

The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

# Investigation of incidents on the example of account theft

**Chechulin A.**  
Ph.D., leading researcher  
St.Petersburg Institute for  
Informatics and Automation of  
the Russian Academy of Sciences





# Story

- It is became known that John received several spam messages from Lisa
- You decide to take up the issue in detail
- What should you do?



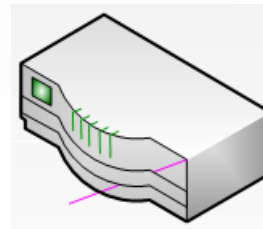


# Info from Lisa

- Lisa said that she didn't send these messages
- She use a web mail – yahoo.com



# Info from system administrator



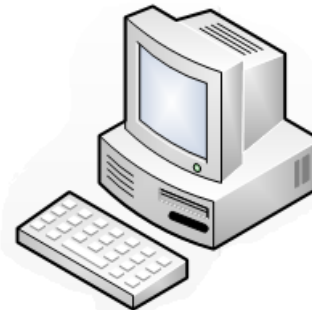
**Router-gateway**  
(192.168.238.2)



**Patrick**  
**Debian**  
(192.168.238.128)



**Lisa**  
**Ubuntu**  
(192.168.238.129)



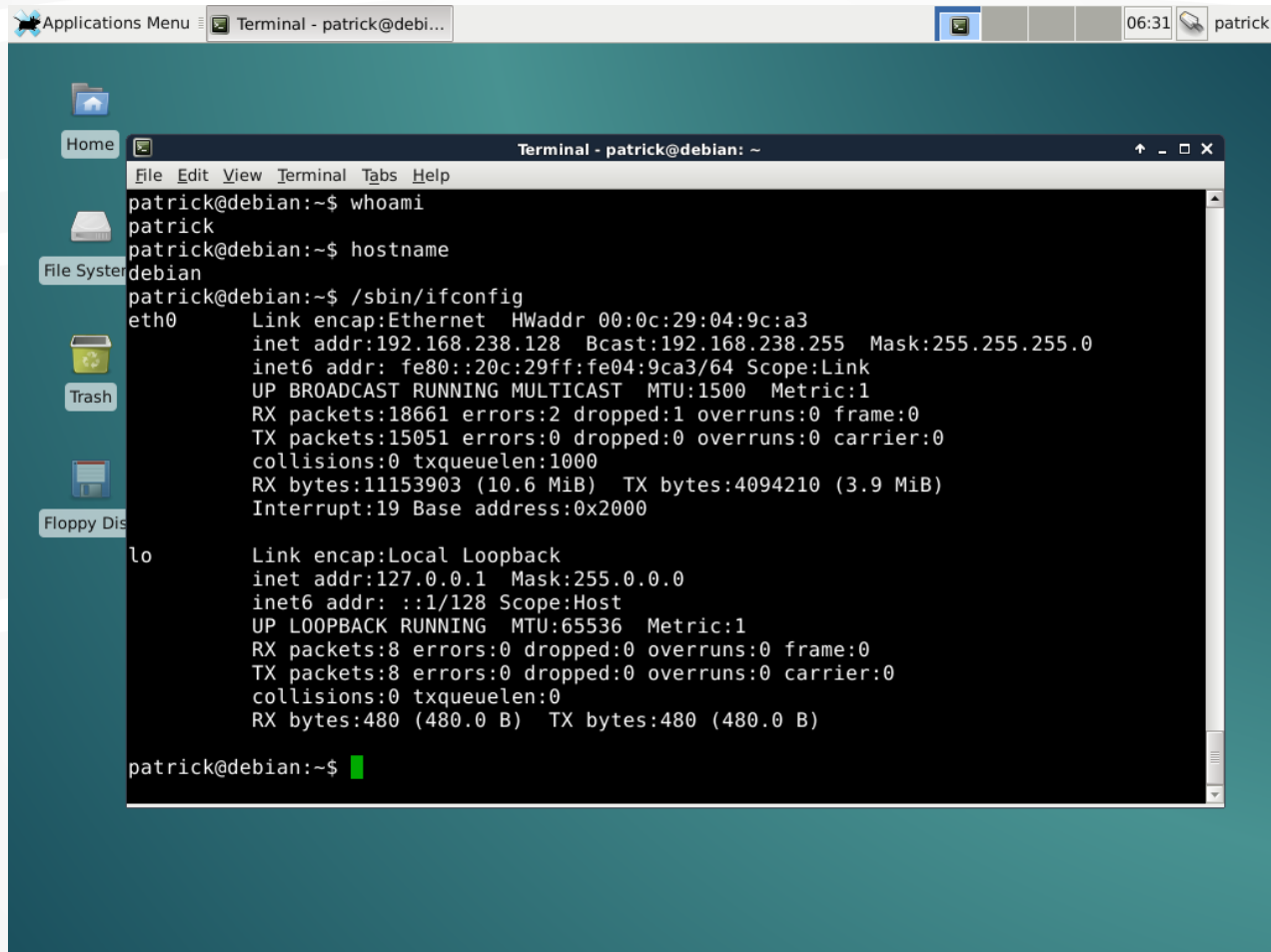
**John**  
**CentOS**  
(192.168.238.130)



**Harry**  
**Manjaro**  
(192.168.238.131)



# Network configuration (Debian)



The image shows a terminal window on a Debian system. The terminal title is "Terminal - patrick@debi...". The user "patrick" is logged in. The terminal shows the following commands and their outputs:

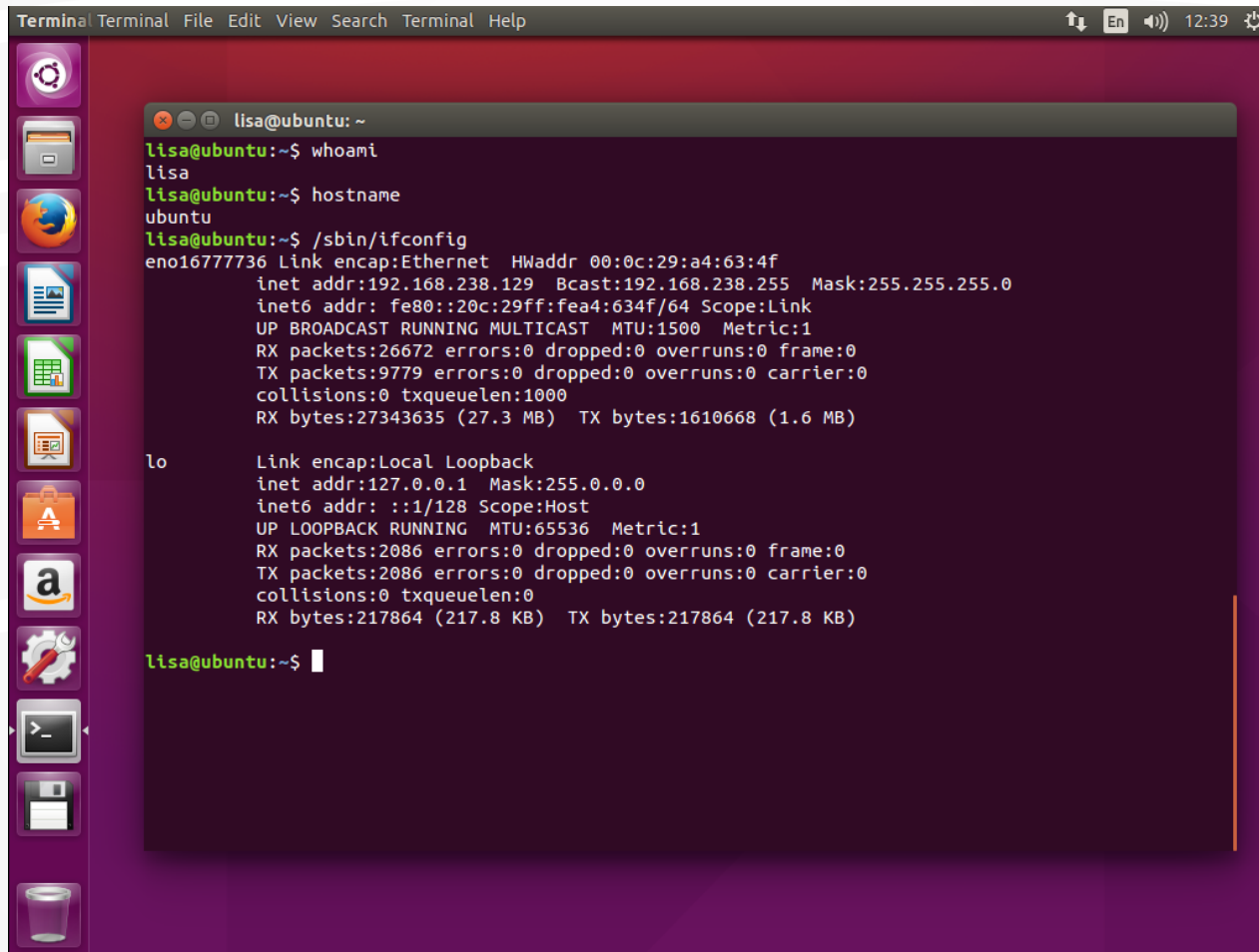
```
patrick@debian:~$ whoami
patrick
patrick@debian:~$ hostname
debian
patrick@debian:~$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:04:9c:a3
          inet addr:192.168.238.128  Bcast:192.168.238.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe04:9ca3/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18661 errors:2 dropped:1 overruns:0 frame:0
          TX packets:15051 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11153903 (10.6 MiB)  TX bytes:4094210 (3.9 MiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 B)  TX bytes:480 (480.0 B)

patrick@debian:~$
```



# Network configuration (Ubuntu)

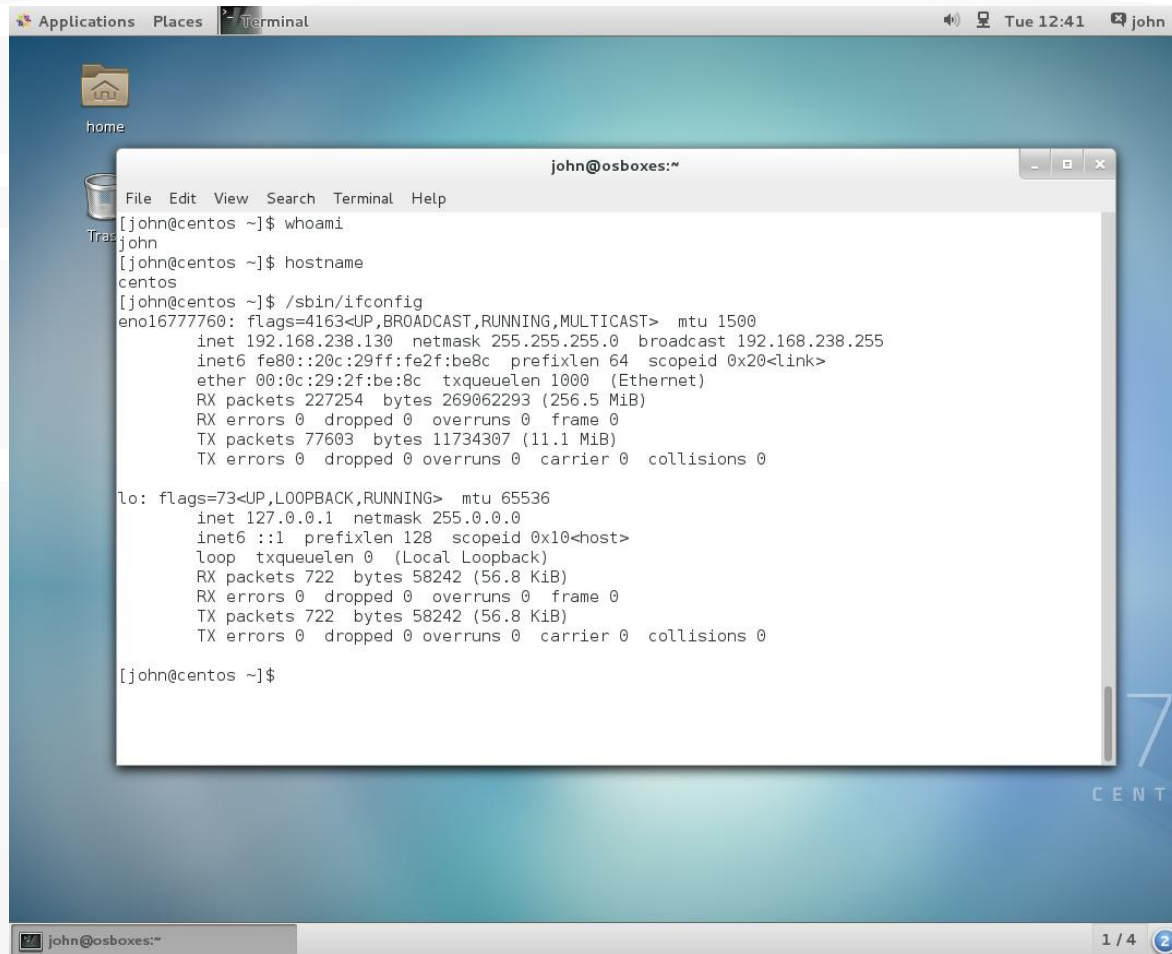


The image shows a terminal window in Ubuntu with a dark purple background. The window title is "Terminal Terminal File Edit View Search Terminal Help". The terminal output shows the following commands and their results:

```
lisa@ubuntu: ~  
lisa@ubuntu:~$ whoami  
lisa  
lisa@ubuntu:~$ hostname  
ubuntu  
lisa@ubuntu:~$ /sbin/ifconfig  
eno16777736 Link encap:Ethernet HWaddr 00:0c:29:a4:63:4f  
  inet addr:192.168.238.129 Bcast:192.168.238.255 Mask:255.255.255.0  
  inet6 addr: fe80::20c:29ff:fea4:634f/64 Scope:Link  
  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
  RX packets:26672 errors:0 dropped:0 overruns:0 frame:0  
  TX packets:9779 errors:0 dropped:0 overruns:0 carrier:0  
  collisions:0 txqueuelen:1000  
  RX bytes:27343635 (27.3 MB) TX bytes:1610668 (1.6 MB)  
  
lo Link encap:Local Loopback  
  inet addr:127.0.0.1 Mask:255.0.0.0  
  inet6 addr: ::1/128 Scope:Host  
  UP LOOPBACK RUNNING MTU:65536 Metric:1  
  RX packets:2086 errors:0 dropped:0 overruns:0 frame:0  
  TX packets:2086 errors:0 dropped:0 overruns:0 carrier:0  
  collisions:0 txqueuelen:0  
  RX bytes:217864 (217.8 KB) TX bytes:217864 (217.8 KB)  
  
lisa@ubuntu:~$
```



# Network configuration (CentOS)



The screenshot shows a CentOS desktop environment with a terminal window open. The terminal window title is "john@osboxes:~". The terminal output shows the following commands and their results:

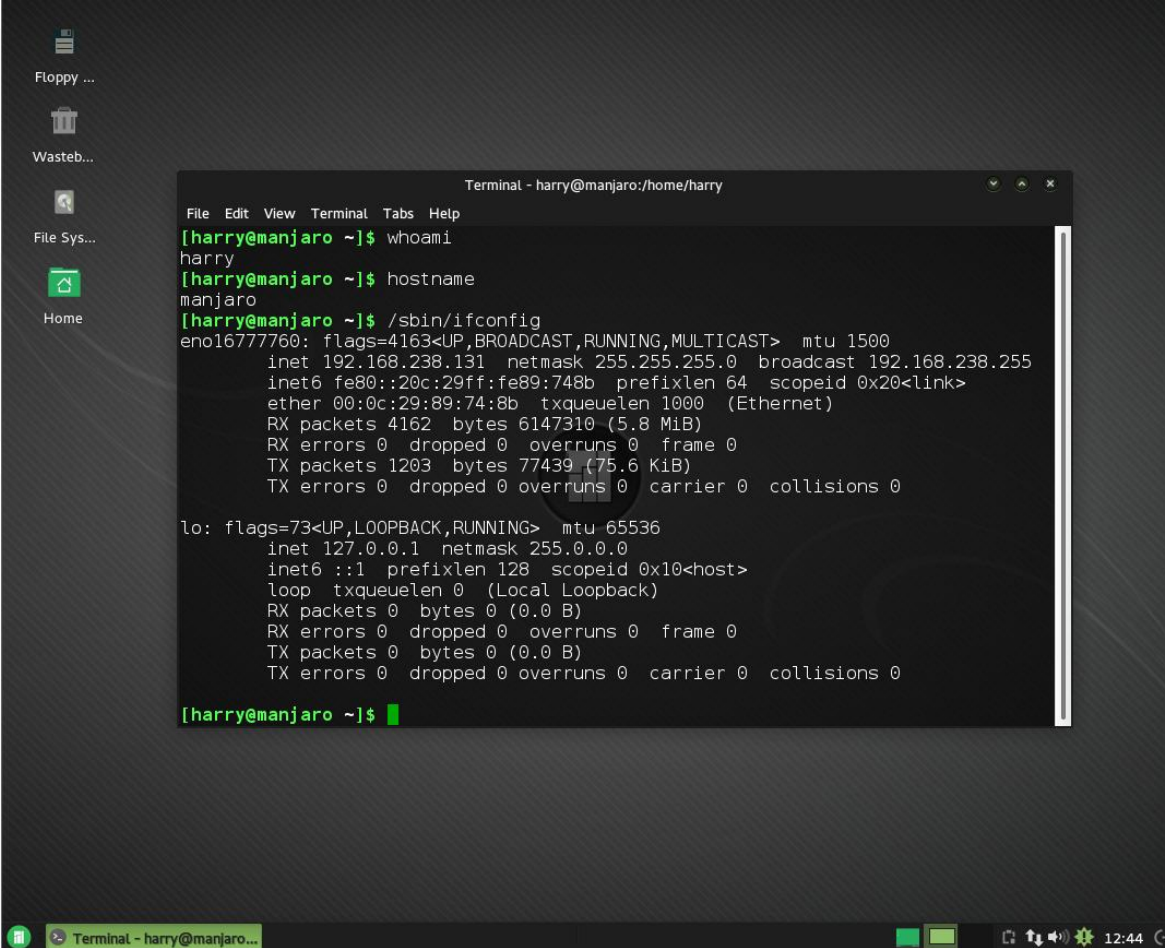
```
[john@centos ~]$ whoami
john
[john@centos ~]$ hostname
centos
[john@centos ~]$ /sbin/ifconfig
eno16777760: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.238.130 netmask 255.255.255.0 broadcast 192.168.238.255
    inet6 fe80::20c:29ff:fe2f:be8c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:2f:be:8c txqueuelen 1000 (Ethernet)
    RX packets 227254 bytes 269062293 (256.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 77603 bytes 11734307 (11.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 722 bytes 58242 (56.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 722 bytes 58242 (56.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[john@centos ~]$
```



# Network configuration (Manjaro)



The screenshot shows a Manjaro Linux desktop environment with a dark theme. On the left side, there is a sidebar with icons for 'Floppy ...', 'Wasteb...', 'File Sys...', and 'Home'. The main area displays a terminal window titled 'Terminal - harry@manjaro:/home/harry'. The terminal shows the following commands and output:

```
Terminal - harry@manjaro:/home/harry
File Edit View Terminal Tabs Help
[harry@manjaro ~]$ whoami
harry
[harry@manjaro ~]$ hostname
manjaro
[harry@manjaro ~]$ /sbin/ifconfig
eno16777760: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.238.131 netmask 255.255.255.0 broadcast 192.168.238.255
inet6 fe80::20c:29ff:fe89:748b prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:89:74:8b txqueuelen 1000 (Ethernet)
RX packets 4162 bytes 6147310 (5.8 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1203 bytes 77439 (75.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[harry@manjaro ~]$
```





# List of case participants

<b>Name and role</b>	<b>Operating system</b>	<b>IP address</b>	<b>HW address</b>
Patrick	Debian 8.2	192.168.238.128	00:0c:29:04:9c:a3
Lisa	Ubuntu 15.10	192.168.238.129	00:0c:29:a4:63:4f
John	CentOS 7.1	192.168.238.130	00:0c:29:2f:be:8c
Harry	Manjaro 15.9	192.168.238.131	00:0c:29:89:74:8b

