

Computer Network Security

Minnesota State Community and
Technical College

Detroit Lakes Campus

Overview

- Philosophy
- Note on 2 year Colleges
- Certifications
- Program Courses
- CCDC
- Program Numbers
- Faculty
- Future
- Questions

Philosophy

- You cannot defend what you do not understand.
- The program is designed to train students to work in entry level jobs
 - Network security
 - Network administration

Philosophy (cont'd)

- Program is based in skills students need to be employed.
- Advisory Committee of Security and Network Administrators meet yearly to update curriculum

Note on 2 Year Colleges

- Students care about real world experience
- Education is focused on learning a job skill
- Vital for technical faculty to stay current in the field to maintain credibility

Certifications

- Microsoft
 - MCP
 - MCSA
 - MCSE
- Planet 3
 - CWNA
- CompTIA
 - Security+
 - Linux+
 - Server+
 - Network+
- Cisco
 - CCNA

Program Overview

- Associates of Applied Science (71 credits)
- Half of the degree is network administration
- Half of the degree is security administration

Program Objectives

- Design and maintain secure computer networks
- Recognize security breaches and implement countermeasures
- Develop a disaster recovery plan
- Demonstrate professional communication skills in relation to computer networking
- Demonstrate ethical skills in relation to computer security
- Evaluate current practices and recommend security measures
- Demonstrate need for policy in implementation of security

General Education

- GSWS 1102 Contemporary Career Search
- INTD 1104 Systems Administration
- ENGL 1101 College Writing I
- PHIL 1201 Ethics
- CSEC 1102 Careers in Information Systems
- PSYC 1200 General Psychology
- SPCH 1114 Intro to Public Speaking
- MN Transfer Electives (2 classes)
- CPTR1104 Intro to Computer Tech
- MATH 0090 Introductory Algebra

Networking Courses

- CPTR 1108 Cisco 1
- CPTR 2224 Linux I
- INTD 1104 Systems Administration
- CPTR 1118 Cisco 2
- CPTR 2272 Network Operating Systems
- CSEC 2202 Introduction to Wireless Networking
- CSEC 2204 Managing Directory Services
- CSEC 2216 Advanced Routing
- CSEC 2218 Disaster Recovery
- CPTR 2282 E-Mail Administration

Security Courses

- CSEC 1110
Fundamentals of IT
Security
- CSEC 2210 Security
Breaches &
Countermeasures
- CSEC 2212 Web Security
- CSEC 2222 Network
Security Design
- CSEC 2228 Network
Defense
- CSEC 2230 Computer
Forensics

Students are required to sign a statement of ethics

CSEC1110 Fundamentals of IT Security

- Course Objectives:
 - Identify the components of Information Systems Security (INFOSEC)
 - Explain Operations Security (OPSEC)
 - Discuss the components of Information Security
 - Employ the elements of Information Systems Security (INFOSEC)
 - Formulate security policies and guidance documents
 - Interpret legal issues within Information Security
 - Apply the concepts of risk assessment
 - Analyze the concepts of system life cycle management
 - Demonstrate the concept of trust
 - Employ the modes of computer operation
 - Analyze the roles of various organizational personnel
 - Apply the facets of Information Security

CSEC1110 Fundamentals of IT Security (cont'd)

- Book:
 - Security+ Guide to Network Security Fundamentals Second Edition – Course Technology; CSSIA Lab Manual
- Course Activities:
 - Students use some basic tools to get an overview of security
 - MBSA; Wireshark; IPSorcery; EBCD; Snadboy Revolution; Cain and Able
 - Write weekly papers on security vulnerabilities

CSEC 2210 Security Breaches & Countermeasures

- Objectives:
 - Describe threats to and vulnerabilities of systems
 - Perform risk management functions
 - Plan a security assessment using current practices
 - Perform a security assessment using current practices
 - Utilize current tools to assess network security
 - Conduct a penetration test using current practices
 - Employ information reconnaissance techniques
 - Conduct an IT audit using current best practices
 - Implement countermeasures for networks
 - Complete written documentation of threats
 - Evaluate methods of non-network methods to gain network access
 - Analyze methods attackers avoid detection
 - Conduct attacks on a controlled network
 - Demonstrate ethics

CSEC 2210 Security Breaches & Countermeasures (cont'd)

- Books:
 - Assessing Network Security - Microsoft Press (no longer in print); Network Security Assessment - O'Reilly; Microsoft VBSCRIPT Step by Step – Microsoft Press; CSSIA Lab Manual
- Course Activities:
 - 3 weeks on VBScript
 - 10 weeks on
 - Penetration Testing
 - Information gathering
 - Report generation
 - Hacking techniques
 - Defensive measures
 - 2 weeks on capture the flag

CSEC2212 Web Security

- Objectives:
 - Investigate current web technologies
 - Apply current web browser security best practices
 - Create web site virtual servers and directories
 - Manage web folders
 - Implement secure web communications with SSL
 - Troubleshoot web client connectivity
 - Implement effective logging
 - Employ web site authentication
 - Implement FTP server to current standards
 - Apply current best practices to secure an Apache web server
 - Apply current best practices to secure an IIS server
 - Install IIS following current best practices
 - Install Apache web server following current best practices

CSEC2212 Web Security (cont'd)

- Books:
 - Apache Security - O'Reilly; Microsoft IIS 6.0 Administrator's Pocket Consultant - Microsoft Press; Apache Phrasebook - O'Reilly
- Course Activities:
 - Students spend 7 weeks on securing Apache
 - Students spend 7 weeks on securing IIS
 - Certificates / SSL
 - Directory security
 - Browser security
 - Securing FTP

CSEC 2228 Network Defense

- Objectives:
 - Outline physical security measures to current best practices
 - Identify personnel security practices and procedures
 - Explain software security best practices
 - Outline network security
 - Describe administrative security procedural controls
 - Define cryptosecurity
 - Indicate proper key management procedures
 - Interpret transmission security models
 - Name the elements of TEMPEST security
 - Complete firewall planning and design to current best practices
 - Distinguish firewall cryptography strategies
 - Construct a packet filtering firewall

CSEC 2228 Network Defense (cont'd)

- Books:
 - Guide to Firewalls and Network Security Intrusion Detection and VPNs -Course Technology; Managing Security with Snort and IDS Tools - O'Reilly
- Course Activities:
 - Learn proper design of network defenses
 - Work with Cisco PIX
 - Build and configure a Snort system
 - Implement Proxies
 - Work with various personal firewalls
 - Complete a written proposal and presentation on firewalls

CSEC 2230 Computer Forensics

- Objectives:
 - Examine computer forensics as a profession
 - Explain the steps in a computer investigation
 - Evaluate current computer forensic tools
 - Employ proper procedures for processing crime and incident scenes
 - Apply digital evidence controls
 - Select the best data acquisition methods for each investigation.
 - Describe computer forensics analysis
 - Demonstrate procedures to recover image files
 - Employ standard procedures to perform network forensics
 - Use specialized e-mail computer forensics tools
 - Formulate report findings with forensic software tools
 - Examine disks of various file systems
 - Demonstrate proper e-mail investigation techniques

CSEC 2230 Computer Forensics (cont'd)

- Book:
 - Guide to Computer Forensics and Investigations
3rd Edition - Course Technology
- Course Activities:
 - Students use Windows tools:
 - FTK, WinHex, ProDiscover, Helix
 - Students learn to use Linux tools:
 - Autopsy, Sleuth, dd, Fubuntu
 - Required to write a report on starting up a forensic lab.

CSEC 2222 Network Security Design

- Objectives:
 - Identify components of network security planning
 - Describe components of systems life cycle management
 - Conduct a network vulnerability analysis using current best practices
 - Implement a computer network
 - Construct a secure network framework
 - Implement security countermeasures using current best practices
 - Demonstrate ability to secure a network client to current best practices
 - Demonstrate ability to secure network resources to current best practices
 - Demonstrate ability to secure network server to current best practices
 - Implement a DMZ

CSEC 2222 Network Security Design (cont'd)

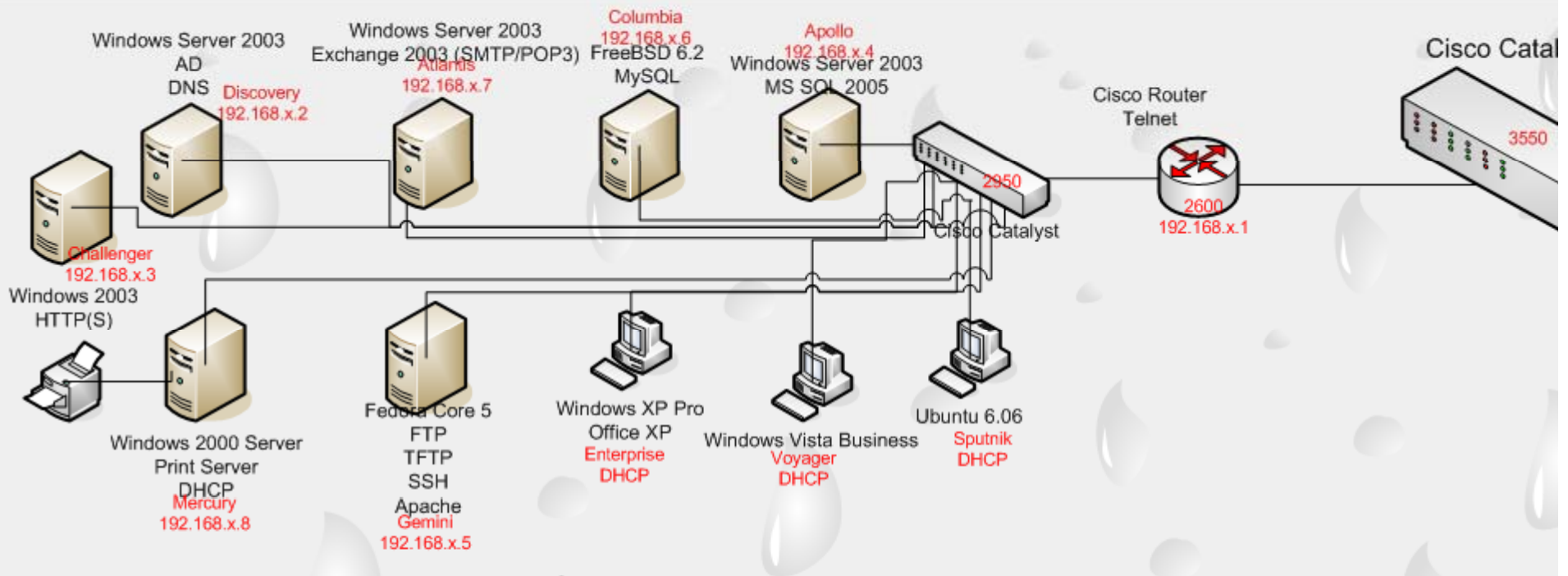
- Book:
 - MCSE Guide to Designing Security for a Microsoft Windows Server 2003 Network - Course Technology
- Course Activities:
 - Capstone course: students must use a technology learned in each class used in their education
 - 5 weeks on secure design
 - 6 weeks on building and securing their network
 - 4 weeks on conducting a security assessment on a different team's network
 - The building a assessment phases require a written report and presentation

CSEC 2222 Network Security Design (cont'd)

- **Capstone Project Requirements for 2008**
- **Provided Equipment**
 - 3 servers
 - 2 laptop
 - 2 Cisco 2500 router
 - 1 Cisco Switch
 - 1 Cisco 1232 Access Point.
- **Minimum System Requirements**
 - Active Directory
 - DNS
 - DHCP
 - Exchange 2003
 - Cisco Wireless
 - Cisco Router
 - Cisco Switch
 - Wireless client machine
 - IIS
 - Apache
 - FTP site

CCDC

- Collegiate Cyber Defense Competition
 - 8 students from the program on the team each year
 - 2007 and 2008 held at InverHills CC
 - <http://ccdc.minnesota.edu>



Inside Addresses

Team 1: 192.168.1.0/24

Team 2: 192.168.2.0/24

Team 3: 192.168.3.0/24

Team 4: 192.168.4.0/24

Team 5: 192.168.5.0/24

Team 6: 192.168.6.0/24

Outside Addresses

Team 1: 192.168.10.0/24

Team 2: 192.168.20.0/24

Team 3: 192.168.30.0/24

Team 4: 192.168.40.0/24

Team 5: 192.168.50.0/24

Team 6: 192.168.60.0/24

Domain Names

Team1.wolfclaw.local

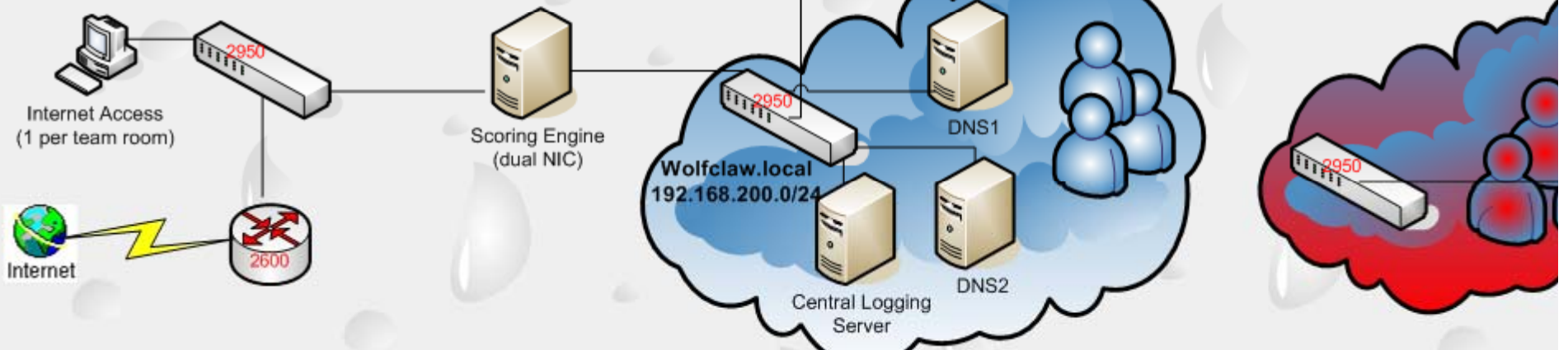
Team2.wolfclaw.local

Team3.wolfclaw.local

Team4.wolfclaw.local

Team5.wolfclaw.local

Team6.wolfclaw.local



Program Numbers

- Class of 2007
 - 11 Graduates
 - 3 continued education
 - 1 military (Army Info Sec)
 - 1 family business
 - 1 State of Montana
 - 1 Veterans Admin
 - 1 small business owner
 - 3 ISP
- Class 2008
 - 10 Graduates
 - 1 K-12 school
 - 3 Microsoft
 - 6 unknown at this time
- Class of 2009
 - 5 students
- Class of 2010
 - 21 students

Faculty

- Information Technology
 - 5 faculty
 - 1 Computer Network Security
 - 2 Web Development
 - 1 Computer Network Technology (Online degree)
 - 1 Help Desk Technician

Future

- Certificate in Computer Network Security
- Scheduled to be offered Spring 2009 (Online)
 - 4 classes
 - Web Security
 - Fundamentals of IT Security
or
Network Security
 - Security Breaches and Countermeasures
 - Network Defense
 - Enrollment controlled by interview with instructor

Future (cont'd)

- Pursuing CNSS 4011 and 4013 certification

Questions