**PERPLEXING –THE ETHICAL HACKING COMPETITION**

1. What would you call a person that uses his skills for defensive purpose?

A) Phreaker B) Cracker C) Hacker D) Ethical Hacker

2. A grey hat hacker is defined as:

A) A hacker with a split personality. At times, this individual will not break the law and might help to defend a network. At other times, they revert to illegal and malicious hacking.

B) A hacker who perform ethical hacking activities using their abilities to increase the security posture of information systems and defend them from malicious attacks

C) A hacker who conducts unethical and illegal attacks against information systems to gain unauthorized access to sensitive information.

D) None of the above.

3. Security Professionals often time refer to the tenets of Security. Some books and publications has 3 elements listed as the tenets. Within the CEH curriculum there are 4 tenets on which security rests, what are those 4 tenets?

A) Confidentiality, Integrity, Accounting, Authenticity B) Complexity, Integrity, Availability, Authenticity

C) Confidentiality, Integrity, Availability, Authenticity D) Confidentiality, Integrity, Availability, Authorization

4 .How do you call someone who aims at bringing down critical infrastructure for a cause while not worrying about facing a stiff penalty of 30 years in jail for their actions if they get caught?

A) White Hats B) Suicide Hackers C)Grey Hats D) Black Hats

5. The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security.

Common Criteria is based upon a framework in which computer system users can specify their security requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

The Common Criteria came with it's own jargon and terms that you should be familiar with for the purpose of the exam. Under the CC which of the following is the term used to describe the Product, System, or software being evaluated?

A) Target of Evaluation (TOE) B) Protection Profile (PP)

C) Security Target (ST) D) Evaluation Assurance Levels (EAL)

6. Which of the following choices is not part of the triangle showing how user accessibility, their access to needed function, and the need for protection all play together?

A) Functionality B) Security C) Cost D) Ease of use

7. How would you call the process of validating that a user is who s/he represents her/himself to be?

A) Authorization B)Authentication C) Two factors D) Identification

8. Within the CEH curriculum there are 4 tenets on which information security sits. Which of the following is NOT one of the four basic tenets of information system security?

A) Invisibility B) Availability C) Integrity D)Confidentiality

9. Which of the following task would normally be done while performing "Reconnaissance"?

A) You attempt to find out what host, ports, and services are running within the network

B) You remove log entries to make sure that nobody knows that reconnaissance was done on the remote computers

C) You collect as much information as possible about your target prior to moving to other phases

D) You attempt to escalate your privilege to be able to further compromise hosts within the remote internal network

10. Which of the following is one of the most commonly used port scanner?

A) Wireshark B) Ettercap C) Nmap D) Packetyzer

11. Which of the following best describes an exploit?

A) A condition where a program (either an application or part of the operating system) stops performing its expected function and also stops responding to other parts of the system

B) A chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software

C) An anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer

D) An intentional hidden message or feature in an object such as a piece of software or a movie.

12. Nathalie has shown a keen interest in learning more about Security testing and Penetration Testing. She visited the local library in her town and found there were a few books about hacking which she signed out for the week end. Passing by her preferred news stand she saw a copy of the Hakin9 magazine and decided to buy it. She was very pleased to note that it comes with a bootable CDROM that contains a modified version of BackTrack which is a special Linux Distribution for penetration tester.

The next day she went back to the library and used her new bootable operating system to probe the network and attempt to identify vulnerabilties that she could report to the library manager in order to help them secure systems against malicious attackers.

What is wrong with Nathalies action and do you think it was justified?

A) Nathalie did not have authorization from the owner of the resources and it was NOT justified even though she wanted to protect the network.

B) Usage of bootable Linux CDROM is forbidden in most librairies but her actions were justifed by her willingness to help.

C) As long as she does not exploit the weaknesses that were found Nathalie did the right thing and her actions were justified.

D) Nathalie did not have authorization from the owner of the resources but it was justified as she wanted to protect the network.

13. All of the following are phases of a malicious hacking except:

A) Gaining access B) Reconnaissance

C) Covering, clearing tracks, and installing back doors D) Submit a Remediation plan

14. What are the two main types of Reconnaissance that can be performed?

A) During Working hours and After working hours B) Day and Night

C) Active and Passive D) With and Without tools

15.The Biba Model or Biba Integrity Model developed by Kenneth J. Biba in 1977, is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. Which of the following is NOT one of the goals of the Biba Model?

A) Prevent data modification by unauthorized parties B) Maintain internal and external consistency

C) Prevent unauthorized data modification by authorized parties

D) Prevent interception of message content by unauthorized parties

16. How would you describe an Hacktivist?

A) It is simply a member of the Cult of the Dead Cow Hacking club (CDC) who has reached a total site defacement number of over 200 sites

B) It is someone who is living in his mother basement and has very limited social skills

C) It is someone who has a constant urge to hack into other people systems. He will often time stay up all night to attempt compromising as many system as he could within a short timeframe

D) It is someone who is hacking for a cause

17. Which of the following organization has the mission to enforce the law and defend the interests of the United States; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans?

A) Secret Service B) DOJ C) FBI D) GOA

18. Which of the following term best describes a weakness that could potentially be exploited?

A) Target of evaluation (TOE) B) Threat C) Risk D) Vulnerability

19. Which of the following is one of the main reason that computer probes and attacks and the level of damage being caused has been steadily increasing over the years?

A) The amount of bandwidth offered to most home and business users is a lot greater than five years ago. More speed means more systems can be probed within a specific period of time.

B) Today's operating systems are a lot more powerful than years ago, some of them uses 64 bits instead of 32 bits.

C) All colleges and Universities have programs that shows students how to conduct security testing and penetration testing. Students are coming out with the knowledge needed to break into systems with ease.

D) The availability of hacking tools and their ease of use if one of the key factor contributing to an increase in the number of attacks and the lethality of those attacks as well.

20. What is the essential difference between an 'Ethical Hacker' and a 'Cracker'?

A. The ethical hacker does not use the same techniques or skills as a cracker.

B. The ethical hacker does it strictly for financial motives unlike a cracker.

C. The ethical hacker has authorization from the owner of the target.

D. The ethical hacker is just a cracker who is getting paid.

21- What does the term "Ethical Hacking" mean?

A. Someone who is hacking for ethical reasons.

B. Someone who is using his/her skills for ethical reasons.

C. Someone who is using his/her skills for defensive purposes.

D. Someone who is using his/her skills for offensive purposes.

22- Who is an Ethical Hacker?

A. A person who hacks for ethical reasons

B. A person who hacks for an ethical cause

C. A person who hacks for defensive purposes

D. A person who hacks for offensive purposes

23- What is "Hacktivism"?

A. Hacking for a cause

B. Hacking ruthlessly

C. An association which groups activists

D. None of the above

24- Where should a security tester be looking for information that could be used by an attacker against an

organization? (Select all that apply)

A. CHAT rooms

B. WHOIS database

C. News groups

D. Web sites

E. Search engines

F. Organization's own web site

25- What are the two basic types of attacks?(Choose two)

A. DoS

B. Passive

C. Sniffing

D. Active

E. Cracking

26- You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com websire for

contact information and telephone number numbers but do not find it listed there. You know that they

had the entire staff directory listed on their website 12 months ago but now it is not there. How would it

be possible for you to retrieve information from the website that is outdated?

A. Visit google search engine and view the cached copy.

B. Visit Archive.org site to retrieve the Internet archive of the acme website.

C. Crawl the entire website and store them into your computer.

D. Visit the company's partners and customers website for this information.

27- Which of the following activities will NOT be considered as passive footprinting?

A. Go through the rubbish to find out any information that might have been discarded.

B. Search on financial site such as Yahoo Financial to identify assets.

C. Scan the range of IP address found in the target DNS database.

D. Perform multiples queries using a search engine.

28- Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP)

addresses/names with the intent of diverting traffic?

A. Network aliasing

B. Domain Name Server (DNS) poisoning

C. Reverse Address Resolution Protocol (ARP)

D. Port scanning

29- You are footprinting an organization to gather competitive intelligence. You visit the company's website

for contact information and telephone numbers but do not find it listed there. You know that they had

the entire staff directory listed on their website 12 months ago but not it is not there.

How would it be possible for you to retrieve information from the website that is outdated?

A. Visit google's search engine and view the cached copy.

B. Visit Archive.org web site to retrieve the Internet archive of the company's website.

C. Crawl the entire website and store them into your computer.

D. Visit the company's partners and customers website for this information.

30-What is stegnography?

A) Hiding

B) Encryption

C) Coding

D) Coloring