C S 53B: FIREWALLS & THREAT MANAGEMENT

Foothill College Course Outline of Record

Heading	Value
Effective Term:	Summer 2021
Units:	4.5
Hours:	4 lecture, 2 laboratory per week (72 total per quarter)
Advisory:	C S 53A.
Degree & Credit Status:	Degree-Applicable Credit Course
Foothill GE:	Non-GE
Transferable:	CSU
Grade Type:	Letter Grade (Request for Pass/No Pass)
Repeatability:	Not Repeatable

Student Learning Outcomes

- A successful student will be able to apply techniques used by firewalls to counteract vulnerabilities
- A successful student will be able to describe basic network security vulnerabilities

Description

Survey of topics in field of firewall, advanced threats and their characteristics. Students will learn how to manage firewalls and advanced threats using security policies, profiles and signatures to protect networks against emerging threats.

Course Objectives

The student will be able to:
A. Describe basic network security vulnerabilities.
B. Explain firewalls and their features.
C. Apply techniques used by firewalls to counteract vulnerabilities.
D. Incorporate common solutions and strategies.
E. Apply different business models and appropriate solutions.
F. Describe firewalls' use of digital signature authentication.
G. Explain the operation of firewalls with built-in virus scanning.
H. Perform installation and configuration of common firewalls.

Course Content

A. Review of basic network security vulnerabilities
B. Firewalls, primary definition and features
1. Restricts inbound traffic to protect the network
2. Placed at the perimeter, acts as a gatekeeper
3. Types of firewalls
a. Software (personal firewalls)
b. Hardware (appliances), routers as firewalls
4. Problems with firewalls, weaknesses
5. Firewall components, including rules, or policies
C. Main techniques used by firewalls
1. Packet filtering
a. By protocol, by IP address, by port
b. Which ports are required for major services
c. Stateful Packet Inspection (SPI)
2. Proxy service
a. Checks inbound and outbound
b. Provides caching of recent pages
3. Circuit-level gateway
4. Application gateway
D. Common solutions and strategies
1. Proxy servers
a. Caching servers
b. Microsoft's Internet Security and Acceleration (ISA) server
2. Network Address Translation (NAT)
a. Hides IP addresses of all clients on internal network
b. Allows company to make best use of one IP address
c. Configuration of the interfaces
3. DMZ (demilitarized zone) gateway computer
a. Allows access to web-based business servers
b. Permit certain ports
c. Setting up a workstation on a DMZ, test access
4. Intrusion Detection System (IDS)
a. Monitor and interpret logs
b. Policy: record, alert, alarm
5. VPNs (Virtual Private Network)
a. In conjunction with firewalls
b. Encryption; encryption protocols
c. Create VPN policies and test
E. Different business models and appropriate solutions
1. Software firewalls for personal use
2. Hardware firewalls appropriate for Small Office/Home Office (SOHO)
3. Hardware firewalls plus additional devices for professional enterprises
F. Firewalls and digital signature authentication
1. Pass through to certificate server
2. Creates the ultimate level of security
G. Firewalls with built-in virus scanning
1. Virus scanning options
2. Set up a quarantine area
H. Installation of common firewalls
1. ZoneAlarm or other popular freeware host-based firewalls
2. Microsoft ISA server - set up for caching
3. Cisco ASA hardware device
4. Palo Alto Networks "Next Generation Firewalls"
5. Linksys or similar inexpensive device
6. Explore all the features of all devices

Lab Content

A. Lab access
1. Configure your computer to access the online lab
2. Connect to the lab server using Remote Desktop
3. Review the firewall operating system and accept the license
4. Configure a role for assistant administrator on the firewall
5. Create an account for yourself
6. Load and examine the baseline configuration
B. Basic interface configuration
1. Create security zones
2. Configure basic interface type
C. Perform basic Interface Management configuration
1. Create Interface Management configuration profiles
2. Configure Ethernet interfaces and subinterfaces with Layer 3 address
3. Configure DHCP
4. Create a virtual router
5. Create a Source NAT policy
D. Application identification

1. Create a security policy to allow basic internet connectivity and log dropped traffic
2. Enable application block pages
3. Create application filters and application groups
4. Configure destination NAT to allow FTP traffic to flow to your student desktop
E. Content identification
1. Configure security profiles
2. Create a security profile group
3. Associate security profiles and security profile groups to security policy
4. Generate a custom report
F. Decryption
1. Create a self-signed SSL certificate
2. Configure the firewall as a forward-proxy using decryption rules
G. User identification
1. Connect your firewall to a User-ID agent
2. Install a software User-ID agent on a Windows host
3. Configure the PAN-OS User-ID agent on the firewall
4. Configure a zone or the User-ID
5. Configure User-ID policies
H. VPN
1. Configure an IPsec tunnel to another student firewall
I. High availability
1. Set up an active/passive HA configuration
J. Administration and management
1. Configure log forwarding
2. Schedule an FTP log export
3. Create a certificate signing request (CSR)
4. Create a self-signed CA certificate
K. Interface configuration
1. Configure a Layer-3 sub-interface
2. Configure QoS
L. Layer 3 routing configuration
1. Configure OSPF
M. Application identification
1. Examine an HTTP GET request from Chrome with Wireshark
N. Content identification
1. Configure a data filtering profile
2. Configure a custom vulnerability signature
O. User identification
1. Configure a captive portal
P. GlobalProtect
1. Configure GlobalProtect portal and gateway
Q. High availability
1. Configure active/active HA with another student firewall

Special Facilities and/or Equipment

A. Access to a network laboratory with current Cisco network equipment host computers required to support the class.
B. A website or course management system with an assignment posting component (through which all lab assignments are to be submitted) and a forum component (where students can discuss course material and receive help from the instructor). This applies to all sections, including on-campus (i.e., face-to-face) offerings.
C. When taught via Foothill Global Access on the Internet, the college will provide a fully functional and maintained course management system through which the instructor and students can interact.
D. When taught via Foothill Global Access on the Internet, students must have currently existing email accounts and ongoing access to computers with internet capabilities.

Method(s) of Evaluation

Tests and quizzes
Written laboratory assignments
Final examination

Method(s) of Instruction

Lectures which include motivation for the architecture of the specific topics being discussed
In-person or online labs (for all sections, including those meeting face-to-face/on-campus), consisting of:
1. An assignment webpage located on a college-hosted course management system or other department-approved internet environment. Here, the students will review the specification of each assignment and submit their completed lab work
2. A discussion webpage located on a college-hosted course management system or other department-approved internet environment. Here, students can request assistance from the instructor and interact publicly with other class members
Detailed review of laboratory assignments which includes model solutions and specific comments on the student submissions
In-person or online discussion which engages students and instructor in an ongoing dialog pertaining to all aspects of designing, implementing and analyzing programs
When course is taught fully online:
1. Instructor-authored lecture materials, handouts, syllabus, assignments, tests, and other relevant course material will be delivered through a college-hosted course management system or other department-approved internet environment
2. Additional instructional guidelines for this course are listed in the attached addendum of CS department online practices

Representative Text(s) and Other Materials

Gilman, Evan, and Doug Barth. Zero Trust Networks, 1st ed.. 2019.

Types and/or Examples of Required Reading, Writing, and Outside of Class Assignments

A. Reading
1. Textbook assigned reading averaging 30 pages per week.
2. Online curriculum averaging 20 pages per week.
3. Online resources as directed by instructor though links pertinent to networking.
4. Library and reference material directed by instructor through course handouts.
B. Writing
1. Technical prose documentation that supports and describes the laboratory exercises that are submitted for grades.

Discipline(s)

Computer Science