Lab Course: System Administration and Cybersecurity

Contents

Course Description

This course provides an immersive learning experience through a comprehensive series of hands-on laboratory exercises. Designed to enhance students' proficiency in System Administration and Network Security in an Internet context, these practical exercises allow students to apply their IT skills in a simulated real-world environment.

This course takes a proactive approach to learning, allowing students to actively participate and apply theoretical knowledge to practical situations. With a focus on practical skill development, students can confidently refine their abilities in System Administration and Network Security, building a strong foundation for their future careers.

Course outline

DNS and Mail server Setup

- Setting up and maintaining DNS and Mail servers
- Anti-spam (Access list, RBL, DCC, SPF, greylist.. etc) and anti-virus techniques
- Tools for DNS record and domain registration information queries (nslookup, host, dig and whois)

Building Public Key Infrastructure (PKI)

- PKI model
- Setting up secure HTTPS web server
- Operating a Certificate Authority (CA)
- Client Authentication and Web Access Control

Network Monitoring and Debugging

- Methods of Network Troubleshooting (Hping, traceroute, arp, tcpdump, ... etc)
- Tools for Network Monitoring (IPtraf, Wireshark, SNMP, MRTG, Netflow, NTOP, Network Miner, IPAudit, ... etc)

Hacking Techniques

- Trends of Attacks and the Threats
- Attackers' workflow
- Social Engineering
- Stealth and decoy port scanning
- Buffer Overflow (both local and remote exploits)
- Remote root exploit through invalid input of printf()
- WEB Hacking
  - CGI exploit
  - JavaScript exploit
  - Google hack
- Cross-site Scripting (XSS)
- SQL Injectioin
- Cross Site Image Overlaying (XSIO)
- Cross-Site Request Forgery (CSRF)
- Phishing (Internet fraud by spoof e-mail and bogus web sites)
  - URL Obfuscation
  - Page Redirect
  - Window Injection
  - Visual spoofing
- Sniffer, Pharming, and Man-In-Ihe-Middle attack
  - By ARP poisoning
  - By DNS poisoning
  - By DNS Hijacking
  - By Cookie Session Stealing
  - SSL Stripping
  - By Transparency Proxy
  - By Changing Network Setting
  - By Evilgrade framework
- Wireless LAN attack (sniffering and WEP cracking demo)
- Distributed Denial of Service (DDoS)
- Trojan Horse Programs
  - Stealth
  - Backdoor Establishment
  - Detection
- Risks and vulnerabilities in different ports/services/protocols/applications
- Real Cases Studies

Computer Forensics Analysis

- Steps of Incident Handling
- Computer Forensic Techniques and Tools on UNIX and Windows platforms.
- Malware Analysis
  - Malware general behaviors
  - Reverse Engineering Malware (REM): Tools and Techniques

        - Real Cases Studies: IRC botnet, URL monitoring, form/screen scraping, keystroke logging, spam relay, rootkit... etc
    - Dynamic Analysis (On-line Inspection)
        - Preserving and collecting evidences (e.g. cloning the disk, copying data and dumping the process memory content)
        - Collecting network information (e.g. capturing suspected traffic)
    - Static Analysis (Off-line Inspection)
        - Examining the log files and data files
        - Malware code review
        - Data Recovery and Analysis
            - Recovering and examining of removed and hidden files (not from back up tape)
    - Rootkit analysis
    - Honeynet
        - Tools and techniques for setting up and running a Honeynet
        - Data Capturing
        - Data Analysis
        - Results Sharing

Security Audit

- Security Model
- General steps and procedures to conduct a security audit
- Using vulnerability scanner (NESSUS)
- Penetration Test with Backtrack4
- Penetration tests with Metasploit framework
- Writing a vulnerability analysis report of a network

Intrusion Detection System (IDS)

- Host base and network base IDS
- Setting up a Network Intrusion Detection System (NIDS using SNORT)
- Fine tuning the NIDS (excluding the false alarm)
- Setting up a IDS console with database and web interface support
- Common IDS weakness

Firewall

- Firewall architectures
- Setting private network with Network Address Translation (NAT)
- Setting up transparency proxy with NAT and squid
- Fine tuning the firewall rules to suit your access control policy
- Examining the firewall log
- Setting up a IDS gateway or Network Intrusion Prevention System (NIPS) by integrating the firewall and NIDS
- Setting up VPN server
- Common Leaks of Firewall and their counter measures