

eLearning

anytime,



anywhere
education

EliteCertify

LEADING THE WAY TO SUCCESS

1 D0-470 SECURITY PROFESSIONAL DEMO



© Copyright 1997-2003, EliteCertify.com, All Rights Reserved.

What is the final step in assessing the risk of network intrusion from an internal or external source?

- A. Using the existing management and control architecture
- B. Evaluating the existing perimeter and internal security
- C. Analyzing, categorizing and prioritizing resources
- D. Considering the business concerns

Answer: A

Explanation: All four proposed answers are part of the risk assessment. What I am going to do is list them in the proper order:

Analyzing, categorizing and prioritizing resources

Considering the business concerns

Evaluating the existing perimeter and internal security

Using the existing management and control architecture

A file is replaced by another file that provides the same service but also has a secret operation that is meant to subvert security. What is this type of attack called?

- A. A buffer overflow attack
- B. A Trojan attack
- C. A denial-of-service attack
- D. An illicit server attack

Answer: B

Explanation: This question can be confused with the illicit server attack. The question is asking about the process of the file replacement, not the execution of the service that the file provides. The file replacement process, where a file containing a service – but with a security back door, is called a Trojan horse, usually passed as the result of a virus.

Incorrect Answers:

A: A buffer overflow attack is where you send enough data to either deplete all the buffers or overflow the buffer itself. For example, you send a packet that is larger than the maximum size of the buffer, causing part of the system to be overlaid, and crashing the task or system. This occurs when there are bugs in the code that do not properly check for these conditions, and corrupt the system, leading to a failure.

C: Denial of service is when the attack prevents legitimate users from accessing the server. Usually the server is flooded with so many messages that no one else can gain access. Of course, if you crash the

server, and the server is down, that too is a denial of service because the server was made inaccessible to legitimate users.

D: An illicit server attack is when you have an unauthorized service or daemon running on the system that can cause harm.

Most hackers run two services first learn information about a computer or Windows server attached to the Internet or intranet. These services enable hackers to find weaknesses in order to infiltrate the computer or network. Which one of the following choices lists the two services?

- A. Ping and traceroute
- B. Nslookup and whois
- C. Whois and ping
- D. Nslookup and traceroute

Answer: B

Explanation: WHOIS is used to gain information about the primary and secondary name servers. NSLOOKUP is then used to query these name servers to find names and types of existent resources on the network. These tools are used by the hacker in the discovery phase.

Incorrect Answers:

- A:** The traceroute and the ping commands are essentially the same, both built on the ICMP command. Ping tells you if you can contact the target, and so does traceroute. However, traceroute ALSO gives you the path to the server, identifying hops and the routers along the way. Essentially the two commands are redundant.
- C:** Ping is useful to test connectivity and existence of resources. Nslookup is, however, a much more dangerous tool in the hands of a hacker.
- D:** WHOIS would identify the primary and secondary name servers, which you would need before you can use the NSLOOKUP command to query the name servers. At this stage, a ping would be sufficient to find IP addresses in use, and it is not required yet to determine path information.

What common target can be reconfigured to disable an interface and provide inaccurate IP addresses over the Internet?

- A. Routers
- B. E-mail servers
- C. DNS servers

D. Databases

Answer: A

Explanation: Routers are attacked, because they may have weak security. If the router uses SNMP, which passes the community name in cleartext, attacking the router is an easy target. One into the router, either via SNMP or using Telnet, interfaces can be disabled, or reconfigured with a new address.

Incorrect Answers:

- B:** E-mail servers do not have an interface that can be disabled, nor would it be easy to target the e-mail server to change the IP address.
- C:** DNS servers do not have an interface that can be disabled, no would it be easy to target the DNS server to change the IP address. It is possible to hack a secondary DNS server and fake a zone transfer into it, thus changing the addresses that the DNS server provides. But the server does not provide a means that a hacker can get into configuration and disable any interfaces.
- D:** Databases do not have interfaces (although database servers do), nor are there IP addresses in the databases that could be used to allow inaccurate distribution of data.

Lucy obtains the latest stable versions of server, services or applications. Which type of attack does this action help to prevent?

- A. Dictionary attack
- B. Buffer overflow attack
- C. Trojan attack
- D. Illicit server attack

Answer: B

Explanation: A buffer overflow attack is where you send enough data to either deplete all the buffers or overflow the buffer itself. For example, you send a packet that is larger than the maximum size of the buffer, causing part of the system to be overlaid, and crashing the task or system. This occurs when there are bugs in the code that do not properly check for these conditions, and corrupt the system, leading to a failure. These bugs are discovered as the system matures, and when the bugs are discovered, the vendor will distribute fixes to plug the holes.

Incorrect Answers:

- A:** A dictionary attack does not exploit bugs or holes in the system, so applying fixes should not help prevent the attack.
- C:** A trojan attack does not exploit bugs or holes in the system, so applying fixes should not help prevent the attack. Note that a Trojan may have been deposited by a virus and maybe the fixes will prevent or