Vendor:GIAC

Exam Code:GPEN

Exam Name:GIAC Certified Penetration Tester

Version: Demo

QUESTION 1

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP

B. Implement WPA

C. Don\\'t broadcast SSID

D. Implement MAC filtering

Correct Answer: C

QUESTION 2

Which of the following tools are used for footprinting?

Each correct answer represents a complete solution. Choose all that apply.

A. Brutus

B. Sam spade

C. Whois

D. Traceroute

Correct Answer: BCD

QUESTION 3

During a penetration test you discover a valid set of SSH credentials to a remote system. How can this be used to your advantage in a Nessus scan?

A. This information can be entered under the \\'Hydra\\' tab to launch a brute-forcepassword attack.

B. There isn\\'t an advantage as Nessus will ultimately discover this information.

C. The "SSH\\' box can be checked to let Nessus know the remote system is running

D. This information can be entered under the \\'credentials\\' tab to allow Nessus to log into the system

Correct Answer: C

QUESTION 4

Which type of Cross-Sire Scripting (XSS> vulnerability is hardest for automated testing tools to detect, and for what

reason?

A. Stored XSS. because it may be located anywhere within static or dynamic sitecontent

B. Stored XSS. because it depends on emails and instant messaging systems.

C. Reflected XSS. because It can only be found by analyzing web server responses.

D. Reflected XSS: because it is difficult to find within large web server logs.

Correct Answer: A

QUESTION 5

Which of the following are the countermeasures against WEP cracking? Each correct answer represents a part of the solution. Choose all that apply.

A. Using the longest key supported by hardware.

B. Using a 16 bit SSID.

C. Changing keys often.

D. Using a non-obvious key.

Correct Answer: ACD

QUESTION 6

Which of the following tools can be used to find a username from a SID?

A. SNMPENUM

B. SID

C. SID2User

D. SIDENUM

Correct Answer: C

QUESTION 7

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He performs a Teardrop attack on the we-are-secure server and observes that the server crashes. Which of the following is the most likely cause of the server crash?

A. The spoofed TCP SYN packet containing the IP address of the target is filled in both the source and destination fields.

B. The we-are-secure server cannot handle the overlapping data fragments.

C. The ICMP packet is larger than 65,536 bytes.

D. Ping requests at the server are too high.

Correct Answer: B

QUESTION 8

When DNS is being used for load balancing, why would a penetration tester choose to identify a scan target by its IP address rather than its host name?

A. Asingle IP may have multiple domains.

B. A single domain name can only have one IP address.

C. Scanning tools only recognize IP addresses

D. A single domain name may have multiple IP addresses.

Correct Answer: C

Reference: http://www.flashcardmachine.com/sec-midterm.html

QUESTION 9

The employees of CCN Inc. require remote access to the company\\'s proxy servers. In order to provide solid wireless security, the company uses LEAP as the authentication protocol. Which of the following is supported by the LEAP protocol? Each correct answer represents a complete solution. Choose all that apply.

A. Public key certificate for server authentication

B. Password hash for client authentication

C. Strongest security level

D. Dynamic key encryption

Correct Answer: BD

QUESTION 10

LM hash is one of the password schemes that Microsoft LAN Manager and Microsoft Windows versions prior to the Windows Vista use to store user passwords that are less than 15 characters long. If you provide a password seven characters or less, the second half of the LM hash is always _____.

A. 0xAAD3B435B51404EE

B. 0xBBD3B435B51504FF

C. 0xBBC3C435C51504EF

D. 0xAAD3B435B51404FF

Correct Answer: A

QUESTION 11

Which of the following tools is an example of HIDS?

A. Anti-Spector

B. Auditpol.exe

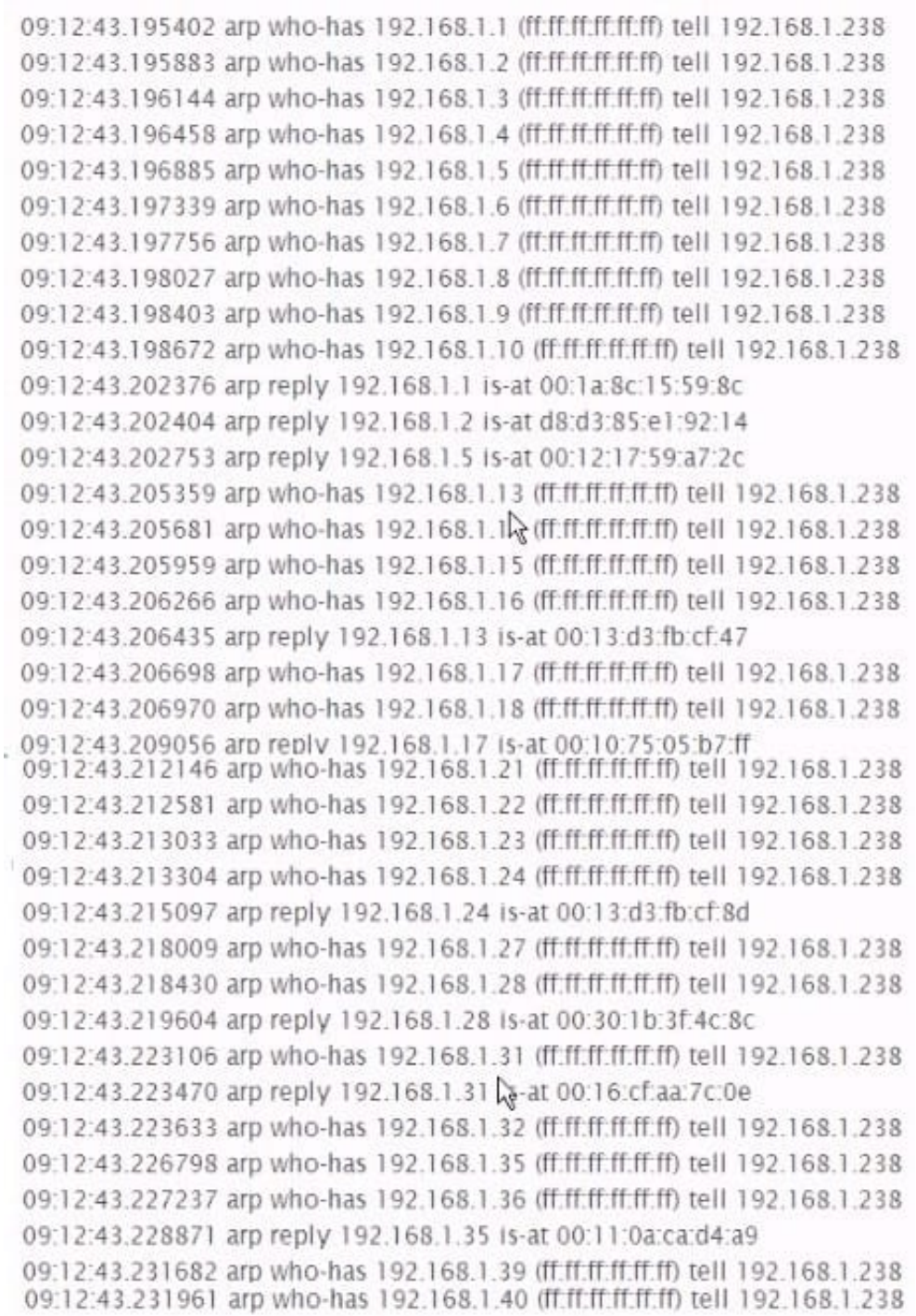
C. Elsave

D. Log File Monitor

Correct Answer: D

QUESTION 12

Identify the network activity shown below; A. A sweep of available hosts on the local subnet



B. A flood of the local switch\\'s CAM table.

C. An attempt to disassociate wireless clients.

D. An attempt to impersonate the local gateway

Correct Answer: D