A Comprehensive Guide to TCP/IP Network Security

No comments

This guide does not intend to provide a detailed description of TCP/IP's basic concepts but addresses security concerns related to TCP/IP. For various reasons, the person who administers your system might have to meet a certain level of security. For example, the corporate policy might dictate the level of security. It might be necessary for a system to communicate at a certain level of security with government systems. Security standards may apply to the network, the operating system, applications, or your systems administrator's applications.

TCP/IP Security Features

The purpose of this section is to describe both the standard and secure features of TCP/IP and to discuss some issues of security that would be appropriate in a network environment.

Operating system-specific security

The operating system provides many security features available for TCP/IP, such as network access control and auditing.

TCP/IP command security

TCP/IP provides a secure operating environment via commands such as ftp, rexec, and telnet.

Trusted processes

Trusted programs, or trusted processes, are programs, shell scripts, or daemons that meet a particular threshold of security defined by the US Department of Defense, which certifies some trusted programs.

Network Trusted Computing Base

TCP/IP is one of the components of the Network Trusted Computing Base (NTCB), which consists of hardware and software.

Data security and information protection

In TCP/IP, user data is not encrypted when being transmitted over a network.

Control of TCP ports with discretionary access for internet ports based on user authentication

Users can control access to TCP ports for communication between AIX® hosts using DACinet (Discretionary Access Control for Internet Ports).

Countermeasures to possible attacks on the TCP/IP protocol stack

Threats can threaten both applications and assets, making companies vulnerable to serious risks. Intentional attacks can be perpetrated by outsiders or internal staff, including ex-employees, disgruntled workers, or malicious actors. Personnel who have knowledge of security systems and the structure of an information system, as well as authorization to access the system itself, are more likely to get hold of information or insert malicious code. Security has become increasingly important as the Internet has developed and information has been distributed over shared lines. The corporate network can be compromised, and data will be stolen if not adequately protected from unauthorized access.

Vulnerabilities in network communication

Following the TCP/IP implementation paradigm, network communication on the Internet follows a layered approach, with each layer adding to the activity of the previous layer. Compared to the standard ISO/OSI protocol stack (Application, Presentation, Session, Transport, Network, Data Link, Physical), the TCP/IP protocol stack consists of only four layers: Application, TCP, IP, and Network Access. Following this model, any data, divided into packets by the host at each layer, is sent along a network path involving many intermediate nodes to a remote recipient host. Attacks that exploit the system, control, and security policy vulnerabilities can affect each layer.

Consider what types of threats each layer could face

The Application Layer

Its purpose is to interface with the users and to provide services for application processes, which is the highest layer in a stack. Additionally, this layer contains standard and native applications such as Telnet, SMTP, and FTP. Because of this, it can be vulnerable to attacks such as phishing (scammers pose as legitimate contacts) and hijacking (unauthorized access to the system).

Transport layer

Transporting data, dividing it into packets, and handling transmission errors are the responsibilities of the TCP layer (Transport layer). By saturating the transmission bandwidth, this layer can be subjected to a classic attack known as Denial of Service, which disables, interrupts, or damages a website, a service, or the entire network communication. In contrast, the IP layer, which manages data addresses through their transmission through the network, can be subjected to a common attack scenario known as the Man in the Middle attack.

Two ISO/OSI layers

Finally, the network access layer comprises two layers of ISO/OSI: the data link and the physical channel. Regardless of the network type, the data link specifies how the network card should send data. In network communication, for example, ARP spoofing hides an unknown source as legitimate and trustworthy by manipulating the data link layer. By capturing data circulating over the network (for example, copper cable/electrical pulses or fiber optics/light modulation), packet sniffing techniques can pose a real threat to the confidentiality of communications on the physical channel that converts digital data over the transmission medium.

Mitigating the damage

The following defense tools can make it more difficult and costly for an attacker to execute and detect an attack and mitigate its effects:

Firewall

An application layer firewall is a hardware/software tool that protects hosts or network segments from potentially harmful traffic coming from external networks (for example, the Internet). There are four levels of firewalls that are supported by this tool: Application (Application Layer Firewall), TCP (Stateful Firewall), IP (Network Layer Firewall), and Data Link (Bridge Firewall).

Intrusion Detection System (IDS)

The purpose of an IDS is to detect possible unwanted manipulations of a system or network. It can detect, for instance, sniffing attacks (Network Access Layer) or DoS attacks (TCP Layer).

Protocol security

Generally, it is difficult to ensure that network traffic does not get intercepted. As a result, one solution might be to encrypt the transmitted data so that it cannot be spied upon. Using a VPN (Virtual Private Network), a secure communication network can be created over the Internet, which is not secure. It encapsulates network packets and transports them over a virtual tunnel before being encrypted and decrypted at both ends of the VPN network after an authentication phase. Depending on the layer of the ISO/OSI stack, encapsulation and tunneling can help protect the data transmitted. In terms of security protocols, PPTP and L2PT are commonly used (Data link layer), IPSEC and SSL/TLS are common (Transport layer), and HTTPS is common (Application layer).

Security analysis

An audit of a company's security policies can be used to monitor and evaluate them. Performing this operation, which is only possible within the company's network, requires an in-depth understanding of all the network resources to be examined. A penetration test can be conducted as an alternative or in conjunction with a security audit to simulate an attack from outside the network without knowing the infrastructure characteristics in advance.

Security awareness

For the organization to be protected better, it is more important than ever to increase awareness of the various aspects of IT security and user awareness. An adequate security awareness programme provides basic skills to users (employees and managers) and establishes appropriate prevention guidelines and rules of conduct, as well as internal/external training, newsletters, and intranets.

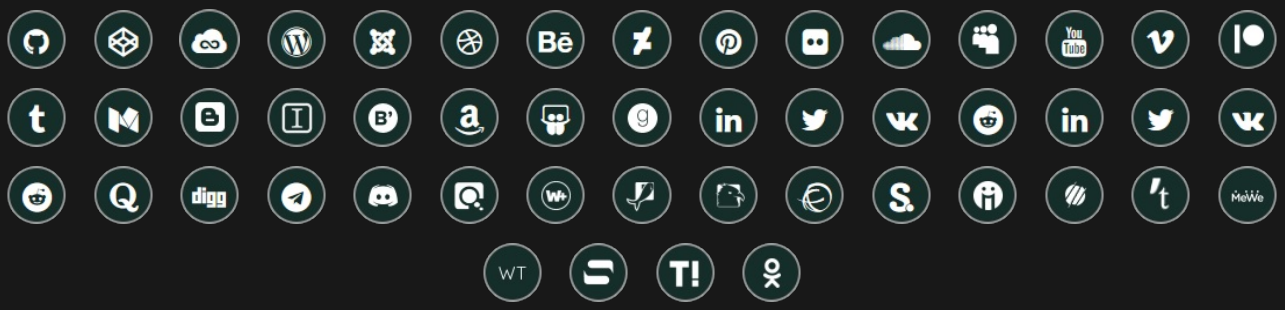
Conlusion

Default security settings on the TCP/IP server include a user ID and a clear-text password, so as soon as the server is installed, all inbound connection requests must contain a clear-text password for the user ID under which the server job will run. The security features in TCP/IP, such as network auditing and access control, are similar to those in operating systems. Despite that, several serious security flaws are inherent in the protocols, regardless of the correctness of any implementation. The threats each layer may face and how to mitigate them were described.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.



Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP | NEWSLETTER | RSS FEED