Chapter 1
Know the types and sources of network attacks

Chapters

1 Know the types and sources of network attacks
2 Know about security related hardware and software
3 Understand organisational aspects of network security
4 Be able to apply system security.

Chapter 1

Network Attacks

Chapter 2

Security Systems

Chapter 3

Organisational Security

Chapter 4

Apply System Security

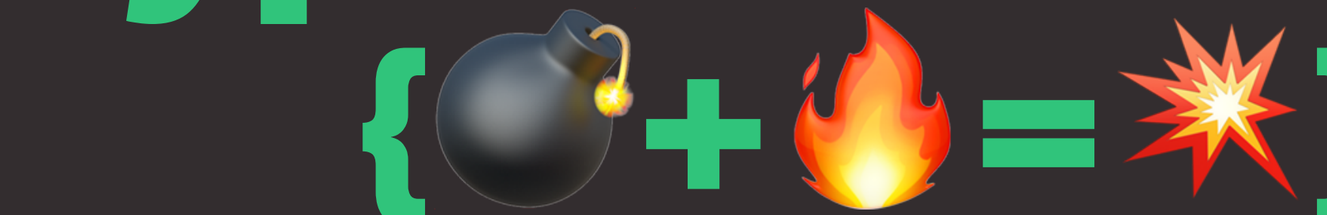
C1 - Know the types and sources of network attacks

1.1 Types of Attacks
1.2 Sources of Attacks

What is an attack ?

& Why do we do it ?

Types of Attacks



Attacks:

Denial of service
Back door
Spoofing
Mathematical
Brute force
Software exploitation Attack

Denial of service Attack

Back door Attack

Spoofing Attack

Brute force Attack

Software exploitation Attack

2 Types of Software

Good Software
Bad Software

Good Software
Bad Software / Malicious Software

MALicious SoftWARE

MALWARE

MALWARE

Any kind of intrusive software that is installed without consent can be classified malware.
It can be it code, scripts or active content.

Malware Attacks

Viruses
Worms
Trojans
Spyware
Adware
Rootkits

Virus

spreads via deliberate user action such as downloading a file or running a program

Worm

spreads automatically by replicating itself across computers or networks

Trojan

spreads by appearing safe or desirable but disguising its true intent (e.g., backdoors)

Bots

runs in the background while hijacking computing resources (e.g., bot networks)

Spyware

monitors user activities for marketing purposes or keylogs user credentials

Adware

serves unwanted ads or redirects user’s browser traffic

OWASP

OWASP

Open Web Application Security Project

OWASP Top 10

1. Injection
2. Weak Authentication and session management
3. XSS (Cross site scripting)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross Site Request Forgery
9 Using Components with Known Vulnerabilities
10 Unvalidated Redirects and Forwards

Sources of attacks

Internal
    Disaffected staff
External
    Via internet connections
    Through unsecured wireless access point
    Viruses introduced by email

Assignments

Assignment 1

1 Are we safe ? (P1, P2, M1, D1)

Phase 1: an overview of current network security threats and how to protect against them.
P1: describe how networks can be attacked
D1: discuss recent network threats
P2: describe how networked systems can be protected [IE2]
M1: explain the operation of different intruder detection systems

Assignment 2

2 What's best ? (P3, M2, D2)

Phase 2: how to minimise risks.
P3: explain what an organisation can do to minimise security breaches in networked systems [SM4]
M2: suggest how users can be authenticated to gain access to a networked system
D2: compare the security benefits of different cryptography techniques.

Assignment 3

3 Start installing. (P4, P5, M3)

Phase 3: configure and test network security hardware/ software.
P4: plan procedures to secure a network
P5: configure a networked device or specialist software to improve the security of a network.
M3: report on the similarities and differences between securing wireless and wired networked systems.