RISK LESSON

Nancy Stevens – First Flight High School, Kill Devil Hills, NC

This material is based upon work supported by
the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

RISK

NATIONAL VULNERABILITY DATABASE ACTIVITY

Instructions: Go to the National Vulnerability Database at https://nvd.nist.gov/. Once there, explore the site in order to answer these key questions.

KEY QUESTIONS

Answer the following questions:

TRUE OR FALSE

1. True or False (circle one): The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.

MULTIPLE CHOICE

2. The NVD is a provided and sponsored by two of these three organizations. Which one does NOT provide/sponsor the NVD?
   a) NIST Computer Security Division, Information Technology Laboratory
   b) Department of Homeland Security's National Cyber Security Division
   c) National Security Agency

3. CVSS stands for the Common _____ Scoring System.

   a) Valuation
   b) Verification
   c) Vulnerability

4. Select which of the following statements is False and write in the correct answer(s).

   a) The base CVSS score include impact, exploitability and temporal components.
   b) The base score goes from 0 – 100.
   c) The exploitability metric includes: attack vector, attack complexity, privileges requires, user interaction, and scope.
   d) The impact metric includes: confidentiality, integrity, availability, and authentication.

The correct answer(s):

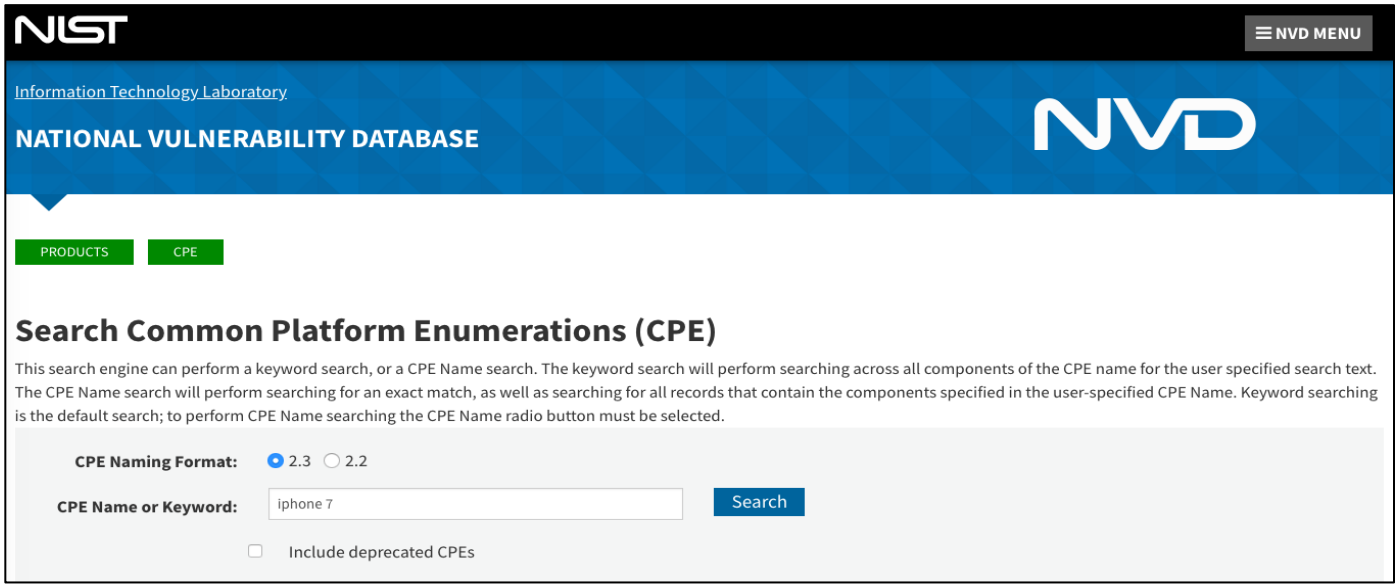
5. Which statement describes the purpose of the Common Platform Enumeration (CPE) dictionary?

a) The CPE is a subscore derived from the base CVSS score.
b) The CPE provides an agreed upon list of technology to uniquely identify vulnerable products.
c) The CPE is a list of vendors participating in the NVD.
d) The CPE provides a common language for explaining the cause of vulnerabilities.

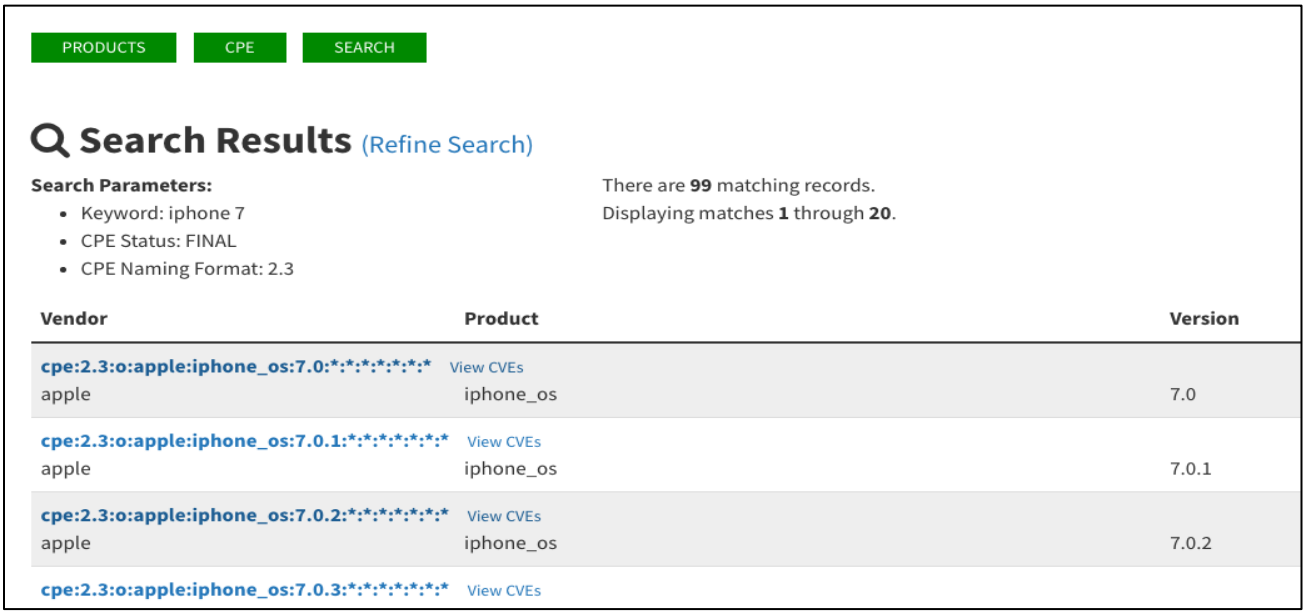
SEARCH PRODUCTS

Now go to the search engine , select Products – CPE, put in the name of one of the devices that you listed on the Asset Classification Activity.

For example, type in "iPhone 7" as the product as shown in the figure below.



Here is a screenshot of the results when you type in "iPhone 7" as the product.



PRODUCTS CPE SEARCH

Search Results (Refine Search)

Search Parameters:

- Keyword: iphone 7
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are **99** matching records.
Displaying matches **1** through **20**.

Vendor	Product	Version
cpe:2.3:o:apple:iphone_os:7.0:*:*:*:*:*:*:* View CVEs		
apple	iphone_os	7.0
cpe:2.3:o:apple:iphone_os:7.0.1:*:*:*:*:*:*:* View CVEs		
apple	iphone_os	7.0.1
cpe:2.3:o:apple:iphone_os:7.0.2:*:*:*:*:*:*:* View CVEs		
apple	iphone_os	7.0.2
cpe:2.3:o:apple:iphone_os:7.0.3:*:*:*:*:*:*:* View CVEs		

Scroll through the vulnerabilities and read about them. Select one and report the following things about it here:

CVE Number			
Overview:			
CVSS Severity		CVSS Impact	

CVSS Base Score		CVSS Exploitability Score	

Now circle each of the follow ratings for exploitability and impact:

Base Score Metrics	
Exploitability Metrics	Impact Metrics
Attack Vector (AV) Network Adjacent Network Local Physical	Confidentiality Impact (C) None Low High
Attack Complexity (AC) Low High	Integrity Impact (I) None Low High
Privileges Required (PR) None Low High	Availability Impact (A) None Low High
User Interaction (UI) None Required	
Scope (S) Unchanged Changed	

Now go to the "Search Vulnerability Database", select Vulnerabilities – CVE, and research CVE-2019-11510

CVE Number	CVE-2019-11510		
Analysis Description:			
CVSS Severity Score		CVSS Impact Subscore	

CVE Number	CVE-2019-11510		
CVSS Base Score		CVSS Exploitability Subscore	

Now circle each of the follow ratings for exploitability and impact:

Base Score Metrics	
Exploitability Metrics	Impact Metrics
Attack Vector (AV) Network Adjacent Network Local Physical	Confidentiality Impact (C) None Low High
Attack Complexity (AC) Low High	Integrity Impact (I) None Low High
Privileges Required (PR) None Low High	Availability Impact (A) None Low High
User Interaction (UI) None Required	
Scope (S) Unchanged Changed	