1. CyberCIEGE Identity Database

CyberCIEGE is an information assurance (IA) training tool that illustrates computer and network security principles through simulation and resource management trade-offs. CyberCIEGE players construct computer networks and make choices affecting the ability of these networks and the virtual users to protect valuable assets from attack by both vandals and well-motivated professionals.

The Identity Database scenario requires players to protect an identity database that is used in the generation of smart card IDs. The scenario does not address smart cards per se; rather it highlights some issues related to protecting a centralized database that is accessed by a variety of users. Security issues raised in this scenario include:

- Use of network filters and/or VPNs to protect information that must be accessed via the Internet;
- Use of background checks to reduce the risks of insider threats
- Use of operating system access control mechanisms to limit modes of access (e.g., read only rather than read-write).
- Reliance on smartcard activated locks to protect high value information can increase an attacker's motive to compromise the databases used in creating the smartcards.

As with all CyberCIEGE scenarios, students are encouraged to explore the effects of "wrong" choices as well as trying to select the correct choices. Plan on playing the scenario several times before finally going through it making what you believe are the correct choices.

1.1 Preparation

From the "Campaign Player", select the "Identity Management" campaign and the "Identity Database" scenario.

The player is expected to have first completed the Network Filters and Introductory VPNs scenarios prior to playing this scenario.

Select the "Identity Database" scenario from the scenario list. Then click the "Play" button.

Read the briefing and the objectives screens, and explore the encyclopedia (via the "F1" key). As you play the scenario, remember you can save the game at any time and come back to that state later. Also, the game automatically saves your state at each transition to a new phase.

1.2 Play

1.2.1 Phase 1 – Remote access to the identity database

- Read the objectives and review user goals.
- Observe the network topography, locate the identity database and review who is permitted to access the identity database.
- Run for a while and respond to attacks as they occur – or try to preclude attacks before they occur.

1.2.2 Phase 2 – Contractor access to the identity database

- Locate the user who needs new access to the identity database.
- Determine why the user is not permitted access, and find a way to provide access for this user. If you run for a while, the user might give you a hint.
- Reflect on the meaning what might be meant by providing the contractor with "least privilege".

1.2.3 Phase 3 – Use of smartcard controlled smart locks

- Consider replacing the guard with smartlocks.
- Review what the guard is protecting.
- Consider relative motives of the different assets and possible consequences of relying on smartlocks.

1.3 Clean Up

The "View Log" button lets you view a log of what occurred during the game.

END OF LAB