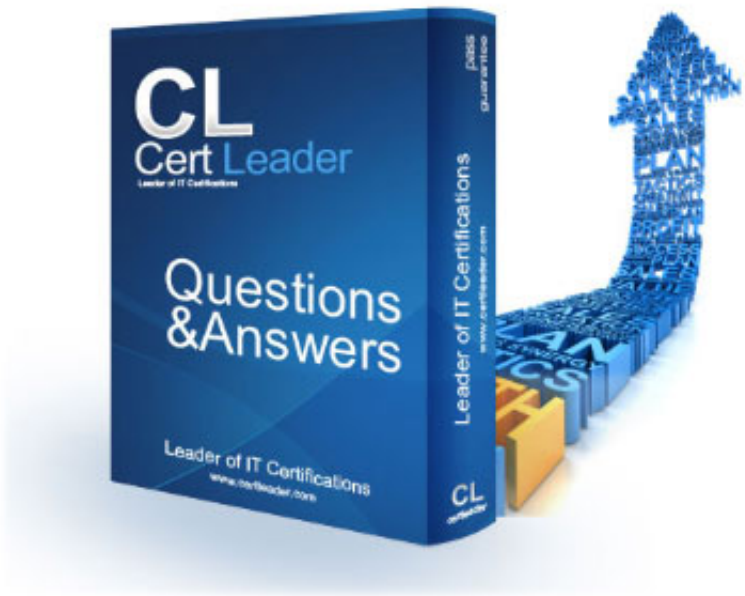
GPEN - GIAC Certified Penetration Tester

https://www.certleader.com/GPEN-dumps.html



1. What is the main difference between LAN MAN and NTLMv1 challenge/responses?

A. NTLMv1 only pads IS bytes, whereas LANMAN pads to 21 bytes

B. NTLMv1 starts with the NT hash, whereas LANMAN starts with the LANMAN hash

C. NTLMv1utilizes DES, whereas LANMAN utilizes MD4

D. NTLMv1 splits the hash into 3 eight-byte pieces, whereas LAN MAN splits the hash Into 3 seven-byte pieces

Answer: A

2. You are conducting a penetration test for a private company located in Canada. The scope extends to all internal-facing hosts controlled by the company. You have gathered necessary hold-harmless and non-disclosure agreements. Which action by your group can incur criminal liability under Criminal Code of Canada Sections 184 and 542 CC 184?

A. Analyzing internal firewall router software for vulnerabilities

B. Exploiting application vulnerabilities on end-user workstations

C. Attempting to crack passwords on a development server

D. Capturing a VoIP call to a third party without prior notice

Answer: D

3. You are pen testing a Windows system remotely via a raw netcat shell. You want to get a listing of all the local users in the administrators group, what command would you use?

A. Net account administrators

B. Net user administrators

C. Net localgroup administrators

D. Net localuser administrators

Answer: C

4. What problem occurs when executing the following command from within a netcat raw shell? sudo cat /etc/shadow

A. Sudo does not work at all from a shell

B. Sudo works fine if the user and command are both in the /etc/sudoers file

C. The display blanks after typing the sudo command

D. You will not be able to type the password at the password prompt

Answer: A

5. You are running a vulnerability scan on a remote network and the traffic Is not making It to the target system. You investigate the connection issue and determine that the traffic is making it to the internal interface of your network firewall, but not making. It to the external Interface or to any systems outside your firewall. What is the most likely problem?

A. Your network firewall is blocking the traffic

B. The NAT or pat tables on your network based firewall are filling up and droppingthe traffic

C. A host based firewall is blocking the traffic

D. Your ISP Is blocking the traffic

Answer: C

6. You are done pen testing a Windows system and need to clean up some of the changes you have made. You created an account ‘pentester’ on the system, what command would you use to delete that account?

A. Net user pentester /del

B. Net name pentester /del

C. Net localuser pentester /del

D. Net account pentester /del

Answer: D

7. Raw netcat shells and telnet terminals share which characteristic?

A. Ability to send commands to a target machine.

B. Ability to adapt output to the size of display window

C. Shells and terminals are exactly the same.

D. Ability to process standard output control sequences.

Answer: D

Explanation: Reference:

http://tartarus.org/~simon/putty-snapshots/htmldoc/Chapter3.html

8. You suspect that system administrators In one part of the target organization are turning off their systems during the times when penetration tests are scheduled, what feature could you add to the ' Rules of engagement' that could help your team test that part of the target organization?

A. Un announced test

B. Tell response personnel the exact lime the test will occur

C. Test systems after normal business hours

D. Limit tests to business hours

Answer: C

9. 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.

Answer: A

10. You suspect that a firewall or IPS exists between you and the target machine. Which nmap option will elicit responses from some firewalls and IPSs while being silently dropped by the target, thus confirming the existence of a firewall or IPS?

A. –Traceroute

B. –Firewalk

C. –Badsum

D. --SF

Answer: B

11. You successfully compromise a target system's web application using blind command injection. The command you injected is ping-n 1 192.168.1.200. Assuming your machine is

192.168.1 200, which of the following would you see?

A. Ping-n 1 192.168.1 200 on the compromised system

B. A 'Destination host unreachable' error message on the compromised system

C. A packet containing 'Packets: Sent - 1 Received = 1, Loss = 0 (0% loss) on yoursniffer

D. An ICMP Echo packet on your sniffer containing the source address of the target

Answer: A

12. Which of the following modes describes a wireless interface that is configured to passively grab wireless frames from one wireless channel and pass them to the operating system?

A. Monitor Mode

B. Promiscuous Mode

C. Managed Mode

D. Master Mode

Answer: C

Explanation: Reference:

http://www.willhackforsushi.com/books/377_eth_2e_06.pdf

13. While performing a code audit, you discover a SQL injection vulnerability assuming the following vulnerable query, what user input could be injected to make the query true and return data?

select * from widgets where name = '[user-input]';

A. 'or 1=1

B. ‘or l=l…

C. 'or 1=1--

D. ‘or l=1’

Answer: D

14. How can a non-privileged user on a Unix system determine if shadow passwords are being used?

A. Read /etc/password and look for "x" or “II” in the second colon-delimited field

B. Read /etc/shadow and look for “x” or “II” in the second colon-delimited field

C. Verify that /etc/password has been replaced with /etc/shadow

D. Read /etc/shadow and look NULL values In the second comma delimited field

Answer: B

15. ACME corporation has decided to setup wireless (IEEE 802.11) network in it's sales branch at Tokyo and found that channels 1, 6, 9,11 are in use by the neighboring offices. Which is the best channel they can use?

A. 4

B. 5

C. 10

D. 2

Answer: D

16. Given the following Scapy information, how is default Layer 2 information derived?

```
>>> packet=Ether()/IP(src="10.10.10.9",dst="10.10.10.10")/TCP(dport=80)/"GET / HTTP/1.1"
>>> packet.summary
<bound method="" ether.summary="" of="" type="0x800" frag="0" proto="tcp" src="10.10.10.9"
dst="10.10.10.10" dport="http" load="GET / HTTP/1.1">>>>> </bound>
```

A. The default layer 2 information is contained in a local scapy.cfg configuration fileon the local system.

B. If not explicitly defined, the Ether type field value Is created using the hex value ofthe destination port, in this case 80

C. If not explicitly defined, pseudo-random values are generated for the Layer 2 defaultinformation.

D. Scapy relies on the underlying operating system to construct Layer 2 information touse as default.

Answer: C

17. 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.

Answer: C

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

18. What section of the penetration test or ethical hacking engagement final report is used to detail and prioritize the results of your testing?

A. Methodology

B. Conclusions

C. Executive Summary

D. Findings

Answer: C

19. Why is OSSTMM beneficial to the pen tester?

A. It provides a legal and contractual framework for testing

B. It provides in-depth knowledge on tools

C. It provides report templates

D. It includes an automated testing engine similar to Metasploit

Answer: C

Explanation: Reference:

http://www.pen-tests.com/open-source-security-testing-methodology-manual-osstmm.html

20. You are conducting a penetration test for a private company located in the UK. The scope

extends to all internal and external hosts controlled by the company. You have gathered necessary hold-harmless and non-disclosure agreements. Which action by your group can incur criminal liability under the computer Misuse Act of 1990?

A. Sending crafted packets to internal hosts in an attempt to fingerprint the operatingsystems

B. Recovering the SAM database of the domain server and attempting to crackpasswords

C. Installing a password sniffing program on an employee's personal computer withoutconsent

D. Scanning open ports on internal user workstations and exploiting vulnerableapplications

Answer: B

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your GPEN Exam with Our Prep Materials Via below:

https://www.certleader.com/GPEN-dumps.html