SECPOINT®

SecPoint® Penetrator Methodology

SECPOINT® PENETRATOR METHODOLOGY

VULNERABILITY SCANNING & ASSESSMENT METHODOLOGY EXPLAINED:

The Penetrator vulnerability scanning software engine is designed to have the best, most intelligent & most effective scanning capability based on the presented scanning methodology in this document.

Using the same approach, techniques while scanning as real attackers/hackers & black hat hackers would deploy to compromise a target system or systems.

The vulnerability scanning software engine don't just rely on attacker's black hat approach it is also optimized for government & corporate environments to give the customer the most optimal scanning process.

Utilizing scanning feedback & requirements from thousands of customers across more than 100 countries allows the penetrator software to get a better result than traditional scanning solutions.

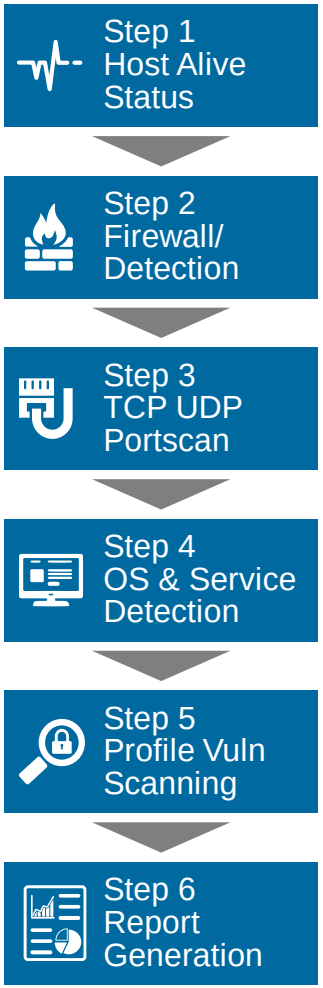
The Penetratror Vulnerability Scanner & Assessment product methodology is build up in the same way as a real attacker would target a system.

It uses advanced techniques for information discovery juts like an attacker would do it. The Penetrator Scanning engine is updated with the latest advanced scanning modules to comply with the scanning tasks.

Optimized with an intelligent scanning backbone structure to maximize overall performance, data traffic, scan speed & scan results.

Taking advantage of detected services for faster results.

The scanning engine modules can utilize threads for faster but accurate scans results. This can increase overall performance when scanning large network segments.



SECPOINT® PENETRATOR METHODOLOGY (CONT'D)

VULNERABILITY SCANNING METHODOLOGY STEP BY STEP

Step 1
Host Alive Status

Checking if the target system is alive & information gathering.

To consume data, use the most optimized scanning the Penetrator will determine if the target IP address must be scanned. It uses different techniques for this to also detect firewalled systems or otherwise hard to detect a pulse from.

One technique is to probe for open TCP & UDP ports.

Popular ports includes but not limited to TCP Ports 1-111,135,139,443,445 & more. For UDP 53,111,135,137,161 & 500. It is also possible to customize the profile to add other ports. A scan can also be forced even if the target appear to be offline or not alive.

Step 2
Firewall/Detection

Determine if the target system is behind a firewall, IDS or IPS system.

Some systems appear to be offline where in reality they are just firewalled off & can still be wide open to attack.

In the Firewall detection module it can use different techniques to detect firewalling/filtering/IPSed devices.

The test will also gather more network information from the infrastructure when doing TCP & UDP port probing.

Step 3
TCP UDP Portscan

TCP & UDP port scanning to determine open ports & services. Depending on the chosen profile there can be scanned the most common 2000 ports or more.

In the full profiles all 65.535 TCP & UDP ports will be probed & scanned. In most setups using the best scan profile can be recommended to save time & network bandwidth. For more in-depth analysis the full scan profiles are recommended.

SECPOINT® PENETRATOR METHODOLOGY (CONT'D)

VULNERABILITY SCANNING METHODOLOGY STEP BY STEP

Step 4
OS & Service Detection

Services, OS & services version detection. Operating system detection & optimizing.

Once the TCP & UDP port scanning has completed, the Penetrator will use different techniques to identify operating system running on the target host.

Step 5
Profile Vulnerability Scanning

Based on selection of one of the nine scanning profiles selected. Right profile is applied for optimized Vulnerability Scanning results. Launch scanning modules, exploits or Denial of Service (DoS) depending on which of 9 profile selected.

- 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 8000 among the most common ports
- Performs 55.000+ 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.