Computer Security Homework 7 (Due Friday 10/9/20)

1. True or False.
   (a) `ds4307-xr97-cc09.tracker.msmary.edu` is likely a phishing site designed to steal your Mount credentials.
   (b) The domain name `espn.tv` and the country Tuvalu have nothing in common.
   (c) If we DoS the Mount's DNS resolver, then most people worldwide will not be able to get to `msmary.edu`.

2. Why is it so much easier for an attacker to get their fake answer to a DNS query accepted when they are on a local network with the target versus being remote?
   (a) DNSSEC is applied to queries from a remote network but not on a trusted local network.
   (b) They can see the transaction ID and port number by sniffing traffic.
   (c) They can send more replies in a shorter amount of time since they are closer to the target.
   (d) The target's computer will trust the attacker's answers because the attacker's IP is from the local network.

3. Which of the following are ways that your computer could end up using an attacker's DNS resolver? Choose all that apply.
   (a) You use the public WiFi in an airport.
   (b) You don't secure your home WiFi router's login.
   (c) You get infected with malware.
   (d) You visit an HTTPs site over plain HTTP.
   (e) You let Stumpo have physical access to your laptop.

4. If you are worried that your ISP's DNS resolver's cache has been poisoned, which of the following can you do to make sure you don't get misdirected to a phishing site? Choose all that apply.
   (a) Instead use an open resolver like 8.8.8.8.
   (b) Memorize the IPs of the domains you want to visit and skip the DNS lookup.
   (c) Wait awhile for the poisoned cache entries to expire.
   (d) Stop using the internet and do something productive with your time.

5. In the DNS amplification attack, an attacker carefully crafts a packet. Answer the questions below about the packet and the attack.
   (a) The source address of the packet is of what machine?
   (b) The destination address of the packet is sent is of what machine?
   (c) One machine that is part of the attack is a DNS resolver misconfigured in what way?
   (d) One machine that is part of the attack is a DNS name server that has what specifically?

6. If the Mount wanted to make it harder for students to access the site `stackoverflow.com`, the school could use their DNS resolvers to do this.
   (a) What specifically would they do?
   (b) How could Mount students get around this?