Topic A2: System Vulnerabilities

Unit 2: Cyber Security and Incident Management

Rons Tech Hub

System Vulnerabilities Overview

Rons Tech Hub

- A vulnerability is a weakness in a computer system.
- Hackers use these gaps to attack an organisation.
- IT professionals must identify and fix these risks.

Network: Firewall Ports

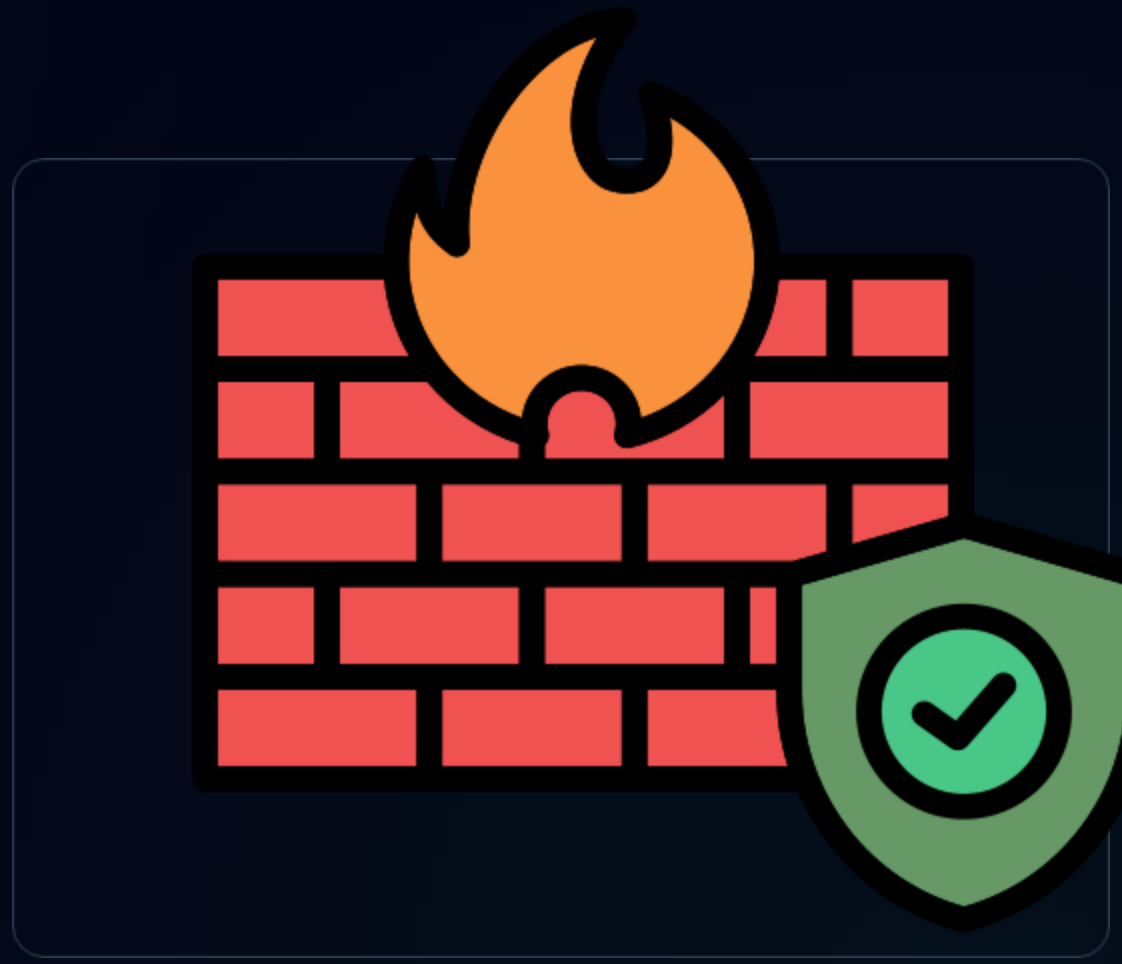
Rons Tech Hub

Understanding Ports

Firewall ports act like gateways for data to travel through.

If a port is left open, an attacker can get into the system.

Closing unused ports is a key security step.



Common Firewall Port Types

Rons Tech Hub

Well-known: Standard ports like Port 80 for web browsing.

Registered: Used by specific services and software.

Dynamic: Temporary ports used for private or custom needs.

Network Vulnerabilities

- **Open Ports:** Allow unauthorised traffic to enter the network.
- **Spoofing:** When an attacker pretends to be a trusted user.
- **DoS:** Flooding the system so it crashes and stops working.

External Storage Devices

- USB drives and SD cards can spread malware between computers.
- External hard drives and SSDs can be stolen easily.
- Backup tapes and disks are risks if they are not stored safely.

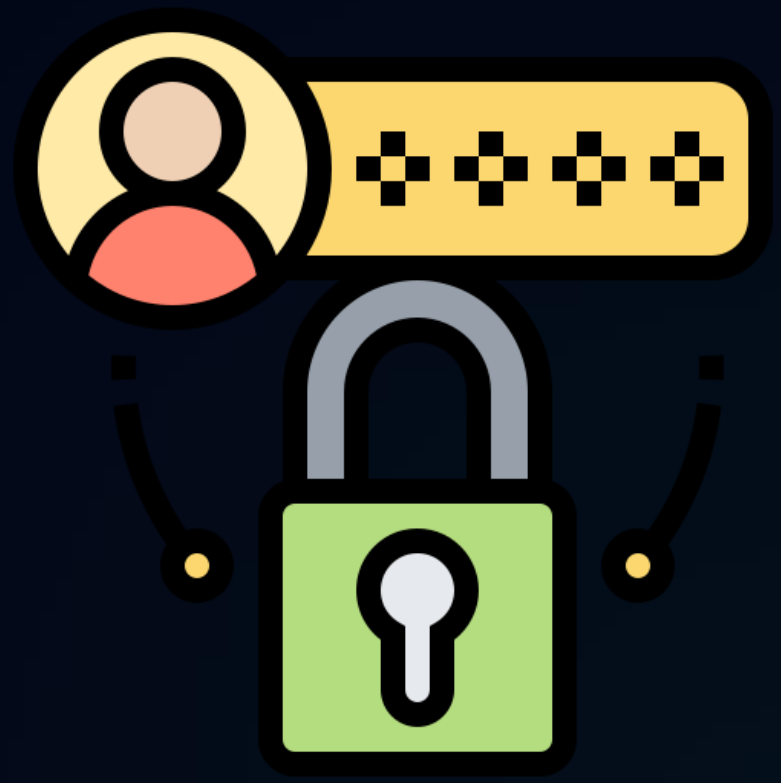
Organisational Permissions

Rons Tech Hub

- Permissions control who can read, write, or change files.
- Access should be restricted to users, admins, and systems.
- Limiting access prevents users from seeing data they don't need.

Password Policy Rules

- Policies should set a minimum length and use special characters.
- Users should be blocked from using names or birthdays.
- Changing passwords too often or reusing them increases risk.



Password Management Tools

- Password managers store and create strong passwords securely.
- Passwords can be synced between your phone, PC, and the cloud.
- Locking accounts after failed logins prevents guessing attacks.

Untrustworthy Software

- Downloading software from unknown sites is very dangerous.
- This software may contain hidden malware or trackers.
- Organisations should only use trusted, verified software sources.

Software Download Requirements

- Always check for the HTTPS lock symbol on websites.
- Scan every file for malware before you install it.
- Use hash checks to ensure the file hasn't been changed.

Deceptive Installers

- Deceptive installers may look real but install viruses.
- Illegal software copies often lack vital security updates.
- Hackers may leave 'backdoors' in the code to get back in later.

Zero-day Exploits

- A zero-day exploit is a new threat with no known fix.
- There is a window of time where systems are vulnerable.
- Fixes are only applied once a 'patch' is created by the owner.

Software: SQL Injection

- Attackers use malicious code to trick data storage software.
- They can steal or change data in the organisation's database.
- Flaws in web forms make these attacks much easier.

Operating System Risks

- Unsupported versions of an OS stop getting security updates.
- Missing patches leave the system open to old and new threats.
- Incorrect settings can expose the system to cyber criminals.

Mobile Device Updates

- Mobile security relies on manufacturers (OEMs) to send updates.
- If updates are not provided, the device remains vulnerable.
- Users must install these updates as soon as they arrive.

Physical Security Risks

- Equipment like laptops or servers can be physically stolen.
- Restricted areas with poor security can be entered by anyone.
- Losing a mobile device risks exposing all the data on it.

Rons Tech Hub

System Process Flaws

- Sharing security details with others is a major weakness.
- Accidental leaks of data can happen if processes are flawed.
- Cyber security relies on people following safe rules.

Cloud Computing Security

Rons Tech Hub

- Incorrect cloud settings can leave data open to the public.
- You must rely on the third-party provider to keep data safe.
- Moving data over the internet risks it being intercepted.

IoT Security Risks

- Smart devices often have weak encryption and default passwords.
- Many IoT devices are never updated with security patches.
- Smart hubs can 'listen' and send voice data without permission.

Finding Vulnerability Info

- Visit manufacturer websites for the latest software news.
- Join IT forums to learn from other cyber security specialists.
- Use third-party websites that track specific hardware flaws.

Rons Tech Hub

Understanding Attack Vectors

Rons Tech Hub

Ways to Attack

An attack vector is the path a hacker takes to enter a system.

This includes wireless signals, cables, and mobile links.

Hackers look for the easiest path into the network.

Wireless Attack Vectors

Rons Tech Hub

- **Wi-Fi:** Standards like 802.11 can be targeted.
- **Bluetooth & NFC:** Short-range signals can be intercepted.
- **Satellite & Cellular:** Links used for data and 5G.

Internet Connection Vectors

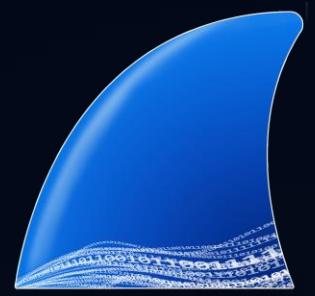
- Copper cables and optical fibres can be physically tapped.
- Modems and routers are targets for network attacks.
- Wireless routers are often a weak spot in a system.

Internal Access Devices

- Routers and switches manage data inside the network.
- Wireless access points allow devices to connect internally.
- Each device must be secured to prevent internal attacks.

Vulnerability Assessment Tools

Tool	Purpose
Port Scanner	Checks for open ports.
Network Mapper	Finds all system devices.
Registry Checker	Checks system settings.



Scanners and User Checks

- Website scanners find flaws in online pages and forms.
- Vulnerability management software tracks risks over time.
- Assessing user vulnerabilities checks for human errors.

Independent System Reviews

- Experts review network designs before they are built.
- This helps establish 'due diligence' for the organisation.
- Third-party certification proves the system is safe.

Penetration Testing (Pentesting)

- Pentesting involves simulating a real cyber attack.
- Tests focus on common threats like the OWASP top 10.
- The goal is to find weak spots before a criminal does.

Testing and Reports

- Tests use many techniques to find every possible flaw.
- Systems are checked against lists of known vulnerabilities.
- Final reports explain the risks and how to fix them.

Passive Risk Measures

Risk Transfer: Handing the risk to another party, like insurance.

Risk Avoidance: Stopping an activity entirely to remove the risk.

Risk Acceptance: Identifying the risk but deciding to live with it.

Summary & Questions

Understanding vulnerabilities is the first step in cyber defense.

Using the right tools keeps our systems and data protected.

www.ronstechhub.com

Rons Tech Hub

Image Sources

Flaticon and Wikipedia Commons.

Rons Tech Hub