

EET 354

Microcomputer Security

Instructor: Professor Kilgore
Office: 402 Whalin Complex
E-mail: E-mail: jeff.kilgore@eku.edu

Lecture/lab/demonstration: MW 8:00 - 09:50 a.m.
Prerequisite: EET 303
Credit: 3 credit hours.

Intended Audience: Those persons having some knowledge concerning microcomputers and local area networks and desiring a basic understanding of network security. This would be an excellent course for the person that is wanting to perform basic network security audits and implementing basic network security. The course participant will be given the opportunity to conduct basic network security audits and implement basic hardware and software network security.

General description: The intent of this course is to provide the participant with current information as to the relevant characteristics of network security as implemented in network hardware and software, in home and office environments, on networks utilizing Windows 9x, Windows 2000, Windows XP, Windows 2003, Linux and or a combination of the aforementioned operating systems.

Textbooks/ Resource (s) :

Exam Cram2 Security+
Anti-hacker Tool Kit
WWW...!!!!!!
Handouts

University Disability Statement: If you are registered with the Office of Services for Individuals with Disabilities, please make an appointment with the course instructor to discuss any academic accommodations you need. If you need academic accommodations and are not registered with the Office of Services for Individuals with Disabilities, please contact the office on the third floor of the Student Services Building, by e-mail at disabilities@eku.edu or by telephone at (859) 622-2933 V/TDD. Upon individual request, this syllabus can be made available in alternative forms

Attendance: You are expected to attend each lecture and lab. If you miss a test you should inform the instructor beforehand and provide a written, valid excuse. Each absence in excess of two will reduce your final grade by one letter.

NOTE: Quizzes cannot be made up.

EET 354

Microcomputer Security

Grading:

You are expected to complete all reading and lab assignments. Your grade will be determined as follows:

1. Three tests each worth 100 points.
2. Four brief research reports on current LAN and PC security topics each worth 5 points. NOTE: These reports must be developed utilizing a word processor, and be based on computer communications journals published in 2005/6.
3. Labs will be worth 5 points each.
4. Quizzes - vary in point value and will be given as needed.

Tentative Exam Schedule:

Test 1 02/08
Test 2 03/08
Final University Exam Schedule

Grading scale:

| | |
|-----------|---|
| 94 - 100% | A |
| 85 - 93 | B |
| 70 - 84 | C |
| 60 - 70 | D |
| < 60 | F |

NOTE: Quizzes cannot be made up

Progress Report. Each student must make an appointment with the instructor following each test. The student and the instructor will discuss the students progress in the course and if needed ways to improve the students performance.

Last Withdraw Date: March 10, 2006

Instructor Access.... very easy! Welcome to 2006 my e-mail address is jeff.kilgore@eku.edu
I will check e-mail at least once a class weekday. I will attempt to answer your problems by e-mailing back an answer or if the question is of value to the class I will answer the question in class. Technology is great!

Objectives:

Upon successful completion of this course the participant will be able to :

EET 354

Microcomputer Security

- A. Identify and to a relative extent rectify the common security flaws in Windows 9x.
- B. Identify and to a relative extent rectify the common security flaws in Windows 2000.
- C. Identify and to a relative extent rectify the common security flaws in Windows XP.
- D. Identify and to a relative extent rectify the common security flaws found in Network application programs. (IIS, IE, FTP servers, etc..)
- E. Identify and to a relative extent rectify the common security problems found with common network hardware. (Copper wire, fiber, wireless, hubs, switches, routers, etc..)
- F. Identify and to a relative extent rectify the common security problems found with common network management "features" wake on LAN, wake on ring, etc...
- G. Identify common viruses and implement anti virus programs and precautions in Windows 98, 2000 XP, 2003.
- H. Be able to conduct a security audit.
- I. Be able to setup and manage a network monitor.
- J. Be able to install and manage encryption software.
- K. Identify, download, install and configure a fire wall in a Windows network.
- L. Install, configure and manage a hardware router.
- M. Install, configure and manage a hardware fire wall.
- N. Install, configure and manage security on a wireless network.

Topical Outline:

- I. Foot printing scanning

EET 354

Microcomputer Security

A. General concepts.

- B. How is scanning done?
- C. How can one defend.
- D. Implementation & Troubleshooting.

II. Enumeration.

- A. General concepts.
- B. How is enumeration done?
- C. How can one defend?
- D. Implementation & Troubleshooting.

III. Securing W 9x

- A. General concepts.
- B. Testing the OS.
- C. Defending the systems?
- D. Defense is basically impossible.
- E. What is left?

IV. Securing the Windows NT family.

A. Securing NT

- 1. General concepts.
- 2. Testing the OS.
- 3. Defending the systems?
- 4. Implementation & Troubleshooting.

B. Securing 2000

- 1. General concepts.
- 2. Testing the OS.
- 3. Defending the systems?
- 4. Implementation & Troubleshooting

EET 354

Microcomputer Security

C. Securing XP

1. General concepts.
2. Testing the OS.
3. Defending the systems?
4. Implementation & Troubleshooting

D. Securing 2003

1. General concepts.
2. Testing the OS.
3. Defending the systems?
4. Implementation & Troubleshooting

V. Internet security.

- A. General concepts.
- B. Testing Internet security.
- C. Defending the systems?
- D. Implementation & Troubleshooting

VI. Novell security.

- A. General concepts.
- B. Testing Novell security.
- C. Defending the systems?
- D. Implementation & Troubleshooting

VII. Linux security.

- A. General concepts.
- B. Testing Linux security.
- C. Defending the systems?
- D. Implementation & Troubleshooting

EET 354

Microcomputer Security

VIII. Network devices security

- A. General concepts.
- B. Testing device security.
- C. Defending the systems?
- D. Implementation & Troubleshooting

IX. WAN Routers / Encryption

- A. General concepts.
- B. Testing WAN routers and encryption.
- C. Defending the systems?
- D. Implementation & Troubleshooting

X. Cisco Routers

- A. General concepts.
- B. Testing Cisco devices security.
- C. Defending the systems?
- D. Implementation & Troubleshooting

XI. Wireless networks.

- A. General concepts.
- B. Testing wireless network security.
- C. Defending the systems?
- D. Implementation & Troubleshooting

XII. Certification

- A. Why certification
- B. Certification content.

EET 354
Microcomputer Security

Tentative time schedule.

- Week 1** Foot printing Scanning
- Week 2** Enumeration Windows 95/98/ME multiple security problems.
- Week 3** Securing the Windows NT family
- Week 4** Securing the Windows NT family.
- Week 5** Securing the Windows NT family
- Week 6** Windows 2003 services security / Conducting security audits.
- Week 7** Internet security
- Week 8** Novell security
- Week 9** Linux security
- Week 10** Network devices security
- Week 11** Routers / Encryption
- Week 12** Cisco Routers
- Week 13** Securing wireless networks.
- Week 14** Securing wireless networks.
- Week 15** Certification review