Instructor Notes for the Advanced VPN Scenario
September 2009

Students should be provided with the "CyberCIEGE Advanced VPN Scenario Lab Manual". Players are assumed to have completed the VPN introduction scenario and its prerequisites.

This scenario builds off of the VPN introduction scenario, requiring the player to choose between public key and symmetric key encryption types. The scenario introduces Certification Authorities (servers having CA software) and the concept of "installed roots". 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. Also see the PKI tutorial. The scenario has several phases:

- Phase 1: Students must deploy a VPN gateway and a VPN client to authenticate modifications to moderately valuable assets.
    - Asset's computer initially lacking remote authentication. Player might set that, but session would still be hijacked.
        - Blocking NFS via filters keeps users from achieving goals
    - The player has enough money to buy one VPN gateway, forcing the vpnplayer to configure a VPN client as well as the gateway.
    - Rogue user has vpn gateway initially configured with key ID "A", which is treated as the general purpose enterprise VPN key. If player selects public key, then the rogue user's VPN is magically issued a cert from the CA that will allow it to communicate.
    - If the player selects public key encryption, the player must then either buy a CA or use a pay-per-cert CA to issue certificates and serve as the installed root.
    - If the player fails to configure connection profiles, goals are not achieved and player is informed of the problem.
    - Player must either configure strict connection profiles, or require remote authentication at the asset's computer to prevent an insider from using his VPN gateway to maliciously modify the asset.
- Phase 2: Users at both sites require internet access.
    - Player must provide a topology or connection profiles that permit the users to access the Internet. The simplest solution is to add unprotected access to the connection profiles.
    - Lisa's computer lacks some basic procedural security that can lead to corruption of the Marketing Roadmap.
- Phase 3: Higher value confidential assets (with higher motive) are introduced. The motive is high enough to drive Trojan horses to exfiltrate the confidential data. And the motive is high enough to subvert the VPN client unless a special client with "measured boot" is selected. But the motive is not so high as to subvert the VPN gateways.
    - Player is warned of risks as follows:

    - If Public Key:
        - Split tunnel
        - Island hop
        - Measured boot
        - Subverted CAs (if the player is using the pay-per-cert CA, or has put their own CA on the network.)

    - If symmetric key is "A" (same as default on rogue user's VPN), attack occurs due to spoofed routing of packets between data-side VPN and rogue user.

- Phase 4: Students must protect high value assets using high assurance VPN gateways. The value of the motive to compromise the Merger Plan asset is increased such that low or moderate assurance gateways will be subverted.
- Phase 5: A new remote site is introduced. The remote site is a vender with whom one of the users must place orders via an electronic ordering system. The vendor requires a VPN to provide access, and the vendor uses their own PKI.
    - If the student had been using secret (symmetric) keys, the student will have to change the two VPNs to use a PKI, and purchase and use a CA.
    - Once the student has configured components to use a purchased CA, the scenario automatically causes the vendor's CA to sign (cross certify) the CA's certificate.
    - If the student installs the vendor's root, the player will always end up losing.
    - The player must cross certify the vendor's CA certificate and establishes a certificate policy for the high value connection profiles that precludes use of cross certified certificate chains.

Getting Student's Started

Students should be provided with a copy of the "CyberCIEGE Advanced VPN Lab Manual". This scenario is intended to follow the "Introductory VPN" scenario.

Student Assessment

Student progress and results can be assessed using the Campaign Analyzer. From the CyberCIEGE desktop folder, select the "ccse" directory and then start the "Campaign Analyzer". It defaults to the "Starting Scenarios" campaign. Use the "Select" button to select the "Encryption" campaign. Select the "Advanced VPNs". Each student that has played the game will appear in the list, along with summary status. If the student did not "win" the game, the status identifies the most advanced phase the student had reached. To view details of a student's play, select that student entry and press the "View Log" button.