Instructor Notes for the Hard Rain email Scenario

October 2009

Students are expected to have completed the Advanced VPN scenario to learn about use of PKI elements.

The scenario is intended to illustrate the use of PKI-based email encryption and signatures to protect email assets from unauthorized disclosure and modification.

The scenario has several phases:

- Phase 1: Insiders want to snoop into emails related to potential layoffs. .
  - The player is provided no means by which to prevent disclosure of the email messages to unauthorized insiders except by use of email encryption.
  - Insiders have administrator access to the email server and the player cannot modify that.
  - Disconnecting insiders from the network causes them to fail goals and bad things happen.
  - Player has the choice of using a pay-per-cert CA or buying a CA.
  - Installing pay-per-cert CA roots leads to spoofing and compromise of the secret email.
  - Attempts to rely on smart-cards fail because there are no smart-card minters available to purchase or use.
  - Purchase of a CA requires hiring an IT staff to serve a registrar.
- Phase 2: New user replaces insider who had been snooping. The new user is spying on the other user for management and submitting secret reports via email. Player must configure new user's email client to use encryption.
- Phase 3: Customer requires a digitally signed quote from the same user who is snitching for management.
  - Player must purchase and connect a router to connect to the Internet.
  - Customer uses the public CA for its certificates.
  - If player selects encryption for this goal, the encryption fails because the user cannot verify the customer's certificate.
  - If the player adds the public CA as an installed root, the certificate is spoofed.
  - Player can simply select to sign the quote (rather than encrypt) and not further action is needed.