PQC Network Scanner – User Guide

The **PQC Network Scanner** is a purpose-built assessment tool designed to help organisations understand their cryptographic exposure as they transition toward a post-quantum security posture. Unlike traditional TLS scanners that focus solely on certificate validity or classical cryptographic strength, this scanner evaluates endpoints through a quantum-aware lens. It inspects not only RSA and elliptic-curve keys but also identifies emerging post-quantum algorithms, hybrid deployments and experimental PQC indicators embedded within certificates, extensions and cipher suites. This makes it uniquely suited for environments preparing for the cryptographic shift driven by NIST's PQC standardisation and the growing threat of "harvest now, decrypt later" adversaries.

At its core, the scanner performs deep inspection of TLS endpoints across an internal network. It retrieves and analyses full certificate chains, evaluates key types and sizes, detects PQC-related OIDs, and identifies hybrid key-exchange mechanisms such as X25519+Kyber. The tool also examines TLS protocol versions and cipher suites to determine whether endpoints support Perfect Forward Secrecy (PFS) or rely on legacy, quantum-vulnerable configurations. By combining these the scanner provides a comprehensive view of both classical and quantum-era cryptographic resilience.

Beyond cryptography, the scanner incorporates intelligent device identification. It correlates certificate metadata, DNS information and naming conventions to classify endpoints such as routers, firewalls, VPN gateways, web servers and application hosts. This contextual awareness helps security teams understand not just what cryptography is deployed, but where it resides within the network. An essential capability for building a crypto inventory and prioritising remediation.

The output report contains technical detail with clear, actionable commentary. Each endpoint is assessed for quantum vulnerability, PQC readiness, TLS posture, and certificate chain integrity. The report highlights high-risk configurations, identifies PQC-enabled or hybrid deployments and provides migration guidance aligned with emerging standards such as ML-DSA and ML-KEM. Summary sections consolidate findings across the scanned environment, offering a high-level view of organisational readiness and exposure.

In practice, the PQC Network Scanner serves as both a diagnostic instrument and a strategic planning tool. It enables organisations to map their cryptographic landscape, detect weak or outdated configurations, and identify early adopters of PQC technologies. By bridging classical TLS analysis with post-quantum detection, it supports crypto-agility initiatives and helps teams prepare for the inevitable transition to quantum-safe cryptography.

It can be run as either a standalone Windows executable or as Python script both versions are available on GitHub at: https://github.com/cyberjez/PQC-Scanner

Overview

The **PQC Network Scanner** is a desktop application designed to evaluate TLS-enabled endpoints across an internal network for:

- Classical cryptographic strength (RSA/ECC)
- Quantum vulnerability (Shor-susceptible algorithms)
- Post-Quantum Cryptography (PQC) readiness
- Hybrid deployments (e.g., X25519+Kyber)
- TLS protocol and cipher suite security
- -Certificate chain composition
- -Device identification (routers, firewalls, servers, etc.)

The scanner produces a consolidated, examiner-friendly report summarizing cryptographic posture, quantum exposure, and transition readiness. There are two versions an executable version which runs in Windows and a Python version.

System Requirements (Python Version)

Operating System: Windows, macOS, or Linux
Python Version: 3.9 or later

Required Libraries:

- cryptography
- tkinter
- ipaddress
- ssl
- concurrent.futures
- OpenSSL (for enhanced chain retrieval)

Launching the Application

- Open a terminal or command prompt.
- Navigate to the directory containing the script.
- Run: *python PQC_Network_Scannerv2.py*

The graphical interface will open automatically.

Network Scan Configuration

P Range Field

Accepts:

- CIDR notation (e.g., `192.168.1.0/24`)
- IP range (e.g., `10.0.0.1-10.0.0.50`)
- Single IP (e.g., `172.16.0.10`)

Ports Field

Accepts:

- Comma-separated list (e.g., `443,8443`)
- Range (e.g., `443-445`)
- Mixed formats

Options

- Only scan open ports (faster)
- Performs a quick TCP check before attempting TLS.

Progress Bar

Shows real-time scan progress.

Running a Scan

Click: *Start Network Scan*

The scanner will:

1. Parse IP and port ranges
2. Validate input
3. Launch parallel scanning threads
4. Retrieve TLS certificates
5. Analyze:
   - Certificate chain
   - Key type and size
   - PQC OIDs
   - Hybrid KEM indicators
   - TLS version and cipher suite
   - Device type
6. Generate a structured report

Cancel Scan

Stops all remaining tasks and displays partial results.

Clear Results

Resets the output window and progress bar.

Save Report
Exports the full report as a `.txt` file.

Understanding the Results

Each scanned endpoint includes detailed cryptographic posture.

Target Header
Example: 192.168.1.10:443 (webserver.local) [Web Server]
Includes:

- IP and port
- Resolved hostname
- Device classification

Certificate Details

- Key family (RSA, EC, PQC)
- Key size
- Quantum risk
- Severity rating
- Commentary

PQC Readiness
If PQC or hybrid features are detected:
PQC Ready : YES
PQC Details : Hybrid KEX in cipher: TLS_AES_256_GCM_SHA384; PQC signature: ML-DSA-65

Certificate Chain Analysis
Shows:

- Chain length
- Leaf / Intermediate / Root roles
- Key types per certificate
- PQC indicators
- Mixed-algorithm chains

TLS Protocol & Cipher Suite
Evaluates:

- TLS version
- PFS support
- RSA key exchange
- Deprecated protocols

Summary Section
The final section includes:

- Total targets assessed
- High/Medium/Low/Informational findings
- PQC-ready endpoints
- Errors/unreachable hosts
- Quantum risk summary
- PQC transition recommendations

Best Practices

- Run scans during maintenance windows
- Use smaller IP ranges for faster results
- Enable OpenSSL fallback for full chain retrieval
- Save reports for historical comparison
- Integrate results into your crypto inventory program

Troubleshooting

No certificates retrieved

- Port may not support TLS
- Device may require SNI
- Try specifying a hostname

Timeouts

- Increase timeout in code for high-latency networks

GUI freezes

- Avoid scanning extremely large subnets in one run