1. CyberCIEGE DMZ

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 DMZ scenario builds on concepts learned in the Network Filters scenario.

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.

The DMZ scenario explores the following concepts:

- Some server applications will forever have flaws that are periodically exploited by attackers.
- If the flaws result in access to moderately high level assets, then attackers can exploit some of these flaws before patches are available.
- One strategy for mitigating the vulnerabilities resulting from these flaws is to not expose servers containing sensitive assets to the Internet.
- For example, an email server that contains sensitive internal company email can be hidden behind an internal network filter. An external email “proxy” can be configured to receive email from outside of the company and forward that email to the internal server.
- Network filters can be configured to block all traffic except for that originating from a specific host or domain, and such a configuration can be used to protect an internal server from direct Internet attacks.

In this scenario you can largely ignore Zones and physical security issues.

1.1 Preparation

From the “Campaign Player”, select the “Starting Scenarios” campaign.
The player is expected to have first completed the “Tireply Filters Scenario” prior to playing this scenario.

Select the “DMZ” scenario from the scenario list. Then click the “Play” button.

Review the Objectives and the user goals.

1.2 Play

1.2.1 Phase 1 – Run for a while

- Review the user goals
- Figure out why Dan is failing to achieve his goal and make the necessary adjustment

1.2.2 Phase 2 – External Email

- Check your objectives.
- Try making incremental changes to the configuration and topology.
- When attacks happen, check the Attack Log via the button on the right side of the game window.
- Use the "Discovery/Scan" function to see which application services are visible and their patch status.
- Use F1 to learn about building a DMZ
- Build a DMZ using the topology in the encyclopedia as a guide.
- After buying a second email server, right click on it, select "Applications" and then "Configure Email Server". Then check the "Email Proxy" checkbox to make this new server a proxy for the PCA Server.
- Configure the network filters on the two routers as suggested in the encyclopedia.

1.3 Clean Up

Exit the scenario by clicking the **Quit** button in the GAME screen.

Collect the game logs into a zipped folder by clicking the "**Advanced**" menu button and selecting "**Collect Logs**". Feel free to provide comments on the game within the provided space. Enter your NPS User ID as the user name in the field. Then click "**OK**" to create the zipped file on the desktop.

If you are running the exercise in the NPS Lab:
- copy the `logCollection.zip` file from the VM's desktop
- Minimize the VM (click on the "_" in the grey bar at the top of the screen)
- paste it into the workstation host's desktop "CyberCIEGE-Logs" folder.
- if prompted to overwrite the file, click **Yes**.

If you are running the exercise <u>outside</u> of the NPS Lab:
- please email the `logCollection.zip` file to CyberCIEGELogs@nps.edu.

Click on the minimized VMware Workstation session to resume it (and press **<Ctrl>-<Alt>-<Enter>** if it doesn't return to full-screen).

Click the **CLOSE** button to exit CyberCIEGE.

Shutdown or suspend the VM and logoff the workstation if you are finished in the lab.

END OF LAB