7.3.2 Vulnerability Scoring System Facts

This lesson focuses on vulnerability scoring systems. In the United States, the Department of Homeland Security has a color-coded advisory system that signifies levels of potential threat to our citizens. This gives those who are working to protect us direction on how quickly to act and what efforts to make to keep us safe. Similarly, there is a scoring system in place for IT security threats to organizations and businesses called the Common Vulnerability Scoring System (CVSS).

This lesson covers the following topics:

- Common Vulnerability Scoring System
- CVSS calculator
- Government resources
- Non-government resources

Common Vulnerability Scoring System

This scoring system creates a way to organize and prioritize vulnerabilities that you look for and discover in your work as an ethical hacker. Because this scoring system is nationally and internationally recognized, using it will give you credibility when you present your findings and plan of action for remediation.

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
-	-	None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
-	-	Critical	9.0-10.0

CVSS Calculator

A CVSS calculator can determine the risk and severity of a vulnerability based on the three metrics described in the following table:

Metric	Description
Base	Denotes a vulnerability's unique characteristics.
Temporal	Denotes the changeable attributes of a vulnerability.
Environmental	Denotes vulnerabilities that are present only in certain environments or implementations.

Government Resources

The US government through the Department of Homeland Security has sponsored five valuable resources for ethical hackers.

Resource	Description
Common Vulnerabilities and Exposures (CVE)	The CVE is a list of standardized identifiers for known software vulnerabilities and exposures. It is free to use, and it is publicly available at cve.mitre.org. Benefits of this system include the following: ▪ There are currently 94 CVE Numbering Authorities from 16 countries providing a baseline for evaluation. ▪ The identifiers provide standardization, which allows data exchange for cybersecurity automation. ▪ This list aids in determining the best assessment tools. ▪ The CVE list supplies the National Vulnerability Database.
National Vulnerability Database (NVD)	The National Vulnerability Database (NVD) was originally created in 2000. It can be found at nvd.nist.gov. The NVD list: ▪ Includes detailed information for each entry in the CVE list, such as fix information, severity scores, and impact ratings.

	▪ Is searchable by product name or version number, vendor, operating system, impact, severity, and related exploit range.
Computer Emergency Response Team (CERT)	CERT is a government agency. Its website is www.us-cert.gov. The government site provides: ▪ Information exchange ▪ Training and exercises ▪ Risk and vulnerability assessments ▪ Data synthesis and analysis ▪ Operational planning and coordination ▪ Watch operations ▪ Incident response and recovery
Common Weakness Enumeration (CWE)	CWE is a community-developed list of common software security weaknesses. Its website is cwe.mitre.org. The CWE strives to create commonality in the descriptions of weaknesses of software security. This creates a reference for identification, mitigation, and prevention of vulnerabilities. This list provides a standardization for evaluating assessment tools. This site combines the diverse ideas and perspectives from professionals, academics, and government sources to create a unified standard for cybersecurity.
Common Attack Pattern Enumeration & Classification (CAPEC)	CAPEC is a dictionary of known patterns of cyber attack used by hackers. Its website is capec.mitre.org. This list is searchable by mechanisms of attack or domains of attack, as well as by key terms and CAPEC ID numbers. This resource is valuable because you can browse through it to see common attacks used by hackers, and you can search for specific patterns of attack.

Non-Government Resources

Two non-government sites also provide valuable information for the ethical hacker.

Resources	Description
JPCERT	JPCERT is Japan's CERT organization. It provides security alerts and Japanese Vulnerability Notes (JVN). The website is www.jpcert.or.jp/english/vh/project.html. This site provides detailed information about each vulnerability, including: ▪ Affected products ▪ Possible impacts ▪ Solutions ▪ Vendor statements ▪ Reference documents
Full Disclosure	Full Disclosure is a mailing list from nmap. Its website is seclists.org/fulldisclosure. This mailing list often shows the newest vulnerabilities before other sources. This list gives researchers the right to decide how they will disclose the vulnerabilities they discover. It is also a source of events of interest for the security community.