Penetration Testing Methodology

Overview

This document describes the penetration testing offering from Syrinx Technologies. The penetration testing offering consists of several major components, with each component having smaller sub-components. This hierarchy allows the client to pick and choose only those services needed at the time, thereby reducing the complexity and cost of the solution. The major components of the offering include the following:

- External Penetration Testing
- Internal Penetration Testing
- Social Engineering Testing

General Penetration Testing Methodology

When performing external or internal penetration tests, Syrinx Technologies employs a standard 3-step methodology. This methodology allows for a systematic testing process that ensures all appropriate tests have been applied to the proper devices. The testing process is cyclical by nature and often involves discovering and re-testing new networks and devices as they are uncovered during the testing process.

The typical external and internal penetration test consists of the following phases:

1. Reconnaissance – This step attempts to discover as much information about the client as possible using publicly available resources. Various web search engines are used along with information from the client's web site(s). DNS queries also provide useful information along with queries to the various domain registries. Other sources of information include local, state and Federal regulatory agencies.

2. Scanning – During this phase various scanning tools are used to determine the operating systems, protocols, ports and applications in use. Depending on the operating systems and applications discovered, various other port, vulnerability and application scanners are then used to further define the exact environment. The goal at the end of this phase is to understand in detail the exact applications, versions and configurations for all network devices.
3. Verification – The final phase in the analysis attempts to document and verify any possible vulnerabilities discovered in the network devices. This phase involves a wide variety of exploits depending on the nature of the issue and what type of device on which it is found. The client always has the option of how far the verification stage pursues any discovered flaws.

Testing Parameters

Syrinx Technologies will never delete files or data during testing. No web pages will be defaced or changed in any way. No user accounts will be deleted, although during testing it is generally acceptable to add accounts where needed and when possible. These accounts will be documented fully to allow the client to remove them once testing is complete. For any high-risk exploits, screen captures will usually be taken to reduce the overall chance of causing downtime for any system.

Syrinx Technologies will not use Denial of Service (DoS) or Distributed DoS (DDoS) attacks on any client network. The client should be aware that during testing it is possible for any given network device to be affected by the testing. Log files are especially susceptible during the Scanning phase. The client should be aware of this and notify Syrinx Technologies in the event that an application is affected or logs are filling up and causing a problem. Syrinx Technologies will not use untested software tools or techniques in their assessments.

External Penetration Testing Options

- All publicly available network applications
    - Email, DNS, FTP, database
    - Web sites/applications
        - SQL Injection
        - Cross Site Scripting (XSS)
        - Cookie tampering
        - Incorrect directory permissions

        - Directory traversal
        - Privilege escalation
        - Missing patches
        - Authentication credentials
        - Backend database connections
        - Operating system components
        - Middleware
- Network infrastructure devices
    - Firewalls
    - Routers
    - VPN concentrators
- 802.11(abg) wireless access points
- Bluetooth devices
- Dial-In
    - Specific modems attached to network devices
    - Blocks of phone numbers (1 to 1000's)

Internal Penetration Testing Options

- Testing of all internal networks, infrastructure devices and applications
    - Servers
    - Desktops
    - Application servers
    - Network management devices
    - Routers, switches
    - PBX, VoIP devices
- Extranet/Intranet networks/servers

Social Engineering

Social engineering testing is designed to test the human components of a network. Often the best security technologies in the world can be circumvented by a single employee not following the proper procedures. This testing is designed to test anything from a single employee to a whole department. The testing is carefully designed in cooperation with the client to ensure specific components of existing policies are tested.

The testing can be performed either with some information provided by the client or with no information provided by the client. Whether or not information is shared before testing begins depends largely on the nature of the testing and the time allotted to the testing. Social engineering testing works best when there are specific policies and procedures that are being tested. This testing also has the most effect when it is combined with regular security awareness training for all employees.

Social Engineering Testing Options

- External phishing emails
    - Attempt to elicit sensitive information, including network login using external email addresses
- Internal phishing emails
    - Attempt to elicit sensitive information, including network login using spoofed internal email addresses
- Dumpster diving
- External calls to help desks, support personnel, etc.
    - Attempt to elicit sensitive information, including network login
- Attempts to physically access computer rooms, wiring closets, etc.
    - Pretending to be various support personnel
- Building walk-through's
    - Sensitive information laying on desks
    - PC's with no screen saver/passwords
    - Accounts/passwords written on white boards, monitor, etc.
    - Unlocked cabinets
    - Other tests as determined by corporate policy
    - Check of trash can for sensitive information