PhoneSweep®

The industry's best analog phone audit tool

DATASHEET

Features & Benefits

- *Powerful, reliable and accurate tool to perform security audits of phone systems*
- *Aids in the detection and facilitates the removal of unauthorized (rogue) modems*
- *Scans the telephone network to identify and classify modems, fax machines, and other answering devices*
- *Identifies over 470 types of systems with modem connections*
- *Unobtrusive scanning to minimize organizational disruptions*
- *Reduces security audit time by using the Single Call Detect feature*
- *Brute force user name and password guessing to detect security holes*
- *Flexible and configurable reporting that highlights problems and vulnerabilities*

Challenge

Everyone concerned with IT security is aware of the range of threats that the Internet presents. Most are also aware of how poorly managed USB devices or optical media can create a "backdoor" that bypasses firewalls and proxies, in order to gain access to the heart of your critical service, data and infrastructure. Mismanaged or unauthorized modems can be an equally effective backdoor target for attackers, but they rarely attract the same level of attention. Best practices dictate that modem management should be an integral part of every organization's security policy, and that they should be audited just like other areas covered by the policy. Identification and control of these "rogue" modems is a crucial part of executing a successful security strategy.

Solution

NIKSUN's PhoneSweep is a security audit tool that searches for modems, fax machines, and other devices within a set of phone numbers. It "sweeps" the telephone network to detect security risks such as unsecured modems and potential vulnerabilities to toll fraud. One or more modems are used to place calls to a set of phone numbers ("profile"). If a modem or fax answers, information about the answering device is collected, recorded and classified. Advanced features such as system identification, brute force user name and password guessing, continuous scanning, and customizable reporting can be used for follow up, device management, and creating an audit trail.

System Identification

As each call is completed, PhoneSweep identifies the lines as Carrier (modem), Voice (a person or answering machine), Fax, Penetrated, Tone, Busy, Ring Timeout or other results. Depending on the mission, the scan can be performed at an appropriate "level of effort" which varies from passive, unobtrusive listening and classification into different categories of devices, to active penetration testing of the identified device.

Scanning speed can be increased by using the Single Call Detect feature, which evaluates the result of each call as it is being made and modifies its behavior to avoid making extra calls to complete the identification.

Unobtrusive Scanning

Dialing rules are customizable on a per-profile, per-number basis to avoid inconvenience or business disruption. For example, PhoneSweep can be instructed to not make any calls during a specified interval or to stop retrying numbers after a specified number of calls. PhoneSweep allows users to control when phone numbers are dialed by specifying time periods when numbers or ranges of numbers are to be called and blackout hours, intervals when PhoneSweep should not make any calls.

Continuous Scanning

Continuous scanning can be used to monitor a set of phone numbers to determine when their status has changed, like when a system or phone line has gone down or is otherwise unavailable. It can also be used for sweeping sets of phone numbers on a regular basis.

A set of phone numbers is scanned repeatedly at a configurable interval. For each scan the profile is copied and the new profile is swept, and the results compared with the base case. Full and differential reports can be generated and emailed to the user. These can done on an always, never or conditional basis, depending on whether differences are found.

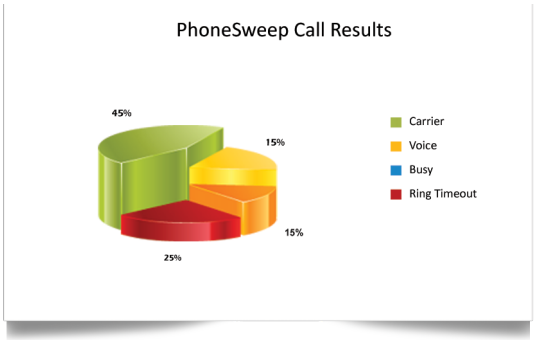
Flexible Reporting

PhoneSweep compiles call results and organizes them into an easily readable format that highlights problems and vulnerabilities. Two basic types of reports are generated: Basic Reports list what happened in a single profile; and Differential Reports compare two profiles and indicate all the differences detected.

The Anomaly Detection feature can be used to list anomalies or inconsistent features found during checks on remote modems. These often indicate an unauthorized or misconfigured modem.

Brute Force User Name and Password Guessing

PhoneSweep can perform brute force user name and password guessing attacks on discovered modems. Various system configuration files are used to specify the user name and password combinations used. These combinations can be either recycled, where they are used once during every scan, or not recycled, where they are used only once during a scan on the assumption that all modems share the same user name and password database.



Technical Information

Models	Minimum System Requirements:
PhoneSweep Basic - 1 modem	» CPU: 200MHz (PC or Laptop) Intel Celeron/PII
	» RAM: 32MB
	» Disk Space: 50MB (with small profiles)
PhoneSweep Plus 4 or 8	» CPU: 333MHz (PC or Laptop) Intel Celeron/PII or Pentium III
	» RAM: 64MB
	» Disk Space: 100MB (with large profiles)
PhoneSweep Plus 12 or 16	» CPU: 600 - 700MHz (PC or Laptop) Pentium III or equivalent
	» RAM: 128M
Operating System Requirements	» Windows 7 / 2000 Pro SP2 / 2000 Server SP1 / XP / 2003 Server / Vista

457 North Harrison Street Princeton, NJ 08540
t: +1.609.936.9999 toll free: +1.888.504.3336
f: +1.609.419.4260 info@niksun.com

About NIKSUN, Inc. NIKSUN is the recognized worldwide leader in making the Unknown Known. The company develops a highly scalable array of real time and forensics-based cyber security and performance management solutions for large enterprises, government & intelligence agencies, service providers and financial services companies. NIKSUN's award winning enterprise solutions deliver unprecedented flexibility and packet capture power. The company's patented real-time analysis and recording technology is the industry's most comprehensive solution for secure and reliable network infrastructure and services. NIKSUN, headquartered in Princeton, New Jersey, has sales offices and distributors throughout the US, Europe, the Mid East and Asia-Pacific. For more information, please visit www.niksun.com.