SOVOS

Analyzing Network Connections

Windows and Linux Server Environments

Sovos.com

Overview

This report outlines methodologies for analyzing network connections across various Windows desktop, Windows Server, and Linux operating systems. It emphasizes SSL/TLS protocol and cipher identification and includes instructions for using third-party tools where built-in options are limited. It focuses on using Telnet, Test-NetConnection (Tnc), Curl, and OpenSSL for network testing and SSL/TLS protocol and cipher analysis.

Windows Systems

Windows XP and Windows Server 2003

Network Testing

- Basic connectivity: `ping [endpoint address]` and `tracert [endpoint address]`.
- **Telnet:** Pre-installed. Use `telnet [endpoint address] [port]` for TCP connection testing.
- **Curl:** If installed, `curl -Iv https://[endpoint address]`. Download from https://curl.se/download.html. The `-Iv` flag increases verbosity, showing the header information and the SSL handshake process, including cipher negotiation.

SSL/TLS Analysis

- **OpenSSL:** Download from https://www.openssl.org/source/. Use `openssl s_client -connect [endpoint address]:443`. This command initiates an SSL/TLS connection to the specified endpoint, revealing details about the handshake process, including the default cipher suite used.

Windows Vista and Windows Server 2008

Network Testing

- Basic connectivity: `ping [endpoint address]` and `tracert [endpoint address]`
- **Telnet:** May need enabling via Windows Features.
- **Curl:** After installation, `curl -Iv https://[endpoint address]`. Download from https://curl.se/download.html. The `-Iv` flag increases verbosity, showing the header information and the SSL handshake process, including cipher negotiation.

SSL/TLS Analysis

- OpenSSL: As described for XP/Server 2003.

Windows 7 and Windows Server 2008 R2

Network Testing

- **Ping and Tracert:** Standard tools for initial testing.
- **Telnet:** Enable via Windows Features.
- **Curl:** After installation, `curl -Iv https://[endpoint address]`. Download from https://curl.se/download.html. The `-Iv` flag increases verbosity, showing the header information and the SSL handshake process, including cipher negotiation.

SSL/TLS Analysis

- OpenSSL: As earlier versions.

Windows 8 and Windows Server 2012

Network Testing

- Standard analysis: `ping` and `tracert`.
- **Telnet:** Enable if necessary.
- **Tnc:** Use `Test-NetConnection -ComputerName [endpoint address] -Port [port]`.
- **Curl:** Install and use `curl -Iv https://[endpoint address]`. Download from https://curl.se/download.html. The `-Iv` flag increases verbosity, showing the header information and the SSL handshake process, including cipher negotiation.

SSL/TLS Analysis

- OpenSSL: Install and use as before.

Windows 10 and Windows Server 2016/2019/2022

Network Testing

- **Ping and Tracert:** For basic connectivity tests.
- **Telnet:** Can be enabled if needed.
- **Tnc:** Available in PowerShell.
- **Curl:** Pre-installed. Use `curl -Iv https://[endpoint address]`. Download from https://curl.se/download.html. The `-Iv` flag increases verbosity, showing the header information and the SSL handshake process, including cipher negotiation.

SSL/TLS Analysis

- OpenSSL: Follow the download and installation instructions.

Linux Systems

General Network Testing Tools

Ping and Traceroute

- **Function**: Basic connectivity and route tracing.
- **Commands**:
  - `ping [endpoint address]`: Tests the basic connectivity to your endpoint.
  - `traceroute [endpoint address]`: Traces the path packets take to the endpoint.

Netcat (nc)

- **Function**: Versatile tool for anything related to TCP, UDP, or UNIX-domain sockets.
- **Command**: `nc -vz [endpoint address] [port]`: Tests connectivity to a specific port.

Telnet

- **Function**: Simple TCP connection testing tool.
- **Command**: `telnet [endpoint address] [port]`: Used to test TCP connections to a port.

Curl

- **Function**: Data transfer tool supporting various protocols, useful for testing HTTP, HTTPS, FTP, etc.
- **Command**: `curl -Iv https://[endpoint address]`: Displays detailed information about the connection, including SSL/TLS protocols and ciphers.

SSL/TLS Analysis Tools

OpenSSL

- **Function**: Powerful tool to inspect SSL/TLS connections.

- **Command**: `openssl s_client -connect [endpoint address]:443`: Connects to an SSL/TLS server and provides detailed handshake information, including cipher suite.

Nmap

- **Function**: Network exploration tool and security scanner.
- **Command**: `nmap --script ssl-cert,ssl-enum-ciphers -p 443 [endpoint address]`: Scans for SSL/TLS certificates and supported cipher suites on a given port.

Additional Considerations

- **Tool Availability**: Most of these tools are pre-installed on Linux systems. If not, they can be easily installed via the package manager (e.g., `apt-get install nmap` on Debian/Ubuntu).
- **Permissions**: Some commands may require elevated privileges (using `sudo`).
- **Customization**: Commands can be customized according to specific needs or network configurations.

Notes

- **Adaptability**: Linux environments vary widely; commands may need adjustment depending on the specific distribution and its version.
- **Documentation**: It's advisable to consult the man pages (`man [command]`) for detailed usage information on each tool.