December 2003

SOHO Security: A Technical Briefing

Alberto Bento
University of Baltimore

SOHO SECURITY: A TECHNICAL BRIEFING

Al Bento
University of Baltimore
abento@ubmail.ubalt.edu

Abstract

Small businesses and home offices (SOHO) are increasingly connected to the Internet through broadband networking (cable, DSL, wireless) twenty-four hours a day, seven days a week (24/7). Of course, neither small businesses, nor individuals working in their home offices, have the financial resources, or the technical expertise, to protect themselves as effectively as organizations with well-staffed Information Systems Departments. What can SOHO do? The answer to this question is the objective of this briefing, particularly aiming to provide materials for a class meeting on Security in the MBA core course in information systems.

Security threats to SOHO are becoming a problem for mid to large-size organizations, too. Many of the security breaches in large-size organizations, as was the case recently at Microsoft, were in reality security breaches in the home office of their employees. DoS (Denial of Service) attack to large organization sites (CNN, Yahoo, etc) are done using zombies planted in home PCs using broadband networking. SOHO should be able to protect themselves using cheap firewalls (hardware and software), detect potential hazardous hacker activities, prevent the installation of backdoors and Trojans, and be able to remove back doors and Trojans from their systems.

Outline

Basic Security Concepts

- requirements: secrecy, integrity and availability
- threats: interruption, interception, modification and fabrication
- assets: hardware, software, data, communication lines, etc.

Explains the basic tenets of security in simple terms

Internet Attacks Framework

- target acquisition and information gathering: footprinting, scanning and enumeration
- initial access: physical access, trojans and brute force
- privilege escalation: becoming administrator, root, and consolidation of power by obtaining other accounts, accessing other resources (hosts, networks).
- covering tracks: avoid detection by deleting or modifying logs, disguising trojans.

Reveals the hacker logic and comprehensive attack framework

Free Tools for Footprinting, Scanning and Enumeration

- CyberKit: whois, single ping, ping sweep, traceroute, and port scanning

- Sam Spade: DIG tool requests all the DNS records for a host or domain, Zone Transfer - ask a DNS server for all it knows about a domain, SMTP Relay Check - check whether a mail server allows third party relaying, Scan Addresses - scan a range of IP addresses looking for open ports, etc.
- SuperScan: ping sweep (finding active hosts) and TCP port scan (finding open ports)
- Nmap: ping sweep, TCP and UDP port scan, OS detection, etc.

How to obtain and use basic hacker tools to find unprotected assets. Shows how easy is for the hacker to obtain information about user machines -- an eye opener to the attendees.

Common Types of Attacks

- Backdoor and Trojans: BO, NetBus and SubSeven
- DoS: Smurf, Fraggle and Syn
- DDoS: servers and zombies (slaves)

Detailed explanation of the types of hacker attacks (how to use tools to create these attacks is not discussed in the presentation).

Firewalls

- types of and free (software) personal firewalls: Zone Alarm, Tiny and ICF(XP), and
- hardware firewalls: Cisco, Watchgard, SonicWall and D-Link.

Basic protection through firewalls is demonstrated using software firewalls.

Detection and Prevention

- Detection: ZombieZapper, NFR BackOffice Friendly, ActivePorts, SNORT and
- Virus checking and detection: detect backdoors and Trojans, but need regular virus definition updates.

Detection and prevention is better than protection, but together all three can provide a safer environment for SOHO.

Web Software Security

- Web browsers: Netscape and Internet Explorer,
- E-mail: attachments, JavaScript, macros in Office applications, etc.

Basic security precautions using browsers, e-mail and macros in office applications.

VPN and Remote Control Programs

- Tunnel technology and unintended backdoors.

Remote use or access to computers and networks require special security precautions. Most common pitfalls, threats and attacks are discussed.