Course Materials

Kali Linux and Ubuntu downloads

Kali Linux has a few variants:

ISO images for writing to USB: https://www.kali.org/downloads/

Virtual images for VirtualBox or VMware: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

Ubuntu is currently at version 18.04.x: https://www.ubuntu.com/download

Note: DETER already has versions of Kali, BackTrack (former name of Kali), and Ubuntu that you can use.

VirtualBox can be found here: https://www.virtualbox.org/

Complementary readings

Here students will find a list of complementary (more in-depth) readings for each assigned chapter.

Chapter 1 Overview

Anderson, J. Computer Security Threat Monitoring and Surveillance. Fort Washington, PA: James P. Anderson Co., April 1980.

Chapter 2 Cryptographic Tools

Schneier, B. "Why Cryptography is Harder Than It Looks." Information Security Bulletin, 1997.

Chapter 3 User Authentication

Wagner, D., and Goldberg, I. "Proofs of Security for the UNIX Password Hashing Algorithm." Proceedings, ASIACRYPT '00, 2000.

Chapter 4 Access Control

Sandhu, R. "Lattice-Based Access Control Models." Computer, November 1993.

Barkley, J. "Comparing Simple Role-Based Access Control Models and Access Control Lists." Proceedings of the Second ACM Workshop on Role-Based Access Control, 1997.

Bell, D. "Looking Back at the Bell-Lapadula Model." Proceedings, 21st Annual IEEE Computer Security Applications Conference, 2005.

Mackenzie, D., and Pottinger, G. " Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the U.S. Military." IEEE Annals of the History of Computing, Vol. 19, No. 3, 1997.

Chapter 5 Database Security

Griffiths, P., and Wade, B. "An Authorization Mechanism for a Relational Database System." ACM Transactions on Database Systems, September 1976.

Chapter 6 Malware

Levine, J.; Grizzard, J.; and Owen, H. "A Methodology to Detect and Characterize Kernel Level Rootkit Exploits Involving Redirection of the System Call Table." Proceedings of the Second IEEE International Information Assurance Workshop, 2004.

Chapter 8 Intrusion Detection

Anagostakis, K., et al. "Detecting Targeted Attacks Using Shadow Honeypots." 14th USENIX Security Symposium, 2005.

Allen, J., Christie, A., Fithen, W., McHugh, J. and Pickel, J. State of the practice of intrusion detection technologies. Technical Report CMU/SEI-99-TR-028. Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 2000.

Chapter 9 Firewalls

Ioannidis, S. "Implementing a Distributed Firewall." ACM CCS '00, 2000.

Guster, D "A Firewall Configuration Strategy for the Protection of Computer Networked Labs in a College Setting." Journal of Computing Sciences in Colleges, October 2001.

Chapter 10 Buffer Overflow

Levy, E., "Smashing The Stack For Fun And Profit." Phrack Magazine, file 14, Issue 49, November 1996.

Chapter 11 Other Software Security Issues

Miller, B.; Cooksey, G.; and Moore, F. “An Empirical Study of the Robustness of MacOS Applications Using Random Testing.” First International Workshop on Random Testing. Portland, Maine, ACM, 2006.

Chapter 12 OS Security

Jiang, X., and Solihin, Y "Architectural Framework for Supporting Operating System Survivability" IEEE
Computer Architecture, 2011.

Chapter 20 Symmetric Encryption

Blaze, M., et al. "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Securi
RFC 1750 Randomness Recommendations for Security. December 1994.

Chapter 21 Public-Key Cryptography

Asymmetric Encryption: Evolution and EnhancementsCryptobytes Volume 2, No. 1 - Spring 1996.

Chapter 22 Internet Security

Neuman, B. "Security, Payment, and Privacy for Network Commerce." IEEE Journal on Selected Areas in Communications, October 1995.

Chapter 23 Internet Authentication

Yu, T., et al. "The Perils of Unauthenticated Encryption: Kerberos Version 4." Proceedings of the Network and Distributed System Security Symposium. The Internet Society, February 2004.

Chapter 24 Wireless Network Security

Welch, D., and Lathrop, S. "Wireless Security Threat Taxonomy." Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2003.

Complementary writing

Students get to practice writing with the following quick exercises related to the weekly reading assignments:

Chapter 1 Overview

1.1 Compare and contrast the different approaches to characterizing computer security in Sections 1.3 and 1.4.

Chapter 2 Cryptographic Tools

2.1 Briefly summarize what you know about the field of cryptography.

2.2 List seven questions or things you don't know about cryptography. For each question you list, indicate why it might be important to know the answer.

2.3 Describe situations in your life when you might need to use encryption or secret codes. How important would it be to have enough understanding of the subject of cryptography to assess the strength of the code you used?

2.4 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 3 User Authentication

3.1 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 4 Access Control

4.1 Which do you think is harder to understand: DAC or RBAC? Explain.

4.2 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 5 Database Security

5.1 Prepare a one-paragraph objective summary of the main ideas in this chapter.

5.2 Evaluate the chapter you have just read. What more do you think you need to know on this subject, or what aspects of this subject are not clear to you?

Chapter 6 Malware

6.1 List seven questions or things you don't know about keeping a computer system secure from malicious software. For each question you list, indicate why it might be important to know the answer.

6.2 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 7 & Mirkovic Chapters 1-6 Denial of Service

7.1 Prepare a one-paragraph objective summary of the main ideas described here.

7.2 Which of the main topics described here do you think is hardest to understand? Explain.

Chapter 8 Intrusion Detection

8.1 List seven questions or things you don't know about keeping a computer system secure from intruders. For each question you list, indicate why it might be important to know the answer.

8.2 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 9 Firewalls

9.1 Summarize what you know at this point about firewalls. What points or questions would you like to discuss further?

9.2 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 10 Buffer Overflow

10.1 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 11 Other Software Security Issues

11.1 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 12 OS Security

12.1 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 20 Symmetric Encryption

20.1 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 21 Public-Key Cryptography

21.1 Summarize the cryptographic algorithms available at http://www.bouncycastle.org/index.html. What do you think of the selections they have made? Is this a useful service? Explain.

21.2 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 22 Internet Security

22.1 Briefly summarize what you know about the use of cryptographic techniques for securing Internet protocols and applications.

22.2 Describe what you think are the most important requirements for secure use of the Internet.

22.3 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 23 Internet Authentication

23.1 Prepare a one-paragraph objective summary of the main ideas in this chapter.

Chapter 24 Wireless Network Security

24.1 Prepare a one-paragraph objective summary of the main ideas in this chapter

CSAW CTF 2019

The annual Capture The Flag contest North American edition will take place Nov 6-9, 2019 at NYU Tandon School Cyber Security Awareness Week (CSAW).

Think you can hack? Show off your skills in a worldwide competition. Work as an individual, or work as a team (hint: it's better as a team).

Qualifications are due September 13, 2019 at the link provided.