

## HIGHWAY CYBER SECURITY FUNDAMENTALS (HCSF) QUIZ version 1.0

DATE:	6-1-16
NAME:	Ray Murphy
AGENCY:	US DOT/FHWA
TITLE:	ITS Specialist
EMAIL:	ray.murphy@dot.gov

Please answer all questions – save your completed quiz as:

HCSF quiz – Your NAME DATE .pdf (i.e. HCSF quiz – Ray Murphy 6-1-16.pdf) and email to: ray.murphy@dot.gov

**1. Which one of the following hacker classifications best describes an “Ethical” hacker or “Penn Tester”?**

a. Grey	<input type="radio"/>	a
b. Black	<input type="radio"/>	b
c. White	<input type="radio"/>	c
d. Blue	<input type="radio"/>	d

**2. Which one of the following best describes a “Bitcoin” currency?**

a. peer-to-peer	<input type="radio"/>	a
b. crypto or digital	<input type="radio"/>	b
c. European	<input type="radio"/>	c
d. Coinage	<input type="radio"/>	d

**3. What would best describe the intent or purpose of “Social Engineering”?**

a. Zero-day attack	<input type="radio"/>	a
b. divulge confidential information	<input type="radio"/>	b
c. mitigate software vulnerabilities	<input type="radio"/>	c
d. manipulate or erase information	<input type="radio"/>	d

4. What are Firewalls often categorized as either?

a. network or host-based	<input type="radio"/>	a
b. physical or logical	<input type="radio"/>	b
c. biased or unbiased	<input type="radio"/>	c
d. red or blue	<input type="radio"/>	d

5. Vulnerability is a weakness which allows an attacker to reduce a system's \_\_\_\_\_?

a. attack surface	<input type="radio"/>	a
b. dumpster diving	<input type="radio"/>	b
c. information assurance	<input type="radio"/>	c
d. social engineering	<input type="radio"/>	d

6. What is the time from when the security hole was introduced or manifested in deployed software (launched), to when access was removed, a security fix was available (deployed), or the attacker was disabled called?

a. golden window	<input type="radio"/>	a
b. real-time window	<input type="radio"/>	b
c. window of vulnerability	<input type="radio"/>	c
d. window of opportunity	<input type="radio"/>	d

7. What is vulnerability with one or more known instances of working and fully implemented attacks (an exploit exists) is classified as what type of vulnerability?

a. zero day	<input type="radio"/>	a
b. threat	<input type="radio"/>	b
c. network	<input type="radio"/>	c
d. exploitable	<input type="radio"/>	d

8. What does an exploit take advantage of?

a. Trust	<input type="checkbox"/>	a
b. Clients	<input type="checkbox"/>	b
c. Criminals	<input type="checkbox"/>	c
d. vulnerability	<input type="checkbox"/>	d

9. How much time does “zero-day” vulnerability have once the flaw becomes known?

a. Zero days	<input type="checkbox"/>	a
b. twenty four hours	<input type="checkbox"/>	b
c. minutes	<input type="checkbox"/>	c
d. days	<input type="checkbox"/>	d

10. Which term(s) best describe “malware”?

a. Viruses	<input type="checkbox"/>	a
b. Worms	<input type="checkbox"/>	b
c. Ransomware	<input type="checkbox"/>	c
d. all indicated	<input type="checkbox"/>	d

11. What is the payload of ransomware disguised as?

a. Trojan	<input type="checkbox"/>	a
b. Stuxnet	<input type="checkbox"/>	b
c. Signature	<input type="checkbox"/>	c
d. file	<input type="checkbox"/>	d

**12. What is the name of the self-propagating ransomware that exploits computer server vulnerabilities without requiring human interaction and targets servers instead of end-users?**

a. cryptoworm	<input type="radio"/>	a
b. SamSam	<input type="radio"/>	b
c. zero-hour	<input type="radio"/>	c
d. Stuxnet	<input type="radio"/>	d

**13. What is the attackers' purpose or goal of a denial-of-service attack?**

a. Service vulnerabilities	<input type="radio"/>	a
b. overload the server	<input type="radio"/>	b
c. deny access to ransomware	<input type="radio"/>	c
d. prevent information services	<input type="radio"/>	d

**14. What is the name of the malware family used in the Ukrainian electric power attack?**

a. PowerPoint 0-day	<input type="radio"/>	a
b. White Hat	<input type="radio"/>	b
c. DoS	<input type="radio"/>	c
d. BlackEnergy	<input type="radio"/>	d

**15. What best describes Regin malware?**

a. Penetration toolkit	<input type="radio"/>	a
b. targeted multi-purpose collection tool	<input type="radio"/>	b
c. propagates trojans	<input type="radio"/>	c
d. systematic ransomware trojan	<input type="radio"/>	d

16. Which malware determines what antivirus software is installed?

a. Stuxnet	<input type="radio"/>	a
b. Samsam	<input type="radio"/>	b
c. Flame	<input type="radio"/>	c
d. BlackEnergy	<input type="radio"/>	d

17. Are any of these listed below the result of code injection?

a. all listed	<input type="radio"/>	a
b. privilege escalation	<input type="radio"/>	b
c. install (inject) malware	<input type="radio"/>	c
d. compromise sensitive data	<input type="radio"/>	d

18. What is the ability to trigger arbitrary code execution from one machine on another often referred to as?

a. deactivate code automatically	<input type="radio"/>	a
b. general cyber-espionage	<input type="radio"/>	b
c. code execution tool	<input type="radio"/>	c
d. remote code execution	<input type="radio"/>	d

19. Select the answer which best describes what the Metasploit Project provides. It is a computer security project that provides: \_\_\_\_\_?

a. information about security vulnerabilities	<input type="radio"/>	a
b. all listed	<input type="radio"/>	b
c. aids in IDS signature development	<input type="radio"/>	c
d. aids in penetration testing	<input type="radio"/>	d

20. A “sandbox”, as it relates to computer security, is a designated, separate and restricted environment (or “container”, with tight control and permissions). Which statement below is true regarding a “sandbox”?

a. Acts as a backdoor	<input type="checkbox"/>	a
b. often used to execute untested code	<input type="checkbox"/>	b
c. provides privilege escalation exploit in order to gain control	<input type="checkbox"/>	c
d. includes fuzzing tools	<input type="checkbox"/>	d

21. A man-in-the-middle (MITM) attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Which statement below is true of a MITM attack?

a. Forensic analysis cannot verify	<input type="checkbox"/>	a
b. succeeds when the attacker can impersonate one endpoint	<input type="checkbox"/>	b
c. must be able to intercept all relevant messages passing between the two victims	<input type="checkbox"/>	c
d. cannot be used against cryptographic protocols	<input type="checkbox"/>	d

22. What does the acronym CVSS stand for?

a. Central Valley Software Solutions	<input type="checkbox"/>	a
b. Center for Vector System Studies	<input type="checkbox"/>	b
c. Common Vulnerability Scoring System	<input type="checkbox"/>	c
d. Common Vulnerability Sector System	<input type="checkbox"/>	d

23. Which keylogger type listed below is frequently implemented as rootkits?

a. software-based	<input type="checkbox"/>	a
b. hypervisor-based	<input type="checkbox"/>	b
c. Memory Injection (MitB)-based	<input type="checkbox"/>	c
d. kernel-based	<input type="checkbox"/>	d

24. Pivoting refers to a method used by penetration testers that uses the compromised system to attack other systems on the same network. What is pivoting also referred to or known as?

a. island jumping	<input type="checkbox"/>	a
b. island hopping	<input type="checkbox"/>	b
c. island diving	<input type="checkbox"/>	c
d. island surfing	<input type="checkbox"/>	d

25. Hosts in the DMZ are permitted to have only limited connectivity to specific hosts in the internal network, as the content of DMZ is not as secure as the internal network. What is a DMZ referred to?

a. Analyzer network	<input type="checkbox"/>	a
b. sub-network	<input type="checkbox"/>	b
c. perimeter network	<input type="checkbox"/>	c
d. local area network	<input type="checkbox"/>	d

26. A data diode (also known as a unidirectional security gateway) is a network appliance or device allowing data to travel only in one direction, used in guaranteeing information security. They are most commonly found at the industrial control level, where they serve as connections between what?

a. Two or more diodes	<input type="checkbox"/>	a
b. two or more protocols	<input type="checkbox"/>	b
c. two or more security classifications	<input type="checkbox"/>	c
d. two or more networks	<input type="checkbox"/>	d

**27. An application that creates a sandbox-like environment to trap attackers is called a “honeypot.” Which of the following are not honeypots?**

a. Database honeypot	<input type="checkbox"/>	a
b. SQL honeypot	<input type="checkbox"/>	b
c. high interaction honeypot	<input type="checkbox"/>	c
d. Malware honeypot	<input type="checkbox"/>	d

**28. Which of the following are under the Industrial Control Systems umbrella?**

a. Dynamic Message Signs (DMS) installations	<input type="checkbox"/>	a
b. Traffic Signal Installations	<input type="checkbox"/>	b
c. Road Weather Information Systems (RWIS)	<input type="checkbox"/>	c
d. all listed	<input type="checkbox"/>	d

**29. Which of the following is not an example of a SCADA system?**

a. PLC-based Reversible Lane Control (REVLAC)	<input type="checkbox"/>	a
b. Transportation Management System (TMS)	<input type="checkbox"/>	b
c. Roadway Pumping Station System	<input type="checkbox"/>	c
d. Tunnel Ventilation System	<input type="checkbox"/>	d

**30. There are many different ICS devices, but in common they typically include some type of?**

a. field devices, field controllers and interface	<input type="checkbox"/>	a
b. nonvolatile, volatile and firmware	<input type="checkbox"/>	b
c. jumpers, dip switches, and switches	<input type="checkbox"/>	c
d. none listed	<input type="checkbox"/>	d

**31. In the context of cyber-physical systems, resilient control systems are an aspect that focuses on the unique interdependencies of a control system, as compared to?**

a. embedded systems	<input type="radio"/>	a
b. ladder diagram systems	<input type="radio"/>	b
c. IT computer systems	<input type="radio"/>	c
d. process control systems	<input type="radio"/>	d

**32. Why is achieving resilience in the next generation of control systems important?**

a. cyber security protections are part of the design such that the system defends itself from attack by changing its behaviors	<input type="radio"/>	a
b. all listed	<input type="radio"/>	b
c. addressing the complex control system interdependencies, including the human systems interaction and cyber security	<input type="radio"/>	c
d. considers both benign and malicious human interaction	<input type="radio"/>	d

**33. In computing, which definition below best describes what protocol or communication protocols are?**

a. a set of metrics and standards associated with codifying promising technologies	<input type="radio"/>	a
b. messages from the supervisory system to control connected objects	<input type="radio"/>	b
c. any system that gathers information on an industrial process and modifies, regulates, or manages the process to achieve a desired result	<input type="radio"/>	c
d. a set of rules in which computers communicate with each other	<input type="radio"/>	d

**34. What are ports 80 and 443 defaults for?**

a. HTTP & HTTPS	<input type="radio"/>	a
b. TCP & FTP	<input type="radio"/>	b
c. ICMP	<input type="radio"/>	c
d. SSH & SMB	<input type="radio"/>	d

**35. What is UDP suitable for?**

<ul style="list-style-type: none"><li>a. ensuring the network's stable and secure operation</li><li>b. use of ordinary HTTP over an encrypted SSL/TLS connection</li><li>c. where error checking and correction is either not necessary or is performed in the application</li><li>d. abstracts the application's communication from the underlying networking details</li></ul>	<ul style="list-style-type: none"><li><input type="radio"/> a</li><li><input type="radio"/> b</li><li><input type="radio"/> c</li><li><input type="radio"/> d</li></ul>
--	---

**36. Why is understanding the OSI reference model important?**

<ul style="list-style-type: none"><li>a. it is an important part of understanding the differences between interconnection devices</li><li>b. helps understand how networks and network protocols function and which protocols and devices can interact with each other</li><li>c. an early packet switching network and the first network to implement the protocol suite TCP/IP</li><li>d. both it is an important part of understanding the differences between interconnection devices and helps understand how networks and network protocols function and which protocols and devices can interact with each other</li></ul>	<ul style="list-style-type: none"><li><input type="radio"/> a</li><li><input type="radio"/> b</li><li><input type="radio"/> c</li><li><input type="radio"/> d</li></ul>
---	---

**37. Which layer is the single most complex layer in the OSI model?**

<ul style="list-style-type: none"><li>a. Transport</li><li>b. Network</li><li>c. data link</li><li>d. Application</li></ul>	<ul style="list-style-type: none"><li><input type="radio"/> a</li><li><input type="radio"/> b</li><li><input type="radio"/> c</li><li><input type="radio"/> d</li></ul>
---	---

38. Vulnerabilities exist in each of the 7 OSI layers. Which are common attacks to Layer 2?

a. Sniffing & spoofing	<input type="checkbox"/>	a
b. DoS & port scanning	<input type="checkbox"/>	b
c. exploit code & malicious software	<input type="checkbox"/>	c
d. hijacking & password attacks	<input type="checkbox"/>	d

39. A network packet is a formatted unit of data carried by a packet-switched network and consists of control information and user data, which is also known as the payload. In the OSI model, *packet* strictly refers to a data unit at which layer?

a. 2	<input type="checkbox"/>	a
b. 3	<input type="checkbox"/>	b
c. 4	<input type="checkbox"/>	c
d. 5	<input type="checkbox"/>	d

40. What is the utility used for network discovery, security auditing, determines what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, and what type of packet filters/firewalls are in use?

a. Nmap	<input type="checkbox"/>	a
b. Ncat	<input type="checkbox"/>	b
c. Ndiff	<input type="checkbox"/>	c
d. Nping	<input type="checkbox"/>	d

41. What is the computer program called which has complete control over everything that occurs in the system, is the first program loaded on startup, and then manages the remainder of the startup, as well as input/output requests from software, and is also responsible for managing memory?

a. Daemon	<input type="checkbox"/>	a
b. Shell	<input type="checkbox"/>	b
c. kernel	<input type="checkbox"/>	c
d. operating system	<input type="checkbox"/>	d

**42. ARP is the Address Resolution Protocol and is used to find the MAC address, a tool to view ARP table and is used to forward IP datagrams to local routers. What does MAC stand for?**

a. manage access control	<input type="radio"/>	a
b. monitor application classification	<input type="radio"/>	b
c. media access control	<input type="radio"/>	c
d. media application control	<input type="radio"/>	d

**43. Often this attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks; what is this attack called?**

a. ARP spying	<input type="radio"/>	a
b. ngrep, aka "network grep"	<input type="radio"/>	b
c. command-line interface (CLI)	<input type="radio"/>	c
d. ARP spoofing	<input type="radio"/>	d

**44. MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. A MAC address may be referred to as?**

a. Ethernet Hardware Address (EHA)	<input type="radio"/>	a
b. Burned-In Address (BIA)	<input type="radio"/>	b
c. none listed	<input type="radio"/>	c
d. both Ethernet Hardware Address (EHA) and Burned-In Address (BIA)	<input type="radio"/>	d

**45. As data streams flow across the network, the computer program captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications; what is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network?**

a. EUI-48 identifier	<input type="radio"/>	a
b. packet sniffer	<input type="radio"/>	b
c. ARP scan	<input type="radio"/>	c
d. interface configuration	<input type="radio"/>	d

**46. What is the difference between passive and active network discovery?**

a. one uses network intrusion and the other uses endpoint security	<input type="radio"/> a
b. one uses ipconfig and the other uses ifconfig	<input type="radio"/> b
c. one uses tcpdump and the other uses wireshark	<input type="radio"/> c
d. one is more difficult to detect than the other	<input type="radio"/> d

**47. A routing table is a data table that lists the routes to particular network destinations; the primary function of a \_\_\_\_\_ is to forward a packet toward its destination network, which is the destination IP address of the packet. To do this, a \_\_\_\_\_ needs to search the routing information stored in its routing table. Which of the following terms best fits in both blanks?**

a. Gateway	<input type="radio"/> a
b. Switch	<input type="radio"/> b
c. Protocol	<input type="radio"/> c
d. Router	<input type="radio"/> d

**48. Why should one look at routing tables?**

a. Identify router/gateway IP addresses	<input type="radio"/> a
b. Identify new network and host targets	<input type="radio"/> b
c. Gateway hosts great target for Man-in-the-Middle (MitM) attack.	<input type="radio"/> c
d. all (Identify router/gateway IP addresses, new network and host targets and gateway hosts great target for Man-in-the-Middle (MitM) attack)	<input type="radio"/> d

**49. If a rootkit is detected to reside in the kernel, then what solution may be required?**

a. OS reinstallation	<input type="radio"/> a
b. kernel hopping	<input type="radio"/> b
c. kill rootkit	<input type="radio"/> c
d. HMAC (Hash the MAC)	<input type="radio"/> d

**50. Some standard applications that employ hash functions include?**

<p>a. authentication, message integrity, and message fingerprinting</p> <p>b. data corruption detection, and digital signature efficiency</p> <p>c. assuring integrity of transmitted data, and is the building block for HMACs</p> <p>d. both (authentication, message integrity, and message fingerprinting and data corruption detection, and digital signature efficiency)</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
--	---

**51. What is the term for random data that is used as an additional input to a one-way function that hashes a password or passphrase and its primary function is to defend against dictionary attacks versus a list of password hashes and against pre-computed rainbow table attacks?**

<p>a. pepper</p> <p>b. pass the hash</p> <p>c. salt</p> <p>d. rootkit</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
---	---

**52. What are the 7 layers which constitute defense-in-depth?**

<p>a. ethernet, 802.11, Bluetooth, IEEE 802.5 token ring, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM), Fiber Channel</p> <p>b. data, applications, host, internal network, perimeter, physical, policies/procedures/awareness</p> <p>c. anti-virus software, authentication and password security, biometrics, DMZ, data-centric security, encryption, firewalls</p> <p>d. none listed</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
--	---

**53. Which definition best describes an intrusion detection system (IDS)?**

<p>a. A device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.</p> <p>b. An information assurance concept in which multiple layers of security controls (defense) are placed throughout an information technology system. Its intent is to provide redundancy in the event a security control fails or vulnerability is exploited.</p> <p>c. A name server for the root zone of the Domain Name System (DNS) of the Internet. It directly answers requests for records in the root zone and answers other requests by returning a list of the authoritative name servers for the appropriate Top-Level Domain (TLD).</p> <p>d. A compromised password hashing function that was the primary hash that Microsoft LAN Manager and Microsoft Windows versions prior to Windows NT used to store user passwords, hash of a user's password, instead of requiring the associated plaintext password (Privilege Escalation).</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
--	---

**54. Within the realm of intrusion detection system terminology, what best defines the detection rate?**

<p>a. a value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack</p> <p>b. the number of 'normal' patterns classified as attacks (False Positive) divided by the total number of 'normal' patterns</p> <p>c. none listed</p> <p>d. the number of intrusion instances detected by the system (True Positive) divided by the total number of intrusion instances present in the test set</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
---	---

**55. What does the acronym HIDS mean?**

<p>a. hardware-based intrusion detection system</p> <p>b. honey-bear intrusion detection system</p> <p>c. host-based intrusion detection system</p> <p>d. hmap-based intrusion detection system</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
---	---

**56. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size. Elliptic curves are applicable for which of the following tasks?**

<p>a. password-based key derivation functions (PBKDF2), algorithms for performing encryption or decryption)) and various testing &amp; scanning procedures</p> <p>b. encryption, digital signatures, and pseudo-random generators</p> <p>c. determines the functional output of a cryptographic algorithm, specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms</p> <p>d. both password-based key derivation functions (PBKDF2), algorithms for performing encryption or decryption)) and various testing &amp; scanning procedures and determines the functional output of a cryptographic algorithm, specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
---	---

**57. Which of the following best describes encryption?**

<p>a. the process of encoding messages or information in such a way that only authorized parties can read it</p> <p>b. the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted</p> <p>c. usually uses a pseudo-random encryption key generated by an algorithm</p> <p>d. all of the above</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
---	---

**58. The NSA ANT catalog is a classified document listing technology available to the United States National Security Agency (NSA) Tailored Access Operations (TAO) to aid in cyber surveillance.; what does the acronym ANT stand for?**

a. advanced network technology	<input type="radio"/>	a
b. advanced NIDS technique	<input type="radio"/>	b
c. authentication network tcpdump	<input type="radio"/>	c
d. advanced NMAP table	<input type="radio"/>	d

**59. What is the basic difference between vulnerability scanning and penetration testing?**

a. one is largely automated and the other is a logical process	<input type="radio"/>	a
b. one is an advanced process and the other is an encrypted process	<input type="radio"/>	b
c. one is more vulnerable than the other	<input type="radio"/>	c
d. one is largely automated and the other is a manual process	<input type="radio"/>	d

**60. What best describes tcpdump?**

a. Packet analyzer	<input type="radio"/>	a
b. capture packets	<input type="radio"/>	b
c. network sniffer	<input type="radio"/>	c
d. all listed	<input type="radio"/>	d

**61. Research indicates that cyber attackers are getting quieter once they are inside the network. They know they are being watched and as such, they are choosing attack methods that will help them to hide longer in the network so they can spy and steal more data over a longer period of time. What is the fairly new and stealthy approach to command-and-control called?**

a. hidden tunnels	<input type="radio"/>	a
b. pcap file	<input type="radio"/>	b
c. tcpdump man page	<input type="radio"/>	c
d. Galois fields	<input type="radio"/>	d

**62. SNORT has become the standard for (IDP/IPS) Intrusion Detection Perimeter/Intrusion Prevention Systems. Its open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. The program can be used to detect what?**

a. buffer overflows and server message block probes	<input type="radio"/>	a
b. operating system fingerprinting attempts and stealth port scans	<input type="radio"/>	b
c. both buffer overflows and server message block probes and operating system fingerprinting attempts and stealth port scans	<input type="radio"/>	c
d. none described above	<input type="radio"/>	d

**63. What is the one of the foremost network protocol analyzers called?**

a. quantum encryption	<input type="radio"/>	a
b. clandestine	<input type="radio"/>	b
c. masquerader	<input type="radio"/>	c
d. wireshark	<input type="radio"/>	d

**64. What are some of the features of Wireshark?**

<p>a. both live data can be read from various communication platforms, decryption support for many protocols, output can be exported to XML, CSV, or plain text and deep inspection of hundreds of protocols, live capture and offline analysis, rich VoIP analysis and capture files compressed with gzip can be decompressed on the fly</p> <p>b. live data can be read from various communication platforms, decryption support for many protocols, output can be exported to XML, CSV, or plain text</p> <p>c. none listed</p> <p>d. both deep inspection of hundreds of protocols, live capture and offline analysis, rich VoIP analysis and capture files compressed with gzip can be decompressed on the fly</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
---	---

**65. What is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message?**

<p>a. Pseudorandom</p> <p>b. Universal</p> <p>c. randomization</p> <p>d. Decompression</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
--	---

**66. What is the term within cryptography that is the starting variable for a fixed-size input?**

<p>a. VoIP analyzer</p> <p>b. intuitive analysis</p> <p>c. attack vector</p> <p>d. initialization vector</p>	<p><input type="radio"/> a</p> <p><input type="radio"/> b</p> <p><input type="radio"/> c</p> <p><input type="radio"/> d</p>
--	---

67. Which protocol is prone to related-IV attacks?

a. TCP/IP	<input type="radio"/>	a
b. WEP	<input type="radio"/>	b
c. FTP	<input type="radio"/>	c
d. ATM	<input type="radio"/>	d

68. Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. Typically it is information from a private TCP/IP computer network to the Internet that is \_\_\_\_\_. Which of the following terms best fits in the blank?

a. Filtered	<input type="radio"/>	a
b. released	<input type="radio"/>	b
c. controlled	<input type="radio"/>	c
d. Configured	<input type="radio"/>	d

69. Egress filtering helps ensure that unauthorized or malicious traffic never leaves which network?

a. internal	<input type="radio"/>	a
b. External	<input type="radio"/>	b
c. Host	<input type="radio"/>	c
d. Client	<input type="radio"/>	d

**70. Defense in depth seeks to delay rather than prevent the advance of an attacker by yielding space to buy time. The placement of protection mechanisms, procedures and policies is intended to increase the dependability of an ICS, where multiple layers of defense prevent espionage and direct attacks against critical systems. In terms of computer network defense, defense in depth measures should not only prevent security breaches but also buy an organization time to detect and respond to an attack and so reduce and mitigate the consequences of a breach. Where did this strategy originate from?**

a. DEFCON b. Sandboxing c. Honeypots d. Military	<input type="radio"/> a <input type="radio"/> b <input type="radio"/> c <input type="radio"/> d
---	--