Safety of information systems

Lecturer: Roman Danel

Network security

To understand network security, basic knowledge about network architecture and protocols is necessary.

Protocols overview

- OSI model (ISO 7498) – 7 layers
- TCP/IP
- UDP – User Datagram Protocol
- ICMP – Internet Control Message Protocol
- ARP – Address Resolution Protocol (IP to MAC address)
- DNS – Domain Name System

Standard ISO 7498-2 – security architecture.

Attacks

- ARP Flooding
- False MAC
- MAC Flood - a switch is fed many ethernet frames, each containing different source MAC addresses, by the attacker. The intention is to consume the limited memory set aside in the switch to store the MAC address table.
- False ARP
- False IP address
- Fraggle attack - Sending UDP packets to port 7 (echo) or port 19 -> enhanced traffic will occur
- Smurf attack - uses spoofed ICMP traffic rather than UDP traffic to achieve the same goal
- Land attack - source and destination IP address set to victim address - packet generated artificially -> high CPU usage
- Packet size inconsistencies
- IP packet fragmentation
    - duplicate packets
    - overlapping packets
    - ping of death – can cripple a network based on a flaw in the TCP/IP system. The maximum size for a packet is 65,535 bytes. If one were to send a packet larger than that, the receiving computer would ultimately crash from confusion.
    - odd packets
- SYN Flood - attack takes advantage of the TCP three-way handshake
- Teardrop attack - packet fragments are sent in a jumbled and confused order. When the receiving device attempts to reassemble them, it obviously won't know how to handle the request. Older versions of operating systems will simply just crash when this occurs
- Ping Flood

- Password attack
    - Brute force
    - Dictionary
- Packet sniffing
- Man-in-the-middle – false of identity

Attacks classification:

- Passive wiretapping
- Inserting false information
- Inserting older messages
- Inserting damaged messages (Trying to disable or damage computer system)
- Active attacker:
    - Data integrity attack
    - Changing identities in favor of attacker
    - Damage to transmitted data

Securing computer networks

- Prevention
- Detection of attacks
- Reaction

Securing:

- CRC checksums
- Encryption of data
- Ports protection
- Setting access rights
- Authentication of network nodes
- Firewall
    - security interface between public network / private network
    - definition of access rules
    - limit access to parts of the internal network
    - protocol and service restrictions
    - access control and statistics
- VPN – **virtual private network -** secure authenticated and encrypted connections using the public network
- Protocol IPSec
    - Data protection in IPv4, mandatory in IPv6
    - Encrypted tunnel, specification RFC 2784
    - Authentication and encryption of each datagram
    - Works on the OSI network layer

    - Unlike SSH, it does not require application support
    - Protocols:
        - AHP - Authentication Header
        - ESP - Encapsulating Security Payload - packet encryption
- SSL = Secure Socket Layer
- Electromagnetic protection - Computer monitors, communication networks, power distribution -> can be eavesdropped

WAN security

Elements that can be attacked:

- Router (own IP address)
- Firewall
- Communication channel - wiretapping
- Communication Data Interface
- Endpoint device

Intrusion Detection System – IDS

- Host-based
- Network-based - analyzes network packets
- Hybrid

Detection systems: TCPdump, RealSecure, Cisco Secure IDS, Snort, NFR Security…

Intrusion Prevetion System

IPS monitors the network and takes action at an event.

IDIP – Intrusion Detection and Isolation Protocol (from DARPA).

Automatic response to a network attack:

- dropping the connection
- throttling
- shunning
- session sniping and RESET

Firewall

Firewall is a "security gateway". It is a device or software that separates traffic between two networks (e.g. the company's internal and public internet), and transmits data in one or another direction according to pre-defined rules. In particular, it prevents from unauthorized intrusions into networks and sending data from the network without the knowledge and consent of user.

Firewall can be installed either on the terminal device (e.g. PC, mobile device) or under any of the active network elements and network infrastructure.

Firewall:

- Hardware
- Software

Black list/While list.

What the firewall enables/disables?

- Port
- Protocol
- Computer
- Network

Web Security

Attacks:

- **SQL injection** - insert SQL code through URL
- **Session Hijacking** - gets the SESSION ID of the Administrator and logs in to his account
- **DOS – Denial of Service**
- **Cross-Site Scripting** - attack a poorly secure web application by inserting a script in one of the client languages - damaging or disabling the page, obtaining information
- **Cross Site Request Forgery** - an unexpected (unintended) request to perform an action in an application, which, however, originates from an illegitimate resource; when another user is logged in

Potentially dangerous web elements:

- CGI scripts
- ActiveX and Java applet in browsers
- SNMP protocol
- Symbolic links
- Missing index.html -> list of directories
- Error messages with a name of script and directories
- Error messages with SQL commands
- Use rights

Dictionary attack is a technique of the attack to the password using familiar words from a list of known or probable words.

DDoS stands for Dedistributed Denial of Service. It is an attack on a Web server where the attacker floods a server with a large number of requests from a number of different locations. That result the server is flooded and inoperable during the attack.

OWASP

OWASP – Open Web Application Security Project is a worldwide not-for-profit charitable organization focused on improving the security of web software.

https://www.owasp.org

Secure Communication

HTTP Secure (**HTTPS**) is an adaptation of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network, and is widely used on the Internet.

SSL – Secure Socket Layer - is a protocol, a layer embedded between a transport layer (e.g., TCP / IP) and an application (e.g., HTTP) that provides communication security by encrypting and authenticating communicating pages.

An SSL follower is **Transport Layer Security (TLS)**.

Demilitarized Zone

Demilitarized Zone (DMZ) is a special part of computer network that is used to increase the security of the communication with the external environment (the Internet). It also plays the role of the firewall. Servers in the DMZ are not allowed access to the local network. In the case of their attack, the attacker will not be able to attack servers on the local network. Demilitarized Zone is used to connect the protected local network (private or corporate) and unprotected network of the Internet.