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

QUESTION 205
A _______ vulnerability scan would typically be focused on a specific set of requirements.

A. Full
B. Stealth
C. Compliance
D. Discovery

Answer: C

QUESTION 206
Which of the following can be used for post-exploitation activities?

A. WinDbg
B. IDA
C. Maltego
D. PowerShell

Answer: D

QUESTION 207
Which of the following can be used to perform online password attacks against RDP?

A. Hashcat
B. John the Rippef
C. Aircrack-ng
D. Ncrack

Answer: D

QUESTION 208
A company received a report with the following finding While on the internal network the penetration tester was able to successfully capture SMB broadcasted user ID and password information on the network and decode this information This allowed the penetration tester to then join their own computer to the ABC domain Which of the following remediation's are appropriate for the reported findings'? (Select TWO)

A. Set the Schedule Task Service from Automatic to Disabled
B. Enable network-level authentication
C. Remove the ability from Domain Users to join domain computers to the network
D. Set the netlogon service from Automatic to Disabled

E. Set up a SIEM alert to monitor Domain joined machines
F. Set "Digitally sign network communications" to Always

Answer: BC

QUESTION 209
Which of the following actions BEST matches a script kiddie's threat actor?

A. Exfiltrate network diagrams to perform lateral movement
B. Steal credit cards from the database and sell them in the deep web
C. Install a rootkit to maintain access to the corporate network
D. Deface the website of a company in search of retribution

Answer: B

QUESTION 210
A penetration tester has compromised a system and wishes to connect to a port on it from the attacking machine to control the system Which of the following commands should the tester run on the compromised system?

A. nc looalhot 4423
B. nc -nvlp 4423 -?/bin/bash
C. nc 10.0.0.1 4423
D. nc 127.0.0.1 4423 -e /bin/bash

Answer: B

QUESTION 211
An organization has requested that a penetration test be performed to determine if it is possible for an attacker to gain a foothold on the organization's server segment During the assessment, the penetration tester identifies tools that appear to have been left behind by a prior attack Which of the following actions should the penetration tester take?

A. Attempt to use the remnant tools to achieve persistence
B. Document the presence of the left-behind tools in the report and proceed with the test
C. Remove the tools from the affected systems before continuing on with the test
D. Discontinue further testing and report the situation to management

Answer: A

QUESTION 212
A penetration tester has obtained access to an IP network subnet that contains ICS equipment intercommunication. Which of the following attacks is MOST likely to succeed in creating a physical effect?

A. DNS cache poisoning
B. Record and replay
C. Supervisory server SMB
D. Blind SQL injection

Answer: A

QUESTION 213
Which of the following BEST describes the difference between a red team engagement and a penetration test?

A. A penetration test has a broad scope and emulates advanced persistent threats while a red team engagement has a limited scope and focuses more on vulnerability identification
B. A red team engagement has a broad scope and emulates advanced persistent threats, while a

penetration test has a limited scope and focuses more on vulnerability identification

C. A red team engagement has a broad scope and focuses more on vulnerability identification, while a penetration test has a limited scope and emulates advanced persistent threats

D. A penetration test has a broad scope and focuses more on vulnerability identification while a red team engagement has a limited scope and emulates advanced persistent threats

Answer: D