

Tools to scan a Linux / Unix Web server for Malware and Rootkits / Lynis and ISPProtect - clean Joomla / Wordpress and other CMS for malware and malicious scripts and trojan codes

Author : admin



If you have been hacked or have been suspicious that someone has broken up in some of the shared web hosting servers you happen to manage you already probably have tried the [server with rkhunter, chroot and unhide tools which gives a general guidance where a server has been compromised](#)

However with the evolution of hacking tools out there and the boom of **Web security XSS / CSS / Database injections and PHP scripts vulnerability catching an intruder especially spammers has been becoming more and more hard to achieve.**

Just lately a mail server of mine's load average increased about 10 times, and the CPU's and HDD I/O load jump over the sky.

I started evaluating the situation to find out what exactly went wrong with the machine, starting with a hardware analysis tools and a physical check up whether all was fine with the hardware Disks / Ram etc. just to find out the machine's hardware was working perfect.

I've also thoroughly investigated on Logs of Apache, MySQL, TinyProxy and Tor server and bind DNS and DJBDns which were happily living there for quite some time but didn't find anything strange.

Not on a last place I investigated TOP processes (with **top** command) and **iostat** and realized the CPU high burst lays in excessive Input / Output of Hard Drive. Checking the Qmail Mail server logs and the queue with **qmail-qstat** was a real surprise for me as on the queue there were about 9800 emails hanging unsent, most of which were obviously a spam, so I realized someone was heavily spamming through the server and started more thoroughly investigating ending up to a Wordpress Blog temp folder (writable

by all system users) which was existing under a Joomla directory infrastructure, so I guess **someone got hacked through the Joomla and uploaded the malicious php spammer script to the Wordpress blog**. I've instantly stopped and first **chmod 000** to stop being executed and after examining deleted **view73.php**, **javascript92.php** and **index8239.php** which were full of PHP values with binary encoded values and one was full of encoded strings which after being decoding were actually the **recepient's spammed emails**.

BTW, the **view*.php** **javascript*.php** and **index*.php** files were owned by **www-data** (the user with which Apache was owned), so obviously someone got hacked through some vulnerable joomla or wordpress script (as joomla there was quite obscure version 1.5 - where currently Joomla is at version branch 3.5), hence my guess is the spamming script was uploaded through Joomla XSS vulnerability).

As I was unsure whether the scripts were not also mirrored under other subdirectories of Joomla or WP Blog I had to scan further to check whether there are no other scripts infected with malware or trojan spammer codes, webshells, rootkits etc.

And after some investigation, I've actually caught the 3 scripts being mirrored under other website folders with other numbering on filename **view34.php** **javascript72.php**, **index8123.php** etc..

I've used 2 tools to scan and catch malware the trojan scripts and make sure no common rootkit is installed on the server.

- 1. Lynis (to check for rootkits)*
- 2. ISPProtect (Proprietary but superb Website malware scanner with a free trial)*

1. Lynis - Universal security auditing tool and rootkit scanner

Lynis is actually the well known **rkhunter**, I've used earlier to check servers BSD and Linux servers for rootkits.

To have up-to-date version of Lynis, I've installed it from source:

```
cd /tmp
wget https://cisofy.com/files/lynis-2.1.1.tar.gz
tar xvfz lynis-2.1.1.tar.gz
mv lynis /usr/local/
ln -s /usr/local/lynis/lynis /usr/local/bin/lynis
```

Then to **scan the server for rootkits**, first I had to **update its malware definition database** with:

lynis update info

Then to actually scan the system:

lynis audit system

*Plenty of things will be scanned but you will be asked on a multiple times **whether you would like to conduct different kind fo system services and log files, loadable kernel module rootkits and common places to check for installed rootkits or server placed backdoors.*** That's pretty annoying as you will have to press Enter on a multiple times.

```
[+] Initializing program
-----
- Detecting OS... [ DONE ]

-----
Program version:      2.1.1
Operating system:     Linux
Operating system name: Debian
Operating system version: 8.3
Kernel version:       3.16.0
Hardware platform:    x86_64
Hostname:             server1
Auditor:              [Unknown]
Profile:              /usr/local/lynis/default.prf
Log file:             /var/log/lynis.log
Report file:          /var/log/lynis-report.dat
Report version:       1.0
Plugin directory:     /usr/local/lynis/plugins
-----
- Checking profile file (/usr/local/lynis/default.prf)...
- Program update status... [ NO UPDATE ]

[+] System Tools
-----
- Scanning available tools...
- Checking system binaries...

[+] Plugins (phase 1)
-----
Note: plugins have more extensive tests, which may take a few minutes to complete

- Plugins enabled [ NONE ]

[+] Boot and services
-----
- Service Manager [ UNKNOWN ]
- Checking presence GRUB2 [ FOUND ]
- Checking for password protection [ WARNING ]
- Check running services (systemctl) [ DONE ]
  Result: found 28 running services
- Check enabled services at boot (systemctl) [ DONE ]
  Result: found 19 enabled services
- Check startup files (permissions) [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

Once scan is over you will get a **System Scan Summary** like in below screenshot:

Follow-up:

- Check the logfile for more details (`less /var/log/lynis.log`)
- Read security controls texts (<https://cisofy.com>)
- Use `--upload` to upload data (Lynis Enterprise users)

Lynis security scan details:

Hardening index : 69 [#####]
Tests performed : 211
Plugins enabled : 0

Quick overview:

- Firewall [V] - Malware scanner [V]

Lynis Modules:

- Heuristics Check [NA] - Security Audit [V]
- Compliance Tests [X] - Vulnerability Scan [V]

Files:

- Test and debug information : `/var/log/lynis.log`
- Report data : `/var/log/lynis-report.dat`

Tip: Disable all tests which are not relevant or are too strict for the purpose of this particular machine. This will remove unwanted suggestions and also boost the hardening index. Each test should be properly analyzed to see if the related risks can be accepted, before disabling the test.

Lynis 2.1.1

Auditing, hardening and compliance for BSD, Linux, Mac OS and Unix

Copyright 2007-2015 - CISOfy, <https://cisofy.com>

Enterprise support and plugins available via CISOfy

Lynis suggests also a very good things that might be tampered to make the system more secure, so using some of its output when I have time I'll work out on hardening all servers.

To prevent further incidents and keep an eye on servers I've deployed Lynis scan via cron job once a month on all servers, I've placed under a root cronjob on every first day of month in following command:

```
server:~# crontab -u root -e
0 3 1 * * /usr/local/bin/lynis --quick 2>&1 | mail -s "lynis output of my server" admin-
mail@my-domain.com)
```

2. ISPProtect - Website malware scanner

ISPProtect is a malware scanner for web servers, I've used it to scan all installed CMS systems like Wordpress, Joomla, Drupal etc.

ISPProtect is great for PHP / Python / Perl and other CMS based frameworks.

ISPProtect contains 3 scanning engines: **a signature based malware scanner, a heuristic malware scanner, and a scanner to show the installation directories of outdated CMS systems.**

Unfortunately it is not free software, but I personally used the **FREE TRIAL** option which can be used without registration to test it or clean an infected system.

I first webserver first locally for the infected site and then globally for all the other shared hosting websites.

As I wanted to check also rest of hosted websites, I've run ISPProtect over the all bunch of installed websites.

Pre-requirement of ISPProtect is to have a working *PHP Cli and Clamav Anti-Virus installed* on the server thus on RHEL (RPM) based servers make sure you have it installed if not:

```
server:~# yum -y install php
```

```
server:~# yum -y install clamav
```

Debian based Linux servers web hosting admins that doesn't have php-cli installed should run:

```
server:~# apt-get install php5-cli
```

```
server:~# apt-get install clamav
```

Installing **ISPProtect** from source is with:

```
mkdir -p /usr/local/ispprotect
chown -R root:root /usr/local/ispprotect
chmod -R 750 /usr/local/ispprotect
cd /usr/local/ispprotect
wget http://www.ispprotect.com/download/ispp_scan.tar.gz
tar xzf ispp_scan.tar.gz
rm -f ispp_scan.tar.gz
ln -s /usr/local/ispprotect/ispp_scan /usr/local/bin/ispp_scan
```

To initiate scan with **ISPProtect** just invoke it:

```
server:~# /usr/local/bin/ispp_scan
```



I've used it as a trial

Please enter scan key: **trial**

Please enter path to scan: **/var/www**

You will be shown the scan progress, be patient because on a multiple shared hosting servers with few hundred of websites.

The tool will take really, really long so you might need to leave it for 1 hr or even more depending on how many source files / CSS / Javascript etc. needs to be scanned.

Once scan is completed scan and infections found logs will be stored under **/usr/local/ispprotect**, under separate files for different Website Engines and CMSes:

After the scan is completed, you will find the results also in the following files:

Malware => /usr/local/ispprotect/found_malware_20161401174626.txt
Wordpress => /usr/local/ispprotect/software_wordpress_20161401174626.txt
Joomla => /usr/local/ispprotect/software_joomla_20161401174626.txt
Drupal => /usr/local/ispprotect/software_drupal_20161401174626.txt
Mediawiki => /usr/local/ispprotect/software_mediawiki_20161401174626.txt
Contao => /usr/local/ispprotect/software_contao_20161401174626.txt
Magentocommerce =>
/usr/local/ispprotect/software_magentocommerce_20161401174626.txt
Woltlab Burning Board =>
/usr/local/ispprotect/software_woltlab_burning_board_20161401174626.txt
Cms Made Simple => /usr/local/ispprotect/software_cms_made_simple_20161401174626.txt
Phpmyadmin => /usr/local/ispprotect/software_phpmyadmin_20161401174626.txt
Typo3 => /usr/local/ispprotect/software_typo3_20161401174626.txt
Roundcube => /usr/local/ispprotect/software_roundcube_20161401174626.txt

ISPProtect is really good in results is definitely the best malicious scripts / trojan / trojan / webshell / backdoor / spammer (hacking) scripts tool available so if your company could afford it you better buy a license and settle a periodic cron job scan of all your servers, like lets say:


```
server:~# crontab -u root -e
0 3 1 * * /usr/local/ispprotect/ispp_scan --update && /usr/local/ispprotect/ispp_scan
--path=/var/www --email-results=admin-email@your-domain.com --non-interactive --scan-
key=AAA-BBB-CCC-DDD
```

Unfortunately ispprotect is quite expensive so I guess most small and middle sized shared hosting companies will be unable to afford it.

But even for a one time run this tools worths the try and will save you an hours if not days of system investigations.

I'll be glad to hear from readers if aware of any available free software alternatives to ISPProtect. The only one I am aware is **Linux Malware Detect (LMD)**.

I've used LMD in the past but as of time of writting this article it doesn't seems working any more so I guess the tool is currently unsupported / obsolete.