Computer Security Homework 9 (Due Friday 10/25/20)

1. True or False.

   (a) _____ During an HTTP Flood DoS attack, network administrators have a hard time blocking attackers' traffic because it is hard to distinguish from legitimate traffic.

   (b) _____ The devices with MAC addresses 80-CE-62-D6-B9-FB and 80-CE-62-23-97-B2 were made by the same manufacturer.

   (c) _____ To find out the MAC address associated with a specific IP, a router will issue a DNS query.

   (d) _____ When you visit a website, your MAC address is typically logged by the web server.

   (e) _____ If a network administrator blocks all outgoing traffic except pings, then it will not be possible for people inside the network to use the network to transfer files to people outside the network.

   (f) _____ In an HTTP flood, attackers often request resources that cause the server to do a lot of processing.

   (g) _____ Many devices randomize their MAC address to avoid MAC-based tracking.

   (h) _____ ARP spoofing is typically performed by people on the same network as their target.

2. If an attacker hacks a single device running one of the protocols below, they can make large portions of the internet inaccessible to much of the world. Which protocol most likely is it?

   (a) ARP (b) BGP (c) ICMP (d) TCP

3. How do static ARP tables defend against ARP spoofing?

   (a) Administrators can easily tell if there are two entries in the table for a given IP.

   (b) There is no need for a query since the answer is in the table, so there is no way for an attacker to give a fake answer to the query.

   (c) They can be configured to automatically notify administrators when they have been changed.

   (d) They reside on each user's computer, so any changes to them will only affect that user.

4. If you and some friends want to perform a DoS attack without any help and are not particularly technically savvy (i.e. you can't program or use command line tools), which of the following would be easiest for you?

   (a) ARP flood (b) DNS reflection (c) NTP reflection (d) SYN flood

5. Which of the following DoS attacks would be viable options for a lone attacker trying to take down a server if the attacker is on a low bandwidth connection? Choose all that apply.

   (a) DNS reflection (b) HTTP flood (c) NTP reflection (d) ping flood

6. Which of the following attacks are still common in 2020? Choose all that apply

   (a) Echo-chargen attack (b) HTTP flood (c) Ping of Death (d) Smurf attack

7. Which of these attacks can directly allow an attacker to read the traffic destined for others? Choose all that apply.

   (a) ARP spoofing (b) BGP attacks (c) Echo-chargen attack (d) HTTP flood

8. An attacker sends a particular type of message that goes to the entire network, where the source IP address in the message is spoofed to be the target's address. This is part of which attack we covered?

9. An attacker sends a particular message that is larger than the receiver is expecting. This causes a memory problem that crashes the system. This is a description of what attack we covered?

10. Ports 7 and 19 are important in which attack we covered?

11. Here is a part of the IP to MAC address mappings on my laptop. Which, if any of the entries were obtained through ARP queries?

```
Internet Address      Physical Address      Type
169.254.255.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

12. Network administrators are supposed to not allow traffic out of their network that has a source IP not from their network. And ISPs that provide connectivity to a certain range of IP addresses should not allow traffic from those IPs if the source addresses are not in that range. Explain how if everyone actually followed these rules, a lot of DDoS attacks would no longer work.

"Bonus": Send any complaints about this assignment to the standard service running at the Math & CS Department's servers at port 9.