

JANUARY 02, 2015



SECURITY REPORT

MADE 02.01.2015 BETWEEN 18:00 – 22:00

by John Doe

Security Specialist at Keios Solutions

for NewTech United, London

WWW.KEIOS.EU



CLUSTER INFORMATION

Number of servers: 1

In reports, servers will be called S1, S2, according to the list below:

SERVER S1

OPERATING SYSTEM

Type: Linux

Name: Debian Linux 7.4 „Wheezy“ 64bit

Kernel: 3.2.0-4-amd64

NETWORK

hostname: debian4al

Server Network Adapters:

eth0 **1.2.3.4** (public)

eth1 **192.168.0.10** (local)

SERVICES

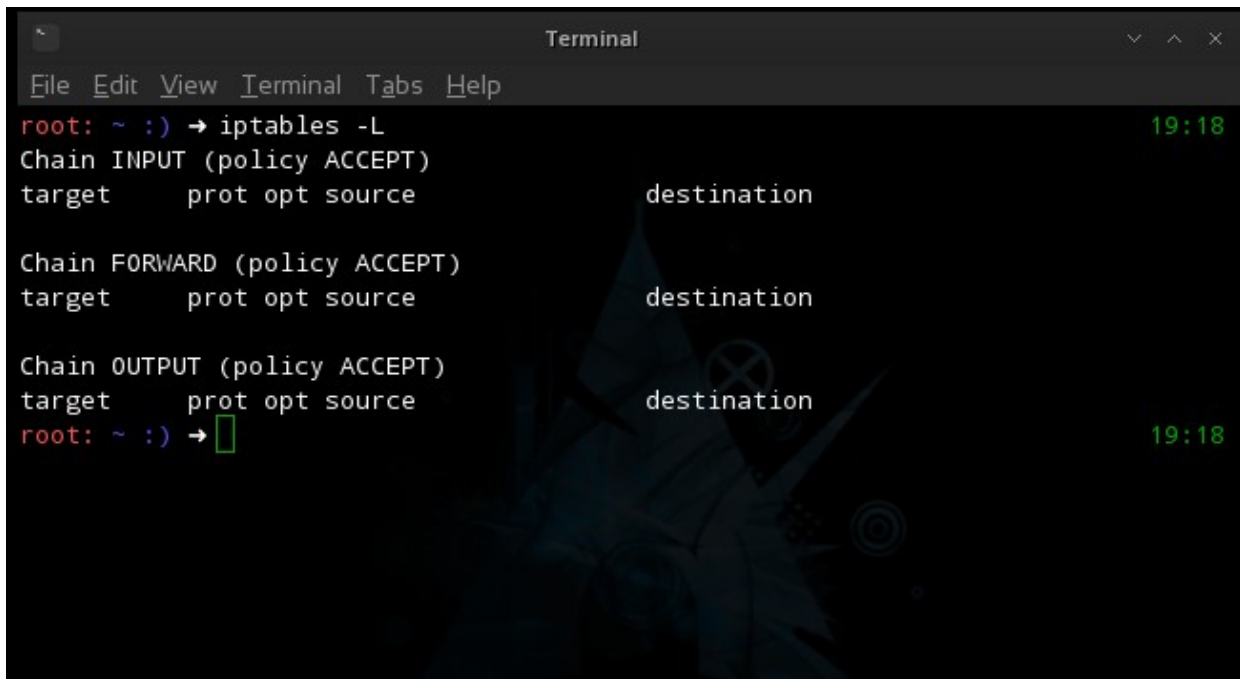
1.2.3.4 is a multipurpose server with following services active and in production:

- VoIP SoftSwitch (*asterisk*)
- Webserver (*nginx*)
- Database (*MySQL*)
- FTP (*vsftpd*)
- Admin Panel (*Ajenti*)

REPORT

FIREWALL

According to customer, server is not protected by any external firewall. Internally, **iptables firewall** is active, but its ruleset was empty, which means that all traffic was allowed.



```
Terminal
File Edit View Terminal Tabs Help
root: ~ :) → iptables -L 19:18
Chain INPUT (policy ACCEPT)
target      prot opt source                destination

Chain FORWARD (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination
root: ~ :) → █ 19:18
```

SECURITY RISK: HIGH

SERVER ACCESS

There are two methods of connecting to server:

- SSH
 - Runs on default port | Security Risk: **Medium**
 - Access enabled to public | Security Risk: **High**
 - Root password is strong | Security Risk: **Low**
- VNC
 - Runs on request (x11vnc command) | Security Risk: **Low**
 - Access enabled to public | Security Risk: **Medium**
 - Allowed to run without password | Security Risk: **High**



USERS

There are 3 user accounts created on the server:

- root *(administrator permissions)*
- johndoe *(no administrator permissions, prompt set to /bin/false)*
- marktwin *(no administrator permissions, prompt set to /bin/false)*

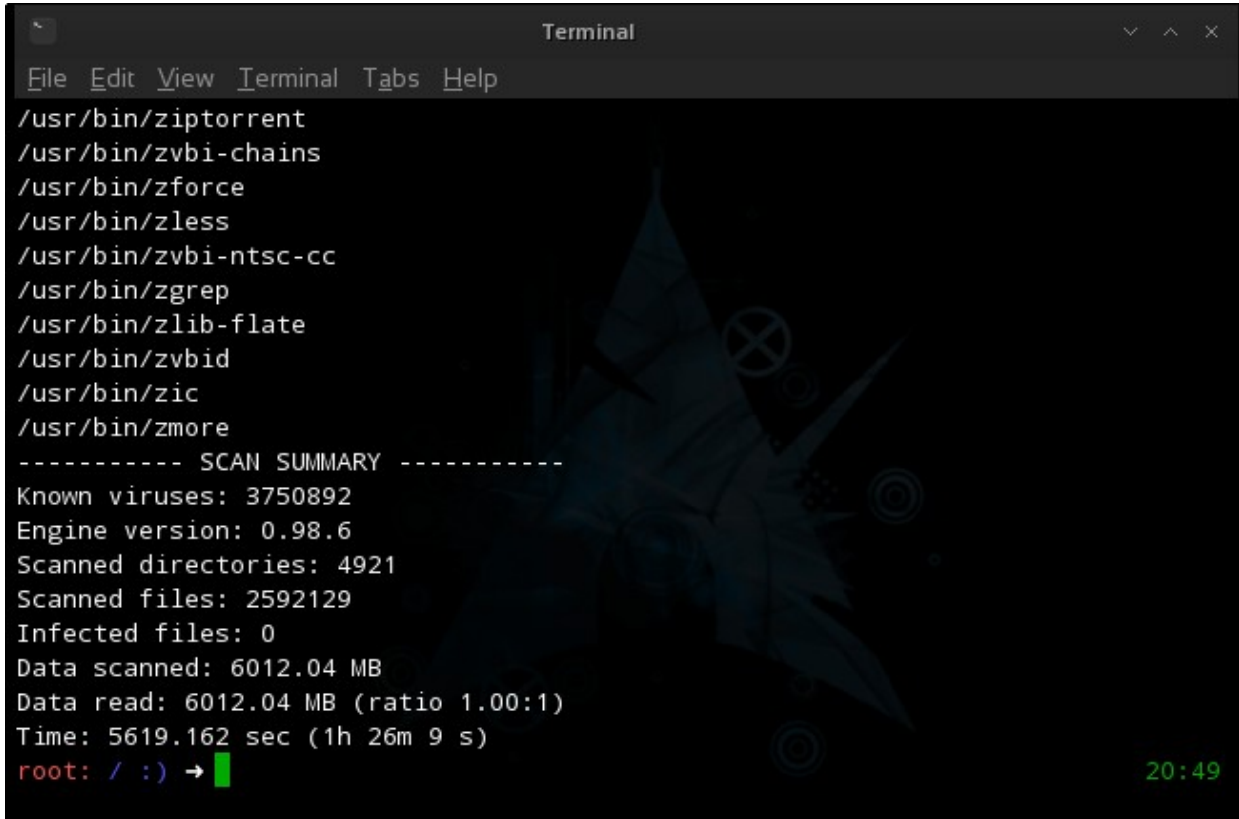
SYSTEM SECURITY ISSUES

- Processes
 - No unknown processes were running
- Services
 - No unknown services were created in /etc/init.d
- Scheduler Tasks
 - No unknown tasks were created in crontab
- Serious Security Bugs
 - Bash version was 4.1 – **vulnerable to shellshock security bug**
 - Glibc version was 2.12 – **vulnerable to GHOST security bug**
 - OpenSSL version was 0.9.8 – not vulnerable to Heartbleed security bug
- Autostart
 - Two third party executables were added to rc.local:
 - PermScript (Script setting up proper permissions to FTP folders)
 - CacheScript (Script clearing up cache of php webapplications)
 - One third party executable was added to /etc/profile:
 - keios-sstatus (Script showing status of important running services)

All of the above executables were known to customer and are safe to use.

VIRUSES

- **ClamAV** scan with latest database displayed no results



```
Terminal
File Edit View Terminal Tabs Help
/usr/bin/ziptorrent
/usr/bin/zvbi-chains
/usr/bin/zforce
/usr/bin/zless
/usr/bin/zvbi-ntsc-cc
/usr/bin/zgrep
/usr/bin/zlib-flate
/usr/bin/zvbid
/usr/bin/zic
/usr/bin/zmore
----- SCAN SUMMARY -----
Known viruses: 3750892
Engine version: 0.98.6
Scanned directories: 4921
Scanned files: 2592129
Infected files: 0
Data scanned: 6012.04 MB
Data read: 6012.04 MB (ratio 1.00:1)
Time: 5619.162 sec (1h 26m 9 s)
root: / :) → 20:49
```

SHARED FILES

- **Samba**
 - Not installed
- **NFS**
 - Disabled
- **FTP**
 - **Active**
 - Local user access | Security Risk: **Low**
 - Users are binded to their home directories | Security Risk: **Low**
 - No anonymous access | Security Risk: **Low**
 - Logging enabled | Security Risk: **Low**
 - Disk quota disabled | Security Risk: **Medium**
 - Not protected by SSL (SFTP) | Security Risk: **Medium**



- **Dropbox / Google Drive / Box** (or other cloud storage options)
 - None installed
- **WebDav**
 - Not Installed
- **Webserver File Sharing**
 - Directory Listing disabled
 - Wordpress Website Backup stored in zip archive on webserver root.
This file includes database password.

```
Terminal
File Edit View Terminal Tabs Help
root: http :) → ls -al                                     20:27
total 9272
drwxr-xr-x 6 root root    4096 Feb 23 20:26 .
drwxr-xr-x 5 root root    4096 Sep 15 01:09 ..
drwxr-xr-x 2 http http    4096 Feb 23 20:26 ajenti
drwxr-xr-x 2 http http    4096 Feb 23 20:26 control
drwxr-xr-x 2 http http    4096 Feb 23 20:26 website1
drwxr-xr-x 2 http http    4096 Feb 23 20:26 wordpress
-rwxr-xr-x 1 http http 9468347 Feb 23 20:26 wordpress.zip
root: http :) → █                                         20:27
```

DATABASE

Database was running on default port 3306.

Port was unlocked in iptables firewall.

Database was set to listen only on localhost.

There was only root@localhost user created.



OPEN TCP PORTS

Running (netstat)

21, 22, 80, 443, 3306, 5038, 5060, 8000.

Detectable (nmap)

21, 22, 80, 443, 5060, 8000

HACKING INCIDENT ANALYSIS (IF REPORTED)

Customer didn't report any hacking activities.

VOIP SECURITY

- Asterisk was running on default port (5060)
- Access to Asterisk server was public
- Access to FreePBX Admin Portal was public
- FreePBX admin password was difficult
- Asterisk Manager was using non-default password
- There were no easy-to-guess extensions (like 100, 101)
- Passwords of extensions were medium and difficult
- IP Logging was enabled
- There was no Fail2Ban service installed

ADDITIONAL NOTES

Ajenti Administrator Panel is running on default port with very weak password.

Ajenti is available on Public IP.



ADVISED SOLUTIONS

FIREWALL

- Installation of Vuurmuur IPTables GUI
- Setup of iptables
- Setting up rules for public and private services access
- Fail2Ban module installation

SERVER ACCESS

- Changing SSH port to non default.
- VNC Removal (*X Windows system is not used for anything*)
- Setting up access for selected IP only (ACL)

USERS

- No security issues found

SYSTEM SECURITY ISSUES

- Bash Upgrade
- Glibc Upgrade

VIRUSES

- No security issues found

SHARED FILES

- Setting up space quota for users
- Urgent removal of Wordpress Backup file
- Optional: Secure FTP setup

DATABASE

- Setting up firewall will resolve all issues.

OPEN TCP PORTS

- Setting up firewall will resolve all issues.



HACKING INCIDENT

- No security issues found.

VOIP SECURITY

- If possible – changing SIP port to non-default
- Installation of Fail2Ban
- Limiting access to FreePBX Admin Panel to given IP list (ACL)

ADDITIONAL

- Urgent password change
- Change in config for agenti to work only on 192.168.0.10
- Optional: OpenVPN Deployment

SOLUTIONS COST: 200 USD

CONTACT: INFO@KEIOS.EU

Representing Keios Solutions

John Doe
Security Specialist