30 Point Checklist for Network Security

Offering a network assessment is a strong way to get your foot in the door. **Network Detective Pro** makes auditing network security a snap! Use this simple checklist to help document misconfigurations and vulnerabilities when you are offering IT assessments to prospects.

- Missing critical patches
- Missing or out-of-date antivirus and anti-spyware
- On-prem synch failures
- Computers with open listening ports
- Unsupported operating systems in use
- Enabled logins for former employees/vendors
- Weak/insufficient password requirements
- Systems with weak local passwords
- Multi-factor authentication not enabled
- Non-administrators with Admin or Domain Admin privileges
- Improper network share permissions
- Credit card/PII stored on unauthorized systems
- Excessive inactive SharePoint sites
- Firewall has open ports with known exploitable issues
- Lack of outbound (egress) filtering by the firewall
- Lack of content filtering
- Systems inside the network with exploitable ports/protocols
- Application vulnerabilities
- TLS Deprecation
- Auto screen lock disabled
- Account lock out disabled
- Incorrect and/or inconsistent application of security settings
- Confirm domain policies and local security policies match best practices
- Confirm recommended Microsoft security controls implemented
- Large number of failed logins
- Anomalous user logins
- Untested or missing backup/business continuity
- Improper physical security for server room
- Physical threats in server room
- Rogue or unauthorized devices and computers

Network Detective Pro is a powerful IT assessment tool that non-intrusively scans networks and individual computers, analyzes the results, and generates a wide range of professionally designed reports. Learn more at **www.rapidfiretools.com**.

RapidFireTools®
A Kaseya COMPANY