Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Networked Systems
ETH Zürich — seit 2015

Communication Networks

Prof. Laurent Vanbever

Solution: Exercise 9 – Applications: DNS, HTTP & Email

9.1 Curious students

Consider that ITET has a local DNS server serving the DNS requests for all students' devices connected in the department. How could you determine if an external website has been visited recently by a fellow colleague of yours? Explain.

Solution: You can simply use dig to issue a query for any external website you're interested in and observe the response time. If the external website has been visited recently, the response time should be close to immediate (as the local DNS server is located close by). If not, the response time will be slower as the local DNS server would have to initiate a new remote query.

You could also look at the TTL value returned by the local server and compare it to the TTL you get when querying directly the authoritative DNS server for that domain. If the TTL returned by the local server is lower than the one from the authoritative DNS server, you know that the entry has been cached by the local server and hence, someone has visited the website recently.

9.2 HTTP host header

Perform a DNS lookup for `google.ch` and open `http://216.58.198.3` in your browser. What do you observe?

Now try to repeat the same process for `nsg.ee.ethz.ch` and `comm-net.ethz.ch`. Open the websites in your browser using the IP(s) from the DNS lookup. Do you see the expected websites?

Normally, one machine can host multiple websites at the same time. To distinguish which website has to be provided by the server, clients can add a so called "host header" in their HTTP request which specifies the website they want to access. You can try that yourself with the two websites from above. For example with the following commands:

```
telnet comm-net.ethz.ch 80

GET / HTTP/1.1
Host: comm-net.ethz.ch
```

Do you see another way how you could host multiple websites on the same machine? Can you see potential problems with this approach compared to the host header?

Solution: You could assign the server multiple IP addresses and link each IP address to a single website. The biggest drawback of this solution is the need for multiple IP addresses. IPv4 addresses are limited and hence expensive.

9.3 E-mail

Answer the following questions about e-mail with True or False and justify your choice.

a) SMTP and IMAP can be used to forward e-mails from one e-mail server to another one.

Solution: False, the Simple Mail Transfer Protocol (SMTP) is mainly used to forward e-mails from the e-mail client to the server or between servers. The Internet Message Access Protocol (IMAP) is one possible protocol for the client to retrieve e-mails from the server.

b) Looking at the header of a received e-mail, you can reconstruct through which e-mail servers the message was forwarded.

Solution: True, every e-mail server adds a received entry to the header.

c) IMAP is the encrypted counter-part of POP.

Solution: False, IMAP is like POP a protocol for a client to retrieve e-mails from the server. IMAP has more features than POP. For example, it allows to download e-mails partially and to connect multiple clients to the same mailbox.

d) It is not possible to verify that the e-mail was actually sent by the given FROM address.

Solution: True, no checks are performed to verify that the sender is authorized to send e-mails on behalf of that address.

e) The IP address of the mail server of a domain can be found by issuing a DNS query asking for the A record of that domain.

Solution: False, a mail server is identified using a DNS query asking for MX records (e.g., `dig MX ethz.ch`).

f) Images attached to an e-mail are transformed to text for transmission.

Solution: True, as e-mail relies on 7-bit U.S. ASCII, all non-English text and binary files have to be encoded in 7-bit U.S. ASCII. For this purpose MIME is used.

9.4 E-Mail analysis (Exam Style Question)

You received an email with the raw content shown in Figure 1.

a) According to Figure 1, what are the e-mail addresses of the sender and the receiver of this message?

Solution:

- Sender: john.doe@anonymous.ch
- Receiver: lvanbever@ethz.ch

```
Received: from edge20.ethz.ch (82.130.99.26) by CAS10.d.ethz.ch
 (172.31.38.210) with SMTP Server (TLS) id 14.3.408.0; Thu, 2 Aug
 2018 11:17:27 +0200
Received: from phil2.ethz.ch (129.132.65.3) by edge20.ethz.ch (82.130.99.26)
 with SMTP Server id 14.3.408.0; Thu, 2 Aug 2018 11:17:23 +0200
Received: from filter.spam.ch ([5.152.185.154]  helo=filter.spam.ch)
 by phil2.ethz.ch with esmtps  (TLSv1:AES128-SHA:128)   (Exim 4.69)
 (envelope-from <john.doe@anonymous.ch>)        id  1fl9jO-0004C9-7T
 for lvanbever@ethz.ch; Thu, 02 Aug 2018 11:17:15 +0200
X-Note: This Email was scanned by filter.spam.ch
Received: by filter.spam.ch with PIPE id
 93122453; Thu, 02 Aug 2018 11:17:13 +0200
Received: from [10.40.0.131] (HELO smtp.ch.exg7.mailhost.com)  by
 filter.spam.ch with ESMTPS id 93122443
 for lvanbever@ethz.ch; Thu, 02 Aug 2018 11:17:10 +0200
Received: from exg7.mailhost.local (192.168.40.105) by
 exg7.mailhost.local (192.168.40.107) with SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1531.3; Thu, 2 Aug 2018 11:17:09 +0200
From: Anonymous Student <john.doe@anonymous.ch>
To: Laurent Vanbever <lvanbever@ethz.ch>
Subject: Exam solutions
Date: Thu, 2 Aug 2018 09:17:09 +0000
Message-ID: <11A5442F-4D6E-436F-A873-2E3DA3656C06@anonymous.ch>
Accept-Language: de-CH, en-US
Content-Language: en-US
Content-Type: text/plain; charset="us-ascii"
Content-ID: <F43C7219ADA84040984B4640587C2B70@fwd7.mailhost.com>
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0

Hey, can you give me the solutions for the exam?
```

Raw content of a received email

b) List the IP addresses of all servers that have seen this email according to Figure 1 in chronological order starting with the server that saw the email *first*.

Solution:

- 192.168.40.105 (exg7.mailhost.local)
- 192.168.40.107 (exg7.mailhost.local)
- 10.40.0.131 (smtp.ch.exg7.mailhost.com)
- 5.152.185.154 (filter.spam.ch)
- 129.132.65.3 (phil2.ethz.ch)
- 82.130.99.26 (edge20.ethz.ch)
- 172.31.38.210 (CAS10.d.ethz.ch)

c) According to the header in Figure 1, the email passed a spam filter (`filter.spam.ch`). Could one of the other servers have added this entry without the email actually passing `filter.spam.ch`? If yes: why and which server(s) could have done it? If no: why not?

Solution: Yes other servers could have added the entry as the header is not authenticated. All the servers that see the email after `smtp.ch.exg7.mailhost.com` can add the entry (i.e. `phil2.ethz.ch`, `edge20.ethz.ch`, `CAS10.d.ethz.ch`)

d) Which servers (according to Figure 1) could modify the email message ("Hey, ..."))? Why?

Solution: All of the servers could have modified the message as it is not encrypted or signed.

e) Assume you have `telnet` access to an open SMTP server that does not appear in Figure 1 and you want to fake the email shown in Figure 1. That is, your goal is that the receiver of the email in Figure 1 receives the same email again (with the same sender). Which parts of the email in Figure 1 can you replicate in your email and which parts will be different? Use the line numbers in Figure 1 to list parts that are equal or different in your email and briefly explain the reasons why they are equal or different.

Solution: You can replicate everything from line 20 and below but not the headers because one cannot influence where the server will send the email next to.