Exam Report: 6.3.4 Practice Questions

Date: 1/21/2020 4:18:35 pm
Time Spent: 2:45

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What common design feature among instant messaging clients make them less secure than other means of communicating over the internet?

- Transfer of text and files
- Freely available for use
- Real-time communication
- Peer-to-peer networking

Explanation

The common design feature among instant messaging clients that makes them less secure than other means of communicating over the Internet is their use of peer-to-peer networking. Peer-to-peer networking is inherently less secure than traditional client/server communication or networking mechanisms. With peer-to-peer networking, there is no centralized access control authority, so any client on the system can introduce malicious code or perform malicious actions without restriction.

The other design features listed here are typically seen as strengths of instant messaging clients, rather than as aspects of insecurity or vulnerability.

References

LabSim for Security Pro, Section 6.3.
[All Questions SecPro2017_v6.exm NETWORK_APPS_01]

Question 2: Correct

What type of attack is most likely to succeed with communications between instant messaging clients?

- Denial of service
- Brute force password attack
- DNS poisoning
- Sniffing

Explanation

A sniffing attack is most likely to succeed for communications between instant messaging clients. Many instant messaging clients communicate in cleartext or use an easily broken basic encryption scheme to protect integrity, rather than confidentiality. When you employ an instant messaging system, you should assume all of your communications are being intercepted and never discuss confidential, personal, or sensitive issues.

Denial of service and DNS poisoning attacks may be successful with a single target or a few targets using a common network routing path, but these types of attacks are not successful with instant messaging systems as a whole. Brute force password attacks are pointless for instant messaging.

References

LabSim for Security Pro, Section 6.3.
[All Questions SecPro2017_v6.exm NETWORK_APPS_02]

Question 3: Correct

Instant messaging does **not** provide which of the following?

- Real-time communications
- Privacy
- Indication of when you are online
- Ease of file transfers

Explanation

Instant messaging does not provide privacy. Many Instant messaging clients communicate in cleartext or use an easily broken basic encryption scheme to protect integrity rather than confidentiality. Because of this, a sniffing attack is most likely to succeed with communications between instant messaging clients. When you employ an instant messaging system, you should assume all of your communications are being intercepted and never discuss confidential, personal, or sensitive issues.

References

LabSim for Security Pro, Section 6.3.
[All Questions SecPro2017_v6.exm NETWORK_APPS_03]

Question 4: Correct

Your organization's security policy specifies that peer-to-peer file sharing is not allowed. Recently, you received an anonymous tip that an employee has been using a BitTorrent client to download copyrighted media while at work.

You research BitTorrent and find that it uses TCP ports 6881–6889 by default. When you check your perimeter firewall configuration, only ports 80 and 443 are open. When you check your firewall logs, you find that no network traffic using ports 6881–6889 has been blocked.

What should you do?

- Implement an application control solution.
- Block all outbound ports in the perimeter firewall.
- Call Human Resources and have the employee fired for violation of the security policy.
- Determine that the accused employee is innocent and being framed.

Explanation

In this scenario, the best solution would be to implement an application control solution. A firewall alone may be insufficient to block the use of network applications. Knowledgeable users can circumvent firewall ACLs by reconfiguring network applications to use ports commonly left open. In this scenario, if the accusations are founded, then the employee may have reconfigured his BitTorrent client to use port 80 or 443, allowing the traffic through the firewall unimpeded. An application control solution can be used to block unauthorized network applications. Application control implementations use application signatures to identify specific applications. The contents of packets are inspected and compared to these signatures to identify the associated application, regardless of which protocol or port is in use.

Blocking all outbound ports would cut off legitimate web-based traffic for all users. No determination of the employee's guilt or innocence should be made until concrete evidence can be gathered.

References

LabSim for Security Pro, Section 6.3.
[All Questions SecPro2017_v6.exm NETWORK_APPS_04]

Question 5: Correct

You are implementing a new application control solution.
Prior to enforcing your application whitelist, you want to monitor user traffic for a period of time to discover user behaviors and log violations for later review.

How should you configure the application control software to handle applications not contained in the whitelist?

- ○ Block
- ○ Drop
- ○ Tarpit
- ➡ ◉ Flag

Explanation

When using an application control solution, an application whitelist is defined centrally and applied to all network devices. Only applications contained in the whitelist are allowed. Applications not whitelisted can have several actions applied:

- *Blocked* applications are not allowed. The session will be dropped if it uses UDP and reset if it uses TCP.
- *Flagged* applications are allowed, but a violation is logged when they are identified.
- *Tarpitted* applications are not allowed. However, the connection between hosts is kept alive while the application data itself is silently dropped. This makes it appear to both hosts that the other host is receiving the data, but is not responding.

Note: Not all application control solutions support tarpitting application traffic.

References

LabSim for Security Pro, Section 6.3.
[All Questions SecPro2017_v6.exm NETWORK_APPS_05]