

Security+ Study Guide

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity

The main function of an Intrusion Prevention System (IPS) is to identify malicious activity, log info about this activity, attempt to block/stop it, and report it

Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host

A proxy is a device that acts on behalf of other(s). In the interest of security, all internal user interaction with the Internet should be controlled through a proxy server. The proxy server should automatically block known malicious sites. The proxy server should cache often-accessed sites to improve performance

Port Address Translation (PAT), is an extension to network address translation (NAT) that **permits multiple devices on a local area network (LAN) to be mapped to a single public IP address**. The goal of PAT is to conserve IP addresses

A signature-based monitoring or detection method relies on a database of signatures or patterns of known malicious or unwanted activity. The strength of a signature-based system is that it can quickly and accurately detect any event from its database of signatures

To establish a TCP connection, the three-way (or 3-step) handshake occurs:

SYN: The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.
SYN-ACK: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B+1.
ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1

An all-in-one appliance, also known as Unified Threat Management (UTM) and Next Generation Firewall (NGFW), is one that provides a good foundation for security. A variety is available; those that you should be familiar with for the exam fall under the categories of providing URL filtering, content inspection, or malware inspection

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments

A subinterface is a division of one physical interface into multiple logical interfaces. Routers commonly employ subinterfaces for a variety of purposes, most common of these are for routing traffic between VLANs. Also, IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Implicit deny is the default response when an explicit allow or deny isn't present

A Hyper-V Virtual Switch implements policy enforcement for security, isolation, and service levels

It is a common and recommended practice to separate voice and data traffic by using VLANs

NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request

Remote Procedure Call (RPC) is a programming interface that allows a remote computer to run programs on a local machine

Quality of Service (QoS) facilitates the deployment of media-rich applications, such as video conferencing and Internet Protocol (IP) telephony, without adversely affecting network throughput

Infrastructure as a Service - a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis (the cloud user patches and maintains the operating systems and the application software)

Software as a Service (SaaS) allows for on-demand online access to specific software applications or suites without having to install it locally

Monitoring-as-a-service (MaaS) is a cloud delivery model that falls under anything as a service (XaaS). MaaS allows for the deployment of monitoring functionalities for several other services and applications within the cloud

Asymmetric vs Symmetric

Symmetric uses the same key to encrypt/decrypt data (sometimes called a secret key or session key)

Asymmetric uses 2 keys in a matched pair to encrypt/decrypt data (only a private key can decrypt information encrypted with a matching public key)

When you are dealing with **integrity** you are using a **hash**

If you are dealing with **confidentiality**, you are using **symmetric algorithm**

If you are dealing with **non-repudiation**, you are using **asymmetric algorithm**

Network Access Control (NAC)

- Evaluates system security status before connecting to the network
- Anti-virus status
- System update level
- Configuration settings
- Software firewall enabled

Name	Type	Algorithm	Size
DES	Symmetric	Block cipher	Block: 64 bits; Key 64 bits (56 + 8 parity)
3DES	Symmetric	Block cipher (used in PGP/GPG)	Block: 64 bits; Key 192 bits (168 + 24 parity)
AES	Symmetric	Rijndael Block cipher (used in PGP/GPG)	Block: 128; Key: 128, 192, 256 bits
Blowfish	Symmetric	Block cipher	Block: 64 bits; Key: variable 32 to 448 bits
Twofish	Symmetric	Block cipher (used in PGP/GPG)	Block: 128 bits; Key: variable 128, 192, 256 bits
CAST-128	Symmetric	Block cipher; used in PGP/GPG	Block: 64 bits; Key: variable 40 to 128
CAST-256	Symmetric	Block cipher; used in PGP/GPG	Block: 128 bits; Key: Variable (128, 160, 192, 224, 256)
RC4	Symmetric	Stream cipher (used in WEP)	Stream; Variable key size (40-2048 bits)
RC5	Symmetric	Block cipher	Block: 32, 64,128 bits; Key: Variable (0 to 2048)
RC6	Symmetric	Block cipher	Block: 128 bits; Key: variable 0 to 2048; (includes integer multiplication and four 4-bit registers, instead of two)
IDEA	Symmetric	Block cipher (used in PGP/GPG)	Block: 64 bits; Key: 128 bits
SAFER+	Symmetric	Block cipher (bluetooth for key derivation)	Block; 128 bits Key:128, 192 and 256 bits
SAFER++	Symmetric	Block cipher (bluetooth for key derivation)	Block:64 bits and 128 bits; Key;64 and 128 bits
RSA	Asymmetric	Key Exchange, Encryption, Digital Signatures; used in PGP/GPG	Large prime numbers; Based on the difficulty of factoring N , a product of two large prime numbers Key: 512-bit to arbitrarily long (1024-2048 considered safe)
Diffie-Hellman	Asymmetric	Key Exchange (used in PGP/GPG)	Based on discrete logarithms Key: 512-bit to arbitrarily long (1024-2048 considered safe)
EI Gamal	Asymmetric	Key Exchange, Encryption, Digital Signatures	Based on discrete logarithms; very slow when used to create digital signatures Key: 256-bit to arbitrarily long (1024-2048 considered safe)
ECC	Asymmetric	Key Exchange, Encryption, Digital Signatures (used in cell phones and wireless devices)	Based on points on an elliptic curve
HMAC	Hash		Variable
MD5	Hash		512-bit block processing / 128 bit digest
SHA-1	Hash	used in PGP/GPG	512-bit processing /160 bit digest
Whirlpool	Hash		512 bit block processing / 512 bit digest

The following should be implemented in order to limit web traffic based on country of origin

- Proxies
- URL Filter
- Firewall

A **Web Application Firewall (WAF)** is a device, server add-on, virtual service, or system filter that defines a strict set of communications for a website and all visitors

Cryptography has 4 primary functions

1. Confidentiality
2. Integrity
3. Authentication
4. Non-repudiation

Confidentiality: Symmetric/Asymmetric

Integrity: Hashing

Authentication: X509 Digital Certificates, password hashes

Stream cipher encrypts data **one bit at a time**

Block cipher encrypts data in **blocks**

A hash is used to establish/maintain data integrity

Mandatory Access Control (MAC)

- Assigned security labels
- Most secure

Role-Based Access Control

- Implement access by job function/responsibility

Rule-Based Access Control

- Operational rules or restrictions to govern access (network devices such as firewalls/routers)

Discretionary Access Control

- Owner establishes privileges to the info they own

Business Continuity Planning (BCP)

- Goal is to maintain business operations with reduced or restricted infrastructure
- Implement policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes
- Business Impact Analysis
- Assessing Risk

Business continuity planning (BCP) is the planning which identifies the organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, whilst maintaining competitive advantage and value system integrity. The logistical plan used in BCP is called a business continuity plan. The intended effect of BCP is to ensure business continuity, which is an ongoing state or methodology governing how business is conducted.

In layman's terms, **BCP is working out how to stay in business in the event of disaster**. Incidents include local incidents like building fires, regional incidents like earthquakes, or national incidents like pandemic illnesses.

Avoid/Remove Single points of failure - Clustering servers, redundant network protocols/devices, redundant power, backups, etc

Properly plan and test your BCP

Continuity of operations- -various measures designed to ensure that the organization continues operating

Disaster Recovery - subset of business continuity

Succession planning-process for identifying and developing internal people to fill key leadership positions

Business Impact Analysis (BIA)

- Identify critical business functions
- Prioritize critical business functions
- Establish a timeframe of critical systems loss
- Estimate tangible and intangible impact
- Assessing Risk
 - o Identify exposed risks to the organization
 - o Identify risks that need to be addressed
 - o Coordinate with BIA

Backups

Full

- Restore only the last backup
- Time consuming to perform
- Fastest method to make a complete restore

Full + Incremental

- Restore the last full backup, then every subsequent incremental

Full + Differential

- Restore the last full backup, then the last differential backup

Recovery time Objective (RTO)

- Acceptable amount of data loss measured in time

A forensic analyst is asked to respond to an ongoing network attack on a server. The correct order in which the forensic analyst should preserve them.

CPU cache

RAM

Swap

Hard drive

Application hardening

- Remove all applications not being used
- Restrict access to the application, provide access only to those who must have it
- Update all applications to the latest patches
- Code-review internally developed applications for security weaknesses
- Proper input validation
- Use encryption for application communications

Trusted OS

- An operating system that meets the government's requirements for security

Steps to Incident Response

1. Preparation setting up systems to detect threats and policies for dealing with them, including identifying roles staff will play in incident response, and creating emergency contact lists
2. Identification identifying what the threat is, and/or the effects it is having on your systems/networks, including keeping records of the time/systems involved/what was observed, and making a full system backup as soon after the intrusion was observed, as possible, to preserve as much information about the attack as you can
3. Containment limiting the effects of an incident by confining the problem to as few systems as possible, freezing the scene so that nothing further happens to the compromised system(s) by disconnecting its network connections and possibly console keyboard
4. Eradication getting rid of whatever the attacker might have compromised by deleting files or doing a complete system reinstall – should err on the side of deleting MORE rather than less in order to restore a system to production, since the intruder may have left very-well disguised Trojan Horse binaries around the system, to be activated once the system is reconnected to the Internet
5. Recovery getting back into business, by putting the system back into normal operations, reconnecting it to the network, restoring from backups if necessary, etc.
6. Follow up if possible tightening security so that the intrusion cannot happen again, determining the “cost” of the intrusion based on staff time/lost data/lost user work time

802,1,X (wireless communication)

Identification

- Process of identifying an entity for authentication
- User Identification Guidelines
- Uniqueness
- Non-descriptive
- Issuance secure
- Most common forms:
 - o User Name, User ID, Account Number

Authentication

- Reconciliation of a user's identity
- Accomplished by challenging the claim about who is accessing the resource
- Authentication systems or methods are based on one or more of these five factors:

Authentication Types Examples

Something you know Password or PIN

Something you have Smart Card, Token, or Device

Something you are Fingerprints or Retinal Pattern



Something you do Keystroke Authentication

Somewhere you are Location

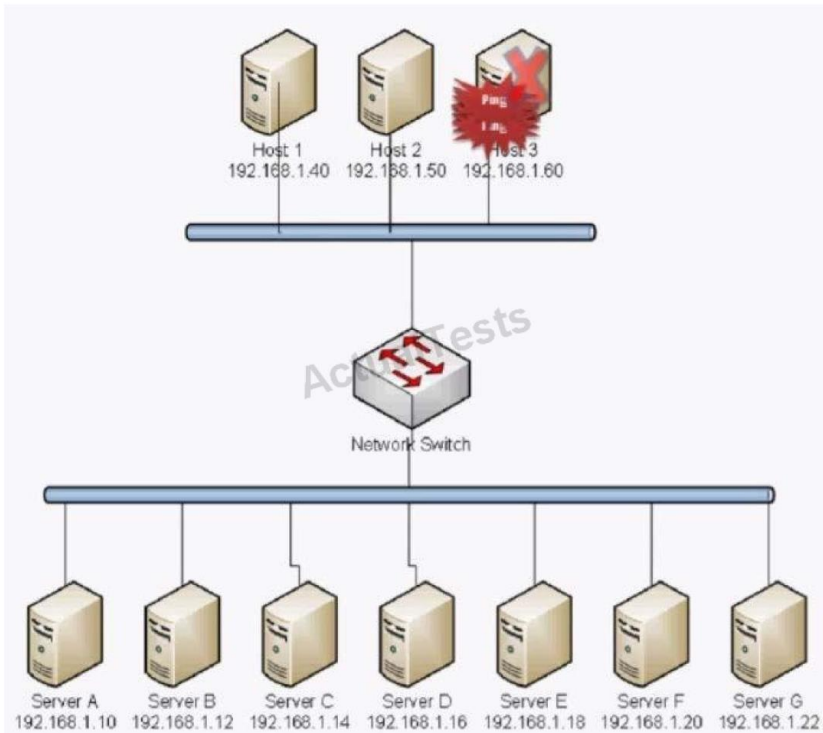
ISA/ Interconnection Security Agreement is an agreement between two organizations that have connected systems. The agreement documents the technical requirements of the connected systems

Service Level Agreement (SLA)

An agreement between you and your company and a service provider

Controls	Company Manager Smart Phone	Data Center Terminal Server
Screen Locks		
Strong Password		
Device Encryption		
Remote Wipe	Screen Locks	Cable Locks
GPS Tracking	Strong Password	Antivirus
Pop-up Blocker	Device Encryption	Host Based Firewall
Cable Locks	Remote Wipe	Proximity Reader
Antivirus	GPS Tracking	Sniffer
Host Based Firewall	Pop-up Blocker	Mentor app
Proximity Reader		
Sniffer		
Mentor app		

Smurf Attack



A **smurf attack** is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address

By disabling IP-directed broadcasts on all routers, we can prevent the smurf attack by blocking the ping requests to broadcast addresses

Floor Plan

Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.

Unsupervised Lab

Office

Data Center

Security Controls

Locking Cabinets	1
Safe	1
CCTV	1
Man Trap	1
Biometric Reader	4
Proximity Badge	2
Cable Locks	6

Reset All

Employee laptop




















Types of Security

security for the shown devices. Not all fields need to be filled. Not all items need to be used.

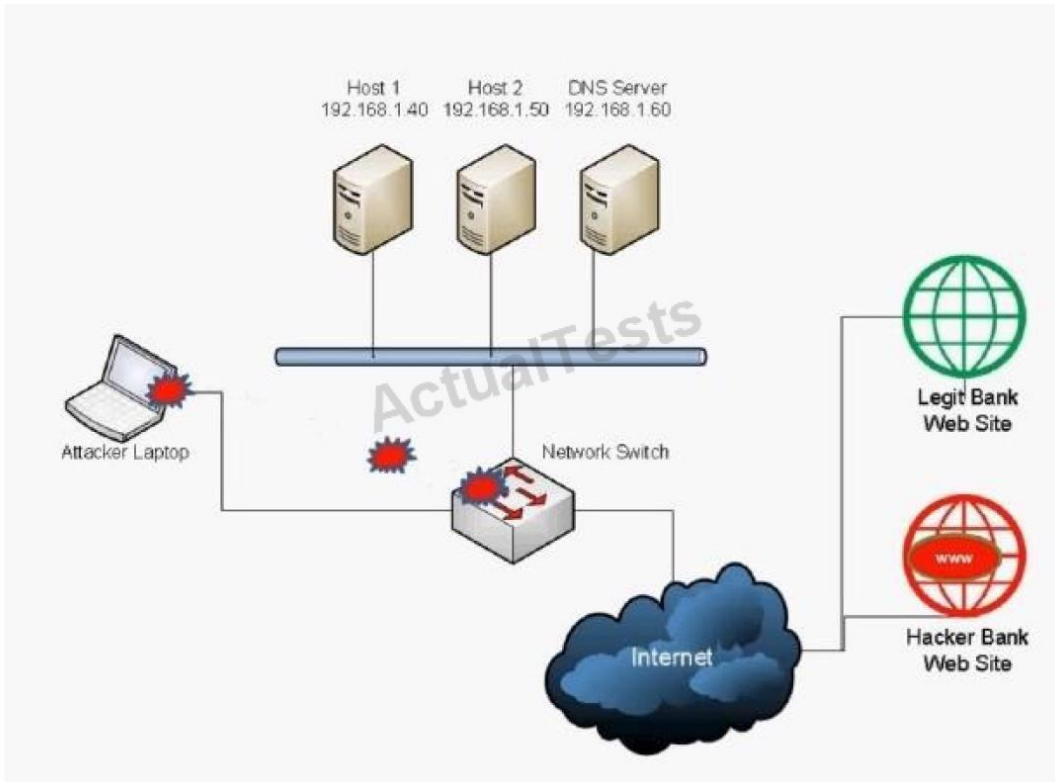
1. GPS Tracking
2. Mantrap
3. Remote wipe
4. Strong Passwords
5. Cable lock
6. Biometrics
7. Proximity Badges
8. FM-200
9. HVAC
10. Device Encryption
11. Antivirus



Mobile Device Security	Server in Data Center Security
1. GPS Tracking	8. FM-200
3. Remote wipe	6. Biometrics
10. Device Encryption	7. Proximity Badges
4. Strong Passwords	2. Mantrap

Attack Vector			Target	Identified Attack
 <p>Attacker gains confidential company information</p>			Targeted CEO and board members	<input type="text" value="SPEAR PHISHING"/>
 <p>Attacker posts link to fake AV software</p>	  <p>Multiple social networks</p> 		Broad set of victims	<input type="text" value="HOAX"/>
 <p>Attacker collecting credit card details</p>			Phone-based victim	<input type="text" value="VISHING"/>
 <p>Attacker mass-mails product information to parties that have already opted out of receiving advertisements</p>			Broad set of recipients	<input type="text" value="PHISHING"/>
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>			 Fraudulent site  Legitimate site Victims	<input type="text" value="PHARMING"/>

DNS Spoofing/ARP attack



The hacker has a laptop connected to the network. The hacker is redirecting bank web site users to the hacker bank web site instead of the legit bank web site. This can be done using two methods: DNS Spoofing and ARP Attack (ARP Poisoning) **ARP is not used on IPv6 networks** DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer).

If the application is running on a client computer, this would be a client side attack. Attacking a service or application on a server would be a server side attack

Risk Formulas

Single Loss Expectancy (SLE)

$$SLE = AV \times AF$$

Annualized Loss Expectancy (ALE)

$$ALE = SLE \times ARO$$



Security Assertion Markup Language (SAML) Open standard format centered on XML. It is used for supporting the exchange of authentication and authorization details between systems, services, and devices

LDAP communications are encrypted with SSL/TLS

Allows subjects and applications to interact with the directory

- Interoperability agreements
 - Service-level Agreement (SLA)
 - This agreement clearly defines what services are to be provided to the client, and what support, if any, will be provided.
 - Business partner agreement (BPA)
 - This agreement defines how a partnership between business entities will be conducted, and what exactly is expected of each entity in terms of services, finances, and security.
 - Memorandum of understanding (MOU)
 - This type of agreement is usually not legally binding and typically does not involve courts or money. They are less formal and are typically enacted as a way to express a desire for all parties to achieve the same goal in the agreed-upon manner.
 - Interconnection security agreement (ISA)
 - This type of agreement is geared toward the information systems of partnered entities to ensure that the use of inter-organizational technology meets a certain security standard.

Malware

- Adware
 - typically “harmless” as it just displays ads for products or wanting the user to click on a banner
 - the banner ads will usually appear as browser window popups
 - can be a sign of a larger infection
- Virus
 - Malware that requires a program to piggyback on.
 - Needs the program to execute for the virus to execute its payload
 - Needs some type of user interaction.
- Spyware
 - Malware that is intended to report information on a user’s habits. an invasion of privacy.
 - Spyware can also be targeting a specific set of files or information such as browsing history to financial information
- Trojan
 - Malware posing as a legitimate program
 - Trojans do not replicate or attach to other files
 - Composed of a suite of exploits allowing the attacker to remotely control and/or monitor a pc
- Rootkits
 - Malware that is intended to take full or partial control of a pc at the lowest system levels without authentication
 - A service that listen on a specific port
 - Microsoft Protection Center on [RootKits](#)
- Logic bomb
 - Malware that sits dormant until it is triggered by a specific action or event
 - When the trigger is reached logic bomb executes whatever it was programmed to do
- Botnets
 - A set of computers that have been infected by a control program acting at the will of the attacker to mount various attacks
 - Once infected the pc is considered a **zombie** or **drone**
 - Hard to detect since rootkits can “hook” themselves onto various system files evading detection by reporting to be a legitimate process
 - Various types of rootkits depending on where they reside
- Backdoors
 - Programs that enable attacker to enter at any time
 - Large botnets can be used to issue DDoS attacks
 - Mine for data
 - Send spam emails
- Ransomware
 - Malware that will infect a pc restricting the user access to the files or information contained on it
 - Encryption can be used to encrypt documents
 - Money must be paid to the attackers to receive the private key to decrypt the data
- Polymorphic malware
 - A virus that encrypts itself while each time it runs alters itself and encrypts again
 - Paired with a decryption module
 - The virus is changing its code and encryption
 - It is difficult for AV companies to write definitions for them
- Armored virus
 - These viruses can be large in size because they include *garbage code* to make themselves hard to identify and for AV companies to properly reverse engineer them to write definitions
- Worms
 - These are not mentioned but worth noting

- Worms do not require a program to piggyback on or a separate program to execute. they simply propagate
- some worms can contain a payload that can open up backdoors allowing the attacker in
- many times a worm spreading is enough to slow network traffic

Mitigation and Deterrents

- Remove the GUI:
 - `yum grouplist`
 - `yum groupremove "GNOME Desktop Environment"`
 - `vi /etc/inittab`
- Change the run level to text only `id:3:initdefault:`
- Examine services: `service --status-all chkconfig --list netstat -tulpn`
- Remove/Disable Services `yum erase inetd xinetd telnet-server chkconfig inetd off`
- Monitoring system logs
 - Event logs - computer performance, etc.
 - Audit logs - time stamps, etc.
 - Security logs - logon events, etc.
 - Access logs - key fob events, etc.
 - could also consider monitoring system performance logs
- Hardening
 - Disabling unnecessary services
 - Protecting management interfaces and applications
 - if only administering by SSH, disable the web config
 - Password protection
 - Disabling unnecessary accounts
 - user, computer and service accounts
- Network security (keeping those who shouldn't be on your network off your network)
 - MAC limiting (port security) and filtering (kiosk or public access drops unknown macs)
 - 802.1x (RADIUS)
 - Disabling unused interfaces and unused application service ports
 - Rogue machine detection (BYOD)
- Security posture (the position a company takes on securing all areas of its business)
 - Initial baseline configuration
 - to help with creating and maintaining a baseline user template, images, GPOs
 - Continuous security monitoring
 - whenever changes are made to the network a review of the security should be done
 - Remediation
- Reporting (use along with audits and logs)
 - Alarms -> used to bring attention to a fault in the system
 - Alerts -> used to communicate that a condition has occurred and needs attention
 - Trends -> performance or event across a specified time frame
 - good reporting can help to determine trends
- Detection controls (monitor a situation or activity) vs. prevention controls (monitor AND react to situations)
 - to determine whether you need detection or prevention controls all boils down to risk.
 - if a situation has a low impact then detection is appropriate. if a situation has a high impact then prevention is ideal

A network-based DLP (data loss prevention) device This device normally sits on the perimeter of the network and can be configured to analyze traffic for confidential information and prevent it from going outside the network. DLP devices can also be storage-based and endpoint-based

Performance monitoring software can be used to create a baseline and monitor for any changes to that baseline. An example of this would be the Performance console window within Windows Server. (It is commonly referred to as Performance Monitor.)

Baseline reporting A Security Posture Assessment (SPA) is used to find out the baseline security of an application, a system, or a network, as long as the application (or system or network) already exists. By checking past results and comparing them with current (and future) results, a security professional can see whether an application is secure, or has a “secure posture.” Some applications come with built-in baseline reporting tools, which allow you to tell whether a system is compliant and secure. The other three answers don’t (by definition) associate with the “security posture” of an application.

Some **network mapping programs** such as AirMagnet require that a network adapter be placed in promiscuous mode. This is when the network adapter captures all packets that it has access to regardless of the destination of those packets. Some protocol analyzers (for example, Wireshark) also require that a network adapter be placed in promiscuous mode.

Patch management is an example of verifying any new changes in software on a test system (or live systems for that matter.) Verifying the changes (testing) is the second step of the standard patch management strategy.

Physical security and environmental controls

- **Environmental controls**
 - HVAC
 - Fire suppression
 - EMI shielding
 - Hot and cold aisles
 - Environmental monitoring
 - Temperature and humidity controls
- **Physical security**
 - Hardware locks
 - Mantraps
 - Video surveillance
 - Fencing
 - Proximity readers
 - Access list
 - Proper lighting
 - Signs
 - Guards
 - Barricades
 - Biometrics
 - Protected distribution (cabling)
 - Alarms
 - Motion detection

- Control types
 - Deterrent
 - Discourage attackers from attacking in the first place
 - Preventive
 - stop an attack before it can cause damage
 - Detective
 - Identify attacks in progress
 - Compensation
 - support other physical controls
 - Technical
 - Hardware or software that aid in protecting physical assets
 - Administrative
 - Leverage security policies and are used to train personnel

Various types of attacks.

- Man-in-the-middle
 - a form of eavesdropping where the attacker makes an independent connection between two victims and relays information between the two as if they were directly connected
- DDoS
 - a type of attack where multiple systems are used to consume the resources of a particular system so that it no longer can respond to legitimate requests
- DoS
 - same as DDoS but used with a single pc
 - UDP floods
 - SYN floods
 - Reflected DoS attack
- Replay
 - an attack where information about a particular session is captured and then used at a later time to gain unauthorized access to a particular resource.
- Smurf attack
 - also called ICMP flood it is when large amounts of ICMP ping packets are sent to a target via broadcast/multicast IP on the network. This causes all clients to answer to the server..
 - these are not really effective with today's networking equipment
- Fraggle attack
 - Similar to Smurf, but using other UDP ports to conduct to DoS.
- ARP Poisoning
 - Interception /modification of the Address Resolution Protocol causing misdirection of traffic.
 - IP addresses are not correctly mapped to the MAC address of the original recipient.
 - Often used to set the conditions for a Man in the Middle Attack.
- Spoofing
 - human or software based attack where the goal is to impersonate or pretend to be someone else for the purpose of identity concealment
 - can spoof IPs, MAC, email
- Spam
 - unsolicited email
- Phishing
 - email based social engineering attack where the email is claimed to be sent directly to the victim and requests personal information or money to be sent to the attacker
- Spim
 - spam that is sent through instant messaging

-
- Vishing
 - also called voice phishing, it is done through phone systems and VoIP system. can be effective since people can be more trusting when speaking in real time
- Spear phishing
 - targeted phishing
- Xmas Tree attack
 - Packets with all Flags turned-on resulting in additional server side processing overhead.
 - A mass spectrum port/protocol scanning attack to determine vulnerabilities.
- Pharming
 - An attack where a request for a website is redirected to a similar website that looks the same but is really fake.
 - website is usually an e-commerce site
- Privilege escalation
- Malicious insider threat
- DNS poisoning and ARP poisoning
- Transitive access
 - giving access to resources without the need to authenticate.
 - individuals having transitive access can be saved in a log file
 - an attacker who gains access to this file can add himself and the exploit the trust relationship
- Client-side attacks
- Password attacks
- Brute force
 - This type of attack is used when it is not possible to take advantage of other weaknesses that would be easier
 - It consists of systematically checking all possible combinations until the correct one is found
 - the key length determines the practical feasibility of performing a brute force attack since longer keys take an exponentially longer time to crack than shorter ones
 - the use of GPU's and ASICs (application-specific integrated circuit) are often used as the hardware for performing brute force attacks
 - brute force attacks are commonly performed offline since countermeasures such as password lockout policies are typically implemented to protects against these attacks
- Dictionary attacks
 - this attack involves using every word in the dictionary as either the password into a system or the key to decrypt a message or document
 - this type of attack works because so many people use ordinary words as passwords

dictionary attacks are very successful against single-word passwords, less successful against multiple-word passphrases, and unsuccessful against randomly generated letters/numerals

Scarcity, in the area of social psychology, works much like scarcity in the area of economics. Simply put, humans place a higher value on an object that is scarce, and a lower value on those that are abundant.

Bluejacking is the sending of **unsolicited messages over Bluetooth to Bluetooth-enabled** devices such as mobile phones

Bluesnarfing is the **theft of information** from a wireless device through a Bluetooth connection

A **sniffer (packet sniffer)** is a tool that **intercepts data flowing in a network**

Network Administration Principles

- Rule-based management
 - The use of operational rules or restrictions to govern the security of an organization's infrastructure. A security policy used to determine how employees can access the Internet and other network resources is an example of rule-based management.
- Firewall rules
 - Used to control traffic flowing through a firewall device.
 - Inbound rules: Define the action to be performed by the firewall on the data that enters the system from another system.
 - Outbound rules: Define the action to be performed by the firewall on the data that flows out of the system.
- VLAN management
 - Can be complex. Most organizations will keep track of VLAN configuration using diagrams and documentation.
- Secure router configuration
 - Ensuring that all routers on the network are properly secured to protect your network from attacks and can also prevent routing loops.
- Access control lists
 - Networking ACLs
 - On routers and switches, rules that are applied to port numbers or IP addresses to control both inbound and outbound traffic
 - Filesystem ACLs
 - A table that contains entries that specify individual user or group rights to specific system objects such as programs, processes or files.
- Port security
 - Disable unnecessary services.
 - Close ports that are by default open or have limited functionality.
 - Regularly applying the appropriate patches.
 - Hiding responses from ports that indicate their status and allow access to pre-configured connections only.
- 802.1x
 - IEEE standard used to provide a port-based authentication mechanism for wireless communications. It uses the Extensible Authentication Protocol (EAP) to provide user authentication against a directory service.
- Flood guards
 - Used to protect resources from flooding attacks, such as Distributed Denial of Service (DDoS) attacks.
 - Detectors are placed throughout the network and will react and apply the appropriate mitigation techniques when an attack occurs.
- Loop protection
 - Occurs when one or more pathways exist between the endpoints in a network and packets get forwarded over and over again.
 - Loop protection is done by applying proper router configuration and manufacturer recommended configurations.
- Implicit deny
 - Principle of denying all traffic unless it is specifically allowed.
- Network separation
 - Splitting your network into two or more logically separated networks in order to separate critical network functions from non-critical network functions.

- It can also prevent intruders from getting to other systems, and helps enforce access control efforts.
- Log analysis
 - Logs must be regularly monitored and analyzed to detect any unauthorized intrusion attempts, and to assess any data leaks and insider threats.
- Unified threat management
 - A system that centralized various security techniques like firewall, anti-malware, network intrusion prevention, URL filtering, content inspection, malware inspection, etc., into a single appliance.
 - They usually include a single management interface.
 - A downside to UTM is can become a single point of failure that could affect an entire network.
- WAP (Wireless Applications Protocol)
 - Low resource protocol developed for use in (cellular) mobile devices.
 - Uses WAP-TLS (WTLS) to add additional surety.
 - 64/128 Bit (actually 20/104 bit for data because uses 24 -bit Initialization Vectors).
- WPA (Wi-Fi Protected Access)
 - Provides improved data encryption through the Temporal Key Integrity Protocol (TKIP), which is a security protocol created by the IEEE 802.11i task group to replace WEP.
 - It is combined with the existing WEP encryption to provide a 128-bit encryption key that fixes the key length issues of WEP
- WPA2
 - In addition to TKIP, WPA2 adds Advanced Encryption Standard (AES) encryption for even greater security and to replace TKIP. It provides 128-bit encryption
- WEP (Wired Equivalent Privacy)
 - Provides 64-bit, 128-bit, and 256-bit encryption using the Rivest Cipher 4 (RC4) algorithm.
 - WEP is considered a security hazard and had been depreciated due to vulnerabilities to initialization vector (IV) attacks
- EAP (Extensible Authentication Protocol)
 - A framework that allows clients and servers to authenticate with each other using one of a variety of plug-ins.
 - It can be used with a wide range of current authentication methods, and is extensible for use with future authentication methods.
- PEAP
 - Open standard implementation of EAP, developed by a coalition made up of Cisco System, Microsoft, and RSA Security
- LEAP
 - Cisco System's proprietary implementation of EAP. Uses MS-CHAP, which is not considered secure
- MAC filtering
 - The technique of allowing or denying devices with certain MAC addresses to connect to a network. A whitelist is used to specify which MAC addresses are granted access.
 - A blacklist is used to specify which MAC addresses are explicitly blocked.
- Disable SSID broadcast
- TKIP (Temporal Key Integrity Protocol)
 - Strap-on which adds additional security to WEP utilizing existing WEP hardware.
- CCMP
 - Counter Mode Cipher Block Chaining Message Authentication Code Protocol or Counter Mode CBC-MAC Protocol
 - Adds AES encryption to WEP to provide greater security; requires new hardware.
- Antenna placement
 - The radio frequency range of each access point should not extend beyond the physical boundaries of the organization's facilities

- Power level controls
 - Used to reduce your wireless LAN transmitter power. Also helps to minimize power consumption within the wireless network
- Captive portals
 - A technique that requires a client attempting to connect to the Internet to authenticate through a web page.
 - Commonly used by free and / or public Wi-Fi hotspots in order to get the user to agree to an acceptable use policy before they begin using the service
- Antenna types
 - Omni-directional
 - Directional
 - Yagi
 - A directional antenna used primarily in radio, but also used in long distance wireless networking to extend the range of hotspots
- Site surveys
 - the collection of information on a location, including access routes, potential obstacles and best positioning of materials for the purpose of constructing a wireless network that provides quality coverage and bandwidth while at the same time being conscious of security protocols and requirements
 -
- VPN (over open wireless)

Used to provide authentication techniques and encrypt your data in transit over the network even when using an insecure wireless hotspot

OSI Layers

Protocols

All	Application	FTP/TFTP/SNMP/SMTP/Telnet/HTTP
People	Presentation	
Seem	Session	
To	Transport	TCP/UDP/SSL/SPX
Need	Network	IP/ICMP/IGMP/RIP/OSPF/IPX
Data	Data Link	ARP/RARP/PPP/SLIP/Ethernet/Token Ring/Wireless Ethernet
Processing	Physical	

Port Numbers

20-21	FTP (File Transfer Protocol)
22	SSH/SCP/SFTP (Secure Shell/Secure Copy/Secure File Transfer Protocol)
23	Telnet (Legacy protocol, transmits in clear text)
25	SMTP (Simple Mail Transfer Protocol)
49	TACACS+ (Terminal Access Controller Access Control System)
53	DNS (Domain Name Service)
67/68	DHCP (Dynamic host Configuration Protocol)
69	TFTP (Trivial File Transfer Protocol)
80	HTTP (Hyper Text Transfer Protocol)
88	Kerberos
110	POP3 (Post Office Protocol)
119	NNTP
137-139	NetBIOS (Network Basic Input/Output System)
143	IMAP4 (Internet Access Message Protocol)
161-162	SNMP (Simple Network Management Protocol)
389	LDAP (Lightweight Directory Access Protocol)
443	HTTPS (Hyper Text Transfer Protocol Secure)
445	TCP SMB
465	SMTP/SSL
514	Sys Log
636	LDAP (Lightweight Access Directory Protocol/over SSL)
989/990	FTPS
993	IMAP4/SSL
1433	Microsoft SQL Server
1701	L2TP (Layer 2 Tunneling Protocol)
1723	PPTP (Point to Point Tunneling Protocol)
3306	MYSQL
3389	Terminal Services

Cryptography

Symmetric

23BRAIDS

Twofish

3DES

Blowfish

RC5

AES

IDEA

DES

SAFER

Asymmetric

DEREK

Diffie-Hellman

ECC

RSA

El Gamal

Knapsack

Hash

M@SHH!T

MD5

SHA

HMAC

Haval

Tiger

Antiquated protocols

Are protocols that were not specifically designed with security as a primary focus. Many of the protocols commonly used over the internet or within a private network are of this ilk. Many protocols commonly users rely on daily, such as email, the web, and ftp, were developed over 30 years ago and have little to no security built in to them. Unfortunately, these antiquated protocols often cannot be replaced with secure alternatives due to lack of interoperability or backwards compatibility of the secure protocols with legacy services and clients. Therefore, you must be aware of the limitation of antiquated protocols and tak precautions against potential security breaches.

SMTP, POP2, IMAP4, FTP

TCP/IP hijacking

TCP session hijacking is when a hacker takes over a TCP session between two machines. Since most authentication only occurs at the start of a TCP session, this allows the hacker to gain access to a machine.

A popular method is using source-routed IP packets. This allows a hacker at point A on the network to participate in a conversation between B and C by encouraging the IP packets to pass through its machine.

If source-routing is turned off, the hacker can use "blind" hijacking, whereby it guesses the responses of the two machines. Thus, the hacker can send a command, but can never see the response. However, a common command would be to set a password allowing access from somewhere else on the net.

Null sessions

A **null session** is an anonymous connection to a freely accessible [network share](#) called [IPC\\$](#) on [Windows](#)-based [servers^{\[1\]}](#). It allows immediate [read and write access](#) with [Windows NT/2000](#) and read-access with [Windows XP](#) and [2003](#).

A null session is how Windows represents an anonymous user. To understand how it is used, imagine the sort of code you have to write in a server to deal with authenticated clients. After authenticating a client using Kerberos (WhatIsKerberos), say, your server receives a token for that client that contains group SIDs, and you can use that token to perform access checks against ACL'd resources (WhatIsACLBasedSecurity). For instance, given the client's token it's quite easy to check whether that client should be granted write access to a file. We can simply impersonate the client (WhatIsImpersonation) and try to open the file for writing. The operating system will compare the DACL on the file with the client's token (that we're impersonating) to make this determination. The administrator can control access to files by editing their ACLs. But what if you also service anonymous requests—that is, those for which you won't get any token for the client at all? It's impossible to impersonate a client for whom you don't have a token.

This is where the null session comes in. It's a logon session that represents anonymous users, and here's how you use it. In your code that services anonymous requests, grab a token to represent the anonymous logon by calling the Win32 API `ImpersonateAnonymousToken` (see [HowToDealWithUnauthenticatedClients](#) for sample code). This is a null session token, and it has a user SID of ANONYMOUS LOGON and a single group SID, Everyone1. One group SID conspicuously not present is Authenticated Users (all tokens other than null sessions or guest logons have this special SID, in case you were wondering). This is the key to using the null session. By granting access to Everyone, you're granting access to all users, both authenticated and anonymous. By granting access only to Authenticated Users, you're implicitly denying anonymous users. This simple model allows an administrator to use ACLs to control access to all users, both authenticated and anonymous.

Spoofing

In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage

Man-in-the-middle attack and internet protocol spoofing

An example from cryptography is the man-in-the-middle attack, in which an attacker spoofs Alice into believing the attacker is Bob, and spoofs Bob into believing the attacker is Alice, thus gaining access to all messages in both directions without the trouble of any cryptanalytic effort.

The attacker must monitor the packets sent from Alice to Bob and then guess the sequence number of the packets. Then the attacker knocks out Alice with a SYN attack and injects his own packets, claiming to have the address of Alice. Alice's firewall can defend against some spoof attacks when it has been configured with knowledge of all the IP addresses connected to each of its interfaces. It can then detect a spoofed packet if it arrives at an interface that is not known to be connected to the IP address.

Many carelessly designed protocols are subject to spoof attacks, including many of those used on the Internet. See Internet protocol spoofing

[edit] URL spoofing and phishing

Another kind of spoofing is "webpage spoofing," also known as phishing. In this attack, a legitimate web page such as a bank's site is reproduced in "look and feel" on another server under control of the attacker. The main intent is to fool the users into thinking that they are connected to a trusted site, for instance to harvest user names and passwords.

This attack is often performed with the aid of URL spoofing, which exploits web browser bugs in order to display incorrect URLs in the browsers location bar; or with DNS cache poisoning in order to direct the user away from the legitimate site and to the fake one. Once the user puts in their password, the attack-code reports a password error, then redirects the user back to the legitimate site.

[edit] Referrer spoofing

Some websites, especially pornographic paysites, allow access to their materials only from certain approved (login-) pages. This is enforced by checking the Referer header of the HTTP request. This referrer header however can be changed (known as "Referer spoofing" or "Ref-tar spoofing"), allowing users to gain unauthorized access to the materials.

[edit] Poisoning of file-sharing networks

"Spoofing" can also refer to copyright holders placing distorted or unlistenable versions of works on file-sharing networks, to discourage downloading from these sources.

[edit] Caller ID spoofing

Main article: Caller ID spoofing

In public telephone networks, it has for a long while been possible to find out who is calling you by looking at the Caller ID information that is transmitted with the call. There are technologies that transmit this information on landlines, on cellphones and also with VoIP. Unfortunately, there are now technologies (especially associated with VoIP) that allow callers to lie about their identity, and present false names and numbers, which could of course be used as a tool to defraud or harass. Because there are services and gateways that interconnect VoIP with other public phone networks, these false Caller IDs can be transmitted to any phone on the planet, which makes the whole Caller ID information now next to useless. Due to the distributed geographic nature of the Internet, VoIP calls can be generated in a different country to the receiver, which means that it is very difficult to have a legal framework to control those who would use fake Caller IDs as part of a scam.

[edit] E-mail address spoofing

Main article: E-mail spoofing

The sender information shown in e-mails (the "From" field) can be spoofed easily. This technique is commonly used by spammers to hide the origin of their e-mails and leads to problems such as misdirected bounces (i.e. e-mail spam backscatter).

E-mail address spoofing is done in quite the same way as writing a forged return address using snail mail. As long as the letter fits the protocol, (ie. stamp, postal code) the SMTP protocol will send the message. It can be done using a mail server with telnet.

Man-in-the-middle

the man-in-the-middle attack (often abbreviated MITM), or bucket-brigade attack, or sometimes Janus attack, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle).

A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, SSL authenticates the server using a mutually trusted certification authority.

Replay

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

DOS & DDOS

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used with regards to computer networks, but is not limited to this field, for example, it is also used in reference to CPU resource management. [1]

One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Denial-of-service attacks are considered violations of the IAB's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet Service Providers. They also commonly constitute violations of the laws of individual nations.[2]

Domain Name Kiting

Domain tasting is the practice of a domain name registrant using the five-day "grace period" (the Add Grace Period or AGP) at the beginning of the registration of an ICANN-regulated second-level domain to test the marketability of the domain. During this period, when a registration must be fully refunded by the domain name registry, a cost-benefit analysis is conducted by the registrant on the viability of deriving income from advertisements being placed on the domain's website.

Domains that are deemed "successes" and retained in a registrant's portfolio often represent domains that were previously used and have since expired, misspellings of other popular sites, or generic terms that may receive type-in traffic. These domains are usually still active in search engines and other hyperlinks and therefore receive enough traffic such that advertising revenue exceeds the cost of the registration. The registrant may also derive revenue from eventual sale of the domain, at a premium, to a third party

DNS poisoning

DNS cache poisoning is a maliciously created or unintended situation that provides data to a caching name server that did not originate from authoritative Domain Name System (DNS) sources. This can happen through improper software design, misconfiguration of name servers, and maliciously designed scenarios exploiting the traditionally open architecture of the DNS system. Once a DNS server has received such non-authentic data and caches it for future performance increase, it is considered poisoned, supplying the non-authentic data to the clients of the server.

A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer.

ARP poisoning

Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP Spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The attack can only be used on networks that actually make use of ARP and not another method of address resolution.

The principle of ARP spoofing is to send fake, or "spoofed", ARP messages to an Ethernet LAN. Generally, the aim is to associate the attacker's MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead. The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The attacker could also launch a denial-of-service attack against a victim by associating a nonexistent MAC address to the IP address of the victim's default gateway.

ARP spoofing attacks can be run from a compromised host, or from an attacker's machine that is connected directly to the target Ethernet segment.

DMZ

In computer security, a DMZ, or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The term is normally referred to as a DMZ by IT professionals. It is sometimes referred to as a Perimeter Network. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

NAT

In computer networking, network address translation (NAT) is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another.

Most often today, NAT is used in conjunction with network masquerading (or IP masquerading) which is a technique that hides an entire address space, usually consisting of private network addresses (RFC 1918), behind a single IP address in another, often public address space. This mechanism is implemented in a routing device that uses stateful translation tables to map the "hidden" addresses into a single address and then rewrites the outgoing Internet Protocol (IP) packets on exit so that they appear to originate from the router. In the reverse communications path, responses are mapped back to the originating IP address using the rules ("state") stored in the translation tables. The translation table rules established in this fashion are flushed after a short period without new traffic refreshing their state.

Network interconnections

NAC

Network Access Control (NAC) is an approach to computer network security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.[1][2]

Network Access Control (NAC) is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to a network nodes by devices when they initially attempt to access the network.[citation needed] NAC might integrate the automatic remediation process (fixing non-compliant nodes before allowing access) into the network systems, allowing the network infrastructure such as routers, switches and firewalls to work together with back office servers and end user computing equipment to ensure the information system is operating securely before interoperability is allowed.

Network Access Control aims to do exactly what the name implies—control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

"NAC's roots trace back to the trusted computing movement. In this context an open-architecture was created as an alternative to proprietary NAC initiatives. TNC-WG aims at enabling network operators to provide endpoint integrity at every network connection, thus enabling interoperability among multi-vendor network endpoints."[3]

Initially 802.1x was also thought of as NAC. Some still consider 802.1x as the most simple form of NAC, but most people think of NAC as something more.

In plain English

When a computer connects to a computer network, it is not permitted to access anything unless it complies with a set standard, including anti-virus protection level, system update level and configuration. While the computer is being checked by a pre-installed software agent, it can only access resources that can remediate (resolve or update) any

issues. Once the standard is met, the computer is able to access network resources and the Internet, within the policies defined by the NAC system.

Subnetting

A subnetwork, or subnet, is a logically visible, distinctly addressed part of a single Internet Protocol network.[1] The process of subnetting is the division of a computer network into groups of computers that have a common, designated IP address routing prefix.

Subnetting breaks a network into smaller realms that may use existing address space more efficiently, and, when physically separated, may prevent excessive rates of Ethernet packet collision in a larger network. The subnets may be arranged logically in a hierarchical architecture, partitioning the organization's network address space (see also Autonomous System) into a tree-like routing structure. Routers are used to interchange traffic between subnetworks and constitute logical or physical borders between the subnets. They manage traffic between subnets based on the high-order bit sequence (routing prefix) of the addresses.

Telephony

In telecommunication, telephony (pronounced /tə'liːfəni/ or teh-LEH-fuh-nee) encompasses the general use of equipment to provide voice communication over distances, specifically by connecting telephones to each other.

NIDS

A Network Intrusion Detection System (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic.

A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. If, for example, a large number of TCP connection requests to a very large number of different ports are observed, one could assume that there is someone conducting a port scan of some or all of the computer(s) in the network. It also (mostly) tries to detect incoming shellcodes in the same manner that an ordinary intrusion detection system does.

A NIDS is not limited to inspecting incoming network traffic only. Often valuable information about an ongoing intrusion can be learned from outgoing or local traffic as well. Some attacks might even be staged from the inside of the monitored network or network segment, and are therefore not regarded as incoming traffic at all.

Often, network intrusion detection systems work with other systems as well. They can for example update some firewalls' blacklist with the IP addresses of computers used by (suspected) crackers[citation needed].

Certain DISA documentation, such as the Network STIG, uses the term NID to distinguish an internal IDS instance from its outward-facing counterpart

NIPS

An Intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. Network-based IPS, for example, may operate in-line to monitor all network traffic for malicious code or attacks . When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. Intrusion prevention technology is considered by some to be an extension of intrusion detection (IDS) technology .

Intrusion prevention systems evolved in the late 1990s to resolve ambiguities in passive network monitoring by placing detection systems in-line. Early IPS were IDS that were able to implement prevention commands to firewalls and access control changes to routers. This technique fell short operationally for it created a race condition between the IDS and the exploit as it passed through the control mechanism. Inline IPS can be seen as an improvement upon firewall technologies, IPS can make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done. However, in order to improve performance and accuracy of classification mapping, most IPS use destination port in their signature format. As intrusion prevention systems were originally a literal extension of intrusion detection systems, they continue to be related.

Intrusion prevention systems may also serve secondarily at the host level to deny potentially malicious activity. There are advantages and disadvantages to host-based IPS compared with network-based IPS. In many cases, the technologies are thought to be complementary.

An Intrusion Prevention system must also be a very good Intrusion Detection system to enable a low rate of false positives. Some IPS systems can also prevent yet to be discovered attacks, such as those caused by a buffer overflow.

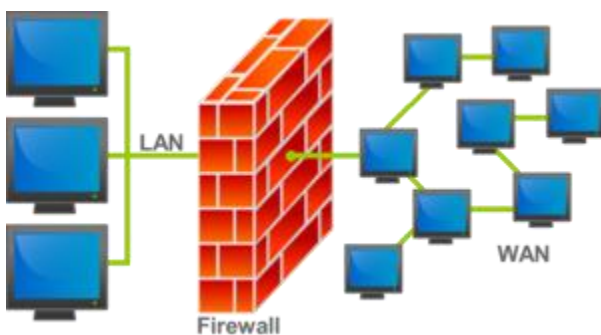
Firewalls

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer based application upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

1. Packet filter: Packet filtering inspects each packet passing through the network and accepts or rejects it based on user-defined rules. Although difficult to configure, it is fairly effective and mostly transparent to its users. It is susceptible to IP spoofing.
2. Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
3. Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
4. Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.



Proxy servers

In computer networks, a proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it 'caches' responses from the remote server, and returns subsequent requests for the same content directly.

A proxy server has many potential purposes, including:

To keep machines behind it anonymous (mainly for security).[1]

To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.[2]

To apply access policy to network services or content, e.g. to block undesired sites.

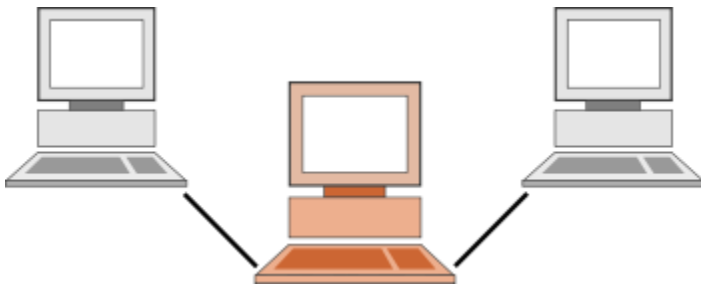
To log / audit usage, i.e. to provide company employee Internet usage reporting.

To bypass security/ parental controls.

To scan transmitted content for malware before delivery.

To scan outbound content, e.g., for data leak protection.

To circumvent regional restrictions.



Honeypot

In computer terminology, a honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers.

Internet content filters

Content-control software, also known as censorware or web filtering software, is a term for software designed and optimized for controlling what content is permitted to a reader, especially when it is used to restrict material delivered over the Web. Content-control software determines what content will be available.

The restrictions can be applied at various levels: a government can attempt to apply them nationwide (see internet censorship), or they can, for example, be applied by an ISP to its clients, by an employer to its personnel, by a school to its students, by a library to its visitors, by a parent to a child's computer, or by an individual user to his or her own computer.

The motive is often to prevent persons from viewing content which the computer's owner(s) or other authorities may consider objectionable; when imposed without the consent of the user, content control can constitute censorship. Some content-control software includes time control functions that empowers parents to set the amount of time that child may spend accessing the Internet or playing games or other computer activities.

In some countries, such software is ubiquitous. In Cuba, if a computer user at a government controlled internet cafe types certain words, the word processor or browser is automatically closed, and a "state security" warning is given.[1]



Protocol analyzers

A packet analyzer (also known as a network analyzer, protocol analyzer or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network.[1] As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.

Privilege escalation

Privilege escalation is the act of exploiting a bug or design flaw in a software application to gain access to resources which normally would have been protected from an application or user. The result is that the application performs actions with more privileges than intended by the application developer or system administrator.

Weak passwords

As with any security measure, passwords vary in effectiveness (i.e., strength); some are weaker than others. For example, the difference in weakness between a dictionary word and a word with obfuscation (i.e., letters in the password are substituted by, say, numbers — a common approach) may cost a password cracking device a few more seconds — this adds little strength. The examples below illustrate various ways weak passwords might be constructed, all of which are based on simple patterns which result in extremely low entropy:[4]

Default passwords (as supplied by the system vendor and meant to be changed at installation time): password, default, admin, guest, etc. All are typically very easy to discover.

Dictionary words: chameleon, RedSox, sandbags, bunnyhop! IntenseCrabtree etc. Can be automatically tried at very high speeds.

Words with number substitutions: password1, deer2000, john1234, etc. Easily tested for automatically with little lost time.

Words with simple obfuscation: p@ssw0rd, l33th4x0r, g0ldf1sh, etc. Easily tested for automatically with little lost time.

Doubled words: crabcrab, stopstop, treetree, "passpass", etc. Easily tested for automatically.

Common sequences: qwerty, 12345678, mnbvcxz (from a keyboard row, reversed), etc. Easily tested for automatically.

Numeric sequences based on well known numbers such as 911 (9-1-1, 9/11), 314159... (pi), or 27182... (e), etc. Easily tested for automatically.

Identifiers: jsmith123, 1/1/1970, 555-1234, "your username", etc Easily tested for automatically.

Anything personally related to you: license plate number, Social Security number, current or past telephone number, student ID, address, birthday, relatives' or pets' names/nicknames/birthdays/initials, etc. Easily tested for automatically after a minor amount of investigation of you and your details.

There are many other ways a password can be weak,[18] corresponding to the strengths of various attack schemes; the core principle is that a password should have high entropy (usually taken to be equivalent to randomness) and not be readily derivable by any "clever" pattern, nor should passwords be mixed with information identifying the user.

Back doors

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device.

Default accounts

Vampire taps

A vampire tap (also called a piercing tap) is a device for physically connecting a station (i.e. a PC, a printer, or another device) to a network that uses 10BASE5 cabling. This device clamps onto and "bites" into the cable (hence the vampire name), forcing a spike through a hole drilled through the outer shielding to contact the inner conductor while other spikes bite into the outer conductor. From the vampire tap, a short cable called an AUI (Attachment Unit Interface) is connected directly from the tap to the network card in the PC. Vampire taps allow new connections to be made on a given physical cable while the cable is in use. This allows administrators to expand bus-topology network sections without interrupting communications.

Without a vampire tap, the cable has to be cut and connectors have to be attached to both ends.

Vampire taps may also be used for malicious purposes such as transparent network monitoring.

Fiber optic cable vampire taps exist today.

Data emanation

TEMPEST is a codename referring to investigations and studies of conducted emission[1] (CE). Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.

Compromising emanations consist of electrical, mechanical, or acoustical energy intentionally or by mishap unintentionally emitted by any number of sources within equipment/systems which process national security information. This energy may relate to the original encrypted message, or information being processed, in such a way that it can lead to recovery of the plaintext. Laboratory and field tests have established that such CE can be propagated through space and along nearby conductors. The interception/propagation ranges and analysis of such emanations are affected by a variety of factors, e.g., the functional design of the information processing equipment; system/equipment installation; and, environmental conditions related to physical security and ambient noise. The term "compromising

emanations" rather than "radiation" is used because the compromising signals can, and do, exist in several forms such as magnetic- and/or electric field radiation, line conduction, or acoustic emissions.[2]

The term TEMPEST is often used broadly for the entire field of Emission Security or Emanations Security (EMSEC). The term TEMPEST was coined in the late '60s and early '70s as a codename for the NSA operation to secure electronic communications equipment from potential eavesdroppers[3] and vice versa the ability to intercept and interpret those signals from other sources.

The U.S. government has stated that the term TEMPEST is not an acronym and does not have any particular meaning,[4][5] however various backronyms have been suggested, laconically, including "Transmitted Electro-Magnetic Pulse / Energy Standards & Testing"; "Telecommunications ElectroMagnetic Protection, Equipment, Standards & Techniques"; "Transient ElectroMagnetic Pulse Emanation STandard";[6] and "Telecommunications Electronics Material Protected from Emanating Spurious Transmissions";[7] or, jokingly (but just as factually as the other attempts), "Tiny ElectroMagnetic Particles Emitting Secret Things" and "Tremendously Endowed Men Performing Exciting Sexual Techniques"[8].

War driving

A free public Wi-Fi access pointWardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer or PDA.

Software for wardriving is freely available on the Internet, notably NetStumbler for Windows, Kismet or SWScanner for Linux, FreeBSD, NetBSD, OpenBSD, DragonFly BSD, and Solaris, and KisMac for Macintosh. There are also homebrew wardriving applications for handheld game consoles that support Wi-fi, such as sniff_jazzbox/wardrive for the Nintendo DS, Road Dog for the Sony PSP, WiFi-Where for the iPhone, and G-MoN for the Android operating system and WlanPollution for Symbian NokiaS60 devices. There also exists a mode within Metal Gear Solid: Portable Ops for the Sony PSP (wherein the player is able to find new comrades by searching for wireless access points) which can be used to wardrive. Treasure World for the DS is a commercial game in which gameplay wholly revolves around wardriving.



SSID broadcast

In security breaches, wireless cracking is the unauthorized use or penetration of a wireless network. A wireless network can be penetrated in a number of ways. There are methods ranging from those that demand a high level of technological skill and commitment to methods that are less sophisticated and require minimal technological skill. Once within a network a skilled hacker can modify software, network settings, other security items and much more. To counter the security threat of an intrusion into a wireless network, there are many precautions available.

Trivia



Lists of miscellaneous information should be avoided. Please [relocate](#) any relevant information into appropriate sections or articles. *(November 2008)*

People and crackers surveying WLANs have already opened up GPS-locations of many WLANs. They have been posted on websites such as [wige](#).

When a cracker is passively scanning each radio channel that wireless networks are broadcast on to check for activity, they cannot be detected. This, as by passive scanning the presence of that scanner is not revealed since they are not actually transmitting any traceable material to the network at this point.

Detecting a wireless “sniffer” is extremely difficult. It is only after the cracker starts to probe and insert packets into the network that the location of the attacker or the device can be isolated. For some crackers the main goal of an intrusion is to obtain the [WEP](#) key. There are several methods that are used to achieve this. A WEP key can be obtained within minutes and does not take significant computing since it is deeply flawed.

The information that a cracker can collect from sniffing alone is limited; in order to gain all the information that they want crackers must then engage in actively probing a network. In actively probing a network a cracker increases the probability of detection. This risk comes as a result of the packets that are sent to the target in an effort to get back the desired information in return.

Blue jacking

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another bluetooth enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.



Bluesnarfing

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, emails and text messages, and on some phones users can copy pictures and private videos. Currently available programs must allow connection and to be 'paired' to another phone to copy content. There may be other programs that can break into the phones without any control, but if they exist they are not made publicly available by the developer. One instance of Bluesnarfing software that was demonstrated (but never made available for download) utilized weaknesses in the Bluetooth

connection of some phones. This weakness has since been patched by the Bluetooth standard. There seem to be no available reports of phones being Bluesnarfed without pairing, since the patching of the Bluetooth standard.

Bluesnarfing is much more serious than Bluejacking, but both exploit others' Bluetooth connections without their knowledge. Any device with its Bluetooth connection turned on and set to "discoverable" (able to be found by other Bluetooth devices in range) may be susceptible to Bluejacking, and possibly to Bluesnarfing when and if Bluesnarfing of the current Bluetooth security becomes possible.

By turning off this feature, the potential victim can be safer from the possibility of being Bluesnarfed; although a device that is set to "hidden" may be Bluesnarfable by guessing the device's MAC address via brute force. As with all brute-force attacks, the main obstacle to this approach is the sheer number of addresses. Bluetooth uses a 48-bit unique MAC Address, of which the first 24 bits are common to a manufacturer [1]. The remaining 24 bits have approximately 16.8 million possible combinations, requiring an average of 8.4 million attempts to guess by brute force.

Because Bluesnarfing is an invasion of privacy, it is illegal in many countries.

It is important not to confuse Bluesnarfing with Bluejacking. While Bluejacking is essentially harmless and does not result in the exposure of any data in the victim's handset, Bluesnarfing is the copying of information from the victim's Bluetooth device.

Rogue access points

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator,[1] or has been created to allow a cracker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can ignorantly or maliciously install an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.

To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.

Presence of large number of wireless access points can be sensed in airspace of typical enterprise facility. These include managed access points in the secure network plus access points in the neighborhood. Wireless intrusion prevention system facilitates the job of auditing these access points on a continuous basis to find out if there are any rogue access points among them.

In order to detect rogue access points, two conditions need to be tested: i) whether or not the access point is in the managed access point list, and ii) whether or not it is connected to the secure network. The first of the above two conditions is easy to test - compare wireless MAC address (also called as BSSID) of the access point against the managed access point BSSID list. However, automated testing of the second condition can become challenging in the light of following factors: a) Need to cover different types of access point devices such as bridging, NAT (router), unencrypted wireless links, encrypted wireless links, different types of relations between wired and wireless MAC addresses of access points, and soft access points, b) necessity to determine access point connectivity with acceptable response time in large networks, and c) requirement to avoid both false positives and negatives which are described below.

False positive (crying wolf) occurs when the wireless intrusion prevention system detects an access point not actually connected to the secure network as wired rogue. Frequent false positives result in wastage of administrative bandwidth

spent in chasing them. Possibility of false positives also creates hindrance to enabling automated blocking of wired rogues due to the fear of blocking friendly neighborhood access point.

False negative occurs when the wireless intrusion prevention system fails to detect an access point actually connected to the secure network as wired rogue. False negatives result in security holes.

If an unauthorized access point is found connected to the secure network, it is the rogue access point of the first kind (also called as “wired rogue”). On the other hand, if the unauthorized access point is found not connected to the secure network, it is an external access points. Among the external access points, if any is found to be mischievous or potential risk (e.g., whose settings can attract or have already attracted secure network wireless clients), it is tagged as rogue access point of the second kind (also called as “honeypot”).

Weak encryption

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. The purpose of password cracking might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk, but involves system administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crackable passwords. On a file-by file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.