Computer Network Security

Syllabus

Description

This course will cover some key topics in network and host level security.

The course will begin with an introduction to networking. Students will get hands on experience with enterprise level networking equipment (switches, routers, firewalls). It will be followed by an introduction to network level attacks and various defense mechanisms. Students will learn to mount attacks and defend against them using a variety of software tools. The class will then focus on wireless networking security. Students will learn how to configure, attack, and defend wireless networks. After that the class will concentrate on host level security. Students will learn to attack and defend common network services such as DNS, HTTP, SQL, and FTP.

Organization

This is lecture lab course. Every week starts with a lecture where the instructor presents a certain networking or security concept. This theoretical knowledge is reinforced by performing a lab assignment. To further enhance your knowledge we will ask you to complete several programming assignments.

Course topics

Network communications

Switch management, LANs and virtual LANs, ARP and IP protocols, routing, spanning tree protocol, link aggregation protocol

Expected outcome: knowledge of switch level network configuration

Network security

IP Routing, Firewalls, ACLs, network address translation, virtual networking, network services (DHCP, DNS)

Expected outcome: knowledge of IP routing basics, ability to configure network services

Network services vulnerabilities

ARP spoofing, network scanning and fingerprinting, vulnerability exploitation

Expected outcome: ability to navigate unknown network environments; basic knowledge of penetration testing; knowledge of vulnerability mitigation techniques

Wireless network security

Connecting to WEP/WPA PSK secured networks, monitoring and diverting wireless traffic

Expected outcome: knowledge of a security level attainable by wireless networks

Grading Policy

Labs: 40% in lab performance

Projects: 20%

Midterm and Final: 40% (consists of written test and in lab assignment)

Course Outline

1. File System
    a. Adding users, groups, adding users to groups
    b. Creating files, directories, assigning access rights
    c. Listing directories and files access rights
    d. All basic filesystem operations: copying, finding files, moving files, editing files
    e. Testing access as different users
    f. Basic understanding of linux filesystem tree (where the thing usually are), what is home folder, what is root folder
2. Getting Familiar with Equipment
    a. How to connect everything, Switch CLI
    b. Configuring IP address on host
    c. Port Mirroring & Wireshark
3. Configuring VLANs
    a. Configuring Linux to understand VLANs
4. Arp spoofing, Link Aggregation
    a. Configuring Link Aggregation
    b. Inducing broadcast storm
    c. ARP spoofing, hijacking SSL session
5. Xen
    a. Configuring software bridges
    b. Permanent network configuration
    c. Configuring Xen
    d. Creating VM
6. Network Services
    a. configuring file sharing with samba
    b. testing file sharing under multiple users
    c. Configuring DNS server
7. Routing Creating bidges according to the map
    a. Configuring router to mamange subnets
8. Nat, Firewall, Network Services
    a. Configure switches with VLANs
    b. Configure IPs
    c. Configure DHCP server
    d. Configure NAT
    e. Configure firewall

9. Midterm
    a. Filesystem
    b. VLANs
    c. Networking
10. Wireless
    a. Configure WEP Access point
    b. Bypass WEP encryption
    c. Bruteforcing WPA encryption
11. VPN
    a. Configuring SSH and port forwarding
    b. Configuring site to site VPN
12. Network Reconnaissance
    a. Network scanning
    b. Network mapping
    c. Vulnerability Identification
13. Network Penetration Testing
    a. Network scanning
    b. Exploiting Linux/Windows
14. Final
    a. Wireless
    b. Windows attack
    c. Pivoting and Linux attack

Projects

1. Introduction to Python. File input/output. String Processing.

2. DNS log files processing

3. Intrusion Detection System