

Highway Cyber Security Fundamentals - Quiz

The intent of this quiz is to reinforce concepts covered in the Read Ahead and in preparation for the workshop. A passing grade of 70% (49 correct out of 70 questions) is required to attend the workshop.

* 1. Participant Contact Information

Name	<input type="text"/>
Company	<input type="text"/>
State/Province	<input type="text" value="-- select state --"/>
Email Address	<input type="text"/>
Phone Number	<input type="text"/>

* 2. Which one of the following hacker classifications best describes an "Ethical" hacker?

- grey
- black
- white
- penn tester

* 3. Which one of the following best describes a "Bitcoin" currency?

- peer-to-peer
- crypto
- European
- digital

* 4. What would best describe the intent or purpose of "Social Engineering"?

- Zero-day attack
- divulge confidential information
- mitigate software vulnerabilities
- manipulate or erase information

* 5. What are Firewalls often categorized as?

- network or host-based
- physical or logical
- biased or unbiased
- red or blue

* 6. A vulnerability is a weakness which allows an attacker to reduce a system's _____?

- attack surface
- dumpster diving
- information assurance
- social engineering

* 7. 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?

- golden window
- real-time window
- window of vulnerability
- window of opportunity

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

- zero day
- threat
- network
- exploitable

* 9. What does an exploit take advantage of?

- trust
- bug
- criminals
- vulnerability

* 10. How much time does a zero-day vulnerability have once the flaw becomes known?

- zero days
- twenty four hours
- minutes
- zero hours

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

- viruses
- worms
- ransomware
- all (viruses, worms & ransomware)

* 12. What is the payload of ransomware disguised as?

- trojan
- Stuxnet
- signature
- file

* 13. 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?

- cryptoworm
- SamSam
- zero-hour
- Stuxnet

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

- service vulnerabilities
- overload the server
- deny access to ransomware
- prevent access to information or services

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

- PowerPoint 0-day
- White Hat
- DoS
- BlackEnergy

16. What best describes Regin malware?

- Penetration toolkit
- targeted multi-purpose collection tool
- propagates trojans
- systematic ransomware trojan

* 17. Which malware determines what antivirus software is installed?

- Stuxnet
- SamSam
- Flame
- BlackEnergy

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

- all (privilege escalation, install (inject) malware, compromise sensitive data)
- privilege escalation
- install (inject) malware
- compromise sensitive data

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

- deactivate code automatically
- general cyber-espionage
- code execution tool
- remote code execution

* 20. Select the answer which best describes what the Metasploit Project provides.

It is a computer security project that provides: _____?

- information about security vulnerabilities
- all (information about security vulnerabilities, aids in IDS signature development, aids in penetration testing)
- aids in IDS signature development
- aids in penetration testing

* 21. 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”?

- acts as a backdoor
- often used to execute untested code
- provides privilege escalation exploit in order to gain control
- includes fuzzing tools

* 22. 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?

- forensic analysis cannot verify
- succeeds when the attacker can impersonate one endpoint
- must be able to intercept all relevant messages passing between the two victims
- cannot be used against cryptographic protocols

* 23. What does the acronym CVSS stand for?

- Central Valley Software Solutions
- Center for Vector System Studies
- Common Vulnerability Scoring System
- Common Vulnerability Sector System

* 24. Which keylogger type listed below are frequently implemented as rootkits?

- software-based
- hypervisor-based
- Memory Injection (MitB)-based
- kernel-based

* 25. 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?

- island jumping
- island hopping
- island diving
- island surfing

* 26. 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?

- analyzer network
- sub-network
- perimeter network
- local area network

* 27. 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?

- two or more diodes
- two or more protocols
- two or more security classifications
- two or more networks

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

- Database honeypot
- SQL honeypot
- High interaction honeypot
- Malware honeypot

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

- Dynamic Message Signs (DMS) installations
- Traffic Signal Installations
- Road Weather Information Systems (RWIS)
- all (Dynamic Message Signs (DMS) installations, Traffic Signal Installations, and Road Weather Information Systems (RWIS))

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

- PLC-based Reversible Lane Control (REVLAC)
- Transportation Management System (TMS)
- Roadway Pumping Station System
- Tunnel Ventilation System

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

- field devices, field controllers and interface
- nonvolatile, volatile and firmware
- jumpers, dip switches, and switches
- none of the above

* 32. 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?

- embedded systems
- ladder diagram systems
- IT computer systems
- process control systems

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

- cyber security protections are part of the design such that the system defends itself from attack by changing its behaviors
- all (cyber security protections are part of the design such that the system defends itself from attack by changing its behaviors, addressing the complex control system interdependencies, including the human systems interaction and cyber security, considers both benign and malicious human interaction)
- addressing the complex control system interdependencies, including the human systems interaction and cyber security
- considers both benign and malicious human interaction

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

- a set of metrics and standards associated with codifying promising technologies
- messages from the supervisory system to control connected objects
- any system that gathers information on an industrial process and modifies, regulates, or manages the process to achieve a desired result
- a set of rules in which computers communicate with each other

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

- HTTP & HTTPS
- TCP & FTP
- ICMP
- SSH & SMB

* 36. What is UDP suitable for?

- ensuring the network's stable and secure operation
- use of ordinary HTTP over an encrypted SSL/TLS connection
- where error checking and correction is either not necessary or is performed in the application
- abstracts the application's communication from the underlying networking details

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

- it is an important part of understanding the differences between interconnection devices
- helps understand how networks and network protocols function and which protocols and devices can interact with each other
- an early packet switching network and the first network to implement the protocol suite TCP/IP
- both (it is an important part of understanding the differences between interconnection devices and it helps understand how networks and network protocols function and which protocols and devices can interact with each other)

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

- transport
- network
- data link
- application

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

- Sniffing & spoofing
- DoS & port scanning
- Exploit code & malicious software
- Hijacking & password attacks

* 40. 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?

- 2
- 3
- 4
- 5

* 41. 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?

- Nmap
- Ncat
- Ndiff
- Nping

* 42. 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?

- daemon
- shell
- kernel
- operating system

* 43. Which one of the following hacker classifications best describes an "Ethical" hacker?

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?

- manage access control
- monitor application classification
- media access control
- media application control

* 44. 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?

- ARP spying
- ngrep, aka "network grep"
- command-line interface (CLI)
- ARP spoofing

* 45. 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?

- Ethernet Hardware Address (EHA)
- Burned-In Address (BIA)
- none (not Ethernet Hardware Address (EHA) nor Burned-In Address (BIA))
- both (Ethernet Hardware Address (EHA) and Burned-In Address (BIA))

* 46. 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. 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?

- EUI-48 identifier
- packet sniffer
- ARP scan
- interface configuration

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

- one uses network intrusion and the other uses endpoint security
- one uses ipconfig and the other uses ifconfig
- one uses tcpdump and the other uses wire shark
- one is more difficult to detect than the other

* 48. 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. Select the term that best fits in both blanks.

- gateway
- switch
- protocol
- router

* 49. Why should one look at routing tables?

- Identify router/gateway IP addresses
- Identify new network and host targets
- Gateway hosts great target for Man-in-the-Middle (MitM) attack.
- all (Identify router/gateway IP addresses, new network and host targets and gateway hosts great target for Man-in-the-Middle (MitM) attack)

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

- OS reinstallation
- kernel hopping
- kill rootkit
- HMAC (Hash the MAC)

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

- authentication, message integrity, and message fingerprinting
- data corruption detection & digital signature efficiency
- assuring integrity of transmitted data, and is the building block for HMACs
- both (authentication, message integrity, and message fingerprinting and data corruption detection & digital signature efficiency)

* 52. 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?

- pepper
- pass the hash
- salt
- rootkit

* 53. What are the 7 layer which constitute defense-in-depth?

- ethernet, 802.11, Bluetooth, IEEE 802.5 token ring, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM), Fiber Channel
- data, applications, host, internal network, perimeter, physical, policies/procedures/awareness
- anti-virus software, authentication and password security, biometrics, DMZ, data-centric security, encryption, firewalls
- none listed

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

- 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.
- is 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.
- is 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).
- is 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).

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

- a value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack
- the number of 'normal' patterns classified as attacks (False Positive) divided by the total number of 'normal' patterns
- none listed
- the number of intrusion instances detected by the system (True Positive) divided by the total number of intrusion instances present in the test set

* 56. What does the acronym HIDS mean?

- hardware-based intrusion detection system
- honey-bear intrusion detection system
- host-based intrusion detection system
- hmap-based intrusion detection system

* 57. 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?

- password-based key derivation functions (PBKDF2, algorithms for performing encryption or decryption)) and various testing & scanning procedures
- encryption, digital signatures, and pseudo-random generators
- determines the functional output of a cryptographic algorithm, specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms
- both password-based key derivation functions (PBKDF2, algorithms for performing encryption or decryption)) and various testing & scanning procedures and determines the functional output of a cryptographic algorithm, specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms.

* 58. Which of the following best describes encryption?

- the process of encoding messages or information in such a way that only authorized parties can read it
- 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
- usually uses a pseudo-random encryption key generated by an algorithm
- all of the above

* 59. 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?

- advanced network technology
- advanced NIDS technique
- authentication network tcpdump
- advanced NMAP table

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

- one is largely automated and the other is a logical process
- one is an advanced process and the other is an encrypted process
- one is more vulnerable than the other
- one is largely automated and the other is a manual process

* 61. What best describes tcpdump?

- packet analyzer
- capture packets
- network sniffer
- all of the above

* 62. 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?

- hidden tunnels
- pcap file
- tcpdump man page
- galois fields

* 63. 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?

- buffer overflows and server message block probes
- operating system fingerprinting attempts and stealth port scans
- both described above
- none described above

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

- quantum encryption
- clandestine
- masquerader
- wireshark

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

- 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
- live data can be read from various communication platforms, decryption support for many protocols, output can be exported to XML, CSV, or plain text
- none listed
- 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

* 66. 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?

- pseudorandom
- universal
- randomization
- decompression

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

- VoIP analyzer
- intuitive analysis
- attack vector
- initialization vector

* 68. Which protocol is prone to related-IV attacks?

- TCP/IP
- WEP
- FTP
- ATM

* 69. 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 _____. Select the word which best fits.

- filtered
- released
- controlled
- configured

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

- internal
- external
- host
- client

* 71. 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?

- DEFCON
- Sandboxing
- Honeypots
- Military

Questions & Answers: