UNIT 23: Conducting Security Testing & Assessments

Estimated Time in Hours: 12

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
7 Risk 1 Ethics 6 Adversarial Thinking	6.2	- Investigate common security testing tools.

Guiding Questions:

- Why are security testing and assessments important?
- What forces threaten security?
- How are security resources allocated?
- What are common security testing tools?
- How can they be abused?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
6.2 EU: Adversarial thinking is the process of reasoning about how opposing forces could prevent a system from meeting both its functional and security goals. 6.2.1 LO: Students will know how natural events and unintentional errors can cause a system to fail. 6.2.1a EK: Cyber systems are susceptible to disruption and destruction from natural disasters; for example, flooding, earthquakes, and hurricanes.	• Computer, lecture slides, projector, graphic organizers, access to Internet • "6 Scenarios for Business Continuity Plan Testing." Agility Recovery, *AgilityRecovery.com*, 16 Sep 2019, https://www.agilityrecovery.com/7-scenarios-for-business-continuity-plan-testing/	• Failing to plan is planning to fail. Have students explain this saying. • Give students an ABC brainstorm page. Using it, they should list all the things, starting with each letter of the alphabet, that can damage a system. Examples: A = adversary, B = botnet, C = criminals. Students can work together if you wish. Have them share their answers. Did any of them list natural disasters? • List types of natural disasters on the board. Have students brainstorm ways each can harm a system. How do these disruptions impact confidentiality, integrity, and availability?

6.2.1b EK: Disaster planning includes provisioning for the confidentiality, integrity and availability of cyber systems during natural disasters. 6.2.1c EK: Disaster planning includes prevention, detection, and response and recovery. 6.2.1d EK: Natural event and unintentional errors typically do not adapt in response to defenses.		• Explain to students that cybersecurity experts have to plan for natural disasters as well as other threats to a system. This is called disaster planning. Disaster planning includes prevention, detection, and response to recovery. Stress that human life should always be a priority. • Discuss the need for business continuity plans. These outline how an organization stays operational during a disruption. Disaster recovery outlines how a business will get up and running after a disaster (typically another location). The source linked left can assist with this. If time allows, have students examine sample business continuity plans and disaster recovery plans. Templates for these are freely available on various websites.
7.1.5 LO: Students will understand the trade-offs between cybersecurity benefits and the total cost of cybersecurity protections. 7.1.5a EK: The outcome of a risk assessment should prioritize what needs to be remediated. 7.1.5b EK: If the data or resources cost less or are of less value than their protection,	• "Choosing a Higher Level of Assurance." *YouTube*, uploaded by KirkpatrickPrice, 18 July 2019, https://www.youtube.com/watch?time_continue=8&v=Sfawv5dP8TQ&feature=emb_logo	• Show students a picture of an inexpensive television. Tell students that an attacker plans to steal the television. How could they protect it? After students strategize, have them come up with the cost of protecting the television. Did the cost of securing it exceed the cost of the asset? If so, is protecting it a good idea? • Stress to students that assets can also have value that exceeds the cost of the technology. For example, data stored on a laptop may be worth thousands (or even millions) of dollars. That data would merit protecting the laptop.

adding security mechanisms is not cost effective. 7.1.5c EK: The level of protection is a function of the attack occurring and the effects of the attack should it succeed.		• Risk management is risk identification, risk assessment, and risk control. • Review risk assessments with students (see previous units). Remind students that risk assessments help determine what kind of controls show be in place. • Audits determine if controls exist (compliance) and if they are functioning to an acceptable level (adequacy). Explain that there are many types of audits (IS, compliance, financial, operational, integrated, administrative, specialized, computer forensic, and functional. The short video linked left gives a brief overview of an audit.
7.1.4 LO: Students will be able to conduct standard security testing and assessments. 7.1.4a EK: Vulnerability assessment identifies known vulnerabilities on the system. 7.1.4b EK: Known vulnerabilities can be found in databases that collect, maintain, and disseminate information. 7.1.4c EK: There are various automated vulnerability scanning tools, which are used for pinpointing vulnerabilities and	• Barnett, Patrick. "Vulnerability Scanning vs. Penetration Testing." Secureworks, *Secureworks.com*, 20 Dec 2017, https://www.secureworks.com/blog/vulnerability-scanning-vs-penetration-testing • Network Scanners: ○ ipconfig/ifconfig/ip (cmd) ○ ping and arp (cmd) ○ nmap (tool) • Service Discovery: ○ netstat (cmd)	• Explain to students that there are different types and scopes of security assessments. However, most require reconnaissance, security posture assessment, vulnerability scanning or penetration testing, and interviewing. • Note that vulnerabilities can be found in databases that collect, maintain, and distribute information. Have students list examples of these databases. • Note that vulnerability tests can be found using tools. Review/cover these tools (network scanners, DNS harvesting, fingerprinting/sniffing software, wireless scanner/crackers). Discuss passive versus active scanning and false positives/false negatives. Also note that scans can be credentialed or non-credentialed. See list to the left. The source linked to the left also provides notes and further resources. **It is up to the teacher to determine the**

providing remediation for these vulnerabilities. 7.1.4d EK: Not all vulnerabilities can be exploited and not all vulnerabilities need to be mitigated. 7.1.4e EK: Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.	○ nmap (tool) • Fingerprinting: ○ nmap (tool) ○ traceroute (cmd) • Banner/OUI Grabbing ○ nmap • Sniffer & Protocol Analyzers ○ Wireshark • Nadhori, Isbat Uzzin. "Modul 2 | Footprinting Scanning Enumeration." Insitut Teknologl Sepuluh (ITS), https://studylib.net/doc/9262668/modul-2---footprinting-scanning-enumeration • Site: "Onine Banking Login." Altoro Mutual (test website published by IBM), http://www.testfire.net/login.jsp • Web Application Report: https://www.ibm.com/developerworks/community/blogs/48a78681-82cc-434f-9c78-	**maturity of the student in introducing these resources. Teachers should work with their school's IT team before having students use these tools on a school's system.** • Introduce honeypots and honeynets. Note that they assist in identifying and analyzing attacks and act as decoys. • Ask students if all vulnerabilities can be exploited. Why not? Ask students if all vulnerabilities need to be mitigated. Why not? • Define the term penetration test. Have students do a Venn diagram comparing/contrasting a vulnerability scan to a penetration test. Students can use the source linked left to help with this. • Note that before doing a penetration test, a pen tester should obtain written consent from the company and any related vendors, such as the Internet service provider. Additionally, the pen tester should outline the rules of engagement. This includes defining the perimeter, any restrictions, the attack profile (black, white, gray), the environment and timing, how to disclose results, and confidentiality requirements. Pen testers should understand that the legality of pen testing varies from country-to-country and may require end user warning or other documentation. • Pen testing includes reconnaissance (open source intelligence, social engineering, and scanning), initial

	3e9117bfd466/resource/demo.testfire.netSecurityReport.pdf?lang=en • Solutions: "How to hack www.testfire.net." *LSABlog.com*, 21 May 2017, https://www.lsablog.com/networksec/penetration/how-to-hack-www-testfire-net/	exploitation, persistence, escalation of privilege and pivot, and action on objectives. The site and resources linked left are related to a demonstration of a weak site. **Teachers may allow students to experiment on this site; however, teachers should stress that the skills students practice should be limited to this site and should only be done under supervision. Other sites (hackthissite.org and owasp.org/www-project-webgoat/ also offer avenues for supervised student practice.**
1.2.2b EK: Security tools were designed to help system administrators and users to improve security, but an adversary can use the same tools to exploit the target for nefarious goals.		• Note that the same tools used by network administrators to find weaknesses in a system can also be used by adversaries. Have students brainstorm how this can be the case.
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.		• Explore a career, such as exploitation analyst or IT auditor