CompTIA® Security+ Exam Notes : Given a scenario, analyze and determine the type of malware

examguides.com/security+/security+2.htm

1. Threats, Attacks and Vulnerabilities

1.1 Given a scenario, analyze and determine the type of malware

Viruses, worms, and Trojan horses are all harmful pieces of software. The way they differ is how they infect the computers, and spread across the systems and networks.

Virus: A computer virus attaches itself to a program or file so it can spread from one computer to another. Most of the viruses are attached to an executable file, and it cannot infect your computer unless you run or open the malicious program. Note that, usually, a virus cannot be spread without a human action, (such as running an infected program) to keep it going.

WORM: Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. The danger with a worm is its capability to replicate itself. Unlike Virus, which sends out a single infection at a time, a Worm could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

Trojan Horse: The Trojan Horse, at first glance appears to be a useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening it because it appears to be receiving legitimate software or file from a legitimate source.

Rootkit: A rootkit is a collection of tools that enable administrator-level access to a computer. Typically, a hacker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to gain root access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that monitor traffic, keystrokes, etc. using a "backdoor" into the system.

Backdoor: Back doors allow unauthorized access to a remote system through an entrance in the system of which the user is typically not aware. It allows an attacker to bypass access controls and gain unauthorized access and possible even take remote control of a system. Once the back door is installed the attacker can steal or damage information or implement

other tools for further escalation of the attack. A backdoor attack can be used to bypass the security of a network. A back door is a program that allows access to the system without usual security checks. These are caused primarily due to poor programming practices.

The following are known back door programs:

1. Back Orifice: A remote administration program used to remotely control a computer system.

2. NetBus: This is also a remote administration program that controls a victim computer system over the Internet. Uses client - server architecture. Server resides on the victim's computer and client resides on the hackers computer. The hacker controls the victim's computer by using the client.

3. Sub7: Sub7, or SubSeven or Sub7Server, is the name of a popular backdoor program. This is similar to Back Orifice, and NetBus. Used to take control of victim's computer over the Internet. Its name was derived by spelling NetBus backwards ("suBteN") and swapping "ten" with "seven".

Ransomware: Ransomware is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim, promising not always truthfully - to restore access to the data upon payment.

Crpto-malware: Type of ransomware that encrypts user's files, and demands ransom. Sophisticated crypto-malware uses advanced encryption methods so files could not be decrypted without unique key.

Adware: Software that automatically displays or downloads advertisements when it is used.

Bots: A set of computers that has been infected by a control program called a bot that enables attackers to exploit the computers to mount attacks.

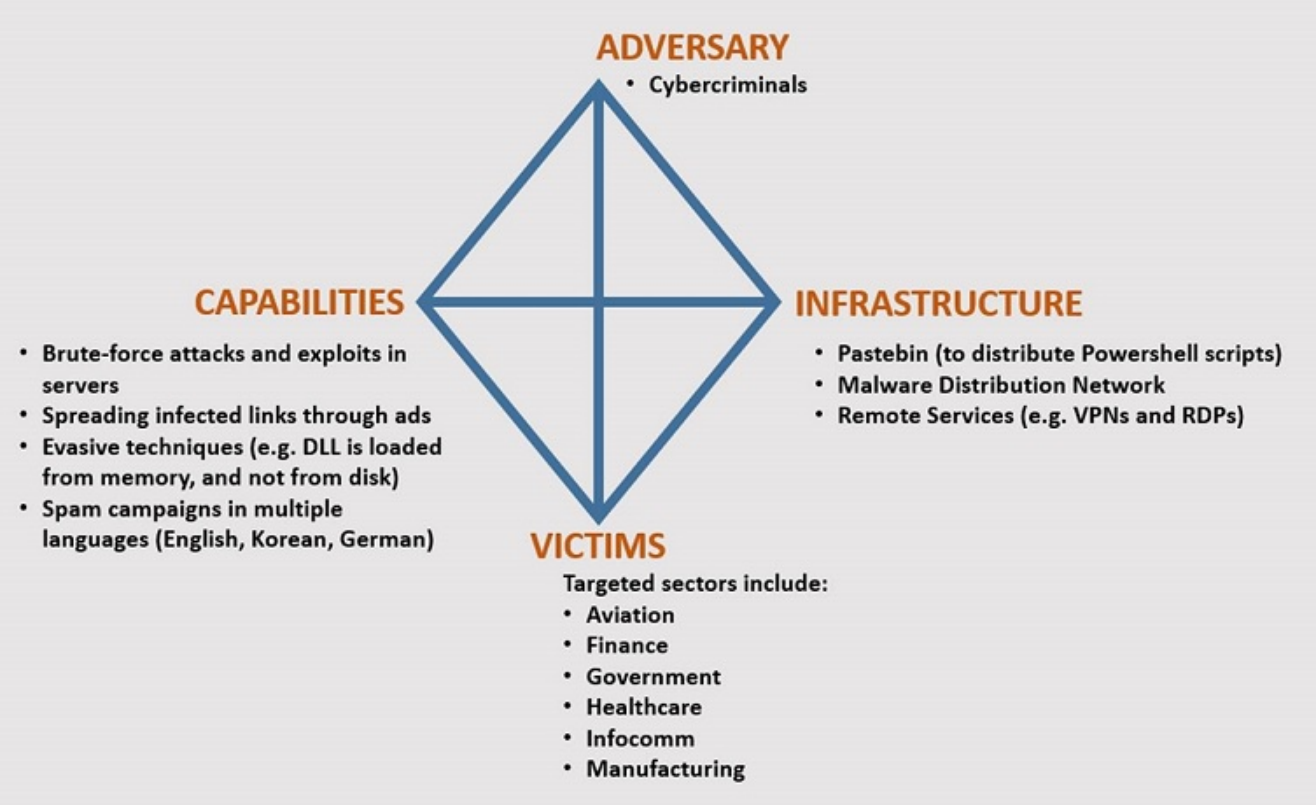
Zombies: Zombies are malware that puts a computer under the control of a hacker. Hackers use zombies to launch DoS or DDoS attacks. The hacker infects several other computers through the zombie computer. Then the hacker sends commands to the zombie, which in turn sends the commands to slave computers. The zombie, along with slave computers start pushing enormous amount of useless data to target computer, making it unable to serve it legitimate purpose. This type of attack is known as DDoS attack.

Computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or a zombie army. Both Kaspersky Labs and Symantec have identified botnets - not spam, viruses, or worms - as the biggest threat to Internet security.

Keylogger: A hardware device or software application that recognizes and records every keystroke made by a user

Logicbomb: A piece of code that sits dormant on a target computer until it is triggered by the occurrence of specific conditions, such as a specific date and time

The Diamond Model of Intrusion Analysis is a cognitive model used by the threat intelligence community to describe a specific event. As an example, a completed diamond could take the following form:



Vulnerability is not a formal node of the Diamond Model for Intrusion Analysis.

Previous Contents Next

CompTIA® Security+ Exam Notes : Compare And Contrast Types Of Attacks

examguides.com/security+/security+3.htm

1. Threats, Attacks and Vulnerabilities

1.2 Compare and contrast types of attacks

Social engineering:

Social engineering is a skill that an attacker uses to trick an innocent person such as an employee of a company into doing a favor.

For example, the attacker may hold packages with both the hands and request a person with appropriate permission to enter a building to open the door.

Social Engineering is considered to be the most successful tool that hackers use.

The term "social engineering" refers to tricking someone into revealing useful information, such as a password.

Social engineering can be used to collect any information an attacker might be interested in, such as the layout of your network, names and/or IP addresses of important servers, installed operating systems and software.

The information is usually collected through phone calls or as new recruit or guest to your boss.

Social engineering is a technique in which an attacker tricks an innocent person into doing something that helps the attacker perform some unlawful activity.

The tricks used may be simple. For instance, the attacker may act like system administrator and ask the victim for his login and password for some kind of troubleshooting.

Social Engineering exploits human behavior.

Defense against social engineering may be built by:

1. Including instructions in your security policy for handling it, and

2. Training the employees what social engineering is and how to deal with it.

Staff training is the most effective tool for preventing attacks by social engineering. Social engineering, and Trojan attack are two well-known problems associated with Discretionary Access Control (DAC).

Cross-site request forgery: It is also known as XSRF or CSRF (pronounced see-surf), is an attack against web-hosted apps whereby a malicious web app can influence the interaction between a client browser and a web app that trusts that browser. These attacks are possible because web browsers send some types of authentication tokens automatically with every request to a website. This form of exploit is also known as a one-click attack or session riding because the attack takes advantage of the user's previously authenticated session. XSRF involves unauthorized commands coming from a trusted user to the website. This is often done without the user's knowledge, and it employs some type of social networking to pull it off.

Cross-site scripting: It is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

- Cross-site scripting (XSS) exploits the trust a user has for a particular site, where as, CSRF exploits the trust that a site has in a user's browser.
- In cross-site scripting (XSS), the attackers will inject JavaScript, VBScript, ActiveX, HTML, or Flash into a web page served to a visitor to fool him and gather data from his computer.
- Note that the code used in XSS is always client side scripting, and not server side scripting.
- Here, for example, the user clicks on an innocent looking hyperlink and get a malicious code installed on his computer.

SQL injection: It is a code injection technique that might destroy your database. SQL injection works by placement of malicious code in SQL statements, via web page input.

Phishing: Phishing is the act of sending an e-mail to a user claiming to be a reputed organization (such as a bank) in an attempt to scam the user into providing information over the Internet. The e-mail directs the user to a Web site where they are prompted to provide private information, such as credit card, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. Phishing is the practice of enticing unsuspecting Internet users to a fake Web site by using authentic-looking email with the legitimate organization's name, in an attempt to steal passwords, financial or personal information, or introduce a virus attack.Phishing is a form of social engineering in which the attacker asks you for a piece of information by making it look as if it is a legitimate request. Usually, in phishing attack, the fraudster will just send one phishing email that will direct you to a website requesting you to enter your personal information such as User ID and Password.

Whaling: Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority. The content is meant to be tailored for upper management, and usually involves some kind of falsified company-wide concern. Sometimes, the whaling email will claim to be from the Better Business Bureau, seeking to confirm a complaint against the target company. Though Phishing, spaming, and email spam are also appropriate, Whaling is a form of spear phishing that attempts to target high-level executives. Whaling is nothing more than phishing or spear phishing, but for big users. Instead of sending out a To Whom It May Concern message to thousands of users, the whaler identifies one person from whom they can gain all of the data they want - usually a manager or owner - and targets the phishing campaign at them.

In Phishing and Whaling, the attacker e-mail to trick a user into revealing personal information or clicking on a link. A phishing attack will often send the user to a malicious website that appears to the user as a legitimate site such as Paypal, a bank of Microsoft.

The "phisher" doesn't know if the recipient has an account at the company, but, if the attacker sends out enough e-mails, the chances are good that someone who receives the e-mail has an account.

Tailgating: When a person just follows another authorized person through an open door that is otherwise secured is called tailgating. Other terms are distractions only.

Vishing: The telephone version of phishing is called vishing. Vishing relies on "social engineering" techniques to trick you into providing information that others can use to access and use your important accounts. People can also use this information to assume your identity and open new accounts. Vishing is the act of using the telephone (voice or VOIP) in

an attempt to scam the user into giving private information that will be used for identity theft. The attacker usually pretends to be a legitimate business. Vishing is telephone equivalent of phishing.

To avoid being fooled by a vishing attempt:

- If you receive an email or phone call requesting you call them and you suspect it might be a fraudulent request, look up the organization's customer service number and call that number rather than the number provided in the solicitation email or phone call.
- Forward the solicitation email to the customer service or security email address of the organization, asking whether the email is legitimate.

Spoofing: A spoofing attack is an attempt by someone or something to masquerade as someone else. This type of attack is usually considered an access attack

SPIM is the same thing as Spam - unsolicited advertisements. The difference is that SPIM appears through instant messaging programs instead of email. SPIM messages are automated messages that urge the person receiving the message to visit a Web site. These systems use special software programs to troll the Internet looking for instant messaging screen names, which are then added to the "spimmer's" contact list.

Scareware: Scareware, also known as rogueware or fake antivirus software, has become one of the fastest-growing, and most prevalent, types of internet fraud.

Vulnerability: Vulnerability refers to what extent a system is prone to attack from a hacker. Soft intrusion is a fictitious answer.

Driver Manipulation: Two popular methods of driver manipulation are shimming and refactoring.

Shimming : A shim is a small library that is created to intercept API calls transparently and do one of three things: handle the operation itself, change the arguments passed, or redirect the request elsewhere. Sophisticated attackers may reach down into device drivers and manipulate them in ways that undermine security.

Refactoring : Refactoring is the name given to a set of techniques used to identify the flow and then modify the internal structure of code without changing the code's visible behavior. In the non-malware world, this is done in order to improve the design, to remove unnecessary steps, and to create better code. In other words, refactoring consists of improving the internal structure of an existing program's source code, while preserving its external behavior.

Cryptographic Attacks:

Rainbow tables: A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a password (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. Rainbow table attack refers to a method wherein known MD5 signatures are stored and corresponding text based password is deduced. However, it is not possible to deduce the text based password with certainity because MD5 is a hash algorithm. It is just taking a chance. The tables wherein the MD5 and corresponding text based passwords (guessed) are known as Rainbow tables.This type attack occurs when an attacker uses Rainbow tables (tables matching clear text passwords to hash code) to access a victim's account.

Hijacking and related attacks

Typosquatting : It is also known as URL hijacking, is a form of cybersquatting (sitting on sites under someone else's brand or copyright) that targets Internet users who incorrectly type a website address into their web browser (e.g., "Gooogle.com" instead of "Google.com"). When users make such a typographical error, they may be led to an alternative website owned by a hacker that is usually designed for malicious purposes.

An attacker purchases similar domain names in typo squatting attacks for malicious intentions like using it for selling similar fake products, advertising, etc. Users visit the typo squatting domain when they enter the URL with a typo error.

Example: microsoft.com and microsfot.com

Watering hole attack: Occurs when an attacker places some malicious code on a website known to be frequented by some company executives. The attacker then plants some kind of remote access code on the visitors computer with the intention of exploiting the visitors computer.

Dictionary attack: A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password.

Cognitive password : A cognitive password is a form of authentication password that relates to the user in some form or the other. For example, a user may have to input his/her mother's maiden name or the color of his first car. By divulging such information in social web sites, it is possible for a hacker to use cognitive passwords to exploit the victim's account on a server.

LSO (Locally Shared Objects): LSO attack (also known as Flash cookie attack) results from misusing the Flash cookie by an attacker. Note that Flash cookies are stored in different locations and not deleted when you delete normal text based cookies. For example, such a cookie may be used to track the visitors Internet access over a period of time. Flash Cookie is not stored in the same folder as that of normal cookies when you are browsing a Flash

enabled website. They are stored in several different locations. Several spammers use this to their advantage. A Flash cookie may be programmed such that it tracks the User activity over the Internet, and report it back to the spammer. Normal deletion of cookies will not delete Flash cookies.

Arbitrary code execution attack: Here, when a user visits a malicious website, malware application is downloaded and installed on the victim's computer. The malicious program then runs by itself, causing the target system vulnerable to various attacks.

Remote code execution: is some what similar to that of arbitrary code execution, however, here the victims computer becomes accessible by the attacker from a remote location after the malware is installed. As a result, an attacker would be able to run commands on the victim's computer.

Session hijacking: Also known as cookie hijacking, it exploits a valid computer session (also called a session key) to gain unauthorized access to information or services in a computer system.

Malicious add-ons: As the name implies, malicious add-ons are add-on to a browser such as pop-up blocker. A malicious add-on appears to be genuine, but installs a malware that may be used to exploit the victim's computer. One needs to be very careful when trying to install any browser add-ons.

Header manipulation: It is done by manipulating the header of a TCP/IP packet. For example, an attacker may gain access to the session cookie using cookie hijack. Then, he may use the session code in the TCP/IP packet header. If the server is only relying on the session key to validate the user access, then it may give control of the session to the attacker. Thus the attacker effectively taken control of the session by manipulating the TCP/IP header.

Clickjacking: Clickjacking involves an attacker using multiple transparent or opaque layers to trick a user into clicking a button or link on another page when they were intending to click the top-level page.

Application/Service attacks:

Buffer-overflow attack: The extra data sometimes holds specific instructions for actions intended by a hacker or malicious user; for example, the data could trigger a response that damages files, changes data or unveils private information.

Web servers are most prone to CGI script exploits, and buffer overflow attacks. CGI scripts run at server side performing a given functionality, such as writing to database or reading from database etc. Hackers may use the loopholes the scripts to hack in to the web server. Similarly, buffer-overflow can be used to run undesirable code on the server making it vulnerable.

Java applets are executable programs that run within the browser window. The environment in which a Java applet runs is known as JVM (Short for Java Virtual Machine). Vulnerabilities associated with Java applets include buffer overflow, excessive utilization of computer resources, opening up of back-door for hacking, etc.

CGI is a server side script, and does not run on a browser. Javascript, and XHTML, though client side scripts, are not appropriate choice here.

DoS attack: The Internet architecture provides an unregulated network path to attack innocent hosts. Denial-of-service (DoS) attacks exploit this to target mission-critical services. DoS attacks, are explicit attempts to block legitimate users system access by reducing system availability. Any physical or host-based intrusions are generally addressed through hardened security policies and authentication mechanisms. Although software patching defends against some attacks, it fails to safeguard against DoS flooding attacks, which exploit the unregulated forwarding of Internet packets.

A hacker begins a DDoS attack by exploiting a vulnerability in one computer system and making it the DDoS "master", also called as "zombie". It is from the zombie that the intruder identifies and communicates with other systems that can be compromised. The intruder loads hacking tools on the compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target.

Distributed Denial of Service (DdoS): It is an attack where multiple compromised systems (which are usually infected with a Trojan) are used to send requests to a single system causing target machine to become unstable or serve its legitimate users.

The DoS and DdoS attacks are associated with denial of service. Smurf attack is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system

Man-in-the-middle: A man-in-the-middle attack attempts to fool both ends of a communications session into believing that the system in the middle is the other end.

Zero-day: A man-in-the-middle attack attempts to fool both ends of a communications session into believing that the system in the middle is the other end.

Replay: An attack that captures portions of a session to play back later to convince a host that it is still talking to the original connection. In Replay attack, the hacker intercepts the victim's encrypted user name and password while it is being transmitted to a server, and uses the same to access the server fraudulently by replaying the reply. Here the attacker gets the same privileges as that of the victim's computer since the user name and password match those.

Input validation refers to validation of user input in a browser based form. It is done in two ways:

1. Client side validation: Here the validation is done in the browser itself. It is possible that a hacker may use direct html input and also disable script validation. Therefore, client-side input validation needs to be supplemented by server side validation of user input.

2. Server side validation: When using server side validation, it is not possible for the attacker to manipulate the method to send the User input. Various types of attacks that may result due to non-implementation or insufficient implementation of server-side input validation are as given below:

1. Buffer-overflow attack

2. SQL injection attack

3. Command injection attack

4. Cross-site scripting attack

Malicious add-ons occur when you mistake a browser add-on for a genuine add-on. A malicious add-on installs malware on the victims computer.

DNS poisoning: This is also known as cache poisoning. Here, a rogue machine caches the DNS replies from a DNS server and uses the information fraudulently to redirect the victim's browser to attacker's site.

TCP/IP hijacking: TCP/IP hijacking occurs when an attacker replaces the victim's system with his own, without being detected. This allows access privileges to be kept in the session. Hijacking attacks take advantage of the sequencing numbers used in TCP sessions.

ARP poisoning: Address Resolution Protocol (ARP) poisoning, convinces the network that the attacker's MAC address is the one associated with the victim's IP address. As a result, the traffic sent to that IP address is wrongly delivered to the attacker's machine.

IP address spoofing: IP address spoofing is a technique that involves replacing the IP address of an IP packet's sender with another machine's IP address. The IP address spoofing technique can enable an attacker to send packets on a network without having them be intercepted by the packet filtering system (firewall). Firewall systems are usually based on filtering rules indicating the IP addresses that are authorized to communicate with the network's internal machines. In IP spoofing, the attacker uses somebody else's IP address as the source IP address. Since routers forward packets based on the destination IP address, they simply forward the packets to the destination without verifying the genuineness of the source IP address.

Cryptographic attacks:

Given below are some of the widely known password guessing methods:

1. Dictionary: this is the method in which dictionary terms are used for guessing a password.

2. Birthday: It takes advantage of probabilities, much like two people in a 50-person room shared the same birthday. With every person, the chances of two people having the same birth date increases. In the same way, when you start guessing the password, the chances of a hit keep increasing.

3. Brute force: In a Brute Force attack, muscle (in this case, CPU and/or network muscle) is applied to break through a particular security mechanism, rather than using particular intelligence or logic. "Brute force" is most commonly applied to password guessing, taking advantage of computer power available to an attacker, to try every possible password value, until the right one is found. In cryptography, a brute-force attack is an attempt to recover a cryptographic key or password by trying every possible combination until the correct one is found. How quickly this can be done depends on the size of the key, and the computing resources applied.

4. Rainbow tables: Rainbow tables are huge lists of keys or passwords. A password-guessing program uses these lists of keys or passwords rather than generating each key or password itself.

Wireless Attacks:

Rogue AP: A Rogue Access Point is a Wi-Fi Access Point which is setup by an attacker for the purpose of sniffing wireless network traffic. 802.11 (Wi-Fi) utilizes SSIDs (Service Set Identifiers) to authenticate NICs to wireless access points. There is no similar protocol for authenticating wireless access points. It is possible to place a rogue wireless access point into an 802.11 network. This rogue wireless access point can then be used to hijack the connections of legitimate network users.

An evil twin is a rogue access point set up by an attacker that produces a stronger signal than the legitimate access point. Therefore, by virtue of stronger signal, the users are attracted to the rogue access point.

Hoax: A virus hoax typically offers millions of dollars on providing some personal information or asks for doing something else such as deleting some file. You should notify the system admin about such viruses.

Weak encryption: WEP encryption allows an attacker using readily available software to crack the key within minutes. WEP encryption uses a shared key authentication and sends the same key with data packets being transmitted across the wireless network. If malicious

users have enough time and gather enough data they can eventually piece together their own key. Another disadvantage to using WEP encryption is that if the master key needs to be changed, it will have to be manually changed on all devices connected to the network. This can be a tedious task if you have many devices connected to your network.

RFID: RFID, short for Radio Frequency Identification, is a technology that enables identification of a tag (that is normally attached with an entity) by using electromagnetic waves. The function served by RFID is similar to bar code identification, but line of sight signals are not required for operation of RFID.

IV: IV, short for Initialization Vector, an attack that involves looking at repeated results in order to crack the WEP secret key.

NFC: NFC, short for Near field communication is a form of contactless communication between devices like smartphones or tablets. Contactless communication allows a user to wave the smartphone over a NFC compatible device to send information without needing to touch the devices together or go through multiple steps setting up a physical connection.

Bluejacking: Blue jacking is a term given to unsolicited messages on your blue tooth enabled phone. For example, assume that a message "'Hello, you've been bluejacked" has just been received on your mobile. This is a case of blue jacking. You can prevent this kind of annoyances by turning off the blue tooth when not required. It is the sending of unsolicited messages over a Bluetooth connection.

Bluesnarfing: Bluesnarfing is the theft of information from a wireless device such as a mobile phone or PDA through a Bluetooth connection. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information such as the user's calendar, contact list and e-mail and text messages.

Previous Contents Next

CompTIA® Security+ Exam Notes : Explain Threat Actor Types And Attributes

examguides.com/security+/security+4.htm

1. Threats, Attacks and Vulnerabilities

1.3 Explain threat actor types and attributes

Script kiddie: Script kiddie is an unsophisticated individual with little or no skills when it comes to technology. The person uses code that was written by others and is freely accessible on the internet. It might copy a malicious script directly from one website to another , only the knowledge of copy and paste is required. It uses code and probably doesn't understand how it works and what the effect will be.

Hactivist: A hacker who gains unauthorized access to and causes disruption in a computer system in an attempt to achieve political or social change. It is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist.

Insiders: Present and past employees, contractors, partners, and any entity that has access to proprietary confidential information and whose actions result in compromised security

Hacktivists, Insiders, and so on will usually have a higher level of sophistication when it comes to technology.

APT: An Advanced Persistent Threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.

Previous Contents Next

CompTIA® Security+ Exam Notes : Explain Penetration Testing Concepts

examguides.com/security+/security+5.htm

1. Threats, Attacks and Vulnerabilities

1.4 Explain penetration testing concepts

Penetration Testing: A method of evaluating security by simulating an attack on a system

Penetration testing can be conducted using various techniques classified by the following terms

Blackbox : In this type of test assessor has no knowledge of the inner workings of the system or the source code. The assessor simply tests the application for functionality.

Whitebox : In this type of testing assessor has knowledge of the inner workings of either the system or the source code.

Graybox : This type of testing combines white and black box techniques. The tester has some limited knowledge of the inner workings

Vulnerability scanning can be done in either a credentialed or non-credentialed manner. The difference is that a credentialed vulnerability scan uses actual network credentials to connect to systems and scan for vulnerabilities. Non-credentialed scans are very useful tools

that provide a quick view of vulnerabilities by only looking at network services exposed by the host.

Vulnerability Scanning: A vulnerability scanner can execute intrusive or non-intrusive tests. An intrusive test tries to exercise the vulnerability, which can crash or alter the remote target. A non-intrusive test tries not to cause any harm to the target. A crash or degradation of the service is only a side effect of an intrusive test, not a goal.

Passive reconnaissance: It is the process of collecting information about an intended target without the target knowing what is occurring. Typical passive reconnaissance can include physical observation of an enterprise's building, sorting through discarded computer equipment in an attempt to find equipment that contains data or discarded paper with usernames and passwords, eavesdropping on employee conversations, etc.

Active reconnaissance: The process of collecting information about an intended target of a malicious hack by probing the target system. Active reconnaissance typically involves port scanning in order to find weaknesses in the target system. The process of exploiting the system can then be carried out once the hacker has found a way to access the system. Tools such as port scans, traceroute information, and network mapping are used to find weaknesses in the target system

Pivot: The attacker starts by sending a phishing email from outside of the organization. Once he gained access to the victim's machine, he does his info gathering and then uses that info to look as if he's a normal user on the network moving to the real target. He jumps from one target to another, thus making the earlier victim as a pivot to reach the real target.

Persistence: In persistence, the attacker does not limit their attack to a limited time. Instead, they watch and wait, looking for an opening to strike the target system. When one presents itself, they take penetrate the victims system. Afterwards, the attacker will continue to monitor the target network for further vulnerabilities.

Passive and active reconnaissance:

Reconnaissance: Reconnaissance can be one of two types: Passive reconnaissance and Active reconnaissance. Passive reconnaissance is performed using methods to gain information about targeted computers and networks without actively engaging with the target systems and thus avoiding detection. In active reconnaissance, the attacker engages with the target system, typically conducting a port scan to find any open ports. Active reconnaissance involves using packets that can be traced; it involves engaging services that can be logged.

Pivoting: In pivoting, one moves to a new location in a network and begins the attack process over again, performing scans to see machines that were not visible from the outside. Pivoting is one of the key methods of learning where to move next.

Lateral Movement: Lateral movement, sometimes referred to as network lateral movement, refers to the process used by attackers to move deeper into a network to get to the target data. Lateral movement and pivoting work hand in hand. The purpose of lateral movement is to go to where the data is, and pivoting is one of the key methods of learning where to move next.

Footprinting: Footprinting is the first step in gaining active information on a network during the reconnaissance process.

Bug bounty: Bug bounty programs are mechanisms where companies pay hackers for revealing the details of vulnerabilities that they discover, providing the companies an opportunity to correct the issues.

Cleanup: Cleanup involves the steps of clearing logs and other evidence to prevent one from being easily discovered. Clearing logs, blocking remote logging, messing with system history, and using reverse shells and Internet Control Message Protocol (ICMP) tunnels to avoid detection and logging are some of the methods employed.

Persistence: Persistence is the condition where a system connects to the same target in a load-balanced system. This can be important for maintaining state and integrity of multiple round-trip events

War flying: War flying is when someone on a plane, drone, or helicopter uses a WiFi-enabled device to look for open APs. It's sometimes called war storming.

OSINT (open source intelligence): OSINT is the technique of using publicly available information sources to gather information on a system. OSINT is not a single method but rather an entire set of both qualitative and quantitative methods that can be used to collect useful information. OSINT is a passive activity, so passive reconnaissance is the correct answer. All of the other answers involve active measures

Drones: Drones are unmanned aerial platforms capable of carrying cameras, mobile devices, and other items across normal boundaries such as walls, fences, and checkpoints. This provides pen testers a means of getting closer to signals such as wireless networks and then recording traffic

Explain the techniques used in penetration testing

Rules of engagement: The rules of engagement describe the scope of an engagement and provide important information regarding contacts and permissions. Obtaining these rules is essential before any pen test work begins. The rules of engagement also establishes the boundaries associated with the test.

Below are some of the different things captured and detailed in this section:

1. Treatment of sensitive information during the project
2. How project status updates will be communicated
3. Emergency contact information
4. Handling of a sensitive and critical vulnerability
5. Steps taken if a prior compromise is uncovered
6. Security controls impact and specifics
7. IP addresses of testing machines for monitoring/whitelisting
8. Requirements for third-party hosting provider approvals to test, etc.

Lateral Movement: Lateral movement, sometimes referred to as network lateral movement, refers to the process used by attackers to move deeper into a network to get to the target data.

Reconnaissance: Reconnaissance can be one of two types: passive or active. Passive reconnaissance and Active reconnaissance. Passive reconnaissance is performed using methods to gain information about targeted computers and networks without actively engaging with the target systems and thus avoiding detection. In active reconnaissance, the attacker engages with the target system, typically conducting a port scan to find any open ports. Active reconnaissance involves using packets that can be traced; it involves engaging services that can be logged.

Privilege escalation The step in an attack where an attacker increases their privilege, preferably to administrator or root level.

Exercise Type:

Red team: Red Teams are internal or external entities dedicated to testing the effectiveness of a security program by emulating the tools and techniques of likely attackers in the most realistic way possible.

Blue Team: Blue Teams refer to the internal security team that defends against both real attackers and Red Teams. Blue team members come from the IT and security operations departments, and they typically perform two functions. The first is establishing defenses, configuring defensive elements such as firewalls and security appliances, managing permissions, and logging. The second involves monitoring and incident response functions.

White Team: When an exercise involves scoring and/or a competition perspective, the team of judges is called the white team. If the exercise is such that it requires an outside set of coordinators to manage it, independent of the defending team, these coordinators are also called the white team.

Purple team: A purple team is composed of both red team and blue team members. These team members work together to establish and test defenses.

Note: Red team is the attacker, the blue team is the defender, the white team is the exercise manager/judge, and the purple team is composed of a combination of red and blue team members.

When conducting a penetration testing on a Company network, it is important that a network administrator take permission from the manager or owner so that he is not blamed with any suspicious activity. The activity of the technician or network admin should be consistent with the company security policy.

Purple teams have both offensive (red) and defensive (blue) personnel to provide a balanced response. Red team is the attacker, the blue team is the defender, the white team is the exercise manager/judge, and the purple team is composed of a combination of red and blue team members.

Previous Contents Next

CompTIA® Security+ Exam Notes : Explain Vulnerability Scanning Concepts

examguides.com/security+/security+6.htm

1. Threats, Attacks and Vulnerabilities

1.5 Explain vulnerability scanning concepts

There are several tools available for testing network hardening. Some of these are:

1. Nmap: Nmap stands for Network Mapper. It is used for security scanning of a single host to a large network. Nmap is an open-source software, and available free. It can be used to determine what hosts are available on the network, what services (ports) they are offering, what operating system they are running etc.

2. Security Administrator's Tool for Analyzing Networks (SATAN): It recognizes several commonly found networking-related security problems, and reports the problems without actually exploiting them.

3. Security Administrator's Integrated Network Tool (SAINT): It is an enhanced version of SATAN, and used for network security assessment.

4. Nessus: A security scanner that audits remotely a given network and determine whether hackers may break into it, or misuse it in some way.

5. Scanless: Scanless is a command-line utility to interface with websites that can perform port scans as part of a penetration test. When you use this tool, the source IP address for the scan is the website, not your testing machine.

6. theHarvester: theHarvester is a tool like sublist3r which is developed using Python. This tool can be used by penetration testers for gathering information of emails, sub-domains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.

7. hping: An open-source packet generator and analyzer for the TCP/IP protocol that is used for security auditing and testing of firewalls and networks.

8. Netcat: Netcat is the network utility designed for Linux environments. It has been ported to Windows but is not regularly used in Windows environments. The actual command to invoke netcat is nc - options - address. The netcat utility is the tool of choice in Linux for reading from and writing to network connections using TCP or UDP.

9. Curl: Curl is a tool designed to transfer data to or from a server, without user interaction. Here's a simple example of using curl to simulate a GET request for a website URL: curl https://www.example.com

10. Sn1per: Sn1per is a Linux-based tool used by penetration testers. Sn1per is an automated scanner designed to collect a large amount of information while scanning for vulnerabilities. It runs a series of automated scripts to enumerate servers, open ports, and vulnerabilities.

11. IP scanners: IP scanners scan IP networks and can report on the status of IP addresses. There are a wide range of free and commercial scanning tools, and most come with significantly greater functionality than just reporting on address usage.

Some other network security scanning tools include SAFEsuite, and Tiger Tools TigerSuite. There is no tool by name Trittor.

Port scanner: Port scanner is a device that is used to verify any insecure ports. Spectrum analyzer is used for analyzing the frequency spectrum and not a correct choice. Cookie and backups are not relevant choices.

OVAL (Open Vulnerability and Assessment Language): OVAL is an information security community standard to promote open and publicly available security content, and to standardize the transfer of this information across security tools and services

Previous Contents Next

CompTIA® Security+ Exam Notes : Explain Impact Associated With Types Of Vulnerabilities

examguides.com/security+/security+7.htm

1. Threats, Attacks and Vulnerabilities

1.6 Explain the impact associated with types of vulnerabilities

The term **"vulnerability"** represents security flaws in hardware, software, or configuration of a device or process. Vulnerability testing should be performed on an ongoing basis by the parties responsible for resolving such vulnerabilities,

The term **"risk"** refers to the likelihood of being targeted by a given attack, of an attack being successful, and general exposure to a given threat. As can be seen, risk occurs when both the threat and vulnerability are present.

The term **"threat"** refers to the source and means of a particular type of attack. A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of threat.

Exploit: An exploit is the way or tool by which an attacker uses a vulnerability to cause damage to the target system.

War-driving is related to exploiting the vulnerabilities in wireless networks.

Tempest was the name of a classified (secret) U.S. government project to study the susceptibility of some computer and telecommunications devices to emit electromagnetic radiation (EMR) in a manner that can be used to reconstruct intelligible data. TEMPEST certification ensures that the building is shielded adequately and the EM radiations are within limits to prevent intruders from accessing the information from outside the building.

The practice of marking the buildings with unsecured wireless networks is called war-chalking. The practice of sniffing wireless networks is known as war-driving.

Race conditions: Race conditions are a vulnerability related to multithreaded applications. When a multi-threaded application does not properly handle various threads accessing a common value, this can lead to unpredictable values for that variable. This is called a race condition.

Memory/buffer vulnerability

DLL injection: DLL injection s a technique used for running code within the address space of another process by forcing it to load a dynamic-link library. DLL injection is often used by external programs to influence the behavior of another program in a way its authors did not anticipate or intend.

Buffer overflow: Buffer overflow occurs when the input is more than that allocated for that purpose. The system doesn't know what to do with the additional input, and it may result in freezing of the system, or sometimes to take control of the system by a hacker. By validating the inputs, it is possible to reduce this vulnerability to a great extent.

Shadow IT: Shadow IT is the use of information technology systems, devices, software, applications, and services without explicit IT department approval. It has grown exponentially in recent years with the adoption of cloud-based applications and services.

While shadow IT can improve employee productivity and drive innovation, it can also introduce serious security risks to your organization through data leaks, potential compliance violations, and more.

Open Source Intelligence (OSINT): Open source intelligence, sometimes called open source threat intelligence, refers to intelligence data collected from public sources. There is a wide range of public sources of information concerning current cybersecurity activity.

Dark web: The dark web is a subset of the worldwide content on the Internet that has its access restricted via specific obfuscation methods.

Insider Threats: One of the hardest threats that security professionals will have to address is that of the insider. Since employees already have access to the organization and its assets, additional mechanisms need to be in place to detect attacks by insiders and to lessen the

ability of these attacks to succeed.

Vulnerability scans

It is a bit tricky question. You have the following possibilities:

Software having virus: Positive Class
Software having no virus: Negative Class

1) Software is free of virus and scan reported the same (that it doesn't have any virus): True Negative

2) Software is having virus and the scan reported the same (that it has virus): True Positive

3) Software is free of virus and scan reported that it has virus: False Positive

4) Software has virus and the scan reported it doesn't have virus: Flase Negative

What is a bit tricky is that "having virus" is considered as Positive Class. Therefore, if there is no virus, but the scan reveals a virus the it is considered as False Positive.

The same is given below in different words:

False positive: False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. A false positive from a vulnerability scan indicates the scan detected a vulnerability, but the vulnerability doesn't actually exist.

False Negative: A false negative occurs if a vulnerability scanner does not report a known vulnerability. This is when the IDS identifies an activity as acceptable when the activity is actually an attack.

True Positive: True if a software contains virus and it is reported by the scan as having virus.

True Negative: True if a software doesn't contain any virus and the scan reports the same, that the software is free of any virus.

Previous Contents Next

CompTIA® Security+ Exam Notes : Install And Configure Both Hardware And Software-based Network Components

examguides.com/security+/security+8.htm

2. Technologies and Tools

2.1 Install and configure network components, both hardware and software-based, to support organizational security

VPN: Short for Virtual Private Network is private network formed using public Internet. It is formed between two hosts using tunneling protocols such as PPTP, L2TP, etc. Using VPN, you can connect two LANs in geographically distant locations together, as if they were located in the same building. The cost of connecting these LANs together is small since public Internet is used for providing the WAN link. A VPN provides a mechanism to access corporate networks safely using Internet. VPN uses encryption to ensure only authorized user can access the corporate resources. A secure tunnel is created through the public network through which the packets are transported between the remote computer and the corporate network. VPN are used for accessing a corporate network securely from remote locations using public Internet.

The host-to-host configuration provides the highest security for the data. However, a Gate-to-Gateway VPN is transparent to the end users.

The VPN can be implemented in any of the following combinations:

1. Gateway-to-gateway VPN

2. Gateway-to-host VPN

3. Host-to-gateway VPN

4. Host-to-host VPN

The host-to-host configuration provides the highest security for the data. However, a Gate-to-Gateway VPN is transparent to the end users.

There are two widely known protocols that can be implemented for enabling VPN communications:

1. PPTP

2. L2TP

PPTP stands for Point to Point Tunneling Protocol. It is a PPTP is pioneered by Microsoft and others is a widely used protocol.

L2TP stands for Layer Two (2) Tunneling Protocol. L2TP merges the best features of PPTP and L2F (from Cisco Systems).

PPTP and L2TP protocols together with PPP protocol enable ISPs to operate Virtual Private Networks (VPNs).

Ipsec: The two primary security services that are provided by IPSec are:

1. Authentication Header (AH), and

2. Encapsulating Security Payload(ESP)

AH: Authentication Header provides the authentication of the sender, and ESP provides encryption of the payload.

Hub: A hub is basically a multi-port repeater. When it receives a packet, it repeats that packet out each port. This means that all computers that are connected to the hub receive the packet whether it is intended for them or not. It's then up to the computer to ignore the packet if it's not addressed to it. This might not seem like a big deal, but imagine transferring a 50 MB file across a hub. Every computer connected to the hub gets sent that entire file (in essence) and has to ignore it.

HSM:A hardware security module (HSM) is a hardware encryption device that's connected to a server, typically using PCI, SCSI, serial, or USB interfaces and managed separately from the operating system. These modules provide a secure hardware store for CA keys, as well as a dedicated cryptographic processor to accelerate signing and encrypting operations.

DMZ: Demilitarized zone (DMZ) A network segment that exists in a semi-protected zone between the Internet and the inner, secure trusted network.

Jump Server: A jump host (also known as a jump server) is an intermediary host or an SSH gateway to a remote network, through which a connection can be made to another host in a dissimilar security zone, for example a demilitarized zone (DMZ). It bridges two dissimilar security zones and offers controlled access between them.

HTML5: HTML5 is the current version of the HTML protocol standard, and this version was developed to handle the modern web content of audio and video as well as to enhance the ability of a browser to function without add-ins such as Flash, Java, and browser helper

objects for common functions.

Bridge: A bridge is a kind of repeater, but it has some intelligence. It learns the layer 2 (MAC) addresses of devices connected to it. This means that the bridge is smart enough to know when to forward packets across to the segments that it connects. Bridges can be used to reduce the size of a collision domain or to connect networks of differing media/topologies, such as connecting an Ethernet network to a Token Ring network.

Switch: A switch is essentially a multi-port bridge. The switch learns the MAC addresses of each computer connected to each of its ports. So, when a switch receives a packet, it only forwards the packet out the port that is connected to the destination MAC address. Remember that a hub sends the packet out every port.

Flood guard: Flood guard is a defence mechanism against flooding type of attacks such as distributed Denial of Service (DDoS) attacks. Floodguards are used to prevent massive attacks against a public or private network.

Router: A router works at the logical layer of the IP stack. It is basically required to route packets from one network (or subnet) to another network (or subnet). In the given question, all the computers are within the same subnet and a router is inappropriate.

Gateway: A gateway works at the top layers of the TCP/IP stack. For example, a Gateway may be used to facilitate communication between a Unix mail server and a Windows mail server.

Firewall:

- The Packet Filters work at Network Layer of OSI model.
- The Application Layer Proxy works at the Application Layer of OSI model
- A Firewall implemented with stateful technology (like Checkpoint Firewall) works at all layers of the OSI model.
- A personal firewall is software that resides on the end users computers. This is different from a regular firewall, in the sense that a personal firewall is geared to protect a single user computer.

NAT: NAT short for Network Address Translation device changes the source IP address of a packet passing through it. Because of this, the destination host would not be able to receive the packets. The NAT devices at either side need to be configured so that it allows VPN packets through it. It is primarily used to hide internal network from external network, such as the Internet. A NAT basically translates the internal IP addresses to external IP addresses and vice-versa. This functionality assures that external users do not see the internal IP addresses, and hence the hosts.

ACL(Access Control List): An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject, an operator, and an object. For instance, if a file has an ACL that contains (Alex, delete, file-name), this would give Alex permission to delete the file. ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface. ACL statements are processed top-down until a match is found, and then no more statements in the list are processed. If no match is found in the ACL, the packet is dropped due to implicit deny. That is, you down type specifically to drop the traffic, but it is understood by the ACL to drop all traffic that does not match atleast one of the statements.

NIDS: As opposed to Network Intrusion Detection Systems (NIDS), Network Intrusion Prevention Systems (NIPS) focus on prevention. Arguably, NIPS is a subset of NIDS. Honeyspot is an example of NIPS

Vampire tape: A vampire tap is a type of connection that hooks directly into a coax by piercing the outer sheath and making contact with the center conductor. A vampire tap is widely used in 10Base5 networks. The mechanism allows an attacker to monitor network traffic without being detected.

Network Access Control (NAC): NAC controls access to a network with policies, including pre-admission checks and security policy checks and post-admission controls as and when a user or a device connects to a network and determines what they can do. Other schemes such as NAT, private addressing, and subnetting are only security mechanisms that take care of only one aspect of network security, and not policy based as in case of NAC.

Data loss prevention (DLP): DLP may used for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer. DLP solution can be used to filter documents sent to a printer based on the content, thus disabling any sensitive data from being transmitted to the printer.

USB Blocking: Microsoft Windows 7 comes with bit locker technology to encrypt files. You can use the same to encrypt USB drive. Note that the motherboard also should support encryption for bit-locker technology to work. If you use file-level encryption, you need to encrypt the required file separately. That may again pose problem as you may forget to encrypt or forget the key used for file-level encryption. Further, some encryption programs does not support file-level encryption.

MAC Filtering: MAC filtering is a security access control method in which MAC address is used to determine access to the network. With MAC Filtering each host is identified by its MAC address and allowed (or denied) access based on that

SSL decryptor: Another layer of security can be added to the network with an SSL decryptor . These gateways decrypt encrypted traffic (SSL or TLS), inspect it, and then re-encrypt it before sending it on to its destination. It is a processor-intensive process, but the advantage it offers is in the inspection step-making sure that you are not forwarding problems that did not get caught simply because the data was encrypted.

Port spanning/port mirroring

Access Point (TAP): TAP is a passive signal-copying mechanism installed between two points on the network. The TAP can copy all packets it receives, rebuilding a copy of all messages. TAPs provide the one distinct advantage of not being overwhelmed by traffic levels, at least not in the process of data collection. Port taps, when placed between sending and receiving devices,can be used to carry out man-in-the-middle attacks. Thus, when placed by an unauthorized party, they can be a security risk.

An aggregator switches is a device that takes multiple inputs and combines them to a single output.

Port Spanning/Port Mirroring: Most enterprise switches have the ability to copy the activity of one or more ports through a Switch Port Analyzer (SPAN) port, also known as a port mirror. This traffic can then be sent to a device for analysis. Port mirrors can have issues when traffic levels get heavy, as the aggregate SPAN traffic can exceed the throughput of the device.

Mitigation techniques

Runbooks: Operations runbooks, often simply called runbooks, are a set of standardized documents, references, and procedures used to describe common IT tasks. Runbooks are created for the purpose of walking someone through the steps necessary for accomplishing a specific task or troubleshooting a particular issue

Playbooks: A playbook is a set of approved steps and actions required to successfully respond to a specific incident or threat. Playbooks are commonly instantiated as itemized checklists, with all pertinent data prefilled in systems, team members, actions, and so on.

Firewall rules: Firewall rules state whether the firewall should allow particular traffic to pass through or block it. The structure of a firewall rule can range from simple to very complex,depending on the type of firewall and the type of traffic.

Mobile Device Management (MDM): MDM is the term for a collective set of commonly employed protection elements associated with mobile devices.

Quarantine: In the case of a suspicious file, file change,or configuration change, there is a chance of error in the decision, and having a virtual "undo" capability may be desired. This is where the concept of quarantine enters the equation. Quarantining an item is to render it

disabled but not permanently removed from the system.

Access point configuration

Example 1: Set SSID on the generic WAP router to SECNET.

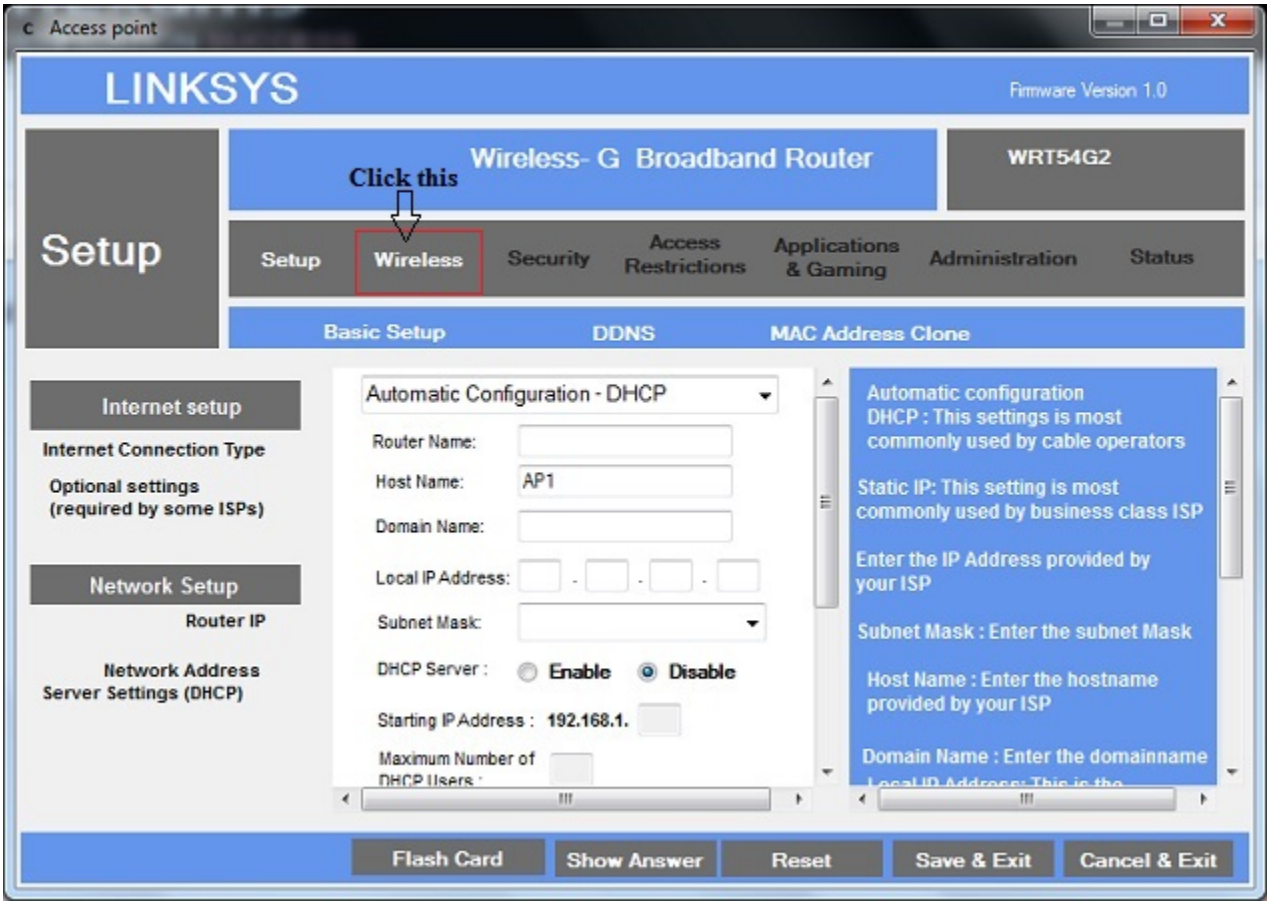
Configuration steps:

Network Name (SSID) is basically the device's wireless network name and is one way of securing your wireless network. The SSID is shared by all devices in your wireless network and therefore, has to be unique since this will identify your wireless network from the rest.

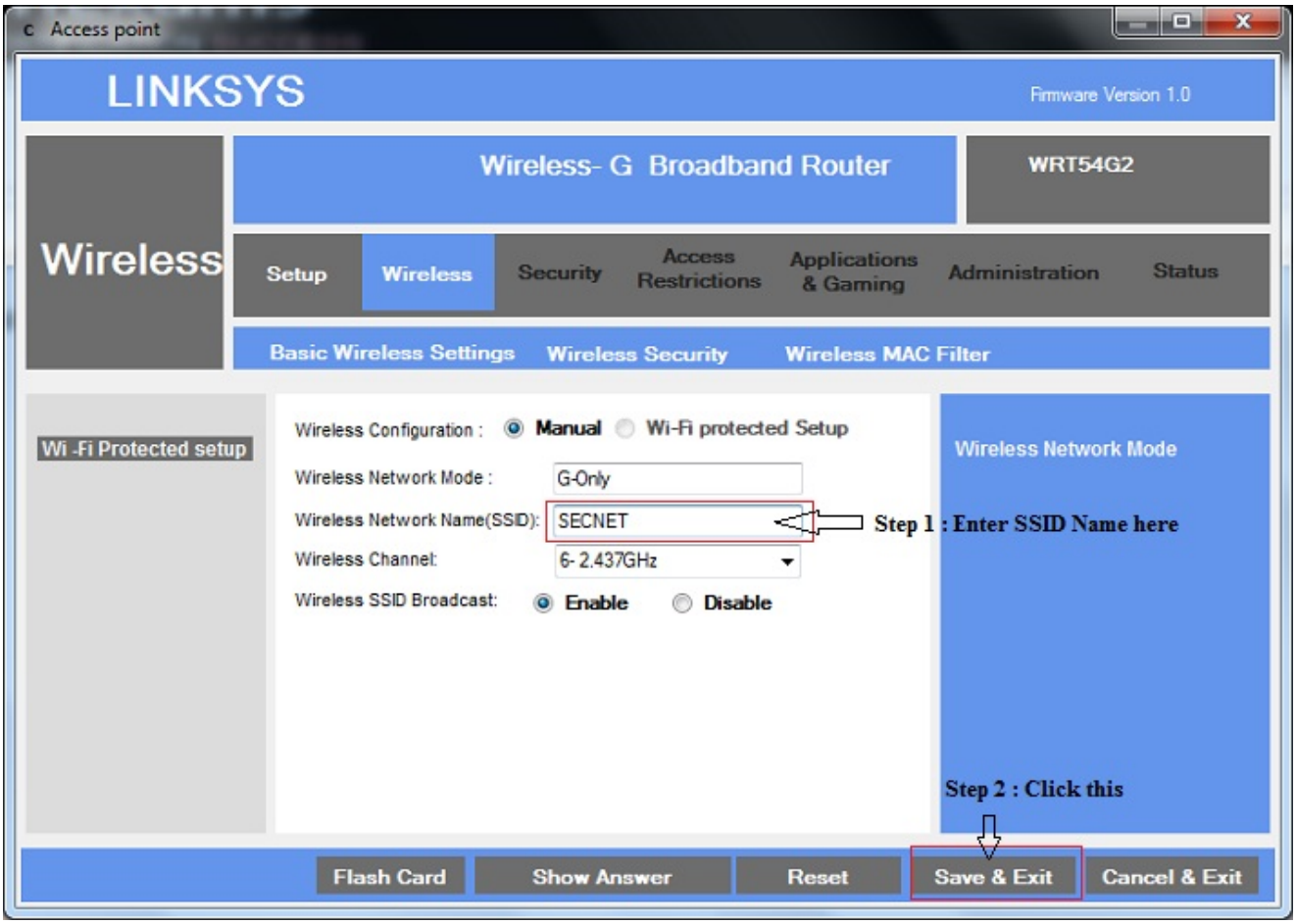
To change the wireless network name of your router, follow the steps below.

Note: SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSIDs.

1. In Access point window click "Wireless" tab



2. In that look for "Wireless Network Name" (SSID), and enter the SSID name "SECNET" in the box provided. Click on "Save & Exit" button.



Note: The exercise is typical for a particular brand of home router and may differ slightly from device to device. When you are configuring any other brand/make routers, please read the manufacturer's documentation provided along with the device.

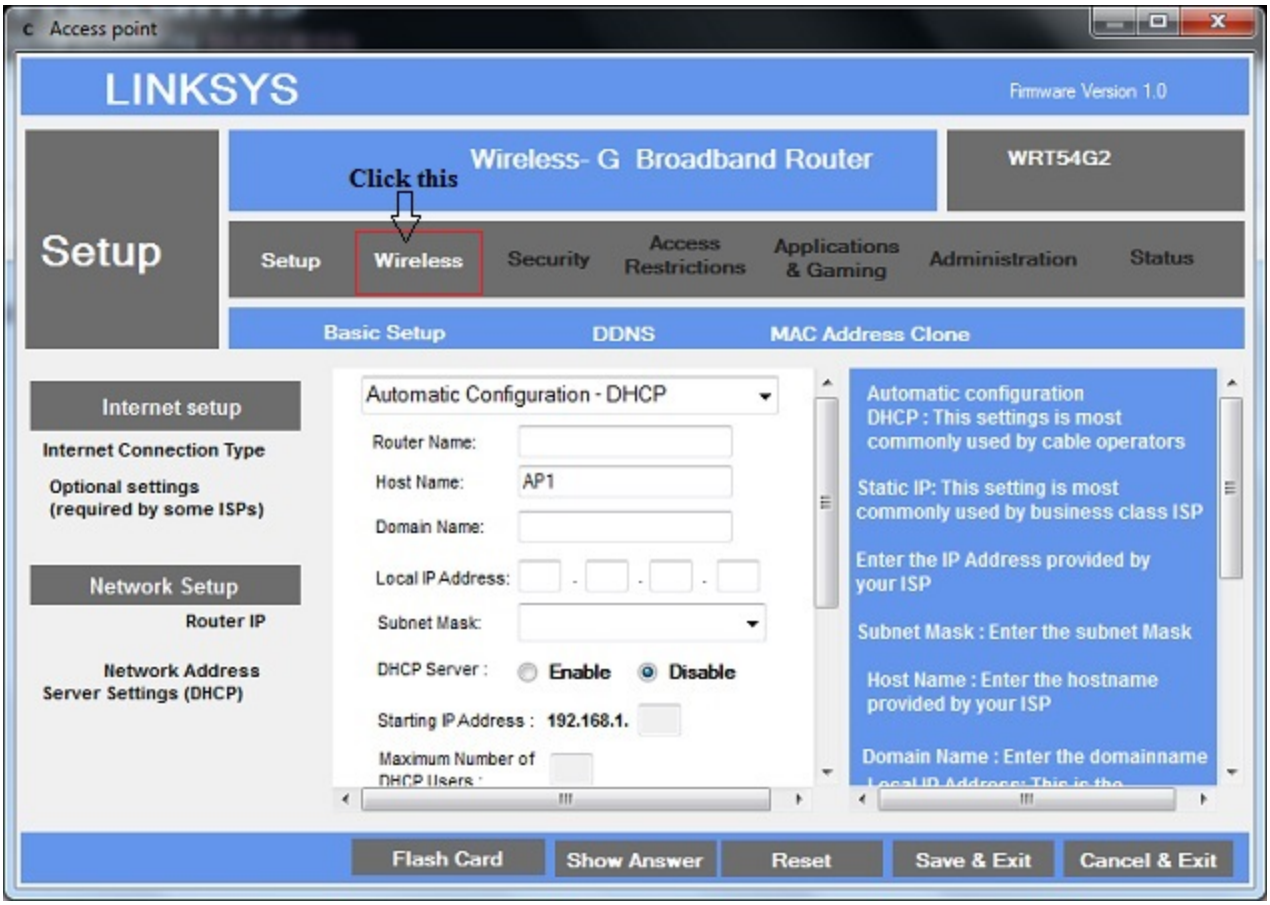
Example 2: Using the simulator, perform the task of disabling SSID broadcast.

A Service Set Identifier (SSID) is the wireless network name broadcast by the wireless device such as a wireless router. When another wireless device searches the area for wireless networks it will detect the SSID to be able to associate with the router. SSID Broadcast is enabled by default however; you may also choose to disable it.

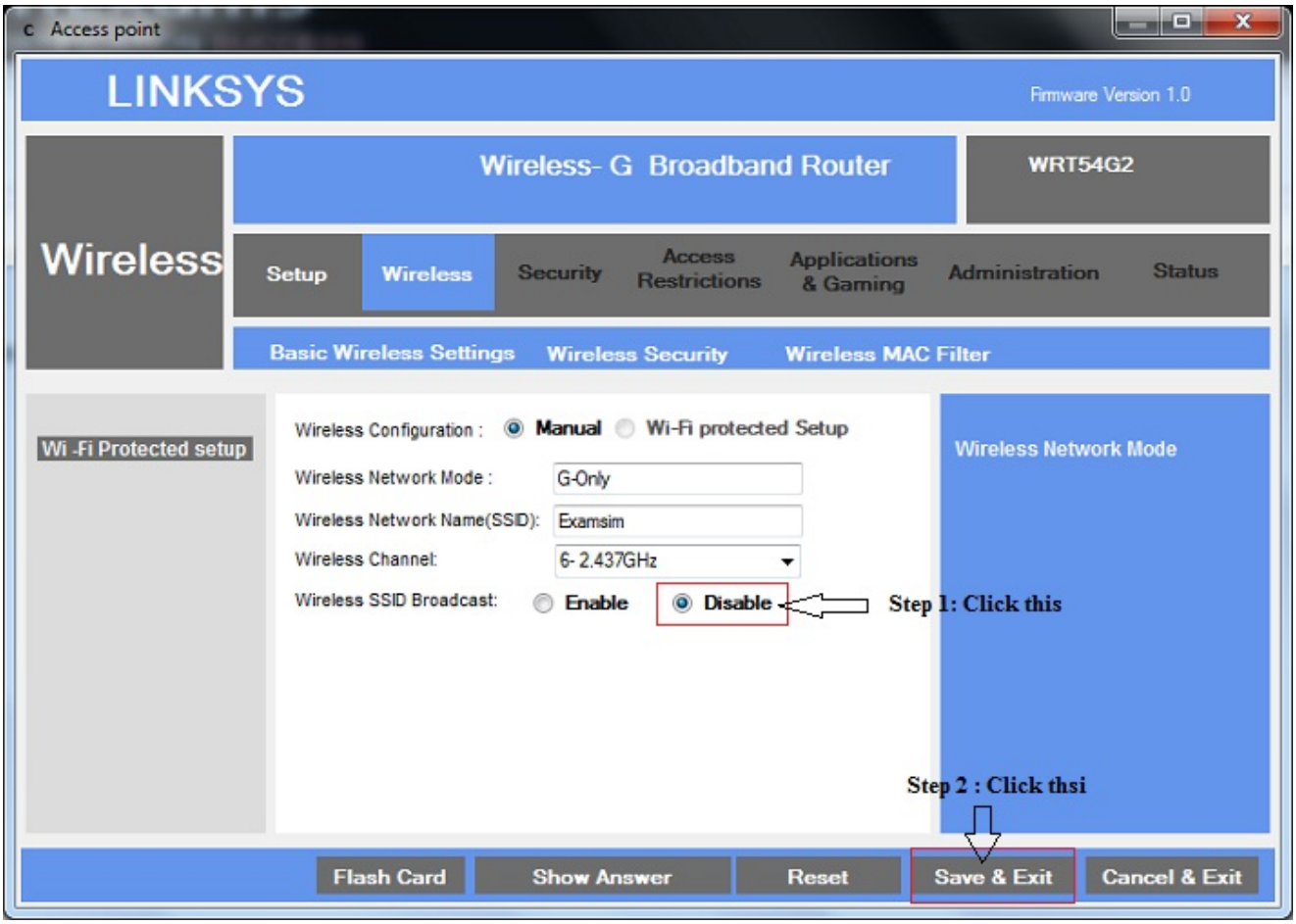
Disabling the SSID Broadcast is one way of securing your wireless network. This procedure will prevent other users from detecting your SSID or your wireless network name when they attempt to view the available wireless networks in your area.

To disable the SSID Broadcast of your Linksys router, follow these steps:

1. In Access point window click "Wireless" tab



2. Click "Disable" radio button against "Wireless SSID Broadcast" and click "Save & Exit" button.



Previous Contents Next

CompTIA® Security+ Exam Notes : Software Tools To Assess The Security Posture Of An Organization

examguides.com/security+/security+9.htm

2. Technologies and Tools

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

Backup Utilities:

1. HDD: Data stored on a hard disk drive (HDD) is permanent in nature. It remains on the hard drive even after the system is powered down and rebooted. However, a normal hard disk drive is prone to errors and may crash because of non-availability of redundancy.

2. Logs stored on remote systems: Any data stored on a remote system is less vulnerable than data stored on the target system. For this reason, many servers send log data to a remote system for centralized collection. Even if the server is completely destroyed, the centralized logs still have valuable data for problem analysis.

3. Archive media: This includes any types of backups or copies of data captured for either recovery or archive purposes. They are generally offline and less likely to be destroyed or corrupted. Examples of archive media include backup tapes and DVDs.

Software Tools:

Honeypot: Honeypots are designed such that they appear to be real targets to hackers. That is a hacker can not distinguish between a real system and a decoy. This enables lawful action to be taken against the hacker, and securing the systems at the same time.

Netstumbler: Netstumbler can be used to sniff wireless networks during wardriving. The software tool provides several details of a wireless network such as SSID.

To reduce vulnerabilities on a web server , you need to apply the latest service packs and patches to a web server or any operating system as a preventive measure. Audit logs may help detect any attempts to hack the web server, and not a preventive measure.

Network Mapper: A network mapper is a tool that identifies what the devices connected to the network and the operating systems being used, if any. Firewall, proxy server, and web security gateway are used for network/host security. System mapper is given to divert the attention from the basic question.

Sniffer: A sniffer is a piece of software that grabs all of the traffic flowing into and out of a computer attached to a network. A sniffer may be used in an IDS, and a sniffer by itself doesn't identify any suspicious traffic.

Proxy Server: A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.

Command line tools:

NBTSTAT: This utility displays current NetBIOS over TCP/IP connections, and display NetBIOS name cache.

NETSTAT: Displays current TCP/IP connections since the server was last booted.

Forensics

Data Dump (dd): is a Linux command-line utility used to convert and copy files. As a result, dd can be used for tasks such as backing up the boot sector of a hard drive, obtaining a fixed amount of random data, or copying (backing up) entire disks

Memdump: Linux has a utility program called memory dumper, or memdump. This program dumps system memory to the standard output stream, skipping over any holes in memory maps. By default, the program dumps the contents of physical memory (/dev/mem). The output from memdump is in the form of a raw dump.

TRACERT: Used to determine which route a packet takes to reach its destination from source.

IPCONFIG: Used to display Windows IP configuration information.

NSLOOKUP : This utility enables users to interact with a DNS server and display resource records.

ROUTE: Used to display and edit static routing tables.

WinHex: WinHex is a hexadecimal file editor. This tool is very useful in forensically investigating files, and it provides a whole host of forensic functions such as the ability to read almost any file, display contents of the file, convert between character sets and encoding, perform hash verification functions,and compare files

FTK imager:FTK imager is designed to capture an image of a hard drive (or other device) in a forensic fashion. FTK Imager retains the file system metadata (and the file path) and creates a log of the files copied.

Autopsy: Autopsy is the open source answer for digital forensic tool suites. Can perform virtually all digital forensic functions. It runs on Windows and offers a comprehensive set of tools that can enable network-based collaboration and automated,intuitive workflows. It has tools to support hard drives, removable devices,and smartphones.

Packet capture and replay

TCPreplay: Open source utilities for editing and replaying previously captured network traffic. As a tool, it specifically replays a packet captures, called PCAP files on a network.

TCPdump: The tcpdump utility is designed to analyze network packets either from a network connection or a recorded file. You can use tcpdump to create files of packet captures, called PCAP files, and perform filtering between input and output.

Wireshark: Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet.

Arp: The arp command is designed to view and modify the ARP table entries on the local computer

File manipulation

Head: Head is a utility designed to return the first lines of a file. A common option is the number of lines one wishes to return. For example, head -5 returns the first five lines of a file.

Tail: Tail is a utility designed to return the last lines of a file. A common option is the number of lines one wishes to return. For example, tail - 5 returns the last five lines of a file.

Cat: Cat is a Linux command, short for concatenate, that can be used to create and manipulate files. It can display the contents of a file, handle multiple files,and can be used to input data from stdin, which is a stream of input, to a file if the file does not exist. Here is an example:# cat textfile.txt

The cat command can be piped through more or less to limit scrolling of long files: # cat textfile.txt | more

Grep: Grep is a Linux utility that can perform pattern-matching searches on file contents. The name grep comes from "Globally search for Regular Expression and Print the matching lines."

Chmod: Chmod is the Linux command used to change access permissions of a file. The general form of the command is chmod <options> <permissions> <filename>

Permissions can be entered either in symbols or octal numbers

logger: The Linux command logger is how you can add log file information to /var/log/syslog. The logger command works from the command line, from scripts, or from other files, thus providing a versatile means of making log entries. The syntax is simple:

logger <message to put in the log>

This command will put the text in the option into the syslog file.

Previous Contents Next

CompTIA® Security+ Exam Notes : Given A Scenario,Troubleshooting Common Security Issues

2. Technologies and Tools

2.3 Given a scenario, troubleshoot common security issues

Whether required or not, several services are installed by default. Disabling the services that are not required will ensure better security for the system.

Scenario: You have recently productionized a web server after several internal checks. In the process of testing the server, you have created several sample files on the server. What should you do with such files when the server is put in production environment?

Solution: *It is important that any extraneous files are removed from the server before making it available in production environment. Any such files may lead to security loop holes in ways that are not easily predictable.*

Scenario: You are a network admin for an organization, and need to monitor the network traffic. What needs to be performed for monitoring the network traffic?

Solution: *Your NIC card must be in promiscuous mode to be able to examine all the network traffic.*

Content Filter: Internet content filter is used to block specific types of information from being passed on to the user. Other options are devious and not correct.

Software Backout procedure is a term used for restoring the system or software in the event of any recent failure due to upgrade.

Standard is a mandatory element in the implementation of policies, where as guidelines and procedures are descriptive.

Confidentiality, Integrity, and Availability are the three main goals when it comes to information security.

- **Confidentiality:** Confidentiality means that the message retains its privacy. To make data confidential, the organization must work hard to make sure that it can be accessed only by authorized individuals
- **Integrity:** means that the message can't be altered without detection. Authorization is necessory before data can be modified in any way, this is done to protect the data's integrity.
- **Availability:** means that data is obtainable regardless of how information is stored,accessed, or protected. It also means that data should be available regardless of the malicious attack that might be perpetrated on it.

These three principles should be applied when dealing with the security of hardware, software, or communications.

Previous Contents Next

CompTIA® Security+ Exam Notes : Given a Scenario,Analyze And Interpret Output From Security Technologies

examguides.com/security+/security+11.htm

2. Technologies and Tools

2.4 Given a scenario, analyze and interpret output from security technologies

IDS: IDS stands for Intrusion Detection System. There are primarily two types of IDSs. These are Network based IDS (NIDS), and Host based IDS (HIDS). If the IDS monitors network wide communication, it is called Network based IDS, and if the IDS monitors security on a per host basis, it is called Host based IDS. Network based IDS collects widespread intrusions effectively.

A host based IDS should be place on a host computer such as a server. Network based IDS is typically placed on a network device such as a router.

IDS Tools that identify attacks using defined rules or logic and are considered passive. An IDS can be network based or host based. An IDS monitors network traffic, but it does not take any specific action and is therefore considered passive.

Usually, several services are installed by default when an Operating System is installed. Nonessential services are the services that are not used. It is important that non-essential services are either disabled or removed; otherwise, hackers may use these services to get

back-door entry into the computer system. These attacks usually do not draw the attention of system admins because they are not monitored actively. IDS (short for Intrusion Detection Systems) can detect such type of attacks.

A few techniques used by IDS (Intrusion Detection Systems) include the following:

1. Anomaly detection

2. Signature detection

3. Target monitoring, and

4. Stealth probes

Anomaly detection: This method establishes a baseline of normal usage patterns, and anything that widely deviates from the baseline is investigated for possible intrusion. An example of this would be if a user logs on and off of a machine 10 times a day instead of the normal once or twice a day.

Signature detection: This uses specifically known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures.

Target monitoring systems do not actively search for anomalies or misuse, but instead look for the modification of specified files.

IDS (Intrusion Detection Systems, like NIDS, HIDS) use signature matching for detecting abnormal activities in a host or network.

An active IDS responds to an intrusion by taking pre-configured steps to prevent the intruder doing any further damage. Such steps may include preventing the IP address from accessing the network or disabling the intruded port, etc.

There are several key terms that one needs to be familiar with IDS

Alert: An alert is a message from the analyzer indicating that an event of interest has occurred. Alerts occur when activities of a predefined type exceed a threshold. value set by the operator.

Analyzer: The analyzer processes the data collected by the sensor. Analyzer monitors the events and determines any unusual activities. They can also use a rule-based process and send alerts when a rule is met or not met.

Data Source: Data source is the raw information available to the analyzer. Data source is used by an analyzer to analyze any suspicious activity.

Event: An event is an occurrence in a data source that indicates that a suspicious activity has occurred. Analyzer processes any such events and may generate an alert.

Manager: The manager is the interface that an operator uses to manage the IDS. An operator uses IDS manager to configure the IDS.

Notification: Notification is the process by which the IDS manager makes the operator aware of an alert.

Operator: The operator is the human interface responsible for configuring and managing the IDS.

Sensor: A sensor is the IDS component that collects data from the data source and passes it on to the analyzer.

The first thing to be done when an intrusion is detected is to contain the damage. For example, if the intrusion is in the form of an unauthorized user, ensure that the user cannot access any network resource.

There are primarily three types of Intrusion Detection Schemes.

1. Behaviour based

2. Signature based, and

3. Anomaly based.

Signature based IDS: It is also called Misuse-Detection IDS is based on detecting known patterns (signatures) of data. SD-IDS uses huge data (signatures) to detect any intrusions or intrusion attempts.

Anomaly based IDS: This looks for any anomalous activity. This type of detection is normally based on artificial intelligence.

Web Application Firewall: A web application firewall (WAF) is server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection. By customizing the rules to your application, many attacks can be identified and blocked.

Unified Threat Management (UTM): UTM involves an approach to information security whereby a single hardware- or software-installation provides multiple security functions. UTM is a single solution that combines multiple security controls. The overall goal of UTMs is to provide better security, while also simplifying management requirements. In many cases, a UTM device will reduce the workload of administrators without sacrificing security.

CompTIA® Security+ Exam Notes : Given A scenario,Steps To Deploy Mobile Devices Securely

examguides.com/security+/security+12.htm

2. Technologies and Tools

2.5 Given a scenario, deploy mobile devices securely

Some security controls frequently used for mobile devices are given below:

Screen lock: Uses a password to lock the device. This prevents a thief from using a stolen device. Screen lock helps in preventing the un-authorized user from seeing the contents. However, an attacker may ultimately gain access to the data.

Proximity lock: Automatically locks your mobile device or smart-phone when you are away from the phone. It uses a proximity sensor that you may personally carry such as a blue tooth device.

Strong password: Any time a password is used to protect a mobile device (or any device or system), it should be strong. This means they are at least eight characters and include multiple character types, such as upper case, lower case, numbers, and symbols.

Data encryption: Encryption protects the confidentiality of data and smart-phone security includes device encryption to protect the data against loss of confidentiality. It's possible to selectively encrypt some data on a system, an entire drive, or an entire device.

Remote wipe: Remote wipe capabilities are useful if the phone is lost. The owner can send a remote wipe signal to the phone to delete all the data on the phone. Remote wipe executed from another machine over a network This also deletes any cached data, such as cached online banking passwords, and provides a complete sanitation of the device, ensuring that all valuable data is removed.

Screen lock may prevent the thief from accessing the device for some time, but susceptible to brute force method. The thief may also resort to other methods to open the screen lock. By using remote wipe, it is possible to completely erase the data. However, note that the portable device may not be accessible after remote wipe. Further, it may not show up using geo-tagging as all applications are erased.

Voice encryption: It's possible to use voice encryption with some phones to help prevent the interception of conversations

Biometric: A biometric authentication depends on the physical characteristic of a human being. It is not something that can be remembered. Usually, bio authentication is very secure, though not widely used due to cost constraints.

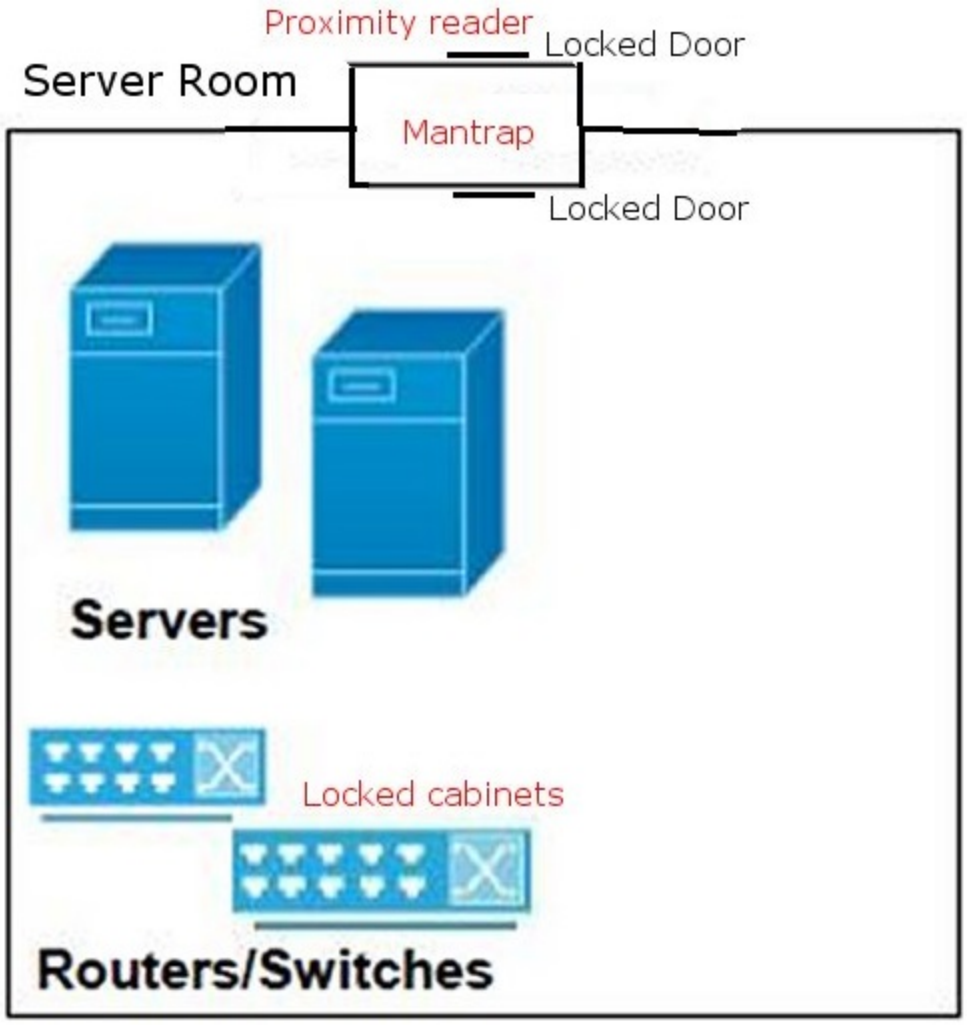
Global positioning system (GPS): tracking. A GPS pinpoints the location of the phone. Many phones include GPS applications that you can run on another computer. If you lose your phone, GPS can help you find it. If the data is sensitive, you use remote wipe feature to erase the data on the mobile. This is useful to know before you send a remote wipe signal. GPS tracking helps locate the lost device, but does not protect the data.

Cable locks: The number of laptops stolen during lunches at conferences is astronomical. Many people don't seem to know how common thefts are and often leave their laptops unprotected. Cable locks can secure a mobile computer. They often look about the same as a cable lock used to secure bicycles.

Locked cabinet : Small devices can be secured within a locked cabinet or safe. When they aren't in use, a locked cabinet helps prevent their theft. Locking of cabinets that hold switches and routers is a good way to maintain security of equipment, as well as the network. It is possible that a hacker use an unused port on a switch to connect SPAN (mirror another port) and have access to confidential information.

Mantrap: A mantrap is a small room with an entry door on one wall and an exit door on the opposite wall. One door of a mantrap cannot be unlocked and opened until the opposite door has been closed and locked. Mantraps are most often used in physical security to separate non-secure areas from secure areas and prevent unauthorized access. They can also be found in high tech manufacturing to provide entry and exit chambers for server rooms or data centers.

Proximity reader: are typically activated with a proximity card, which can be shared between people. A sophisticated mantrap can be activated with a proximity card that also requires a PIN unique to the card and the user. This provides multi-factor authentication (something you have and something you know). However, the primary purpose of a mantrap is to prevent tailgating, not authentication.



Bring Your Own Device (BYOD): BYOD policy is not relevant in this context because the company has already provided laptops to it's employees. This is a common issue in the modern workplace, and it can pose substantial security risks.

COPE: In Company-Owned and - Provided Equipment (COPE), the company owns mobile devices. Using COPE, the company has complete control of the devices, and thus it can ensure a higher level of security. With this approach, the company creates a list of approved devices that meet the company's minimum security standards. Employees then can select from among this list of pre-approved devices.

Geo-tagging: Geo-tagging is the process of tagging the geo information to the file being generated. Sometimes, it may become a threat to the employee or the organization because an attacker would be able to know where the owner of the file is residing. An example of geo-tagging is when you append the place information to a picture uploaded to a social media site. Geo tagging is used to identify the location of a mobile device, such as a smart phone over a network.

Mobile device management ensures that up to date patches or bug fixes are applied to the mobile device.

Full device encryption is another method in preventing an un-authorized user from accessing the data.

Geofencing: Geofencing relies on GPS tracking, but it goes a step further. With geofencing, the device will only function if it is within certain geographical locations. So, if a mobile device is stolen, that device will not work when taken outside the company perimeter.

DLL hijacking: DLL highjacking takes advantage of the load order of legitimate DLLs by placing a spoofed version in a higher load position than the real DLL

Sideloading: It works in a similar fashion as DLL hijacking. DLL side loading makes use of the WinSxS directory (C:\Windows\WinSxS). This directory holds multiple versions of DLL files for application compatibility reasons. An application using this directory to retrieve a DLL will need to have a manifest. The manifest lists the DLL file that the program needs to load at runtime execution and is used by the DLL loader to determine which version should be used. A malicious DLL with a spoofed name could be placed in this location due to the lack of verifications that are performed on files in this folder. As a result, a vulnerability similar to the one that allows DLL hijacking exists in the side-by-side feature.

USB OTG (USB On The Go): USB OTG introduces the concept of a device performing both master and slave roles, Whenever two USB devices are connected and one of them is a USB OTG device, they establish a communication link. For instance, a mobile phone may read from removable media as the host device, but present itself as a USB Mass Storage Device when connected to a host computer. This means that any portable device carried into your network could be used to exfiltrate files and data from your network by presenting itself as a storage device or a Wi-Fi hotspot to the attacker.

Mobile Devices

MDM/Unified Endpoint Management (UEM): MDM software is an application that runs on a mobile device and, when activated, can manage aspects of the device, including connectivity and functions. The purpose of an MDM application is to turn the device into one where the functionality is limited in accordance with the enterprise policy.

Unified endpoint management (UEM): Unified endpoint management refers to securely managing all the endpoints in an organization using a comprehensive solution. IT asset footprints are growing rapidly and managing these assets such as laptops, desktops, tablets, and smart phones has become critical. Endpoint management becomes even harder

with heterogeneous devices, or with devices that travel outside of the organization's network. The best way to ensure your devices are being managed properly is by employing an endpoint management software, such as UEM solution.

Mobile Application Management (MAM): Mobile Application Management (MAM) or mobile app management, refers to the management of the complete lifecycle of every app used in an enterprise, including installing, updating and deleting apps on both corporate and personally owned devices in the organization. Enterprise mobile application management also includes managing mobile app licenses, permissions, configurations, and defining organizational app policies that includes restrictions pertaining to the apps and data stored on the apps.

Mobile device management (MDM): MDM is a type of security software used by an IT department to monitor, manage and secure employees' mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization.

Containerization: In mobile device management, "containerization" is used to isolate the mobile application from the mobile operating system or other applications installed on the same device.

Mobile Content Management: A mobile content management strategy enables employees to securely access mission-critical enterprise data and collaborate with other employees across any network or mobile device without being slowed down or restricted from data they need access to for their work function.

Push notification services: A push notification is a message that pops up on a mobile device. App publishers can send them at any time; users don't have to be in the app or using their devices to receive them. They can do a lot of things; for example, they can show the latest sports scores, get a user to take an action, such as downloading a coupon, or let a user know about an event, such as a flash sale. Push notifications provide convenience and value to app users. For example, users can receive:

Sports scores and news right on their lock screen

Utility messages like traffic, weather and ski snow reports

Flight check in, change, and connection information

Deployment models

VDE: A virtual desktop environment (VDE) stores everything related to the user (wallpaper,folders,windows and so on) remotely and client software locally simulates the user's desktop environment and capabilities while running them on the host.

VDI: Virtual desktop infrastructure (VDI) is the process of running a user desktop inside a virtual machine that lives on a server in the data center. It enables fully personalized desktops for each user yet maintains centralized management and security.

There are two main types of desktops you can deploy in a virtual desktop infrastructure (VDI):

1. persistent and
2. non-persistent.

With persistent VDI (one-to-one desktop), each user gets his or her own desktop The user's settings are saved and appear each time at login. persistent VDI is basically the same setup you had with your physical desktops, making it easier for many admins to manage.

Nonpersistent desktops are many-to-one, meaning that they are shared among end users. When users access a nonpersistent desktop, none of their settings or data is saved once they log out. At the end of a session, the desktop reverts back to its original state and the user receives a fresh image the next time he logs in.

Previous Contents Next

CompTIA® Security+ Exam Notes : Given A Scenario,Implenent Secure Protocols

examguides.com/security+/security+13.htm

2. Technologies and Tools

2.6 Given a scenario, implement secure protocols

The following port numbers are important from Sec+ exam:

Description	IP protocol	Port
FTP - File Transport Protocol	TCP	20, 21
SSH - Secure Shell	SCTP,TCP	22
SFTP - Secure File Transport Protocol (uses SSH)	SCTP,TCP	22
SCP - Secure Copy (uses SSH)	SCTP,TCP	22
Telnet	TCP	23
SMTP - Simple Mail Transport Protocol	TCP	25
TACACS - Terminal Access Controller Access-Control System	TCP/UDP	49
DNS - Domain Name System	UDP	53

TFTP - Trivial File Transport Protocol	UDP	69
HTTP - Hypertext Transfer Protocol	TCP	80
HTTPS - Hypertext Transfer Protocol Secure	TCP	443
Kerberos	UDP	88
POP3 - Post Office Protocol version 3	TCP	110
NNTP - Network News Transfer Protocol	TCP	119
IMAP4 - Internet message access protocol version 4	TCP	143
SNMP - Simple Network Management Protocol	TCP,UDP	161
SNMP Trap - Simple Network Management Protocol Trap	TCP,UDP	162
ISAKMP (VPN) - Internet Security Association and Key Management Protocol (virtual private network)	UDP	500
Syslog	TCP/UDP	514
L2TP - Layer 2 Tunneling Protocol	UDP	1701
PPTP - Point-to-Point Tunneling Protocol	TCP	1723
RDP - Remote Desktop Protocol	TCP/UDP	3389

DNS server uses UDP for name resolution uses port 53. Web server uses port 80. DHCP uses port 67 by default. FTP uses port 21.

A MAC address filter works at the Physical layer of OSI model.

FTP: File Transfer Protocol (FTP) transfers files in unencrypted form. Even the authentication occurs in clear text for FTP and Telnet. A hacker may gain access to an FTP server by exploiting this weakness. FTP can also be secured with TLS to become FTPS. If you are transferring files with sensitive information, then you should use FTPS rather than FTP. As an alternative to FTPS there is SFTP, and SCP. Secure File Transfer Protocol and Secure Copy both secure file transfer but they secure with SSH (Secure Shell) rather than SSL/TLS. The use of SFTP, SCP, or FTPS is always recommended if any sensitive files are being transferred.

FTP transfers authentication information in clear text. The security concerns while using FTP also include buffer overflow, and anonymous access. However, the cache mining does not occur while using FTP .

Simple Mail Transfer Protocol (SMTP): The main protocol used when sending email, does not include a way to authenticate where the email message originated. However, the mail server inserts a header at the top of every email message. This gives us a message's route, making it possible to determine the origin of the message.

Email attachments from spammers usually contain malware, and one should never open such attachments.

SMTP relay: SMTP relay enables an email server to forward incoming e-mail (originating in some other domain) to other e-mail servers. This feature, if not disabled is used by many spammers to send unsolicited emails. In some cases, it is also possible that the email server IP is blocked by other ISPs from sending emails. It is important that the SMTP relay feature is disabled if not used. If relay function is required, then the domains that use the server may be specified so that spammers can't misuse the email servers

L2TP: The Layer 2 Tunnel Protocol (L2TP) is a standard that combines the best features of Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP).

L2TP does not provide information confidentiality by itself. IPSec is normally used in combination with L2Tp for providing confidentiality of communication. L2TP cannot traverse NAT at it uses encrypted checksum that are not readable by NAT device. One possible solution is to terminate L2TP at the firewall itself or to provide NAT pass-through, which some NAT devices offer.

ISAKMP: ISAKMP Short for Internet Security Association and Key Management Protocol defines payloads for exchanging key generation and authentication data.

Domain Name System Security Extensions (DNSSEC): DNSSEC are security specifications for secure DNS. DNSSEC involves many security features such as digitally signed DNS responses. These mechanisms are meant to mitigate the risk of DNS attacks such as DNS poisoning. Also, when the DNS resolution process is sent in clear text, that leaves it vulnerable to packet sniffing. Therefore, DNS resolution should also be secured/encrypted.

SNMP (Simple Network Management Protocol): SNMP is used to manage networks. Each managed device has a software agent installed that reports issues and problems to a centralized SNMP management server. Versions 1 and 2 of SNMP sent all data as clear text. SNMP v3 encrypts all data. In all cases, SNMPv3 should be used. The detailed network information being sent by SNMP is sensitive enough that it should never be sent in clear text. SNMP is based on the manager/agent model. The manager runs on the server, and the agent runs on the client computers. Three important constituents of SNMP are a manager, an agent, and a database of management information. The manager provides the interface between the human network manager and the management system. The agent provides the

interface between the manager and the physical device(s) being managed. The manager and agent use a Management Information Base (MIB) and a set of commands to exchange information.

Lightweight Directory Access Protocol (LDAP): LDAP is a directory protocol that contains literally all the information about your network. It lists all directory services, servers,workstations, users, etc. An attacker would find this information very useful. Therefore, it is recommended that you encrypt this traffic with TLS. Anytime you have a concern about any attacker enumerating your network, you should use LDAPS.

Syslog stands for System Logging Protocol and is a standard protocol used in Linux systems to send system log or event messages to a specific server, called a syslog server. Journalctl is the command that is used to view these logs.

NXLog: This tool suite is capable of handling syslog-type data as well as other log formats, including Microsoft Windows.

Syslog, rsyslog, and syslog-ng all move data into log files on a log server. Rsyslog and syslog-ng both extend the original syslog standard by adding capabilities such as content filtering, log enrichment, and correlation of data elements into higher-level events.

IPFIX works like NetFlow, identifying which machines are communicating with each other. The primary purpose of IPFIX is to provide a central monitoring station with information about the state of the network. IPFIX is a push-based protocol,where the sender sends the reports and receives no response from the receiver.

Previous Contents Next

CompTIA® Security+ Exam Notes : Purpose For Frameworks,and Secure Configuration Guides

examguides.com/security+/security+14.htm

3. Architecture and Design

3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides

Web Server:

All web applications such as Web servers, News servers, email servers etc. need to be configured as secure as possible. This can be achieved by

- Removing all unnecessary services. These are the services that are installed but not used. For example, you might have installed TFTP, but not using it. It is better to remove the application or service that is not used as it may provide an opportunity to a hacker to abuse the resource.
- Remove all unnecessary protocols: These are the protocols that are installed but not used. For example, you might have installed Novell Netware protocol but not necessary. It is preferable to remove that protocol.

Enable server and application logs: The logs provide an opportunity to look into the activity on the server over the past few hours or days. Check for any unusual activity such as failed login attempts etc.

Example: You are administering a web server that is hosting an e-commerce web site for your company. The manufacturer of the web server has released a new patch that plugs some critical security loopholes. What needs to be done?

Solution: *It is wise to implement software updates on a web server located in the lab, and then implement the same on production web server. It is also important to take a backup of the web server before implementing any software updates. In the event that anything goes wrong during the update, you can always restore the systems back to its previous state using the backup.*

Previous Contents Next

CompTIA® Security+ Exam Notes : Implementing Secure Network Architecture Concepts

examguides.com/security+/security+15.htm

3. Architecture and Design

3.2 Given a scenario, implement secure network architecture concepts

The following are the basic types of firewall architectures:

1. Bastion host: A bastion host typically has two network cards, one connected to the Internet and the other to the internal network. A firewall or a proxy is installed on the bastion host providing separation of Internet from the internal network. It can also be a router providing NAT or something similar to it.

2. Screened host gateway: It is implemented with a router (Internet end) in series with a bastion host (acting as application gateway). The router filters the packets, and the application gateway routes the packets to appropriate host computers on the internal network and vice versa.

3. Screened subnet gateway (or DMZ): It includes two screened gateway devices, one each on either side of the bastion host. The arrangement involves two sebnets one on each side of the bastion host. The arrangement is also known as DMZ (De Militarized Zone). DMZ is considered most secure of the three discussed here since the internal network is separated by a DMZ.

SSL(Secure Sockets Layer) or more correctly TLS (Transport Layer Security) is a method of offloading the processor-intensive public-key encryption algorithms involved in SSL transactions to a hardware accelerator. An SSL accelerator does not have sniffer functionality. Since encrypting data is very processor-intensive, SSL accelerators can be used to offload the public-key encryption to a separate plug-in card.

Load Balancer: A load balancer can be implemented as a software or hardware solution and is usually associated with a device - a router, a firewall, NAT, and so on. As the name implies, it is used to shift a load from one device to another.

Proxy Firewall: Proxy firewalls are used to process requests from an outside network; the proxy firewall examines the data and makes rule-based decisions about whether the request should be forwarded or refused

Correlation engines : A correlation engine is a software application that programmatically understands relationships. Correlation engines are used in SIEM Security information and event management (SIEM) systems to aggregate, normalize and analyze event log data, using predictive analytics and fuzzy logic to alert the systems administrator when there is a problem.

Scenario: Your company hosts its own web server and email server. You intend to secure the internal resources of the Company using a DeMilitarized Zone (DMZ). To create DMZ what do you need?

Solution: *If a company intends to host its own servers to be accessed from public Internet, a DMZ is the most preferred solution. The network segment within the DMZ is secured by two firewalls, one interfacing with the public Internet, and the other interfacing the internal corporate network. Thus, a DMZ provides additional layer of security to internal corporate network. The type of servers that are hosted on DMZ may include web servers, email servers, file servers, DNS servers, etc.*

The employees of a Company typically use Intranet within the Company. The customers and vendors of the Company use Extranet.

Extranet: An Extranet is basically an extension of Intranet using public Internet. A typical use is when a Company has multiple vendors and do the order processing, and inventory control on-line.

Note that, on the other hand, Internet is accessible to everybody, i.e. general public.

The benefit of implementing Intranets and Extranets is security and customization. Intranets and Extranets are relatively safe because general public cannot access these networks. Intranets and Extranets are usually connected securely by means of Virtual Private Network (VPN).

CompTIA® Security+ Exam Notes : Implementing Secure Systems Design

examguides.com/security+/security+16.htm

3. Architecture and Design

3.3 Given a scenario, implement secure systems design

Hardware and Firmware Security:

Hardware Security Modules (HSMs) are devices that handle digital keys. They can be used to facilitate encryption as well as authentication via digital signatures. Most HSMs support tamper-resistant mechanisms. A hardware security module uses RSA keys, but not a storage root key.

The process of securing a computer system is called Hardening. There are several things that one need to remember for hardening a PC. These include:

1. Removing non-essential programs, and services. These may provide back-doors for an attacker.

2. Installing an anti-virus package, and a spyware remover

3. Removing unnecessary protocols. If you are using only TCP/IP (required for connecting to the Internet), keep that protocol and remove all other protocols.

4. Disable guest account

5. Rename Administrator account

6. Enable auditing, so that you can view any logon attempts.

7. Installing latest patches, and service packs to operating system, and software.

Instant Messaging (IM): IM, unless otherwise encrypted, transmits all messages in clear text. This makes IM vulnerable to sniffing. Additionally, several IM clients come with advanced features like File Transfer. Such features may allow a hacker to gain access to your system, and transmit viruses.

Application hardening is the process of applying most recent patches and bug fixes to make the applications more robust, thus discouraging an attacker from exploiting the bugs in the application.

Disabling the use of removable media such as USB drive will prevent data being stolen to some extent.

For detecting spamware and virus, one need to install anti spamware, and anti virus programs. Installing the latest updates to Operating Systems will protect your system from exploits (like gaining back-door entry), but not necessarily from downloaded virus or spamware.

Example: A company has 10 staff working on hourly wages at a rate of $50 per hour. The systems are not virus protected, and the company is contemplating an anti-virus package that costs $1000 per year. It is estimated that 50% of the systems fail and the average restoration time is 6 hours. If the company implements the anti virus solution, what is the expected savings per year?

Solution: *The number of machines that are likely to have restored: 5 (50% chance of getting infected)*

Average time for restoration per machine: 6 hours

Man power cost per hour: 50

Total cost for restoration: 5 multiplied by 6 multiplied by 50 or $1500.

Cost of anti virus software: 1000

Therefore net savings: 1500 - 1000 or $500.

Example: You want to prevent the computer users from copying any data to external removable storage media. You have disabled floppy disk drives, and ensured that the computers are configured with read-only DVD drive. What do you need to do further achieve the objective?

Solution: *The objective is to prevent the users from copying the computer files to any removable storage media. The floppy disk is already removed, and the CD/DVD drives are made to read-only. Therefore, you need to disable all USB ports in the system BIOS and then password protect the system BIOS. If not password protected, users may enable the USB ports again.*

1. You should not disable hard disk drive in the system BIOS. This may result in the computer not booting up

2. Flashing is the method used to update the BIOS, and is not necessary unless otherwise required.

3. If you disable hard drive controllers, the hard disk stops working. Again, this may result in the hard disk not working at all.

Given below are some of the precautions that may be required to secure the local network resources:

1. Rename default accounts so that blind attacks will not succeed

2. Use strong passwords and change passwords periodically

3. Secure the server rooms with lock and key

4. Use strong encryption for user names and passwords

Note that disabling local admin access is not an option because your manager wants to administer the servers locally. Anti virus software will not protect a server from un-authorized login.

TPM (Trusted Platform Module): TPM is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). A Trusted Platform Module (TPM) includes a storage root key. The TPM generates this key when a user activates the TPM.

NT File System (NTFS): NTFS supports encryption with Encrypting File System (EFS). However, it is a software based encryption system. TPM is a hardware chip on the computer's motherboard that stores cryptographic keys used for encryption. Many laptop computers include a TPM, but if the system doesn't include it, it is not feasible to add one. The TPM includes a unique RSA key burned into it, which is used for asymmetric encryption. Additionally, it can generate, store, and protect other keys used in the encryption and decryption process. TPMs can also be used to facilitate FDE.

A hardware security module (HSM) and a Trusted Platform Module (TPM) both provide full disk encryption, but cannot block documents sent to a printer or an external network.

Application whitelisting/blacklisting

Whitelisting identifies what software (applications) can be installed on a computer (or a server or any mobile device) and prevents users from installing or running any other software.

Converse of Whitelisting is Blaclisting. Blacklisting identifies which software/applications should not be installed on a system

Full disk encryption (FDE): FDE is encrypting the entire disk, rather than a specific file or folder. This is recommended for full security of the system. Microsoft, beginning with Windows 7, offers BitLocker on the professional and higher versions of its operating system.

Self-Encrypting Drive (SED): SED has a controller chip built into it that automatically encrypts the drive and decrypts it, provided the proper password is entered. The encryption key used in SEDs is called the media encryption key (MEK). Locking and unlocking a drive requires another key, called the key encryption key (KEK), supplied by the user. The KEK is used to decrypt the MEK, which in turn is what encrypts and decrypts the drive.

You are configuring a computer running Windows Server 2008 R2 for use as a network email server. You want to ensure that the most recent updates have been applied to the server. What should you do?

You need to follow the manufacturer's recommendation regarding updates. Microsoft recommends that you enable automatic updates on your client as well as server operating systems so that the latest patches and fixes may be applied.

A Linux or UNIX file with the permission 755 means rwx for the owner, rx for the group and others. 4 = read(r), 2 = write (w), and 1 = execute(x). In the question, the owner permission is 7, the group permission is 5 and others permission is also 5.

Sandboxing: Sand box refers to using software and/or hardware in a test environment. In sandbox environment, all the machines work as usual. However, they are not yet put to actual production. Dummy loads are applied as if they were in production environment. Any glitches or overload conditions as well as security related tests are made, and necessary fixes may be applied during this period. It is a testing environment that isolates untested code changes and outright experimentation from the production environment.

Previous Contents Next

CompTIA® Security+ Exam Notes : Secure Application Development And Deployment Concepts

examguides.com/security+/security+17.htm

3. Architecture and Design

3.4 Summarize secure application development and deployment concepts

Baselining: The process of establishing standards for security of computers in your network is called security baselining. A security baseline will include control over services, permissions on files, Registry permissions, authentication protocols, and more. There will be a security baseline established for each type of computer in your organization. This will include domain controllers, file servers, print servers, application servers, clients, etc.

Deployment Life cycle models:

- The **waterfall method** has these steps: requirements gathering, design, implementation (also called coding), testing (also called verification), deployment, and maintenance. Each stage is completely self-contained. Once one stage is completed, then you move on to the next stage. This approach is appropriate for situations wherein the requirements are clearly defined well in advance.
- **Agile** is a method of software development meant to be rapid.
- **DevOps** is the practice of operations and development engineers participating together in the entire service lifecycle, from design through the development process to production support.
- **Scrum** is an agile framework for managing work with an emphasis on software development.

Fuzz testing or fuzzing: Fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks.

Hardening: The Windows Registry is where configuration parameters for the OS and applications are stored. It is not associated with the Root of Trust,as it is not even accessible during the establishment of this trust chain.

Root of Trust: Root of Trust refers to a condition by which the hardware and BIOS work together to ensure the integrity of the BIOS and all subsequent software and firmware loads. Once complete, this forms a Root of Trust that can be attested to via the TPM chip. Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM.

Unified Extensible Firmware Interface (UEFI) A specification that defines the interface between an OS and the hardware firmware. This is a replacement to BIOS.

DLP: Data Loss Prevention (DLP) solutions serve to prevent sensitive data from leaving the network without notice.

HIDS: Host-based intrusion detection systems (HIDSs) act to detect undesired elements in network traffic to and from the host.

HIPS: A host-based intrusion prevention system (HIPS) is a HIDS with additional components to permit it to respond automatically to a threat condition.

Note: Remember that HIDS can only detect malicious activity and send alerts. HIPS, on the other hand, can detect and prevent attacks.

FDE: Self-encrypting drives (SEDs) and full disk encryption (FDE) are methods of implementing cryptographic protection on hard drives and other similar storage media, even if the drive is removed from the machine.

EDR: Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

The primary functions of an EDR security system are to:

1. Monitor and collect activity data from endpoints that could indicate a threat

2. Analyze this data to identify threat patterns

3. Automatically respond to identified threats to remove or contain them, and notify security personnel

4. Forensics and analysis tools to research identified threats and search for suspicious activities

Intel's Field-Programmable Gate Array (FPGA) allows system designers to easily make changes to the code embedded on the chip. Arduino UNO is a micro-controller that runs a single instruction repeatedly. Raspberry Pi is a mini-computer and operating system that runs on embedded components. A Subscriber Identity Module (SIM) holds the activation information on cell phones or smartphones. Wearables and smart devices are not embedded systems.

Previous Contents Next

CompTIA® Security+ Exam Notes : Summarize Cloud And Virtualization Concepts

examguides.com/security+/security+18.htm

3. Architecture and Design

3.5 Summarize cloud and virtualization concepts

Cloud Deployment Models:

IaaS: In the Infrastructure as a Service (IaaS) model, the consumer can "provision" and is able to "deploy and run," but they still do not "manage or control" the underlying cloud infrastructure.

PaaS: In the Platform as a Service (PaaS) model, the consumer has the ability to create applications and host them.

SaaS: In the Software as a Service (SaaS) model, the consumer has the ability to use applications provided by the cloud provider over the Internet.

SecaaS: Security as a Service (SecaaS) offers a way for enterprises to access security services that are robust, scalable and cost effective. SECaaS is a subscription-based business model intended to be more cost effective than smaller individuals/corporations.

Different cloud models are explained below:

Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but that are bound together by standardized or proprietary technology enabling data and application portability.

SOAR: SOAR stands for Security Orchestration, Automation, and Response. The term is used to describe three software capabilities - threat and vulnerability management, security incident response and security operations automation. SOAR allows companies to collect threat-related data from a range of sources and automate responses to most commonly encountered threats.

Managed service provider (MSP)/managed security service provider (MSSP): A managed service provider (MSP) is a company that remotely manages a customer's IT infrastructure. A managed security service provider (MSSP) does the same thing as a third party that manages security services. A third-party service is usually expensive and suitable for medium and large companies.

Anything as a service (XaaS): XaaS describes a wide array of services that can be delivered to users from the cloud services. It recognizes the vast number of products, tools, and technologies that are now delivered to users as a service over the internet.

Common Vulnerability Scoring System (CVSS): It is an open framework for communicating the characteristics and severity of software vulnerabilities. This does not include incident response system.

Remote-Access Trojan (RAT): A set of malware designed to exploit a system providing remote access. It is a malware program that includes a back door for administrative control over the target computer. RATs usually accompany a known user-requested program such as a game or sent as an email attachment without the users knowledge.

Virtualization

Virtualization sprawl: Virtualization sprawl is a phenomenon that occurs when the number of virtual machines (VMs) on a network reaches a point where the administrator can no longer manage them effectively. Virtualization sprawl may also be referred to as virtual machine sprawl, VM sprawl or virtual server sprawl.

How to Prevent Virtualization sprawl

Audit Vms: It may seem like a simple solution, but make it a policy that every VM and virtual server must be documented and registered.

Optimize storage and implement data policies: To prevent the usage of unnecessary disk and storage space, use technologies like snapshots and thin provisioning.

Implement lifecycle management tools: To keep track of all virtual machines, as well as virtual servers, it's a good idea to use a lifecycle management tool. With such a tool, it's possible to provide virtual machines only for the users of one specific project or track all objects within a centralized database. When a project is finished, it's far easier to identify unneeded or unused VMs for secure erasure.

Implement VM archiving: Many users create virtual machines just for one project, use it a couple of times, and then leave it untouched for months. Instead of keeping these VMs inside the production environment, they should be archived. Many backup solutions provide the possibility to archive unused VMs on cheaper storage or tape.

Sandboxing: Sandboxing involves running applications in restricted memory areas. It limits the possibility of an application crash, allowing a user to access another application or the data associated with it.

Patch Management: Patch management ensures that systems and applications stay up to date with current patches.

Physical security controls: A physical security control is something you can physically touch, such as a hardware lock, a fence, an identification badge, and a security camera

Virtualization enables virtual servers be installed instead of physical servers, thus reducing the cost of ownership.

A failover cluster is a group of servers that work together to maintain high availability of applications and services. Obviously, it increases the cost.

Archiving is the process of taking backups, and it does not help in making services available.

Previous Contents Next

CompTIA® Security+ Exam Notes : Explain How Resiliency And Automation Strategies Reduce Risk

examguides.com/security+/security+19.htm

3. Architecture and Design

3.6 Explain how resiliency and automation strategies reduce risk

Resilient systems: Resilient systems are those that can return to normal operating conditions after a disruption. You can improve the resiliency of your systems, and thereby reduce risk associated with their failure, through the proper use of various configuration and setup strategies, such as snapshots and the capability to revert to known states, and by implementing redundant and fault-tolerant systems. Automation is used to improve efficiency and accuracy when administering machines using commands.

Automation/Scripting: Automation is the control of systems on a regular scheduled,periodic or triggered basis that does not require manual interaction. Automation includes concepts such as scheduled backups,archiving of log files,blocking of failed access attempts,. It can be implemented by scripting. Scripting is the crafting of a file of individual lines of commands that are executed one after another.

Templates: A template is a preestablished starting point . The template is likely to produce more consistent and reliable results.

Elasticity: Elasticity is the ability of a system to adapt to workload changes by allocating or provisioning resources in an automatic responsive manner. Elasticity is the common feature of cloud computing , where additional system resources or even hardware resources can be provisioned to a server when its demand for services increases.

Scalability: Scalability is the ability for a system to handle an ever-increasing level or load of work. It can also be the potential for a system to be expanded to server. In the event of failure of the primary server, the secondary or redundant server can immediately take over and replace the primary server in providing services to the network.

High Availability: Availability is the assurance of sufficient bandwidth and timely access to resources. It is the availability of a system has been secured to offer very reliable assurance that the system will be online, active, and able to respond to requests in a timely manner, and there will be sufficient bandwidth to accomplish requested tasks in the time required.

RAID: RAID short for Redundant Array of Inexpensive Disks can be used to provide fault tolerance on a computer. There are several RAID levels such as RAID 1, RAID 5, etc. RAID 1 provides disk mirroring, where as RAID 5 provides striping with parity and minimum 3 disks are required for RAID 5.

Clustering: Clustering is a technique where two or more computers are clustered and share the load. If one computer fails, the other computer's take the load off the failed computer. Clustering is more expensive and requires two or more computers.

Automation/scripting

1. Continuous Monitoring: Continuous Monitoring is used to enable rapid detection of compliance issues and security risks.

2. Continuous Validation: Continuous Validation is the extension of testing to support the software development that occurs in DevOps by team members. As code is changed in the DevOps process, the new code is tested against the existing codebase to ensure functionality and stability.

3. Continuous Integration: Continuous Integration (CI) is the practice of automating the integration of code changes from multiple contributors into a single software project. It's a primary DevOps practice, allowing developers to frequently merge code changes into a central repository where its validated and integrated.

4. Continuous Delivery: Continuous delivery is an extension of continuous integration since it automatically deploys all code changes to a testing and/or production environment after the build stage.

This means that on top of automated testing, you have an automated release process and you can deploy your application any time by clicking a button.

5. Continuous Deployment: Continuous Deployment (CD) is a software release process that uses automated testing to validate if changes to a codebase are correct and stable for immediate autonomous deployment to a production environment.

After delivery, the software may be first tested in a test bed or deployed in production environment, as decided by the project manager. For large projects, sand box deployment is done before production release.

CompTIA® Security+ Exam Notes : Explain The Importance Of Physical Security Controls

examguides.com/security+/security+20.htm

3. Architecture and Design

3.7 Explain the importance of physical security controls

Some security controls frequently used for server's devices are given below. Some of these are the same as the mobile devices, and some are unique for servers:

Strong password: Any time a password is used to protect a mobile device (or any device or system), it should be strong. This means they are at least eight characters and include multiple character types, such as upper case, lower case, numbers, and symbols.

Least privilege: Least privilege is a technical control. It specifies that individuals or processes are granted only those rights and permissions needed to perform their assigned tasks or functions. Rights and permissions are commonly assigned on servers, but rarely on mobile devices such as tablets and smart-phones.

Data encryption: Encryption protects the confidentiality of data on servers just as it can protect the confidentiality of data on mobile devices. It's possible to selectively encrypt individual files or entire disk volumes.

Mantrap and cipher lock: These are examples of physical security and they can be used to restrict access to a server room. A man-trap refers to a small space having two sets of interlocking doors such that the first set of doors must close before the second set opens. Identification is usually required for each door. One door may use a token and the other may use some biometric parameter to provide access. "Man-traps" may be configured so that when an alarm is activated, all doors lock and trap the suspect between the doors in the "dead-space". A man-trap usually allows only one person at a time. If multiple persons try to enter, a security alarm may be raised.

Proximity lock: This secures the Server by locking it when the sensor (say a blue-tooth device worn by the administrator) is not within a specified distance from the server.

Firewall: Software-based firewalls are commonly used on servers but are extremely rare on mobile devices.

TPM and HSM. Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs) are hardware encryption devices.

Note that Remote Wipe, GPS tracking, Cable lock, and Screen Lock are typically used with mobile devices.

Biometrics is the ability measure physical characteristics of a human such as fingerprints, speech etc. These measured values are then used for authentication purpose. Given below are few of the measurable quantities:

- Fingerprint: Scans and matches finger print to a securely stored value.
- Voiceprint: Identifies a person by measuring speech pattern.
- Iris profile: Identifies a person by using Iris part of the eye.
- Signature: Matches an individual's signature with the stored value.

Cable Lock : If your laptop rarely leaves your home and the house itself has good security, you may not want to bother with a laptop cable lock. However, if you're using the laptop in a place where a lot of people have access to it, like a university library or an unsupervised lab, you'd really benefit from a lock. According to one research, college dorms are another hotspot for notebook theft.

Most laptops have some kind of security slot built into their chassis. Locks can connect to this opening, which makes it hard for a thief to pull them out.

There are other types of cable locks which may differ in the way that they secure your laptop, but essentially perform the same function. If you own a MacBook or another laptop that doesn't have a built-in lock slot, you can buy a slot on a plate that superglues onto the lid, like Kensington's Security Slot Adapter kit and then use a standard Kensington lock.

Fingerprint scanners : are security systems of biometrics. A fingerprint scanner identifies and authenticates the fingerprints of an individual in order to grant or deny access to a computer system or a physical facility.

Tablet with Finger Print Scan

As may be seen in the figure above, a finger print scanner is frequently integrated with laptops, mobiles, and tablet PCs.

In employer issued laptops, the employer usually ties the laptop with the employee so that the machine is not misused by any other person, and the data is secure.

Advantages of fiber optic cable over CAT5 cable include the following:

1. It provides communication over longer distance

2. It is difficult to tap into a fiber optic cable

3. It provides higher communication bandwidth

4. It is more immune to external interference

However, from security point of view, two chief advantages are

a. difficulty to tap and

b. immunity to external interference, which makes the communication not easily interruptible.

Fire Suppression:

There are five types of extinguishers:

a. Water

b. Dry chemical

c. Halon

d. Carbon dioxide

e. Foam

Water is used with Class A fires. Regular dry chemical extinguishers have a sodium bicarbonate base and are effective on Class B and C fires. Carbon Dioxide Extinguishers are used primarily on Class C fires and are also effective on Class B fires. Halon Extinguishers are best used on Class B or C fires. Foam extinguishers are less commonly used.

There are primarily 5 classes of fire:

- Class 'A' Fire: Involves ordinary combustible materials such as wood, cloth and paper. Most fires are of this class.
- Class 'B' Fire: Involves flammable liquids or liquid flammable solids such as petrol, paraffin, paints, oils, greases and fat.
- Class 'C' Fire: Involves gases. Gaseous fires should be extinguished only by isolating the supply. Extinguishing a gas fire before the supply is off may cause an explosion.
- Class 'D' Fire: Involves burning metals. These should only be dealt with, by using special extinguishers, by personnel trained in the handling of combustible metals.
- Class 'F' Fire: Involves flammable liquids (Deep Fat Fryers)
- The first three classes are most common.

Logs: Computer log files can be tampered with by a hacker to erase any intrusions. Computer logs can be protected using the following methods:

1. Setting minimal permissions

2. Using separate logging server

3. Encrypting log files

4. Setting log files to append only

5. Storing them on write-once media

Implementing all the above precautions ensures that the log files are safe from being tampered.

Three widely used logs in Windows OS are:

Application log: The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The developer decides which events to record.

System log: The system log contains events logged by the Windows operating system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are

predetermined.

Security log: The security log can record security events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.

Antivirus log: Antivirus log analyzer can process log files from various antivirus packages and generate dynamic statistics from them, analyzing and reporting events.

Faraday cage: A Faraday cage consists of an electrically conductive wire mesh or other conductor woven into a "cage" that surrounds a room that needs to be secured. The conductive cage is then grounded. This arrangement provides a ground path to electromagnetic signals that are emanating from the computer room. Only the signals that are routed through physical cables can make it outside the Faraday cage. Faraday cage is useful in securing a computer system from leaking any information outside the room.

HVAC: HVAC is an acronym for heating, ventilating and air conditioning. As the name represents, HVAC system designer will take care of heating, ventilation, and air conditioning of the facility. Preventing fire is done by fire extinguishers, and are not necessarily a part of HVAC. Similarly, EMI shielding and physical security are not part of HVAc.

Previous Contents Next

CompTIA® Security+ Exam Notes : Compare And Contrast Identity And Access Management Concepts

examguides.com/security+/security+21.htm

4. Identity and Access Management

4.1 Compare and contrast identity and access management concepts

The five factors of authentication are given below:

1. Something you know, such as a username and password

2. Something you have, such as a smart card, PIV, or a token

3. Something you are, using biometrics, such as fingerprint or retina scan

4. Somewhere you are, such as your location using geolocation.

5. Something you do, such as gestures on a touch screen

However, first three factors are widely recognized factors of authentication. "Somewhere you are" and "something you do" are not widely recognized. For example, if you use "somewhere you are" as authentication, some one else may come in to you position (geographically speaking) at a later time and claim access to the resource. Similarly, repeatability of hand gestures is questionable, and it may lead to uncertainty in identifying the user with certainty. Some experts doubt that 4 and 5 could be used a factors of authentication at all, because one of the requirements of factor of authentication is that it should be able to be used as a stand alone method of authentication.

Authentication Types:

Mutual authentication: Here both the server and client computers authenticate each other. This type of authentication is more secure than one-way authentication, where only the client is authenticated.

Multifactor authentication: Here two or more number of authentication methods are used for granting access to a resource. Usually, it combines a password with that of a biometric authentication.

MFA combines two or more independent credentials (factors). The five broadly known independent credentials are:

1. What the user knows (password),

2. What the user has (security token)

3. What the user is (biometric verification).

4. Where the user is

5. What the user is doing

The goal of MFA is to create a layered defense and make it more difficult for an intruder to access a target such as a physical location, computing device, network or database.

Note that Authentication methods using two or more variables in the same factor still constitute single-factor authentication. For example, a password and a PIN are both in the something you know category, so they can only provide single-factor authentication even when they are used together.

Biometric authentication: Biometric authentication uses measurable physical attributes of a human being such as signature, fingerprint.

CHAP: It is an authentication type that uses three-way hand shake. The passwords are transmitted in encrypted form ensuring security. Compare this with PAP, which transmits passwords in clear text.

Four important aspects of security are authentication, authorization, integrity, and non-repudiation.

- Authentication refers to identifying a user or a system. For example, when you logon to an FTP server, it is authenticating you after verifying the user name, and password.

- Authorization refers to the right to access data. For example, after accessing a remote FTP server, you may be allowed to transfer files only to your home folder but not to other folders.
- Integrity ensures that the data is not compromised. A simple integrity checker is parity. By ensuring that the parity of a transmitted message is correct, you can accept the message. For complex systems, where confidential information is involved, encryption is used for verifying the integrity of a transmitted message.
- Non-repudiation ensures that the sender, as well as the receiver cannot refuse having sent or received a message. For example, you receive an email from your perspective employer. By using an unsigned email, it might so happen that your employer later denies having sent any such email. Non-repudiation ensures that neither the sender nor the receiver can deny the transmission or the reception of a message respectively.
- Non-repudiation ensures that the sender of a message or contract can not refuse having sent the message or signed the contract at a later date. This is done by mean of digital signature.

Single sign-on: Single sign-on enables one to use all the eligible services with one sign-in.

1. SSO is used for authenticating a user across multiple platforms without having to login each time.

2. Security Assertion Markup Language (SAML) is an XML- based data format used for SSO on web browsers

3. Normally, SSO provides authentication only. Using SSO, an authenticated user will be able to move from one website to another trusted website without having to sign-on again.

4. SAML provides SSO for web-based applications.

5. SAML is used to exchange authentication and authorization information between different parties.

Client Authentication: A client authenticating itself to a server and that server authenticating itself to the client in such a way that both parties are assured of the others' identity is known as mutual or two-way authentication.

Always try to download, and apply latest patches and service packs (if any) directly from the manufacturer's website. Downloading from unreliable sources may compromise the system security.

Message Authentication Codes (MACs): MAC also called "keyed hashes", are used to verify the authenticity of a message. Let us say, Jane (the sender of a message) and Mike (the recipient) share a secret key. Jane uses the message and the key to compute the MAC, and

sends the MAC along with the message. When Mike receives the message, he computes the MAC, and then checks to see if his MAC matches Jane's. If it does, then he knows the message is from Jane and that nobody has changed it since she sent it.

Previous Contents Next

CompTIA® Security+ Exam Notes : Install And Configure Identity And Access Services

examguides.com/security+/security+22.htm

4. Identity and Access Management

4.2 Given a scenario, install and configure identity and access services

Usually the user names and passwords are transmitted in plain text. But this kind of transmission of authentication details is not secure. Any body with a packet sniffer can read the login and password.

Kerberos : Kerberos is basically an authentication protocol that uses secret-key cryptography for secure authentication. In Kerberos, all authentication takes place between clients and servers. The name Kerberos comes from Greek mythology; it is the three-headed dog that guarded the entrance to Hades. It was developed by the Massachusetts Institute of Technology, USA. Kerberos require that the time sources are approximately in synchronization (with in 5 minutes) with each other. However, with recent revisions of Kerberos software, this rule has become flexible. It is an authentication protocol uses a Key Distribution Center (KDC) to orchestrate the process. The KDC authenticates the principal (which can be a user, program, or system) and provides it with a ticket. After this ticket is issued, it can be used to authenticate against other principals.

- When a user first authenticates to Kerberos, he talks to the Authentication Service on the KDC to get a Ticket Granting Ticket (TGT). This ticket is encrypted with the user's password.

- When the user wants to talk to a Kerberized service, he uses the TGT to talk to the Ticket Granting Service (TGS, also runs on the KDC). The TGS verifies the user's identity using the TGT and issues a ticket for the desired service.
- The TGT ensures that a user doesn't have to enter in their password every time they wish to connect to a Kerberized service. The TGT usually expires after eight hours. If the Ticket Granting Ticket is compromised, an attacker can only masquerade as a user until the ticket expires.

The following are the important properties of Kerberos:

1. It uses symmetric encryption

2. Tickets are time stamped

3. Passwords are not sent over the network

4. Tickets are time stamped

5. Passwords are not sent over the network

Some of the features of Kerberos authentication system:

1. Uses client-server based architecture.

2. Kerberos server, referred to as KDC (Key Distribution Ceter) implements the Authentication Service (AS) and the Ticket Granting Service (TGS).

3. The term "application server" generally refers to Kerberized programs that clients communicate with using Kerberos tickets for authentication purpose. For example, the Kerberos telnet daemon (telnetd) is an example of an application server.

4. Unlike other authentication protocols (FTP, PAP, etc. which transmits passwords over the network) passwords are not transmitted over the network.

Kerberos uses port 88 by default. FTP uses port 21, https uses port 443, and SNMP uses port 161.

CHAP (Challenge Handshake Authentication Protocol): CHAP works on point to point connections. It uses a three step process for authentication (excluding making the connection itself). If making the connection is also involved, it would be a 4 step process.

The **PAP (Password Authentication Protocol)** transmits login and password in clear text. CHAP, MS-CHAT, and MS-CHAP-v2 encrypt the login credentials while transmitting on the network.

SAML(Security Assertions Markup Language): The Security Assertion Markup Language is an open standard that allows security credentials to be shared by multiple computers across a network. SAML is an XML-based data format used for Single Sign On (SSO) on web browsers

SAML defines three roles:

1. Principal: This is normally a user. The user logs on once.

2. Identity provider: An identity provider creates, maintains, and manages identity information for principals. An Identity Provider (IdP), sometimes called an Identity Service Provider or Identity Assertion Provider, is an online service or website that authenticates users on the Internet by means of security tokens.

The normal Identity Provider process is:

- Accept a SAML authentication request from the Service Provider a user wants to access.
- Authenticate the user against your organization's existing authentication service.
- Collect user data from your organization's existing data stores;
- Apply policy to control what data is released to which Service Provider.
- Securely transmit the collected information to the Service Provider.

3. Service provider: A Service Provider (SP) is an entity that provides Web Services like Application Services, Storage Services, etc. An SP provides provides services to principals. When a user tries to access a website, the service provider redirects the user to an identity provider for authentication.

LDAP: LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other programs use to look up information from a server. Secure LDAP encrypts transmissions with SSL or TLS

AAA: Authentication, Authorization and Accounting (AAA) is a system for tracking user activities on an IP-based network and controlling their access to network resources. AAA is often is implemented as a dedicated server. Examples of AAA protocol include RADIUS and TACACS+ .

RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a mechanism that allows authentication of remote and other network connections. Originally intended for use on dial-up connections. Radius enables a single server to become responsible for all remote-access authentication, authorization, and auditing (or accounting) services. It is an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes

access to the ISP network. RADIUS implements a client/server architecture, where typical client is a router, switch, or AP and the typical server is a Windows or Unix device that is running RADIUS software.

TACACS: Short for Terminal Access Controller Access Control System, is a client-server-oriented environment, and it operates in a manner similar to RADIUS. Extended TACACS (XTACACS) replaced the original version and combined authentication and authorization with logging to enable auditing.

TACACS+: a TCP-based access control protocol, TACACS+ allows a device to forward a user's username and password to an authentication server to determine whether access can be allowed. TACACS+ itself can also act as an authentication server, if configured so. TACACS+ can also provide authorization and accounting services. TACACS+ services are maintained in a database on a server with TACACS+ daemon running, typically, on a UNIX or Windows workstation. It provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service authentication, authorization, and accounting independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service.

Previous Contents Next

CompTIA® Security+ Exam Notes : Implement Identity And Access Management Controls

examguides.com/security+/security+23.htm

4. Identity and Access Management

4.3 Given a scenario, implement identity and access management controls

Access Control Models:

Computer based access controls prescribe not only who or what process may have access to a given resource, but also the type of access that is permitted. These controls may be implemented in the computer system or in external devices. Different types of access control are:

1. Mandatory access control

2. Discretionary access control

3. Rule based access control

4. Role based access control

Mandatory Access Control (MAC) secures information by assigning sensitivity labels on objects (resources) and comparing this to the level of sensitivity a subject (user) is operating at. MAC ensures that all users only have access to that data for which they have matching or greater security label (or security clearance). In general, MAC access control mechanisms are more secure than DAC. MAC is usually appropriate for extremely secure

systems including multilevel secure military applications or mission critical data applications. Sensitivity labels are associated with Mandatory Access Control (MAC). Here the access control is determined by the security policy of the system. The object owner or the user have almost no control over the resource.

Discretionary Access Control (DAC): Discretionary Access Control (DAC) is a means of restricting access to information based on the identity of users and/or membership in certain groups. Access decisions are typically based on the authorizations granted to a user based on the credentials he presented at the time of authentication (user name, password, hardware/software token, etc.). In most typical DAC models, the owner of information or any resource is able to change its permissions at his discretion. DAC has the drawback of the administrators not being able to centrally manage these permissions on files/information stored on the web server.Here the access control is determined by the owner of an object.

Role Based Access Control (RBAC): In Role-Based Access Control (RBAC), access decisions are based on an individual's roles and responsibilities within the organization. For instance, in a corporation, the different roles of users may include those such as chief executive, manager, executive, and clerk. Obviously, these members require different levels of access in order to perform their functions, but also the types of web transactions and their allowed context vary greatly depending on the security policy. In Role Based Access Control, the administrator sets the roles. Therefore, this type of access control is sometimes considered as a subset of MAC. As the name suggests, the access to an object is determined by the role of an employee. Users are assigned roles first and then the permissions are assigned to roles.

Rule Based Access Control (RBAC): The access to a resource in Rule Based Access Control is based a set of rules. ACLs (Access Control Lists) are used for this type of access control. In Rule Based Access Control, the administrator sets the rules. Therefore, this type of access control is sometimes considered as a subset of MAC.

Note that the divisions do not want the information to be made available to the group personnel only. A role based access control is suitable under this situation because it provides security, as well as flexibility. Here individual users are given privileges based on their respective roles in the organization rather than by name.

Using Discretionary Access Control (DAC), the access rights for resources are controlled by the owner of a given resource.

Tokens: A token can be a physical device such as a smart card or an electronic process such as RSA's SecureID token. Tokens provide one of the most secure authentication environments, because typically a token is unique to a user, and it is difficult to spoof.

Physical tokens are usually smart cards that a user must have on him to access a network resources. Smart card is an example of physical token, where as SecurID, from RSA is basically an electronic token that could be implemented as software token or as a hardware token.

Smart card: Smart cards usually come in two forms. The most common takes the form of a rectangular piece of plastic with an embedded microchip. The second is as a USB token. It contains a built in processor and has the ability to securely store and process information. A "contact" smart card communicates with a PC using a smart card reader whereas a "contactless" card sends encrypted information via radio waves to the PC.

The following are some of the attributes of a smart card:

1. A smart card is typically a credit card sized device that has a micro-computer and memory built in. It is highly tamper proof, and provides high degree of security while transacting on-line.

2. On the client-side, the smart card software essentially consists of two parts:

- Card reader software (also known as host software) that runs on a computer connected to a smart card.
- Card software that runs on the smart card itself. As a counterpart of reader-side software, card software is also referred to as card-side software.

3. The smart card usually requires two-factor authentication. In addition to presenting the card to the system, you need to enter authentication password or code when prompted. Double authentication (One is physical possession of the card and the second authentication code) ensures better security.

Fingerprint and retina scan, both belong to same: "what you are". Hence constitute single-factor authentication.

Small device storage may be used to store valuable documents and devices under lock and key. Fingerprint scanner may be used to provide entry only to the authorized personnel into the admin office. CCTV system may be used to monitor the activity within the admin office. All these measures improves the security of the admin office.

Single sign on

Shibboleth: This identity solution is an open-sourced, federated single sign-on (SSO) system that runs on SAML. Most users of Shibboleth are research and educational institutions. Whereas most federated systems are designed to work only with identity and service providers in the same organization, Shibboleth works on an inter-organizational basis.

OpenID Connect: OpenID Connect is an authentication service that can be used to sign into any website or web app that accepts it. This authentication service is often provided by a third party.

OAUTH: Open Standard for Authorization is an authorization service that can be used to gain access to information. The main use for OAUTH is to share information with third party applications.

Operationally speaking, OAUTH works with HTTP to allow access tokens to be allotted to third-party clients under the approval of the owner of the information resources.

Secure Token: Secure tokens are protected data sets, sometimes encrypted, that serve as verification for users and systems. Benefits of using secure tokens include the fact that secure tokens do not leak information about credentials and that impersonation of secure tokens is not easy.

NTLM: New Technology LAN Manager, or NTLM, is a proprietary Microsoft Windows password hash storage system. NTLM is a challenge-response protocol system that has enhanced security because it is non-reversible. NTLM is often used in active directory environments that do not provide for user logon authentication via TACACS or Radius.

Previous Contents Next

CompTIA® Security+ Exam Notes : Differentiate Common Account Management Practices

examguides.com/security+/security+24.htm

4. Identity and Access Management

4.4 Given a scenario, differentiate common account management practices

Audits: Three important types of audits are:

a. Privilege audit

b. Usage audit

c. Escalation audit

d. Administrative audit

Privilege audits: Privilege audits verify that accounts, groups, and roles are correctly assigned and that policies are being followed. A privilege audit may include complete review of all accounts and groups to ensure that they're correctly implemented. Privilege auditing is used to verify that users are granted proper privileges. It can be applied for large corporations. Of course, it cannot determine the intentions of people using the privileges.

Usage auditing: Usage auditing verifies that systems and software are used appropriately and consistently with organizational policies. A usage audit may include physically inspecting systems and software, and conducting other verification tests as per the polic

Escalation audits: Escalation audits is primarily focused around the issue of gaining access to higher-ups through the hierarchy in a time of crisis. These types of audits ensure that the management is ready for intervention in case of any disaster.

Administrative audits: It is important to document the procedures undertaken during the information processing and who is involved in this process. The individuals involved in the policy implementations and their responsibilities are documented.

Password Complexity: Ideally, a password should have uppercase, lowercase letters combined with numbers and symbols.

Ex: Us%25enL is a recommended password, ensuring highest safety.

Onboading/offboarding: The terms onboading/offboarding are also extensively used with new employee hiring and employee exit procedures. The addition of a employee to an organization's Identity and Access Management (IAM) system in a new role is known as onboarding. Conversely, offboarding refers to the IAM processes surrounding the removal of an identity for an employee who has left the network. In identity management, onboarding policy is the procedure that an employee has to follow when he connects his laptop or mobile device to a network Offboarding is the policy that an employee has to follow when he disconnect his mobile device to the Company's network.

Time-of-day restrictions: Limitations imposed as to when a user can log on to a system. If these are broken, it may require further investigation. It is an access control concept that limits a user account to be able to log into a system or network only during specific hours and days of the week. Note that off boarding deals with procedures after resignation and not before.

Permission auditing and review: An audit that analyzes user privileges. It identifies the privileges (rights and permissions) granted to users, and compares them against what the users need.

Group policy: Group policy is the mechanism by which Windows systems can be managed in a Windows network domain environment. A Group Policy Object (GPO) is a collection of registry settings that can be applied to a system at the time of boot-up or at the moment of user login. Group policy enables windows administrator to maintain consistent configurations and security settings across all members of a large network.

Previous Contents Next

CompTIA® Security+ Exam Notes : Importance Of Policies, Plans And Procedures Related To Organizational Security

examguides.com/security+/security+25.htm

5. Risk Management

5.1 Explain the importance of policies, plans and procedures related to organizational security

The following are true in terms of security policy

- The security policy should clearly state that no one is ever allowed to share his/her password with anyone else.
- Secondly, the security policy should state that the help desk can only change or assign a new password after positive identification of the individual requesting the information.
- According to the principle of least privilege, a user should be given only the minimum privileges that are required to do his/her works accurately and completely.

The following policies is best suited to reduce the risk of employees within an organization colluding to embezzle company funds

- Mandatory vacations help to reduce the possibility of fraud and embezzlement as a person is enforced to take leave.
- Time of Day (TOD) ensures that a person may sign in only during a selected times.
- Training helps employees to be aware of policies, and how to use them.

Acceptable use policy: Acceptable use policy specifies what employees can do with their systems, and network access. The policy may put limits on personal use of resources, and resource access time. AUP defines the intended uses of the resources in an organization and the consequences for non-compliance. AUP ensures that the resources are utilized in a proper way. For example, you may restrict that no social websites be visited by the employees during working hours.

Some issues that need to be taken care of, while planning security policies are:

1. Due Care

2. Privacy

3. Separation of Duties

4. Need to Know

5. Password Management

6. Disposal Management

7. Human Resource Policies, and

8. Incident Management

Personnel management

Separation of duties: Separation of duties prevents any single person from performing multiple job functions that might allow the person to commit fraud. Separation of duties happens when the responsibilities have been split between two or more people, thus reducing the incidence of fraud. Separation of duties ensures that the vital activities are bifurcated among several individuals. This ensures that one or two individuals can not perform a fraud.

Clean desk: Clean desk policy ensures that the personnel keeps the desks clean during and after the work. It ensures that login/password information is not inadvertently left on the desk which may lead to hacking or even loss of data or sensitive information.

Job rotation: Job rotation helps in managing the work with different people, thus reducing any down time when one of the employees has quit or on leave. Further, job rotation gives the employee the opportunity to develop skills in a variety of changing jobs.

NDA: It is important to review the NDA (Short for Non-Disclosure Agreement) that Company B has entered into with Company A. It can only enter into NDA with a third party (Company C) only if the NDA between the first and second party permit it. For example, if

the NDA rules out sharing data with a third party, then B can not enter into NDA with C. It is important to verify whether the third party provider has relevant experience. However, it is not the first thing to be considered. An NDA with the third party is subject to NDA entered already between the first two parties. Similarly, having security policies in place for C is not relevant at this point.

Example1: A newly hired employee is asked to review security of the computers within the company premises. What he needs to do first?

Solution: *He needs to go through the security policy first. A company's security policy outlines the security measures to be taken. Implementing the security policy is the first thing that needs to be done.*

Example 2: A security manager observed that the incoming inspection of material as well as payment is done by the same person. He implemented a policy such that one employee does incoming inspection of material and another employee does the payment processing. This is an example of security enhancement by separation of duties.

Agreement Types:

SLA (Service Level Agreement): Service Level Agreement is the formal negotiated document between two parties. It is a legal document that binds both the parties during the tenure of the agreement. SLA usually pertains to performance expectations such as up-time, and mean-time-between-failures.

BPA (Business Partners Agreement): It defines the relationship between business partners, including their roles and responsibilities toward the partnership.

MOU (Memorandum of Understanding): A memorandum of understanding (MoU) describes a bilateral or multilateral agreement between two or more parties.

ISA (Interconnection Security Agreement): It specifies requirements for establishing, maintaining, and disconnecting a secure connection between two parties.

In the context of risk management, three types of control classes are defined. These are Management (or Administrative), Technical, Operational (or Physical). For each of these classes, there are four types of controls, namely, Preventive, Detective, Corrective, and Compensating.

Account recertification: Account re-certification refers to several account management principles. First, recertification refers to performing a periodic assessment of a user's responsibilities against their account permissions and rights, confirming the principle of least privilege. Recertification can also verify if a user has the proper level of skill or

knowledge to have access to a certain account type. Finally, recertification of an IT system's account management controls can also occur, validating if a system can adhere to proper levels of account security.

Federated identity: A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.

Account maintenance: Account maintenance is the regular or periodic activity of reviewing and assessing the user accounts of an IT environment. Any accounts that no longer required should be disabled, such as those used by previous employees or related to services that have been uninstalled.

Offboarding: Offboarding refers to the IAM(Identity and Access Management) processes surrounding the removal of an identity for an employee who has left the network.

Roles and responsibilities

Multiple personnel in an organization are associated with the control and administration of data. These data roles include data owners, data controllers, data processors, data custodian/stewards, and users

Data owners: All data elements in an organization should have defined requirements for security, privacy, retention, and other business functions. It is the responsibility of the designated data owner to define these requirements.

Data Controllers: The data controller is the person responsible for managing how and why data is going to be used by the organization.

Data Processors: The data processor is the entity that processes data given to it by the data controller. Data processors do not own the data, nor do they control it. Their role is the manipulation of the data as part of business processes.

Data custodian/steward: A data custodian or data steward is the role responsible for the day-to-day caretaking of data. The data owner sets the relevant policies, and the steward or custodian ensures they are followed.

Data Protection Officer(DPO): A data protection officer is a role within a company or organization whose responsibility is to ensure that the company or organization is correctly protecting individuals' personal data according to current legislation.

International Organization for Standardization (ISO) 27001/27002/27701/31000:

ISO 27001 is the international standard defining an information security management system (ISMS).
ISO 27001 is one of many related standards in the 27000 family. ISO 27002 is a document that defines security techniques and a code of practice for information security controls.
ISO 27701 is a privacy extension to the 27000 series and adds the requirements to establish and maintain a privacy information management system.

The ISO 31000 series is a set of guidelines, principles, framework, and process for managing risk. ISO 31000 addresses all forms of risk and management, not just cybersecurity risk

Payment Card Industry Data Security Standard (PCI-DSS) control objectives include:

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- mplement strong access control measures
- Regularly monitor and test networks
- Maintain an Information Security Polity

G**eneral Data Protection Regulation(GDPR):** GDPR is a regulation that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. And non-compliance could cost companies dearly.

Cyber Security Framework(CSF): The CSF is designed to assist organizations in the early stages of planning their cybersecurity posture.

Center of Internet Security (CIS): CIS is a not-for-profit NGO that develops its own Configuration Policy Benchmarks (CPB).

Previous Contents Next

CompTIA® Security+ Exam Notes : Summarize Business Impact Analysis Concepts

examguides.com/security+/security+26.htm

5. Risk Management

5.2 Summarize business impact analysis concepts

Business Impact Assessment or Business Impact Analysis is a management-level analysis aimed at identifying a firm's exposure to sudden loss of critical business functions and supporting resources due to an accident, disaster, emergency, and/or threat. BIA involves assessing both financial and non-financial (customer service, market confidence, creditor or supplier confidence) costs during business disruption and business restoration periods. BIA is used in the development of business Disaster Recovery Plan (DRP).

Any business continuity planning preferably include the following:

- Redundant network connectivity
- Clustering
- Fault tolerance using Raid or similar technique
- Facilities management

Security policy planning should include the following:

- Due care, acting responsibly and doing right thing.
- Privacy, letting the employees and administrator know of the privacy issues
- Separation of duties

- Need to know, providing employees only the information required to perform their role or duties.
- Password management, auditing the passwords
- Disposal and destruction
- Human rights policies, and
- Incident response, should take care of response to an act.

Mean Time to Repair(MTTR): MTTR (mean time to repair) is the average time required to fix a failed component or device and return it to production status.

Mean time to repair includes the time it takes to find out about the failure, diagnose the problem and repair it. MTTR is a basic measure of how maintainable an organization's equipment is and, ultimately, is a reflection of how efficiently an organization can fix a problem.

Mean Time Between Failures (MTBF): The most common failure related metric is also mostly used incorrectly. "Mean time between failures" or "MTBF" refers to the amount of time that elapses between one failure and the next. Mathematically, this is the sum of MTTF and MTTR, the total time required for a device to fail and that failure to be repaired.

RTO/RPO: The recovery point objective (RPO) and the recovery time objective (RTO) are two very specific parameters that are closely associated with recovery. The RTO is how long you can basically go without a specific application. This is often associated with your maximum allowable or maximum tolerable outage.

RPO limits how far to roll back in time, and defines the maximum allowable amount of lost data measured in time from a failure occurrence to the last valid backup.

RTO is related to downtime and represents how long it takes to restore from the incident until normal operations are available to users

Single point of failure (SPOF): A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. SPOFs are undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial system.

Privacy Impact assessment: A privacy impact assessment (PIA) is a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system.

Privacy threshold assessment: It is OPM policy to ensure that all information technology (IT) systems that collect, maintain, or disseminate information in an identifiable form have a privacy impact assessment (PIA) or privacy threshold analysis (PTA).

Previous Contents Next

CompTIA® Security+ Exam Notes : Explain Risk Management Processes And Concepts

examguides.com/security+/security+27.htm

5. Risk Management

5.3 Explain risk management processes and concepts

Risk Response Features:

Risk mitigation: is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on

Risk avoidance: Elimination of the vulnerability that gives rise to a particular risk so that it is avoided altogether. This is the most effective solution, but often not possible due to organizational requirements. Eliminating email to avoid the risk of email-borne viruses is an effective solution but not likely to be a realistic approach in the modern enterprise.

Risk assessment: Should include planning against both external and internal threats. During a risk assessment, it is important to identify potential threats and document standard responses.

Risk Transference: A risk or the effect of its exposure may be transferred by moving to hosted providers who assume the responsibility for recovery and restoration or by acquiring insurance to cover the costs emerging from equipment theft or data exposure.

While performing risk assessment for an organization. Following should be done during impact assessment and quantification

- Asset identification - Identify organizational assets
- Threat assessment - Identify the threats to the assets or resources
- Impact definition and quantification - Study the likely loss to the assets or resources due to a given threat. The loss may be the brand image, and not necessarily a physical resource
- Control design and evaluation - Put controls in place to mitigate the threat. The controls may be device based, software based, or personnel training.

Assets need to be identified first as part of risk assessment.

Vulnerability assessment is part of an organization's security architecture.

ALE: The Annualized Loss Expectancy (ALE) is the expected monetary loss that can be expected for an asset due to a risk over a one year period. It is defined as: ALE = SLE * ARO

where SLE is the Single Loss Expectancy and ARO is the Annualized Rate of Occurrence.

An important feature of the Annualized Loss Expectancy is that it can be used directly in a cost-benefit analysis. If a threat or risk has an ALE of $5,000, then it may not be worth spending $10,000 per year on a security measure which will eliminate it.

The risk-assessment component, in conjunction with the business impact analysis (BIA), provides an organization with an accurate picture of the situation it faces.

The following four strategies comprise the strategies that are normally used for risk:

1. Acceptance: Acceptance of a risk means that the severity of the risk is low enough that we will do nothing about the risk unless it occurs. Using the acceptance strategy means that the severity of the risk is lower than our risk tolerance level.

2. Transfer: The transfer strategy in managing risk is to give responsibility for the risk to someone outside the project. The risk does not go away; the responsibility of the risk is simply given to someone else.

3. Risk Avoidance: This strategy is used to make the risk cease to be a possibility. In risk avoidance, we completely eliminate the possibility of the risk. If the sponsor of the project agrees to allow a risk-filled deliverable to be removed from the project, the risk is removed along with the deliverable.

4. Mitigation: Risks that are above the risk tolerance maximum value are not acceptable risks and that something had to be done about them. Mitigation is a strategy where some work is done on unacceptable risks to reduce either their probability or their impact to a point where their severity falls below the maximum risk tolerance level.

Vulnerability testing:

Vulnerability testing is part of testing corporate assets for any particular vulnerability. These may include:

1. Blind testing: Here the hacker doesn't have a prior knowledge of the network. It is performed from outside of a network.

2. Knowledgeable testing: Here the hacker has a prior knowledge of the network.

3. Internet service testing: It is a test for vulnerability of Internet services such as web service.

4. Dial-up service testing: Here the hacker tries to gain access through an organization's remote access servers.

5. Infrastructure testing: Here the infrastructure, including protocols and services are tested for any vulnerabilities.

6. Application testing: The applications that are running on an organization's servers are tested here.

Any software is inherently prone to vulnerabilities. Therefore, software manufacturers provide updates or patches to the software from time to time. These updates usually take care of any known vulnerabilities. Therefore, it is important to apply these updates.

Additional functionality is also one of the reasons for applying software updates. However, many times, it is not the compelling reason to apply the updates.

Scenario: You are assessing the risk factor of an organization. You find that only one employee in your organization has been trained and solely responsible for the complete product life cycle. What is a possible risk resulting from this?

Solution: *While assessing the risk of an organization, avoiding single point failures is one of the most important issues. A single point failure may be avoided by separation of duties, and training more than one employee in any given area of expertise.*

Risk assessment types

Qualitative risk assessment is the process of subjectively determining the impact of an event that affects a project, program, or business. The likelihood of occurrence is the chance that a particular risk will occur. Functional recovery plans represent the transition from operations under business continuity back to normal operations.

Quantitative risk assessment is the process of objectively determining the impact of an event that affects a project, program, or business. A single point of failure is any aspect of a system that, if triggered,could result in the failure of the entire system.

Previous Contents Next

CompTIA® Security+ Exam Notes : Disaster Recovery And Continuity Of Operations Concepts

examguides.com/security+/security+28.htm

5. Risk Management

5.4 Explain disaster recovery and continuity of operations concepts

Disaster Recovery plan: Disaster recovery plan is also called as business continuity plan or business process continuity plan.

DRP: DRP stands for Disaster Recovery Planning should include information security, asset security, and financial security plans.

As part of disaster recovery, it is important to have a location from which the recovery of a failed site can take place. This location is known as a backup site. In the event of a disaster, your site is recreated at the specified backup site and made available. Once the failed site is recovered, the backup site will be reverted to its previous status.

There are three different types of backup sites:

1. Cold backup sites

2. Warm backup sites

3. Hot backup sites

1. Cold site: Here the bare minimums, such as space and furniture are available. Everything else need to be procured. The delay going to a fully operational site could be very large in this case

2. Warm site: Here, most of the hardware is in place, and probably you need to recover the site from off-site backup, and configure. The site could be restored in a reasonable amount of time.

3. Hot site: A facility designed to provide immediate availability in the event of a system or network failure. All the systems are appropriately configured and working. Only thing that is required is the restoration of latest backup.

Note that onsite backup is not a back up site.

Backup concepts: It is recommended to store the backup tapes in a secure, physically distant location. This would take care of unforeseen disasters like natural disasters, fire, or theft. It is also important that the backup tapes are regularly verified for proper recovery in a test server, even though recovery is not really required at that time. Otherwise, it may so happen that you find a backup tape corrupt when it is really required. The backup policy identifies the methods used to archive electronic and paper file systems. This policy works in conjunction with the information retention and storage policies.

A properly managed tape backups should include the following:

- Regular backups according to a pre-determined plan
- Verifying the backup tapes for integrity
- Labeling tapes properly for easy and unique identification
- Storing tapes securely at off-site location
- Destroying data on old tapes before disposing off the same

There are primarily three types of backups:

1. Full backup: Here all the data gets backed up. It usually involves huge amounts of data for large systems, and may take hours to complete. A full backup is preferred instead of incremental or differential backups where it is feasible. However, when there is large amount of data, full backup is done once in a while and incremental or differential backups are done in between. A backup plan is usually put in place prior to taking backup of data.

2. Differential backup: A differential backup includes all the data that has changed since last full backup. The "differential backup" that was taken earlier (after the "full backup" but before the current "differential backup") becomes redundant. This is because all changed data since last "full backup" gets backed up again.

3. Incremental backup: It includes all the data changed since last incremental backup. Note that for data restoration the full backup and all incremental backup tapes since last full backup are required. The archive bit is set after each incremental backup. Incremental backup is useful for backing up large amounts of data, as it backs up only the changes files since previous incremental backup.

Previous Contents Next

CompTIA® Security+ Exam Notes : Compare And Contrast Various Types Of Controls

examguides.com/security+/security+29.htm

5. Risk Management

5.5 Compare and contrast various types of controls

Various Types of controls:

1. Preventive control: It prevents any security breach from occurring. Aimed at preventing an incident from occurring.

Example

- Security guards at door,
- Proximity cards or bio-metrics at the entrance to the building,
- Change management policy, etc.

2. Detective controls: Detective controls attempt to detect any break-in that has already happened. Aimed at detecting incidents after they have occurred.

Example

- Log monitoring,
- Trend analysis,
- Security audit
- video surveillance systems

- motion detection systems.

3. Corrective controls: Corrective controls attempt to reverse the impact of an incident or problem after it has occurred. Aimed at reversing the impact of an incident.

Example:

- Active IDS. Active intrusion detection systems (IDSs) - IDS detects an intruder and engage systems that block the progression of intrusion.
- Backups and system recovery.

4. Deterrent controls attempt to prevent incidents by discouraging threats. Aimed at discouraging individuals from causing an incident.

Example:

- Cable locks
- Hardware locks

5. Compensating controls: These are alternative controls used when a primary control is not feasible. are when it isn't possible to use the primary control or to enhance a primary control.

Example:

- TOTP (Time-based One Time Password).
- Using Proximity card or a PIN number are examples of Preventive control.

Managerial: Managerial controls are those that are based on overall risk management. These security controls focus on the management of risk or the management of the cybersecurity system. The use of cybersecurity audits is an example of a managerial control

Physical: A physical control is one that prevents specific physical actions from occurring, such as a mantrap prevents tailgating. Physical controls prevent specific human interaction with a system and are primarily designed to prevent accidental operation of something

Compensating: A compensating control is one that is used to meet a requirement when there is no control available to directly address the threat. Fire suppression systems do not prevent fire damage, but if properly employed, they can mitigate or limit the level of damage from fire.

Operational: An operational control is a policy or steps used to limit security risk. These security controls are done by people, as opposed to systems. Instructions to guards are an example of an operational control.

Technical: These security controls are primarily built into the information system through mechanisms contained in its hardware, software, or firmware components. Biometrics is an example of a technical control.

Previous Contents Next

CompTIA® Security+ Exam Notes : Compare and contrast basic concepts of cryptography

examguides.com/security+/security+30.htm

6. Cryptography and PKI

6.1 Compare and contrast basic concepts of cryptography

A cryptographic hash function is a "one-way" operation. It is practically not possible to deduce the input data that had produced the output hash.

You can decrypt an encoded message using matching secret key. Similarly, Digital certificate is issued by a CA, and can be decrypted to find the contents of the certificate.

Quantum cryptography offers secure communication by providing security based on the fundamental laws of physics, instead of the mathematical algorithms or computing technology. Quantum cryptography is most suitable for secure key distribution. Other options are distractions only.

The important terms of information security are confidentiality, integrity, availability, and non-repudiation.

Confidentiality is the term used to prevent disclure of information to unauthorized persons. Integrity is the term used ensure that the data cannot be modified undetectably. Confidentiality ensures that a message is not disclosed to any unintended parties. Note that

integrity is to do with the correctness of information, and authorization refers to privileges to access a given resource. Authentication is used in conjunction with validation of a user or a process to login.

Availability ensures that the data (or information) is available when needed. Authenticity ensures that the transaction is genuine and accepted by both the parties concerned.

Non-repudiation means that both the parties cannot refuse having performed the transaction. Non-repudiation ensures that the sender, as well as the receiver cannot refute having sent or received a message. For example, you receive an email from your perspective employer. By using an unsigned email, it might so happen that your employer later denies having sent any such email. Non-repudiation ensures that neither the sender nor the receiver can deny the transmission or the reception of a message respectively. Non-repudiation is used to ensure that a sender cannot refuse later that he had not sent the message. A digital signature on the message ensures that the sender is the original sender of the electronic message. Non-repudiation prevents either the sender or the receiver of messages from denying having sent or received a message.

Secret-key encryption is also known as single-key or symmetric encryption. It involves the use of a single key that is shared by both the sender and the receiver of the message.

Typically, the sender encrypts the message with a key and transmits the message to the recipient. The recipient then decrypts it by using a copy of the same key used to encrypt it.

It is very important to know the distinction between Hashing, Digital signature, and Encryption.

Hashing produces a small footprint (basically, signature) of the original message. It is used to verify the integrity of a message. Hash is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. In other words, Hash used to ensure that transmitted messages have not been tampered with. Hashing ensures that the message is not tampered with, during transit or storage. Note that Hashing not necessarily encode or encrypt a message.

Typically, the sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message (by using the same formula that was used to produce the Hash by the sender), and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact.

Encryption is used to translate a message in to secret code. To read an encrypted file, you must have access to a secret key that enables you to decrypt it. Encrypted data is referred to as cipher text. Encryption ensures that the message cannot be read by any person who do not

have matching key to decode the coded message

Two main types of encryption are

1. Asymmetric encryption (also called public-key encryption) and

2. Symmetric encryption.

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message. A digital signature can be used with encrypted or even un-encrypted message. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real. Digital signature ensures that the sender cannot repudiate having sent the message at a future date.

Scenario: Some of the temporary employees get renewed every year in your company. Each time the renewal takes place, they will be given a new smart cards. The smart card is used for digitally signing the email sent by the employees. When they tried to copy the digital signature from the old card to the new smart card, it was not successful. What should be done so that the digital signature works with the new smart card?

Solution: *You should advice the employees to publish the PIV certificate (a part of PKI, or Public Key Infrastructure) on the new smart card using global address list (GAL).*

It is not possible for users to copy a certificate, a public key, or a private key to a smart card.

Hashing a message ensures that the message is delivered without any distortion.

The disadvantages of using symmetric encryption over asymmetric encryption are given below:

1. Inability to support non-repudiation: Since both the sender and receiver use the same key, it is difficult to determine who is the sender, should a dispute arise.

2. Impractical for web commerce: Imagine thousands of customers buying goods and services over the Internet. If symmetric encryption standard is used, one unique private key-pair needs to be used for each user. It is therefore, impractical.

3. Another major difficult is with the transmission of private key. With symmetric encryption, the private key needs to be transmitted to the other party for decryption, which may pose security risk.

There are two primary types of keys.

Static keys usually remain the same over the period of validity of a certificate. The disadvantage of static keys (for example, RSA uses static private-public key pair) is that it is predictable and relatively more prone to hacking.

Ephemeral keys are temporary in nature. The key is valid only for one session, and it is discarded soon after the session ended. Some versions of Diffie-Hellman algos use ephemeral keys.

Eliptic Curve: The primary benefit of Elliptic Curve Cryptography is that it uses smaller key size, reducing storage and transmission requirements, i.e., that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key.

For example, a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key.

U.S. National Security Agency (NSA) approved ECC for digital signatures and Diffie-Hellman key agreements

1. Diffie-Hellman is used to securely share symmetric encryption keys over a public network.

2. Elliptic curve cryptography (ECC) is commonly used with small wireless devices.

3. ECDHE is a version of Diffie-Hellman that uses elliptic curve cryptography to generate encryption keys.

4. Diffie-Hellman methods support both static keys and ephemeral keys.

5. RSA is based on the Diffie-Hellman key exchange mechanism using static keys

The following are true about wildcard domains in the context of a PKI infrastructure:

1. It can be used for the domain and all of its first level sub-domains.

2. It reduces administrative work in maintaining the certificates.

Steganography: Steganography is the process of hiding information within information. For example, an attacker may use the least significant bits in an image to transfer a harmful virus. The picture looks harmless. Steganography is also used to embed watermark within an image by authors.

Previous Contents Next

CompTIA® Security+ Exam Notes : Explain cryptography algorithms and their basic characteristics

examguides.com/security+/security+31.htm

6. Cryptography and PKI

6.2 Explain cryptography algorithms and their basic characteristics

Symmetric Algorithms:

Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. The standard is slowly replacing its predecessor DES and 3DES.

1. AES (Advanced Encryption Standard) is more secure than DES or 3DES.

2. AES is a symmetric block cipher that can encrypt (encipher) or decrypt (decipher) information

3. AES is based on Rijndael algorithm

BitLocker Drive Encryption is a full disk encryption feature included with some versions of Microsoft's Windows Vista, By default it uses the AES encryption algorithm.WEP uses RC4 encryption scheme.

Hashing Algorithms: Hash algorithms produce a hash of a message and encrypt it. They use a mathematical formula for hashing, and it is extremely difficult to tamper with the message and still produce the same hash. Basically, Hashing enable a recipient to check whether a message is received intact without being tampered by a third party.

1. SHA (Secure Hashing Algorithms): There are several Secure Hashing Algorithms and they primarily differ in the hash length. They are SHA-1, SHA-256, SHA-384 and SHA-512. In SHA-1 the bit length is 160 bits, in SHA-256 it is 256 bits, for SHA-384, 384 bits and in SHA-512 it is 512 bits.

2. MD2, MD4, MD5 (Message Digest Series Algorithms): These are another type of hash algorithms. These algorithms were developed by Rivest. All three algorithms take a message of arbitrary length and produce a 128-bit message digest. MD2 is meant for 8 bit machines and MD4, MD5 are suitable for 32 bit machines. These algorithms are primarily used for digital signature applications.

MD5 hash is 128 bits long and displayed as 32 hexadecimal characters. That is MD5 length in bits : 32*4 or 128 bits.

MD5("The quick brown fox jumps over the lazy dog.")

gives hexadecimal: e4d909c290d0fb1ca068ffaddf22cbd0

As can be seen above, it is 32 hex characters long.

SHA (Secure Hash Algorithm) comes in different flavors.

SHA-1 length in hex is 40 i.e. it's length in bits : 40*4 or 160 bits.

Example of SHA-1 Hash:

SHA1("The quick brown fox jumps over the lazy cog")

gives hexadecimal: de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3

As ca be seen above, it is 40 hex characters long in the above example.

SHA-2 includes four versions: SHA-224, SHA-256, SHA-384, and SHA-512. The numbers represent the number of bits in the hash. For example, SHA-256 creates 256-bit hashes.

SHA-3 includes multiple versions with hashes of 224 bits, 256 bits, 384 bits, and 512 bits.

Block cipher: Block cipher derives its name from the fact that a block of data is taken at a time to cipher.

Asymmetric Algorithms:

PGP (Pretty Good Privacy): PGP can use Diffie-Hellman or RSA algorithms, but not AES or DES. PGP is used primarily for securing email communications. PGP uses public-key encryption for sending and receiving email messages. Diffie-Hellman and RSA algorithms are used for encryption/ decryption of PGP messages.

PGP certificates differ from X.509 certificates in two ways:

1. PGP certificates are issued (signed) by normal people while the X.509 certificates must be issued by a professional CA, and

2. PGP implements a security fault tolerance mechanism, called the Web of Trust. Here an individual is allowed to sign and issue certificates to people they know.

Diffie-Hellman:

ECDHE: Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) allows entities to negotiate encryption keys securely over a public network.

Key Stretching Algorithms:

Bcrypt and Password-Based Key Derivation Function 2 (PBKDF2) are key stretching algorithms. It is used to make a short key, typically a password or passphrase, more secure against a brute force attack by increasing the time it takes to test each possible key. Usually, passwords are short and we don't remember long passwords. Short passwords are easy to crack by brute force method.

PKI Trust Models:

Hierarchical: A root CA at the top controls all the subordinate CAs. The subordinate CAs are next in the hierarchy, and they only trust information provided by the root CA. In a strict hierarchy, however, a root CA normally issues or revokes certificates only on an occasional basis. Therefore, the root CA usually works offline to protect its key infrastructure.

Bridge: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. The root CAs can communicate with each other, allowing cross certification.

Mesh: The mesh trust model expands the concepts of the bridge model by cross connecting multiple root CAs. Each of the root CAs can also communicate with the intermediate CAs in their respective hierarchies. This structure may be useful in a situation where several organizations must cross-certify certificates. The major disadvantage of a mesh is that each root CA must be trustworthy in order to maintain security. Further, the complexity grows exponentially with each node, and becomes difficult to use and maintain when the numbers become large.

Hybrid: When independent enterprises establish separate subordinated hierarchies, and then develop a need to communicate, some form of cross-certification must be applied to link the hierarchies. The hybrid trust model has the following properties:

1. Multiple root CAs exist

2. All non-root CAs are certified within a root CA's hierarchy, with paths certified both "downward" from the root and "upward" towards it

3. Root CAs establish a cross-certified mesh among themselves, so each hierarchy can reach every other hierarchy via a single cross-certificate at the root level

4. Selective cross-certification between non-root CAs is permitted

Note that wildcard certificate supports only one private/public key pair.

Previous Contents Next

CompTIA® Security+ Exam Notes : Given a scenario, install and configure wireless security settings

6. Cryptography and PKI

6.3 Given a scenario, install and configure wireless security settings

The standard 802.1x corresponds to wireless network access protocols. Various wireless LAN protocols are given below:

1. IEEE 802.11 - supports data rate up to 2 Mbps in the 2.4 GHz frequency band.

2. IEEE 802.11a - supports data rates up to 54 Mbps in the 5 GHz frequency band.

3. IEEE 802.11b - supports data rates up to 11 Mbps in the 2.4 GHz frequency band.

4. IEEE802.11n - supports data rates 2.4 to 5 GHz

5. IEEE802.11ac - bandwidth rated up to 6.9 Gbps at 5 GHz band

6. IEEE 802.3 - describes CSMA/CD Ethernet standard.

7. IEEE 802.5 - describes Token Ring networks.

8. IEEE 802.4 - is a standard for Token bus networks.

Note that IEEE 802.11x, 802.11xx standards pertain to wireless LANs.

Cryptographic Protocols:

CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (Also known as CCM Protocol) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology. The CCMP algorithm is based on the U.S. federal government's Advanced Encryption Standard (AES).

TKIP (Temporal Key Integrity Protocol): TKIP is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). It was designed to provide more secure encryption than the notoriously weak Wired Equivalent Privacy (WEP), the original WLAN security protocol.

WEP (Wired Equivalent Protection): is a security standard for 802.11 WAP networks. WEP key length should be at least 40 bits long. Wireless networks broadcast messages using radio, and therefore more susceptible to eavesdropping than wired networks. WEP was intended to provide confidentiality comparable to that of a traditional wired network. WEP is 802.11's optional encryption standard implemented in the MAC Layer that most radio network interface card (NIC) and access point vendors support. If a user activates WEP, the NIC encrypts the payload (frame body and CRC) of each 802.11 frame before transmission using an RC4 stream cipher provided by RSA Security. The receiving station, such as an access point or another radio NIC, performs decryption upon arrival of the frame. Note that, 802.11 WEP only encrypts data between 802.11 stations. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies.

WPA and WPA2: Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i . WPA is forward compatible with the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared.802.11i includes dynamic key exchange, stronger encryption, and user authentication. It is not backward compatible with WPA. The 802.11i standard is widely known as WPA2

The key features of the WPA protocol are given below:

1. It supports both static and dynamic key distribution

2. It provides Device Authentication, as well as User Authentication.

3. It uses TKIP (Temporal Key Integrity Protocol) encryption for dynamic key exchange. Note that WPA2 uses AES encryption where as WPA uses TKIP. AES encryption is a stronger encryption protocol.

4. WPA is forward compatible with WPA2.

Authentication Protocols:

EAP: The Extensible Authentication Protocol (EAP) is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

PEAP: PEAP (Protected Extensible Authentication Protocol) is a version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections. PEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area

networks) that support 802.1X port access control.

LEAP: LEAP (Lightweight Extensible Authentication Protocol) is a Cisco-proprietary version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections. LEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control.

EAP-Fast: EAP-FAST, also known as Flexible Authentication via Secure Tunneling, is an Extensible Authentication Protocol (EAP) developed by Cisco. It is used in wireless networks and point-to-point connections to perform session authentication. Its purpose is to replace the Lightweight Extensible Authentication Protocol (LEAP).

EAP-TLS: EAP-TLS uses the TLS public key certificate authentication mechanism within EAP to provide mutual authentication of client to server and server to client. With EAP-TLS, both the client and the server must be assigned a digital certificate signed by a Certificate Authority (CA) that they both trust.

EAP-TTLS: EAP-TTLS (Tunneled Transport Layer Security) developed as an extension of EAP-TLS. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel (or tunnel), as well as a means to derive dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

EAP-MD-5 (Message Digest): EAP-MD-5 is an EAP authentication type that provides base-level EAP support. EAP-MD-5 is typically not recommended for Wi-Fi LAN implementations because it may allow the user's password to be derived. It provides for only one-way authentication - there's no mutual authentication of Wi-Fi client and the network. And very importantly it doesn't provide a means to derive dynamic, per session wired equivalent privacy (WEP) keys.

IEEE 802.1x: 802.11x is generic term to refer to the IEEE 802.11 standard for defining communication over a wireless LAN (WLAN). 802.11, commonly known as Wi-Fi, specifies an interface between two wireless clients. These standards are used to implement WLAN communication in 2.4, 3.6 and 5 GHz frequency bands. This is the standard that pertains to wireless LANs.

Methods:

Captive portal: A captive portal is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources. The captive portal is presented to the client and is stored either at the gateway or on a web server hosting the web page. Captive portals are mostly used for wireless hotspot and to manage the internet access on campus grounds, hospital wireless networks, school wireless networks, or even for larger organizations.

RADIUS federation: RADIUS Federation is a federation service where access to the network is gained by using WAPs. RADIUS federation allows users to use their normal credentials across trusted networks. It uses IEEE 802.1x as the authentication method with a RADIUS database at the back-end.

EAP-TLS: EAP-TLS is an IETF open standard. It also uses TLS to secure the authentication process. It is one the most secure methods because it typically employs client-side certificates. This means that the attacker must also possess that client-side certificate key to break the TLS channel.

WPA2-PSK: WPA stands for "Wi-Fi Protected Access", and PSK is short for "Pre-Shared Key."

WPA2-PSK [AES] is the recommended secure method of making sure no one can actually listen to your wireless data while it's being transmitted back and forth between your router and other devices on your network.

EAP-PEAP: EAP-Protected Extensible Authentication Protocol (EAP-PEAP) is a protocol that creates an encrypted (and more secure) channel before the password-based authentication occurs. PEAP is an 802.1X authentication method that uses server-side public key certificate to establish a secure tunnel in which the client authenticates with server.

Configuration of wireless security settings:

Example 1:Configure security encryption to WPA 2 with pass phrase "SECPLUS"

You need to know how to configure basic security setting such as WPA (Short for Wi-Fi Protected Access) or WPA2. You can typically select the appropriate setting from a drop down box and then enter the appropriate pass phrase. The security settings entered on the access point must be used on all the devices that connect to the access point.

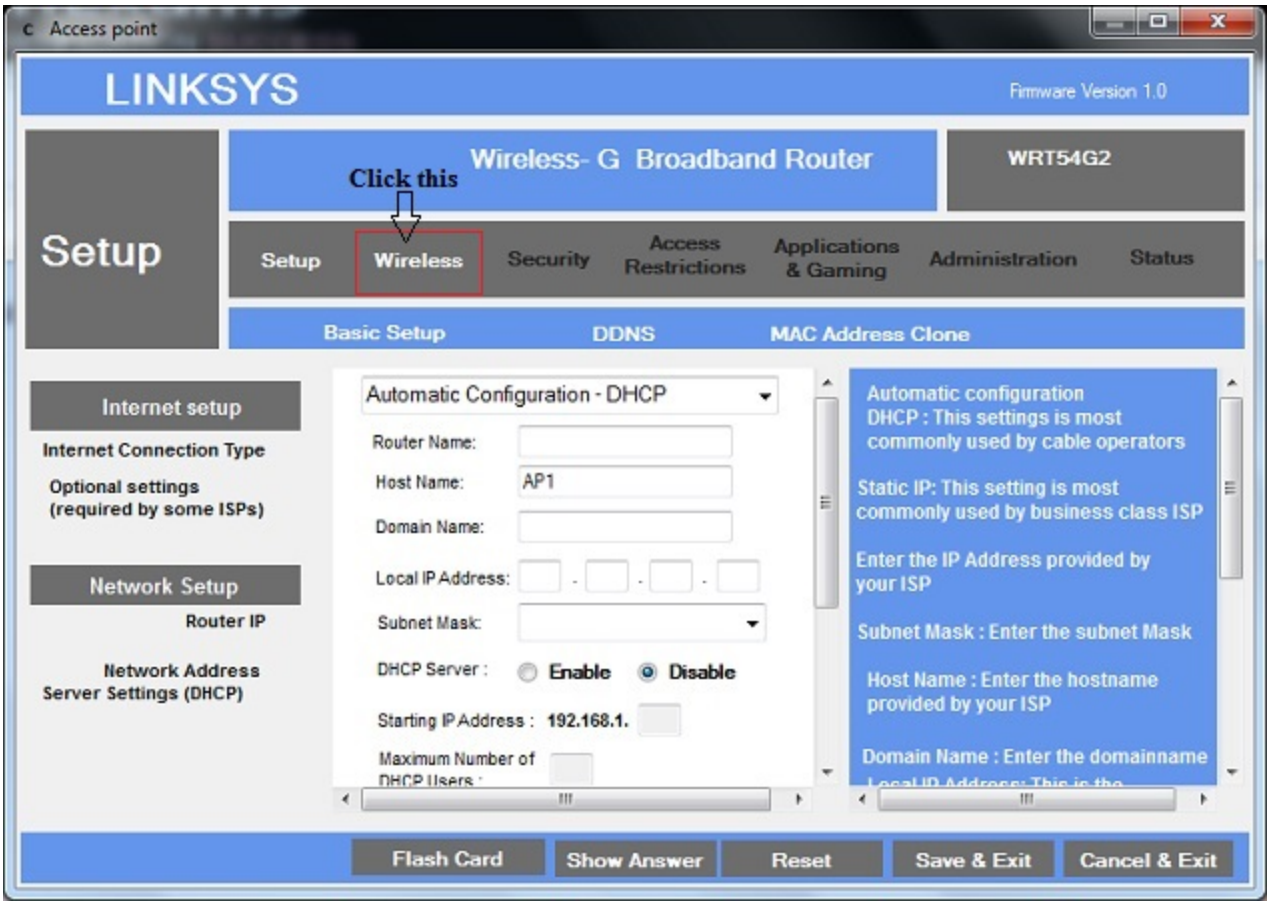
Both WPA and WPA2 operate in either Personal or Enterprise modes. Most home and small business networks use Personal mode using a passphrase or password.

Big enterprises add additional security to WAPs with WPA Enterprise or WPA2 Enterprise. Enterprise mode provides additional security by adding an authentication server such as RADIUS, and requiring each user to authenticate with a username and password.

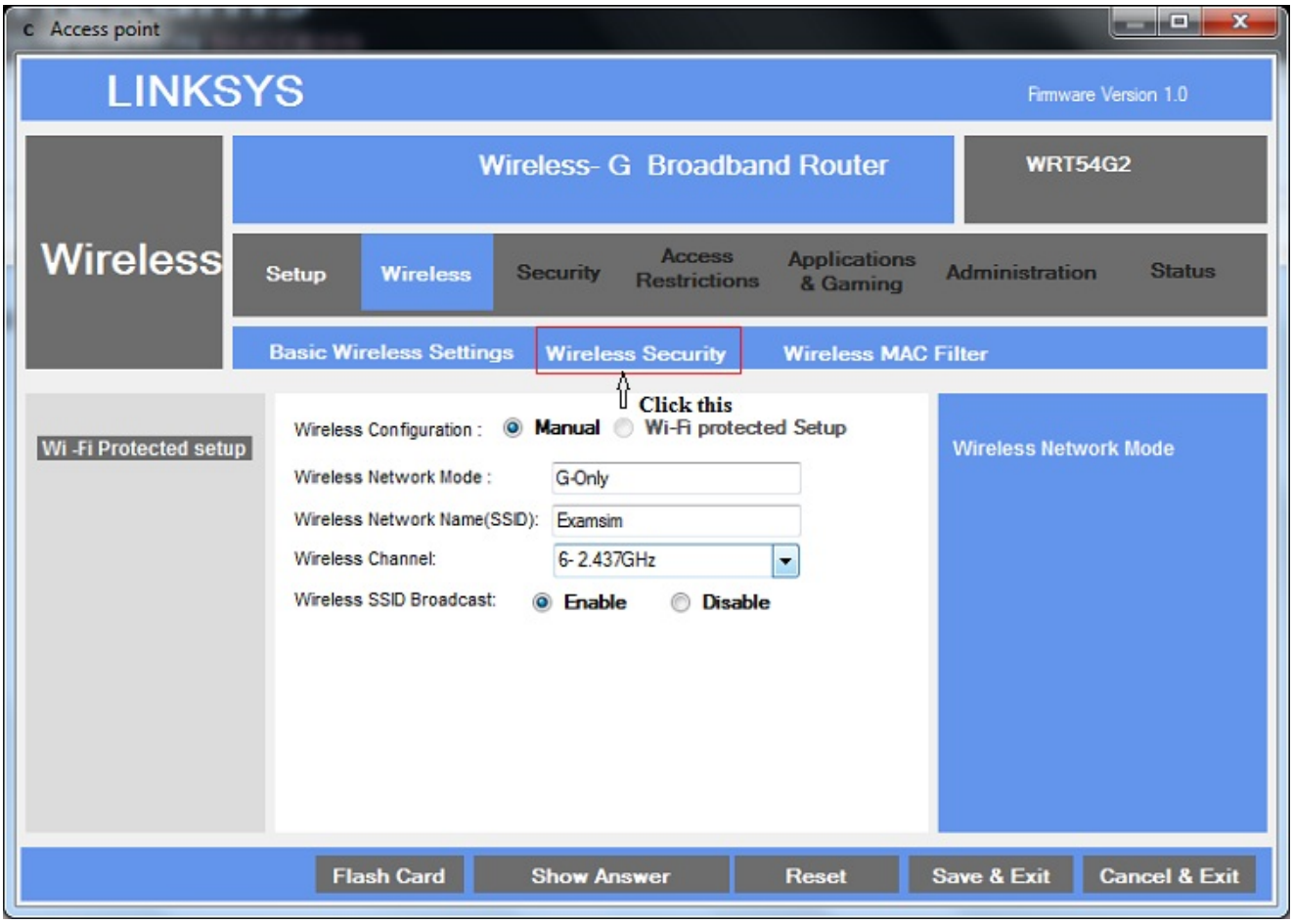
Enterprise mode requires a server typically configured as a Remote Authentication Dial-In User Service (RADIUS) server, which is configured separately from the access point. The RADIUS server has access to the user's authentication credentials and can verify when a user has entered authentication information correctly

Steps involved in configuring encryption level to WPA2:

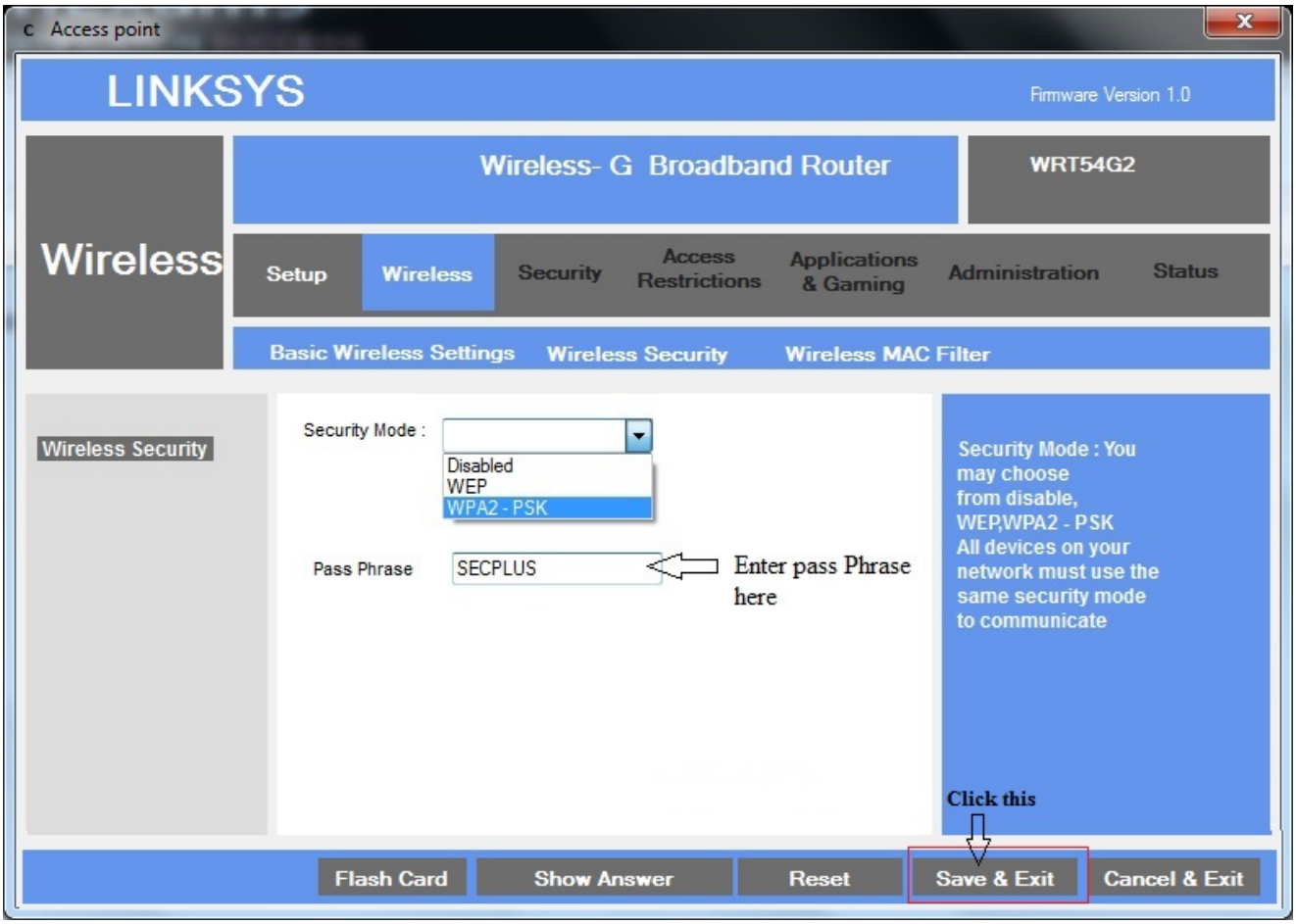
1. In Wireless Access point window click "Wireless" tab



2. In "Wireless" window click "Wireless Security" tab.



3. In "Wireless Security" window select WPA2 - PSK as encryption mode from "Security Mode" drop down and enter "SECPLUS" as Pass Phrase and click "Save & Exit" button.



Note: The exercise uses "Linksys" Access point for demonstration purpose only. The settings are similar in any other home wireless access points or Wi-Fi routers. Knowing the functionality of the wireless access point is important.

Example 2: Enable MAC Address Filtering in the WAP device, so that the machines matching the MAC addresses are permitted to communicate using the wireless network.

The following MAC addresses need to be allowed:

a. 18:F4:6A:1A:A2:12

b. 1E:F4:6A:1A:A2:12

c. 1F:F4:6A:1A:A2:12

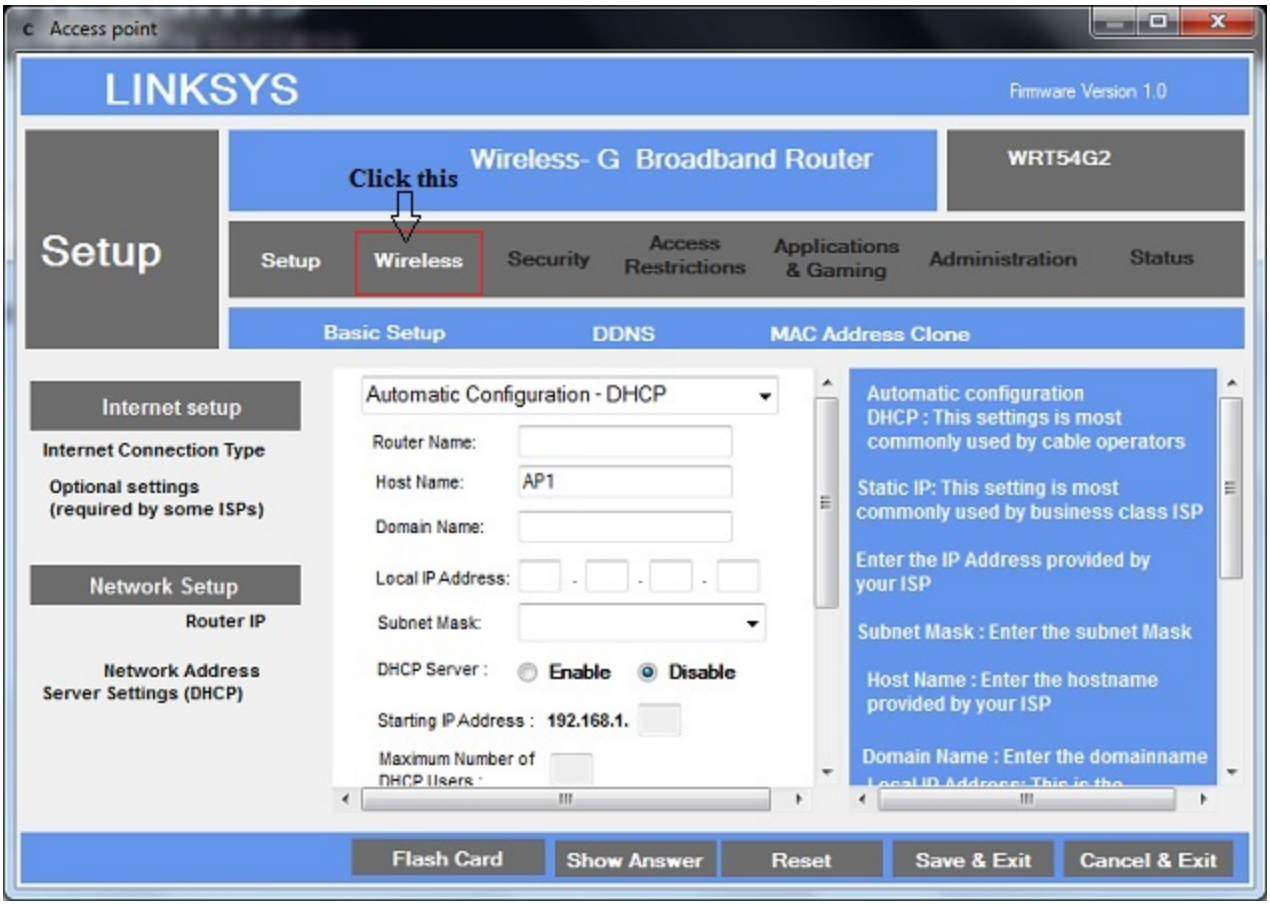
d. 1D:F4:6A:1A:A2:12

Every Wi-Fi device is assigned a MAC (Media Access Control) address, a unique 12-digit hexadecimal identifier issued by the IEEE, the standards body that developed the Wi-Fi protocol. The MAC address is "hard-coded" into the device and sent automatically to a Wi-Fi access point when the device tries to connect to the network.

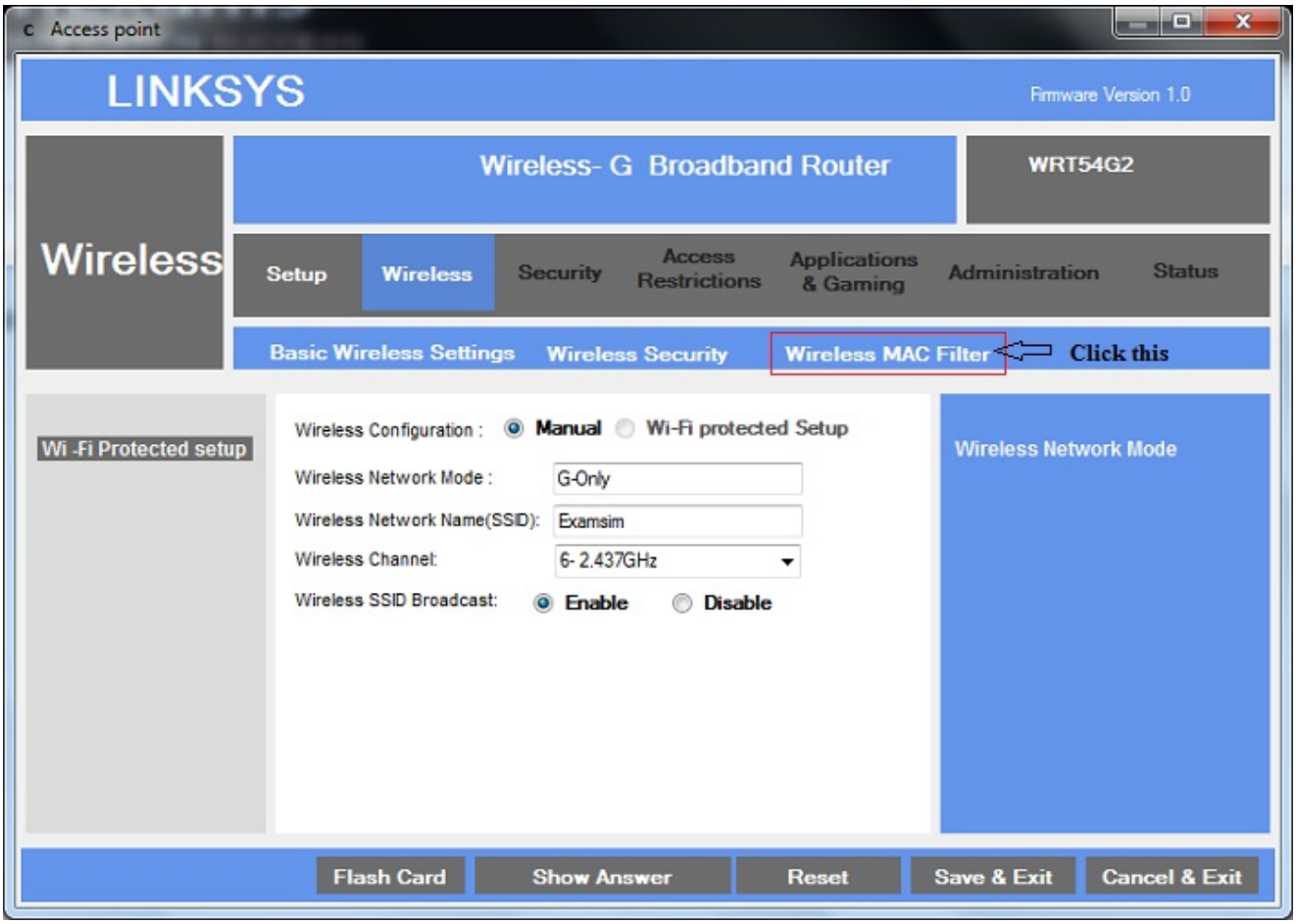
Using the access point configuration software, you can create a safe list of allowed client devices or a black list of banned devices. If MAC filtering is activated, regardless of what encryption security is inplace, the AP only allows devices on the safe list to connect, or blocks all devices on the black list.

To enable MAC address filtering and to allow the devices with matching MAC addresses, perform these steps (these steps are generic in nature, and likely to change from one device type to another):

1. In wireless Access point window click "Wireless" tab.



2. Click "Wireless MAC Filter" tab in wireless window.

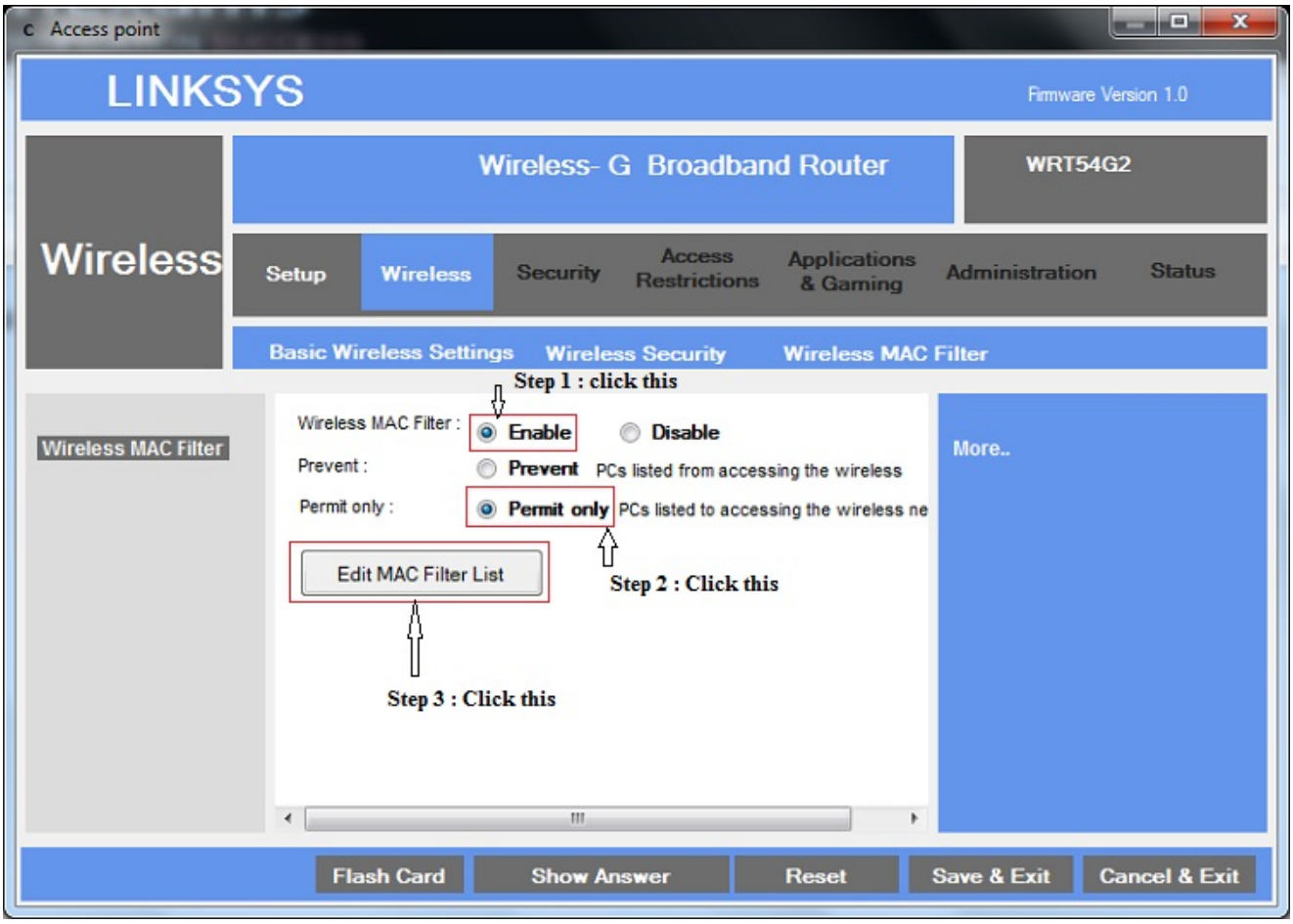


3. In MAC Filter window

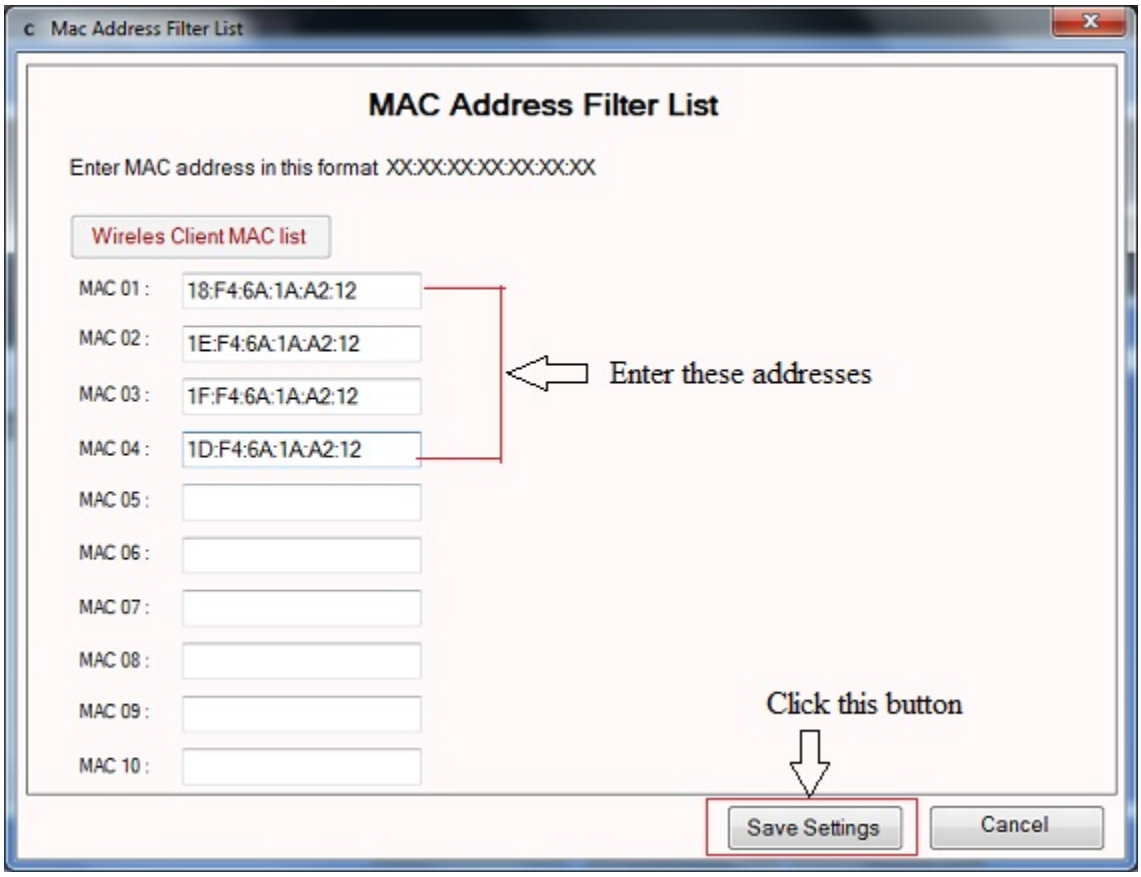
step 1: Click Enable radio button

step 2 : Click Permit only radio button

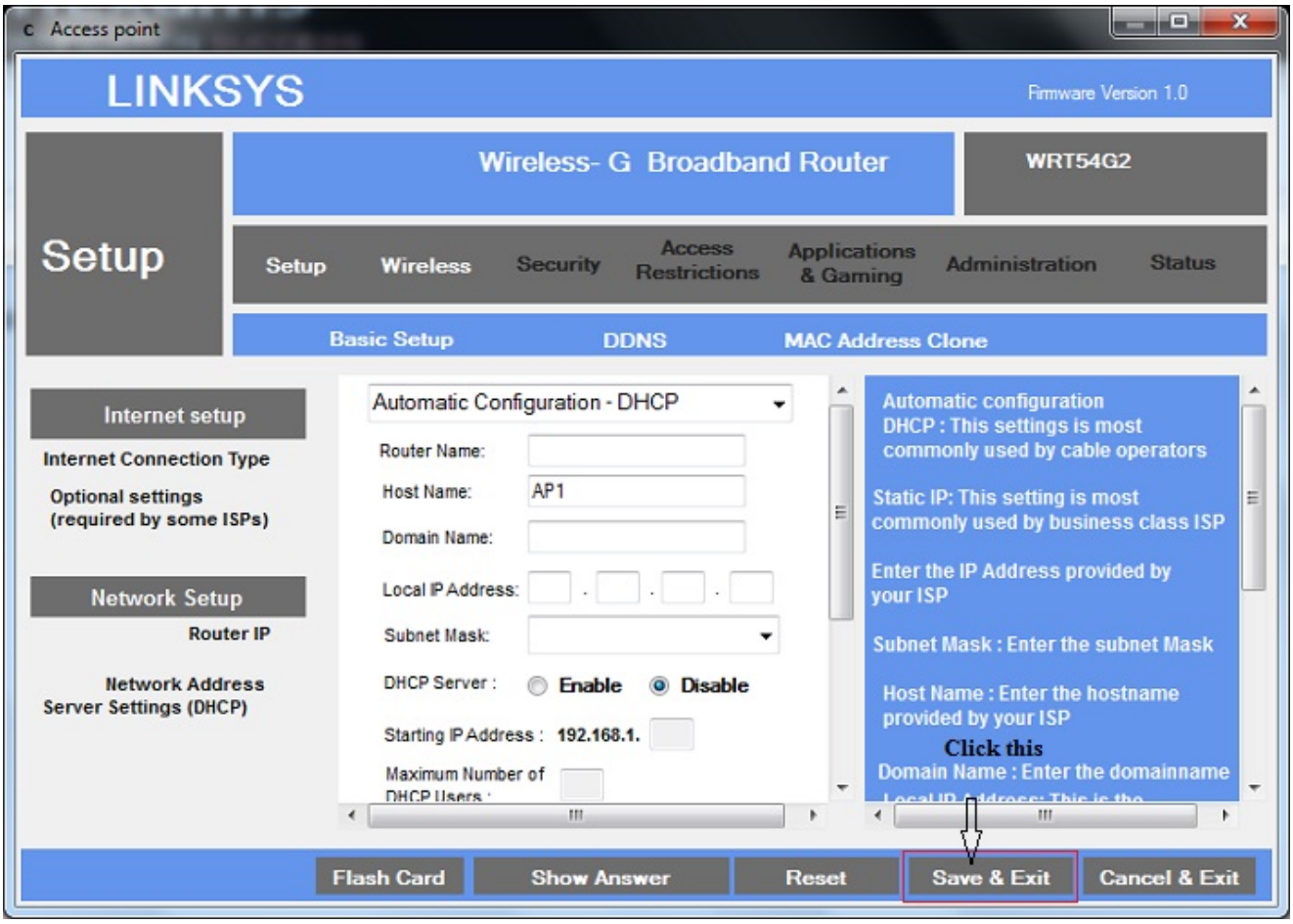
step 3 : Click Edit MAC Filter List button



4. MAC Address List window appears , enter the address of the device as mentioned in the question and click on Save settings button.



5. Click again "Save & Exit" button in wireless Access point window.



Note: Encryption protocols like WPA2 (Short for Wi-Fi Protected Access 2), reduced the necessity for using MAC filtering. Hackers may break into MAC filtering device by sniffing addresses of connected devices and then spoofing or masquerading as one of them.

Previous Contents Next

CompTIA® Security+ Exam Notes : Given a scenario, implement public key infrastructure

examguides.com/security+/security+33.htm

6. Cryptography and PKI

6.4 Given a scenario, implement public key infrastructure

In Public Key Infrastructure parlance, the term Principal means an entity whose identity can be verified.

Trust Model:

Three basic types of distributed trust models are:

1. Hierarchical trust model: Here one root CA and one or more subordinate CAs will be present. The subordinate CAs provide redundancy and load balancing. The root CA is usually off-line. Here even if a subordinate CA is compromised, the root CA can revoke the subordinate CA, thus providing redundancy.

2. Web of Trust: This is also called cross-certification model. Here CAs form peer-to-peer relationship. This model is difficult to manage as the number of CAs grow larger. This kind of trust relationship may happen when different divisions of a company has different CAs, and need to work together. Here CAs must trust one another.

3. Bridge CA architecture: Bridge CA overcomes the complexity involved with Web of Trust model. Here Bridge CA act as the central co-ordinate point. All other CAs (known as principals) must trust only the Bridge CA.

If the CA's private key is compromised, certificates' private key is compromised, certificates issued by that CA issued by that CA are affected. This will lead to issuance of new certificates to all users, and registration. These problems can be overcome by use of a distributed trust model, in which multiple CAs are involved.

In public key infrastructure:

- A key is required to encode/decode a message, and the security of a message depends on the security of key.
- A cipher text is the encoded message, and
- A certificate is a digitally signed document by a trusted authority.

CRL: A certificate revocation list (CRL) is a list of certificates, which have been revoked, and are no longer valid. The client requests a copy of the CRL from the CA and then checks the CRL to see if the certificate is on the list. If it's on the list, it's considered invalid and wouldn't be used.

Online Certificate Status Protocol (OCSP): Here, instead of the client requesting a copy of the CRL, the client queries the CA about the certificate, identified uniquely by a serial number. The CA then replies indicating the certificate is healthy (not revoked), not healthy (revoked), or unknown (the serial number is not known by the CA. A certificate authority uses a CSR to create your SSL certificate.

Key escrow: Key escrow (also known as a fair cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, an authorized third party may gain access to those keys. These third parties may include the government or an employer wanting to see the communication of an employee.

A digital certificate is a credential issued by a trusted authority that binds you (and individual or an organization) to an identity that can be recognized and verified electronically by other agencies. Locally issued digital certificates are valid only within an organizations network (like intranet). Therefore, any secure pages or digital signatures containing local registration will not work on the Internet.

SAN: A Storage Area Network (SAN) provides a pool of storage resources that can be centrally managed and allocated as needed. Instead of having isolated storage capacities across different servers, you can share a pool of capacity across a bunch of different workloads and carve it up as you need. It's easier to protect, it's easier to manage.

A SAN consists of interconnected hosts, switches and storage devices. The devices are typically connected using Fibre Channel, though other protocols are possible. SAN and NAS (short for network-attached storage) are both network-based storage solutions. A SAN typically uses Fibre Channel connectivity, while NAS typically ties into to the network through a standard Ethernet connection. A SAN stores data at the block level, while NAS accesses data as files. To a client OS, a SAN typically appears as a disk and exists as its own separate network of storage devices, while NAS appears as a file server.

Online vs. offline Certification Authority

Stapling: Stapling is the process of combining related items to reduce communication steps. An example is when someone requests a certificate, stapling sends both the certificate and OCSP responder information in the same request to avoid the additional fetches the client would have to perform during path validations.

Pinning: When a certificate is presented for a host, either identifying the host or providing a public key, this information can be saved in an act called pinning, which is the process of associating a host with a previously provided X.509 certificate or public key. This can be important for mobile applications that move between networks frequently and are much more likely to be associated with hostile networks where levels of trust are low and risks of malicious data are high. Pinning assists in security through the avoidance of the use of DNS and its inherent risks when on less-than-secure networks.

Certificate chaining: Certificate chain, a chain of trust from one certificate to another, based on signing by an issuer, until the chain ends with a certificate that the user trusts.

Code signing: Code signing, which involves applying a digital signature to code, providing a mechanism where the end user can verify the code integrity.

Secure Cookies: Cookies are text files sent with every request to a website. They have been used for a variety of functions, including maintaining state, preferences,usage parameters, and so on

Public key Infrastructure:

One of the protocols used for online revocation services is the Online Certificate Status Protocol (OCSP), a request and response protocol that obtains the serial number of the certificate that is being validated and reviews CRLs for the client.

Certificate Signing Request (CSR): A certificate signing request (CSR) is the actual request to a CA containing a public key and the requisite information needed to generate a certificate. The CSR contains all the identifying information that is to be bound to the key by the certificate-generation process. A message sent from an applicant to a certificate authority in order to apply for a digital identity certificate

.pfx file: Digital certificates are defined in RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. This RFC describes the X.509 v3 digital certificate format in detail. There are numerous ways to encode the information in a certificate before instantiation as a file, and the different methods result in different file extensions. Common extensions include .der, .pem, .crt, .cer, .pfx, .p12, and .p7b.

Certificate Revocation List (CRL): A digitally signed object that lists all of the current but revoked certificates issued by a given certification authority. This allows users to verify whether a certificate is currently valid even if it has not expired. A CRL is analogous to a list of stolen charge card numbers that allows stores to reject bad credit cards.

Certificate formats:Certificates can have various file extension types, some extension types are interchangeable, but not all are. Below table provides a brief comparison of common certificate formats.

Certificate Format	Encoding	Systems	Extensions
DER	Binary	Java	.der,.cer,.crt
PEM	Base64 ASCII	Apache HTTP	.pem,.cer,.crt. .key
PFX(PKCS#12)	Binary	Windows	pfx, .p12
P7B (PKCS#7)	Base64 ASCII	Windows and Java Tomcat	p7b,.p7c

The most common format and extension for certificates is PEM, which is mostly associated with Apache web servers. Another Base64-encoded certificate format is P7B, also known as PKCS#7. It uses .p7b and .p7c extensions. Most servers (Ex: Apache) expect the certificates and private key to be in a separate files.

A P7B file only contains certificates and chain certificates (Intermediate CAs), not the private key.

Another binary certificate format is PFX, also known as PKCS#12. Extensions for PFX encoded certificates include .pfx or .p12. This type of certificate is common to the windows operating system for importing and exporting private keys. PFX supports a private key and can store one or more certificates within a single binary file.

Previous Contents