detection and analysis

**Trend**

**Anomaly**

**Heuristic**

**Correct answer**

**Behavio**

REGEX search string

What control provides the best protection against both SQL injection and cross-site scripting attacks?

**CSRF**

**Input validation**

**Hypervisors**

**Network layer firewalls**

**SHA-256**

**AES**

**RSA**

**3DES**

**Alert volume**

**Mean time to remediate**

**buffer overflow**

**Buffer overflow exploit**

**SQL injection exploit**

**Chained exploit**

**Denial of Service exploit**

**Which of the following is NOT considered a phase in the incident response cycle?**

**Containment, eradication, and recovery**

**Preparation**

**Notification and communication**

**Detection and analysis**

**directory traversal attack**

**XML injection**

**SQL injection attack**

**port to 636**

**port 389**

**Diamond Model of Intrusion Analysis**

**True positive**

**False positive**

**True negative**

**False-negative**

**Data enrichment**

**Your answer is incorrect**

**Continuous integration**

**Machine learning**

**Deep learning**

**Purple team**

**White team**

**nmap scan of a target network types**

**telnet**

**wget**

**netcat**

**ftp**

**Pivoting**

**Lateral movement**

**Golden ticket**

**Pass the hash**

**DNS assessment technique**

**A whois query**

**Correct answer**

**A zone transfer**

**Using maltego**

**A DNS forward or reverse lookup**

**SQL injection**

[**http://ezproxy.apus.edu/login?url=https://www.oreilly.com/library/view/temporary-access/?email=%5Eu**](http://ezproxy.apus.edu/login?url=https://www.oreilly.com/library/view/temporary-access/?email=%5Eu)

**Cybsecurity frameworks**

**XSS**

**XML INJECTION**

**INCIDENT RESPONSE REPORT**

**SQL INJECTION**

**A zone transfer**

**A whois query**

**Using maltego**

**A DNS forward or reverse lookup**

**TLS or IPSec**

**BLIND SQL INJECTION**

**Acceptable User Policy (AUP)**

**BlueKeep**

**Meltdown**

**Stuxnet**

**Heartbleed**

**CONTAINERIZATION**

**Buffer overflow**

**Malicious logic**

**REGEX**

**RSA**

**AES**

**SHA-256**

**3DES**

**Virtual hosts**

**Log disposition**

**Your answer is incorrect**

**Processor utilization**

**default nmap scan type**

**PRACTICE ANALYZING LOGS**

**static analysis source code**

**Process Monitor**

**Autoruns**

**DiskMon**

**ProcDump**

**major differences between conducting reconnaissance of a wireless network versus a wired network?**

**OpenVAS**

**ScoutSuite**

**Prowler**

**Pacu**

**CVE**

**CCE**

**CPE**

**XCCDF**

**DNS resolver**

**fast flux network**

**Jumpbox**

**Bastion hosts**

**Airgap**