

List of Dangerous Open Ports

Port: 21

Explanation: This port is used for FTP (File Transfer Protocol).

Impact: This port sends its data over plain text, meaning that attackers can abuse this port to intercept and steal credentials.

Mitigation: Close port 21 or use SFTP instead.

- **Windows:** Go to Windows Firewall settings and block port 21.
- **Linux:** Use the command `sudo ufw deny 21` to close this port.

Port: 23

Explanation: This port is used for Telnet.

Impact: Telnet sends its data, including passwords, over plain text, making it vulnerable to eavesdropping.

Mitigation: Close port 23 and use SSH instead.

- **Windows:** Disable Telnet services and block port 23 in Windows Firewall.
- **Linux:** Use `sudo ufw deny 23` to block this port.

Port: 25

Explanation: This port is used for SMTP (Simple Mail Transfer Protocol).

Impact: Attackers can exploit this port to send spam or phishing emails if not properly secured.

Mitigation: Secure port 25 with proper authentication and spam filtering, or use alternative secure ports like 587 or 465.

- **Windows:** Configure mail server settings to require authentication.
- **Linux:** Use firewall rules to restrict access to port 25.

Port: 53

Explanation: This port is used for DNS (Domain Name System).

Impact: Open DNS ports can be exploited for DNS amplification attacks.

Mitigation: Secure port 53 by configuring DNS servers to prevent open recursion.

- **Windows:** Configure DNS services to only allow trusted networks.
- **Linux:** Use `sudo ufw allow from trusted_ips to any port 53`.

Port: 80

Explanation: This port is used for HTTP (Hypertext Transfer Protocol).

Impact: HTTP traffic is unencrypted, making it susceptible to eavesdropping and man-in-the-middle attacks.

Mitigation: Redirect HTTP traffic to HTTPS (port 443).

- **Windows:** Configure web server settings to redirect traffic from port 80 to 443.
- **Linux:** Use firewall rules to enforce HTTPS and redirect HTTP traffic.

Port: 110

Explanation: This port is used for POP3 (Post Office Protocol version 3).

Impact: POP3 can transmit email credentials in plain text, making them vulnerable to interception.

Mitigation: Use POP3S (POP3 over SSL) on port 995 instead, or prefer IMAP.

- **Windows:** Configure email clients to use POP3S or IMAP.
- **Linux:** Use `sudo ufw deny 110` to block this port.

Port: 135

Explanation: This port is used for Microsoft RPC (Remote Procedure Call).

Impact: Vulnerabilities in RPC have been exploited in various Windows attacks.

Mitigation: Block this port unless absolutely necessary for your network.

- **Windows:** Use Windows Firewall to block port 135 for external connections.
- **Linux:** Use `sudo ufw deny 135` to block this port.

Port: 139

Explanation: This port is used for NetBIOS Session Service.

Impact: Can be exploited for network enumeration and potential unauthorized access.

Mitigation: Disable NetBIOS over TCP/IP if not needed.

- **Windows:** Disable NetBIOS over TCP/IP in network adapter settings.
- **Linux:** Use `sudo ufw deny 139` to block this port.

Port: 161

Explanation: This port is used for SNMP (Simple Network Management Protocol).

Impact: SNMP can be exploited to gather information about network devices or for denial-of-service attacks.

Mitigation: Use SNMPv3 with proper authentication and encryption, or restrict access to trusted IPs.

- **Windows:** Configure SNMP service to use SNMPv3 and restrict access in Windows Firewall.
- **Linux:** Use `sudo ufw allow from trusted_ip to any port 161` to allow only trusted IPs.

Port: 389

Explanation: This port is used for LDAP (Lightweight Directory Access Protocol).

Impact: Unencrypted LDAP can expose sensitive directory information.

Mitigation: Use LDAPS (LDAP over SSL) on port 636 instead.

- **Windows:** Configure Active Directory to require LDAPS.
- **Linux:** Use `sudo ufw deny 389` and configure LDAPS on port 636.

Port: 445

Explanation: This port is used for SMB (Server Message Block).

Impact: Vulnerabilities in SMB have been exploited in major ransomware attacks.

Mitigation: Keep systems updated and block this port from external access.

- **Windows:** Use Windows Firewall to block port 445 for external connections.
- **Linux:** Use `sudo ufw deny 445` to block this port.

Port: 1433

Explanation: This port is used for Microsoft SQL Server.

Impact: Attackers can attempt to exploit vulnerabilities or weak credentials in SQL Server.

Mitigation: Restrict access to this port and use strong authentication.

- **Windows:** Configure SQL Server to use strong authentication and restrict network access.
- **Linux:** Use `sudo ufw deny 1433` to block this port if SQL Server is not needed.

Port: 1521

Explanation: This port is used for Oracle database.

Impact: Attackers can attempt to exploit vulnerabilities or weak credentials in Oracle databases.

Mitigation: Restrict access to this port and use strong authentication.

- **Windows/Linux:** Use firewall rules to allow access only from application servers or trusted IPs.

Port: 3306

Explanation: This port is used for MySQL database server.

Impact: Attackers can attempt to exploit vulnerabilities or weak credentials in MySQL.

Mitigation: Restrict access to this port and use strong authentication.

- **Windows:** Configure MySQL to bind to localhost or use Windows Firewall to restrict access.
- **Linux:** Use `sudo ufw allow from trusted_ip to any port 3306` to allow only trusted IPs.

Port: 3389

Explanation: This port is used for Remote Desktop Protocol (RDP).

Impact: Attackers can attempt brute-force attacks or exploit RDP vulnerabilities.

Mitigation: Use a VPN for remote access instead of exposing RDP directly.

- **Windows:** Use Windows Firewall to restrict RDP access to trusted IP ranges.

Port: 5900

Explanation: This port is used for VNC (Virtual Network Computing).

Impact: Unsecured VNC can allow unauthorized remote access to systems.

Mitigation: Use VPN for remote access or implement strong authentication for VNC.

- **Windows/Linux:** Configure VNC to use strong passwords and encrypt connections. Use firewall rules to restrict access.

Port: 8080

Explanation: This port is often used for web servers and proxies.

Impact: Can be exploited similarly to port 80 if not properly secured.

Mitigation: Use HTTPS, implement proper authentication, and restrict access if used for administrative interfaces.

- **Windows/Linux:** Configure web servers to use HTTPS and implement proper access controls.

Port: 27017

Explanation: This port is used for MongoDB database.

Impact: Unsecured MongoDB instances can lead to data breaches.

Mitigation: Enable authentication and encryption, bind to localhost or use firewall rules.

- **Windows/Linux:** Configure MongoDB to require authentication and encrypt connections. Use firewall rules to restrict access.

Revision #6

Created 15 September 2024 19:22:37 by Raphael

Updated 16 September 2024 09:24:41 by Raphael