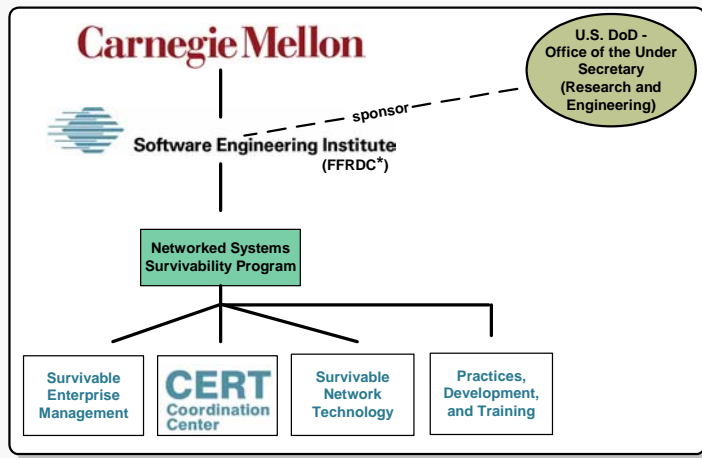


This course combines lecture, demonstrations, scenario exercises, and hands-on laboratories which are designed to introduce technical staff to information security and to provide a solid foundation for further learning in the field.

Who We Are



*FFRDC - Federally Funded Research and Development Center

© 2002 Carnegie Mellon University

Introduction - slide 2

This slide depicts the current structure of the SEI's Networked Systems Survivability program.

For more detailed information see:

www.sei.cmu.edu and www.cert.org



Intended Audience

Network/System Administrators with about 3 years of technical experience


Relatively New to the field of Information Security

Prerequisite knowledge

- General familiarity with data networking to include:
 - OSI 7-Layer Model
 - Ethernet
 - TCP/IP Suite
 - Some knowledge/experience with Windows and Unix

This course is intended for technical staff members who manage or support networked information systems. Three years of practical experience with networked systems or equivalent training/education is assumed, however the intended audience should be relatively new to information security.


In general, students should have some familiarity with the concepts of data networking. They should have some degree of specific familiarity with the ISO/OSI 7-layered reference model as well as Ethernet, TCP/IP, and major network operating systems such as Windows NT/2000/XP and Unix.



Networked Systems Survivability

Logistics, etc.

- Restrooms
- Breaks
- Catering
- Cell Phones/Pagers, etc.
- Directions/local area
- Local Calls
- Course Materials
- Using the Lab equipment
 - What's Available?
 - What's Appropriate?



© 2002 Carnegie Mellon University Introduction - slide 4


Please raise any concerns you may have regarding course logistics with the instructor.



Course Objectives

- Describe the components of Survivability
- Identify and define the components of an Information Security (IS) Model
- Describe the components of Risk and Asset management as applied to networked systems
- Identify the benefits of invoking sound security policies and methods for implementing them
- Describe the steps of the SkiP methodology
- Summarize key security concerns of the TCP/IP protocol suite
- Describe the benefits of cryptography when applied to IS properties of confidentiality, integrity, and availability
- Describe common information gathering attack methods
- Identify threats and attacks that can compromise IS properties
- Describe best practices for hardening and actively defending host and networked systems from intrusions

At the end of this course, students should be able to do the above objectives.



Overview of Course Content

| | |
|-----------|---------------------------------------|
| Module 1 | The Challenge of Survivability |
| Module 2 | Asset and Risk Management |
| Module 3 | Policy Formulation and Implementation |
| Module 4 | Security Knowledge in Practice |
| Module 5 | TCP/IP Security |
| Module 6 | Cryptography |
| Module 7 | Prelude to a Hack |
| Module 8 | Threats, Vulnerabilities, and Attacks |
| Module 9 | Host System Hardening |
| Module 10 | Securing Network Infrastructure |
| Module 11 | Deploying Firewalls |
| Module 12 | Securing Remote Access |
| Module 13 | Intrusion Detection Systems |

© 2002 Carnegie Mellon University

Introduction - slide 6

The course is broken down into 13 modules of instruction and they are listed above. In general, the course starts out with some of the high-level concepts and issues in the field and gets progressively more technical as it goes on.

Course Schedule

| MONDAY | TUESDAY | WEDNESDAY | THURSDAY | FRIDAY |
|---------------------|---------------------|---------------------|----------------------|----------------------|
| 0900 - Course | 0900 - Mod 5 | 0900 - Mod 8 | 0900 - Mod 10 | 0900 - Mod 12 |
| Intro/Overview | 1045 - Break | 1030 - Break | 1030 - Break | 1000 - Break |
| 0930 - Mod 1 | 1100 - Mod 6 | 1045 - Mod 8 | 1045 - Mod 10 | 1015 - Mod 12 |
| 1045 - Break | 1200 - Lunch | 1200 - Lunch | 1200 - Lunch | 1115 - Mod 12 |
| 1100 - Mod 2 | 1300 - Mod 6 | 1300 - Mod 8 | 1300 - Mod 10 | (Lab) |
| 1200 - Lunch | 1400 - Break | (Lab) | (Lab) | 1200 - Lunch |
| 1300 - Mod 3 | 1415 - Mod 6 | 1345 - Break | 1345 - Break | 1300 - Mod 13 |
| 1415 - Break | (Lab) | 1400 - Mod 9 | 1400 - Mod 11 | 1415 - Break |
| 1430 - Mod 4 | 1500 - Mod 7 | 1500 - Break | 1500 - Break | 1430 - Mod 13 |
| 1530 - Break | 1600 - Break | 1515 - Mod 9 | 1515 - Mod 11 | 1530 - Break |
| 1545 - Scenario | 1615 - Mod 7 | 1615 - Mod 9 | 1615 - Mod 11 | 1545 - Mod 13 |
| Exercises | (Lab) | (Lab) | (Lab) | (Lab) |
| 1700 - END | 1700 - END | 1700 - END | 1700 - END | 1700 - END |

The course will proceed (for the most part!) as depicted above.



R.O.E./Introductions

R.O.E

- Learn from each other and actively participate
- Share your knowledge/experience
- Ask Questions—if you know the answer, shout it out!
- Get your hands dirty
- Try something new (OS, Tools, etc.)
- PLEASE critique the course—so it always gets better!

Introductions

- Name, Position, Tech Experience, Expectations of Course

© 2002 Carnegie Mellon University

Introduction - slide 8

Following the above recommended rules of engagement will help to optimize student and instructor learning. Please attempt to fill in the Course Critique and feedback form as each module is completed.