BSI - VPN configuration in W2K

author: Zbigniew Suski

1. Checking communication paths

Note: perform the following exercises in teams, two computers in each one.

- run *Security Monitor* (IPSECMON) on both computers. Set the refresh time (press Options button) to 2sec.
- install a sniffer on both computers. It can be WinPcap + Ethereal, Iris or MS Network monitor.
- Apply filters to the sniffer to catch network traffic only between the machines from your team
- Test pinging between the machines and observe the test with the sniffer. Formulate conclusions.

2. IPSec tunnel configuration

Note: do this on both computers

- run MMC with *IP security policy management* snap-in (either run *Computer management* or run *mmc* and add this snap-in)
- create a policy:
  - in the context menu of *IP Security Policies on local machine* choose “Create IP Security Policy”
  - name the policy <your computer name>, clear option “Activate the default response rule“
- set the policy properties:
  - in the “Rules” tab clear “Use Add Wizard”, then choose Add
  - in the IP filter list choose Add
  - in the IP filter list window clear "Use add wizard" option, then choose Add
  - name the rule "outbound filter", set *My IP Address* as the source address.
  - set *a specific IP address* as the destination address. Consider the meaning of other options.
  - clear "Mirrored" option
  - in the "protocol" tab choose Any
  - in the "IP filter list" tab choose "Outbound filter"
  - enter the address of the other computer in "Tunnel settings" tab
  - in the "Filter action" tab clear "Use add wizard", then press "Add"
  - in the new filter settings leave the "Negotiate Security" option on, but clear the "Accept unsecured communication, but always respond using IPSec" option.
  - press "Add" and in the new window make sure "High (ESP)"option is checked
  - in the "Authentication method" tab set *Preshared key* and enter an agreed password. This option is least secure, but the other options require more advanced system configuration e.g. the computers should belong to the same domain tree.
- create another filter for inbound traffic in the same way.
- Activate the defined policy by choosing "Assign" in its context menu

3. IPsec tunnel testing

- restart packet sniffing
- run the *ping* command on one computer, then after 1 minute delay run it again. Notice the ping output each time and watch *Security Monitor* and sniffer windows
- do the same from another computer.
- on one computer run "net policyagent stop" from a command window. Test pinging afterwards.
- run "net policyagent start", then test pinging again.
- deactivate the policy on both machines: unassign it from the context menu and run "net policyagent stop"

4. PPTP server configuration. (to be done on one computer within each team)

Note :to be done on one computer within each team

- Add the "Routing and Remote Access" snap-in to the *MMC* console.
- From its context menu choose "add server", then select *This computer*
- run the "Configure and enable Routing and Remote Access" wizard from the server's context menu.
    - window "common configurations" : choose "Virtual private network server"
    - window "remote client protocols" : do not install additional protocols.
    - window "internet connection" : choose <no internet connection>
    - window "IP address assignment" : choose "from a specified range...", enter the range 192.168.diskNo.1..192.168.diskNo.1
    - window "managing multiple remote access servers" : choose "No, I don't want to set ..."
- in the properties of the Administrator account, in the "Dial-in” tab mark "Allow access"
- in the "Routing and Remote Access" snap-in leave the *Ports* container visible on the screen

5. VPN-PPTP client configuration.

Note :to be done on the other computer within each team

- open the "Network and dial-up connections" window
- doubleclick "Make new connection"
    - window "network connection type" : choose "connect to a private network through the internet"
    - window "destination address" : enter the address of the first computer
    - window "connection availability" : choose "only myself"
    - accept the connection name
    - do not connect now
- using a sniffer check the communication with the ping command.

6. Testing VPN-PPTP connection

- connect the client (an option in the context menu of the connection)
- enter Administrator login and password

- watch the process of connecting using the sniffer.
- refresh the "Routing and Remote Access" window
- run *ipconfig* on both machines, remember the results
- check the communication with the ping command using the normal IP of the other computer. Remember sniffing results
- check the communication with the ping command using this time the VPN IP. Remember sniffing results
- disconnect the client using the “Virtual private connection” context menu in the "Network and dial-up connections" window
- refresh the "Routing and Remote Access" window
- delete the connection on the client, disable "Routing and Remote Access" on the VPN server, then delete the server from the "Routing and Remote Access" window

Describe results of each task in the report (one report per team)