

Network Security: Theoretical Concepts and Hands-On Analysis in a Laboratory Environment

Guevara Noubir

College of Computer and Information Science

Northeastern University

<http://www.ccs.neu.edu/course/csg254>

<http://www.ccs.neu.edu/home/noubir/Courses/CSG254/S05/>

Course Outline

- Course Goals and Structure
- Lectures
- Problems Sets
- Laboratory Setup and Assignments
- Competition

Course Goals and Structure

- Provide theoretical foundation and practical experience for designing and building secure networked systems
- Lab assignments and problem sets:
 - Small scale and focused experience with specific vulnerabilities and preventive measures
- Competition:
 - Two-day larger scale supervised and confined environment to test learned concepts and techniques

Grading Policy

- Problem Sets: 25%
- Midterm exam: 30%
- Lab Homework: 25%
- Competition: 20%
 - including report and pre-competition

- Lab HW: 6 assignments
 - only best 5 grades count

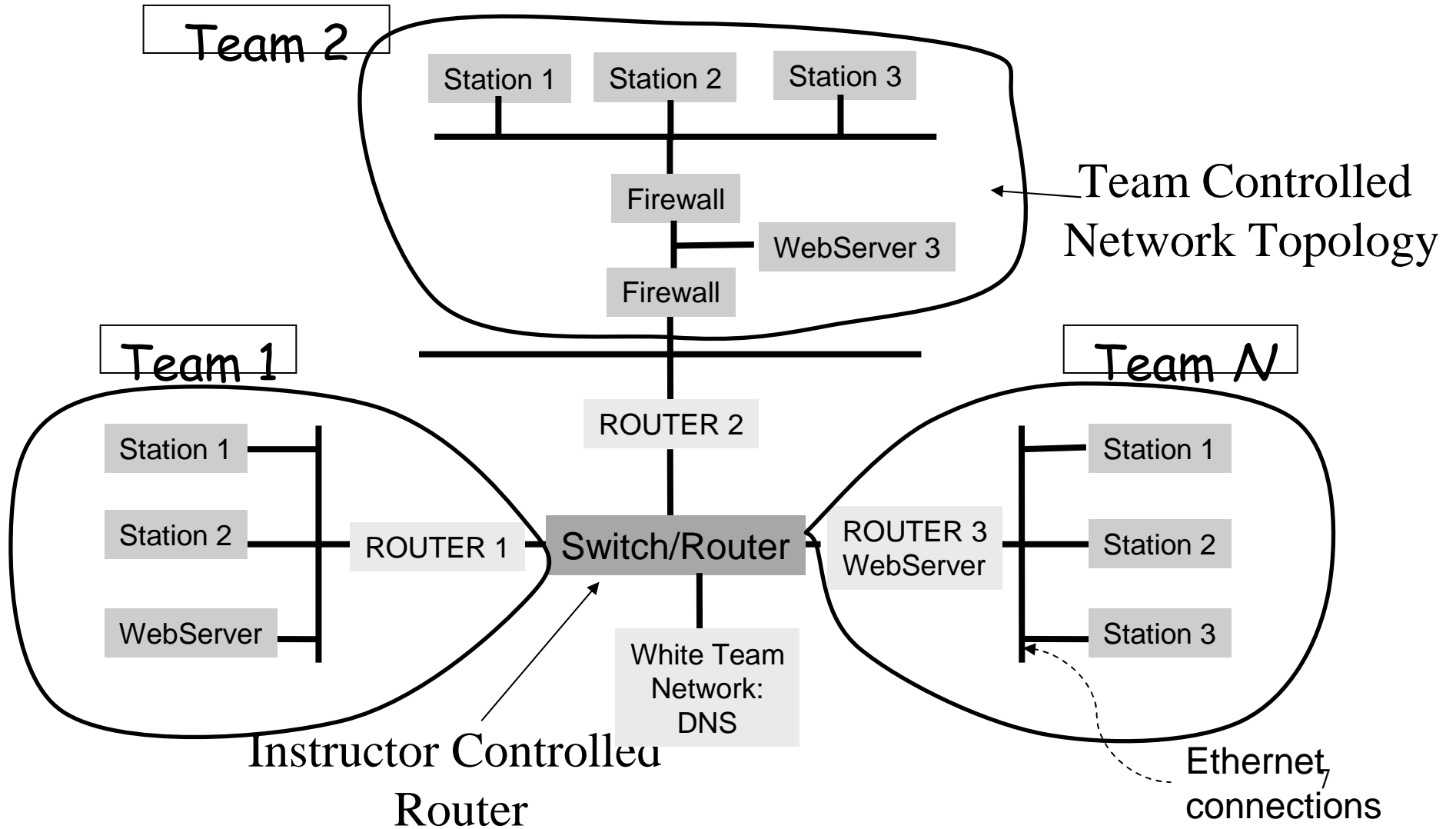
Lectures

- CSG254 is one of four courses in the security concentration area:
 - Cryptography, Software Security, Usability Privacy and Security
- Conceptual foundation of Network Security:
 - Review of Cryptographic Mechanisms
 - Review of Internetworking
 - Authentication Protocols
 - Security Standards: Kerberos, IPSec/IKE, SSL/TLS, PKI
 - Secure Applications: S/MIME, PGP, ssh
 - Secure Multicast, Sensor Networks
- One lecture (+ invited short presentations) on practical network security tools
 - Intrusion detection and vulnerability scanning

Problem Sets

- Goal:
 - Test theoretical concepts:
 - Example: analyze an authentication protocol
 - Put into practice theoretical concepts:
 - Design and implement a secure application
- Last year's application: Secure Instant Messaging
 - Discuss alternatives and tradeoffs:
 - Usability, trust in server, services (user-to-server authentication, user-to-user authentication, confidentiality, integrity), efficiency, weak password protection
 - Discuss known attacks on design: DoS, reflection, replay
 - Implement and Deploy
- Make the design document and source code available to all teams

Lab Setup



Lab Setup

- Each team is given:
 - Hardware: a set of PCs that can run Windows/Linux, hubs, CISCO router
 - Software: Windows, Linux, VMware (for multiple hosts emulation)
 - Other: subnet IP addresses (10.0.0.x)
- Each team designs its own network topology and can choose its favorite OS, and tools (e.g., IDS, VPN), use DMZ/firewalls...
- The team networks are interconnected through a router controlled by the instructor:
 - Audit and rate control the traffic
 - Isolate misbehaving teams
 - Emulate larger networks
- Machines with vulnerabilities placed on the network
- Green indicates planned but not 100% sure

Lab 1: Network and Host Setup

- Students are assigned a subnet and hardware
 - Install and configure Windows 2000 system to spec
 - Install and configure RedHat Linux system to spec
 - Demonstrate network connectivity and service deployment

Lab 2: Scans and Probes

- Attacker Tools and Preventative Measures
 - DNS Zone Transfers and preventing information leaks
 - Scanning Hosts with NMAP and network discovery tools, trade-offs with limiting ICMP traffic
 - UNIX and Windows Enumeration Techniques and hardening systems to limit information disclosure
 - SMB, SNMP Enumeration
 - Vulnerability Scanners and how they work (helpful to administrators too!)
- Tools Used
 - Dig, Traceroute, NMAP, Finger, NBTScan, Legion, Solar Winds IP Network Browser, Nessus

Lab 3: Network-Based Attacks and Password Cracking

- Attacker Tools and Preventative Measures
 - Network Sniffing, Secure Protocol Replacements
 - Sniffing on Switched Networks, ARP Spoofing
 - Securing a Website
 - Common Email Insecurities
 - DNS Spoofing, IP Spoofing, MITM, and Session Hijacking Attacks
 - Password Auditing on UNIX and Windows Systems, Password Policies and Enforcement
- Tools Used
 - TCPDump, Ethereal, Dsniff, FragRouter, ArpWatch, LC4, John the Ripper, DumpSec, OpenSSL, HTPasswd

Lab 4: Firewalling, Intrusion Detection, and Denial of Service

- Attacker Tools and Preventative Measures
 - Rudimentary Routing setup to accommodate reconfigured switch settings (students gain experience using either a Cisco 1700-series router or a dual-interface Linux system)
 - Stateful Firewall configuration and rule tweaking
 - DoS Discussion: Syn Floods, Smurfs, DDoS, prevention
 - IDS Installation, analysis of attack traffic, and custom rule creation
 - IDS Evasion techniques used by attacks, pre-processor use, fragmentation re-assembly: trade-offs
- Tools Used:
 - IPTables or Cisco IOS Access-Lists/Inspects Rules, Snort, ACID

Lab 5: Remote/Local Exploits and Compromised Servers

- Attacker Tools and Preventative Measures
 - Buffer Overflows discussion, example exploit analysis
 - Secure coding practices, how to “fix” the exploitable application provided to the class (included learning about SUID programs and the use of Chroot Jails)
 - Analysis of well-known Remote/Local exploits, prevention
 - Detecting RootKits and Backdoors with TripWire
 - Covert Channels and the difficulty of detection
- Tools Used:
 - Custom Overflow Exploit, IIS-Koei, PipeUpAdmin, Subseven, TripWire, Backdoored SSHd, Reverse WWW Shell

Competition Goals

- The main goal is to get a hands-on experience with securing networks and deploying secure applications
 - Design and configure a secure and reliable network in a practical setting
 - Define user policies for network usage
 - Protect against known network vulnerabilities
 - Practice network penetration tools and techniques
 - Learn how to quickly react to new security threats
 - Tradeoffs between offered services and security
 - Deploy a self-designed secure application

Three Scenarios

- Scenario 1:
 - Each team has its own network: no insider attacker
- Scenario 2:
 - Each team has its own network + one user account on other teams networks
- Scenario 3:
 - Each team has its own network + one compromised machine on other teams networks
- Require a wireless component?

Rules

- Teams are allowed to configure their own networks and choose their OS
 - At least one windows and one linux machine
 - Teams are allowed to setup honeypots/honeynets
- Teams are given a traffic quota to avoid flooding based DoS
 - This quota will be enforced by the interconnection router
- Attacking the white team network is forbidden
- Social engineering is allowed to break-in other teams
- The services (defined in services slide) should be provided

Services

- Webservice
- Anonymous ftp server
- SSH
- SMB, NFS, MySQL
- User accounts for each team and white team
- Secure Instant Messaging Application
 - The documentation and code made available from the webservice main webpage.

Scoring

- Since the goal is to learn how to protect a network:
 - More points for successfully protecting a network
 - High penalty for not protecting against simple known attacks
 - In order to generate a competition environment points are given when successfully breaking into other networks
- Services are periodically scanned (~10 min)
 - Nessus plugins
- Teams submit a report documenting:
 - Discovered theoretical attacks on application design
 - Vulnerabilities in other teams networks and how they can be exploited and protected
 - Evidence of exploited vulnerabilities

Competition Phases

- Pre-competition
 - Week 10 [5% of final grade]
- Final competition
 - Week 14 [15% of final grade]