Learning Penetration Testing

with Lisa Bock

LEARNING

Hyperlinks for each chapter

Note: Links may change or be unavailable over time.

Chapter 1. Organizational Penetration Testing

01_01. Understanding penetration testing

- To view a visual of malware, ransomware, phishing, and intrusion attacks around the world that have transpired in a 24-hour window, visit the SonicWall Live Cyber Attacks Map

01_02. Auditing security mechanisms

- No links

01_03. Managing risk

- No links

01_04. Analyzing risk

- Visit https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/ for a discussion on how to conduct a risk assessment
- Learn more about the Security Risk Assessment (SRA) tool, a way for an organization to proactively evaluate their organization, by visiting here: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

01_05. Recognizing the attack surface

- For a more in-depth discussion of attack vectors, visit: https://www.cloudflare.com/learning/security/glossary/attack-vector/
- For a visual of a live threat map, visit: https://threatbutt.com/map/
- Learn more about the human attack surface: https://elevatesecurity.com/blog-what-is-human-attack-surface-management/

Chapter 2. Types of Penetration Testing

02_01. Comparing different environments

- No links

02_02. Checking from the outside in

- No links

02_03. Looking Inside the organization

- For some fun Easter eggs:
- Go to https://www.google.com/ and type **Do a Barrel Roll** in the search box
- Open Firefox and type **about:robots**
- Open a new Word doc, type **=rand(5,10)**, and then press enter

02_04. Determining testing methods

- No links

02_05. Discovering penetration testing tools

- One powerful suite of tools is Kali Linux; find a premade virtual machine for either VMware or VirtualBox here: https://www.osboxes.org/kali-linux/
- To find a list of reconnaissance tools, visit: https://www.firecompass.com/blog/top-10-tools-for-reconnaissance/
- Ethical hackers use a variety of tools when testing; learn more here: https://www.softwaretestinghelp.com/penetration-testing-tools/
- Learn about Nmap, an open-source tool for network discovery and security auditing, by visiting: https://nmap.org/
- In addition to scanners, the ethical hacker will use a variety of password cracking tools; find a list of the 10 most popular tools here: https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/

02_06. Challenge and solution: Explain the NIST five framework core functions

The publications in the NIST Special Publications (SP) 800 series were developed to address and support the security and privacy needs of US federal government information and information systems. They are freely available and can provide a ton of valuable information. Learn more here: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

If you'd like to share this information with your team, go to https://www.nist.gov/cyberframework/online-learning/components-framework and scroll down to the bottom where you will find the PowerPoint file for the cybersecurity framework.

Chapter 3. Penetration Testing Techniques

03_01. Following a structured plan

- No links

03_02. Planning the penetration test

- No links

03_03. Footprinting the target

- No links

03_04. Escalating privileges

- No links

03_05. Attacking the system

- No links

03_06. Delivering the results

- No links

03_07. Outlining remediation strategies

- Learn more about penetration testing remediation by visiting: https://www.emagined.com/blog/penetration-testing-remediation-faqs
- For details on how to maintain PCI DSS compliance, visit: https://www.pcisecuritystandards.org/documents/PCI_DSS_V2.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf

Chapter 4. Penetration Testing Blueprint

04_01. Checking physical security

- To learn how to connect to a secure wireless network from a computer or other device using Wi-Fi Protected Setup (WPS), visit: https://www.sony-asia.com/electronics/support/articles/00022337

04_02. Identifying wireless vulnerabilities

- Visit https://www.endoacustica.com/signal-jammers.php to see some examples of portable signal jammers

04_03. Testing the website

- To see the results of a simple scan, go to https://hostedscan.com/openvas-vulnerability-scan and scan example.com

04_04. Leaking data via email or VoIP

- To demonstrate what you might hear when eavesdropping, go to https://wiki.wireshark.org/VoIP_calls and select SampleCaptures/rtp_example.raw.gz and extract the file

04_05. Safeguarding cloud services

- Learn more about NIST 800-53 compliance for containers and Kubernetes by visiting: https://sysdig.com/blog/nist-800-53-compliance/

- Payment Card Industry Data Security Standard (PCI-DSS) outlines requirements for multi-tenant service providers (cloud environment) in Appendix A1 found here: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf

04_06. Assessing the mobile infrastructure

- Learn how to secure your mobile device by visiting: https://www.networksolutions.com/blog/resources/ebooks/how-to-secure-mobile-devices-from-common-vulnerabilities

04_07. Hacking the human

- No links

Chapter 5. Outsourcing Penetration Testing

05_01. Contracting the penetration test

- No links

05_02. Defining the project scope

- No links

05_03. Hiring consultants

- During the penetration test, the team may need to test cloud resources; visit https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-cloud-need-know/ for an example on what restrictions might be in place

05_04. Agreeing on terms

- No links

05_05. Creating the contracts

- To learn more about the master service agreement (MSA), visit: https://avokaado.io/blog/master-service-agreement/

Conclusion

06_01. What’s next

- To see a list of courses on my homepage, visit: https://www.linkedin.com/learning/instructors/lisa-bock?u=2125562