CyberMax Protects

Lightning Fast ⚡ Easy ⚡ Awesome

IP Vulnerability Scan Report

Client: Example.com | Scan Date: 3/26/25

Introduction

Your network has exposed services that could put your business at risk. Cybercriminals actively scan for open ports and misconfigured systems, seeking ways to gain unauthorized access, steal data, or deploy malware.

This IP port scan has identified potential risks that should be evaluated. While this is not a complete security audit, it highlights serious risks that could lead to breaches if left unresolved.

Scan Summary

Security Risks Detected

Some services on your network are accessible from the internet, which could leave your systems vulnerable to cyberattacks. We recommend reviewing these exposed services to understand the risks and consider more secure alternatives.

Key Risks Identified

- **Web and email services** (HTTP, SMTP, DNS) can be exploited for phishing, redirection, and credential theft.

Detailed Results

Service	Port	Status	Risk Level
File Transfer Protocol (FTP)	21	✓ Closed	No Risk
Secure Shell (SSH)	22	✓ Closed	No Risk
Telnet	23	✓ Closed	No Risk
Simple Mail Transfer Protocol (SMTP)	25	✓ Closed	No Risk
Domain Name System (DNS)	53	✓ Closed	No Risk
Trivial File Transfer Protocol (TFTP)	69	✓ Closed	No Risk
HyperText Transfer Protocol (HTTP)	80	✗ Closed	Moderate
Post Office Protocol 3 (POP3)	110	✓ Closed	No Risk
NetBIOS	137	✓ Closed	No Risk
Server Message Block (SMB)	139	✓ Open	High
Internet Message Access Protocol (IMAP)	143	✓ Closed	No Risk
Simple Network Management Protocol (SNMP)	161	✓ Closed	No Risk
HyperText Transfer Protocol Secure (HTTPS)	443	✗ Closed	Moderate
Microsoft Directory Services (Microsoft-DS)	445	✓ Closed	No Risk
MySQL Database	3306	✓ Closed	No Risk
Remote Desktop Protocol (RDP)	3389	✓ Open	No Risk
Alternate HTTPS Port (HTTPS Alt)	4433	✓ Closed	No Risk
Microsoft SQL Server (MSSQL)	1433	✓ Closed	No Risk
Radmin (Remote Desktop Utility)	4899	✓ Closed	No Risk
PostgreSQL Database	5432	✓ Closed	No Risk
Virtual Network Computing (VNC)	5900	✓ Closed	No Risk
AnyDesk (Remote Desktop Utility)	7070	✓ Closed	No Risk
Alternate HTTP Port (HTTP Alt)	8080	✗ Open	Moderate

Your network exposes services to the public internet

Risk Findings

Service	Port	Status	Risk Level	Threat Overview
HyperText Transfer Protocol (HTTP)	80	✖ Open	Moderate	Unencrypted web services. Vulnerable code and business-logic flaws can potentially be exploited
HyperText Transfer Protocol Secure (HTTPS)	443	✖ Open	Moderate	Encrypted web services. Vulnerable code and business-logic flaws can potentially be exploited
Alternate HTTP Port (HTTP Proxy)	8080	✖ Open	Moderate	Web proxy services. Vulnerable code and business-logic flaws can potentially be exploited

Attention is recommended to prevent potential security incidents.

Next Steps

Your external network perimeter allows inbound connections from the public internet, which cybercriminals could exploit to gain access to sensitive systems and data. If left unaddressed, these risks may result in:

Data breaches resulting in financial loss and reputational damage.

Malware and ransomware infections through exposed remote access services.

Service disruptions caused by unauthorized access or denial-of-service attacks.

Immediate Recommended Actions

- **Close all unnecessary open ports** to block external access.
- **Enforce strong authentication** (e.g., SSH keys, multi-factor authentication) for remote services.
- **Encrypt communications** by replacing HTTP, POP3, and IMAP with secure alternatives (HTTPS, TLS-based email protocols).
- **Conduct a full security assessment** to identify and mitigate additional risks.

Your business is at risk. Don’t wait for an attack.

Our security team can help you secure your network and implement a long-term protection strategy.