CEH v12
125 Questions and Answers

Linkedin: https://www.linkedin.com/in/moshe-ovadia

2024

What is the purpose of the demilitarized zone?

- To provide a place for a honeypot.
- TO add an extra layer of security to an organization’s local area network.
- To add a protect to network devices.
- To scan all traffic coming through the DMZ to the internal network.

Ivan, the black hat hacker, split the attack traffic into many packets such that no single packet triggers the IDS. Which IDS evasion technique does Ivan use?

- Flooding.
- Low-bandwidth attacks.
- Session Splicing
- Unicode Splicing.

Which of the following requires establishing national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers?

- SOX
- DMCA
- PCI-DSS
- HIPAA

John, a cybersecurity specialist, received a copy of the event logs from all firewalls, Intrusion Detection Systems (IDS) and proxy servers on a company's network. He tried to match all the registered events in all the logs, and he found that their sequence didn't match. What can cause such a problem?

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

You are configuring the connection of a new employee's laptop to join an 802.11 network. The new laptop has the same hardware and software as the laptops of other employees. You used the wireless packet sniffer and found that it shows that the Wireless Access Point (WAR) is not responding to the association requests being sent by the laptop. What can cause this problem?

- The laptop is configured for the wrong channel.
- The WAP does not recognize the laptop’s MAC address.
- The laptop cannot see the SSID of the wireless network.
- The laptop is not configured to use DHCP.

Which of the following flags will trigger Xmas scan?

- -sX
- -sP
- -sA
- -sV

Ivan, an evil hacker, conducts an SQLi attack that is based on True/False questions. What type of SQLi does Ivan use?

- Blind SQLi
- Compound SQLi
- Classic SQLi
- DMS-specific SQLi

Rajesh, a system administrator, noticed that some clients of his company were victims of DNS Cache Poisoning. They were redirected to a malicious site when they tried to access Rajesh's company site. What is the best recommendation to deal with such a threat?

- Use of security agents on customers’ computers.
- Use a multi-factor authentication.
- Customer awareness.
- Use Domain Name System Security Extensions (DNSSEC)

Which of the following wireless standard has bandwidth up to 54 Mbit/s and signals in a regulated frequency spectrum around 5 GHz?

- 802.11a
- 802.11i
- 802.11n
- 802.11g

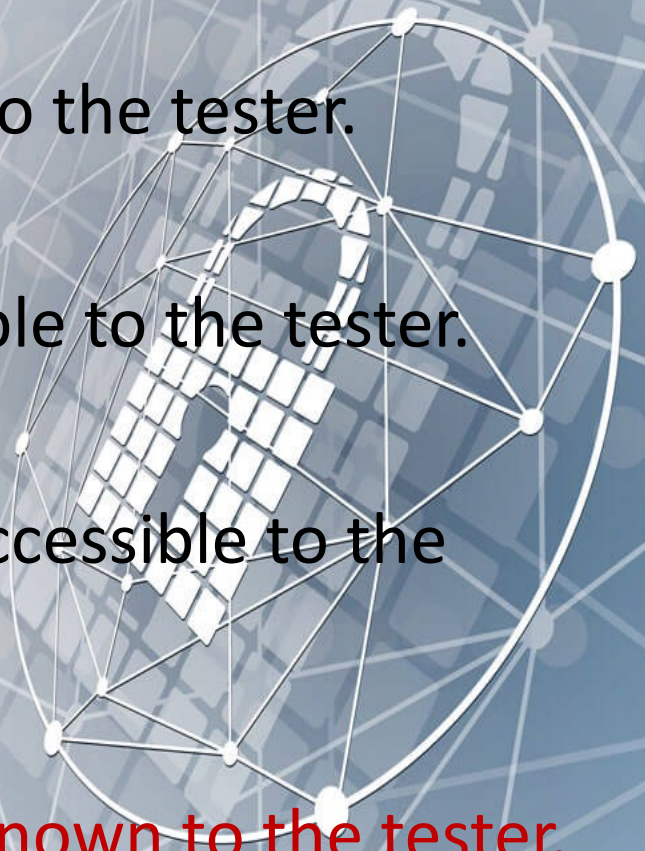
Michael works as a system administrator. He receives a message that several sites are no longer available. Michael tried to go to the sites by URL, but it didn't work. Then he tried to ping the sites and enter IP addresses in the browser - it worked. What problem could Michael identify?

- Traffic is Blocked on UDP Port 56
- Traffic is Blocked on UDP Port 69
- Traffic is Blocked on UDP Port 53
- Traffic is Blocked on UDP Port 88

The attacker enters its malicious data into intercepted messages in a TCP session since source routing is disabled. He tries to guess the responses of the client and server. What hijacking technique is described in this example?

- RST
- Blind
- TCP/IP
- Registration

Which of the following best describes the "white box testing" methodology?



- Only the internal operation of a system is known to the tester.
- Only the external operation of a system is accessible to the tester.
- The internal operation of a system is only partly accessible to the tester.
- The internal operation of a system is completely Known to the tester.

Which of the following SQL injection attack does an attacker usually bypassing user authentication and extract data by using a conditional OR clause so that the condition of the WHERE clause will always be true?

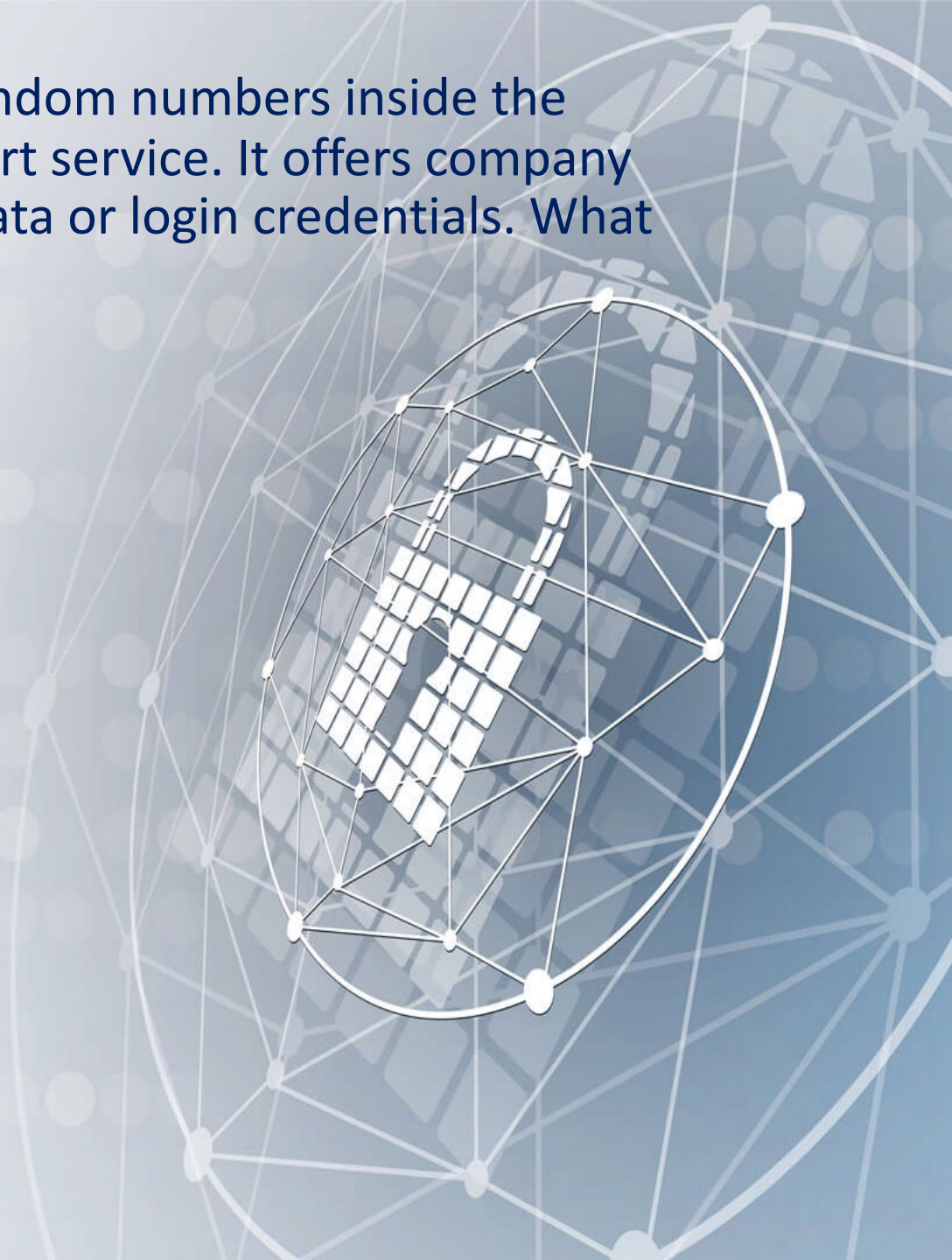
- Error-Based SQLi
- Tautology
- End-of-Line Comment
- UNION SQLi

Wireshark is one of the most important tools for a cybersecurity specialist. It is used for network troubleshooting, analysis, software, etc. And you often have to work with a packet bytes pane. In what format is the data presented in this pane?

- Hexadecimal
- Decimal
- ASCII only
- Binary

Ivan, a black hat hacker, tries to call numerous random numbers inside the company, claiming he is from the technical support service. It offers company employee services in exchange for confidential data or login credentials. What method of social engineering does Ivan use?

- Quid Pro Quo
- Reverse Social Engineering
- Elicitation
- Tailgating



Black hat hacker Ivan wants to implement a man-in-the-middle attack on the corporate network. For this, he connects his router to the network and redirects traffic to intercept packets. What can the administrator do to mitigate the attack?

- Use the Open Shortest Path First (OSPF).
- Use only static routes in the corporation’s network.
- Redirection of the traffic is not possible without the explicit admin’s confirmation.
- Add message authentication to the routing protocol.

Andrew is conducting a penetration test. He is now embarking on sniffing the target network. What is not available for Andrew when sniffing the network?

- Collecting unencrypted information about usernames and passwords.
- Modifying and replaying captured network traffic.
- Identifying operating systems, services, protocols and devices.
- Capturing network traffic for further analysis.

Ivan, a black hat hacker, sends partial HTTP requests to the target webserver to exhaust the target server's maximum concurrent connection pool. He wants to ensure that all additional connection attempts are rejected. What type of attack does Ivan implement?

- HTTP GET/POST
- Spoofed Session Flood
- Fragmentation
- Slowloris

You managed to compromise a server with an IP address of 10.10.0.5, and you want to get fast a list of all the machines in this network. Which of the following Nmap command will you need?

- nmap –T4 –F 10.10.0.0/24
- nmap –T4 –p 10.10.0.0/24
- nmap –T4 –q 10.10.0.0/24
- nmap –T4 –r 10.10.1.0/24

Which of the following can be designated as "Wireshark for CLI"?

- John the Ripper
- nessus
- ethereal
- tcpdump

Which of the following layers in IoT architecture helps bridge the gap between two endpoints, such as a device and a client, and carries out message routing, message identification, and subscribing?

- Internet.
- Middleware.
- Edge Technology.
- Access Gateway.

Which of the following is the risk that remains after the amount of risk left over after natural or inherent risks have been reduced?

- Residual risk.
- Impact risk.
- Inherent risk.
- Deferrred risk.

Identify a vulnerability in OpenSSL that allows stealing the information protected under normal conditions by the SSL/TLS encryption used to secure the Internet?

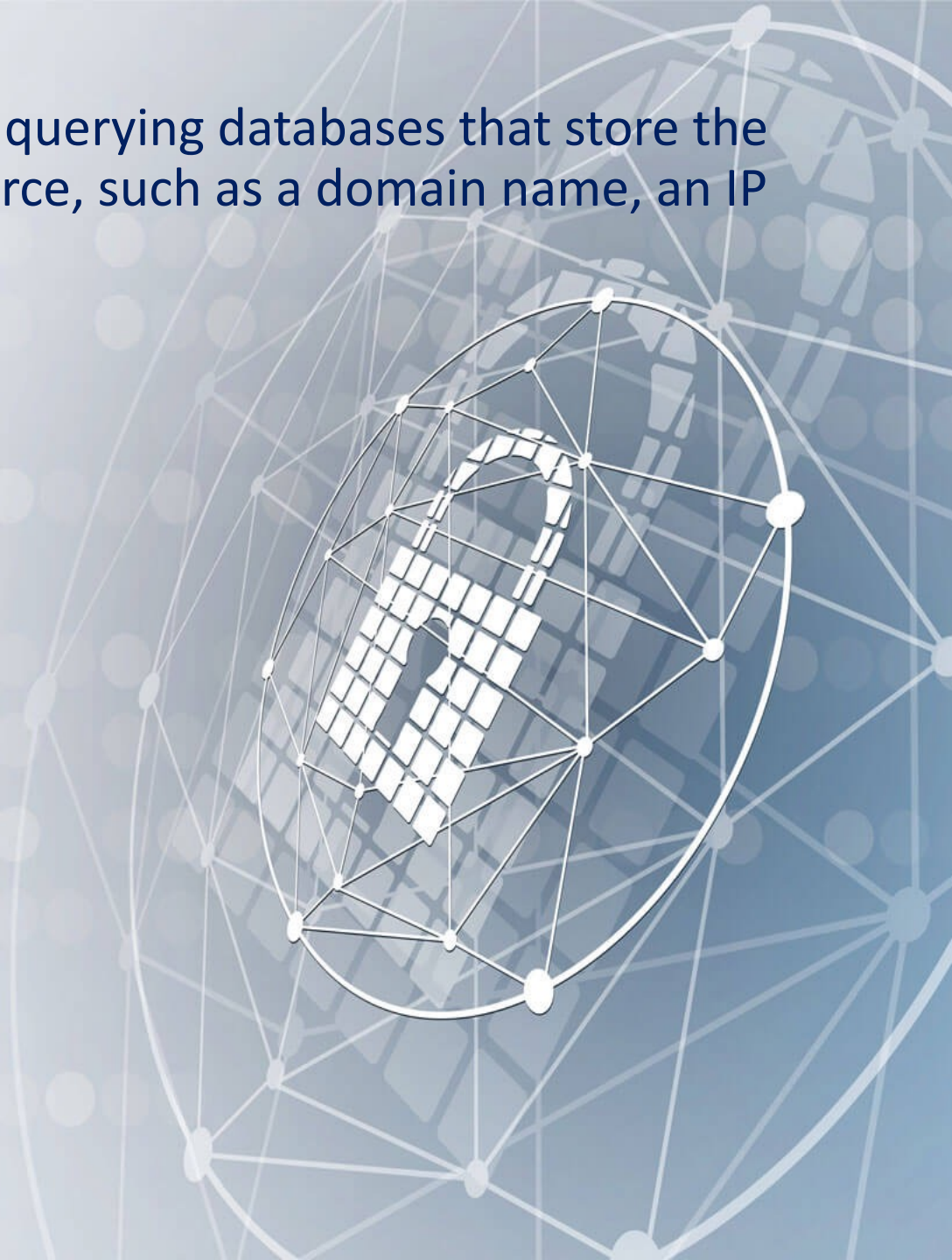
- SSL/TLS Renegotiation Vulnerability.
- Shellshock.
- POODLE.
- Heartbleed Bug.

The attacker posted a message and an image on the forum, in which he embedded a malicious link. When the victim clicks on this link, the victim's browser sends an authenticated request to a server. What type of attack did the attacker use?

- Cross-site request forgery.
- Session hijacking
- SQL injection
- Cross-site scripting.

Which of the following is a protocol that used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system?

- CAPTCHA
- WHOIS
- Internet Engineering Task Force.
- Internet Assigned Numbers Authority

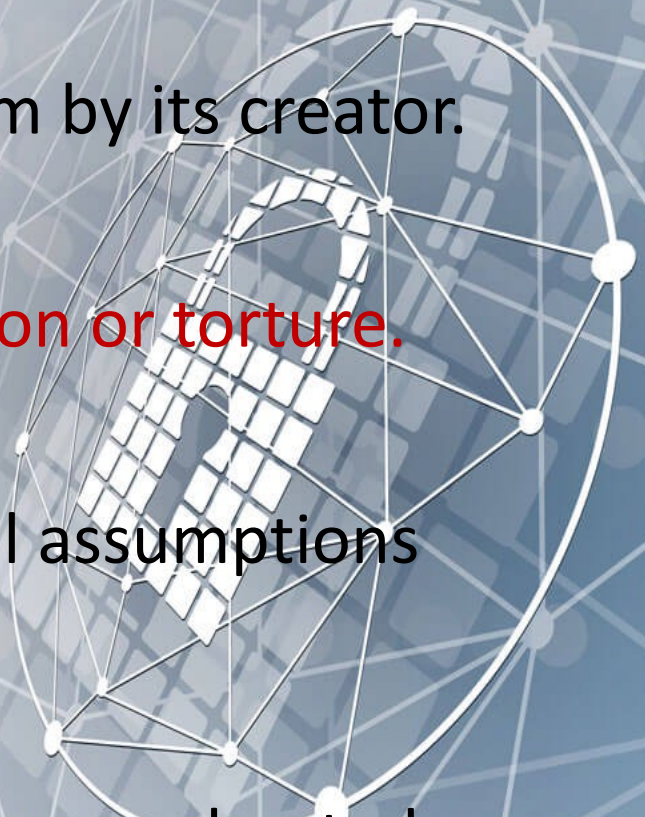


John, a penetration tester, decided to conduct SQL injection testing. He enters a huge amount of random data and observes changes in output and security loopholes in web applications. What SQL injection testing technique did John use?

- Static Testing.
- Function Testing.
- Dynamic Testing.
- Fuzzing Testing.

What is meant by a "rubber-hose" attack in cryptography?

- A backdoor is placed into a cryptographic algorithm by its creator.
- Extraction of cryptographic secrets through coercion or torture.
- Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plain text.
- Forcing the targeted keystream through a hardware-accelerated device such as an ASIC



Ivan, an evil hacker, is preparing to attack the network of a financial company. To do this, he wants to collect information about the operating systems used on the company's computers. Which of the following techniques will Ivan use to achieve the desired result?

- IDLE/IPID Scanning.
- Banner Grabbing.
- UDP Scanning.
- SSDP Scanning.

Which of the following does not apply to IPsec?

- Provides authentication.
- Use Key exchange.
- Work at the Data Link Layer.
- Encrypts the payloads.

What actions should be performed before using a Vulnerability Scanner for scanning a network?

- Firewall detection.
- TCP/UDP Port scanning.
- TCP/IP stack fingerprinting.
- Checking if the remote host is alive.

Which of the following is the type of violation when an unauthorized individual enters a building following an employee through the employee entrance?

- Announced.
- Tailgating.
- Reverse Social Engineering.
- Pretexting.

Which of the following option is a security feature on switches leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- DAI
- Port security.
- Spanning tree.
- DHCP relay.

Maria conducted a successful attack and gained access to a Linux server. She wants to avoid that NIDS will not catch the succeeding outgoing traffic from this server in the future. Which of the following is the best way to avoid detection of NIDS?

- Encryption.
- Out of band signaling.
- Alternate Data Streams.
- Protocol Isolation.

Which of the following Nmap's commands allows you to most reduce the probability of detection by IDS when scanning common ports?

- nmap -A --host-timeout 99-T1
- nmap -sT -O -T0
- nmap -A -Pn
- nmap -sT -O -T2

Identify Secure Hashing Algorithm, which produces a 160-bit digest from a message on principles similar to those used in MD4 and MD5?

- SHA-0
- SHA-3
- SHA-1
- SHA-2

What best describes two-factor authentication for a credit card (using a card and pin)?

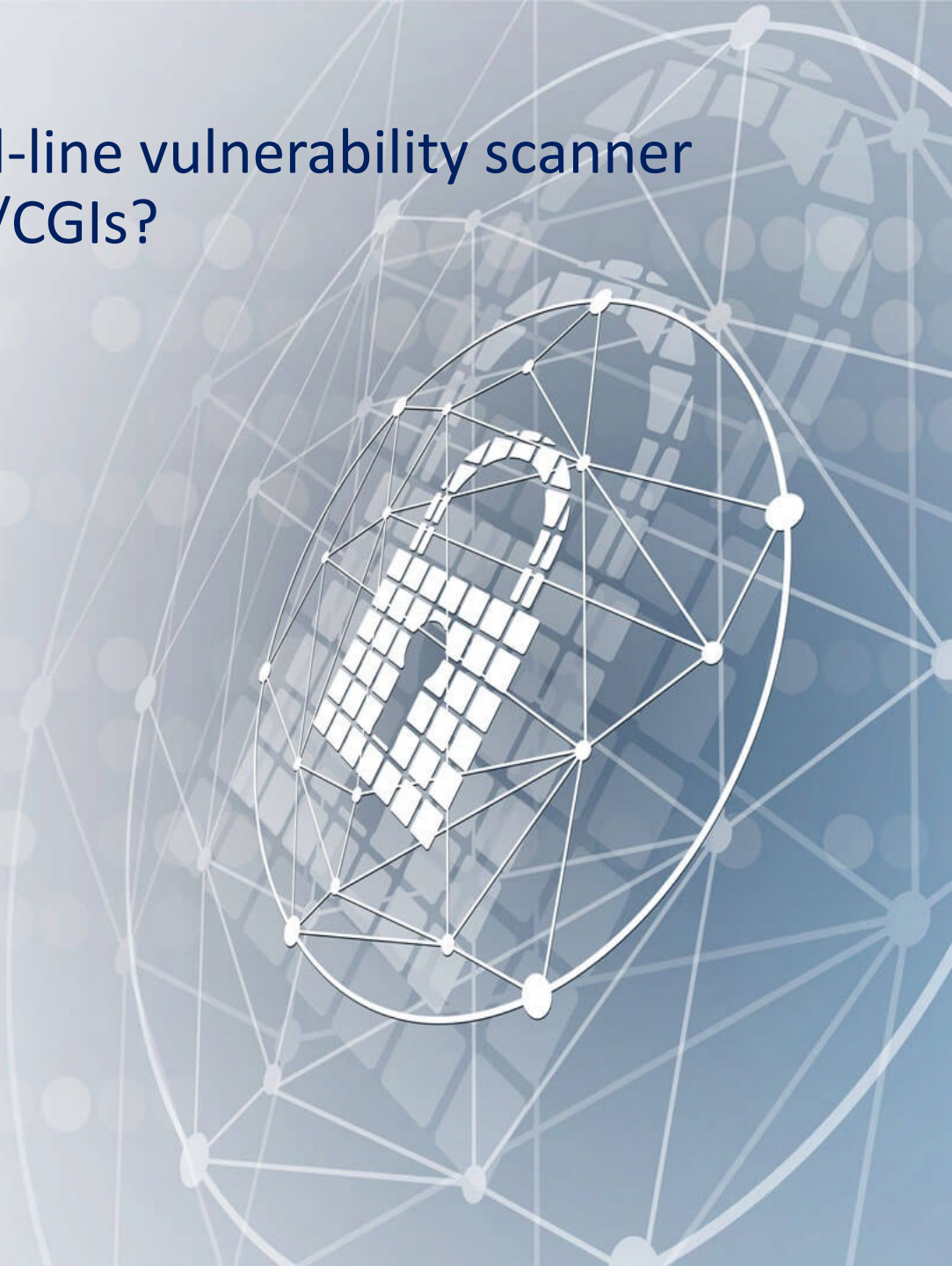
- Something you have and something you are.
- Something you are and something you remember.
- Something you Know and something you are.
- Something you have and something you Know.

Which of the following command-line flags set a stealth scan for Nmap?

- -sT
- -sU
- -sS
- -sM

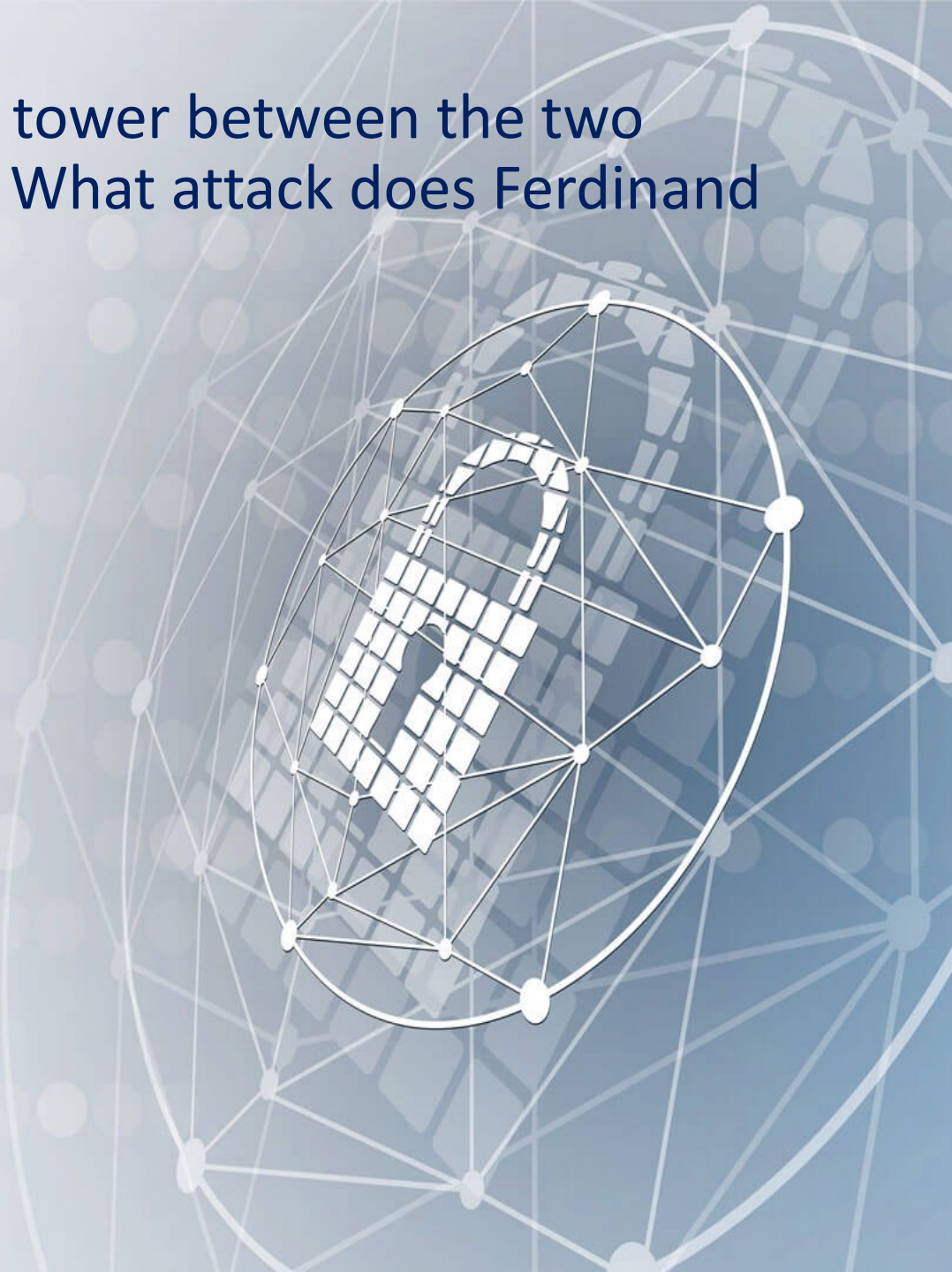
Which of the following tools is a command-line vulnerability scanner that scans web servers for dangerous files/CGIs?

- Nikto
- John the Ripper
- Snort
- Kon-Boot



Ferdinand installs a virtual communication tower between the two authentic endpoints to mislead the victim. What attack does Ferdinand perform?

- Wi-Jacking
- Sinkhole
- aLTEr
- Aspidistra



Determine the attack by the description: The known-plaintext attack used against DES. This attack causes 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.

- Replay attack
- Meet-in-the-middle attack
- Man-in-the-middle attack
- Traffic analysis attack

Identify the type of jailbreaking which allows user-level access and does not allow iboot-level access?

- Userland Exploit
- Bootrom Exploit
- iBootrom Exploit
- iBoot Exploit

What means the flag "-oX" in a Nmap scan?

- Output the results in XML format to a file.
- Run a Xmas scan.
- Run an express scan.
- Output the results in truncated format to the screen.

Identify the standard by the description:
A regulation contains a set of guidelines that everyone who processes any electronic data in medicine should adhere to. It includes information on medical practices, ensuring that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to secure patient data.

- ISO/IEC 27002
- FISMA
- HIPAA
- COBIT

Session splicing is an IDS evasion technique that exploits how some IDSs do not reconstruct sessions before performing pattern matching on the data. The idea behind session splicing is to split data between several packets, ensuring that no single packet matches any patterns within an IDS signature. Which tool can be used to perform session splicing attacks?

- Burp
- Whisker
- tcpsplice
- Hydra

You makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions. What type of attack are you trying to perform?

- Chosen-plaintext attack
- Ciphertext-only attack
- Known-plaintext attack
- Adaptive chosen-plaintext attack

Rajesh, the system administrator analyzed the IDS logs and noticed that when accessing the external router from the administrator's computer to update the router configuration, IDS registered alerts. What type of an alert is this?

- False negative
- False positive
- True positve
- True negative

Alex, the penetration tester, performs a server scan. To do this, he uses the method where the TCP Header is split into many packets so that it becomes difficult to determine what packages are used for. Determine the scanning technique that Alex uses?

- IP Fragmentation Scan
- Inverse TCP flag scanning
- TCP Scanning
- ACK flag scanning

What identifies malware by collecting data from protected computers while analyzing it on the provider’s infrastructure instead of locally?

- Cloud-based detection
- Real-time protection
- Heuristics-based detection
- Behavioural-based detection

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
- IPID scanning
- SYN/FIN scanning using IP fragments.
- ACK scanning

Which of the following UDP ports is usually used by Network Time Protocol (NTP)?

- 19
- 123
- 177
- 161

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

- Cannot deal with encrypted network traffic.
- Can identify unknown attacks.
- Produces less false positives.
- Requires vendor updates for a new threat.

Rajesh, a network administrator found several unknown files in the root directory of his FTP server. He was very interested in a binary file named "mfs". Rajesh decided to check the FTP server logs and found that the anonymous user account logged in to the server, uploaded the files and ran the script using a function provided by the FTP server's software. Also, he found that "mfs" file is running as a process and it listening to a network port. What kind of vulnerability must exist to make this attack possible?

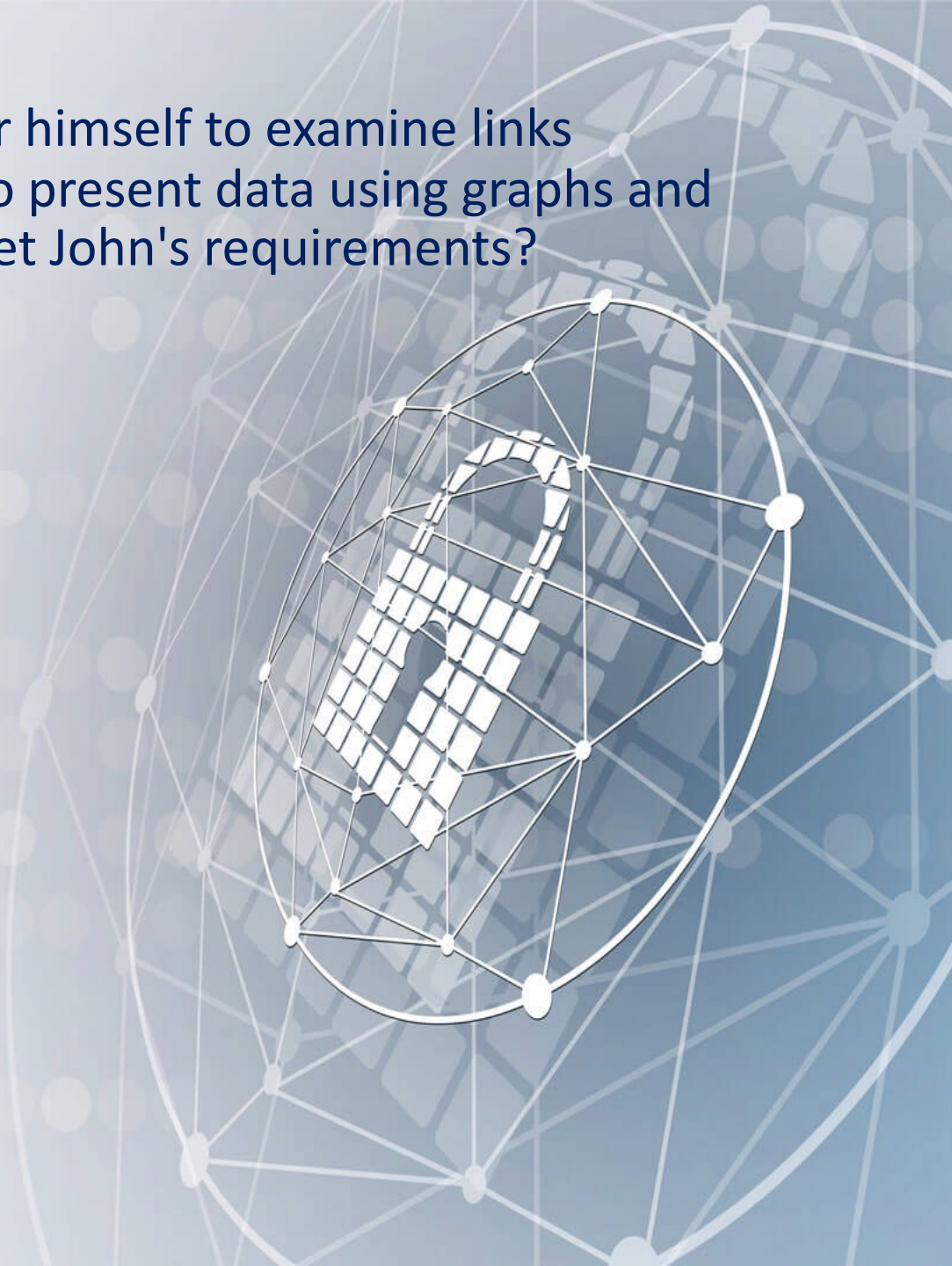
- Brute force login.
- Privilege escalation.
- Directory traversal.
- File system permissions.

Which type of viruses tries to hide from antivirus programs by actively changing and corrupting the chosen service call interruptions when they are being run?

- Cavity virus
- Polymorphic virus
- Tunneling virus
- Stealth/Tunneling virus

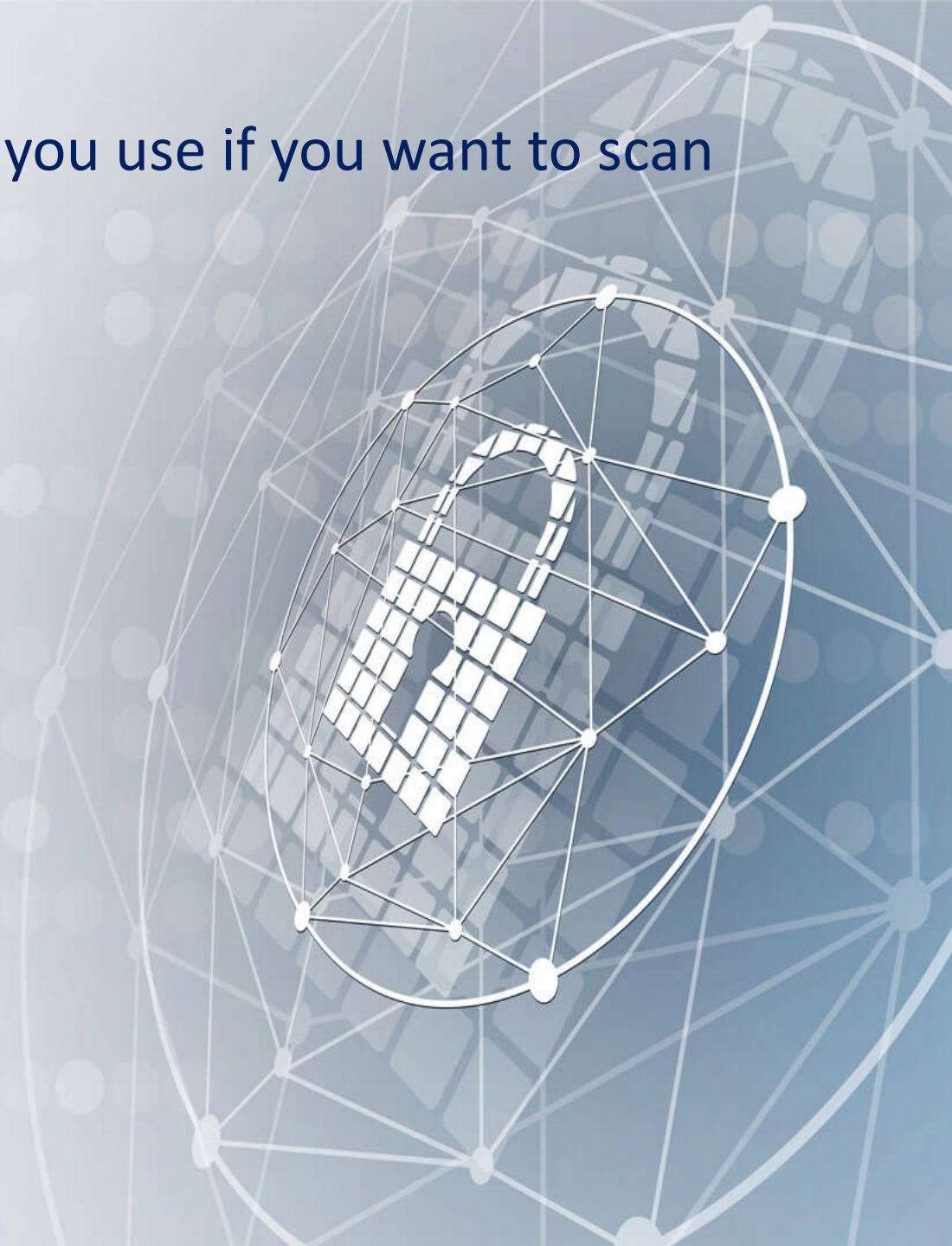
Josh, a security analyst, wants to choose a tool for himself to examine links between data. One of the main requirements is to present data using graphs and link analysis. Which of the following tools will meet John's requirements?

- Analyst’s Notebook.
- Metasploit.
- Maltego.
- Palantir.



Which of the following Nmap options will you use if you want to scan fewer ports than the default?

- -F
- -sP
- -T
- -p



With which of the following SQL injection attacks can an attacker deface a web page, modify or add data stored in a database and compromised data integrity?

- Information Disclosure.
- Loss of data availability.
- Unauthorized access to an application.
- Compromised Data Integrity.

Which of the following methods is best suited to protect confidential information on your laptop which can be stolen while travelling?

- Password protected files.
- Full disk encryption.
- Hidden folders.
- BIOS password.

After several unsuccessful attempts to extract cryptography keys using software methods, Mark is thinking about trying another code-breaking methodology. Which of the following will best suit Mark based on his unsuccessful attempts?

- One-Time pad.
- Frequency Analysis.
- Brute-Force.
- Trickery and Deceit.

Viktor, the white hat hacker, conducts a security audit. He gains control over a user account and tries to access another account's sensitive information and files. How can he do this?

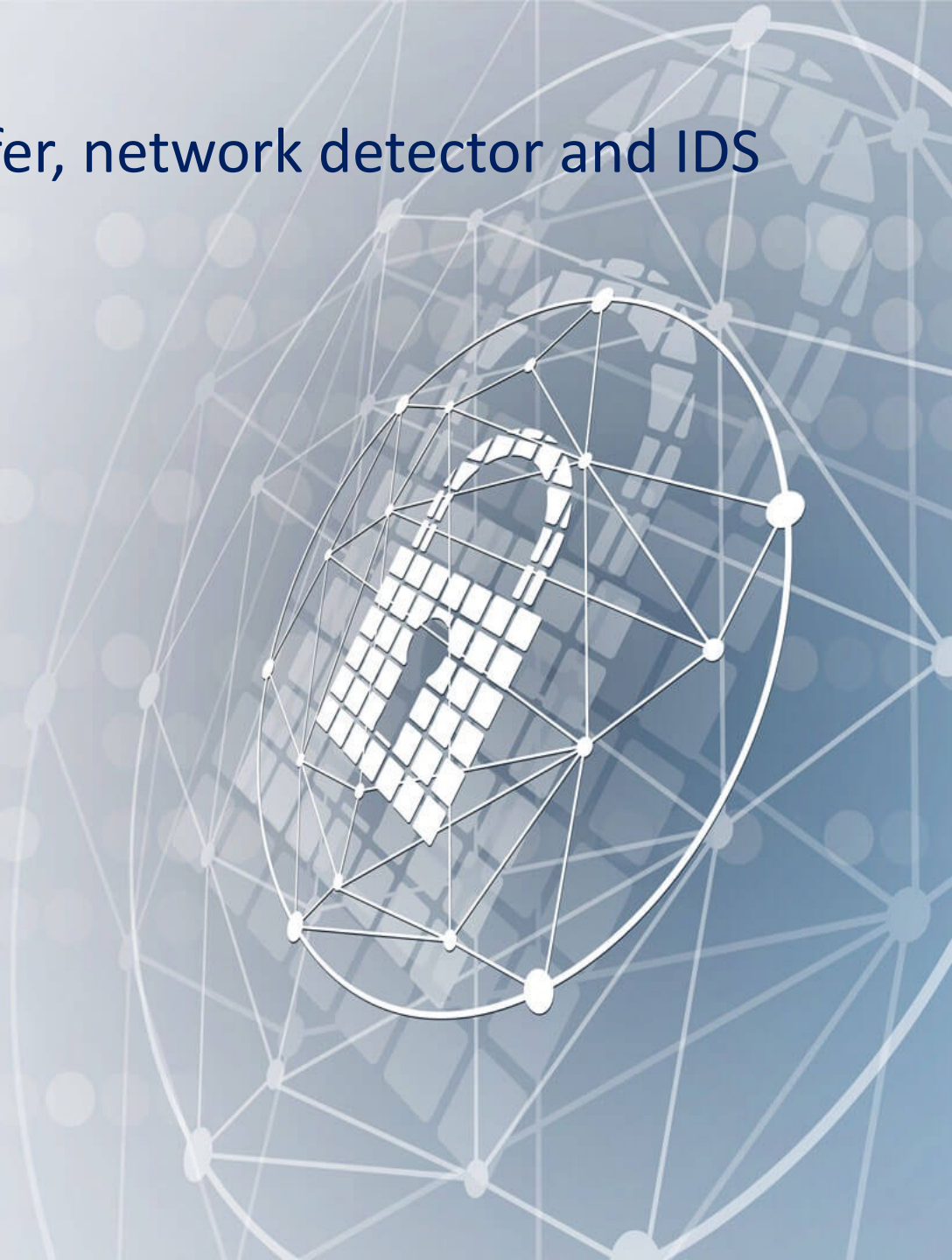
- Shoulder-Surfing
- Privilege Escalation.
- Port Scanning
- Fingerprinting.

The evil hacker Ivan has installed a remote access Trojan on a host. He wants to be sure that when a victim attempts to go to "www.site.com" that the user is directed to a phishing site. Which file should Ivan change in this case?

- Sudoers
- Networks
- Boot.ini
- Hosts

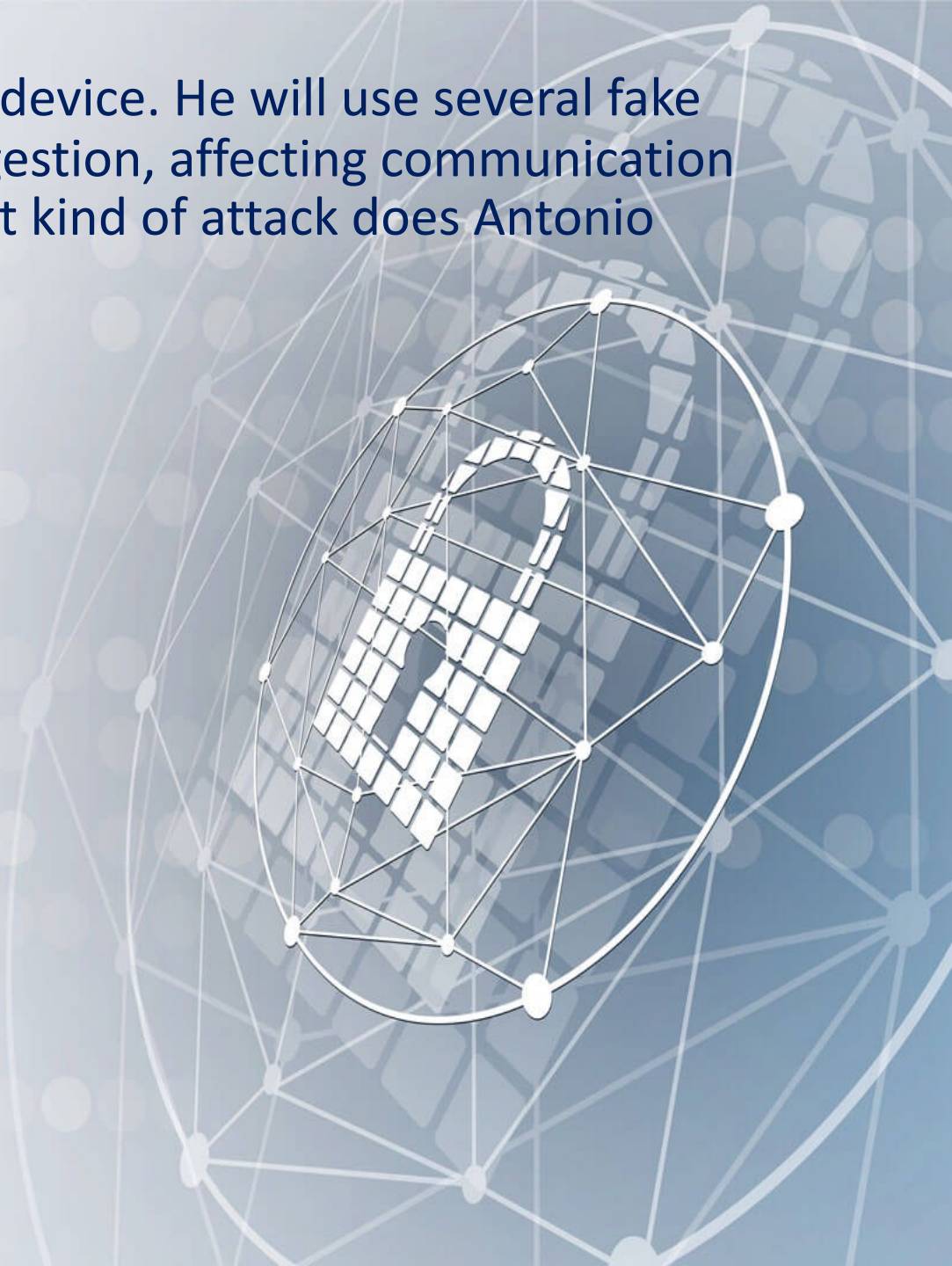
Which of the following tools is packet sniffer, network detector and IDS for 802.11(a, b, g, n) wireless LANs?

- Nessus
- Nmap
- Kismet
- Abel



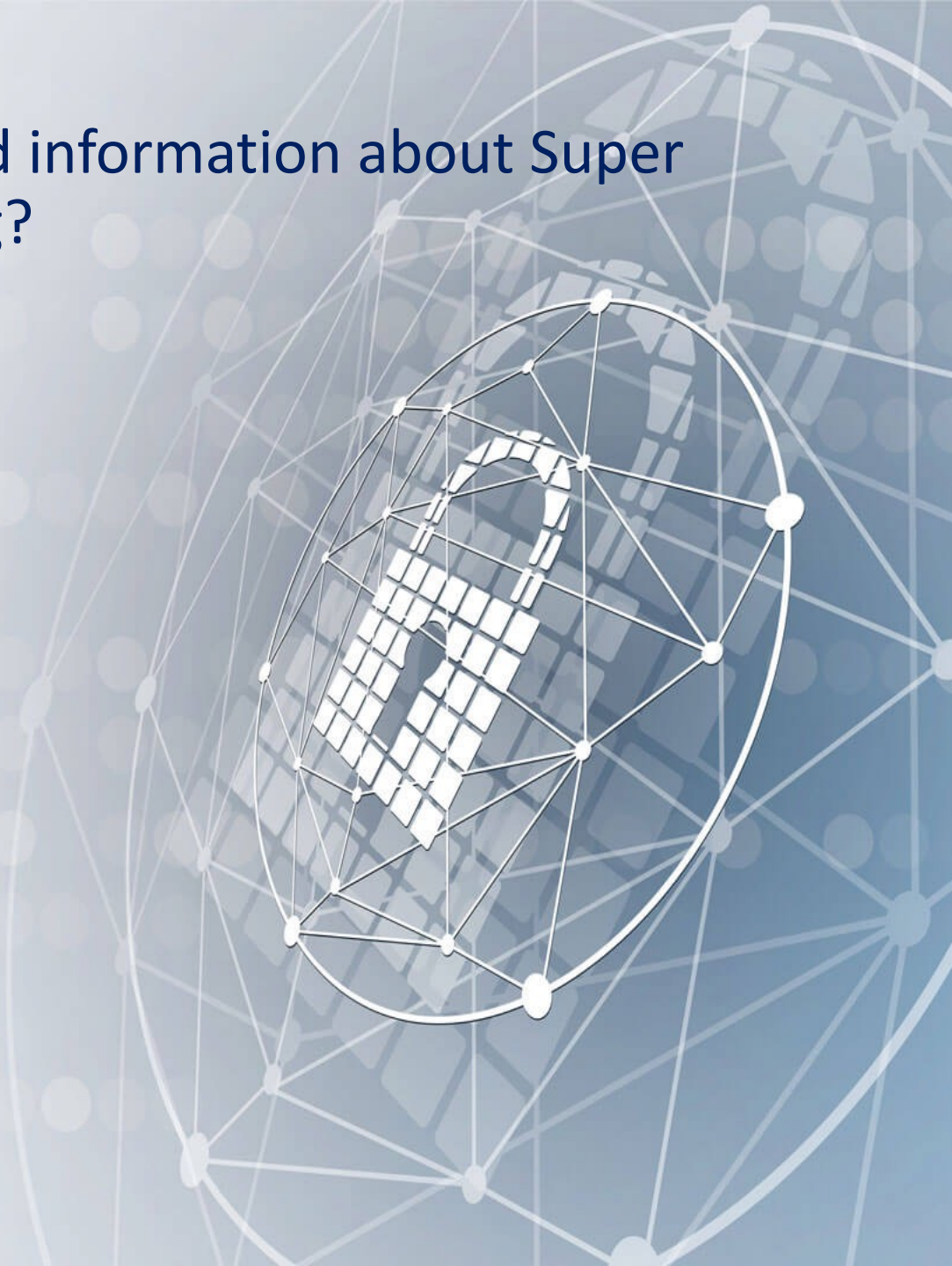
The evil hacker Antonio is trying to attack the IoT device. He will use several fake identities to create a strong illusion of traffic congestion, affecting communication between neighbouring nodes and networks. What kind of attack does Antonio perform?

- Sybil Attack
- Forged Malicious Device
- Side-Channel Attack
- Exploit Kits



Maria is surfing the internet and try to find information about Super Security LLC. Which process is Maria doing?

- System Hacking
- Enumeration
- Scanning
- Footprinting



Determine what of the list below is the type of honeypots that simulates the real production network of the target organization?

- High-interaction Honeypots.
- Pure Honeypots.
- Low-interaction Honeypots.
- Research Honeypots.

Michael, a technical specialist, discovered that the laptop of one of the employees connecting to a wireless point couldn't access the Internet, but at the same time, it can transfer files locally. He checked the IP address and the default gateway. They are both on 192.168.1.0/24. Which of the following caused the problem?

- The laptop is using an invalid IP address.
- The gateway is not routing to a public IP address.
- The laptop isn’t using a private IP address.
- The laptop and the gateway are not on the same network.

The Web development team is holding an urgent meeting, as they have received information from testers about a new vulnerability in their Web software. They make an urgent decision to reduce the likelihood of using the vulnerability. The team beside to modify the software requirements to disallow users from entering HTML as input into their Web application. Determine the type of vulnerability that the test team found?

- Website defacement vulnerability.
- Cross-site scripting vulnerability.
- Cross-site Reguest Forgery vulnerability.
- SQL injection Vulnerability.

Identify Bluetooth attck techniques that is used in to send messages to users without the recipient's consent, for example for guerrilla marketing campaigns?

- Bluesnarfing
- Bluesmacking
- Bluebugging
- Bluejacking

Which of the following is a network software suite designed for 802.11 WEP and WPA-PSK keys cracking that can recover keys once enough data packets have been captured?

- Aircrack-ng
- Airguard
- Wificracker
- WLAN-crack

Which one of the following Google search operators allows restricting results to those from a specific website?

- [cache:]
- [site:]
- [link:]
- [inurl:]

Define Metasploit module used to perform arbitrary, one-off actions such as port scanning, denial of service, SQL injection and fuzzing?

- Exploit Module.
- NOPS Module.
- Payload Module.
- Auxiliary Module.

Which layer 3 protocol allows for end-to-end encryption of the connection?

- FTPS
- SFTP
- IPsec
- SSL

alert tcp any any -> 10.199.10.3 21 (msg: "FTP on the network!";)
Which system usually uses such a configuration setting?

- Firewall IPTable
- Router IPTable
- FTP Server rule
- IDS

John, a pentester, received an order to conduct an internal audit in the company. One of its tasks is to search for open ports on servers. Which of the following methods is the best solution for this task?

- Scan servers with Nmap.
- Telnet to every port on each server.
- Manual scan on each server.
- Scan servers with MBSA.

Let's assume that you decided to use PKI to protect the email you will send. At what layer of the OSI model will this message be encrypted and decrypted?

- Presentation layer.
- Application layer.
- Transport layer.
- Session layer.

Which of the following is an encryption technique where data is encrypted by a sequence of photons that have a spinning trait while travelling from one end to another?

- Homomorphic.
- Elliptic Curve Cryptography.
- Hardware-Based.
- Quantum Cryptography.

Which of the following program attack both the boot sector and executable files?

- Macro virus
- Stealth virus
- Polymorphic Virus
- Multipartite Virus

Which of the following command will help you launch the Computer Management Console from "Run" windows as a local administrator Windows 7?

- compmgmt.msc
- services.msc
- gpedit.msc
- ncpa.cpl

Which of the options presented below is not a Bluetooth attack?

- Bluedriving
- Bluesmacking
- Bluejacking
- Bluesnarfing

Which of the following is a logical collection of Internet-connected devices such as computers, smartphones or Internet of things (IoT) devices whose security has been breached and control ceded to a third party?

- Spear Phishing
- Botnet
- Rootkit
- Spambot

John performs black-box testing. It tries to pass IRC traffic over port 80/TCP from a compromised web-enabled host during the test. Traffic is blocked, but outbound HTTP traffic does not meet any obstacles. What type of firewall checks outbound traffic?

- Packet Filtering
- Stateful
- Application
- Circuit

Which of the following will allow you to prevent unauthorized network access to local area networks and other information assets by wireless devices?

- AISS
- NIDS
- WIPS
- HIDS

Alex, a cybersecurity specialist, received a task from the head to scan open ports. One of the main conditions was to use the most reliable type of TCP scanning. Which of the following types of scanning should Alex use?

- Half-open Scan.
- Xmas Scan.
- TCP Connect/Full Open Scan.
- NULL Scan.

Philip, a cybersecurity specialist, needs a tool that can function as a network sniffer, record network activity, prevent and detect network intrusion. Which of the following tools is suitable for Philip?

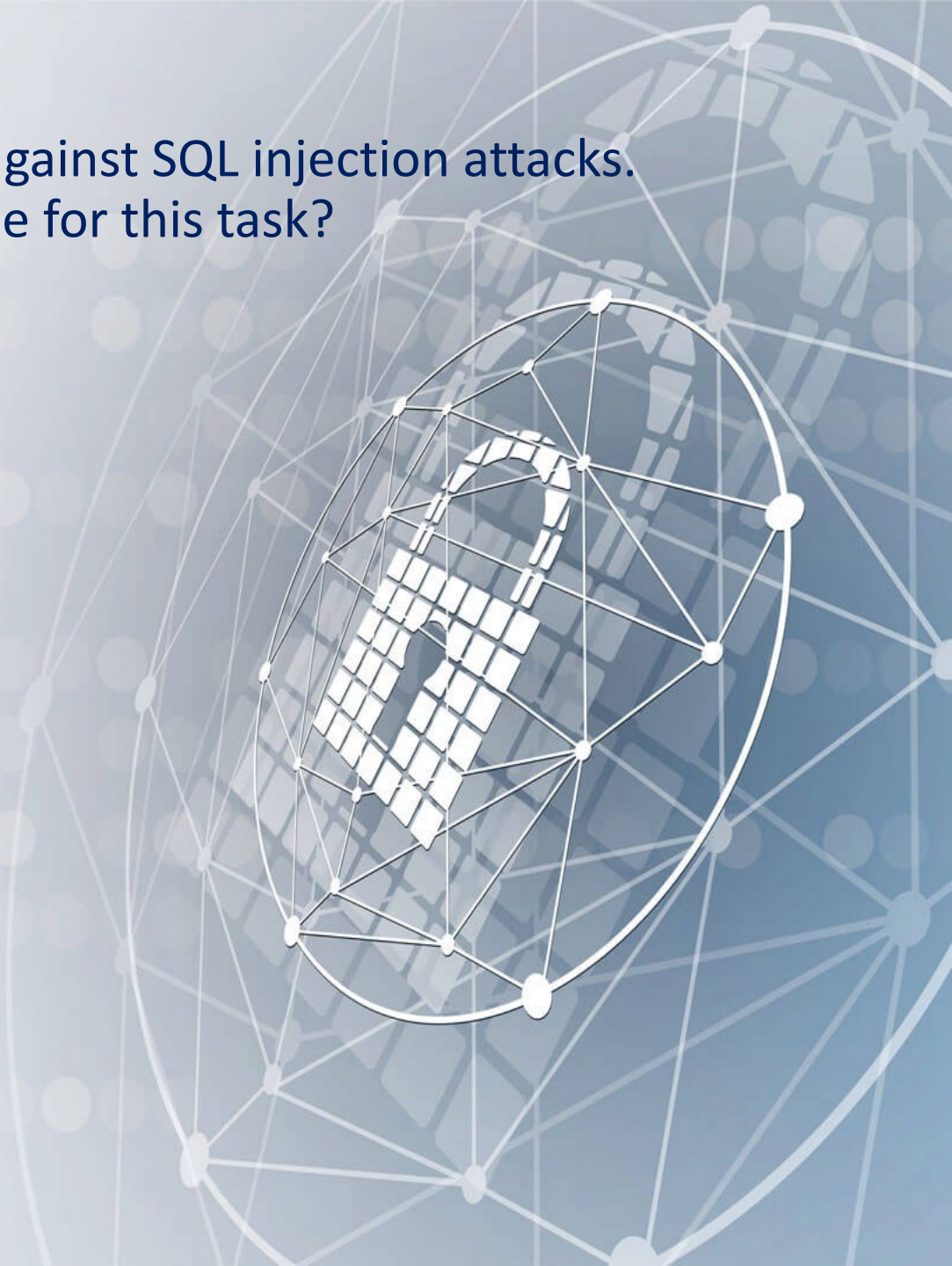
- Nmap
- Snort
- Nessus
- Cain & Abel

Alex, a cyber security specialist, should conduct a pentest inside the network, while he received absolutely no information about the attacked network. What type of testing will Alex conduct?

- Internal, White-box.
- Internal, Grey-box.
- Internal, Black-box.
- External, Black-box.

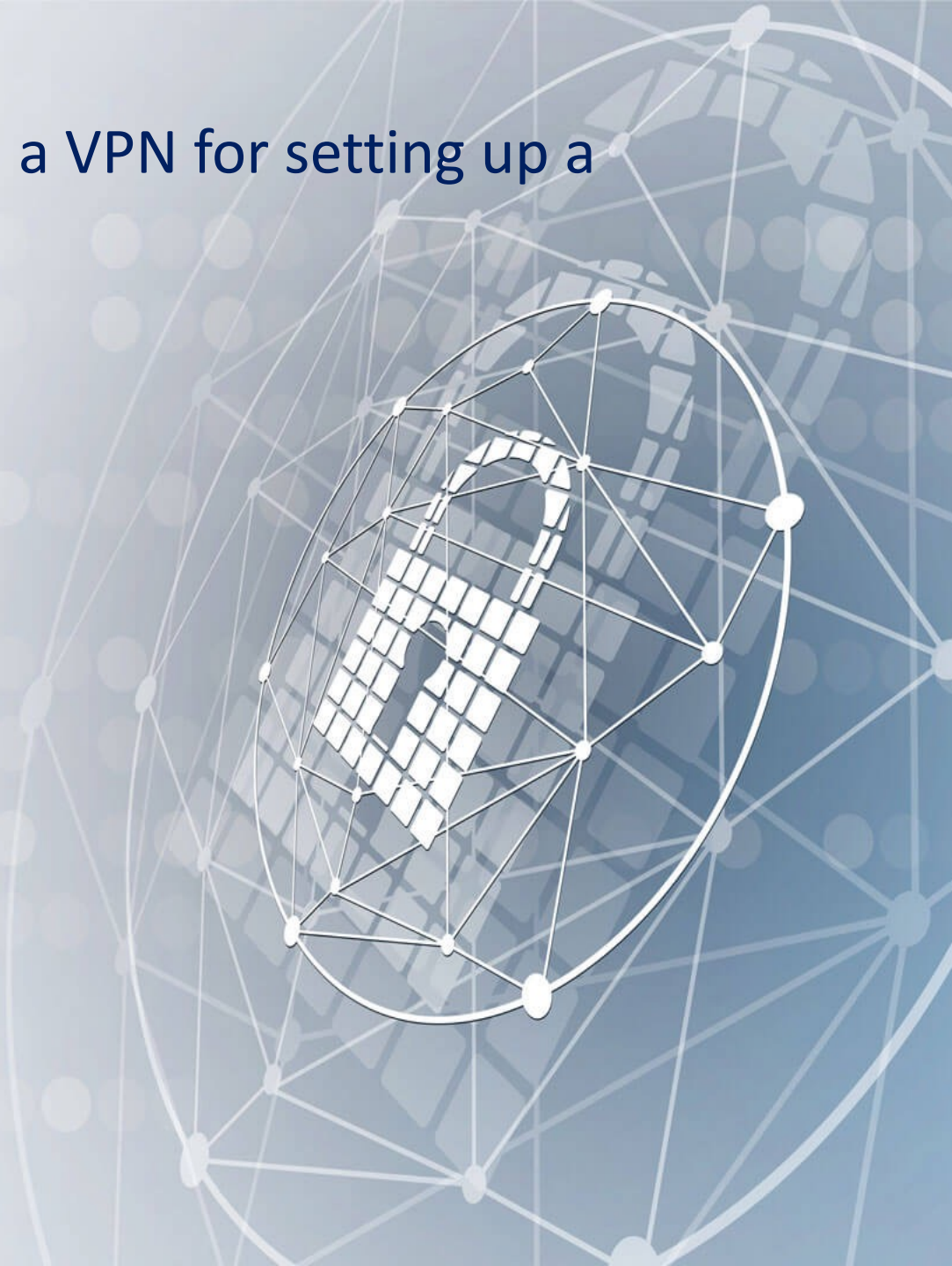
John needs to choose a firewall that can protect against SQL injection attacks. Which of the following types of firewalls is suitable for this task?

- Web application firewall.
- Hardware firewall.
- Stateful firewall.
- Packet firewall.



Which of the following protocols is used in a VPN for setting up a secure channel between two devices?

- IPSEC
- PEM
- SET
- PPP



What is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication, authenticated denial of existence and data integrity, but not availability or confidentiality?

- Zone transfer
- Resource records
- DNSSEC
- Resource transfer

Jack sent an email to Jenny with a business proposal. Jenny accepted it and fulfilled all her obligations. Jack suddenly refused his offer when everything was ready and said that he had never sent an email. Which of the following digital signature properties will help Jenny prove that Jack is lying?

- Integrity
- Non-Repudiation
- Confidentiality
- Authentication

Which of the following is the method of determining the movement of a data packet from an untrusted external host to a protected internal host through a firewall?

- MITM
- Firewalking
- Session hijacking
- Network sniffing

Which of the following incident handling process phases is responsible for defining rules, employees training, creating a back-up, and preparing software and hardware resources before an incident occurs?

- Identification
- Recovery
- Containment
- Preparation

Which of the following cipher is based on factoring the product of two large prime numbers?

- MD5
- SHA-1
- RC5
- RSA

Which of the following web application attack inject the special character elements "Carriage Return" and "Line Feed" into the user’s input to trick the web server, web application, or user into believing that the current object is terminated and a new object has been initiated?

- CRLF Injection.
- HTML Injection.
- Log Injection.
- Server-Side JS Injection.

Which of the following characteristics is not true about the Simple Object Access Protocol?

- Using Extensible Markup Language.
- Only compatible with the application protocol HTTP.
- Exchanges data between web services.
- Allows for any programming model.

What type of cryptography is used in IKE, SSL, and PGP?

- Digest
- Secret Key
- Public Key
- Hash

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

- Collision
- Sinkhole
- Evil Twin
- Signal Jamming

Which of the following type of hackers refers to an individual who works both offensively and defensively?

- Black Hat
- Gray Hat
- Suicide Hacker
- White Hat

An attacker tries to infect as many devices connected to the Internet with malware as possible to get the opportunity to use their computing power and functionality for automated attacks hidden from the owners of these devices. Which of the proposed approaches fits description of the attacker's actions?

- Creating a botnet
- Using Banking Trojans
- Mass distribution of Ransomware
- APT attack

Which of the following is correct?

- Sniffers operate on Layer 4 of the OSI model.
- Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
- Sniffers operate on Layer 2 of the OSI model.
- Sniffers operate on Layer 3 of the OSI model.

Black-hat hacker Ivan wants to determine the status of ports on a remote host. He wants to do this quickly but imperceptibly for IDS systems. For this, he uses a half-open scan that doesn't complete the TCP three-way handshake. What kind of scanning does Ivan use?

- XMAS scans
- TCP SYN (Stealth) Scan
- PSH Scan
- FIN scan

Which of the following components of IPsec provides confidentiality for the content of packets?

- IKE
- AH
- ISAKMP
- ESP

Alex, a cybersecurity science student, needs to fill in the information into a secured PDF-file job application received from a prospective employer. He can't enter the information because all the fields are blocked. He doesn't want to request a new document that allows the forms to be completed and 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 attack is the student attempting?

- Dictionary-attack
- Man-in-the-middle attack
- Brute-force attack
- Session hijacking

The ping utility is used to check the integrity and quality of connections in networks. In the process, it sends an ICMP Echo-Request and captures the incoming ICMP Echo-Reply, but quite often remote nodes block or ignore ICMP. Which of the options will solve this problem?

- Use broadcast ping
- Use hping
- Use arping
- Use traceroute

Which of the following Linux-based tools will help you change any user's password or activate disabled accounts if you have physical access to a Windows 2008 R2 and an Ubuntu 9.10 Linux LiveCD?

- CHNTPW
- SET
- John the Ripper
- Cain & Abel

Ivan, a black-hat hacker, performs a man-in-the-middle attack. To do this, it uses a rogue wireless AP and embeds a malicious applet in all HTTP connections. When the victims went to any web page, the applet ran. Which of the following tools could Ivan probably use to inject HTML code?

- Wireshark
- Aircrack-ng
- Ettercap
- tcpdump

The attacker managed to gain access to Shellshock, and now he can execute arbitrary commands and gain unauthorized access to many Internet-facing services. Which of the following operating system can't be affected by an attacker yet?

- Unix
- Windows
- OS X
- Linux

To protect the enterprise infrastructure from the constant attacks of the evil hacker Ivan, Viktor divided the network into two parts using the network segmentation approach.
· In the first one (local, without direct Internet access), he isolated business-critical resources.
· In the second (external, with Internet access), he placed public web servers to provide services to clients.
Subnets communicate with each other through a gateway protected by a firewall. What is the name of the external subnet?

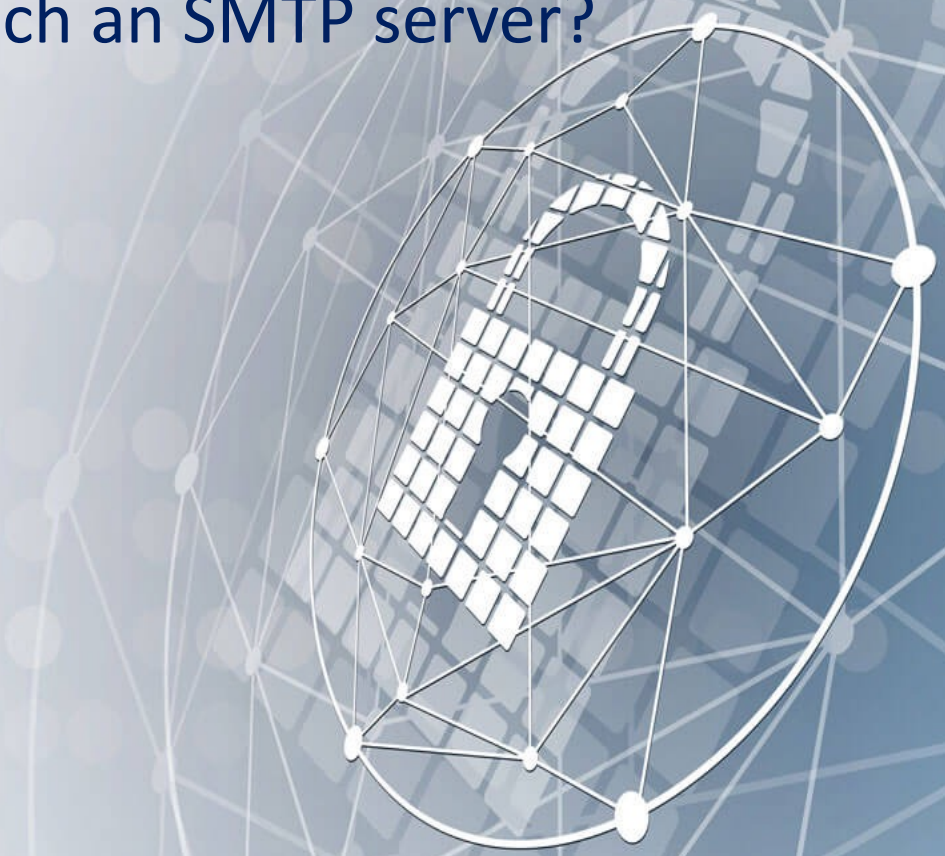
- Demilitarized Zone
- Bastion host
- Network access control
- WAF

You want to surf safely and anonymously on the Internet. Which of the following options will be best for you?

- Use VPN
- Use SSL sltes
- Use Tor network with multi-node
- Use public WIFI

Lisandro is engaged in sending spam. To avoid blocking, he connects to incorrectly configured SMTP servers that allow e-mail relay without authentication (which allows Lisandro to fake information about the sender's identity). What is the name of such an SMTP server?

- Weak SMTP
- Open mail relay
- Public SMTP server
- Message transfer agent

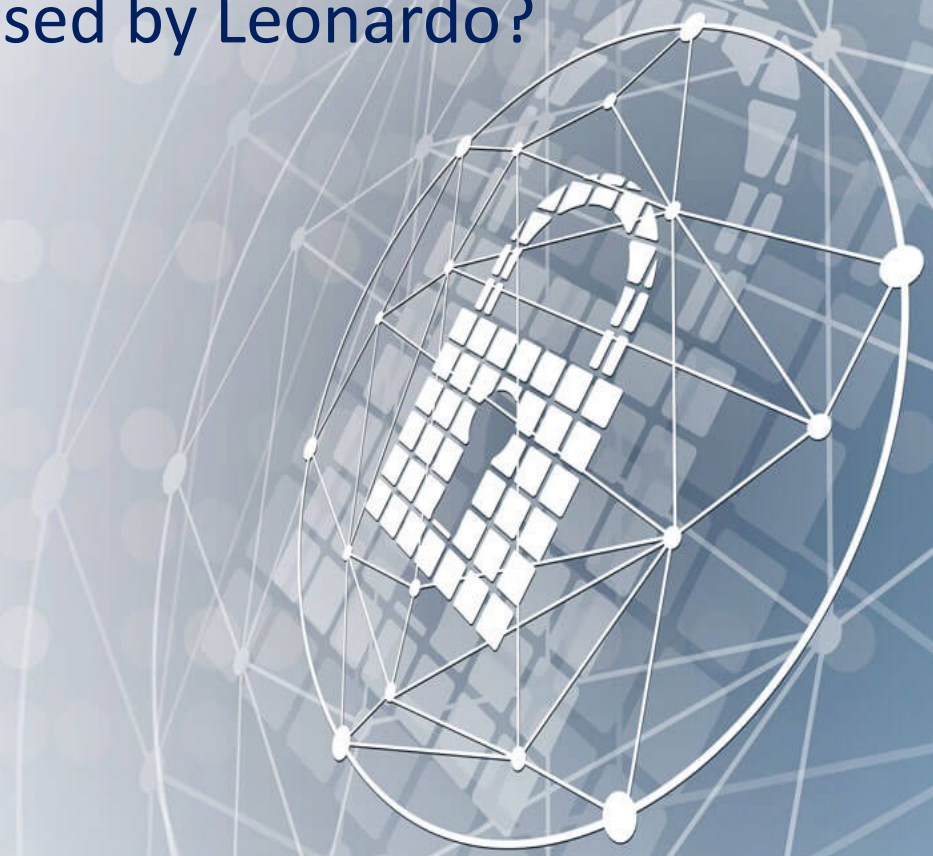


What is the first and most important phase that is the starting point for penetration testing in the work of an ethical hacker?

- Reconnaissance
- Maintaining Access
- Scanning
- Gaining Access

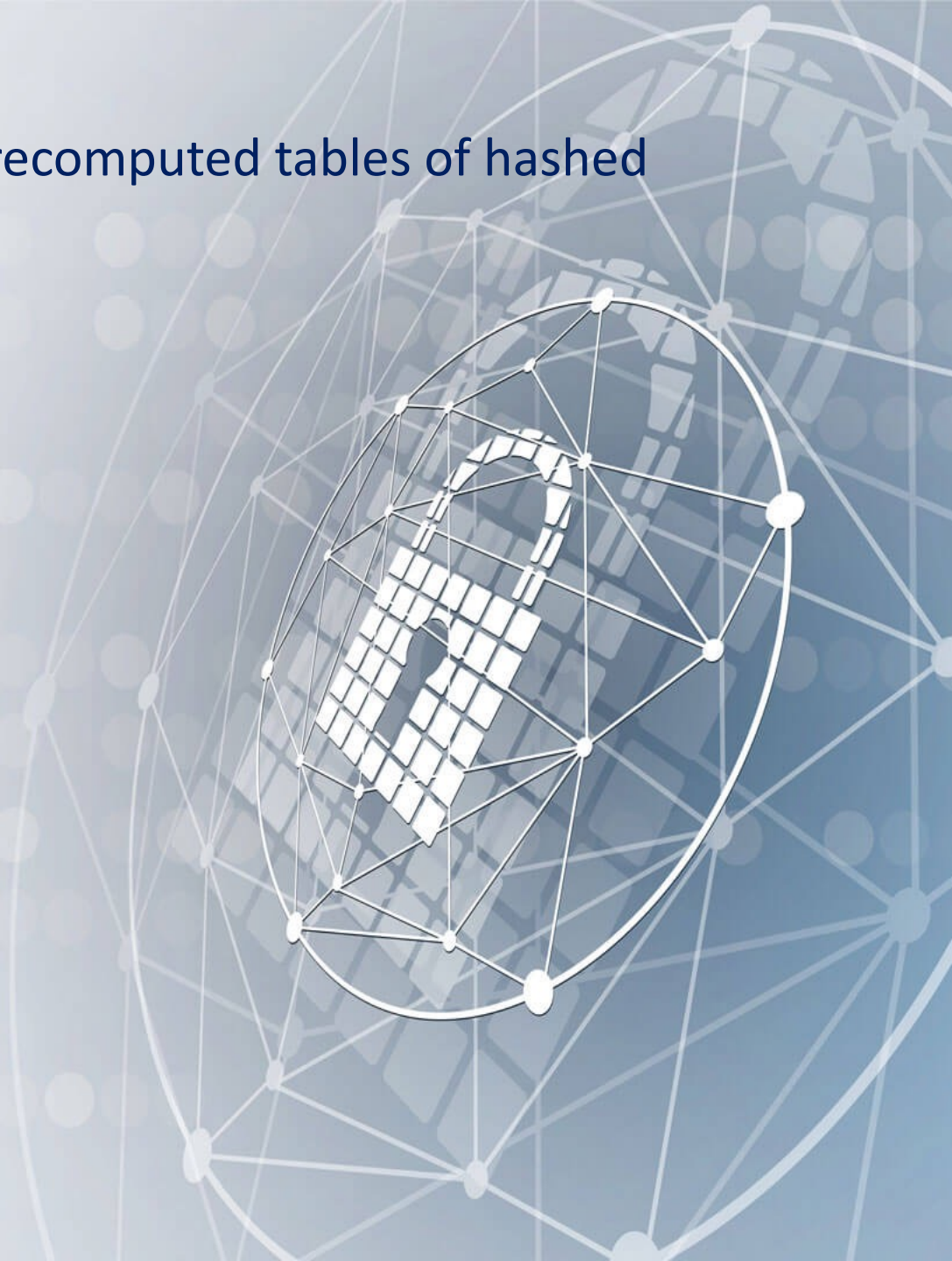
Leonardo, an employee of a cybersecurity firm, conducts an audit for a third-party company. First of all, he plans to run a scanning that looks for common misconfigurations and outdated software versions. Which of the following tools is most likely to be used by Leonardo?

- Armitage
- Nmap
- Nikto
- Metasploit



Which of the following is an attack where used precomputed tables of hashed passwords?

- Rainbow Table Attack
- Brute Force Attack
- Dictionary Attack
- Hybrid Attack



Alex works as a network administrator at ClassicUniversity. There are many Ethernet ports are available for professors and authorized visitors (but not for students) on the university campus. However, Alex realized that some students connect their notebooks to the wired network to have Internet access. He identified this when the IDS alerted for malware activities in the network. What should Alex do to avoid this problem?

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

IPsec is a suite of protocols developed to ensure the integrity, confidentiality, and authentication of data communications over an IP network. Which protocol is NOT included in the IPsec suite?

- Media Access Control (MAC)
- Security Association (SA)
- Encapsulating Security Protocol (ESP)
- Authentication Header (AH)

Which of the following is the type of message that sends the client to the server to begin a 3-way handshake while establishing a TCP connection?

- ACK
- RST
- SYN-ACK
- SYN

The SOC analyst of the company wants to track the transfer of files over the unencrypted FTP protocol, which filter for the Wireshark sniffer should he use?

- tcp.port == 80
- tcp.port == 443
- tcp.port == 23
- tcp.port == 21

Identify the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- biometrics
- single sign-on
- PKI
- SOA

Identify a security policy that defines using of a VPN for gaining access to an internal corporate network?

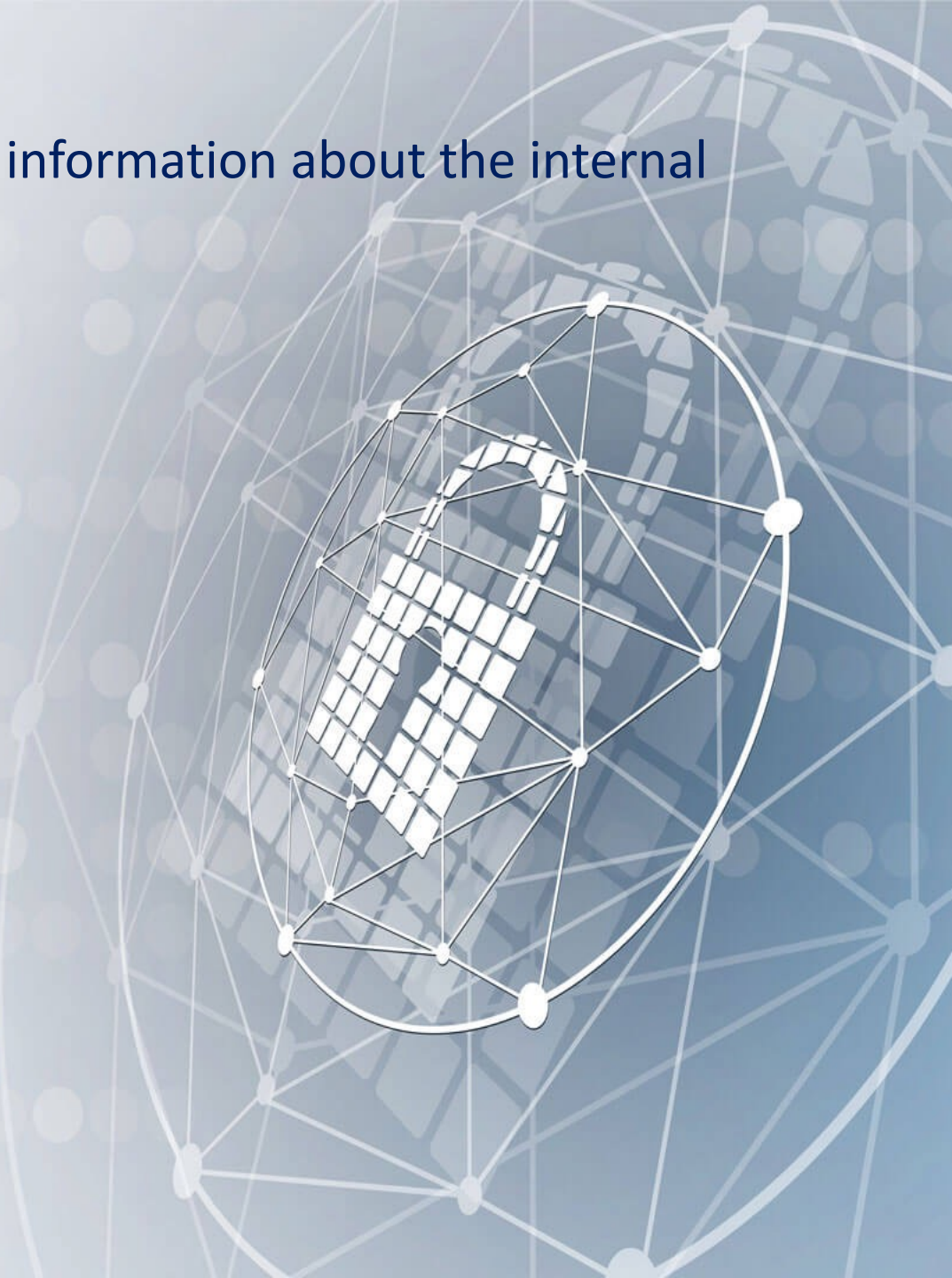
- Information protection policy
- Access control policy
- Network security policy
- Remote access policy

The evil hacker Ivan wants to attack the popular air ticket sales service. After careful study, he discovered that the web application is vulnerable to introduced malicious JavaScript code through the application form. This code does not cause any harm to the server itself, but when executed on the client's computer, it can steal his personal data. What kind of attack is Ivan preparing to use?

- SQL injection
- LDAP Injection
- CSRF
- XSS

In what type of testing does the tester have some information about the internal work of the application?

- Announced
- Black-box
- White-box
- Grey-box



Monitoring your company's assets is one of the most important jobs you can perform. What warnings should you try to reduce when configuring security tools, such as security information and event management (SIEM) solutions or intrusion detection systems (IDS)?

- False Positives and False Negatives
- True Positives and True Negatives
- Only True Negatives
- Only False Positives

What is the name of a popular tool (or rather, an entire integrated platform written in Java) based on a proxy used to assess the security of web applications and conduct practical testing using a variety of built-in tools?

- Burp Suite
- Wireshark
- Nmap
- CxSAST

Which of the following parameters is Nmap helps evade IDS or firewalls?

- -T
- -A
- -r
- -R

Passwords are rarely stored in plain text, most often, one-way conversion (hashing) is performed to protect them from unauthorized access. However, there are some attacks and tools to crack the hash. Look at the following tools and select the one that can NOT be used for this.

- John the Ripper
- Ophcrack
- Netcat
- Hashcat

You have been instructed to organize the possibility of working remotely for employees. Their remote connections could be exposed to session hijacking during the work, and you want to prevent this possibility. You decide to use the technology that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. Which of the following technologies will you use?

- VPN
- Split tunneling
- DMZ
- Bastion host

Lisandro was hired to steal critical business documents of a competitor company. Using a vulnerability in over-the-air programming (OTA programming) on Android smartphones, he sends messages to company employees on behalf of the network operator, asking them to enter a PIN code and accept new updates for the phone. After the employee enters the PIN code, Lisandro gets the opportunity to intercept all Internet traffic from the phone. What type of attack did Lisandro use?

- Tap ‘n ghost attack.
- Bypass SSL pinning.
- Social engineering.
- Advanced SMS phishing.

Good luck

Linkedin: https://www.linkedin.com/in/moshe-ovadia

C|EH® v12
Certified Ethical Hacker