INLS 690-263: Information Security and Assurance (Practical Elements of Information Security Assessment)

Course Summary

Hands-on, practical review of current security tools and concepts. Using a fictional company profile, students will walk through a complete security review of a small company from soup to nuts, using each area as an excuse to delve into security technology and management and connecting technical reviews of packets and software to the IT processes that control them. Students should leave comfortable with the use of common security tools, with identifying and prioritizing the risks present in an IT system, and with presenting their findings to a non-technical audience.

Audience

Course will cover a survey of information security topics similar to INLS490-248, but aimed at the MSIS graduate student who is expected to be more proficient in and more focused on specific technical topics in information systems security.

Requirements

Students should meet have basic familiarity with the following topics:

- Elementary concepts of IP addressing
- Use of the Linux command line
- Virtualization software such as VMware Workstation or VirtualBox.

Students will require a working computer for class and/or assignments, but may run MacOS, Windows, or Linux as desired.

Assignments

Tech

We will have periodic technical, hands-on assignments in the form of projects to complete. These won't be weekly: instead, you'll get a full package that will be due roughly every two to three weeks, and you'll need to keep up.

Writing

As a technology professional, you'll be expected to stay abreast of new developments in technology and security, and to be able to explain these to non-technical*less technical people. To that end, you will be doing a series of /short* weekly writing assignments (seriously, I mean short). Each week, you need to pick a significant development in security: a new vulnerability, a new research finding, a new product announcement or open-source project, etc. In about a page, you should explain this new topic to the CEO of our imaginary company, Tarheel Electronics. Here are some things she'll want to know:

- What is this thing, in non-technical language?

- Why is this important or significant?
- Does this affect our company? Could it affect us? Is it a positive or negative impact, and how big?
- How could this affect our company?

This should take you *approximately one page* to explain, give or take[0], and I'm looking for quality over quantity, with a hard limit of one page. CEOs are busy people!

Schedule

Class will meet for three hours once per week. Students will be expected to complete assignments outside of class that will typically include a technical portion and a writing portion.

Week 1

Class

- Introduction
- Course Walkthrough and Expectations
- Security Concepts
  - CIA Triad
  - Risk/Threat Calculus and Prioritization
  - Information Security Audit and Assessment

Homework

Technical

(Start working on project 1)

Writing

First writing assignment

Week 2 [Host Security]

Class

- Patching
- Security Baselines and Hardening
- Reviewing System Security Controls
- System Security Management: Whose Job?

Homework

Technical Project 1

- Install VMware Workstation/VirtualBox (your choice) on your computer.
- Install and configure two Linux virtual machines for class using the profiles supplied in homework 1 directions.
- Successfully test connectivity to and between virtual machines.
- Run `yum update` and the CI Security benchmark tool on your Linux server.
- Run scans against your Linux server using `nmap` and `OpenVAS`.

Review the information you just gathered. Select a subset of the information you collected

and provide a summary of the threats presented by each element. Prioritize the risks presented by those threats into recommendations: what would you recommend resolving first, and how quickly?

Writing

Second writing assignment

Week 3 [Host Security]

Class

- Access Control Concepts: AuthC and AuthZ
- Access Management Models: RBAC, DAC, and friends
- System Access Methods
- System Access Controls

Homework

Technical

Review the corporate profile for TarHeel Electronics as provided with the course materials. Given the personnel information provided, outline a set of system access roles and profiles that would meet the stated requirements while satisfying the requirement of minimized/least-privilege access.

Writing

Third writing assignment

Week 4 [Host Security]

Class

- Anti-malware measures on hosts: from antivirus to anti-rootkit
- Containing services: chroot, jails, containers, VMs
- Attack prevention: memory and stack protection

Test: OS Security concepts

Homework

[Reading TBD]

Writing

Fourth writing assignment

Week 5 [Network Security]

Class

- Network Layout, Design, and Addressing for Security
- Choke Points and Redundancy
- Perimeters and Access Control: Closing the Holes

Homework

Technical

(Start work on project 2)

Writing

Part 1: Review the network access diagram provided for TarHeel Electronics. Identify the

access points and choke points on the diagram. Consider the threat presented by the different points you identified and present an analysis of risks involved, remembering to consider Confidentiality, Integrity, and Accessibility.

Part 2: Consider the OS security concepts we covered in weeks 1-4. What elements introduced in that section would apply to the network equipment in scope here?

Week 6 [Network Security]

Class

- Firewall Concepts: ACLs to Statefulness
- Modern Firewalling Technologies and Developments

[Hopefully, we'll have a guest speaker in the second hour on firewall developments, management, and technologies.]

Homework

Technical

Run an `nmap` scan against your Linux server and collect the results. Activate `firewalld` on your Fedora server, using the instructions provided in the homework 6 materials. Run a new `nmap` scan against the server: what changes are you seeing? Turn off the SSH server service using the homework instructions, and run one final `nmap` scan: what difference do you see now?

Week 7 [Network Security]

Class

- TCP/IP Fundamentals
- Network Packet Analysis: Finding your way around tcpdump and Wireshark

Homework

Technical

Load the packet dumps included with the homework 7 materials into Wireshark and examine the headers and packet contents. What types of sessions are these? What sorts of things are you seeing? (You may need to spend some time researching the ports and protocols involved in order to identify what you're looking at.)

Week 8 [Network Security]

Class

- Network Security Tools: From IDS to Deep Packet Inspection

[Hopefully we'll have a guest speaker in the second hour on modern network security technologies, attack detection, and incident response management]

Homework

Technical

Activate Bro IDS on your Fedora server using the instructions provided with the homework 8 materials. Using one of the tools on your attack VM such as `nmap`, run a scan against the Linux server with Bro active.

Writing

Part 1: Review the output of the Bro IDS alerts on the console. What attacks did it detect? Is there anything it didn't see?

Part 2: Consider the network diagram for TarHeel Electronics provided with the class materials. Provide at least two different locations for IDS on this map, and discuss the advantages and disadvantages of each placement.

Week 9 [Network Security]

Class

- Wireless Security: 802.11, WAP, and WPA
- Network Security Management: Whose Job?

Test: OS Security concepts

Homework

[Reading TBD]

Writing

Writing assignment

Week 10 [Data Security]

Class

- Data Access: Revisiting AuthC and AuthZ
- Data Classification: The Perennial Problem
- Security in Transport: SSL and TLS introduced

Homework

[Reading TBD]

Technical

Review the contents of your browser and operating system trust stores using the instructions provided in the homework 11 materials. What's different about the contents of each trust store? What's common?

Writing

Part 1: Examine the entry requirements for the Mozilla, Microsoft, and Apple trust stores. What's different about each and what do they share? Why might each have different trust requirements?

Part 2: Looking at the differing lists of trusted CAs you collected, what might not need to be there for your daily work? How difficult would it be to manage that for a company, and what pitfalls might occur as a result of modifying those trust lists?

Week 11 [Data Security]

Class

- SSL & TLS Continued: Understanding PKI
- Whom do you trust and why?

Homework

Technical

Using the instructions included with the week 10 materials, create a certificate authority in your Linux server VM and issue yourself a certificate. Using the instructions for `openssl`, collect the certificate authority chain for a trusted website online.

Writing

Part1: Compare the contents of the certificate you have to one from a trusted website online using the instructions for looking at certificate contents with `openssl`. What differences do you see in the root CA certificates and the end-entity certificates?

Part 2: Considering what we know about TarHeel Electronics, would you recommend they purchase certificates from a known CA, operate their own CA, or a mixture of the two for different functions? Provide your best estimates for costs and risks for each as a comparison.

Week 12 [Data Security]

Class

- Encryption at Rest: Introduction to PGP/GPG
- Further Encryption-at-rest technologies: Veracrypt, Bitlocker, FileVault
- Data Security: Whose Job?

Homework

Technical

Generate a GPG key-pair using the instructions in the homework 12 materials, and upload your public key to the key-servers as specified, then import Jos's public key. Select a file from the class materials, encrypt it to Jos, and then sign it with your public key. Verify the signature on the file, and then email it to Jos.

Writing

Look over the process for creating your GPG key and encrypting the file to Jos. How difficult would a process like this be for a small company like TarHeel Electronics to manage for protecting files over email? What about other transfers not involving email? What tools might make it easier to manage this technology?

Week 13 [Final Wrap-up]

TarHeel Technologies: The 50,000 Foot Overview

Homework

[Reading/Writing TBD]

Footnotes

[0] Assuming reasonable document defaults: one-inch margins, 12-point non-monospaced font, single or 1.5-line spacing.