Exercises - Week 10
Network security

1. Are the following statements True or False:

a) **Intrusion Detection can eliminate DNS poisoning**
b) **The reason why TCP can be hijacked is the poor authentication mechanisms**
c) **DNSSEC provides confidentiality of DNS queries**
d) **A honeypot is a bot used to detect hijacking of the botnet.**
e) **Routing security relates to the capability of an adversary to influence the routes that messages will follow.**
f) **You can use IPSEC in tunnel mode to build a VPNs**

a) False - Intrusion detection systems can detect threats, but not prevent DNS poisoning as the DNS resolver itself is corrupted and sends wrong information.
b) True - TCP can use weak random number generator, which imply that an attacker could guess the sequence numbers and hijack the session. An authentication mechanism using a weak random number generator is considered as poor.
c) False - The answers are signed by the authoritative DNS resolvers, which provides authentication and integrity, but are not encrypted, so DNSSEC doesn't provide confidentiality.
d) False - A honeypot is a vulnerable computer on purpose, it serves to attract attackers and observe their behavior. It is a mean of defense against botnets, because we can study their behavior in order to develop a defense against them.
e) True - An adversary should not be able to influence the route and the delivery of messages over a network.
f) True - A lot of VPN are built over IPSEC in tunnel mode, because it guarantees confidentiality, integrity, authenticity and protection against replay attacks. IPSEC protects the IP packet by encrypting the payload using symmetric cryptography, and it ensures authentication and integrity of the IP header. It also add a security against replay attacks.

2. One of the uses of VPNs is to hide the destination of a communication. This is because, when a user connects to the internet through a VPN, this user service provider (or anybody observing his communication in the path to the VPN) can only see the VPN IP and not the final destination thanks to the IPSec Tunnel encryption.

a) **To maintain this property with respect to the ISP:**
    a) **DNS have to be routed through the VPN**
    b) **DNS have to be routed outside the VPN**
    c) **Who cares about DNS, we are not hiding the IP of the DNS resolver**

Justify

b) Would the fact that no-one can see the final IP hold if the VPN was built using IPSec in transport mode?

c) John is a member of a MyPrivateDiary.com site which provides private diary over the cloud. After learning about VPNs in Com-301, John bought an application called VPNX which uses IPSec Tunnel mode to create a tunnel and redirect every connection through the tunnel. John wrote a story about his new VPN application on his diary. Which one of the following entities can read John's diary? (Justify)

a. **VPNX company**
b. **John's ISP (internet service provider)**
c. **John's curious friend**
d. **MyPrivateDiary.com**
e. **MyPrivateDiary's ISP**

We will provide the answer to this question next week so that you have time to do this exercise after the lecture explaining VPNs.
(If you have done it and you can't wait for the answer, you can always drop an email)

3. If we suspect that a DNS resolver has been poisoned. Is it a good idea to consult other DNS resolvers for the answer? Why?

Yes. Following the separation of privilege principle, if we ask more than once we force the adversary to compromise more than one resolver effectively increasing the cost of the attack.

4. Can Intrusion Detection Systems help to prevent: (Justify)

a) **BGP hijacking?**
b) **DNS Poisoning?**

No and no. Intrusion Detection Systems (IDS) analyze the patterns (signatures or anomalies) in your network. These attacks affect routing tables / IP-domain assignments. No analysis on your network will help avoiding them.

If you think about IDS in the neworks of the routers / resolvers. This also does not help much. There is no signature or pattern. The real problem is the content, which is hard to decide whether it is right or wrong (Though, as said in the class, some filtering can actually be done for corner cases. But it will not eliminate, or mitigate much the problem).

5. You are the network administrator for a large company.

(a) Your company will be held liable for any spoofing attacks that originate from within your network and are sent out to the global Internet. What can you do to prevent spoofing attacks by your own employees?

Do not let packets with origin IP out of your network leave to the outside world.

(b) What can be done to prevent parties outside your network from sending your employees spoofed traffic that impersonates your own employees?

Do not let packets that come from the outside world with an origin IP inside your network enter.

6. John is a PhD student who wastes his time on Facebook. John's sympathetic professor decides to monitor John's internet connection and guide Facebook visit to Google Scholar. Which of the following approaches allows John's professor, who has full control over the local network, to help John? (Justify)

a. **Filtering outgoing IP connections**
b. **Dropping DNS responses to filtered sites**
c. **ARP poisoning**
d. **DNS hijacking**
e. **BGP hijacking**

a. This only prevents connections to the Facebook without guiding to the Scholar.
b. John needs to know Facebook's IP address to visit the site. This only prevents connections to the Facebook without guiding to the Scholar.
c. ARP poisoning is only for local networks. It doesn't work here.
d. DNS hijacking is the best approach to guide John.
e. BGP hijacking is only possible for ASs and internet middle nodes.

The best way to ensure that John doesn't stray from the research path is enforcing all a, b, and d option together.

Unfortunately, John is very stubborn and he still wants to visit Facebook. Which of the following approaches can help John to visit Facebook without getting caught? (Justify)

a. **IPSec in transport mode**
b. **IPSec in traffic mode**
c. **IPSec in tunnel mode**
d. **DNSSEC**
e. **DNS over HTTPS**

We will provide the answer to this question next week so that you have time to do this exercise after the lecture explaining VPNs.
(If you have done it and you can't wait for the answer, you can always drop an email)

7. You want to do man in the middle between a PhD at EPFL and the Amazon Cloud Services. Can you do it if (justify your answer)

(a) You are in the EPFL local network

(b) You are on the other side of Earth

(c) You are an Internet Service provider

a) Yes, you can use ARP poisoning to make the gateway believe that you are the PhD machine, and the PhD machine that you are the gateway.
b) Yes, you can use DNS poisoning on the resolver used by the PhD student to try to reroute the traffic between the student and Amazon through your server.
c) Yes, besides DNS poisoning, in this case you can also change the routing tables inside your / other ASs to re-route packets through your server (BGP hijacking).

8. University decides to retire the use of Gaspar accounts for authenticating to WiFi. They decide to register students MAC to give access to the WiFi and only 1Gb per month so that they study and not go on Facebook. What are the security implications of this decision?

Since MAC addresses have no impersonation you can:

Do impersonation, which leads to students stealing each other's allocated bytes.

Abuse resources: one student can create fake MACs to get access to more resources than those assigned to him/her.