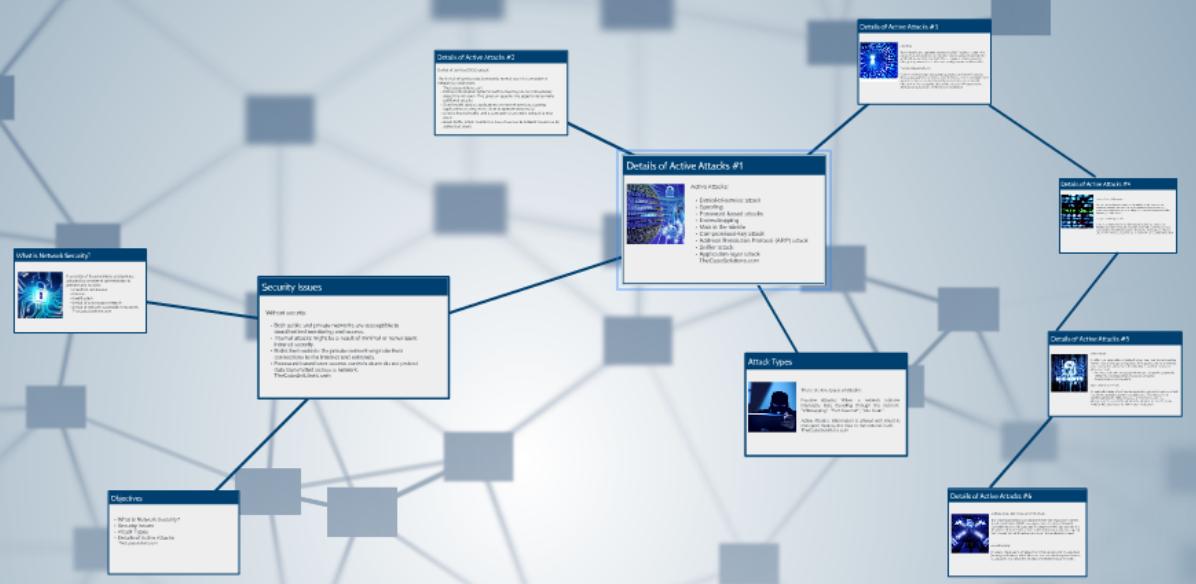
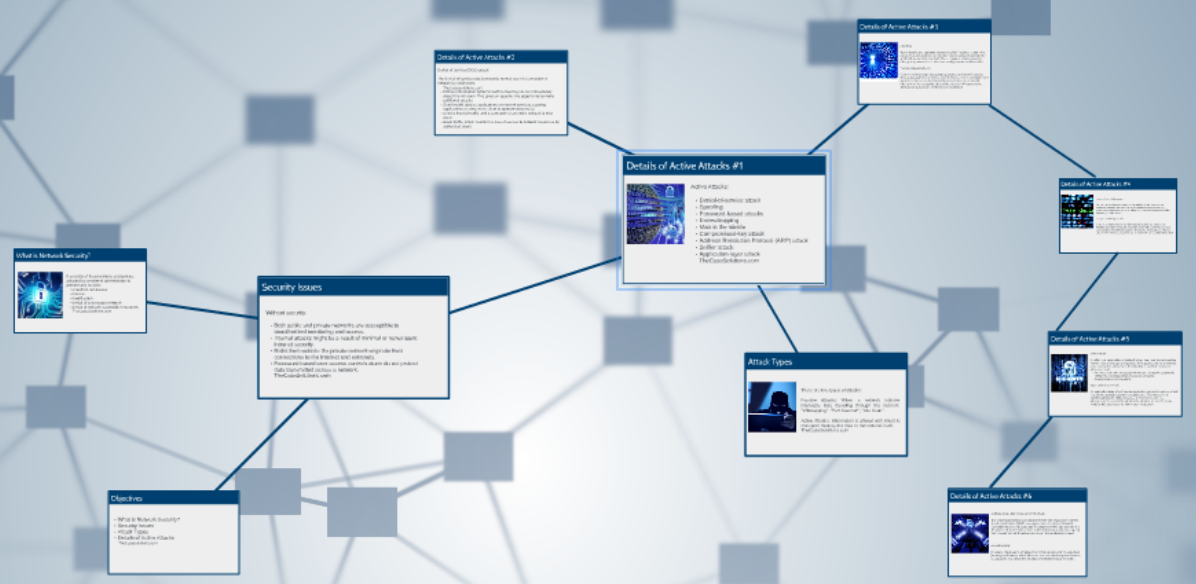


TheCaseSolutions.com

What Should I Do if I End-up Working in a Corrupted Network?

Yakup Güneyli A146676IVEM
TheCaseSolutions.com



TheCaseSolutions.com

What Should I Do if I End-up Working in a Corrupted Network?

Yakup Güneyli A146676IVEM
TheCaseSolutions.com

Yakup Güneyli A146676IVEM

TheCaseSolutions.com

Objectives

- What is Network Security?
- Security Issues
- Attack Types
- Details of Active Attacks

What is Network Security?

It consists of the provisions and policies adopted by a network administrator to prevent and monitor;

- unauthorized access
- misuse
- modification
- denial of a computer network
- denial of network-accessible resources

Security Issues

Without security:

- Both public and private networks are susceptible to unauthorized monitoring and access.
- Internal attacks might be a result of minimal or nonexistent intranet security.
- Risks from outside the private network originate from connections to the Internet and extranets.
- Password-based user access controls alone do not protect data transmitted across a network.

Attack Types

There are two types of attacks:

Passive Attacks: When a network intruder intercepts data traveling through the network. "Wiretapping", "Port Scanner", "Idle Scan" .

Active Attacks: Information is altered with intent to corrupt or destroy the data or the network itself.
TheCaseSolutions.com

Details of Active Attacks #1

Active Attacks:

- Denial-of-service attack
- Spoofing
- Password-based attacks
- Eavesdropping
- Man in the middle
- Compromised-key attack
- Address Resolution Protocol (ARP) attack
- Sniffer attack
- Application-layer attack

Details of Active Attacks #2

Denial-of-service (DOS) attack:

The denial-of-service attack prevents normal use of a computer or network by valid users.

TheCaseSolutions.com

- Distract information systems staff so that they do not immediately detect the intrusion. This gives an attacker the opportunity to make additional attacks.
- Send invalid data to applications or network services, causing applications or services to close or operate abnormally.
- Send a flood of traffic until a computer or an entire network is shut down.
- Block traffic, which results in a loss of access to network resources by authorized users.