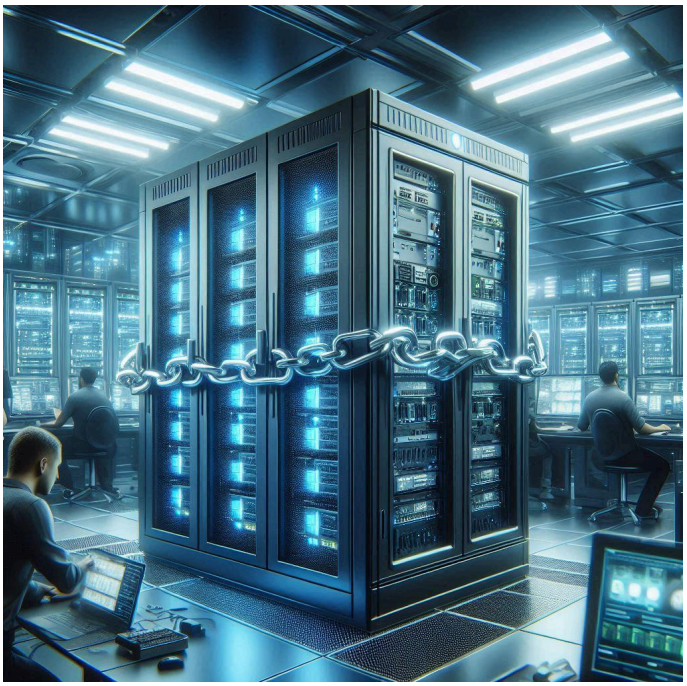

Windows Server Security

1. Keep the system updated

a. Regularly install Windows updates and security patches.
b. Use Windows Server Update Services (WSUS) for managing updates internally.

2. Limit Admin Access

a. Follow the principle of least privilege—only give admin rights to those who absolutely need it.
b. Use Role-Based Access Control (RBAC).

3. Strong Password Policies

a. Enforce complex passwords
b. Set password expiration, history, and lockout policies via Group Policy.

4. Configure Windows Firewall

a. Enable and properly configure the built-in Windows Firewall.
b. Allow only necessary inbound/outbound rules.

5. Audit and Enable Logging

a. Turn on Event Logging and configure Audit Policies.
b. Monitor logs using tools like Event Viewer or Sysmon.

6. Install Antivirus/Antimalware

a. Use Microsoft Defender for Endpoint or a reputable third-party solution. Recommended to use Defender since they have become one of the best.
b. Keep virus definitions up to date.

7. Enable BitLocker Encryption

a. Encrypt drives to protect data at rest.
b. Store recovery keys securely (e.g., in Active Directory).

8. Disable Unnecessary Services

a. Only run services that are required for your workload.
b. Disable things like Print Spooler, Telnet, and SMBv1 if not in use.

9. Use Secure Remote Access

a. Disable RDP if not required. If needed:
    i. Use Network Level Authentication (NLA).
    ii. Set up RDP Gateway.
    iii. Enable two-factor authentication (2FA).
    iv. Restrict by IP and time.

10. Regularly Review Users and Groups
    a. Check for inactive accounts, unexpected admin memberships, or strange group policy objects.
    b. Use PowerShell or AD tools for audits.

11. IPBan and IP allowed IP
    a. Use IPBand to band to find login attempts and rapidly block their IP addresses to access the system
    b. You can also use IPBan to only allow certain IP addresses to access the system for extra security.
    c. Eliminate brute force and botnet attacks.

Botnet:

Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks.

Brute force:

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.

DoS and DDoS attacks:

With a DoS attack, the target site gets flooded with illegitimate requests. Because the site has to respond to each request, its resources get consumed by all the responses. This makes it impossible for the site to serve users as it normally does and often results in a complete shutdown of the site.

MITM attacks:

Man-in-the-middle (MITM) types of cyber attacks refer to breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a “man in the middle” attack because the attacker positions themselves in the “middle” or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two parties.

Phishing attacks:

A phishing attack occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target. Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect, “fishing” for access to a forbidden area by using the “bait” of a seemingly trustworthy sender.

Ransomware:

In a ransomware attack, the target downloads ransomware, either from a website or from within an email attachment. The malware is written to exploit vulnerabilities that have not been addressed by either the system’s manufacturer or the IT team. The ransomware then encrypts the target's workstation. At times, ransomware can be used to attack multiple parties by denying access to either several computers or a central server essential to business operations.

Password attacks:

Passwords are the access verification tool of choice for most people, so figuring out a target’s password is an attractive proposition for a hacker. This can be done using a few different methods. Often, people keep copies of their passwords on pieces of paper or sticky notes around or on their desks. An attacker can either find the password themselves or pay someone on the inside to get it for them.

An attacker may also try to intercept network transmissions to grab passwords not encrypted by the network. They can also use social engineering, which convinces the target to input their password to solve a seemingly “important” problem. In other cases, the attacker can simply guess the user’s password, particularly if they use a default password or one that is easy to remember such as “1234567.”

DNS spoofing:

With Domain Name System (DNS) spoofing, a hacker alters DNS records to send traffic to a fake or “spoofed” website. Once on the fraudulent site, the victim may enter sensitive information that can be used or sold by the hacker. The hacker may also construct a poor-quality site with derogatory or inflammatory content to make a competitor company look bad.

Trojan horses:

A Trojan horse attack uses a malicious program that is hidden inside a seemingly legitimate one. When the user executes the presumably innocent program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network. This threat gets its name from the story of the Greek soldiers who hid inside a horse to infiltrate the city of Troy and win the war. Once the “gift” was accepted and brought within the gates of Troy, the Greek soldiers jumped out and attacked. In a similar way, an unsuspecting user may welcome an innocent-looking application into their system only to usher in a hidden threat.

To prevent Trojan attacks, users should be instructed not to download or install anything unless its source can be verified. Also, NGFWs can be used to examine data packets for potential threats of Trojans.