SECPOINT®

www.secpoint.com

SecPoint® Penetrator™ Methodology

NCC-DK
DENMARK CYBERSECURITY COORDINATION CENTRE

CYBERSECURITY™
MADE IN EUROPE

Initiated by ECSO. Issued by CenSec

CenSec
CENTER FOR DEFENCE, SPACE & SECURITY

Defense Network North

INTERFORCE

SECPOINT® PENETRATOR METHODOLOGY

VULNERABILITY SCANNING & ASSESSMENT METHODOLOGY EXPLAINED:

The Penetrator vulnerability scanning software is engineered to offer superior, intelligent, and highly effective scanning capabilities, as outlined in the methodology presented in this document.

Employing the same strategies and techniques that real attackers, hackers, and black hat professionals utilize to breach target systems.

The vulnerability scanning software engine doesn't solely rely on a black hat attacker's approach. It's also optimized for government and corporate settings, ensuring the most effective scanning process for our customers.

By leveraging feedback and requirements from thousands of users across over 100 countries, the Penetrator software delivers superior results compared to conventional scanning solutions.

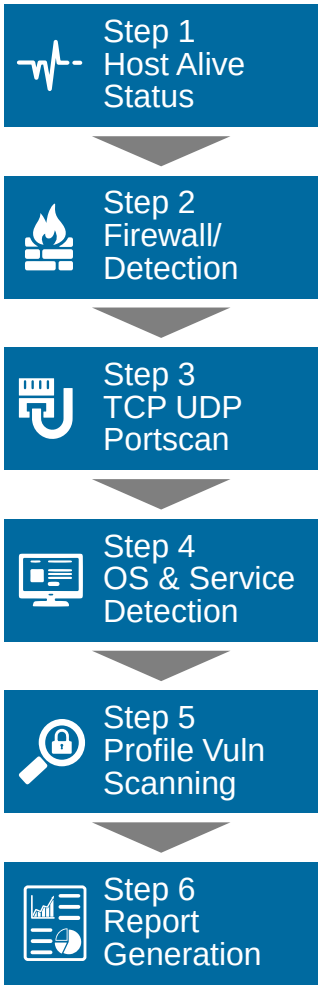
The Penetrator Vulnerability Scanner & Assessment product employs a methodology that mirrors the approach a real attacker would use to target a system.

It employs advanced techniques for information discovery, mirroring the methods of an attacker. The Penetrator Scanning engine is regularly updated with the latest advanced scanning modules ensuring optimal performance.

Enhanced with a smart scanning backbone, the system is designed to optimize overall performance, data traffic, scan speed, and result accuracy

Leveraging identified services for expedited results.

The scanning engine's modules are capable of using threads to achieve faster yet precise scan results. This enhances overall performance, especially when scanning extensive network segments.



SECPOINT® PENETRATOR METHODOLOGY (CONT'D)

VULNERABILITY SCANNING METHODOLOGY STEP BY STEP

Step 1
Host Alive Status

Determining the status of the target system and gathering information is essential. The Penetrator uses optimized scanning methods to ascertain whether the target IP address should be scanned. It employs a variety of techniques not only to identify active systems but also to detect those behind firewalls or those that might be challenging to recognize otherwise.

One such method involves probing for open TCP and UDP ports. Commonly checked TCP ports include, but are not limited to, 1-111, 135, 139, 443, 445, and others. For UDP, this includes ports 53, 111, 135, 137, 161, and 500. Users can also customize the scanning profile to include additional ports. Moreover, a scan can be initiated even if the target seems to be offline or unresponsive.

Step 2
Firewall/Detection

Determine whether the target system is protected by a firewall, IDS, or IPS. Some systems might seem offline, but in reality, they could merely be shielded by a firewall, leaving them potentially vulnerable to attacks. The Firewall Detection module employs various techniques to identify devices with firewall, filtering, or IPS protections. This test will also collect additional network information from the infrastructure during TCP and UDP port probing.

Step 3
TCP UDP Portscan

TCP and UDP port scanning are used to identify open ports and services. Depending on the selected profile, the scan can target the most common 2,000 ports or even more. In the full profiles, all 65,535 TCP and UDP ports will be probed and scanned. For most configurations, using the optimal scan profile is recommended to conserve time and network bandwidth. However, for a more comprehensive analysis, the full scan profiles are advised.

SECPOINT® PENETRATOR METHODOLOGY (CONT'D)

VULNERABILITY SCANNING METHODOLOGY STEP BY STEP

Step 4
OS & Service Detection

Service, OS, and Version Detection: After completing TCP and UDP port scans, the Penetrator employs various techniques to identify the operating system on the target host and optimize its performance.

Step 5
Profile Vulnerability Scanning

Based on the choice more than 34 scanning profiles, the appropriate profile is applied to optimize vulnerability scanning results. Depending on the selected profile, scanning modules, exploits, or Denial of Service (DoS) attacks are launched.

- Best Scan – Popular Ports
- CMS Web Scan – Joomla, Wordpress, Drupal, General CM
- Quick Scan – Most Common Ports
- Best Scan – 65.535 Ports
- Firewall Scan – Stealth Scan
- Aggressive Scan – Full Scan, Exploits & DoS Attacks
- OWASP Top 10 Scan – OWASP Checks
- PCI-DSS Preparation for Web Applications
- HIPAA Policy Scan for Compliance
- SCADA ICS PLC

Step 6
Report Generation

Reporting Generation in different formats and outputs risk analysis and remediation suggestion.

- Popular categories to scan for includes and not limited to:
- Recommended ports. Scans the most common ports
- Performs Vulnerability checks ,Web application vulnerability scanner WAS
- Automatic Service Identification, SQL Injection, XSS Cross Site Scripting, Command Execution
- Web Crawler, Google Hack DB, Joomla Security Scan, Google Safe Browsing, 50+ Blacklist Checks
- Wordpress Security Scan, Firewall, DNS, FTP, Web, SSL, SSH, SQL, Netbios and much more.
- Scans Windows, Mac OS X, Linux, Nix and other operating systems.
- Duration can be several hours depending on how many services are found during the scan.
- It is designed to be non harmful and not flood the services by simulating the human behaviour.