Tentamen Network Security, 6 november 2015, 8:30-11:30

(tot 12:30 voor studenten met extra tijd)

Dit tentamen bestaat uit vijf opgaven. Wees duidelijk, en kort maar krachtig in je antwoorden. Je mag gewoon in het Nederlands antwoorden. Succes!

1. **(20 points)** Consider a switched ethernet network (all hosts connected through a single switch) with gateway 192.168.1.1/24 and additional hosts 192.168.1.2, 192.168.1.3, and 192.168.1.66. Assume the following MAC addresses for the computers in the network:

IP address	MAC address
192.168.1.1	11:11:11:11:11:11
192.168.1.2	22:22:22:22:22:22
192.168.1.3	33:33:33:33:33:33
192.168.1.66	66:66:66:66:66:66

   (a) Assume that each node has a "complete" ARP cache, i.e., each node knows the IP-address-MAC-address pairs of all other nodes. Write down all the entries in the ARP cache of 192.168.1.3

   (b) Assume that the attacker at IP address 192.168.1.66 runs an ARP spoofing attack to become a man in the middle between 192.168.1.1 and 192.168.1.2. Assume further that the attacker uses *ARP request spoofing* with the destination MAC address set as usual for ARP requests. What ARP request messages does the attacker have to send? Give destination IP and MAC address and source IP and MAC address for all packets.

   (c) What does the ARP cache of 192.168.1.3 look like after the attack?
   Note: The question is *not* about the ARP cache of one of the targets of the attack!

   (d) How could 192.168.1.2 have prevented the attack?

2. **(20 points)** Consider again the network from exercise 1. Assume that a new computer joins that network (by plugging in a cable and booting up). Assume that this new computer does not know anything about the network and attempts to learn the network configuration via DHCP.

   (a) What pieces of information does the new computer need to receive via DHCP so that the user can fire up a browser, enter `http://wikipedia.com` in the address bar and the website of `wikipedia.com` website actually loads?

   (b) Assume that an attacker with IP address 192.168.1.66 sets up a rogue DHCP server to become a man in the middle between the new computer and `wikipedia.com`. Which of the pieces of information from part a) could he modify to become a man in the middle? What information would he send? How would the attack proceed (if there are any further steps required)? Give all possibilities for an attack.

   (c) Why could a rogue-DHCP attack fail? What possibilities does an attacker have to increase the chances of success?

3. **(20 points)** For each of the following three different port scan types

   - connect scan,
   - SYN scan, and
   - idle scan

   answer the following questions:

(a) How does it work? What packets are being sent to probe whether the port is open, what answer packet(s) are expected if the port is open, what answer packet(s) are expected if it's closed?

(b) The scans are listed in increasing order of "stealthiness". Explain briefly why this is the case by explaining how a system administrator could notice those scans and attribute their origin.

4. **(20 points)** Consider the following iptables firewall script running on a laptop called `mylaptop`:

```
iptables -F
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

For each of the following tasks decide whether the firewall allows it or not. If the firewall does not allow it, give an iptables rule that enables it. In each part you can assume the presence of additional rules from the previous parts.
Note: The rules have to be *minimal* and must not allow anything beyond the required functionality; in particular something like `iptables -P INPUT ACCEPT` is not a valid solution.

(a) A web browser running on `mylaptop` tries to load the website at `https://www.google.com`.

(b) The user runs the `ping` utility on `mylaptop` to test whether the host `www.ru.nl` is reachable.

(c) A mail client on `mylaptop` retrieves e-mail from `post.science.ru.nl` through IMAPS (TCP port 993).

(d) Another computer (not the laptop with the firewall) uses the `ping` utility to test wether `mylaptop` is reachable.

(e) Somebody else from outside tries to connect to the SSH server running on port 22 of `mylaptop`.

5. **(20 points)** Consider a confidential e-mail being sent from a user A (using e-mail provider P_A) to another user B (using e-mail provider P_B). Consider the following independent cryptographic protections for this e-mail communication:

- **P1:** User A is in a WPA2-protected WiFi using pre-shared keys.
- **P2:** User A uses TLS to communicate with the SMTP server of P_A.
- **P3:** User B uses TLS to communicate with the IMAP server of P_B.
- **P4:** Provider P_A and P_B communicate through IPSec with encapsulated security payloads (ESP) in tunnel mode.
- **P5:** User A obtains B's PGP public key from `pgp.mit.edu` and then encrypts the e-mail using PGP with this public key.

Consider the following attacks against this e-mail communication:

- **A1:** An attacker, who is not in the WiFi network that A is in, sniffs the WiFi traffic near A to read the e-mail.
- **A2:** An attacker, who is in the WiFi network that A is in, sniffs the WiFi traffic to read the e-mail.
- **A3:** An attacker, who is in the same network that B is in, sniffs the network to read the e-mail.
- **A4:** An attacker (controlling an Internet router) sniffs the traffic between A and the SMTP server of P_A.
- **A5:** An attacker (controlling an Internet router) sniffs the traffic between P_A and P_B.
- **A6:** A's provider is reading and analyzing the e-mail.
- **A7:** B's provider is reading and analyzing the e-mail.

(a) Fill in a checkmark (✓) in each cell of the following table, if and only if the cryptographic protection alone is effective to prevent the attack:

	P1	**P2**	**P3**	**P4**	**P5**
A1					
A2					
A3					
A4					
A5					
A6					
A7					

Note: Don't forget to submit this sheet together with your exam or copy the table to your exam sheet.

(b) Can you think of an attack that would work against each of the protections (and any combination of those)?