Tentamen Network Security, 3 november 2014, 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**) The following `iptables` script is written to only allow outgoing packets on TCP ports 80 and 443 (i.e., typically HTTP and HTTPS) and the corresponding replies, but block (`DROP`) all other traffic.

   ```
   iptables -F
   iptables -P INPUT DROP
   iptables -P FORWARD DROP
   iptables -P OUTPUT DROP
   iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
   iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
   iptables -A INPUT -p tcp --sport 80 -j ACCEPT
   iptables -A INPUT -p tcp --sport 443 -j ACCEPT
   ```

   Note: If you remember the `iptables` syntax, then please write the answers to parts b) and d) as an `iptables` script. If not, use pseudocode `iptables` syntax with a brief explanation to explain what the rules are supposed to accomplish.

   (a) Explain why the firewall rules do not accomplish what they are supposed to.

   (b) How do the firewall rules have to be changed to achieve the desired effect?

   (c) Why would those firewall rules not make much sense in most environments (think about how HTTP/HTTPS is typically used and what else is required to allow this typical usage).

   (d) Modify the rules such that typical use of HTTP and HTTPS is possible.

   (e) Explain in detail how you would, as an attacker, circumvent this firewall to transmit arbitrary traffic through the firewall.

2. (**20 points**) Assume that an attacker finds the following computers (IP addresses and MAC addresses) in a network:

`10.0.5.1`	`11:11:11:11:11:11`
`10.0.5.2`	`22:22:22:22:22:22`

   The attacker's computer has IP address `10.0.5.5` and MAC address `66:66:66:66:66:66`. The attacker's target is to launch a man-in-the-middle (MitM) attack against the communication between `10.0.5.1` and `10.0.5.2`.

   (a) Assume that `10.0.5.1` and `10.0.5.2` have been communicating over TCP/IP. What do their respective ARP-cache entries look like before any attack?

   (b) Explain what gratuitous ARP reply packets the attacker would send to the two targeted machines. For each packet specify source and destination IP address, source and destination MAC address.

(c) Explain what packets the attacker would send to achieve the same goal with *ARP request* packets. Again, list in detail what packets (with IP and MAC source and destination addresses) the attacker would send to the two target machines.

(d) What do the ARP cache-entries of `10.0.5.1` and `10.0.5.2` look like after the successful ARP-spoofing attack by `10.0.5.5`?

3. (**10 points**) Many operating systems increase the fragment identification number (IPID) for each IP packet they send. Explain how this can be used for an idle scan. Consider the case that `192.168.42.6` uses an idle scan to determine if port 22 on `192.168.42.2` is open or closed. Assume that the zombie host for this scan is `192.168.42.5`. Describe in detail what packets go over the network (with source and destination addresses and ports) during this scan,

   (a) if port 22 on `192.168.42.2` is open, and

   (b) if port 22 on `192.168.42.2` is closed.

4. (**10 points**) Assume that a firewall blocks all incoming and outgoing ICMP packets.

   (a) What kind of port scan is prevented by such a firewall rule? Explain why.

   (b) Explain why traceroute does not work through such a firewall.

5. (**40 points**) Consider the following situation: A machine called `mylaptop` boots up and requests network information via DHCP. From a DHCP server with address 192.168.42.3 it receives the following configuration:

   - IP address: 192.168.42.7
   - Netmask: 255.255.255.0
   - Gateway: 192.168.42.1
   - DNS Server: 192.168.42.4

   After having received this information and configured its network interface correspondingly, the user of `mylaptop` starts a web browser and enters `http://www.mybank.com` in the address bar. The webserver at `www.mybank.com` redirects this request to HTTPS; the browser loads the website over HTTPS, the user enters his username and password to log into his online banking account.

   An attacker is sitting in the same network at a computer with IP address `192.168.42.23`. His target is to obtain the user's username and password for online banking.

   (a) Describe **three different ways other than ARP spoofing** how the attacker can become a man in the middle (MitM) in the communication between `mylaptop` and `www.mybank.com`. For each of these attacks describe

   - how they work,
   - what the attacker needs to do (i.e., what packets he needs to send at what time with what information), and
   - why they may fail.

   Note: The target of the attacker is to be a MitM in *both directions* of the communication between `mylaptop` and `www.mybank.com`!

   (b) Describe what the attacker can do to obtain username and password, although the request to `http://www.mybank.com` is redirected to an HTTPS connection. Again, describe in detail how the attack works.