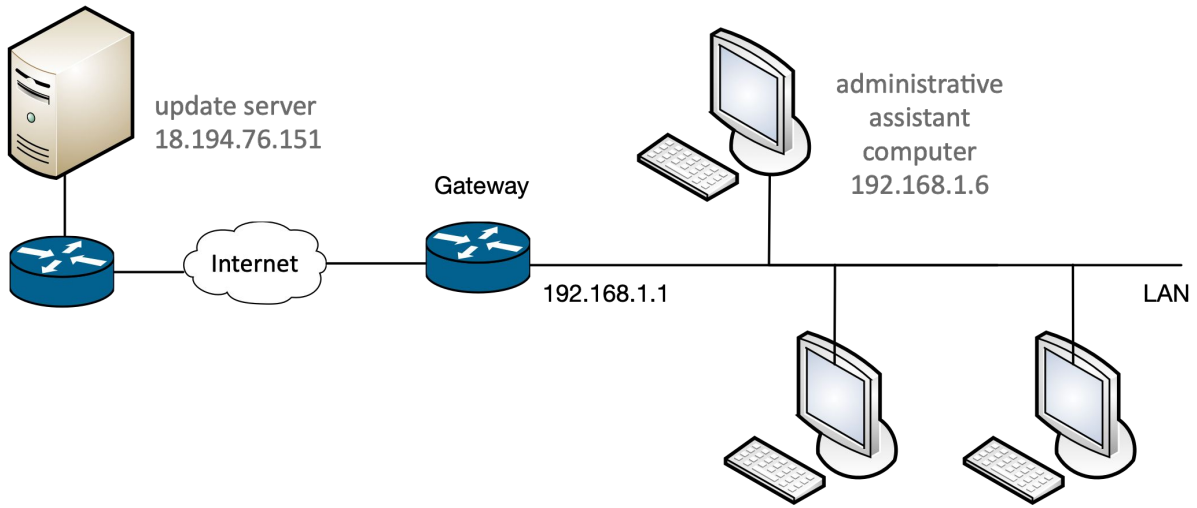
Exercises
Network Protocols Attacks

Computer Security

Question

As part of your job as a security analyst, one of your clients discovers that their network is compromised. In particular, from an early analysis, they have ground to suspect that the start of the compromise was a network attack against the computer of the administrative assistant.

Consider the following (simplified) schema of the company network.



1. Your client managed to capture the network traffic on the administrative assistant's computer (IP address *192.168.1.6* and MAC address *dc:a9:04:7a:ce:29*) when the attack was taking place. During the traffic capture, the computer was automatically updating a well-known accounting software from the software vendor's web server (IP address *18.194.76.151* and MAC address *dc:a6:03:01:02:fe*). You also know that the IP address of the LAN interface of the company's network gateway is *192.168.1.1*, and its MAC address is *b6:28:97:ca:b7:48*.

1 dc:a9:04:7a:ce:29 → ff:ff:ff:ff:ff:ff **ARP** *Who has 192.168.1.1? Tell 192.168.1.6*
2 38:60:77:b9:79:98 → dc:a9:04:7a:ce:29 **ARP** *192.168.1.1 is at 38:60:77:b9:79:98*
3 b6:28:97:ca:b7:48 → dc:a9:04:7a:ce:29 **ARP** *192.168.1.1 is at b6:28:97:ca:b7:48*
4 192.168.1.6 (dc:a9:04:7a:ce:29) → 18.194.76.151 (38:60:77:b9:79:98) **TCP** *SYN*
5 18.194.76.151 (38:60:77:b9:79:98) → 192.168.1.6 (dc:a9:04:7a:ce:29) **TCP** *SYN, ACK*
6 38:60:77:b9:79:98 → dc:a9:04:7a:ce:29 **ARP** *192.168.1.1 is at 38:60:77:b9:79:98*
7 192.168.1.6 (dc:a9:04:7a:ce:29) → 18.194.76.151 (38:60:77:b9:79:98) **TCP** *ACK*
8 38:60:77:b9:79:98 → dc:a9:04:7a:ce:29 **ARP** *192.168.1.1 is at 38:60:77:b9:79:98*
9 192.168.1.6 (dc:a9:04:7a:ce:29) → 18.194.76.151 (38:60:77:b9:79:98) **TCP** *HTTP GET /downloads/software-update.exe*
10 18.194.76.151 (38:60:77:b9:79:98) → 192.168.1.6 (dc:a9:04:7a:ce:29) **TCP** *HTTP 200 OK ...*

(assume that the traffic is captured directly from the network interface card of the employee's PC)

1.1 [2 points]. Describe the attack going on in the network, specifying the name and providing a short explanation of how the attack works *in general*.

1.1 [2 points]. Describe the attack going on in the network, specifying the name and providing a short explanation of how the attack works *in general*.

ARP spoofing, see slide.

1.2 [1 point]. What is the goal of the attack, in this specific case? Motivate your answer.

1.2 [1 point]. What is the goal of the attack, in this specific case? Motivate your answer.

Sniffing or manipulation of the traffic to\from the compromised machine. We can rule out DOS as the traffic passes (there are responses from the server).

Likely, given the scenario (malware infection), the attack is targeted at tampering with the data in transit rather than (or in addition to) sniffing.

1.3 [1 point]. Can you tell the IP address of the attacker? And the MAC address?

1.3 [1 point]. Can you tell the IP address of the attacker? And the MAC address?

IP address: no

MAC address: the attacker is using 38:60:77:b9:79:98, but it could very well be a spoofed address.

1.4 [1 point]. Given only the above packet capture, can you tell whether the attacker is located (i.e., on the LAN, on the same network of the web server, or on an arbitrary Internet-connected network)? Why?

1.4 [1 point]. Given only the above packet capture, can you tell whether the attacker is located (i.e., on the LAN, on the same network of the web server, or on an arbitrary Internet-connected network)? Why?

The attacker is located on the same network of the target machine, i.e., on the LAN.

Question

Suppose that you are the network security administrator of the network `131.168.0.0/24`, with gateway `131.168.0.1` and DNS servers `131.168.0.100` and `131.168.0.101`. While examining the network activity, you notice a DHCP offer packet coming from IP `131.168.0.10` with gateway set to `131.168.0.5`. Answer the following questions and provide a reason. Answers with no reason will not give any point.

- What kind of attack do you suspect, and how does it work?

- What kind of attack do you suspect, and how does it work?

DHCP poisoning. Someone is trying to trick a client connected to 131.168.0.0/24 into believing that `131.168.0.5` *is the gateway, by sending a crafted DHCP offer before, which comes before the real offer sent out by the real DHCP server.*

- Why such an attack works?

- Why such an attack works?

Because the DHCP protocol does not support authentication, so the client must blindly believe any DHCP offer that it sees, and because an arbitrary client can race (and win) against the real DHCP server.

- Can you tell the IP address of the host where those packets come from?

- Can you tell the IP address of the host where those packets come from?

Not really. 131.168.0.10 is the sender of the DHCP offer, but the address may be spoofed. We could look at the MAC address of the scender, but it could be spoofed as well.

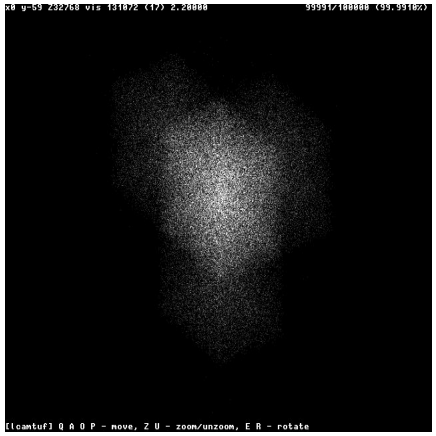
- Can you tell the IP address or network address of the victim?

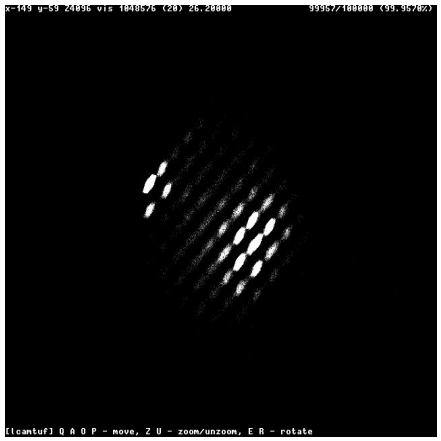
- Can you tell the IP address or network address of the victim?

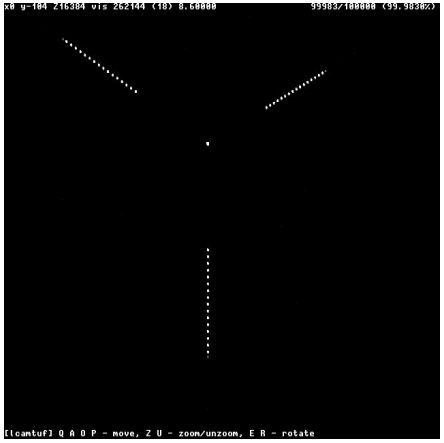
From the above information there is little evidence to say that, although the potential victims are those that will receive and accept the spoofed DHCP offers. So, likely, 131.168.0.0/24.

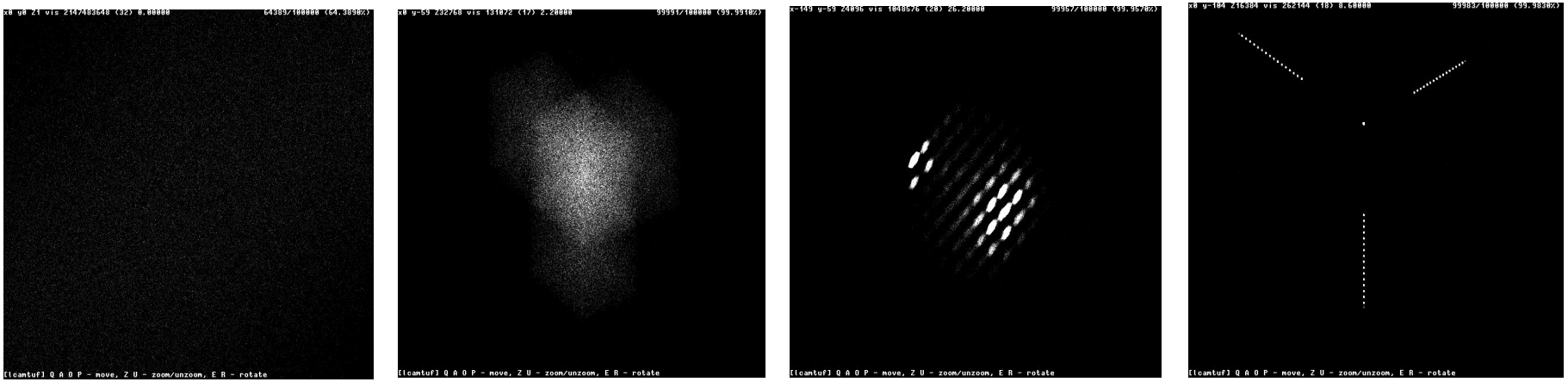
Question

- Explain why the Initial Sequence Number (ISN) in a TCP connection should be random.
- Which of the following TCP stacks is more vulnerable to the above attack, and why (in brief)?









1. If an attacker can guess the ISN value of a TCP connection, they can forge a response TCP packet that will be valid (because the acknowledgment of the ISN is correct). This means that the attacker can spoof a TCP connection, even if they are blind, i.e. not on the route of packets (MITM)

2. Bottom right is easiest, as only a few values are used and there's no uniform spreading in the space

Ref: https://www.ietf.org/rfc/rfc1948.txt

Question

A network analyst is analyzing some traffic captured from a network belonging to Politecnico di Milano. The network is: 131.175.0.0/16. In particular, we suspect that a database server, whose IP address is 131.175.14.12, is victim of an attack. Indeed, observing the network traffic, we notice the following pattern:

131.175.14.12 → 131.175.255.255 (broadcast) [ICMP] Echo (ping) request

131.175.0.2 → 131.175.14.12 [ICMP] Echo (ping) reply

7a:ce:29 → ff:ff:ff (broadcast) Tell 131.175.0.2 [ARP] Who has 131.175.14.12?

4b:74:28 → 7a:ce:29 [ARP] 131.175.14.12 is at 4b:74:28

131.175.0.3 → 131.175.14.12 [ICMP] Echo (ping) reply

131.175.0.4 → 131.175.14.12 [ICMP] Echo (ping) reply

⋮

131.175.255.251 → 131.175.14.12 [ICMP] Echo (ping) reply

131.175.255.252 → 131.175.14.12 [ICMP] Echo (ping) reply

131.175.255.253 → 131.175.14.12 [ICMP] Echo (ping) reply

1. [2 point] Describe what attack you think is going on, and what is the feature (or lack thereof) of the involved protocol(s) that enable this attack.

1. [2 point] Describe what attack you think is going on, and what is the feature (or lack thereof) of the involved protocol(s) that enable this attack.

PING Smurf - see slides ....

Authentication

2. [2 point] Describe what you think is the **concrete** goal(s) of the attack in this scenario

2. [2 point] Describe what you think is the **concrete** goal(s) of the attack in this scenario

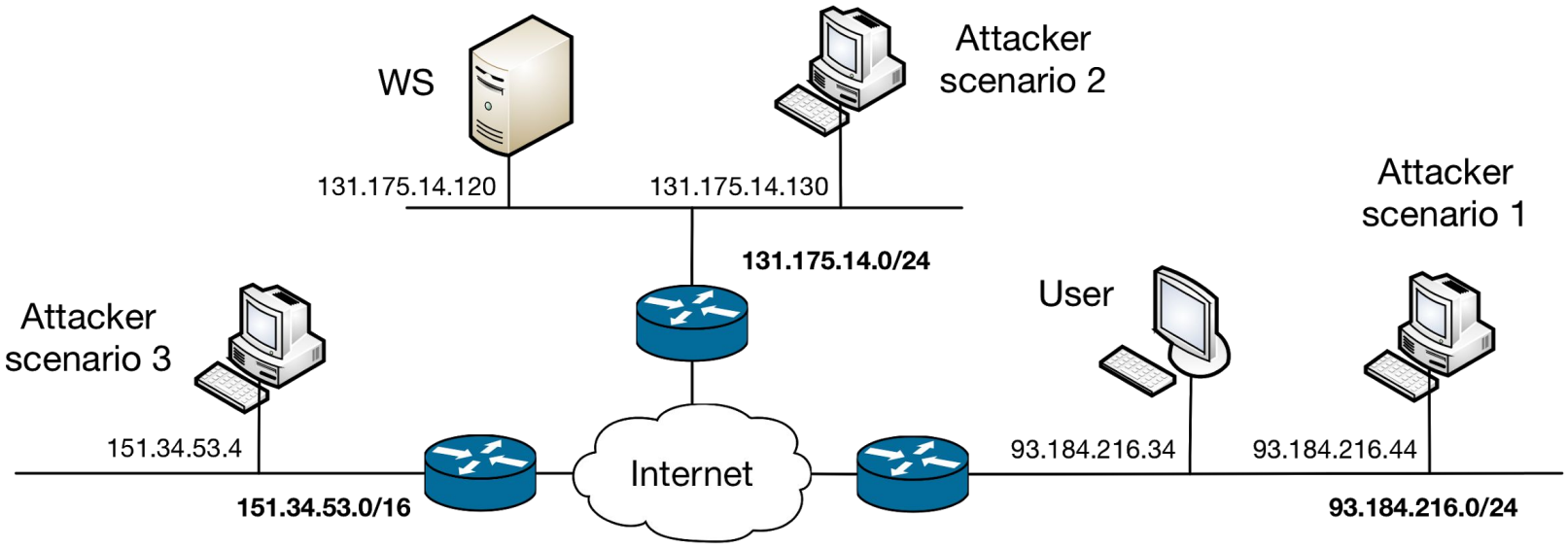
The goal is to saturate the resources of the victim using other machines on the network as an amplification mean. This results in a denial of service.

3. [1 point] Can you tell the IP and MAC address of the attacker? Why?

3. [1 point] Can you tell the IP and MAC address of the attacker? Why?

No, the IP address is spoofed for sure, and the MAC address can be spoofed as well.

Consider the following network diagram:



A user, with IP address 93.184.216.34, is attempting to download a software executable from a webserver in the Politecnico di Milano network, http://downloads.polimi.it, with IP address 131.175.14.120, over the HTTP protocol (no HTTPS, no signatures, nothing). Assume that the user's browser already cached the IP address of downloads.polimi.it (i.e., it does not perform any DNS request), and that there is no firewall involved. An attacker, who knows that the user is about to download this software, wants to target our user by carrying out an attack to replace the downloaded software with a piece of malware.

For each of the following attack scenarios, state whether the attacker is able to fulfill his\her goals. If you deem it possible, describe an attack that allows to do so: state the name of the class of attacks, and describe all the steps needed to make it work in this specific scenarios. If multiple classes of attacks are possible, focus on the simplest one that gets the job done. If no attack is possible, please explain why.

Scenario 1 (attacker: 93.184.216.44; same network and broadcast domain of the user):
Scenario 2 (attacker: 131.175.14.130; same network of web server, but different than user):
Scenario 3 (attacker: 151.34.53.4; attacker, user and webserver on three different networks):

For each of the following attack scenarios, state whether the attacker is able to fulfill his\her goals. If you deem it possible, describe an attack that allows to do so: state the name of the class of attacks, and describe all the steps needed to make it work in this specific scenarios. If multiple classes of attacks are possible, focus on the simplest one that gets the job done. If no attack is possible, please explain why.

Scenario 1 (attacker: 93.184.216.44; same network and broadcast domain of the user):

ARP spoofing ...

Scenario 2 (attacker: 131.175.14.130; same network of web server, but different than user):

Scenario 3 (attacker: 151.34.53.4; attacker, user and webserver on three different networks):

For each of the following attack scenarios, state whether the attacker is able to fulfill his\her goals. If you deem it possible, describe an attack that allows to do so: state the name of the class of attacks, and describe all the steps needed to make it work in this specific scenarios. If multiple classes of attacks are possible, focus on the simplest one that gets the job done. If no attack is possible, please explain why.

Scenario 1 (attacker: 93.184.216.44; same network and broadcast domain of the user):

ARP spoofing ...

Scenario 2 (attacker: 131.175.14.130; same network of web server, but different than user):

ARP spoofing ... (same as before but this time target the server)

Scenario 3 (attacker: 151.34.53.4; attacker, user and webserver on three different networks):

For each of the following attack scenarios, state whether the attacker is able to fulfill his\her goals. If you deem it possible, describe an attack that allows to do so: state the name of the class of attacks, and describe all the steps needed to make it work in this specific scenarios. If multiple classes of attacks are possible, focus on the simplest one that gets the job done. If no attack is possible, please explain why.

Scenario 1 (attacker: 93.184.216.44; same network and broadcast domain of the user):

ARP spoofing ...

Scenario 2 (attacker: 131.175.14.130; same network of web server, but different than user):

ARP spoofing ... (same as before but this time target the server)

Scenario 3 (attacker: 151.34.53.4; attacker, user and webserver on three different networks):

No attack possible, because HTTP uses TCP and, if sequence numbers are correctly implemented, not possible to perform TCP hijacking. Also, DNS poisoning not possible as DNS response already cached.

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

2. [2 points]. Describe the security issue with the proposed ISN implementation, and propose a way to solve the issue

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

2. [2 points]. Describe the security issue with the proposed ISN implementation, and propose a way to solve the issue

Can predict ISN -> solve by using random ISN

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

3. [2 points]. Describe how the attacker can perform the above attack, this time *exploiting the security issues raised by the custom ISN implementation*. Describe all the steps and assumptions that you need to perform this attack.

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

3. [2 points]. Describe how the attacker can perform the above attack, this time *exploiting the security issues raised by the custom ISN implementation*. Describe all the steps and assumptions that you need to perform this attack.

TCP hijacking. We can guess the ISN of the SYN packet sent by the victim (the user), we can spoof the webserver IP and send a "correct" SYN+ACK to it and, if we can guess the content of the request (we do), subsequent packets. This way we can send a different payload. In parallel we can also use TCP hijacking to send a fake RST to the actual server spoofing the user's IP address.
Problem\assumption: we need to know the ephemeral port used by the client to initiate the connection.

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

4. [1 points]. Assume you are the network security administrator of the network of the attacker (in the scenario 3 and assuming the custom TCP initial sequence number implementation), and that you control the border router between the network 151.34.53.0/24 and the rest of the Internet. Propose a way to prevent the attack. Can the administrator of the other two border routers in the diagram deploy the same mitigation, and obtain the same result? Why?

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

4. [1 points]. Assume you are the network security administrator of the network of the attacker (in the scenario 3 and assuming the custom TCP initial sequence number implementation), and that you control the border router between the network 151.34.53.0/24 and the rest of the Internet. Propose a way to prevent the attack. Can the administrator of the other two border routers in the diagram deploy the same mitigation, and obtain the same result? Why?

We can filter the packets with source IPs not belonging to our network. Other routers can't do this, they can only filter out packets coming from "outside" with spoofed IPs belonging to their network, but it's of little use in this scenario.

The End