Week 3

Session 1

Email

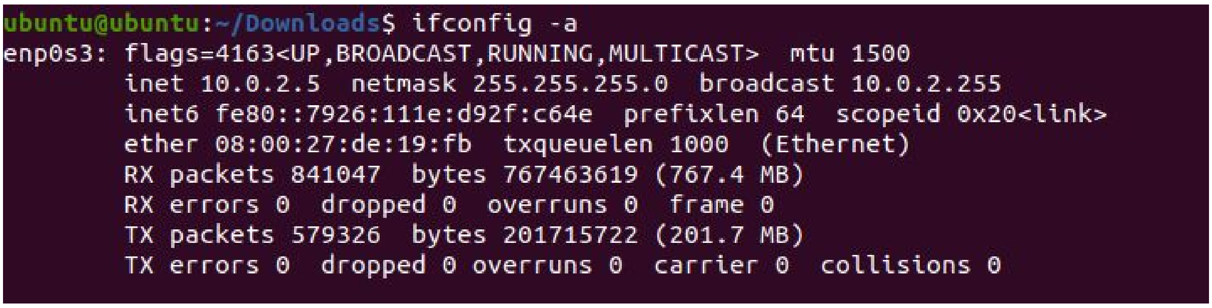
Olga Chernukhina

Register your local domains in both of your clients as of following in both of your machine's hosts file:

```
<ip of your machine1 interface>        innopolis.local

<ip of your machine2 interface>        innopolis.domain
```

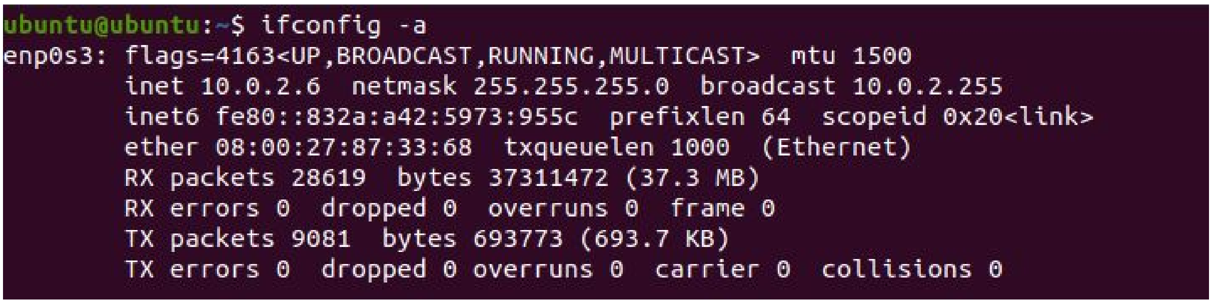
First, I checked the IP on each machine using `ifconfig -a`

Client 1



```
ubuntu@ubuntu:~/Downloads$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::7926:111e:d92f:c64e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:de:19:fb  txqueuelen 1000  (Ethernet)
        RX packets 841047  bytes 767463619 (767.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 579326  bytes 201715722 (201.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

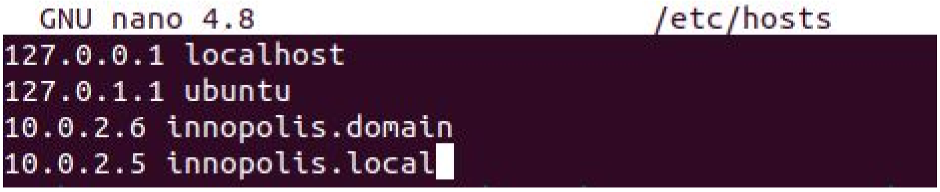
Client 2



```
ubuntu@ubuntu:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.6  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::832a:a42:5973:955c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:87:33:68  txqueuelen 1000  (Ethernet)
        RX packets 28619  bytes 37311472 (37.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9081  bytes 693773 (693.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

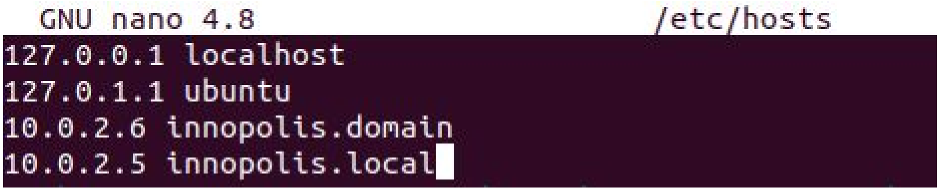
Then modified the file `/etc/hosts`

Client 1



```
  GNU nano 4.8                    /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu
10.0.2.6 innopolis.domain
10.0.2.5 innopolis.local
```

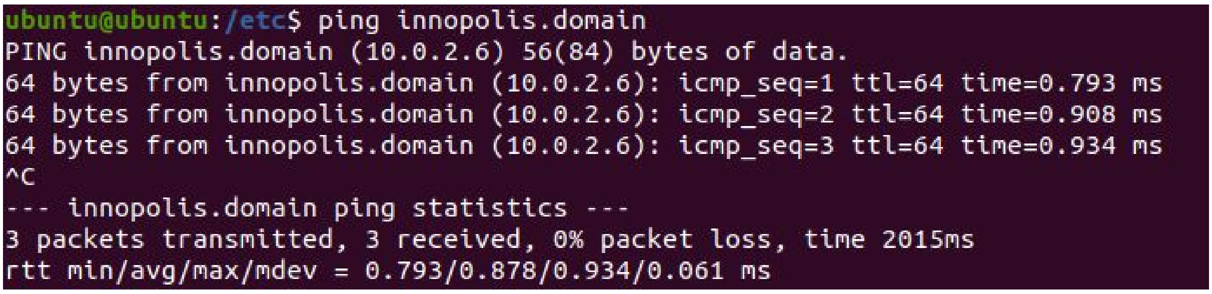
Client 2



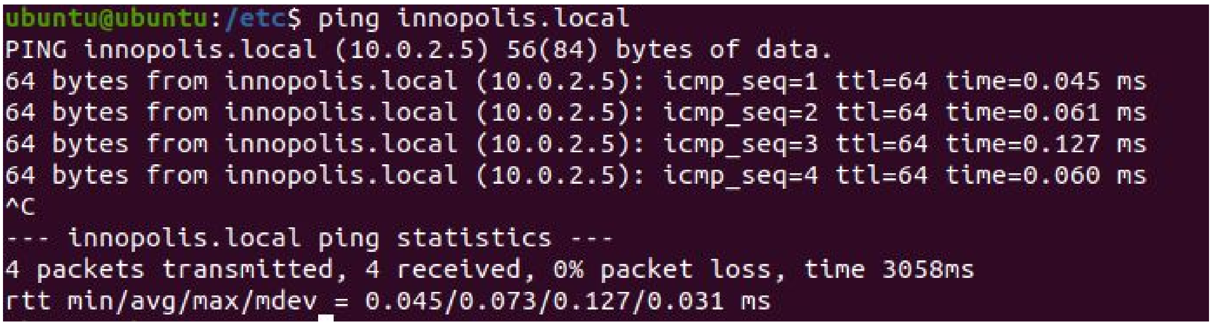
```
  GNU nano 4.8                    /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu
10.0.2.6 innopolis.domain
10.0.2.5 innopolis.local
```

You should be able to ping both domains from both machines

Client 1

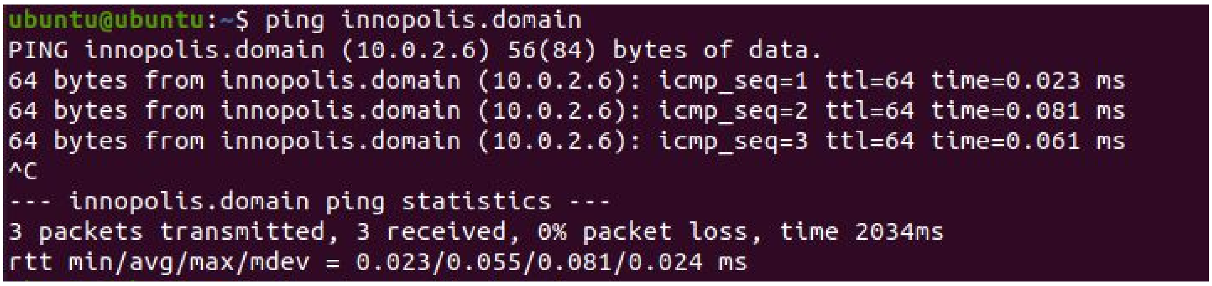


```
ubuntu@ubuntu:/etc$ ping innopolis.domain
PING innopolis.domain (10.0.2.6) 56(84) bytes of data.
64 bytes from innopolis.domain (10.0.2.6): icmp_seq=1 ttl=64 time=0.793 ms
64 bytes from innopolis.domain (10.0.2.6): icmp_seq=2 ttl=64 time=0.908 ms
64 bytes from innopolis.domain (10.0.2.6): icmp_seq=3 ttl=64 time=0.934 ms
^C
--- innopolis.domain ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2015ms
rtt min/avg/max/mdev = 0.793/0.878/0.934/0.061 ms
```

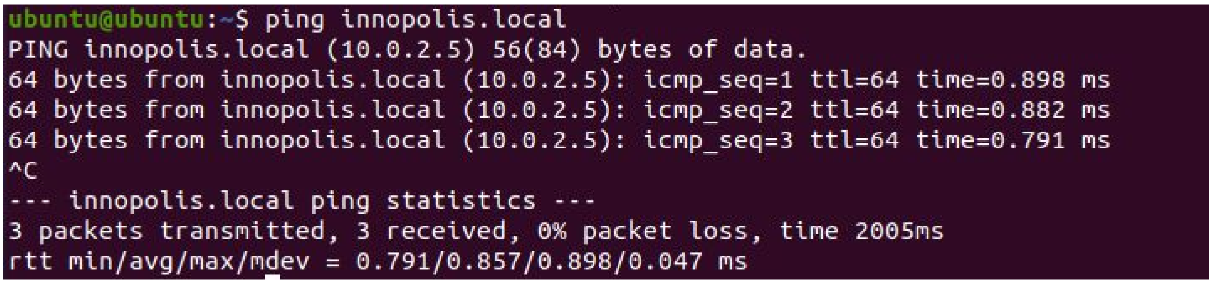


```
ubuntu@ubuntu:/etc$ ping innopolis.local
PING innopolis.local (10.0.2.5) 56(84) bytes of data.
64 bytes from innopolis.local (10.0.2.5): icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from innopolis.local (10.0.2.5): icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from innopolis.local (10.0.2.5): icmp_seq=3 ttl=64 time=0.127 ms
64 bytes from innopolis.local (10.0.2.5): icmp_seq=4 ttl=64 time=0.060 ms
^C
--- innopolis.local ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.045/0.073/0.127/0.031 ms
```

Client 2



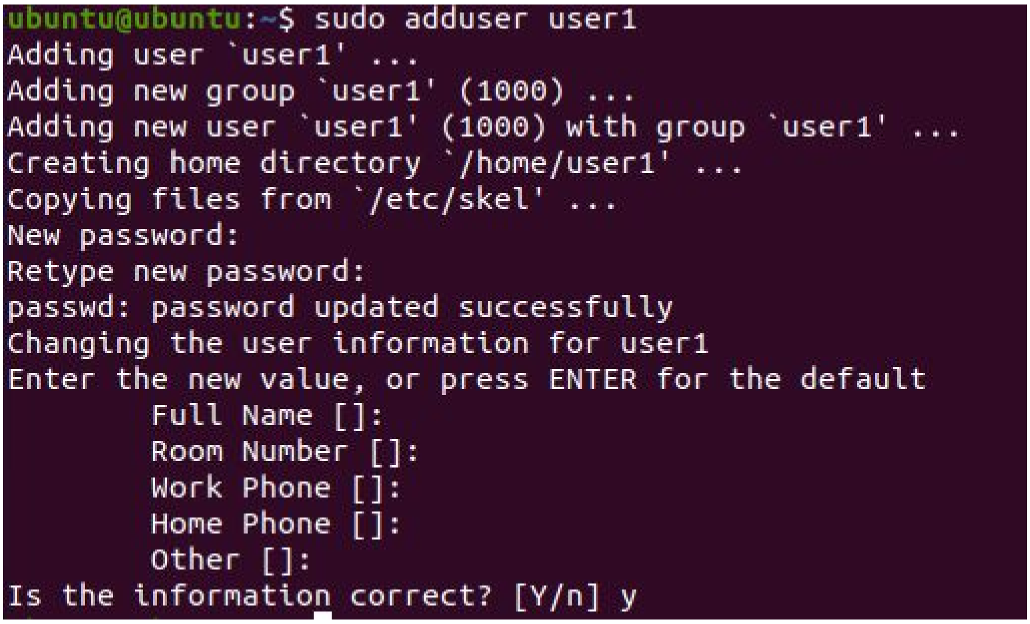
```
ubuntu@ubuntu:~$ ping innopolis.domain
PING innopolis.domain (10.0.2.6) 56(84) bytes of data.
64 bytes from innopolis.domain (10.0.2.6): icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from innopolis.domain (10.0.2.6): icmp_seq=2 ttl=64 time=0.081 ms
64 bytes from innopolis.domain (10.0.2.6): icmp_seq=3 ttl=64 time=0.061 ms
^C
--- innopolis.domain ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.023/0.055/0.081/0.024 ms
```



```
ubuntu@ubuntu:~$ ping innopolis.local
PING innopolis.local (10.0.2.5) 56(84) bytes of data.
64 bytes from innopolis.local (10.0.2.5): icmp_seq=1 ttl=64 time=0.898 ms
64 bytes from innopolis.local (10.0.2.5): icmp_seq=2 ttl=64 time=0.882 ms
64 bytes from innopolis.local (10.0.2.5): icmp_seq=3 ttl=64 time=0.791 ms
^C
--- innopolis.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.791/0.857/0.898/0.047 ms
```

Create account user1 on innopolis.local machine and account user2 on innopolis.domain machine.

1. I added users without root privileges on both machines - **user1 on Client 1 and user2 on Client 2**



```
ubuntu@ubuntu:~$ sudo adduser user1
Adding user `user1' ...
Adding new group `user1' (1000) ...
Adding new user `user1' (1000) with group `user1' ...
Creating home directory `/home/user1' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user1
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

2. I added those users to the file `/etc/sudoers` to enable root privileges for them:
   `user1 ALL=(ALL) ALL`

   The same for user2.

Install Postfix on both of you machines and configure each of them to represent one specific domain.

On both machines:

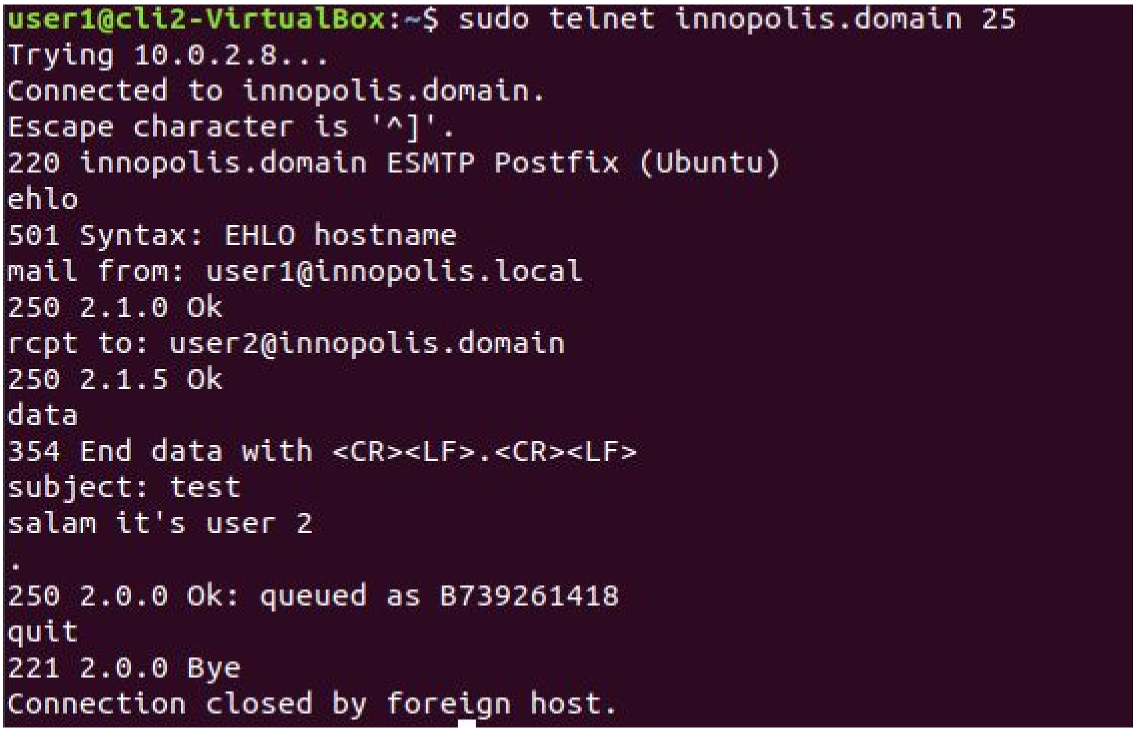
```
sudo apt-get install postfix
sudo dpkg-reconfigure postfix
```

For the configuration I used the following parameters:

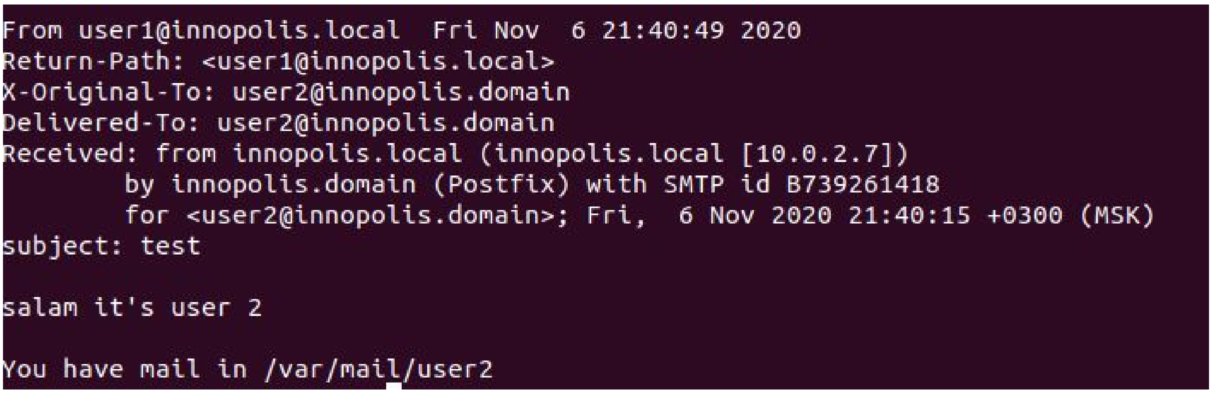
- **General type of mail configuration**: Internet Site
- **System mail name**: innopolis.local (for user2 innopolis.domain)
- **Root and postmaster mail recipient**: user1 (or user2)
- **Other destinations to accept mail for**: cli2-VirtualBox, innopolis.local (or innopolis.domain), localhost, localhost.localdomain
- **Force synchronous updates on mail queue**: No
- **Local networks**: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
- **Mailbox size limit**: 0
- **Local address extension character**: +
- **Internet protocols to use**: all

Send an email from them to each other and show the emails with their headers.

From user1 to user2:

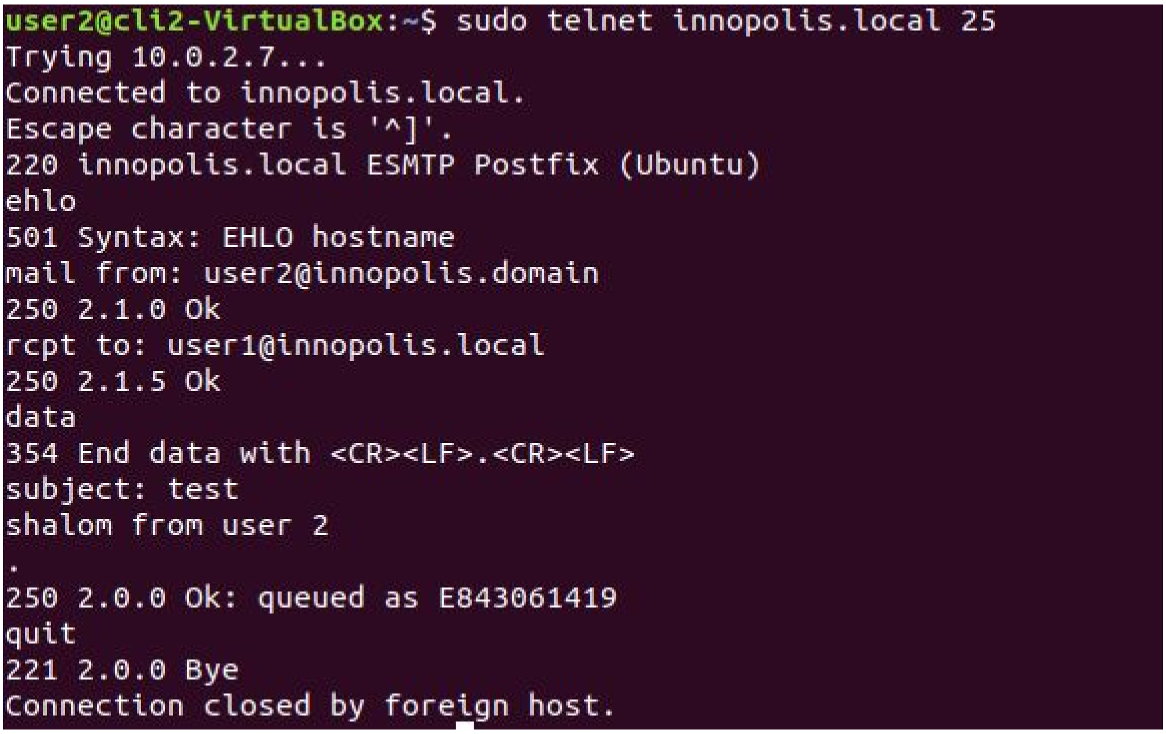


```
user1@cli2-VirtualBox:~$ sudo telnet innopolis.domain 25
Trying 10.0.2.8...
Connected to innopolis.domain.
Escape character is '^]'.
220 innopolis.domain ESMTP Postfix (Ubuntu)
ehlo
501 Syntax: EHLO hostname
mail from: user1@innopolis.local
250 2.1.0 Ok
rcpt to: user2@innopolis.domain
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: test
salam it's user 2
.
250 2.0.0 Ok: queued as B739261418
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

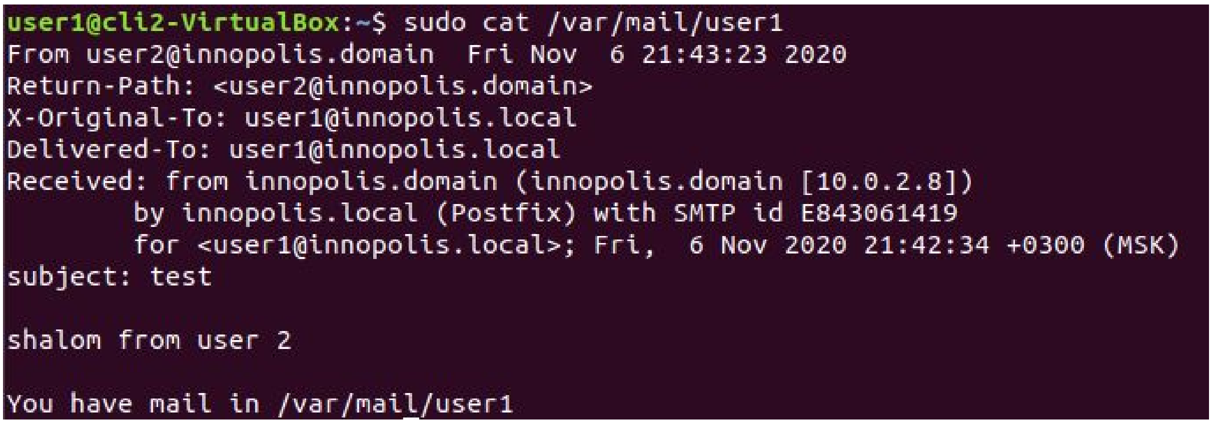


```
From user1@innopolis.local  Fri Nov  6 21:40:49 2020
Return-Path: <user1@innopolis.local>
X-Original-To: user2@innopolis.domain
Delivered-To: user2@innopolis.domain
Received: from innopolis.local (innopolis.local [10.0.2.7])
        by innopolis.domain (Postfix) with SMTP id B739261418
        for <user2@innopolis.domain>; Fri,  6 Nov 2020 21:40:15 +0300 (MSK)
subject: test

salam it's user 2

You have mail in /var/mail/user2
```

From user2 to user1:



```
user2@cli2-VirtualBox:~$ sudo telnet innopolis.local 25
Trying 10.0.2.7...
Connected to innopolis.local.
Escape character is '^]'.
220 innopolis.local ESMTP Postfix (Ubuntu)
ehlo
501 Syntax: EHLO hostname
mail from: user2@innopolis.domain
250 2.1.0 Ok
rcpt to: user1@innopolis.local
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: test
shalom from user 2
.
250 2.0.0 Ok: queued as E843061419
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

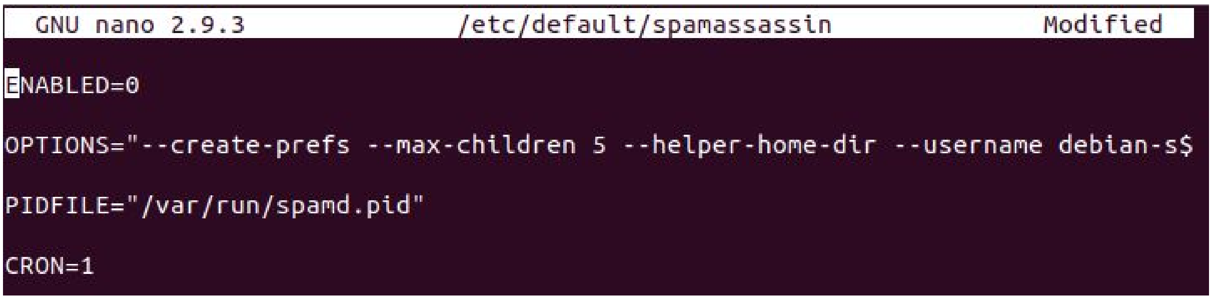


```
user1@cli2-VirtualBox:~$ sudo cat /var/mail/user1
From user2@innopolis.domain  Fri Nov  6 21:43:23 2020
Return-Path: <user2@innopolis.domain>
X-Original-To: user1@innopolis.local
Delivered-To: user1@innopolis.local
Received: from innopolis.domain (innopolis.domain [10.0.2.8])
        by innopolis.local (Postfix) with SMTP id E843061419
        for <user1@innopolis.local>; Fri,  6 Nov 2020 21:42:34 +0300 (MSK)
subject: test

shalom from user 2

You have mail in /var/mail/user1
```

Install spam assasin on both mail servers and configure them to use spam assasin.

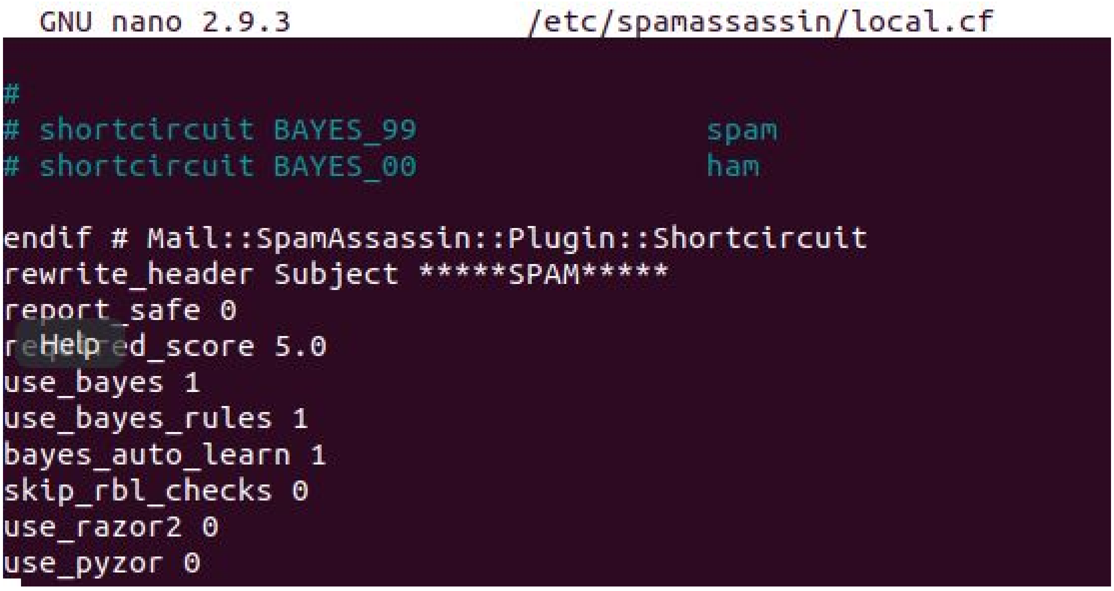
On both machines run
`sudo apt-get install spamassassin spamc`

In the file `/etc/default/spamassassin` make the following modifications:



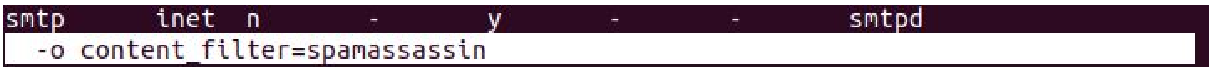
```
  GNU nano 2.9.3              /etc/default/spamassassin              Modified

ENABLED=0

OPTIONS="--create-prefs --max-children 5 --helper-home-dir --username debian-s$

PIDFILE="/var/run/spamd.pid"

CRON=1
```

In the file `/etc/spamassassin/local.cf` add:



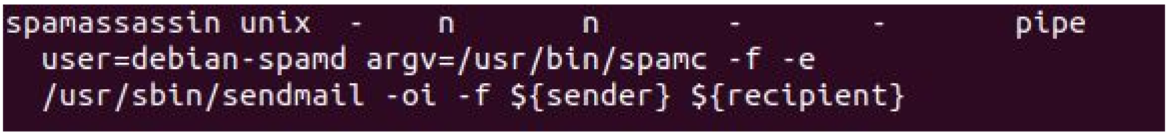
```
  GNU nano 2.9.3              /etc/spamassassin/local.cf

#
# shortcircuit BAYES_99                    spam
# shortcircuit BAYES_00                    ham

endif # Mail::SpamAssassin::Plugin::Shortcircuit
rewrite_header Subject *****SPAM*****
report_safe 0
required_score 5.0
use_bayes 1
use_bayes_rules 1
bayes_auto_learn 1
skip_rbl_checks 0
use_razor2 0
use_pyzor 0
```

In the file `/etc/postfix/master.cf` at the beginning add



```
smtp      inet  n       -       y       -       -       smtpd
  -o content_filter=spamassassin
```

at the end add



```
spamassassin unix  -     n       n       -       -       pipe
  user=debian-spamd argv=/usr/bin/spamc -f -e
  /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

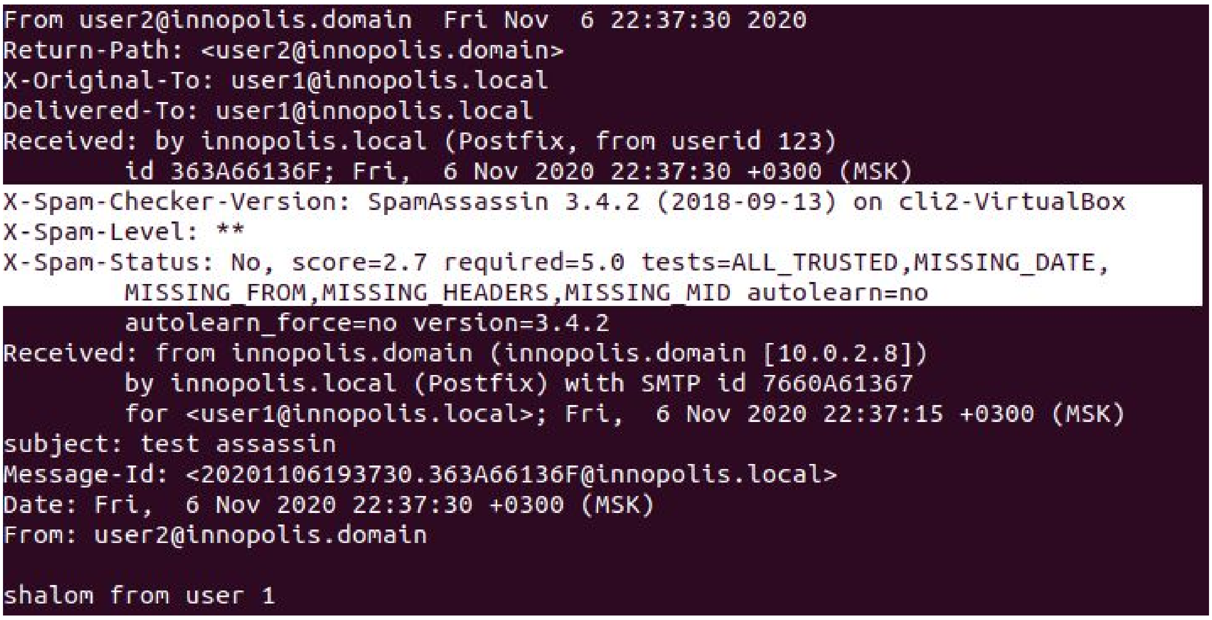
Then start assassin by `sudo /etc/init.d/spamassasin start`

Restart postfix by `sudo systemctl restart postfix`

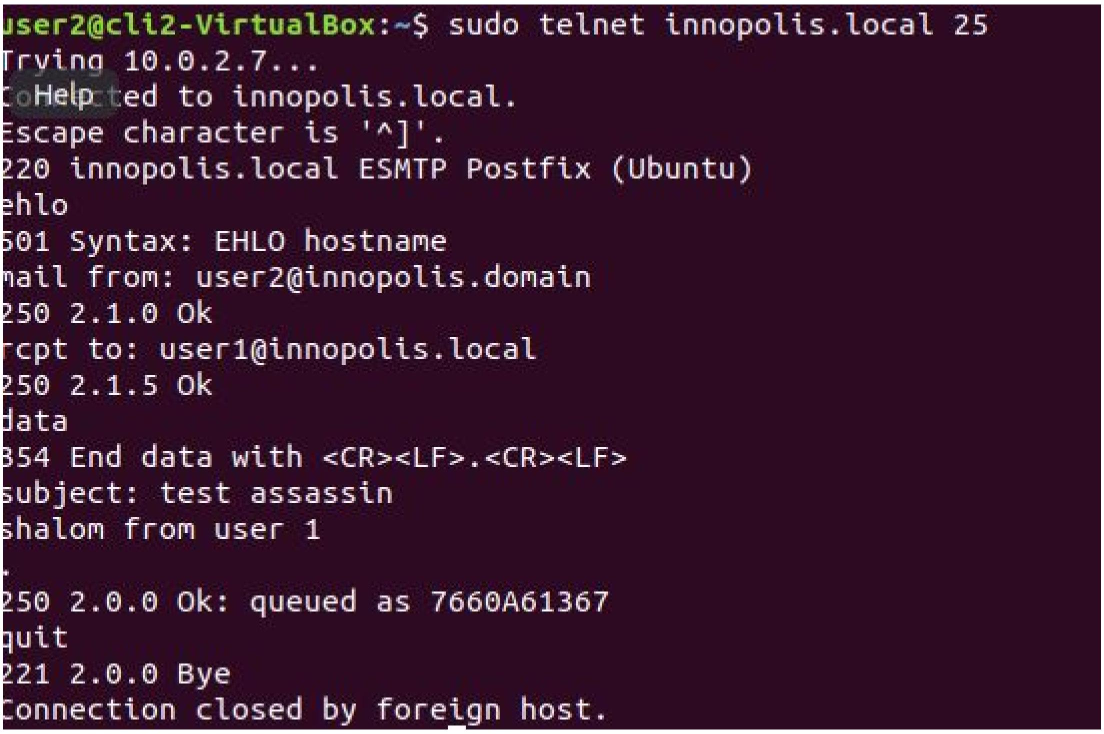
And check everything is fine by `sudo systemctl status postfix` or `sudo systemctl spamassassin`

Send an email from them to each other and show the emails with their headers.

From user1 to user2:

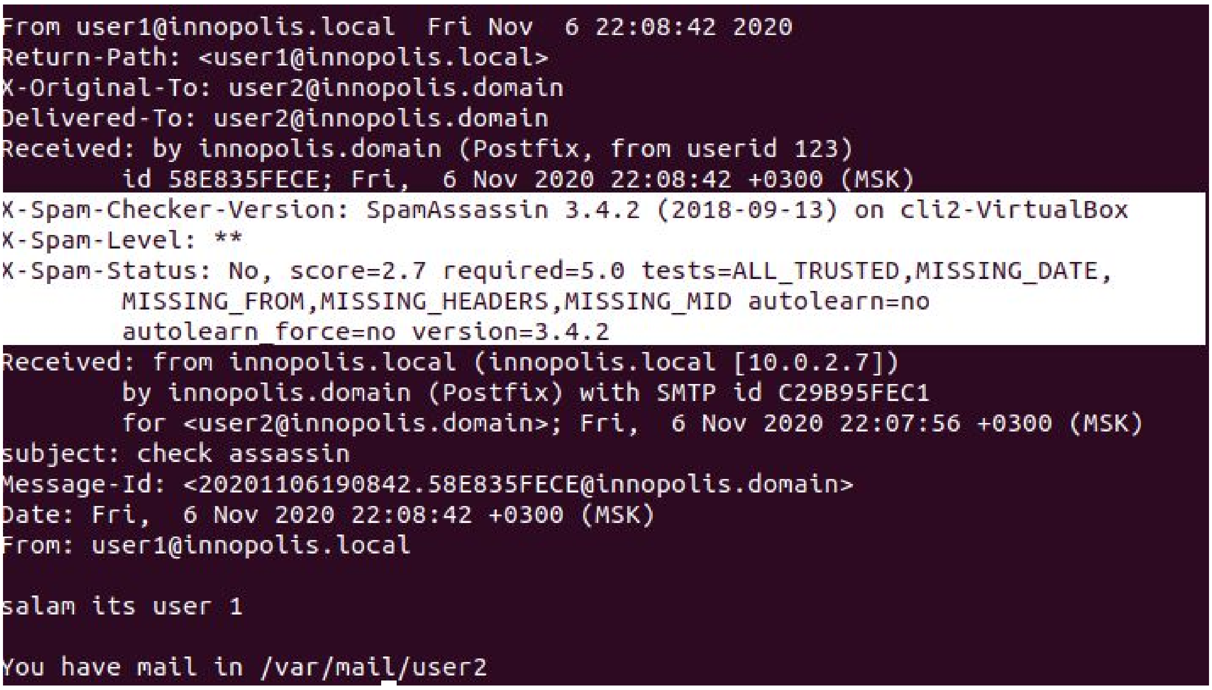


```
From user2@innopolis.domain  Fri Nov  6 22:37:30 2020
Return-Path: <user2@innopolis.domain>
X-Original-To: user1@innopolis.local
Delivered-To: user1@innopolis.local
Received: by innopolis.local (Postfix, from userid 123)
        id 363A66136F; Fri,  6 Nov 2020 22:37:30 +0300 (MSK)
X-Spam-Checker-Version: SpamAssassin 3.4.2 (2018-09-13) on cli2-VirtualBox
X-Spam-Level: **
X-Spam-Status: No, score=2.7 required=5.0 tests=ALL_TRUSTED,MISSING_DATE,
        MISSING_FROM,MISSING_HEADERS,MISSING_MID autolearn=no
        autolearn_force=no version=3.4.2
Received: from innopolis.domain (innopolis.domain [10.0.2.8])
        by innopolis.local (Postfix) with SMTP id 7660A61367
        for <user1@innopolis.local>; Fri,  6 Nov 2020 22:37:15 +0300 (MSK)
subject: test assassin
Message-Id: <20201106193730.363A66136F@innopolis.local>
Date: Fri,  6 Nov 2020 22:37:30 +0300 (MSK)
From: user2@innopolis.domain

shalom from user 1
```

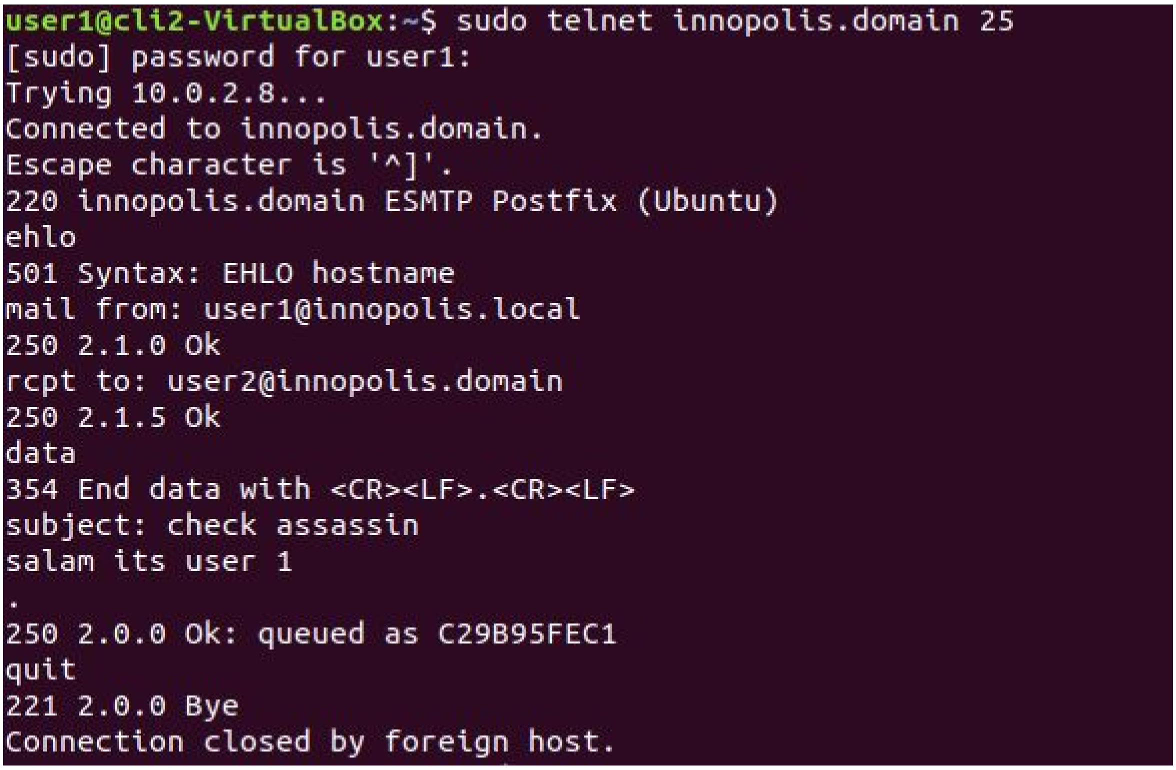


```
user2@cli2-VirtualBox:~$ sudo telnet innopolis.local 25
Trying 10.0.2.7...
Connected to innopolis.local.
Escape character is '^]'.
220 innopolis.local ESMTP Postfix (Ubuntu)
ehlo
501 Syntax: EHLO hostname
mail from: user2@innopolis.domain
250 2.1.0 Ok
rcpt to: user1@innopolis.local
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: test assassin
shalom from user 1
.
250 2.0.0 Ok: queued as 7660A61367
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

From user 1 to user2:



```
From user1@innopolis.local  Fri Nov  6 22:08:42 2020
Return-Path: <user1@innopolis.local>
X-Original-To: user2@innopolis.domain
Delivered-To: user2@innopolis.domain
Received: by innopolis.domain (Postfix, from userid 123)
        id 58E835FECE; Fri,  6 Nov 2020 22:08:42 +0300 (MSK)
X-Spam-Checker-Version: SpamAssassin 3.4.2 (2018-09-13) on cli2-VirtualBox
X-Spam-Level: **
X-Spam-Status: No, score=2.7 required=5.0 tests=ALL_TRUSTED,MISSING_DATE,
        MISSING_FROM,MISSING_HEADERS,MISSING_MID autolearn=no
        autolearn_force=no version=3.4.2
Received: from innopolis.local (innopolis.local [10.0.2.7])
        by innopolis.domain (Postfix) with SMTP id C29B95FEC1
        for <user2@innopolis.domain>; Fri,  6 Nov 2020 22:07:56 +0300 (MSK)
subject: check assassin
Message-Id: <20201106190842.58E835FECE@innopolis.domain>
Date: Fri,  6 Nov 2020 22:08:42 +0300 (MSK)
From: user1@innopolis.local

salam its user 1

You have mail in /var/mail/user2
```



```
user1@cli2-VirtualBox:~$ sudo telnet innopolis.domain 25
[sudo] password for user1:
Trying 10.0.2.8...
Connected to innopolis.domain.
Escape character is '^]'.
220 innopolis.domain ESMTP Postfix (Ubuntu)
ehlo
501 Syntax: EHLO hostname
mail from: user1@innopolis.local
250 2.1.0 Ok
rcpt to: user2@innopolis.domain
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: check assassin
salam its user 1
.
250 2.0.0 Ok: queued as C29B95FEC1
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Bonus

Describe DKIM, OSINT, TheHarvester

DKIM

Dkim (DomainKeys Identified Mail) technology calculates fake email addresses and helps fight spam and theft of personal data (usernames, passwords). DKIM adds a digital signature to the email. Thanks to it, mail providers (Mail.ru, Gmail) can check that the message came from your domain. The dkim signature is a TXT record that needs to be entered in the site's DNS zone settings. A DKIM signature will prevent scammers from sending emails on behalf of your domain. Together with SPF and DMARC, this technology protects your subscribers and your mailing lists. DKIM improves the domain's reputation. The recipient server uses DKIM to determine the sender's authenticity and overall rating. Emails with a good reputation are more likely to end up in your Inbox.

OSINT

OSINT (or as it sounds in the full English version of Open Source INTelligence) is a technology for searching, accumulating and analyzing data collected from available sources on the Internet. The technology allows you to collect maximum information from open sources for full professional analysis. The data can be placed in various forms: articles, publications, discussions on forums, video and audio files, documents, images, animations, gifs, etc. Note that it is not the same as just serfing the net in the sense of the depth of the approach.

OSINT marks content publication dates, user interest and activity, important details in images, geolocation tags, evaluates the target audience, and determines the IP address. Then you can scan the ports to find out what technological equipment is located near a particular person: cameras, printers, PCs, routers, and other equipment connected over the network.

The Harvester

This is a very fast and effective tool for performing OSINT written in python and preinstalled in Kali Linux. It is very useful to extract information from the specified targets.

Sources

https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-18-04-ru

https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-18-04

https://ixnfo.com/nastrojka-spamassassin-postfix.html

https://spspa.ru/chto-takoe-osint-osnovnye-instrumenty-i-metody/