Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System

B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System

C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System

D. Sniffer, Packet Logger, and Host Intrusion Prevention System

Suggestion:

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

A. Performing content enumeration on the web server to discover hidden folders

B. Using wget to perform banner grabbing on the webserver

C. Flooding the web server with requests to perform a DoS attack

D. Downloading all the contents of the web page locally for further examination

Suggestion:

The correct answer(s): B

-q, --quiet quiet (no output) -S, --server-response print server response

---------------------------------------------------------------------------------------------------------

Frederickson Security Consultants is currently conducting a security audit on the networks of Hawthorn Enterprises, a contractor for the Department of Defense. Since Hawthorn Enterprises conducts business daily with the federal government, they must abide by very stringent security policies. Frederickson is testing all of Hawthorn's physical and logical security measures including biometrics, passwords, and permissions. The federal government requires that all users must utilize random, non-dictionary passwords that must take at least 30 days to crack. Frederickson has confirmed that all Hawthorn employees use a random password generator for their network passwords. The Frederickson consultants have saved off numerous SAM files from Hawthorn's servers using Pwdump6 and are going to try and crack the network passwords. What method of attack is best suited to crack these passwords in the shortest amount of time?

A. Brute force attack

B. Birthday attack

C. Dictionary attack

D. Brute service attack

Suggestion:

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open-Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.

B. OSSTMM is gray box testing and OWASP is black box testing.

C. OWASP addresses controls and OSSTMM does not.

D. OSSTMM addresses controls and OWASP does not.

Suggestion:

The correct answer(s): D

---------------------------------------------------------------------------------------------------------

Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.

Which of the following host discovery techniques must he use to perform the given task?

A. UDP scan

B. TCP Maimon scan

C. arp ping scan (A)

D. ACK flag probe scan

---------------------------------------------------------------------------------------------------------

Neil is an IT security consultant working on a contract for Davidson Avionics.

Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance. What type of social engineering attack has Neil employed here?

A. Neil has used a tailgating social engineering attack to gain access to the offices

B. He has used a piggybacking technique to gain unauthorized access

C. This type of social engineering attack is called man trapping

D. Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionic

Suggestion:

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

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?

A. Social engineering

B. Piggybacking

C. Tailgating

D. Eavesdropping

Suggestion:

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

Suggestion:

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected in the core components of the operating system. What is this type of rootkit an example of?

A. Mypervisor rootkit

B. Kernel toolkit

C. Hardware rootkit

D. Firmware rootkit

Suggestion:

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

The “Gray-box testing” methodology enforces what kind of restriction?

A. Only the external operation of a system is accessible to the tester.

B. The internal operation of a system in only partly accessible to the tester

C. Only the internal operation of a system is known to the tester

D. The internal operation of a system is completely known to the tester

Suggestion:

The correct answer(s): D

---------------------------------------------------------------------------------------------------------

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23.

Which of the following IP addresses could be teased as a result of the new configuration?

A. 210.1.55.200

B. 10.1.4.254

C. 10.1.5.200

D. 10.1.4.156

Suggestion:

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.

If these switches' ARP cache is successfully flooded, what will be the result?

A. The switches will drop into hub mode if the ARP cache is successfully flooded.

B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.

C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.

D. The switches will route all traffic to the broadcast address created collisions.

Suggestion:

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

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

A. WHOIS

B. CAPTCHA

C. IANA

D. IETF

Suggestion:

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user’s password or activate disabled Windows accounts?

A. John the Ripper

B. SET

C. CHNTPW

D. Cain & Abel

Suggestion:

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system

B. Determine the impact of enabling the audit feature

C. Perform a cost/benefit analysis of the audit feature

D. Allocate funds for staffing of audit log review

Suggestion:

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

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. Preparation

B. Cleanup

C. Persistence

D. initial intrusion

Suggestion:

The correct answer(s): D

---------------------------------------------------------------------------------------------------------

Mirai malware targets loT devices. After infiltration, it uses them to propagate and create botnets that then used to launch which types of attack?

A. MITM attack

B. Birthday attack

C. DDoS attack

D. Password attack

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**Which of the following is a component of a risk assessment?**

A. Administrative safeguards

B. Physical security

C. DMZ

D. Logical interface

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server. Which of the following tools is used by Jack to perform vulnerability scanning?**

A. Infoga

B. WebCopier Pro

C. Netsparker

D. NCollector Studio

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**Which of the following tools can be used to perform a zone transfer?**

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

F. Netcat

G. Neotrace

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A C E

**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. JSON-RPC

B. SOAP API

C. RESTful API

D. REST API

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**What type of virus is most likely to remain undetected by antivirus software?**

A. Cavity virus

B. Stealth virus

C. File-extension virus

D. Macro virus

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**Which type of virus can change its own code and then cipher itself multiple times as it replicates?**

A. Stealth virus

B. Tunneling virus

C. Cavity virus

D. Encryption virus

**Suggestion:**

The correct answer(s): A

A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to merge into the now-infected machine, a stealth viruses hides itself by continually renaming and moving itself round the disc. Like other viruses, a stealth virus can take hold of the many parts of one’s PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software. Once moved and renamed a stealth virus will usually replace the detected ‘infected’ file with a clean file that doesn’t trigger anti-virus detection. It’s a never-ending game of cat and mouse.The intelligent architecture of this sort of virus guarantees it’s impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely eradicate the presence of a stealth virus. Using regularly-updated antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them. https://www.techslang.com/definition/what-is-a-stealth-virus/

---------------------------------------------------------------------------------------------------------

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain. If the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

* A. list domain=abccorp.local type=zone
* B. Is -d accorp.local
* C. list server=192.168.10.2 type=all
* D. Iserver 192.168.10.2 -t all

Suggestion:

* The correct answer(s): B
* type "ls -d <URL>", if the domain is having DNS Zone Transfer Misconfiguration, then it will show up.
* nslookup -ls just sends a raw AXFR query to the remote nameserver, which will initiate a zone transfer if and only if the remote nameserver is dumb enough to respond to unsolicited, unauthorized AXFRs originating from random machines on the Internet.

---------------------------------------------------------------------------------------------------------

**MX record priority increases as the number increases. (True/False.)**

1. true
2. False

Answer: B

The priority is used to determine which MX server to connect to first, in order to get to your inbox. If there are multiple addresses with the same priority, it simply connects to one at random. You can also change your MX records from the existing one if you deem it necessary.

---------------------------------------------------------------------------------------------------------

**You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page.  
What Is the best Linux pipe to achieve your milestone?**

A. dirb https://site.com | grep "site"

B. curl -s https://site.com | grep ‘’< a href-\’http" | grep "Site-com- | cut -d "V" -f 2

C. wget https://site.com | grep "< a href=\\*http" | grep "site.com"

D. wgethttps://site.com | cut-d"http-

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

Most people voted: B

---------------------------------------------------------------------------------------------------------

**How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?**

A. There is no way to tell because a hash cannot be reversed

B. The right most portion of the hash is always the same

C. The hash always starts with AB923D

D. The left most portion of the hash is always the same

E. A portion of the hash will be all 0's

**Suggestion:**

The correct answer(s): B

[There is no way to determine whether an LM hash you extracted contains a password that is less than eight characters long because a hash cannot be reversed](https://www.bing.com/ck/a?!&&p=c37ad7b3b4cddc96JmltdHM9MTcyNTMyMTYwMCZpZ3VpZD0xYjI1NzE5OC01OWIwLTYwNmYtMGNjYS02MDY3NTgyYjYxYmImaW5zaWQ9NTY2NA&ptn=3&ver=2&hsh=3&fclid=1b257198-59b0-606f-0cca-6067582b61bb&psq=How+can+you+determine+if+an+LM+hash+you+extracted+contains+a+password+that+is+less+than+8+characters+long%3f&u=a1aHR0cHM6Ly93d3cucGVhcnNvbml0Y2VydGlmaWNhdGlvbi5jb20vYXJ0aWNsZXMvYXJ0aWNsZS5hc3B4P3A9MjE2MzE4OCZzZXFOdW09Mw&ntb=1)[1](https://www.bing.com/ck/a?!&&p=f1b84c1149eaebd4JmltdHM9MTcyNTMyMTYwMCZpZ3VpZD0xYjI1NzE5OC01OWIwLTYwNmYtMGNjYS02MDY3NTgyYjYxYmImaW5zaWQ9NTY2NQ&ptn=3&ver=2&hsh=3&fclid=1b257198-59b0-606f-0cca-6067582b61bb&psq=How+can+you+determine+if+an+LM+hash+you+extracted+contains+a+password+that+is+less+than+8+characters+long%3f&u=a1aHR0cHM6Ly93d3cucGVhcnNvbml0Y2VydGlmaWNhdGlvbi5jb20vYXJ0aWNsZXMvYXJ0aWNsZS5hc3B4P3A9MjE2MzE4OCZzZXFOdW09Mw&ntb=1)[2](https://www.bing.com/ck/a?!&&p=bec06e300d679320JmltdHM9MTcyNTMyMTYwMCZpZ3VpZD0xYjI1NzE5OC01OWIwLTYwNmYtMGNjYS02MDY3NTgyYjYxYmImaW5zaWQ9NTY2Ng&ptn=3&ver=2&hsh=3&fclid=1b257198-59b0-606f-0cca-6067582b61bb&psq=How+can+you+determine+if+an+LM+hash+you+extracted+contains+a+password+that+is+less+than+8+characters+long%3f&u=a1aHR0cHM6Ly9leGFtcHJhY3RpY2V0ZXN0cy5jb20vZWNjb3VuY2lsL2NlaC12OS9jZXJ0aWZpZWQtZXRoaWNhbC1oYWNrZXItY2VoLTMxMi01MC1xdWVzdGlvbjU3Ny8&ntb=1). [However, the LM hash value for 7 null characters is AAD3B435B51404EE. Therefore, a password less than 8 characters long will end with AAD3B435B51404EE, and an empty password will always be exactly AAD3B435B51404EEAAD3B435B51404EE](https://www.bing.com/ck/a?!&&p=83c415fe80b297f8JmltdHM9MTcyNTMyMTYwMCZpZ3VpZD0xYjI1NzE5OC01OWIwLTYwNmYtMGNjYS02MDY3NTgyYjYxYmImaW5zaWQ9NTY2Nw&ptn=3&ver=2&hsh=3&fclid=1b257198-59b0-606f-0cca-6067582b61bb&psq=How+can+you+determine+if+an+LM+hash+you+extracted+contains+a+password+that+is+less+than+8+characters+long%3f&u=a1aHR0cHM6Ly93d3cubWlja3B1dGxleS5uZXQvMjAxOS8wNi9sbS1oYXNoLWxtLWhhc2hlcy1hcmUtd2Vhay1hbmQtYXJjaGlhYy5odG1s&ntb=1)

---------------------------------------------------------------------------------------------------------

**The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?**

A. Have the network team document the reason why the rule was implemented without prior manager approval.

B. Monitor all traffic using the firewall rule until a manager can approve it.

C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.

D. Immediately roll back the firewall rule until a manager can approve it

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

---------------------------------------------------------------------------------------------------------

**Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?**

A. har.txt

B. SAM file

C. wwwroot

D. Repair file

**Suggestion:**

The correct answer(s): B

**You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?**

A. Reconnaissance

B. Command and control

C. Weaponization

D. Exploitation

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?**

A. [inurl:]

B. [related:]

C. [info:]

D. [site:]

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

related: This operator displays websites that are similar or related to the URL specified

---------------------------------------------------------------------------------------------------------

**SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.  
Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?**

A. Union-based SQLI

B. Out-of-band SQLI

C. ln-band SQLI

D. Time-based blind SQLI

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. … Out-of-band SQLi techniques would believe the database server’s ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable). Out-of-band SQLi techniques would rely on the database server’s ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server’s xp\_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database’s UTL\_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

---------------------------------------------------------------------------------------------------------

**which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?**

A. Bluesmacking

B. Bluebugging

C. Bluejacking

D. Bluesnarfing

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

---------------------------------------------------------------------------------------------------------

**Elante company has recently hired James as a penetration tester. He was tasked with performing enumeration on an organization's network. In the process of enumeration, James discovered a service that is accessible to external sources. This service runs directly on port 21. What is the service enumerated byjames in the above scenario?**

A. Border Gateway Protocol (BGP)

B. File Transfer Protocol (FTP)

C. Network File System (NFS)

D. Remote procedure call (RPC)

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?**

A. Preparation phase

B. Containment phase

C. Identification phase

D. Recovery phase

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**You have compromised a server and successfully gained root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?**

A. Use Alternate Data Streams to hide the outgoing packets from this server.

B. Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.

C. Install Cryptcat and encrypt outgoing packets from this server.

D. Install and use Telnet to encrypt all outgoing traffic from this server.

**Suggestion:**

The correct answer(s): C

https://linuxsecurityblog.com/2018/12/23/create-a-backdoor-with-cryptcat/ Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish, one of many excellent encryption algorithms from Bruce Schneier et al. Twofish’s encryption is on par with AES encryption, making it nearly bulletproof. In this way, the IDS can’t detect the malicious behavior taking place even when its traveling across normal HTTP ports like 80 and 443.

---------------------------------------------------------------------------------------------------------

**Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data has 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. Phishing malware

B. Zero-day malware

C. File-less malware

D. Logic bomb malware

**Suggestion:**

The correct answer(s): C

https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

---------------------------------------------------------------------------------------------------------

**A DDOS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target server opens multiple connections and keeps waiting for the requests to complete.  
Which attack is being described here?**

A. Desynchronization

B. Slowloris attack

C. Session splicing

D. Phlashing

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

Slowloris is DDoS attack software that permits one computer to require down an internet server. Due the straightforward yet elegant nature of this attack, it requires minimal bandwidth to implement and affects the target server’s web server only, with almost no side effects on other services and ports.Slowloris has proven highly-effective against many popular sorts of web server software, including Apache 1.x and 2.x.Over the years, Slowloris has been credited with variety of high-profile server takedowns.

---------------------------------------------------------------------------------------------------------

**Which tool can be used to silently copy files from USB devices?**

A. USB Grabber

B. USB Snoopy

C. USB Sniffer

D. USB Dumper

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

---------------------------------------------------------------------------------------------------------

**This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?**

A. WPA2 Personal

B. WPA3-Personal

C. WPA2-Enterprise

D. WPA3-Enterprise

**Suggestion:**

The correct answer(s): D

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network.WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data:• Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)• Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)• Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve• Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network. It protects sensitive data using many cryptographic algorithms It provides authenticated encryption using GCMP-256 It uses HMAC-SHA-384 to generate cryptographic keys It uses ECDSA-384 for exchanging keys

---------------------------------------------------------------------------------------------------------

**While using your bank’s online servicing you notice the following string in the URL bar:  
“http: // www. MyPersonalBank. com/ account?id=368940911028389&Damount=10980&Camount=21” You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes. Which type of vulnerability is present on this site?**

A. Cookie Tampering

B. SQL Injection

C. Web Parameter Tampering

D. XSS Reflection

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**What port number is used by LDAP protocol?**

A. 110

B. 389

C. 464

D. 445

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?**

A. PGP

B. S/MIME

C. SMTP

D. GPG

**Suggestion:**

The correct answer(s): D

**--------------------------------------------------------------------------------------------------------**

**During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?**

A. Circuit

B. Stateful

C. Application

D. Packet Filtering

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in text. The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web-based applications running either locally in the browser or on a third-party server. These clients communicate with chat servers to transfer messages to other clients. IRC is a plaintext protocol that is officially assigned port 194, according to IANA. However, running the service on this port requires running it with root-level permissions, which is inadvisable. As a result, the well-known port for IRC is 6667, a high-number port that does not require elevated privileges. However, an IRC server can also be configured to run on other ports as well. You can't tell if an IRC server is designed to be malicious solely based on port number. Still, if you see an IRC server running on port a WKP such as 80, 8080, 53, 443, it's almost always going to be malicious; the only real reason for IRCD to be running on port 80 is to try to evade firewalls. https://en.wikipedia.org/wiki/Internet\_Relay\_Chat An application firewall is a form of firewall that controls input/output or system calls of an application or service. It operates by monitoring and blocking communications based on a configured policy, generally with predefined rule sets to choose from. The application firewall can control communications up to the OSI model's application layer, which is the highest operating layer, and where it gets its name. The two primary categories of application firewalls are network-based and host-based. Application layer filtering operates at a higher level than traditional security appliances. This allows packet decisions to be made based on more than just source/destination IP Addresses or ports. It can also use information spanning across multiple connections for any given host. Network-based application firewalls Network-based application firewalls operate at the application layer of a TCP/IP stack. They can understand certain applications and protocols such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP). This allows it to identify unwanted applications or services using a non-standard port or detect if an allowed protocol is being abused. Host-based application firewalls A host-based application firewall monitors application system calls or other general system communication. This gives more granularity and control but is limited to only protecting the host it is running on. Control is applied by filtering on a per-process basis. Generally, prompts are used to define rules for processes that have not yet received a connection. Further filtering can be done by examining the process ID of the owner of the data packets. Many host-based application firewalls are combined or used in conjunction with a packet filter. https://en.wikipedia.org/wiki/Application\_firewall

---------------------------------------------------------------------------------------------------------

**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. PyLoris

B. Slowloris

C. Evilginx

D. PLCinject

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**Lewis, a professional hacker, targeted the loT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the loT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?**

A. Censys

B. Wapiti

C. NeuVector

D. Lacework

**Suggestion:**

The correct answer(s): A

Censys scans help the scientific community accurately study the Internet. The data is sometimes used to detect security problems and to inform operators of vulnerable systems so that they can fixed

---------------------------------------------------------------------------------------------------------

**Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?  
The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.**

A. My Doom

B. Astacheldraht

C. R-U-Dead-Yet?(RUDY)

D. LOIC

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?**

A. Traffic is Blocked on UDP Port 53

B. Traffic is Blocked on TCP Port 80

C. Traffic is Blocked on TCP Port 54

D. Traffic is Blocked on UDP Port 80

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script.  
After infecting the victim's device. Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives. What is the tool employed by Mason in the above scenario?**

A. NetPass.exe

B. Outlook scraper

C. WebBrowserPassView

D. Credential enumerator

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

Currently, Emotet uses five known spreader modules: NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, and a credential enumerator. Credential enumerator is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for the enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet writes the service component on the system, which writes Emotet onto the disk. Emotet’s access to SMB can result in the infection of entire domains (servers and clients).

---------------------------------------------------------------------------------------------------------

**Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?**

A. PGP

B. S/MIME

C. SMTP

D. GPG

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.  
What is the port scanning technique used by Sam to discover open ports?**

A. Xmas scan

B. IDLE/IPID header scan

C. TCP Maimon scan

D. ACK flag probe scan

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?**

A. http-methods

B. http enum

C. http-headers

D. http-git

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**An attacker scans a host with the below command. Which three flags are set?  
# nmap -sX host.domain.com**

A. This is SYN scan. SYN flag is set.

B. This is Xmas scan. URG, PUSH and FIN are set.

C. This is ACK scan. ACK flag is set.

D. This is Xmas scan. SYN and ACK flags are set.

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**Password cracking programs reverse the hashing process to recover passwords. (True/False.)**

A. True

B. False

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**Why containers are less secure that virtual machines?**

A. Host OS on containers has a larger surface attack.

B. Containers may full fill disk space of the host.

C. A compromise container may cause a CPU starvation of the host.

D. Containers are attached to the same virtual network.

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network’s external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?**

A. Protocol analyzer

B. Network sniffer

C. Intrusion Prevention System (IPS)

D. Vulnerability scanner

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**What hacking attack is challenge/response authentication used to prevent?**

A. Replay attacks

B. Scanning attacks

C. Session hijacking attacks

D. Password cracking attacks

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**in this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstall the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?**

A. Chop chop attack

B. KRACK

C. Evil twin

D. Wardriving

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**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?**

A. tcp.srcport= = 514 && ip.src= = 192.168.0.99

B. tcp.srcport= = 514 && ip.src= = 192.168.150

C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99

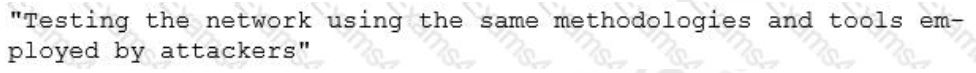
D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

**Suggestion:**

The correct answer(s): D

---------------------------------------------------------------------------------------------------------

**Identify the correct terminology that defines the above statement.**



A. Vulnerability Scanning

B. Penetration Testing

C. Security Policy Implementation

D. Designing Network Security

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**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’

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

---------------------------------------------------------------------------------------------------------

**which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?**

A. Bluesmacking

B. Bluebugging

C. Bluejacking

D. Bluesnarfing

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

---------------------------------------------------------------------------------------------------------

**In the context of Windows Security, what is a 'null' user?**

A. A user that has no skills

B. An account that has been suspended by the admin

C. A pseudo account that has no username and password

D. A pseudo account that was created for security administration purpose

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

---------------------------------------------------------------------------------------------------------

**Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.  
Which of the following master components is explained in the above scenario?**

A. Kube-controller-manager

B. Kube-scheduler

C. Kube-apiserver

D. Etcd cluster

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

Kube-scheduler is a master component that scans newly generated pods and allocates a node for them.

---------------------------------------------------------------------------------------------------------

**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. Dark web footprinting

B. VoIP footprinting

C. VPN footprinting

D. website footprinting

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

The deep web is the layer of the online cyberspace that consists of web pages and content that are hidden and unindexed.

---------------------------------------------------------------------------------------------------------

**What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?**

A. Man-in-the-middle attack

B. Meet-in-the-middle attack

C. Replay attack

D. Traffic analysis attack

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

https://en.wikipedia.org/wiki/Meet-in-the-middle\_attack The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space–time tradeoff cryptographic attack against encryption schemes that rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2112 operations. The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the 3DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

---------------------------------------------------------------------------------------------------------

**Which of the following statements is TRUE?**

A. Packet Sniffers operate on the Layer 1 of the OSI model

B. Packet Sniffers operate on Layer 2 of the OSI model.

C. Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model

D. Packet Sniffers operate on Layer 3 of the OSI model

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?**

A. 110

B. 135

C. 139

D. 161

E. 445

F. 1024

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B C E

---------------------------------------------------------------------------------------------------------

**An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password. What kind of attack is this?**

A. MAC spoofing attack

B. Evil-twin attack

C. War driving attack

D. Phishing attack

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------------

**Which among the following is the best example of the third step (delivery) in the cyber kill chain?**

A. An intruder sends a malicious attachment via email to a target.

B. An intruder creates malware to be used as a malicious attachment to an email.

C. An intruder's malware is triggered when a target opens a malicious email attachment.

D. An intruder's malware is installed on a target's machine.

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

A. Use the built-in Windows Update tool

B. Use a scan tool like Nessus

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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.

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

In IP networking, a private network is a computer network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments. Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries. Private IP address spaces were originally defined to assist in delaying IPv4 address exhaustion. IP packets originating from or addressed to a private IP address cannot be routed through the public Internet. The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks: • 10.0.0.0 – 10.255.255.255 • 172.16.0.0 – 172.31.255.255 • 192.168.0.0 – 192.168.255.255 Backbone routers do not allow packets from or to internal IP addresses. That is, intranet machines, if no measures are taken, are isolated from the Internet. However, several technologies allow such machines to connect to the Internet. • Mediation servers like IRC, Usenet, SMTP and Proxy server • Network address translation (NAT) • Tunneling protocol NOTE: So, the problem is just one of these technologies. https://en.wikipedia.org/wiki/Private\_network

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

File system permissions

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?**

A. tcpsplice

B. Burp

C. Hydra

D. Whisker

**Suggestion:**

The correct answer(s): D\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report\_queue/rq\_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?**

A. Paros Proxy

B. BBProxy

C. Blooover

D. BBCrack

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?**

A. Port 53

B. Port 23

C. Port 50

D. Port 80

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-lnternal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?**

A. Dragonblood

B. Cross-site request forgery

C. Key reinstallation attack

D. AP Myconfiguration

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**During an Xmas scan what indicates a port is closed?**

A. No return response

B. RST

C. ACK

D. SYN

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level visualization, delivers containerized software packages, and promotes fast software delivery. What is the cloud technology employed by Alex in the above scenario?**

A. Virtual machine

B. Serverless computing

C. Docker

D. Zero trust network

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

A. c:\compmgmt.msc

B. c:\services.msc

C. c:\ncpa.cp

D. c:\gpedit

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?**

A. Nikto

B. Nmap

C. Metasploit

D. Armitage

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:  
You are hired to conduct security testing on their network. You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection. You want to retrieve the Cisco configuration from the router. How would you proceed?**

A. Use the Cisco's TFTP default password to connect and download the configuration file

B. Run a network sniffer and capture the returned traffic with the configuration file from the router

C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address

D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?**

A. Interceptor

B. Man-in-the-middle

C. ARP Proxy

D. Poisoning Attack

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Attacker uses various IDS evasion techniques to bypass intrusion detection mechanisms. At the same time, IDS is configured to detect possible violations of the security policy, including unauthorized access and misuse. Which of the following evasion method depend on the Time-to-Live (TTL) fields of a TCP/IP ?

● Denial-of-Service Attack ● Unicode Evasion ● Insertion Attack (Correct) ● Obfuscation

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Elon plans to make it difficult for the packet filter to determine the purpose of the packet when scanning. Which of the following scanning techniques will Elon use?

● ICMP scanning. ● ACK scanning. ● IPID scanning. ● SYN/FIN scanning using IP fragments.(Correct)

Explanation SYN/FIN scanning using IP fragments is a process of scanning that was developed to avoid false positives generated by other scans because of a packet filtering device on the target system. The TCP header splits into several packets to evade the packet filter. For any transmission, every TCP header must have the source and destination port for the initial packet (8-octet, 64-bit). The initialized flags in the next packet allow the remote host to reassemble the packets upon receipt via an Internet protocol module that detects the fragmented data packets using field-equivalent values of the source, destination, protocol, and identification.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the IDAP service for sensitive information such as usernames. addresses, departmental details, and server names to launch further attacks on the target organization.  
What is the tool employed by John to gather information from the IDAP service?**

A. jxplorer

B. Zabasearch

C. EarthExplorer

D. Ike-scan

**Suggestion:**

The correct answer(s): A

JXplorer could be a cross platform LDAP browser and editor. it’s a standards compliant general purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface. It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program. JX is is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools. JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release. JXplorer could be a absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol. it’s been tested on Windows, Solaris, linux and OSX, packages are obtainable for HPUX, AIX, BSD and it should run on any java supporting OS.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Windows LAN Manager (LM) hashes are known to be weak.  
Which of the following are known weaknesses of LM? (Choose three.)**

A. Converts passwords to uppercase.

B. Hashes are sent in clear text over the network.

C. Makes use of only 32-bit encryption.

D. Effective length is 7 characters.

**Suggestion:**

The correct answer(s): A B D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior 10 the Intrusion. This Is likely a failure in which of the following security processes?**

A. vendor risk management

B. Security awareness training

C. Secure deployment lifecycle

D. Patch management

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

Patch management is that the method that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a pc, enabling systems to remain updated on existing patches and determining that patches are the suitable ones. Managing patches so becomes simple and simple. Patch Management is usually done by software system firms as a part of their internal efforts to mend problems with the various versions of software system programs and also to assist analyze existing software system programs and discover any potential lack of security features or different upgrades. Software patches help fix those problems that exist and are detected solely once the software’s initial unharness. Patches mostly concern security while there are some patches that concern the particular practicality of programs as well.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What is a NULL scan?**

A. A scan in which all flags are turned off

B. A scan in which certain flags are off

C. A scan in which all flags are on

D. A scan in which the packet size is set to zero

E. A scan with an illegal packet size

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.  
Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?**

A. .stm

B. .html

C. .rss

D. .cms

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**in an attempt to increase the security of your network, you Implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know It. How do you accomplish this?**

A. Delete the wireless network

B. Remove all passwords

C. Lock all users

D. Disable SSID broadcasting

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.  
When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?**

A. Wireshark

B. Ettercap

C. C. Aircrack-ng

D. Tcpdump

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What is the least important information when you analyze a public IP address in a security alert?**

A. DNS

B. Whois

C. Geolocation

D. ARP

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

A. 3.0-6.9

B. 4.0-6.0

C. 4.0-6.9

D. 3.9-6.9

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**John, a security analyst working for an organization, found a critical vulnerability on the organization's LAN that allows him to view financial and personal information about the rest of the employees. Before reporting the vulnerability, he examines the information shown by the vulnerability for two days without disclosing any information to third parties or other internal employees. He does so out of curiosity about the other employees and may take advantage of this information later. What would John be considered as?**

A. Cybercriminal

B. Black hat

C. White hat

D. Gray hat

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website. www.movlescope.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 bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.**

A. Null byte

B. IP fragmentation

C. Char encoding

D. Variation

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

One may append the comment “–” operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the — operator would be considered as comment and not dead. To launch such an attack, the value passed for name could be ’OR ‘1’=‘1’ ; —Statement = “SELECT \* FROM ‘CustomerDB’ WHERE ‘name’ = ‘ ”+ userName + “ ‘ AND ‘password’ = ‘ ” + passwd + “ ‘ ; ” Statement = “SELECT \* FROM ‘CustomerDB’ WHERE ‘name’ = ‘ ’ OR ‘1’=‘1‘;– + “ ‘ AND ‘password’ = ‘ ” + passwd + “ ‘ ; ” All the records from the customer database would be listed. Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn’t strongly used in or isn’t checked for sort constraints. This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric. Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as “' or '1'='1'” in any basic injection statement such as “or 1=1” or with other accepted SQL comments. Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as “' or '1'='1'” in any basic injection statement such as “or 1=1” or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as “true” so that any mathematical or string comparison can be used, where the SQL can perform the same.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

A. OS Detection

B. Firewall detection

C. TCP/UDP Port scanning

D. Checking if the remote host is alive

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

A. Regularly test security systems and processes.

B. Encrypt transmission of cardholder data across open, public networks

C. Assign a unique ID to each person with computer access.

D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.  
Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.**

A. SNMPUtil

B. SNScan

C. SNMPScan

D. Solarwinds IP Network Browser

E. Nmap

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A B D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?**

A. WEP

B. RADIUS

C. WPA

D. WPA3

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the loT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of loT devices and detect whether they are using the default, factory-set credentials. What is the tool employed by John in the above scenario?**

A. loTSeeker

B. loT Inspector

C. AT&T loT Platform

D. Azure loT Central

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message ''Hacker Message: You are dead! Freaks!” From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.  
No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page: (ảnh) After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?**

A. ARP spoofing

B. SQL injection

C. DNS poisoning

D. Routing table injection

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.  
Which cryptography attack is the student attempting?**

A. Man-in-the-middle attack

B. Brute-force attack

C. Dictionary attack

D. Session hijacking

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Which of the following tools can be used to perform a zone transfer?**

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

F. Netcat

G. Neotrace

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A C D E

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111  
(content:"|00 01 86 a5|"; msG. "mountd access";)**

A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111

B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet

C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet

D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Which DNS resource record can indicate how long any "DNS poisoning" could last?**

A. MX

B. SOA

C. NS

D. TIMEOUT

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

The SOA contains information of secondary servers, update intervals and expiration times.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?**

A. Red hat

B. white hat

C. Black hat

D. Gray hat

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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. D. The document can be sent to the accountant using an exclusive USB for that document

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands. Which of the following commands was used by Clark to hijack the connections?**

A. btlejack-f 0x129f3244-j

B. btlejack -c any

C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s

D. btlejack -f 0x9c68fd30 -t -m 0x1 fffffffff

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Which of the following tools are used for enumeration? (Choose three.)**

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER

E. DumpSec

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B D E

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Which of the following steps for risk assessment methodology refers to vulnerability identification?**

A. Determines if any flaws exist in systems, policies, or procedures

B. Assigns values to risk probabilities; Impact values.

C. Determines risk probability that vulnerability will be exploited (High. Medium, Low)

D. Identifies sources of harm to an IT system. (Natural, Human. Environmental)

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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. SaaS

B. IaaS

C. CaaS

D. PasS

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?**

A. Error-based injection

B. Boolean-based blind SQL injection

C. Blind SQL injection

D. Union SQL injection

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.  
Why he cannot see the servers?**

A. He needs to add the command ““ip address”” just before the IP address

B. He needs to change the address to 192.168.1.0 with the same mask

C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range

D. The network must be dawn and the nmap command and IP address are ok

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept. What is the Wi-Fi encryption technology implemented by Debry Inc.?**

A. WEP

B. WPA

C. WPA2

D. WPA3

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Dorian Is sending a digitally signed email to Polly, 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 Polys public 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 Polys private key. and Poly will verify mat the message came from Dorian by using Dorian's public key.

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

https://blog.mailfence.com/how-do-digital-signatures-work/ https://en.wikipedia.org/wiki/Digital\_signature A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide evidence of origin, identity, and status of electronic documents, transactions, or digital messages. Signers can also use them to acknowledge informed consent. Digital signatures are based on public-key cryptography, also known as asymmetric cryptography. Two keys are generated using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), creating a mathematically linked pair of keys, one private and one public. Digital signatures work through public-key cryptography's two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**By using a smart card and pin, you are using a two-factor authentication that satisfies**

A. Something you are and something you remember

B. Something you have and something you know

C. Something you know and something you are

D. Something you have and something you are

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?**

A. Identifying operating systems, services, protocols and devices

B. Modifying and replaying captured network traffic

C. Collecting unencrypted information about usernames and passwords

D. Capturing a network traffic for further analysis

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.  
What is the technique used by Jacob in the above scenario to improve the security of the mobile application?**

A. Reverse engineering

B. App sandboxing

C. Jailbreaking

D. Social engineering

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses\_\_\_\_\_\_\_to encrypt the message, and Bryan uses\_\_\_\_\_\_\_\_\_\_to confirm the digital signature.**

A. Bryan’s public key; Bryan’s public key

B. Alice’s public key; Alice’s public key

C. Bryan’s private key; Alice’s public key

D. Bryan’s public key; Alice’s public key

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

Alice should Use Bryan's public key so only Brian can decrypt it with his private key. Bryan will use Alice's public key to confirm this msg came from Alice as she is the only one with the private key.

Alice: Signs msg with own private key & uses Bryan's public key is used for encryption Bryan: decrypts with own private key & uses Alice's public key to verify the signed msg

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What is a “Collision attack” in cryptography?**

A. Collision attacks try to get the public key

B. Collision attacks try to break the hash into three parts to get the plaintext value

C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key

D. Collision attacks try to find two inputs producing the same hash

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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. DROWN attack

B. Padding oracle attack

C. Side-channel attack

D. DUHK attack

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

The DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attack is a cross-protocol security bug that attacks servers supporting modern SSLv3/TLS protocol suites by using their support for the obsolete, insecure, SSL v2 protocol to leverage an attack on connections using up-to-date protocols that would otherwise be secure.[1][2] DROWN can affect all types of servers that offer services encrypted with SSLv3/TLS yet still support SSLv2, provided they share the same public key credentials between the two protocols.[3] Additionally, if the same public key certificate is used on a different server that supports SSLv2, the TLS server is also vulnerable due to the SSLv2 server leaking key information that can be used against the TLS server.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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 packet, but the target web server can decode them.  
What is the technique used by Kevin to evade the IDS system?**

A. Desynchronization

B. Obfuscating

C. Session splicing

D. Urgency flag

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?**

A. list server=192.168.10.2 type=all

B. is-d abccorp.local

C. Iserver 192.168.10.2-t all

D. List domain=Abccorp.local type=zone

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?**

A. Docker client

B. Docker objects

C. Docker daemon

D. Docker registries

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

Docker daemon is also called docker server and it listens for Docker API requests and manages Docker objects such as images, containers, networks, and volumes. A daemon can also communicate with other daemons to manage Docker services.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?**

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.

B. He will activate OSPF on the spoofed root bridge.

C. He will repeat this action so that it escalates to a DoS attack.

D. He will repeat the same attack against all L2 switches of the network.

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?**

A. DroidSheep

B. Androrat

C. Zscaler

D. Trident

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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. What is the type of vulnerability assessment performed by Martin?**

A. Credentialed assessment

B. Database assessment

C. Host-based assessment

D. Distributed assessment

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?**

A. msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.10.30 LPORT=4444 -f c

B. msfvenom -p windows/meterpreter/reverse\_tcp RHOST=10.10.10.30 LPORT=4444 -f c

C. msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

D. msfvenom -p windows/meterpreter/reverse\_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?**

A. Role Based Access Control (RBAC)

B. Discretionary Access Control (DAC)

C. Single sign-on

D. Windows authentication

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.  
Which file do you have to clean to clear the password?**

A. .X session-log

B. .bashrc

C. .profile

D. .bash\_history

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed.BASH\_HISTORY files are hidden files with no filename prefix. They always use the filename .bash\_history.NOTE: Bash is that the shell program employed by Apple Terminal.Our goal is to assist you understand what a file with a \*.bash\_history suffix is and the way to open it.The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we’ve tested and validated.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Why should the security analyst disable/remove unnecessary ISAPI filters?**

A. To defend against social engineering attacks

B. To defend against webserver attacks

C. To defend against jailbreaking

D. To defend against wireless attacks

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

---------------------------------------------------------------------------------------------------

**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 deckled 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

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?**

A. Residual risk

B. Impact risk

C. Deferred risk

D. Inherent risk

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Attempting an injection attack on a web server based on responses to True/False QUESTION NO:s is called which of the following?**

A. Compound SQLi

B. Blind SQLi

C. Classic SQLi

D. DMS-specific SQLi

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-lnternal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?**

A. Dragonblood

B. Cross-site request forgery

C. Key reinstallation attack

D. AP Myconfiguration

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command you would use?**

A. wireshark --fetch ''192.168.8\*''

B. wireshark --capture --local masked 192.168.8.0 ---range 24

C. tshark -net 192.255.255.255 mask 192.168.8.0

D. sudo tshark -f''net 192 .68.8.0/24''

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**E-mail scams and mail fraud are regulated by which of the following?**

A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers

B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices

C. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems

D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Which of the following is a low-tech way of gaining unauthorized access to systems?**

A. Social Engineering

B. Eavesdropping

C. Scanning

D. Sniffing

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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.mlb or by entering the DNS library name and Lseries.mlb. 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. WINS.MIB

C. DHCP.MIS

D. MIB\_II.MIB

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): A

DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts HOSTMIB.MIB: Monitors and manages host resources LNMIB2.MIB: Contains object types for workstation and server services MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system WINS.MIB: For the Windows Internet Name Service (WINS)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files. What is the type of injection attack Calvin's web application is susceptible to?**

A. Server-side template injection

B. Server-side JS injection

C. CRLF injection

D. Server-side includes injection

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): D

Server-side Includes is an application feature. Attackers exploit this feature to pass malicious SSI directives as input values and perform malicious activities.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Clark, a professional hacker, was hired by an organization lo gather sensitive Information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whole 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. AOL

B. ARIN

C. DuckDuckGo

D. Baidu

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

https://search.arin.net/rdap/?query=199.43.0.43

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**During an Xmas scan what indicates a port is closed?**

A. No return response

B. RST

C. ACK

D. SYN

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What does the following command in netcat do?  
nc -l -u -p55555 < /etc/passwd**

A. logs the incoming connections to /etc/passwd file

B. loads the /etc/passwd file to the UDP port 55555

C. grabs the /etc/passwd file when connected to UDP port 55555

D. deletes the /etc/passwd file when connected to the UDP port 55555

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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. Hootsuite

C. VisualRoute

D. HULK

Answer Mark and next Verify

**Suggestion:**

The correct answer(s): B

Hootsuite may be a social media management platform that covers virtually each side of a social media manager’s role. With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI. There area unit many totally different plans to decide on from, from one user set up up to a bespoken enterprise account that’s appropriate for much larger organizations. Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...