- **Vendor:** **CompTIA**
- **Exam Code:** **PT0-001**
- **Exam Name:** **CompTIA PenTest+ Exam**
- **New Updated Questions from Braindump2go (Updated in Nov./2020)**

Visit Braindump2go and Download Full Version PT0-001 Exam Dumps

QUESTION 194
Software developers should escape all characters (including spaces but excluding alphanumeric characters) with the HTML entity &#xHH; format to prevent what type of attack?

A. DDoS attacks
B. XSS attacks
C. CSRF attacks
D. Brute-force attacks

Answer: B

QUESTION 195
A security consultant finds a folder in "C VProgram Files" that has writable permission from an unprivileged user account Which of the following can be used to gam higher privileges?

A. Retrieving the SAM database
B. Kerberoasting
C. Retrieving credentials in LSASS
D. DLL hijacking
E. VM sandbox escape

Answer: C

QUESTION 196
Which of the following documents BEST describes the manner in which a security assessment will be conducted?

A. BIA
B. SOW
C. SLA
D. MSA

Answer: A

QUESTION 197
A penetration tester found a network with NAC enabled Which of the following commands can be used to bypass the NAC?

A. macchanger
B. sslbump
C. iptafcles

D. proxychains

Answer: A

QUESTION 198

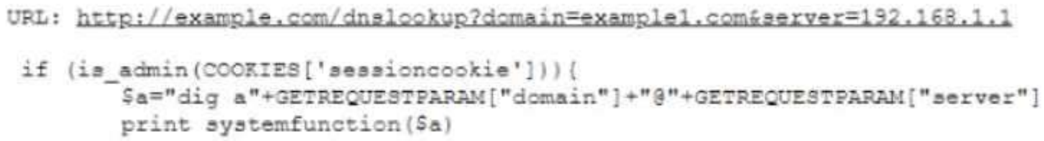
An internal network penetration test is conducted against a network that is protected by an unknown NAC system In an effort to bypass the NAC restrictions the penetration tester spoofs the MAC address and hostname of an authorized system Which of the following devices if impersonated would be MOST likely to provide the tester with network access?

A. Network-attached printer
B. Power-over-Ethernet injector
C. User workstation
D. Wireless router

Answer: A

QUESTION 199

A penetration tester is performing a code review against a web application Given the following URL and source code:



```
URL: http://example.com/dnslookup?domain=example1.com&server=192.168.1.1

 if (is_admin(COOKIES['sessioncookie'])){
        $a="dig a"+GETREQUESTPARAM["domain"]+"@"+GETREQUESTPARAM["server"]
        print systemfunction($a)
```

Which of the following vulnerabilities is present in the code above?

A. SQL injection
B. Cross-site scripting
C. Command injection
D. LDAP injection

Answer: C

QUESTION 200

After an Nmap NSE scan, a security consultant is seeing inconsistent results while scanning a host.
Which of the following is the MOST likely cause?

A. Services are not listening
B. The network administrator shut down services
C. The host was not reachable
D. A firewall/IPS blocked the scan

Answer: D

QUESTION 201

Which of the following wordlists is BEST for cracking MD5 password hashes of an application's users from a compromised database?

A. . /wordlists/rockyou.txt
B. ./dirb/wordlists/big.txt
C. ./wfuzz/wordlist"vulns/sq1_inj -txt
D. ./wordlists/raeta3ploit/roet_uaerpass.txt

Answer: A

QUESTION 202

A penetration tester calls human resources and begins asking open-ended questions Which of the following social engineering techniques is the penetration tester using?

A. Interrogation
B. Elicitation
C. Impersonation
D. Spear phishing

Answer: B

QUESTION 203
An attacker is attempting to gain unauthorized access to a WiR network that uses WPA2-PSK Which of the following attack vectors would the attacker MOST likely use?

A. Capture a three-way handshake and crack it
B. Capture a mobile device and crack its encryption
C. Create a rogue wireless access point
D. Capture a four-way handshake and crack it

Answer: D

QUESTION 204
The SELinux and AppArmor security frameworks include enforcement rules that attempt to prevent which of the following attacks?

A. Lateral movement
B. Sandbox escape
C. Cross-site request forgery (CSRF)
D. Cross-site- scripting (XSS)

Answer: B