User Account and Password Security

by Sophia

WHAT'S COVERED

In this lesson, you will learn about user account management and authentication.

Specifically, this lesson will cover the following:

1. Managing User Accounts
    1a. Disabling Accounts
    1b. Limiting Simultaneous Connections
    1c. Renaming the Maintenance Account
2. Authentication
    2a. Managing Passwords
    2b. Minimum Length
    2c. Using Characters to Make a Strong Password
    2d. Password Management Features
    2e. Lightweight Directory Access Protocol (LDAP)
    2f. Certificates
    2g. Multifactor Authentication

1. Managing User Accounts

Usernames and passwords are vital to network security because their whole purpose is to control initial access to the network. Even if the system administrator assigns individuals their usernames and passwords, users can and often do change them, so you need to make sure your network’s users know the difference between a good password and a bad one and how to keep their passwords safe from theft.

We will cover the important security issues related to user account and password management. Moreover, in the following sections, we will discuss more secure methods of authentication (two-factor and multifactor authentication) and a widely used concept in the enterprise networks called single sign-on.

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

The first step in managing access to network resources is through user accounts and the rights you assign to the network resources. System administrators usually maintain user accounts on a daily basis, doing things like renaming accounts and setting the number of simultaneous connections. You can also specify where users can log in, how often, and when; plus, you can adjust how often their passwords expire and delimit when their accounts expire as well.

1a. Disabling Accounts

☆ BIG IDEA

This is important, so remember it—when a user leaves the organization, you have these three options:

- Leave the account in place.
- Delete the account.
- Disable the account.

EXAMPLE Leaving the account active is a bad idea because the user to whom it belonged can still log in. This is clearly insecure, but simply deleting the account presents its own set of problems. If you delete an account, the numeric ID associated with that user will be lost, and it is through this number that passwords and rights to network resources are associated with the user account. When you disable an account, it still exists, but no one can use it to log in. Another good time to disable an account is when someone leaves for an extended period, like taking maternity/paternity leave or other medical leaves or going on sabbatical. Because it is really common for companies today to have contract and temporary employees, you need to know how to manage temporary accounts that will be used for only a short time and then disabled. Managing these temporary accounts is easy; you just set the account to expire on the employee's expected last day of work.

1b. Limiting Simultaneous Connections

There is a good reason to limit how many times a user can connect to the network. Users should normally be logged in to the network for one instance because they can only be in one place at a time. So, if your system is telling you that someone is logged in from more than one place, it is probably because someone else is using their account. By disallowing simultaneous connections, only a single user at a single workstation can gain access to the network using a specific user account.

You may also want to limit the specific location from which a user logs in because most of the time, your users will be logging on to the network only from their own workstations. Although this makes sense, this rule is not usually enforced because, sometimes, users move around without taking their computers with them or log in at someone else's station to get their jobs done.

1c. Renaming the Maintenance Account

Network operating systems automatically give the network maintenance (or administration) account a default name. On Windows servers, it is "Administrator," and in Unix, it is "root." The best practice is to change these account names to make it more difficult for an attacker to gain unauthorized access to a server.

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

2. Authentication

Authentication, in relation to computing, involves mechanisms for providing proof of the identity of a user logging on to a network or device. For example, when you unlock your smartphone using a passcode, fingerprint, or facial recognition, you are authenticating yourself to the device so that it allows you to access its functions and resources.

TERM TO KNOW

Authentication

Providing proof of the identity of a user logging on to a network or device.

2a. Managing Passwords

Like any other aspect of network security, passwords must be managed, and doing that involves ensuring that all passwords for user accounts follow security guidelines so that bad guys cannot easily guess or crack them. You have also got to implement certain features of your network operating system to prevent unauthorized access.

HINT

Basically, a strong password is some combination of alphanumeric and special characters that is easy for you to remember but really hard for someone else to guess. Like server account names, they should never be written down on anything that is then put into your desk or stuck onto your computer. Let us look at some characteristics of strong passwords.

2b. Minimum Length

Strong passwords should be at least 8 characters, but they should not be any longer than 15 characters to make them easier to remember. You absolutely must specify a minimum length for passwords because a short password is easily cracked. The upper limit depends on the capabilities of your operating system and the ability of your users to remember complex passwords.

2c. Using Characters to Make a Strong Password

A strong password needs to include a combination of numbers, letters, and special characters. Special characters are not letters or numbers, but symbols like the following: $ % ^ # @.

EXAMPLE A strong password would be tqbf4#jotld. It looks like gibberish, but remember that famous sentence, “The quick brown fox jumped over the lazy dog.”? Well, this particular password uses the first letter of each word in that sentence with a 4# thrown in the middle of it. You can do this with favorite quotes, song lyrics, and so on, with a couple of numbers and symbols stuck in the middle.

If you want to test the strength of passwords to make sure they are nice and tight, you can use auditing tools like crack programs that try to guess passwords. Clearly, if that program has a really tough time or even fails to crack the password, you have a good one. It is best to not just use a regular word preceded by or ending with a

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

special character because good crack programs strip off the leading and trailing characters during decryption attempts.

2d. Password Management Features

All network operating systems include built-in features for managing passwords to help ensure that your system remains secure and that passwords cannot be easily hacked with crack programs. These features usually include automatic account lockouts and password expiration. This is done by storing and recalling saved passwords locally. They make it practical to use longer, stronger passwords than you could remember otherwise..

Automatic account lockouts prevent hackers and users who forget their passwords, from trying to log in by guessing passwords. This is why most network operating systems will lock you out after a few unsuccessful attempts. Some will even disable the account. Once that happens, the user won’t be able to log in to that account even if they enter the correct password. This feature prevents a potential hacker from running an automated script to crack account passwords by continuously attempting to log in using different character combinations.

DID YOU KNOW

When an account is on lockdown, network staff will have to unlock the account if the network operating system does not unlock it after a preset period. In any high-security network, it is a good idea to require an administrator to manually unlock every locked account instead of setting the network operating system to do it automatically. This way, the administrator will be sure to know about any possible security breaches.

Password expiration and password histories support common practice where passwords expire after a specific amount of time. While this is debated because of users often using less secure passwords, most organizations set up passwords to expire every 30 to 45 days, after which the network’s users must all reset their passwords either immediately or during a preset grace period. The grace period is usually limited to a specific number of login attempts, or it may allow a couple of days.

DID YOU KNOW

You can force users to change their passwords to ones that have not been used before, because the latest operating systems require unique passwords and can, depending on the network operating system, store more than 20 previously used passwords. This feature makes it harder to revert to any previous passwords.

In today’s enterprises, users can be overwhelmed by the number of points in the network where they may be challenged to identify themselves. Most users have to log onto the domain to have network access at all, and then there may be company websites that require an authentication process to access databases, secured drives, personal folders, and more. **Single sign-on (SSO)** helps users access multiple accounts with one sign-on event.

When users must remember multiple passwords, as the number increases, they begin to resort to unsafe security practices such as writing passwords on sticky notes, hiding passwords in their drawers, and even sharing them with coworkers. All of these practices undermine the security of the network.

HINT

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

Single sign-on (SSO) addresses this problem. With single sign-on, when the user logs into the domain, the domain controller issues them an access token. This access token contains a list of all the resources (which can include folders, drives, websites, databases, and so on) to which they should have access. As a result, any time the user accesses a resource, the token is verified behind the scenes, and the user never needs to provide another password.

TERM TO KNOW

Single Sign-On (SSO)

An authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

2e. Lightweight Directory Access Protocol (LDAP)

A **directory service** is a database designed to centralize data management regarding network subjects and objects, including user accounts. A typical directory contains a hierarchy that includes users, groups, systems, servers, client workstations, and so on. Because the directory service contains data about users and other network entities, it can be used by many applications that require access to that information. A common directory service standard is Lightweight Directory Access Protocol (LDAP), which is based on the earlier standard X.500.

TERM TO KNOW

Directory Service

A database that maps the names of network resources to their respective network addresses.

2f. Certificates

A **digital certificate** provides an entity, usually a user, with the credentials to prove its identity and associates that identity with a public key. At minimum, a digital certification must provide the serial number, the issuer, the subject (owner), and the public key. An X.509 certificate complies with the X.509 standard.

KEY CONCEPT

VeriSign first introduced the following digital certificate classes:

- Class 1: For individuals and intended for email; these certificates get saved by web browsers
- Class 2: For organizations that must provide proof of identity
- Class 3: For servers and software signing in which independent verification and identity and authority checking is done by the issuing CA

TERM TO KNOW

Digital Certificate

An electronic document used to prove the validity of a public key.

2g. Multifactor Authentication

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

Multifactor authentication is designed to add an additional level of security to the authentication process by verifying more than one characteristic of a user before allowing access to a resource. Users can be identified in one of five ways:

- By something they know (password)
- By something they are (retinas, fingerprint, and facial recognition)
- By something they possess (smart card)
- By somewhere they are (location)
- By something they do (behavior)

Two-factor authentication is when two of the above factors are being tested, while **multifactor authentication** is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. An example of two-factor authentication would be requiring both a smart card and a **personal identification number (PIN)** to log onto the network. The possession of either by itself would not be sufficient to authenticate. This protects against the loss and theft of the card as well as the loss of the password. An example of multifactor would be when three items are required, such as a smart card, a PIN, and a username and password.

HINT

This process can get as involved as the security requires. In an extremely high-security situation, you might require a smart card, a password, a retina scan, and a fingerprint scan.

The trade-off to all the increased security is an inconvenient authentication process for the user and the high cost of biometric authentication devices.

TERMS TO KNOW

Two-Factor Authentication

An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two pieces of evidence (or factors) to an authentication mechanism.

Multifactor Authentication

A layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login.

Personal Identification Number (PIN)

A numeric passcode used in the process of authenticating a user accessing a system.

SUMMARY

In this lesson, you learned about user account management and **authentication**. We discussed **managing user accounts**, including **disabling accounts**, **limiting connections**, and **renaming the maintenance account**. You also learned about authentication mechanisms, specifically **managing passwords**, **minimum password lengths**, **using characters to make a strong password**, **password**

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

management features, **Lightweight Directory Access Protocol (LDAP)**, **certificates**, and **multifactor authentication**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Authentication
Providing proof of the identity of a user logging on to a network or device.

Digital Certificate
An electronic document used to prove the validity of a public key.

Directory Service
A database that maps the names of network resources to their respective network addresses.

Multifactor Authentication
A layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user’s identity for login.

Personal Identification Number (PIN)
A numeric passcode used in the process of authenticating a user accessing a system.

Single Sign-On (SSO)
An authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

Two-Factor Authentication
An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two pieces of evidence (or factors) to an authentication mechanism.

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.