Testpassport Q&A

Higher Quality Better Service!

We offer free update service for one year

Http://www.testpassport.com

Exam : **EX0-107**

Title : SCNP Strategic Infrastructure Security

Version : Demo

1. In the process of public key cryptography, which of the following is true?

A. Only the public key is used to encrypt and decrypt

B. Only the private key can encrypt and only the public key can decrypt

C. Only the public key can encrypt and only the private key can decrypt

D. The private key is used to encrypt and decrypt

E. If the public key encrypts, then only the private key can decrypt

Answer: E

2. As per the guidelines in the ISO Security Policy standard, what is the purpose of the section on Physical and Environmental Security?

A. The objectives of this section are to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements, and to ensure compliance of systems with organizational security policies and standards.

B. The objectives of this section are to prevent unauthorized access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.

C. The objectives of this section are to provide management direction and support for information security.

D. The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

E. The objectives of this section are to control access to information, to prevent unauthorized access to information systems, to ensure the protection of networked services, and to prevent unauthorized computer access.

Answer: B

3. During a one week investigation into the security of your network you work on identifying the information that is leaked to the Internet, either directly or indirectly. One thing you decide to evaluate is the information stored in the Whois lookup of your organizational website. Of the following, what pieces of information can be identified via this method?

A. Registrar

B. Mailing Address

C. Contact Name

D. Record Update

E. Network Addresses (Private)

Answer: ABCD

4. You are aware of the significance and security risk that Social Engineering plays on your company. Of the following Scenarios, select those that, just as described, represent potentially dangerous Social Engineering:

A. A writer from a local college newspapers calls and speaks to a network administrator. On the call the writer requests an interview about the current trends in technology and offers to invite the administrator to speak at a seminar.

B. An anonymous caller calls and wishes to speak with the receptionist. On the call the caller asks the receptionist the normal business hours that the organization is open to the public.

C. An anonymous caller calls and wishes to speak with the purchaser of IT hardware and software. On the call the caller lists several new products that the purchaser may be interested in evaluating. The caller asks for a time to come and visit to demonstrate the new products.

D. An email, sent by the Vice President of Sales and Marketing, is received by the Help Desk asking to reset the password of the VP of Sales and Marketing.

E. An email is received by the Chief Security Officer (CSO) about a possible upgrade coming from the ISP to a different brand of router. The CSO is asked for the current network's configuration data and the emailer discusses the method, plan, and expected dates for the rollover to the new equipment.

Answer: DE

5. During the review of the security logs you notice some unusual traffic. It seems that a user has connected to your Web site ten times in the last week, and each time has visited every single page on the site. You are concerned this may be leading up to some sort of attack. What is this user most likely getting ready to do?

A. Mirror the entire web site.

B. Download entire DNS entries.

C. Scan all ports on a web server.

D. Perform a Distributed Denial of Service attack through the Web server.

E. Allow users to log on to the Internet without an ISP.

Answer: A

6. What type of cipher is used by an algorithm that encrypts data one bit at a time?

A. 64-bit encryption Cipher

B. Block Cipher

C. Stream Cipher

D. Diffuse Cipher

E. Split Cipher

Answer: C

7. You have just become the senior security professional in your office. After you have taken a complete inventory of the network and resources, you begin to work on planning for a successful security implementation in the network. You are aware of the many tools provided for securing Windows 2003 machines in your network. What is the function of Secedit.exe?

A. This tool is used to set the NTFS security permissions on objects in the domain.

B. This tool is used to create an initial security database for the domain.

C. This tool is used to analyze a large number of computers in a domain-based infrastructure.

D. This tool provides an analysis of the local system NTFS security.

E. This tool provides a single point of management where security options can be applied to a local computer or can be imported to a GPO.

Answer: C

8. To increase the security of your network and systems, it has been decided that EFS will be implemented in the appropriate situations. Two users are working on a common file, and often email this file back and forth between each other. Is this a situation where the use of EFS will create effective security, and why (or why not)?

A. No, the security will remain the same since both users will share the same key for encryption.

B. Yes, since the file will be using two keys for encryption the security will increase.

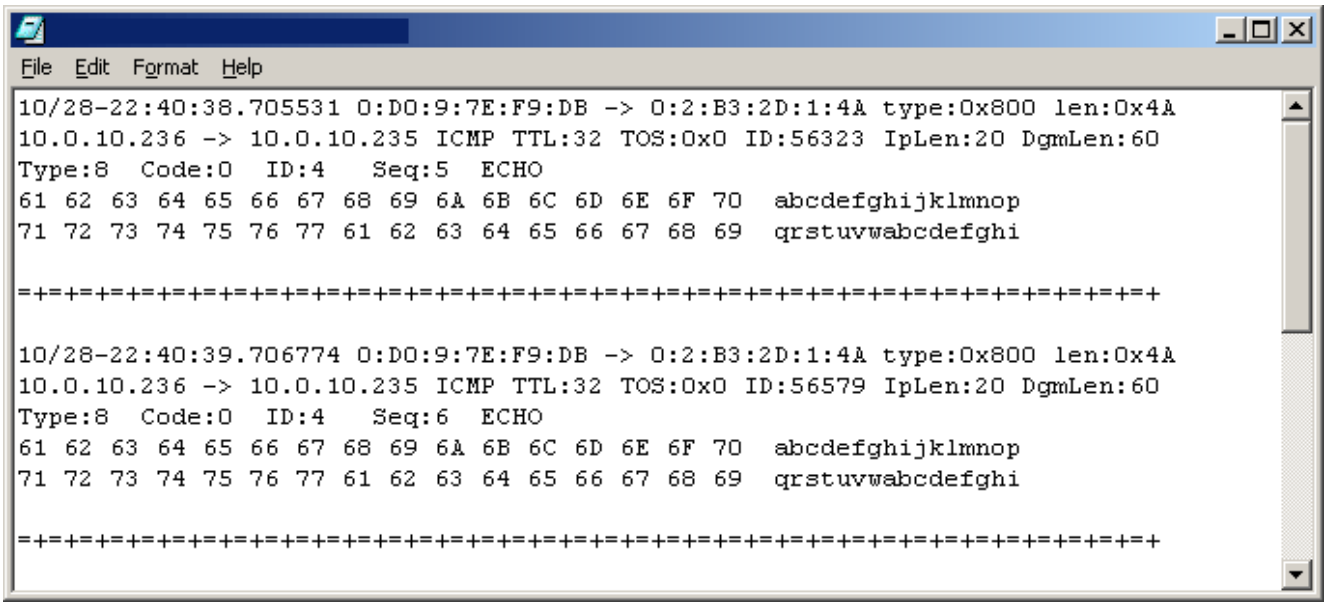
C. No, the security will remain the same since both users will share the same key for decryption.

D. Yes, since the file will be using two keys for decryption the security will increase.

E. No, EFS cannot be used for files that are shared between users.

Answer: E

9. Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



```
File  Edit  Format  Help
10/28-22:40:38.705531 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x4A
10.0.10.236 -> 10.0.10.235 ICMP TTL:32 TOS:0x0 ID:56323 IpLen:20 DgmLen:60
Type:8  Code:0  ID:4   Seq:5  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/28-22:40:39.706774 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x4A
10.0.10.236 -> 10.0.10.235 ICMP TTL:32 TOS:0x0 ID:56579 IpLen:20 DgmLen:60
Type:8  Code:0  ID:4   Seq:6  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

A. Windows 2000 Ping Request

B. Windows NT 4.0 Ping Request

C. Linux Ping Request

D. Linux Ping Response

E. Windows NT 4.0 Ping Response

Answer: B

10. In order for your newly written security policy to have any weight, it must be implemented. Which of the following are the three components of a successful Security Policy Implementation in an organization?

A. Policy Monitoring

B. Policy Design

C. Policy Committee

D. Policy Enforcement

E. Policy Documentation

Answer: ABD

11. Attackers have the ability to use programs that are able to reveal local passwords by placing some kind of a pointer/cursor over the asterisks in a program's password field. The reason that such tools can uncover passwords in some Operating Systems is because:

A. the passwords are simply masked with asterisks

B. the etc/passwd file is on a FAT32 partition

C. the passwords are decrypted on screen

D. the password text is stored in ASCII format

E. the etc/passwd file is on a FAT16 partition

Answer: A

12. To maintain the security of your network you routinely run several checks of the network and computers. Often you use the built-in tools, such as netstat. If you run the following command: netstat -e which of the following will be the result?

A. Displays all connections and listening ports

B. Displays Ethernet statistics

C. Displays addresses and port numbers in numerical form

D. Shows connections for the protocol specified

E. Displays per-protocol statistics

Answer: B

13. You have become the lead security professional for a mid-sized organization. You are currently studying DNS issues, and configuration options. You come across the concepts of DNS Spoofing, and investigate more. What is DNS Spoofing?

A. DNS Spoofing is when the DNS client submits a false DNS request to the DNS server, and the DNS server responds with correct data.

B. DNS Spoofing is the DNS client submits a DNS request to the DNS server using a bogus IP address, and the DNS server responds to the incorrect host.

C. DNS Spoofing is when a DNS Server responds to an unauthorized DNS client, providing that client with name resolution.

D. DNS Spoofing is when a DNS client is forced to make a DNS query to an imposter DNS server, which send the client to an imposter resource.

E. DNS spoofing is when a DNS server provides name resolution to clients that are located in a different IP subnet than the server itself.

Answer: D

14. What is a problem with symmetric key cryptography?

A. It is slower than asymmetric key cryptography

B. Secure distribution of the public key

C. There is a lack of encryption protocols that can use symmetric key cryptography

D. Secure distribution of a secret key

E. Symmetric key cryptography is reserved for the NSA

Answer: D

15. What is the name of the informational page that is relevant to a particular command in Linux?

A. Readme Page

B. Lnx_nfo Page

C. Man Page

D. X_Win Page

E. Cmd_Doc Page

Answer: C

16. You have just downloaded a new file, called scnpfile.tar.gz. You are going to verify the file prior to un-archiving the file. Which command do you need to type to un-compress the file, prior to un-archiving?

A. tar xvf scnpfile.tar.gz

B. tar -zxvf scnpfile.tar.gz

C. gunzip scnpfile.tar.gz

D. gunzip -xvf scnpfile.tar.gz

E. gunzip -zxvf scnpfile.tar.gz

Answer: C

17. You are configuring the lines that control access to exported objects on your server running NFS. If you have a directory called /Tech and you wish to export this directory to network 192.168.20.0/24, allowing root access, and the permissions of read and write, which of the following lines will accomplish this?

A. (RW) no_root_squash /Tech 192.168.20.0/24

B. /Tech 192.168.20.0/24 (rw) no_root_squash

C. (RW) no_root_squash 192.168.20.0/24 /Tech

D. (RW)no_root_squash:/Tech 192.168.20.0/24

E. /Tech 192.168.20.0/24(rw) no_root_squash

Answer: E

18. You are working on the authentication systems in your network, and are concerned with your legacy systems. In Windows NT 4.0, before Service Pack 4 (SP4), there were only two supported methods of authentication. What were those two methods?

A. NetBIOS

B. LM

C. NTLM

D. NTLMv2

E. Kerberos

Answer: BC

19. If you encrypt or decrypt files and folders located on a remote computer that has been enabled for remote encryption; the data that is transmitted over the network by this process is not encrypted. In order to keep data encrypted as it is transmitted over the network, which of the following must you do?

A. You must implement EFS.

B. You must implement B2 security for Windows.

C. You must use IPSec.

D. You must use a recovery agent.

E. You must transmit the entire folder, not individual files.

Answer: C

20. Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

```
File  Edit  Format  Help
10/27-23:56:37.033614 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3469 -> 10.0.10.235:1 TCP TTL:128 TOS:0x0 ID:1315 IpLen:20 DgmLen:48
******S* Seq: 0x17CA2BE3  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:56:37.042943 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3470 -> 10.0.10.235:2 TCP TTL:128 TOS:0x0 ID:1316 IpLen:20 DgmLen:48
******S* Seq: 0x17CAD3B4  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:56:37.052969 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3471 -> 10.0.10.235:3 TCP TTL:128 TOS:0x0 ID:1317 IpLen:20 DgmLen:48
******S* Seq: 0x17CB969A  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:56:37.062946 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3472 -> 10.0.10.235:4 TCP TTL:128 TOS:0x0 ID:1318 IpLen:20 DgmLen:48
******S* Seq: 0x17CC52C7  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:56:37.072986 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3473 -> 10.0.10.235:5 TCP TTL:128 TOS:0x0 ID:1319 IpLen:20 DgmLen:48
******S* Seq: 0x17CD1091  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:56:37.082983 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3474 -> 10.0.10.235:6 TCP TTL:128 TOS:0x0 ID:1320 IpLen:20 DgmLen:48
******S* Seq: 0x17CDEF72  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:56:37.093010 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3475 -> 10.0.10.235:7 TCP TTL:128 TOS:0x0 ID:1321 IpLen:20 DgmLen:48
******S* Seq: 0x17CEB24E  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

A. NetBus Scan

B. Trojan Scan

C. Ping Sweep

D. Port Scan

E. Ping Sweep

Answer: D

21. As per the guidelines in the ISO Security Policy standard, what is the purpose of the section on

Business Continuity Planning?

A. The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

B. The objectives of this section are to provide management direction and support for information security.

C. The objectives of this section are to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

D. The objectives of this section are to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements, and to ensure compliance of systems with organizational security policies and standards.

E. The objectives of this section are to control access to information, to prevent unauthorized access to information systems, to ensure the protection of networked services, and to prevent unauthorized computer access.

Answer: C

22. On Monday, during a routine check of a users Windows workstation, you find the following program, called regedit.bat on the users local hard drive:

Net localgroup administrators local /all

Start regedit.exe

Exit

What is this program capable of doing on this computer?

A. Nothing, the first line is coded wrong.

B. It will add the administrators to the local group

C. It will add the local user to all local groups

D. It will add the administrators to all local groups

E. It will add the local user to the administrators group

Answer: E

23. Often times attackers will run scans against the network to identify different network and operating systems, and resources that are available. If an attacker runs scans on the network, and you are logging the connections, which of the following represent the legitimate combination of packets that will be sent

between the attacker and target?

A. Attacker PSH-FIN Scan, Target RST-FIN Response

B. Attacker ACK Scan, Target NULL Response

C. Attacker NULL Scan, Target RST Response

D. Attacker SYN Scan, Target NULL Response

E. Attacker FIN Scan, Target RST Response

Answer: CE

24. You are discussing the design and infrastructure of the Internet with several colleagues when a disagreement begins over the actual function of the NAP in the Internets design. What is the function of a NAP in the physical structure of the Internet?

A. The NAP provides for a layered connection system of ISPs connecting to the backbone.

B. The NAP provides the actual connection point between a local user and the Internet.

C. The NAP provides the physical network with communication channels for the Internet and voice/data applications.

D. The NAP provides a national interconnection of systems, called peering centers, to the NSPs.

E. The NAP provides for a connection point between an ISP and the backbone of the Internet.

Answer: E

25. When using the 3DES encryption (C = EK1[DK2[EK1[P]]]) , what is the function of C?

A. C is the text before encryption

B. C is the first encryption key

C. C is the second encryption key

D. C is the decryption key

E. C is the text after encryption

Answer: E

26. Which of the following are symmetric encryption algorithms?

A. MD5

B. RSA

C. Diffie-Hellman

D. 3DES

E. AES

Answer: DE

27. During the configuration of your Linux system, you are working with the available drives in the computer. What syntax defines the First (Primary) IDE hard disk drive?

A. /dev/sda

B. /dev/fda

C. /dev/hd1

D. /dev/hda

E. /dev/fd1

Answer: D

28. You are configuring the permissions to a file, called file1, on your Linux file server. You wish to change the permissions to remove the execute permission from the others and group. Which of the following commands will complete this task?

A. umask x-og file1

B. umask og-x file1

C. chmod xog- file1

D. chmod x-og file1

E. chmod og-x file1

Answer: E

29. In the past it was, at times, difficult to locate current information on security vulnerabilities. What is the name of the security communitys effort to create a comprehensive database of multiple vulnerabilities and security tools?

A. Common Vulnerabilities and Exploits

B. Cataloged Venerations and Exposures

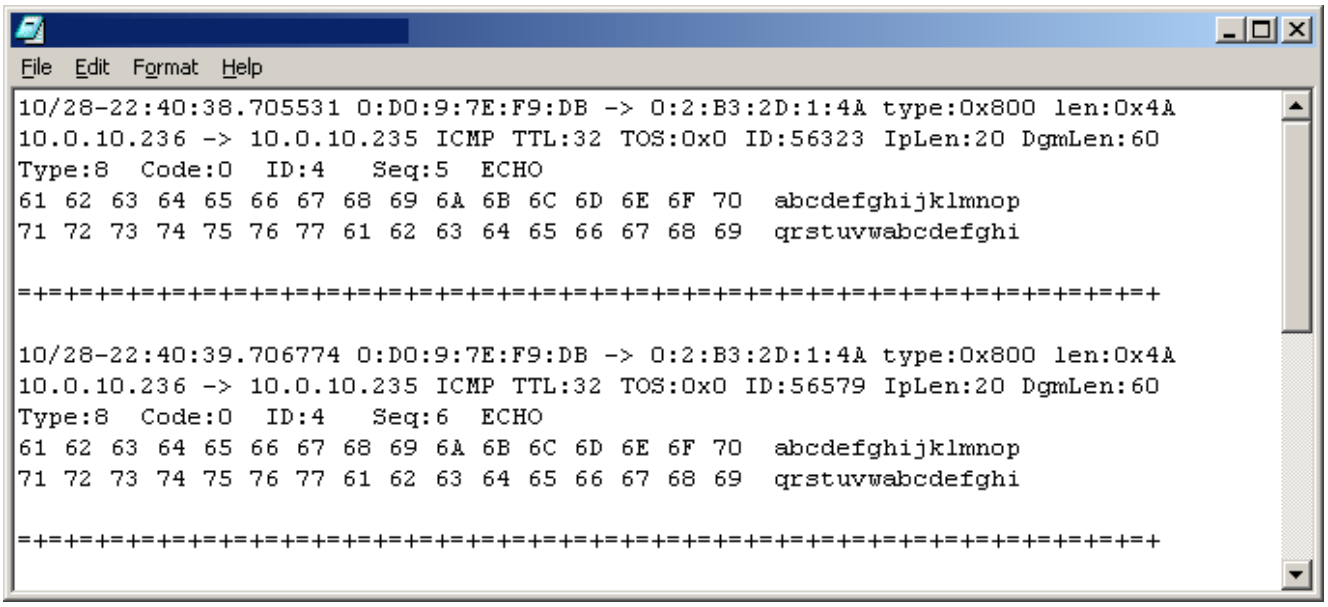
C. Common Vulnerabilities and Exposures

D. Cataloged Vulnerabilities and Exposures

E. Cataloged Vulnerabilities and Exploits

Answer: C

30. Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



```
File  Edit  Format  Help
10/28-22:40:38.705531 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x4A
10.0.10.236 -> 10.0.10.235 ICMP TTL:32 TOS:0x0 ID:56323 IpLen:20 DgmLen:60
Type:8  Code:0  ID:4   Seq:5  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/28-22:40:39.706774 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x4A
10.0.10.236 -> 10.0.10.235 ICMP TTL:32 TOS:0x0 ID:56579 IpLen:20 DgmLen:60
Type:8  Code:0  ID:4   Seq:6  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

A. Windows 2000 Ping Request

B. Windows NT 4.0 Ping Request

C. Linux Ping Request

D. Linux Ping Response

E. Windows NT 4.0 Ping Response

Answer: B