

# CompTIA PenTest+

Hướng dẫn đến

Kiểm tra thâm nhập, 1e

Mô-đun 10: Các vectơ tấn công máy chủ  
và các cuộc tấn công công nghệ đám mây

# Mục tiêu của mô-đun (1 trong 3)

Đến cuối mô-đun này, bạn sẽ có thể:

1. Mô tả các cuộc tấn công vào máy chủ cụ thể không phải là hoạt động như lợi dụng lỗi cấu hình quyền, truy cập thông tin xác thực đã lưu trữ, khai thác thông tin xác thực mặc định và tấn công bằng cách dùng vũ lực
2. Mô tả các phương pháp tấn công truy cập từ xa khác nhau như ẩn các cuộc tấn công bằng SSH, NETCAT/Ncat, truy cập từ xa của khung Metasploit và proxy
3. Mô tả các cuộc tấn công máy chủ Linux/Unix như SUID/GUID SUDO, nâng cấp shell và khai thác kernel, thu thập thông tin xác thực và bẻ khóa mật khẩu

## Mục tiêu của mô-đun (2 trong 3)

Đến cuối mô-đun này, bạn sẽ có thể:

4. Mô tả các cuộc tấn công vào máy chủ Windows như băm thông tin xác thực, bí mật LSA, cơ sở dữ liệu SAM và khai thác hạt nhân, thu thập thông tin xác thực và bẻ khóa mật khẩu
5. Mô tả các cuộc tấn công vào ảo hóa như máy ảo (VM), hypervisor và khai thác kho lưu trữ VM, thoát VM và khai thác container

# Mục tiêu của mô-đun (3 trong 3)

Đến cuối mô-đun này, bạn sẽ có thể:

6. Mô tả các cuộc tấn công vào các mục tiêu dựa trên đám mây như tài khoản, cấu hình sai, khai thác lưu trữ dữ liệu, tiêm phần mềm độc hại, tấn công từ chối dịch vụ và cạn kiệt tài nguyên, và khai thác trực tiếp đến nguồn gốc
7. Mô tả các công cụ tấn công đám mây và cách sử dụng chúng
8. Mô tả các cuộc tấn công vào lưu trữ dữ liệu trên nền tảng đám mây

# Máy chủ tấn công (1 trong 31)

Khai thác không dành riêng cho hệ điều hành

- Một số khai thác hữu ích và độc lập với nền tảng hoặc hệ điều hành
- Ví dụ bao gồm khai thác lỗi cấu hình hoặc quản trị khác  
lỗi

Lỗi cấu hình quyền hệ thống tập tin

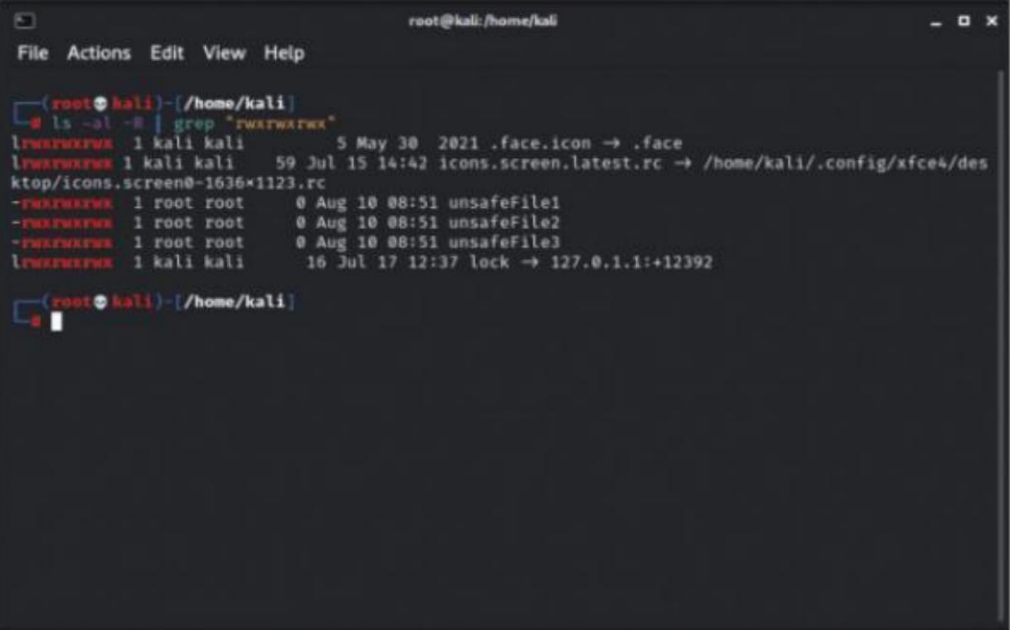
- Hệ thống tập tin của máy chủ được bảo vệ bằng một tập hợp các quyền phức tạp để cung cấp quyền truy cập cho người dùng được ủy quyền và từ chối những người khác

# Chủ nhà tấn công (2 trong số 31)

Khai thác không dành riêng cho hệ điều hành

Lỗi cấu hình quyền hệ thống tập tin

- Lỗi gán quyền có thể từ chối quyền truy cập hợp lệ của người dùng hợp pháp và có thể mở ra cánh cửa cho những kẻ đe dọa và do thám
- Máy chủ Linux có thể sử dụng lệnh `ls` và `grep` công cụ quét toàn bộ hệ thống tập tin để tìm lỗi cấp phép



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)~[/home/kali]
# ls -al -R | grep "rwxrwxrwx"
lrwxrwxrwx 1 kali kali      5 May 30  2021 .face.icon -> .face
lrwxrwxrwx 1 kali kali    59 Jul 15 14:42 icons.screen.latest.rc -> /home/kali/.config/xfce4/desktop/
icons.screen@-1636x1123.rc
-rwxrwxrwx 1 root root      0 Aug 10 08:51 unsafeFile1
-rwxrwxrwx 1 root root      0 Aug 10 08:51 unsafeFile2
-rwxrwxrwx 1 root root      0 Aug 10 08:51 unsafeFile3
lrwxrwxrwx 1 kali kali    16 Jul 17 12:37 lock -> 127.0.1.1:+12392

(root@kali)~[/home/kali]
#
```

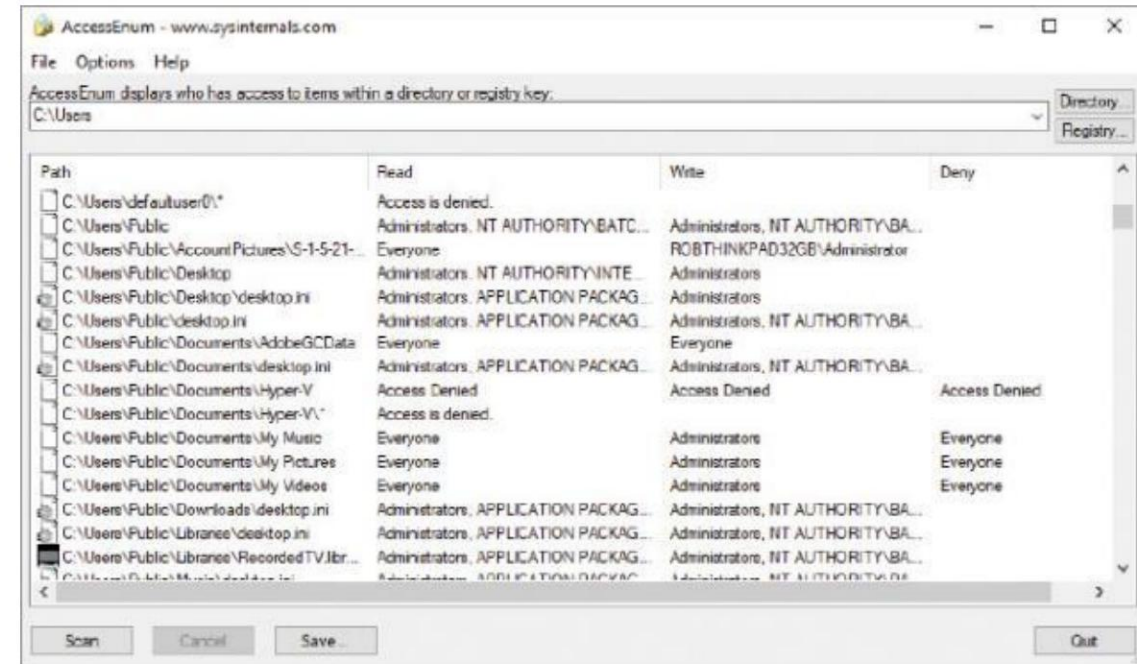
`ls` và `grep` được sử dụng để tìm các tập tin không an toàn

# Chủ nhà tấn công (3 trong số 31)

Khai thác không dành riêng cho hệ điều hành

Lỗi cấu hình quyền hệ thống tập tin

- Các công cụ Windows từ Sysinternals như AccessEnum và Accesschk có thể khám phá quyền hệ thống tập tin lỗi
- Windows PowerShell cũng có các lệnh mạnh mẽ để thực hiện các nhiệm vụ này



Công cụ Sysinternals AccessEnum

# Chủ nhà tấn công (4 trong số 31)

## Khai thác không dành riêng cho hệ điều hành

Thông tin đăng nhập đã lưu trữ

- Các ứng dụng và hệ điều hành có thể lưu trữ thông tin xác thực của người dùng

Thường được thực hiện để thuận tiện trong trình duyệt web và các ứng dụng khác

- Những thông tin xác thực này có thể được lưu trữ trong sổ đăng ký Windows
- Registry là tập hợp các cơ sở dữ liệu về cài đặt cấu hình Windows • Việc truy cập vào máy tính có thể cung

cấp quyền truy cập vào trình quản lý mật khẩu người dùng

công cụ hoặc các vị trí lưu trữ thông tin xác thực khác



# Chủ nhà tấn công (5 trong số 31)

## Khai thác không dành riêng cho hệ điều hành

### Mặc định

- Các thiết lập mặc định không thay đổi là một lỗ hổng bảo mật
- Các biện pháp thực hành tốt nhất chỉ ra việc thay đổi nhiều cài đặt mặc định, đặc biệt là thông tin đăng nhập
- Thông tin xác thực mặc định cho hệ thống và ứng dụng có thể cung cấp quyền truy cập
- Cài đặt cấu hình cũng có thể được để ở mức truy cập cao hơn mức khuyến nghị theo mặc định

# Chủ nhà tấn công (6 trong số 31)

## Khai thác không dành riêng cho hệ điều hành

Tấn công bằng Brute Force để xác thực

- Có nhiều công cụ khác nhau để thực hiện các cuộc tấn công bằng vũ lực

THC-Hydra, Medusa và Patator hỗ trợ nhiều phương pháp khác nhau

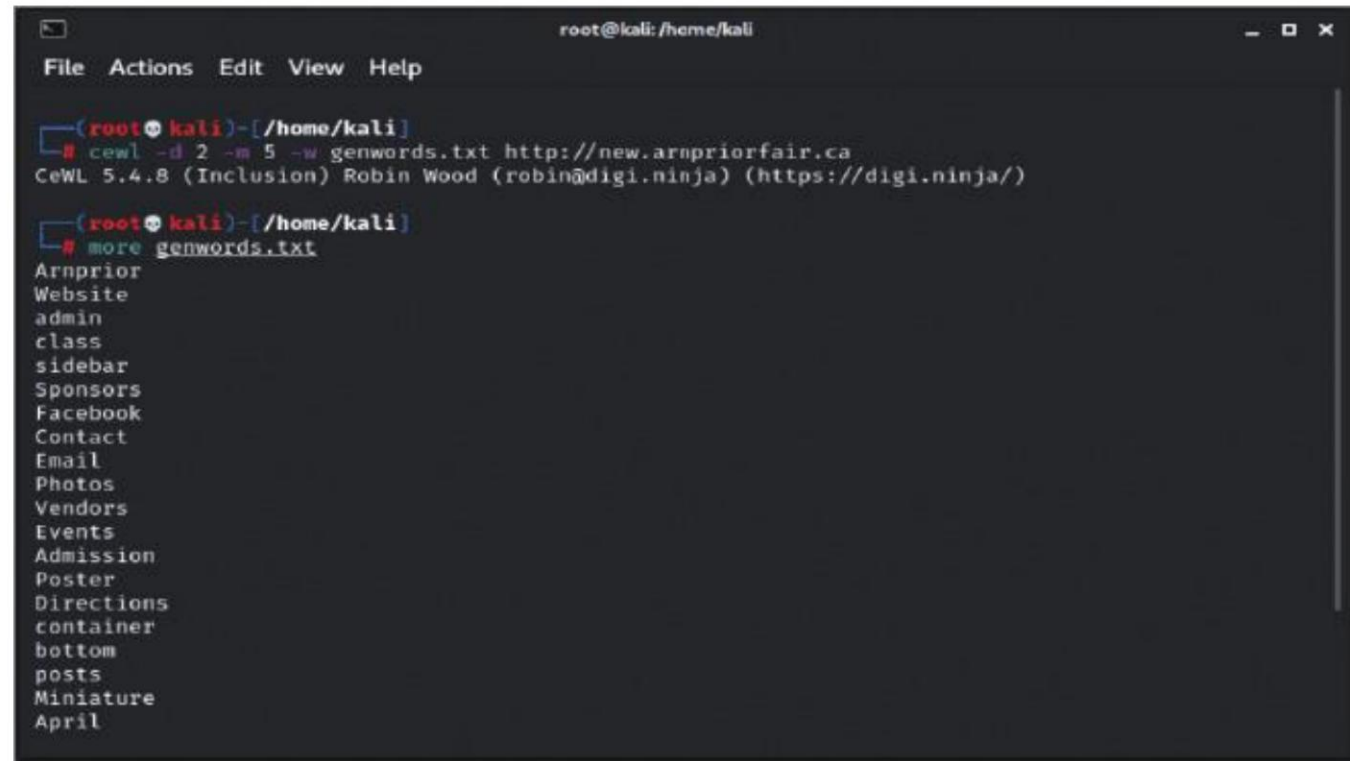
- Các cuộc tấn công có thể nhắm vào hệ điều hành hoặc ứng dụng
- Các thực thể thường bị tấn công bao gồm thông tin đăng nhập hệ điều hành, ứng dụng web, cơ sở dữ liệu
- Các giao thức thường bị tấn công bằng brute force là SSH, SMB, SMB, nhưng nhiều giao thức có thể bị tấn công theo cách này

# Chủ nhà tấn công (7 trong số 31)

## Khai thác không dành riêng cho hệ điều hành

Tấn công bằng Brute Force để xác thực

- Danh sách được tạo ra từ các vi phạm tài khoản có thể được sử dụng trong các cuộc tấn công thông tin xác thực
- Các công cụ như Danh sách từ tùy chỉnh Generator (CeWL) có thể thu thập và phân tích một trang web và tạo danh sách từ và tạo danh sách bằng các phương tiện khác



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# cewl -d 2 -m 5 -w genwords.txt http://new.arnpriorfair.ca
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

(root@kali)-[/home/kali]
# more genwords.txt
Arnprior
Website
admin
class
sidebar
Sponsors
Facebook
Contact
Email
Photos
Vendors
Events
Admission
Poster
Directions
container
bottom
posts
Miniature
April
```

CeWL tạo danh sách từ bằng cách quét một trang web

# Chủ nhà tấn công (8 trong số 31)

## Khai thác không dành riêng cho hệ điều hành

### Vỏ bảo mật (SSH)

- SSH - phương pháp truy cập từ xa phổ biến cho người dùng thông thường, người kiểm tra thâm nhập, quản trị viên hệ thống và tác nhân đe dọa
- Khả năng mã hóa của SSH cho phép những kẻ tấn công ẩn các hành động; cũng có thể được sử dụng để tạo đường hầm cho các giao thức và lưu lượng khác
- Chuyển tiếp cổng SSH có thể chuyển tiếp lưu lượng truy cập giữa các hệ thống một cách bí mật
- Thư mục hệ thống tập tin của người dùng có thể chứa khóa SSH
- SSH thường chạy theo mặc định trên máy chủ Linux

# Chủ nhà tấn công (9 trong số 31)

## Khai thác không dành riêng cho hệ điều hành

### NETCAT và Ncat

- Netcat và Ncat kế nhiệm là các công cụ mạng nhỏ gọn được sử dụng để tạo ra các phiên họp và nhiều ứng dụng hữu ích khác cho người kiểm tra bút
- Công cụ dòng lệnh nc có thể thiết lập shell ngược từ máy chủ
- lệnh nc cho Linux và Windows tương tự nhau
- Ncat có thể được sử dụng như một trình nghe từ xa hoặc cửa sau
- Một số công cụ chống phần mềm độc hại phát hiện nc là ứng dụng có khả năng không mong muốn

# Chủ nhà tấn công (10 trong số 31)

Khai thác không dành riêng cho hệ điều hành

Khai thác truy cập từ xa của Metasploit Framework

- Metasploit và Meterpreter nổi tiếng của nó hỗ trợ nhiều shell đảo ngược và liên kết trên các mục tiêu
- Reverse shell khởi tạo từ máy chủ bị xâm nhập đến hệ thống của kẻ tấn công

Proxy

- Máy chủ proxy hoạt động như một trung gian giữa người dùng và các máy chủ khác
- Giao tiếp thông qua nhiều proxy được gọi là chuỗi proxy và là một phương pháp khác để ẩn lưu lượng truy cập

# Chủ nhà tấn công (11 trong số 31)

## Máy chủ Linux/Unix

- Linux và Unix có nhiều phiên bản hoặc bản phân phối khác nhau (distro)
- Mỗi hệ điều hành hoặc nhân cơ bản tương tự nhau, nhưng có nhiều ứng dụng, giao diện, cấu hình và mục đích

Red Hat là một bản phân phối cấp doanh nghiệp

Ubuntu tập trung vào người dùng gia đình nhưng đã phát triển các dịch vụ của mình

Nhiều phiên bản Unix thương mại và miễn phí cũng tồn tại

- Tính linh hoạt và cấp phép mở của Linux làm cho nó trở nên phổ biến trên các hệ thống nhúng, thiết bị mạng, IoT và các hệ thống khác

# Chủ nhà tấn công (12 trong số 31)

Máy chủ Linux/Unix

## Khai thác SUID/GUID

- Đặt ID người dùng (SUID hoặc SETUID) và đặt ID nhóm (GUID) là các bit quyền được đặt đến 1 hoặc 0 để chỉ ra quyền chạy tệp thực thi
- Nếu người dùng root tạo tệp thực thi và đặt bit SUID thành bật hoặc 1, tệp này sẽ luôn thực thi với quyền cấp root ngay cả khi chương trình được chạy bởi người dùng chuẩn
- Bit quyền GUID có thể được thiết lập để chạy với quyền của chủ sở hữu nhóm



# Chủ nhà tấn công (13 trong số 31)

## Máy chủ Linux/Unix

## Khai thác SUID/GUID

- **Lệnh Linux như cp**  
và tìm sẽ được thiết lập để cho phép các lệnh này thực hiện các hành động mà thông thường nằm ngoài quyền thực thi của người dùng
- **Xác định SUID và GUID trên**  
các tệp thực thi có thể giúp các hoạt động kiểm tra thâm nhập sâu hơn vào mục tiêu Linux

```
(root@kali)~# find / -perm -u+s -type f 2>/dev/null
/usr/sbin/mount.nfs
/usr/sbin/mount.cifs
/usr/sbin/pppd
/usr/sbin/exim4
/usr/bin/newgrp
/usr/bin/kismet_cap_rz_killerbee
/usr/bin/kismet_cap_linux_bluetooth
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/fusermount3
/usr/bin/chfn
/usr/bin/kismet_cap_nrf_mousejack
/usr/bin/su
/usr/bin/kismet_cap_ti_cc_2540
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/ntfs-3g
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/kismet_cap_nrf_52840
/usr/bin/kismet_cap_linux_wifi
/usr/bin/pkexec
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/kismet_cap_nrf_51822
/usr/bin/mount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool
/usr/lib/xorg/Xorg.wrap
/usr/lib/virtualbox/VBoxSDL
/usr/lib/virtualbox/VBoxNetNAT
/usr/lib/virtualbox/VBoxNetAdpCtl
/usr/lib/virtualbox/VirtualBoxVM
/usr/lib/virtualbox/VBoxNetDHCP
/usr/lib/virtualbox/VBoxHeadless
/usr/libexec/polkit-agent-helper-1
/usr/libexec/spice-client-glib-usb-acl-helper
```

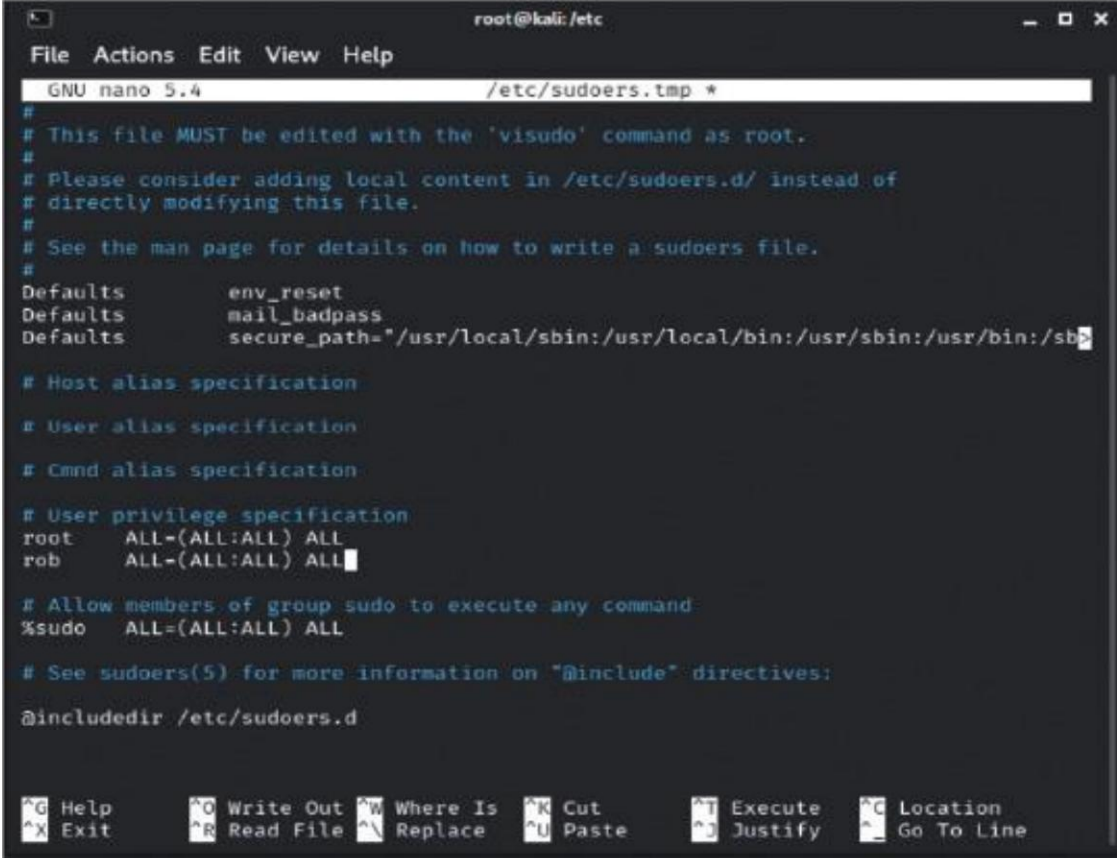
Tìm kiếm các tệp tin có SUID được thiết lập

# Chủ nhà tấn công (14 trong số 31)

## Máy chủ Linux/Unix

### Khai thác SUDO

- Super User Do (SUDO) cho phép người dùng nâng cao đặc quyền cho Siêu người dùng hoặc root để thực hiện một lệnh cụ thể
- Tập Linux /etc/sudoers liệt kê những người dùng được phép sử dụng sudo
  - Kẻ tấn công có thể sửa đổi tập này
- Tập Sudoers có thể chỉ định lệnh nào mà người dùng có thể chạy với tư cách là root hoặc cho phép tất cả



```

root@kali: /etc
File Actions Edit View Help
GNU nano 5.4 /etc/sudoers.tmp *
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
rob     ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@include::/etc/sudoers.d

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
  
```

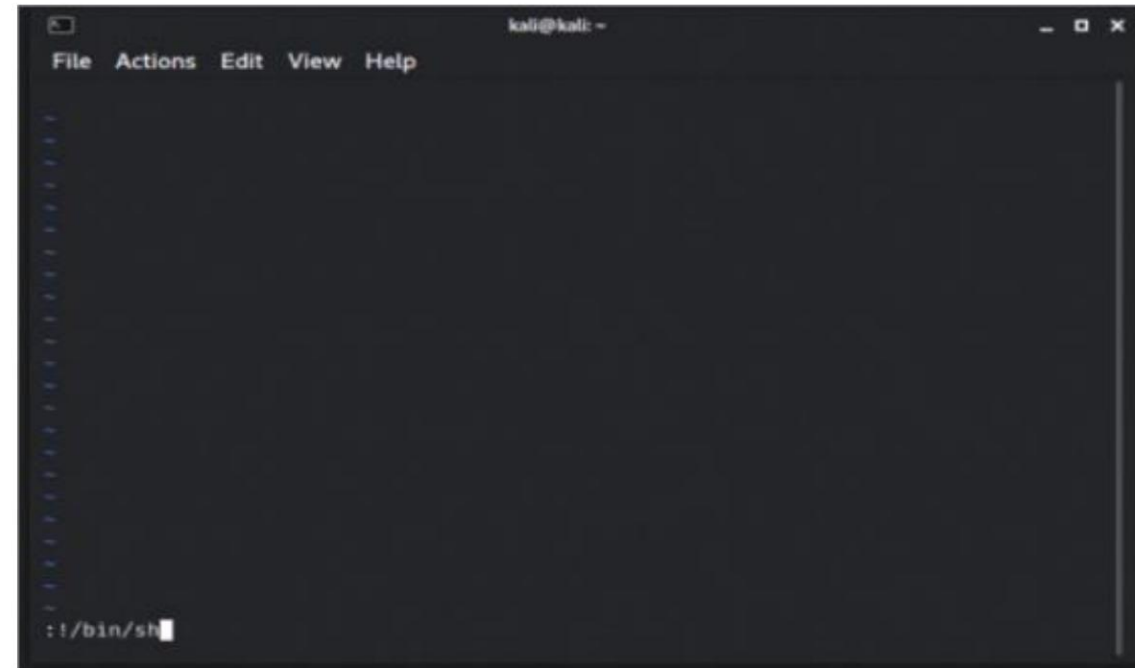
Tập sudoers của Linux

# Chủ nhà tấn công (15 trong số 31)

## Máy chủ Linux/Unix

### Khai thác nâng cấp Shell

- Khai thác nâng cấp Shell liên quan đến việc tìm cách thoát khỏi các hạn chế của Shell
- Các hạn chế của Shell đối với người dùng hạn chế khả năng thực hiện các nhiệm vụ nâng cao
- Trình soạn thảo vi và các công cụ khác có thể cho phép người dùng thực hiện các lệnh trong
  - Có thể khai thác để nâng cấp lên root shell bằng cách khởi chạy trong trình soạn thảo vi chạy với SUID cho root



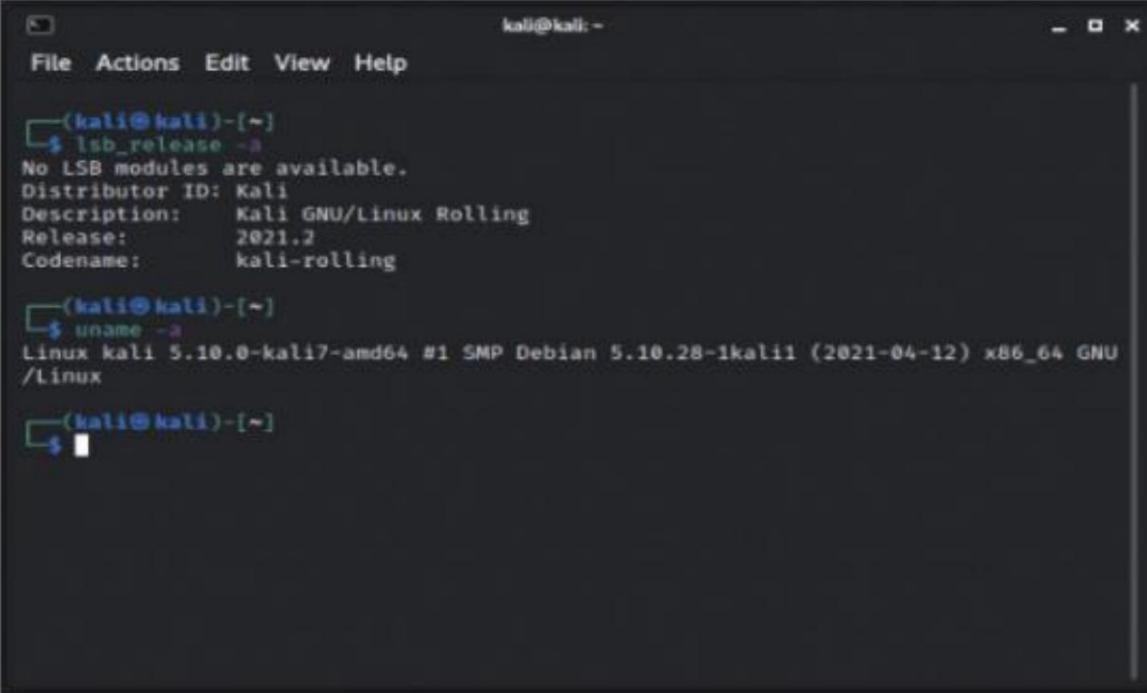
Sử dụng trình soạn thảo vi để thử khởi động một shell đầu cuối

# Chủ nhà tấn công (16 trong số 31)

## Máy chủ Linux/Unix

### Khai thác hạt nhân

- Kernel là lõi của hệ điều hành xử lý I/O, truy cập CPU và quản lý bộ nhớ
- Có nhiều phiên bản hạt nhân Linux, một số có lỗ hổng rất nghiêm trọng
- Xác định hạt nhân cụ thể của mục tiêu  
Hệ thống Linux có thể xác định các lỗ hổng tiềm ẩn
- Các lỗ hổng bảo mật của kernel rất mạnh nhưng khó sử dụng



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ lsb_release -a  
No LSB modules are available.  
Distributor ID: Kali  
Description:   Kali GNU/Linux Rolling  
Release:       2021.2  
Codename:      kali-rolling  
  
(kali@kali)-[~]  
$ uname -a  
Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux  
  
(kali@kali)-[~]  
$
```

Sử dụng `lsb_release` và `uname` để xác định bản phân phối và phiên bản của hệ điều hành Linux

# Chủ nhà tấn công (17 trong số 31)

## Máy chủ Linux/Unix

### Thu thập thông tin xác thực

- Khi hệ thống đã bị xâm phạm, việc lấy được kho thông tin xác thực cục bộ cho tên người dùng và mật khẩu hệ thống là chiến thuật phổ biến của kẻ tấn công
- Hệ thống Linux lưu trữ thông tin xác thực ở hai vị trí:

`/etc/passwd` - chứa các tài khoản người dùng dạng văn bản rõ, thường có thể đọc được bởi tất cả mọi người

`/etc/shadow` - vị trí của mật khẩu đã băm của người dùng Linux

Mật khẩu băm bị đánh cắp sau khi hệ thống bị xâm phạm

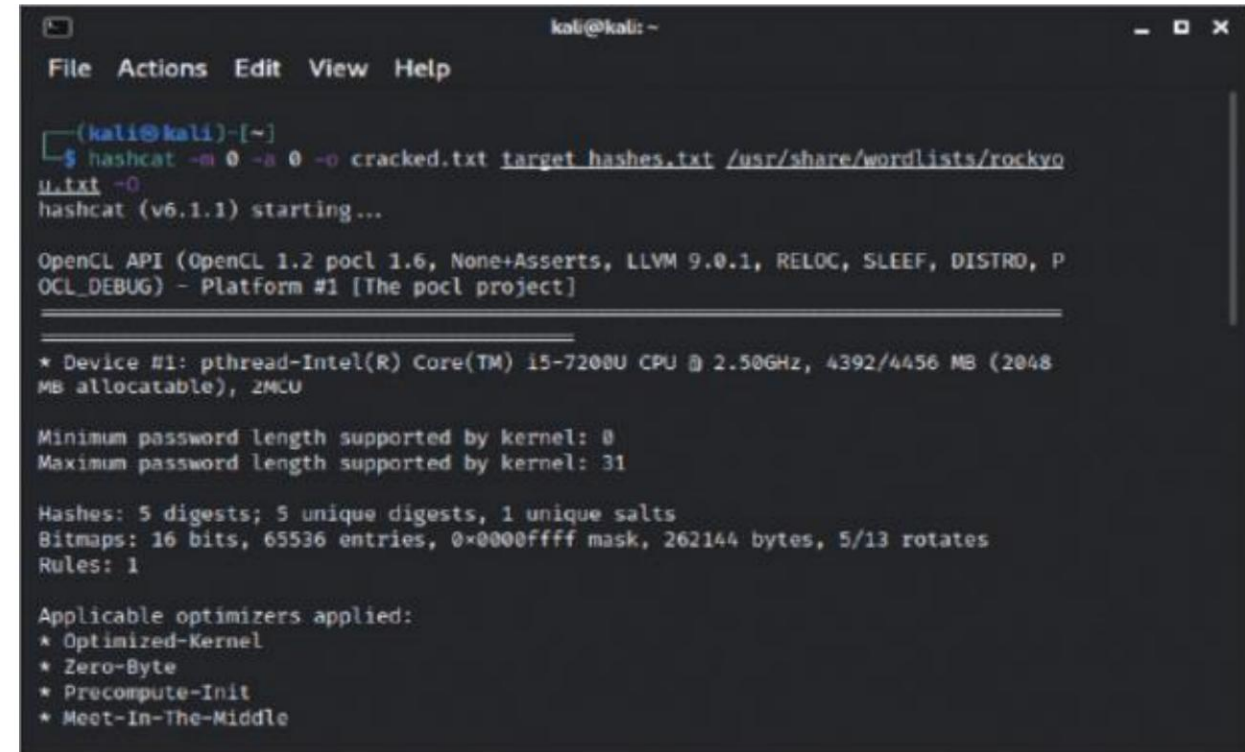
Bẻ khóa mật khẩu - thủ tục tiếp theo thường được thực hiện

# Chủ nhà tấn công (18 trong số 31)

## Máy chủ Linux/Unix

### Bẻ khóa mật khẩu

- Mật khẩu băm được lưu trữ trong dạng mật mã không thể đảo ngược
- Có một số công cụ để tấn công các hàm băm này, khám phá mật khẩu
- Mức độ khó phụ thuộc vào loại băm và quy trình băm



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ hashcat -m 0 -a 0 -o cracked.txt target hashes.txt /usr/share/wordlists/rockyou  
u.txt -O  
hashcat (v6.1.1) starting...  
  
OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, P  
OCL_DEBUG) - Platform #1 [The pocl project]  
  
-----  
* Device #1: pthread-Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 4392/4456 MB (2048  
MB allocatable), 2MCU  
  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 31  
  
Hashes: 5 digests; 5 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates  
Rules: 1  
  
Applicable optimizers applied:  
* Optimized-Kernel  
* Zero-Byte  
* Precompute-Init  
* Meet-In-The-Middle
```

Sử dụng Hashcat để bẻ khóa mật khẩu băm

# Hoạt động thảo luận 10-1

Trong mô-đun này, bảo mật của hệ điều hành máy chủ Windows và Linux được trình bày. Một số cuộc tấn công là phổ biến đối với cả hai hệ điều hành. Cả Windows và Linux cũng có các cuộc tấn công và lỗ hổng cụ thể cho từng hệ điều hành.

Thảo luận về nhiều cuộc tấn công hệ điều hành khác nhau chỉ xảy ra với một hệ điều hành. Mô hình cấp phép nguồn mở mà hầu hết các phiên bản Linux được phát hành có thúc đẩy hay cản trở tính bảo mật cho hệ điều hành này không? Tại sao và tại sao không?

# Chủ nhà tấn công (19 trong số 31)

## Máy chủ Windows

- Microsoft Windows chiếm 75% thị phần máy tính xách tay và máy tính để bàn\*
- Hệ điều hành Windows Server chiếm 73% các triển khai hệ thống máy chủ\*

## Khai thác băm thông tin xác thực

- NT LAN Manager (NTLM) - Cơ chế xác thực Windows sử dụng hàm băm mật khẩu
- NTLM là công cụ xác thực mặc định cho các hệ thống Windows cũ từ Windows 2000 trở về trước
- Có thể vẫn được sử dụng để tương thích ngược

\*Tính đến thời điểm viết sách



# Chủ nhà tấn công (20 trong số 31)

## Máy chủ Windows

### Khai thác bẫy thông tin xác thực

- Có thể thực hiện việc đổ mã bẫy NTLM bằng cách sử dụng Mimikatz và các công cụ khác
- Bẫy NTLM không được thêm muối và yếu; dễ bẻ khóa

Bẫy muối thêm giá trị vào mật khẩu trước khi bẫy

Mật khẩu được mã hóa khó bị bẻ khóa hơn

- Một số bẫy mật khẩu phát lại các bẫy đã chụp để tránh xác thực cơ chế

# Chủ nhà tấn công (21 trong số 31)

## Máy chủ Windows

### Khai thác bí mật LSA

- Bí mật LSA – Vị trí sổ đăng ký Windows lưu trữ người dùng hiện đang đăng nhập mật khẩu ở dạng được mã hóa
- Quyền truy cập quản trị vào máy chủ Windows có thể cho phép lấy được những mật khẩu này băm và các khóa liên quan
- Sau đó có thể giải mã mật khẩu người dùng hiện tại

# Chủ nhà tấn công (22 trong số 31)

## Máy chủ Windows

### Khai thác cơ sở dữ liệu SAM

- Quản lý tài khoản bảo mật (SAM)  
cơ sở dữ liệu chứa các băm mật khẩu
- Thường là mục đầu tiên bị các nhà kiểm tra và tác nhân đe dọa nhắm tới
- Việc xóa cơ sở dữ liệu SAM yêu cầu thông tin xác thực hệ thống được nâng cao

```

mimikatz 2.2.0 (x64) #19041 Aug 20 2021 17:19:53
.###. mimikatz 2.2.0 (x64) #19041 Aug 20 2021 17:19:53
..#.#. "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::sam
Domain : DESKTOP-FPWB5H8
SysKey : 97af2931edef1132c178768803670829
ERROR kuhl_m_registry_OpenAndQueryWithAlias : kuhl_m_registry_RegOpenKeyEx KO
ERROR kuhl_m_lsadump_getUsersAndSamKey : kuhl_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

564 (0;000000e7) 1 D 19072 NT AUTHORITY\SYSTEM 5-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : (0;00076920) 1 F 4606421 DESKTOP-FPWB5H8\rob 5-1-5-21-3156019167-3713297788-247219011-1001 (14g,
24p) Primary
* Thread Token : (0;000000e7) 1 D 4666312 NT AUTHORITY\SYSTEM 5-1-5-18 (04g,21p) Impersonation (Delega
tion)

mimikatz # lsadump::sam
Domain : DESKTOP-FPWB5H8
SysKey : 97af2931edef1132c178768803670829
Local SID : 5-1-5-21-3156019167-3713297788-247219911
SAMKey : 15021248b0fad5695adba97138c900d

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount
  
```

Sử dụng Mimikatz để dump cơ sở dữ liệu SAM

# Chủ nhà tấn công (23 trong số 31)

## Máy chủ Windows

### Khai thác hạt nhân

- Khai thác hạt nhân Windows yêu cầu quyền truy cập cục bộ; thành công nhất sau khi đã đạt được quyền truy cập vào mục tiêu
- Microsoft vá các lỗ hổng của hạt nhân sớm nhất có thể
- Việc thiếu các bản vá cho lỗ hổng của hạt nhân là một nhiệm vụ quản trị quan trọng

# Tấn công ảo hóa (1 trong 2)

- Ảo hóa đã thay đổi mô hình điện toán
- Các ứng dụng và hệ điều hành có thể dễ dàng di chuyển từ máy tính này sang máy tính khác nền tảng này sang nền tảng khác
- Ảo hóa Hypervisor sử dụng khái niệm máy ảo (VM) với hệ điều hành và ứng dụng được tích hợp đầy đủ
- Hypervisor hoạt động như một lớp giữa VM và hệ điều hành máy chủ
  - Điều phối quyền truy cập vào phần cứng vật lý của máy chủ thông qua phần cứng ảo hóa được mô phỏng
- Ảo hóa container chạy các ứng dụng trực tiếp trên hệ điều hành máy chủ nhưng bị cô lập và trong container ảo hóa

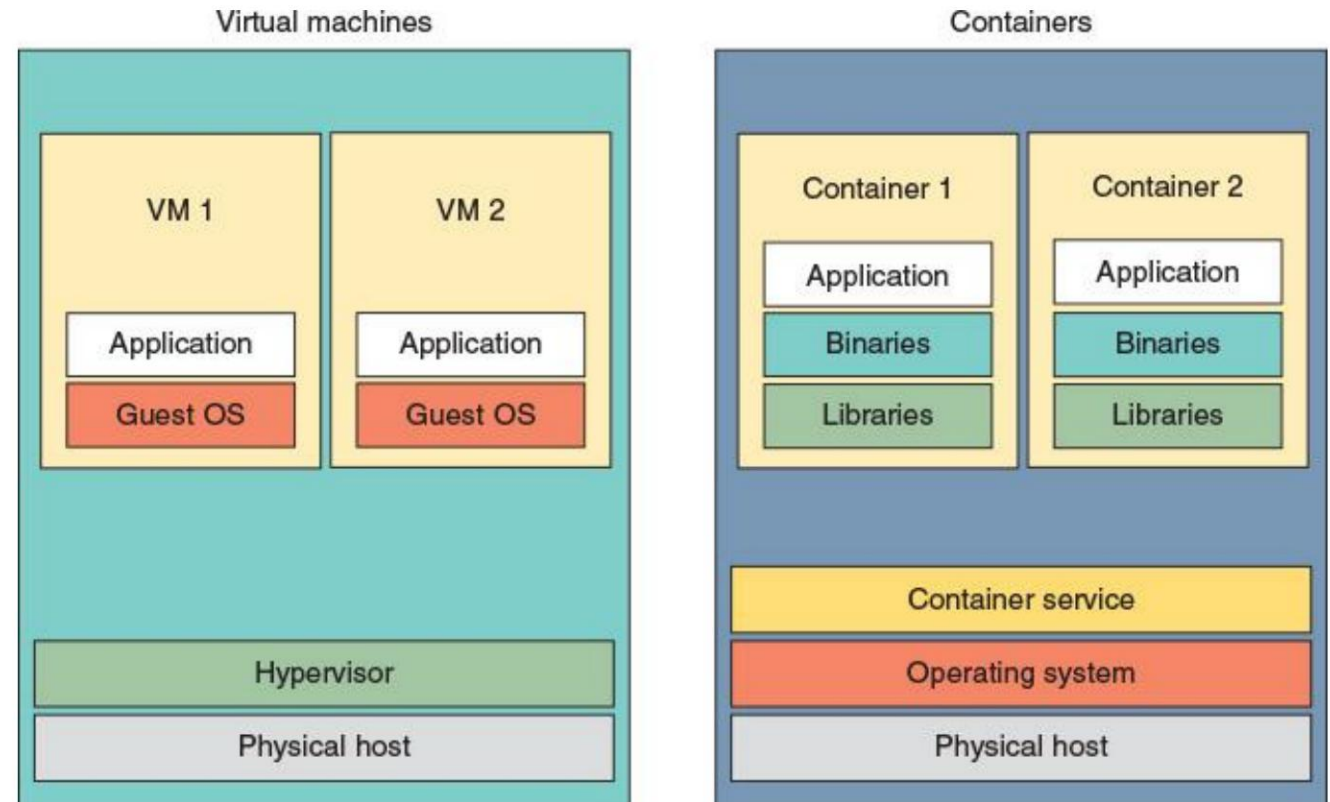
# Tấn công ảo hóa (2 trong 2)

- Có nhiều nền tảng tồn tại cho ảo hóa
- Mỗi người đều có sự khác biệt trong cách tiếp cận với ảo hóa và khả năng

Oracle VirtualBox

Microsoft Hyper-V

Máy ảo VMware



Ảo hóa máy ảo và container

# Chủ nhà tấn công (24 trong số 31)

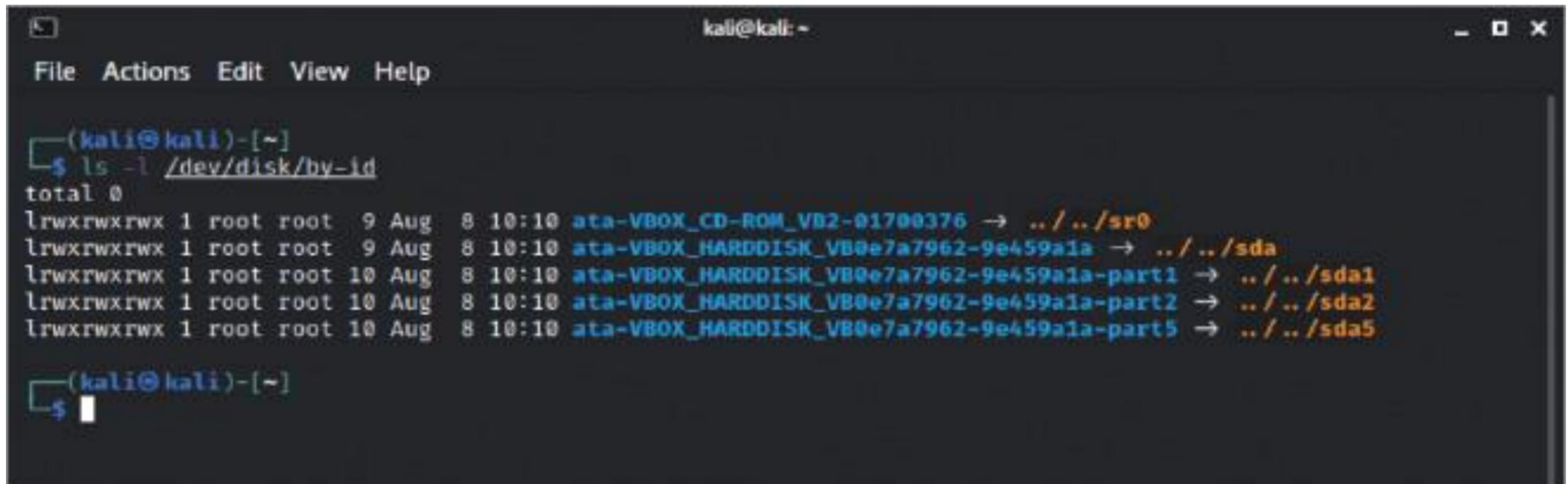
## Khai thác máy ảo

- VM hoạt động giống như máy tính vật lý; có thể không rõ ràng nếu mục tiêu là máy tính vật lý máy hoặc máy chủ ảo hóa
- Phương pháp tấn công cho VM giống như máy chủ vật lý
- Việc xâm phạm VM có thể là cách duy nhất để biết mục tiêu được ảo hóa
- Tìm kiếm phần cứng ảo hóa trên mục tiêu có thể chỉ ra đó là VM
- Các phương pháp khác để xác định xem mục tiêu có được ảo hóa hay không tồn tại và thay đổi tùy theo hệ điều hành khách và trình quản lý ảo hoặc hệ điều hành máy chủ đang sử dụng

# Chủ nhà tấn công (25 trong số 31)

## Khai thác máy ảo

- Kiểm tra chi tiết phần cứng đĩa có thể xác định xem máy chủ có phải là VM hay không



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ls -l /dev/disk/by-id  
total 0  
lrwxrwxrwx 1 root root 9 Aug 8 10:10 ata-VBOX_CD-ROM_VB2-01700376 -> ../.. /sr0  
lrwxrwxrwx 1 root root 9 Aug 8 10:10 ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a -> ../.. /sda  
lrwxrwxrwx 1 root root 10 Aug 8 10:10 ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part1 -> ../.. /sda1  
lrwxrwxrwx 1 root root 10 Aug 8 10:10 ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part2 -> ../.. /sda2  
lrwxrwxrwx 1 root root 10 Aug 8 10:10 ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part5 -> ../.. /sda5  
  
(kali@kali)-[~]  
$
```

Sử dụng ID đĩa để xác định xem mục tiêu Linux có phải là VM không



# Chủ nhà tấn công (26 trong số 31)

## Khai thác máy ảo

### Khai thác Hypervisor và VM Repository

- Nền tảng ảo hóa và trình quản lý siêu phức tạp và phụ thuộc vào phần mềm khuyết điểm và điểm yếu và các vấn đề khác
- Các nền tảng lưu trữ đám mây VM như Amazon Web Services và Microsoft Azure cung cấp các VM được cấu hình sẵn để khách hàng dễ dàng sử dụng các triển khai của họ
- Nếu một trong những VM này bị xâm phạm hoặc chứa cửa hậu, tất cả các hệ thống được xây dựng từ mẫu đó đều có thể bị khai thác
- Các nền tảng lưu trữ VM đám mây có các quy tắc kiểm tra thâm nhập riêng

# Chủ nhà tấn công (27 trong số 31)

Khai thác máy ảo

Thoát khỏi VM

- Tấn công máy chủ từ bên trong VM là “thoát” VM
- Các lỗ hổng thoát VM được vá rất nhanh, thu hẹp cửa sổ khai thác

# Chủ nhà tấn công (28 trong số 31)

## Khai thác máy ảo

### Thoát khỏi VM

- Tấn công máy chủ từ bên trong VM là “thoát” VM
- Các lỗ hổng thoát VM được vá rất nhanh, thu hẹp cửa sổ khai thác

### Khai thác container

- Khai thác container bắt đầu bằng cách nhắm mục tiêu vào ứng dụng đang chạy bên trong container và có thể sử dụng khai thác tiêu chuẩn cho ứng dụng đó
- Việc xâm phạm vùng chứa có thể dẫn đến việc khai thác máy chủ mà nền tảng container hóa chạy

# Chủ nhà tấn công (29 trong số 31)

## Khai thác máy ảo

### Khai thác container

- Docker và Kubernetes là các nền tảng container hóa phổ biến
- Docker là bộ công cụ phát triển để tạo, chia sẻ và triển khai thùng chứa
- Kubernetes là một hệ thống được sử dụng để triển khai và vận hành các container trên cụm máy chủ lưu trữ

# Chủ nhà tấn công (30 trong số 31)

## Khai thác máy ảo

## Khai thác container

- Docker và Kubernetes thường được triển khai dưới dạng dịch vụ đám mây
- Amazon Elastic Container Service (ECS) là dịch vụ lưu trữ container đám mây
- Tấn công các container dựa trên đám mây đòi hỏi phải có kiến thức về các dịch vụ đám mây và cơ bản cơ sở hạ tầng
- Các cuộc tấn công khối lượng công việc container khai thác các ứng dụng container dễ bị tấn công
- Các cuộc tấn công cấu hình sai container bao gồm các lỗ hổng ở nhiều loại khác nhau, bao gồm lỗi quyền và API bị lộ không an toàn

# Tấn công các mục tiêu dựa trên đám mây (1 trong 7)

## Khai thác tài khoản

- Các nền tảng lưu trữ đám mây như AWS, Google Cloud Platform (GCP) và Microsoft Azure rất phổ biến vì nhiều lý do hấp dẫn
- Các tổ chức đã chuyển từ việc triển khai phần cứng trong phòng máy chủ của họ sang triển khai VM trên các dịch vụ
- Môi trường dịch vụ đám mây bao gồm tài khoản và thông tin xác thực
- Các loại tài khoản đám mây khác nhau với các mức độ cấp phép và quyền truy cập khác nhau để quản lý dịch vụ các công cụ có thể là đáng sợ
- Nền tảng đám mây có thể truy cập qua internet theo bản chất của chúng, khiến chúng dễ bị tấn công hơn so với các hệ thống mục tiêu cục bộ hoặc tại chỗ

# Tấn công các mục tiêu dựa trên đám mây (2 trong số 7)

## Khai thác tài khoản

- Thông tin xác thực đám mây có thể được lấy thông qua các phương tiện tương tự như thông thường

Tấn công bằng vũ lực, quét thư mục và dump vi phạm trực tuyến là những nguồn

- Xác thực đa yếu tố (MFA) được triển khai rộng rãi

Có thể xảy ra lỗi cấu hình MFA

Các cuộc tấn công MFA có thể gửi thông báo đến chủ sở hữu tài khoản mục tiêu

- Việc chiếm đoạt tài khoản bị xâm phạm có thể cho phép tấn công dịch vụ siêu dữ liệu

Nhắm mục tiêu thông tin xác thực tạm thời của máy chủ đám mây cho nhu cầu tài nguyên đám mây

Thông tin tình báo có thể hành động đáng kể có khả năng tiếp cận được

# Chủ nhà tấn công (31 trong 31)

## Máy chủ Windows

### Thu thập thông tin xác thực

- Sau khi xâm phạm mục tiêu thu thập thông tin xác thực hệ thống Windows bằng cách sử dụng trước đó phương pháp hoặc một trong số nhiều công cụ khác để thực hiện điều đó
- Mimikatz - lựa chọn thường xuyên và được sử dụng sau khi khai thác, sau khi thỏa hiệp

### Bẻ khóa mật khẩu

- Mật khẩu Windows được băm hoặc mã hóa phải được bẻ khóa hoặc đảo ngược
- Các công cụ thường được sử dụng bao gồm Hashcat, John the Ripper và RainbowCrack



# Tấn công các mục tiêu dựa trên đám mây (3 trong số 7)

## Khai thác cấu hình sai

- Quản lý danh tính và quyền truy cập (IAM) đề cập đến các quy trình, thủ tục và phương pháp để làm cho việc xác thực và ủy quyền an toàn hơn
- IAM có thể bị cấu hình sai hoặc để lại các thiết lập mặc định yếu
- Các biện pháp thực hành tốt nhất cho cấu hình IAM có thể bị bỏ qua hoặc bỏ qua
- Các vị trí lưu trữ dữ liệu, chẳng hạn như thùng Amazon S3 là mục tiêu đám mây

Lưu trữ có thể được truy cập công khai; vô tình mở cho các hành động lưu trữ

- Cấu hình sai liên kết liên quan đến các lỗi trong mối quan hệ tin cậy như thế này giữa Active Directory truyền thống và Azure AD

# Tấn công các mục tiêu dựa trên đám mây (4 trong số 7)

## Tiêm phần mềm độc hại

- Các cuộc tấn công tiêm phần mềm độc hại vào đám mây là cuộc tấn công MITM chuyển hướng nạn nhân đến mối đe dọa máy ảo đám mây và dịch vụ của diễn viên

Có thể sử dụng cross-site scripting để thực hiện việc này

## Từ chối dịch vụ và cạn kiệt tài nguyên

- Mô hình định giá dịch vụ đám mây có thể thay đổi rất nhiều

Trả tiền theo lượng tài nguyên sử dụng là mô hình phổ biến

Quá tải dịch vụ đám mây đến mức cạn kiệt tài nguyên gây ra tình huống DoS

Loại tấn công DoS này có thể tốn kém để nhắm mục tiêu

# Tấn công các mục tiêu dựa trên đám mây (5 trong số 7)

## Khai thác kênh phụ

- Nhiều máy ảo chạy song song trên một máy chủ ảo hóa

Tấn công kênh phụ tìm cách sử dụng một VM để truy cập VM khác hoặc đạt được mục tiêu có thể thực hiện được trí thông minh

## Khai thác trực tiếp đến nguồn gốc (D2O)

- D2O là DDoS nhắm vào cơ sở hạ tầng của mạng phân phối nội dung (CDN)
- Bằng cách lấy được địa chỉ IP thực của máy chủ mục tiêu, bảo mật đám mây đã bị bỏ qua

Bỏ qua bộ cân bằng tải, dịch vụ giảm thiểu DoS và proxy

# Tấn công các mục tiêu dựa trên đám mây (6 trong số 7)

## Công cụ tấn công đám mây

Có một số công cụ cho các cuộc tấn công đám mây khác nhau:

- Cloud Custodian – Tạo báo cáo về điểm yếu của môi trường đám mây
- CloudBrute – liệt kê các tài nguyên ứng dụng và lưu trữ
- Pacu – Khung khai thác AWS với nhiều khai thác
- ScoutSuite – công cụ kiểm toán nguồn mở cho nhiều nhà cung cấp đám mây
- Bộ công cụ phát triển phần mềm (SDK) – do các nhà cung cấp đám mây cung cấp để hỗ trợ các nhà phát triển phần mềm xây dựng các tính năng đám mây vào ứng dụng của họ

Được sử dụng để liệt kê tài nguyên, tạo tập lệnh thử nghiệm, v.v.

# Tấn công các mục tiêu dựa trên đám mây (7 trong số 7)

## Khai thác lưu trữ dữ liệu

- Khai thác lưu trữ dữ liệu nhằm mục tiêu vào các đối tượng lưu trữ đám mây
- Việc liệt kê lưu trữ đám mây có thể được sử dụng cho các khai thác tiếp theo
- Có thể sử dụng thông tin xác thực mặc định và quyền hạn yếu

# Hoạt động thảo luận 10-2

Công nghệ đám mây và ảo hóa đã cách mạng hóa bối cảnh điện toán hiện đại. Những thách thức nào có thể tồn tại khi thử nghiệm bút trên môi trường đám mây? Có những cuộc tấn công hoặc phương pháp nào để thử nghiệm bút trên đám mây có thể dễ hơn so với môi trường điện toán truyền thống không?

# Tóm tắt (1 trong 3)

Đến cuối mô-đun này, bạn sẽ có thể:

1. Mô tả các cuộc tấn công vào máy chủ cụ thể không phải là hoạt động như lợi dụng lỗi cấu hình quyền, truy cập thông tin xác thực đã lưu trữ, khai thác thông tin xác thực mặc định và tấn công bằng cách dùng vũ lực
2. Mô tả các phương pháp tấn công truy cập từ xa khác nhau như ẩn các cuộc tấn công bằng SSH, NETCAT/Ncat, truy cập từ xa của khung Metasploit và proxy
3. Mô tả các cuộc tấn công máy chủ Linux/Unix như SUID/GUID SUDO, nâng cấp shell và khai thác kernel, thu thập thông tin xác thực và bẻ khóa mật khẩu

# Tóm tắt (2 trong 3)

Đến cuối mô-đun này, bạn sẽ có thể:

4. Mô tả các cuộc tấn công vào máy chủ Windows như băm thông tin xác thực, bí mật LSA, cơ sở dữ liệu SAM và khai thác hạt nhân, thu thập thông tin xác thực và bẻ khóa mật khẩu
5. Mô tả các cuộc tấn công vào ảo hóa như máy ảo (VM), hypervisor và khai thác kho lưu trữ VM, thoát VM và khai thác container



# Tóm tắt (3 trong 3)

Đến cuối mô-đun này, bạn sẽ có thể:

6. Mô tả các cuộc tấn công vào các mục tiêu dựa trên đám mây như tài khoản, cấu hình sai, khai thác lưu trữ dữ liệu, tiêm phần mềm độc hại, tấn công từ chối dịch vụ và cạn kiệt tài nguyên, và khai thác trực tiếp đến nguồn gốc
7. Mô tả các công cụ tấn công đám mây và cách sử dụng chúng
8. Mô tả các cuộc tấn công vào lưu trữ dữ liệu trên nền tảng đám mây