**Review Questions: Intro to ICS/OT Cyber Security** A picture containing sky

Description automatically generated

This document contains review questions for each Units in the Introduction to ICS/OT Cyber Security course. An answer key is provided at the end of the document.

**Unit 1: ICS/OT Cyber Security Overview**

Question #1

Which of the following is of the least concern in industrial control environments?

1. Physical safety
2. Environmental safety
3. Data confidentiality
4. Site availability

Question #2

Discovered in 2010, which of the following ICS/OT-specific malware attacks targeted the Natanz nuclear facility in Iran and has been described as “crossing the Rubicon?”

1. Stuxnet
2. Havex
3. Trisis
4. Pipedream

Question #3

Which of the following was developed as an attack framework for targeting common ICS/OT assets from common vendors (e.g., Schneider Electric, Omron) and industrial protocols (e.g., Modbus, OPC UA, CODESYS)?

1. CosmicEnergy
2. Pipedream
3. Industroyer
4. Havex

Question #4

Which party is ultimately responsible for the cyber security of a facility?

1. Asset owner
2. Asset operator
3. Asset supplier
4. The facility’s cyber security team

Question #5

In 2015, which nation state adversary group was responsible for the Ukrainian blackout?

1. Fancy Bear
2. Sandworm
3. Tailored Access Operations (TAO)
4. Bene Gesserit

Question #6

Which of the following is not considered a critical infrastructure sector according to the Cybersecurity & Infrastructure Security Agency (CISA)?

1. Communications
2. Dams
3. Data Centers
4. Nuclear Reactors, Materials, and Waste

Question #7

Which critical infrastructure sector refers to those organizations which act as contractors and subcontractors in helping the United States government accomplish its goals and mission?

1. Emergency Services
2. Defense Industrial Basis
3. Government Facilities
4. Critical Manufacturing

Question #8

Which of the following is the most overlooked aspect of cyber security in both ICS/OT and IT networks?

1. Physical security
2. Data confidentiality
3. Phishing attacks
4. PLC vulnerabilities

Question #9

What is the least important aspect of cyber security in traditional IT networks?

1. Confidentiality
2. Integrity
3. Availability
4. Compliance

Question #10

In 2021, Colonial Pipeline had to take the United States’ largest oil pipeline offline for approximately a week due to an attack launched by a ?

1. Nation-state adversary
2. Ransomware group
3. Hacktivist
4. Script Kiddie

**Unit 2: Main Types of Control Systems & Protocols**

Question #1

Which of the following would be considered a field device?

1. Programmable Logic Controller
2. Data historian
3. Sensor
4. Modbus

Question #2

Which of the following industrial control assets is used to program a PLC?

1. Engineering Workstation (EWS)
2. Human Management Interface (HMI)
3. Safety Instrumented System (SIS)
4. Data Historian

Question #3

To secure a PLC using its key switch, which of the following is true?

1. Place the PLC in Program mode when the PLC is operational.
2. Place the PLC in Secure mode when the PLC is operational.
3. Place the PLC in Store mode when the PLC is operational.
4. Place the PLC in Run mode when the PLC is operational.

Question #4

Which of the following control systems typically runs commodity operating systems (e.g., Windows, Linux) and commodity software (e.g., MS SQL Server, Oracle) making it a prime target for attackers?

1. HMI
2. Data Historian
3. PLC
4. RTU

Question #5

Which of the following is the most common language used to program PLCs?

1. Ladder logic
2. S7 Comm
3. .Net Framework
4. Cobol

Question #6

Which of the following control systems is used to coordinate the operations of multiple systems at a single location?

1. PLC Server
2. DCS
3. PCI
4. SCADA

Question #7

Which of the following control systems is a graphical interface used to monitor and make changes to a PLCs operation?

1. DCS
2. SCADA
3. IACS
4. HMI

Question #8

Which of the following control systems acts as a fail safe backup which can be used to safely shutdown the facility in the event of a plant fault or emergency situation?

1. DCS
2. PLC
3. RTU
4. SIS

Question #9

Due to its use of commodity operating systems and software that are popular in IT environments, which of the following is a primary target for attackers?

1. PLC Server
2. Supervisory Control and Data Acquisition
3. Data Historian
4. DCS

Question #10

Which of the following is not considered an industrial control protocol?

1. NetBIOS
2. S7comm
3. Modbus
4. BACnet

**Unit 3: Secure Network Architecture**

Question #1

Which level of the Purdue Model does a PLC typically reside on?

1. Level 0
2. Level 1
3. Level 2
4. Level 3

Question #2

The IT-OT DMZ resides between which two levels of the Purdue Model?

1. Levels 1 and 2
2. Levels 2 and 3
3. Levels 3 and 4
4. Levels 4 and 5

Question #3

Which of the following network-based appliances should be used to create the IT-OT DMZ?

1. Firewall
2. Switch
3. Router
4. Network gateway

Question #4

Which of the following levels of the Purdue Model would an HMI typically be hosted on?

1. Level 1
2. Level 2
3. Level 3
4. Level 4

Question #5

Which of the following levels of the Purdue Model should be the only level that is connected directly to the Internet?

1. Level 6
2. Level 5
3. Level 4
4. Level 3

Question #6

Which of the following ICS-specific malware attacks compromised the Safety Instrumented System (SIS) of a petrochemical facility in the Middle East to target human life?

1. Havex
2. Stuxnet
3. Trisis
4. Shamoon

Question #7

According to ISA 62443, the ICS/OT network should further be broken down into which logical grouping of systems?

1. Zones
2. VLANs
3. Subnets
4. SANs

Question #8

The term IIoT refers to which of the following?

1. Use of a shared Active Directory structure between IT and OT
2. Deployment of IoT-based sensors within the ICS/OT network for defense
3. The IT connection directly to the Internet
4. Allowing ICS/OT assets to send data directly to the Internet for analysis

Question #9

Which of the following is typically not a consideration for cyber security teams?

1. Network security monitoring
2. Physical security
3. Secure remote access
4. Secure network architecture

Question #10

Which of the following social engineering attacks can be used to obtain sensitive information that has been printed out?

1. Eavesdropping
2. Phishing
3. Shoulder surfing
4. Dumpster diving

**Unit 4: Asset Registers and Control Systems Inventory**

Question #1

An asset register should include all of the following except:

1. Hardware
2. Software
3. Firmware
4. Personnel records

Question #2

Which of the following is not considered a method for building a complete ICS/OT asset register?

1. Physically walking the environment
2. Reviewing network packet captures
3. Actively scanning Levels 4 & 5 of the Purdue Model
4. Review existing data in project files

Question #3

Which of the following could potentially create availability issues within the ICS/OT network?

1. Passive scanning of networks with Nmap
2. Active scanning of networks with Nmap
3. Passive scanning of networks with Wireshark
4. Active scanning of networks with Wireshark

Question #4

Which is considered the most dangerous method of building an asset register?

1. Physically walking the environment
2. Reviewing network packet captures
3. Actively scanning Levels 4 & 5 of the Purdue Model
4. Reviewing existing data in project files

Question #5

Which of the following properties would normally not be included in an asset register?

1. Asset name
2. Serial number
3. Invoice approver
4. Last maintenance date

Question #6

When should an asset register be considered 100% complete and accurate?

1. Once the Change Management process is completed
2. Once the initial register is completed and before the annual update process
3. Only after the asset register has received an annual update
4. Never

Question #7

Which of the following is the most common way to store asset registers?

1. Microsoft Excel
2. COTS
3. Notepad / Wordpad
4. Cloud-based inventory application

Question #8

Which of the following should be completed while building an asset register while walking the site?

1. Check the key switch position for each PLC
2. Ensure anti-virus software is installed and updated on each Windows host
3. Review the structural integrity of both sides of a WAN connection
4. Conduct a review of the firewall ACL’s between the IT and OT networks

Question #9

Which of the following commands can be used to display the arp cache on a Windows system?

1. arp
2. arp -c
3. arp -a
4. cat /proc/net/arp

Question #10

Which of the following tools could be used for active discovery of ICS/OT network hosts?

1. Wireshark
2. Nmap
3. Network Miner
4. Shodan

**Unit 5: Threat & Vulnerability Management**

Question #1

Which of the following is the most important to successful vulnerability management in ICS/OT environments?

1. Asset registers
2. Active scanning
3. Passive scanning
4. Vulnerability remediation

Question #2

To calculate risk, the Threat is multiplied with three other factors. Which of the following is not one of these three factors?

1. Vulnerability
2. Exploitation
3. Probability
4. Impact

Question #3

In the Vulnerability Management lifecycle for IT, what happens after the Remediate phase?

1. Verification
2. Scanning
3. Prioritization
4. Asset Management

Question #4

A recently announced vulnerability has a CVSS score of 8.8. What risk classification would this vulnerability be assigned?

1. Critical
2. High
3. Medium
4. Low

Question #5

Traditional vulnerability scanners by default search for vulnerabilities associated with all of the following except which?

1. Operating system
2. Installed applications
3. Exposed services
4. Web applications

Question #6

Which of the following vulnerabilities would more than likely be the last to be remediated?

1. A Windows-system directly exposed to the Internet
2. A pressure sensor at Level 0 of the Purdue Model
3. A data historian located in the IT/OT DMZ running Linux
4. An engineering workstation running Windows at Level 3

Question #7

Which of the following levels of the Purdue Model is typically considered not suitable for active scanning?

1. Level 1
2. Level 2
3. Level 3
4. Level 3.5

Question #8

Which of the following levels of the Purdue Model is typically not going to receive immediate updates on software and firmware?

1. Level 1
2. Level 2
3. Level 3
4. Leve 3.5

Question #9

Which of the following would not be considered an Indicator of Compromise (IOC)?

1. IP address
2. File hash
3. Serial number
4. Domain name

Question #10

Which of the following is an organization that shares intel about cyber threats associated with a particular sector?

1. ISSA
2. ISACA
3. ISAC
4. ISA

**Unit 6: OSINT for Industrial Controls**

Question #1

Which of the following would refer to intelligence gathers from confidential informants and spies?

1. HUMINT
2. SIGINT
3. COMINT
4. ELINT

Question #2

Which records can help provide further information associated with a specific domain name and its registration?

1. nslookup
2. arp
3. whois
4. dns

Question #3

Which of the following sites can be used to obtain a list of hosts associated with a domain name?

1. whois.com
2. dnsdumpster.com
3. linkedin.com
4. iana.org

Question #4

Which of the following sites could be used to gain sensitive information posted about a target organization such as what ICS vendors they use?

1. whois.com
2. dnsdumpster.com
3. linkedin.com
4. iana.org

Question #5

Which of the following is not considered an ICS/OT-specific protocol that is discovered by Shodan?

1. HTTPS
2. Modbus
3. S7comm
4. BACnet

Question #6

Which of the following Shodan searches could be used to find potential devices exposed to the Internet via Modbus?

1. port:502
2. port:102
3. port:80
4. port:443

Question #7

Which of the following Shodan searches could be used to search for findings across an entire subnet range?

1. subnet:14.14.14.0/24
2. range:14.14.14.0/24
3. region:14.14.14.0/24
4. net:14.14.14.0/24

Question #8

Which of the following ICS-specific protocols is associated with building automation systems?

1. HTTPS
2. Modbus
3. S7comm
4. BACnet

Question #9

Which of the following devices is designed to purposefully be hacked?

1. NIDS
2. NIPS
3. Honeypot
4. Deep packet inspection firewall

Question #10

Which of the following Shodan features could be used to find HMIs that are exposed to the Internet?

1. Images search
2. SCADA tag search
3. Siemens tag search
4. RDP search

**Unit 7: Incident Detection**

Question #1

According to the Pyramid of Pain, which of the following IOC’s is the easiest to use to find malicious activity?

1. Hash values
2. IP addresses
3. Domain Names
4. TTPs

Question #2

Which of the following is a framework provided to help defenders understand what attackers do once they have gained a foothold in the environment?

1. The Cyber Kill Chain
2. The Diamond Model
3. MITRE ATT&CK
4. OSINT

Question #3

Which of the following would not be considered network forms of incident detection?

1. NIPS
2. NIDS
3. EDR
4. Network firewall

Question #4

Which of the following types of intrusion detection platforms can be used to alert on known malicious traffic at the network level, but it takes no further action?

1. NIDS
2. NIPS
3. HIDS
4. HIPS

Question #5

Which of the following types of host-based intrusion detection platforms can be used to alert on known malicious traffic and take steps to block the activity?

1. NIDS
2. NIPS
3. HIDS
4. HIPS

Question #6

Which of the following network devices broadcasts a received packet out all available physical ports?

1. Hub
2. Switch
3. Router
4. Firewall

Question #7

Which of the following can be used to centrally store security events while performing event correlation to identify suspicious and malicious activity requiring human investigation?

1. Stateful inspection firewall
2. Deep packet inspection firewall
3. HIPS
4. SEIM

Question #8

Which of the following is not true related to logging and collection of security event data?

1. Security event data should be forwarded to a central location for archiving.
2. Human analysts are capable of manually analyzing large amounts of security event data.
3. Archived logging data should be protected by security controls to ensure integrity.
4. Threat and Vulnerability Management data can be incorporated with security event data to provide additional context.

Question #9

Which of the following is an open-source Honeypot platform that can simulate an ICS/OT asset?

1. Honeypot
2. T-Pot
3. Sanders
4. SEIM

Question #10

Proactively searching for signs of malicious activity on the network is referred to as which of the following?

1. Intrusion detection
2. Honeypot activity
3. Threat hunting
4. Intrusion prevention

**Unit 8: Incident Response**

Question #1

Without additional context, which of the following is neither good nor bad?

1. Event
2. Alert
3. Incident
4. Breach

Question #2

A security incident which includes unauthorized access to sensitive data is classified as a what?

1. Event
2. Alert
3. Incident
4. Breach

Question #3

A single maintenance laptop is determined to be infected with malware and spreads to a Windows-based data historian and engineering workstation. Which risk classification should be assigned to this incident?

1. Low
2. Medium
3. High
4. Critical

Question #4

If a cyber security incident presents risk to either physical or environmental safety, which risk classification should be assigned to this incident?

1. Low
2. Medium
3. High
4. Critical

Question #5

Which of the following phases of the Incident Response process includes providing training to the Incident Response Team members?

1. Preparation
2. Identification
3. Recovery
4. Lessons Learned

Question #6

Which of the following phases of the Incident Response process includes resetting any passwords and tokens for employees?

1. Preparation
2. Containment
3. Eradication
4. Recovery

Question #7

Which of the following phases includes members of the Incident Response Team working to understand the organization’s strengths during an incident as well as opportunities for improvement?

1. Preparation
2. Identification
3. Recovery
4. Lessons Learned

Question #8

During an incident, which of the following is necessary for communications?

1. Informing all employees of the incident
2. Informing all clients and partners of the incident
3. Use out-of-band communication for responders
4. Work with local news media to publish an appropriate news story

Question #9

Which of the following can be used as a tool for reinforcing the actions to be taken by Incident Response Team members during an incident?

1. Tabletop Exercise
2. Email phishing campaign
3. Incident playbook
4. Incident runbook

Question #10

Which of the following tools can be used to help people learn and understand incident response better?

1. Chutes & Ladders
2. Backdoors & Breaches
3. Dungeons & Dragons
4. Offices & Cubicles

**Unit 9: Risk Assessments, Governance & Compliance**

Question #1

At which phase of the ISA 62443 life cycle is a target level assigned to a zone’s Security Level?

1. Assess
2. Design & Implement
3. Improve
4. Maintain

Question #2

Which of the following is a logical grouping of systems with a shared mission?

1. Conduit
2. Network
3. Subnet
4. Zone

Question #3

Which of the following Security Levels would be assigned when protection against nation state adversaries is required?

1. SL-0
2. SL-1
3. SL-4
4. SL-5

Question #4

Which of the following zones should be assigned the highest possible Security Level?

1. Safety Instrumented System (SIS)
2. Engineering
3. Operations Center
4. Plant Maintenance WiFi

Question #5

At which phase of the ISA 62443 life cycle is an achieved Security Level assigned to a zone?

1. Assess
2. Design & Implement
3. Improve
4. Maintain

Question #6

Which of the following is not one of the four T’s of addressing risk?

1. Tolerate
2. Triage
3. Transfer
4. Terminate

Question #7

Which of the following is not one of the five D’s of cyber security defense?

1. Deter
2. Direct
3. Deflect
4. Delay

Question #8

Which of the following establishes the need for cyber security within an organization and authorizes a cyber security program?

1. Policy
2. Standard
3. Guideline
4. Best Practice

Question #9

Which of the following governs cyber security regulations for entities responsible for electricity generation and transmission in the United States?

1. FERC
2. NERC
3. JERC
4. WERC

Question #10

Which of the following ISA 62443 Foundational Requirements (FRs) addresses secure network architecture?

1. Use Control (UC)
2. System Integrity (SI)
3. Timely Response to Events (TRE)
4. Restricted Data Flow (RDF)

**Unit 10: Penetration Testing for ICS/OT**

Question #1

Which of the following is absolutely required before any penetration testing may be performed against a system?

1. Rules of engagement
2. Authorization
3. Obtaining tools
4. Review of client’s policies, standards and procedures

Question #2

Which of the following tools can be used to craft a payload and launch an exploit against a potentially vulnerable asset?

1. Nmap
2. Wireshark
3. Metasploit
4. CrackMapExec

Question #3

Which stage of the ICS Kill Chain is associated with an attacker being on the ICS network?

1. Stage 0
2. Stage 1
3. Stage 2
4. Stage 3

Question #4

Which type of penetration test involves the penetration tester receiving no information about a target environment?

1. Black box
2. Grey box
3. White box
4. Red box

Question #5

Which of the following Nmap commands would effectively enumerate an ICS asset running Modbus?

1. nmap 10.10.10.15 -p 102 --script modbus-discover
2. nmap 10.10.10.15 -p 502 --script discover-modbus
3. nmap 10.10.10.15 -p 102 --script discover-modbus
4. nmap 10.10.10.15 -p 502 --script modbus-discover

Question #6

Which of the Modbus function codes is for the command ‘Read Coils?’

1. 1
2. 2
3. 17
4. 20

Question #7

Which of the following tactics is used when an attacker sends large amounts of junk data to an application or service to see how the target responds?

1. Spraying
2. Fuzzing
3. Scanning
4. Obfuscating

Question #8

Which of the following tactics is used when attempting to determine a login password for a target asset over the network using a pre-compiled file of hundreds of possible passwords?

1. Brute force
2. Dictionary attack
3. Wordlist attack
4. Password spray

Question #9

Which of the following web application vulnerabilities allows an attacker to access information outside of the web app’s root directory? Choose the most appropriate answer.

1. Directory traversal
2. Local file inclusion
3. Remote file inclusion
4. SQL injection

Question #10

Which of the following ICS assets is most likely to be running a web service which could be used to gain access to the host?

1. PLC
2. Engineering workstation
3. RTU
4. HMI

**Answer Key**

**Unit 1: ICS/OT Cyber Security Overview**

1. C

2. A

3. B

4. A

5. B

6. C

7. B

8. A

9. C

10. B

**Unit 2: Main Types of Control Systems & Protocols**

1. C

2. A

3. D

4. B

5. A

6. B

7. D

8. D

9. C

10. A

**Unit 3: Secure Network Architecture**

1. B

2. C

3. A

4. C

5. B

6. C

7. A

8. D

9. B

10. D

**Unit 4: Asset Registers and Control Systems Inventory**

1. D

2. C

3. B

4. A

5. C

6. D

7. A

8. A

9. C

10. B

**Unit 5: Threat & Vulnerability Management**

1. A

2. B

3. A

4. B

5. D

6. B

7. A

8. A

9. C

10. C

**Unit 6: OSINT for Industrial Controls**

1. A

2. C

3. B

4. C

5. A

6. A

7. D

8. D

9. C

10. A

**Unit 7: Incident Detection**

1. A

2. C

3. C

4. A

5. D

6. A

7. D

8. B

9. B

10. C

**Unit 8: Incident Response**

1. A

2. D

3. B

4. D

5. A

6. C

7. D

8. C

9. A

10. B

**Unit 9: Risk Assessments, Governance & Compliance**

1. A

2. D

3. C

4. A

5. B

6. B

7. B

8. A

9. B

10. D

**Unit 10: Penetration Testing for ICS/OT**

1. B

2. C

3. C

4. A

5. B

6. A

7. B

8. C

9. A

10. D