Guaranteed Accomplishment with Newest Dec-2023 FREE ECCouncil 312-50v12 [Q279-Q296

Guaranteed Accomplishment with Newest Dec-2023 FREE ECCouncil 312-50v12
Use Valid New Free 312-50v12 Exam Dumps & Answers

NEW QUESTION 279

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient’s consent, similar to email spamming?
* Bluesmacking
* BlueSniffing
* Bluejacking
* Bluesnarfing

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

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluejacking is usually harmless, but because bluejacked people generally don’t know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it’s possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Bluejacking is also confused with Bluesnarfing, which is the way in which mobile phones are illegally hacked via Bluetooth.

NEW QUESTION 280

Which of the following is the primary objective of a rootkit?
* It opens a port to provide an unauthorized service
* It creates a buffer overflow
* It replaces legitimate programs
* It provides an undocumented opening in a program

NEW QUESTION 281

which of the following protocols can be used to secure an LDAP service against anonymous queries?
* SSO
* RADIUS
* WPA
* NTLM

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 282

Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128,192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

* TEA
* CAST-128
* RC5
* serpent

NEW QUESTION 283

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

* An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
* An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
* An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
* An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

NEW QUESTION 284

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

* Port 53
* Port 23
* Port 50
* Port 80

DNS uses Ports 53 which is almost always open on systems, firewalls, and clients to transmit DNS queries. instead of the more familiar Transmission Control Protocol (TCP) these queries use User Datagram Protocol (UDP) due to its low-latency, bandwidth and resource usage compared TCP-equivalent queries. UDP has no error or flow-control capabilities, nor does it have any integrity checking to make sure the info arrived intact. How is internet use (browsing, apps, chat etc) so reliable then? If the UDP DNS query fails (it’s a best-effort protocol after all) within the first instance, most systems will retry variety of times and only after multiple failures, potentially switch to TCP before trying again; TCP is additionally used if the DNS query exceeds the restrictions of the UDP datagram size – typically 512 bytes for DNS but can depend upon system settings. Figure 1 below illustrates the essential process of how DNS operates: the client sends a question string (for example, mail.google[.]com during this case) with a particular type – typically A for a number address. I’ve skipped the part whereby intermediate DNS systems may need to establish where ‘.com’ exists, before checking out where ‘google[.]com’ are often found, and so on.

Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it’s really no

surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an upgrade to the foremost current version of the telnet Daemon or OS upgrade. As is usually the case, this upgrade has not been performed on variety of devices. this might flow from to the very fact that a lot of systems administrators and users don’t fully understand the risks involved using telnet. Unfortunately, the sole solution for a few of telnets vulnerabilities is to completely discontinue its use. the well-liked method of mitigating all of telnets vulnerabilities is replacing it with alternate protocols like ssh. Ssh is capable of providing many of an equivalent functions as telnet and a number of other additional services typical handled by other protocols like FTP and Xwindows. Ssh does still have several drawbacks to beat before it can completely replace telnet. it’s typically only supported on newer equipment. It requires processor and memory resources to perform the info encryption and decryption. It also requires greater bandwidth than telnet thanks to the encryption of the info . This paper was written to assist clarify how dangerous the utilization of telnet are often and to supply solutions to alleviate the main known threats so as to enhance the general security of the web Once a reputation is resolved to an IP caching also helps: the resolved name-to-IP is usually cached on the local system (and possibly on intermediate DNS servers) for a period of your time . Subsequent queries for an equivalent name from an equivalent client then don’t leave the local system until said cache expires. Of course, once the IP address of the remote service is understood , applications can use that information to enable other TCP-based protocols, like HTTP, to try to to their actual work, for instance ensuring internet cat GIFs are often reliably shared together with your colleagues. So, beat all, a couple of dozen extra UDP DNS queries from an organization’s network would be fairly inconspicuous and will leave a malicious payload to beacon bent an adversary; commands could even be received to the requesting application for processing with little difficulty.

NEW QUESTION 285

what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?
* httpd.conf
* administration.config
* idq.dll
* php.ini

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 286

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

https://www.darknet.org.uk/2017/07/bluto-dns-recon-zone-transfer-brute-forcer/

“Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records.” CEH Module 02 Page 138

NEW QUESTION 287

An attacker scans a host with the below command. Which three flags are set?

nmap -sX host.domain.com
* This is SYN scan. SYN flag is set.
* This is Xmas scan. URG, PUSH and FIN are set.
* This is ACK scan. ACK flag is set.
* This is Xmas scan. SYN and ACK flags are set.

NEW QUESTION 288

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company’s application whitelisting?
* Phishing malware
* Zero-day malware
* File-less malware
* Logic bomb malware
https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

NEW QUESTION 289

Which of the following statements is TRUE?
* Packet Sniffers operate on the Layer 1 of the OSI model.
* Packet Sniffers operate on Layer 2 of the OSI model.
* Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
* Packet Sniffers operate on Layer 3 of the OSI model.

NEW QUESTION 290

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?
* Reconnaissance
* Maintaining access
* Scanning
* Gaining access
This phase having the hacker uses different techniques and tools to realize maximum data from the system. they’re – * Password cracking – Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered. * Password attacks – Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

NEW QUESTION 291

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?
* -T5
* -O

* -T0
* -A

NEW QUESTION 292

You have successfully logged on a Linux system. You want to now cover your trade Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:
* user.log
* auth.fesg
* wtmp
* btmp

NEW QUESTION 293

Which among the following is the best example of the third step (delivery) in the cyber kill chain?
* An intruder sends a malicious attachment via email to a target.
* An intruder creates malware to be used as a malicious attachment to an email.
* An intruder’s malware is triggered when a target opens a malicious email attachment.
* An intruder’s malware is installed on a target’s machine.

NEW QUESTION 294

Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website. www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as ”or ‘1’=’1″ In any bask injection statement such as “or 1=1.” Identify the evasion technique used by Daniel in the above scenario.
* Null byte
* IP fragmentation
* Char encoding
* Variation

One may append the comment “-” operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the – operator would be considered as comment and not dead.

To launch such an attack, the value passed for name could be ‘OR ‘1’=’1′ ; – Statement = “SELECT * FROM ‘CustomerDB’ WHERE ‘name’ = ‘ “+ userName + ” ‘ AND ‘password’ = ‘ ” + passwd + ” ‘ ; ” Statement = “SELECT * FROM ‘CustomerDB’ WHERE ‘name’ = ‘ ‘ OR ‘1’=’1′;- + ” ‘ AND ‘password’ = ‘ ” + passwd + ” ‘ ; ” All the records from the customer database would be listed.

Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn’t strongly used in or isn’t checked for sort constraints.

This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.

Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as “‘ or ‘1’=’1′” in any basic injection statement such as “or 1=1” or with other accepted SQL comments.

Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as “‘ or ‘1’=’1′” in any basic injection statement such as “or 1=1” or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as “true” so that any mathematical or string comparison can be used, where the SQL can perform the same.

NEW QUESTION 295

Which of the following tools can be used to perform a zone transfer?
* NSLookup
* Finger
* Dig
* Sam Spade
* Host
* Netcat
* Neotrace

NEW QUESTION 296

Jude, a pen tester, examined a network from a hacker’s perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.

What is the type of vulnerability assessment that Jude performed on the organization?
* External assessment
* Passive assessment
* Host-based assessment
* Application assessment