Computer Security Homework 8 (Due Friday 10/16/20)

1. True or False.

   (a) From a security perspective, the most important OSI layer is the session layer.

   (b) The tcpkill utility works by injecting SYN flags to make it seem like the connection is restarting.

   (c) The second part of the TCP three-way handshake involves a SYN-ACK.

   (d) Like TCP, UDP, establishes a connection with a three-way handshake

   (e) Whenever a system needs to find the IP address of a domain name, it typically makes a request to a system using port 53.

   (f) Disabling services you don't need on a server is generally considered a good security practice.

2. If you have a server that is accessible by SSH and you decide to move SSH from port 22 to port 7321, then

   (a) No one will be able to reach it, including you, because it's not the standard SSH port.

   (b) You will get somewhat less attackers trying to log onto your server because many simple attackers don't check that port.

   (c) You will get the same amount of attackers trying to log onto your server because they all do full port scans of your system.

   (d) Only you will be able to log onto the system because you're the only one that knows the magic port number.

3. Moving SSH from port 22 to port 8762301045

   (a) won't work

   (b) is more secure than leaving it at port 22

   (c) is no more secure than leaving it at port 22

   (d) will likely get you a call from the IETF (Internet Engineering Task Force) for a rules violation.

4. Suppose you are on the Mount's network and your friend is on MIT's network. Your friend says their IP address is 10.83.101.25 If you send Packet #1 to that IP address, who will get it?

   (a) your friend

   (b) someone on the Mount's network if they are using that IP address

   (c) you

5. In the Mitnick-Shimomura attack, the reason Mitnick DoS-ed the trusted server was

   (a) so that Shimomura could not access it to stop the attack.

   (b) if not, the SYN-ACK from Shimomura's computer would have caused the server to send an RST, stopping the connection attempt.

   (c) to reset any connections Shimomura had with it.

   (d) so that Shimomura would not be able to notice the attacker's machine performing the attack.

6. In the Mitnick-Shimomura attack, Mitnick could not see the replies to the commands they issued to Shimomura's computer. Why?

   (a) An unfortunate side-effect of the DoS attack is that the attacker could only send commands but not see their output.

   (b) The network was a wired network (not wireless) and so sniffing traffic was more difficult.

   (c) Those replies were going to the server that the attacker was impersonating.

   (d) None of the above. The attacker was able to see the output of their commands.

7. SYN cookies help defend against SYN floods by

   (a) denying traffic from IP addresses whose connections are not in its connection table.
   (b) blocking all incoming packets with the SYN flag set.
   (c) making sure that connections won't sit half-open using server resources.
   (d) only allowing traffic from TCP servers that don't use sequential (or predictable) sequence numbers.

8. In a SYN scan, if you receive a SYN-ACK, that means

   (a) the port is open
   (b) the port is closed
   (c) nothing yet because you can't tell if its open or closed until the final ACK arrives
   (d) nothing yet because it depends on whether or not the SYN-ACK is followed by an ACK or an RST

9. Which one of these does not typically use IP address spoofing?

   (a) SYN flood (b) SYN scan (c) DNS amplification (d) they all use it

10. Which of the following is an IP address of stackoverflow.com ?

    (a) 192.168.5.14 (b) 10.243.197.201 (c) 645.33.347.99 (d) 151.101.1.69

11. In a UDP port scan, if a port is open, what type of reply will you get?

    (a) SYN-ACK
    (b) RST
    (c) data in whatever format the service at that port is using
    (d) possibly some data in the format the service is using, but possibly nothing

12. Which attack can be performed by the following two lines of Python, using Scapy?

```
p = IP(dst='10.0.0.2')/TCP(sport=RandShort(), dport=80, flags='S')
srloop(p, inter=.01)
```

13. Suppose a web server is under attack from a SYN flood. The administrator decides to block all SYN packets for the next 24 hours, until the attack subsides. What is the biggest potential problem with this?

14. Once an attacker has a list of open ports, what do they do with that information?

15. Answer these questions about the TCP reset attack:

    (a) An attacker needs to know a target's IP address, the source and destination ports, and one other key piece of TCP header information. What is it?
    (b) How can attackers figure out this piece of information when they are on the same network as the target?
    (c) Is this piece of information easy to figure out if the attacker is hundreds of miles away on a different network from the target?