

Hệ thống quét Malware và Rootkits trên Linux

admin Sun, Apr 14, 2019 [Cài Đặt Cơ Bản & Hướng Dẫn](#) 0 1909



Linux

Malware (t? ghép c?a malicious và software) là ph?n m?m ??c h?i, nó là m?t lo?i ph?n m?m h? th?ng do các hacker t?o ra nh?m gây h?i cho các máy tính.

Rootkit là ph?n m?m ho?c b? công c? ph?n m?m che gi?u s? t?n t?i c?a m?t ph?n m?m khác mà th??ng là virus xâm nh?p vào h? th?ng máy tính. Rootkit th??ng ??c hacker dùng sau khi chi?m ??c quy?n truy c?p vào h? th?ng máy tính. Nó s? che d?u d? li?u h? th?ng, t?p tin ho?c ti?n trình ?ang ch?y, t? ?ó hacker có th? vào h? th?ng máy tính mà không th? bi?t ??c.

Trong bài viết này tôi sẽ giới thiệu cho các bạn 3 phần mềm dùng để quét Malware và Rootkit.

1. **Chkrootkit.**
2. **Rkhunter.**
3. **ISPProtect.**

1.Chkrootkit

Chkrootkit là phần mềm quét rootkit miễn phí, nó kiểm tra máy chủ của bạn xem những quy trình rootkit đang hoạt động và so sánh với các tệp rootkit đã biết.

Cài đặt

Nếu bạn đang dùng Ubuntu hoặc Debian các bạn có thể gõ lệnh sau:

```
# apt-get install chkrootkit
```

Hoặc có thể download qua trang web <http://www.chkrootkit.org/> và cài đặt như sau

```
# wget --passive-ftp ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz# tar xvfz chkrootkit.tar.gz# cd chkrootkit-*/# make sense
```

Đổi tên thư mục thành chkrootkit

```
# cd ../# mv chkrootkit-0.52/ /usr/local/chkrootkit
```

Tạo liên kết đến thư mục bin

```
# ln -s /usr/local/chkrootkit/chkrootkit /usr/local/bin/chkrootkit
```

Và bây giờ hãy kiểm tra máy chủ của bạn bằng lệnh:

```
# chkrootkit
```

```
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... not tested: can't exec
Checking `rexedcs'... not found
Checking `sniffer'... not tested: can't exec ./ifpromisc
Checking `w55808'... not infected
Checking `wted'... not tested: can't exec ./chkwtmp
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... not tested: can't exec ./chklastlog
Checking `chkutmp'... not tested: can't exec ./chkutmp
Checking `OSX_RSPLUG'... not tested
```

Chúng ta cũng có thể cấu hình cho chkrootkit tự động làm việc bằng cron và máy sẽ gửi thông báo vào email chúng ta.

Trước khi cấu hình tự động chúng ta cần phải xác định trước đường dẫn của lệnh chkrootkit bằng cách nhập lệnh dưới đây

```
# which chkrootkit
```

Chạy lệnh crontab

```
# crontab -e
```

Nhập nội dung sau vào file

```
0 3 * * * /usr/sbin/chkrootkit 2>&1 | mail -s "chkrootkit
output of my server" you@yourdomain.com)
```

Máy s? t? ??ng ch?y l?nh này vào lúc 3 gi? sáng. Thay th? ??a ch? email b?ng ??a ch? email th?c c?a b?n.

2.Lynis

Lynis là công c? ki?m tra an ninh ki?u ph? c?p và quét rootkit, nó th?c hi?n m?t bài ki?m tra chi ti?t và nhi?u khía c?nh an ninh và c?u hình c?a h? th?ng.

?? cài ??t Lynis các b?n làm theo b??c sau

```
# cd /usr/local/# wget https://cisofy.com/files/lynis-2.4.8.tar.gz# tar xvfz lynis-2.4.8.tar.gz# ln -s /usr/local/lynis/lynis /usr/local/bin/lynis
```

Chúng ta ch?y l?nh sau ?? update phiên b?n m?i nh?t

```
# lynis update info
```

Ch?y l?nh sau ?? b?t ??u quét

```
# lynis audit system
```

Ho?c ch?y l?nh quét nhanh

```
# lynis --quick
```

```
Lynis security scan details:

Hardening index : 64 [#####]
Tests performed : 207
Plugins enabled : 0

Components:
- Firewall [X]
- Malware scanner [V]

Lynis Modules:
- Compliance Status [?]
- Security Audit [V]
- Vulnerability Scan [V]

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

=====

Lynis 2.4.8

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2017, CISOFy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /usr/local/lynis/default.prf for all settings)
```

Bây giờ chúng ta sẽ cài đặt Lynis và thêm nó vào cron

```
# crontab -e
```

Thêm dòng sau vào đầu file

```
0 3 * * * /usr/local/bin/lynis --quick 2>&1 | mail -s "lynis output of my server" you@yourdomain.com)
```

Hiện nay sẽ chạy lynis vào 3.00h mỗi hôm. Thay thế địa chỉ email bằng địa chỉ email thích hợp của bạn.

3.ISPProtect

ISPProtect là phần mềm quét malware cho các máy chủ web. ISPProtect chia 5 công cụ quét:

- Máy quét phần mềm độc hại dựa trên chủ ký.
- Máy quét phần mềm độc hại nội tuyến.
- Một máy quét nội tuyến các thành phần cài đặt của hệ thống CMS nội tuyến.
- Máy quét nội tuyến các plugin WordPress đã nội tuyến của toàn bộ máy chủ.
- Máy quét nội tuyến các dữ liệu kiểm tra các dữ liệu MySQL và nội tuyến độc hại.

ISPProtect là phần thu phí, nhưng có một bản dùng thử miễn phí có thể được sử dụng mà không cần đăng ký kiểm tra nó hoặc đăng nhập hệ thống bất kỳ.

ISPProtect yêu cầu PHP được cài đặt trên máy chủ

Trên Ubuntu 16

```
# apt-get install php7.0-cli -y
```

Trên Centos

```
# yum install php -y
```

Cài đặt xong php chúng ta sẽ cài đặt ISPProtect

```
# 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
```

?? b?t ??u quét chúng ta ch?y l?nh

```
# ispp_scan
```

Dòng ??u máy s? h?i key ,n?u b?n mua key thì nh?p key còn dùng th? thì nh?p 'TRIAL'

Dòng th? hai máy s? h?i b?n mu?n quét th? m?c nào, chúng ta s? nh?p vào th? m?c ch?a code web

```
root@Mr:/tmp# ispp_scan
```

```
ISPProtect
```

```
WebScanner
```

```
Version 1.20.6
```

```
(c) 2015-2017 by ISPConfig UG  
all rights reserved
```

```
ionCube Check succeeded.
```

```
Please enter scan key (or TRIAL if you have none, yet): TRIAL
```

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

K?t.

Trên đây tôi đã hướng dẫn cho các bạn 3 phần mềm dùng để quét Malware và Rootkit. Hy vọng là các bạn trong các bài tiếp theo, chúc các bạn thành công!

Online URL: <https://huongdan.maxserver.com/article-147.html>