Computer Security   Homework 10 (Due Friday 10/30/20)

1. True/False.

   (a) ______ WPA2 security is generally pretty easy to break.

   (b) ______ If you try to use a stateless packet filter to block the outside world from making TCP connections with machines inside the network, some unwanted TCP packets may make it through the firewall.

   (c) ______ A certain type of malware contains the machine language instructions FA A7 04 4B 9E. An IPS that notices this sequence and blocks the malware would be doing so via anomaly-based detection.

   (d) ______ To stop outsiders from initiating connections with users inside your network, you can block all incoming packets with the SYN flag set.

   (e) ______ To block people inside your network from making HTTP connections, it's necessary to use an application layer firewall.

2. If you're behind a NAT router and you visit a website without using a VPN or proxy, what address will the website see?

   (a) Your machine's address (like 10.0.0.2)

   (b) The NAT router's global IP address

   (c) Neither, since IP addresses aren't visible to the site since it uses HTTP (layer 7) and IP addresses are at layer 3.

3. To try to stop people inside a network from visiting any websites outside the network, a network administrator could block all outgoing traffic with destination ports 80 and 443. This will

   (a) not stop people visiting websites that run on nonstandard ports

   (b) not stop people visiting websites through a VPN service

   (c) both

   (d) neither

4. Which of these is *not* something a packet filter can do?

   (a) Block traffic from a certain range of IP addresses.

   (b) Block traffic to all ports except 80 and 443.

   (c) Block all incoming traffic that contains executable files.

   (d) Block all UDP traffic.

5. In class, we talked about a statistical attack on WEP that relies on biases in RC4. The attack typically takes how long?

   (a) a few minutes   (b) a few hours   (c) a few days   (d) a few years

6. If you disable SSID broadcasts on your Wifi router, what will happen?

   (a) No one will be able to find your network, let alone connect to it.

   (b) Only people whom you tell the BSSID (MAC address) to will be able to connect to it

   (c) Anyone with commonly available tools will be able to find it and attempt to connect to it.

   (d) Disabling SSID broadcasts is not possible on most commercial routers.

7. If an attacker wants to set up an evil twin AP in a café, they need to know the real AP's MAC address. They usually get this from where?

   (a) Social-engineering the café's IT people.

   (b) A web search for common default MAC address settings for routers.

   (c) Physically inspecting the AP.

   (d) The AP's beacon frames, which contain this info.

8. In the chop-chop attack on WEP, an attacker sends packets with varying checksums to an AP. How will they know when they have a valid checksum?

   (a) They compare it to the value sent by the AP.

   (b) They have to compute it using some linear algebra.

   (c) The AP sends back an ACK.

   (d) They don't. They just have to keep guessing until they figure out the key.

9. Here is a set of firewall rules for the iptables firewall on Linux.

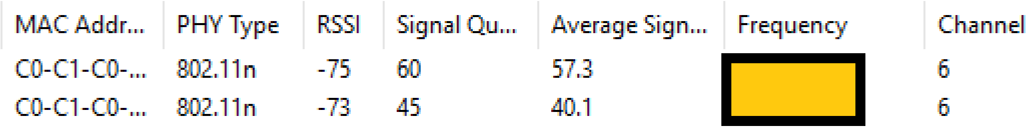
```
iptables -A myfirewall.rules -p icmp --icmp-type any -j ACCEPT
iptables -A myfirewall.rules -p tcp --destination-port 22 -j ACCEPT
iptables -A myfirewall.rules -p tcp --destination-port 80 -j ACCEPT
iptables -A myfirewall.rules -p all -j DROP
```

   (a) Is this a whitelist or a blacklist?

   (b) Is it possible to ping this server and get a reply back?

   (c) What specific services (email server, DNS, etc.) is this server running?

10. What frequency has been obscured in the image below?



MAC Addr...	PHY Type	RSSI	Signal Qu...	Average Sign...	Frequency	Channel
C0-C1-C0-...	802.11n	-75	60	57.3	[redacted]	6
C0-C1-C0-...	802.11n	-73	45	40.1	[redacted]	6

11. If you want to boot a random person off the MSMWireless network by sending a carefully crafted packet/frame to their computer, what is it that you need to send?

12. If your home Wi-Fi router has no firewall, it's likely people from the outside still won't easily be able to start connections with machines on your network. Why?

13. One weakness of WEP was that it used a 24-bit IV, which led to certain IVs likely occurring more than once after just a few thousand Wifi frames. One improvement made to WEP was to use 48-bit IVs. How many frames would it take now before we start getting repeat IVs?

14. After 3 failed guesses at a WPS pin, the system is supposed to lock out users for 60 seconds before they can try again (though many systems don't do this). If a system did do this, how long would it take someone to brute-force a WPS pin in the worst-case scenario (where they have to go through all possible pins)? Remember that there are far less than 10^8 pins an attacker needs to try.

15. Suppose Alice and Bob are using the very secure ChaCha stream cipher. Alice then decides that since both she and Bob share the secret key, she can use that to determine that someone claiming to be Bob really is Bob. To do this, she sends some plaintext over to Bob and asks Bob to encrypt it with his copy of the key and send back the ciphertext. Alice will then use her copy of the key to decrypt Bob's ciphertext and verify that it matches the original plaintext. Assume that Alice and Bob truly are the only ones with copies of the key. There is a serious flaw with this plan as concerns Eve the eavesdropper. Explain.