312-50V11 Q&As

Certified Ethical Hacker v11 Exam

Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

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

https://www.certbus.com/312-50v11.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network\\'s external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.

What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer

B. Network sniffer

C. Intrusion Prevention System (IPS)

D. Vulnerability scanner

Correct Answer: A

QUESTION 2

Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

A. Preparation

B. Cleanup

C. Persistence

D. initial intrusion

Correct Answer: D

After the attacker completes preparations, subsequent step is an effort to realize an edge within the target\\'s environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target\\'s browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim\\'s computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment. Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim\\'s applications to ultimately execute malware on the victim\\'s computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public

email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public- facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required .

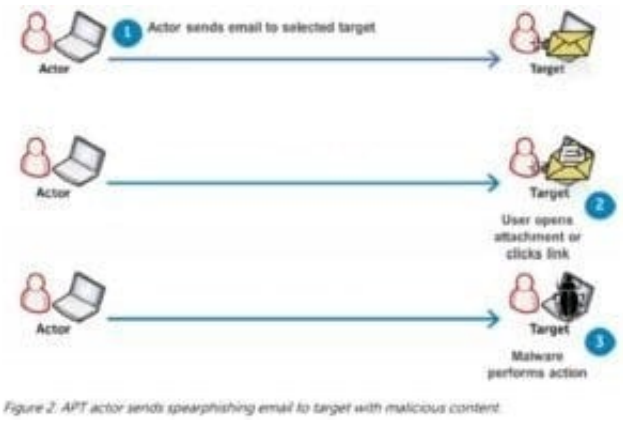

Figure 2: APT actor sends spearphishing email to target with malicious content

Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it\\'s able to accept commands.

QUESTION 3

During an Xmas scan what indicates a port is closed?

A. No return response

B. RST

C. ACK

D. SYN

Correct Answer: B

QUESTION 4

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. Reverse engineering

B. App sandboxing

C. Jailbreaking

D. Social engineering

Correct Answer: A

QUESTION 5

CORRECT TEXT

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

identify the NetBIOS code used for obtaining the messenger service running for the logged- in user?

A.

B.

C.

D.

Correct Answer: C

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

QUESTION 6

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

Correct Answer: B

QUESTION 7

Cross-site request forgery involves: A. A request sent by a malicious user from a browser to a server

B. Modification of a request by a proxy between client and server

C. A browser making a request to a server without the user\\'s knowledge

D. A server making a request to another server without the user\\'s knowledge

Correct Answer: C

QUESTION 8

Let\\'s imagine three companies (A, B and C), all competing in a challenging global environment. Company

A and B are working together in developing a product that will generate a major competitive advantage for

them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing.

With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails

from company B.

How do you prevent DNS spoofing?

A. Install DNS logger and track vulnerable packets

B. Disable DNS timeouts

C. Install DNS Anti-spoofing

D. Disable DNS Zone Transfer

Correct Answer: C

QUESTION 9

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company\\'s application whitelisting?

A. Phishing malware

B. Zero-day malware

C. File-less malware

D. Logic bomb malware

Correct Answer: C

QUESTION 10

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

Correct Answer: B

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.

QUESTION 11

Jim\\'s company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim\\'s company keeps the backup tapes in a safe in the office. Jim\\'s company is audited each year, and the results from this year\\'s audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Encrypt the backup tapes and transport them in a lock box.

B. Degauss the backup tapes and transport them in a lock box.

C. Hash the backup tapes and transport them in a lock box.

D. Encrypt the backup tapes and use a courier to transport them.

Correct Answer: A

QUESTION 12

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. UDP flood attack

B. Ping-of-death attack

C. Spoofed session flood attack

D. Peer-to-peer attack

Correct Answer: C

QUESTION 13

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace

B. Nessus

C. OpenVAS

D. tcptraceroute

Correct Answer: A

QUESTION 14

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator\\'s Computer to update the router configuration. What type of an alert is this?

A. False negative

B. True negative

C. True positive

D. False positive

Correct Answer: D

QUESTION 15

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

A. OS Detection

B. Firewall detection

C. TCP/UDP Port scanning

D. Checking if the remote host is alive

Correct Answer: D