1. CyberCIEGE Advanced 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 Advanced VPNs scenario extends the Introductory VPN scenario to include public and symmetric key mechanisms and associated vulnerabilities. It is assumed that the student has first played the Introductory VPN 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.

In addition to the topics explored in the Introductory VPN scenario, this scenario explores the following concepts:

- VPNs encryption mechanisms can rely on either symmetric keys (shared secrets) or public keys.
- Use of symmetric keys requires a means to security distribute shared secrets, and this can be costly.
- Shared secrets can become "stale" and there is a risk that an unwanted party has access to the secret, thereby potentially defeating the protection provided by encryption.
- Use of public keys requires some form of public key infrastructure (PKI). This includes the use of a Certification Authority to issue certificates and the management of installed root certificates. See the Advanced Key Management section of the Network Device Configuration" entry in the CyberCIEGE encyclopedia for a description of PKI elements used in VPNs.
- Use of public keys implies a reliance on the security of the elements of the PKI (e.g., the CAs and the procedures that manage which CA roots will be accepted).
- Extending an enterprise's PKI to recognize certificates signed by external CAs requires an enterprise to either install the external CA's root certificate as a root, or cross certify (i.e., sign) a certificate containing the external CA's public key.
- Cross certification can lead to a need to trust external entities to enforce security policies.
- Establishing certificate policies (i.e., constraining which certificates can be used for specific purposes) can be used to bound risks of relying on external parties.

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

1.1 Preparation

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

The player is expected to have first completed the "Introductory VPNs" scenario prior to playing this scenario.

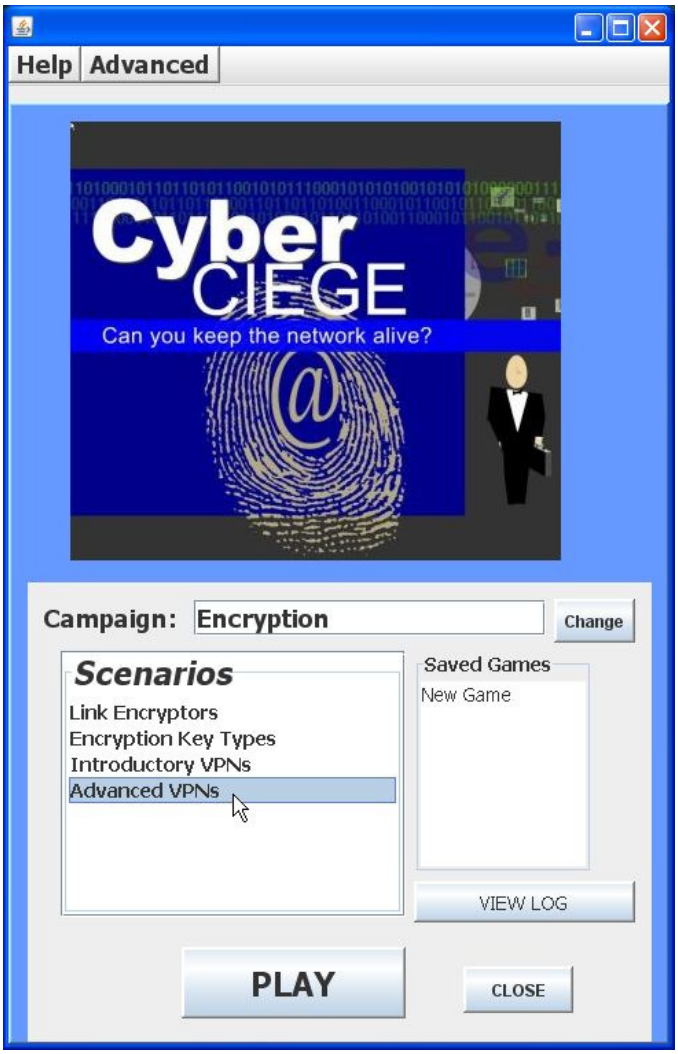

Figure 1: Select Virtual Private Networks and Click Play

Select the "Advanced VPNs" 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). From the Cryptography entry in the "Tutorials and Movies" content page of the online help, view the "Public Key Infrastructure" movie. 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: Authenticate the Source of Asset Modifications

In this phase you must deploy VPN gateways 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.
- Decide whether you want to use symmetric keys or public keys. Try playing the scenario each way. If you choose public keys, you will need to select a CA and install one or more CA roots. You have an option of purchasing your own CA, or buying certificates from a public pay-per-cert CA. If you chose symmetric keys, you must select a "key identifier".
- 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.

1.2.2 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.

1.2.3 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.

1.2.4 Phase 4: Deploy a High Assurance VPN Gateway

Check the objectives. You now must protect a very high value asset from disclosure. 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.

1.2.5 Phase 5: Use PKI to purchase from an external vendor

- Check the objectives. You must let Harry communicate with an external vendor who has their own PKI and CA.
- Look into the possibility of cross certifying certificates and the use of "Certificate Policies" with your connection profiles. Also, note the vendor is quite promiscuous and will cross certify your CA's certificate should you purchase and start using one.

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 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.

END OF LAB