- Easier to sell approach to management to perform analysis of some systems rather than detail of all.
- Exposes where major risks are likely to occur.
- Use of baseline ensures basic ~~intrusion~~ protection is implemented early on.
- Resources are applied to systems that need it and detailed analysis of these systems is carried out early on.
- If informal analysis results in inaccurate results during detailed risk analysis some systems may still be vulnerable.
- Recommended for almost all organizations.

Chapter 9: Firewalls & Intrusion Prevention Systems

* Affective means of protecting a local system / network of systems from network-based threats.

9.1: Need for Firewalls

* Organizations can no longer function without the internet. Internet allows the world to be able to reach with local network assets.
* Equipping local assets with intrusion protection may not

be sufficient or cost effective.

* If a flaw in PC's operating system is discovered each system should be upgraded to fix the flaw. Requires scalable configuration management & aggressive patching to function effectively. Used when host-based security used.
* Alternative to host-based security is firewall.
* Firewall is inserted between premises network & the internet to make a controlled link & form an outer perimeter.
* Aim of firewall is used to protect premises network and provide a single choke point to impose security & auditing.
* Firewall can be single computer system or a set of two or more systems to act as firewall.

9.2: Firewall characteristics & access policy

Goals of Firewall

- Only authorized traffic allowed to pass. Various firewalls implement various policies
- All traffic must pass through firewall from inside & outside. Block all access to local network except via firewall.
- Firewall itself immune to penetration. Use of hardened system with secured operating system

* A critical component in planning & implementation of a firewall is specifying a suitable access policy.
* Policy includes traffic authorized to pass, address ranges, protocols, applications & content types.
* Policy should be developed through security risk assessment & policy.

characteristics to filter traffic

Application Protocol: on basis of authorized application protocol data. Used by application level gateway that relay & monitor exchange of information e.g SMTP / HTTP

IP address & protocol values: controls based on source / destination address or port numbers, direction of flow (inbound / outbound), network / transport layer charteristics. Used by packet filter & stateful inspection firewalls to limit access to specific services.

User Identity: based on user identity who identifies themselves using some form of authenication e.g. IPSec

Network Activity: based on considerations such as time or request

What firewall provides?

- Location for monitoring security related activities. Audits & alarms can be implemented
- Single choke point - allow authorized IP to pass, protect against various IP spoofing & routing attacks. Simplifies security management.
- Serve as a platform for IPsec to implement virtual private networks
- Convient platform for internet functions like network address translator, network management function

Limitation of firewalls

- Improperly secured LAN accessed from outside organization.
- Cannot protect fully against internal threats. Employee collaborating with external attacker
- Cannot prevent against attacks that bypass firewall
- Cannot guard against an external affected device that is used internally.

9.3: Types of Firewall.

* Firewall can monitor traffic from network layer to application layer.
* Level of appropriate firewall implementation determined by access policy.

* Firewall can act as positive filter allow only packets to pass that meet criteria or negative filter to reject packets that meet criteria.

* Packet Filtering Firewall

- Applies a set of rules to each incoming & outgoing IP packet then forwards or discards the packet.
- configures packets going in both direction.
- Filtering rules are based on source IP address, destination IP address, source & destination transport-level address (TCP/UDP port number), IP protocol field, interface (for firewalls with 3 or more ports, which interface it came from & destined for).
- Matched by the IP/TCP fields the rule is invoked from firewalls rules list. If no match default a rule is applied.
- Default policy can be to forward / discard.
- Default discard policy preferred by bussiness & government organizations. Is conservative.
- Default forward policy provides ease of use but reduced security.
- This type of filtering is simple, transparent to users & fast.

Weakness of packet filtering firewall

- due to limited info available log info is same as access control decisions
- does not check application layer so cannot prevent attacks initiated from that layer
- Do not support advanced user authentication schemes
- Vulnerable to attacks & exploits that take advantage of TCP/IP specification or protocol stack. cannot detect altered layer information. Used to bypass security controls of firewalls
- Small no. of variables are susceptible to security breaches caused by improper configurations.

Attacks on packet filtering firewall

- Source Routing Attacks: Specifies route a packet should take in hopes to bypass security that does not check source routing info. Discard all packets that use this option
- IP address spoofing: transmits packet with source IP of internal host. aim to penetrate the system. counter-measure to discard such a packet if it arrives on external interface
- Tiny fragment attacks: make small fragments of header in hope that only first fragment will be checked and rest will be discarded / forwarded based on that. Define a rule that first fragment must contain predefined min amount of TCP header.

* Stateful Firewalls:

- in simple packet filtering for an SMTP all ports used to create connection between server & host should be permitted by firewall which creates a vulnerability.
- Stateful packet inspection firewall tightens up rules for TCP traffic by checking against outbound TCP connections directory.
- Directory has entry for each established connection & only allows packets that fit that profile.
- Uses same packet info as packet filtering but keeps records of TCP connection & sequence numbers to avoid session hijacking. can even track limited amount of application data.

* Application level Gateway:

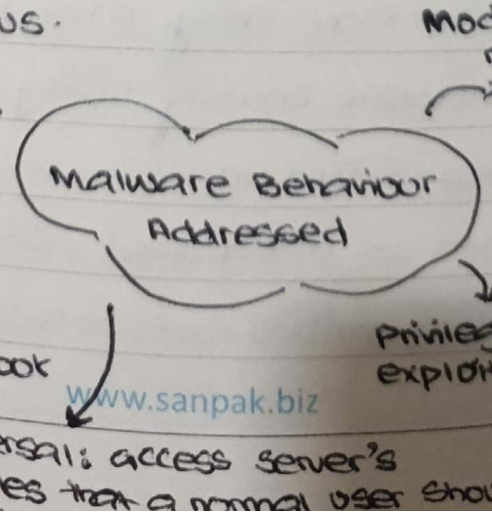
- aka application proxy.
- TCP/IP application contacts gateway which asks for remote host ID (user ID & authentication information) On valid remote host gateway contacts it & relays TCP segments between both endpoints.
- If gateway does not have proxy code for application service not supported & ~~contacted~~ forwarded across firewall.

- Gateway can be configured to allow only certain features of an application.
- Secure than packet filters. Only needs to scrutinize few allowable applications.
- Easy to log & audit all incoming traffic at application level.
- causes additional processing overhead on each connection.

* Circuit - level Gateway:
  - aka circuit level proxy
  - can be stand alone system or a specialized function performed by application level gateway for certain applications.
  - Does not permit end-to-end TCP connection but setsup two TCP connection. Outer host $\xleftrightarrow{TCP}$ gateway $\xleftrightarrow{TCP}$ Inner host
    Relay TCP segments from one connection to another without examining.
  - Used when inner hosts are trusted to only create overhead on inbound traffic not outbound.
  - Security functions determines which connection will be allowed.
  - Example is SOCKS package

9.6: Intrusion prevention systems.

* Type of security product is intrusion prevention system (IPS).
* includes capability to block or prevent detected malicious system/activity.
* can be host-based, network-based or distributed/hybrid.
* can detect behaviour not of legitamate users, or signature/heuristic detection to identify known malicious behaviour.
* When malicious activity is detected blocks or modifies network packet across perimeter or into a host or modifies/blocks system calls of programs on a host.
* Works like a firewall but has algorithms to decide when to do what.
* Host based IPS:
  - uses signature/heuristic or anomaly detection techniques.
  - Focuses on specific content of application network traffic, or sequence of system calls patterns that identify as malicious.



* HIPS can be trailored to protect specific types of servers such as database/web. It will look for those particular application attacks.
* HIPS can also utilize sandbox approach. Suited for mobile codes. Quarantines code in an isolated system area, then runs it & monitors behaviour. If violates policies or matches a signature, it is halted & prevented to run in normal system environment.

Desktop Protection by HIPS

- File system access: calls are not malicious & meet policy
- System calls: Examine system call to check for malicious characteristics. Exploit code executes atleast one system call.
- System registry settings: maintains persistant configuration info often exploited to extend life of exploit. HIPS ensures it maintains its integrity
- Host input/output: local or network based can move exploit code & malware. HIPS examine & enforces proper client interaction with network & other devices.

* PC & computers are more likely to be attacked, they are equipped with endpoint security using antivirus, antispyware, antispam & personal firewalls.
* ~~HP~~ HIPS provides an integrated, single product suite of functions allowing various tools to work closely,

comprehensive threat protection & easier management.

* HIPS can be used as an element in ~~an~~ a defense-in-depth strategy along with firewalls / network-based IPS.

* Network based IPS:
  - Has authority to modify / discard packets & tear down TCP connections. Along with signature / heuristic detection & anomaly detection.
  - Implements flow data protection not common in firewalls. Requires application payload in a sequence to reassembled. On each new packet of flow, all related packets are examined if malicious activity detected all are dropped.

Modes to identify malicious packets

Stateful matching: Scan attack signatures in entire traffic stream than individual packets

Pattern matching: Scans incoming packet for byte sequence to match with those of known attacks.

Protocol anomaly: Searches deviation from standards of RFC

Traffic anomaly: unusual traffic activities e.g. flood of UDP packets or new service of network.

Statistical Anomaly: develops baseline of normal traffic activity & throughput. Alerts if deviation noticed.

* Distributed or Hybrid IPS:
  - Gathers data from large no of hosts & network-based systems

relays it to central analysis system to analyze to return update signatures & patterns to allow systems to coordinate & defend against attacks.

- One type is the digital immune system.

- Motivation was due to rising threat of internet-based malware, increasing malware propagation due to internet & to acquire global view of situation.
- Expands on the use of sandbox analysis.
- Provides rapid response to prevent malware attack asap.
- When new malware enters, immune system captures it, analyzes it, pass info to system, discards malware. Info allows system to detect such malware in the future itself.
- Success depends on ability to detect new malware & analyze it. Constantly analyze & monitore malware found in wild.
- Working:
  - → sensors on various network & hosts capture potential malware scanning, infection or execution.
  - → Sensors sends alerts to central server which correlates & analyzes to determine malware's likelihood & key characteristics.
  - → Server forwards information to protected environment where malware is sandboxed for analysis & testing.
  - → Protected system tests malware against copy of targeted

Date ..... / ..... / .....

MON TUE WED THU FRI SAT SUN

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

application to identify vulnerability.

-> Protected system generates software patches & tests.

-> If patch does not compromise application functionality system sends it to application host to update it.

- Another type is snort inline:

- based on lightweight intrusion detection system snort.
- Has 3 new rules:
  - -> Drop: rejects packet based on rule & logs result.
  - -> Reject: rejects packet, logs results, returns error message. In TCP sends reset TCP message in UDP sends ICMP port unreachable message to originator.
  - -> Sdrop: rejects packet does not log result.
- Also has replace to modify packets than reject them.
- Replace used for honeypot attacks, ~~dis~~ modifies packets of known attacks to disable the attack & protect remote systems.