Vendor: EC-Council

Exam Code: 312-50v9

Exam Name: Certified Ethical Hacker v9

Version: DEMO

QUESTION 1
You have successfully comprised a server having an IP address of 10.10.0.5.
You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?

A. nmap -T4 -F 10.10.0.0/24
B. nmap -T4 -r 10.10.1.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -q 10.10.0.0/24

Answer: A
Explanation:
command = nmap -T4 -F
description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.
https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

QUESTION 2
You have compromised a server on a network and successfully opened a shell.
You aimed to identify all operating systems running on the network.
However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!
```

What seems to be wrong?

A. OS Scan requires root privileges.
B. The nmap syntax is wrong.
C. This is a common behavior for a corrupted nmap application.
D. The outgoing TCP/IP fingerprinting is blocked by the host firewall.

Answer: A
Explanation:
You requested a scan type which requires root privileges.
http://askubuntu.com/questions/433062/using-nmap-for-information-regarding-web-host

QUESTION 3
Which of the following statements is TRUE?

A. Sniffers operate on Layer 2 of the OSI model
B. Sniffers operate on Layer 3 of the OSI model
C. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
D. Sniffers operate on the Layer 1 of the OSI model.

Answer: A
Explanation:
The OSI layer 2 is where packet sniffers collect their data.
https://en.wikipedia.org/wiki/Ethernet_frame

QUESTION 4
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?

A. c:\compmgmt.msc
B. c:\services.msc
C. c:\ncpa.cp
D. c:\gpedit

Answer: A
Explanation:
To start the Computer Management Console from command line just type compmgmt.msc / computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
http://www.waynezim.com/tag/compmgmtmsc/

QUESTION 5
What is the best description of SQL Injection?

A. It is an attack used to gain unauthorized access to a database.
B. It is an attack used to modify code in an application.
C. It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
D. It is a Denial of Service Attack.

Answer: A
Explanation:
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
https://en.wikipedia.org/wiki/SQL_injection

QUESTION 6
Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications
B. Register all machines MAC Address in a Centralized Database
C. Restrict Physical Access to Server Rooms hosting Critical Servers
D. Use Static IP Address

Answer: A
Explanation:
A way to protect your network traffic from being sniffed is to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn't prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet's payload so that all the sniffer sees is encrypted gibberish.
http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

QUESTION 7
You have successfully gained access to a linux server and would like to ensure that the

succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?

A. Encryption
B. Protocol Isolation
C. Alternate Data Streams
D. Out of band signalling

Answer: A
Explanation:
When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.
http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/

QUESTION 8
You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?

```
alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!";)
```

A. An Intrusion Detection System
B. A firewall IPTable
C. A Router IPTable
D. FTP Server rule

Answer: A
Explanation:
Snort is an open source network intrusion detection system (NIDS) for networks .
Snort rule example:
This example is a rule with a generator id of 1000001.
alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)
http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

QUESTION 9
What is the benefit of performing an unannounced Penetration Testing?

A. The tester will have an actual security posture visibility of the target network.
B. Network security would be in a "best state" posture.
C. It is best to catch critical infrastructure unpatched.
D. The tester could not provide an honest analysis.

Answer: A
Explanation:
Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry.
A possible solution to this danger is to conduct intermittent "unannounced" penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management

staff instead of every security employee, as would be the case with "announced" penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.
http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

QUESTION 10
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?

A. ICMP could be disabled on the target server.
B. The ARP is disabled on the target server.
C. TCP/IP doesn't support ICMP.
D. You need to run the ping command with root privileges.

Answer: A
Explanation:
The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

QUESTION 11
Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test state.
Which of the following activities should not be included in this phase? (see exhibit)

I. Removing all files uploaded on the system

II. Cleaning all registry entries

III. Mapping of network state

IV. Removing all tools and maintaining backdoor for reporting

A. III
B. IV
C. III and IV
D. All should be included.

Answer: A
Explanation:
The post-attack phase revolves around returning any modified system(s) to the pretest state.
Examples of such activities:
Removal of any files, tools, exploits, or other test-created objects uploaded to the system during testing
Removal or reversal of any changes to the registry made during system testing
Computer and Information Security Handbook, John R. Vacca (2012), page 531

QUESTION 12
It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.
Which of the following regulations best matches the description?

A. HIPAA
B. ISO/IEC 27002
C. COBIT
D. FISMA

Answer: A
Explanation:
The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)[15] By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".
https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

QUESTION 13
Which of the following is a component of a risk assessment?

A. Administrative safeguards
B. Physical security
C. DMZ
D. Logical interface

Answer: A
Explanation:
Risk assessment include:
The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources.
It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.
The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources.
It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.
https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

QUESTION 14
A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?

A. Delegate
B. Avoid
C. Mitigate
D. Accept

Answer: A
Explanation:
There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.
http://www.dbpmanagement.com/15/5-ways-to-manage-risk

QUESTION 15
Your company was hired by a small healthcare provider to perform a technical assessment on the network.
What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use a scan tool like Nessus
B. Use the built-in Windows Update tool
C. Check MITRE.org for the latest list of CVE findings
D. Create a disk image of a clean Windows installation

Answer: A
Explanation:
Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.
The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix-or Windows-based operating systems.
Note: Significant capabilities of Nessus include:
- Compatibility with computers and servers of all sizes.
- Detection of security holes in local or remote hosts.
- Detection of missing security updates and patches.
- Simulated attacks to pinpoint vulnerabilities.
- Execution of security tests in a contained environment.
- Scheduled security audits.

QUESTION 16
Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability.
What is this style of attack called?

A. zero-day
B. zero-hour
C. zero-sum
D. no-day

Answer: A
Explanation:
Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon.
Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software.
https://en.wikipedia.org/wiki/Stuxnet

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**