312-50$^{\text{Q\&As}}$

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Study the snort rule given below and interpret the rule.

alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "mountd access";)

A. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet

B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet

C. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111

D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Correct Answer: D

Refer to the online documentation on creating Snort rules at
http://snort.org/docs/snort_htmanuals/htmanual_261/node147.html

QUESTION 2

Which of the following is not considered to be a part of active sniffing?

A. MAC Flooding

B. ARP Spoofing

C. SMAC Fueling

D. MAC Duplicating

Correct Answer: C

QUESTION 3

Rebecca is a security analyst and knows of a local root exploit that has the ability to enable local users to use available exploits to gain root privileges. This vulnerability exploits a condition in the Linux kernel within the execve() system call. There is no known workaround that exists for this vulnerability. What is the correct action to be taken by Rebecca in this situation as a recommendation to management?

A. Rebecca should make a recommendation to disable the () system call

B. Rebecca should make a recommendation to upgrade the Linux kernel promptly

C. Rebecca should make a recommendation to set all child-process to sleep within the execve()

D. Rebecca should make a recommendation to hire more system administrators to monitor all child processes to ensure that each child process can\\'t elevate privilege

Correct Answer: B

QUESTION 4

Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

A. Network aliasing

B. Domain Name Server (DNS) poisoning

C. Reverse Address Resolution Protocol (ARP)

D. Port scanning

Correct Answer: B

This reference is close to the one listed DNS poisoning is the correct answer. This is how DNS DOS attack can occur. If the actual DNS records are unattainable to the attacker for him to alter in this fashion, which they should be, the attacker can insert this data into the cache of there server instead of replacing the actual records, which is referred to as cache poisoning.

QUESTION 5

Angela is trying to access an education website that requires a username and password to login. When Angela clicks on the link to access the login page, she gets an error message stating that the page can\\'t be reached. She contacts the website\\'s support team and they report that no one else is having any issues with the site. After handing the issue over to her company\\'s IT department, it is found that the education website requires any computer accessing the site must be able to respond to a ping from the education\\'s server. Since Angela\\'s computer is behind a corporate firewall, her computer can\\'t ping the education website back.

What ca Angela\\'s IT department do to get access to the education website?

A. Change the IP on Angela\\'s Computer to an address outside the firewall

B. Change the settings on the firewall to allow all incoming traffic on port 80

C. Change the settings on the firewall all outbound traffic on port 80

D. Use a Internet browser other than the one that Angela is currently using

Correct Answer: A

Allowing traffic to and from port 80 will not help as this will be UDP or TCP traffic and ping uses ICMP. The browser used by the user will not make any difference. The only alternative here that would solve the problem is to move the computer to outside the firewall.

QUESTION 6

Sandra is the security administrator of ABC.com. One day she notices that the ABC.com Oracle database server has been compromised and customer information along with financial data has been stolen. The financial loss will be estimated in millions of dollars if the database gets into the hands of competitors. Sandra wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crime investigations throughout the United States?

A. NDCA

B. NICP

C. CIRP

D. NPC

E. CIA

Correct Answer: D

QUESTION 7

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

See foobar

What is this attack?

A. Cross-site-scripting attack

B. SQL Injection

C. URL Traversal attack

D. Buffer Overflow attack

Correct Answer: A

QUESTION 8

_________ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

A. Trojan

B. RootKit

C. DoS tool

D. Scanner

E. Backdoor

Correct Answer: B

Rootkits are tools that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

QUESTION 9

Giles is the network administrator for his company, a graphics design company based in Dallas. Most of the network is comprised of Windows servers and workstations, except for some designers that prefer to use MACs. These MAC users are running on the MAC OS X operating system. These MAC users also utilize iChat to talk between each other. Tommy, one of these MAC users, calls Giles and says that his computer is running very slow. Giles then gets more calls from the other MAC users saying they are receiving instant messages from Tommy even when he says he is not on his computer. Giles immediately unplugs Tommy\\'s computer from the network to take a closer look. He opens iChat on Tommy\\'s computer and it says that it sent a file called latestpics.tgz to all the other MAC users. Tommy says he never sent those files. Giles also sees that many of the computer\\'s applications appear to be altered. The path where the files should be has an altered file and the original application is stored in the file\\'s resource fork.

What has Giles discovered on Tommy\\'s computer?

A. He has discovered OSX/Chat-burner virus on Tommy\\'s computer

B. Giles has found the OSX/Leap-A virus on Tommy\\'s computer

C. This behavior is indicative of the OSX/Inqtana.A virus

D. On Tommy\\'s computer, Giles has discovered an apparent infection of the OSX/Transmitter.B virus

Correct Answer: B

OSX.Leap.A is a worm that targets installs of Macintosh OS X and spreads via iChat Instant Messenger program. http://www.symantec.com/security_response/writeup.jsp?docid=2006-021614-4006-99

QUESTION 10

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 his dial-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:

Y0u @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. ARP spoofing

B. SQL injection

C. DNS poisoning

D. Routing table injection

Correct Answer: C

External calls for the Web site has been redirected to another server by a successful DNS poisoning.

QUESTION 11

Kevin sends an email invite to Chris to visit a forum for security professionals. Chris clicks on the link in the email message and is taken to a web based bulletin board. Unknown to Chris, certain functions are executed on his local system under his privileges, which allow Kevin access to information used on the BBS. However, no executables are downloaded and run on the local system. What would you term this attack?

A. Phishing

B. Denial of Service

C. Cross Site Scripting

D. Backdoor installation

Correct Answer: C

This is a typical Type-1 Cross Site Scripting attack. This kind of cross-site scripting hole is also referred to as a non-persistent or reflected vulnerability, and is by far the most common type. These holes show up when data provided by a web client is used immediately by server-side scripts to generate a page of results for that user. If unvalidated user-supplied data is included in the resulting page without HTML encoding, this will allow client-side code to be injected into the dynamic page. A classic example of this is in site search engines: if one searches for a string which includes some HTML special characters, often the search string will be redisplayed on the result page to indicate what was searched for, or will at least include the search terms in the text box for easier editing. If all occurrences of the search terms are not HTML entity encoded, an XSS hole will result.

QUESTION 12

The follows is an email header. What address is that of the true originator of the message?

Return-Path:

Received: from smtp.com (fw.emumail.com [215.52.220.122]. by raq-221-181.ev1.net (8.10.2/8.10.2. with ESMTP id h78NIn404807 for ; Sat, 9 Aug 2003 18:18:50 -0500 Received: (qmail 12685 invoked from

network.; 8 Aug 2003 23:25:25 -0000 Received: from ([19.25.19.10].

by smtp.com with SMTP

Received: from unknown (HELO CHRISLAPTOP. (168.150.84.123.

by localhost with SMTP; 8 Aug 2003 23:25:01 -0000

From: "Bill Gates"

To: "mikeg"

Subject: We need your help!

Date: Fri, 8 Aug 2003 19:12:28 -0400

Message-ID:

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary="----=_NextPart_000_0052_01C35DE1.03202950"

X-Priority: 3 (Normal.

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook, Build 10.0.2627

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165 Importance: Normal

A. 19.25.19.10

B. 51.32.123.21

C. 168.150.84.123

D. 215.52.220.122

E. 8.10.2/8.10.2

Correct Answer: C

Spoofing can be easily achieved by manipulating the "from" name field, however, it is much more difficult to hide the true source address. The "received from" IP address 168.150.84.123 is the true source of the

QUESTION 13

Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

A. CHAT rooms

B. WHOIS database

C. News groups

D. Web sites

E. Search engines

F. Organization\\'s own web site

Correct Answer: ABCDEF

A Security tester should search for information everywhere that he/she can access. You never know where you find that small piece of information that could penetrate a strong defense.

QUESTION 14

While probing an organization you discover that they have a wireless network. From your attempts to connect to the WLAN you determine that they have deployed MAC filtering by using ACL on the access points. What would be the easiest way to circumvent and communicate on the WLAN?

A. Attempt to crack the WEP key using Airsnort.

B. Attempt to brute force the access point and update or delete the MAC ACL.

C. Steel a client computer and use it to access the wireless network.

D. Sniff traffic if the WLAN and spoof your MAC address to one that you captured.

Correct Answer: D

The easiest way to gain access to the WLAN would be to spoof your MAC address to one that already exists on the network.

QUESTION 15

Which of the following systems would not respond correctly to an nmap XMAS scan?

A. Windows 2000 Server running IIS 5

B. Any Solaris version running SAMBA Server

C. Any version of IRIX

D. RedHat Linux 8.0 running Apache Web Server

Correct Answer: A

When running a XMAS Scan, if a RST packet is received, the port is considered closed, while no response means it is open|filtered. The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled closed. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400.

Latest 312-50 Dumps   312-50 Study Guide   312-50 Braindumps