

NETWORK SECURITY: AN INTRODUCTION TO PARANOIA

Common Misconceptions

- > My network is not interesting enough to be attacked.
- > If the system is working fine, we have not been cracked yet.
- > Installing (*insert panacea here*) will solve all our problems.
- > We can't afford the investments to properly secure our systems.
- > Crackers are very skilled, and to thwart them I will have to learn more than they know.

How Systems are Cracked

☺ **A Script Kiddie Attack**

- > 1337 hax0r learns about a neat new exploit. He downloads the exploit script and reads the directions on how to run it.
- > Before going to bed, he sets up his port scanner to find any computers that are vulnerable to this attack.
- > The next afternoon, he checks the scan results to find systems that he can compromise.
- > He selects an available target, runs the exploit and gains root access.
- > As root, he creates a back door to the system, then runs a script to cover his tracks.
- > Using the compromised system, he runs the exploit on another system.

☺ **Social Engineering Attack: Discredit the Source**

- > Student wants to stop email going to parents about bad conduct.
- > She gets a copy of the bad conduct email.
- > Spoofing a school email address, she modifies the email and sends it to every parent in school for the next 3 weeks.
- > Email system is discredited and bad conduct emails cease.

☺ **Social Engineering Attack: Ask for Login Rights**

- > Student wants to change grades in computer system.
- > Pretending to be a new techie, calls office secretary and asks for her password.
- > Logs in as secretary (with her privileges) and changes grades.

Security Checks: Preparing for the inevitable

☺ **The Most Common Mistakes**

- > Vulnerable CGI scripts on web servers
- > Weak or blank passwords
 - : User and administrative accounts have weak passwords
 - : Using default passwords
 - : Using the same administrative password for everything
- > Not applying patches
 - : Not keeping up with vulnerability announcements
 - : Not applying security patches on a regular basis
- > Running unnecessary services
- > Not having a security plan

NETWORK SECURITY: AN INTRODUCTION TO PARANOIA

☺ **Preparing Desktops**

- > Require logins for all users
 - : Keep computers logged out
 - : Set computers for auto-logout
- > Apply policies to limit access
 - : Don' let users install software
 - : Lock users out of sensitive directories
- > Prohibit booting from CD-ROM and floppy
 - : Password protect the CMOS
 - : Consider computers without CD-ROM and floppy drives
- > Test security features on desktop

☺ **Preparing Servers**

- > Keep software updated (patches, virus definitions, etc.)
- > Remove all unnecessary software and services
- > Keep server physically secure
- > Do not leave server logged in
- > Close all unused ports
- > Run and monitor an intrusion detection system
- > Keep good backups
- > Run network scans to assess vulnerability
- > Keep network information private

☺ **Preparing Users**

- > Keep user accounts up-to-date
 - : Make sure they are in correct groups, OU, etc.
 - : Disable or remove accounts for users who leave
- > Use auditing to require strong passwords
- > Educate users on basic security
 - : Never sharing password (even to admins who ask for it)
 - : Logging out when finished
 - : Concepts of having a strong password

☺ **To Do When You Get Home**

- > Establish and implement a security plan
 - : Designate people responsible for security
 - : Provide time and materials for training
 - : Create an incident recovery team
 - : Install necessary tools to implement plan
- > Sign up for vulnerability email lists
- > Remove unnecessary services
- > Patch all applications
- > Scan yourself
- > With permission, run a password audit

NETWORK SECURITY: AN INTRODUCTION TO PARANOIA

Resources: Where to go to get prepared

☺ **Tools**

- > Snort: Open source intrusion detection system. www.snort.org
- > John the Ripper: Password auditing program. www.openwall.com/john/
- > Nmap: Port scanner. www.insecure.org/nmap
- > Ethereal: Packet capture tool for reading binary logs. www.ethereal.com
- > Tripwire: File integrity tool. Identifies files that have changed. www.tripwire.com
- > More tools: www.insecure.org/tools.html

☺ **Education and News**

- > SANS Institute: Articles, resources, and vulnerability listings. www.sans.org
- > HoneyNet Project: White papers, challenges, and detailed analysis from a honeypot project. www.honeynet.org
- > Security Focus: Vulnerability listings and home of the Bugtraq mailing list. www.securityfocus.com
- > CERT: Vulnerability advisories and security articles. www.cert.org

☺ **Practical Help**

- > Mission Critical Security Planner. Book by Eric Greenberg. Focuses on balancing security with business needs. Includes worksheets. www.criticalsecurity.com
- > SANS Essential Security Actions. Steps for attaining three levels of security. www.sans.org/resources/esa.php
- > Security Testing Methodology. A long paper on the methodology for securing networks. www.isecom.org/projects/osstmm.htm