Q: Which of the following illustrates a use case of Stealth TCP Port Sweeping?
A: Slowly probe port 3306 across hosts over hours to map which machines run MySQL.

Q: What is the primary focus of 'extra capacity' in the principle of redundancy?
A: Fault Tolerance

Q: As an attacker is developing a master program, what threats are compatible for complexing in the process of weaponization?
A: Rootkit > Worm > Buffer Overflow > Denial of Service

Q: Which type of vulnerability scan is more effective?
A: Credentialed, runs with valid credentials to reveal privilege/config issues but needs secure handling

Q: Which is the first step in Penetration Testing:
A: Planning

Q: BDO separates its payment systems from its office network and limits communication to authorized middleware servers. Which primary benefit of segmentation is achieved in this setup?
A: Minimized lateral movement in case of a breach

Q: What tool is commonly integrated with SIEM to allow incident response?
A: SOAR

Q: Which of the following is an application of UDP Port Scanning?
A: Probe UDP port 53 across many IPs to locate DNS servers on the network.

Q: In the following SPOFs, which of the following is NOT a Logical Layer SPOF?
A: A lone hard drive or storage array with no redundancy.

Q: What is the major enhancement in WPA2 in the wireless network evolution?
A: Made AES mandatory and replaced TKIP with CCMP.

Q: The act of removing Apple’s restrictions, allowing unauthorized apps to run on iOS devices:
A: Jailbreaking

Q: What does NTP as a security protocol do?
A: Synchronizes network computer system clocks

Q: Which of the following statements is FALSE?
A: In Extranet, the risk level is medium-high, and the trust level medium-low

Q: In which core strategy of network hardening for IT does a network specialist enforce strict rules so IoT devices can only communicate with the services or servers they truly need?
A: Restriction

Q: Which of the following DOES NOT concern server profiling?
A: The parameters defining user access and behavior

Q: How will you characterize 'Securely Provision' based on NIST governance framework?
A: Conceptualizes, designs, procures or builds secure IT systems

Q: The type of policy that is leaning on the IT security infrastructure:
A: System-specific Policy

Q: A metric that captures the level of access required for successful exploit of vulnerability:

A: Privileges Required

Q: Measures like disabling the lost device and encrypting the data on the device fall under:
A: Mobile Device Management

Q: It is the intentional hindering or interruption of the functioning of a computer system, may also involve cybersquatting:
A: System Interference

Q: Also termed as Unsolicited Commercial Communications:
A: Spamming

Q: These controls can repair damage, in addition to stopping any further damage:
A: Corrective

Q: It enables attackers to inject client-side script into Web pages viewed by other users:
A: Cross-Site Scripting

Q: This is an act of exploiting holes in unpatched or poorly configured software.
A: Shrink Wrap Code

Q: Which of the following is NOT a threat intelligence sharing standard?
A: SIEM

Q: Type of vulnerability scanner that surveys for logic errors and coding vulnerabilities:
A: Application Scanner

Q: Which of the following is NOT a goal of a stand-alone SIEM?
A: Threat and vulnerability management

Q: Examines logs and events from disparate systems or applications:
A: Correlation

Q: 'Five Nines' uptime (99.999%), failover clustering, load balancing are under which principle?
A: Availability

Q: The foundation of highly secure identification and personal verification solutions:
A: Biometrics

Q: Writes data across multiple drives so that consecutive segments are stored on different drives:
A: Striping

Q: IoT systems process data using algorithms or AI to support decision-making and automation:
A: Intelligence

Q: Which of the following is not considered a secured wireless IoT device?
A: Webcam

Q: Which of the following is NOT part of the Diamond Model of Intrusion Analysis?
A: Threat

Q: Which set of practices is applicable DURING an attack?
A: Incident Response

Q: Statement 1 - RAID prevent loops when switches interconnect via multiple paths. Statement 2 - Hardening applies to network security to the exception of IoT devices.

A: Statement 1 is False, Statement 2 is True

Q: Statement 1 - Tunneling involves the distribution of traffic between devices or network paths. Statement 2 - Corroborative is evidence that supports an assertion that is developed from best evidence.
A: Statement 1 is False, Statement 2 is True

Q: Statement 1 - Point-in-Time Replication requires high bandwidth. Statement 2 - Non-credentialed scans are less invasive and give an outsider's point of view.
A: Statement 1 is False, Statement 2 is True

Q: Statement 1 - SOAR stands for Security Orchestration Automation and Recovery. Statement 2 - Vulnerability assessments can be conducted in-house or by external contractors.
A: Statement 1 is False, Statement 2 is True

Q: Statement 1 - Correct timestamps accurately track network events such as security violations. Statement 2 - Network segmentation isolates IoT devices into dedicated network zones.
A: Both statements are True