More "Theoretical" Projects

T1) Privacy-Preserving Data Dissemination
Goal: Contribute to design and develoment of a scheme for privacy-preserving data dissemination. (Research papers are available from the instructor.)

Note: Possibility of project continuation in the following semesters.

T2) Authentication in Healthcare
Goal: Investigate and survey authentication. (A preliminary white paper is available from the instructor.)

Note: Possibility of project continuation in the following semesters.

T3) Projects proposed by you.

More "Practical" Projects

Note: The projects described here are for MS Windows (but some require use of Linux Server for experiments).
If you want to run projects on Linux, most of the projects can be run in the Linux environment (with different tools).

P1) Scanning and Enumerating the Network for Targets [LL: #4]
Scanning and enumerating a network – to discover what machines are attached to it an operating.

Task 1: IP Address and Port Scanning, Service Identity Determination
a-- Nmap - IP scanning in Windows

Goal:
Locating target machine, and identifying its OS, open ports, types of services it runs.
Tools:
1) Windows XP Pro
2) Windows Server
3) Nmap – multi-functional scanning and enumeration utility used to quickly gather info about network hosts (incl. their availability, ports, IP addresses, names, their OSs, services they run). Used by hackers as the first attack step

4) Ethereal packet sniffer for analyzing network traffic
5) telnet to grab service banners (sent by service after initial connection), incl. server's type/version

Task 2: Researching System Vulnerabilities
(Internet - access CVE database of vulnerabilities)

Goals:
1) Identifying vulnerabilities for the target machine.
2) Finding utilities to test these vulnerabilities.
Tools:
1) Google to find CVE (at Mitre Corp.)
2) CVE database
3) Packet Storm Web site

Task 3: GUI-Based Vulnerability Scanners
a-- NeWT - Using a Vulnerability Scanner in Windows

Goals:
Use vulnerability scanner to inspect Windows Server vulnerabilities.
Tools:
1) Windows XP Pro
2) Windows Server
3) Tenable NeWT vulnerability scanner

P2) Attacks-Web Server, Email, DOS and Trojan Attacks [LL: #5]

Task 1: Web Server Exploits
a-- Web Server Exploits (in Windows)

Goals:
1) Exploit MS web server, attacking vulnerabilities explained in CVE-2001-0333 (a directory traversal vulnerability).
Tools:
1) Windows XP Pro
2) Windows Server, incl. MS Internet Information Server (IIS)
3) Internet Explorer

Task 2: E-mail System Exploits
c--(Windows + Linux Server) Exploiting E-mail Vulnerabilities in Windows

Goals:

1) Spoofing an e-mail address.
2) Analyzing how use of HTML (esp. hyperlinks) in e-mail can be used to spread viruses.
3) Analyzing how e-mail can be crafted to convince someone to do sth they should not.
Tools:
1) Windows XP Pro, incl. Outlook Express
2) Windows Server
3) Linux Server
4) Telnet

Task 3: Denial of Service Exploits
a-- Windows Denial of Service SMBDie

Goals:
1) Understanding how DOS attacks are run.
Tools:
1) Windows XP Pro
2) Windows Server
3) nmap - multi-functional scanning and enumeration utility used to quickly gather info about network hosts (incl. their availability, ports, IP addresses, names, their OSs, services they run). Used by hackers as the first attack step
4) ping
5) SYN Flood – DOS attack utility
6) netstat
7) SMBDie – buffer overflow attack utility
8) Ethereal - to analyze network traffic (generated by SMBDie)

Task 4: Trojan Attacks
a-- Using the Netbus Trojan (in Windows)
a-- Using the SubSeven Trojan (in Windows)

Goals:
1) Experimenting with Trojans (installing, deploying, controlling).
Tools:
1) Windows XP Pro
2) Windows Server
3) Netbus Trojan
4) netstat
x) SubSeven trojan

P3) Escalating Privilege-Sniffing, Keylogging, Password Cracking Attacks [LL: #6]

Task 1: Intercepting and Sniffing Network Traffic
c--(Windows + Linux Server) Sniffing Network Traffic in Windows

Goals:
1) Using a packet sniffer to capture and analyze network traffic to reveal sensitive information.
Tools:
1) Windows XP Pro
2) Windows Server
3) Linux Server
4) Ethereal packet sniffer to analyze network traffic
5) Telnet
6) FTP

Task 2: Keystroke Logging
a-- Keystroke Logging in Windows

Goals:
1) Install, configure, and run a key logger.
Tools:
1) Windows XP Pro
2) Windows Server
3) A key logger utility.

Task 3: Password Cracking
a-- Password Cracking in Windows

Goals:
1) Experimenting with password-cracking utilities, attempting dictionary, hybrid, and brute-force attacks.
Tools:
1) Windows XP Pro
2) Windows Server
3) pwdump3 utility to otain password hashes
4) John the Ripper password cracking utility

Task 4: Man-in-the-Middle Attack
(Windows + Linux Client)

Goals:
1) Understanding Man-in-the-Middle (MITM) attacks, including “ARP poisoning” and intercepting passwords.
Tools:
1) Windows XP Pro
2) Windows Server

3) Linux client
4) Ethereal packet sniffer to analyze network traffic
5) Ettercap utility for attacking the ARP protocol (by trapping passwords, other session data, and for poisoning ARP cache—storing MAC addresses, used by computers to communicate on LAN)

Task 5: Steganography
a-- Steganography in Windows

Goals:
1) Using steganography for hiding information in images.
Tools:
1) Windows XP Pro
2) Windows Server
3) Camouflage steganographic utility

P4) Hardening the Host Computer [LL: #7]

Task 1: Hardening the OS
a-- Hardening Windows 2000

Goals:
1) Using tools for hardening the OS, incl. CIS Security Scoring Tool and MS Windows security templates. Creating secure passwords.
Tools:
1) Windows XP Pro
2) Windows Server
3) CIS Windows Security Scoring Tool (CIS-Win)
4) MS Windows security templates
5) NeWT vulnerability scanner

Task 2: Windows XP Service Pack2

Goals:
1) Install, explore, and test security-enhancing Windows XP Service Pack 2, esp. its Security Center.
Tools:
1) Windows XP Pro
2) Windows Server
3) Windows XP Service Pack 2
4) ping
5) nmap

Task 3: Using Antivirus Applications
c--(Windows + Linux Server) Antivirus in Windows

Goals:
1) Install, configure, and experiment with antivirus software and malware (a Trojan); use antivirus s/w to scan e-mail.
Tools:
1) Windows XP Pro
2) Windows Server
3) Linux Server
4) Outlook Express
5) McAfee Antivirus

Task 4: Using Firewalls
a-- Personal Firewall in Windows

Goals:
1) Install, configure, and experiment with personal firewalls and their rulesets. Observe and analyze firewall log.
Tools:
1) Windows XP Pro
2) Windows Server
3) Visnetic Personal Firewall
4) nmap port scanning utility
5) ftp
6) Internet Explorer

P5) Securing Network Communications 1: GPG (for E-mail), SSH, and SCP [LL: #8: 28-30]

Task 1: Using GPG to Encrypt and Sign E-mail
c--(Windows + Linux Server) Using GPG in Windows

Goals:
1) Using a public key encryption tool (GPG) to generate a public-private key pair and exchange keys.
2) Using GPG to encrypt/decrypt and sign e-mail.
Tools:
1) Windows XP Pro
2) Windows Server (DNS Server)
3) Linux Server (mail server)
4) Outlook Express
5) WinPT (Windows Privacy Tool) software for public key encryption

Task 2: Using Secure Shell (SSH)
c--(Windows + Linux Server) Using Secure SHell in Windows

Goals:
1) Configure and use SSH software to establish and experiment with secure connection. Detecting MITM attacks (impostors) with PuTTY.
Tools:
1) Windows XP Pro
2) Windows Server
3) Linux Server
4) SSH
5) PuTTY, an SSH client program detecting MITM attacks
6) Ethereal for analyzing captured session

Task 3: Using Secure Copy (SCP)
c--(Windows + Linux Server) Using Secure Copy in Windows

Goals:
1) Install, configure, and experiment with SCP to transfer files to/from a remote computer.
2) Use Blowfish symmetric encryption system.
Tools:
1) Windows XP Pro
2) Windows Server
3) Linux Server
4) SSH - Secure Shell
5) WinSCP – Windows SCP client with Blowfish
6) Ethereal for analyzing captured session

P6) Securing Network Communications 2: Certificates, SSL, and IPsec [LL: #8: 31-32]

Task 1: Using Certificates and SSL
a-- Using Certificates and SSL in Windows

Goals:
1) Learn about default Certificate Authorities (CAs) for your browser.
2) Install and configure in-house CA server.
3) Learn how to configure a Web server to use the SSL and SSL certificates.
4) Experiment with SSL for authentication via certificates.
Tools:
1) Windows XP Pro

2) Windows Server
3) Ethereal for analyzing captured session

Task 2: Using IPSec
a-- Using IPSec in Windows

Goals:
1) Configure and use Virtual Private Network (VPN) in Windows (using IPsec).
2) Configure and use IPsec in Windows to allow/disallow certain types of network traffic.
Tools:
1) Windows XP Pro
2) Windows Server
3) ping
4) FTP
5) Ethereal for analyzing captured session

P7) Preparing for and Detecting Attacks 1: Log Analysis and Intrusion Detection
[LL: #9: 33-34]

Task 1: System Log File Analysis
a-- Log Analysis in Windows

Goals:
1) Learn configuring system logs (set up auditing), generating log entries, and analyzing logs.
Tools:
1) Windows XP Pro
2) Windows Server
3) FTP
4) Internet Explorer

Task 2: Intrusion Detection Systems
a-- Using Intrusion Detection Systems in Windows (Snort)

Goals:
1) Install and configure Snort (an Intrusion Detection System), use it to detect and record anomalous traffic, analyze Snort alert file.
2) Configure Snort as detection engine detecting attacks based on signatures defined by rulesets.
3) Create simple Snort rules.
Tools:
1) Windows XP Pro
2) Windows Server

3) Snort intrusion detection system
4) ping
5) nmap scan utility and Xmas scan
6) SubSeven Trojan
7) Telnet
8) Internet Explorer

P8) Preparing for and Detecting Attacks 2: Honeypots, Spyware, Backing Up and Restoring [LL: #9: 35-37]

Task 1: Using Honeypots
a-- Using Honeypots in Windows

Goals:
1) Install, configure, and experiment with a honeypot to detect, capture, and analyze attacks.
2) Create simple honeypot scenarios and alerts, and test them with test attacks.
Tools:
1) Windows XP Pro
2) Windows Server
3) KFsensor honeypot for Windows
4) nmap scan utility with port scan
5) Telnet
6) Internet Explorer
7) Netbus client utility

Task 2: Detecting Spyware
d--(Internet) Spyware Detection and Removal in Windows

Goals:
1) Install, configure, and experiment with anti-spyware software.
2) Detect spyware (adware) infection, and learn to remove spyware.
Tools:
1) Windows XP Pro — Virtual PC
2) Internet access
3) MS anti-spyware s/w
4) HijackThis browser hijacker detector and remover

Task 3: Backing Up and Restoring
a-- Backing Up and Restoring in Windows

Goals:

1) Configure computer to back up files, create backup scripts, and run full and differential backups.
2) Restore deleted files.
Tools:
1) Windows XP Pro
2) Windows Server
3) ntbackup Windows utility

P9) Digital Forensics [LL: #10]

Task 1: Initial Response - Incident Determination
a-- Initial Response - Incident Determination (in Windows)

Goals:
1) Perform "live initial response" to detect presence of malware, to capture volatile data from the infected computer, and to generate report.
2) Analyze "initial response" reports.
Tools:
1) Windows XP Pro
2) Windows Server
3) Second hard drive (rogue drive)
4) Netbus utility
5) Keylogger utility
6) Helix Live CD ISO (v.1.6, dated 3-12-2005) with Live Analysis program
7) Windows Forensic Toolchest (WFT)
8) Internet Explorer

Task 2: Acquiring the Data
a-- Acquiring the Data (in Windows)

Goals:
1) Learn to preserve entire disk drive for forensic analysis, make its forensic duplicate, and verify its integrity with a fingerprint (MD5 hash).
Tools:
1) Windows XP Pro
2) Windows Server
3) Forensic drive
4) Second hard drive (rogue drive)
5) dcfldd, fdisk and mkfs utilities for zeroing out drives, partitioning, and formatting them
6) Helix Live CD ISO (v.1.6, dated 3-12-2005) with Live Analysis program
7) Grab utility to capture rogue drive image
8) hashtab utility producing File Hashes tab.

Task 3: Forensic Analysis
a-- Forensic Analysis (in Windows)

Goals:
1) Learn to perform forensic analysis of a supect drive image, including file analysis, keyword search in images, and file type search.
Tools:
1) Windows XP Pro
2) Second hard drive (rogue drive)
3) Helix Live CD ISO (v.1.6, dated 3-12-2005) >>>>>>>> with Live Analysis program
4) Autopsy Forensic Browser – graphical interface to command-line digital forensic analysis tools in The Sleuth Kit
5) stegdetect utility detecting uses of steganography.

P10) The DETER security testbed

NOTE:
Great possibilities esp. for students planning to continue research beyond the current semester).

Goals:
1) Learn how to use the DETER testbed and test data. Investigate possibilities for deploying DETER in our labs.
2) Run simple experiments on DETER.
Tools:
1) Information on DETER: http://www.isi.edu/deter/
2_ Deter testbed - a shared testbed infrastructure that is specifically designed for medium-scale (e.g., 100 node) repeatable experiments, and especially for experiments that may involve "risky" code.

P11) Fighting Web Bugs

Goals:
1) Identify tools for web bug detection and learn how to detect Web bugs.
Tools:
1) Bugnosis for locating web bugs.

P12) Projects proposed by you.

Appendix 1: Checking out s/w on ELMS

(from Mr. Sai Kirirn Kovvuri)

1) Enter www.cs.wmich.edu/~scst (Student

2) Click “ELMS for CS”

3) Login using your CS account username and password

4) Order a new copy of software that you want

5) The license key (if needed)will be emailed to your CS Webmail.

6) Bring CD for copy of software to C-208.