Introduction

Introduction to CCNA Security

The “CCNA Security” certificate is a test that validates the knowledge and qualifications required to secure a network made up of Cisco infrastructure.

This allows a network professional to demonstrate the skills required to develop security infrastructure, recognize threats to the network and vulnerabilities in the network, and mitigate these threats in order to maintain integrity, confidentiality and the availability of data and devices.

Prerequisites

1) In order to optimize your learning from this book, it is highly recommended that you examine the objectives required for the following certifications:

– CCENT Cisco;

– CCNA routing and commutation.

Conventions for command syntax

2) The conventions followed in this book to present the syntax for commands are given below:

– text in **bold**: indicates the commands or keywords;

– *italics*: denote the arguments or user variables;

– vertical lines (|): indicate alternative and mutually exclusive elements;

– square brackets ([]): indicate optional elements;

– curly brackets ({}): indicate a necessary choice;

– curly brackets within square brackets ([{}]): indicate a necessary choice in an optional element.

1

Fundamentals of Network Security

This chapter studies the following subjects:

– the chief objectives of securing a network;

– information security terminology:

  - general terminology,

  - types of hackers,

  - malicious codes;

– the types of network security:

  - physical security,

  - logical security,

  - administrative security;

– the chief risks related to the logical security of a network:

  - the different kinds of network attacks,

  - measures for network security,

  - vulnerability audit measures

1.1. Introduction

Network security is the branch of computer science that consists of protecting all components of a computer network in order to prevent unauthorized access, data stealing, misuse of a network connection, modification of data, etc. The aim of

Computer Network Security, First Edition. Ali Sadiqui.

network security is to provide proactive defense methods and mechanisms to protect a network against internal and external threats.

1.1.1. *The main objectives of securing a network*

The three main objectives in securing a network are to ensure:

– **confidentiality**: this consists of protecting data stored on or traveling over a computer network from unauthorized persons;

– **integrity**: this maintains or ensures the reliability of data. The data received by a recipient must be identical to the data transmitted by the sender;

– **availability**: this ensures that network data or services are constantly accessible to users.

1.1.2. *Information security terminology*

1.1.2.1. *General terminology*

– **A resource**: any object that has value for an organization and must be protected.

– **A vulnerability**: a weakness in a system, which may be exploited by a threat.

– **A threat**: a potential danger to a resource or to the functioning of a network.

– **An attack**: this is an action carried out to harm a resource.

– **A risk**: the possibility of an organization's resource being lost, modified, destroyed or suffering other negative consequences. The risk may arise from a single threat or several threats or the exploitation of a vulnerability:

A risk = a resource + a threat + a vulnerability

– **A countermeasure**: protection that mitigates a potential threat or a risk.

1.1.2.2. *Types of hackers*

There are different kinds of hackers in the field of information technology:

– "**hackers**": this group is defined as people who are "network maniacs" and only wish to understand the working of computer systems, while also testing their own knowledge and tools;

– "**white hat hackers**": these are individuals who carry out safety audits in order to test that an organization's computer networks are well-protected;

– "**black hat hackers**": these are experienced individuals who work towards illegal ends by carrying out data theft, hacking accounts, infiltrating systems etc.;

– "**gray hat hackers**": individuals who are a mix of a "white hat" and "black hat" hackers;

– "**blue hat hackers**": these are individuals who test bugs in order to ensure that applications work smoothly;

– "**script-kiddies**": these are individuals with very basic IT security management skills and who try to infiltrate systems using scripts and programs developed by others;

– "**hacktivists**": these are individuals who are chiefly driven by ideological motives;

– "**phreakers**": these are individuals who are specialized in attacking telephonic systems. In general, they work towards placing free calls;

– "**carders**": these are individuals who specialize in attacking smart card systems.

1.1.2.3. *Malicious codes*

The most common types of malicious codes or malware that may be used by hackers are:

– **virus**: this is a program that attaches itself to a software to carry out a specific, undesirable function on a computer. Most viruses need to be activated by the user. However, they can also be set to "idle mode" for prolonged periods as they can also be programmed to avoid detection;

– **worms**: these are independent programs that exploit known vulnerabilities with the aim of slowing down a network. They do not need to be activated by the user, and they can duplicate themselves and attempt to infect other hosts in the network;

– **spyware**: these are spy software that are generally used in order to influence the user, to buy certain products or services. Spyware is not usually automatically self-propagating but install themselves without permission. They are programmed to:

- collect the user's personal information,

- track browsing activity on the internet in order to detect the user's preferences,

- redirect HTTP requests towards pre-set advertising sites;

– **adware**: this refers to any software that displays advertisements without the user's permission, often in the form of pop-up windows;

– **scaryware**: this refers to a category of software that is used to convince users that their system has been infected by viruses and suggests solutions, with the goal being to sell software;

– **Trojan horse**: this is a program characterized by two features:

- behavior that is apparently useful to the user,

- hidden malicious behavior, which usually leads to access to the machine on which this software is executed;

– **ransomware**: ransomware is a program that is designed to block access to a computer system, by encrypting the contents until a certain amount of money is paid in order to restore the system.

1.2. Types of network security

We identify three categories of network security.

1.2.1. *Physical security*

Physical security involves all aspects of the environment in which the resources are installed. This may include:

– the physical security of server rooms, network devices etc.;

– the prevention of accidents and fires;

– uninterrupted power supply;

– video surveillance etc.

1.2.2. *Logical security*

Logical security refers to the implementation of an access control system (using a software) in order to secure resources. This may include:

– applying a reliable security strategy for passwords;

– setting up an access model that is based on authentication, authorization and traceability;

– ensuring the correct configuration of network firewalls;

– putting in place IPS (intrusion prevention systems);

– using VPNs (Virtual Private Network) etc.

1.2.3. *Administrative security*

Administrative security allows the internal monitoring of an organization using a manual of procedures.

This may include:

– preventing errors and frauds;

– defining the responsibilities of different actors or operators;

– protecting the integrity of the company's property and resources;

– ensuring that all operations concerning handling of material are recorded;

– rationally managing the company's property;

– ensuring effective and efficient management of activities.

NOTE.– You can now attempt Exercise 1.

1.3. The main risks related to the logical security of the network

1.3.1. *Different kinds of network attacks*

1.3.1.1. *Reconnaissance attacks*

The aim of reconnaissance attack or "passive attack" is to collect information on the target network in order to detect all the vulnerabilities. In general, this attack uses the following basic methods:

– "**ping sweep**": the attacker sends ping packets to a range of IP addresses to identify the computers that are part of a network.

– **port scanning**: the attacker carries out a port analysis (TCP and UDP) in order to discover what services are being run on a target computer;

– **packet sniffing**: "packet sniffing" makes it possible to capture data (generally Ethernet frames) that are traveling over a network, with the aim of identifying MAC addresses, IP addresses or the number of ports used in a target network. This attack can even make it possible to discover user names or passwords. The most commonly used packet capture software is **wireshark** and **tcpdump**.

1.3.1.2. *Password attacks*

The goal of these attacks is to discover usernames and passwords in order to access various resources. There are two commonly used methods in this type of attack:

– **dictionary attack**: this method uses a list of words or phrases that are commonly used as passwords;

– **brute force attack**: this method tries out all possible combinations of letters, numbers and symbols to detect a user's password.

1.3.1.3. *Access attacks*

The aim of these attacks is to try and recover sensitive information about network components. The following methods are commonly used to carry out an access attack:

– **phishing**: phishing is an attempt to recover sensitive information (usually financial information such as credit card details, login, password, etc.), by sending unsolicited emails with fake URLs;

– **pharming**: this is another network attack that aims to redirect traffic from one website to another website;

– "**Man-in-the-middle**" **attack**: an attacker places themselves between two network components to try and benefit from the data being exchanged. This attack is based, among other things, on:

- **spoofing**: this is a practice in which communication is sent from an unknown source disguised as a reliable source for the receiver. This makes it possible to deceive a firewall, a TCP service, an authentication server etc. Spoofing may take place at several levels: MAC address, IP address, TCP/UDP port, a DNS domain name,

- **hijacking**: the attacker hijacks a session between a host and server to obtain unauthorized access to this service. This attack relies on spoofing;

– **mixed attacks**: Mixed attacks combine the characteristics of viruses, worms, and other software to collect user information.

1.3.1.4. *Network attacks against availability*

– **DoS** or Denial of Service attacks are attacks that render a service unavailable in various ways. These attacks can be divided into two main categories:

- denial of service by saturation: these attacks consist of flooding a machine with false requests so that it is unable to respond to real requests;

- denial of service by exploiting vulnerability: these attacks consist of exploiting a weakness in a remote system in order to make it unavailable.

– **DDoS** or *Distributed Denial of Service* attacks are a type of DoS attack originating from many connected computers controlled by hackers who attack from different geographic locations. The principles underlying these attacks are based on the follow methods (among others):

- SYN flood attacker: an attacker sends several TCP-SYN packets to set up a 'TCP' connection without sending a "SYN-ACK" message;

- ICMP flood: an attacker sends the target computer multiple fake ICMP packets.

1.3.1.5. *Close attacks*

A close attack is unusual in that the attacker is physically close to the target system. The attacker takes advantage of the fact that they are close to the target devices to reset a router, for example, or start a server with a CD etc.

1.3.1.6. *Attacks on the approval relationships*

When taking control of a network machine, the attacker exploits the relationship of approval between this machine and the various peripheral devices on a network in order to gain greater control.

1.3.2. *Network security measures*

In order to ensure greater security to a network within a company, the following measures are recommended:

– **separation of resources**: the network of resources of an organization and various sensitive data must be located in different security zones (for example, creation of a DMZ cone). Access to the network of an organization and to databases must be carried out through highly monitored mechanisms.

– **deep protection**: network security devices must be used in different locations of the organization's network;

– **the "least privilege" rule**: each user must be assigned only the minimal level of access required to carry out a given task;

– **adequate protection**: protection mechanisms must be installed in a reliable and effective manner at all levels of the network;

– **restricting the consultation of information**: only information required for carrying out a specific task must be provided to a given employee.

– **separation of tasks and job rotation**: the separation of tasks and job rotation contributes to a better implementation of security policies in organizations and to the reduction of vulnerabilities.

1.3.3. *Vulnerability audit measures*

A computer network audit must include the following five categories:

– **preventive measures**: these include precautions taken to prevent the exploitation of a vulnerability, through the use of a firewall, physical locks and an administrative security strategy;

– **detective measures**: these include the retrieval of all information on intrusion into the network or system using system logs, intrusion prevention systems (IPS), anti-spoofing technologies and surveillance cameras;

– **corrective measures**: these include determining the cause of a security violation and then mitigating these effects through updating viruses or IPS;

– **recovery measures**: these enable system recovery after an incident;

– **deterrence measures**: these discourage persons who try to breach network security.

1.4. Exercises to test learning

ETL 1.–

1. What security term refers to property or data that is valuable to an organization?

a. A risk.
b. A resource.
c. A countermeasure.
d. A vulnerability.

2. Which of the following elements represents a physical security measure?

a. The policy of changing security agents.
b. The daily verification of equipment event logs.
c. Implementing electronic locks.
d. Putting in place access lists.

3. Which of the following is a reason for using firewalls?

a. Preventing unauthorized access of incoming or outgoing requests into a network.
b. Preventing damage to a computer in case of fire.
c. Facilitating the downloading of data from websites.
d. Detecting and cleaning viruses on a computer.

4. Which of the following respects confidentiality of information?

a. Discussing confidential data over the telephone.
b. Disclosing confidential information only to authorized persons.
c. Downloading confidential information on a shared website.
d. Sending confidential information to a colleague.

5. Match the type of hacker to their description.

Type of hacker	Description
1. Carders	a. Individuals who use their computer skills for financial gain or to harm individuals or organizations
2. Hacktivists	b. They usually contribute to the identification and repair of security weaknesses within a system.
3. Phreakers	c. They chiefly attack smartcard systems in order to exploit their vulnerabilities.
4. White Hat	d. Individuals who use their computer skills in order to bring about political or social change.
5. Black Hat	e. People who make use of telephone networks to place calls for free.

6. What kind of malicious program *may be described as a software that attaches itself to another program in order to execute an undesirable function*?

a. Virus.

b. Spyware.
c. Trojan.
d. Adware.
e. Worm.

7. What is the chief characteristic of worms?

a. A worm can run independently.
b. A worm must be activated by an event on the host system.
c. A worm disguises itself as a legitimate software.
d. Once installed on the host system, the worm does not replicate itself.

8. Classify the security measures into physical, logical or administrative.

Physical security	Logical security	Administrative security

- Defining the time of entry and exit from the computer room.
- Installing an incident protection system.
- Installing a firewall.
- Defining rules for an ACL.
- Recording all operations related to the handling of equipment.
- Installing surveillance cameras.
- Changing the location of an IPS system.
- Defining the length of encryption key.
- Mandating that all visitors wear badges.
- Putting in place the “least privilege” principle for accessing equipment.

9. Which of these describes spam?

a. Collecting information about a person or an organization without authorization.
b. Carrying out an unauthorized action such as modifying or deleting files.
c. Putting an unnecessary load on the system by copying files.
d. Sending unwanted masses in bulk.

10. Which of the following elements describes how a security breach must be reported?

a. Using the telephone.
b. Sending an email to the IT manager.

c. Using any means of communication.
d. Using the method given in the organization's security policy.

11. When you access a website, what icon in the address bar indicates that the site is secured?

a. An arrow.
b. A lock.
c. A star.
d. A shield.

12. Which of the following may intercept and use your messages for its own purposes?

a. The media.
b. Governments.
c. Advertising agencies.
d. Crime networks.
e. All of the above.

13. What is the main method that is used to protect against malware?

a. Using encrypted authentication technologies.
b. Installing an antivirus software on all host devices.
c. Blocking ICMP responses.
d. Deploying intrusion prevention systems across the network.

14. Which of the following describes a Trojan horse?

a. Malware embedded in a seemingly legitimate executable program.
b. Malware that sends extreme amounts of data in order to block a service.
c. An electronic dictionary used to obtain the network administrator's password.
d. A software used to convince users that their system has been infected by viruses.

ETL 2.–

1. What simple countermeasure can be used to mitigate a "**ping sweep**" attack?

a. Use encrypted authentication protocols.
b. Installing an antivirus on the hosts.

c. Deploying “anti-sniffer” software on all network devices.
d. Blocking ICMP echo responses on all network devices.

2. What network security countermeasures can be used to protect against DoS attacks? Choose two answers.

a. Installing antivirus software.
b. Putting in place IPS (intrusion protection systems).
c. Installing applications to authenticate users.
d. Installing anti-spoofing technology.
e. Putting in place data encryption technology.

3. How can you define a **“ping sweep”**?

a. This is a network scanning technique that can discover available hosts available in an IP address range.
b. This is an application that allows the capture of all network packets sent over a LAN.
c. This is a technique that examines a range of port numbers (TCP or UDP) available on a LAN.
d. This is a technique that can discover all the IP addresses available on a LAN using frame analysis.

4. What are the two characteristics of DoS attacks? Choose two answers.

a. They always precede access attacks.
b. They try to compromise the availability of a network, host, or application.
c. They are difficult to carry out and are only initiated by highly skilled attackers.
d. They always use the ICMP protocol.
e. They are easy to detect.

5. What happens in a spoofing attack?

a. An attacker modifies the data that transits over the network to access confidential information.
b. An attacker sends large amounts of network traffic to a device to make it inaccessible to users.
c. An attacker sends poorly formatted frames to a target device to cause it to malfunction.
d. An attacker sends malicious code to steal all data stored on a device.

6. What is the type of attack where an attacker uses an unauthorized access point to capture network traffic from a targeted user?

a. Attacks on the approval relationship.
b. Buffer overflow attack.
c. “Man-in-the-middle” attack.
d. DDoS attack

7. This is a type of network security attack in which the intruder takes control of communication between two entities in order to use it for his benefit.

a. Phishing.
b. Buffer overflow.
c. Pharming.
d. Hijacking.
e. SYN flood.

8. What happens in a buffer overflow attack?

a. An attacker redirects traffic from one website to another website.
b. Attackers send multiple queries from many connected computers in different geographic regions to render a service unavailable.
c. The attacker combines the characteristics of viruses, worms and other software to collect information about users.
d. The attacker tries to write additional data in the saturated memory of an equipment.

9. What is the risk of sharing too much information on social networking sites?

a. Phishing.
b. Buffer overflow.
c. Pharming.
d. Hijacking.
e. Ransom.

10. How many characters must be used to create a strong password?

a. Eight characters.
b. Sixteen characters.
c. The maximum number of characters possible.
d. The number of characters does not matter.

11. Strong passwords can be difficult to remember, what can you do to avoid forgetting them?

a. Use acronyms or phrases that are easy to remember.
b. Develop a password strategy.
c. Use password management software with encryption.
d. All of the above.

12. How long does it take for an attacker to detect a 10-character password?

a. Less than an hour.
b. Less than a week.
c. Less than a month.
d. It depends on many factors.

13. An attacker uses the **wireshark** tool to discover usernames and administrative passwords. What kind of network attack is this?

a. A “Man-in-the-middle” attack.
b. A DoS attack.
c. A reconnaissance attack.
d. A close attack.