CyberCIEGE Identity Management

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 CyberCIEGE *Identity Management* scenario explores issues related to identifying people who need access to a military base. The scenario includes a guard who enforces policies selected by the player. Players may purchase devices such as card readers and eye scanners to aid in the management of identities.

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.

This scenario explores the following concepts:

- Policies must be established to identify who is allowed to enter the base, and these policies must somehow account for (or exclude) visitors.
- Enforcement of physical access policies relies upon methods of identifying individuals such that their authorizations can be determined. Some identification mechanisms are more robust than others (e.g., any old picture ID vs. a badge issued by the enterprise.
- Use of automated identification devices can simplify the tracking of base entry.
- Use of biometric devices might require the establishment of databases and connections between the devices and those databases.
- Policies must take into account the potential for false negatives when using biometric scanners.
- In some situations, policies and procedures must be established to recognize authorized visitors who are not individually known to local staff or local databases.
- Reliance on remote databases implies reliance on networks that connect to those databases.

1.1 Preparation

You should be familiar with concepts introduced in the Network Filters scenario and the Introduction to VPNs scenario before attempting this scenario.

1.2 Play

1.2.1 Phase 1, Who should the guard allow into the base?

The guard will only do what he is instructed to do, and will only allow people into the base based on the choices you make. Also consider the need to permit visitors. As users approach the guard checkpoint, click on them to see their thoughts. Pause the game if you need time to sort out your choices.

1.2.2 Phase 2, Logging entry to the base

How can you log entry to the base without requiring the guard to manually maintain a log? Consider the purchase of ID Devices and take into account the need to connect those devices to databases. And don't forget that you need to protect those databases.

1.2.3 Phase 3, Authorized Strangers

Explore your options for identifying and authenticating authorized individuals for whom you have no local information. You can't add them to zone access lists, yet you must somehow let them into the base.

Initially, you must deal with authorized strangers, i.e., people for whom there exists an explicit authorization to enter the base. This might be in the form of an authorization on a smartcard. Or perhaps an authorization managed on a central database. If it is the latter, you must consider the security of the link between your ID devices and the remote database. Note that CyberCIEGE ID devices typically include VPN clients.

1.3 Clean Up

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

END OF LAB