CompTIA

PT0-002

CompTIA PenTest+ Certification Exam

Exams Boost

Boost Up Your Career

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Latest Version: 18.1

Question: 1

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.
B. Verify the client has granted network access to the hot site.
C. Determine if the failover environment relies on resources not owned by the client.
D. Establish communication and escalation procedures with the client.

Answer: A

Explanation:
The statement of work (SOW) is a document that defines the scope, objectives, deliverables, and timeline of a penetration testing engagement. It is important to have the client sign the SOW before starting the assessment to avoid any legal or contractual issues.

Question: 2

Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

A. devices produce more heat and consume more power.
B. devices are obsolete and are no longer available for replacement.
C. protocols are more difficult to understand.
D. devices may cause physical world effects.

Answer: D

Explanation:
"A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully." And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence idle open connections may result into errors that cannot be handled by the devices.
Reference: https://www.hindawi.com/journals/scn/2018/3794603/

Question: 3

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

A. NDA
B. MSA
C. SOW
D. MOU

Answer: C

Explanation:
As mentioned in question 1, the SOW describes the specific activities, deliverables, and schedules for a penetration tester. The other documents are not relevant for this purpose. An NDA is a non-disclosure agreement that protects the confidentiality of the client's information. An MSA is a master service agreement that defines the general terms and conditions of a business relationship. An MOU is a memorandum of understanding that expresses a common intention or agreement between parties.

Question: 4

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

A. PLCs will not act upon commands injected over the network.
B. Supervisors and controllers are on a separate virtual network by default.
C. Controllers will not validate the origin of commands.
D. Supervisory systems will detect a malicious injection of code/commands.

Answer: C

Explanation:
PLCs are programmable logic controllers that execute logic operations on input signals from sensors and output signals to actuators. They are often connected to supervisory systems that provide humanmachine interfaces and data acquisition functions. If both systems are connected to the company intranet, they are exposed to potential attacks from internal or external adversaries. A valid assumption is that controllers will not validate the origin of commands, meaning that an attacker can send malicious commands to manipulate or sabotage the industrial process. The other assumptions are not valid because they contradict the facts or common practices.

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

A. A signed statement of work
B. The correct user accounts and associated passwords
C. The expected time frame of the assessment
D. The proper emergency contacts for the client

Answer: A

Explanation:
According to the CompTIA PenTest+ Study Guide, Exam PT0-0021, a statement of work (SOW) is a document that defines the scope, objectives, deliverables, and terms of a penetration testing project. It is a formal agreement between the service provider and the client that specifies what is expected from both parties, including the timeline, budget, resources, and responsibilities. A SOW is essential for any penetration testing engagement, as it helps to avoid misunderstandings, conflicts, and legal issues.
The CompTIA PenTest+ Study Guide also provides an example of a SOW template that covers the following sections1:
Project overview: A brief summary of the project's purpose, scope, objectives, and deliverables.
Project scope: A detailed description of the target system, network, or application that will be tested, including the boundaries, exclusions, and assumptions.
Project objectives: A clear statement of the expected outcomes and benefits of the project, such as identifying vulnerabilities, improving security posture, or complying with regulations.
Project deliverables: A list of the tangible products or services that will be provided by the service provider to the client, such as reports, recommendations, or remediation plans.
Project timeline: A schedule of the project's milestones and deadlines, such as kickoff meeting, testing phase, reporting phase, or closure meeting.
Project budget: A breakdown of the project's costs and expenses, such as labor hours, travel expenses, tools, or licenses.
Project resources: A specification of the project's human and technical resources, such as team members, roles, responsibilities, skills, or equipment.
Project terms and conditions: A statement of the project's legal and contractual aspects, such as confidentiality, liability, warranty, or dispute resolution.
The CompTIA PenTest+ Study Guide also explains why having a SOW is important before starting an assessment1:
It establishes a clear and mutual understanding of the project's scope and expectations between the service provider and the client.
It provides a basis for measuring the project's progress and performance against the agreed-upon objectives and deliverables.
It protects both parties from potential risks or disputes that may arise during or after the project.

Thank You for Trying Our Product

For More Information – **Visit link below:**

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**