Information Security Fundamentals

Module Number: 04

Module Name: Network Infrastructure Security and Connectivity

Version Code:IS1_Updated
Released Date:15-Feb-2019

Network Infrastructure Security and Connectivity

AIM:

To familiarise students with the knowledge of infrastructure security, network monitoring and OS hardening.

Objectives

The objectives of this module are to:

- Understand infrastructure Security basics.
- Define device security and various ways to protect it.
- List the basic concept of network monitoring.
- Understand the basic concept of monitoring device like firewall, IDPS etc?
- Understand the concept of system security to extend the protection of the system.
- Define key elements in policy, procedures and guidelines.

Outcomes

At the end of this module, students are expected to:

- Explain the concepts of infrastructure security.
- Describe the process of securing infrastructure devices like routers, hub, switches etc.
- Explain the importance of network monitoring.
- Summaries working and types of IDPS.
- Outline the various system hardening techniques.

Contents

- Understanding Infrastructure Security
- Device Based Security, Media-Based Security
- Monitoring and Diagnosing; Monitoring Network- Firewall
- Intrusion Detection System, Intrusion Prevention system;
- OS and Network Hardening, Application Hardening;
- Physical and Network Security- Policies, Standards and Guidelines

Network Infrastructure Security and Connectivity

Network Infrastructure Security

- On a computer network, the network infrastructure includes the cables, connectivity devices, hosts, and connection points of the network.
- You must control access to critical resources, protocols, and network access points. This includes protecting the physical security of equipment and the configuration of devices.
- Attacks against your network infrastructure can include physical attacks, such as destruction or theft of equipment, and the physical modification of equipment configurations. Attacks can also involve the logical modification of network infrastructure device configurations, such as changing a routing or switching table.
- You can protect your physical network infrastructure with security personnel, closed-circuit TV, alarms, access cards, locks, tamper-proof seals, backup electrical power, and similar measures.
- Restrict remote administration of network infrastructure equipment whenever possible. When you must allow remote administration, be sure to use the most secure authentication and encryption possible.

Network Infrastructure Security and Connectivity

Device Security

- A device is a node helping to form the topology of the network.
- A compromised device may be used by the attacker as a jumping board.
- A DoS attack may be launched against a device.
- Device security is an important and required step in ensuring **infrastructure security** in a network.

Layered view of device security

- Physical security
  - Confidentiality, integrity, availability
  - Placing the device in a secure location?
  - Power got cut off

- Logical security
  - Securing the device against nonphysical attacks
  - Static core configuration of the device
  - Dynamic configuration and performance
  - Network traffic flow through the device

- The security of each layer depends on the security of the layers within.

Network Infrastructure Security and Connectivity

Physical security

Considerations:

- Using redundant devices?
- Network topology (serialised, star, fully meshed?)
- Where to place the network devices?
- Media security (wire tapping, physical eavesdropping)
- Adequate/uninterrupted power supply
- Disasters

Device Redundancy

- A backup device (router, switch, gateway, …) is configured to take over the functionality of a failed active device.
- Means of achieving redundancy:

A. Use routing to enable redundancy

B. Use a redundancy protocol

  - Hot Standby Router Protocol (HSRP)
  - Virtual Router Redundancy Protocol (VRRP)
  - Failover protocols: a feature of Cisco PIX firewalls

Network Infrastructure Security and Connectivity

Security of major devices

How to protect the device against attacks aimed at compromising the device itself?

- Routers
- Firewalls
- Switches
- Authentication servers
- Wireless access points

Network Infrastructure Security and Connectivity

Steps to secure a device (hardening):

- Physical security
- Password management
- ROMmon (ROM monitor, or the bootstrap program)
- Controlling access to the device (tty, vty ports)
- Securing access to the device (via SSH)
- Backup of configuration files and the device software
- Logging events on the device
- Disabling unnecessary services

Network Infrastructure Security and Connectivity

(Continued) Steps to secure a device (hardening):

- Login banner messages
- Controlling SNMP as a management protocol
- Controlling HTTP as a management protocol
- Using CEF as a switching mechanism
- Setting up the scheduler from a security perspective
- Using the Network Time Protocol (NTP)
- Capturing core dumps
- Using service nagle to improve Telnet access during high CPU events

Password Management

- Passwords stored on the router should be properly encrypted.
- The default password-encryption is either type 0 (clear text passwords) or type 7 (weak encryption).
- Service password-encryption

Securing access to the router using encryption

- IPsec VPN client (preferred; more details in Ch 13)
  - **Two cases:**
    - A. The VPN client access a back-end LAN (the destination) by building a tunnel between itself and a router (the IPsec gateway), behind which the LAN is located.
    - B. The VPN client is used to remotely administer the router, which is both the gateway and the destination.
- SSH: Only SSH v1 is supported by Cisco IOS

Disable unnecessary services

- If a service is not being actively used on a device, it should be disabled.
- Otherwise, it may be used as a back door for the attacker to gain access to the device.
- Sample services to be disabled:

  TCP small servers, UDP small servers, Finger server, …

Banner messages

- Informational messages displayed to users who connect to the device.
- To warn the unauthorised users of their activity and to warn them that, they are being monitored and logged.
- Useful for law enforcement and system admin.

Sequence:

- MOTD banner
- Login banner
- login session
- EXEC banner (or incoming banner) -- for users to enter commands; show the contexts

Backup of the Device Software

- Cisco IOS Resilient Configuration feature.
- Enables a router to secure a working copy of the running image and configuration (the primary bootset).
- Those files can withstand malicious attempts to erase the contents of persistent storage.
- Those secure files are protected by the IOS File System (IFS); cannot be removed by the user.
- **secure boot-image**
- **secure boot-config**

Device Security Checklist

- Device security policy written, approved, distributed, and reviewed on regular basis.
- Facilities (room, building, area) housing the devices secured—physical security.
- Password policies to ensure that good passwords are created that cannot be easily guessed or hacked.
- Password encryption used so that passwords are not visible when device configuration is viewed.
- Access methods such as Console, VTY, AUX using ACLs, and authentication mechanisms secured.
- Access methods such as SSH with AAA authentication chosen wisely.
- Unneeded services and protocols to be disabled.
- Unused interfaces shut down or disabled.
- Configuration hardened for network services and protocols in use (for example, HTTP and SNMP).
- Port and protocol needs of the network and use access lists to limit traffic flow identified.
- Access list for anti-spoofing and infrastructure protection and for blocking reserved and private addresses considered.
- Routing protocols established that use authentication mechanisms for integrity.
- Appropriate logging enabled with proper time information.
- Device’s time of day set accurately, maintained with NTP.

Securing Network Cabling

Network cabling is a vulnerable part of your network infrastructure. However, an attacker or spy must have physical access to your cable (or at least be able to get close to the cable) to exploit or attack your network cable infrastructure.

Sabotage is a simple matter for a saboteur who is able to gain physical access to your network cable infrastructure. Use the following techniques to protect your cable infrastructure:

- Document your entire cable infrastructure. Keep that documentation current.
- Investigate all hosts and connectivity devices that are not documented.
- Protect your network cable as much as possible by burying it underground, placing it inside walls, and protecting it with tamper-proof containers.
- Check the physical integrity of your network infrastructure cabling on a regular basis. Verify your network infrastructure after power outages.
- Enable managed devices to alert you of the presence of disconnected cables or unauthorised connections. Investigate all alerts and outages.

Securing Hubs

- Because hubs are physical devices, they should be physically protected. Try to lock hubs in wiring closets. If the hub cannot be locked in a room or closet, try to secure it in some other type of protective encasement. At a minimum, you should periodically check hubs to be sure that all cables are connected properly and that no rogue connections exist.
- Managed hubs can be used to detect physical configuration changes. Managed hubs report hub statistics and connection information to management software. You can configure a managed hub to send an alert when a configuration is modified. Of course, because a managed hub has a (software) configuration, an attacker could compromise the hub's configuration to disrupt network communication or mask evidence of another attack.

Network Infrastructure Security and Connectivity

Switches and Bridges

There are several measures you can take to prevent attacks against your switches and bridges. As with other network devices, you should physically secure them, so they cannot be tampered with or destroyed. Here are other suggestions that can help to secure your switches and bridges:

- Secure all physical connections on your network segments. Be sure that no unauthorised connections can be made. Also, limit physical access to your switch locations and use security personnel and monitoring devices to ensure connectivity devices are secure.
- Set complex passwords for administrative consoles. Restrict device administration to as few people as possible from as few locations as possible. Also, be sure to change administrative passwords routinely and whenever an administrator leaves the company.

Switches and Bridges

- Manually enter ARP mappings on critical devices, such as central servers, switches, bridges, and so on. If you manually enter all necessary MAC addresses, prevent the switch or bridge from learning new addresses.
- Keep your switches and bridges current with the latest vendor security patches.
- Document your device configurations, so you know for sure what is normal and authorised.
- Monitor your network with management tools that alert you to unauthorised connections. Tools such as ARPWATCH can monitor activity on your network and keep a database of MAC-to-IP address mappings. The tool can also alert you to changes in these ARP mappings.

Securing Routers

- Set access list entries to prevent inappropriate connections and routing of traffic. For example, packets with the IP address of your internal network should not be coming from the external interface on the router. If this happens, it is usually an indication that someone is trying to perform IP address spoofing.
- Keep your routers current with the latest vendor security patches.
- Be sure to document and regularly review your network configuration.
- Disable RIPv1 and utilise only RIPv2 or other routing protocols that allow you to secure router updates with passwords.

Securing Firewall

As described in the previous section, there are several ways an attacker might attempt to neutralise your firewall, so protecting it requires vigilance. To protect your firewall, follow this advice:

- Keep track of security bulletins concerning your firewall product. Apply all software patches as they are made available.
- Update virus definition files routinely.
- Physically protect the firewall.
- Document the firewall configuration and review that configuration regularly.
- Limit the methods for managing the firewall. If remote management is allowed, use the most secure authentication available.
- Use complex passwords. Be sure to change administrative passwords routinely, and always change them when an administrator leaves your organisation.
- Know and test the firewall rules by trying to make connections to unauthorised ports or services from outside the firewall.
- Ensure that there are no network paths or connections that can be used to circumvent the firewall.

What is network monitoring?

- Monitoring an active communications network in order to diagnose problems and gather statistics for administration and fine tuning.
- The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages via email, pager or other alarms. It is a subset of the functions involved in network management.

Network monitoring systems and tools

There are three kinds of tools. They are:

- **Diagnostic tools –** used to test connectivity, ascertain that a location is reachable, or a device is up – usually active tools.
- **Monitoring tools –** tools running in the background (”daemons” or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.
- **Performance tools –** tell us how our network is handling traffic flow.

Network monitoring systems and tools

Active tools

- Ping – test connectivity to a host
- Traceroute – show path to a host
- MTR – combination of ping + traceroute
- SNMP collectors (polling)

Passive tools

- log monitoring, SNMP trap receivers, NetFlow

Automated tools

- SmokePing – record and graph latency to a set of hosts, using ICMP (Ping) or other protocols
- MRTG/RRD – record and graph bandwidth usage on a switch port or network link, at regular intervals

Network monitoring systems and tools

Monitor your critical Network Services

- DNS/Web/Email
- Radius/LDAP/SQL
- SSH to routers

How will you be notified?

Don't forget log collection!

- Every network device (and UNIX and Windows servers as well) can report system events using syslog
- You **MUST** collect and monitor your logs!
- Not doing so is one of the most common mistakes when doing network monitoring

Network Infrastructure Security and Connectivity

Network management protocols

SNMP – Simple Network Management Protocol

- Industry standard, hundreds of tools exist to exploit it.
- Present on any decent network equipment.
  - Network throughput, errors, CPU load, temperature, ...
- UNIX and Windows implement this as well
  - Disk space, running processes, ...

SSH and telnet

- It is also possible to use scripting to automate monitoring of hosts and services.

Statistics and accounting tools

- Traffic accounting and analysis
- What is your network used for, and how much
- Useful for Quality of Service, detecting abuses, and billing (metering)
- Dedicated protocol: NetFlow
- Identify traffic ”flows”: protocol, source, destination, bytes
- Different tools exist to process the information
- Flowtools, flowc
- NFSen

What is a Firewall?

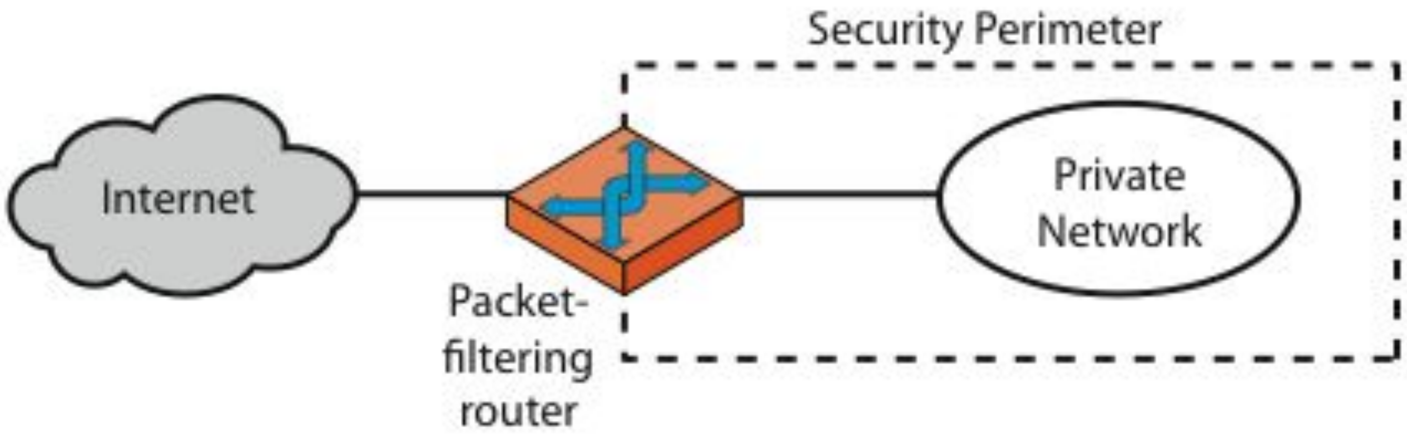
- A **choke point** of control and monitoring
- Interconnects networks with differing trust
- Imposes restrictions on network services
    - Only authorised traffic is allowed
- Auditing and controlling access
    - Can implement alarms for abnormal behavior
- Itself immune to penetration.
- Provides **perimeter defence.**

Classification of Firewall

Characterised by protocol level it controls in

- Packet filtering
- Circuit gateways
- Application gateways

Firewalls – Packet Filters



(a) Packet-filtering router

Firewalls – Packet Filters

- Simplest of components
- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type

Examples

- DNS uses port 53
  - No incoming port 53 packets except known trusted servers

Usage of Packet Filters

- Filtering with incoming or outgoing interfaces

  Example: Ingress filtering of spoofed IP addresses

  - Egress filtering

- Permits or denies certain services

  - Requires intimate knowledge of TCP and UDP port utilisation on a number of operating systems.

Network Infrastructure Security and Connectivity

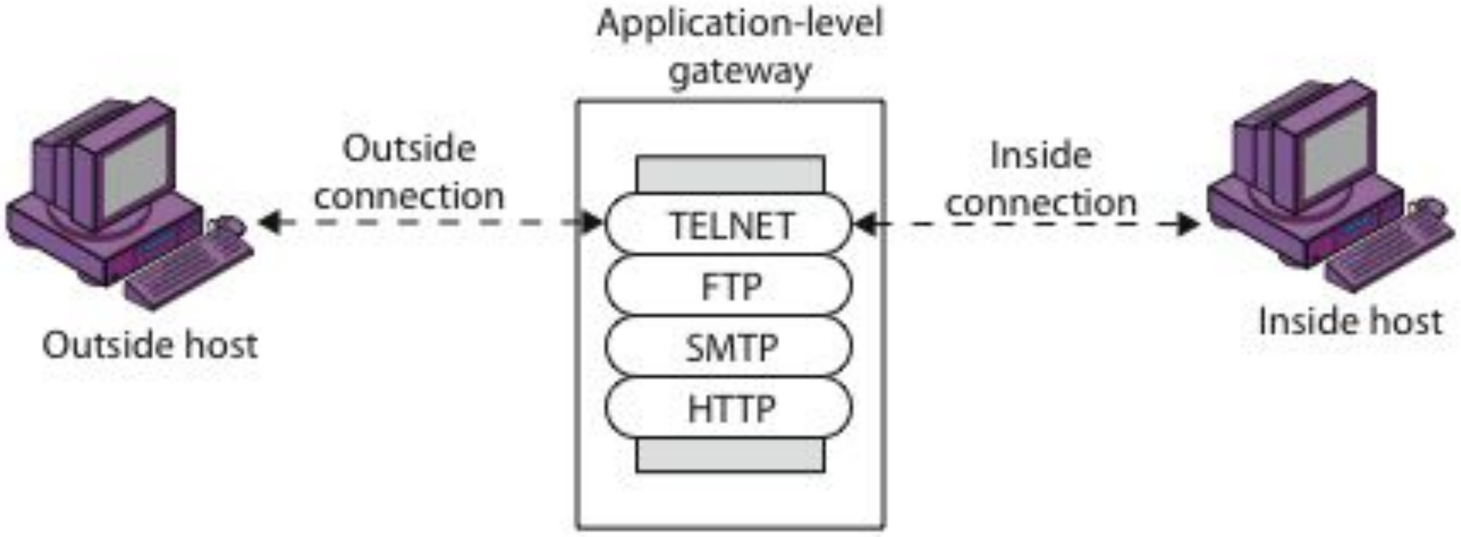
Firewall Gateways

- Firewall runs set of proxy programs
  - Proxies filter incoming, outgoing packets
  - All incoming traffic directed to firewall
  - All outgoing traffic appears to come from firewall
- Policy embedded in proxy programs

Two kinds of proxies

- Application-level gateways/proxies
  - Tailored to http, ftp, smtp, etc.
- Circuit-level gateways/proxies
  - Working on TCP level

Firewalls - Application Level Gateway (or Proxy)



(b) Application-level gateway

Application-Level Filtering

Has full access to protocol

- User requests service from proxy
- Proxy validates request as legal
- Then actions request and returns result to user

Need separate proxies for each service

- E.g., SMTP (E-Mail)
- NNTP (Net news)
- DNS (Domain Name System)
- NTP (Network Time Protocol)
- custom services generally not supported

Firewalls - Circuit Level Gateway

- Relays two TCP connections.
- Imposes security by limiting which such connections are allowed.
- Once created usually relays traffic without examining contents.
- Typically used when trust internal users by allowing general outbound connections.
- SOCKS commonly used for this.

Introduction to IDS/IPS

- Intrusion Detection Systems (IDSs) will be obsolete very soon (if they are not already). In it's place is something much more capable, an Intrusion Prevention System (IPS).
- IPSs are not a new technology, they are simply an evolved version of IDS.
- IPSs combine IDSs and improved firewall technologies, they make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done.
- Because IDS and IPS technologies offer many of the same capabilities, administrators can usually disable prevention features in IPS products, causing them to function as IDSs.

Network Infrastructure Security and Connectivity

Definitions

- **Intrusions:** attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer system or network (illegal access).
- Intrusions have many causes, such as malware (worms, spyware, etc…), attackers gaining unauthorised access to systems from the Internet, and authorised users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorised.
- Although many intrusions are malicious in nature, many others are not; for example: a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorisation.

Definitions

- **Intrusion detection:** It is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible intrusions (incidents).
- **Intrusion Detection System (IDS):** It is a software that automates the intrusion detection process. The primary responsibility of an IDS is to detect unwanted and malicious activities.
- **Intrusion Prevention System (IPS):** It is a software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Why Intrusion Detection Prevention Systems should be used?

- It is a direct fact that while every enterprise has a firewall, most still suffer from network security problems. IT professionals are acutely aware of the need for additional protective technologies, and network equipment vendors are anxious to fill in the gap.
- Intrusion Prevention Systems have been promoted as cost-effective ways to block malicious traffic, to detect and contain worm and virus threats, to serve as a network monitoring point, to assist in compliance requirements, and to act as a network sanitising agent.

Why Intrusion Detection Prevention Systems should be used?

IDPSs are primarily focused on:

- Identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
- Identifying problems with security policies.
- Documenting existing threats.
- Deterring individuals from violating security policies.

Types of IDPSs

- **Network-based:** perform packet sniffing and analyse network traffic to identify and stop suspicious activity. They are typically deployed inline. Like a network firewall. They receive packets, analyse them, decide whether they should be permitted, and allow acceptable packets to pass through.
- Allow some attacks, such as network service worms, e-mail.borne worms and viruses with easily recognisable characteristics (e.g., subject, attachment filename), to be detected on networks before they reach their intended targets (e.g., e-mail servers, Web servers).
- Most products use a combination of attack signatures and analysis of network and application protocols.
- Network-based products might be able to detect and stop some unknown threats through application protocol analysis.
- Some products allow administrators to create and deploy attack signatures for many major new malware threats in a matter of minutes. Although poorly written signature triggers false positives that block benign activity, a custom signature can block a new malware threat hours before antivirus signatures becomes available.
- However, network-based products are generally not capable of stopping malicious mobile code or Trojan horses.

Types of IDPSs

- **Host-based:** are similar in principle and purpose to network-based, except that a host-based product monitors the characteristics of a single host and the events occurring within that host, such as monitoring network traffic (only for that host), system logs, running processes, file access and modification, and system and application configuration changes.
- They often use a combination of attack signatures and knowledge of expected or typical behaviour to identify known and unknown attacks on systems.
- If a host-based product monitors the host's network traffic, it offers detection capabilities similar to a network-based.
- Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

Types of IDPSs

- **Network Behaviour Analysis (NBA):** Examines network traffic to identify threats that generate unusual traffic flows, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems).
- NBA systems are most often deployed to monitor flows on an organisation’s internal networks, and are also sometimes deployed where they can monitor flows between an organisation’s networks and external networks (e.g., the Internet, business partners’ networks).

Types of IDPSs

- **Wireless:** monitors wireless network traffic and analyses its wireless networking protocols to identify suspicious activity involving the protocols themselves.
- It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring.
- It is most commonly deployed within range of an organisation’s wireless network to monitor it, but can also be deployed to locations where unauthorised wireless networking could be occurring.

Network Infrastructure Security and Connectivity

Before evaluating IDPS products

- Organisations need to understand the characteristics of their system and network environments, so that a compatible IDPS can be selected that can monitor the events of interest on the systems and/or networks.
- Organisations should articulate the goals and objectives they wish to attain by using an IDPS, such as stopping common attacks, identifying misconfigured wireless network devices, and detecting misuse of the organisation’s system and network resources.
- Organisations should also review their existing security policies, which serve as a specification for many of the features that the IDPS products need to provide.
- Organisations should determine if they require IDPSs or other specific system security resources.

Organisations also need to define specialised sets of requirements for the following:

- Security capabilities: including information gathering, logging, detection, and prevention.
- Performance: including maximum capacity and performance features.
- Management: including design and implementation (e.g., reliability, interoperability, scalability, product security), operation and maintenance (including software updates), and training, documentation, and technical support Life cycle costs, both initial and maintenance costs.

In addition, all types of IDPSs perform the following:

- **Recording information related to observed events.** Information is usually recorded locally, and might also be sent to separate systems such as centralised logging servers, Security Information and Event Management (SIEM) solutions, and enterprise management systems.
- **Notifying security administrators of important observed events.** This notification, known as an alert, may take the form of audible signals, e-mails, pager notifications, or log entries. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.
- **Producing reports.** Reports summarise the monitored events or provide details on particular events of interest.

In addition, all types of IDPSs perform the following:

- An IDPS might also alter the settings for when certain alerts are triggered or what priority should be assigned to subsequent alerts after a particular threat is detected.
- IPSs respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques:
- The IPS stops the attack itself.

Examples:

- Terminate the network connection or user session that is being used for the attack. Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute. Block all access to the targeted host, service, application, or other resource.

In addition, all types of IDPSs perform the following:

- **The IPS changes the security environment**. The IPS could change the configuration of other security controls to disrupt an attack. Such as reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.
- **The IPS changes the attack's content**. Some IPS technologies can remove or replace malicious portions of an attack to make it benign. An example, is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient.
- **Most IDPSs also offer features that compensate for the use of common evasion techniques.** Evasion is modifying the format or timing of malicious activity, so that its appearance changes but its effect is the same. Attackers use evasion techniques to try to prevent IDPSs from detecting their attacks.
- **For example:** An attacker could encode text characters in a particular way, knowing that the target understands the encoding and hoping that any monitoring IDPSs do not. Most IDPSs can overcome common evasion techniques by duplicating special processing performed by the targets. If the IDPS can "see" the activity in the same way that the target would, then evasion techniques will generally be unsuccessful at hiding attacks.

Classes of detection methodologies:

- Signature-based: Compares known threat signatures to observed events to identify incidents.
- This is very effective at detecting known threats, but largely ineffective at detecting unknown threats and many variants on known threats.
- Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

Examples:

- A telnet attempt with a username of “root”, which is a violation of an organisation’s security policy.
- An e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware.

Network Infrastructure Security and Connectivity

Classes of detection methodologies:

- Anomaly-based detection: Sample network activity to compare to traffic that is known to be normal.
- When measured activity is outside baseline parameters or clipping level, IDPS will trigger an alert.
- Anomaly-based detection can detect new types of attacks.
- Requires much more overhead and processing capacity than signature-based.
- May generate many false positives.

Classes of detection methodologies:

- State-full protocol analysis: A key development in IDPS technologies was the use of protocol analysers.
- Protocol analysers can natively decode application-layer network protocols, like HTTP or FTP. Once the protocols are fully decoded, the IPS analysis engine can evaluate different parts of the protocol for anomalous behaviour or exploits against predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state.
- Problems with this type include that it is often very difficult or impossible to develop completely accurate models of protocols, it is very resource-intensive, and it cannot detect attacks that do not violate the characteristics of generally acceptable protocol behaviour.

Drawbacks

- IDPS technologies cannot provide completely accurate detection. When an IDPS incorrectly identifies benign activity as being malicious, a false positive has occurred. When an IDPS fails to identify malicious activity, a false negative has occurred. It is not possible to eliminate all false positives and negatives; in most cases, reducing the occurrences of one increases the occurrences of the other.
- Many organisations choose to decrease false negatives at the cost of increasing false positives, which means that more malicious events are detected but more analysis resources are needed to differentiate false positives from true malicious events. Altering the configuration of an IDPS to improve its detection accuracy is known as tuning.

Implementing IDPS

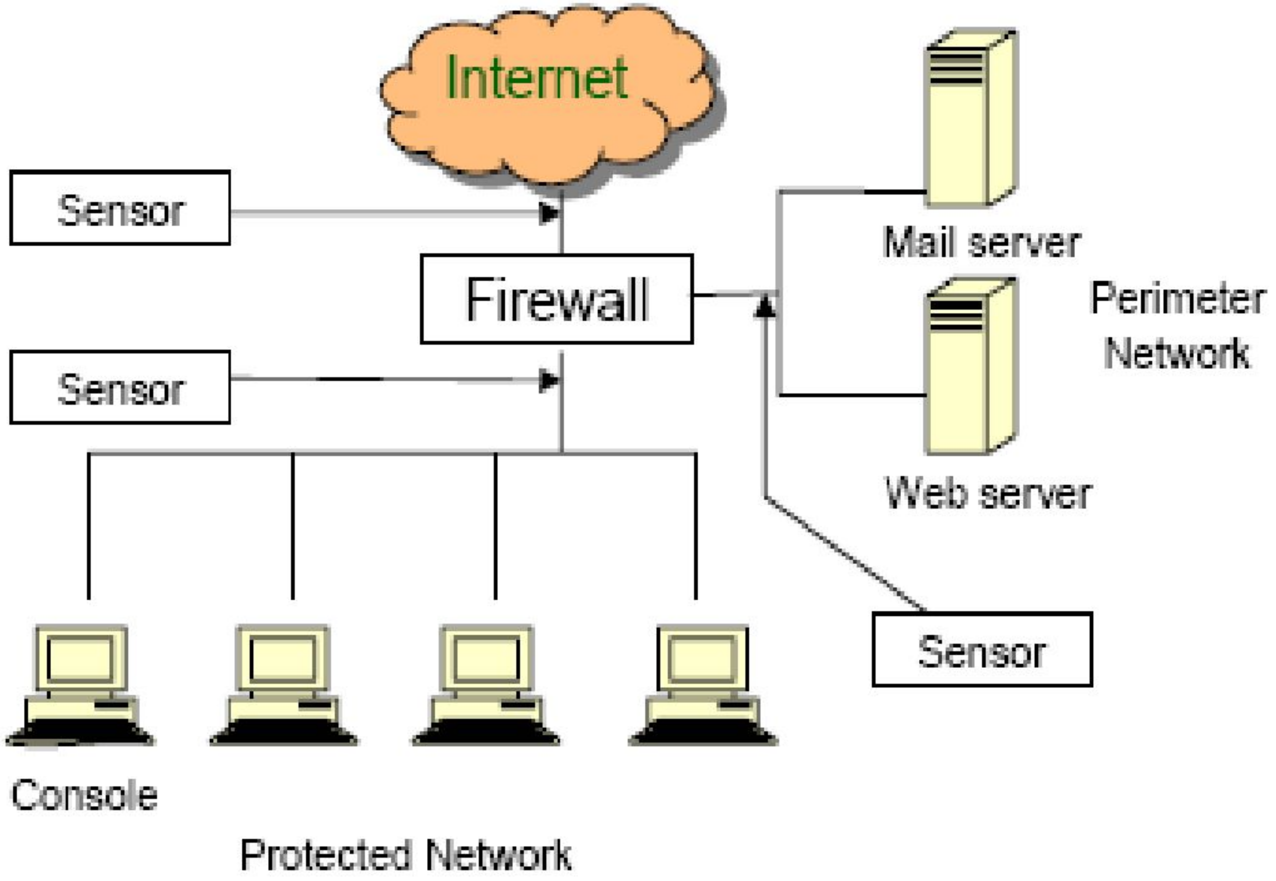
- Organisations should consider using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity.
- For most environments, a combination of network-based and host-based IDPSs is needed for an effective IDPS solution.
- NBA technologies can also be deployed if organisations desire additional detection capabilities for DoS & DDoS attacks, worms, and other threats that NBAs are particularly good at detecting.
- Wireless IDPSs may also be needed, if the organisation determines that its wireless networks need additional monitoring or if the organisation wants to ensure that rogue wireless networks are not in use in the organisation’s facilities.

Placement of Network IDPSs

Deployment options:

- Outside firewall
- Just inside firewall
    - Combination of both will detect attacks getting through
    - Firewall and may help to refine firewall rule set.
- Behind remote access server
- Between business units
- Between corporate network and partner networks
- Sensors may need to be placed in all switched
- Network segments

Network Infrastructure Security and Connectivity



Placement of host IDPSs

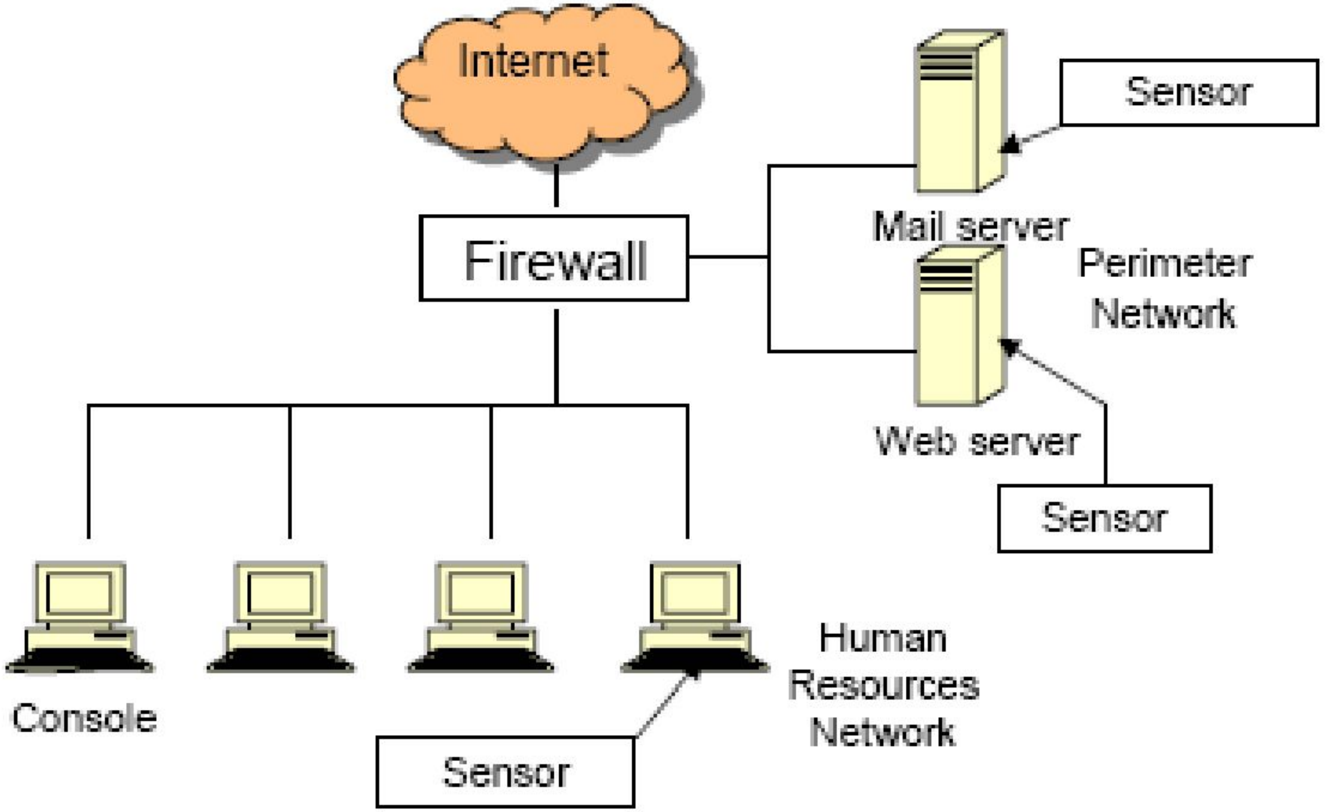
Deployment options:

- Key servers that contain mission-critical and sensitive information.
- Web servers.
- FTP and DNS servers.
- E-commerce database servers, etc.

Other high value assets.

- May also emplace these randomly to obtain probabilistic measure of hosts becoming compromised.

Network Infrastructure Security and Connectivity



OS and Network Hardening Overall Goal

- Asses risks and plan the system development.
- Secure the underlying OS and then key applications.
- Ensure any critical content is secured.
- Ensure appropriate network protection mechanisms are used.
- Ensure appropriate process are used to maintain security (policies).

Network Infrastructure Security and Connectivity

Things to keep in mind

- Purpose of the system, type of information stored, applications and services provided.
- Users of the system and their privileges.
- How are users authenticated?
- How information on system is managed?
- What other hosts / DBs are accessed by system?
- Who will manage system and how (remote or local)?
- Additional measures such as: firewall, anti-virus, logging

Hardening the OS

- Default OS configurations are for ease of use

Measures have to be done at all stages

- Installing and patching
- Configuring
  - Remove unnecessary applications, services and protocols.
  - Users, groups, controls and privileges.
- Install additional software (anti-virus, firewall, intrusion detection system, etc.)
- Test Security

Network Infrastructure Security and Connectivity

Installing and Patching

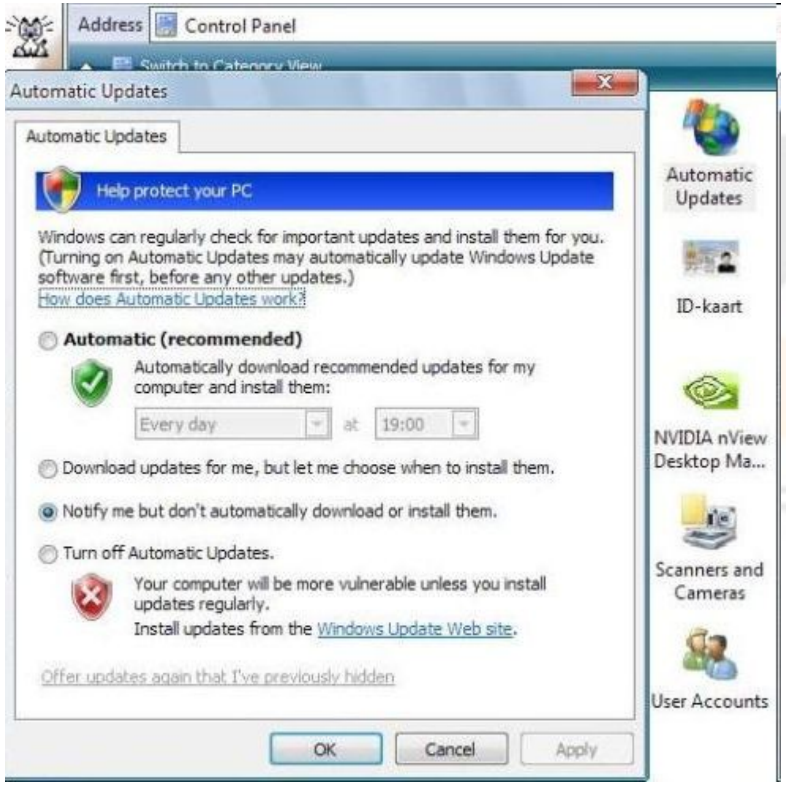
Installation

- Machines should not connect to network until secured
  - However, removable media may be infected as well,
- Limited network (firewall) is acceptable, ideally:
  - No inbound connections
  - Only out to certain key sites
- Install only required services and drivers (from trusted sources)
- Set up automatic updates (only if update time is not an issue)

Booting

- Protect BIOS changes with password
- Disable some bootable media
- Cryptographic hard drives? Pros and Cons

Automatic Updates



Automatic Updates

Automatic Updates

Help protect your PC

Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

○ **Automatic (recommended)**

Automatically download recommended updates for my computer and install them:

Every day at 19:00

○ Download updates for me, but let me choose when to install them.

● Notify me but don't automatically download or install them.

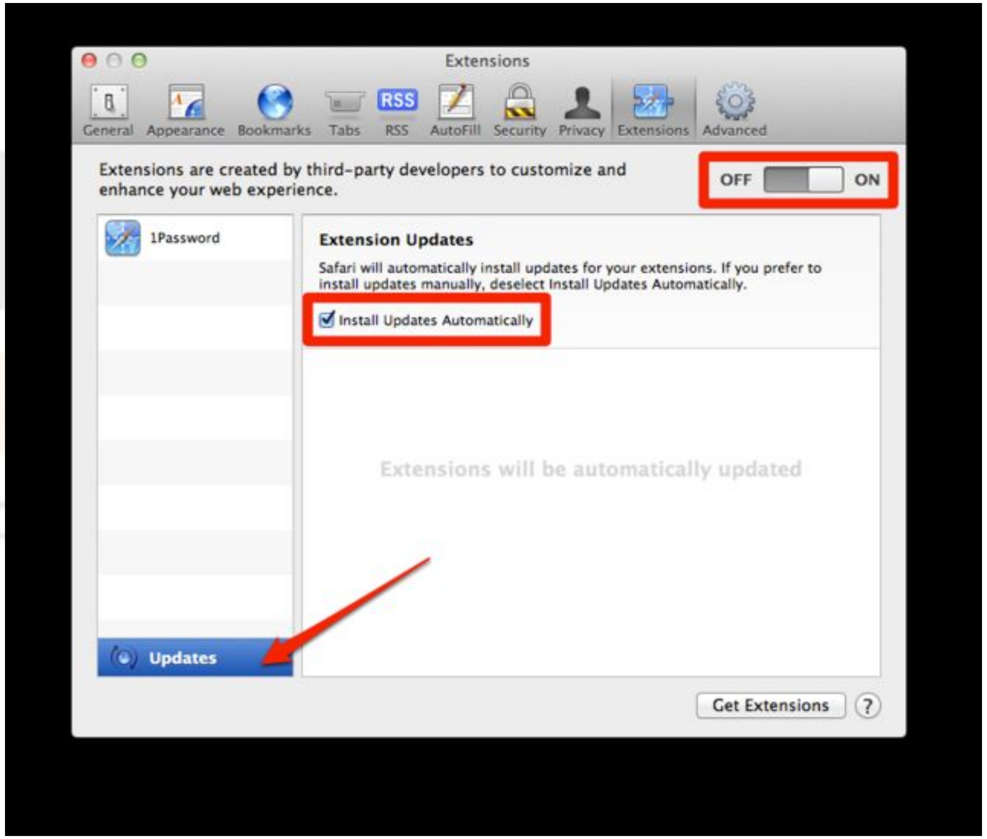
○ Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.

Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

OK Cancel Apply



Extensions are created by third-party developers to customize and enhance your web experience.

OFF ON

1Password

Updates

Extension Updates

Safari will automatically install updates for your extensions. If you prefer to install updates manually, deselect Install Updates Automatically.

☑ Install Updates Automatically

Extensions will be automatically updated

Get Extensions ?

Remove Unnecessary Support

- Software have vulnerabilities, hence more software = more vulnerabilities.
- Better to not install it at all.
  - Uninstallers sometimes fail to clean all dependency.
  - Disabled software may be enabled by an attacker upon control acquisition.
- Disabling can be done via msconfig command (Windows), yast or equivalent (Linux) or Control Panel (Windows / Linux).

Configure U/G Authentication

- Define user types and privileges
  - Admin (ideally only temporary)
  - Normal
  - Limited
- Authentication
  - Force default password change
  - Password definition
  - Password lifespan
- Remove or disable old accounts
- Allow for remote connections.

Additional Security and Testing

- Anti-virus
- Firewalls, IDS, IPS
- White list
  - If attackers manages to install a program what will happen?
- Run some test cases which attempts to break security (stress testing), good hackers make a lot of money here.

Maintenance

Now that system is set, keep it secure. This involves the following:

- Monitoring and analysing logging information.
- Performing regular backups.
- Recovering from security compromises.
- Regular testing of security.
- Patch, update, and revise critical software.

Logging

- Keep a record of important events in the computer.
- **Problems**
  - Need to make sure to have enough space.
  - Manual analysis is hard, so these logs should contain a format such that a program (e.g. in Perl) can parse messages.

Data Backup

- Backup is the act of creating copies of information such that it may be recovered.
- Archive is to keep these backups for a long period of time in order to meet some legal aspects.
- Should the backup be kept online or offline?
  - Online makes easier access, faster recover.
  - Offline is more secure, harder to recover.
  - Why not both?: Users should keep their own offline backups, in case online backup gets removed.
- Data may be lost accidentally (hardware failures, human mistake) or intentionally.

Network Infrastructure Security and Connectivity

Application Security

- Configure applications properly
- Use encryption when possible as seen earlier.
  - For storing
  - For transmit (SSH connections)
- Limit privileges as with users
  - Remember what we have said about security in Android, Blackberry, and iPhone.
- Applications may provide backdoors if not configured properly.

Application Security Threats

- **Executing Commands with the Privileges of a Compromised Application**
  - If an attacker takes over an application, the attacker can execute commands with the privileges of that application.
  - Many applications run with super user (root) privileges.

Application Security Threats

Buffer Overflow Attacks

- Vulnerabilities, exploits, fixes (patches, manual work-around or upgrades).
- Buffers are places where data is stored temporarily.
- If an attacker sends too much data, a buffer might overflow, overwriting an adjacent section of RAM.

Hardening Applications

- **Basics**
  - Physical Security
  - Backup
  - Harden the Operating System
  - Etc.
- **Minimise Applications**
  - Main applications
  - Subsidiary applications
  - Be guided by security baselines

Hardening Applications

- **Create Secure Application Program Configurations**
  - Use baselines to go beyond default installation configurations for high-value targets.
  - Avoid blank passwords or well-known default passwords.
- **Install Patches for All Applications**
- **Minimize the Permissions of Applications**
  - If an attack compromises an application with low permissions, will not own the computer.

Hardening Applications

Add Application Layer Authentication, authorisations, and Auditing

- More specific to the needs of the application than general operating system logins.
- Can lead to different permissions for different users.

Implement Cryptographic Systems

- For communication with users.

Securing Custom Applications

Custom Applications

- Written by a firm’s programmers.
- Not likely to be well trained in secure coding.

The Key Principle

- Never trust user input.
- Filter user input for inappropriate content.

Securing Custom Applications

Buffer Overflow Attacks

- In some languages, specific actions are needed.
- In other languages, not a major problem.

Login Screen Bypass Attacks

- Website user gets to a login screen.
- Instead of logging in, enters a URL for a page that should only be accessible to authorised users.

Securing Custom Applications

Cross-Site Scripting (XSS) Attacks

- One user’s input can go to another user’s webpage.
- Usually caused, if a website sends back information sent to it without checking for data type, scripts, etc.

Example: If you type your username, it may include something like, “Hello username” in the webpage it sends you.

Policies, Standards and Guidelines

- Define management’s role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines.
- Describe an information security blueprint, identify its major components, and explain how it is used to support the network security program.
- Discuss how an organisation institutionalises its policies, standards, and practices using education, training, and awareness programs.
- Explain what contingency planning is and how incident response planning, disaster recovery planning, and business continuity plans are related to contingency plannings.

Network Infrastructure Security and Connectivity

Introduction

- Creation of information security program begins with creation and/or review of organisation's information security policies, standards, and practices.
- Then, selection or creation of information security architecture and the development and use of a detailed information security blueprint creates plan for future success.
- Without policy, blueprints, and planning, organisation is unable to meet information security needs of various communities of interest.

Information Security Policy, Standards and Practices

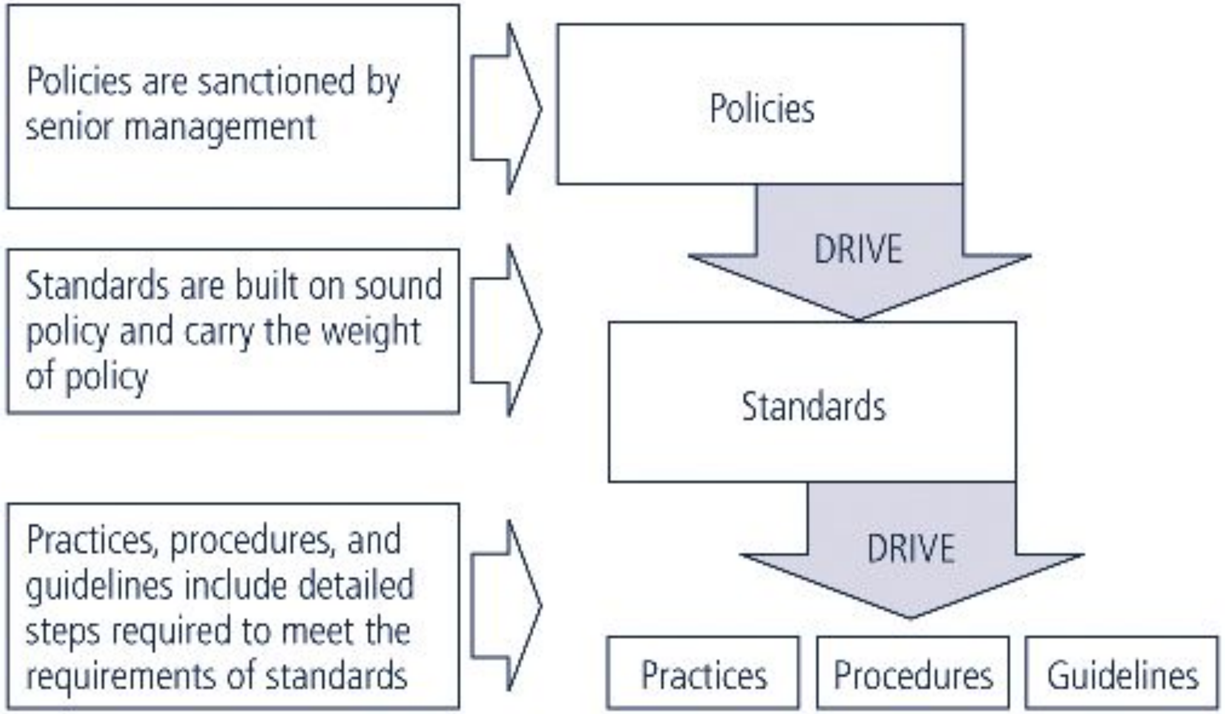
- Communities of interest must consider policies as basis for all information security efforts.
- Policies direct how issues should be addressed and technologies used.
- Security policies are least expensive controls to execute but most difficult to implement.
- Shaping policy is difficult.

Definitions

- Policy: Course of action used by organisation to convey instructions from management to those who perform duties.
- Policies are organisational laws.
- Standards: More detailed statements of what must be done to comply with policy.
- Practices, procedures and guidelines effectively explain how to comply with policy.
- For a policy to be effective, must be properly disseminated, read, understood and agreed to by all members of organisation.

Relationship

Policies, Standards, and Practices



Policies are sanctioned by senior management

Standards are built on sound policy and carry the weight of policy

Practices, procedures, and guidelines include detailed steps required to meet the requirements of standards

Enterprise Information Security Policy (EISP)

- Sets strategic direction, scope, and tone for all security efforts within the organisation.
- Executive-level document, usually drafted by or with CIO of the organisation.

Typically addresses compliance in two areas:

- Ensure meeting requirements to establish program and responsibilities assigned therein to various organisational components.
- Use of specified penalties and disciplinary action.

Issue-Specific Security Policy (ISSP)

The ISSP:

- Addresses specific areas of technology.
- Requires frequent updates.
- Contains statement on organisation’s position on specific issue.

Three approaches when creating and managing ISSPs:

- Create a number of independent ISSP documents.
- Create a single comprehensive ISSP document.
- Create a modular ISSP document.

Systems-Specific Policy (SysSP)

- SysSPs frequently codified as standards and procedures used when configuring or maintaining systems.
- Systems-specific policies fall into two groups. They are:
  - Access Control Lists (ACLs)
  - Configuration rules

(Continued) Systems-Specific Policy (SysSP)

- Both Microsoft Windows and Novell Netware 5.x/6.x families translate ACLs into configurations used to control access.
- ACLs allow configuration to restrict access from anyone and anywhere.
- Rule policies are more specific to operation of a system than ACLs.
- Many security systems require specific configuration scripts telling systems what actions to perform on each set of information they process.

Network Infrastructure Security and Connectivity

Policy Management

- Policies must be managed as they constantly change
- To remain viable, security policies must have:
  - Individual responsible for reviews.
  - A schedule of reviews.
  - Method for making recommendations for reviews.
  - Specific policy issuance and revision date.

Information Classification

- Classification of information is an important aspect of policy.
- Policies are classified.
- A clean desk policy stipulates that at end of business day, classified information must be properly stored and secured.
- In today's open office environments, may be beneficial to implement a clean desk policy.

The Information Security Blueprint

- Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls.
- More detailed version of security framework (outline of overall information security strategy for organisation).
- Should specify tasks to be accomplished and the order in which they are to be realised.
- Should also serve as scalable, upgradeable, and comprehensive plan for information security needs for coming years.

Network Infrastructure Security and Connectivity

Summary

- Device security is an important and required step in ensuring infrastructure security in a network.
- If a service is not being actively used on a device, it should be disabled.
- Monitoring an active communications network in order to diagnose problems and gather statistics for administration and fine tuning.
- A firewall provides perimeter defence. It Permits or denies certain services.
- IPSs combine IDSs and improved firewall technologies, they make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done.
- Purpose of the system, type of information stored, applications and services provided must be kept in mind while planning for system hardening.
- Without policy, blueprints, and planning, organisation is unable to meet information security needs of various communities of interest.

Self Assessment Question

1. Restrict remote administration of network infrastructure equipment whenever possible. State whether True or False.

   a. True

   b. False

Answer: True

Self Assessment Question

2. Confidentiality, integrity and availability are part of ____________________.

   a. Physical Security

   b. Logical Security

Answer: Physical Security

Self Assessment Question

3. Dynamic configuration and performance are part of _________________.

a. Physical Security

b. Logical Security

Answer: Logical Security

Self Assessment Question

4. A backup device (router, switch, gateway, …) is configured to take over the functionality of a failed ______ device.

   a. Overloaded

   b. Weak

   c. Active

Answer: Active

Self Assessment Question

5. VPN is a _____________.

a. Device

b. Network

c. Policy

d. Protocol

Answer: Network

Self Assessment Question

6. Network cabling is a vulnerable part of the network infrastructure, it is vulnerable to ________.

a. MITM

b. ARP Poisoning

c. DNS

d. Sabotage

Answer: Sabotage

Self Assessment Question

7. Hubs are used to transmit packet to different network. State whether True or False.

a. True

b. False

Answer: False

Self Assessment Question

8. Which device broadcast the packet it received to all the connected devices?

a. Router

b. Servers

c. Repeaters

d. Hubs

Answer: Hubs

Self Assessment Question

9. Which one of the following is not the correct choice to protect switches and bridges?

a. Manually enter ARP mappings.

b. Keep your switches and bridges updated.

c. Document your device configurations.

d. Disable RIPv1 and utilize only RIPv2.

Answer: Disable RIPv1 and utilize only RIPv2.

Self Assessment Question

10. Which one of the following is not the correct choice for Network monitoring systems & tools?

a. Monitoring tools

b. Performance tools

c. Disk Management tools

d. Diagnostic tools

Answer: Disk Management tools

Self Assessment Question

11. Which one of the following is a passive tool?

a. SmokePing

b. log monitoring

c. Ping

d. MTR

Answer: log monitoring

Self Assessment Question

12. Abbreviation of SNMP is ____________________.

a. Simple Network Management Protocol

b. Similar Network Management Protocol

c. Simple New Management Protocol

d. Simple Network Message Protocol

Answer: Simple Network Management Protocol

Self Assessment Question

13. Circuit Level Gateway Firewalls – relays _____ packets.

a. 1

b. 2

c. 3

d. 4

Answer: 2

Self Assessment Question

14. Abbreviation of IDPS is ____________________.

a. Inter Domain Protocol Suit

b. Intrusion Denial Protocol Suit

c. Intrusion Detection And Prevention System

d. Intrusion Detection And Prevention Solutions

Answer: Intrusion Detection And Prevention System

Self Assessment Question

15. Because IDS and IPS technologies offer many of the same capabilities, administrators can usually disable prevention features in IPS products, causing them to function as IDSs. State whether True or False.

a. True

b. False

Answer: True

Self Assessment Question

16. Which one of the following is not a type of IDPS?

a. Network based

b. Host based

c. Wireless

d. Application

Answer: Application

Self Assessment Question

17. Network-based products are generally capable of stopping malicious mobile code or Trojan horses. State whether True or False.

a. True

b. False

Answer: False

Self Assessment Question

18. ________-based IDPSs are most commonly deployed on publicly accessible servers and servers containing sensitive information.

    a. Network

    b. Host

Answer: Host

Self Assessment Question

19. The IDS stops the attack itself. State whether True or False.

a. True

b. False

Answer: False

Self Assessment Question

20. Signature-based detection can track and understand the state of complex communications. State whether True or False.

a. True

b. False

Answer: False

Self Assessment Question

21. An e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of ______.

a. Virus

b. Worm

c. Malware

d. Trojan Horse

Answer: Malware

Self Assessment Question

22. ___________technologies can also be deployed if organisations desire additional detection capabilities for DoS & DDoS attacks, worms, and other threats.

a. ARP Spoofing

b. Firewall

c. NBA

d. Anomaly based

Answer: NBA

Self Assessment Question

23. A network IDPS should not be placed _____________.

a. Outside firewall

b. Just inside firewall

c. Behind remote access server

d. At Web servers

Answer: At Web servers

Self Assessment Question

24. Disabling can be done via uninstall command in Windows. State whether True or False.

a. True

b. False

Answer: False

Self Assessment Question

25. Limit privileges of the user will ensure the __________ security.

a. Application

b. Physical

c. Logical

Answer: Application

Assignment

1. Explain security infrastructure requirements.
2. What is device based security?
3. What are the threats associated with router and how to protect it?
4. Write a short note on media security.
5. What is system monitoring?
6. Write short notes on monitoring tools and software.
7. What is IDS? Explain with an example.
8. What are the types of IDS?
9. What is IPS used for and how are they different from IPS?
10. Describe the concept of OS and Network Hardening.
11. Explain the methods to provide application security.
12. What are policies, procedures and standards? Explain with an example.
13. Discuss the importance of guidelines in detail.

Document Links

Topic	URL's	Description
Infrastructure Security	https://www.techotopia.com/index.php/IT_Infrastructure_Security	The link describes the concept of infrastructure security.
Media security	http://www.ijatir.org/uploads/136524IJATIR12401-552.pdf	The link explains the role of media security.
Network Monitoring	https://www.solarwinds.com/basics-of-network-monitoring	The link explains the basics of network monitoring.
Intrusion Detection and Prevention system	https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901146	The Link explains the basic concept and the advantages of using IDPS system.
System Hardening	https://techterms.com/definition/systemhardening	The Link explains the requirement of system hardening to make it more secure.
Policies, Standards, Guidelines, and Procedures	http://www.pearsonitcertification.com/articles/article.aspx?p=30287&seqNum=5	The Link explains about the differences between policies and procedures.

Network Infrastructure Security and Connectivity

Video Links

Topic	URL's	Description
Infrastructure security	https://www.youtube.com/watch?v=jaL2t934DN0	The link describe the concept of infrastructure security
Device Security	https://www.youtube.com/watch?v=R9V20FNyyOk	The link explain the device security
Network Monitoring	https://www.youtube.com/watch?v=ccRI8wCzCdg	The link explains the basics of network monitoring
Intrusion Detection and Prevention system	https://www.youtube.com/watch?v=mmt4B60xSj0	The Link explain the basic concept and the advantages of using IDPS system
System Hardening	https://www.youtube.com/watch?v=YSwTfealIV4	The Link explain the requirement of system hardening to make it more secure
Policies, Standards, Guidelines, and Procedures	https://www.youtube.com/watch?v=vX67CpWLFg0	The Link explain about the differences between policies and procedures

E-Book Links

Topic	URL's	Description
Infrastructure security	https://brage.bibsys.no/xmlui//bitstream/id/101192/CSharma2013.pdf	ALL
Device Security	http://www.potaroo.net/t4/pdf/security.pdf	ALL