Concept Review /w Bloom's Taxonomy Verbs

1. Networking

1.1. OSI Model

1.1.1. Create new connections using Layers 3 and 4 of the OSI model.

1.1.2. Apply conceptual knowledge of Static and Dynamic port forwarding to communicate with networked devices.

1.1.3. Evaluate networking information to determine how best to interact with new machines.

1.1.4. Design static ssh forward tunnels to maneuver through the network.

2. Reconnaissance

2.1.1. Use command line tools to discover hosts on a subnet

2.1.2. Use command line tools enumerate ports on a host

2.1.3. Interpret data from host discovery and port enumeration to determine the best method of interacting with a target host and port.

3. Web Exploitation

3.1.1. Identify a web server and its most likely location on a Linux server.

3.1.2. Understand the difference between client and server side scripts

3.1.3. Apply knowledge of HTTP request methods to interact with a web server

3.1.4. Use advanced functionality of a network scanner to enumerate web directories

3.1.5. Demonstrate the ability to interact with enumerated web directories

3.1.6. Interpret HTML source code

3.1.7. Appraise a web server for the best method to obtain terminal access.

4. SQL

4.1.1. Understand how HTML and PHP interact to run SQL queries

4.1.2. Understand String Literals in SQL and how they are formatted.

4.1.3. Demonstrate knowledge of SQL syntax to generate valid UNION SELECT queries

4.1.4. Demonstrate knowledge of SQL syntax to generate valid queries

4.1.5. Demonstrate knowledge of SQL injection to inject 1=1 into a valid SQL query

4.1.6. Demonstrate knowledge of SQL injection to test if a database is vulnerable to SQL UNION Attacks

4.1.7. Assemble an SQL injection to enumerate a database using ANSI standard information schema information.

4.1.8. Examine the contents of a database to determine what information is of value.

5. Reverse Engineering

5.1.1. Understand the difference between Windows and Linux executable file formats

5.1.2. Demonstrate the ability to understand assembly language

5.1.3. Examine an executable using a debugger to determine program flow and expected input/output

5.1.4. Demonstrate the ability to use Static and Dynamic analysis to analyze a program.

5.1.5. Determine what the excepted input of a binary is

6. Exploit Development

6.1.1. Determine how many characters are required to overflow a programs allocated stack frame in order to reach the calling function's next instruction on the stack

6.1.2. Determine what function in a C++ program are vulnerable using command line tools and open source information.

6.1.3. Perform a stack based buffer overflow to read a file

7. Linux

7.1. System Architecture

7.1.1. Determine critical locations of interest on a Linux operating system in regards to system enumeration

7.2. Privilege Escalation

7.2.1. Demonstrate knowledge of Linux command line tools to locate executables vulnerable to privilege escalation

SUID and GUID

SUDO

7.2.2. Evaluate binaries which might be vulnerable to privilege escalation and apply the appropriate technique to escalate privileges

7.3. Logging

7.3.1. Determine what programs, if enabled, might warrant further investigation.

rsyslog

7.4. Permissions

7.4.1. Break down the Linux access rights model.

7.4.2. Analyze Linux permissions in numerical form

7.4.3. Analyze file and folder permissions on the command line using default tools

7.4.4. Determine SUDO, SUID, and GUID permissions on binaries from the command line

7.4.5. Appraise Linux binaries for exploitation and successfully exploit them.

7.5. Host Enumeration

7.5.1. Remember default Linux user directory and configuration file locations

7.5.2. Demonstrate the ability to use command line tools to enumerate users, directories, groups, ports, and processes

7.5.3. Demonstrate the ability to find items from the Linux command line

7.5.4. Appraise host information for data that will further mission objectives

8. Windows

8.1. Privilege Escalation

8.1.1. Analyze a Windows computer to find a location where privilege escalation can occur.

8.1.2. Create a DLL and transfer it to a target system to exploit a vulnerable executable.

8.2. Persistence

8.2.1. Evaluate a Windows system to find locations where persistence may be configured

8.2.2. Determine how persistence is being has been established on a Windows system

8.3. Logging

8.3.1. Determine what Windows Command Line interface is set to log

8.4. Host Enumeration

8.4.1. Analyze a Windows computer to find a location where privilege escalation can occur.

8.4.2. Demonstrate the ability to use command line tools to enumerate users, directories, groups, ports, processes, and registry keys

8.4.3. Demonstrate the ability to use the graphical user interface to enumerate users, groups, ports, processes, and registry keys