6.3.3 Network Application Facts

Be aware of security concerns for the following networking software:

Software	Considerations
Peer-to-Peer (P2P)	Peer-to-peer (P2P) software allows users to share content and access content shared by other users without centralized servers or centralized access control. P2P software uses ad hoc connections that allow peers to connect and disconnect at will. Common examples of P2P file sharing software are Kazaa and BitTorrent. The latest version of Windows also has a built-in peer-to-peer component for distributing operating system updates. Security considerations for P2P software include the following: - Files accessible from other users might be posted illegally. - Files available for download could contain malware. - File sharing uses network bandwidth and could consume so much bandwidth that regular traffic is affected. - Weaknesses in P2P software could allow attackers to access more than just the files shared on a system. Steps a security administrator can take include the following: - Use content filters to block downloading and uploading copyrighted files that the file owners do not want to be shared. - Block the port the P2P software is using. - Enable encryption in the P2P program.
Instant Messaging (IM)	Instant messaging (IM) provides real-time text messaging communication and supports picture, music, and document exchange. Common examples of instant messaging are Google Talk, Skype, iMessage, Facebook Messenger, IRC, and Slack. Although it offers a quick way to communicate, IM has the following problems: - Use of peer-to-peer networking makes IM clients less secure than other communication methods. - IM is either in cleartext or uses an easily broken basic encryption scheme to protect integrity rather than confidentiality. IM traffic is subject to sniffing, capturing, and viewing by others. - Loss of productivity is considered a major IM problem. - Malicious code propagation, worms, and viruses are easily spread through IM. - *Spim*, which is a type of spam targeting users of instant messaging (IM) services. - IM systems contain user directories, making it easy to identify spim targets. - IM systems often contain demographic information about users. - Information in contact lists can be remotely accessed. Create a whitelist or use an IM blocker as a countermeasure to spim. - Client-side scripting allows attackers to send messages on behalf of other IM users and can be used to create social engineering attacks. - IM clients often indicate when you are online, even without your consent. IM software, especially free software with ads, may track your use for marketing purposes.

Use the following to control the use of networking software:

- Have a written policy that identifies the allowed (or not allowed) use of all software.
- Use Group Policy or other methods to prevent installation of the software.
- Block firewall ports that are used by the software.
- Consider implementing an application control solution.
  - A firewall alone may be insufficient in blocking the use of network applications.
    - Knowledgeable users can circumvent firewall ACLs by reconfiguring network applications to use ports commonly left open.
    - Packet filtering firewalls do not inspect the contents of a packet. Only the source IP address, destination IP address, protocol, and port are used to determine if a packet should be blocked.
  - 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 against these signatures to identify the associated application.
  - An application whitelist is defined centrally and applied to all network devices.
    - Only applications contained in the whitelist are allowed.
    - Several actions can be applied to applications that not whitelisted:
      - *Flagged* applications are allowed, but a violation is logged when they are identified.
      - *Blocked* applications are not allowed and are blocked. The session will be dropped if it uses UDP and reset if it uses TCP.
      - *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.

      Not all application control solutions support tarpitting application traffic.

- If a user tries to use a disallowed application, they can be prompted to contact the help desk or system administrator to get the application reviewed and approved for use.