

Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)

<https://www.2passeasy.com/dumps/312-50v12/>



NEW QUESTION 1

Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company.

After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on Jane?

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

Answer: D

NEW QUESTION 2

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 start 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 3

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 4

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. HIPAA/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 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 phone 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 5

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

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

Answer: B

Explanation:

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key

https://en.wikipedia.org/wiki/Pretty_Good_Privacy Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, emails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.

https://en.wikipedia.org/wiki/Public-key_cryptography

Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with anyone who will be securely communicating with the key owner. However, the owner's secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

NEW QUESTION 6

Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unknornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

- A. 64
- B. 128
- C. 255
- D. 138

Answer: B

Explanation:

Windows TTL 128, Linux TTL 64, OpenBSD 255 ... <https://subinsb.com/default-device-ttl-values/> Time to Live (TTL) represents to number of 'hops' a packet can take before it is considered invalid. For Windows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

NEW QUESTION 7

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 Trust LMv2 uses the NT MD4 primarily based a method operate (NTOWF).

NEW QUESTION 8

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>

Answer: C

Explanation:

<03>

Windows Messenger administration

Courier 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 naturally. Along these lines, numerous clients got such messages.

Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

NEW QUESTION 9

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 10

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 10

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 connectionoriented protocol, it needs acknowledgement to line up end-to-end communications. only a 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 14

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 encrypting about the firewall.
- C. It is a stateful firewall
- D. It Is a non-stateful firewall.

Answer: B

NEW QUESTION 15

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 19

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 23

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

- A. OS Detection
- B. Firewall detection
- C. TCP/UDP Port scanning
- D. Checking if the remote host is alive

Answer: D

Explanation:

Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

* 1. Locating nodes: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.

* 2. Performing service and OS discovery on them: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services and the operating system on the target systems.

* 3. Testing those services and OS for known vulnerabilities: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

NEW QUESTION 25

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 29

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 31

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 35

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

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

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 40

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 42

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 45

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

- A. Error-based injection
- B. Boolean-based blind SQL injection
- C. Blind SQL injection
- D. Union SQL injection

Answer: D

NEW QUESTION 47

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

- A. Application
- B. Transport
- C. Session
- D. Presentation

Answer: D

Explanation:

https://en.wikipedia.org/wiki/Presentation_layer

In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as the data translator for the network. It is sometimes called the syntax layer. The presentation layer is responsible for the formatting and delivery of information to the application layer for further processing or display.

Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages. Decryption is also handled at the presentation layer. For example, when logging on to bank account sites the presentation layer will decrypt the data as it is received.

NEW QUESTION 48

What does the -oX flag do in an Nmap scan?

- A. Perform an eXpress scan
- B. Output the results in truncated format to the screen
- C. Output the results in XML format to a file
- D. Perform an Xmas scan

Answer: C

Explanation:

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

-oX <filespec> - Requests that XML output be directed to the given filename.

NEW QUESTION 50

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- A. nessus
- B. tcpdump
- C. ethereal
- D. jack the ripper

Answer: B

Explanation:

Tcpdump is a data-network packet analyzer computer program that runs under a command-line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

<https://www.wireshark.org/>

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NOTE: Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

NEW QUESTION 54

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

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

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

Answer: A

Explanation:

DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, some of the essential cryptographic protocols for net security. These protocols allow everyone on the net to browse the net, use email, look on-line, and send instant messages while not third-parties being able to browse the communication.

DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March 2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack.

fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.

What will the attackers gain?Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

Who is vulnerable?Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:

Operators of vulnerable servers got to take action. there's nothing practical that browsers or end-users will do on their own to protect against this attack.

Is my site vulnerable?Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.

It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.

Its private key is used on any other serverthat allows SSLv2 connections, even for another protocol.

Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.

How do I protect my server?To protect against DROWN, server operators need to ensure that their private keys software used anyplace with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.

Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:

OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users

ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s. Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.

Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more moderen version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere

Other affected software and in operation systems:

A server is vulnerable to DROWN if SSLv2

Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat

Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators ar

ready to take action to guard against the attack.

NEW QUESTION 59

An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages. What is the attack performed in the above scenario?

- A. Timing-based attack

- B. Side-channel attack
- C. Downgrade security attack
- D. Cache-based attack

Answer: B

NEW QUESTION 62

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 66

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-50v12 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-50v12 Product From:

<https://www.2passeasy.com/dumps/312-50v12/>

Money Back Guarantee

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