Identifying and blocking the backdoors in Linux

Enkli Ylli [a], Julian Fejzaj [b], Igli Tafa[a]

[a] *Faculty of Information Technology, Polytechnic University of Tirana, Sheshi Nënë Tereza ,Tiranë, Albania*
[b] *Faculty of Natural Sciences, University of Tirana, Bulevardi Zogu i Pare, Tiranë, Albania*

Abstract

Security and privacy is becoming a hot topic not only for the people in the field but also at social and family gatherings. It looks like attackers are finding sensational ways to gain access to systems and networks. On the other side, white hatters are developing new ways to block and protect customers from these attacks, and it feels like this process will never come to an end. However, it is important to have eyes open wide for our own safety. Knowledge is power. In this paper we introduce backdoors as a mean of attacking and gaining access over a system. We do that by using some tools in Ubuntu, a set of commands that will be explained in next sessions. We give a demonstration of how to inspect hidden backdoors. Finally, we introduce a way to stop backdoor attack.

Keywords

bacdoors, RK hunter, Ubuntu

1. Introduction

Nowadays, the knowledge required to keep networks and systems well-protected, need to be regularly updated. A strong reason for that is that attackers are becoming more and more sophisticated, by using a wide diversity of ways to achieve an approach to a system or a network. All those working in the field, need to roll up their sleeves and be equipped with the proper background so that next time when a sensational attack is reported on the news, they won't consider themselves blessed that their company weren't the objective. However, no matter how much secured a system is, there will be a manner to crack it. We should take in consideration, that even if a system is not vulnerable today, it may be in danger at some point in the future. Setting "night terrors" apart, delightedly, there are only a few highly developed aggressors especially in our country, against which our defence will fail. In this paper, we introduce backdoors as a mean of gaining access to a specific technology. We put emphasis that backdoors aren't only used for dreadful purposes; those of the non-criminal category are used to help clients who are desperately outside of their devices or for damage assessment and dealing with software concerns. Also, we will demonstrate in Linux Ubuntu how to find hidden backdoors, by using a set of commands and tools. Finally, we will show a way how to stop a backdoor attack.

2. RELATED WORK

There are different types of backdoors that accomplish attacks when systems have vulnerabilities. In [1], there are treated vulnerabilities of the authentication system and how attackers can establish malicious backdoors to bypass authentication logic. They describe three types of backdoors and propose their elimination. In [2], there are given some statistics about methods used by actors to hack and crack systems, and the result is that even one may say that backdoors are old, they are still one of the most used methods to gain unauthorized access in a system or network.

3. THEORETICAL APPROACH

In the cybersecurity world, the backdoor is a method where unauthorized and authorized users have the capability to get security measures and earn the most important access level which is root access. So gaining this access on a software application, network or computer system is very dangerous because they can steal your personal data, financial information and install more and more malware to control everything they have hacked. Backdoor malwares are generally mentioned as a Trojan. A Trojan is a malicious computer program that acts to be something different for the purposes of delivering malware, stealing your data, or opening up a backdoor on your computer

Proccedings of RTA-CSIT 2021, May 2021, Tirana, Albania
EMAIL: eylli@yahoo.com (A. 1); julian.fejzaj@fshn.edu.al (A. 2); itafaj@gmail.com (A. 3)

system. Much like the Trojan horse in Greece history, computer Trojans always contain a really bad surprise. Trojans sometimes have the ability to recreate themselves and spread to other computer systems without any additional commands from the cyber “criminal” who created them. An attacker can gain control of your computer using a backdoor to:

▪ Upload or Download files

▪ Fulfill DDoS attacks on further devices

▪ Adjust device settings as he wants, including user

credentials or even passwords.

▪ Steal data

▪ Install other malware on the system

▪ Shut down or restart the machine

▪ Download extra files

▪ Run processes and tasks

▪ Control the device on remote

Backdoors are of different types and not all of them have malicious intent.

Administrative backdoors are created by the hardware and software makers themselves.

Unlike backdoor malware, administrative backdoors aren't necessarily thought up with an illegitimate purpose in mind. Most of the times, built-in or administrative backdoors exist as artifacts of the process of software creation.

4. ENVRIONMENT SETUP

We chose to do our experiments in Ubuntu. Initially, we need to install Virtual Box in order to plant Ubuntu on it. We are using Ubuntu because it is user-friendly and is compatible with Debian packages.

Setting up Virtual Box on Windows platform.

To install Virtual Box first and foremost, Windows Installer must “live” in our system.

▪ Start Oracle VM VirtualBox installation by double clicking on the executable file.

▪ Welcome dialog enables us to choose where to install Oracle VM VirtualBox and which components to install.

The components available are:

- USB support
- Python support
- Networking

In the end, the installer will construct an Oracle VM VirtualBox gather in the Windows Start menu, which facilitates you to start the app and entry its dossier.

▪ With basic settings, Oracle VM VirtualBox will be planted for all customers on the regional device. [5]

Setting Up Ubuntu on VirtualBox

▪ Open the just installed VirtualBox and choose New. At this moment new window will appear.

▪ Select the architecture (32 or 64 bit) and the guest OS.

▪ Apply the Base Memory (RAM)

▪ Hit “Next” until it displays the VM storage size. Decide how much space we need determined by our hard disk and finish the wizard by hitting thecreate button.

▪ Next on VirtualBox window, select “Start” and choose the “media source”. In our situation, select the

“.iso” on the desktop.

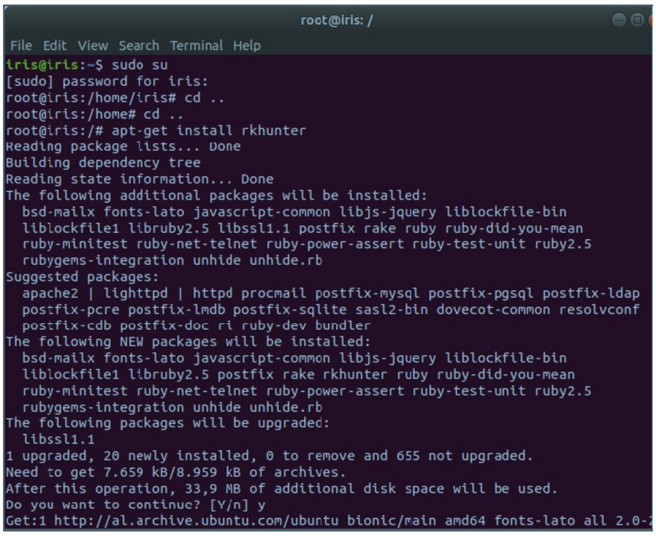
▪ Accomplish the installation.[6]

5. RESULTS

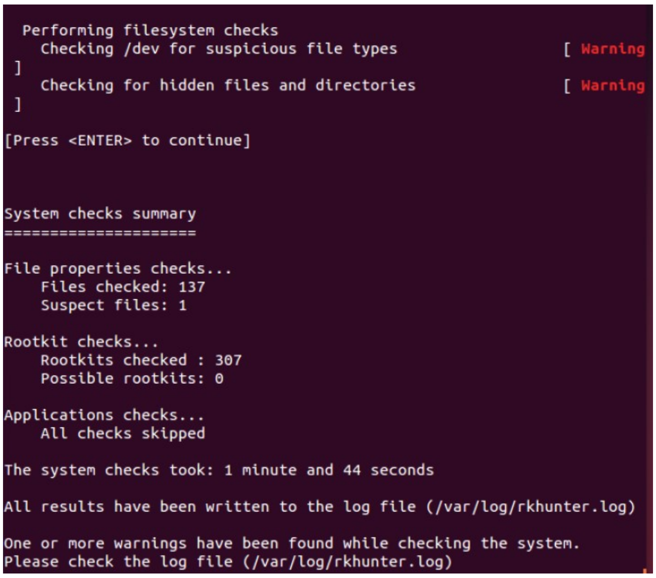
How to find strongly hidden backdoor, rootkit and port?

The 1st step [8]:

sudo apt-get install rkhunter

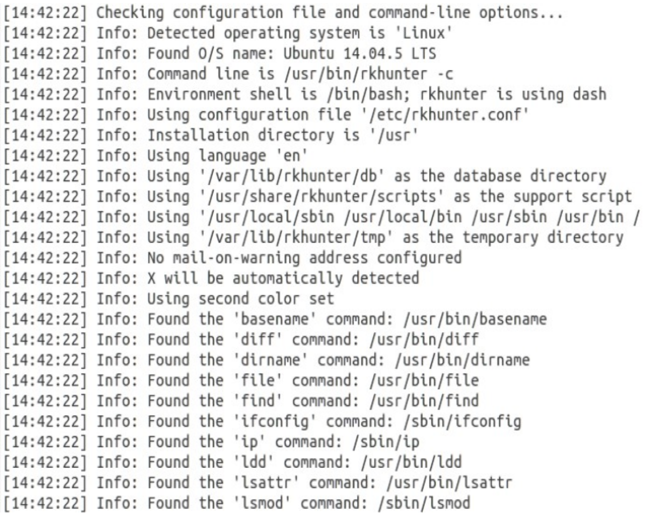


```
iris@iris:~$ sudo su
[sudo] password for iris:
root@iris:/home/iris# cd ..
root@iris:/home# cd ..
root@iris:/# apt-get install rkhunter
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin
  liblockfile1 libruby2.5 libssl1.1 postfix rake ruby ruby-did-you-mean
  ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.5
  rubygems-integration unhide unhide.rb
Suggested packages:
  apache2 | lighttpd | httpd procmail postfix-mysql postfix-pgsql postfix-ldap
  postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin dovecot-common resolvconf
  postfix-cdb postfix-doc ri ruby-dev bundler
The following NEW packages will be installed:
  bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin
  liblockfile1 libruby2.5 postfix rake rkhunter ruby ruby-did-you-mean
  ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.5
  rubygems-integration unhide unhide.rb
The following packages will be upgraded:
  libssl1.1
1 upgraded, 20 newly installed, 0 to remove and 655 not upgraded.
Need to get 7.659 kB/8.959 kB of archives.
After this operation, 33,9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://al.archive.ubuntu.com/ubuntu bionic/main amd64 fonts-lato all 2.0-2
```

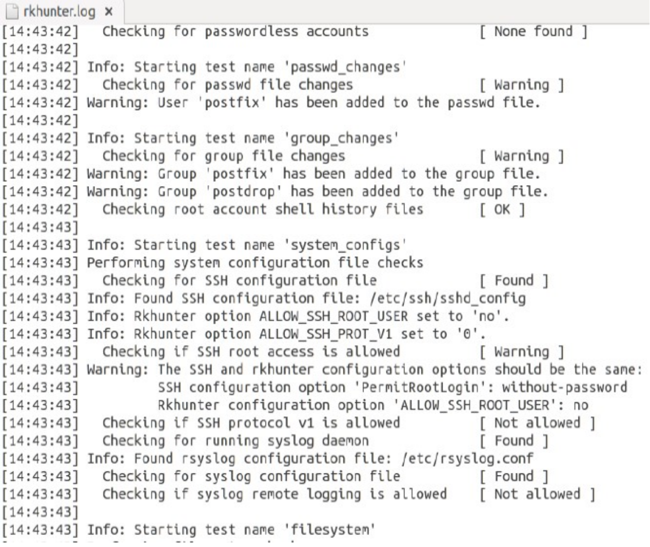


```
  Performing filesystem checks
    Checking /dev for suspicious file types                  [ Warning
 ]
    Checking for hidden files and directories                [ Warning
 ]

[Press <ENTER> to continue]



System checks summary
=====================

File properties checks...
    Files checked: 137
    Suspect files: 1

Rootkit checks...
    Rootkits checked : 307
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 1 minute and 44 seconds

All results have been written to the log file (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

sudo gedit /var/log/rkhunter.log



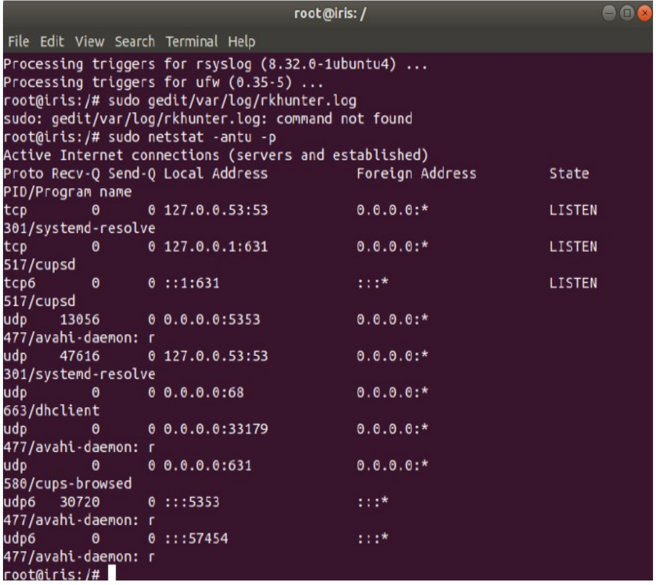
```
[14:42:22] Checking configuration file and command-line options...
[14:42:22] Info: Detected operating system is 'Linux'
[14:42:22] Info: Found O/S name: Ubuntu 14.04.5 LTS
[14:42:22] Info: Command line is /usr/bin/rkhunter -c
[14:42:22] Info: Environment shell is /bin/bash; rkhunter is using dash
[14:42:22] Info: Using configuration file '/etc/rkhunter.conf'
[14:42:22] Info: Installation directory is '/usr'
[14:42:22] Info: Using language 'en'
[14:42:22] Info: Using '/var/lib/rkhunter/db' as the database directory
[14:42:22] Info: Using '/usr/share/rkhunter/scripts' as the support script
[14:42:22] Info: Using '/usr/local/sbin /usr/local/bin /usr/sbin /usr/bin /
[14:42:22] Info: Using '/var/lib/rkhunter/tmp' as the temporary directory
[14:42:22] Info: No mail-on-warning address configured
[14:42:22] Info: X will be automatically detected
[14:42:22] Info: Using second color set
[14:42:22] Info: Found the 'basename' command: /usr/bin/basename
[14:42:22] Info: Found the 'diff' command: /usr/bin/diff
[14:42:22] Info: Found the 'dirname' command: /usr/bin/dirname
[14:42:22] Info: Found the 'file' command: /usr/bin/file
[14:42:22] Info: Found the 'find' command: /usr/bin/find
[14:42:22] Info: Found the 'ifconfig' command: /sbin/ifconfig
[14:42:22] Info: Found the 'ip' command: /sbin/ip
[14:42:22] Info: Found the 'ldd' command: /usr/bin/ldd
[14:42:22] Info: Found the 'lsattr' command: /usr/bin/lsattr
[14:42:22] Info: Found the 'lsmod' command: /sbin/lsmod
```



```
[14:43:42]   Checking for passwordless accounts                [ None found ]
[14:43:42]
[14:43:42] Info: Starting test name 'passwd_changes'
[14:43:42]   Checking for passwd file changes                  [ Warning ]
[14:43:42] Warning: User 'postfix' has been added to the passwd file.
[14:43:42]
[14:43:42] Info: Starting test name 'group_changes'
[14:43:42]   Checking for group file changes                   [ Warning ]
[14:43:42] Warning: Group 'postfix' has been added to the group file.
[14:43:42] Warning: Group 'postdrop' has been added to the group file.
[14:43:42]   Checking root account shell history files         [ OK ]
[14:43:43]
[14:43:43] Info: Starting test name 'system_configs'
[14:43:43] Performing system configuration file checks
[14:43:43]   Checking for SSH configuration file               [ Found ]
[14:43:43] Info: Found SSH configuration file: /etc/ssh/sshd_config
[14:43:43] Info: Rkhunter option ALLOW_SSH_ROOT_USER set to 'no'.
[14:43:43] Info: Rkhunter option ALLOW_SSH_PROT_V1 set to '0'.
[14:43:43]   Checking if SSH root access is allowed            [ Warning ]
[14:43:43] Warning: The SSH and rkhunter configuration options should be the same:
[14:43:43]          SSH configuration option 'PermitRootLogin': without-password
[14:43:43]          Rkhunter configuration option 'ALLOW_SSH_ROOT_USER': no
[14:43:43]   Checking if SSH protocol v1 is allowed            [ Not allowed ]
[14:43:43]   Checking for running syslog daemon                [ Found ]
[14:43:43] Info: Found rsyslog configuration file: /etc/rsyslog.conf
[14:43:43]   Checking for syslog configuration file            [ Found ]
[14:43:43]   Checking if syslog remote logging is allowed      [ Not allowed ]
[14:43:43]
[14:43:43] Info: Starting test name 'filesystem'
```

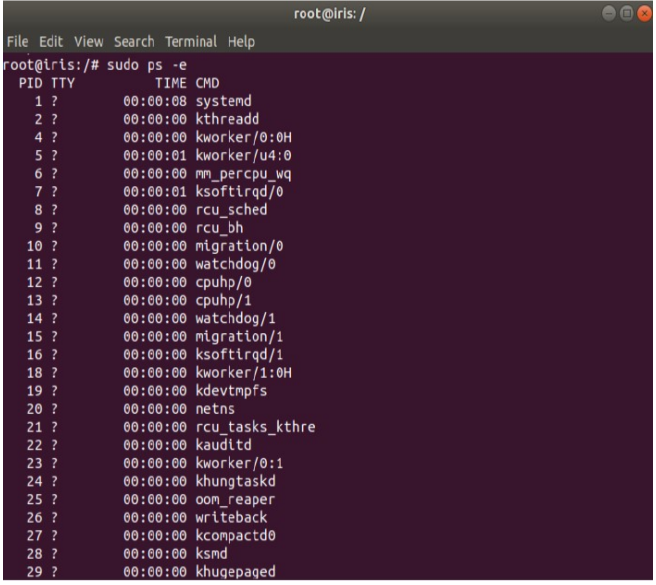
The 2nd step – Port Scan [7]:

sudo netstat -antu –p



```
Processing triggers for rsyslog (8.32.0-1ubuntu4) ...
Processing triggers for ufw (0.35-5) ...
root@iris:/# sudo gedit/var/log/rkhunter.log
sudo: gedit/var/log/rkhunter.log: command not found
root@iris:/# sudo netstat -antu -p
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
301/systemd-resolve
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
517/cupsd
tcp6       0      0 ::1:631                 :::*                    LISTEN
517/cupsd
udp    13056      0 0.0.0.0:5353            0.0.0.0:*
477/avahi-daemon: r
udp    47616      0 127.0.0.53:53           0.0.0.0:*
301/systemd-resolve
udp        0      0 0.0.0.0:68              0.0.0.0:*
663/dhclient
udp        0      0 0.0.0.0:33179           0.0.0.0:*
477/avahi-daemon: r
udp        0      0 0.0.0.0:631             0.0.0.0:*
580/cups-browsed
udp6   30720      0 :::5353                 :::*
477/avahi-daemon: r
udp6       0      0 :::57454                :::*
477/avahi-daemon: r
root@iris:/#
```

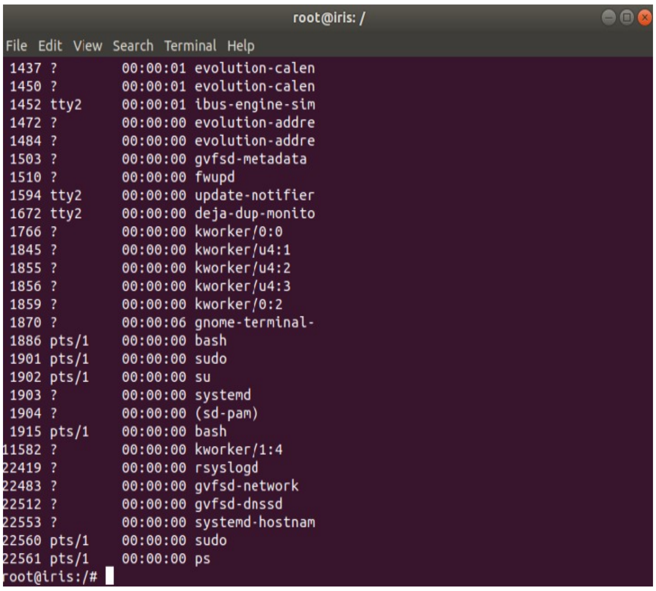
The 3rd step List of processes:
sudo ps –e



```
root@iris:/# sudo ps -e
  PID TTY          TIME CMD
    1 ?        00:00:08 systemd
    2 ?        00:00:00 kthreadd
    4 ?        00:00:00 kworker/0:0H
    5 ?        00:00:01 kworker/u4:0
    6 ?        00:00:00 mm_percpu_wq
    7 ?        00:00:01 ksoftirqd/0
    8 ?        00:00:00 rcu_sched
    9 ?        00:00:00 rcu_bh
   10 ?        00:00:00 migration/0
   11 ?        00:00:00 watchdog/0
   12 ?        00:00:00 cpuhp/0
   13 ?        00:00:00 cpuhp/1
   14 ?        00:00:00 watchdog/1
   15 ?        00:00:00 migration/1
   16 ?        00:00:00 ksoftirqd/1
   18 ?        00:00:00 kworker/1:0H
   19 ?        00:00:00 kdevtmpfs
   20 ?        00:00:00 netns
   21 ?        00:00:00 rcu_tasks_kthre
   22 ?        00:00:00 kauditd
   23 ?        00:00:00 kworker/0:1
   24 ?        00:00:00 khungtaskd
   25 ?        00:00:00 oom_reaper
   26 ?        00:00:00 writeback
   27 ?        00:00:00 kcompactd0
   28 ?        00:00:00 ksmd
   29 ?        00:00:00 khugepaged
```

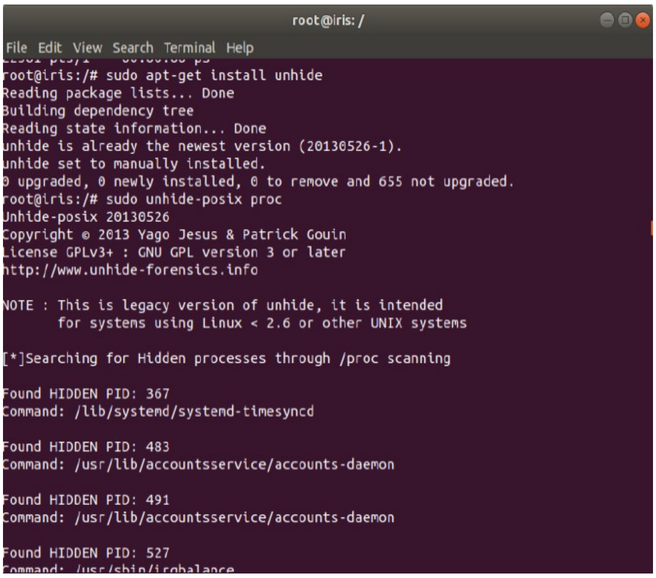
Proccedings of RTA-CSIT 2021, May 2021, Tirana, Albania

EMAIL: eylli@yahoo.com (A. 1); julian.fejzaj@fshn.edu.al (A. 2); itafaj@gmail.com (A. 3)

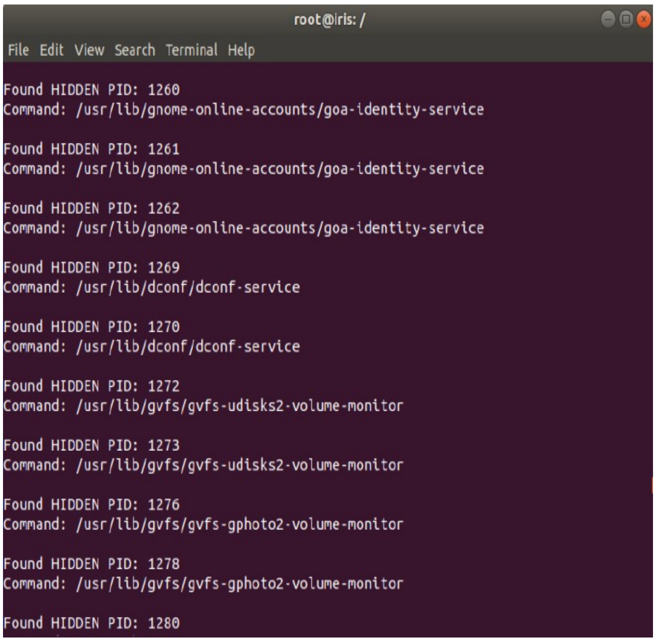


```
 1437 ?        00:00:01 evolution-calen
 1450 ?        00:00:01 evolution-calen
 1452 tty2     00:00:01 ibus-engine-sim
 1472 ?        00:00:00 evolution-addre
 1484 ?        00:00:00 evolution-addre
 1503 ?        00:00:00 gvfsd-metadata
 1510 ?        00:00:00 fwupd
 1594 tty2     00:00:00 update-notifier
 1672 tty2     00:00:00 deja-dup-monito
 1766 ?        00:00:00 kworker/0:0
 1845 ?        00:00:00 kworker/u4:1
 1855 ?        00:00:00 kworker/u4:2
 1856 ?        00:00:00 kworker/u4:3
 1859 ?        00:00:00 kworker/0:2
 1870 ?        00:00:06 gnome-terminal-
 1886 pts/1    00:00:00 bash
 1901 pts/1    00:00:00 sudo
 1902 pts/1    00:00:00 su
 1903 ?        00:00:00 systemd
 1904 ?        00:00:00 (sd-pam)
 1915 pts/1    00:00:00 bash
11582 ?        00:00:00 kworker/1:4
22419 ?        00:00:00 rsyslogd
22483 ?        00:00:00 gvfsd-network
22512 ?        00:00:00 gvfsd-dnssd
22553 ?        00:00:00 systemd-hostnam
22560 pts/1    00:00:00 sudo
22561 pts/1    00:00:00 ps
root@iris:/#
```

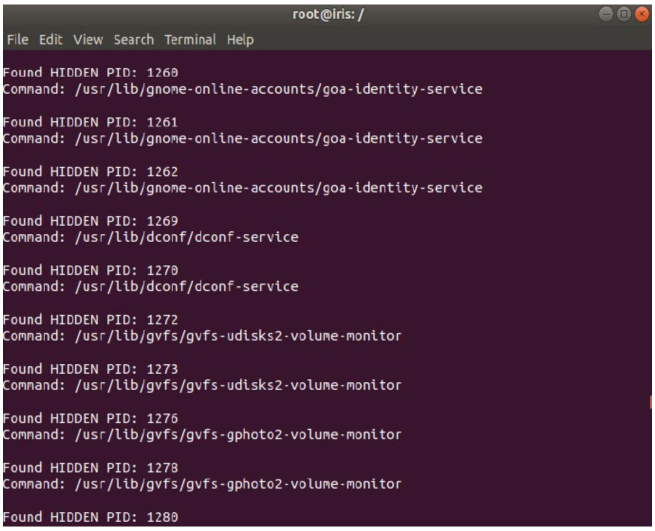
The 4th step - List of hidden processes [4]:
sudo apt-get install unhide
sudo unhide-posix proc



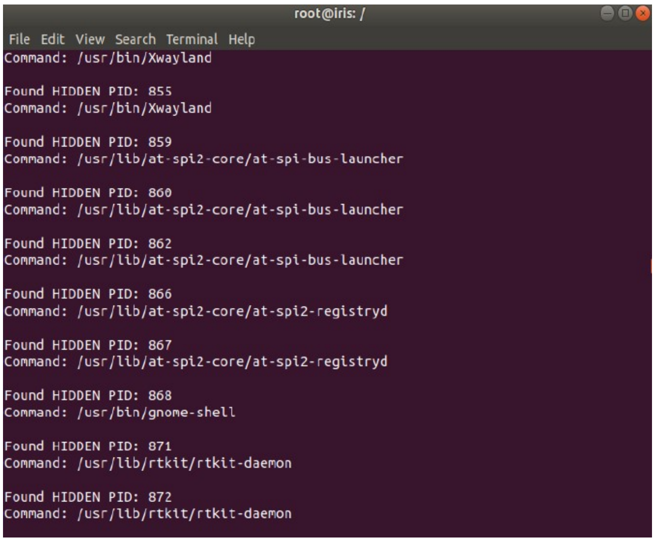
```
22561 pts/1    00:00:00 ps
root@iris:/# sudo apt-get install unhide
Reading package lists... Done
Building dependency tree
Reading state information... Done
unhide is already the newest version (20130526-1).
unhide set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 655 not upgraded.
root@iris:/# sudo unhide-posix proc
Unhide-posix 20130526
Copyright © 2013 Yago Jesus & Patrick Gouin
License GPLv3+ : GNU GPL version 3 or later
http://www.unhide-forensics.info

NOTE : This is legacy version of unhide, it is intended
       for systems using Linux < 2.6 or other UNIX systems

[*]Searching for Hidden processes through /proc scanning

Found HIDDEN PID: 367
Command: /lib/systemd/systemd-timesyncd

Found HIDDEN PID: 483
Command: /usr/lib/accountsservice/accounts-daemon

Found HIDDEN PID: 491
Command: /usr/lib/accountsservice/accounts-daemon

Found HIDDEN PID: 527
Command: /usr/sbin/irqbalance
```



```
Found HIDDEN PID: 1260
Command: /usr/lib/gnome-online-accounts/goa-identity-service

Found HIDDEN PID: 1261
Command: /usr/lib/gnome-online-accounts/goa-identity-service

Found HIDDEN PID: 1262
Command: /usr/lib/gnome-online-accounts/goa-identity-service

Found HIDDEN PID: 1269
Command: /usr/lib/dconf/dconf-service

Found HIDDEN PID: 1270
Command: /usr/lib/dconf/dconf-service

Found HIDDEN PID: 1272
Command: /usr/lib/gvfs/gvfs-udisks2-volume-monitor

Found HIDDEN PID: 1273
Command: /usr/lib/gvfs/gvfs-udisks2-volume-monitor

Found HIDDEN PID: 1276
Command: /usr/lib/gvfs/gvfs-gphoto2-volume-monitor

Found HIDDEN PID: 1278
Command: /usr/lib/gvfs/gvfs-gphoto2-volume-monitor

Found HIDDEN PID: 1280
```



```
Found HIDDEN PID: 1260
Command: /usr/lib/gnome-online-accounts/goa-identity-service

Found HIDDEN PID: 1261
Command: /usr/lib/gnome-online-accounts/goa-identity-service

Found HIDDEN PID: 1262
Command: /usr/lib/gnome-online-accounts/goa-identity-service

Found HIDDEN PID: 1269
Command: /usr/lib/dconf/dconf-service

Found HIDDEN PID: 1270
Command: /usr/lib/dconf/dconf-service

Found HIDDEN PID: 1272
Command: /usr/lib/gvfs/gvfs-udisks2-volume-monitor

Found HIDDEN PID: 1273
Command: /usr/lib/gvfs/gvfs-udisks2-volume-monitor

Found HIDDEN PID: 1276
Command: /usr/lib/gvfs/gvfs-gphoto2-volume-monitor

Found HIDDEN PID: 1278
Command: /usr/lib/gvfs/gvfs-gphoto2-volume-monitor

Found HIDDEN PID: 1280
```



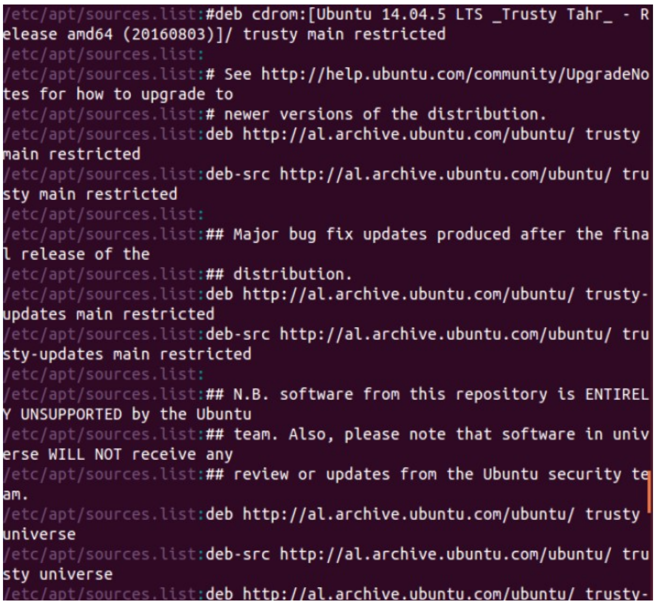
```
Command: /usr/bin/Xwayland

Found HIDDEN PID: 855
Command: /usr/bin/Xwayland

Found HIDDEN PID: 859
Command: /usr/lib/at-spi2-core/at-spi-bus-launcher

Found HIDDEN PID: 860
Command: /usr/lib/at-spi2-core/at-spi-bus-launcher

Found HIDDEN PID: 862
Command: /usr/lib/at-spi2-core/at-spi-bus-launcher

Found HIDDEN PID: 866
Command: /usr/lib/at-spi2-core/at-spi2-registryd

Found HIDDEN PID: 867
Command: /usr/lib/at-spi2-core/at-spi2-registryd

Found HIDDEN PID: 868
Command: /usr/bin/gnome-shell

Found HIDDEN PID: 871
Command: /usr/lib/rtkit/rtkit-daemon

Found HIDDEN PID: 872
Command: /usr/lib/rtkit/rtkit-daemon
```

The 5th step - View logs[10]:

```
sudo gedit /var/log/dpkg.log
sudo gedit /var/log/daemon.log
sudo gedit /var/log/user.log
```

The 6th step - Check Repository:

```
grep ^ /etc/apt/sources.list
/etc/apt/sources.list.d/*
```



```
/etc/apt/sources.list:#deb cdrom:[Ubuntu 14.04.5 LTS _Trusty Tahr_ - R
elease amd64 (20160803)]/ trusty main restricted
/etc/apt/sources.list:
/etc/apt/sources.list:# See http://help.ubuntu.com/community/UpgradeNo
tes for how to upgrade to
/etc/apt/sources.list:# newer versions of the distribution.
/etc/apt/sources.list:deb http://al.archive.ubuntu.com/ubuntu/ trusty
main restricted
/etc/apt/sources.list:deb-src http://al.archive.ubuntu.com/ubuntu/ tru
sty main restricted
/etc/apt/sources.list:
/etc/apt/sources.list:## Major bug fix updates produced after the fina
l release of the
/etc/apt/sources.list:## distribution.
/etc/apt/sources.list:deb http://al.archive.ubuntu.com/ubuntu/ trusty-
updates main restricted
/etc/apt/sources.list:deb-src http://al.archive.ubuntu.com/ubuntu/ tru
sty-updates main restricted
/etc/apt/sources.list:
/etc/apt/sources.list:## N.B. software from this repository is ENTIREL
Y UNSUPPORTED by the Ubuntu
/etc/apt/sources.list:## team. Also, please note that software in univ
erse WILL NOT receive any
/etc/apt/sources.list:## review or updates from the Ubuntu security te
am.
/etc/apt/sources.list:deb http://al.archive.ubuntu.com/ubuntu/ trusty
universe
/etc/apt/sources.list:deb-src http://al.archive.ubuntu.com/ubuntu/ tru
sty universe
/etc/apt/sources.list:deb http://al.archive.ubuntu.com/ubuntu/ trusty-
```

Finally, we are giving some commands what to do in case of a backdoor attack.

We block outgoing traffic to prevent backdoor damage. We can use iptables to contain further damage if a malware has been able to infect our host. By applying iptables filters with 'OUTPUT' option we block any unwanted traffic coming out from the host.

Commands [9]:

Iptables –A OUTPUT –o eth1 –j DROP

We can add extra rules for logging and analyzing.

Build a new link named LOGGING:

iptables -N LOGGING

Then add outgoing traffic to LOGGING link:

iptables -A OUTPUT -j LOGGING

Decline packets

iptables -A LOGGING -j DROP

6. CONCLUSIONS

To conclude, security is an important topic and everyone should have some basic information in order to protect themselves from possible attacks. Remember that if your system is safe today it can be a target tomorrow. One of most popular ways even in 2020 are backdoors. We learned that backdoors are used from good guys and bad guys too. Through the sections of this paper we learned what backdoors are and how attackers use them to gain access over a computer. In the experimental section, we demonstrated a simple way how to detect hidden processes. Finally, we gave a solution what to do in case of a backdoor attack. We blocked traffic to prevent damage.

7. References

[1] A. Mishra, J.P. Jyotiyana "Secure Authentication: Eliminating Possible Backdoors in Client-Server Endorsement", 2016

[2] "Data breach investigation report", 2019

[3] https://www.malwarebytes.com/backdoor/

[4]https://www.cyberciti.biz/tips/linux-unixwindows-find-hidden-processes-tcp-udpports.html

[5]https://www.virtualbox.org/manual/ch02.html

[6]https://askubuntu.com/questions/142549/how-to-install-ubuntu-on-virtualbox

[7]http://manpages.ubuntu.com/manpages/trusty/man8/netstat.8.html

[8]https://help.ubuntu.com/community/RKhunter

[9]https://www.thegeekstuff.com/2011/06/iptables-rules-examples/

[10]https://helpdeskgeek.com/linux-tips/displaya-list-of-recently-installed-software-packagesin-ubuntu/

Proccedings of RTA-CSIT 2021, May 2021, Tirana, Albania
EMAIL: eylli@yahoo.com (A. 1); julian.fejzaj@fshn.edu.al (A. 2); itafaj@gmail.com (A. 3)