Exam Network Security, June 25, 2018, 12:30-14:30

(until 15:00 for students with extra time)

Be clear and concise in your answers. Je mag gewoon in het Nederlands antwoorden.

1. (**20 points**) Assume that an attacker has successfully used ARP spoofing to become a man in the middle in the communication between the following two computers:

   ```
   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`.

   (a) What do the ARP tables of the two victim nodes look like?

   (b) After the attack, the attacker wants to restore the victims' original ARP tables. What packets does the attacker need to send to achieve this? For each packet specify source and destination IP address, source and destination MAC address.

   (c) If ARP spoofing is not an option to become a man in the middle in a local-area network (for example because hosts are using static ARP tables), what other options does an attacker have? Name two different options.

2. (**20 points**) The `iptables` script below is written to run on a gateway computer that only forwards packets between two networks. The addresses in both networks are routed on the Internet, the gateway is thus *not* a NAT router. The firewall shall allow only web (HTTP and HTTPS) traffic and DNS in both directions.

   ```
   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 OUTPUT -p tcp --dport 53 -j ACCEPT
   iptables -A INPUT -p tcp --sport 80 -j ACCEPT
   iptables -A INPUT -p tcp --sport 443 -j ACCEPT
   iptables -A INPUT -p tcp --sport 53 -j ACCEPT
   ```

   (a) The above firewall rules to not accomplish their goal at all. Describe at least three different mistakes in these rules.

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

   (c) Explain in detail how you would, as an attacker, circumvent this firewall (i.e., the firewall *with* your proposed changes) to transmit arbitrary traffic through the firewall.

3. (**20 points**)

   (a) Explain the difference between a TCP connect scan and a SYN scan.

   (b) What are the reasons to prefer a TCP connect scan over a SYN scan?

   (c) What are the reasons to prefer a SYN scan over a TCP connect scan?

   (d) Explain why UDP ports scans are different from TCP port scans and how UDP port scans work.

4. (**24 points**) Consider a typical e-mail communication scenario:

   - Alice (`alice@herisp.com`) is sending an e-mail to Bob (`bob@zijnprovider.nl`).
   - Alice sends the e-mail through a gateway in her local-area-network over the Internet to the SMTP server of `herisp.com`.
   - The SMTP server of `herisp.com` sends the e-mail to the SMTP server of `zijnprovider.nl`.
   - The SMTP server of `zijnprovider.nl` sends the e-mail to the IMAP server of `zijnprovider.nl`.
   - Bob receives the e-mail through a gateway in his local-area-network over the Internet from the IMAP server of `zijnprovider.nl`.

   For each of the following network communication encryption scenarios

   - describe one attack against confidentiality of this e-mail communication that is prevented by the encryption, and
   - describe one attack against confidentiality of this e-mail communication that is *not* prevented by the encryption.

   For each of the attacks describe who the attacker is (in what network, with what capabilities). Assume that the attacker cannot break cryptographic protection.

   (a) Both Alice and Bob use a WPA2 encrypted link between their computers and the respective gateways of their local area networks.

   (b) The SMTP server of `herisp.com` uses IPSEC ESP in transport mode to communicate with the SMTP server of `zijnprovider.nl`.

   (c) Alice uses TLS to encrypt the communication to the SMTP server of `herisp.com` and Bob uses TLS encryption to receive the mail from `zijnprovider.nl`.

   (d) Alice obtains Bob's PGP public key from a keyserver and encrypts the e-mail with PGP to that public key.

5. (**8 points**) Consider again the standard e-mail communication scenario from exercise 4. Even with end-to-end encryption of the e-mail, an passive attacker listening on the network sees that Alice and Bob are communicating. Alice is considering to use Tor for her e-mail connections to prevent this kind of attack against confidentiality of traffic data. Is this a good idea? Explain your answer.

6. (**8 points**) DNS can be used for DDOS amplification, because DNS replies are larger (often a lot larger) than DNS requests. The same is true for HTTP; why is it much harder to use HTTP for DDOS amplification?