Instructor Notes for the "User Identification" Scenario

January 28, 2009

The "User Identification" scenario illustrates the advantages of using centralized authentication servers. It also identifies challenges associated with identifying users who must utilize remote computers and networks that are potentially hostile.

The topology includes a public facing web server on the same computer that includes enterprise assets. Some players may desire to recast the topology to implement a "DMZ", but players have no ability to buy computers or software. Players must make due with the given topology.

The virtual users are unable to login to their workstations until the player either adds each user to their workstation, or defines an authentication server. The latter is a lot less work.

Some players may choose to configure the workstations to not require local authentication – in which case malicious insiders compromise assets due to the lack of authentication (local ACLs are not applied if workstation has no accounts and does not require local authentication.)

After the computers are configured to identify users, an arbitrary management decision dictates the use of "long" passwords. If the player configured an authentication server, this can be implemented via a single step.

After long passwords are implemented, attention turns to the server which initially does not require remote authentication and has public access to a shared asset. The player is warned that "unaccountable access" to the asset makes it hard to determine the source of questionable changes to the asset. The access may have been "authorized", but you don't know which authorized user made a mistake. After accountability is established, attacks commence. If the player does not set the ACL on the sugar spinner asset, it is compromised via the weak web server. Players don't have the ability to move the outward facing web functions to a different machine (e.g., a DMZ) in this scenario – they are forced to consider use of access control mechanism.

The second phase requires the player to configure the system to let a remote user access an asset on one of the servers. The remote user is forced to use a "public" PC on a potentially hostile network. Once the remote user is able to login to the server, the user's password is "sniffed" and attackers use the password to compromise the server. This occurs until the player deploys a counter measure – i.e., requiring the use of one-time passwords. Malicious software on the remote computer can still capture and/or corrupt data on the server during the remote user's session, but the one-time passwords prevent attackers from later gaining access to the server.

The third phase requires the player to deploy mechanisms that allow authorized visitors (i.e., from some branch office) to use a local computer to access a protected asset. Visitors cannot be given explicit accounts on workstations or authentication servers.

However, visitors do have smart cards that include their authorizations. If players define a validation profile on the visitor computer, and deploy a suitable ID Device, then the visitor can use that workstation.

The lab manual for this scenario walks the player through the steps that must be performed to complete the scenario.