Quizlet

NAME _____

20 Matching questions

1. _____ Malware

2. _____ Asymmetric Algorithm

3. _____ Smurf attack

4. _____ Non Repudiation

5. _____ Man in the middle (MiM)

6. _____ Availability

7. _____ Worm

8. _____ Ping of death

9. _____ Integrity

10. _____ Attack

11. _____ Vishing

12. _____ Threat

13. _____ Symmetric Algorithm

14. _____ IP Spoofing

A. Code that contains unexpected, undocumented, additional functionality

B. Provides protection against denial by one of the entities involved in a communication of having participated in all/part of the communication

C. the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals t reveal personal information, such as passwords and credit card numbers

D. An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other

E. Code that causes malicious behavior and propagates copies of itself to other programs

F. Program that intercepts and covertly communicates data on the user of the user's activity

G. Guarding against information modifications or destruction, including ensuring information non-repudiation and authenticity

H. A distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address

I. Algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

J. Cryptography where a secret key can be divided into two parts, a public key and a private key. The public key can be given to anyone, trusted or not, while the private key must be kept secret

15. _____ Denial of Service

16. _____ Virus

17. _____ Phising

18. _____ Confidentiality

19. _____ Spyware

20. _____ Trojan Horse

K. Code that propagates copies of itself through a network; impact is usually degraded performance

L. The criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for purpose of financial reward

M. a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet

N. Potential for violation of security, which exist when there is a circumstance, capability, action, or event that could breach security and cause harm.

O. Type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer.

P. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Q. An assault on system security that derives from an intelligent threat; that is, an intelligent act that is deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system

R. Ensuring timely and reliable access to and use of information

S. an attacker sends IP packets from a false source address in order to disguise itself.

T. General name for programs or program parts planted by agent with malicious intent to cause unanticipated or undesired effects