Nowgong Polytechnic
Subject: Professional Practice-II
Branch: Computer Engineering
Semester: 4th
Session: Jan-202-June-2020

Server Security and Administration

Secure Server Connectivity

1. Establish and Use a Secure Connection

When connecting to a remote server, it is essential to establish a secure channel for communication.

Using the **SSH** (**Secure Shell**) **Protocol** is the best way to establish a protected connection. Unlike the previously used Telnet, SSH access encrypts all data transmitted in the exchange.

You need to install the SSH Daemon and to have an SSH Client with which you issue commands and manage servers to gain remote access using the SSH protocol.

By default, **SSH uses port 22**. Everyone, including hackers, knows this. Most people do not configure this seemingly insignificant detail. However, changing the port number is an easy way to reduce the chances of hackers attacking your server. Therefore, the best practice for SSH is to **use port numbers between 1024 and 32,767**.

2. Use SSH Keys Authentication

Instead of a password, you can authenticate an SSH server using a pair of SSH keys, a better alternative to traditional logins. The keys carry many more bits than a password and are not easily cracked by most modern computers. The popular RSA 2048-bit encryption is equivalent to a 617-digit password.

The key pair consists of a public key and a private key.

The public key has several copies, one of which remains on the server, while others are shared with users. Anyone that has the public key has the power to encrypt data, while only the user with the corresponding private key can read this data. The private key is not shared with anyone and must be kept secure. When establishing a connection, the server asks for evidence that the user has the private key, before allowing privileged access.

3. Secure File Transfer Protocol

To transfer files to and from a server without danger of hackers compromising or stealing data, it is vital to use **File Transfer Protocol Secure (FTPS)**. It encrypts data files and your authentication information.

FTPS uses both a command channel and a data channel, and the user can encrypt both. Bear in mind that it only protects files during transfer. As soon as they reach the server, the data is no longer encrypted. For this reason, encrypting the files before sending them adds another layer of security.

4. Secure Sockets Layer Certificates

Secure your web administration areas and forms with **Secure Socket Layer (SSL)** that guards information passed between two systems via the internet. SSL can be used both in server-client and in server-server communication.

The program scrambles data so that sensitive information (such as names, IDs, credit card numbers, and other personal information) is not stolen in transit. Websites that have the SSL certificate have HTTPS in the URL, indicating they are secure.

Not only does the certificate encrypt data, but it is also used for user authentication. Therefore, by managing certificates for your servers, it helps establish user authority. Administrators can configure servers to communicate with centralized authority and any other certificate that the authority signs.

5. Use Private Networks and VPNs

Another way to ensure secure communication is to use private and virtual private networks (VPNs), and software such as OpenVPN. Unlike open networks which are accessible to the outside world and therefore susceptible to attacks from malicious users, private and virtual private networks restrict access to selected users.

Private networks use a private IP to establish isolated communication channels between servers within the same range. This allows multiple servers under the same account to exchange information and data without exposure to a public space.

When you want to connect to a remote server as if doing it locally through a private network, use a VPN. It enables an entirely secure and private connection and can encompass multiple remote servers. For the servers to communicate under the same VPN, they must share security and configuration data.

Server User Management

6. Monitor Login Attempts

Using intrusion prevention software to monitor login attempts is a way to protect your server against brute force attacks. These automated attacks use a trial-and-error method, attempting every possible combination of letters and numbers to gain access to the system.

Intrusion prevention software oversees all log files and detects if there are suspicious login attempts. If the number of attempts exceeds the set norm, intrusion prevention software blocks the IP address for a certain period or even indefinitely.

7. Manage Users

Every server has a root user who can execute any command. Because of the power it has, the root can be very hazardous to your server if it falls into the wrong hands. It is widespread practice to disable the root login in SSH altogether.

Since the root user has the most power, hackers focus their attention on trying to crack the password of that specific user. If you decide to disable this user entirely, you will put attackers in a significant disadvantage and save your server from potential threats.

To ensure outsiders do not misuse root privileges, you can create a limited user account. This account does not have the same authority as the root but is still able to perform administrative tasks using sudo commands.

Therefore, you can administer most of the tasks as the limited user account and use the root account only when necessary.

Server Password Security

8. Establish Password Requirements

The first thing is to set password requirements and rules that must be followed by all members on the server.

Do not allow empty or default passwords. Enforce minimum password length and complexity. Have a lockout policy. Do not store passwords using reversible encryption. Force session timeout for inactivity and enable two-factor authentication.

9. Set Password Expiration Policy

Setting an expiration date for a password is another routine practice when establishing requirements for users. Depending on the level of security required, a password may last a couple of weeks or a couple of months.

10. Use Passphrases For Server Passwords

There are several reasons why using a passphrase rather than a password can help elevate server security. The main difference between the two is that a passphrase is longer and contains spaces between the words. Therefore, it is often a sentence, but it does not have to be one.

For example, a password passphrase may be: **Ilove!ToEatPizzaAt1676MainSt.**

The given example is longer than a usual password, and it contains upper and lower case letters, numbers, and unique characters.

Furthermore, it is much easier to remember a passphrase than a string of random letters. Finally, since it consists of 49 characters, it is more difficult to crack.

11. Password Don’ts

If you want to maintain a secure server, there are a few things you want to avoid when it comes to passwords. Firstly, be mindful where you store passwords. Do not write them on pieces of paper and hide them around the office.

It is generally advisable not to use personal information like your birthday, hometown, pet names and other things that can connect you, the user, to the password. These are extremely easy to guess, especially by people who know you personally.

Passwords that only contain simple dictionary words are also easy to crack, especially by dictionary (brute force) attacks. Mindful of the same risk, try to avoid repeating sequences of characters in the same password.

Finally, **do not use the same password for multiple accounts**. By recycling passwords, you put yourself at significant risk. If a hacker manages to get access to a single account, all other accounts with the same password may be in danger. Try to use a different password for every separate account and keep track of them using a password manager such as KeePass.

Other Best Practices to Secure a Server

12. Update and Upgrade Software Regularly

Regularly updating the software on a server is a crucial step in keeping it safe from hackers. Outdated software has already been explored for its weak points, leaving it open for hackers to take advantage of these and harm your system. If you keep everything up-to-date, you ensure that it is updated to protect itself in the first line of defense.

Automatic updates are one way to guarantee that no updates are forgotten. However, allowing the system to make such changes on its own may be risky. Before updating your production environment, it is good practice to examine how the update performs in a test environment.

Make sure to update the server control panel routinely. You also need to regularly update content management systems, if you use one, as well as any plugins it may have. Each new release includes security patches to fix known security issues.

13. Remove or Turn Off All Unnecessary Services

Increase server security by reducing the so-called attack vector.

This cyber-security term refers to installing and maintaining only the bare minimum requirements needed to keep your services running. Just enable the network ports used by the OS and installed components. The less you have on the system, the better.

A Windows OS server should only have required operating system components. A Linux operating system server should have a minimal installation with only the truly necessary packages installed.

Since most Linux distributions listen for incoming connections on the internet, you want to configure a firewall to allow only specific ports and deny all other unnecessary communication.

Check for dependencies before installing software on your system to ensure you are not adding anything you do not need. Additionally, inspect which dependencies were auto-started on your system and whether you want them there.

14. Hide Server Information

Try to provide as little information about the underlying infrastructure as possible. The less is known about the server, the better.

Also, it is a good idea to hide version numbers of any software you have installed on the server. Often they reveal, by default, the exact release date which can aid hackers when searching for weaknesses. It is usually simple to remove this information by deleting it from the HTTP header of its greeting banner.

15. Use Intrusion Detection Systems

To detect any unauthorized activities, use an **intrusion detection system (IDS)**, such as Sophos, which monitors processes running on your server. You may set it to check day-to-day operations, run periodical automated scans, or decide to run the IDS manually.

16. File Auditing

File auditing is another good way to discover unwanted changes on your system.

It is keeping a record of all the characteristics of your system when it is in a good, “healthy,” state and comparing it to the current state. By comparing the two versions of the same system side to side, you can detect all the inconsistencies and track their origin.

17. Service Auditing

Service auditing explores what services are running on the server, their protocols, and which ports they are communicating through. Being aware of these specifics helps configure attack surfaces in the system.

18. Set Up and Maintain a Firewall

Secure your server by controlling and restricting access to your system.

Using CSF (ConfigServer and Firewall) is essential in tightening up security on your server. It allows only specific vital connections, locking down access to other services.

Set up a firewall during the initial server setup or when you make changes to the services the server offers. By default, a typical server runs different services including public, private and internal services.

- **Public services** are generally run by web servers that need to allow access to a website. Anyone can access these services, often anonymously, over the internet.
- **Private services** are used when dealing with a database control panel, for example. In that case, a number of selected people require access to the same point. They have authorized accounts with special privileges inside the server.
- **Internal services** are ones that should never be exposed to the internet or outside world. They are only accessible from within the server and only accept local connections.

The role of the firewall is to allow, restrict and filter access according to the service the user is authorized for. Configure the firewall to restrict all services except those mandatory for your server.

19. Back Up Your Server

Although the previously mentioned steps are designed to protect your server data, it is crucial to have a backup of the system in case something goes wrong.

Store encrypted backups of your critical data offsite or use a cloud solution.

Whether you have automated backup jobs or do them manually, make sure to make a routine of this precautionary measure. Also, you should test backups, doing comprehensive backup testing. This should include “sanity checks” in which administrators or even end users verify that data recovery is coherent.

20. Create Multi-Server Environments

Isolation is one of the best types of server protection you can have.

Full separation would require having dedicated bare metal servers that do not share any components with other servers. Although this is the easiest to manage and provides the most security, it is also the most expensive.

Having isolated execution environments in a data center allow the so-called Separation of Duties (SoD) and setting server configuration according to the functions the server fulfills.

Separating database servers and web application servers is a standard security practice. Separate execution environments are especially beneficial to larger scale businesses that cannot afford any security breaches.

Independent database servers secure sensitive information and system files from hackers that manage to gain access to administrative accounts. Also, isolation lets system administrators to separately configure the web application security and minimize the attack surface by setting web application firewalls.

21. Create Virtual Isolated Environments

If you cannot afford or do not require full isolation with dedicated server components, you can also choose to isolate execution environments.

Doing so helps you deal with any security problems that may arise, ensuring other data is not compromised. You can choose between containers or VM virtualization which are much easier to set up.

Another option for virtualized environments in a UNIX operating system is creating chroot jails. Chroot is separating a process from the central operating system's root directory and allowing it to access only files within its directory tree. However, this is not complete isolation and should be practiced only with other security measures.

Wrapping Up: Securing Your Server

After reading this article and following the security recommendations, you should be more confident in your server security.

Many of the security measures should be implemented during the initial set up of the server, while others should be part of continuous or periodic maintenance. If your server monitoring is not automated, make sure to design and follow scheduled security checks.

ways to secure an SSH connection.

Facilitate by:
SHA Azad
Lecturer cum HoD(i/c) Computer Engineering