Hướng dẫn rà soát phần mềm độc hại trên Linux

DDos · 13/02/2022

Trên Windows, có rất nhiều phần mềm cũng như giải pháp để phát hiện và ngăn chặn phần mềm độc hại. Tuy nhiên, trên các phiên bản phân phối của Linux, dường như có ít các giải pháp để phát hiện và ngăn chặn chúng. Vì vậy trong bài viết này, mình sẽ hướng dẫn các bạn cách rà soát phần mềm độc hại bằng các công cụ có sẵn trên Linux.

Các chương trình độc hại thường có mục đích cụ thể. Để đạt được mục đích này, malware cần thực hiện một số hoạt động cụ thể, chính những hoạt động này để lại dấu vết trên hệ thống, từ đó giúp chúng ta có thể điều tra và phát hiện chúng.

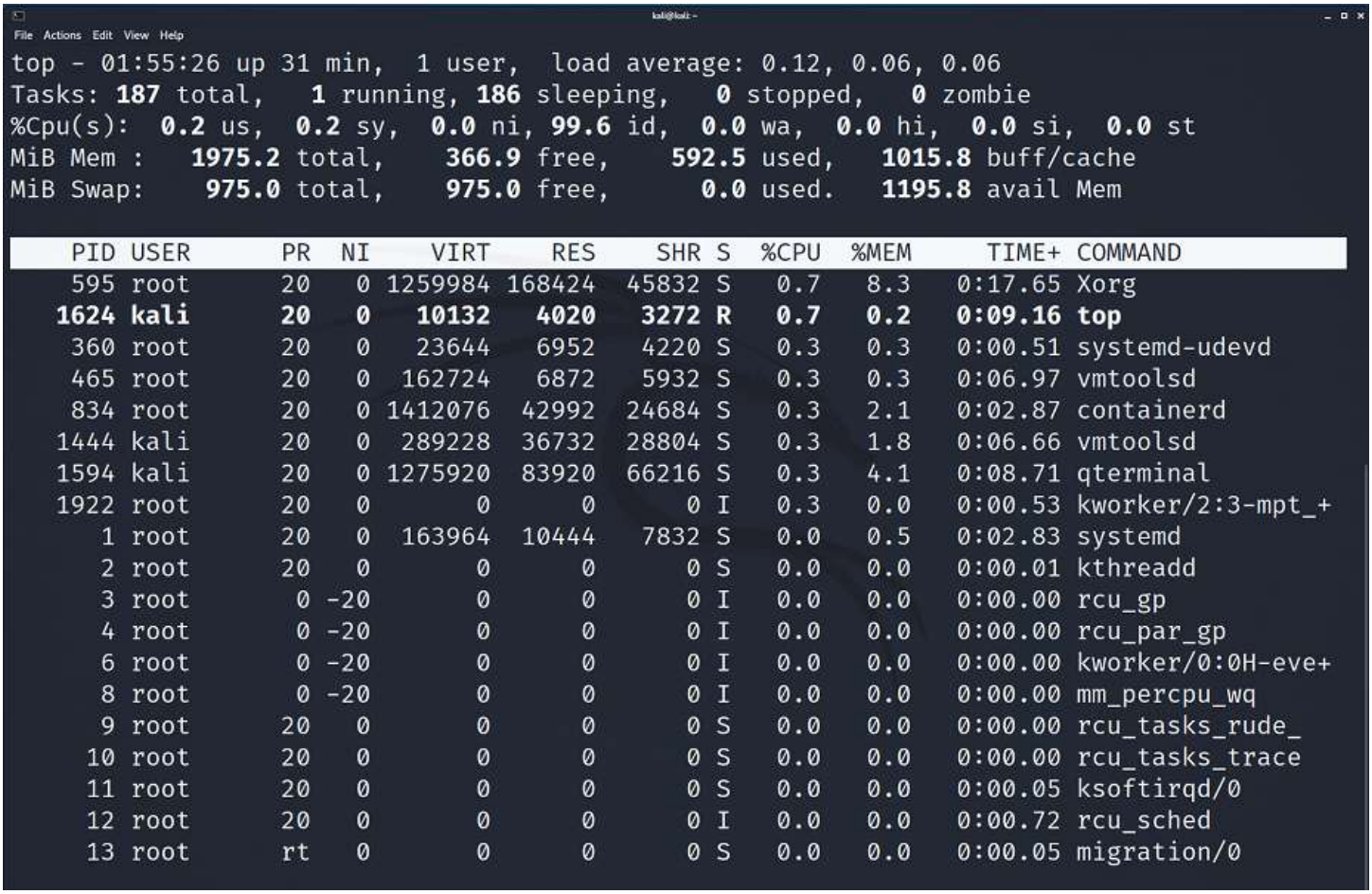
Các biểu hiện thường thấy ở phần mềm độc hại là:

- Nghe trên một hoặc một số cổng xác định hoặc giao tiếp với máy chủ kiểm soát và ra lệnh (C2)
- Tăng mức tiêu thụ tài nguyên máy tính như RAM, CPU, băng thông mạng...

Rà soát phần mềm độc hại

1. Kiểm tra mức độ tiêu tốn tài nguyên

Để kiểm tra tiến trình nào tiêu tốn tài nguyên hệ thống như CPU, RAM, chúng ta sử dụng lệnh: top



Ở đây, chúng ta kiểm tra xem tiến trình nào sử dụng nhiều CPU, RAM và các tên các tiến trình đáng ngờ.

Khi tìm thấy tiến trình đáng ngờ, bạn có thể xem thông tin chi tiết bằng lệnh:

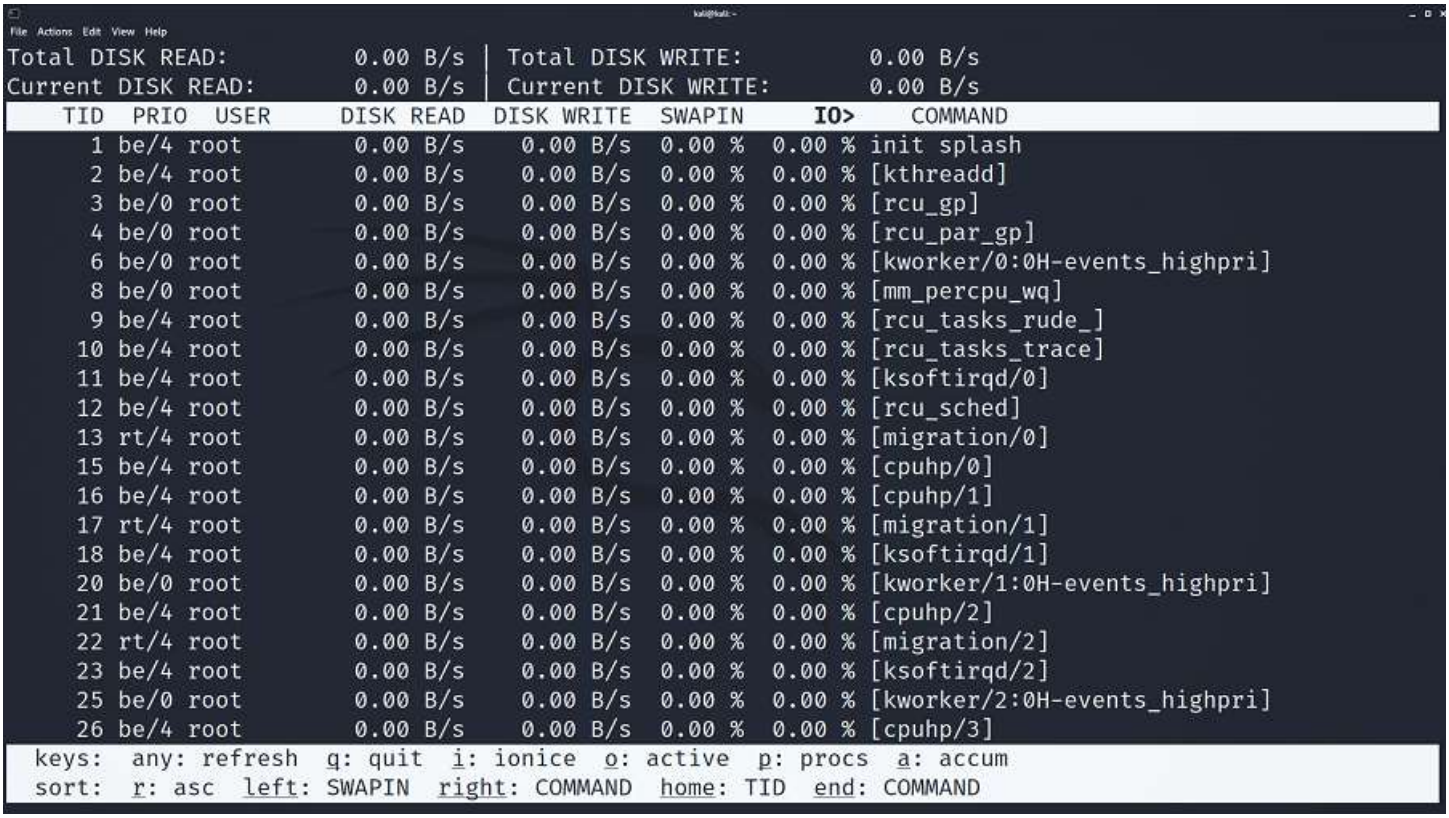
ps -f --forest -C tên_tiến_trình

Để kết thúc tiến trình đáng ngờ, bạn dùng lệnh:

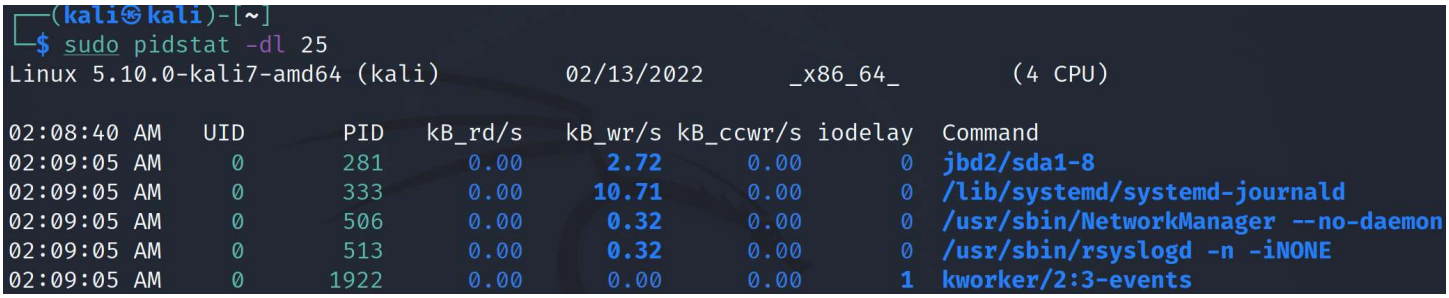
kill -9 pid_tiến trình

2. Kiểm tra mức sử dụng ổ đĩa

Để kiểm tra mức độ sử dụng ổ đĩa, chúng ta dùng công cụ *iotop.*

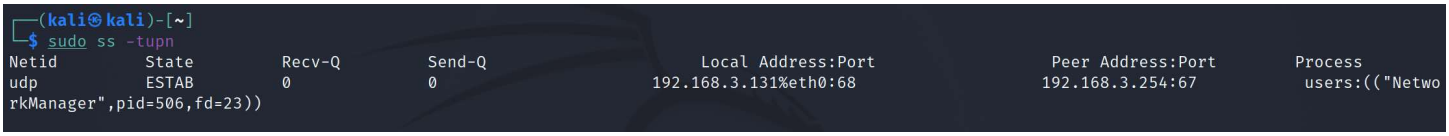


Để xem tiến trình nào đọc và ghi từ ổ đĩa trong mỗi 25 giây, ta dùng lệnh *sudo pidstat -dl 25*



3. Kiểm tra các cổng mở

Phần mềm độc hại thường sẽ chạy trên một cổng nhất định, cố gắng mở cổng và thiết lập kết nối. Để xem các kết nối được thiết lập, ta dùng lệnh *sudo ss -tupn*



Khi thấy một kết nối đáng ngờ, chúng ta có thể chặn chúng bằng cách sử dụng *iptables.*

Để xem trạng thái của các cổng đang mở, chúng ta dùng lệnh *sudo ss -tulpn*

```
┌──(kali㉿kali)-[~]
└─$ sudo ss -tulpn
Netid         State         Recv-Q         Send-Q                 Local Address:Port                  Peer Address:Port         Process
```

4. Phân tích cách tệp được mở

Để xem các tệp nào được mở có liên kết với một tiến trình cụ thể, chúng ta dùng lệnh *sudo lsof* | *grep tên_tiến_trình*

```
File  Actions  Edit  View  Help
lsof       2222                root  txt       REG              8,1   171488     271060 /usr/bin/lsof
lsof       2222                root  mem       REG              8,1  3041456     266619 /usr/lib/locale/locale-archive
lsof       2222                root  mem       REG              8,1   143768     265339 /usr/lib/x86_64-linux-gnu/libpthread-2.33.so
lsof       2222                root  mem       REG              8,1    22864     265030 /usr/lib/x86_64-linux-gnu/libdl-2.33.so
lsof       2222                root  mem       REG              8,1   617128     264236 /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0.10.1
lsof       2222                root  mem       REG              8,1  1835120     264663 /usr/lib/x86_64-linux-gnu/libc-2.33.so
lsof       2222                root  mem       REG              8,1   166120     264244 /usr/lib/x86_64-linux-gnu/libselinux.so.1
lsof       2222                root  mem       REG              8,1    27002     278065 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
lsof       2222                root  mem       REG              8,1   202552     264657 /usr/lib/x86_64-linux-gnu/ld-2.33.so
lsof       2222                root    0u      CHR            136,0      0t0          3 /dev/pts/0
lsof       2222                root    1w     FIFO             0,12      0t0      45790 pipe
lsof       2222                root    2u      CHR            136,0      0t0          3 /dev/pts/0
lsof       2222                root    3r      DIR             0,20        0          1 /proc
lsof       2222                root    4r      DIR             0,20        0      34648 /proc/2222/fd
lsof       2222                root    5w     FIFO             0,12      0t0      34657 pipe
lsof       2222                root    6r     FIFO             0,12      0t0      34658 pipe
lsof       2223                root  cwd       DIR              8,1     4096     794702 /home/kali
lsof       2223                root  rtd       DIR              8,1    36864          2 /
lsof       2223                root  txt       REG              8,1   171488     271060 /usr/bin/lsof
lsof       2223                root  mem       REG              8,1  3041456     266619 /usr/lib/locale/locale-archive
lsof       2223                root  mem       REG              8,1   143768     265339 /usr/lib/x86_64-linux-gnu/libpthread-2.33.so
lsof       2223                root  mem       REG              8,1    22864     265030 /usr/lib/x86_64-linux-gnu/libdl-2.33.so
lsof       2223                root  mem       REG              8,1   617128     264236 /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0.10.1
lsof       2223                root  mem       REG              8,1  1835120     264663 /usr/lib/x86_64-linux-gnu/libc-2.33.so
lsof       2223                root  mem       REG              8,1   166120     264244 /usr/lib/x86_64-linux-gnu/libselinux.so.1
lsof       2223                root  mem       REG              8,1   202552     264657 /usr/lib/x86_64-linux-gnu/ld-2.33.so
lsof       2223                root    4r     FIFO             0,12      0t0      34657 pipe
lsof       2223                root    7w     FIFO             0,12      0t0      34658 pipe
```

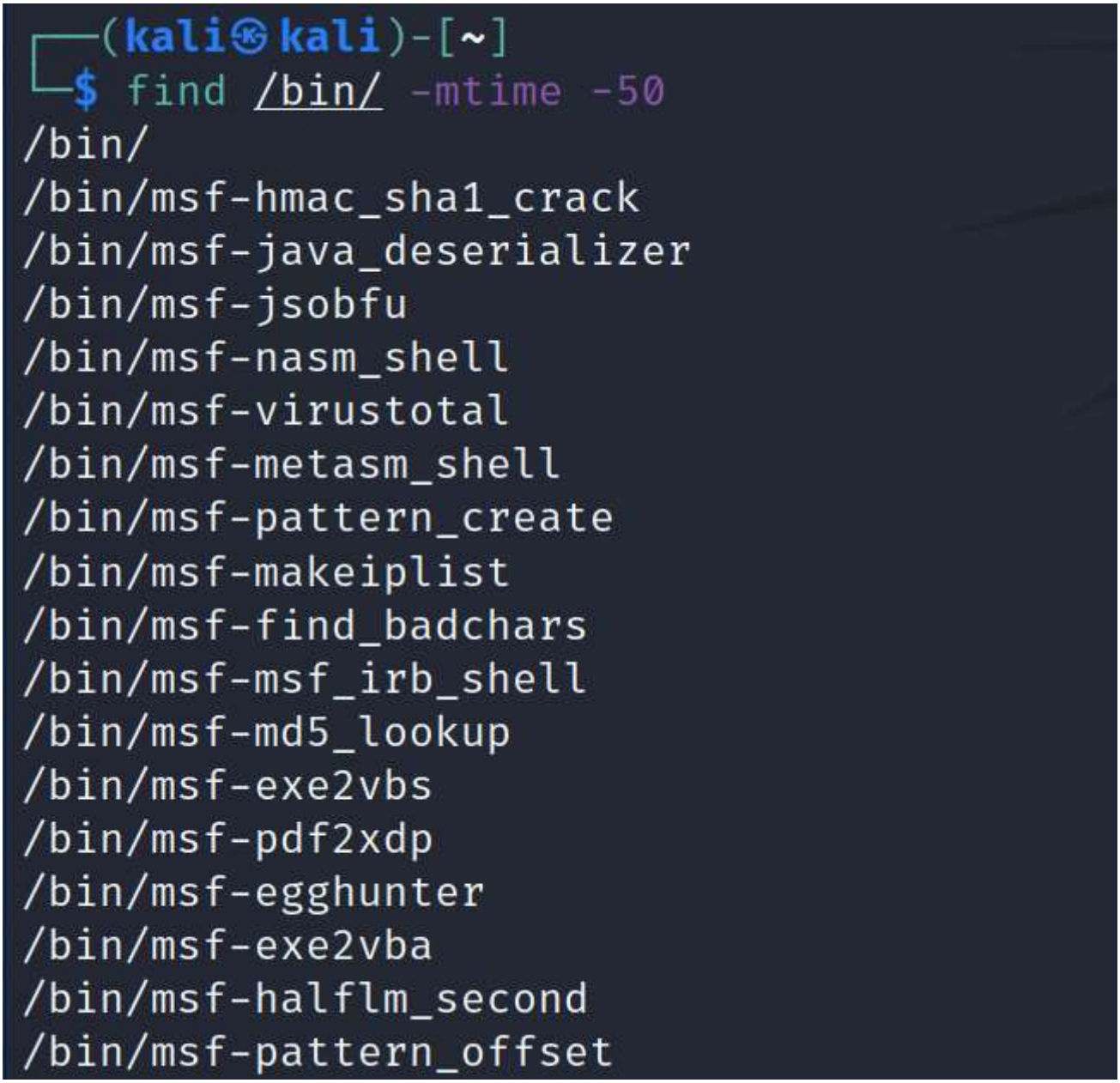
5. Kiểm tra các dịch vụ đang chạy

Để kiểm tra các dịch vụ đang chạy, chúng ta dùng lệnh *systemctl list-unit-files* | *grep active*

6. Tìm các tệp được tạo gần đây

Phần mềm độc hại thường tạo ra một số tệp trên hệ thống cho một mục đích nhất định, chúng ta có thể tìm các tệp được tạo gần đây với lệnh find.

Ví dụ, để tìm các tệp được tạo trong 50 ngày trong thư mục , ta dùng lệnh *find /bin/ -mtime -50*



Để xem tất cả các tệp được truy cập trong 50 ngày, ta dùng lệnh *find / -atime 50*

Để tìm các thuộc tính (permission, owner, group) đã bị thay đổi trong 50 phút trước đó, ta dùng lệnh *find / -cmin -50*

Để tìm tất cả các tệp đã được truy cập trong 60 phút trước đó, ta dùng lệnh *find / -amin -60*

***7.* Kiểm tra các dịch vụ chạy cùng với hệ thống khi khởi động**

Phần mềm độc hại sẽ cố gắng tồn tại bền bỉ trên hệ thống, do đó, nó thường tìm cách khởi chạy cùng với hệ thống khi khởi động. Để kiểm tra các dịch vụ tự động chạy khi hệ thống khởi động, ta dùng lệnh

systemctl list-unit-files | grep enabled

```
┌──(kali㉿kali)-[~]
└─$ systemctl list-unit-files | grep enabled
run-vmblock\x2dfuse.mount                      enabled         enabled
binfmt-support.service                         enabled         enabled
console-setup.service                          enabled         enabled
cron.service                                   enabled         enabled
docker.service                                 enabled         enabled
e2scrub_reap.service                           enabled         disabled
getty@.service                                 enabled         enabled
haveged.service                                enabled         enabled
keyboard-setup.service                         enabled         enabled
lightdm.service                                enabled         disabled
ModemManager.service                           enabled         enabled
networking.service                             enabled         enabled
NetworkManager-dispatcher.service              enabled         disabled
NetworkManager-wait-online.service             enabled         disabled
NetworkManager.service                         enabled         enabled
nfs-common.service                             masked          enabled
open-vm-tools.service                          enabled         enabled
rsync.service                                  enabled         enabled
rsyslog.service                                enabled         enabled
rtkit-daemon.service                           disabled        enabled
smartmontools.service                          enabled         enabled
sudo.service                                   masked          enabled
systemd-fsck-root.service                      enabled-runtime disabled
systemd-networkd.service                       disabled        enabled
systemd-pstore.service                         enabled         enabled
systemd-remount-fs.service                     enabled-runtime disabled
systemd-resolved.service                       disabled        enabled
docker.socket                                  enabled         enabled
```

8. Kiểm tra Cron job.

Để tránh sự phát hiện, phần mềm độc hại thường lập lịch để chạy một tác vụ nào đó trong khoảng thời gian xác định. Để đạt được điều này, malware thường sử dụng *cron.* Để kiểm tra tất cả các tác vụ đã được lập lịch cho tất cả user trên hệ , ta dùng lệnh *for user in* $(cut - f1 - d : /etc/passwd); do sudo crontab - u user -l 2>/dev/null$ | *grep -v '^#'; done*

***9.* Kiểm tra các tập lệnh được thực thi tự động**

Linux có nhiều tập lệnh chạy tự động khi user đăng nhập vào hệ thống. Phần mềm độc hại lợi dụng tính năng này để tự động khởi chạy. Do đó, chúng ta cần rà soát các tệp và thư mục như

- **/etc/profile**
- **/etc/profile.d/***
- **~/.bash_profile**
- **~/.bashrc**
- **/etc/bashrc**

Chỉnh sửa lần cuối bởi người điều hành: 25/02/2022

> mattcilus

Lam Trường

ok nha ad

Mời các bạn tham gia Group WhiteHat để thảo luận và cập nhật tin tức an ninh mạng hàng ngày.
Lưu ý từ WhiteHat: Kiến thức an ninh mạng để phòng chống, không làm điều xấu. Luật pháp liên quan

M **Mũ Nồi**

Bài viết rất hữu ích cám ơn admin

Mời các bạn tham gia Group WhiteHat để thảo luận và cập nhật tin tức an ninh mạng hàng ngày.
Lưu ý từ WhiteHat: Kiến thức an ninh mạng để phòng chống, không làm điều xấu. Luật pháp liên quan

Bạn phải đăng nhập hoặc đăng ký để phản hồi tại đây.

Chuyên mục

Tin tức
WarGame
Thảo luận
Video

Bài viết liên quan

Hướng dẫn phân tích extension trình duyệt độc hại với ExtAnalysis
15/05/2022 · 0

Hướng dẫn xử lý các lỗi của hệ thống phát sinh do mã độc
15/03/2022 · 3

Hướng dẫn rà soát virus, mã độc cơ bản cực kì đơn giản
14/11/2021 · 8

[Tool Re 2] Hướng dẫn debug động virus bằng IDA
10/09/2021 · 1

[Tool Re 1] Hướng dẫn debug động virus bằng IDA
03/08/2021 · 0

Xin hướng dẫn giải mã dữ liệu bị đổi sang đuôi .mpal
09/06/2020 · 1