

<b>FAQ</b>	
Question	Answer
<b>What are some of the tools you use?</b>	We use a variety of professional tools to scan your network and detect potential vulnerabilities. They range from open source tools like Nmap, to commercial scanners like GFI LanGuard, Nessus and Solarwinds. We also use a variety of proprietary tools developed by Spohn Consulting to provide you with a more comprehensive vulnerability assessment.

<b>Sample List of Tools</b>	
<b>GFI LanGuard:</b>	GFI LANguard Network Security Scanner (N.S.S.) checks your network for possible security vulnerabilities by scanning your entire network for missing security patches, service packs, open shares, open ports, unused user accounts and more.
<b>Nessus:</b>	Nessus is a proprietary network vulnerability scanner available. It is constantly updated, and includes more than 14,000 plugins.
<b>MBSA:</b>	Microsoft Baseline Security Analyzer: an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance.
<b>Nmap:</b>	"Network Mapper") is a free open source utility for network exploration or security auditing.
<b>SolarWinds:</b>	Suite of security-related tools which includes many network discovery scanners, an SNMP brute-force cracker, router password decryption, a TCP connection reset program, and more.
<b>L0pht Crack:</b>	An award-winning password audit and recovery tool for Windows and Unix passwords.
<b>Lan Surveyor:</b>	Automatically Diagram Your Entire LAN or WAN, Document All Your Networked Devices, Monitor Up/Down Status of Your Key Systems and Applications.
<b>Paros Web Proxy:</b>	A Java based web proxy for assessing web application vulnerability. It supports editing/viewing HTTP/HTTPS messages on-the-fly to change items such as cookies and form fields. It includes a web traffic recorder, web spider, hash calculator, and a scanner for testing common web application attacks such as SQL injection and cross-site scripting.
<b>Wireshark:</b>	Wireshark (known as Ethereal until a trademark dispute in Summer 2006) is an open source network protocol analyzer for Unix and Windows.
<b>Metasploit:</b>	is an advanced open-source platform for developing, testing, and using exploit code.

### **Sample List of Tools**

**Cain & Abel:** This Windows-only password recovery tool handles an enormous variety of tasks. It can recover passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

**Netstumbler:** Netstumbler is the best known Windows tool for finding open wireless access points ("wardriving").

**Spohn Security Manager:** The Spohn NetAudit Integrated Security Manager is proprietary program we designed from the ground up in order to put it all together. Security Manager allows us to combine the results from Nessus, GFI, MBSA, and more, into one Access Database that we will use to put together a comprehensive assessment of your security posture. The same database is included on the CD-Rom so you can see what we see, and even run your own queries.

**NessusWX:** Open source windows version of the Nessus Client

**Google:** While it is far more than a security tool, Google's massive database is a good mind for security researchers and penetration testers. You can use it to dig up information about a target company by using directives such as "site:target-domain.com" and find employee names, sensitive information that they wrongly thought was hidden, vulnerable software installations, and more.

**Fingergoogle:** Command line program to enumerate Google's enormous database for user names.

**Ike-scan:** ke-scan exploits transport characteristics in the Internet Key Exchange (IKE) service, the mechanism used by VPNs to establish a connection between a server and a remote client.

**Ettercap-NG:** Ettercap is a terminal-based network sniffer/interceptor/logger for ethernet LANs. It supports active and passive dissection of many protocols (even ciphered ones, like ssh and https). Data injection in an established connection and filtering on the fly is also possible, keeping the connection synchronized. It has the ability to check whether you are in a switched LAN or not, and to use OS fingerprints (active or passive) to let you know the geometry of the LAN.

**SamSpade:** Sam Spade provides a consistent GUI and implementation for many handy network query tasks. It was designed with tracking down spammers in mind, but can be useful for many other network exploration, administration, and security tasks. It includes tools such as ping, nslookup, whois, dig, traceroute, finger, raw HTTP web browser, DNS zone transfer, SMTP relay check, website search, and more.

**SuperScan4:** SuperScan is a free Windows-only closed-source TCP/UDP port scanner by Foundstone. It includes a variety of additional networking tools such as ping, traceroute, http head, and whois.

**True Crypt:** TrueCrypt is an excellent open source disk encryption system.

**Netcat:** This simple utility reads and writes data across TCP or UDP network connections. It is designed to be a reliable back-end tool that can be used directly or easily driven by other programs and scripts.

### **Sample List of Tools**

**Hping2:** This handy little utility assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It was inspired by the ping command, but offers far more control over the probes sent.

**Dig:** dig (domain information proper) is a flexible tool for interrogating DNS name servers.

**Nikto:** Nikto is an open source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers.

**Wikto:** Windows version of Nikto with some added features.

**Httpprint:** httpprint is a web server fingerprinting tool.

**Httrack:** allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure.

**Wget:** GNU Wget is a free utility for non-interactive download of files from the Web. It supports HTTP, HTTPS, and FTP protocols, as well as retrieval through HTTP proxies.

**Nemesis:** The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux, and Windows.

**Tcpdump:** Tcpdump is the IP sniffer we all used before Ethereal (Wireshark) came on the scene. It may not have the bells and whistles that Wireshark has, but it does the job well and with fewer security holes. It also requires fewer system resources.

**Packetyzer:** Packetyzer provides a Windows user interface for the well known Ethereal packet capture and dissection library.

**Psk-crack:** psk-crack attempts to crack IKE Aggressive Mode pre-shared keys that have been previously gathered using ike-scan with the --pskcrack option.

**Hydra:** It can perform rapid dictionary attacks against more than 30 protocols, including telnet, ftp, http, https, smb, several databases, and much more.

**For more information about Spohn Consulting services, please contact us at 512-685-1000.**