Windows 10 Firewall Lab

In this lab, you will combine some of the knowledge and skills from previous activities and the information from Chapter 10 on Firewalls. You will have some services running and ports open, scan to make sure they are visible from the outside, then block with firewall rules, and rescan to observe the changes.

1. All of the following are done on your Win 10 VM (not the host machine) & Kali VM. Make sure both VMs are on the same custom VMnets with DHCP enabled.
   - Edit/Virtual Network Editor to check which VMnet# is host-only with DHCP enabled
   - VM/Settings to select that VMnet# for both VMs

2. Start your WIN10 VM and services, & change hostname.
   - Change the name of your system so you can be sure which machine you're seeing in a scan:
     - Right-click Windows Start menu and select System
     - Click Change Settings, Change, then insert your 1st initial + last name for your computer name (i.e. alincoln), and then run the "whoami" command after reboot.
     - **Snip** the output from your command.
   - Make sure your Windows IIS web server is running, and can be reached by your Kali VM.
     - Didn't we make a snap shot earlier? Hmm …

3. Download & install nmap on the Win10 VM, then open a ncat listener.
   - https://nmap.org/download.html --> download latest stable release for Windows on the host machine, & copy it into your Win10 VM's download directory.
   - Nmap also installs ncat, which is what we need (c:\program files x86\nmap)
   - Start ncat running on port 8082 via command line: `ncat -l 8082 -k -v`
   - The -k option is the keep it running even after a scan hits it
   - You should see 2 new ncat inbound rules under Firewall/Advanced Settings
   - **Snip** the 2 new ncat inbound firewall rules
   - While you're here, quickly review & lookup some Window's inbound & outbound firewall rules
   - Disable some of the more obvious inbound & outbound firewall rules
   - From Kali, ping the Win10 VM. Any luck?
   - Hmm … ping uses ICMP, so might have to enable ICMPv4's echo request, and try again.
   - **Snip** the successful pings from Kali VM to Win10 VM.

4. Scan your Windows VM from your Kali VM using nmap to see what services are running.

- You have to set the parameters to scan for more than standard ports to see port 8082
    - nmap -p 1-8085 –T5 –A ***Target_IP***
    - The –p option allows you to specify ports, -A enables OS/version detection, and –T5 is set for a speed of "insane".
- **Snip** the services running. It should show port 8082 open.

5. On the Win10 VM, create a new firewall rule to block web traffic to your Win10 VM.
    - Currently, your Win10VM allows incoming regular web requests via HTTP.
    - Now we're going to test to see if a new Block rule overrules an existing Allow rule.
    - In Windows Firewall's Advanced Settings, create a new rule which blocks all HTTP inbound traffic across all profiles (domain, public & private) named "Blocky" with a description including your first initial and last name.
    - **Snip** the new block firewall rule.
    - Now on Kali, test it via its browser with the Win10 VM's IP. It should not work, and should prove that a Block rule overrides an Allow rule. Thanks Microsoft!

6. Now let's change the default HTTP port, & create a new inbound rule for incoming HTTP request.
    - Everyone with a network connection uses TCP:80 for HTTP requests to get our cat videos. We still want to have them available online, but not for just anybody …
    - On the Win10 VM, open the IIS Manager. In the Default Web Site Connection, Edit the Site Bindings from port 80 to 8888.
    - **Snip** the modified Site Bindings with the new port.
    - Cool, you changed the default port for incoming HTTP requests. Now test it via a browser on the Kali VM.
        - I wonder why it doesn't work?
    - **Snip** a successfully working website using the new port on Kali VM.
    - **Snip** the successful packet's details via Wireshark with the IP & port displaying.

7. Wouldn't it be neat to scan a network using a spoofed IP and port? Zenmap lets you do that rather easily.

    - On the Kali VM, launch Zenmep & create a new profile named "spoofy"
    - Select the Source tab, & specify a source address that is not yours and not the target machine. Also, specify the interfect to use (eth0).
        - Note, if you pick an address that does not exist, the packets will only go to the target and die there. If you pick a spoofed address that does exist, they will receive the replies.

- Under Ping tab, indicate that a ping should not be used before the port scan. That is the –Pn option.
- Your resulting scan command should look like this:
  - nmap -T5 -A -Pn -e eth0 -S spoofed_IP target_IP
- Setup a Wireshark capture on your Win10 if not already doing so, and capture the scan in Wireshark.
- In Wireshark, let's filter for the sneaky port 8888 you created earlier.
  - ip.addr==*spoofed_ip_here*
- **Snip** the successful spoofed packet's details via Wireshark with the IP & port displaying.

8. Set the firewall rules back the way they were.