Lab 10 CyberCIEGE Introductory VPNs

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 VPNs scenario illustrates the use of VPNs to authenticate sources of information and to protect the secrecy of information over packet switched networks.

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:

- Unprotected Internet connections can be hijacked by attackers, allowing them to masquerade as legitimate users.
- VPNs provide a means of authenticating the source of data received over the network.
- Link encryptors don't work over packet switched networks because routers require plain text addressing information
- VPN gateways can be configured to protect traffic depending on its source and destination.
- If a single VPN mechanism permits both protected traffic and unprotected traffic, it introduces the risk that valuable information might flow out via unprotected connections.
- Locking down the configuration of a gateway appliance is often easier than locking down the configuration of a user's workstation. CyberCIEGE VPN clients can be configured to only permit protected communication when the workstation is in an expected state.
- Use of VPNs to protect high value assets requires high assurance in both the VPN mechanism and the underlying platform.

Key management within this scenario is simplified. See the "Simple Key Management" section of the of the Network Device Configuration" entry in the CyberCIEGE encyclopedia.

In this scenario you can largely ignore Zones and physical security issues. Also, don't worry about hiring or firing support staff or the trustworthiness of your virtual users.

10.1 Preparation

From the "Campaign Player", select the "Encryption" campaign as seen in figure 10-1.

The player is expected to have first completed the "Encryption Key Types" scenario prior to playing this scenario.

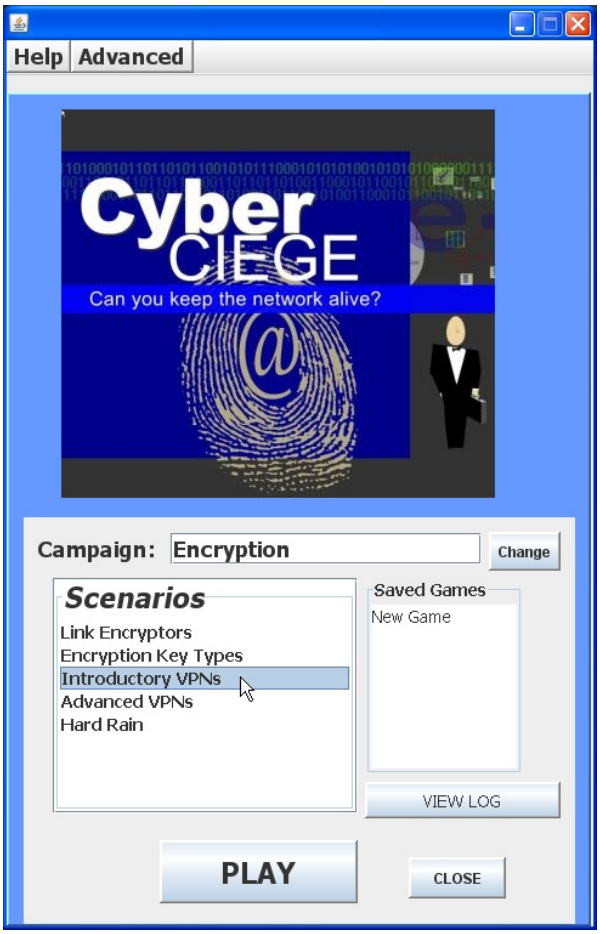

Figure 10-1: Select Introductory VPNs and Click Play

Select "Introductory VPNs" from the scenario list. Then click the "Play" button.

Read the briefing and the objectives screens, and explore the encyclopedia (via the "F1" key). From the Cryptography entry in the "Tutorials and Movies" content page of the online help, view the "Network Authentication through Cryptography" movie. As you play the scenario, remember you can save the state at any time and come back to that state later. Also, the game automatically saves your state at each transition to a new phase.

10.2 Play

10.2.1 Phase 1: Authenticate the Source of Asset Modifications

In this phase you must deploy a VPN gateway and a VPN client to ensure that only authorized individuals are able to modify the Marketing Roadmap asset.

- Click the Objectives tab to learn about your first objective.
- Click the ASSET tab to learn about the asset being protected
- Review the network topology via the NETWORK tab
- Press F1 to learn about using VPN gateways and VPN clients in CyberCIEGE.
- Run the simulation. What do you expect to happen?
- Find a way to protect the user's communications over the Internet. Deploy a VPN gateway at the main office and scrap the router. Go to the network screen and connect the Internet and the local LAN to the VPN gateway. Right click on the VPN gateway and select the protected network and define a connection profile (use F1 to view the encyclopedia to better understand connection profiles.) Consider using the "wild card" entries to define relatively loose profiles and then make them more specific as needed.
- Right click on Lisa's workstation and configure the VPN client.
- Beware of Adam, he has a VPN gateway that is configured to communicate with other VPN gateways and clients that belong to the enterprise.

10.2.2 Phase 2: Web Access

- Configure the connection profiles to permit the users to access the web. Each VPN component must have at least two connection profiles, the first would protect traffic destined for a specific domain (i.e., the domain of the remote user). The second profile would permit unprotected traffic to all other domains.
- Consider the implications of permitting web access to the enterprise computer systems and deploy countermeasures as needed.

10.2.3 Phase 3: Protect a Higher Motive Asset

- Check your objectives and the value of the new asset you must protect
- Consider the risks of Trojan horses. What keeps them from sending high value data out to the Internet?
- Buy Harry a second workstation via which to access the web. Connect it to the VPN via a separate LAN and configure the connection profiles such that traffic from the LAN having high value data must always be protected.
- Buy Lisa a second workstation and connect it to her router. Configure her original workstation connection profiles such that traffic is always protected.
- Locking down the configuration of a gateway is easier than is locking down the configuration of a user's workstation. Investigate the use of "measured boot" to ensure that Lisa's VPN client only works when her workstation is in an expected state.

10.2.4 Phase 4: Deploy a High Assurance VPN Gateway

Check the objectives. The attacker motive to compromise the Merger Plan is now much greater. The assurance of the vpn gateways that you could afford to purchase in phase 1 is not sufficient to protect new assets.

- Click the ASSET tab to learn the value of the new asset that must be protected
- Consider deploying high assurance VPN gateways.

10.3 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 outside 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.

10.4 Additional Questions

Question 1. *In the "Network Authentication Through Cryptography Movie", what was is called when the attacker created data packets that looked like they originated with Mary?*

Question 2. *In the "Network Authentication Through Cryptography Movie", why wasn't the entire data packet run through the public key algorithm?*

END OF LAB