River Valley Community College
One College Place
Claremont, NH 03743

March 2012

NETWORK SECURITY

CURRICULUM AND COURSE NUMBER: CYBS 120R
DEPARTMENT: Business/Computer Technology
CREDIT HOURS: 3
SEMESTER HOURS: **CLASS:** 2 **LAB:** 2
PREREQUISITES/COREQUISITES: CYBS 101R

COURSE DESCRIPTION

Students will learn about network communications from a security standpoint and perform laboratory assignments in securing networks and Operating Systems.

Course Competencies:
Upon successful completion of this course, the student will be able to:

1. Network Defense Fundamentals: In this topic, students are introduced to the core concepts of network security. Network defense technologies are examined, with particular emphasis given to the creation of a layered and diversified defense-in-depth architecture that begins with a security policy defining each layer. Students also identify the foundations of network auditing.
    a. Describe the five keys of network security.
    b. Identify and explain the concepts, policies, and technologies associated with a layered and diversified defense-in-depth strategy.
    c. Discuss the objectives of access control methods and describe how the available methods are implemented in the defense of a network.
    d. Identify the impact of a layered defense on the performance of the network.
    e. Define the concepts of auditing in a network, including the types of audits and the handling of data.
2. Advanced TCP/IP: In this topic, students examine the primary set of protocols that run networks and the Internet today, the Transmission Control Protocol (TCP) and Internet Protocol (IP) suite. Students become familiar with the details of how TCP/IP functions, including core concepts such as addressing and subnetting, and advanced concepts such as session establishment and packet analysis.
    a. Define the core concepts of TCP/IP, including model layers, RFCs, addressing and subnetting, VLSM and CIDR, and the TCP/IP protocol suite.
    b. Utilize a protocol analyzer to examine all the fields of IP, ICMP, TCP, and UDP.
    c. Examine TCP sessions, including the use of control flags, and sequence and acknowledgement numbers in the three-way handshake and session teardowns.
    d. View and analyze network traffic fragmentation.
    e. Utilize a protocol analyzer to observe and analyze a complete FTP session, frame by frame.

3. Routers and Access Control Lists: In this topic, students are introduced to the functioning of routers and routing protocols. Students examine the issues related to securing both routers and routing protocols, including the removal of unnecessary services, creation of access control lists, and configuration of logging to manage and secure the network.
    a. Configure fundamental router security, including the use of banners and the SSH protocol.
    b. Examine the principles of routing by capturing and analyzing routing protocol packets, and observing the IP and MAC address relationships in a routed environment.
    c. Create configurations to harden the core services and protocols on a Cisco router.
    d. Configure and examine the function of Access Control Lists on a Cisco router that defends against network attacks.
    e. Create the required configurations to enable logging on a Cisco router.
4. Designing Firewalls: In this topic, students are introduced to the concepts and technologies used in designing firewall systems. Students will identify the methods of implementing firewalls in different scenarios, using different technologies.
    a. Examine the principles of firewall design and implementation.
    b. Construct a firewall policy based on stated requirements.
    c. Create a rule set for a packet filtering firewall.
    d. Describe the function and processes of a proxy server.
    e. Define bastion host and explain its purpose with respect to network security.
    f. Define honeypot and describe its function in the security of the network.
5. Configuring Firewalls: In this topic, students examine firewalls from a conceptual viewpoint to learn about the types of firewalls, how each of these types work, and what protection they can provide for the network. Students then apply this knowledge, utilizing Microsoft's Internet Security and Acceleration server and Linux IPTables.
    a. Describe standard firewall functionality and common implementation practices.
    b. Install, configure, and monitor Microsoft ISA Server 2006, while exploring management, monitoring, and auditing options.
    c. Examine the concepts of IPTables, including a review of sample rule chains controlling the egress and ingress of specific network traffic.
    d. Apply firewall concepts and knowledge by designing a firewall topology and rule sets to create the required firewall security posture for a specific network situation.
6. Implementing IPSec and VPNs: In this topic, students examine Virtual Private Networks (VPNs) and the security issues related to them. Students are introduced to the concepts of IPSec, then examine and configure the Microsoft Management Console (MMC) and identify the predefined IPSec policies in Windows Server 2003. Students create new policies and implement IPSec to specifically use AH, ESP, or both, in Transport Mode. IPSec traffic is analyzed using a protocol analyzer.
    a. Define the function of IPSec in a networked environment.
    b. Examine IPSec policy management.
    c. Implement and examine IPSec AH configurations.
    d. Implement and examine IPSec AH and ESP configurations.
    e. Analyze the IPSec structure, cryptography, the Encapsulating Security Payload, the Authentication Header, the Internet Key Exchange, and modes of implementation on a running network.

f. Examine the business drivers and technology components for a VPN.
g. Examine the concepts of IPSec and other tunneling protocols, including Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP).
h. Analyze secure VPN design and implementation issues.
i. Examine the issues of VPN and firewall architecture and VPN authentication.
j. Configure VPN options built into Windows 2003 Server.

7. Designing an Intrusion Detection System: In this topic, students are introduced to the concepts surrounding one of the critical areas to the defensive network protection scheme—the Intrusion Detection System (IDS). This system, in conjunction with the firewall technologies in place, is the basis for a very solidly defended network. The IDS is used to detect when an intruder is attempting penetration of the network, or tampering with the firewalls.
    a. Examine the components of Intrusion Detection Systems and describe how these interact to accomplish the goals of intrusion detection.
    b. Describe the technologies and techniques of intrusion detection.
    c. Examine the process of intrusion detection and how behavioral use is implemented in the IDS.
    d. Compare and contrast host-based and network-based IDSs.
    e. Examine the principles of intrusion detection data analysis.
    f. Describe the methods of IDS usage for the detection of, monitoring of, and anticipation of attacks.
    g. Identify IDS limitations.
8. Configuring an IDS: In this topic, students implement an Intrusion Detection System known as Snort. Students use this installation to capture and monitor TCP/IP traffic and to create rule sets that identify suspicious traffic and direct network attacks.
    a. Describe how Snort works as an Intrusion Detection System, highlighting the pros and cons of its implementation in a production network environment.
    b. Install Snort on a stand-alone computer.
    c. Describe, create, and test a Snort rule set.
    d. Configure Snort to send alert data to a MySQL database.
    e. Use Snort to configure a complete Intrusion Detection System on a Linux system, including a MySQL database and the BASE Console to view alerts.
9. Securing Wireless Networks: In this topic, students learn to implement and secure a wireless network. Students examine wireless network components and configurations, and identify the security options required for making wireless networks part of a trusted enterprise. Wireless network analysis tools are used to audit wireless networks.
    a. Examine the fundamental issues, equipment, media, and systems of wireless networking.
    b. Describe the fundamentals of wireless local area networks, including their operations, IEEE 802.11 framing options, configuration essentials, and vulnerabilities.
    c. Implement and analyze wireless security solutions, including WEP, SSID broadcast disabling, MAC address filtering, and WPA.
    d. Utilize wireless tools, including AiroPeek NX and NetStumbler, to audit a wireless network.
    e. Describe the components and procedures required to implement a trusted wireless network.

10. Analyzing Packet Signatures: In this topic, students are introduced to the core concepts of analyzing network packets, including those that are designated as allowed and disallowed for use on a network. Students examine in detail both the headers and payload sections of several packet types.
    a. Describe the concepts of TCP/IP packet signature analysis.
    b. Examine the function and describe the benefits of the Common Vulnerabilities and Exposure (CVE) standard.
    c. Examine the concepts of signatures and their use in identifying multiple types of traffic as malicious.
    d. Identify, examine, and contrast normal and abnormal TCP/IP traffic signatures.
11. Transmission and TEMPEST Security: In this topic, students examine issues related to the interception of data signals and computer emissions. Students study methods for securing computer equipment from detectable emissions, and examine the TEMPEST program.
    a. Identify and describe how data signals may be intercepted.
    b. Identify and describe methods of securing computer equipment emissions.
    c. Examine the TEMPEST program.

Course Outline:

Network Defense Fundamentals
Layered Security
Designing and Configuring Firewall Systems
Configuring VPNs
Designing and Configuring an IDS
Network Security Assessment.
Security Related RFCs
Transmission and TEMPEST Security

Learning/Instructional Methods:

Lectures
PowerPoint Presentations
Lab and Reading Assignments
Discussions
Term Papers

Performance Evaluation:

Midterm and Final Exams
Term Paper
Quizzes
Weekly written assignments
Discussion participation

Suggested Text(s): Please refer to syllabus

Origination date:

Revisions:
March 2012