KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **312-50v11**

Title : Certified Ethical Hacker Exam - C|EH v11

Version : DEMO

1.Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets 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. Cloud cryptojacking
C. Cloudborne attack
D. Man-in-the-cloud (MITC) attack
Answer: A
Explanation:
Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa, India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies. Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

2.Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?
A. Error-based injection
B. Boolean-based blind SQL injection
C. Blind SQL injection
D. Allnion SQL injection
Answer: D

3.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
Answer: A

4.Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs.
Which two SQL Injection types would give her the results she is looking for?
A. Out of band and boolean-based
B. Time-based and union-based
C. union-based and error-based

D. Time-based and boolean-based
Answer: C
Explanation:
Union based SQL injection allows an attacker to extract information from the database by extending the results returned by the first query. The Union operator can only be used if the original/new queries have an equivalent structure Error-based SQL injection is an In-band injection technique where the error output from the SQL database is employed to control the info inside the database. In In-band injection, the attacker uses an equivalent channel for both attacks and collect data from the database.

5.What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?
A. The attacker queries a nameserver using the DNS resolver.
B. The attacker makes a request to the DNS resolver.
C. The attacker forges a reply from the DNS resolver.
D. The attacker uses TCP to poison the ONS resofver.
Answer: A