**HIGHER QUALITY**
**BETTER SERVICE**

# CERTTREE

## QUESTION & ANSWER


Provide One Year
Free Update!

https://www.certtree.com

**Exam** : **SY0-501**

**Title** : CompTIA Security+

**Version** : DEMO

1.A high-security defense installation recently began utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation.
Which of the following types of controls does this BEST describe?
A. Deterrent
B. Preventive
C. Detective
D. Compensating
**Answer:** A

2.An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection.
Which of the following steps should the responder perform NEXT?
A. Capture and document necessary information to assist in the response.
B. Request the user capture and provide a screenshot or recording of the symptoms
C. Use a remote desktop client to collect and analyze the malware m real time
D. Ask the user to back up files for later recovery
**Answer:** A

3.Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations.
Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?
A. Shibboleth
B. RADIUS federation
C. SAML
D. OAuth
E. OpenID connect
**Answer:** B
**Explanation:**
http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html

4.An analyst wants to implement a more secure wifeless authentication for office access points.
Which of the following technologies allows for encrypted authentication of wireless clients over TLS?
A. PEAP
B. EAP
C. WPA2
D. RADIUS
**Answer:** A
**Explanation:**
EAP by itself is only an authentication framework.
PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated.
The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel are protected. As a result, when EAP

messages are able to be discovered in the “clear” they do not provide the protection that was assumed when the protocol was originally authored.
PEAP, EAP-TTLS, and EAP-TLS “protect” inner EAP authentication within SSL/TLS sessions.

5.A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation.
Given these requirements, which of the following technologies should the analyst recommend and configure?
A. LDAP services
B. Kerberos services
C. NTLM services
D. CHAP services
**Answer:** B
**Explanation:**
Only Kerberos that can do Mutual Auth and Delegation.
https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview