

Network Discovery

Documentation, Threat Assessment, and Vulnerability Scanning

What if your existing network is running smoothly, but lacks accurate documentation? Are you confident that your systems are secure and protected from unauthorized access? Our specialists can audit your infrastructure, generate thorough reports, and ensure that your servers are up-to-date on all available security patches and that your network is hardened against vulnerabilities.

1. Standard Discovery –10 Hours , Enhanced (Sell as a bundle)

- Single Site Survey
 - Standard Discovery of network components. (Switches, Routers, Firewalls)
 - ✍ Location of the Device
 - ✍ MAC Address
 - ✍ IP address Usage and Subnet Discovery
 - ✍ Switch Port Assignments
- Network Diagram of Discovered Components
- Basic Security Audit
 - ✍ Passive scan of services running on devices discovered.
 - ✍ External Scan of network for available services
 - ✍ Basic Reports on findings.
- Assessment of overall Network Performance, Network Component Load, and Overall Stability.

2. Enhanced Discovery – Minimum of 20 Hours , Enhanced

- Includes Standard Discovery plus the following
- Addition of Multiple Sites or Offices
(all sites must be reachable via network from one location, travel is not included)
- Enhanced Discovery of Network Components
 - ? Software Versions
 - ? Additional Devices
 - Power Distribution Units
 - Storage Devices
 - Wireless Access Points
 - IP Camera and Security Devices
 - Etc.
- Multi Layered Network Maps
 - ✍ L2, L3, Hierarchal
- Advanced Security Audit
 - ✍ Vulnerability Assessment at the host level. (host credentials required)
 - ✍ Validate AV Running and Current.
 - ✍ Auditing of Network Device Configurations and Firewalls
 - ✍ CIS, NIST, and SANS Top 20 Audits.
 - ✍ Advanced PDF and HTML based reports for all findings.
 - ✍ Analysis of findings