Network Risk Assessment

An external network assessment is the first phase of identifying potential network security vulnerabilities that exist on your systems visible to the general public from the Internet. An internal assessment uses similar methodology, but is conducted from the point of view of a person who has access to the internal network. Using a variety of freeware/commercial tools and techniques to evaluate your Intranet will give you a clear picture of the dangers you face. Your network assessment testing methodology should include (at a minimum):

Analyzing the external network topology for improper firewall configuration
Router filtering rules and configuration
Weak authentication mechanisms (“dictionary”-based authentication attack)
Improperly configured or vulnerable mail and Domain Name Service (DNS) servers
Network layer Web server exploits
Improperly configured database servers
SNMP checks
Vulnerable File Transfer Protocol (FTP) servers

You should place special emphasis on systems that deliver content or services to the public Internet. In my experience, services that provide information through common delivery mechanisms are at a greater security risk of being targeted by potential intruders and automated malicious software. These include attacks such as computer worms because of increased accessibility and exposure. Network services in this category include HTTP and HTTPS web servers providing content to remote Internet users. Your approach should include the following phases: Discovery, Device Profiling, Scanning, and Validation.

Discovery

Discovery is establishing a fingerprint of the target network segment. All active device addresses and their associated Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and other network services accessible from the internal network within should be discovered during this phase.

During this phase, you should use both active and passive sniffers to collect network traffic for parsing and analysis. Information obtained through this method includes identification of active hosts, authentication credentials such as username/password combinations, indication of potential computer worm/Trojan presence, and other vulnerabilities.

The following list describes a few of the most popular tools used for network discovery:

Nmap — A network service port scanner that implements numerous techniques for evasion of Network Intrusion Detection System (IDS) sensors
Ethereal — A passive network sniffer that supports capture and interpretation of most Link Layer (media) and network and application protocols. Used in combination with ettercap and ngrep, the captured network traffic can be extracted to meaningful content such as Web (HTTP,
HTTPS) application transactions, user authentication for numerous protocols, electronic mail messages, and other data.

**Firewalk** — Implements methods of accurately determining network and protocol filtering rules of remote ingress network routing devices.

**hping** — Provides methods of crafting unique packets using multiple protocols (ICMP, TCP, and UDP) to determine host availability, routing information, and several other metrics.

### Device Profile

Using the information gathered during the discovery phase, you can analyzes the list of accessible network services, Internet Protocol (IP) stack fingerprints, and known network architecture to identify potential roles and trust relationships each device plays in your network infrastructure.

### Scanning

You should test each network service identified during the discovery and device profile phases for known vulnerabilities. Vulnerabilities may fall into one or many of several categories, including:

- System compromise
- Unauthorized data access
- Information disclosure
- Command execution
- Denial of Service (DoS)

In some instances, security risks that are associated with a particular network service can be detected and exploited using the following software applications:

**Nessus** — A popular all-in-one vulnerability scanning tool kit that includes many of the most updated tests for a variety of operating systems and network services.

**onesixtwayne** — A Simple Network Management Protocol (SNMP) service scanner and wordlist-based community string testing utility.

**nikto** — A Web server vulnerability scanning tool.

### Validation

After you have discovered, profiled and scanned your network. You should attempt to exploit or validate all results from the vulnerability scanning phase. Tests and techniques applied during this stage of the assessment are often very specific to the potential vulnerabilities detected. It is during this phase of the assessment that bulk of your results will be generated.

### Final thoughts

The Internet is a lawless place. Assessing your network for risk is part of the responsibility of providing network services to your users and customers. If you don’t find and fix the problems on your network, you can be sure that eventually someone else will.