran		No
ADTRAN	NetVanta 7100		Multi	admin	password		No
Advanced Integration	PC BIOS		Console	n/a	Advance	Admin	No
ajFFTmqF	[illegible]			[illegible]	[illegible]	gRnqAKOnkyLONhhp	No
Alcatel	4400		Console	superuser	superuser	Superuser	No
Alcatel	Office 4200		Multi	n/a	1064	Admin	No
Alcatel	OmniPCX Office	4.1	Other	ftp_inst	pbxk1064	Installer	No
Alcatel	OmniPCX Office	4.1	Multi	ftp_admi	kilo1987	Admin	No
Alcatel	OmniPCX Office	4.1	Other	ftp_oper	help1954	Operator	No
Alcatel	OmniPCX Office	4.1	Other	ftp_admi	kilo1987	Admin	No
Alcatel	OmniPCX Office	4.1	Other	ftp_nmc	tuxalize	NMC	No
Alcatel	OmniStack 6024		Telnet	admin	switch	Admin	No
Alcatel	PBX	4400	Port 2533	dhs3pms	dhs3pms	unknown	Yes
Alcatel	PBX	4400	Port 2533	halt	tlah	unknown	Yes
Alcatel	PBX	4400	Port 2533	dhs3mt	dhs3mt	unknown	Yes
Alcatel	PBX	4400	Port 2533	client	client	unknown	Yes
Alcatel	PBX	4400	Port 2533	install	llatsni	unknown	Yes
Alcatel	PBX	4400	Port 2533	kermit	kermit	unknown	Yes
Alcatel	PBX	4400	Port 2533	at4400	at4400	unknown	Yes
Alcatel	PBX	4400	Port 2533	root	letacla	unknown	Yes
Alcatel	PBX	4400	Port 2533	mtch	mtch	unknown	Yes
Alcatel	PBX	4400	Port 2533	mtcl	mtcl	unknown	Yes
Alcatel	PBX	4400	Port 2533	adfexc	adfexc	unknown	Yes
Alcatel Thomson	SpeedTouch580	4.2.19	HTTP	admin	admin		No
allan	acc		Multi	tool	face	tool	No
allied	CJ8MO E-U		Telnet	(none)	(none)	Admin	No
Allied	Telesyn		Multi	secoff	secoff	Admin	No
Allied	Telesyn		Multi	manager	friend	Admin	No
Allied Telesyn	All	All	Telnet	manager	friend	Admin	No
Allied Telesyn	Generic Switch/Router		Multi	manager	friend	Admin	No
Allied Telesyn	Switch	AT-8124XL 1.0.3	Multi	admin	(none)	Admin	Yes
Allied-Telesyn	AT-8550GB		Telnet	manager	friend		No
Allied-Telesyn	AT-RG613LH	2-3_59	Telnet	manager	friend		No
alsVhNqdi	BHfkzyNM2qjjTUx	vCqfr1qyPMgkd		gYwzxarX	[illegible]	dnfYXdTTJdrXkmTSahcYXJFMyhJzrtAl	No
Alteon	ACEDirector3		console	admin	(none)		No
Alteon	ACEswitch	180e	HTTP	admin	linga	Admin	No
Alteon	ACEswitch	180e	Telnet	admin	(none)		No
Alteon	ACEswitch	180e	HTTP	admin	admin	Admin	No
AMBIT	ADSL		Telnet	root	(none)	Admin	No
AMI	PC BIOS		Console	n/a	AM!AMI	Admin	No
AMI	PC BIOS		Console	n/a	AMIDECOD	Admin	No
AMI	PC BIOS		Console	n/a	AMISETUP	Admin	No
AMI	PC BIOS		Console	n/a	BIOSPASS	Admin	No
AMI	PC BIOS		Console	n/a	AM	Admin	No
AMI	PC BIOS		Console	n/a	AMI_SW	Admin	No
AMI	PC BIOS		Console	n/a	AMI?SW	Admin	No
AMI	PC BIOS		Console	n/a	AMI~	Admin	No
AMI	PC BIOS		Console	n/a	HEWITT RAND	Admin	No
AMI	PC BIOS		Console	n/a	aammii	Admin	No
AMI	PC BIOS		Console	n/a	AMI.KEZ	Admin	No

http://www.defaultpassword.com

Dictionary Maker Tool: Word List Compiler

- Word List Compiler is a tool to **compose dictionaries** (word lists) for password recovery using **multiple source text files**
- It **extracts all words from source text files** and puts them into the output dictionary



http://lastbit.com

Step 4: Attempt to Guess Passwords

- Set dictionary words and names, and try all the possible combinations to crack the password
- This method consists of five steps:

Find a valid user account

Create a list of possible passwords

Rank the passwords from high probability to low

Key in each password

If the system allows in – Success, or else try again

ECSA
EC-Council Certified Security Analyst

Step 5: Perform Brute-Force and Dictionary Attacks

- Use a password cracking tool such as Cain & Abel which performs **brute-force** and **dictionary attacks** to crack the password

Dictionary Attack

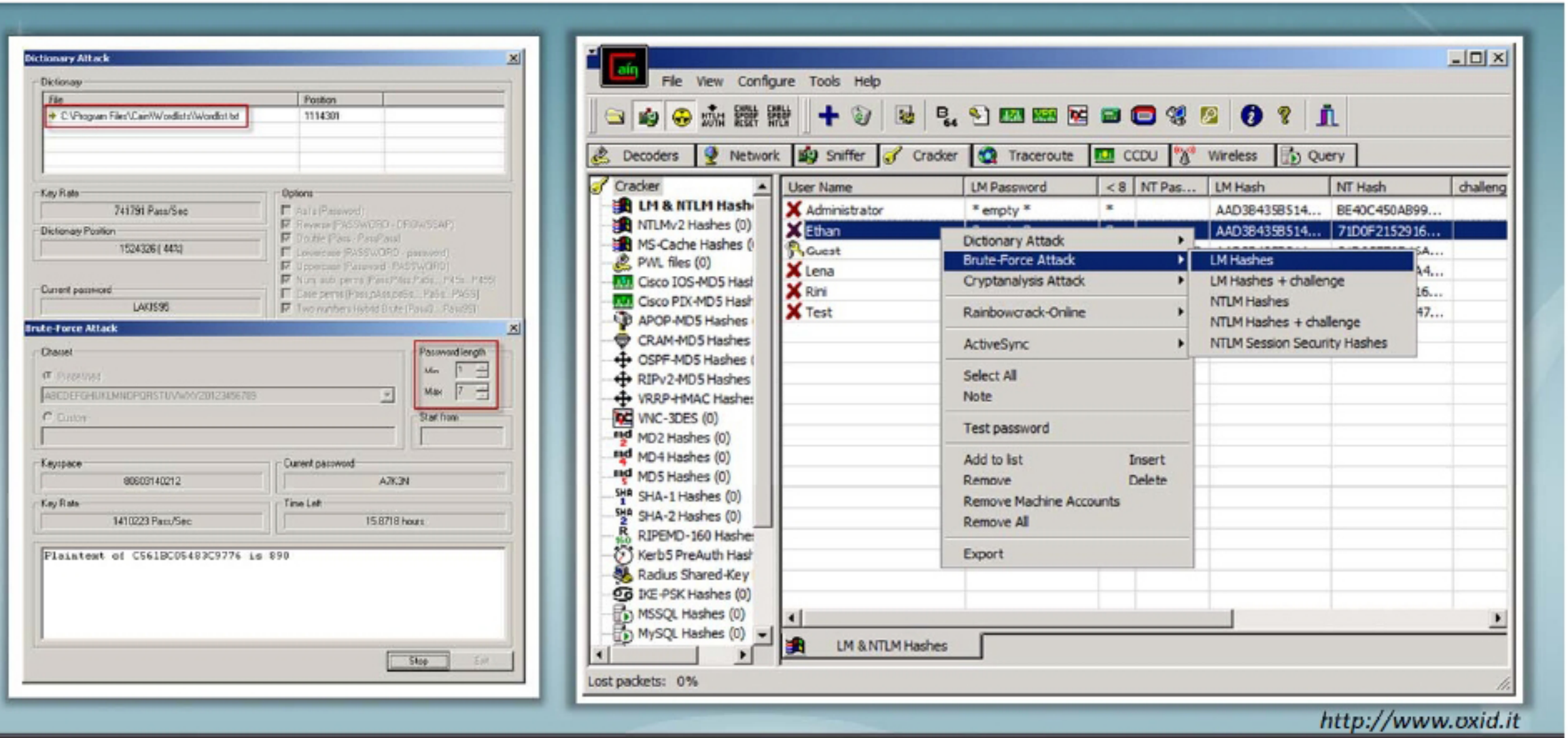
- Load the dictionary file (word list file) into the **password cracking application** that runs against user accounts
- Run a program that tries every **combination of characters** until the password is broken

Brute-force Attack

- Set the password length and **run the password cracking program** that tests all the possible **combinations of characters** in a pre-defined or custom character set

Password Cracking Tool: Cain & Abel

- Cain & Abel allows **recovery of various kind of passwords** by sniffing the network; cracking encrypted passwords using dictionary, brute-force and cryptanalysis attacks; decoding scrambled passwords; recovering wireless network keys; revealing password boxes; and uncovering cached passwords



http://www.oxid.it

Step 6: Perform Wire Sniffing to Capture Passwords

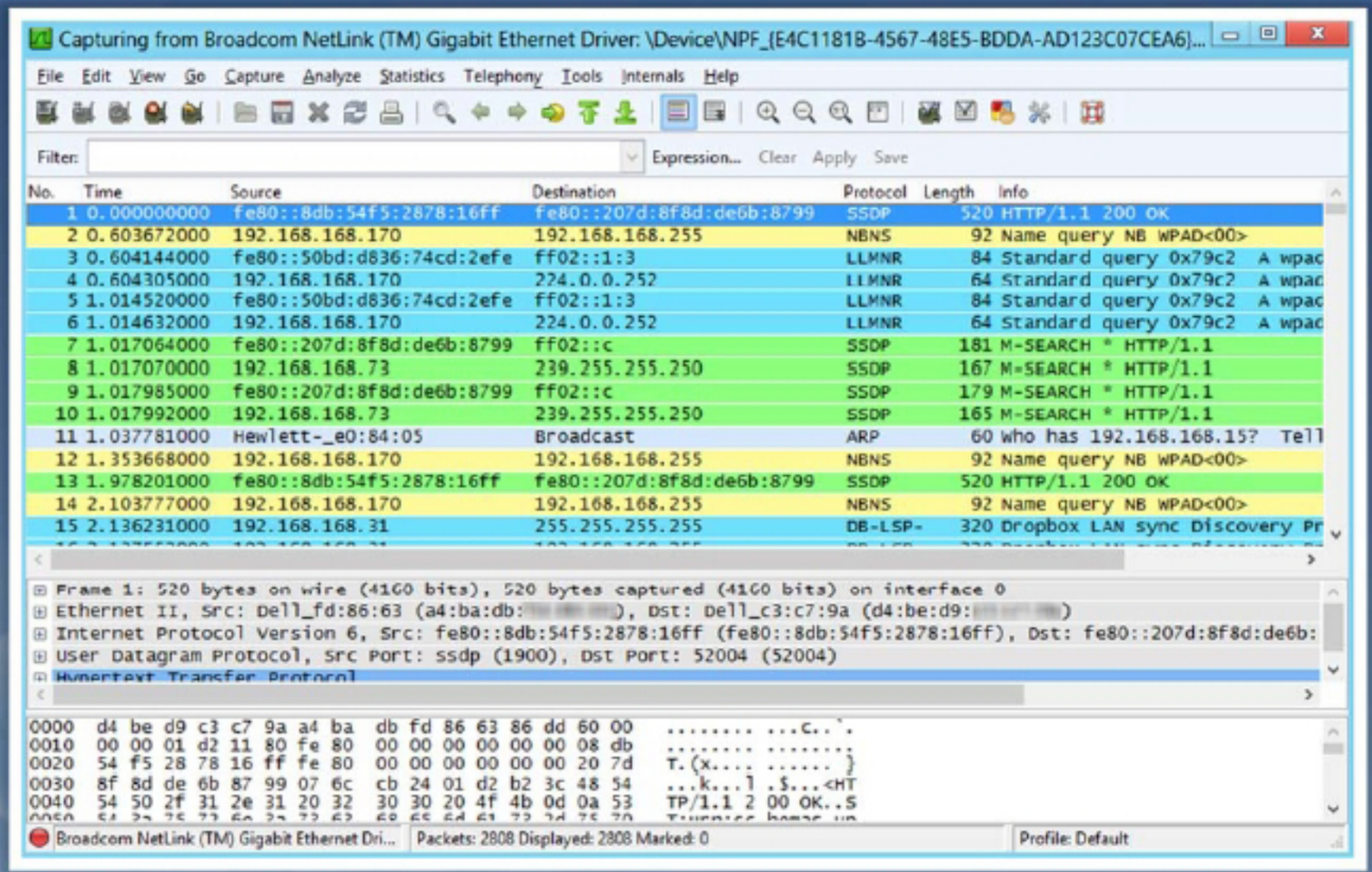
Capture **data packets** flowing across a computer network

Run packet sniffer tools on the **LAN to access** and **record the raw network traffic**

The captured data include **passwords sent to remote systems** during Telnet, FTP, rlogin sessions, and electronic mail sent and received

Packet Sniffing Tool: Wireshark

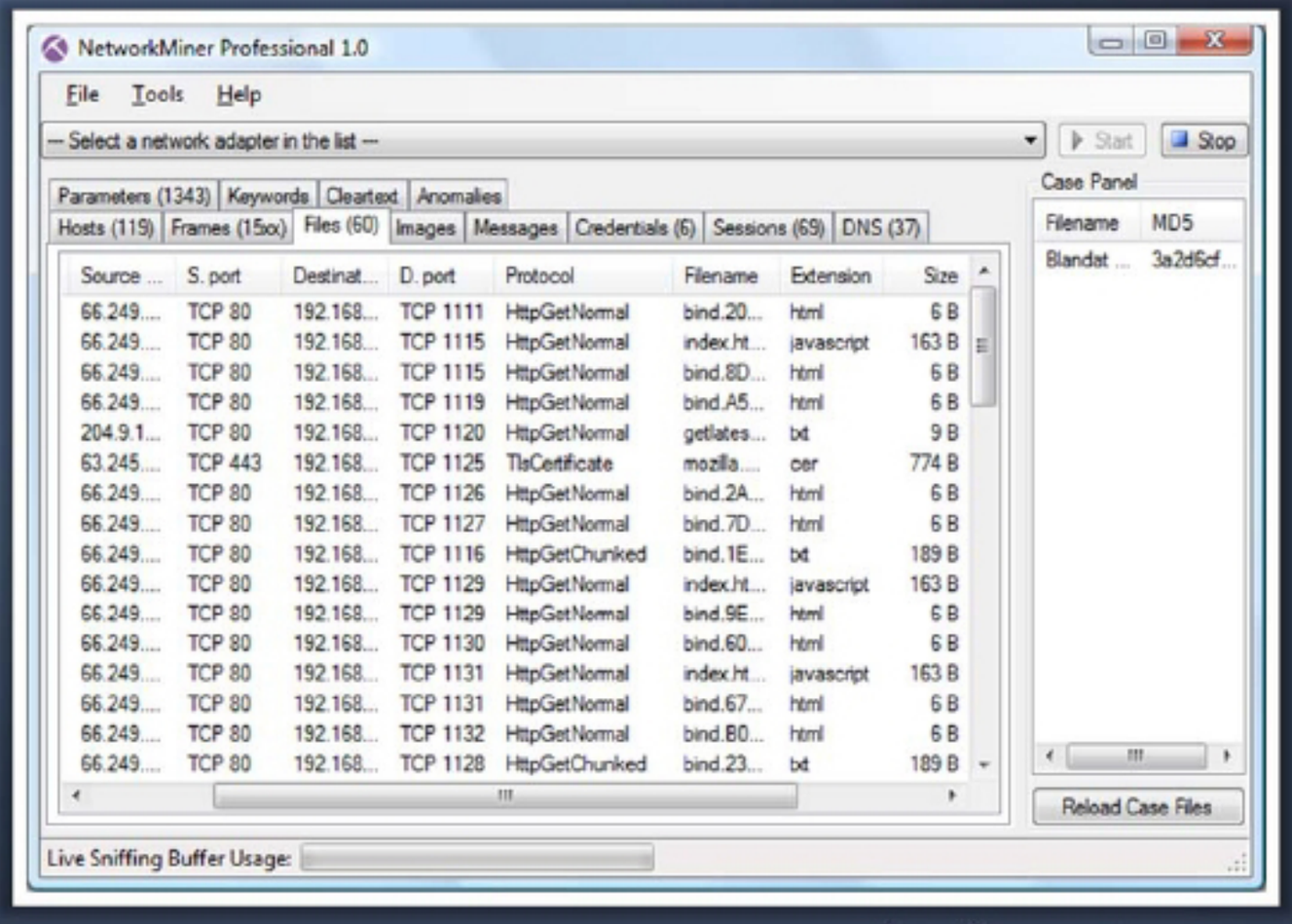
- Wireshark **captures live network traffic** from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks
- A set of filters for **customized data display** can be refined using a display filter



http://www.wireshark.org

Packet Sniffing Tool: NetworkMiner

- NetworkMiner is a **Network Forensic Analysis Tool** (NFAT) for Windows used as a passive network sniffer/packet capturing tool in order **to detect operating systems, sessions, hostnames, open ports**, etc.
- It **extracts files and certificates** transferred over the network by **parsing a PCAP file** or by sniffing traffic directly from the network



http://www.netresec.com

Packet Sniffing Tools

TCPdump
http://www.tcpdump.org

Sniff - O - Matic
http://www.kwakkelflap.com

Dsniff
http://monkey.org

Traffic IQ Professional
http://www.idappcom.com

MaaTec Network Analyzer
http://www.maatec.com

CommView
http://www.tamos.com

Colasoft Capsa Network Analyzer
http://www.colasoft.com

EtherDetect Packet Sniffer
http://www.etherdetect.com

Packet Sniffing Tools (Cont'd)

Ntop
http://www.ntop.org

EffeTech HTTP Sniffer
http://www.effetech.com

AnalogX Packetmon
http://www.analogx.com

IEInspector HTTP Analyzer
http://www.ieinspector.com

OmniPeek Network Analyzer
http://www.wildpackets.com

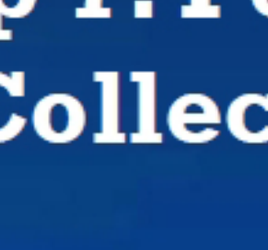
SmartSniff
http://www.nirsoft.net

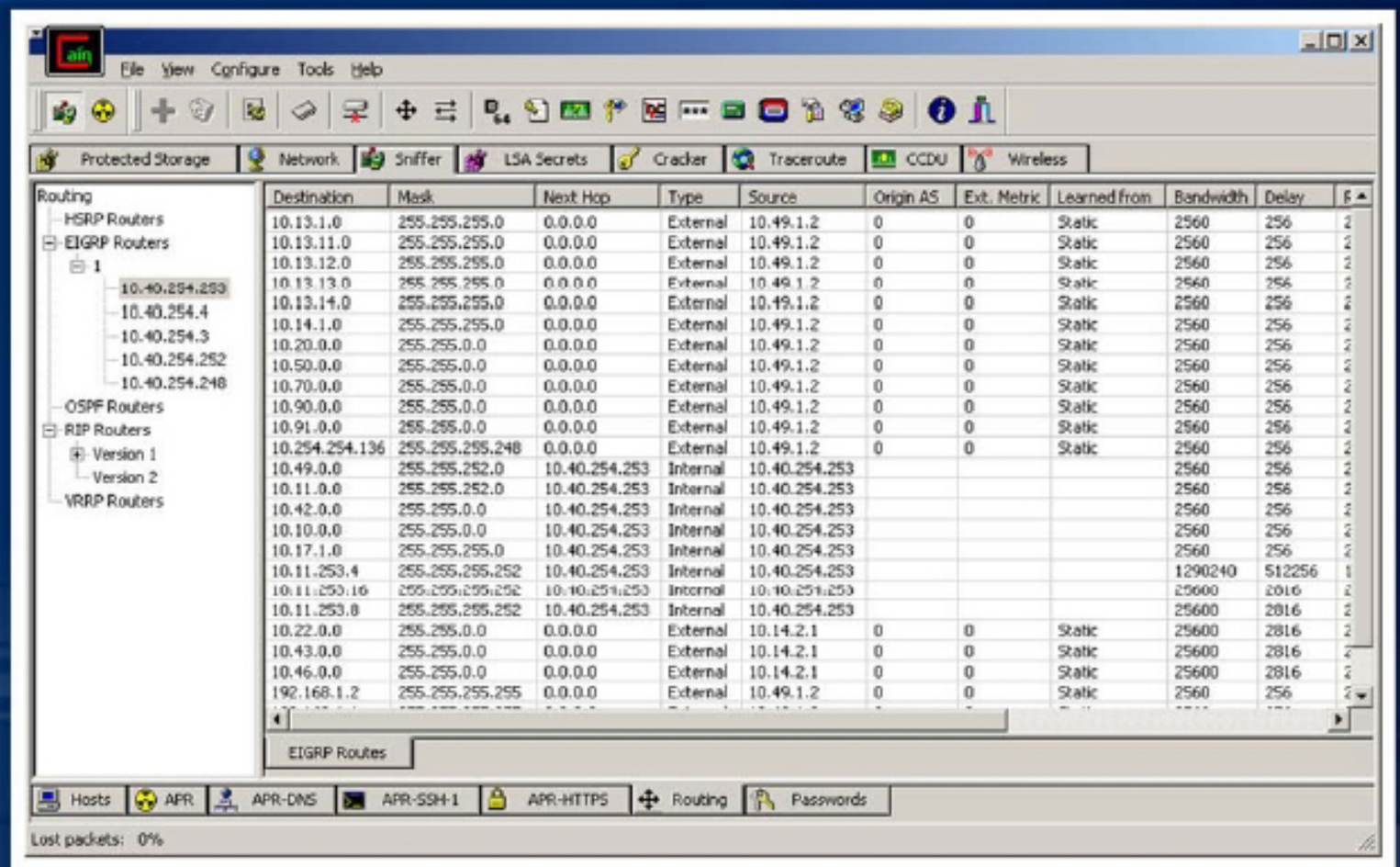
Observer
http://www.networkinstruments.com

Ettercap
http://ettercap.sourceforge.net

Step 7: Perform Man-in-the-Middle Attack to Collect Passwords

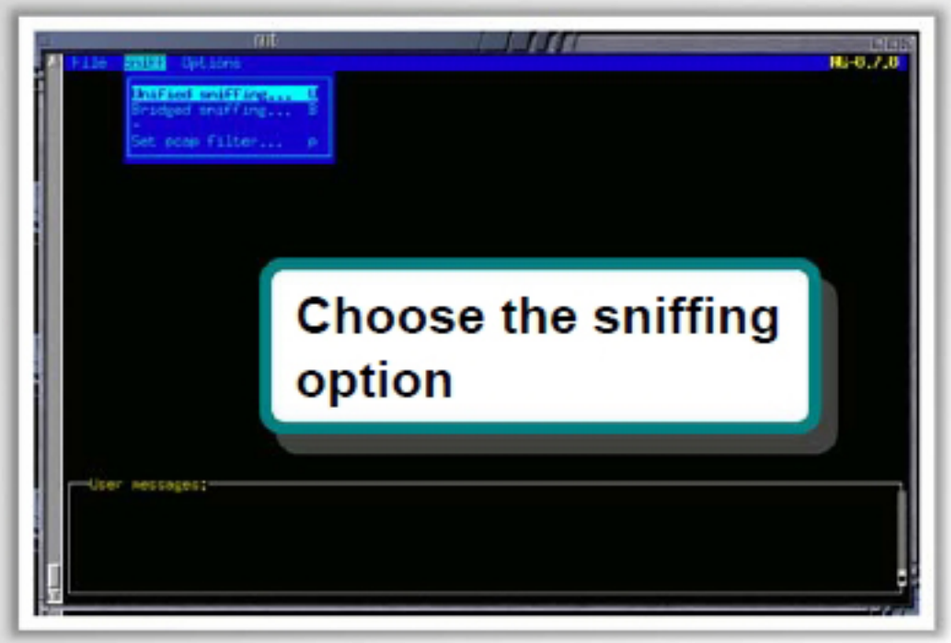
- Perform a MITM attack to **acquire access to the communication channels** between user and server to extract the password
- Use tools such as Cain & Abel, Ettercap, and dsniff to **capture passwords and authentication information** from the network

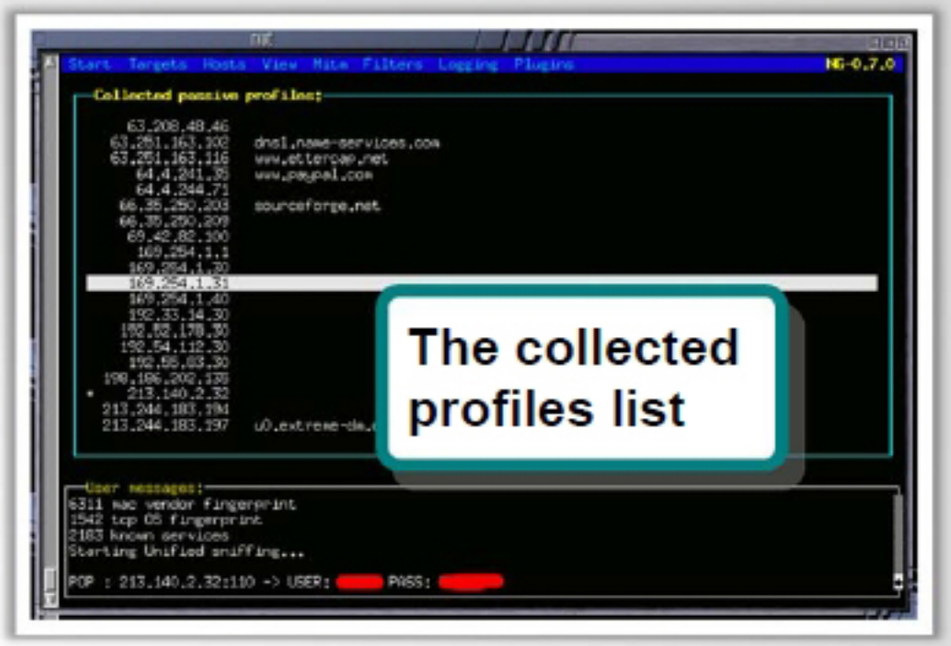


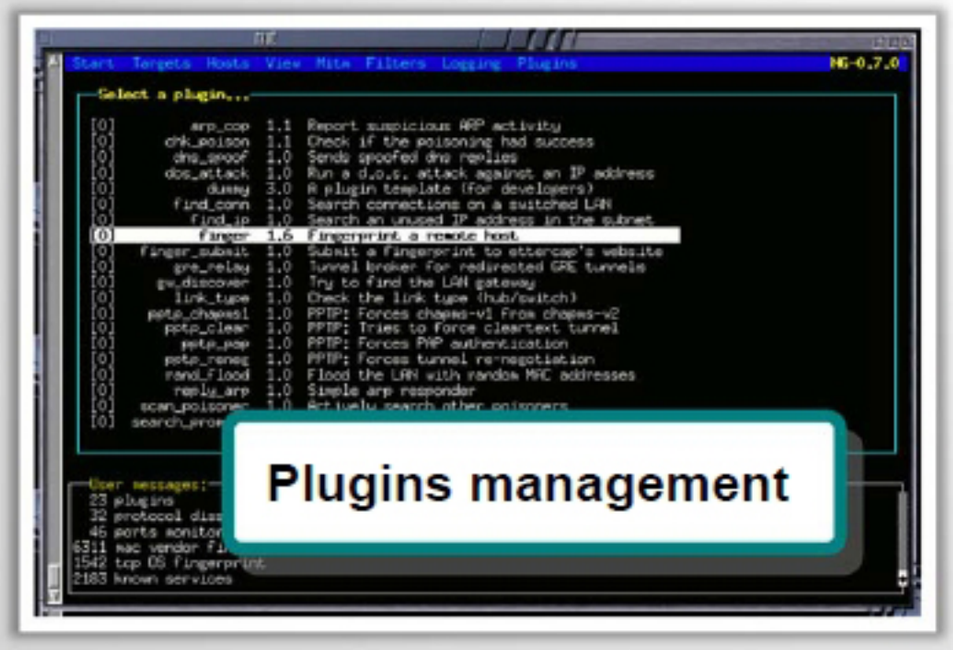


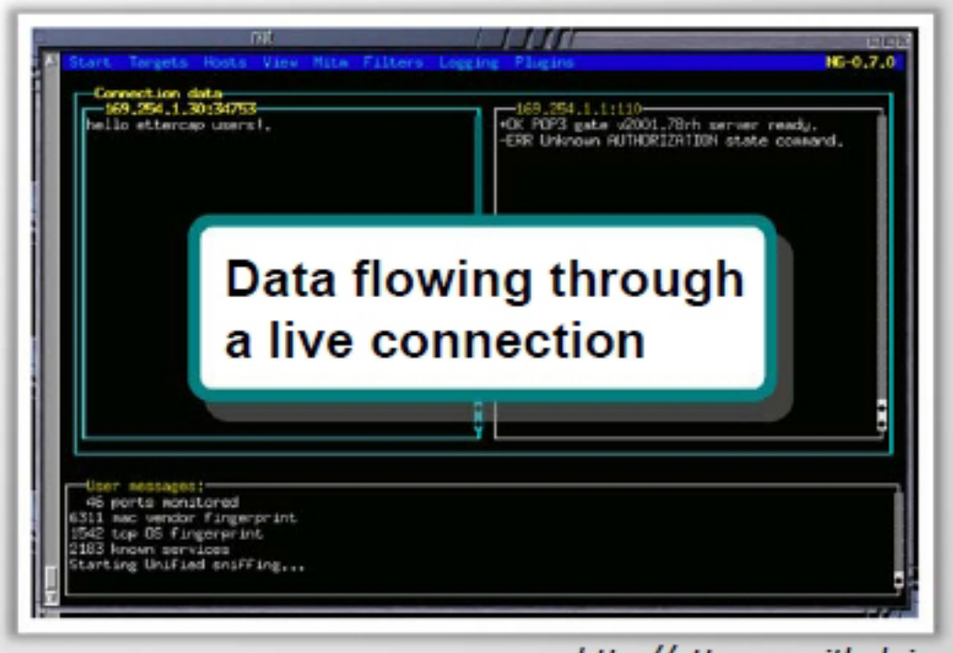
http://www.oxid.it

Man-in-the-Middle Attack Using Ettercap









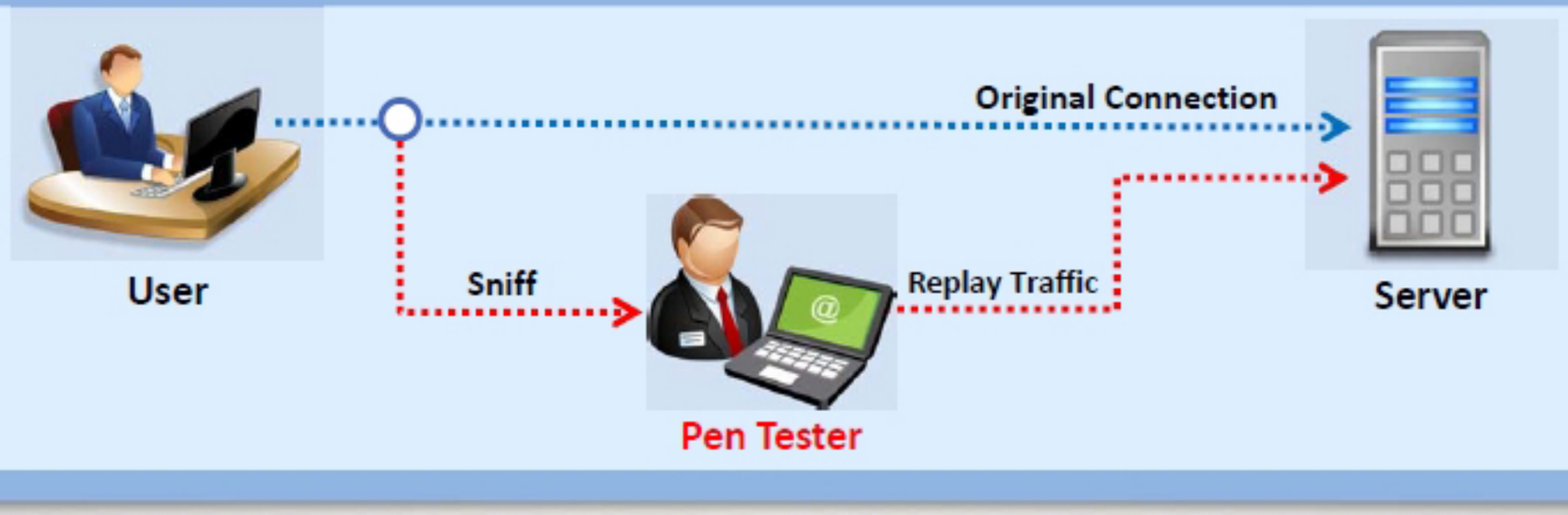
http://ettercap.github.io

Step 8: Perform Replay Attack to Collect Passwords

- In a replay attack, packets and authentication tokens are captured using a packet sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access

- A replay attack intercepts the data packets and resends them to the receiving server without decryption

- The attacker intercepts the communication using a network analyzer or sniffer such as Wireshark, Tcpdump (runs on Linux and UNIX systems), or WinDump (runs on Windows systems)



Network Analyzer: Tcpdump/WinDump

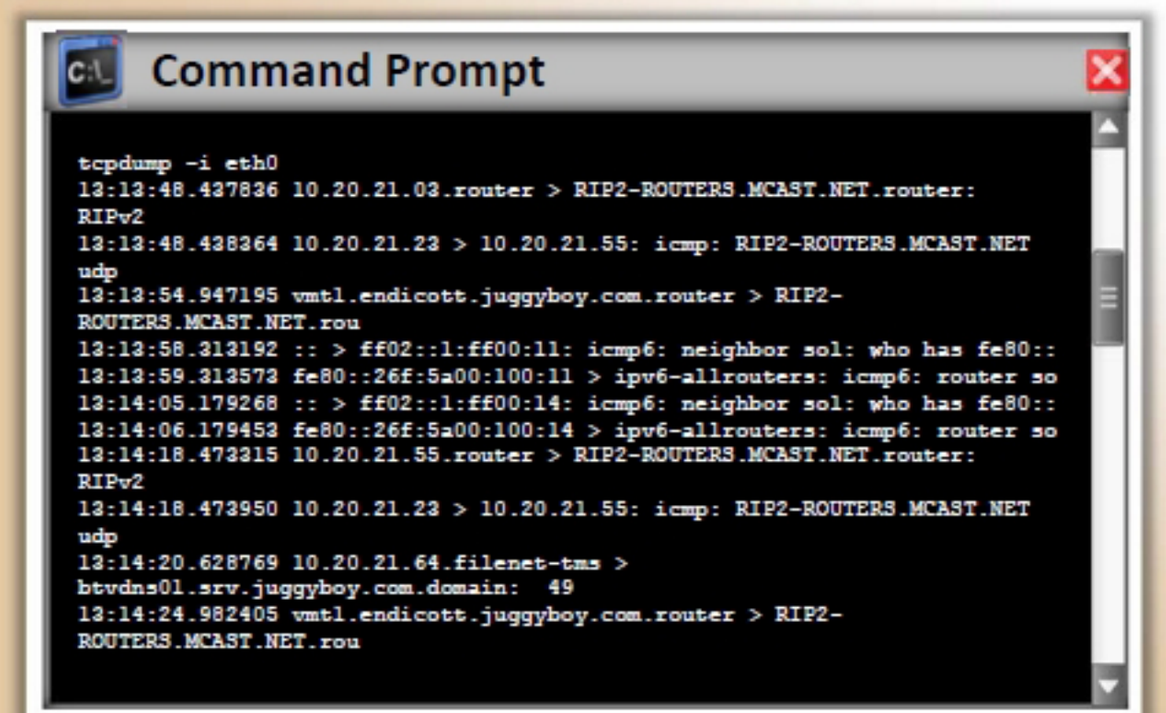
- Tcpdump is a **command line interface packet sniffer** which runs on Linux and UNIX

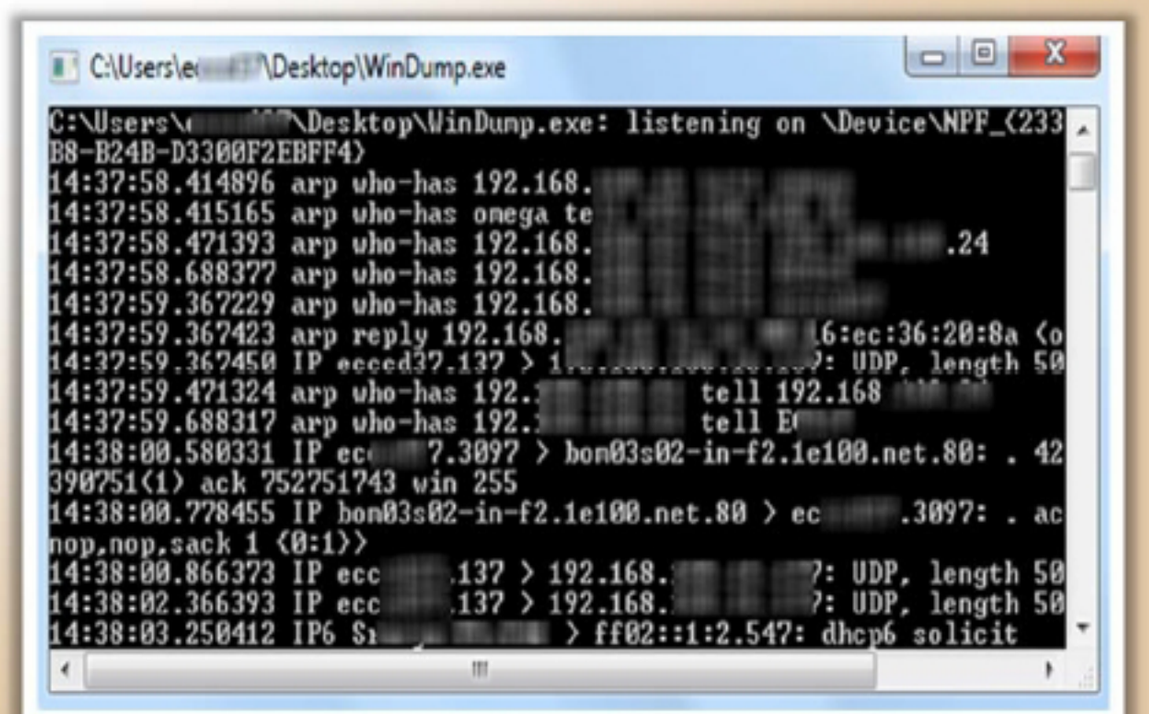
Tcpdump

Runs on Linux and UNIX systems

WinDump

Runs on Windows systems





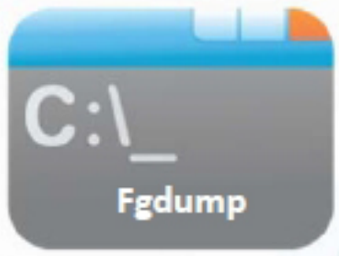
http://www.tcpdump.org

http://www.winpcap.org

Step 9: Extract SAM File in Windows Machines

- The SAM file is located at `c:\windows\system32\config\SAM`
- Use **PWdump7** and **Fgdump** tools to extract the SAM file in Windows machines

pwdump7.exe




```
fgdump.exe -h 192.168.0.10
-u AnAdministrativeUser -p
l4mep4ssw0rd
```

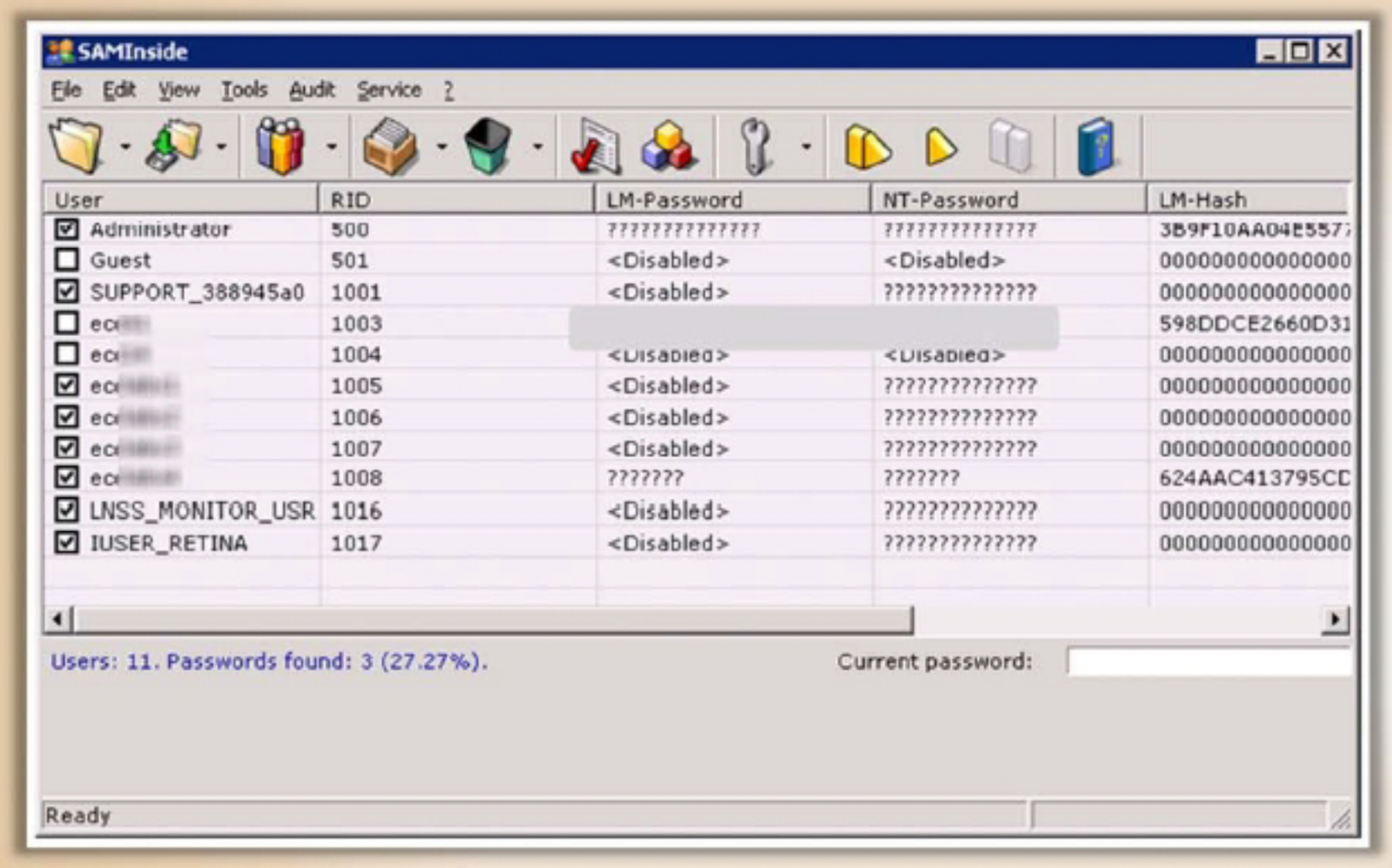
Dumps a remote machine (192.168.0.10) using a specified user

Fgdump works like pwdump but also extracts cached credentials and allows remote network execution

PWDUMP extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database

This tool must be run under an administrator account

Tool: SAMInside

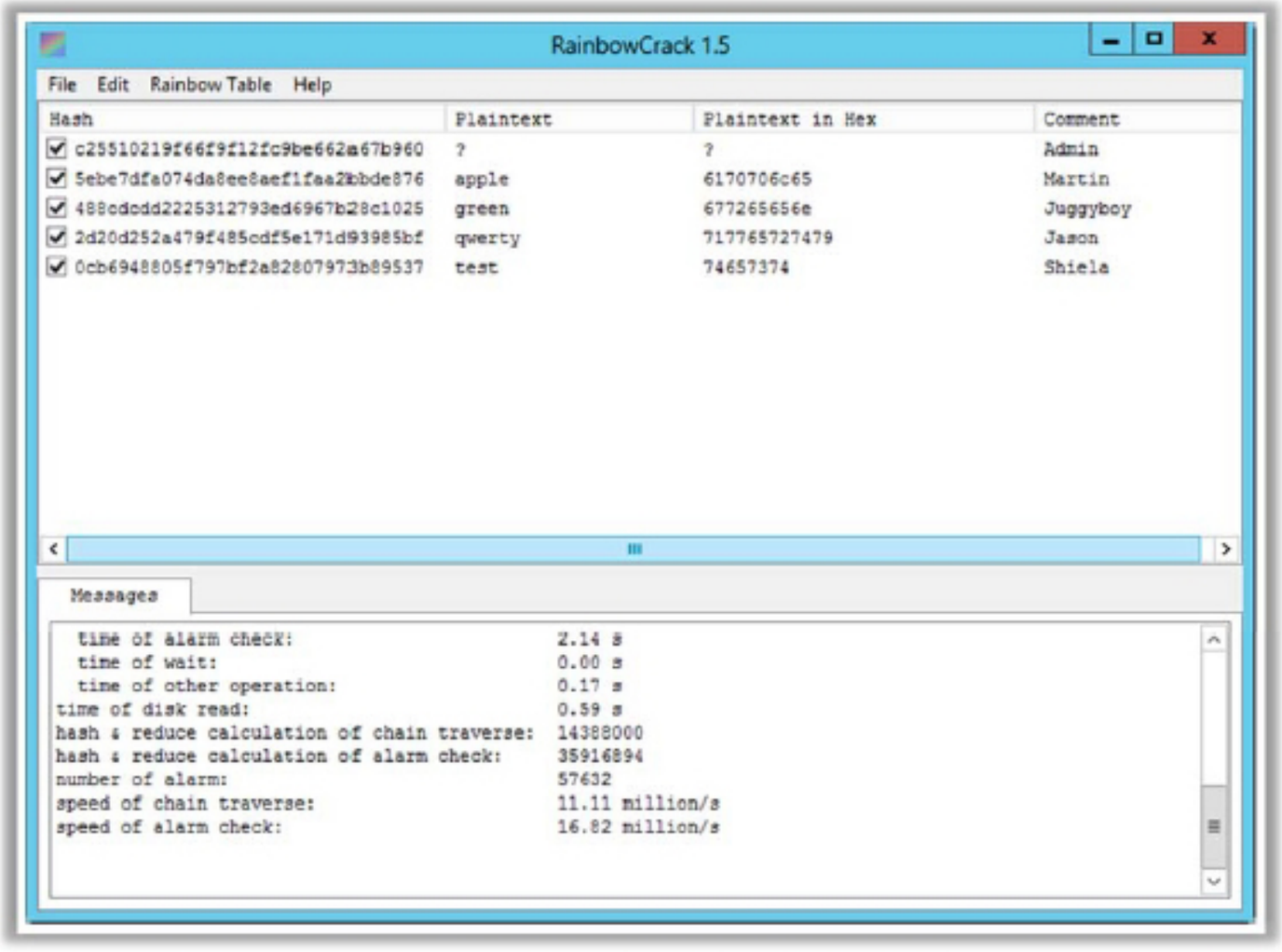


http://insidepro.com

- SAMInside is designated for the **recovery** of Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, and Windows 7 **user passwords**
- It has a **small footprint** and can be run from a diskette, CD/DVD disc or USB drive
- It includes over **10 types of data import** and **6 types of password attack** to recover the password

Step 11: Perform Rainbow Attack (Perform Password Attack Using Pre-Computed Hashes)

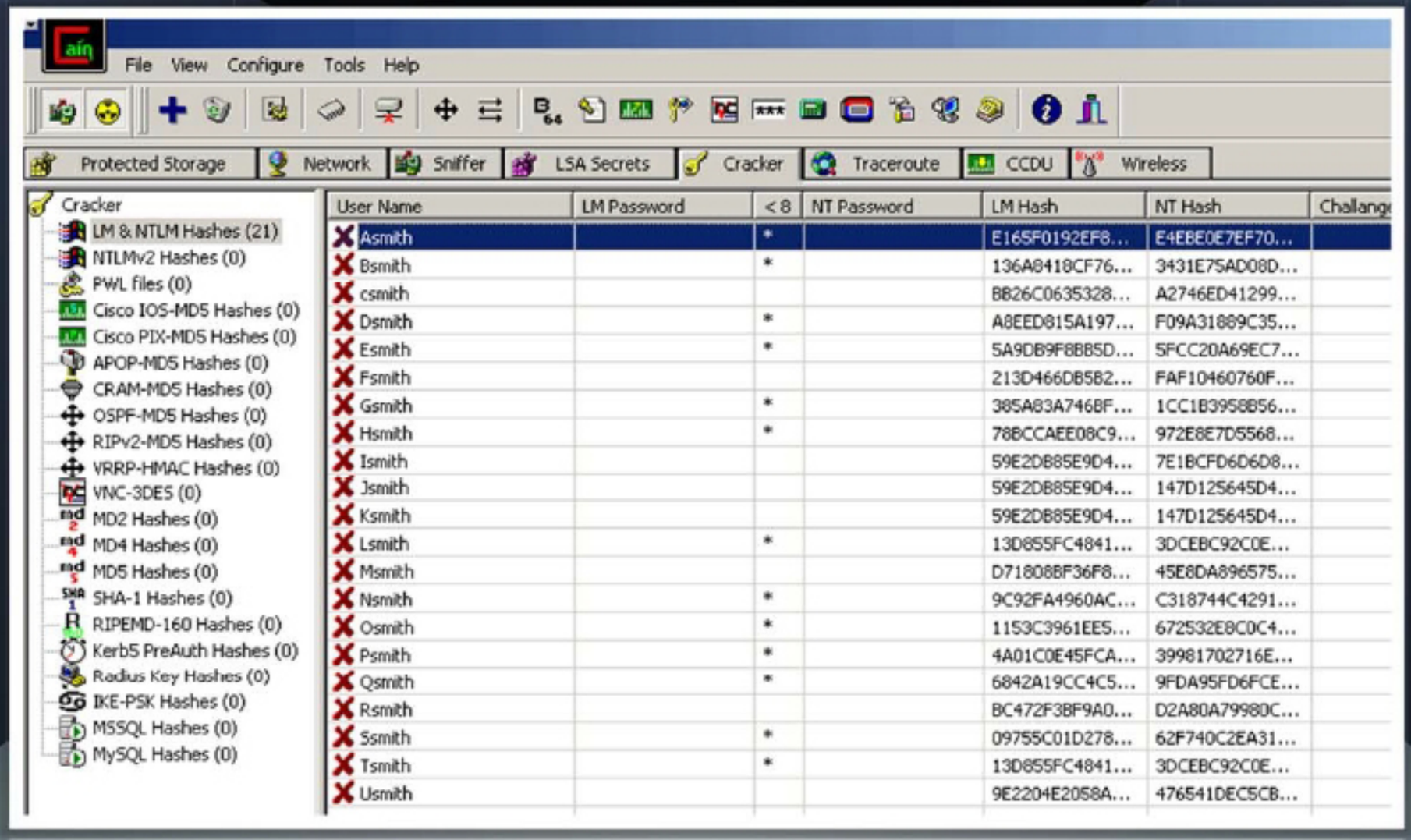
- Rainbow tables are files that **contain pre-computed hashes** of passwords
- **Convert huge word lists** like dictionary files and brute force lists into **password hashes** using techniques such as rainbow tables
- Download **rainbow tables** from the Internet
- **Compute the hash** for a list of possible passwords and **compare it with the pre-computed hash table**. If a **match is found** then the **password is cracked**
- Use the **RainbowCrack** tool to perform this attack



http://project-rainbowcrack.com

Step 12: Extract Cleartext Passwords from an Encrypted LM Hash

- Use the Cain & Abel tool to **extract cleartext passwords** from an **encrypted LM hash**



http://www.oxid.it

Step 13: Perform Password Cracking Using Distributed Network Attack

- A Distributed Network Attack (DNA) technique is used for **recovering password-protected files** using the unused processing power of machines across the network to **decrypt passwords**
- DNA process:

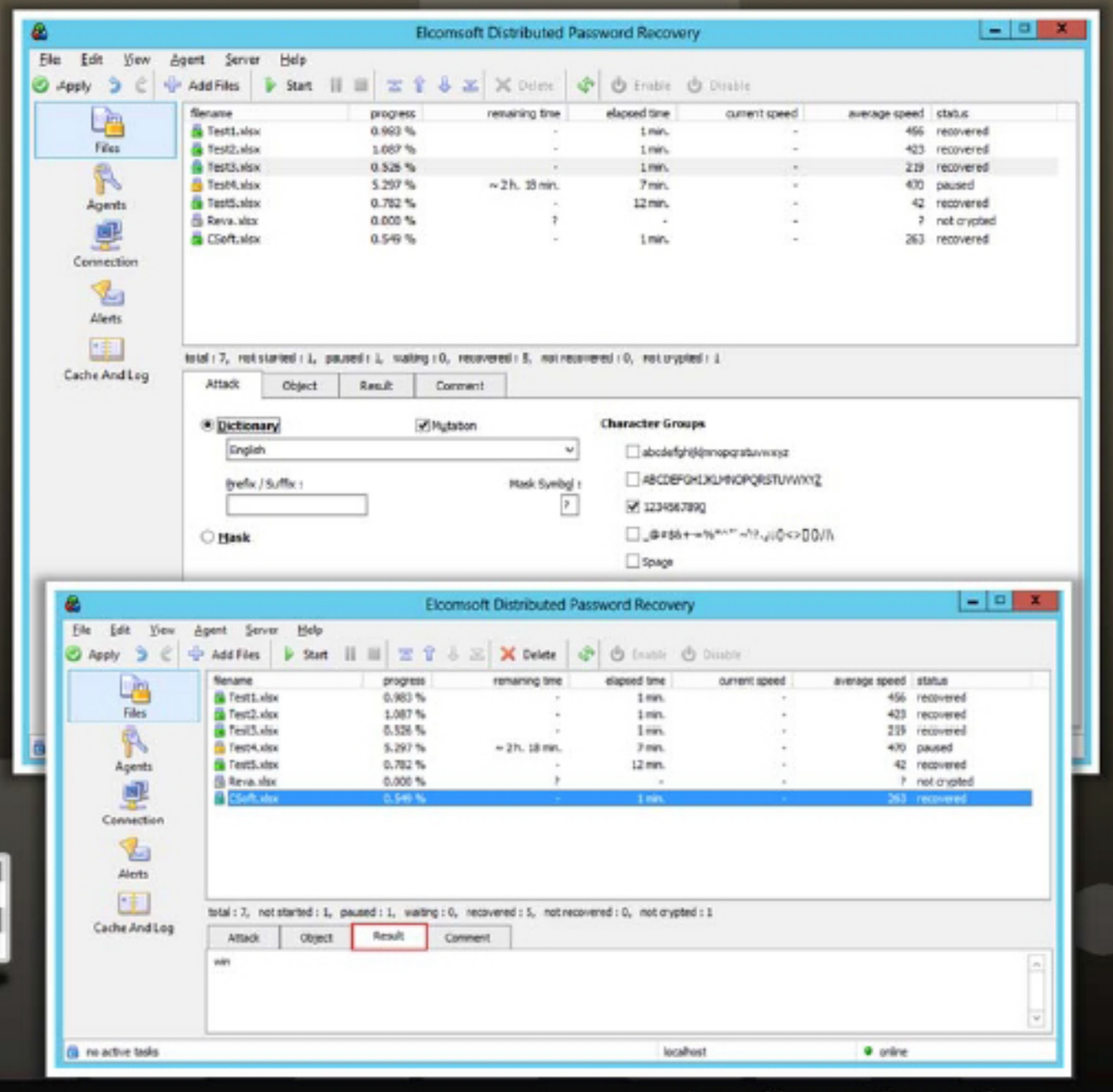
1. Install DNA Server in a **central location** where systems running on **DNA Client can access it over the network**
2. DNA Manager **manages the attack** and **allocates** small portions of the **key search to systems** that are distributed over the network
3. DNA Client runs in the background and **consumes only unused processor time**
4. The program combines the processing capabilities of all the clients connected to the network to perform **key search** and **decryption**

Elcomsoft Distributed Password Recovery

- Elcomsoft Distributed Password Recovery **breaks complex passwords**, **recovers strong encryption keys**, and **unlocks documents** in a production environment

Features

- Brute-force and dictionary attacks
- Distributed password recovery over LAN, Internet, or both
- Install and remove password recovery clients remotely



http://www.elcomsoft.com

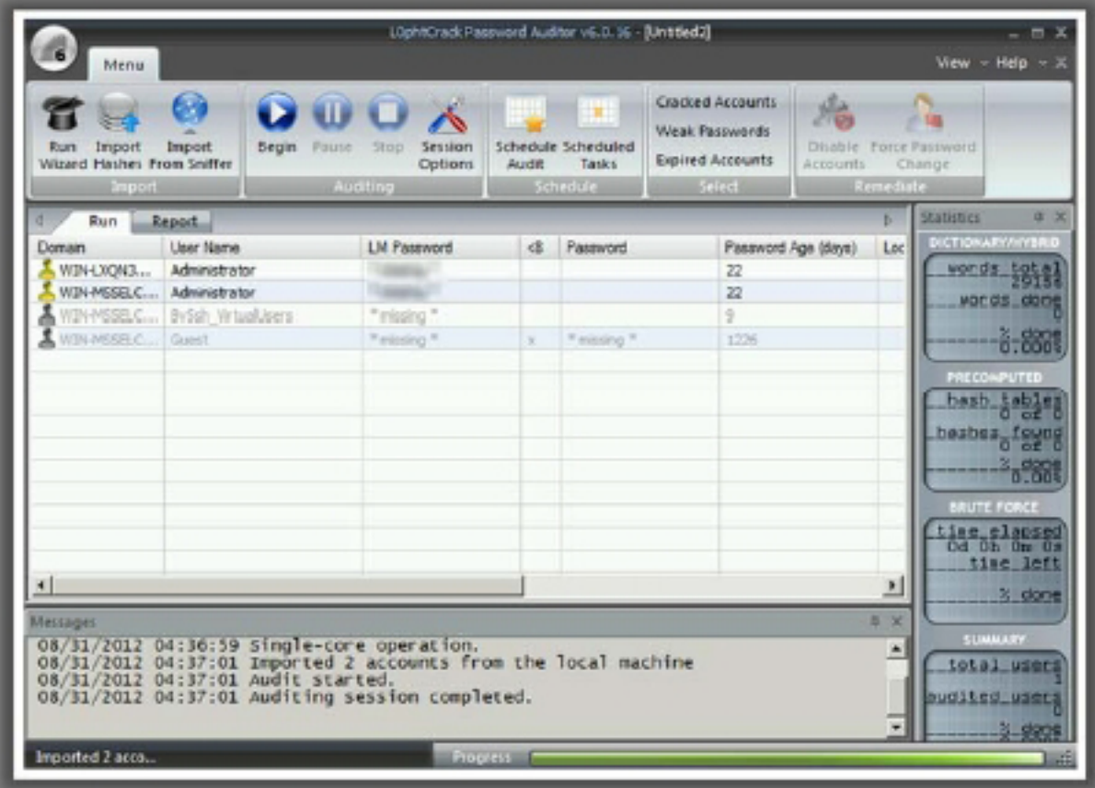
Step 14: Extract /etc/passwd and /etc/shadow Files in Linux Systems

- The password file for Linux is located in `/etc` and is a text file called passwd
- By default and design, this file is readable by anyone on the system
- On a Unix system using NIS/yp or password shadowing the password data may be located elsewhere; this "shadow" file is usually where the password hashes themselves are located
- Passwords can also be stored in `/etc/security/passwd` (accessible by root only)

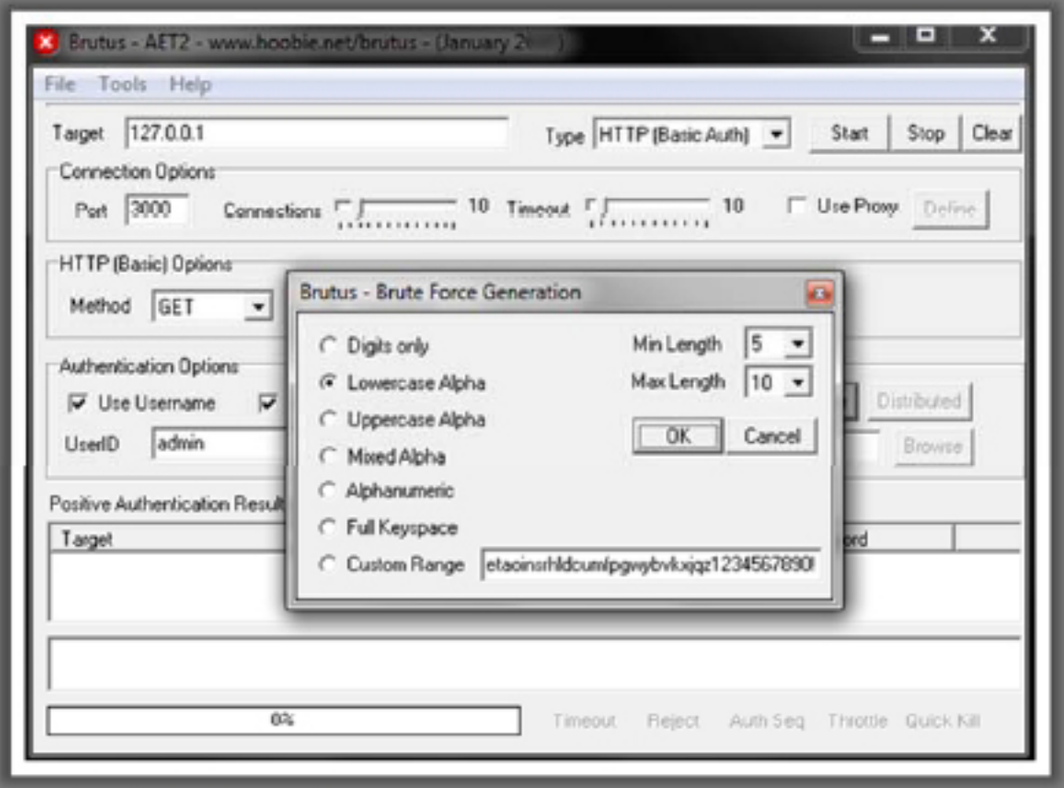
```
root:!:0:0:root:/root:/bin/tcsh
bin:!:1:1:bin:/bin:
daemon:!:2:2:daemon:/sbin:
adm:!:3:4:adm:/var/adm:
lp:!:4:7:lp:/var/spool/lpd:
sync:!:5:0:sync:/sbin:/bin/sync
shutdown:!:6:0:shutdown:/sbin:/sbin/shutdown
halt:!:7:0:halt:/sbin:/sbin/halt
mail:!:8:12:mail:/var/spool/mail:
news:!:9:13:INN (NNTP Server) Admin ID, 525-
2525:/usr/local/lib/inn:/bin/ksh
uucp:!:10:14:uucp login
user:/var/spool/uucppublic:/usr/sbin/uucp/uucico
operator:!:0:0:operator:/root:/bin/tcsh
games:!:12:100:games:/usr/games:
man:!:13:15:man:/usr/man:
postmaster:!:14:12:postmaster:/var/spool/mail:/bin/tcsh
httpd:!:15:30:httpd:/usr/sbin:/usr/sbin/httpd:
nobody:!:65535:100:nobody:/dev/null:
ftp:!:404:100::/home/ftp:/bin/nologin
nomad:!:501:100:Simple Nomad, 525-5252:/home/nomad:/bin/bash
webadmin:!:502:100:Web Admin Group ID:/home/webadmin:/bin/bash
thegnome:!:503:100:Simple Nomad's Old
Account:/home/thegnome:/bin/tcsh
dorkus:!:504:100:Alternate account for
Fred:/home/dorkus:/bin/tcsh
```

Step 15: Use Automated Passwords Crackers to Break Password-protected Files

- Use password cracking tools such as Brutus and L0phtCrack to break password-protected files
- L0phtCrack recovers lost Microsoft Windows passwords by using dictionary and hybrid attacks, rainbow tables, and brute force; it also checks password strength



http://www.l0phtcrack.com



http://www.hoobie.net

Password Cracking Tools

John the Ripper
http://www.openwall.com

Proactive System Password Recovery
http://www.elcomsoft.com

KerbCrack
http://ntsecurity.nu

Password Unlocker Bundle
http://www.passwordunlocker.com

krbpwguess
http://www.cqure.net

Windows Password Reset Professional
http://www.resetwindowspassword.com

Windows Password Cracker
http://www.windows-password-cracker.com

Windows Password Unlocker
http://www.passwordunlocker.com

Password Cracking Tools (Cont'd)

Ophcrack
http://ophcrack.sourceforge.net

RockXP
http://www.korben.info

RainbowCrack
http://project-rainbowcrack.com

PasswordsPro
http://www.insidepro.com

WinPassword
http://lastbit.com

LSASecretsView
http://www.nirsoft.net

Passware Kit Enterprise
http://www.lostpassword.com

LCP
http://www.lcpsoft.com

Step 16: Use Trojan/Spyware/Keyloggers to Capture Passwords

- Use malicious applications to get access to the user's computer and view the user's activities
- Use Trojan, spyware, and keylogger programs to get access to the stored passwords on the user's computer

Command Prompt

```
C:\>nc.exe -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode
        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
C:\>
```

Netcat Trojan

Spyware Tools

Activity Monitor
http://www.softactivity.com

LANVisor
http://www.employeemonitoring.net

Power Spy
http://ematrixsoft.com

Spector Pro
http://www.spectorsoft.com

eBLASTER 2011
http://www.spectorsoft.com

Hidden Recorder
http://www.oleansoft.com

Imonitor Employee Activity
http://www.employee-monitoring-software.cc

Mobile Spy
http://www.phonespysoftware.com

Keyloggers

Advanced Keylogger
http://www.mykeylogger.com

iMonitorPC Business Plus
http://www.imonitorpc.com

Spytech SpyAgent
http://www.spytech-web.com

XPCSpy Pro
http://www.x-pcsoft.com

Perfect Keylogger
http://www.blazingtools.com

Elite Keylogger
http://www.widestep.com

Powered Keylogger
http://www.mykeylogger.com

KeyProwler Pro
http://www.keyprowler.com

Recommendations for Password Cracking Penetration Testing

- Maintain policies for **defining**, **implementing**, and **maintaining passwords**

- Use password encryption for **protecting transmission** or **communication** of information regarding passwords

- Implement a standard policy for password **creation**, **storage**, **transmission**, **composition**, **issuance**, and **reset** procedures

- Implement **standard** policies for the password **recovery process**

- Deploy strong **authentication mechanisms** for the login process

- Configure a password mechanism to reduce the **risks** of password **cracking** and password **guessing attacks**

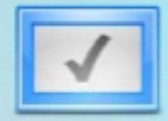
- Maintain a **flexible** password policy to accommodate a variety of **applications** and **operating systems**

- Implement strong **password hashing methods** and **cryptographic algorithms** for protecting passwords

Recommendations for Password Cracking Penetration Testing (Cont'd)

- Change passwords at regular intervals for **applications** and **operating systems** to reduce the **risks** of password cracking

- Deploy user **privilege options** or **restrict access** to files and important applications that contain passwords



- Implement different mechanisms for password expiration to reduce the **inadvertent** or **unauthorized use** of password information

- Define password policies such as **what should be protected** and **how it should be protected for different applications** that store passwords and hashes

- Implement password **expiration methods** for applications and operating systems depending upon the **security** requirements and **needs**

- Educate employees about securing passwords such as not **transmitting** passwords to peers, physically **securing** paper containing passwords in locked drawers, **discarding** or **shredding** paper containing passwords, etc.

- Review the password **policy** regularly for any major **technological** changes affecting password management

- Use **onscreen simulated keyboards** to avoid typing passwords and mitigate the risks of keystroke logging

Recommendations for Password Cracking Penetration Testing (Cont'd)

- Educate staff about the risks of **loading** and **running files** from unknown sources

- Maintain effective password strength requirements such as using a combination of special **characters**, **letters**, **numbers**, etc.

- Educate employees about social engineering **threats**, **phishing emails**, **malware threats**, etc.

- Enable a timeout feature for user accounts that automatically **locks out** after an **idle period** such as 5-10 minutes

- Prevent a **user account** from logging in after a certain number of failed login authentication attempts

- Remove or **disable unused** or **unnecessary** user accounts

- Educate users about maintaining **strong passwords** and the effects of weak passwords

- Deploy different user authentication techniques such as one time **password tokens**, **biometrics**, **smart cards**, etc.

Module Summary

- A password is a secret series of characters that enables a user to access a file, computer, or a program
- Passwords protect a computer's resources and files from unauthorized access by malicious users (attackers)
- Password cracking is the process of extracting or recovering passwords from data from computer systems using password crackers or network analyzers
- Windows stores user passwords in the Security Accounts Manager database (SAM), or in the Active Directory database in domains
- MITM attack is performed to acquire access to the communication channels between user and server to extract the password
- A hash injection attack allows an attacker to inject a compromised hash into a local session and use the hash to validate to network resources