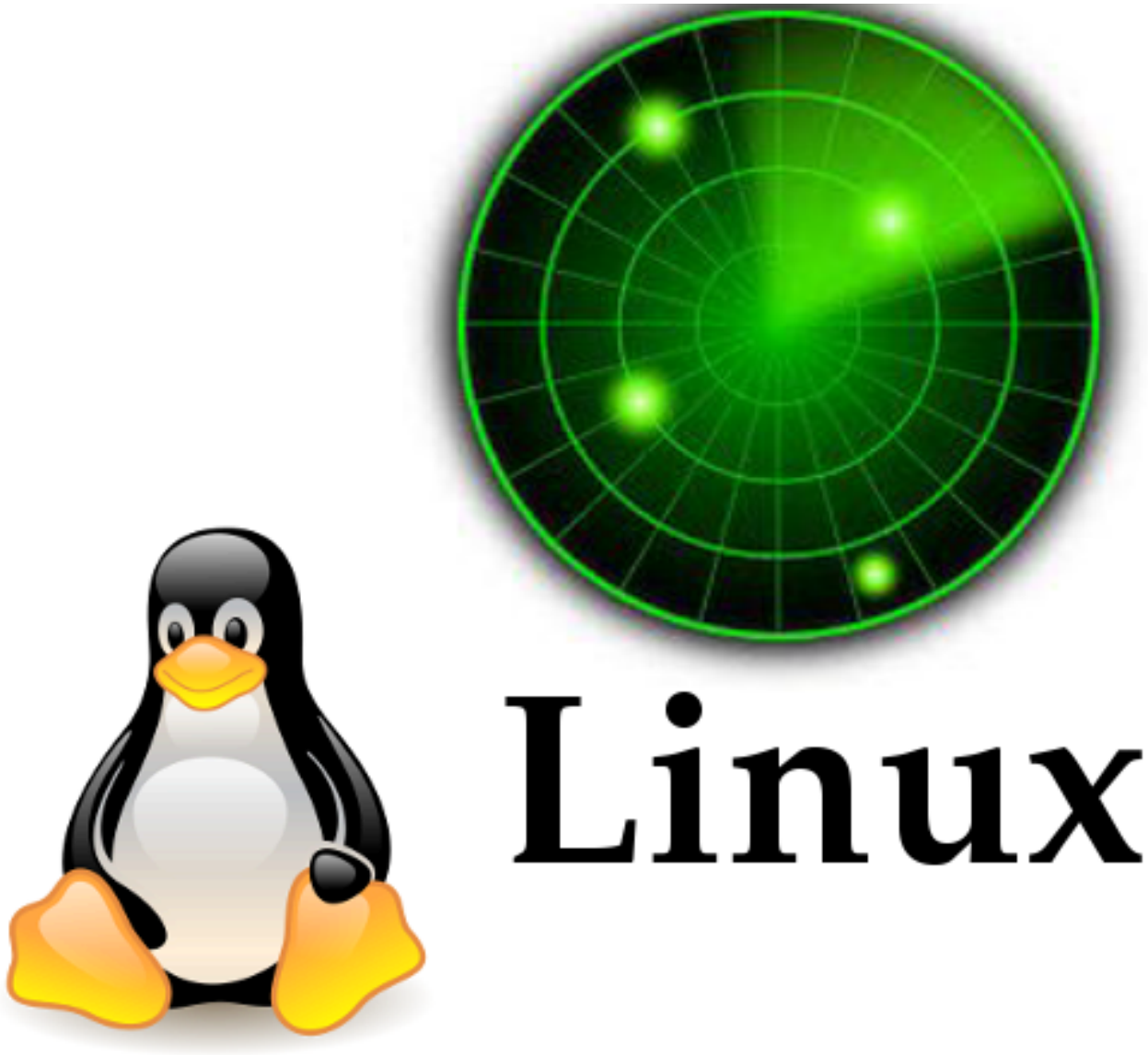
H??ng d?n quét Malware và Rootkits trên Linux

admin Sun, Apr 14, 2019 Cài Đặt Cơ Bản & Hướng Dẫn 0 1664



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 vi?t này tôi s? gi?i thi?u cho các b?n 3 ph?n m?m dùng d? quét Malware và Rootkit.

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

1.Chkrootkit

Chkrootkit là ph?n m?m quét rootkit ki?u c?, nó ki?m tra máy ch? c?a b?n xem nh?ng quy trình rootkit ?áng ng? và so sánh v?i các t?p rootkit ?ã bi?t.

Cài ??t

N?u b?n ?ang dùng Ubuntu ho?c Debian các b?n có th? gõ l?nh sau:

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

Ho?c có th? download qua trang web **http://www.chkrootkit.org/** và cài ??t nh? sau

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

??i tên th? m?c thành chkrootkit

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

T?o liên k?t ??n th? m?c bin

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

Và bây gi? hãy ki?m tra máy ch? c?a b?n b?ng l?nh:

```
# 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 c?ng có th? c?u hình cho chkrookit t? ??ng làm vi?c b?ng crond và máy s? g?i thông báo vào email chúng ta.

Tr??c khi c?u hình t? ??ng chúng ta c?n ph?i xác ??nh ???c ???ng d?n c?a l?nh chkrootkit b?ng cách nh?p l?nh d??i

```
# which chkrootkit
```

Ch?y l?nh crontab

```
# crontab -e
```

Nh?p n?i 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/ly
nis/lynis /usr/local/bin/lynis
```

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

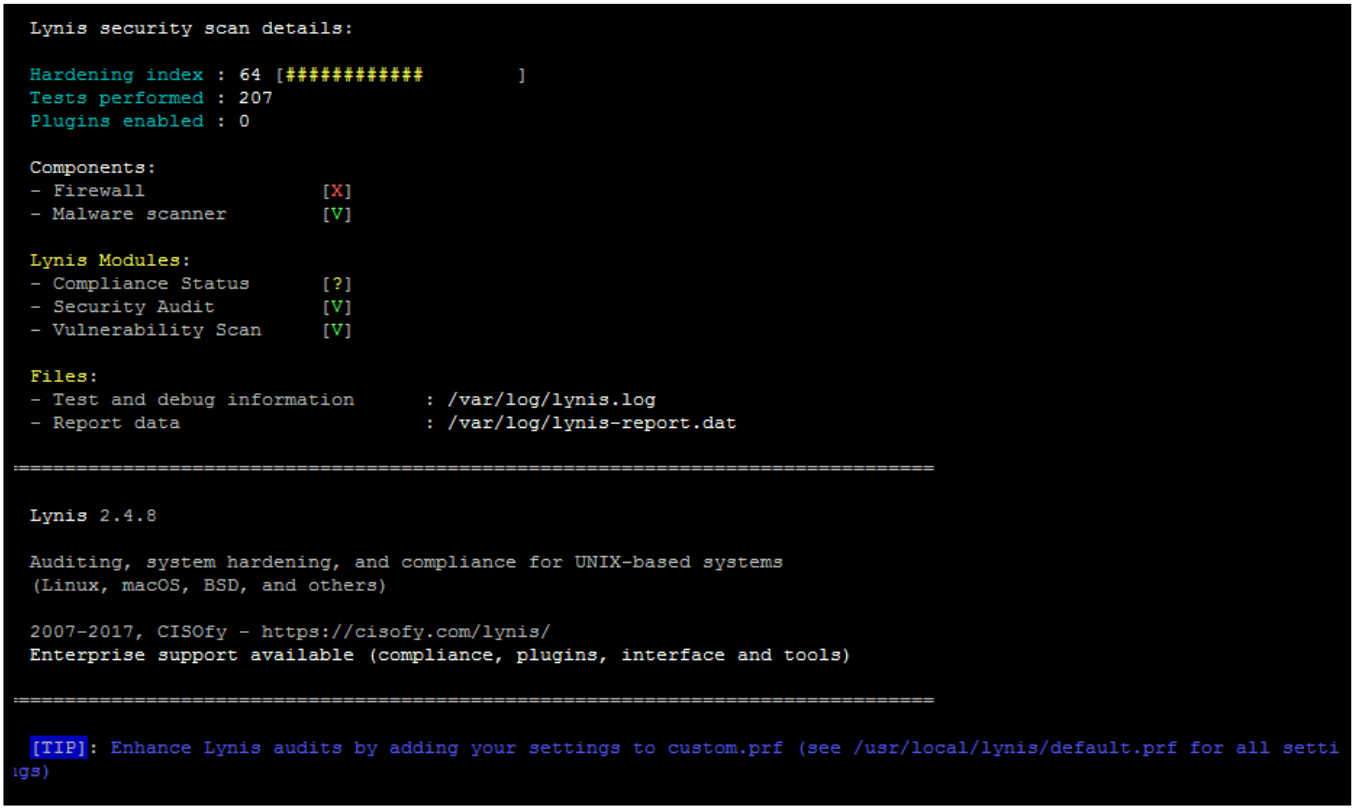
```
# lynis update info
```

Ch?y l?nh sau ?? b?t ??u quét

```
# lynis audit system
```

Ho?c ch?y l?nh quét nhanh

```
# lynis --quick
```



Bây gi? chúng ta s? ??t Lynis t? ??ng vào ban ?êm

```
# crontab -e
```

Thêm dòng sau vào d??i file

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

?i?u này s? ch?y lynis vào 3.00h m?i ?êm. Thay th? ??a ch? email b?ng ??a ch? email th?c c?a b?n.

3.ISPProtect

ISPProtect là ph?n m?m quét malware cho các máy ch? web. ISPProtect ch?a 5 công c? quét:

- Máy quét ph?n m?m ??c h?i d?a trên ch? ký.
- Máy quét ph?n m?m ??c h?i n?i ti?ng.
- M?t máy quét ?? hi?n th? các th? m?c cài ??t c?a h? th?ng CMS l?i th?i.
- Máy quét hi?n th? t?t c? các plugin WordPress ?ã l?i th?i c?a toàn b? máy ch?.
- Máy quét n?i dung c? s? d? li?u ki?m tra các c? s? d? li?u MySQL v? n?i dung ??c h?i.

ISPProtect là ph?n thu phí, nh?ng có m?t b?n dùng th? mi?n phí có th? ???c s? d?ng mà không c?n ??ng ký ?? ki?m tra nó ho?c d?n d?p h? th?ng b? nhi?m.

ISPProtect yêu c?u PHP ???c cài ??t trên máy ch?

Trên Ubuntu 16

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

Trên Centos

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

Cài ??t xong php chúng ta s? cài ??t ISPProtect

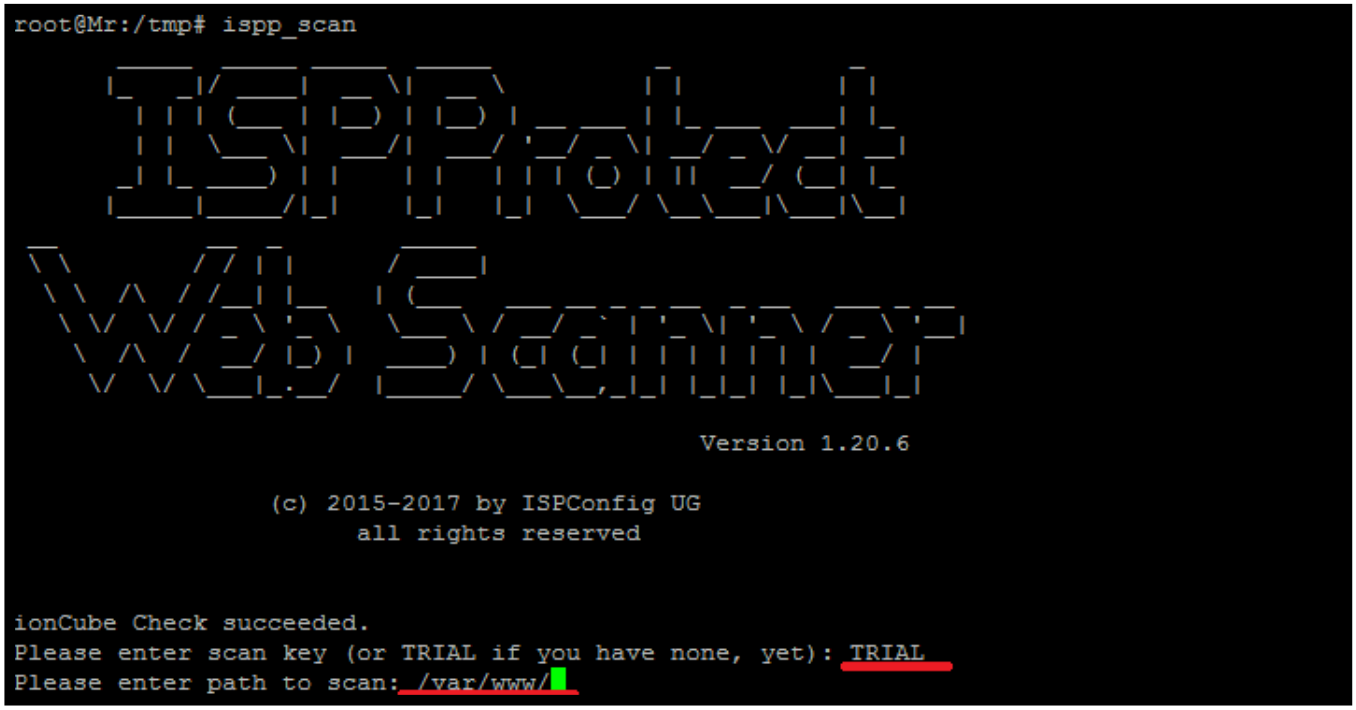
```
# mkdir -p /usr/local/ispprotect# chown -R root:root /usr/
local/ispprotect# chmod -R 750 /usr/local/ispprotect# cd /
usr/local/ispprotect# wget http://www.ispprotect.com/downl
oad/ispp_scan.tar.gz# tar xzf ispp_scan.tar.gz# rm -f ispp
_scan.tar.gz# ln -s /usr/local/ispprotect/ispp_scan /usr/l
ocal/bin/ispp_scan
```

?? 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



K?t.

Trên ?ây tôi ?ã h??ng d?n cho các b?n 3 ph?n m?m dùng d? quét Malware và Rootkit. H?n g?p l?i các b?n trong các bài ti?p theo, chúc các b?n thành công!

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