

Computer Infections

Prevention and Maintenance

ICTSAS308

Contents

- Define the **ultimate goals of security**
- We'll *investigate* a variety of **diagnostic tools**:
 - Manage System Backups
 - Run Anti-Virus Checks
 - Maintain Firewalls
 - Administer User Accounts, Access Control
- Examine the **Organisational Guidelines** for maintaining good security



The goals of IT security

- *To protect* three unique **attributes of information**
 - I. Confidentiality
 - Information should be seen *only by authorized persons*
 - II. Integrity
 - Information must *not be corrupted, degraded, or modified*
 - III. Availability
 - Information must be *available to authorized persons*



How IT attacks affect systems

- **Attacks** and **computer infections** affect systems in such ways as to *compromise one or more of the attributes of information*
- **Information security** aims to protect these personal/organizational attributes
- **Organizations** use proper **planning, prevention & maintenance** to protect these attributes



IT security prevention & maintenance

- Proper **prevention & maintenance**:
 - Greatly **reduces the risks of an attack**
 - Greatly **increase the timely and effective detection** and response if an attack occurs
- An organisation's **security strategy** is only effective if *employees are properly trained on it*
- An effective **security awareness program** should include *education on specific threat types*, such as malware, trojans, viruses & phishing

IT security and personnel

- Training employees is a **critical element of security**
- They need to **understand their role** in keeping information safe
- They also need a **basic grounding in other risks** and how to make good judgments online
- Believe it or not, **password cracking is remarkably easy**, particularly for advanced hackers

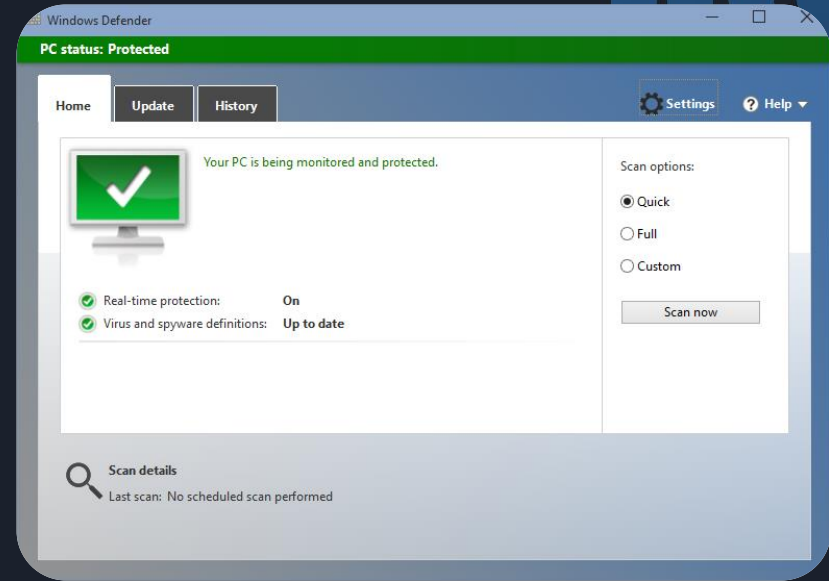
Diagnostics and Maintenance

- Tools like **Anti-virus, Firewalls and Backup** software aid in *maintaining a healthy and safe system*
- Tools like **Anti-virus, Firewalls and Backup** software aid in *maintaining a healthy and safe system*
- They use **diagnostics** as routine maintenance to *analyse the current health of the system*



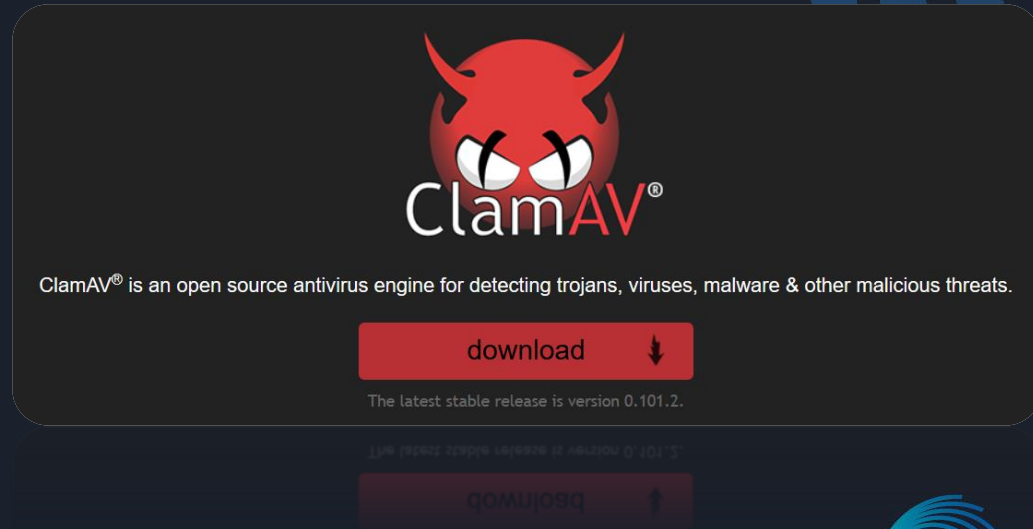
Anti-virus software

- Anti-virus software is a **computer program** used to *prevent, detect, and remove malware*
- Windows includes anti-virus software with it's OS
 - Called **Windows Defender**
 - Auto-updates with OS
 - Can **automatically scan your system** on regular schedule



Anti-virus software

- Other Operating Systems use their own anti-virus solutions
- Linux is an open-source OS with many distros including Ubuntu, Linux Mint & others.
- Linux has a variety of AV solutions
 - ClamAV is open-source software & one of the best known anti-virus software tools for Linux
 - Can scan your system and stays up-to-date with the latest virus definitions

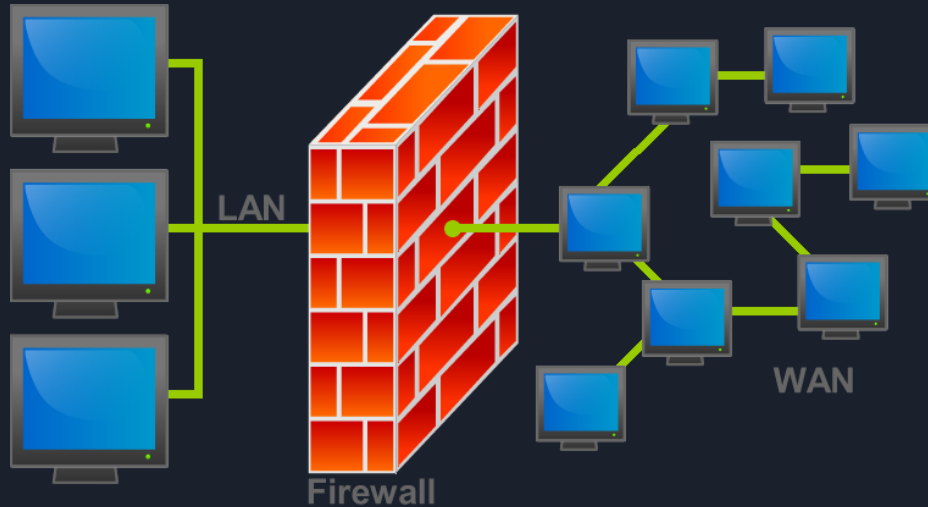


Firewalls

- A **firewall** is a **network security system** that *monitors and controls* incoming and outgoing network traffic based on *predetermined security rules*
- Can be implemented using **hardware** or **software**, or both
- Firewalls are generally categorized as **network-based** or **host-based**

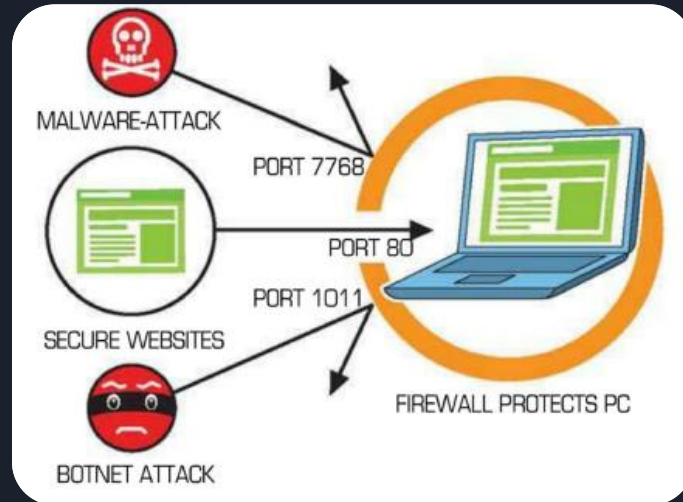
Firewalls

- **Network-based firewalls** are positioned on the *gateway computers* of LANs, WANs and intranets



Firewalls

- **Host-based firewalls** are positioned on the network node itself and control network traffic in and out of those machines



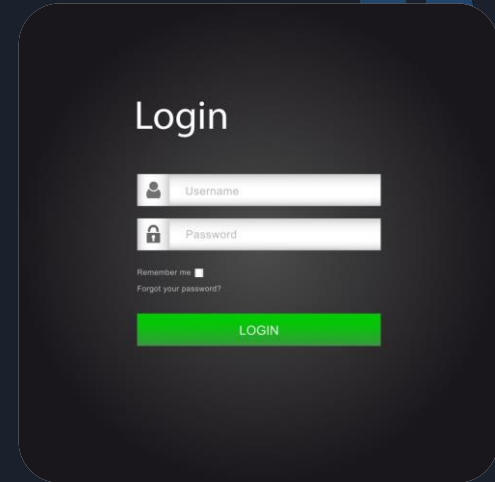
Backups

- A **backup**, or **data backup**, or the process of backing up, refers to the **copying data into an archive file**
- The archived data is stored on a **secondary device**, usually disconnected from the original
- It aims to **provide redundancy** that mitigates against a **data loss event**



User accounts and User access

- **Computer access** is managed using **user accounts**
- Each **user account** has access to:
 - *Private file storage area*
 - User interface *customizations*
 - Shared *public file storage area*
- User accounts are protected by credentials:
 - Passwords (text and/or picture)
 - PINs
 - Biometric identification



Login

Username

Password

Remember me ☐

[Forgot your password?](#)

LOGIN

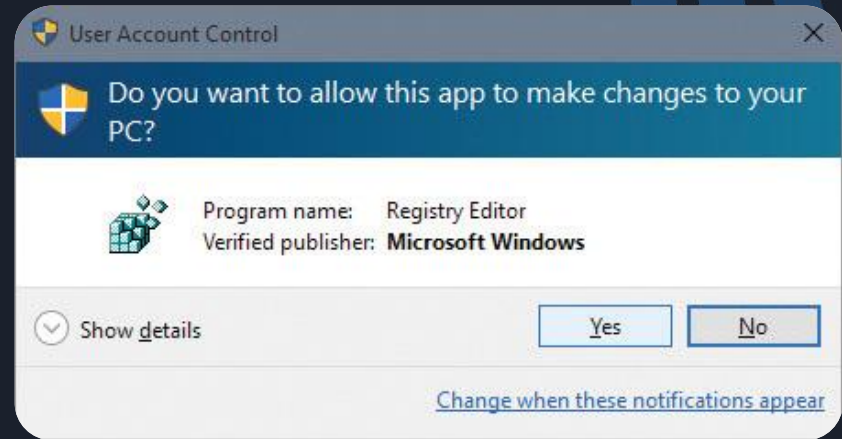
User accounts and User access

- An OS generally requires at least one Admin Account:
 - The Administrator Account
- The administrator *manages other user accounts and global settings*
- Administrators are typically **IT personnel at organisations** and family members on home computers



User Account Control

- An OS controls what a User Account can access
- On Windows, this is known as **User Account Control (UAC)**
- **UAC protects computers** from changes to system settings
 - Requiring that an administrator *expressly permit certain types of changes*



User accounts

- A **user account** is associated with a **user profile**
 - Describes the user environment *looks & operates* for each user
- By default, a **user profile is inaccessible** to other users
 - Keeps *personal information private*
 - Administrators generally *have access to all data* if necessary
- **Use Non-Admin Accounts** for normal day-to-day operations
 - In case you accidentally *copy/install a virus*
 - A *Basic User Account* **doesn't have access to the entire computer!**

IT Security Awareness Programs

- A good Information Security Awareness Program:
 - *Highlights importance* of information security
 - *Introduces and explains* policies and procedures
 - Is *simple yet effective* so that employees are able to understand the policies and are aware of the procedures

About IT Security Awareness Programs

- **Information Classification, Handling & Disposal**
 - Use techniques like encryption, labelling & electronic shredding
- **System Access Management**
 - Every user has a User Account
 - Users are educated on creating safe passwords
- **Virus Protection**
 - All systems have anti-virus software installed, updated & regularly scheduled

About IT Security Awareness Programs

- **System Backups**
 - Use regular automated backup techniques
 - Use offsite backup servers
 - Encourage users to make personal backups
- **Software Licensing**
 - All software to be correctly licensed and installed
 - Pirated software is a *known vector* for malware
- **Internet and Email Usage**
 - Staff must be educated and monitored on the correct and safe usage

About IT Security Awareness Programs

- **Physical Security**

- Hardware such as Laptops and USB should adhere to the same security standards
- Locked securely when not in use
- Use protected user accounts

- **Training**

- All *organisational staff* should be trained on safe IT practice
- All *family members*, including your parents & siblings, should be trained on safe IT practice

Summary

- *Defined* the **ultimate goals of security**
- *We investigated* a variety of **diagnostic tools** such as:
 - Manage System Backups
 - Run Anti-Virus Checks
 - Maintain Firewalls
 - Administer User Accounts, Access Control
- *Examined* the **Organisational Guidelines** for maintaining good security

References

- Symantec. 2015. Training Your Employees on Information Security Awareness. [ONLINE] Available at: <https://www.symantec.com/connect/blogs/training-your-employees-information-security-awareness>. [Accessed 4 July 2019].
- MicrosoftPressStore. 2015. Manage User Accounts and Settings in Windows 10. [ONLINE] Available at: <https://www.microsoftpressstore.com/articles/article.aspx?p=2453566>. [Accessed 11 July 2019].