**Network Security**

**Chapter 1: Introduction to Information Security**

Explain the relationships among the component parts of information security, especially network security:

Network Security is a critical part of any IT infrastructure structure of any organization in our current time and life. Even with the broad view that the information security has reached in the past 20 years, network security managed and still was able to convince the top management executive about the role that it uphold to the point that it had become a topic that separate best business than the worse once. Network security is a component part and layer of the information security layers: Network security is the protection of networking components, connections, and contents.

Define the key terms and critical concepts of information and network security:

Critical understanding of information security and network terms. To have the ability to understand the core we must first see what sort of characteristics each possesses and with that we have: Availability, Accuracy, Authenticity, Confidentiality, Data owners, Data custodians, Data users, Utility, Possession and Privacy. Each one of these mentioned respectively lead to the next one in it side, creating the critical bound and ending with the requirement that up hold security and information which is privacy. With that being said each of them have the same weight in understanding security and reflecting back on information and network security.

Explain the business need for information and network security:

Information security programs reflect the business needs in: protection functions, safety of operation, data usage and collection and safe guards of hardware assets on the organization level. All of that help the IT infrastructure to work without worries and have an effective operational business that meet the needs for Info Sec and Net Sec.

Identify the threats posed to information and network security, as well as the common attacks associated with those threats:

Information security threats and attacks:

Normal threats: Unauthorized Access, Data Theft and Hacking

Social Engineering: a hacking technique that exploits user’s trust and uses physical method and psychological tricks, to gather information. this is famous through the use of Telephone, Snail-mail, E-mail and the Internet.

Network Attacks: IP spoofing Attack, Denial of service DOS Attack, Man in the middle Attack, Software Attack, Malicious code Attack and Software exploitation Attack.

Distinguish between threats to information from within systems and attacks against information from within systems:

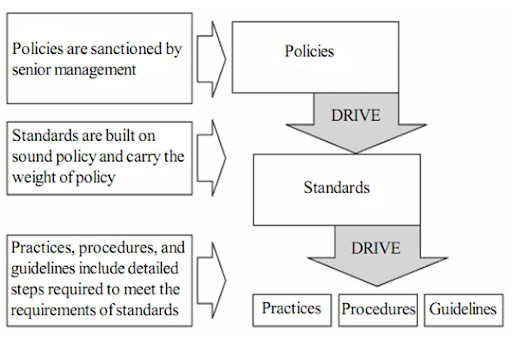
First we need to understand what is an attack and what is a threat: Attack - an act that can cause damage to or otherwise compromise the information. Attacks are different kind some can be active or passive, intentional or unintentional, and direct or indirect. Some attacks originate from what is called a threat. Threat is A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected. Usually an attack has the bigger domain when it comes to the harm. While threat can be an enabler for an attack it can never be an attack by itself or as a standalone.

Describe the organizational roles of information and network security professionals:

Typical Information security professionals titles with in any organization: Security Analyst, Security Engineer, Security Administrator, Security Architect, Security Specialist, and Security Consultant. These are some and does not reflect all of them. Typical network security professionals title with in any organization: Network Security Analyst, Network Engineer, Network Security Administrator, Network Architect, Network Specialist, and Network Consultant. These are some and does not reflect all of them.

Define management’s role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines

Management must consider the policies for all information security, planning, design and deployment. Policies show how issues are addressed and how technologies are used. Information security is a main problem of any management that is not a technical one, Security programs start and ends with a policy. Without policy, blueprints, and planning, organization are unable to meet information security needs of various communities of interest and business direction of quality.



Discuss how an organization institutionalizes policies, standards, and practices using education, training, and awareness programs:

Upon the make of a policy, a responsibility is made on the organization that each and every person which belongs to that organization must be well aware about their organizations rules, regulations and their consequences. So, organizations always start early training and awareness programs that encourage the spread of the knowledge of these policies and in-depth exercises orientation that reflect knowledge and consequences on violating the policy and what is the pros and cons that it up hold and why it came into effect. This is to make their employee focused on meeting the goal of the organization in bigger picture.

**Chapter 2:**

Describe the basic elements of computer-based data communication:

Computer communicates in a process that need the following:

Sending device that initiates an instruction to transmit data, instructions, and information.

Communications device that connects the sending device to a communications channel.

Communications channel (transmission media) on which the data, instructions and information travel.

Communications devices that connects the communications channel to receiving device.

Receiving device that accepts the transmission of data, instructions and information.

Discuss the key entities and organizations behind current networking standards, as well as the purpose of and intent behind the more widely used standards

The network standards serve specific purposes, but they differ in principle, there is more than one as defined by the standard itself. For example, there is a standard for how a network communicate across the internet and a different standard for you to talk across the telephone.

ITU (International Telecommunication Union): The International Telecommunication Union (ITU) is made up of telecommunication policy makers and regulators, network operators, equipment manufacturers, hardware and software developers, regional standards-making organizations, and financing institutions. The activities, policies, and strategic direction of the ITU are determined and shaped by the industry it serves.

The three sectors of the ITU are Radiocommunication (ITU-R), Telecommunication Standardization (ITU-T), and Telecommunication Development (ITU-D). ITU-R draws up the technical characteristics of terrestrial and space-based wireless services and systems, and develops operational procedures. ITU-T experts prepare the technical specifications for telecommunication systems, networks, and services, including their operation, performance, and maintenance. ITU-D experts focus their work on the preparation and development of recommendations, opinions, guidelines, handbooks, manuals and reports. These documents provide decision makers with "best business practices" relating to a host of issues ranging from development strategies and policies to network management.

IEEE 802 Group: The Institute of Electrical and Electronics Engineers (IEEE) is a nonprofit, technical professional association in 150 countries. The IEEE is a leading authority in technical areas ranging from computer engineering, biomedical technology, telecommunications and electric power. The IEEE produces 30 percent of the world's published literature in electrical engineering, computers, and control technology it also has nearly 900 active standards with 700 under development. Some of the best-known IEEE standards are as follows: IEEE 802.1 (LAN/MAN), IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring) and IEEE 802.11 (Wireless LAN)

Explain the nature and intent of the OSI reference model as well as list and describe each of the model’s seven layers

The OSI(Open Systems Interconnection) Model is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software.

Created at a time when network computing was in its infancy, the OSI was published in 1984 by the International Organization for Standardization (ISO).

The layers:

Physical Layer: At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

Data Link Layer: At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

Network Layer: The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol).

Transport Layer: The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

Session Layer: The session layer controls the conversations between different computers.

Presentation Layer: The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts.

Application Layer: This layer sees network services provided to end-user applications such as a web browser. The application layer identifies communication partners, resource availability, and synchronizes communication.

Describe the nature of the Internet and the relationship between the TCP/IP protocol and the Internet

TCP stands for Transmission control protocol, and IP stands for internet protocol. These are the set of protocol which allows two or more computers to communicate each other. Its design has some simple principles which we have to understand like "it selects the suitable device for a particular situation”, “it tells how to connect the devices”, and "it provides the address space for the computer which have to be connected in a network. The TCP/IP permits a computer or user to perform any task and set some instructions to control the things we do on internet which is the main reason for the Decentralized nature of internet. TCP/IP is the main reason that we can connect millions of network or system to another network or we can handle or control the using of internet but in a limit, now this limit is decentralization of internet where we can use internet but we cannot control the network of whole world or we cannot manipulate it, and this limit is provided by some set of rules provided by TCP/IP.

**Chapter 3: Cryptography**

1. Chronicle the most significant event and discoveries in the history of cryptology.

1900 BC - rare hieroglyphic symbols found in the hollow grave of Khnumhotep II in Egypt

100 BC - a form of encryption made by Julius Caesar where characters are shifted by 3 places

16th century - a cipher that first used an encryption key developed by Vigenere where the encryption key was repeated multiple times and the ciphertext is produced by adding the message character with the key character modulo 26.

19th century - Hebern rotor machine

November 1918 - Enigma machine with 3 or more rotors by German engineer Arthur Scherbius

1970 - Lucifer, also known as Data Encryption Standard (DES) formed by IBM and headed by Horst-Feistel

1973 - Request of proposals for a block cipher put out by the Nation Bureau of Standards in the US and Lucifer was an accepter

1997 - DES was broken by an exhaustive search attack

2000 - NIST accepted Rjindal (now Advanced Encryption Standard)

2. Explain the basic principles of cryptography.

**Kerckhoff’s principle**

This principle explains how to design a cryptographic system for it to become secure and all details must be publicly known, except for the keys. This means that the security is dependent on the keys and all of the algorithms are public.

**Symmetric cryptography**

A cryptographic system where only one, secret key is used to encrypt and decrypt electronic information.

**Asymmetric cryptography**

A cryptographic system, also known as public-key cryptography, where a pair of keys -- one public key and one private key -- are used to encrypt and decrypt electronic information to protect it from unauthorized use.

3. Describe the operating principles of the most popular cryptographic tools.

**Public-Key Infrastructure PKI**

A system designed for creating, distributing, and storing digital certificates used to verify a particular public key.

**Digital Signatures**

This is a process used to verify if the contents of a message have not been altered transferred using electronic systems.

**Digital Certificate**

A digital certificate is an electronic password that contains a key value and allows a user to exchange data securely.

**Hybrid Cryptography Systems**

Also known as a hybrid cryptosystem, it is a system that combines the convenience of a public key with the efficiency of symmetric cryptography.

**Steganography**

Steganography is a process where messages or information are concealed within other non-secret text or data.

4. List and explain the major protocols used for secure communications.

**S-HTTP**

S-HHTP, Secure Hypertext Transfer Protocol, is an extension to the Hypertext Transfer Protocol which enables a secure transfer of files on the World Wide Web and is either encrypted, contains a digital certificate, or both.

**SSL**

SSL, Secure Sockets Layer, is a standard security technology that uses public-key encryption to secure a channel.

**S/MIME**

S/MIME, Secure Multipurpose Internet Mail Extensions, is a standard for public-key encryption, based on asymmetric cryptography, and signing of MIME data, typically used in emails.

**PEM**

PEM, Privacy Enhanced Email, is a file format that is used in storing cryptographic keys, certificates, and other data and uses a 3DES symmetric key encryption.

**PGP**

PGP, Pretty Good Privacy, is an encryption program that provides cryptographic privacy and authentication for data communication. This program uses IDEA Cipher for message encoding.

**SET**

SET, Secure Electronic Transactions, is a communications protocol standard for securing credit cards over networks, especially the Internet. It is developed by MasterCard and VISA in 1997 to protect users who use electronic payment from fraud.

**WEP**

WEP, Wired Equivalent Privacy, is a security protocol specified in the IEEE Wi-Fi standard, 802.11b. It is designed to provide WLAN with security and privacy.

**WAP and WAP2**

Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access II (WPA2) is a security standard for users of electronic gadgets equipped with wireless internet connections. WPA2 is more secure than WPA.

5. Discuss the nature and execution of attacks used against cryptosystems.

**Man-in-the-Middle Attack**

A MITM is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.

**Correlation Attacks**

A correlation attack is a divide-and-conquer technique. Attackers attempt to deduce statistical relationships between the structure of unknown key and ciphertext.

**Dictionary Attacks**

This is an attempted illegal entry to a computer system which utilizes a dictionary-like list of words used to produce passwords.

**Timing Attacks**

In this type of attack, the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms.

**Chapter 4: Firewall Technologies and Administration**

1. Describe what a firewall does.

A firewall is used to protect an individual’s or company’s network by supplying the system two basic security functions: packet filtering and acting as an application proxy.

2. Explain how a firewall restricts access to a network.

The firewall in a network acts as a barrier when the firewall blocks the free passage of data to and from the network. It requires a user in the internal network to log in to the firewall system to access hosts on remote networks.

3. List the types of firewall protection as well as the types of firewall implementations and the ways they are used.

**Packet-filtering firewalls**

The most basic and oldest type of firewall is the packet-filtering firewall which creates a checkpoint at a traffic router or switches.

**Circuit-level gateways**

A simple firewall meant to immediately approve or deny traffic without noticeable calculating of resources through the verification of the transmission control protocol (TCP) handshake.

**Stateful inspection firewalls**

This type of firewall combined two pieces of technology into one type of firewall: the packet inspection and TCP handshake verification. Doing this creates a higher level of protection.

**Proxy firewalls**

This is a type of firewall where they are delivered through a cloud-based solution or another proxy device where instead of letting traffic connect directly, the proxy firewall establishes a connection first to inspect the incoming data packet.

**Next-generation firewalls**

Features of next-generation firewalls include deep-packet inspection, TCP handshake verifications, and surface-level packet inspection.

**Software firewalls**

Any type of firewall installed on a local device is a software firewall.

**Hardware firewalls**

This type of firewall utilizes a physical appliance that acts as a traffic router to inspect data packets and traffic requests before making a connection to the server.

**Cloud firewalls**

Delivering a firewall which includes the involvement of a cloud solution is called a cloud firewall. It can also be called FaaS (firewall-as-a-service).

4. Describe how firewall rules are created and how they are used to control the behavior of the firewall.

The creation of firewall rules differs in steps depending on what operating system is installed on a computer. Likewise, firewall behaviors are also varying because firewall vendors increase the diversity of the definition and functions of a firewall. Traditional firewalls may be focused on filtering traffic. Now, modern firewalls vary on combinations of different traditional firewall types.

5. Explain how intrusion detection and prevention systems are related and how they may be made to interact with one another.

An intrusion detection system (IDS) is used in the analysis and monitoring of network traffic to search for signs which might indicate attackers who are probably using cyberthreat. On the other hand, intrusion prevention system (IPS) is located in the same network area as a firewall, and proactively denies traffic based on a security profile. Although they are different, both of them read network packets and compare them to a database of known threats.

**Chapter 5: Network Authentication and Remote Access Using VPN**

1. Define access control and identify the various ways it can be implemented.

Access control is a security technique and the selective restriction of access which regulates which users will be allowed to view or access information or services in an environment. To implement access control, things to consider are the following: preventive measures against unauthorized use of a resource, information classification, and confidentiality is crucial, preventive measures against illegal use of a resource, and assignation of access rights to certain resources on the system.

2. Explain why authentication is a critical aspect of network access control.

In a network access control, authentication is the process of identifying and verifying a user who wants to access the network system. This is important because implementing authentication will guarantee effective security.

3. Identify the parts of virtual private networks (VPNs).

A VPN or virtual private network which extends a private network across a public network and combines device-level components with network-level components to create a secure system of communication. Parts of a VPN could be devices, zones, routers, authentication, users, and NAT.

4. List and define the essential activities that a VPN must be able to perform.

A well-designed VPN can perform activities such as improving security where data lines have not been ciphered, providing global network opportunities, providing telecommuter support, providing broadband network compatibility, simplifying network topology in certain scenarios, and reducing operational costs versus traditional WAN.

5. Explain the various VPN architectures in common use.

**Remote access VPN**

This permits a user to connect and access a private network, services, and resources remotely.

**Site to site VPN (router-to-router)**

Commonly used in large companies, these are used to connect the network of a certain location to the network of another specific location.

**Chapter 6: Network Monitoring and Intrusion Detection and Prevention Systems**

1. Define the basic concepts of network packet analysis.

Packet analysis can be used in logging traffic and traffic interception which goes over a network or part of a network. This process is called packet capture. This is used to analyze network problems, detect network intrusion attempts and misuse by users, document regulatory compliance, and many more.

2. Explain the various network packet formats and standards

Various network packet formats are:

**Header and Type (all packets)**

The data portion of each packet begins with a 4-byte header followed by a byte that identifies the packet type.

**Content-Length (most packets)**

All packets, except heartbeats, include a 2-byte short integer field which indicates the content length (number of bytes remaining).

**Identity String**

The first thing that the server sends to the client after a connection is initiated.

**Connection Request**

A TCP packet is sent from the client to the server.

**Connection Response**

A TCP packet is sent from the server to the client.

**Chat Message**

Sent in a packet from the client to the server.

**Heartbeat**

Allows the server to know which clients are still connected.

The older standard uses a 2-byte hexadecimal number to denote what network protocol type is captured by the packet. The 802.3 standards establish more powerful tools for describing the contents and function of packets.

3. Describe how packet analysis forms the basis of network intrusion detection

A packet analyzer analyzes the content of a packet and decodes them through the packet capture feature. This process can be the basis of network intrusion detection.

4. Discuss the various types of intrusion detection and prevention

Types of the intrusion detection system are NIDS and HIDS. Types of intrusion prevention are NIPS, WIPS, NBA, and HIPS.

NIDS (Network-based Intrusion Detection System) performs analysis on the traffic by looking for patterns and abnormal behaviors and can be undetectable by attackers and are mostly immune to direct attacks. HIDS (Host-based Intrusion Detection System) monitors system data, look for malicious activity on an individual host, and can access encrypted data packets and detect attacks with elusive capabilities.

NIPS (Network-based Intrusion Prevention System) monitors the entire network for suspicious traffic. WIPS (Wireless intrusion prevention system) monitors a wireless network for suspicious traffic. NBA (Network behavior analysis) examines network traffic to identify threats. HIPS (Host-based intrusion prevention system) operates a single host for suspicious activity.

5. Explain intrusion detection and prevention deployments and response strategies

A recommended intrusion detection and prevention deployment and response strategy are to, first, deploy the device in pure IDS mode without any traffic block, then after performance evaluation, slowly change the rules to produce the best results, from IDS rules that simply produce alerts to IPS rules that block the offending traffic.

6. Describe various honeypot technologies

**Pure honeypots**

A complete production system which monitors attacks through bug taps on the link

**Low-interaction honeypots**

Imitate services and systems that frequently attract criminal attention.

**High-interaction honeypots**

Complex setups that behave like real production infrastructure.

**Chapter 7: Wireless Network Security**

1. Identify various wireless technologies and standards

**Radio Frequency Transmission**

Typically used in wireless communication using RF signals that can penetrate through objects and travel long distances.

**Infrared Transmission**

Has longer wavelengths than visible light and typically used in short-range communications. Unlike RF signals, infrared signals do not penetrate through objects.

**Microwave Transmission**

Typically used in long-distance communications and is less expensive. However, these signals do not pass through buildings and bad weather can easily affect transmission.

**Lightwave Transmission**

These are unguided optical signals (laser) and are unidirectional. These signals cannot pass through rain and fog.

2. Recognize the topology and architecture of wireless networks

**WLAN**

Allows users in a local area to form a network to the Internet. It consists of two main components: an access point and wireless adapters.

**WPANS**

Infrared and Bluetooth are two current technologies of WPANS which allows connectivity of personal devices within an area of 30 feet.

**WMANS**

Allows a connection of multiple networks in a metropolitan area.

**WWANS**

Can be maintained in very large areas via multiple satellite systems or antenna sites managed by an ISP. Can also be called 2G systems.

3. Define popular wireless security protocols

**WEP**

The Wired Equivalent Privacy is a security protocol specified in the IEEE Wi-Fi standard, 802.11b. It is designed to provide WLAN with security and privacy. It is developed for wireless networks and approved as a Wi-Fi Security standard in 1999.

**WPA and WPA2**

The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are security standards for users of electronic gadgets equipped with wireless internet connections. One year before WEP was officially abandoned, WPA was formally implemented which has a significant enhancement compared to the other one. However, WPA2 is more secure than WPA. WPA2 uses AES or known as the Advanced Encryption Standard which outlives WPA.

4. Describe various WLAN security concerns

**Denial of service attacks**

The intruder floods the network with messages affecting the availability of the network resources

**Spoofing and session hijacking**

The attacker gains access to network data and resources by assuming the identity of a valid-user

**Eavesdropping**

Unauthorized third-parties intercept the data being transmitted over the secure network

5. Discuss the security issues regarding Bluetooth technology

Bluetooth has risks that may affect the security and privacy of users. Some are eavesdropping and denial of service. Bluetooth headsets can also be used to eavesdrop on user’s conversations with the people around them. Built-in hands-free car kits are also vulnerable. To solve these, use a higher version of Bluetooth and turn it off when not in use.

**Chapter 8: Security of Web Applications**

1. List the various Internet services in use

**Communications services**

Allows users to communicate with other users via the Internet

**Information retrieval services**

Allows users to retrieve information by using the Internet’s search engines

**Web services**

Allows users to exchange information between the applications on the Web

**World Wide Web**

Allows users to access documents over several servers of the Internet.

**Video Conferencing**

Allows users to communicate via a two-way video and audio transmission

2. Identify threats to Internet services and basic countermeasures

Common threats to Internet services are botnets, hacking, malware, pharming, phishing, ransomware, and spam. To counter these threats, the URL of the websites must be checked. HTTPS is more secure than HTTP. Users must also think before clicking. Most ads and illegal downloads are accompanied by these threats which will endanger the user’s privacy and security, not just accounts and information but also their personal computers.

3. Describe the basics of Web client-server communication

A client-server model is an application structure that divides tasks between the servers (providers of resource or service) and clients (service requesters). A web client-server communication contacts each other in this way through the use of Internet communication services.

4. Identify the various Web languages and describe their uses

Common web languages are HTML, CSS, Java, JavaScript, Python, SQL, and PHP. HTML is a dynamic language that can be used in the layout and structure of a website. CSS can be used with HTML to style a website and add visual aesthetics. Java can be used to develop websites, games, apps, and software. JavaScript is used to develop interactive environments for users. Python, used by Instagram and Pinterest, can be used to create a framework needed by any website. SQL is a database language that can be used to calculate large amounts of data on a website. PHP, used by Facebook and Wordpress, is often used on data-heavy websites or for app development.

5. Identify various Web threats and attacks

Malicious websites, malicious scripts, scripts and executable PE files, Trojan downloaders, exploit packs, and adware programs are some of the Web threats and attacks experienced by users and web developers. In 2012 alone, the number of browser-based attacks was 1,595,587,670.

6. Discuss the steps necessary to secure a Web server

* Use Public Key Authentication for SSH
* Strong passwords
* Install malware scanning software
* Keep software up-to-date
* Backup regularly
* Monitor logs
* Turn off unnecessary services

**Chapter 9: Network Vulnerability Assessment**

1. Name the common categories of vulnerabilities

The common categories of vulnerabilities are Network Vulnerabilities, Operating System Vulnerabilities, Human Vulnerabilities, and Process Vulnerabilities.

2. Discuss common system and network vulnerabilities

Common types of system and network vulnerabilities are malware, social engineering attacks, outdated or unpatched software, and firewall/operating system misconfigurations. These are dangerous because, it may not sound complicated, but potential damages of these vulnerabilities may cause a huge amount of money loss if the system is operated by a company.

3. Find network vulnerabilities using scanning tools and in-depth penetration testing

To diagnose a system accurately, the use of scanning tools and in-depth penetration testing must be used. A vulnerability scanner performs an automated process of proactively scanning the network, application, and security vulnerabilities. In-depth penetration testing is a simulated cyber attack against a system to check for exploitable vulnerabilities.

4. Access sources of information about vulnerabilities and determine how best to remediate those vulnerabilities

To remediate vulnerabilities, a proper diagnosis must be first performed. That is why scanning tools and in-depth penetration testing must be performed first so that the user is aware of what problems he or she might be facing. Different diagnoses may involve a different set of solutions.

**Chapter 10: Auditing, Monitoring, and Logging**

1. List the various events that should be monitored in network environments

* Availability of network devices
* Availability of critical services
* Amount of disk space in use
* Percentage of routers’ maximum throughput utilized on average
* Network firewall
* Update servers
* Traffic coming in and out of routers

2. Describe the various network logs available for monitoring

The following are log sources you must monitor infrastructure devices, security devices, server logs, web servers, authentication servers, hypervisors, containers, SAN infrastructure, applications, and client machines.

3. Discuss the various log management, SIEM, and monitoring technologies

Log management is an approach to deal with large quantities of computer-generated log messages. To do this, there are certain log management tools that can be used. SIEM or security information and event management is an approach to security management. It is a combination of the functions of SIM and SEM.

4. Explain the role that configuration and change management play in auditing the network environment

Network auditing tools are available and are ready to be downloaded from the internet. These tools involve configuration and change management which are essential in security assessment. Network auditing can be efficient if performed with network configuration and change management.

5. Discuss formal audit programs and how they relate to network environments

As businesses continue to expand and spread, they typically feel the need to scale up their IT networks to access a more extensive range of capabilities. To manage data, logs, and other information generated by systems, network audit programs make it easier to perform these tasks. Some examples of formal network audit programs include SolarWinds Network Configuration Manager (NCM), ManageEngine OpManager, ITarian Network Management, and Nmap.

6. Describe Certification and Accreditation (C&A) programs implemented by the U.S. federal government and other international agencies

Some C&A programs implemented in the US are ACEJMC Accreditation and PRSA Certification.

**Chapter 11: Contingency Planning and Networking Incident Response**

1. Explain the need for contingency planning

Having a contingency plan is essential, as threats can affect the implementation of existing projects, even when people least expect it. Having back-up plans that are ready to be implemented anytime that unprecedented occurrences take place is better than having nothing at all, and worse, stressing over what to do in the midst of the problem regarding the network security.

2. List the major components of contingency planning

The following are the major components of contingency planning:

* Business impact analysis (BIA)
* Incident response plan (IR plan)
* Disaster recovery plan (DR plan)
* Business continuity plan (BC plan)

3. Create a simple set of contingency plans, using business impact analysis

To successfully create a simple set of contingency plans using BIA, there are three major steps that should be considered according to the NIST Special Publication 800-34, Rev. 1. This includes the following:

* Determine mission/business processes and recovery criticality.
* Identify resource requirements
* Identify recovery priorities for system resources

4. Prepare and execute a test of contingency plans

Preparation and execution of test of contingency plans prior to its actual implementation will result in lesser mistakes and more control on the situation, especially when working on network security. There are five strategies that can be used to test contingency plans:

* Desk check
* Structured walk-through
* Simulation
* Parallel Testing
* Full interruption

5. Explain the network incident response process

The network incident response process pertains with how the management of the company responds to the unprecedented incidents that occur within the network. Five steps that include the process are preparation, detection and reporting, triage and analysis, containment and neutralization, and post-incident activity. The whole process is structured to effectively ensure the security of the network.

6. Explain the need for sound backup and recovery practices and what they consist of

Back-up and recovery practices are necessary to ensure that the needs of the network security are met. Developing accurate and efficient contingency plans as back-up and recovery practices is an intelligent choice for a company that would lead them on the right track as they go on working on the network security. Two varieties of back-up practices and disk backup and tape backup.

**Chapter 12: Digital Forensics**

1. Explain how U.S. law enforcement and the U.S. legal system affect digital forensics

The U.S. law enforcement and legal system affect the digital forensics in a way that there are laws and obligations that restrict the incorrect use of digital forensics. When a company working on digital forensics are accused of some wrongdoing, the law enforcers have the responsibility to perform a search and seizure. Once an authorization from the higher officials is obtained by the law enforcers, they can commence with their collection of evidence.

2. Describe the roles and responsibilities of digital forensic team members

There are usually two teams under a bigger team of people working on digital forensics, and these include the first response team, the analysis and presentation team. The first response team are the ones who record every crucial information and evidences on digital forensics. The team includes an incident manager, scribe or recorder, and an imager. The analysis and presentation team, on the other hand, scrutinize the data acquired by the first response team, and they arrange it to be able to be understood even by non-forensic audiences.

3. List the steps involved in collecting digital evidence

The steps in collecting digital evidence are listed in the following:

* Assessing the scene
* Acquiring the evidence
* Identifying sources
* Authenticating evidentiary material
* Collecting evidence
* Maintaining a chain of custody

4. Discuss the process used to analyze evidence

To analyze digital evidences, the first step is to verify documents on the actual item to ensure the accuracy of the collected evidence. Once through with the first step, a copy of the evidence is created, while the actual one is hidden in a secure place. Disk imaging must then be performed. Two primary tools used on digital forensics are the EnCase Forensic and the Forensic Toolkit. These can provide a huge assistance on the execution of the analysis stage. Once the softwares are utilized, the evidence should now be transcribed in a well-written and organized report.

5. Explain how encryption can thwart digital forensic analysis

Encryption can thwart digital forensic analysis through data leakage. Since digital information can easily be retrieved, shared, and deleted, there is a huge risk that confidential information while the analysis is proceeding can lead to serious predicaments and misuse of evidences.

**References**

Sidhpurwala, H. (2019). *A Brief History of Cryptography*. Retrieved from https://access.redhat.com/blogs/766093/posts/1976023

Nadeeshani, P. (2018). *Basic Principles of Cryptography*. Retrieved from https://medium.com/@nshani/basic-principles-of-cryptography-9a282e7a2d2d

Clark, P.G. (2015). *Modeling Firewalls for Behavior Analysis*. Retrieved from https://pdf.sciencedirectassets.com/280203/1-s2.0-S1877050915X00238/1-s2.0-S1877050915025648/

Petters, J. (2020). *IDS vs. IPS: What is the Difference?* Retrieved from https://www.varonis.com/blog/ids-vs-ips/

Javed, A. (2018). *6 Tips for Implementing Access Control Authentication System with Security*. Retrieved from http://www.xorlogics.com/2018/10/01/6-tips-for-implementing-access-control-authentication-system-with-security/

*Types of Virtual Private Network (VPN) and its Protocols*. (2019). Retrieved from https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/

*Intrusion Prevention System (IPS)*. (2019). Retrieved from https://www.geeksforgeeks.org/intrusion-prevention-system-ips/

EC-Council. (2020). *How do intrusion detection systems work?* Retrieved from https://blog.eccouncil.org/how-do-intrusion-detection-systems-ids-work/

*Different Types of Wireless Communication Technologies*. (2019). Retrieved from https://www.typesnuses.com/different-types-wireless-communication-technologies/

*Securing your wireless network*. (n.d.). Retrieved from https://www.nibusinessinfo.co.uk/content/security-issues-wireless-networks

*Web Threats*. (2013). Retrieved from https://usa.kaspersky.com/resource-center/threats/web

Noonan, C. (2017). *10 Tips to Increase Security on Web Hosting Servers*. Retrieved from https://blog.mailchannels.com/10-tips-to-increase-security-on-web-hosting-servers