Server Security

Importance of Server Security in Layered Security Approach for Data Protection

Edited by **MOHAN DAS VISWAM**

Servers provide a variety of services to internal and external users of an organisation. They manage and store sensitive data for the organisation. Some of the most common types are web, email, database, infrastructure management, and file servers. Server security deals with the protection of apps, data, and resources stored on the servers. It comprises tools and techniques preventing intrusion, hacking and other malicious activities. These measures vary and are typically implemented in layers.

Common Security Threats

Malicious actors may exploit software bugs in the server or its underlying operating system (OS) to gain the unauthorised access to the server. With Denial of service (DoS) attacks, they target servers, to prevent valid users from using their services. In cases of weak or no encryption, they can also access to sensitive data or network resources. After compromising a server, they may replicate the tactics against other entities. These attacks can be direct (from a compromised host against an external server) or indirect (by placing malicious content on a compromised server).

C.J. Antony
Dy. Director General
& HoG
antony@nic.in

Diwan Hauym Khan
Sr. Technical Director
& HoD
dhkhan@nic.in

Rajesh K. Tripathi
Technical Director
rajesht@nic.in

With the rise of web-based apps and services, there is an increase in sophistication and number of cyber-attacks. Massive data breaches have become common and cost of these breaches have sky-rocketed. The primary targets of these attacks are servers hosting the sensitive apps and information. Cyber Security Solutions deployed on the servers have emerged as primary defence mechanisms to protect the apps and information from cyber-threats. These solutions ensure Confidentiality, Integrity and Availability of information stored in the servers.

Measures for Securing Servers

The first step in securing a server is to secure the underlying components such as OS, frameworks, web servers, and databases, which are entry points for cyber-criminals to launch attacks. Many issues can be avoided if things are configured properly. Some of the key measures for securing a server are:

- **Vulnerability Assessment (VA) and Patch Management:** VA should be done by using a state-of-the-art tool to identify vulnerabilities. Its report can be used by the application owners to plug those vulnerabilities. After installing the relevant software, apply patches or upgrades to address the vulnerabilities.
- **Hardening and Configuring the Server:** OEMs regularly release easy-to-install component configurations. When configuring a server, remove unnecessary services, apps, protocols, and non-removable components. If possible, install the minimal OS configuration and later configure it as needed. Remove / disable common services and apps if not required such as file and printer sharing services (e.g., Windows Network BIOS, Network File System, FTP), wireless network services, remote control and access programmes (e.g., Telnet), directory services (e.g., Lightweight Directory Access Protocol, Network Information System), web services, email services (e.g., SMTP), language compilers, system development tools, and network management tools (e.g., Simple Network Management Protocol (SNMP)).
- **Configure User Authentication:** The users who can access the server may range from a few authorised employees to an entire internet community. However, the number of users (admins) who can configure software components can be limited. To enforce policy restrictions, the server admin can configure the server to authenticate a

user by requiring proof of identity. Even if a server allows unauthenticated access, administrative and other specialised access should be limited to specific individuals. In special cases, such as high-value / high-risk servers, organisations may also use alternative authentication mechanisms such as biometrics, smart cards, client / server certificates, and one-time password systems. The reusable authentication mechanisms should be discouraged as they risk data interception. To ensure the appropriate user authentication is in place, take the following steps:

Remove / Disable Unnecessary Accounts: Generally, default configurations for guest accounts, admin or root level accounts, and local or network service accounts are common for each server. Since default account names and passwords are well-known, remove or disable them to prevent intrusion. Change names and passwords on retained accounts. This should be consistent with the organisation policy because they are often used to breach security.

Disable Non-Interactive Accounts: Disable accounts that do not require an interactive login. For Unix / Linux systems, disable the login shell or provide a login shell with NULL functionality.

Create User Groups and User Accounts: Assign users to the appropriate groups. Then assign rights to the groups, as per the deployment plan. This approach is preferable for assigning rights to a large number of users. The deployment plan helps to identify authorised users for each computer and service. It is advisable to only create necessary accounts and permit shared accounts if there is no viable alternative.

Configure Auto-Time Synchronisation: Some authentication protocols (e.g., Kerberos) do not function if the client and authenticating server have a significant time difference. These servers must auto-synchronise with a reliable time server that uses Network Time Protocol (NTP) for synchronisation.

- **Form Organisational Password Policy:** Check password parameters are properly addressed in the password policy, which includes password length, complexity, ageing, reuse, authority and security.

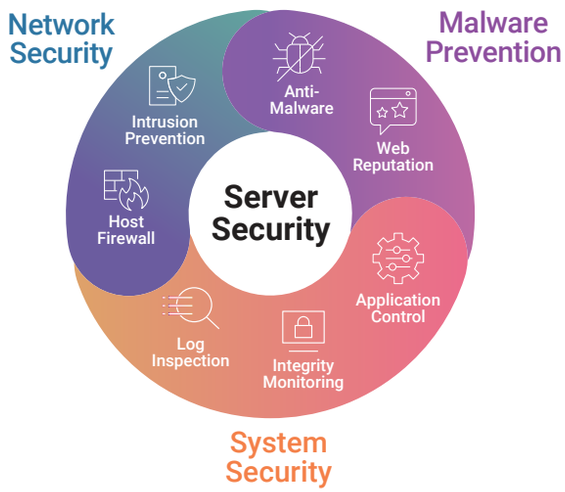
- **Configure Server Resource Controls:** Common server OSs provide the capability to specify access privileges individually for files, directories, devices, and other resources. By carefully setting access controls, the server admin can reduce server breaches. For e.g., denying read access to files and directories ensures data confidentiality, and denying unnecessary write (modify) access maintains data integrity. Furthermore, enable auditing to monitor attempts to access protected resources. In some cases, OS can be configured to provide an isolated virtual environment that a can be run within the server.

- **Configure Additional Security Controls:** OSs often do not include all the necessary security controls. In such cases, administrators need to select, install, configure, and maintain additional software to ensure the server security. There are numerous solutions available globally for this. Some of their key features are:

Anti-malware: Detects and blocks malicious software and protects servers in real time. It can be run on demand or set up to run on a fixed schedule.

Intrusion Prevention Software (IPS): Examines the traffic at the packet level and searches for protocol deviations, policy violations and other suspicious activities such as byte sequence replacement, packet drop, and connection reset that signal an attack. It can detect and block known / unknown / zero-day attacks that target vulnerabilities in server applications.

Host-based Firewall: It is a bi-directional stateful firewall that is responsible for preventing packets from unauthorised sources from reaching host applications. It provides broad coverage for



all IP-based protocols and frame types and filters IP and MAC addresses. It examines the header information in each network packet to control traffic based on direction, frame, transport protocols, source / destination addresses, ports, and header flags. It can thwart both DoS attacks and reconnaissance scans.

Web Reputation: Protects against threats by blocking malicious URLs and checks the reputation of websites by using reputation databases for potential involvement in the malware cycle. The reputation is correlated with the enforcement policy for controlling access based on the credibility score.

Virtual Patching: Intrusion Prevention Rules (IPRs) can avert attacks on unpatched applications. This prevents host from being exploited till the relevant patches are available. Once the patch is applied, IPRs can be unassigned. The process is called Virtual Patching (VP). It does not replace the regular system updates, but can be used when an application is no longer supported.

Integrity Monitoring: Provides real-time detection and reporting of malicious activities and unexpected changes on the server. It tracks both authorised and unauthorised changes made. The ability to detect unauthorised changes is critical as it can indicate the compromise.

Log Inspection: Collects and analyses software logs for suspicious behaviour, security events, and administrative events across the data centre. It optimises the identification of important security events buried in multiple log entries. Suspicious events are forwarded to a Security Information and Event Management (SIEM) system or a centralised log server for correlation, reporting, and archiving.

Application Control: This is an information security practice that restricts the execution of unauthorized applications by whitelisting and blacklisting them. It detects changes to the inventory of executable software such as software installed by users, new web pages, python scripts, unscheduled auto-updates, and zero-day malware.

- **Security Testing / Auditing**: Periodic security auditing / testing helps in identifying vulnerabilities and ensure the existing security measures are effective and properly configured (for e.g., required cryptographic algorithms are in use to protect network communications). Common methods for testing servers include vulnerability scanning (VS) and penetration testing (PT). VS usually entails using an automated vulnerability scanner to scan a host or group of hosts on a network for vulnerabilities. PT is a process designed to compromise a network using the tools and methodologies of an attacker. It involves identifying and exploiting the weakest areas of a network to gain access to the remainder of it, eventually compromising the overall security. VS should be conducted periodically, at least monthly, and PT should be conducted at least annually.

Conclusion

The proper implementation of server security measures plays a key role in the protection of applications and data on the servers and ensures effective service delivery to the citizens.

Contact for more details

Rajesh Kumar Tripathi
Network Security Division, NIC Hqrs.
CGO Complex, Lodhi Road, New Delhi - 110003
Email: rajesht@nic.in, Phone: 011-24305130