Certified Ethical Hacker

Exam Preparation

Sample Questions with Answers

Collected By: Mohammad Alkhudari

Green Circle Co.

@May-2023

I. What is the focus of a security audit or vulnerability assessment?

- A) Locating vulnerabilities
- B) Locating threats
- C) Enacting threats
- D) Exploiting vulnerabilities

Show Answer

The Correct Answer is:- A

II. What kind of physical access device restricts access to a single individual at any one time?

- A) Checkpoint
- B) Perimeter security
- C) Security zones
- D) Mantrap

Show Answer

The Correct Answer is:- D

III. Which of the following is a mechanism for managing digital certificates through a system of trust?

- A) PKI
- B) PKCS
- C) ISA
- D) SSL

Show Answer

The Correct Answer is:- A

---

4. Which protocol is used to create a secure environment in a wireless network?

- A) WAP
- B) WPA
- C) WTLS
- D) WML

Show Answer

The Correct Answer is:- B

5. What type of exercise is conducted with full knowledge of the target environment?

- A) White box
- B) Gray box
- C) Black box
- D) Glass box

Show Answer

The Correct Answer is:- A

---

6. You want to establish a network connection between two LANs using the Internet. Which technology would best accomplish that for you?

- A) IPSec
- B) L2TP
- C) PPP
- D) SLIP

Show Answer

The Correct Answer is:- B

---

7. Which design concept limits access to systems from outside users while protecting users and systems inside the LAN?

- A) DMZ
- B) VLAN
- C) I&A
- D) Router

Show Answer

The Correct Answer is:- A

---

8. In the key recovery process, which key must be recoverable?

- A) Rollover key
- B) Secret key
- C) Previous key
- D) Escrow key

Show Answer

The Correct Answer is:- D

---

9. Which kind of attack is designed to overload a system or resource, taking it temporarily or permanently offline?

- A) Spoofing
- B) Trojan
- C) Man in the middle
- D) SYN flood

Show Answer

The Correct Answer is:- D

---

10. Which component of an NIDS collects data?

- A) Data source
- B) Sensor
- C) Event
- D) Analyzer

Show Answer

The Correct Answer is:- B

---

11. What is the process of making an operating system secure from attack called?

- A) Hardening
- B) Tuning
- C) Sealing
- D) Locking down

Show Answer

The Correct Answer is:- A

---

12. The integrity component provides which feature of the CIA triad?

- A) Verification that information is accurate
- B) Verification that ethics are properly maintained
- C) Establishment of clear access control of data
- D) Verification that data is kept private and secure

Show Answer

The Correct Answer is:- A

---

13. Which mechanism is used by PKI to allow immediate verification of a certificate's validity?

- A) CRL
- B) MD5
- C) SSHA
- D) OCSP

Show Answer

The Correct Answer is:- D

---

14. Which of the following is used to create a VLAN from a physical security perspective?

- A) Hub
- B) Switch
- C) Router
- D) Firewall

Show Answer

The Correct Answer is:- B

---

15. A user has just reported that he downloaded a file from a prospective client using IM. The user indicates that the file was called account.doC) The system has been behaving unusually since he downloaded the file. What is the most likely event that occurred?

- A) Your user inadvertently downloaded a macro virus using IM.
- B) Your user may have downloaded a rootkit.
- C) Your user may have accidently changed a setting on the system.
- D) The system is unstable due to the use of IM.

Show Answer

The Correct Answer is:- A

---

16. Which mechanism or process is used to enable or disable access to a network resource based on attacks that have been detected?

- A) NIDS
- B) NIPS
- C) NITS
- D) NADS

Show Answer

The Correct Answer is:- B

---

17. Which of the following would provide additional security to an Internet web server?

- A) Changing the default port for traffic to 80
- B) Changing the default port for traffic to 1019
- C) Changing the default port for traffic to 443
- D) Changing the default port for traffic to 161

Show Answer

The Correct Answer is:- C

---

18. What type of program exists primarily to propagate and spread itself to other systems and can do so without interaction from users?

- A) Virus
- B) Trojan horse
- C) Logic bomb
- D) Worm

Show Answer

The Correct Answer is:- D

---

19. An individual presents herself at your office claiming to be a service technician. She is attempting to discuss technical details of your environment such as applications, hardware, and personnel used to manage it. This may be an example of what type of attack?

- A) Social engineering
- B) Access control

- C) Perimeter screening
- D) Behavioral engineering

Show Answer

The Correct Answer is:- A

---

20. Which of the following is a major security problem with FTP?

- A) Password files are stored in an unsecure area on disk.
- B) Memory traces can corrupt file access.
- C) User IDs and passwords are unencrypted.
- D) FTP sites are unregistered.

Show Answer

The Correct Answer is:- C

---

21. Which system would you install to provide detective capabilities within a network?

- A) NIDS
- B) HIDS
- C) NIPS
- D) HIPS

Show Answer

The Correct Answer is:- A

---

22. The process of maintaining the integrity of evidence and ensuring no gaps in possession occur is known as what?

- A) Security investigation
- B) Chain of custody
- C) Three As of investigation
- D) Security policy

Show Answer

The Correct Answer is:- B

---

23. What encryption process uses one piece of information as a carrier for another?

- A) Steganography
- B) Hashing
- C) MDA
- D) Cryptointelligence

Show Answer

The Correct Answer is:- A

---

24. Which policy dictates how assets can be used by employees of a company?

- A) Security policy
- B) User policy
- C) Use policy
- D) Enforcement policy
- E. Acceptable use policy

Show Answer

The Correct Answer is:- E

---

25. Which algorithm is an asymmetric encryption protocol?

- A) RSA
- B) AES
- C) DES
- D) 3DES

Show Answer

The Correct Answer is:- A

---

26. Which of the following is an example of a hashing algorithm?

- A) ECC
- B) PKI
- C) SHA
- D) MD

Show Answer

The Correct Answer is:- C

---

27. Which of the following creates a fixed-length output from a variable-length input?

- A) MD5
- B) MD7
- C) SHA12
- D) SHA8

Show Answer

The Correct Answer is:- A

---

28. Granting access to a system based on a factor such as an individual's retina during a scan is an example of what type of authentication method?

- A) Smart card
- B) I&A
- C) Biometrics
- D) CHAP

Show Answer

The Correct Answer is:- C

---

29. What item is also referred to as a physical address to a computer system?

- A) MAC
- B) DAC
- C) RBAC
- D) STAC

Show Answer

The Correct Answer is:- A

---

30. What is the process of investigating a computer system for information relating to a security incident?

- A) Computer forensics
- B) Virus scanning
- C) Security policy
- D) Evidence gathering

Show Answer

The Correct Answer is:- A

31. Which of the following is seen as a replacement for protocols such as Telnet and FTP?

- A) SSL
- B) SCP
- C) Telnet2
- D) SSH

Show Answer

The Correct Answer is:- D

32. Which of the following is commonly used to create thumbprints for digital certificates?

- A) MD5
- B) MD7
- C) SHA12
- D) SHA8

Show Answer

The Correct Answer is:- A

33. Granting access to a system based on a factor such as a password is an example of what?

- A) Something you have
- B) Something you know
- C) Something you are
- D) Something you smell

Show Answer

The Correct Answer is:- B

34. What item is also referred to as a logical address to a computer system?

- A) IP address
- B) IPX address
- C) MAC address
- D) SMAC address

Show Answer

The Correct Answer is:- A

---

35. How many bits are in an IPv6 address?

- A) 32
- B) 64
- C) 128
- D) 256

Show Answer

The Correct Answer is:- C

SECTION 3:

Total No. of Questions = 20

---

1. Enumeration is useful to system hacking because it provides _____.

- A) Passwords
- B) IP ranges
- C) Configuration
- D) Usernames

Show Answer

The Correct Answer is:- A,D

---

2. What does the enumeration phase not discover?

- A) Services
- B) User accounts
- C) Ports
- D) Shares

Show Answer

The Correct Answer is:- C

---

3. How would you use Netcat to set up a server on a system?

- A) nc –l –p 192.168.1.1
- B) nc –l –p 1000
- C) nc –p –u 1000
- D) nc –l –p –t 192.168.1.1

Show Answer

The Correct Answer is:- A

---

4. _____ is the process of exploiting services on a system.

- A) System hacking
- B) Privilege escalation
- C) Enumeration
- D) Backdoor

Show Answer

The Correct Answer is:- A

---

5. How is a brute-force attack performed?

- A) By trying all possible combinations of characters
- B) By trying dictionary words
- C) By capturing hashes
- D) By comparing hashes

Show Answer

The Correct Answer is:- A

---

6. A _____ is a type of offline attack.

- A) Cracking attack
- B) Rainbow attack
- C) Birthday attack
- D) Hashing attack

Show Answer

The Correct Answer is:- B

---

7. An attacker can use a(n) _____ to return to a system.

- A) Backdoor
- B) Cracker
- C) Account
- D) Service

Show Answer

The Correct Answer is:- A

---

8. A _____ is used to represent a password.

- A) NULL session
- B) Hash
- C) Rainbow table
- D) Rootkit

Show Answer

The Correct Answer is:- B

---

9. A _____ is a file used to store passwords.

- A) Network
- B) SAM
- C) Database
- D) NetBIOS

Show Answer

The Correct Answer is:- B

---

10. _____ is a hash used to store passwords in older Windows systems.

- A) LM
- B) SSL
- C) SAM
- D) LMv2

Show Answer

The Correct Answer is:- A

---

11. _____ is used to partially encrypt the SAM.

- A) SYSKEY
- B) SAM

- C) NTLM
- D) LM

Show Answer

The Correct Answer is:- A

---

12. Which system should be used instead of LM or NTLM?

- A) NTLMv2
- B) SSL
- C) Kerberos
- D) LM

Show Answer

The Correct Answer is:- C

---

13. NTLM provides what benefit versus LM?

- A) Performance
- B) Security
- C) Mutual authentication
- D) SSL

Show Answer

The Correct Answer is:- B

---

14. ADS requires what to be present?

- A) SAM
- B) Domain
- C) NTFS
- D) FAT

Show Answer

The Correct Answer is:- C

---

15. What utility may be used to stop auditing or logging of events?

- A) ADS
- B) LM
- C) NTFS
- D) Auditpol

Show Answer

The Correct Answer is:- D

16. On newer Windows systems, what hashing mechanism is disabled?

- A) Kerberos
- B) LM
- C) NTLM
- D) NTLMv2

Show Answer

The Correct Answer is:- B

---

17. Which of the following is a utility used to reset passwords?

- A) TRK
- B) ERC
- C) WinRT
- D) IRD

Show Answer

The Correct Answer is:- A

---

18. A good defense against password guessing is _____.

- A) Complex passwords
- B) Password policy
- C) Fingerprints
- D) Use of NTLM

Show Answer

The Correct Answer is:- A

---

19. If a domain controller is not present, what can be used instead?

- A) Kerberos
- B) LM
- C) NTLMv1
- D) NTLMv2

Show Answer

The Correct Answer is:- D

---

20. Alternate Data Streams are supported in which file systems?

- A) FAT16

- B) FAT32
- C) NTFS
- D) CDFS

Show Answer

The Correct Answer is:- C

SECTION 5:

Total No. of Questions = 20

---

1. Which of the following best describes a web application?

- A) Code designed to be run on the client
- B) Code designed to be run on the server
- C) SQL code for databases
- D) Targeting of web services

Show Answer

The Correct Answer is:- B

---

2. _____ is a client-side scripting language.

- A) JavaScript
- B) ASP
- C) ASP.NET
- D) PHP

Show Answer

The Correct Answer is:- A

---

3. Which of the following is an example of a server-side scripting language?

- A) JavaScript
- B) PHP
- C) SQL
- D) HTML

Show Answer

The Correct Answer is:- B

---

4. Which of the following is used to access content outside the root of a website?

- A) Brute force
- B) Port scanning
- C) SQL injection
- D) Directory traversal

Show Answer

The Correct Answer is:- D

---

5. Which of the following can prevent bad input from being presented to an application through a form?

- A) Request filtering
- B) Input validation
- C) Input scanning
- D) Directory traversing

Show Answer

The Correct Answer is:- B

---

6. _____ can be used to identify a web server.

- A) Session hijacking
- B) Banner grab
- C) Traversal
- D) Header analysis

Show Answer

The Correct Answer is:- B

---

7. In the field of IT security, the concept of defense in depth is layering more than one control on another. Why would this be helpful in the defense of a system of session hijacking?

- A) To provide better protection
- B) To build dependency among layers
- C) To increase logging ability
- D) To satisfy auditors

Show Answer

The Correct Answer is:- A

---

8. Which of the following is used to set permissions on content in a website?

- A) HIDS
- B) ACE
- C) ACL
- D) ALS

Show Answer

The Correct Answer is:- C

---

9. What could be used to monitor application errors and violations on a web server or application?

- A) HIDS
- B) HIPS
- C) NIDS
- D) Logs

Show Answer

The Correct Answer is:- D

---

10. Which of the following is an attribute used to secure a cookie?

- A) Encrypt
- B) Secure
- C) HttpOnly
- D) Domain

Show Answer

The Correct Answer is:- B,C,D

---

11. A POODLE attack targets what exactly?

- A) SSL
- B) TLS
- C) VPN
- D) AES

Show Answer

The Correct Answer is:- A

---

12. What is used to store session information?

- A) Cookie
- B) Snoop
- C) Directory
- D) File

Show Answer

The Correct Answer is:- A

---

13. Which attack can be used to take over a previous session?

- A) Cookie snooping
- B) Session hijacking
- C) Cookie hijacking
- D) Session sniffing

Show Answer

The Correct Answer is:- B

---

14. Which command would retrieve banner information from a website at port 80?

- A) nc 192.168.10.27 80
- B) nc 192.168.19.27 443
- C) nc 192.168.10.27 –p 80
- D) nc 192.168.10.27 –p –l 80

Show Answer

The Correct Answer is:- A

---

15. How is a brute-force attack performed?

- A) By trying all possible combinations of characters
- B) By trying dictionary words
- C) By capturing hashes
- D) By comparing hashes

Show Answer

The Correct Answer is:- A

---

16. What is the command to retrieve header information from a web server using Telnet?

- A) telnet < website name > 80
- B) telnet < website name > 443
- C) telnet < website name > –port:80
- D) telnet < website name > –port:443

Show Answer

The Correct Answer is:- A

---

17. Groups and individuals who may hack a web server or web application based on principle or personal beliefs are known as _____.

- A) White hats
- B) Black hats
- C) Script kiddies
- D) Hacktivists

Show Answer

The Correct Answer is:- D

---

18. The Wayback Machine would be useful in viewing what type of information relating to a web application?

- A) Get Job postings
- B) Websites
- C) Archived versions of websites
- D) Backup copies of websites

Show Answer

The Correct Answer is:- C

---

19. What may be helpful in protecting the content on a web server from being viewed by unauthorized personnel?

- A) Encryption
- B) Permissions
- C) Redirection
- D) Firewalls

Show Answer

The Correct Answer is:- A

---

20. A common attack against web servers and web applications is _____.

- A) Banner grab
- B) Input validation
- C) Buffer validations
- D) Buffer overflow

Show Answer

The Correct Answer is:- D

Section 12:

Q1 - Which of the following is a wireless network detector that is commonly found on Linux?

A. Kismet
B. Abel
C. Netstumbler
D. Nessus

Show Answer

Q2 - A security consultant decides to use multiple layers of anti-virus defense, such as end userdesktop anti-virus and E-mail

gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack
B. ARP spoofing attack
C. Social engineering attack
D. Scanning attack

Show Answer

Q3 - Code injection is a form of attack in which a malicious user:

A. Inserts text into a data field that gets interpreted as code
B. Gets the server to execute arbitrary code using a buffer overflow
C. Inserts additional code into the JavaScript running in the browser
D. Gains access to the codebase on the server and inserts new code

Show Answer

Q4 - Sid is a judge for a programming contest. Before the code reaches him it goes through arestricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?

A. Fuzzy-testing the code
B. Third party running the code
C. Sandboxing the code
D. String validating the code

Show Answer

Q5 - The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories ofcontrol objectives. Each objective contains one or more requirements, which must be followed inorder to achieve compliance. Which of the following requirements would best fit under the objective,"Implement strong access control measures"?

A. Regularly test security systems and processes.

B. Encrypt transmission of cardholder data across open, public networks.
C. Assign a unique ID to each person with computer access.
D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Show Answer

Q6 - Which of the following act requires employer's standard national numbers to identify them onstandard transactions?

A. SOXIT
B. HIPAA
C. DMCA
D. PCI-DSS

Show Answer

Q7 - Which of the following is an NMAP script that could help detect HTTP Methods such as GET,POST, HEAD, PUT, DELETE, TRACE?

A. http-git
B. http-headers
C. http enum
D. http-methods

Show Answer

Q8 - Fred is the network administrator for his company. Fred is testing an internal switch.From an external IP address, Fred wants to try and trick this switch into thinking it already hasestablished a session with his computer. How can Fred accomplish this?

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address ofhis computer.
B. B. He can send an IP packet with the SYN bit and the source address of his computer.

C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Show Answer

Q9 - What is the process of logging, recording, and resolving events that take place in anorganization?

A. Incident Management Process
B. Security Policy
C. Internal Procedure
D. Metrics

Show Answer

Q10 - A hacker has managed to gain access to a Linux host and stolen the password file from/etc/passwd. How can he use it?

A. The password file does not contain the passwords themselves.
B. He can open it and read the user ids and corresponding passwords.
C. The file reveals the passwords to the root user only.
D. He cannot read it because it is encrypted.

Show Answer

Q11 - What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Show Answer

Q12 - You are manually conducting Idle Scanning using Hping2. During your scanning you noticethat almost every query increments the IPID regardless of the port being queried. One or two of thequeries cause the IPID to increment by more than one value. Why do you think this occurs?

A. The zombie you are using is not truly idle.
B. A stateful inspection firewall is resetting your queries.
C. Hping2 cannot be used for idle scanning.
D. These ports are actually open on the target system.

Show Answer

Q13 - Darius is analysing IDS logs. During the investigation, he noticed that there was nothingsuspicious found and an alert was triggered on normal web application traffic. He can mark this alertas:

A. False-Negative
B. False-Positive
C. True-Positive
D. False-Signature

Show Answer

Q14 - What is the proper response for a NULL scan if the port is closed?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Show Answer

Q15 - The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

A. Injection
B. Cross Site Scripting
C. Cross Site Request Forgery
D. Path disclosure

Show Answer

Q16 - A recent security audit revealed that there were indeed several occasions that the company's network was breached. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

A. True Positive
B. False Negative
C. False Positive
D. False Positive

Show Answer

Q17 - A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location. During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as

reviewing the electronic access logs on a weekly basis. Which of the following is an issue with the situation?

A. Segregation of duties
B. Undue influence
C. Lack of experience
D. Inadequate disaster recovery plan

Show Answer

Q18 - Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
B. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Show Answer

Q19 - Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. --
B. ||
C. %%
D. ''

Show Answer

Q20 - Supposed you are the Chief Network Engineer of a certain Telco. Your company is planning for a big business expansion and it requires that your network authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network. Which AAA protocol would you implement?

A. TACACS+
B. DIAMETER
C. Kerberos
D. RADIUS

Show Answer

Q21 - Which of the following lists are valid data-gathering activities associated with a risk assessment?

A. Threat identification, vulnerability identification, control analysis
B. Threat identification, response identification, mitigation identification
C. Attack profile, defense profile, loss profile
D. System profile, vulnerability identification, security determination

Show Answer

Q22 - Which of the following command line switch would you use for OS detection in Nmap?

A. -D
B. -O
C. -P
D. -X

Show Answer

Q23 - A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits

that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

Show Answer

Q24 - What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

A. Cross-site request forgery
B. Cross-site scripting
C. Session hijacking
D. Server side request forgery

Show Answer

Q25 - Which of the following is a hashing algorithm?

A. MD5
B. PGP
C. DES
D. ROT13

Show Answer

Q26 - A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL
B. Mutual authentication
C. IPSec
D. Static IP addresses

Show Answer

Q27 - On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

A. nessus +
B. nessus *s
C. nessus &
D. nessus -d

Show Answer

Q28 - If an attacker uses the command SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'; which type of SQL injection attack is the attacker performing?

A. End of Line Comment
B. UNION SQL Injection
C. Illegal/Logically Incorrect Query
D. Tautology

Show Answer

Q29 - A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

A. Fraggle
B. MAC Flood
C. Smurf
D. Tear Drop

Show Answer

Q30 - Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.
B. given root or administrative privileges.
C. trusted to keep all data and access to that data under their sole control.
D. given privileges equal to everyone else in the department.

Show Answer

Answer: A

Section 22:

Q121 - Emil uses nmap to scan two hosts using this command.
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
He receives this output:

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is his conclusion?

A. Host 192.168.99.7 is an iPad.
B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.
C. Host 192.168.99.1 is the host that he launched the scan from.
D. Host 192.168.99.7 is down.

Show Answer

Q122 - What is GINA?

A. Gateway Interface Network Application
B. GUI Installed Network Application CLASS
C. Global Internet National Authority (G-USA)
D. Graphical Identification and Authentication DLL

Show Answer

Q123 - After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

A. SHA1
B. Diffie-Helman
C. RSA
D. AES

Show Answer

Q124 - A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

A. Use port security on his switches.
B. Use a tool like ARPwatch to monitor for strange ARP activity.
C. Use a firewall between all LAN segments.
D. If you have a small network, use static ARP entries.
E. Use only static IP addresses on all PC's.

Show Answer

Q125 - A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?

A. Botnet Trojan
B. Turtle Trojans
C. Banking Trojans
D. Ransomware Trojans

Show Answer

Q126 - You have initiated an active operating system fingerprinting attempt with nmap against a target system:

```
[root@ceh NG]# /usr/local/bin/nmap -sT -O 10.0.0.1

Starting nmap 3.28 ( www.insecure.org/nmap/) at 2003-06-18 19:14 IDT
Interesting ports on 10.0.0.1:
(The 1628 ports scanned but not shown below are in state: closed)

Port State Service
21/tcp filtered ftp
22/tcp filtered ssh
25/tcp open smtp
80/tcp open http
135/tcp open loc-srv
139/tcp open netbios-ssn
389/tcp open LDAP
443/tcp open https
465/tcp open smtps
1029/tcp open ms-lsa
1433/tcp open ms-sql-s
2301/tcp open compaqdiag
5555/tcp open freeciv
5800/tcp open vnc-http
5900/tcp open vnc
6000/tcp filtered X11

Remote operating system guess: Windows XP, Windows 2000, NT4 or 95/98/98SE Nmap
run completed -- 1 IP address (1 host up) scanned in 3.334 seconds

Using its fingerprinting tests nmap is unable to distinguish between different groups of
Microsoft based operating systems - Windows XP, Windows 2000, NT4 or 95/98/98SE.
```

What operating system is the target host running based on the open ports shown above?

A. Windows XP
B. Windows 98 SE
C. Windows NT4 Server
D. Windows 2000 Server

Show Answer

Q127 - In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.
Example:
allintitle: root passwd

A. Maintaining Access
B. Gaining Access
C. Reconnaissance
D. Scanning and Enumeration

Show Answer

Q128 - A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
B. Attempts by attackers to access the user and password information stored in the company's SQL database.
C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Show Answer

Q129 - Which of the following are well known password-cracking programs?

A. L0phtcrack
B. NetCat
C. Jack the Ripper
D. Netbus
E. John the Ripper

Show Answer

Q130 - One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800

Show Answer

Q131 - LM hash is a compromised password hashing function. Which of the following parameters describe LM Hash:?
I - The maximum password length is 14 characters.
II - There are no distinctions between uppercase and lowercase.
III - It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I
B. I, II, and III
C. II
D. I and II

Show Answer

Q132 - Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. -T0
B. -T5
C. -O
D. -A

Show Answer

Q133 - Which of the following program infects the system boot sector and the executable files at the same time?

A. Stealth virus
B. Polymorphic virus
C. Macro virus
D. Multipartite Virus

Show Answer

Q134 - If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

A. Running a network scan to detect network services in the corporate DMZ
B. Reviewing the need for a security clearance for each employee
C. Using configuration management to determine when and where to apply security patches
D. Training employees on the security policy regarding social engineering

Show Answer

Q135 - Which is the first step followed by Vulnerability Scanners for scanning a network?

A. TCP/UDP Port scanning
B. Firewall detection
C. OS Detection
D. Checking if the remote host is alive

Show Answer

Q136 - While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:
< script >alert(" Testing Testing Testing ")
Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text:
"Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

Show Answer

Q137 - Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. IANA
C. CAPTCHA
D. IETF

Show Answer

Q138 - A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Libpcap
B. Awinpcap
C. Winprom
D. Winpcap

Show Answer

Q139 - You perform a scan of your company's network and discover that TCP port 123 is open. What services by default run on TCP port 123?

A. Telnet
B. POP3
C. Network Time Protocol
D. DNS

Show Answer

Q140 - What does the option * indicate?

```
ping -* 6 192.168.0.101
output
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.101:
Packets: Sent=6, Received=6, Lost=0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
```

A. s
B. t
C. n
D. a

Show Answer

Q141 - Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. tcpdump
B. nessus
C. etherea
D. Jack the ripper

Show Answer

Q142 - Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students. He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

A. Disable unused ports in the switches
B. Separate students in a different VLAN
C. Use the 802.1x protocol
D. Ask students to use the wireless network

Show Answer

Q143 - While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.
B. Do not scan the broadcast IP.
C. Spoof the source IP address.

D. Only scan the Windows systems.

Show Answer

Q144 - While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

A. The port will send an ACK
B. The port will send a SYN
C. The port will ignore the packets
D. The port will send an RST

Show Answer

Q145 - Which of the following techniques will identify if computer files have been changed?

A. Network sniffing
B. Permission sets
C. Integrity checking hashes
D. Firewall alerts

Show Answer

Q146 - Which tool would be used to collect wireless packet data?

A. NetStumbler
B. John the Ripper
C. Nessus
D. Netcat

Show Answer

Q147 - You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are staring an

investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

A. Event logs on the PC
B. Internet Firewall/Proxy log
C. IDS log
D. Event logs on domain controller

Show Answer

Q148 - The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

A. Asymmetric
B. Confidential
C. Symmetric
D. Non-confidential

Show Answer

Q149 - Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

A. Time Keeper
B. NTP
C. PPP
D. OSPP

Show Answer

Q150 - Which command line switch would be used in NMAP to perform operating system detection?

A. -OS
B. -sO
C. -sP
D. -O

Show Answer

Answer: D