ABSOLUTE BEGINNER'S GUIDE CYBER SECURITY PART 1

SECTION 1 QUIZ

1. What term is used to describe a threat that is unknown and has not been addressed

Risk
b. Vulnerability
c. Zero day
d. Threat

2. What protocol is used to determine how files are transferred from one computer to another

a. HTTP
b. b. FTP.
c. c. IMAP
d. d. TCP

3. What does SSL stand for?

a. Secured Sockets Layer
b. b. Secure Sockets Layer
c. c. Security Sockets Layer
d. d. Strong secure layer

4. What is the term used to describe the tactic of making code unclear so that humans or programs like an antivirus cannot understand it?

a. Confustication
b. b. Hack Value
c. c. Obfuscation
d. d. Logic Bomb

5 . Which TCP/IP layer is responsible for standardizing data exchange between applications?

a. Application layer
b. Data link layer
c. Transport layer
d. Internet/Networking layer

SECTION 2 QUIZ

1. Hackers who hack for a political or social cause are referred to as

a. Script kiddies
b. Grey hats
c. Black hats
d. Hacktivists

2. The process where a hacker takes passive steps to gather information about a potential target is known as

a. Foot printing
b. Enumeration
c. Social engineering
d. Target Survey

3. What is typically the last step taking by a hacker in the hacking methodology

a. Escalating privileges
b. Enumeration
c. Installing a backdoor
d. Destroying all evidence of the hack

SECTION 3 QUIZ

1. An attack that is directed specifically against the senior executives of a company is called

a. Phishing
b. Spear phishing
c. Whaling attack
d. Spoofing

2. What is the server that is used to issue commands to bots in a botnet

a. Command and control server
b. Botnet server
c. Bot server
d. Bot herder

3. An attack against a website or web application using malicious scripts of code is referred to as

a. SQL injection attack
b. Man in the middle attack
c. XSS attack
d. Script attack

4. Which of these attacks is most common with unsecured wireless networks

a. SQL injection
b. Man in the middle
c. DoS & DDoS attack
d. Phishing

5. Does the length of a password directly impact the chances of a brute force attack being successful?

a. True
b. False

SECTION 4 QUIZ

1. A virus is able to spread itself across a network without any help

a. True
b. False

2. What sort of Trojan allows a hacker to gain unauthorized access to a system?

a. Infosteal trojan
b. Backdoor trojan
c. Trojan downloader
d. Trojan DDoS

3. What sort of malware is activated even before the infected system boots up?

a. Trojan
b. Worm
c. Rootkit
d. Browser Hijacker
e. Ransomware

4. A virus requires an active host program in order to run and cause damage to existing documents

a. True
b. False
c. Sometimes. Not always

5. What is the device called that can record your keystrokes or take screenshots

a. Keyboard loggers
b. Keyboard trackers
c. Keyloggers
d. Spyware

SECTION 5 QUIZ

1. What does it mean when an antivirus uses ***Heuristic*** methods to detect a virus?

a. It studies the code that makes up the virus
b. It studies the effect the virus has on other files
c. It predicts a file to be a virus by studying its behavior

2. In encryption, what is the term used to refer to a data that is now locked and secretive?

a. Cipher
b. Key
c. Cryptographic data
d. Plaintext

3. When a firewall tracks the state of a connection between systems, this is known as

a. Packet filtering
b. Connection inspection
c. Stateful inspection
d. Proxy service

4. What does WEP stand for?

a. Wired Equivalent Protection
b. Wired Equivalent Privacy
c. Wireless Equivalent Protection
d. Wireless Equivalent Privacy

5. Requiring the use of a username and password to gain access is an example of two factor authentication

a. True
b. False

CYBER RISK MANAGEMENT QUIZ

1. Which of the following is NOT a method of dealing with risk

a. Risk Mitigation
b. Risk Avoidance
c. Risk Documentation
d. Risk Transference

2. An example of risk mitigation might be:

a. David buys a UPS (uninterrupted power supply) box so that all computers and servers in the building can be manually shut down in case of a power failure.
b. CEO Bob James buys an insurance plan that covers flooding for his company building
c. The CEO of Lab Cyber decides to ignore the risk concern raised by his risk manager
d. Peter installs the latest update on the company software to prevent a new vulnerability that was just discovered

3. What is referred to as ***Scoping***?

a. Determining which risks are acceptable or not
b. Identifying possible exploits and threats
c. Identifying vulnerabilities and their safeguards
d. Identifying all assets

4. A statement that describes how much risk an organization is willing to accept is

a. Risk Tolerance
b. Risk Acceptance
c. Risk Appetite
d. Risk Volume