

➤ **Vendor: EC-Council**

➤ **Exam Code: 312-50v12**

➤ **Exam Name: Certified Ethical Hacker Exam (CEH v12)**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [August/2023](#))**

[Visit Braindump2go and Download Full Version 312-50v12 Exam Dumps](#)

QUESTION 1

Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials.

Which of the following tools is employed by Clark to create the spoofed email?

- A. Evilginx
- B. Slowloris
- C. PLCinject
- D. PyLoris

Answer: A

Explanation:

Phishing Tools Phishing tools can be used by attackers to generate fake login pages to capture usernames and passwords, send spoofed emails, and obtain the victim's IP address and session cookies. This information can further be used by the attacker, who will use it to impersonate a legitimate user and launch further attacks on the target organization :=>Tools like BLACKKEYE / PhishX / PhishX / Trape / Evilginx

QUESTION 2

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation.

What is the type of vulnerability assessment tool employed by John in the above scenario?

- A. Agent-based scanner
- B. Network-based scanner
- C. Cluster scanner
- D. Proxy scanner

Answer: A

Explanation:

* Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.

* Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

* Proxy Scanner: Proxy scanners are the network-based scanners that can scan networks from any machine on the network.

* Cluster scanner: Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.

QUESTION 3

[312-50v12 Exam Dumps](#) [312-50v12 Exam Questions](#) [312-50v12 PDF Dumps](#) [312-50v12 VCE Dumps](#)

<https://www.braindump2go.com/312-50v12.html>

Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine.

Which of the following techniques is used by Joel in the above scenario?

- A. Watering hole attack
- B. DNS rebinding attack
- C. MarioNet attack
- D. Clickjacking attack

Answer: A

Explanation:

It is a type of unvalidated redirect attack whereby the attacker first identifies the most visited website of the target, determines the vulnerabilities in the website, injects malicious code into the vulnerable web application, and then waits for the victim to browse the website. Once the victim tries to access the website, the malicious code executes, infecting the victim.

QUESTION 4

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs.

What type of malware did the attacker use to bypass the company's application whitelisting?

- A. File-less malware
- B. Zero-day malware
- C. Phishing malware
- D. Logic bomb malware

Answer: A

Explanation:

In this scenario, the attacker used file-less malware to bypass the company's application whitelisting. File-less malware resides entirely in memory, making it difficult for antivirus software and IDS/IPS to detect. It can run in the context of a trusted process or system application, and can be delivered through various attack vectors, including phishing emails, malicious websites, or network exploits.

QUESTION 5

Dorian is sending a digitally signed email to Poly. With which key is Dorian signing this message and how is Poly validating it?

- A. Dorian is signing the message with his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.
- B. Dorian is signing the message with Poly's private key, and Poly will verify that the message came from Dorian by using Dorian's public key.
- C. Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key.
- D. Dorian is signing the message with Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.

Answer: C

Explanation:

In digital signature, the sender signs the message using their private key, which only the sender knows. The recipient can verify that the message came from the sender by using the sender's public key. Therefore, in this scenario, Dorian is signing the email with his private key, and Poly will validate it using Dorian's public key.

QUESTION 6

Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL

[312-50v12 Exam Dumps](#) [312-50v12 Exam Questions](#) [312-50v12 PDF Dumps](#) [312-50v12 VCE Dumps](#)

<https://www.braindump2go.com/312-50v12.html>

www.bank.com, the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different.

What type of attack he is experiencing?

- A. DHCP spoofing
- B. DoS attack
- C. ARP cache poisoning
- D. DNS hijacking

Answer: D

Explanation:

DNS hijacking: Attacker modifies DNS queries/responses, redirects users to incorrect/malicious websites, steals sensitive information.

QUESTION 7

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account.

What is the attack performed by Boney in the above scenario?

- A. Forbidden attack
- B. CRIME attack
- C. Session donation attack
- D. Session fixation attack

Answer: C

Explanation:

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

QUESTION 8

Kevin, a professional hacker, wants to penetrate CyberTech Inc's network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packets, but the target web server can decode them.

What is the technique used by Kevin to evade the IDS system?

- A. Session splicing
- B. Urgency flag
- C. Obfuscating
- D. Desynchronization

Answer: C

Explanation:

Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode.

QUESTION 9

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based

[312-50v12 Exam Dumps](#) [312-50v12 Exam Questions](#) [312-50v12 PDF Dumps](#) [312-50v12 VCE Dumps](#)

<https://www.braindump2go.com/312-50v12.html>

on Microsoft SQL Server. In the login/password form, you enter the following credentials:

Username: attack' or 1=1 –
Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

- A. `select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'`
- B. `select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'`
- C. `select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'`
- D. `select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'`

Answer: D

Explanation:

SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield'

SQL Query Executed : SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1

Code after -- are now comments : --' AND Password='Springfield'

QUESTION 10

Which of the following commands checks for valid users on an SMTP server?

- A. RCPT
- B. CHK
- C. VRFY
- D. EXPN

Answer: C

Explanation:

The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821. The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

QUESTION 11

Bella, a security professional working at an IT firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking. To address this situation, Bella implemented a protocol that sends data using encryption and digital certificates.

Which of the following protocols is used by Bella?

- A. FTPS
- B. FTP
- C. HTTPS
- D. IP

Answer: A

Explanation:

FTPS includes full support for the TLS and SSL cryptographic protocols, including the use of server-side public key authentication certificates and client-side authorization certificates. It also supports compatible ciphers, including AES, RC4, RC2, Triple DES, and DES. It further supports hash functions SHA, MD5, MD4, and MD2.

QUESTION 12

John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

- A. Use his own private key to encrypt the message.
- B. Use his own public key to encrypt the message.
- C. Use Marie's private key to encrypt the message.
- D. Use Marie's public key to encrypt the message.

Answer: D

Explanation:

PGP (Pretty Good Privacy) is an encryption software that can be used to encrypt and decrypt electronic communications, such as emails. PGP uses a combination of symmetric-key and public-key encryption to provide confidentiality and authenticity to the communications.

QUESTION 13

In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

- A. 4.0-6.0
- B. 3.9-6.9
- C. 3.0-6.9
- D. 4.0-6.9

Answer: D

Explanation:

CVSS v3.0 Ratings

Low 0.1-3.9

Medium 4.0-6.9

High 7.0-8.9

Critical 9.0-10.0

<https://nvd.nist.gov/vuln-metrics/cvss>

QUESTION 14

Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161.

What protocol is this port using and how can he secure that traffic?

- A. RPC and the best practice is to disable RPC completely.
- B. SNMP and he should change it to SNMP V3.
- C. SNMP and he should change it to SNMP V2, which is encrypted.
- D. It is not necessary to perform any actions, as SNMP is not carrying important information.

Answer: B

Explanation:

SNMP (Simple Network Management Protocol) is a protocol used for managing and monitoring network devices, such as routers, switches, and servers. SNMP uses UDP port 161 for communication. However, SNMP V1 and V2 use clear text community strings for authentication, making them vulnerable to eavesdropping and other attacks.

To secure SNMP traffic, Bill should change the SNMP version to SNMP V3, which provides enhanced security features, such as authentication, encryption, and message integrity. SNMP V3 requires a username and password for authentication, and it supports encryption of the data being transmitted.

QUESTION 15

Consider the following Nmap output:

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

What command-line parameter could you use to determine the type and version number of the web server?

- A. -sV
- B. -sS
- C. -Pn
- D. -V

Answer: A

Explanation:

<https://nmap.org/book/man-briefoptions.html>

-sV: Probe open ports to determine service/version info

QUESTION 16

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data.

Which of the following regulations is mostly violated?

- A. PCI DSS
- B. PII
- C. ISO 2002
- D. HIPAA/PHI

Answer: D

Explanation:

HIPAA/PHI: The Health Insurance Portability and Accountability Act (HIPAA) establishes rules and regulations to safeguard protected health information (PHI). It applies to healthcare providers, health plans, and other entities handling patient data to ensure its confidentiality, integrity, and availability.

QUESTION 17

Infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

[312-50v12 Exam Dumps](#) [312-50v12 Exam Questions](#) [312-50v12 PDF Dumps](#) [312-50v12 VCE Dumps](#)

<https://www.braindump2go.com/312-50v12.html>

- A. Scanning
- B. Gaining access
- C. Maintaining access
- D. Reconnaissance

Answer: B

Explanation:

The ethical hacking methodology consists of five phases, which are: reconnaissance, scanning, gaining access, maintaining access, and covering tracks.

The phase that involves infecting a system with malware and using phishing to gain credentials to a system or web application is the gaining access phase. In this phase, the attacker attempts to gain unauthorized access to the target system or network by exploiting vulnerabilities, misconfigurations, or weaknesses in the security controls.

QUESTION 18

Larry, a security professional in an organization, has noticed some abnormalities in the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a few countermeasures to secure the accounts on the web server.

Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

- A. Retain all unused modules and application extensions.
- B. Limit the administrator or root-level access to the minimum number of users.
- C. Enable all non-interactive accounts that should exist but do not require interactive login.
- D. Enable unused default user accounts created during the installation of an OS.

Answer: B

Explanation:

Limiting the administrator or root-level access to the minimum number of users is a best practice for securing user accounts on a web server. This helps to reduce the attack surface and minimize the risk of unauthorized access or privilege escalation.

QUESTION 19

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment.

What is this cloud deployment option called?

- A. Private
- B. Community
- C. Public
- D. Hybrid

Answer: B

Explanation:

The three main types of cloud deployment options are: private, public, and hybrid. However, there is also a fourth deployment option called community cloud.

In a community cloud, a cloud infrastructure is shared by several organizations or groups that have similar computing requirements and concerns. These organizations may be from the same industry, have similar security or compliance requirements, or have other commonalities that make it beneficial for them to share a cloud environment.

Community cloud environments can provide benefits such as lower costs, improved security, and shared expertise. They can also enable collaboration and resource sharing among organizations.

QUESTION 20

Allen, a professional pen tester, was hired by XpertTech Solutions to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. By enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.

[312-50v12 Exam Dumps](#) [312-50v12 Exam Questions](#) [312-50v12 PDF Dumps](#) [312-50v12 VCE Dumps](#)

<https://www.braindump2go.com/312-50v12.html>

Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

- A. <00>
- B. <20>
- C. <03>
- D. <1B>

Answer: C

Explanation:

The <03> NetBIOS code is associated with where you can retrieve the messenger service for a logged-in user.

QUESTION 21

Don, a student, came across a gaming app in a third-party app store and installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after installing the app.

What is the attack performed on Don in the above scenario?

- A. SIM card attack
- B. Clickjacking
- C. SMS phishing attack
- D. Agent Smith attack

Answer: D

Explanation:

Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app, the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands.

QUESTION 22

Samuel, a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.

Which of the following attacks can be performed by exploiting the above vulnerability?

- A. Padding oracle attack
- B. DROWN attack
- C. DUHK attack
- D. Side-channel attack

Answer: B

Explanation:

DROWN attack: Decrypting SSL/TLS communications through SSLv2 vulnerability.

QUESTION 23

Clark, a professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network.

What is the online tool employed by Clark in the above scenario?

- A. DuckDuckGo

[312-50v12 Exam Dumps](#) [312-50v12 Exam Questions](#) [312-50v12 PDF Dumps](#) [312-50v12 VCE Dumps](#)

<https://www.braindump2go.com/312-50v12.html>

- B. AOL
- C. ARIN
- D. Baidu

Answer: C

Explanation:

The scenario describes a reconnaissance phase technique called footprinting, which involves gathering information about a target organization in order to identify potential vulnerabilities or attack vectors.

In this case, Clark has used Whois footprinting to obtain the server IP address of the target organization. He has then used an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network.

One such online tool that can be used for this purpose is ARIN (American Registry for Internet Numbers). ARIN is a non-profit organization that manages the allocation and registration of IP addresses and other Internet number resources in North America.

QUESTION 24

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed source IP addresses." Suppose that you are using Nmap to perform this scan.

What flag will you use to satisfy this requirement?

- A. The -g flag
- B. The -A flag
- C. The -f flag
- D. The -D flag

Answer: D

Explanation:

Nmap may be used to create decoys, that are meant to fool firewalls. whereas decoys is used for nefarious functions, it's usually used to rectify.

```
nmap -D 192.168.0.1,192.168.0.2,...
```

When using the -D command, you'll be able to follow the command with a list of decoy addresses. These decoy addresses also will show as if they're scanning the network, to obfuscate the scan that's actually being done.

QUESTION 25

Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.

What is the type of vulnerability assessment that Jude performed on the organization?

- A. Application assessment
- B. External assessment
- C. Passive assessment
- D. Host-based assessment

Answer: B

Explanation:

B (100%)

QUESTION 26

Widespread fraud at Enron, WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

- A. SOX
- B. FedRAMP

- C. HIPAA
- D. PCI DSS

Answer: A

Explanation:

The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by companies. Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.

The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursing light-emitting diode several to demand an overhaul of decades-old restrictive standards.

QUESTION 27

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a DoS attack, and as a result, legitimate employees were unable to access the client's network.

Which of the following attacks did Abel perform in the above scenario?

- A. Rogue DHCP server attack
- B. VLAN hopping
- C. STP attack
- D. DHCP starvation

Answer: D

Explanation:

Rogue DHCP server attack: Unauthorized DHCP server distributing IP addresses.

VLAN hopping: Exploiting VLAN vulnerabilities for unauthorized network access.

STP attack: Disrupting networks through Spanning Tree Protocol manipulation.

DHCP starvation: Flooding DHCP server to exhaust IP address pool.

QUESTION 28

This form of encryption algorithm is a symmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

- A. HMAC encryption algorithm
- B. Twofish encryption algorithm
- C. IDEA
- D. Blowfish encryption algorithm

Answer: B

Explanation:

The Twofish encryption algorithm is a symmetric key block cipher that was designed to be secure, efficient, and flexible. It uses a block size of 128 bits and can have key sizes up to 256 bits, making it highly secure.

Twofish was one of the five finalists in the Advanced Encryption Standard (AES) competition organized by the U.S. National Institute of Standards and Technology (NIST) in 1997. Although it was not selected as the winner, Twofish is still considered a highly secure encryption algorithm and is widely used in various applications.

QUESTION 29

Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources.

What is the attack technique used by Jude for finding loopholes in the above scenario?

- A. Spoofed session flood attack
- B. UDP flood attack
- C. Peer-to-peer attack
- D. Ping-of-death attack

Answer: A

Explanation:

Jude used a spoofed session flood attack to bypass the network protection tools and firewalls used in his company's network infrastructure. This attack technique involves creating forged TCP sessions by sending multiple SYN, ACK, RST, or FIN packets to the target system. By doing so, the attacker can exhaust the target system's resources and make it unresponsive to legitimate requests.

In a spoofed session flood attack, the attacker sends packets with a forged source IP address, making it difficult for the target system to distinguish between legitimate and malicious traffic. This makes it easier for the attacker to bypass network protection tools and firewalls, which may be configured to block traffic from known malicious IP addresses.

QUESTION 30

Jim, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address.

Which of the following Nmap commands helped Jim retrieve the required information?

- A. `nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >`
- B. `nmap -Pn -sU -p 44818 --script enip-info < Target IP >`
- C. `nmap -Pn -sT -p 46824 < Target IP >`
- D. `nmap -Pn -sT -p 102 --script s7-info < Target IP >`

Answer: B

Explanation:

EtherNet/IP makes use of TCP port number 44818 for explicit messaging and UDP port number 2222 for implicit messaging