Tentamen Network Security, 26 June 2017, 12:30-15:30

(tot 16:30 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)** Answer the following questions about ARP spoofing.

   (a) On a traditional Ethernet using a hub or on a wireless network an attacker can trivially read all traffic between two victim nodes A and B. Why might an attacker still want to use ARP spoofing to become a man in the middle between A and B in such a network?

   (b) Assume the following MAC and IP addresses for the hosts A and B and the attacker node O:

A	192.168.42.1	11:11:11:11:11:11
B	192.168.42.2	22:22:22:22:22:22
O	192.168.42.6	66:66:66:66:66:66

   Assume that O uses ARP-reply spoofing (i.e., standard ARP spoofing) to become a man in the middle between A and B. What ARP packets does O send? For each packet specify the ARP packet type, source IP and MAC address and destination IP and MAC address.

   (c) Now assume that instead of using ARP *reply* packets, the attacker O wants to use ARP request spoofing to become man in the middle between A and B. Again, specify what packets O will send. For each packet specify the ARP packet type, source IP and MAC address and destination IP and MAC address. For the destination MAC address assume the standard destination for ARP requests.

   (d) Assume that there is another node C with IP address 192.168.42.3 and MAC address 33:33:33:33:33:33 in the network. Does any of the two attacks from part b) or c) influence the ARP cache of C? If yes, explain which attack(s) and how it modifies the ARP cache of C.

2. **(20 points)** Consider the following iptables firewall script running on a server called `myserver`:

```
iptables -F
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p tcp --dport 587 -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

   The goal of this script is to allow clients to communicate with the HTTP/HTTPS server (running on ports 80 and 443), to allow SSH connections (on port 22), to act as a mail server (using SMTPS on port 587) and to allow clients to "ping" the computer (using ICMP echo request) to see whether it's up and running. However, the script does not achieve these goals.

   Note: In part a), b), and d) the `iptables` rules should be minimal; i.e., not allow more than what is strictly required to achieve the desired goal.

(a) Explain why connections to the webserver (HTTP and HTTPS), to the mail server, and to the SSH server will fail. Suggest `iptables` rules that fix this problem.

(b) Explain why "pinging" `myserver` will not provide any useful feedback. Suggest an `iptables` rule that fixes this problem.

(c) Can you think of a very small change to the original script that fixes all the above problems?

(d) SMTP(S) servers forward mail to the mail server of the recipient. There are multiple reasons why the mail server won't be able to deliver a mail to `someotherserver.nl` (also using SMTPS on port 587). List all of these reasons and suggest `iptables` rules that fix this problem.
Note: When answering this question, do not assume that the firewall script has been modified as you suggested in parts a), b), or c).

3. **(20 points)** Consider the following network with three hosts: `shaun` with IP address 192.168.42.1, `liz` with IP address 192.168.42.2 and `ed` with IP address 192.168.42.3. Host `ed` is not running any services, i.e. all ports on `ed` are closed.
Note: In this exercise, if some value (e.g., a port number) is not known or does not matter, replace it by variables X, Y, ...

(a) To find out whether TCP port 22 on `liz` is open, `shaun` runs a connect scan. Write down all packets (including IP source and destination address, TCP ports, and TCP flags) that are going over the network for this scan **if the port is closed**.

(b) Now write down what packets (again, including IP source and destination address, TCP ports, and TCP flags) go over the channel during the connect scan from part a) **if the port is open**.

(c) Now `shaun` is running an idle scan on `liz` using `ed` as a zombie host. Again the goal of `shaun` is to determine whether TCP port 22 on `liz` is open. Write down all packets (including IP source and destination address, IPIDs, TCP ports, and TCP flags) that are going over the network for this scan **if the port is closed**.

(d) Now write down what packets (again, including IP source and destination address, TCP ports, and TCP flags) go over the channel during the idle scan from part c) scan **if the port is open**.

(e) Now assume that `liz` is running a firewall that drops all incoming packets to closed ports, except if they belong to an established connection. Does the idle scan from parts c)/d) still work? Explain your answer.

(f) Finally assume that `ed` is running a firewall that drops all incoming packets to closed ports, except if they belong to an established connection. Does the idle scan from parts c)/d) still work? Explain your answer.

4. (**20 points**) A Tor user U connects through Tor nodes A (entry node), B (middle node), and C (exit node) to a server S. Assume that the user already has shared symmetric keys with all the servers; let those keys be K_A (shared key with node A), K_B (shared key with node B), and K_C (shared key with node C. Denote encryption of a message m with key K_i as $E_{K_i}(m)$.

(a) Given a "plaintext" packet m from U to S, what does U send to A?

(b) Given a "plaintext" return packet from S to U, what does S send to C?

(c) Using (at least) three Tor relays in a circuit is crucial for security. Consider a Tor user using only two relays (entry and exit node). Explain an attack that either of the two nodes could peform to break anonymity of this user, which is prevented by three-node circuits.

5. (**20 points**) Consider a network with a gateway at 192.168.42.1, a DNS cache at 192.168.42.2, and a couple of client computers that have a static network configuration (i.e., they are not configured using DHCP, they all use 192.168.42.1 as gateway and 192.168.42.2 as DNS server). Consider an attacker in this network with the goal to obtain banking data from client computers that connect to `http://www.ing.nl`; note that the `www.ing.nl` webserver will redirect this request to HTTPS.

   (a) Describe two different approaches how the attacker can achieve his goal. Each of these approaches must work if *any of the clients* connects to `http://www.ing.nl`. For each of the attacks describe in detail all steps that are involved.

   (b) For each of the two attacks from part a) describe why it might fail or what countermeasures clients, gateway or DNS server could use to prevent such an attack.