Title	Vulnerability Analysis
Long Title	Vulnerability Analysis
Credits	**5**
NFQ Level	Expert
Module Author	Dr George D O'Mahony

Module Description:

A vulnerability assessment analyst performs assessments of systems and networks within the network environment and identifies where those systems/networks deviate from acceptable configurations. This module will provide the learner with the necessary knowledge and tools to find and understand vulnerabilities before attackers can exploit them and to use appropriate tools and resources. On completion, the learner will be able to conduct assessments of threats and vulnerabilities, determine deviations from acceptable configurations, assess the level of risk and develop and/or recommend appropriate mitigation countermeasures. This module was developed under the Cyber Skills HCI Pillar 3 Project. Please refer to the consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Critically evaluate and classify current and emerging vulnerabilities in computer systems.
LO2 Appraise and configure the tools and techniques used for conducting vulnerability scans to recognize vulnerabilities in computer systems.
LO3 Conduct a vulnerability assessment of a computer system and use analysis tools to categorize the vulnerabilities and potential exploits/attacks that may not be identified using scanning techniques.
LO4 Examine the results of the vulnerability scans and analysis tools to determine insights about a computer systems threat environment and identify false positives and highly exploitable vulnerabilities.
LO5 Critically assess and report on the results of a vulnerability assessment with the aim of evaluating an organization's preparedness against security attacks.

Indicative Content

Vulnerabilities

Cyber threats and vulnerabilities. Definition and comparison to exploitation, a threat and an attack. Threat landscape (organization's threat environment), attacker profiles and attacker motivations. Different types of vulnerabilities - hardware, software, human, configuration and policy. Vulnerability databases – CVE Details, NIST National Vulnerability Database, CERT – Vulnerability Notes Database and Exploit Database. Vulnerability scoring - CVSS scores. Recognizing and categorizing types of vulnerabilities and associated attacks. System and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). What constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. Classify current and emerging vulnerabilities.

Vulnerability Scanning Tools

Tools to be used -Nessus and OpenVAS. What is a vulnerability scanner? How do vulnerability scanners find and report vulnerabilities? Selecting a vulnerability scanning tool. What assumptions (if any) are made when scanning? How to install these tools on Kali Linux. Navigation and scan types (Network-based scanners, Host-based scanners, Wireless scanners, Application scanners, Database scanners, cloud-based), Scanning, scanning a Web application. Conduct vulnerability scans and recognize vulnerabilities in security systems. Conduct application vulnerability assessments. External vs Internal vulnerability scans, Authenticated vs. Unauthenticated vulnerability scans. Quantifying and ranking the found vulnerabilities.

Analysis Tools

Using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc). Applying fuzzing techniques and tools to a binary with a view to discovering exploitable vulnerabilities. Common network vulnerabilities and exploitation options (Outdated Or Unpatched Software Firewall/Operating System Misconfigurations). Using network analysis techniques to identify vulnerabilities. Tools include Wireshark, Nmap, metasploit. What is the difference between network/host vulnerability assessment and web-based assessments? Common web-based vulnerabilities such as the OWASP Top 10 and their exploits. Assessing websites and finding vulnerabilities. Spidering, scanning, fingerprinting web servers. Using tools such as OWASPZap, Burp Suite, DirBuster, Nikto, Metasploit. Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

Vulnerability Analysis

Analyze vulnerability scan results to: share meaningful insights about the context of an organization's threat environment, improve risk management posture, identify false positives, identify highly exploitable vulnerabilities, hypothesise potential attacks on an organisation. How to use the results of vulnerability scans to measure an organization's preparedness for security attacks. Establish efficient vulnerability management strategies. Assess vulnerability scans of a system/host/network/web application to identify deviations from acceptable configurations or policy Drawing up a detailed vulnerability assessment report. Providing a strategy for vulnerabilities remediation and mitigation. Linking vulnerabilities to potential attacks.

Vulnerability Assessment

What is a risk assessment? What is a vulnerability risk Assessment? How to perform impact/risk assessments. The importance of conducting a vulnerability assessment. The Defined Process (Planning and design, configuration, scanning, analysis and reporting) to identify weaknesses in the environment, provide insights into degrees of risk from each vulnerability and produce recommendations on how to mitigate the vulnerability. Vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	The learner will use the tools and techniques used by a vulnerability assessment analyst to perform assessments of web and network computer systems to identify deviations from acceptable configurations or policy. This will be assessed through a project consisting of the setup, process and completion of a vulnerability assessment.	1,2,3	40.0	Week 7
Project	The learner will use the techniques used by a vulnerability assessment analyst to analyse the results of a vulnerability assessment to evaluate a computer system's preparedness for security attacks. This will be assessed through a project consisting of vulnerability scan analysis, including both network and web application results.	4,5	60.0	Sem End

No End of Module Formal Examination

Assessment Breakdown	%
Coursework	100

Re-Assessment Requirement

Coursework
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	Workload Description	Hours	Frequency	Average Weekly Leaner Workload
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.0	Every Week	3.0
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Workload – Part Time

Workload Type	Workload Description	Hours	Frequency	Average Weekly Leaner Workload
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.0	Every Week	3.0
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Recommended Book Resources

- *Sagar Rahalkar 2018, Network Vulnerability Assessment: Identify security loopholes in your network's infrastructure, Packt Publishing [ISBN: 9781788627252]*

Supplementary Book Resources

- **Daniel W. Dieterle 2018, Basic Security Testing with Kali Linux 3, Third Ed., CreateSpace Independent Publishing Platform [ISBN: 9781725031982]**
- **Prakhar Prasad 2016, Mastering Modern Web Penetration Testing, Packt Publishing [ISBN: 9781785284588]**
- **Peter Kim 2018, The Hacker Playbook 3: Practical Guide To Penetration Testing, Secure Planet LLC [ISBN: 9781980901754]**
- **Simon Parkinson Andrew Crampton Richard Hill 2018, Guide to Vulnerability Analysis for Computer Networks and Systems, Springer [ISBN: 9783319926230]**
- **Al Sweigart 2020, Automate the Boring Stuff with Python, 2nd Ed., No Starch Press [ISBN: 9781593279929]**