Network Security Concepts and Design

CIA Secrity concepts "Confidentiality - Integrity - Availability"

Confidentiality mean Only authorized users should be able to access specific systems or data "Confidentiality example is the Password"

Integrity mean Only authorized users should have the ability to use or modify systems or data

Availability mean Authorized users should always have access to their systems or data "Availability example is the Packup"

You need to know "Assets - Vulnerability - Threats - Impact"

Risk = Treats *Vulnerability* Impact

we split the Network into 3 parts

- External Public Network "Internet - Router" (Internet Part)
- Demilitarized Zone (DMZ) " Firewall - Web, Mail Servers - Firewall"
- Internal Private Network "Switch - Computers - Servers"

Defense Layers "Defense in Depth (DID)"

- Use more Layers to secure the Network

Network segmentation and Monitoring

Virtual LANS (VLANs): take the big Network on same switch "same broadcast domain" and split it into Virtual LANs

We put the poeple who has same Traffic and in contact all the time on same VLAN

Each Virtual LAN Traffic is seperate from the other VLANs on same switch

To contact 2 seperate VLANs on the same switch: in this case the Traffic should go through a Router Cause each VLAN considered as Subnet different from the other "Inter-VLAN routing"

Port Scanning is one of the Negative attacks methods (scouting)

Port scanning can define Operating System fingerprinting "Operating System - Version - Apps - Serveses"

Port Scanning can scan 65535 ports and see if there is an open port or not

Port Scanning (Softwares) = NMAP - ZENMAP

Dangerous Ports range from " 0 - 1024 "

Passive Attack = Sniffing "Listening to a data without editting it"

Active Attack = when the Hacker edit the data

Sniffing Tools (Softwares) = TCPDUMP - WIRESHRK

TCPDUMP "Time Stampe - Source DM > Destination DM - Protocol Type - Packet type"

WIRESHARK "Packet Num - Time Stampe - Source IP - Destination IP - Packet Protocol - Packet Info"

Firewalls and Honeypots

Firewalls investigate the Traffic depending on some Rules or Criteria

Firewalls could be Software on the Device or Host on the Network filtering the Traffic for the Device only "Host based firewalls"

Firewalls could be a seperatly Hardware box filtering the whole Network "Network based firewall"

Defending the Attack before reaching the firewall called "Early Negation" and mean High Security level

Defending the Attack on the firewall called "Negation using firewall" and mean Very Good security level

Entering the Network through the firewall without detection "Entered private net" thes mean Alert

Firewall Filtering Techniques:

- Packet Filtering
    - Use Access control list (ACL)
    - ACL Define "IP Addresses Range - Port Nums - Protocols"
    - ACL compare the Packets with the Criteria in ACL then take action
    - Depending on the Configuration put by the Authorized

- Stateful Inspection
    - Track connection through the Firewalls and save data in "State Table"
    - State Tables contain "Source IP - Destination IP - Port Num - TCP/UDP"
    - save the Request Packet and compare it to the Return Packet if it's similer then it can pass
    - The Danger in Direct Connection between any device in the network and systems out the network "Show Internal IP"

- Proxy Firewall
    - Act like Mediator between Devices in out Network and the Internet
    - Any Request in the Internal Network got to Proxy Server then the Proxy send it to the Network
    - The Firewall could Hide the IP Address by "Network Address Translation"

Configuration of Firewalls by Access control list (ACL):

- First Choose if you want to
    - Default is Permit All Traffic and Deny the Traffic has the Criteria
    - Default is Deny All Traffic and Accept the Traffic has the Criteria
- Define the Criteria "Port - Src. IP - Src. Port - Dst. IP - Dst. Port"

EX: Computer at Internal Network to a Web Server at Demitirarized zone (DMZ) and the Firewall Permit the Traffic between them:

- Permit
- TCP
- Src. IP "163.121.25.10"
- Src. Port "2050"
- Dst. IP "163.121.11.12"
- Dst. Port "80"

Bypassing Firewall (Firewall Hacking):

- Applications (Peer-to-Peer Software) like BitTorrent
    - BitTorrent "Share files between devises by using specific Network relating to the App"
    - BitTorrent can Change its Port Num to Pass through the Firewall

- Restrictive Configuration "violates Availability"
    - This Make the Users use Modems to skip the Firewall and connect to the IPS Directly

---

Intrusion Detection and Prevention Systems

Intrusion Detection Systems (IDS):

- watching the Network and analyse the Traffic, if there is an Attack it produce Alert
- Attacks like "Port Scanning - Sniffing"
- IDS is like a Camera and can't prevent the Attacker

Intrusion Prevention Systems (IPS):

- watching the Network and analyse the Traffic, if there is an Attack it produce Alert and Block it

Alerts :

- Alerts can be sent by:
  - Emails
  - Recorded at Log file
  - SMS

- True Positive Alert
  - Actual Attack
  - Alert Produced
- False Positive Alert
  - NO Attack
  - Alert Produced
- True Negative Alert
  - No Attack
  - No Alert
- False Negative Alert "Dangerous"
  - Actual Attack
  - No Alert

IDS&IPS Monitoring Methods by scanning the Traffic by:

- Signature Based Detection depending on
  - Database consist of signature of known attacks "Black list"
    - Port Num
    - IP Address
    - Protocol
    - Strings
    - Traffic Flow "Denial of Service (DoS)"
- Anomaly Detection depending on
  - Traffic Nature "Normal Traffic"
    - Put IDS/IPS in learning mode to detect the Normal Traffic

NIDS, NIPS Placement

- put in specific Host "Host-based IDS/IPS"
- put in the whole Network "Network-based IDS/IPS"

Wireless Networks Security

Encryption mean Convert the data to Cipher Text

We use Ceaser Cipher Method "Move each Letter 3 steps from original place (A = D, B = E)"

We need Key to Decrypt the Data into its original shape

Encyptoin Methods:

- Wired Equivalent Privacy (WEP):
  - Protocol (IEEE 802.11 standard)

- Use RC4 Algotithm for Encryption
- Key = 104 bits "Static key"
- Ended in 2003

- Wifi Protected Access 1 (WPA 1):
  - Use RC4 Algotithm for Encryption
  - Key = Pre-Shared Key (PSK) "Changeable Key"
  - Data Integrity mean No Changed Data by using "Temporal Key Integrity Protocol (TKIP)"
  - Replaced in 2006 by "WPA 2"

- Wifi Protected Access 2 (WPA 2):
  - Use Advaced Encryption Standard (AES) Algotithm for Encryption
  - Key =Pre-Shared Key (PSK) "Changeable Key"
  - Data Integrity mean No Changed Data by using "Counter Cipher Mode Protocol (CCMP)"
  - In 2017 "Krack Attack" Appeared and Success to Hack the WPA 2

Wireless Threats and Attacks:

- Eavesdropping (Sniffing):
  - Any nearly Attacker can Sniff your Network
  - We should use Good Encryption "WPA 2 at Data Link Layer"

- Spoofing (Masquerading):
  - It's like Changing Identity
  - Attacker Try to trick the Access point by using:
    - MAC/IP address allowable at the Network
    - Software Applications
    - Network Password
  - We should use Protocols with high authentication

- Denial of Service (DoS)
  - Mean Preventing authourized users from accessing the Network
  - Attackers do this by:
    - Hardware Producing High Radio Signals
    - Using The Default Settings on the Access point that didn't change yet
  - We should Upgrade our Firmwares, Change Default Settings and Put IDS

- Rogue Access Point
  - Mean Access point Working on the Network Without knowing about it
  - This Access point Have "No Pass - No Encryption" so anyone can track the Data and Steal it
  - We should Put IDS and Scanning the Building for any Access point

Wireless Network Design Considerations:

- Wireless Signal:
  - Signal should be inside the Building
  - Signal is Strong enough to prevent using Access points

- Access Point Security:
  - Service Set Identifier (SSID) is Hidded
  - Access Point Filtering "MAC - IP - Port Num - Domain name"
  - Encryption WPA2 (AES Cipher)

- Separates between Wireless and Wired connection:
  - Firewall to Seperate between Them
  - Wireless put in Segregated Switch
  - see Info-graphic

Protecting Your Network

User Based Threats/Attacks "Users Fault":

- Social Engineering

      - Depending on Tricking the Users To get SPII by Using
        - Spam Emails
        - Fishing Scam by Using web pages like the Original page to get the data

- Brute Force Attacks
  - Attacker trying to Guess the Passwords by a Software

- Malwares "Malicious Software"

  - Spyware

    - Software on the Device watch all the activities of the User
    - Can Define PII "Name - Country - Gender - Email"
    - Send it to Creater of the Spyware

  - Coockies

    - Software Downloaded from Websites
    - Save "Browsing sites - Liked Items - User's Data"

  - Trojan Horse

    - Sofware Hidden in a "Photo - Game"
    - Start by Opening the file it's attached to
    - It's like a Back Door

  - Viruses

    - Malware attached to and Excutable fiel ".exe" start with it
    - Can Hurt or Delete Files OR Slowing down the System

  - Worme

    - Move from Device to another by the Network
    - It's like Virus

- Distributed Denial of Service (DDoS) Attack
  - Attacking a Server or Device by More than one Device
  - Denial of Service mean One Device send Many Requests to a Website to make it Unavielable
  - Distributed Denial of Service Like Denial of Service but the Attack come from More Devices at the same time

    Security Education:

    - Training Programs
      - Understand user-based attacks

```
- Awareness of organization security
  - Prevent users from using Personal devices
  - Prevent users from downloading unauthorized softwares of using websited with cookies
  - Use rock-solid password
```

- Technically
  - Using strong antivirus softwares
  - Network security scanning

Mitigating the wireless networks eavesdropping attack requires … the network coverage area

- Minimizing

The main role of IPS is to …. attacks on the monitored system/network

- Respond to

The more restrictive Firewall must have the default … rule

- Deny

In connection establishment using TCP, the SYN packet needs to be responded by a … packet

- SYN, ACK

AES is used in conjunction with …

- WPA II

Incident handling steps are as follows:

- Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned

The DMZ and the wireless networks of an organization are recommended to be ….

- Isolated

In general, the wireless networks are considered to be of … security compared to the wired networks

- Lower

The …. use the network to send copies of themselves to other machines

- Worms

WEP Encryption is considered to be nowadays … encryption algorithm

- Obsolete