**CTF Challenge: Evading IDS, Firewalls, and Honeypots**

**1. Introduction**

****

Intrusion Detection Systems (IDS), Firewalls, and Honeypots are critical components in network security. IDS monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Firewalls act as barriers between trusted and untrusted networks, controlling incoming and outgoing traffic based on predetermined security rules. Honeypots are traps set to detect, deflect, or study attempts to gain unauthorized access to information systems.

**Tools and Requirements**

Nmap (with online scanning interfaces like Nmap Online)  
Shodan: <https://www.shodan.io/>

Nmap: <https://hackertarget.com/nmap-online-port-scanner/>   
URL:- [**http://testphp.vulnweb.com/**](http://testphp.vulnweb.com/)

**Scenario**

****

As a security analyst, your task is to understand and test various techniques to evade IDS, Firewalls, and Honeypots using web-based tools.

**Process to follow while performing CTF**

****

Step 1: Explore Shodan to find publicly exposed devices: (<https://www.shodan.io/>)

Step 2: For scanning the port online based:

<https://hackertarget.com/nmap-online-port-scanner/>

Step 3: Target website: [**http://testphp.vulnweb.com/**](http://testphp.vulnweb.com/)

Step 4: Target IP: 108.167.183.71

**Questions**

Flag 1: Use OWASP ZAP to scan a web application. What is the name of the discovered vulnerability?

Answer: XSS (Cross-Site Scripting)

Flag Captured.

Flag 2: With Nmap Online, perform a scan on a target. What firewall rule is detected?

Answer: Filtered port 22 (SSH)

Flag Captured.

Flag Captured.

Hint

Use the tutorials and documentation provided by each tool to understand how to perform scans and analyze results. Look for common patterns and behaviors that can indicate the presence of security measures like IDS, Firewalls, and Honeypots.

