Revision notes

Chapter 1 (30p)

General terms

Vulnerability: a weakness or flaw in a network

Threat: the potential for a vulnerability to turn into an attack

Mitigation: the action of reducing the severity of a vulnerability

Risk: the potential threat of exploitation of a vulnerability

External threats: threats from the Internet

Internal threats: threats from within the network (hosts)

Outside perimiter: first-level defense, before anyone gets inside

- Security personel
- Fences / gates
- Cameras
- Security alarms

Inside perimiter: defense when someone is already inside

- Biometric access and exit sensors
- Cameras
- Motion detectors

Hackers

- Script kiddies (black hat, no knowledge, uses available scripts)
- Vulnerability brokers (grey hat, deep knowledge, finds vulnerabilities and sells them)
- Hacktivists (grey hat, hacks for political reasons / greater good)
- Cyber criminals (black hats)
- State-Sponsored hackers (black hat, possibly the worst kind)

The three cornerstones of cryptography:

Confidentiality: use encryption to hide data

Availability: data should be accessible

Integrity: use hashing to ensure that data hasn't changed

Types of malware

Trojan Horse

- Security software disabler
- Remote-access
- Data-sending
- Destructive
- Proxy
- FTP
- DoS

Worms

1. Enabling vulnerability
2. Propagation mechanism
3. Payload

Types of attacks

Reconnaissance attack

Mapping out a network before an attack, finding possible vulnerabilities.

- Query the target
- Ping sweep
- Port scan
- Vulnerability scan
- Exploitation tool

Access attacks

Attacker wants to retrieve data, gain access and escalate access privileges

- Password attacks
- Trust exploitation
- Port redirection
- Man-in-the-middle
- Buffer overflow
- IP, MAC and DHCP spoofing

Social engineering

- Phishing
- Spear phishing
- Spam
- Baiting

Network security policy

1. What do you have that others want?
2. What is critical to you?
3. What would stop your services from functioning?

Defending the network

- Develop security policy
- Use strong passwords
- Control physical access
- Encrypt and protect sensitive data
- Perform backups
- Perform security audits
- Update systems
- Employ authentication
- Use a firewall and Intrution Prevention System (IPS)
- Anti-spoofing technologies

Mitigating malware (containment)

1. Inoculation
2. Quarantine
3. Treatment

Planes

Control plane

- Routing Protocol
- IP Routing Table
- Secure using Control Plane Policing (CoPP)
- Routing authentication

Management plane

- Enable login policy
- Present legal information
- Authorization
- Management access reporting
- Role-based access control

Data plane

- IP forwarding table
- Use Access Control Lists (ACLs)
- Use DHCP snooping
- Use Dynamic ARP Inspection (DAI)

Chapter 8 (17p)

VPN

Enables cost savings, security (if enabled), scalability and compatibility.

Remote-Access: a client connect to a site

Site-to-Site: connect one site to another, clients don't see connection - gatway takes care of it

IPsec

Framework

- Protect and authenticate IP packets between source and destination
- Protects traffic from layer 4 to 7
- Confidentiality using encryption (AES or SEAL)
- Integrity using hashes (HMAC)
- Authentication using Internet Key Exchange (IKE) and the Diffie-Hellman (DH) algorithm
    - Pre-Shared Key (PSK) - password based (exchanged using DH, use group > 19)
    - Public Key Infrastructure (PKI) - public key based (RSA)
- Is a framework - can use different algorithms, flexible

TLDR;

- Confidentiality
- Integrity
- Authentication
- Secure Key Exchange

Protocol

Authentication Header (AH): does not provide confidentiality. Header in plain text, but hashed for integrity. Payload is encrypted.

ESP: provides encryption for the entire packet - wraps original packet in a new packet. **Transport mode** encrypts data and ESP trailer. **Tunnel mode** encrypts the IP header as well (more secure).

Internet Key Exchange (IKE)

IKE is a key management protocol. Used for security negotation (IPsec protocol, confidentiality protocol, integrity protocol etc.).

Phase 1 - Negotatiate ISAKMP policy

1. ISAKMP policy is the Security Association (SA) - how to create the tunnel
2. DH key exchange
3. Verify peer identity

Phase 2 - Negotiate IPsec policy

1. Interesting traffic
2. What protocol to use
3. What algorithms to use

Chapter 11 (11p)

Testing and Evaluation (ST&E)

- Uncover design, technical and operational flaws that may violate the security policy
- Determine what is needed to fulfill the security policy
- Assess consistency between documentation and implementation

Types of tests

- Penetration testing
- Network scanning
- Vulnerability scanning
- Password cracking
- Log review
- Integrity checks
- Virus detection

Testing tools

- Nmap / Zenmap (ping sweep / port scan / open source)
- SuperScan (ping sweep / port scan / Microsoft)
- SIEM (forensics / correlation / aggregation / retention)
- GFI LANguard (network scanner / network monitor)
- Tripwire (compliance / monitor configuration)
- Nessus (vulnerability assessment)
- L0phtCrack (password cracker)
- Metasploit (full framework / vulnerabilities etc.)

Security Policy

What it should cover:

1. Identification and authentication policies
2. Password policies
3. Acceptable use policies
4. Remote access policies
5. Network maintainence procedures
6. Incident handling procedures

The hierarchy:

1. Governing policies
    1. Technical policies
    2. End user policies

Governing policies

- States what a policy should solve
- How the policy applies
- Roles and responsibilities
- Consequences of non-compliance

Technical policies

- General policies
- Telephony policies
- Email and communication policies
- Remote access policies
- Network policies
- Application policies

End user policies

Customized for

- Customer
- Employee
- Partner

Security policy documents

- Standard documents
    - Specific requirements that must be met
- Guideline documents
    - Suggestions for best pracitces
    - Strongly recommended
- Procedure documents
    - Step by step of what to do

Security awareness

- Awarenewss campaigns
- Training and education

Chapter 4 (10p)

Access Control List (ACL)

- Basic firewall
- Applied on interfaces and virtual lines (telnet, ssh)
- Filter traffic
- Mitigate some attacks such as DoS and spoofing

Firewall

Packet filtering firewall

- Provides almost all functions of a high end firewall, but at a fraction of the cost
- Layer 3 and 4
- Source / destination IP
- Protocol
- Source / destination port

Application gateway firewall

- Layer 3, 4, 5 and 7

Stateful firewall

- Layer 3, 4 and 5
- Primary means of defense
- Improved performance over packet filtering
- Defends spoofing
- Works well with TCP, not UDP

NAT firewall

- Layer 3 and 4

Next generation

- Granular identification, visibility and control within applications
- Resticting websites based on reputation
- Proactive protection against threats
- Enforcement of policies
- Uses IPS
- Increased performance for NAT, VPN

Zone based firewall (ZPF)

- Each interface in a zone
- Does not depend on ACLs
- Easy to read and troubleshoot policies
- One place for configuration of policies - not each interface
- Typical zones are DMZ, inside, administrator, internet and VPN
- An interface can only be in one zone
- **Inspect** action configures stateful packet inspection
- **Drop** action denies a packet. May log action
- **Pass** action permits a packet. One direction only
- If either source or destination are in a zone, the action is **pass**
- If either source or destination are in a zone, the action is **deny**
- Basically, communication within same zone is permitted, between zones are permitted only if they are a zone-pair. May be inspected if a policy exists

Chapter 2 (8p)

Syslog

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Hardening

1. Physical access
2. Operating system hardening
3. Router hardening

Chapter 5 (8p)

Intrusion Prevention System (IPS)

- Monitors Layer 3 and Layer 4 traffic
- Can stop single packet attacks from reaching target
- Responds immediately, not allowing any malicious traffic to pass
- Introduces delay - inspects each packet
- Impacts the network if it fails or is overloaded
- Deployed as a "sensor"
- Uses signatures to detect packages
- Can detect atomic (single packet) or composite patterns (multiple packets)

Intrusion Detection System (IDS)

- Works passively (only inspects and alerts)
- Works on mirrored traffic (no impact on network speed)
- No impact if it fails or is overloaded

- Cannot stop packets from entering a system
- Deployed as a "sensor"
- Uses signatures to detect packages
- Can detect atomic (single packet) or composite patterns (multiple packets)

Host-based systems

- Provides protection specific to a host OS
- Provides OS and application level protection
- Protects the host after the message is decrypted
- Does not work with encrypted messages
- OS dependent
- Must be installed on all hosts

Network-based systems

- Cost effective
- OS independent
- Not visible to the network
- Lower level network events seen
- Cannot examine encrypted traffic
- Cannot determine whether an attack was successful
- Must stop malicious traffic prior to arriving at host

Types

- Atomic (per-event logging)
- Composite (multiple events combined to one log)

Actions

- Generate an alert
- Log the activity
- Drop or prevent the activity
- Reset a TCP connection
- Block future activity
- Allow the activity

Alarms

- Pattern-based detection (signature-based / pre-defined patterns / only known attacks)
- Anomaly-based detection (profile-based / compared to defined "normal" traffic)
- Policy-based detection (behaviour-based / pre-defined behaviors)
- Honey pot-based detection (uses a dummy server to attract attackers)

Chapter 6 (8p)

CISCO Network Admission Control (NAC)

- Prevents unauthorized access
- Proactively mitigates network threats such as viruses, worms etc.
- Applies posture assessment and remidation
- Enforces policies
- Clientless authentication for guests

CAM table attack

- Overflow the CAM table with MAC addresses
- All frames are sent to all ports in the network
- Mitigate using port-security

VLAN hopping

- Attacker on a VLAN can retrieve data from another VLAN
- Mitigate by disallowing trunking on access ports
- Mitigate by manually configuring all trunks (disable Dynamic Trunking Protocol (DTP))
- Mitigate by assigning the native VLAN of a trunking port to an unused VLAN

DHCP starvation

- An attacker can take up all IP addresses available
- Denies service of legitimate users
- Mitigate by enabling port-security, DHCP snooping and Dynamic ARP Inspection (DAI)

ARP poisoning

- An attacker can pretend to be the router (Man-in-the-middle)
- Mitigate by enabling DHCP snooping and DAI

Address spoofing

- An attacker can pretend to be someone else
- Mitigate by enabling port-security, DHCP snooping, DAI and IP source guard

Spanning Tree Protocol (STP) attacks

- An attacker can make a rogue switch the root switch etc.
- Mitigate by enabling PortFast, BDPU guard, Root guard and loop guard

Chapter 3 (6p)

AAA

- **Authentication** provides a way of telling who's who
- **Authorization** provides a way of permitting a user access to only some parts
- **Accounting** provides a way of knowing who's done what

Local AAA uses a on-device database of users, passwords and priviledge levels. Server-based AAA connects to a server such as RADIUS or TACACS+ to provide the services.

TACACS+

- CISCO protocol
- Seperate processes for authentication and accounting
- Encrypts everything sent
- Uses TCP

RADIUS

- Open protocol
- Same process for authentication and accounting
- Encrypts only the password
- Uses UDP
- Supports 802.11x (port-based security for access control)

Chapter 10 (2p)

General

asdm vlan id

nat-t for vpn auto detection

cws all data through automatically

packet-filter: most of high end at lower cost (-spoofing etc.)

dhcp-snooping: all untrusted hosts dhcp messages. Uses binding table. Verifies hosts. MAC, ip binding. Dynamic ARP inspection, IP source guard use dhcp snooping. `ip dhcp snooping`. Ej på interface.

port security limits mac addresses. static secure (manual), dynamic secure (learned), sticky secure (learned, saved). mode protect: drop, not notified mode restrict: drop, notified shutdown: default, shut down interface must be access interface. Required steps:

1. access mode
2. enable port security
3. define mac addresses

bdpu guard -> layer 2 stp. enabled on end devices. Disables interface when bdpu from unexpected interface. Portfast and bdpu guard on end user ports. Global: `spanning-tree portfast bpduguard default`, per interface: `spanning-tree bpdu guard enable`

root guard -> prevents a designated port form becoming root port. On interfaces connecting to other switches that should not be root `spanning-tree guard root`

VLAN hopping: connected to access, but gets data from other VLANs (sniffing). Make sure access port is not in dynamic desirable, dynamic auto or trunk mode. hard code trunk ports. nonegotiate. disable CDP where its not needed. double tagging: no access port should be native vlan. turn off DTP. Set native vlan of a trunk to an unused vlan. don't send native vlan over trunk.

CAM table attack, overflooding table. Sends to all other ports. Enable port security. Increase memory.

Firewall thing: granularity control over applications.

ip verify source: use dhcp snooping table (switch) to prevent different IPs from same MAC. ip verify source port-security to verify MAC as well. Requires dhcp snooping and port security.

aaa authentication login default local -> all login attempts go through aaa

CoPP - what is allowed for CPU, no unecessary data

Network Access Control NAC: posture checks, incidence response, guest network access, profiling / visiblity, policy life cycle.

NIPS monitors network segments.

Reconnacainse attacks can be prevented by implementing encryption.

PVLANs: community ports talk to buddy community ports and promiscous ports. Isolated ports talk to promiscious ports. Promiscous ports (router ports) allowed for all.

Syslog level 0-7

VPN split tunneling. Router decides what should go through VPN and what should go through internet.

VPN hair pinning. Traffic received by an interface is returned on same interface

Enable login enhancements: issue login block-for command