AMERICAN TECHNOLOGY SERVICES

IP Vulnerability Scan Report

Client: [Name] | Scan Date: [Date]

Introduction

Cybercriminals constantly scan the internet for weaknesses—open ports, misconfigured services, and unpatched systems. While closing unnecessary ports and securing exposed services are essential steps, they are only part of a comprehensive security strategy.

This IP vulnerability scan provides a basic, external assessment of your network's exposure. However, it does not evaluate internal security, endpoint protections, phishing risks, or advanced threats. A more in-depth security approach—such as continuous monitoring, proactive threat detection, and expert-led remediation—helps prevent evolving cyber risks.

Scan Summary

No Critical Issues Detected

Your external network does not show high-risk, openly exposed services.

- **Unnecessary ports are closed.**
- **Essential services are correctly configured.**
- **No immediate external threats were detected.**

While these results are positive, attackers use far more than just open ports to gain access. Phishing attacks, credential theft, malware, and insider threats remain significant risks that this scan does not detect.

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	No Risk
Post Office Protocol 3 (POP3)	110	Closed	No Risk
NetBIOS	137	Closed	No Risk
Server Message Block (SMB)	139	Closed	No Risk
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	No Risk
Microsoft Directory Services (Microsoft-DS)	445	Closed	No Risk
MySQL Database	3306	Closed	No Risk
Remote Desktop Protocol (RDP)	3389	Closed	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	Closed	No Risk

Your network perimeter appears well-protected,
but perimeter security is only one layer of defense.

Next Steps to Strengthen Your Cybersecurity

While your external network is not showing significant vulnerabilities, cyber threats constantly evolve. A well-rounded security strategy goes beyond a single scan:

Ongoing Threat Monitoring

Attackers don't wait for scheduled scans. Advanced threats require 24/7 detection and response.

Internal Security & Access Controls

Employee accounts, internal networks, and cloud services must also be secured.

Proactive Security Measures

Penetration testing, managed detection and response (MDR), and phishing defense strengthen your overall security posture.

ATS' Managed Security Services provide continuous protection beyond basic vulnerability scanning. Work with our cybersecurity team to identify risks, prevent attacks, and implement proactive defenses.

Schedule a Security Consultation Today

info@networkats.com