Quiz - Additional Attack examples today

1. Which of the following measures can be used to counter a mapping attack? **1 / 1 point**

   ◯ Record traffic entering the network

   ◯ Look for suspicious activity like IP addresses or ports being scanned sequentially.

   ◯ Use a host scanner and keep an inventory of hosts on your network.

   ⦿ All of the above.

   ✓ **Correct**

   Correct! All 3 of these options can and should be used.

2. In order for a network card (NIC) to engage in packet sniffing, it must be running in which mode? **1 / 1 point**

   ⦿ Promiscuous

   ◯ Sniffer

   ◯ Inspection

   ◯ Open

   ✓ **Correct**
   Correct, the NIC must be running in promiscuous mode.

3. Which countermeasure can be helpful in combating an IP Spoofing attack?   `1 / 1 point`

   - (◉) Ingress filtering

   - (○) Enable IP Packet Authentication filtering

   - (○) Keep your certificates up-to-date

   - (○) Enable the IP Spoofing feature available in most commercial antivirus software.

   - (○) All of the above.

   > ✓ **Correct**
   >
   > Correct! This works but only if all routers use it.

4. Which two (2) measures can be used to counter a Denial of Service (DOS) attack?   `1 / 1 point`

   - ☐ Enable the DOS Filtering option now available on most routers and switches.

   - ☑ Use traceback to identify the source of the flooded packets.

   > ✓ **Correct**
   >
   > Partially correct! The downside here is that the source is most likely innocent but compromised machines.

   - ☐ Enable packet filtering on your firewall.

   - ☑ Implement a filter to remove flooded packets before they reach the host.

   > ✓ **Correct**
   >
   > Partially correct! The downside is that you will be filtering out some legitimate packets as well.

5. Which countermeasure should be used agains a host insertion attack?

○ Maintain an accurate inventory of of computer hosts by MAC address.

○ Use a host scanning tool to match a list of discovered hosts against known hosts.

○ Investigate newly discovered hosts.

◉ All of the above.

✓ **Correct**

Correct! All of these steps are necessary.