

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ



**BÁO CÁO TỔNG KẾT
ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN**

**XÂY DỰNG MÔI TRƯỜNG THỰC TẬP
KIỂM THỦ BẢO MẬT TRÊN NỀN TẢNG ĐÁM MÂY**
Mã số đề tài: THS2024-77

Chủ nhiệm đề tài: Trương Đặng Trúc Lâm

Cần Thơ, 9/2024

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ



**BÁO CÁO TỔNG KẾT
ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN**

**XÂY DỰNG MÔI TRƯỜNG THỰC TẬP
KIỂM THỬ BẢO MẬT TRÊN NỀN TẢNG ĐÁM MÂY**
Mã số đề tài: THS2024-77

Sinh viên chủ nhiệm đề tài: Trương Đặng Trúc Lâm

Giới tính: Nam

Dân tộc: Kinh

Lớp: Công nghệ Thông tin CLC 03

Trường: CNTT-TT

Năm thứ: 4

Số năm đào tạo: 4.5

Ngành học: Công nghệ Thông tin CLC

Người hướng dẫn: TS. Thái Minh Tuấn

Cần Thơ, 9/2024

CHỦ NHIỆM VÀ CÁC THÀNH VIÊN THAM GIA ĐỀ TÀI

NHỮNG THÀNH VIÊN THAM GIA NGHIÊN CỨU ĐỀ TÀI			
STT	Họ và Tên	Vai trò	MSSV, Lớp, Khoa
1	Trương Đặng Trúc Lâm	Chủ nhiệm đề tài	B2111933, lớp Công nghệ Thông tin CLC 03 khoá 47
2	Đặng Hoàng Hưng	Thành viên chính	B2111984, lớp Công nghệ Thông tin CLC 03 khoá 47
3	Lê Xuân Thành	Thành viên chính	B2111952, lớp Công nghệ Thông tin CLC 01 khoá 47
4	Nguyễn Duy Bằng	Thành viên chính	B2111971, lớp Công nghệ Thông tin CLC 03 khoá 47

CÁN BỘ HƯỚNG DẪN SINH VIÊN THỰC HIỆN ĐỀ TÀI

Họ và tên	Đơn vị công tác và lĩnh vực chuyên môn	Nhiệm vụ
Thái Minh Tuấn	Khoa Công nghệ Thông tin, Trường CNTT-TT	Hướng dẫn nội dung khoa học và hướng dẫn lập dự toán kinh phí đề tài

MỤC LỤC

DANH MỤC HÌNH ẢNH.....	iv
LỜI CẢM ƠN	vii
THÔNG TIN KẾT QUẢ NGHIÊN CỨU CỦA ĐỀ TÀI	viii
INFORMATION ON RESEARCH RESULTS	xii
THÔNG TIN VỀ SINH VIÊN CHỊU TRÁCH NHIỆM CHÍNH THỰC HIỆN ĐỀ TÀI.....	xiii
I. SƠ LUẬC VỀ SINH VIÊN	xiii
II. QUÁ TRÌNH HỌC TẬP	xiii
CHƯƠNG 1: TỔNG QUAN.....	1
1. ĐẶT VÂN ĐỀ.....	1
2. TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU	2
2.1. Trong nước	2
2.2. Ngoài nước	3
3. TÍNH CẤP THIẾT CỦA ĐỀ TÀI.....	5
4. MỤC TIÊU ĐỀ TÀI.....	5
5. CÁCH TIẾP CẬN, PHƯƠNG PHÁP NGHIÊN CỨU	6
5.1. Cách tiếp cận	6
5.2. Phương pháp nghiên cứu.....	6
6. NỘI DUNG, ĐỐI TƯỢNG, PHẠM VI NGHIÊN CỨU	7
6.1. Nội dung nghiên cứu	7
6.2. Đối tượng nghiên cứu.....	7
6.3. Phạm vi nghiên cứu.....	7
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT	8
1. Tổng quan kiểm thử bảo mật.....	8
1.1. Kiểm thử bảo mật	9
1.2. Wargame	10
1.3. Kali Linux	10
2. Điện toán đám mây	12
2.1. Công nghệ ảo hoá	15
2.2. Private Cloud.....	16
2.3. OpenStack	17
CHƯƠNG 3: THIẾT KẾ GIẢI PHÁP	20
1. Thiết kế sơ đồ hệ thống	20
2. Thiết kế cơ sở dữ liệu cho ứng dụng web	21
CHƯƠNG 4: CÀI ĐẶT GIẢI PHÁP.....	23
1. Xây dựng nền tảng OpenStack.....	24
1.1. Cài đặt Ubuntu Server	24
1.2. Cài đặt DevStack	30
1.3. Cấu hình nền tảng OpenStack	32
2. Xây dựng bài tập thực hành kiểm thử bảo mật.....	37
2.1. Cấu hình mạng cho bài tập	37

2.2. Xây dựng Images cho các hệ điều hành	42
2.3. Xây dựng máy ảo tấn công và máy ảo mục tiêu.....	45
3. Xây dựng ứng dụng web	51
3.1. Thiết kế giao diện ứng dụng web	52
3.2. Kết nối đến bài tập kiểm thử bảo mật	62
CHƯƠNG 5: ĐÁNH GIÁ KIỂM THỬ	68
1. Đánh giá kiểm thử nền tảng OpenStack	68
2. Đánh giá kiểm thử ứng dụng web	69
2.1. Đánh giá kiểm thử các lớp học lý thuyết.....	69
2.2. Đánh giá kiểm thử các thử thách CTF.....	71
2.3. Đánh giá kiểm thử bài tập kiểm thử bảo mật	73
CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	76
1. Kết quả đạt được	76
2. Hạn chế.....	76
3. Hướng phát triển	76
TÀI LIỆU THAM KHẢO	77

DANH MỤC HÌNH ẢNH

Hình 1: Sơ đồ hệ thống	6
Hình 2: Hệ điều hành Kali Linux. Nguồn: kali.org.....	11
Hình 3: Điện toán đám mây. Nguồn: spiceworks.com.....	12
Hình 4: Ba mô hình dịch vụ điện toán đám mây. Nguồn: lucidchart.com	13
Hình 5: Public Cloud và Private Cloud. Nguồn: cloud.z.com	16
Hình 6: Nền tảng OpenStack. Nguồn: openstack.org	17
Hình 7: Các dịch vụ của OpenStack. Nguồn: openstack.org	19
Hình 8: Ý tưởng cho sơ đồ hệ thống	20
Hình 9: Mô hình EER của cơ sở dữ liệu	22
Hình 10: Sơ đồ hệ thống của đề tài	23
Hình 11: Cấu hình phần cứng đề xuất cho Ubuntu Server.....	24
Hình 12: Cấu hình card mạng thứ nhất	25
Hình 13: Cấu hình card mạng thứ hai	25
Hình 14: Cấu hình hệ thống	26
Hình 15: Cài đặt hệ điều hành Ubuntu Server.....	26
Hình 16: Cấu hình mạng cho hệ điều hành Ubuntu Server.....	27
Hình 17: Cài đặt dịch vụ SSH cho Ubuntu Server	27
Hình 18: Cài đặt hoàn tất hệ điều hành Ubuntu Server.....	27
Hình 19: Cấu hình mạng thủ công cho Ubuntu Server	28
Hình 20: Kiểm tra kết nối mạng của Ubuntu Server	29
Hình 21: SSH đến Ubuntu Server	29
Hình 22: Thiết lập các thông số cài đặt OpenStack	30
Hình 23: Cài đặt OpenStack thành công	31
Hình 24: Giao diện web của OpenStack	31
Hình 25: Đăng nhập vào OpenStack bằng tài khoản admin.....	32
Hình 26: Tạo một Project cho sản phẩm nghiên cứu	32
Hình 27: Thông tin Project.....	33
Hình 28: Tạo một User mới	33
Hình 29: Đặt mật khẩu, chọn Primary Project và phân quyền admin cho User.....	34
Hình 30: Đăng nhập vào tài khoản của User vừa được tạo	34
Hình 31: Tải OpenStack RC File để có thể kết nối đến OpenStack từ xa.....	35
Hình 32: Tải bộ công cụ dòng lệnh về Ubuntu Server	35
Hình 33: Tải OpenStack RC File lên Ubuntu Server	36
Hình 34: Thực thi Open RC File và đăng nhập để xác minh	36
Hình 35: Một ví dụ về truy cập OpenStack thông qua giao diện dòng lệnh	36
Hình 36: Cấu hình Network	37
Hình 37: Cấu hình Subnet cho Network	38
Hình 38: Cấu hình Allocation Pools và DNS Name Servers cho Network.....	38
Hình 39: Tạo một Router kết nối đến public network.....	39
Hình 40: Thêm nhánh mạng vào giao diện card mạng trong của Router	39
Hình 41: Network Topology	40
Hình 42: Floating IPs	40
Hình 43: Tạo một Security Group mới	41
Hình 44: Thêm các quy tắc vào Security Group	41
Hình 45: Image của hệ điều hành CirrOS	42
Hình 46: Images cho môi trường đám mây của hệ điều hành Kali Linux	42
Hình 47: Tải xuống Generic Cloud Image của hệ điều hành Kali Linux.....	43
Hình 48: Trích xuất RAW Image của hệ điều hành Kali Linux.....	43
Hình 49: QCOW2 Image của hệ điều hành Kali Linux	44
Hình 50: Xây dựng Image Kali Linux trên môi trường OpenStack	44
Hình 51: Images trên môi trường OpenStack.....	45
Hình 52: Máy ảo mục tiêu với hệ điều hành CirrOS.....	45
Hình 53: Thực hiện gắn Floating IP cho máy ảo mục tiêu.....	46
Hình 54: Bảng điều khiển máy ảo mục tiêu	46

Hình 55: Kiểm tra kết nối mạng của máy ảo mục tiêu.....	47
Hình 56: Máy ảo tấn công với hệ điều hành Kali Linux.....	48
Hình 57: Thực hiện gắn Floating IP cho máy ảo tấn công.....	48
Hình 58: Bảng điều khiển máy ảo tấn công.....	49
Hình 59: Kiểm tra kết nối mạng của máy ảo tấn công.....	49
Hình 60: Thiết lập kết nối SSH đến máy ảo tấn công.....	50
Hình 61: Kết nối SSH đến máy ảo tấn công và kiểm tra tính năng.....	50
Hình 62: Cấu trúc của bài tập thực hành.....	51
Hình 63: Giao diện đăng nhập.....	52
Hình 64: Giao diện trang chủ.....	53
Hình 65: Giao diện danh sách lớp học của User.....	53
Hình 66: Giao diện danh sách lớp học của Admin.....	54
Hình 67: Giao diện tạo lớp học mới của Admin.....	54
Hình 68: Giao diện sửa thông tin lớp học của Admin.....	54
Hình 69: Giao diện bên trong lớp học của User.....	55
Hình 70: Giao diện bên trong lớp học của Admin.....	55
Hình 71: Giao diện các thử thách CTF của User.....	56
Hình 72: Giao diện các thử thách CTF của Admin.....	56
Hình 73: Giao diện tạo thử thách CTF của Admin.....	56
Hình 74: Giao diện bên trong thử thách của User.....	57
Hình 75: Giao diện bên trong thử thách của Admin.....	57
Hình 76: Giao diện chế độ chỉnh sửa thử thách của Admin.....	57
Hình 77: Giao diện bài tập thực hành kiểm thử bảo mật.....	58
Hình 78: Giao diện trang cá nhân của mỗi người dùng.....	58
Hình 79: Giao diện dành cho User gửi đóng góp ý kiến.....	59
Hình 80: Giao diện dành cho Admin xem các góp ý từ User.....	59
Hình 81: Giao diện cài đặt.....	59
Hình 82: Giao diện cài đặt ảnh đại diện.....	60
Hình 83: Giao diện đổi mật khẩu.....	60
Hình 84: Chế độ sáng/tối.....	60
Hình 85: Trang chủ với chế độ tối.....	61
Hình 86: Trang cá nhân với chế độ tối.....	61
Hình 87: Các lớp học với chế độ tối.....	61
Hình 88: Các thử thách CTF với chế độ tối.....	62
Hình 89: Các góp ý từ người dùng được xem với chế độ tối.....	62
Hình 90: Mã nguồn PHP OpenStack SDK trên GitHub.....	63
Hình 91: Tập tin README hướng dẫn cài đặt PHP OpenStack SDK.....	63
Hình 92: Cài đặt Composer.....	64
Hình 93: Cài đặt PHP OpenStack SDK thông qua Composer.....	64
Hình 94: Các mã nguồn tham khảo.....	65
Hình 95: Cấu hình kết nối đến máy ảo trên OpenStack với VNC.....	65
Hình 96: Authentication URL kết nối đến OpenStack.....	66
Hình 97: ID của máy ảo tấn công.....	66
Hình 98: ID của máy ảo phòng thủ.....	67
Hình 99: Region của OpenStack.....	67
Hình 100: Kết nối đến máy ảo tấn công từ ứng dụng web.....	67
Hình 101: Thư mục lưu trữ các bài giảng và bài tập An toàn thông tin.....	69
Hình 102: Tạo lớp học mới.....	69
Hình 103: Các tài liệu liên quan đến lớp học.....	70
Hình 104: Tạo một tin tức gửi đến lớp học.....	70
Hình 105: Bảng tin lớp học đã được cập nhật.....	70
Hình 106: Sau khi truy cập đến đường liên kết.....	71
Hình 107: Tập tin chứa flag của thử thách.....	71
Hình 108: Xây dựng thử thách CTF.....	72
Hình 109: Thử thách CTF sau khi nhập kết quả sai.....	72
Hình 110: Thử thách CTF sau khi nhập kết quả đúng.....	72
Hình 111: Kết nối đến bài tập kiểm thử bảo mật từ ứng dụng web.....	73

Hình 112: Kiểm tra kết nối mạng của bài tập từ ứng dụng web.....	73
Hình 113: Cập nhật các gói tin apt của máy ảo tấn công từ ứng dụng web.	74
Hình 114: Cài đặt công cụ Nmap lên máy ảo tấn công từ ứng dụng web.	74
Hình 115: Kiểm tra cấu hình mạng của máy ảo tấn công từ ứng dụng web.	74
Hình 116: Quét cổng từ các máy ảo nằm trên nhánh mạng bài tập từ ứng dụng web.	75
Hình 117: Tiến hành tấn công vào dịch vụ SSH của máy mục tiêu từ ứng dụng web.	75
Hình 118: Kiểm tra tình trạng máy mục tiêu trên nền tảng OpenStack.	75

LỜI CẢM ƠN

Nhóm tác giả xin gửi lời cảm ơn chân thành đến Thầy Thái Minh Tuấn, một người thầy đáng kính đồng thời là người hướng dẫn bài nghiên cứu khoa học của nhóm chúng em. Nhờ sự tận tình chỉ bảo, những kiến thức chuyên môn sâu rộng và kinh nghiệm phong phú của Thầy, nhóm đã được trang bị những hành trang cần thiết để thực hiện thành công đề tài nghiên cứu này. Từ việc xây dựng đề tài, thu thập dữ liệu, phân tích kết quả đến việc hoàn thiện báo cáo, Thầy luôn dành thời gian hướng dẫn tận tình và đưa ra những góp ý quý báu.

Nhóm chúng em cũng xin bày tỏ lòng biết ơn sâu sắc đến Ban giám hiệu nhà trường và các thầy cô đã tạo điều kiện thuận lợi về cơ sở vật chất, tài liệu tham khảo và tạo môi trường nghiên cứu khoa học hiệu quả.

Nhóm nhận thức rằng, đề tài còn nhiều hạn chế. Chúng em rất mong nhận được những đóng góp ý kiến từ Quý thầy cô, các chuyên gia và độc giả để giúp đề tài được hoàn thiện hơn.

Cuối cùng, nhóm xin được gửi lời kính chúc sức khỏe đến quý thầy cô cùng các bạn.

Xin chân thành cảm ơn!

Đại diện nhóm

Trương Đặng Trúc Lâm

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ

THÔNG TIN KẾT QUẢ NGHIÊN CỨU CỦA ĐỀ TÀI

1. Thông tin chung:

Mã số đề tài: THS2024-77

Tên đề tài: Xây dựng môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây

Sinh viên chủ nhiệm đề tài: Trương Đặng Trúc Lâm

Lớp: Công nghệ Thông tin CLC 03, K47

Trường: Công nghệ Thông tin và Truyền thông

Năm thứ: 4

Số năm đào tạo: 4.5

Người hướng dẫn: TS. Thái Minh Tuấn

2. Mục tiêu đề tài:

Xây dựng môi trường thực tập kiểm thử bảo mật đồng thời cung cấp các kiến thức thuộc lĩnh vực An toàn thông tin.

Triển khai các bài giảng và thử thách về cơ sở lý thuyết An toàn thông tin, các kỹ thuật tấn công và phòng thủ trên không gian mạng.

Tích hợp công nghệ điện toán đám mây nhằm xây dựng các máy ảo tấn công và các máy ảo mục tiêu cho các bài tập kiểm thử bảo mật.

3. Tính mới và sáng tạo:

Hệ thống sử dụng công nghệ điện toán đám mây OpenStack nhằm xây dựng sẵn các máy ảo tấn công và máy ảo mục tiêu, giúp cho sinh viên không còn phải tiêu hao thời gian xây dựng môi trường thực tập trên máy cá nhân.

Hệ thống tích hợp công nghệ VNC giúp sinh viên có thể kết nối đến các máy ảo và thực hành bài tập thông qua ứng dụng web.

Nhóm sẽ sưu tầm và sáng tạo thêm các bài giảng và thử thách nhằm cung cấp kiến thức thuộc lĩnh vực An toàn thông tin cho sinh viên.

Tạo tiền đề cho các hệ thống nâng cấp cải tiến về sau.

4. Kết quả nghiên cứu:

Cơ sở hạ tầng điện toán đám mây OpenStack quản lý các cặp máy ảo tấn công và mục tiêu phục vụ cho những thử thách kiểm thử bảo mật được triển khai trên ứng dụng web.

Ứng dụng web gồm có ba phần:

- Các lớp học sẽ cung cấp kiến thức thuộc lĩnh vực An toàn thông tin cho sinh viên thông qua các bài giảng và tài liệu.
- Các thử thách CTF với những chủ đề như Forensics, Web Exploitation, Reverse Engineering, Cryptography,...
- Các bài tập kiểm thử bảo mật sẽ được sinh viên thực hiện trên bảng điều khiển VNC tại ứng dụng web. Bảng điều khiển này sẽ kết nối đến màn hình của máy ảo tấn công được xây dựng sẵn trên nền tảng OpenStack, từ đó ta có thể tấn công máy ảo mục tiêu theo yêu cầu của bài tập.

5. Sản phẩm:

Môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây.

6. Công bố khoa học từ kết quả nghiên cứu của đề tài, hoặc nhận xét, đánh giá của cơ sở đã áp dụng các kết quả nghiên cứu:

Không

7. Đóng góp về mặt kinh tế - xã hội, giáo dục và đào tạo, an ninh, quốc phòng và khả năng áp dụng của đề tài:

Đối với lĩnh vực giáo dục và đào tạo: Là môi trường thực tập kiểm thử bảo mật phù hợp với các sinh viên có định hướng An toàn thông tin. Bên cạnh đó, giảng viên có thể sử dụng ứng dụng minh họa cho các bài giảng có liên quan.

Đối với lĩnh vực khoa học và công nghệ có liên quan: Xây dựng và phát triển môi trường thực tập kiểm thử bảo mật trên nền tảng điện toán đám mây. Kết quả ứng dụng có thể cải tiến, phát triển cho các dự án nghiên cứu khoa học khác.

Đối với phát triển kinh tế - xã hội: Môi trường thực tập kiểm thử bảo mật cung cấp cho sinh viên kiến thức và kỹ năng An toàn thông tin cần thiết để có thể hỗ trợ tăng cường bảo mật cho các cơ quan, doanh nghiệp, tổ chức,...

Đối với tổ chức chủ trì và các cơ sở ứng dụng kết quả nghiên cứu: Hệ thống có thể tiếp tục phát triển trong tương lai với lợi ích giáo dục và đào tạo. Ngoài ra, hệ thống còn là nguồn tài liệu cho sinh viên để thực hiện các ý tưởng sáng tạo khác.

8. Hiệu quả, phương thức chuyển giao kết quả nghiên cứu và khả năng áp dụng:

Hiệu quả: Môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây giúp sinh viên dễ dàng tiếp cận hơn trong việc thực tập kiểm thử bảo mật, tiết kiệm được thời gian và chi phí so với việc tự thiết lập môi trường trên máy cá nhân.

Phương thức chuyển giao: Tài liệu liên quan đến môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây.

Khả năng áp dụng: Có thể phát triển thành sản phẩm hoàn chỉnh và triển khai thực tế.

Ngày 27 tháng 9 năm 2024
Chủ nhiệm đề tài

Nhận xét của người hướng dẫn về những đóng góp khoa học của sinh viên thực hiện đề tài (phản này do người hướng dẫn ghi):

Xác nhận của Trường Đại học Cần Thơ

Ngày tháng năm
Người hướng dẫn

**MINISTRY OF EDUCATION AND TRAINING
CAN THO UNIVERSITY**

INFORMATION ON RESEARCH RESULTS

1. General information:

Project code: THS2024-77

Project title: Cloud-based security testing practice environment

Code number: THS2024-77

Coordinator: Truong Dang Truc Lam

Implementing institution: The College of Information and Communication Technology

Duration: from 4/2024 to 10/2024

2. Objectives:

Building a security testing practice environment and providing knowledge about Information Security.

Implementing lectures and challenges on Information Security theory, attack and defense techniques in cyberspace.

Integrating Cloud Computing technology to build attack VMs and target VMs for security testing exercises.

3. Creativeness and innovativeness:

System uses OpenStack to pre-build attack VMs and target VMs, helping students no longer have to spend time building a practice environment on their personal computers.

System integrates VNC technology to help students connect to VMs through the web application and practice exercises.

Our group will collect and create more lectures and challenges to provide knowledge in the field of Information Security for students.

Creating the premise for future system upgrades and improvements.

4. Research results:

OpenStack Cloud Computing Infrastructure manages attack and target VMs for security testing challenges deployed on the web application.

The application consists of three parts:

- Classes will provide knowledge in the field of Information Security through lectures and documents.
- CTF challenges with topics such as Forensics, Web Exploitation, Reverse Engineering, Cryptography,...
- Security testing exercises will be practiced by students through the VNC Console on the application. This Console will connect to the screen of the attack VM that has been built on the OpenStack platform, from which we can attack the target VM according to the requirements of the exercise.

5. Products:

Cloud-based security testing practice environment.

6. Effects, technology transfer means and applicability:

Effects: This product can help students easily access security testing practice, saving time and cost compared to setting up a practice environment themselves.

Technology transfer means: Documentation related to a cloud-based security testing practice environment.

Applicability: It can be developed into a complete product for deployment.

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ

**THÔNG TIN VỀ SINH VIÊN CHỊU TRÁCH NHIỆM CHÍNH
THỰC HIỆN ĐỀ TÀI**

I. SO' LU' QỨC VỀ SINH VIÊN

Họ và tên: Trương Đặng Trúc Lâm

Sinh ngày: 30 tháng 01 năm 2003

Nơi sinh: Cần Thơ

Lớp: Công nghệ Thông tin CLC 03

Khoa: 47

Trường: CNTT-TT

Địa chỉ liên hệ: 139/169, đường 30/4, quận Ninh Kiều, thành phố Cần Thơ

Điện thoại: 0907543817

Email: lamb2111933@student.ctu.edu.vn

Ảnh 4x6

II. QUÁ TRÌNH HỌC TẬP

***Năm thứ 1:**

Ngành học: Công nghệ Thông tin CLC Trường: CNTT-TT

Kết quả xếp loại học tập: Xếp loại Xuất sắc (Điểm trung bình tích lũy : 3.56)

Kết quả phân loại Đoàn viên: Xuất sắc

Thành tích tiêu biểu

Sđt	Thành tích tiêu biểu	Năm học học kỳ	Số quyết định	Ngày cấp	Lý do
1	Giấy khen Đoàn khoa	2022-2023 HK 1	18-QĐ/ĐTN	14-10-2022	Đã có nhiều thành tích đóng góp trong công tác Đoàn và phong trào thanh niên năm học 2021-2022

***Năm thứ 2:**

Ngành học: Công nghệ Thông tin CLC Trường: CNTT-TT

Kết quả xếp loại học tập: Xếp loại Xuất sắc (Điểm trung bình tích lũy : 3.75)

Kết quả phân loại Đoàn viên: Xuất sắc

Thành tích tiêu biểu

Số	Thành tích tiêu biểu	Năm học học kỳ	Số quyết định	Ngày cấp	Lý do
1	Trao đổi sinh viên	2022-2023 HK 2	3084	18-06-2023	Malaysia, 18/7 - 22/7
2	Giấy khen Đoàn khoa	2022-2023 HK 2	115-QĐ/ĐTN	06-06-2023	Đã có nhiều đóng góp tích cực trong lớp Tập huấn cán bộ đoàn trường Công nghệ Thông tin & Truyền Thông năm 2023
3	Giấy khen Đoàn khoa	2022-2023 HK 2	117-QĐ/ĐTN	06-06-2023	Đã tích cực tham gia Hội diễn văn nghệ truyền thống trường ĐHCT năm 2023
4	Giấy khen Đoàn khoa	2023-2024 HK 1	118-QĐ/ĐTN	20-06-2023	Đã có nhiều đóng góp xuất sắc trong lớp Tập huấn mùa hè xanh - Mùa hè số năm 2023
5	Khen thưởng năm học	2023-2024 HK 1	3925	18-08-2023	

***Năm thứ 3:**

Ngành học: Công nghệ Thông tin CLC Trường: CNTT-TT

Kết quả xếp loại học tập: Xếp loại Xuất sắc (Điểm trung bình tích lũy : 3.68)

Kết quả phân loại Đoàn viên: Xuất sắc

Thành tích tiêu biểu:

Số	Thành tích tiêu biểu	Năm học học kỳ	Số quyết định	Ngày cấp	Lý do
1	Khen thưởng năm học	2023-2024 HK 2	3381	2024-08-20	

Ngày 27 tháng 9 năm 2024

Xác nhận của Trường Đại học Cần Thơ

Chủ nhiệm đề tài

CHƯƠNG 1: TỔNG QUAN

1. ĐẶT VẤN ĐỀ

Trong thời đại số, mạng Internet đã trở thành một phần không thể thiếu trong cuộc sống của mỗi người. Chỉ với một chiếc điện thoại thông minh, chúng ta có thể kết nối với bạn bè khắp nơi trên thế giới, tìm kiếm thông tin một cách nhanh chóng, mua sắm trực tuyến, học tập từ xa và làm việc hiệu quả hơn. Internet đã cách mạng hóa mọi lĩnh vực của cuộc sống, từ kinh tế, xã hội, văn hóa đến chính trị, tạo ra những cơ hội mới và thay đổi sâu sắc cách chúng ta sống và làm việc.

Tuy nhiên, bên cạnh những lợi ích to lớn, không gian mạng vẫn còn tiềm ẩn những nguy cơ. Với những thủ đoạn ngày càng tinh vi, các hacker luôn tìm cách khai thác, lợi dụng các kẽ hở bảo mật để đánh cắp thông tin cá nhân, tài sản, lừa đảo, thậm chí gây ra những tổn thất nghiêm trọng về danh dự và uy tín. Các cuộc tấn công mạng diễn ra hàng ngày có thể gây ra những thiệt hại kinh tế không lồ và ảnh hưởng đến an ninh quốc gia.

Theo số liệu của Trung tâm Công nghệ Thông tin và giám sát an ninh mạng, quý I ghi nhận 32.265 nguy cơ tấn công mạng, trong đó có: 16.584 nguy cơ tấn công truy cập trái phép (đánh cắp dữ liệu, tài khoản, mật khẩu người dùng qua hình thức dò quét mật khẩu hệ thống), 3.888 nguy cơ tấn công khai thác lỗ hổng bảo mật (tin tặc chiếm quyền điều khiển, kiểm soát các máy chủ, dịch vụ), 420 nguy cơ tấn công mã độc và đặc biệt, 11.332 hành vi bất thường.

Có thể thấy rằng một trong những vấn đề nan giải hiện nay là tình trạng thiếu hụt nghiêm trọng nguồn nhân lực An toàn thông tin. Nguyên nhân chính của tình trạng này là do điều kiện học tập và rèn luyện kỹ năng An toàn thông tin còn hạn chế. Các chương trình đào tạo An toàn thông tin tại Việt Nam mặc dù đã có nhiều cải thiện nhưng vẫn chưa đáp ứng được nhu cầu thực tế của thị trường.

Bên cạnh đó, việc xây dựng môi trường thực tập, kiểm thử bảo mật đòi hỏi nguồn lực lớn về thời gian và chi phí. Cụ thể, việc xây dựng các máy ảo để mô phỏng môi trường thực tế phục vụ cho việc học tập và nghiên cứu của sinh viên yêu cầu phải đầu tư máy vật lý cá nhân có cấu hình đáp ứng đủ yêu cầu. Quá trình triển khai và quản lý hệ thống máy ảo cũng tiêu tốn nhiều thời gian, đồng thời gây ra khó khăn trong việc cập nhật, mở rộng quy mô và chia sẻ tài nguyên.

Để giải quyết những hạn chế trên, nhóm đã quyết định xây dựng "Môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây". Đây là một giải pháp sáng tạo, tận dụng tối đa các lợi ích của công nghệ điện toán đám mây để cung cấp môi trường học tập và rèn luyện kỹ năng An toàn thông tin linh hoạt, hiệu quả và tiết kiệm chi phí.

2. TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU

2.1. Trong nước

Việt Nam đang đối mặt với sự gia tăng về tần suất và mức độ phức tạp của các cuộc tấn công mạng. Theo báo cáo của Cục An toàn Thông tin (AIS), hàng nghìn vụ tấn công mạng vào các hệ thống quan trọng xảy ra mỗi năm, dẫn đến sự thiếu hụt trầm trọng về nguồn nhân lực có kỹ năng chuyên sâu trong lĩnh vực bảo mật. Chính vì thế, các tổ chức lớn như ngân hàng, tài chính, doanh nghiệp công nghệ và nhà nước đều đang tăng cường tuyển dụng và đào tạo nhân lực an ninh mạng.

Nhận thấy cơ hội việc làm cao, một số trường đại học đã phát triển các chương trình đào tạo chuyên sâu về an ninh mạng nhằm đáp ứng nhu cầu ngày càng cao về nguồn nhân lực trong lĩnh vực này. Tuy nhiên, việc giảng dạy ngành an ninh mạng và các môn học liên quan đến bảo mật thông tin tại các trường đại học ở Việt Nam cũng gặp phải nhiều khó khăn và thách thức. Dưới đây là một số bất lợi và khó khăn chính:

- Thiếu hụt giảng viên chuyên môn cao: Các giảng viên có chuyên môn sâu về an ninh mạng rất khan hiếm. Những chuyên gia hàng đầu thường được các doanh nghiệp săn đón với mức lương cao, trong khi các trường đại học gặp khó khăn trong việc giữ chân hoặc tuyển dụng những người có chuyên môn cao. An ninh mạng là lĩnh vực thay đổi nhanh chóng với nhiều mối đe dọa và công nghệ mới. Giảng viên cần phải liên tục cập nhật kiến thức và phương pháp giảng dạy để theo kịp sự phát triển của công nghệ, điều này đòi hỏi nguồn lực và thời gian mà không phải trường nào cũng có thể đáp ứng.
- Thiếu cơ sở hạ tầng và trang thiết bị thực hành: Lĩnh vực an ninh mạng đòi hỏi các phòng thí nghiệm, môi trường mạng ảo hóa, các hệ thống bảo mật và thiết bị phần cứng chuyên dụng để sinh viên có thể thực hành các kỹ năng kiểm thử bảo mật, phát hiện và phòng chống tấn công. Nhiều trường đại học, đặc biệt là các trường công lập với ngân sách hạn chế, gặp khó khăn trong việc đầu tư cơ sở hạ tầng và trang thiết bị này.
- Nội dung giảng dạy chưa đáp ứng nhu cầu thực tế: Với tốc độ thay đổi chóng mặt của công nghệ, các chương trình học về an ninh mạng tại một số trường đại học và cao đẳng vẫn chưa được cập nhật kịp thời để phản ánh những xu hướng và mối đe dọa mới nhất trong lĩnh vực này. Điều này dẫn đến một khoảng cách đáng kể giữa kiến thức lý thuyết được giảng dạy trên lớp và những kỹ năng thực tế mà các doanh nghiệp đang tìm kiếm.

Vì vậy, đề đáp ứng được nhu cầu của thị trường và các bạn sinh viên, đề tài đang hướng đến việc xây dựng môi trường thực tập kiểm thử bảo mật. Đề tài sẽ cung cấp các kiến thức An toàn thông tin cho người dùng, giảm chi phí, tài nguyên của người dùng trong quá trình kiểm tra an toàn bảo mật. Ngoài ra, môi trường thực tập này sẽ giúp sinh viên có cơ hội tiếp cận với các tình huống thực tế, nâng cao kỹ năng phân tích và xử lý sự cố bảo mật. Điều này không chỉ trang bị cho người học kiến thức lý thuyết mà còn giúp họ tự tin hơn trong việc áp dụng vào các dự án thực tiễn. Nhờ đó, môi trường này sẽ góp phần giải quyết bài toán thiếu hụt nguồn nhân lực chất lượng cao trong lĩnh vực an ninh mạng, đồng thời thúc đẩy sự phát triển của ngành công nghệ thông tin tại Việt Nam.

2.2. Ngoài nước

Việc xây dựng một môi trường thực tập chuyên sâu về kiểm thử bảo mật đã trở thành một chủ đề nghiên cứu trọng điểm trong những năm gần đây, đặc biệt tại các quốc gia có yêu cầu cao về tiêu chuẩn bảo mật cho các kỹ sư an toàn thông tin. Trên phạm vi toàn cầu, nhiều nhóm nghiên cứu đã tập trung vào lĩnh vực này, đưa ra các phương pháp đa dạng nhằm cung cấp cho sinh viên những kiến thức chuyên sâu và cơ hội thực hành trong môi trường an toàn thông tin. Trong nghiên cứu của mình, T. Andrew Yang và Tuan Anh Nguyen [1] đã nhận thấy tiềm năng cải tiến mô hình bảo mật mạng hiện có. Dựa trên nền tảng bảy bước [2] đã được trình bày trong mô hình, hai tác giả đã chủ động bổ sung thêm hai bước bao gồm: Service Identification, Asset/Resource Identification, Service-Asset Relationship, Threat Assessment, Risk Assessment, Policy Construction, Network Security Design, Network Security Implementation, Audit and Improvement.

Nghiên cứu [3] đã thực hiện một cuộc khảo sát toàn diện về các phương pháp giảng dạy bảo mật hệ thống thông tin, với mục tiêu tìm ra phương pháp tối ưu nhằm trang bị cho sinh viên những kiến thức và kỹ năng cần thiết, bao gồm phương pháp giảng bài truyền thống, phương pháp ghi chép, phương pháp học tập cùng chuyên gia, phương pháp hướng dẫn, phương pháp dự án, phương pháp kết hợp nghiên cứu và giảng dạy, và phương pháp mô phỏng tấn công - phòng thủ trong môi trường cách ly. Trong bài nghiên cứu [4], Christian Willems và Christoph Meinel đã xây dựng nền tảng học tập trực tuyến Tele-Lab phục vụ cho việc đào tạo thực hành an ninh mạng. Đó là sự kết hợp giữa hệ thống hướng dẫn trực tuyến với môi trường đào tạo dựa trên hệ thống máy ảo. Sinh viên có thể truy cập từ xa vào các máy ảo và thực hiện các bài tập, trong khi hệ thống đảm bảo triển khai và phục hồi dễ dàng. Phiên bản mới nhất của Tele-Lab giới thiệu việc phân bổ động nhiều máy ảo cho một người dùng duy nhất, cho phép mô phỏng các cuộc tấn công mạng. Nền tảng bao gồm một nạn nhân ảo mô phỏng hành vi người dùng và phản ứng với các cuộc tấn công.

Bên cạnh đó, tầm ảnh hưởng của công nghệ điện toán đám mây đang ngày một gia tăng và không có dấu hiệu kết thúc. Với những ưu điểm như dịch vụ nhanh chóng, tiết kiệm chi phí và thời gian, thân thiện với môi trường, đồng thời đem đến môi trường hợp tác bền vững. Trong bài nghiên cứu [5], nhóm tác giả đã cho thấy tính hiệu quả trong việc áp dụng nền tảng đám mây áp dụng cho việc giảng dạy. Bên cạnh đó, nghiên cứu [6] đã chỉ ra rằng việc ứng dụng công nghệ điện toán vào giáo dục mang lại những lợi ích vô cùng to lớn. Cụ thể, công nghệ này đã làm phong phú kho tàng các ứng dụng trực tuyến hỗ trợ việc dạy và học, tạo ra một môi trường học tập linh hoạt, tương tác và phù hợp với xu hướng học tập trên thiết bị di động. Đặc biệt, việc áp dụng công nghệ điện toán đám mây không chỉ giúp tiết kiệm chi phí đầu tư vào phần cứng và phần mềm mà còn mở rộng khả năng truy cập và ứng dụng các nguồn tài nguyên học tập. Chính vì thế các nhóm nghiên cứu An toàn thông tin đã chọn giải pháp xây dựng các môi trường thực tập kiểm thử bảo mật sử dụng tài nguyên trên nền tảng điện toán đám mây.

Trong nghiên cứu của mình, Le Xu, Dijiang Huang và Wei-Tek Sai đã giới thiệu một nền tảng phòng thí nghiệm ảo (V-Lab) tiên tiến [7], được xây dựng trên nền tảng điện toán đám mây nhằm phục vụ cho việc giảng dạy và thực hành bảo mật mạng máy tính. V-Lab tận dụng các công nghệ ảo hóa mã nguồn mở hàng đầu như Xen và KVM, kết hợp với các giải pháp mạng được định nghĩa bằng phần mềm (SDN) tiên tiến như OpenFlow switches. Thiết kế của V-Lab dựa trên công trình trước đây của nhóm tác giả với các tính năng cải tiến, bao gồm môi trường thực nghiệm bảo mật mạng độc lập, cung cấp các máy ảo (VM) và mạng ảo riêng cho sinh viên, đảm bảo sự an toàn cho hệ thống bên ngoài. Môi trường mạng có thể cấu hình lại, có thể linh hoạt mô phỏng các mạng máy tính khác nhau trong thế giới thực.

Mặt khác, nền tảng học tập bảo mật trực tuyến như HackTheBox [8], TryHackme [9] và PwnCollege [10] đã khẳng định vai trò quan trọng trong việc cung cấp một môi trường thực hành lý tưởng, góp phần nâng cao đáng kể kỹ năng cho cộng đồng chuyên về an toàn thông tin. Việc ứng dụng thành công công nghệ điện toán đám mây đã mang đến những đột phá, tạo ra các môi trường học tập linh hoạt và mở rộng quy mô, đáp ứng nhu cầu đa dạng của người học. Nhờ đó, người dùng có cơ hội tiếp cận với hệ thống kiến thức phong phú, thực hành trên các hệ thống mô phỏng chân thực, từ đó tự tin ứng dụng vào thực tiễn công việc.

3. TÍNH CẤP THIẾT CỦA ĐỀ TÀI

Tăng cường đào tạo nhân lực An toàn thông tin đang là chủ đề cấp thiết trong nước ta, đặc biệt là khu vực Đồng bằng sông Cửu Long. Hiện nay, Đại học Cần Thơ đã xây dựng và phát triển các hệ thống học tập trực tiếp như CTU E-Learning, ELSE,... nhưng vẫn chưa có môi trường thực tập kiểm thử bảo mật dành cho sinh viên.

Việc thiết lập môi trường thực tập kiểm thử bảo mật trên máy cá nhân đang là một trở ngại lớn đối với nhiều sinh viên. Xây dựng các máy ảo theo cách thủ công đòi hỏi sinh viên phải có kiến thức chuyên sâu về hệ thống, mạng và bảo mật, đồng thời tiêu tốn nhiều thời gian và công sức để cài đặt, cấu hình và khắc phục sự cố. Hơn nữa, để có thể đáp ứng được yêu cầu của các bài thực hành, máy cá nhân cần phải có cấu hình phần cứng mạnh mẽ, điều mà không phải sinh viên nào cũng có thể đáp ứng. Điều này không chỉ hạn chế cơ hội thực hành mà còn tạo ra bất bình đẳng trong quá trình học tập. Bên cạnh đó, việc thiếu tài liệu hướng dẫn chi tiết, cộng đồng hỗ trợ hạn chế và khó khăn trong việc tìm kiếm thông tin cũng là những rào cản lớn đối với sinh viên khi muốn tự mình xây dựng môi trường thực tập kiểm thử bảo mật.

Chính vì thế, đề tài đang hướng đến việc thiết kế một ứng dụng web nhằm xây dựng môi trường thực tập kiểm thử bảo mật dành cho sinh viên. Hệ thống sẽ bao gồm các bài kiểm tra thực hành và các thử thách bao gồm: các tập tin như ảnh, video hoặc các máy chủ được thiết kế nhằm làm mục tiêu để tấn công. Bên cạnh đó, đề tài sẽ tích hợp thêm các lớp học trực tuyến, các tài liệu có liên quan,... vào ứng dụng web.

4. MỤC TIÊU ĐỀ TÀI

Xây dựng môi trường thực tập kiểm thử bảo mật đồng thời cung cấp các kiến thức thuộc lĩnh vực An toàn thông tin cho sinh viên Trường Đại học Cần Thơ.

Triển khai các bài giảng và thử thách về cơ sở lý thuyết An toàn thông tin, các kỹ thuật tấn công và phòng thủ trên không gian mạng.

Tích hợp công nghệ điện toán đám mây nhằm xây dựng các máy ảo tấn công và các máy ảo mục tiêu cho các bài tập kiểm thử bảo mật.

5. CÁCH TIẾP CẬN, PHƯƠNG PHÁP NGHIÊN CỨU

5.1. Cách tiếp cận

Nghiên cứu lý thuyết - thử nghiệm - ứng dụng.

5.2. Phương pháp nghiên cứu

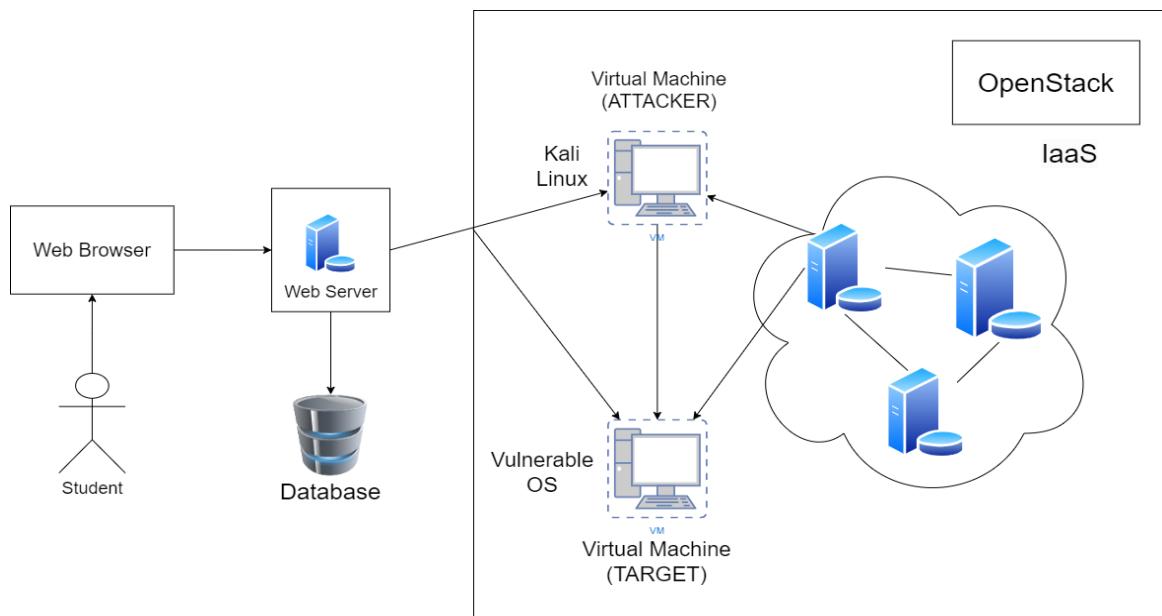
Nghiên cứu cơ sở lý thuyết An toàn thông tin: Thu thập và phân tích các tài liệu tham khảo từ các tổ chức chuyên nghiên cứu về lĩnh vực An toàn thông tin.

Xây dựng môi trường thực tập kiểm thử bảo mật: Tham khảo các môi trường thực tập kiểm thử bảo mật uy tín đã có. Từ đó thu thập, phân tích và chọn ra giải pháp xây dựng hệ thống sao cho phù hợp. Như được mô tả trong Hình 1, đề tài sẽ sử dụng nền tảng OpenStack để thiết lập một cơ sở hạ tầng dịch vụ cho phép xây dựng các máy ảo đóng vai trò là máy tấn công và máy mục tiêu. Bên cạnh đó, nhóm sẽ thiết kế một giao diện web cho phép ta quản lý các bài tập thực hành và thử thách.

Kiểm thử: Tiến hành kiểm thử để đảm bảo tính ổn định và chính xác của hệ thống.

Triển khai hệ thống qua các hoạt động: Tổ chức xây dựng nội dung số gồm các bài giảng, các bài tập thực hành; tổ chức tập huấn cho giảng viên, sinh viên sử dụng hệ thống; đưa hệ thống vận hành thực tế.

Đánh giá kết quả: Kết quả của đề tài sẽ được đánh giá bằng cách so sánh với các môi trường thực tập kiểm thử bảo mật khác. Từ đó đưa ra những đánh giá về tính khả thi và hiệu quả của ứng dụng trong việc giáo dục và đào tạo.



Hình 1: Sơ đồ hệ thống.

6. NỘI DUNG, ĐỐI TƯỢNG, PHẠM VI NGHIÊN CỨU

6.1. Nội dung nghiên cứu

Tìm hiểu các nghiên cứu có liên quan đến đề tài.

Tìm hiểu và đề xuất các công nghệ sử dụng.

Cài đặt môi trường IaaS.

Xây dựng và phát triển ứng dụng web.

Triển khai các bài tập kiểm thử bảo mật trên ứng dụng web.

Kiểm thử và đánh giá hệ thống.

6.2. Đối tượng nghiên cứu

Cơ sở lý thuyết An toàn thông tin và các kỹ thuật tấn công và phòng thủ trên không gian mạng. Đồng thời nghiên cứu phương pháp quy trình phát triển ứng dụng web và tích hợp tài nguyên trên đám mây phục vụ cho việc thiết kế các bài kiểm tra thực hành và thử thách.

6.3. Phạm vi nghiên cứu

Nghiên cứu sẽ tập trung vào việc thiết kế và xây dựng một môi trường thực tập kiểm thử bảo mật dành cho sinh viên. Nội dung bao gồm:

Điện toán đám mây: OpenStack

Lập trình web: PHP

An toàn thông tin: các công cụ trên Kali Linux

Thời gian thực hiện đề tài nghiên cứu: 7 tháng (04/2024 - 10/2024)

Không gian: nghiên cứu trong phạm vi Đại học Cần Thơ

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

1. Tổng quan kiểm thử bảo mật

An toàn thông tin [11] là quá trình bảo vệ thông tin, hệ thống và mạng lưới khỏi mọi hành vi truy cập, sử dụng, tiết lộ, sửa đổi hoặc phá hủy trái phép. Mục tiêu cuối cùng là đảm bảo tính nguyên vẹn, bảo mật và khả dụng của dữ liệu trong môi trường số ngày càng phức tạp.

Trong thời đại số, thông tin đã trở thành tài sản quý giá hơn cả. Tuy nhiên, cùng với sự phát triển của công nghệ, các mối đe dọa đối với an toàn thông tin cũng ngày càng trở nên tinh vi và đa dạng. Các cuộc tấn công mạng không còn đơn thuần là trò đùa của các hacker mà đã trở thành công cụ kiếm lợi của các tổ chức tội phạm xuyên quốc gia, tiêu biểu là vụ tấn công ransomware WannaCry năm 2017 đã khiến hàng nghìn tổ chức trên toàn cầu té liệt, gây thiệt hại kinh tế không lồ.

Hậu quả của các cuộc tấn công mạng không chỉ dừng lại ở việc mất mát dữ liệu. Chúng còn gây ra những thiệt hại nghiêm trọng về tài chính, danh tiếng, và thậm chí đe dọa đến an ninh quốc gia. Các tổ chức có thể bị mất hàng tỷ đô la do rò rỉ dữ liệu khách hàng, gián đoạn hoạt động sản xuất kinh doanh, và mất lòng tin của cổ đông. Đối với cá nhân, việc bị đánh cắp thông tin cá nhân có thể dẫn đến việc bị lừa đảo, trộm cắp danh tính, và ảnh hưởng đến cuộc sống hàng ngày [12].

Để đối phó với những thách thức này, chúng ta cần có một chiến lược bảo mật toàn diện, bao gồm cả các giải pháp kỹ thuật và phi kỹ thuật. Các doanh nghiệp và tổ chức cần đầu tư vào các hệ thống bảo mật tiên tiến, xây dựng tường lửa vững chắc, và thường xuyên cập nhật phần mềm. Bên cạnh đó, việc nâng cao nhận thức về an toàn thông tin cho người dùng cũng là một yếu tố vô cùng quan trọng. Mỗi cá nhân cần chủ động bảo vệ thông tin của mình bằng cách sử dụng mật khẩu mạnh, không click vào các liên kết lạ, và cảnh giác với các cuộc gọi, email lừa đảo.

Cuối cùng, việc xây dựng một không gian mạng an toàn là trách nhiệm của toàn cộng đồng. Các tổ chức chính phủ cần ban hành các quy định pháp luật chặt chẽ để quản lý hoạt động trong không gian mạng, các doanh nghiệp cần tăng cường hợp tác để chia sẻ thông tin về các mối đe dọa mới, và mỗi cá nhân cần đóng góp vào việc xây dựng một xã hội số an toàn, văn minh.

1.1. Kiểm thử bảo mật

Kiểm thử bảo mật là một quá trình đánh giá toàn diện nhằm phát hiện, xác định và phân tích các lỗ hổng tiềm ẩn trong hệ thống phần mềm. Quá trình này nhằm mục tiêu bảo vệ dữ liệu nhạy cảm, ngăn chặn các cuộc tấn công từ bên ngoài và đảm bảo tính toàn vẹn của hệ thống trước những mối đe dọa an ninh mạng ngày càng tinh vi. Bảo mật thông tin được xây dựng trên ba trụ cột [13]:

- Tính bảo mật (Confidentiality): Ngăn chặn việc truy cập trái phép vào thông tin nhạy cảm. Điều này đòi hỏi việc thiết lập và thực thi các biện pháp kiểm soát truy cập chặt chẽ nhằm bảo vệ dữ liệu khỏi sự xâm nhập của các đối tượng không được ủy quyền.
- Tính toàn vẹn (Integrity): Đảm bảo rằng thông tin được bảo vệ khỏi sự sửa đổi, xóa bỏ hoặc thêm vào trái phép. Tính toàn vẹn bảo vệ tính xác thực và đáng tin cậy của dữ liệu, ngăn chặn các hành vi gian lận và phá hoại.
- Tính khả dụng (Availability): Đảm bảo rằng thông tin có thể truy cập được một cách kịp thời và liên tục bởi những người được ủy quyền khi cần. Tính khả dụng đòi hỏi việc xây dựng hệ thống thông tin ổn định, có khả năng phục hồi sau sự cố và đáp ứng được nhu cầu truy cập của người dùng.

Các kỹ thuật kiểm thử bảo mật có thể được phân loại thành nhiều loại nhỏ khác nhau dựa trên mức độ tương tác với hệ thống [14], thời gian thực hiện và các yêu cầu về kiến thức chuyên môn liên quan. Hầu hết các kỹ thuật kiểm thử bảo mật hiện hành được chia thành ba nhóm chính:

- Kiểm thử hộp đen (Black-box Techniques): Phương pháp kiểm thử sử dụng các kỹ thuật trong trường hợp người kiểm thử không có bất kỳ thông tin nào về cấu trúc bên trong, cách thức hoạt động nội bộ của hệ thống. Các kỹ thuật này tập trung vào việc kiểm tra các chức năng bên ngoài của hệ thống, nhằm đảm bảo chúng hoạt động đúng theo yêu cầu và không có lỗ hổng bảo mật rõ ràng.
- Kiểm thử hộp trắng (White-box Techniques): Phương pháp kiểm thử phân mềm chi tiết, trong đó người kiểm thử có quyền truy cập đầy đủ vào mã nguồn và cấu trúc nội bộ của hệ thống. Nhờ đó, ta có thể thực hiện phân tích, xác định và khắc phục các lỗ hổng bảo mật tiềm ẩn ngay từ giai đoạn phát triển.
- Kiểm thử Hộp Xám (Gray-box Techniques): Phương pháp kiểm thử phân mềm kết hợp ưu điểm của cả kiểm thử hộp đen và hộp trắng. Người kiểm thử sẽ được cung cấp kiến thức một cách hạn chế về cấu trúc bên trong của hệ thống, nhưng vẫn có thể tận dụng một số thông tin về thiết kế hoặc triển khai hệ thống.

1.2. Wargame

Wargame, hay còn được biết đến với thuật ngữ "cuộc chiến giả lập", là một hoạt động mô phỏng các cuộc tấn công mạng thực tế nhằm mục tiêu đánh giá toàn diện mức độ an toàn và khả năng bảo mật của hệ thống, mạng lưới hoặc ứng dụng. Thông qua việc thực hiện các cuộc tấn công giả định, những người tham gia wargame có cơ hội tích lũy kinh nghiệm quý báu trong việc phát hiện các lỗ hổng bảo mật tiềm ẩn và đánh giá hiệu quả các biện pháp phòng thủ hiện hành.

Capture the Flag (CTF) hiện nay được xem là một trong những hình thức wargame phổ biến nhất trong lĩnh vực an ninh mạng. Ra đời từ những ngày đầu của DEF CON vào giữa những năm 1990, CTF nhanh chóng trở thành một sân chơi hấp dẫn cho các hacker và chuyên gia bảo mật [15]. CTF mô phỏng các cuộc tấn công mạng, nơi các đội thi đấu trực tiếp để chiếm lấy "cờ" (Flag) của đối thủ đồng thời bảo vệ tài sản kỹ thuật số của mình. Các hình thức thi đấu CTF phổ biến bao gồm Jeopardy, Attack-Defense hoặc kết hợp cả hai loại trên:

- Jeopardy là hình thức thi đấu phổ biến nhất trong các cuộc thi CTF. Các đội thi sẽ phải giải quyết hàng loạt các bài toán bảo mật có độ phức tạp tăng dần, mỗi bài toán sẽ tập trung vào một lỗ hổng bảo mật cụ thể hoặc một kỹ thuật tấn công nhất định. Các chủ đề Jeopardy thường bao gồm Web, Reverse Engineering, Cryptography, Forensics,...
- Trong thể loại Attack-Defense, các đội thi sẽ được cung cấp một hệ thống hoặc một mạng lưới với các dịch vụ và ứng dụng đang hoạt động, mô phỏng môi trường mạng thực tế. Mỗi đội sẽ vừa phải tấn công vào hệ thống của đội khác, vừa phải bảo vệ hệ thống của đội nhà.

Hiện nay, có rất nhiều nền tảng wargame trực tuyến như Hacker101, TryHackMe, HackTheBox, Vulnhub, PicoCTF cung cấp các thử thách đa dạng, từ cơ bản đến nâng cao, đáp ứng nhu cầu học tập và rèn luyện kỹ năng của mọi đối tượng. CTF không chỉ là một cuộc thi, mà còn là một cộng đồng nơi các chuyên gia chia sẻ kiến thức, kinh nghiệm và cùng nhau nâng cao trình độ.

1.3. Kali Linux

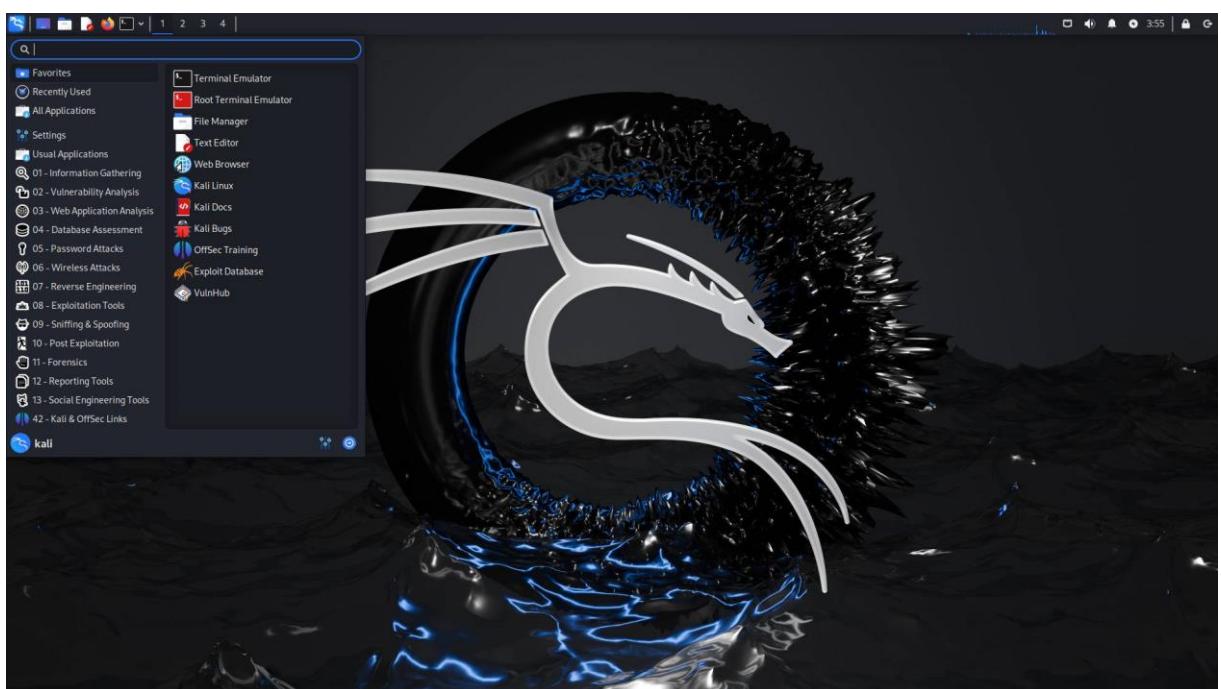
Kali Linux là một bản phân phối Linux mã nguồn mở được phát triển trên nền tảng Debian [16]. Được thiết kế đặc biệt cho các chuyên gia bảo mật, Kali Linux cung cấp một kho công cụ khổng lồ, cấu hình và kịch bản để hỗ trợ các hoạt động kiểm thử thâm nhập và đánh giá bảo mật hệ thống. Với Kali Linux, người dùng có thể thực hiện nhiều tác vụ liên quan đến bảo mật bao gồm pháp y kỹ thuật số và tấn công thăm dò.

BackTrack, tiền thân của Kali Linux, là một bản phân phối Linux được phát triển dựa trên nền tảng Ubuntu, được cộng đồng các nhà nghiên cứu bảo mật đánh giá cao nhờ vào kho công cụ kiểm thử thâm nhập được tích hợp sẵn. Đến năm 2013, Offensive Security, một tổ chức uy tín hàng đầu trong lĩnh vực đào tạo và tư vấn về an ninh mạng, đã chính thức ra mắt Kali Linux dựa trên nền tảng của BackTrack.

Được cộng đồng phát triển và hỗ trợ, Kali Linux nổi bật với khả năng tùy biến cao, cho phép người dùng cấu hình hệ thống một cách linh hoạt để đáp ứng các yêu cầu công việc cụ thể [17]. Một số bộ công cụ được tích hợp vào Kali Linux bao gồm:

- Quét và phân tích hệ thống: Nmap, Nessus,...
- Xâm nhập và khai thác lỗ hổng: Metasploit, Hydra,...
- Kiểm tra bảo mật ứng dụng web: Burp Suite, OWASP ZAP,...
- Phân tích giao thức mạng: Wireshark, Tcpdump,...
- Mật mã học: OpenSSL, GPG,...
- Điều tra số: Autopsy, The Sleuth Kit,...

Kali Linux không chỉ là một công cụ làm việc chuyên nghiệp mà còn là một nền tảng học tập tuyệt vời. Với sự cập nhật liên tục và kho tài nguyên phong phú, Kali Linux giúp người dùng có thể khám phá và nâng cao kiến thức về an ninh mạng. Đặc biệt, Kali Linux đã trở thành một lựa chọn phổ biến nhằm phục vụ cho việc giảng dạy trong các chương trình đào tạo và nghiên cứu về an ninh mạng trên toàn thế giới.



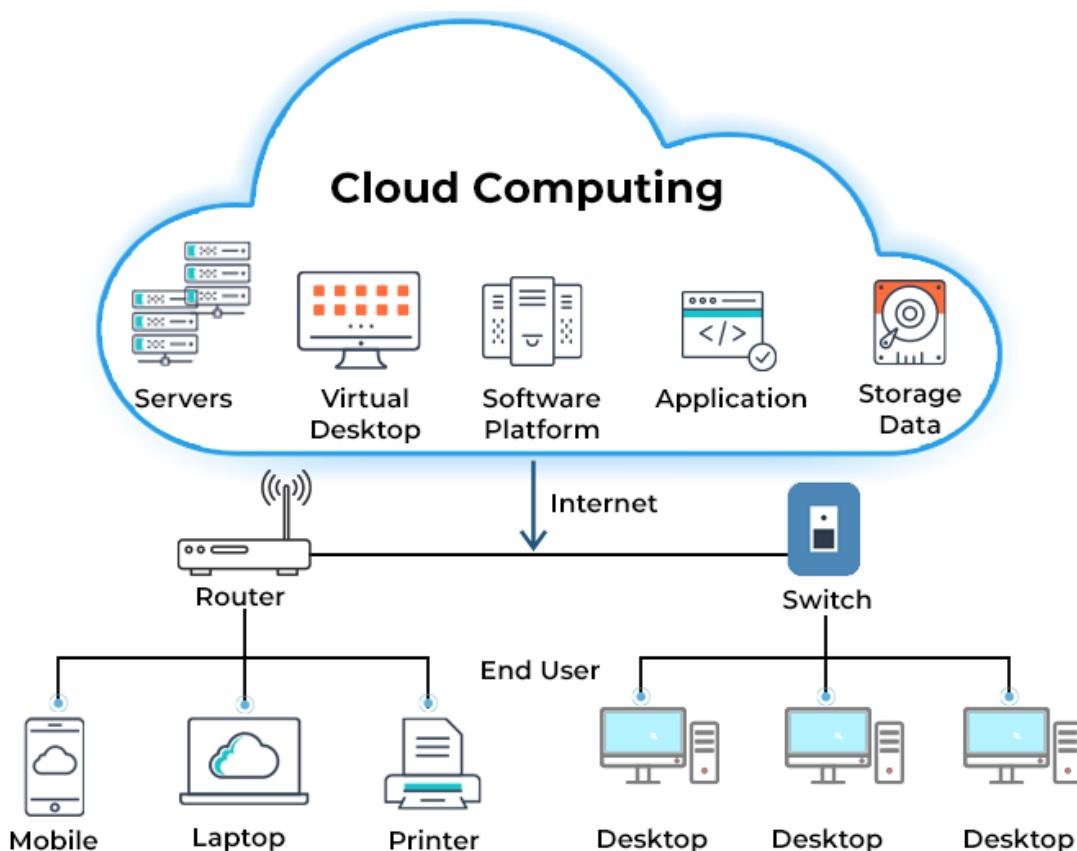
Hình 2: Hệ điều hành Kali Linux. Nguồn: kali.org.

2. Điện toán đám mây

Theo Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ (NIST) [18], điện toán đám mây (hay Cloud Computing) được định nghĩa là: "Mô hình dịch vụ cho phép người dùng truy cập tài nguyên điện toán dùng chung (mạng, server, lưu trữ, ứng dụng, dịch vụ) thông qua kết nối mạng một cách dễ dàng, mọi lúc, mọi nơi, theo yêu cầu. Mô hình đám mây này bao gồm năm đặc điểm thiết yếu, ba mô hình dịch vụ và bốn mô hình triển khai."

Trong đó, năm đặc điểm thiết yếu của điện toán đám mây bao gồm:

- On-demand self-service: Người dùng có thể tự cung cấp các dịch vụ máy tính mà không cần sự tương tác của nhà cung cấp dịch vụ.
- Broad network access: Các dịch vụ có thể được truy cập qua mạng và Internet, từ nhiều loại thiết bị khác nhau và địa điểm khác nhau.
- Resource pooling: Các tài nguyên điện toán được chia sẻ để phục vụ nhiều khách hàng khác nhau, sử dụng một mô hình đa thuê để cung cấp.
- Rapid elasticity: Năng lực máy tính có thể được điều chỉnh nhanh chóng để đáp ứng nhu cầu thay đổi.
- Measured service: Dịch vụ được đo lường, theo dõi, kiểm toán và báo cáo rõ ràng, cho phép cung cấp dịch vụ một cách hiệu quả.

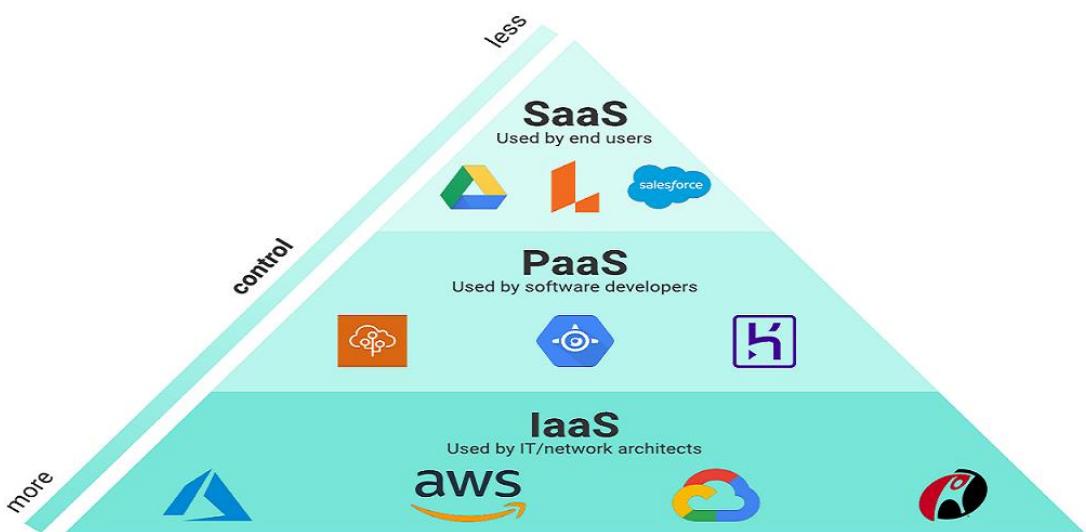


Hình 3: Điện toán đám mây. Nguồn: spiceworks.com.

Các nhà cung cấp dịch vụ điện toán đám mây hiện nay thường cung cấp ba mô hình dịch vụ chính để đáp ứng nhu cầu của khách hàng:

- Cơ sở hạ tầng như một dịch vụ (IaaS): Mô hình này cho phép khách hàng được thuê các tài nguyên hạ tầng cơ bản như máy chủ ảo, lưu trữ, mạng lưới... một cách linh hoạt, tương tự như việc thuê một trung tâm dữ liệu riêng. Ví dụ: Amazon Web Services, Microsoft Azure, Google Cloud Platform,...
- Nền tảng như một dịch vụ (PaaS): Mô hình này cung cấp một nền tảng phát triển hoàn chỉnh, bao gồm hệ điều hành, cơ sở dữ liệu, công cụ phát triển... cho phép khách hàng tập trung vào việc xây dựng và triển khai ứng dụng của mình mà không cần quản lý hạ tầng. Ví dụ: Heroku, Google App Engine,...
- Phần mềm như một dịch vụ (SaaS): Mô hình này cho phép khách hàng truy cập và sử dụng các ứng dụng phần mềm hoàn chỉnh chẳng hạn như phần mềm quản lý khách hàng, phần mềm kế toán... Nhà cung cấp sẽ chịu trách nhiệm quản lý và cập nhật phần mềm. Ví dụ: Google Workspace, Microsoft 365, Salesforce,...

Bên cạnh đó, XaaS (Everything as a Service) là một khái niệm mở rộng từ các mô hình dịch vụ đám mây quen thuộc trên, hiện đang dần trở thành xu hướng toàn cầu. Thay vì chỉ cung cấp cơ sở hạ tầng, nền tảng hoặc ứng dụng, XaaS hướng tới việc cung cấp mọi thứ dưới dạng dịch vụ. Điều này có nghĩa là bất kỳ sản phẩm, dịch vụ, hay thậm chí là trải nghiệm nào cũng có thể được chuyển đổi thành một dịch vụ trực tuyến, được truy cập và sử dụng theo yêu cầu.



Hình 4: Ba mô hình dịch vụ điện toán đám mây. Nguồn: lucidchart.com

Các mô hình triển khai đám mây đều cung cấp những lợi ích và thách thức khác nhau. Việc lựa chọn mô hình phù hợp sẽ ảnh hưởng trực tiếp đến hiệu quả kinh doanh của doanh nghiệp. Có bốn loại mô hình triển khai phổ biến:

- Public Cloud: Public Cloud được xem là mô hình phổ biến nhất, nơi các nhà cung cấp dịch vụ như Amazon Web Services (AWS), Microsoft Azure và Google Cloud Platform cung cấp các tài nguyên điện toán cho nhiều khách hàng khác nhau qua Internet. Với Public Cloud, ta chỉ cần đăng ký tài khoản và trả phí theo lượng tài nguyên sử dụng.
- Private Cloud: Ngược lại với Public Cloud, Private Cloud được xây dựng và quản lý hoàn toàn bởi một tổ chức. Tất cả các tài nguyên đều dành riêng cho tổ chức đó, giúp đảm bảo mức độ bảo mật và kiểm soát cao nhất. Mô hình này phù hợp với các tổ chức có yêu cầu cao về bảo mật dữ liệu.
- Hybrid Cloud: Hybrid Cloud kết hợp cả ưu điểm của Public Cloud và Private Cloud. Các tổ chức có thể triển khai các ứng dụng quan trọng và nhạy cảm trên Private Cloud, đồng thời tận dụng tính linh hoạt và tiết kiệm chi phí của Public Cloud cho các ứng dụng khác. Tuy nhiên, việc quản lý và tích hợp hai môi trường khác nhau có thể phức tạp hơn.
- Community Cloud: Community Cloud được chia sẻ bởi một nhóm các tổ chức có cùng mục tiêu hoặc ngành nghề. Mô hình này giúp giảm chi phí và tăng cường hợp tác giữa các thành viên trong cộng đồng. Tuy nhiên, tính linh hoạt và khả năng mở rộng của Community Cloud thường hạn chế hơn so với Public Cloud và Hybrid Cloud.

Từ việc đơn giản hóa quản lý dữ liệu đến việc thúc đẩy đổi mới sáng tạo, điện toán đám mây đã chứng minh được vai trò không thể thiếu trong kỷ nguyên số. Sự ra đời của các công nghệ mới như trí tuệ nhân tạo, Blockchain khi kết hợp với điện toán đám mây sẽ tạo ra những đột phá đáng kinh ngạc, mở ra những chân trời mới cho lĩnh vực Công nghệ Thông tin.

2.1. Công nghệ ảo hóa

Công nghệ ảo hóa được xem là yếu tố cốt lõi, tạo nên cơ sở hạ tầng của điện toán đám mây. Ảo hóa (Virtualization) [19] là quá trình tạo ra các bản sao ảo của phần cứng vật lý, cho phép chúng ta chạy nhiều hệ điều hành và ứng dụng độc lập trên cùng một máy chủ vật lý nhờ vào hypervisor - phần mềm quản lý và điều phối các máy ảo. Có hai loại hypervisor chính:

- Hypervisor loại 1 (bare-metal hypervisor): Loại hypervisor này được cài đặt trực tiếp lên phần cứng máy chủ, không cần qua một hệ điều hành nào khác. Hypervisor loại 1 thường có hiệu suất cao hơn, độ ổn định tốt hơn và được sử dụng rộng rãi trong các môi trường sản xuất, các trung tâm dữ liệu lớn. Ví dụ: VMware ESXi, Microsoft Hyper-V.
- Hypervisor loại 2 (hosted hypervisor): Loại hypervisor này chạy như một ứng dụng trên một hệ điều hành khác ví dụ như Windows, Linux. Hypervisor loại 2 thường dễ cài đặt và sử dụng hơn, phù hợp với các môi trường nhỏ, các máy tính cá nhân hoặc phục vụ cho các mục đích thử nghiệm. Ví dụ: VirtualBox, VMware Workstation.

Máy chủ vật lý thường sẽ phải đối mặt với các vấn đề bao gồm yêu cầu về điện năng, không gian và yêu cầu bảo trì thường xuyên. Thay vì phải đầu tư vào nhiều máy chủ vật lý, công nghệ ảo hóa sẽ giúp doanh nghiệp giải quyết các vấn đề trên bằng cách tạo ra nhiều máy ảo trên cùng một máy chủ.

Máy ảo (VM) là một trình giả lập một hệ thống máy tính, dựa trên kiến trúc máy tính và cung cấp chức năng của máy tính vật lý. Việc triển khai của chúng có thể liên quan đến phần cứng, phần mềm chuyên dụng hoặc kết hợp [20]. Có nhiều loại máy ảo khác nhau, mỗi loại có chức năng khác nhau:

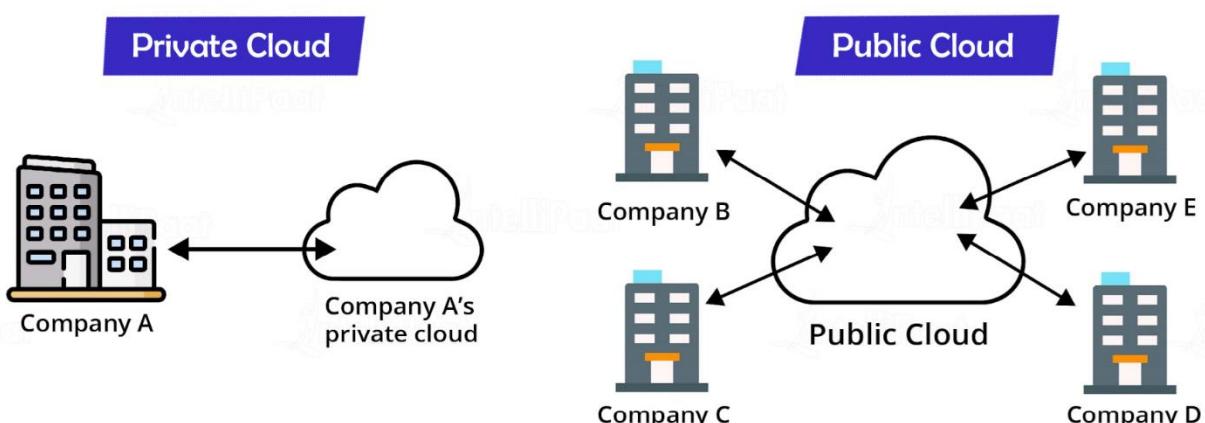
- Máy ảo hệ thống (ảo hóa hoàn toàn) cung cấp một môi trường thay thế cho máy thật với đầy đủ các chức năng cần thiết để thực thi toàn bộ hệ điều hành. Một trình ảo hóa sẽ được thực thi nhằm chia sẻ và quản lý phần cứng, cho phép nhiều máy ảo được cách ly với nhau, nhưng vẫn tồn tại trên cùng một máy vật lý.
- Máy ảo tiến trình được thiết kế để thực thi các chương trình máy tính cho phép các ứng dụng được thực thi một cách nhất quán trên nhiều nền tảng khác nhau. Bằng cách cung cấp một lớp trùu tượng giữa ứng dụng và hệ điều hành, máy ảo tiến trình đảm bảo tính di động và tăng cường bảo mật cho ứng dụng. Ví dụ như máy ảo Java và .NET Common Language Runtime.

2.2. Private Cloud

Private Cloud [21] là một môi trường điện toán đám mây được xây dựng và vận hành riêng biệt cho một tổ chức. Mô hình triển khai này bắt nguồn từ nhu cầu về một môi trường điện toán đám mây an toàn và riêng tư hơn, xuất hiện vào khoảng giữa những năm 2000. Trước những lo ngại về bảo mật dữ liệu, khả năng kiểm soát và hiệu suất của Public Cloud, các tổ chức đã tìm kiếm một giải pháp thay thế. Từ đó Private Cloud ra đời, kết hợp những ưu điểm của Public Cloud như tự động hóa và tự phục vụ, nhưng lại được xây dựng và quản lý hoàn toàn trong môi trường riêng biệt của tổ chức. Qua thời gian, công nghệ Private Cloud không ngừng phát triển, đáp ứng ngày càng tốt hơn các nhu cầu đa dạng của doanh nghiệp, từ các công ty vừa và nhỏ đến các tập đoàn lớn.

Mô hình này có thể được triển khai trên cơ sở hạ tầng vật lý tại trung tâm dữ liệu của tổ chức hoặc được thuê ngoài từ các nhà cung cấp dịch vụ đám mây. Dù được triển khai ở đâu, Private Cloud luôn đảm bảo rằng tài nguyên phần cứng, phần mềm và mạng lưới đều được dành riêng cho một tổ chức duy nhất, giúp tăng cường bảo mật và kiểm soát. Cơ sở hạ tầng Private Cloud thường là một hệ thống phức hợp bao gồm phần cứng, phần mềm ảo hóa và cơ sở hạ tầng mạng:

- Phần cứng là nền tảng vật lý của Private Cloud, bao gồm các máy chủ, thiết bị lưu trữ và thiết bị mạng. Các máy chủ này được cấu hình để chạy nhiều máy ảo, mỗi máy ảo hoạt động như một máy tính độc lập.
- Phần mềm ảo hóa đóng vai trò quan trọng trong việc quản lý và điều phối các tài nguyên phần cứng. Các phần mềm như Hyper-V, VMware hay OpenStack cho phép tạo ra và quản lý các máy ảo một cách hiệu quả.
- Cơ sở hạ tầng mạng kết nối các thành phần của Private Cloud và đảm bảo dữ liệu được truyền tải an toàn và hiệu quả. Mạng lưới này có thể bao gồm các switch, router và các thiết bị mạng khác, tùy thuộc vào quy mô và cấu trúc của đám mây.

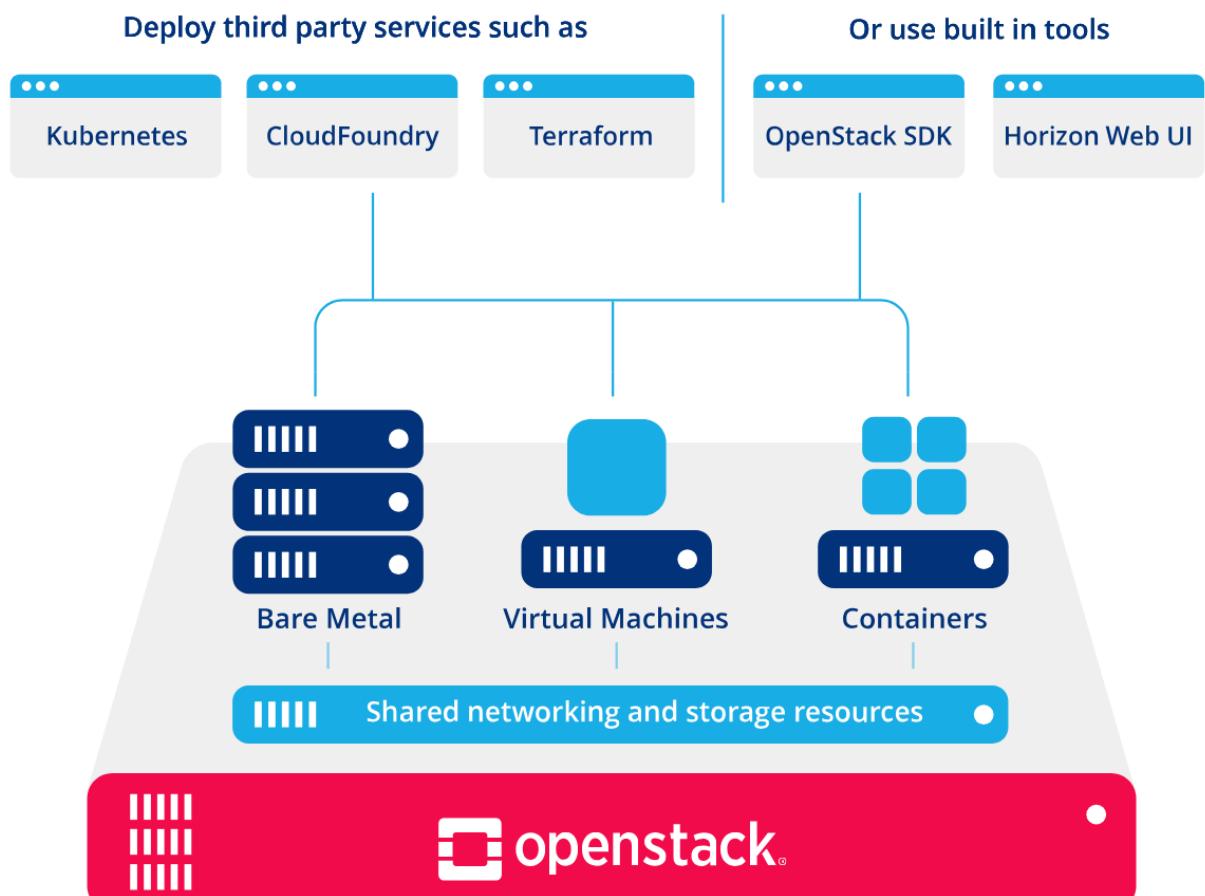


Hình 5: Public Cloud và Private Cloud. Nguồn: cloud.z.com

2.3. OpenStack

OpenStack [22] là một nền tảng phần mềm tự do nguồn mở Điện toán đám mây, thường được thiết kế để triển khai cơ sở hạ tầng như một dịch vụ (IaaS). OpenStack cho phép người dùng tự chủ quản lý các tài nguyên máy tính, lưu trữ và mạng trong trung tâm dữ liệu của mình. Thông qua một bảng điều khiển dựa trên web, các công cụ dòng lệnh, hoặc thông qua một API RESTful, người dùng có thể tạo, cấu hình và quản lý các máy ảo, mạng ảo và khối lượng lưu trữ một cách trực quan và hiệu quả.

Ra đời vào năm 2010, OpenStack là một dự án hợp tác giữa Rackspace Hosting và NASA. Mục tiêu ban đầu của dự án là xây dựng một nền tảng điện toán đám mây mã nguồn mở, linh hoạt và mở rộng được. Đến năm 2015, dự án này đã được chuyển giao cho OpenStack Foundation, một tổ chức phi lợi nhuận được thành lập vào năm 2012 với sứ mệnh phát triển và hỗ trợ cộng đồng OpenStack. Với sự tham gia của hơn 500 công ty công nghệ hàng đầu thế giới như AT&T, IBM, Google, và Red Hat, OpenStack đã trở thành một trong những nền tảng đám mây mã nguồn mở phổ biến nhất.

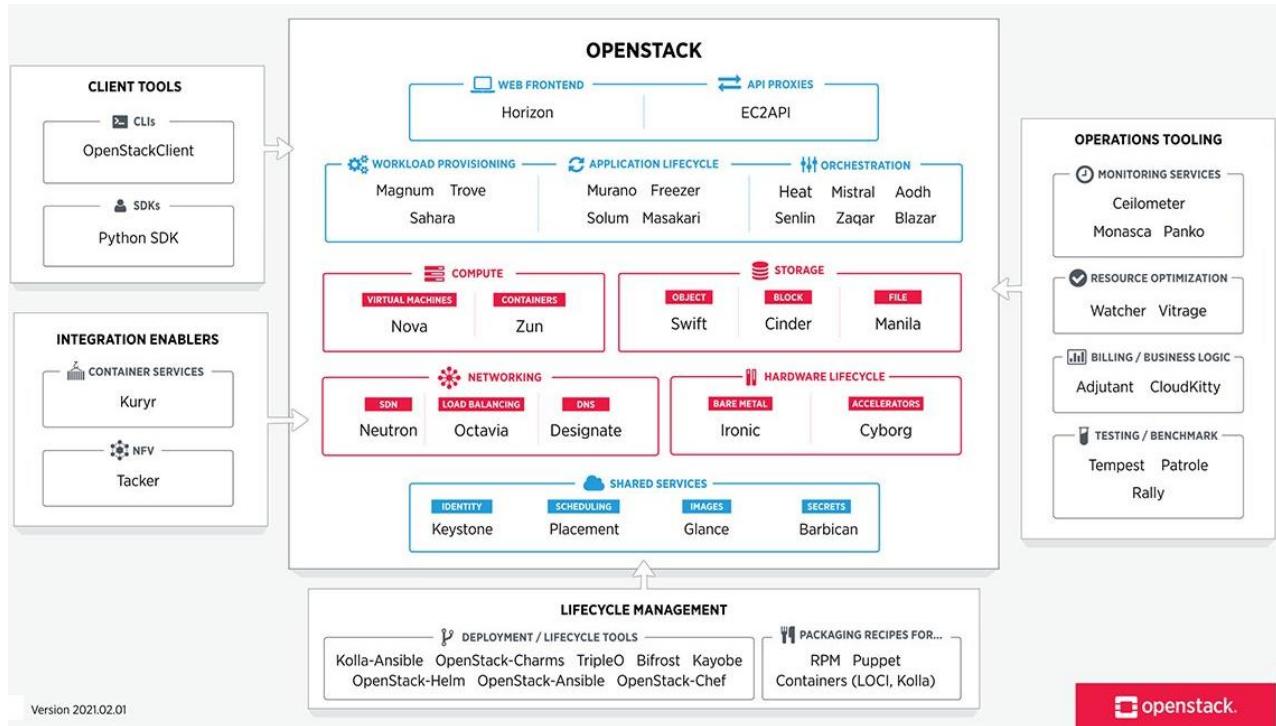


Hình 6: Nền tảng OpenStack. Nguồn: openstack.org

OpenStack bao gồm nhiều thành phần dịch vụ, mỗi dịch vụ đóng một vai trò quan trọng trong việc cung cấp các chức năng cốt lõi của một nền tảng Điện toán đám mây. Dưới đây là một số thành phần chính:

- Nova: Dịch vụ tính toán (Compute Service), chịu trách nhiệm quản lý vòng đời của các máy ảo (instance), từ việc tạo mới, khởi động, dừng, khởi động lại, đến xóa bỏ. Nova cung cấp các tài nguyên tính toán như CPU, RAM, và dung lượng ổ đĩa cứng cho các máy ảo. Dịch vụ này được sử dụng để triển khai các ứng dụng, dịch vụ, hoặc nền tảng khác nhau trên đám mây OpenStack.
- Glance: Dịch vụ hình ảnh (Image Service), lưu trữ và quản lý các hình ảnh hệ điều hành và ứng dụng. Glance cung cấp một kho lưu trữ tập trung cho các hình ảnh, cho phép các dự án chia sẻ và tái sử dụng hình ảnh, có thể triển khai nhanh chóng các máy ảo mới. Dịch vụ này được sử dụng để tạo và quản lý các hình ảnh hệ điều hành, ứng dụng, và các bản sao (snapshot) của máy ảo.
- Neutron: Dịch vụ mạng (Networking), cung cấp các chức năng mạng ảo, bao gồm việc tạo ra các mạng riêng biệt, mạng con (subnet), router, và các thiết bị mạng ảo khác. Neutron cho phép các máy ảo kết nối với nhau và kết nối các máy ảo với thế giới bên ngoài. Dịch vụ này được sử dụng để cấu hình mạng cho các ứng dụng và dịch vụ trên đám mây OpenStack.
- Cinder: Dịch vụ lưu trữ khối (Block Storage), cung cấp các khối lưu trữ ảo cho các máy ảo, tương tự như các ổ đĩa cứng vật lý. Cinder cho phép tăng dung lượng lưu trữ cho các máy ảo và tạo các bản sao của khối lưu trữ. Dịch vụ này được sử dụng để cung cấp dung lượng lưu trữ cho các cơ sở dữ liệu, hệ thống file, và các ứng dụng khác.
- Swift (Object Store): Dịch vụ lưu trữ đối tượng, cung cấp một không gian lưu trữ phân tán và bền vững để lưu trữ các file lớn. Swift được sử dụng để lưu trữ các dữ liệu không cấu trúc, chẳng hạn như hình ảnh, video, và các file backup. Dịch vụ này được sử dụng để xây dựng các ứng dụng lưu trữ đám mây, các hệ thống quản lý nội dung, và các dịch vụ lưu trữ backup.
- Keystone (Identity Service): Dịch vụ quản lý danh tính người dùng, nhóm, và các dự án. Keystone cung cấp các dịch vụ xác thực và ủy quyền, đảm bảo an toàn cho hệ thống OpenStack. Dịch vụ này được sử dụng để quản lý quyền truy cập vào các tài nguyên OpenStack và đảm bảo an toàn cho hệ thống.
- Horizon (Dashboard): Bảng điều khiển web cung cấp một giao diện trực quan để quản lý các tài nguyên OpenStack. Horizon cho phép người dùng tạo, sửa đổi, và xóa các máy ảo, mạng, khối lưu trữ, và các đối tượng khác.

OpenStack hoạt động trên một hệ điều hành cơ bản (thường là Linux) và sử dụng một hypervisor để quản lý các tài nguyên phần cứng ảo. Các thành phần của OpenStack sẽ làm việc cùng nhau thông qua các API để cung cấp các dịch vụ đám mây.

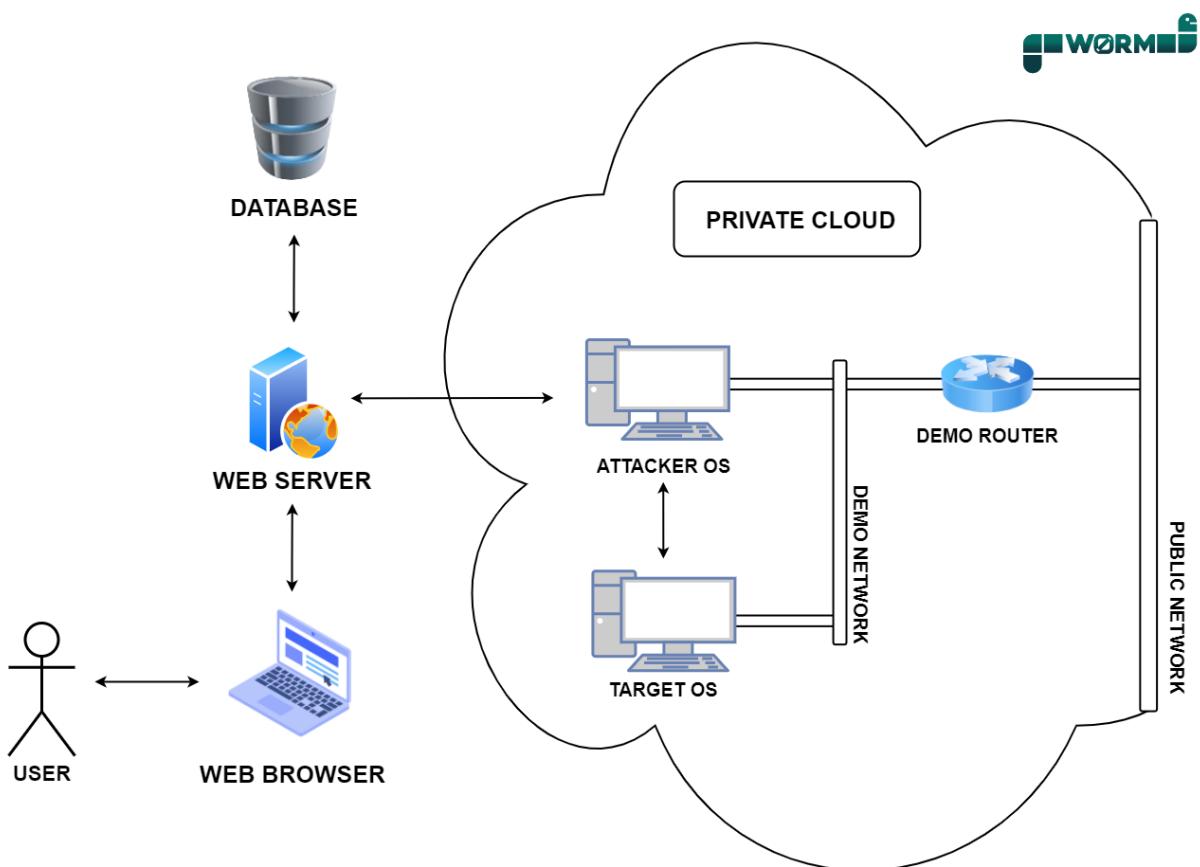


Hình 7: Các dịch vụ của OpenStack. Nguồn: openstack.org

CHƯƠNG 3: THIẾT KẾ GIẢI PHÁP

1. Thiết kế sơ đồ hệ thống

Mục tiêu chính của đề tài là xây dựng một ứng dụng web phục vụ cho việc thực tập kiểm thử bảo mật, dựa trên công nghệ điện toán đám mây. Các bài tập thực hành sẽ được triển khai thông qua tài nguyên điện toán trên một nền tảng Private Cloud tự xây dựng, bao gồm những cặp máy ảo tấn công và máy ảo mục tiêu. Ứng dụng web sẽ kết nối đến màn hình điều khiển máy ảo tấn công, từ đó người dùng có thể xâm nhập hệ thống máy ảo mục tiêu. Ý tưởng cho sơ đồ hệ thống của đề tài sẽ được thể hiện ở Hình 8.



Hình 8: Ý tưởng cho sơ đồ hệ thống.

Do phạm vi thực hiện đề tài nghiên cứu nằm bên trong Trường Đại học Cần Thơ, nhóm đề xuất việc tận dụng tối đa hệ thống máy chủ sẵn có của nhà trường. Điều này không chỉ giúp tiết kiệm chi phí đáng kể so với việc thuê tài nguyên từ các nhà cung cấp dịch vụ điện toán đám mây, mà còn đảm bảo tính bảo mật cao cho đề tài nghiên cứu. Vì vậy, mô hình Private Cloud sẽ được lựa chọn để triển khai nền tảng điện toán đám mây cho đề tài, nhằm đáp ứng nhu cầu tính toán và lưu trữ dữ liệu một cách an toàn và hiệu quả. Một số nền tảng Private Cloud phổ biến bao gồm: OpenStack, VMware vSphere, Microsoft Azure Stack, Red Hat OpenShift,...

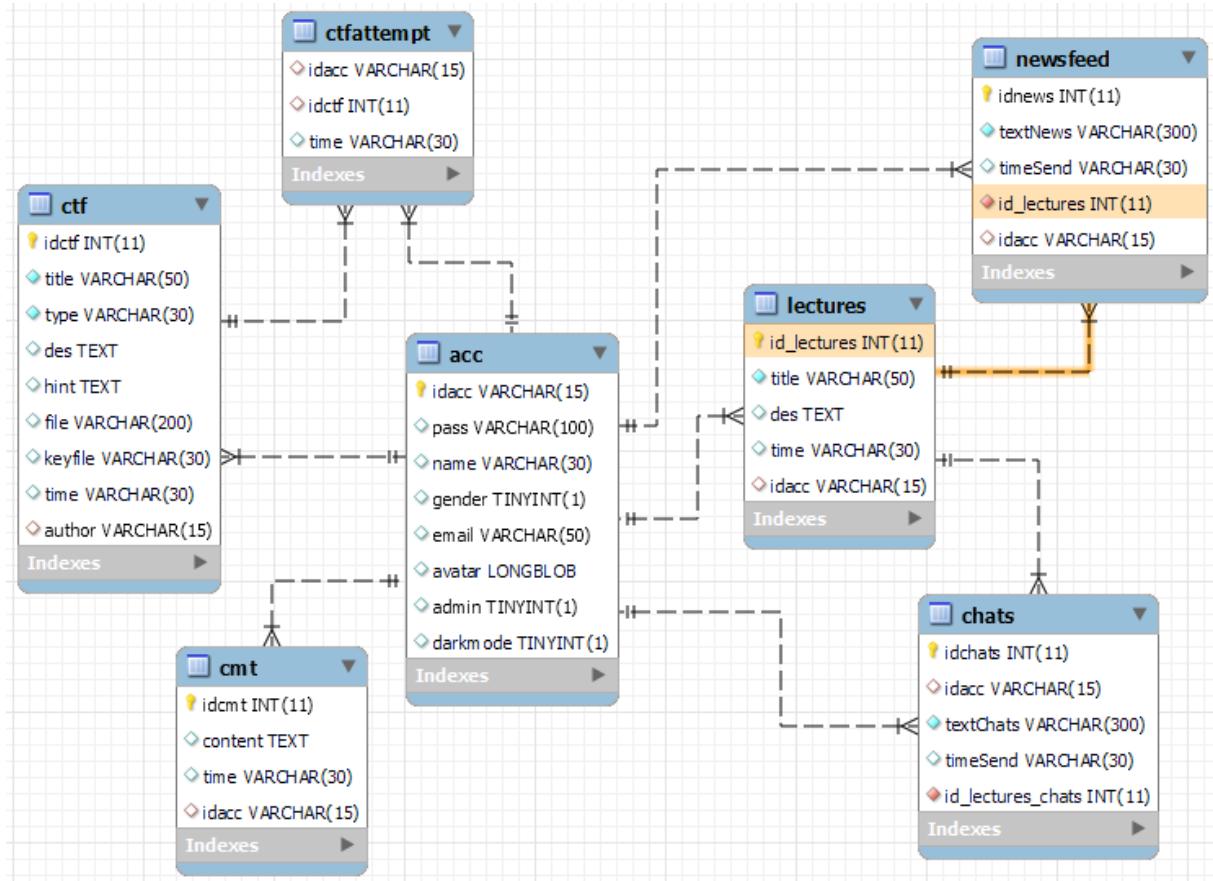
Đối với các bài tập thực hành kiểm thử bảo mật, đề tài sẽ tiến hành tính toán và phân chia mạng, sao cho mỗi bài tập sẽ được xây dựng trên một nhánh mạng độc lập. Mỗi bài tập sẽ bao gồm một máy ảo tấn công và máy ảo mục tiêu. Hiện nay, một số hệ điều hành đã được thiết kế tập trung cho bảo mật và kiểm thử xâm nhập, có thể kể đến: Kali Linux, Parrot Security OS, BlackArch Linux,... Đó là những hệ điều hành rất phù hợp cho việc xây dựng máy ảo tấn công. Về máy ảo mục tiêu, đề tài sẽ hướng đến việc sử dụng các hệ điều hành gọn nhẹ, ít tốn tài nguyên và có thể sở hữu nhiều lỗ hổng bảo mật như Metasploitable 2 và CirrOS.

2. Thiết kế cơ sở dữ liệu cho ứng dụng web

Không chỉ đóng vai trò là môi trường thực tập kiểm thử bảo mật, ứng dụng web còn sẽ được tích hợp thêm các bài giảng và các thử thách CTF, với mục tiêu cung cấp đầy đủ kiến thức và kỹ năng liên quan đến lĩnh vực An toàn thông tin. Đề tài sẽ tập trung vào việc xây dựng các trang web động, nơi mà dữ liệu được lưu trữ và quản lý trong một hệ quản trị cơ sở dữ liệu quan hệ (Relational Database Management System - RDBMS). Cơ sở dữ liệu sẽ được thiết kế với các bảng như sau:

- Thông tin người dùng (acc): Bảng này chứa các thông tin có trong tài khoản bao gồm tên đăng nhập, mật khẩu, họ và tên người dùng, giới tính, địa chỉ email và quyền quản trị. Bên cạnh đó, bảng còn lưu thông tin cài đặt theo yêu cầu của mỗi người dùng như ảnh đại diện và chế độ sáng/tối.
- Thử thách CTF (ctf): Bao gồm các thông tin của mỗi thử thách CTF được tạo. Bao gồm mã số thử thách (id), tiêu đề, thể loại, mô tả, gợi ý, tệp đính kèm, đáp án, tác giả và thời gian tạo. Một tác giả (Admin) có thể tạo ra nhiều thử thách.
- Lượt tham gia thử thách (ctfattempt): Lưu thông tin sau khi một người dùng hoàn thành một thử thách CTF tại một thời điểm nhất định. Một người dùng có thể tham gia nhiều thử thách CTF, và ngược lại một thử thách CTF có thể được nhiều người tham gia.
- Lớp học lý thuyết (lectures): Bao gồm các thông tin cơ bản của mỗi lớp học lý thuyết như mã số lớp học (id), tên lớp học, nội dung mô tả, thời gian tạo ra lớp học và tên người đứng lớp (Admin). Một Admin có thể quản lý nhiều lớp học.
- Tin tức (newfeeds): Mỗi lớp học sẽ có một bảng tin với các tin tức được cập nhật. Bảng này gồm các thông tin của mỗi tin tức như mã số tin tức (id), nội dung, thời gian đăng tin, tên tác giả và thuộc bảng tin của lớp học nào. Mỗi lớp học có nhiều tin tức và mỗi Admin có thể đăng nhiều tin khác nhau.

- Tin nhắn (chats): Mỗi lớp học sẽ sở hữu một box chat tạo điều kiện cho người dùng có khả năng chia sẻ với nhau. Mỗi box chat sẽ chứa các tin nhắn do người dùng đã gửi và mỗi người dùng có thể gửi nhiều tin nhắn. Bảng này sẽ lưu các thông tin của các tin nhắn bao gồm mã số tin nhắn (id), tên người gửi, nội dung, thời gian gửi và tin nhắn thuộc lớp học nào.
- Góp ý (cmt): Bảng này sẽ lưu lại thông tin của các góp ý đến từ người dùng, bao gồm mã số góp ý (id), nội dung, thời gian gửi và tác giả. Mỗi người dùng có thể gửi nhiều góp ý khác nhau, góp phần hoàn thiện ứng dụng web.



Hình 9: Mô hình EER của cơ sở dữ liệu.

Đối với các bài tập kiểm thử bảo mật, hiện nay do nhóm chưa sở hữu một máy chủ (server) thực sự đáp ứng đủ yêu cầu tài nguyên, nên đề tài chỉ hướng đến việc xây dựng một cặp máy ảo với mục đích thử nghiệm. Chính vì thế, đối với cơ sở dữ liệu, đề tài sẽ không thiết kế các bảng dành cho những bài tập thực hành kiểm thử bảo mật.

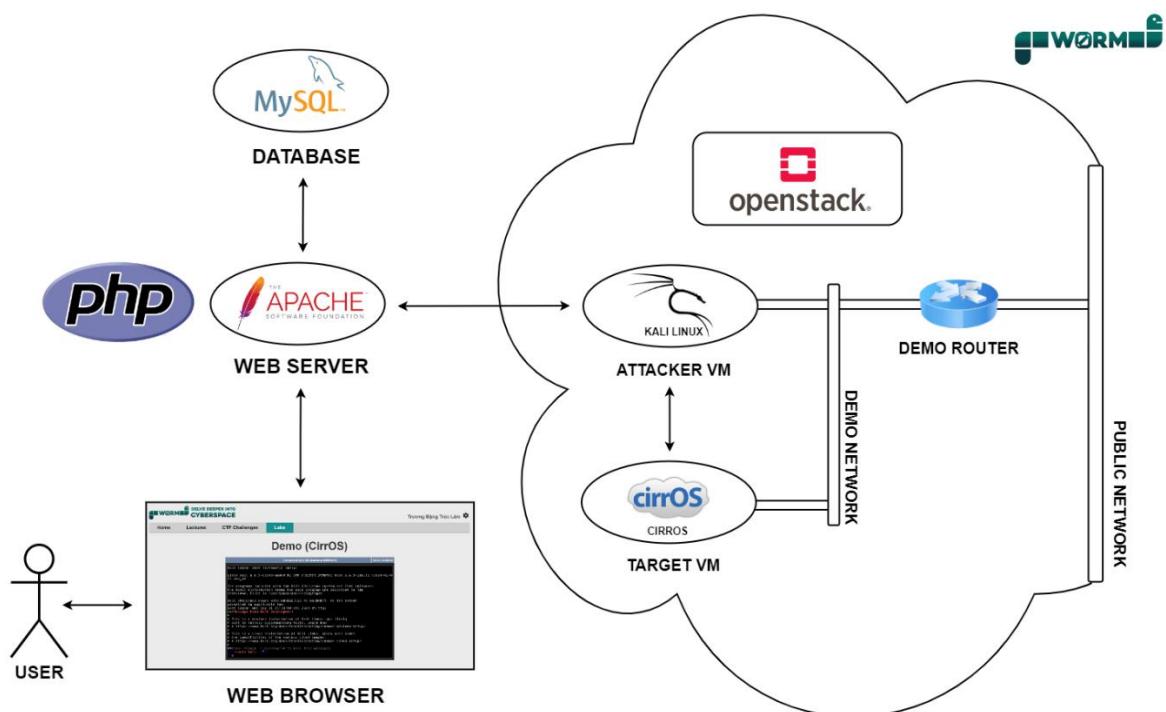
CHƯƠNG 4: CÀI ĐẶT GIẢI PHÁP

Sau thời gian nghiên cứu, nhóm quyết định lựa chọn nền tảng OpenStack cho việc triển khai mô hình Private Cloud. OpenStack là một nền tảng điện toán đám mây mã nguồn mở thường xuyên được phát triển và cập nhật, cung cấp một loạt các dịch vụ cốt lõi bao gồm Compute (tính toán), Storage (lưu trữ), Networking (mạng), và Identity Service (danh tính). Nhờ đó, tổ chức sở hữu có thể tự chủ trong việc quản lý hạ tầng đám mây, đảm bảo tính bảo mật và tuân thủ các quy định, đồng thời tối ưu hóa chi phí vận hành.

Môi trường OpenStack còn tích hợp sẵn Image của CirrOS, một hệ điều hành Linux rất nhẹ, được thiết kế đặc biệt cho các môi trường ảo hóa, rất thích hợp cho việc xây dựng máy ảo mục tiêu. Về máy ảo tấn công, nhóm quyết định sử dụng hệ điều hành Kali Linux, hệ điều hành này luôn là lựa chọn hàng đầu khi nhắc đến lĩnh vực An toàn thông tin. Do hạn chế về mặt tài nguyên, đề tài chỉ thực hiện xây dựng một máy ảo tấn công Kali Linux và một máy ảo mục tiêu CirrOS trên một bài tập thử nghiệm.

Để ứng dụng thực tế các lợi ích mà nền tảng OpenStack mang lại, nhóm sẽ xây dựng một ứng dụng web PHP [23] kết hợp với hệ quản trị cơ sở dữ liệu MySQL [24] và máy chủ web Apache [25]. Ứng dụng web sẽ tương tác với cơ sở hạ tầng đám mây thông qua các API của nền tảng OpenStack, sơ đồ hệ thống của đề tài sẽ được thể hiện ở Hình 10. Để tối ưu hóa quá trình phát triển và quản lý dự án, nhóm chia dự án thành ba giai đoạn:

- Xây dựng nền tảng OpenStack.
- Xây dựng bài tập thực hành kiểm thử bảo mật.
- Xây dựng ứng dụng web.



Hình 10: Sơ đồ hệ thống của đề tài.

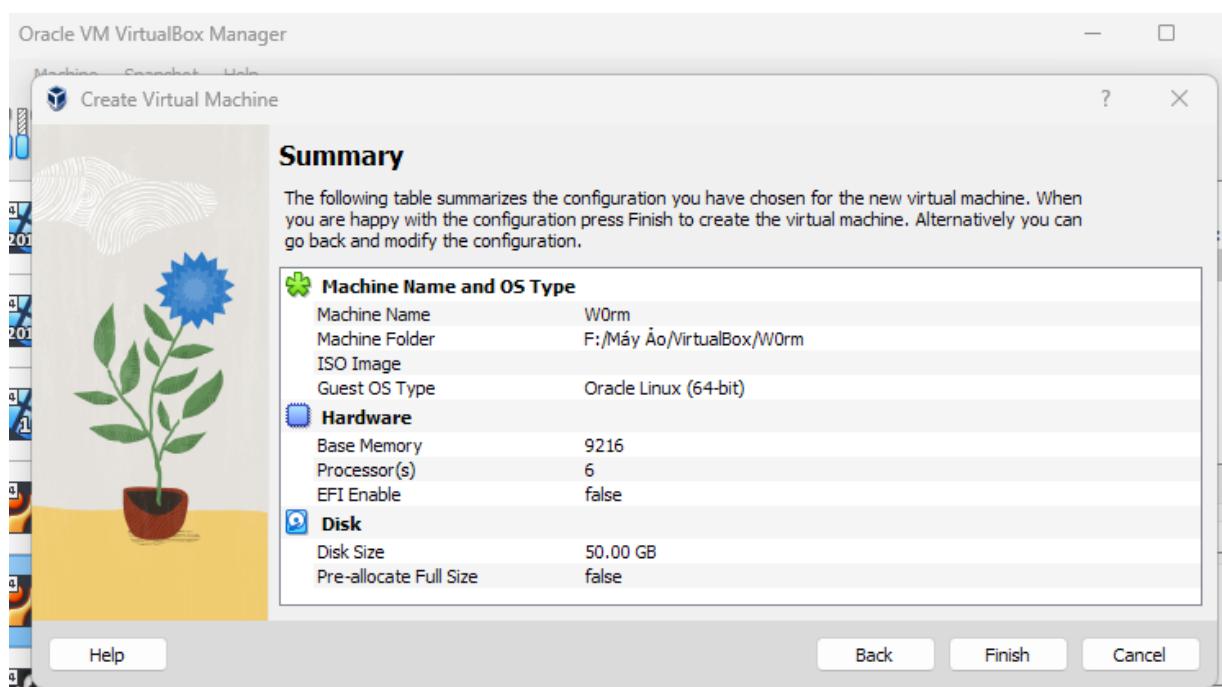
1. Xây dựng nền tảng OpenStack

Đầu tiên, việc triển khai một nền tảng OpenStack hoàn chỉnh sẽ phải đối mặt với nhiều thử thách, đòi hỏi các kiến thức chuyên sâu. Được biết, DevStack [26] là một bộ công cụ tự động hóa mạnh mẽ, gồm các tập lệnh (scripts) và tiện ích (utilities) cho phép người dùng nhanh chóng triển khai một môi trường OpenStack đơn giản hơn, phục vụ cho quá trình nghiên cứu, phát triển và kiểm thử. Chính vì thế, nhóm nghiên cứu quyết định sẽ xây dựng môi trường OpenStack trên một máy chủ ảo Ubuntu Server [27] thông qua bộ công cụ DevStack.

1.1. Cài đặt Ubuntu Server

Thay vì triển khai một mô hình Private Cloud thực tế với các yêu cầu phức tạp, nhóm nghiên cứu sẽ tiến hành cài đặt nền tảng OpenStack lên hệ điều hành Ubuntu Server thông qua phần mềm ảo hoá VirtualBox [28], với mục đích thử nghiệm. Việc xây dựng một máy chủ triển khai môi trường OpenStack sẽ yêu cầu cấu hình tối thiểu như sau:

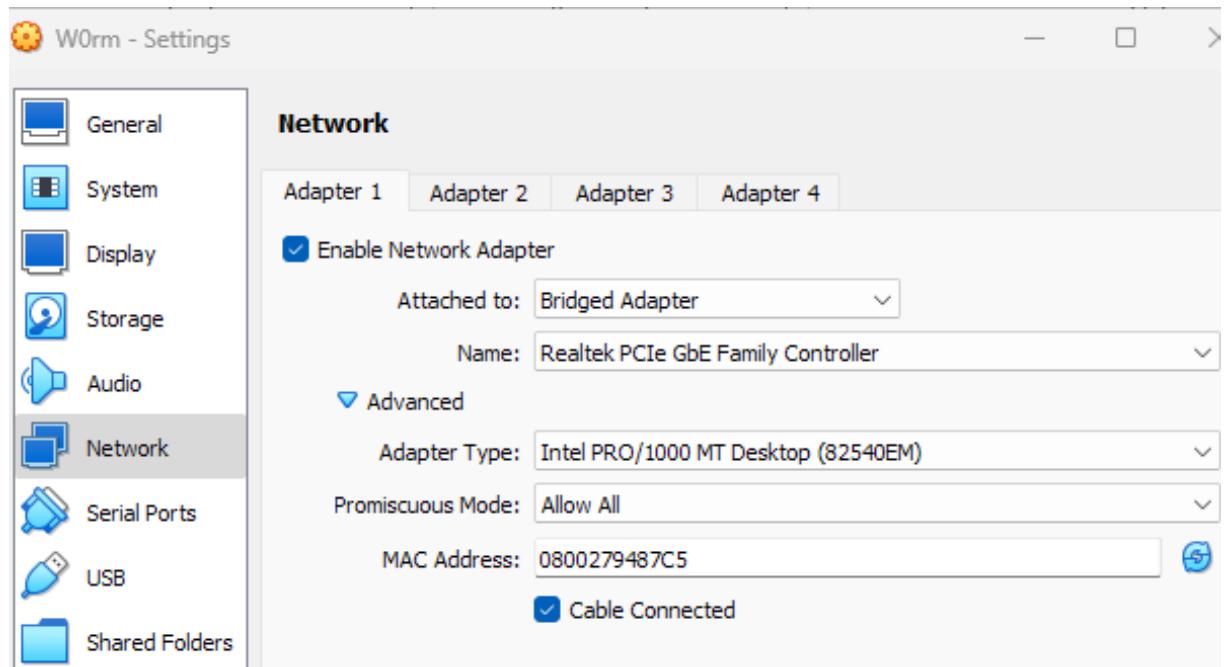
- Memory: 9G
- Processors: 6 CPUs
- Hard Disk: 50G



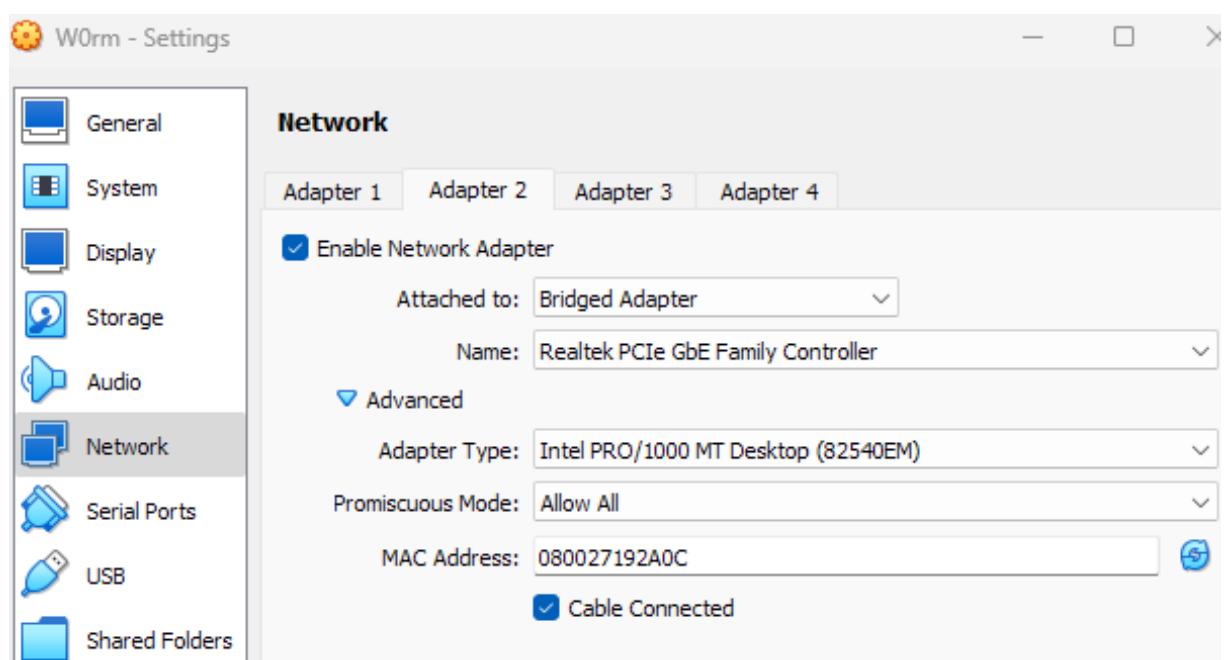
Hình 11: Cấu hình phần cứng đề xuất cho Ubuntu Server.

OpenStack sử dụng các mạng ảo để kết nối những máy ảo với nhau và kết nối đến thế giới bên ngoài. Chế độ Promiscuous Mode cho phép các hypervisor trên máy chủ OpenStack giám sát và điều khiển tất cả lưu lượng truy cập đi qua card mạng. Nhờ đó, hypervisor có thể tạo ra các mạng ảo, phân phối địa chỉ IP, thực hiện routing và các chức năng mạng khác cho các máy ảo.

Đối với cấu hình mạng, ta truy cập vào Network và thiết lập hai card mạng cho máy ảo. Cả hai card mạng đều chọn Attached to: Bridged Adapter. Bên cạnh đó, truy cập mục Advanced và chọn Promiscuous Mode: Allow All.



Hình 12: Cấu hình card mạng thứ nhất.



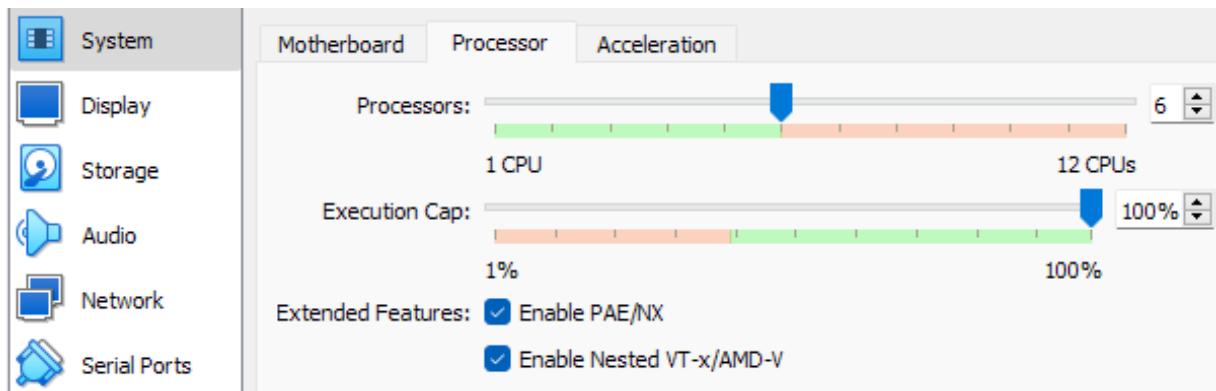
Hình 13: Cấu hình card mạng thứ hai.

Sử dụng các tính năng PAE/NX và Nested VT-x/AMD-v sẽ giúp tối ưu hóa việc sử dụng tài nguyên, đảm bảo hiệu suất, bảo mật và khả năng tương thích của môi trường ảo hóa. Ở mục System, ta truy cập thẻ Processor và đánh dấu vào các ô tuỳ chọn:

- Enable PAE/NX.
- Enable Nested VT-x/AMD-v.

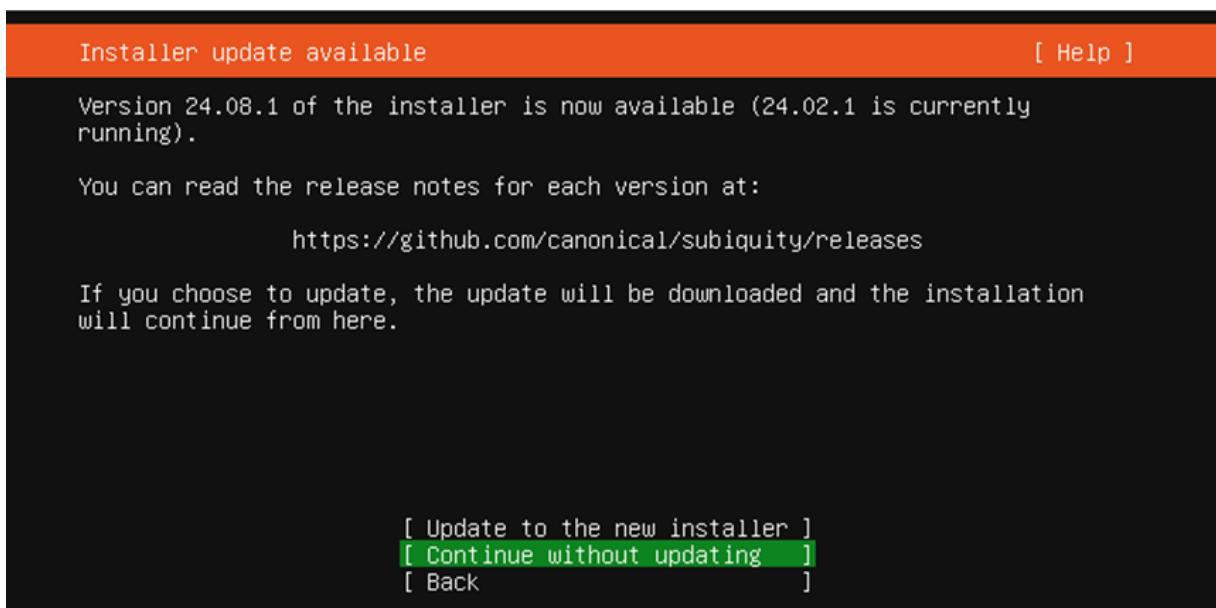
Trong trường hợp các ô tuỳ chọn không khả dụng, ta có thể truy cập thư mục cài đặt phần mềm VirtualBox, mở CMD (Command Prompt) và thực thi câu lệnh:

```
$ VBoxManage modifyvm "vm name" --nested-hw-virt on
```

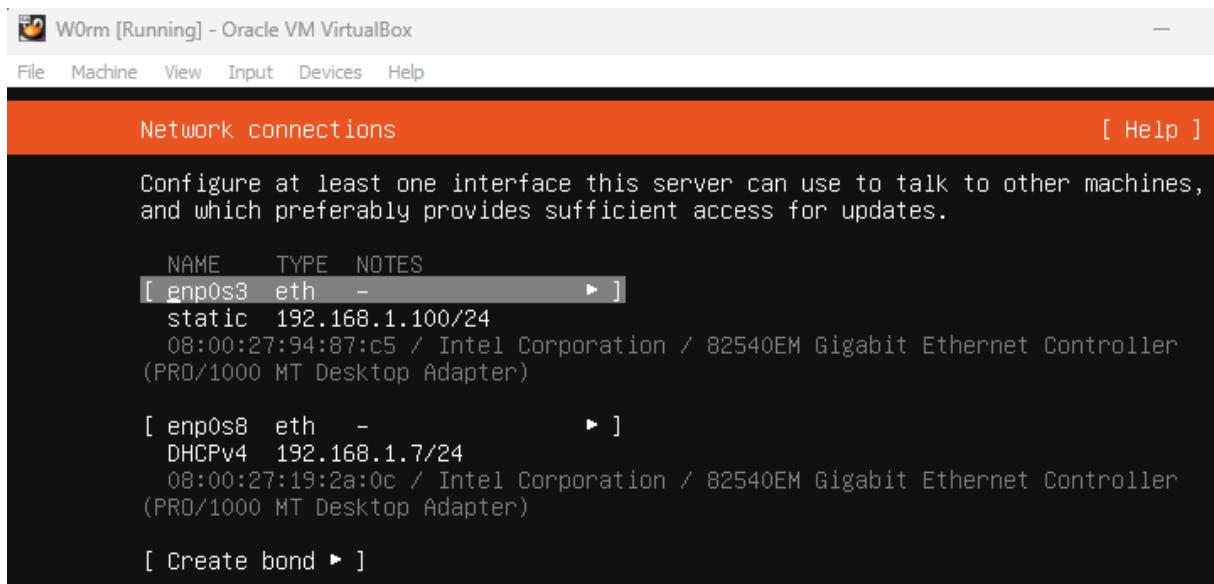


Hình 14: Cấu hình hệ thống.

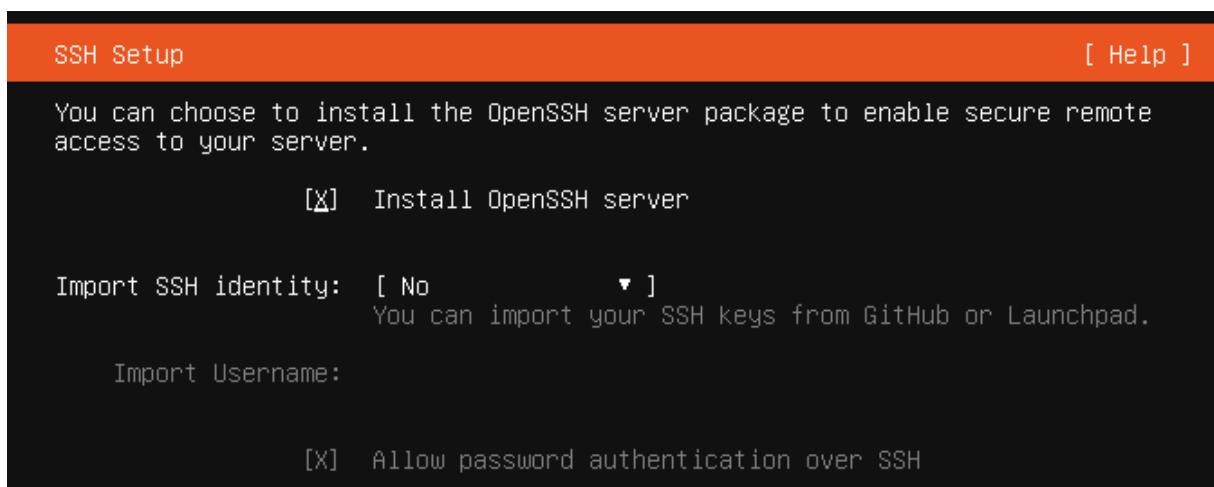
Ở thời điểm hiện tại, nền tảng OpenStack chỉ hỗ trợ đến phiên bản 22.04 LTS của Ubuntu, các phiên bản mới hơn của Ubuntu có thể sẽ được OpenStack hỗ trợ trong tương lai. Chính vì thế, tại thời điểm thực hiện nghiên cứu, nhóm sẽ cài đặt hệ điều hành Ubuntu server 22.04 LTS.



Hình 15: Cài đặt hệ điều hành Ubuntu Server.



Hình 16: Cấu hình mạng cho hệ điều hành Ubuntu Server.



Hình 17: Cài đặt dịch vụ SSH cho Ubuntu Server.

```
w0rm login: b2111933
Password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

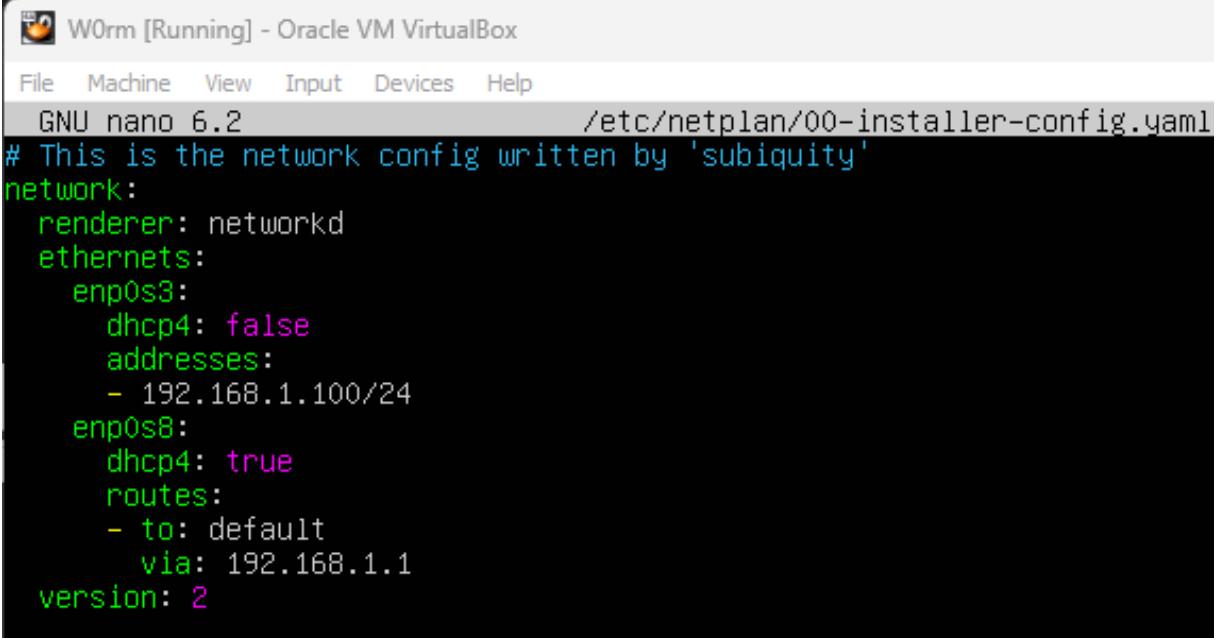
System information as of Sun Sep  8 03:27:55 AM UTC 2024

System load:          1.3759765625
Usage of /:            29.6% of 23.45GB
Memory usage:         2%
Swap usage:           0%
Processes:            152
Users logged in:      0
```

Hình 18: Cài đặt hoàn tất hệ điều hành Ubuntu Server.

Qua quá trình nghiên cứu, nhóm nhận thấy các phương thức cấu hình mạng mặc định của Ubuntu Server (Hình 16) đều sẽ phát sinh một số lỗi ở những lần khởi động lại máy chủ trong tương lai. Chính vì thế, ta cần tiến hành cấu hình mạng thủ công cho Ubuntu Server thông qua tập tin /etc/netplan/00-installer-config.yaml:

```
$ sudo apt update && sudo apt upgrade -y  
$ sudo apt install openvswitch-switch-dpdk  
$ sudo nano etc/netplan/*  
  
# This is the network config written by 'subiquity'  
network:  
    renderer: networkd  
    ethernets:  
        enp0s3:  
            dhcp4: false  
            addresses:  
                - <IP Address/Subnet Mask>  
        enp0s8:  
            dhcp4: true  
            routes:  
                - to: default  
                  via: <Gateway Address>  
version: 2
```

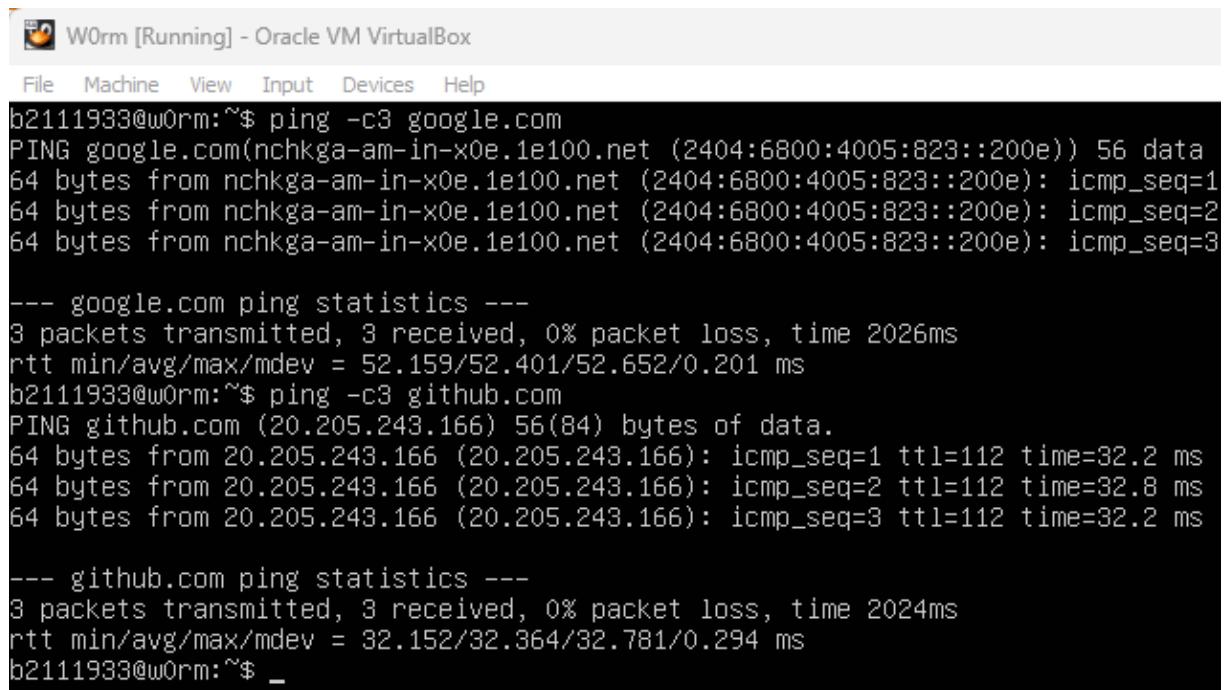


```
File Machine View Input Devices Help  
GNU nano 6.2 /etc/netplan/00-installer-config.yaml  
# This is the network config written by 'subiquity'  
network:  
    renderer: networkd  
    ethernets:  
        enp0s3:  
            dhcp4: false  
            addresses:  
                - 192.168.1.100/24  
        enp0s8:  
            dhcp4: true  
            routes:  
                - to: default  
                  via: 192.168.1.1  
version: 2
```

Hình 19: Cấu hình mạng thủ công cho Ubuntu Server.

```
$ sudo netplan apply
```

Khởi động lại máy ảo và kiểm tra kết nối mạng.



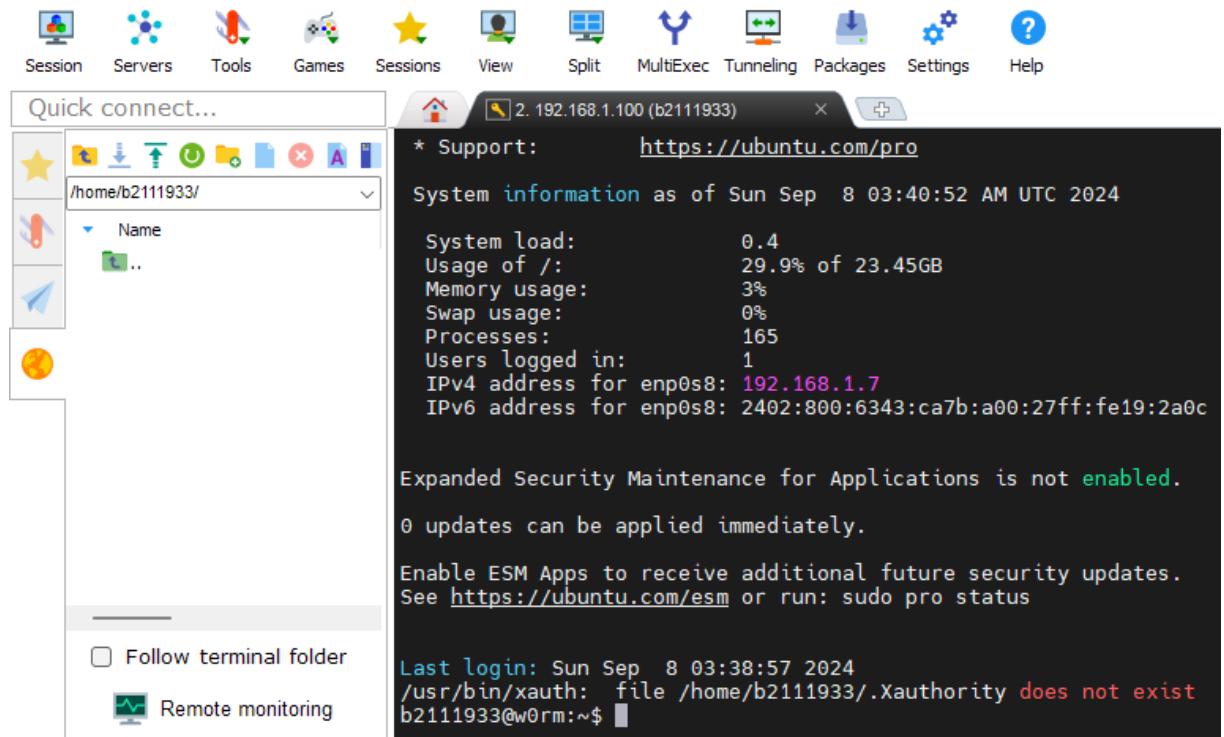
```
W0rm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
b2111933@w0rm:~$ ping -c3 google.com
PING google.com(nchkga-am-in-x0e.1e100.net (2404:6800:4005:823::200e)) 56 data
64 bytes from nchkga-am-in-x0e.1e100.net (2404:6800:4005:823::200e): icmp_seq=1
64 bytes from nchkga-am-in-x0e.1e100.net (2404:6800:4005:823::200e): icmp_seq=2
64 bytes from nchkga-am-in-x0e.1e100.net (2404:6800:4005:823::200e): icmp_seq=3

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 52.159/52.401/52.652/0.201 ms
b2111933@w0rm:~$ ping -c3 github.com
PING github.com (20.205.243.166) 56(84) bytes of data.
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=1 ttl=112 time=32.2 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=2 ttl=112 time=32.8 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=3 ttl=112 time=32.2 ms

--- github.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2024ms
rtt min/avg/max/mdev = 32.152/32.364/32.781/0.294 ms
b2111933@w0rm:~$ _
```

Hình 20: Kiểm tra kết nối mạng của Ubuntu Server.

Để thuận tiện cho quá trình cài đặt về sau, ta có thể thực hiện kết nối SSH đến Ubuntu Server thông qua phần mềm MobaXterm, từ đó việc cài đặt sẽ trở nên dễ dàng hơn với khả năng sao chép và dán văn bản.



Hình 21: SSH đến Ubuntu Server.

1.2. Cài đặt DevStack

DevStack cần được thực thi với tư cách là người dùng không phải người dùng root, nhưng người dùng này vẫn phải được cấp quyền sudo. Chính vì thế, ta nên thiết lập một tài khoản người dùng riêng biệt để chạy DevStack:

```
$ sudo useradd -s /bin/bash -d /opt/stack -m stack  
$ sudo chmod +x /opt/stack  
$ echo "stack ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/stack  
$ sudo -u stack -i
```

Kho lưu trữ trên Git của DevStack chứa một tập lệnh cài đặt OpenStack và các mẫu cho các tệp cấu hình. Ta thiết lập thông số cài đặt DevStack:

```
$ git clone https://opendev.org/openstack/devstack  
$ cd devstack  
$ nano local.conf  
[[local|localrc]]  
ADMIN_PASSWORD=secret  
DATABASE_PASSWORD=$ADMIN_PASSWORD  
RABBIT_PASSWORD=$ADMIN_PASSWORD  
SERVICE_PASSWORD=$ADMIN_PASSWORD  
HOST_IP=<enp0s3 IP, used for DevStack IP>  
PUBLIC_INTERFACE=enp0s8  
FLOATING_RANGE=<Network Address>  
PUBLIC_NETWORK_GATEWAY=<Gateway Address>  
Q_FLOATING_ALLOCATION_POOL=start=<Start of floating IP>,end=<End of  
floating IP>
```

```
GNU nano 6.2                                     local.conf  
[[local|localrc]]  
ADMIN_PASSWORD=secret  
DATABASE_PASSWORD=$ADMIN_PASSWORD  
RABBIT_PASSWORD=$ADMIN_PASSWORD  
SERVICE_PASSWORD=$ADMIN_PASSWORD  
HOST_IP=192.168.1.100  
PUBLIC_INTERFACE=enp0s8  
FLOATING_RANGE=192.168.1.0/24  
PUBLIC_NETWORK_GATEWAY=192.168.1.1  
Q_FLOATING_ALLOCATION_POOL=start=192.168.1.201,end=192.168.1.250
```

Hình 22: Thiết lập các thông số cài đặt OpenStack.

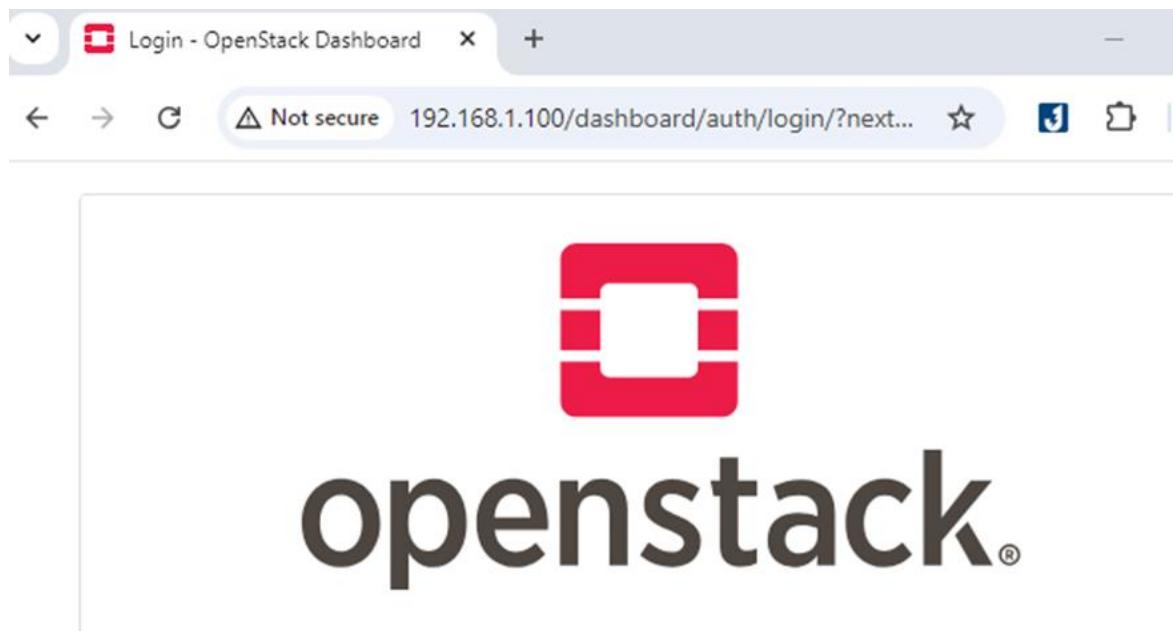
Ta tiến hành cài đặt DevStack, bộ công cụ này sẽ bao gồm các dịch vụ Keystone, Glance, Nova, Placement, Cinder, Neutron và Horizon. Quá trình này sẽ mất từ 15 đến 30 phút, tùy thuộc vào tốc độ kết nối internet.

```
$ ./stack.sh
```

```
3. 192.168.1.100 (b2111933) x +  
nova_cell1 | UPDATE | 42 |  
cinder | SELECT | 56 |  
cinder | INSERT | 5 |  
glance | INSERT | 14 |  
placement | UPDATE | 3 |  
cinder | UPDATE | 5 |  
cinder | DELETE | 1 |  
glance | SELECT | 28 |  
glance | UPDATE | 2 |  
nova_api | INSERT | 20 |  
nova_api | SAVEPOINT | 10 |  
nova_api | RELEASE | 10 |  
nova_cell1 | DELETE | 1 |  
+-----+-----+-----+  
  
This is your host IP address: 192.168.1.100  
This is your host IPv6 address: 2402:800:6343:ca7b:a00:27ff:fe19:2a0c  
Horizon is now available at http://192.168.1.100/dashboard  
Keystone is serving at http://192.168.1.100/identity/  
The default users are: admin and demo  
The password: secret
```

Hình 23: Cài đặt OpenStack thành công.

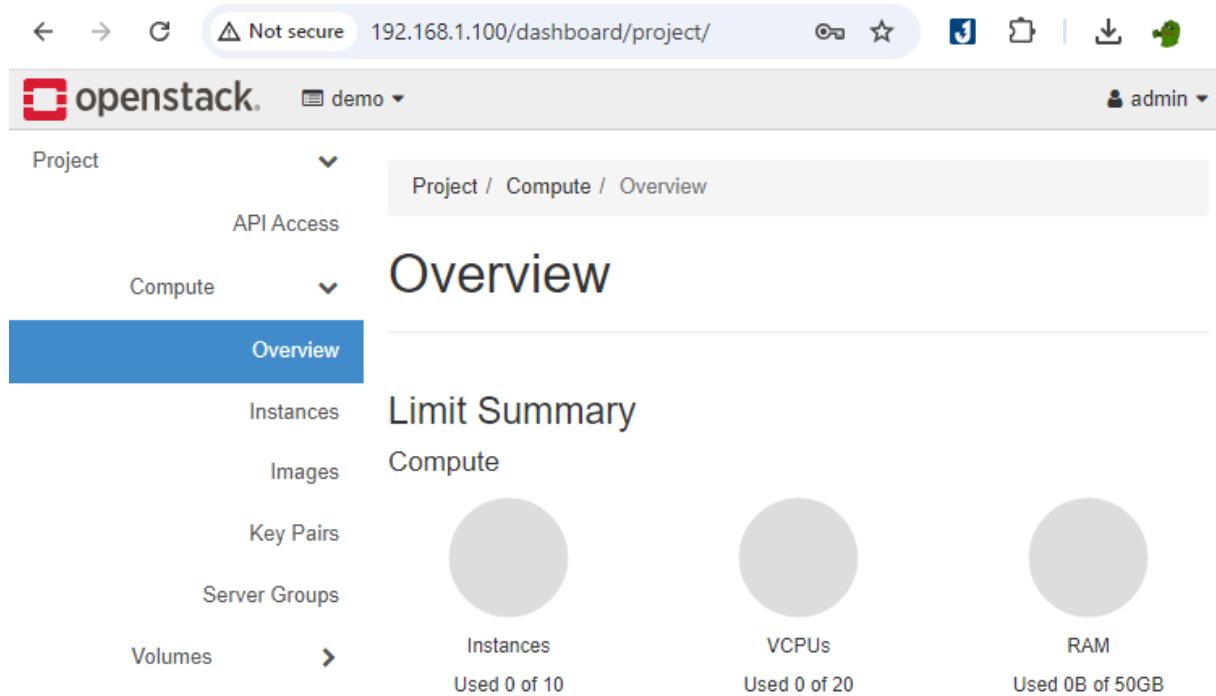
Ta có thể truy cập dịch vụ Horizon để trải nghiệm giao diện web của OpenStack và quản lý các máy ảo, mạng, ổ đĩa và hình ảnh từ `http://<địa chỉ IP của card enp0s3>`.



Hình 24: Giao diện web của OpenStack.

1.3. Cấu hình nền tảng OpenStack

Ta đăng nhập vào OpenStack với tài khoản / mật khẩu: admin / secret.



Hình 25: Đăng nhập vào OpenStack bằng tài khoản admin.

Truy cập mục Identity và tạo một Project mới:

The screenshot shows a "Create Project" dialog box. At the top, there are three tabs: "Project Information *", "Project Members", and "Project Groups", with "Project Information *" being the active tab. The form fields under "Project Information" are as follows: "Domain ID" (set to "default"), "Domain Name" (set to "Default"), "Name *" (set to "W0rm"), and "Description" (an empty text area). Below the form, there is a checkbox labeled "Enabled" which is checked. At the bottom right of the dialog are two buttons: "Cancel" and "Create Project".

Hình 26: Tạo một Project cho sản phẩm nghiên cứu.

W0rm

	Overview	Users	Groups
Name	W0rm		
ID	03fd442c1d2d45d8bda30c56b4c1e2c4		
Domain Name	Default		
Domain ID	default		
Enabled	Yes		
Description	-		

Hình 27: Thông tin Project

Tương tự, trong mục Identity, ta tiến hành tạo một User mới. User này có Primary Project là Project vừa tạo (W0rm) và được cấp quyền admin.

Create User ×

Domain ID	<input type="text" value="default"/>	Description:	
Domain Name	<input type="text" value="Default"/>	Create a new user and set related properties including the Primary Project and Role.	
User Name *	<input type="text" value="B2111933"/>		
Description	<input type="text"/>		

Hình 28: Tạo một User mới.

Password *

Confirm Password *

Primary Project

Role

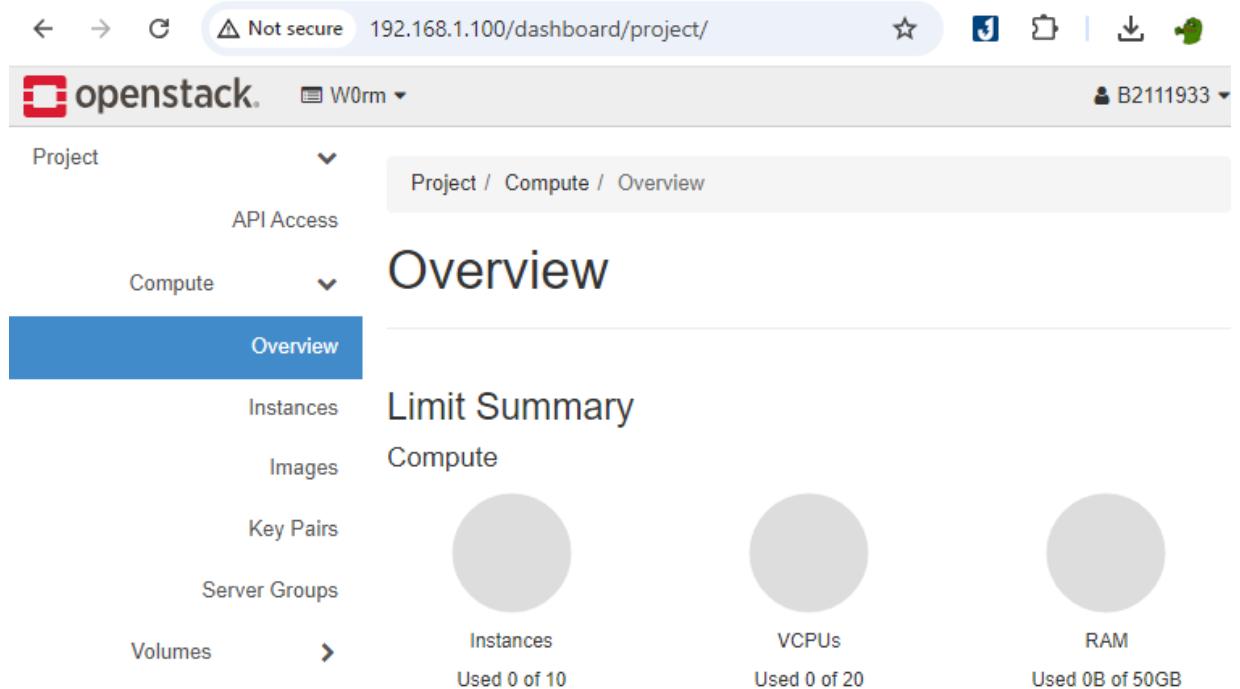
Enabled

Lock password

Cancel Create User

Hình 29: Đặt mật khẩu, chọn Primary Project và phân quyền admin cho User.

Vậy là ta đã khởi tạo thành công một Project cho đề tài nghiên cứu, cùng với một tài khoản người dùng cá nhân được cấp quyền admin. Ta tiến hành đăng xuất khỏi tài khoản admin, sau đó đăng nhập vào tài khoản người dùng vừa được tạo (B2111933).



Hình 30: Đăng nhập vào tài khoản của User vừa được tạo.

Vậy là ta đã hoàn tất việc cấu hình cơ bản cho nền tảng Openstack. Bên cạnh đó, chúng ta có thể truy cập và sử dụng các dịch vụ của OpenStack từ xa, thông qua giao diện dòng lệnh (CLI) và API. Ta tiến hành truy cập vào API Access và tải OpenStack RC File (Remote Command File) về máy tính cục bộ, đây là tập tin văn bản chứa các thông tin cần thiết để có thể kết nối đến OpenStack từ bên ngoài.

Hình 31: Tải OpenStack RC File để có thể kết nối đến OpenStack từ xa.

Từ máy tính cục bộ, ta kết nối SSH đến Ubuntu Server (máy ảo xây dựng nền tảng OpenStack) và cài đặt bộ công cụ dòng lệnh OpenStack.

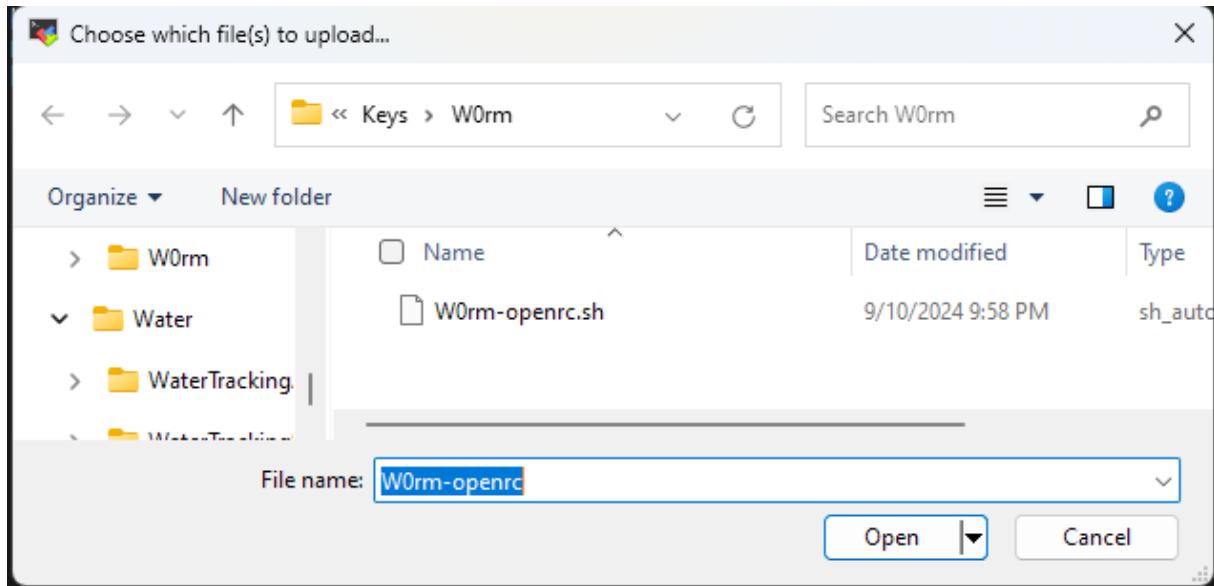
```
$ pip install python-openstackclient
```

```
Defaulting to user installation because normal site-packages is not writeable
Collecting python-openstackclient
  Downloading python_openstackclient-7.0.0-py3-none-any.whl (1.1 MB)
    1.1/1.1 MB 697.3 kB/s eta 0:00:00
Collecting osc-lib>=2.3.0
  Downloading osc_lib-3.1.0-py3-none-any.whl (89 kB)
    89.6/89.6 KB 521.4 kB/s eta 0:00:00
Collecting pbr!=2.1.0,>=2.0.0
  Downloading pbr-6.1.0-py2.py3-none-any.whl (108 kB)
    108.5/108.5 KB 2.6 MB/s eta 0:00:00
Collecting oslo.i18n>=3.15.3
  Downloading oslo.i18n-6.4.0-py3-none-any.whl (46 kB)
    46.8/46.8 KB 7.7 MB/s eta 0:00:00
Collecting stevedore>=2.0.1
  Downloading stevedore-5.3.0-py3-none-any.whl (49 kB)
    49.7/49.7 KB 5.1 MB/s eta 0:00:00
```

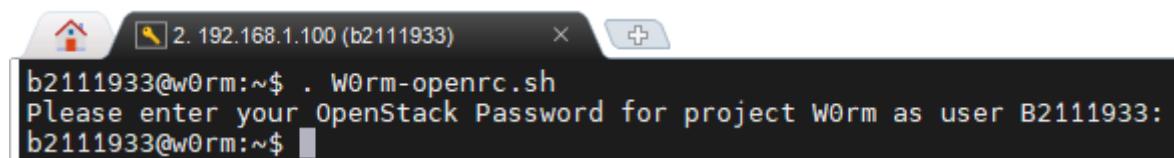
Hình 32: Tải bộ công cụ dòng lệnh về Ubuntu Server.

Ta tiến hành tải OpenStack RC File lên Ubuntu Server và thực thi chương trình.

\$. <tên file>.sh



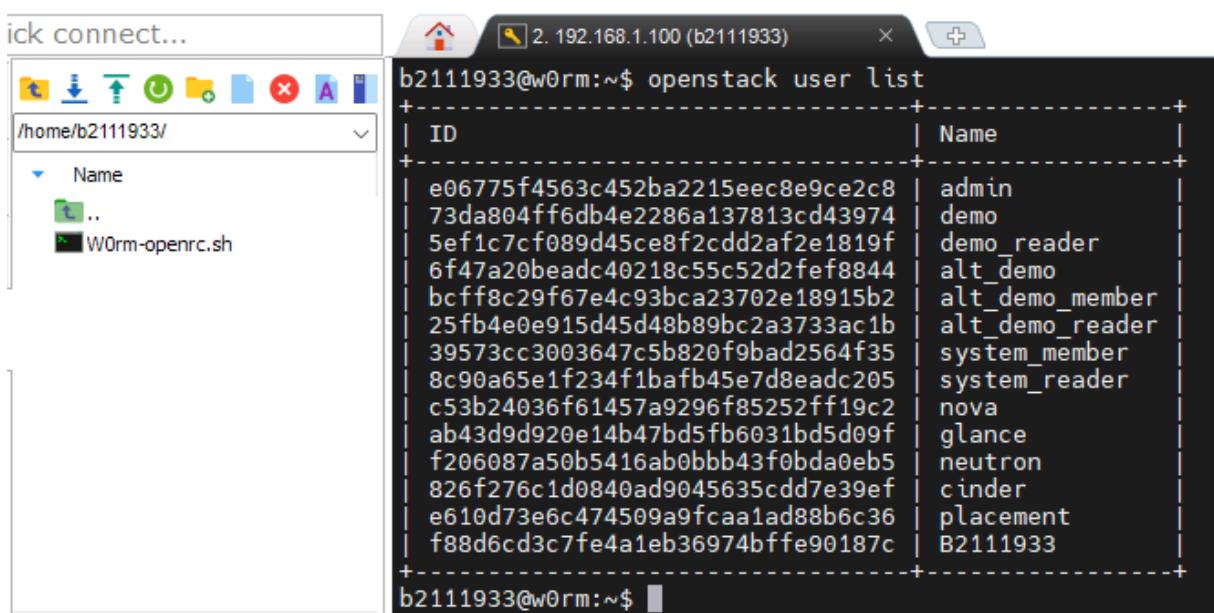
Hình 33: Tải OpenStack RC File lên Ubuntu Server



Hình 34: Thực thi Open RC File và đăng nhập để xác minh.

Giờ đây ta đã có thể quản lý các dịch vụ của OpenStack thông qua giao diện dòng lệnh. Ví dụ: ta có thể liệt kê danh sách người dùng (User).

\$ openstack user list



Hình 35: Một ví dụ về truy cập OpenStack thông qua giao diện dòng lệnh.

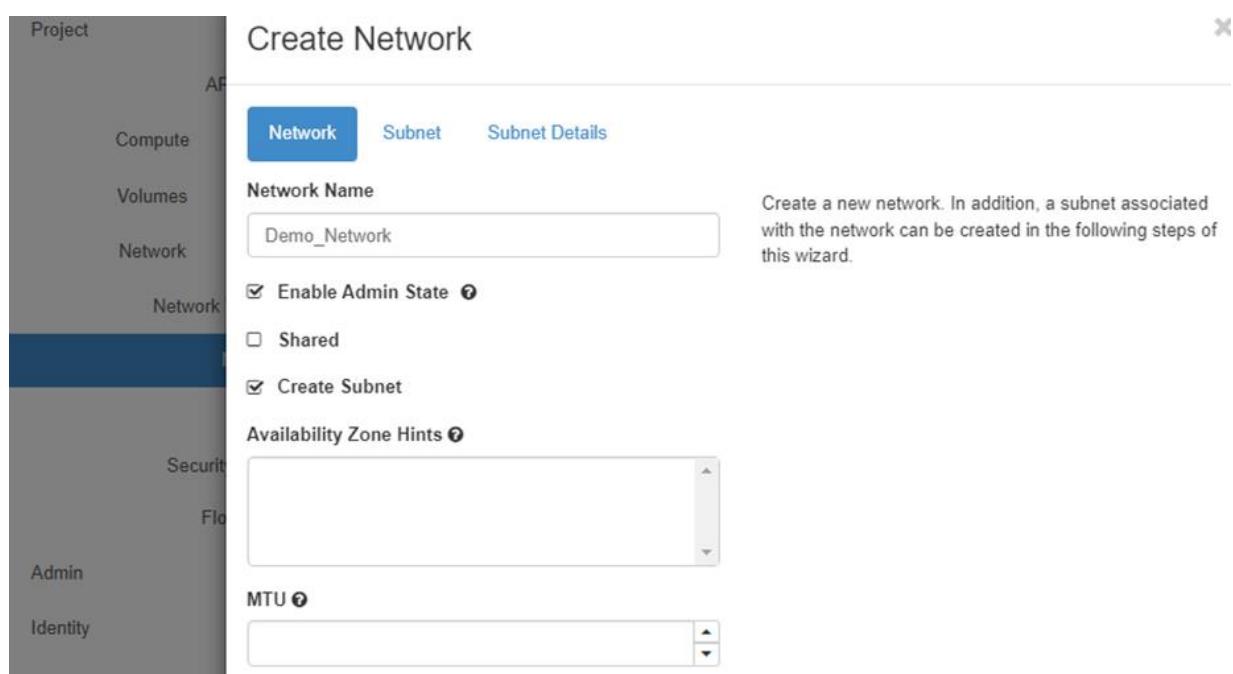
2. Xây dựng bài tập thực hành kiểm thử bảo mật

Về các bài tập thực hành kiểm thử bảo mật trên môi trường OpenStack, mỗi bài tập sẽ được xây dựng trên một nhánh mạng riêng biệt, với một máy ảo tấn công và một máy ảo mục tiêu. Tuy nhiên, do hạn chế về mặt tài nguyên, nhóm chỉ xây dựng duy nhất một bài tập thực hành nhằm phục vụ cho việc chạy thử nghiệm. Trong nghiên cứu này, máy ảo tấn công sẽ được chạy trên hệ điều hành Kali Linux (Generic Cloud Image). Từ máy ảo tấn công, người dùng sẽ có nhiệm vụ xâm nhập vào hệ thống của máy ảo mục tiêu với hệ điều hành CirrOS. Hai máy ảo này được xây dựng trên cùng một nhánh mạng.

2.1. Cấu hình mạng cho bài tập

Để xây dựng một nhánh mạng riêng biệt cho bài tập thực hành. Ta truy cập Networks và tạo một Network mới với các thông tin sau:

- Network Name: “Demo_Network”
- Subnet Name: “Demo_Network_Subnet”
- Network Address: 10.0.1.0/24
- Gateway IP: 10.0.1.1
- Enable DHCP
- Allocation Pools: 10.0.1.100,10.0.1.254
- DNS Name Servers: 8.8.8.8



Hình 36: Cấu hình Network.

Create Network

Network Subnet Subnet Details

Subnet Name
Demo_Network_Subnet

Network Address Source
Enter Network Address manually

Network Address ⓘ
10.0.1.0/24

IP Version
IPv4

Gateway IP ⓘ
10.0.1.1

Disable Gateway

Creates a subnet associated with the network. You need to enter a valid "Network Address" and "Gateway IP". If you did not enter the "Gateway IP", the first value of a network will be assigned by default. If you do not want gateway please check the "Disable Gateway" checkbox. Advanced configuration is available by clicking on the "Subnet Details" tab.

Hình 37: Cấu hình Subnet cho Network.

Network Subnet Subnet Details

Enable DHCP Specify additional attributes for the subnet.

Allocation Pools ⓘ
10.0.1.100,10.0.1.254

DNS Name Servers ⓘ
8.8.8.8

Hình 38: Cấu hình Allocation Pools và DNS Name Servers cho Network.

Trên nền tảng OpenStack, public network là một mạng ảo được cấu hình để cho phép các máy ảo trong môi trường OpenStack kết nối với thế giới bên ngoài cũng như truy cập Internet. Ta tiến hành thiết lập một Router nhằm kết nối nhánh mạng vừa tạo với public network.

Create Router

Router Name

Enable Admin State ?

External Network

Enable SNAT

Availability Zone Hints ?

Description:
Creates a router with specified parameters.
Enable SNAT will only have an effect if an external network is set.

Hình 39: Tạo một Router kết nối đến public network.

Ta truy cập đến thông tin của Router vừa tạo, trong thẻ Interfaces ta tiến hành thêm Demo_Network vào giao diện card mạng trong của Router.

Add Interface

Subnet *

IP Address (optional) ?

Description:
You can connect a specified subnet to the router.
If you don't specify an IP address here, the gateway's IP address of the selected subnet will be used as the IP address of the newly created interface of the router. If the gateway's IP address is in use, you must use a different address which belongs to the selected subnet.

Hình 40: Thêm nhánh mạng vào giao diện card mạng trong của Router.

Vậy là ta đã thiết lập thành công nhánh mạng phục vụ cho bài tập thực hành kiểm thử bảo mật. Ta có thể truy cập đến Network Topology và kiểm tra cấu trúc mạng.



Hình 41: Network Topology.

Tuy nhiên, do nhánh mạng Demo_Network sử dụng địa chỉ IP NAT nên ta không thể xác định địa chỉ IP thật của các máy ảo thuộc nhánh mạng này. Chính vì thế, hiện tại chúng ta không thể kết nối đến các máy ảo từ bên ngoài môi trường Openstack.

Để giải quyết vấn đề này, trong phần cài đặt OpenStack, ta đã thiết lập Floating IPs là dãy địa chỉ IP động dựa trên địa chỉ mạng mà máy vật lý đang kết nối. Ta tiến hành cấp phát Floating IPs cho Project hiện tại, mỗi địa chỉ sẽ được gắn vào một máy ảo chỉ định.

Floating IPs

Floating IP Address = ▾				Filter	Allocate IP To Project	Release Floating IPs
Displaying 2 items						
<input type="checkbox"/>	IP Address	Description	DNS Name	DNS Domain	Mapped Fixed IP Address	Pool Status Actions
<input type="checkbox"/>	192.168.1.223			-		public Down Associate ▾
<input type="checkbox"/>	192.168.1.234			-		public Down Associate ▾
Displaying 2 items						

Hình 42: Floating IPs.

Bên cạnh đó, Security Group trong OpenStack là một khái niệm quan trọng về bảo mật mạng, hoạt động như một tường lửa (firewall) ảo, cho phép ta kiểm soát lưu lượng truy cập vào và ra khỏi các máy ảo. Ở bài tập này, ta sẽ tiến hành thiết lập một Security Group cho phép các giao thức như ICMP, SSH, HTTP, HTTPS truy cập vào máy ảo.

Create Security Group

Name *

Demo_Security_Group

Description:

Security groups are sets of IP filter rules that are applied to network interfaces of a VM. After the security group is created, you can add rules to the security group.

Hình 43: Tạo một Security Group mới.

Manage Security Group Rules: Demo_Security_Group (94c837c5- 2d5c-4141-9d29-e4bd72788a55)

[+ Add Rule](#)

[Delete Rules](#)

Displaying 6 items

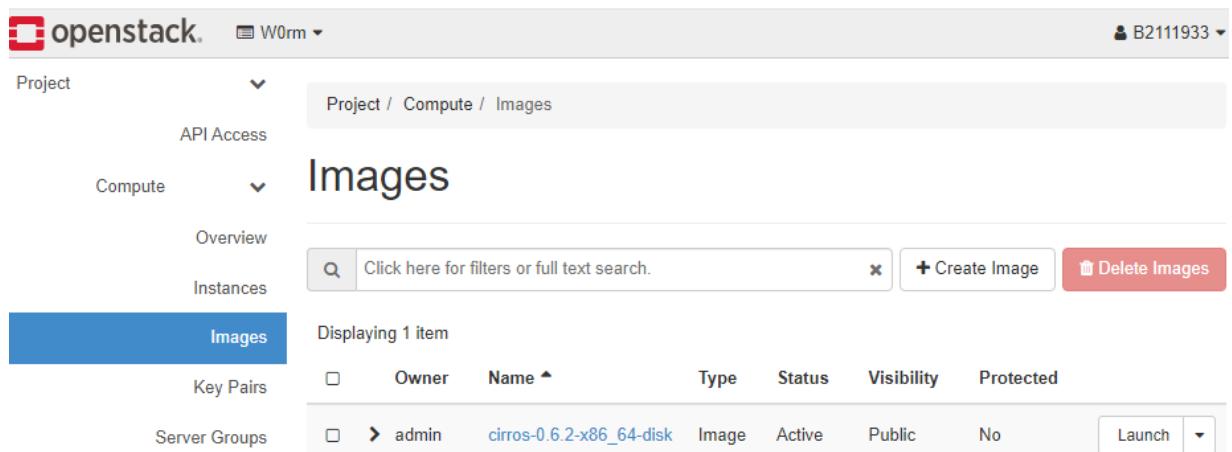
<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
<input type="checkbox"/>	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	-	Delete Rule

Displaying 6 items

Hình 44: Thêm các quy tắc vào Security Group.

2.2. Xây dựng Images cho các hệ điều hành

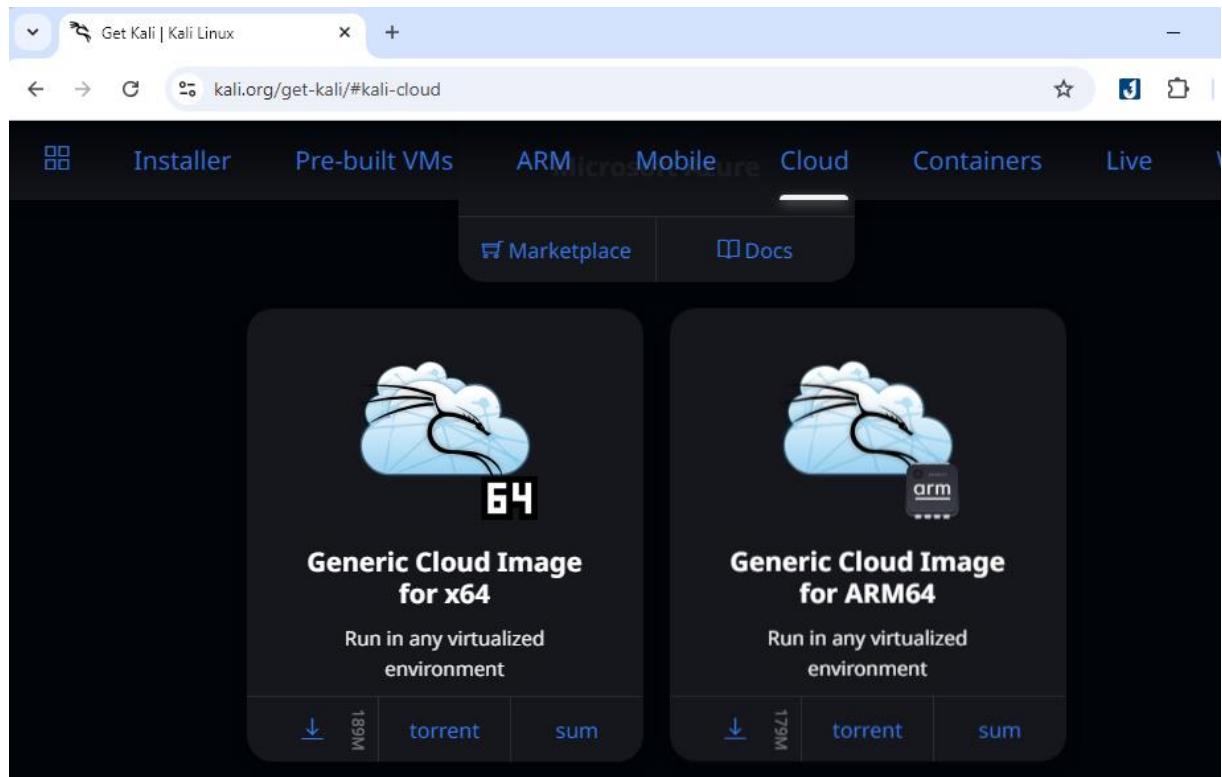
Thông thường, trong quá trình cài đặt, nền tảng OpenStack sẽ tự động tích hợp một Image với hệ điều hành CirrOS. CirrOS là một hệ điều hành ảo rất nhẹ và đơn giản, rất thích hợp cho việc dùng để xây dựng máy ảo mục tiêu cho bài thực hành. Ngoài CirrOS ra, ta có thể sử dụng nhiều loại hệ điều hành khác nhau như Windows, MacOS,... do nền tảng OpenStack có khả năng hỗ trợ hầu hết các hệ điều hành.



The screenshot shows the OpenStack dashboard with the 'Compute' project selected. In the 'Images' tab, there is one item named 'cirros-0.6.2-x86_64-disk'. The details for this image are: Type: Image, Status: Active, Visibility: Public, Protected: No. There is a 'Launch' button and a dropdown menu next to it.

Hình 45: Image của hệ điều hành CirrOS.

Đối với bài thực hành này, máy ảo tấn công của chúng ta sẽ được chạy trên hệ điều hành Kali Linux. Tại trang chủ của Kali (kali.org), ta có thể tìm thấy các Image dành cho môi trường đám mây của hệ điều hành Kali Linux.



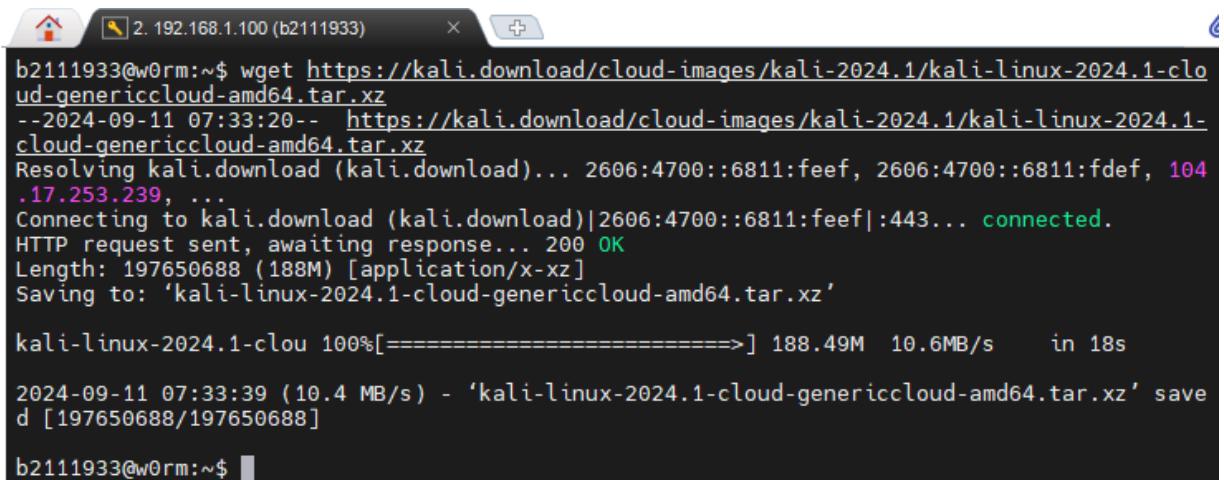
The screenshot shows the Kali Linux website at kali.org/get-kali/#kali-cloud. It features two main sections for generic cloud images:

- Generic Cloud Image for x64**: Described as running in any virtualized environment. It has download links for [WGET](#), [torrent](#), and [sum](#).
- Generic Cloud Image for ARM64**: Described as running in any virtualized environment. It has download links for [WGET](#), [torrent](#), and [sum](#).

Hình 46: Images cho môi trường đám mây của hệ điều hành Kali Linux.

Ta tiến hành tải xuống Generic Cloud Image for x64 thông qua giao diện dòng lệnh.

```
$ wget https://kali.download/cloud-images/kali-2024.1/kali-linux-2024.1-cloud-genericcloud-amd64.tar.xz
```



```
b2111933@w0rm:~$ wget https://kali.download/cloud-images/kali-2024.1/kali-linux-2024.1-cloud-genericcloud-amd64.tar.xz
--2024-09-11 07:33:20-- https://kali.download/cloud-images/kali-2024.1/kali-linux-2024.1-cloud-genericcloud-amd64.tar.xz
Resolving kali.download (kali.download)... 2606:4700::6811:feef, 2606:4700::6811:fdef, 104.17.253.239, ...
Connecting to kali.download (kali.download)|2606:4700::6811:feef|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 197650688 (188M) [application/x-xz]
Saving to: 'kali-linux-2024.1-cloud-genericcloud-amd64.tar.xz'

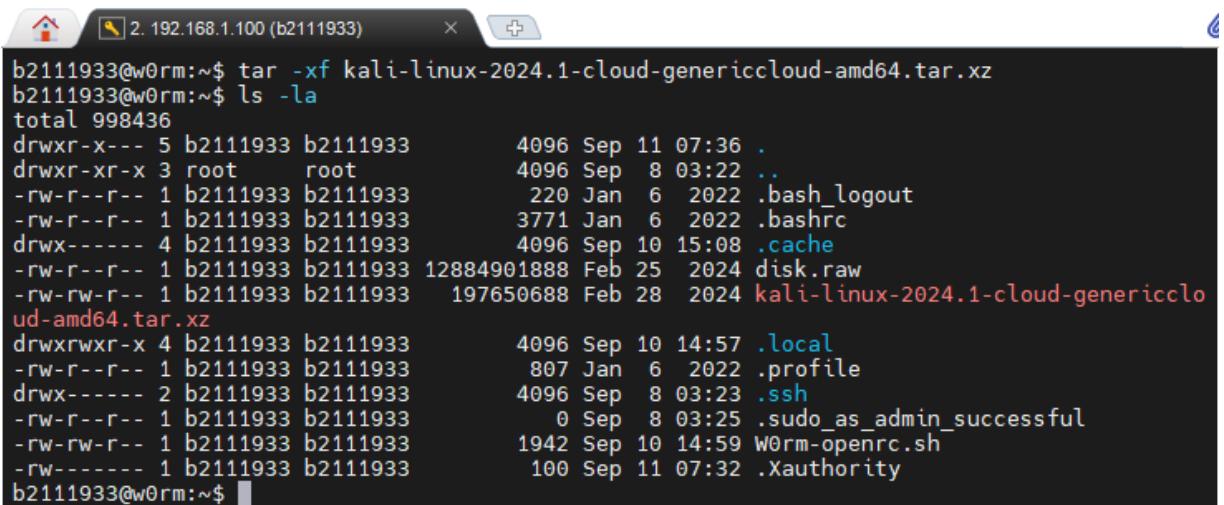
kali-linux-2024.1-clou 100%[=====] 188.49M  10.6MB/s    in 18s
2024-09-11 07:33:39 (10.4 MB/s) - 'kali-linux-2024.1-cloud-genericcloud-amd64.tar.xz' saved [197650688/197650688]

b2111933@w0rm:~$
```

Hình 47: Tải xuống Generic Cloud Image của hệ điều hành Kali Linux.

Sau khi giải nén tập tin vừa được tải xuống, ta có được một RAW Image.

```
$ tar -xf kali-linux-2024.1-cloud-genericcloud-amd64.tar.xz
```



```
b2111933@w0rm:~$ tar -xf kali-linux-2024.1-cloud-genericcloud-amd64.tar.xz
b2111933@w0rm:~$ ls -la
total 998436
drwxr-x--- 5 b2111933 b2111933      4096 Sep 11 07:36 .
drwxr-xr-x  3 root      root        4096 Sep  8 03:22 ..
-rw-r--r--  1 b2111933 b2111933      220 Jan  6 2022 .bash_logout
-rw-r--r--  1 b2111933 b2111933     3771 Jan  6 2022 .bashrc
drwx----- 4 b2111933 b2111933      4096 Sep 10 15:08 .cache
-rw-r--r--  1 b2111933 b2111933 12884901888 Feb 25 2024 disk.raw
-rw-rw-r--  1 b2111933 b2111933   197650688 Feb 28 2024 kali-linux-2024.1-cloud-genericcloud-amd64.tar.xz
drwxrwxr-x  4 b2111933 b2111933      4096 Sep 10 14:57 .local
-rw-r--r--  1 b2111933 b2111933       807 Jan  6 2022 .profile
drwx----- 2 b2111933 b2111933      4096 Sep  8 03:23 .ssh
-rw-r--r--  1 b2111933 b2111933        0 Sep  8 03:25 .sudo_as_admin_successful
-rw-rw-r--  1 b2111933 b2111933     1942 Sep 10 14:59 W0rm-openrc.sh
-rw-----  1 b2111933 b2111933      100 Sep 11 07:32 .Xauthority
b2111933@w0rm:~$
```

Hình 48: Trích xuất RAW Image của hệ điều hành Kali Linux.

Về phần định dạng Image, QCOW2 là lựa chọn ưu tiên cho việc tạo và quản lý máy ảo, với khả năng tiết kiệm không gian lưu trữ, quản lý nhiều snapshot và mang đến hiệu suất cao nhờ cơ chế tối ưu hóa. Ta tiến hành chuyển Image sang định dạng QCOW2.

```
$ qemu-img convert -f raw -O QCOW2 disk.raw kali_linux.QCOW2
```

```

connect...
me/b2111933/
Name
.. disk.raw kali-linux-2024.1-cloud-gener... kali_linux.qcow2 W0rm-openrc.sh
b2111933@w0rm:~$ qemu-img convert -f raw -O qcow2 disk.raw kali_linux.qcow2
b2111933@w0rm:~$ ls -la
total 1852900
drwxr-x--- 5 b2111933 b2111933 4096 Sep 11 07:53 .
drwxr-xr-x 3 root root 4096 Sep 8 03:22 ..
-rw-r--r-- 1 b2111933 b2111933 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 b2111933 b2111933 3771 Jan 6 2022 .bashrc
drwx----- 4 b2111933 b2111933 4096 Sep 10 15:08 .cache
-rw-r--r-- 1 b2111933 b2111933 12884901888 Feb 25 2024 disk.raw
-rw-rw-r-- 1 b2111933 b2111933 197650688 Feb 28 2024 kali-linux-2024.1-cloud-ge
ud-amd64.tar.xz
-rw-r--r-- 1 b2111933 b2111933 874905600 Sep 11 07:53 kali_linux.qcow2
drwxrwxr-x 4 b2111933 b2111933 4096 Sep 10 14:57 .local
-rw-r--r-- 1 b2111933 b2111933 807 Jan 6 2022 .profile
drwx----- 2 b2111933 b2111933 4096 Sep 8 03:23 .ssh
-rw-r--r-- 1 b2111933 b2111933 0 Sep 8 03:25 .sudo_as_admin_successful
-rw-rw-r-- 1 b2111933 b2111933 1942 Sep 10 14:59 W0rm-openrc.sh
-rw----- 1 b2111933 b2111933 100 Sep 11 07:32 .Xauthority
b2111933@w0rm:~$ 

```

Hình 49: QCOW2 Image của hệ điều hành Kali Linux.

Trên phần mềm SSH, ta có thể tải QCOW2 Image của Kali Linux về máy vật lý và tiến hành thiết lập trên môi trường OpenStack. Ở mục Images, ta chọn Create Image:

- File: <tên của QCOW2 Image của Kali Linux vừa tải>
- Format: QCOW2 - QEMU Emulator

Image Details

Specify an image to upload to the Image Service.

Image Name: Kali Linux

Image Description

Image Source

File*: Choose File kali_linux.qcow2

Format*: QCOW2 - QEMU Emulator

Image Requirements

Kernel: Choose an image

Ramdisk: Choose an image

Architecture: Choose an image

Minimum Disk (GB): 0

Minimum RAM (MB): 0

Image Sharing

Visibility: Shared

Protected: Yes

Hình 50: Xây dựng Image Kali Linux trên môi trường OpenStack.

Images

The screenshot shows the 'Images' page in the OpenStack dashboard. At the top, there is a search bar with the placeholder 'Click here for filters or full text search.' and a red 'Delete Images' button. Below the search bar, it says 'Displaying 2 items'. A table lists two images:

	Owner	Name	Type	Status	Visibility	Protected	Disk Format	Size	
<input type="checkbox"/>	admin	cirros-0.6.2-x86_64-disk	Image	Active	Public	No	QCOW2	20.44 MB	<button>Launch</button>
<input type="checkbox"/>	W0rm	Kali Linux	Image	Active	Shared	No	QCOW2	834.38 MB	<button>Launch</button>

Hình 51: Images trên môi trường OpenStack.

2.3. Xây dựng máy ảo tấn công và máy ảo mục tiêu

Chúng ta có thể tiến hành xây dựng các máy ảo dựa trên Images được tạo, bằng cách truy cập mục Instances và chọn Launch Instance.

Đối với máy ảo mục tiêu, do chúng ta lựa chọn sử dụng hệ điều hành CirrOS nên máy ảo này yêu cầu rất ít tài nguyên. Ta tiến hành thiết lập các thông tin như sau:

- Instance name: CirrOS
- Source: CirrOS; Select boot source: image; Create new Volume: No
- Flavor: m1.tiny (VCPUS:1, RAM: 256MB, Total Disk: 1GB)
- Security group: Demo_Security_Group
- Networks: Demo_Network

The screenshot shows the 'Instances' page in the OpenStack dashboard. At the top, there is a search bar with 'Instance ID =', a 'Filter' button, a 'Launch Instance' button, a 'Delete Instances' button, and a 'More Actions' dropdown. Below the search bar, it says 'Displaying 1 item'. A table lists one instance:

	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
<input type="checkbox"/>	CirrOS	cirros-0.6.2-x86_64-disk	10.0.1.184	m1.micro	-	Active		None	Running	1 minute	<button>Create Snapshot</button>

Hình 52: Máy ảo mục tiêu với hệ điều hành CirrOS.

Ta sẽ thực hiện gắn địa chỉ Floating IP cho máy ảo mục tiêu, phục vụ cho việc kết nối đến máy ảo này từ bên ngoài môi trường OpenStack. Ở mục Actions, ta chọn Associate Floating IP và chọn một địa chỉ IP bất kỳ.

Manage Floating IP Associations

IP Address *

Select the IP address you wish to associate with the selected instance or port.

Port to be associated *

Hình 53: Thực hiện gắn Floating IP cho máy ảo mục tiêu.

Vậy là ta đã hoàn tất việc cấu hình máy ảo mục tiêu, ta có thể truy cập đến bảng điều khiển màn hình máy ảo thông qua thẻ Console. Sau khi truy cập đến màn hình máy ảo, ta thực hiện đăng nhập với tài khoản / mật khẩu: cirros / gocubsgo.

CirrOS

If console is not responding to keyboard input: click the grey status bar below. [Click here to show only console](#)
To exit the fullscreen mode, click the browser's back button.

```
Connected to QEMU (instance-00000001)

[ 1.890498] eum: security.ima
[ 1.892060] eum: security.capability
[ 1.893874] eum: HMAC attrs: 0x1
[ 1.895660] PM: Magic number: 8:497:232
[ 1.897696] RAS: Correctable Errors collector initialized.
[ 1.901545] Freeing unused decrypted memory: 2036K
[ 1.904175] Freeing unused kernel image (initmem) memory: 3244K
[ 1.911706] Write protecting the kernel read-only data: 30720k
[ 1.915235] Freeing unused kernel image (text/rodata gap) memory: 2036K
[ 1.918969] Freeing unused kernel image (rodata/data gap) memory: 1448K
[ 1.955400] x86/mm: Checked W+X mappings: passed, no W+X pages found.
[ 1.958745] x86/mm: Checking user space page tables
[ 1.992522] x86/mm: Checked W+X mappings: passed, no W+X pages found.
[ 1.995525] Run /init as init process

further output written to /dev/ttys0
[ 2.032900] virtio_blk virtio2: [vdal] 2097152 512-byte logical blocks (1.07 G
B/1.00 GiB)
[ 2.040853] GPT:Primary header thinks Alt. header is not at the end of the di
sk.
[ 2.044448] GPT:229375 != 2097151
[ 2.046104] GPT:Alternate GPT header not at the end of the disk.
[ 2.048784] GPT:229375 != 2097151
[ 2.050363] GPT: Use GNU Parted to correct GPT errors.
[ 2.078694] virtio_gpu virtio0: [drm] drm_plane_enable_fb_damage_clips() not called
[ 2.085087] random: crng init done

login as 'cirros' user. default password: 'gocubsgo'. use 'sudo' for root.
cirros login:
```

Hình 54: Bảng điều khiển máy ảo mục tiêu.

CirrOS

Overview Interfaces Log **Console** Action Log

Instance Console

If console is not responding to keyboard input: click the grey status bar below. [Click here to show only console](#)
To exit the fullscreen mode, click the browser's back button.

```
Connected to QEMU (instance-00000001)

$ ping -c3 google.com
PING 74.125.130.139 (74.125.130.139) 56(84) bytes of data.
64 bytes from sb-in-f139.1e100.net (74.125.130.139): icmp_seq=1 ttl=102 time=44.6 ms
64 bytes from sb-in-f139.1e100.net (74.125.130.139): icmp_seq=2 ttl=102 time=42.9 ms
64 bytes from sb-in-f139.1e100.net (74.125.130.139): icmp_seq=3 ttl=102 time=42.8 ms

--- 74.125.130.139 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 42.767/43.422/44.647/0.866 ms
$ ping -c3 github.com
PING 20.205.243.166 (20.205.243.166) 56(84) bytes of data.
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=1 ttl=111 time=33.1 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=2 ttl=111 time=34.3 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=3 ttl=111 time=33.2 ms

--- 20.205.243.166 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 33.084/33.507/34.289/0.553 ms
$ uname -a
Linux cirros 5.15.0-71-generic #78-Ubuntu SMP Tue Apr 18 09:00:29 UTC 2023 x86_64 GNU/Linux
$ _
```

Hình 55: Kiểm tra kết nối mạng của máy ảo mục tiêu.

Tiếp đến chúng ta sẽ thực hiện việc xây dựng máy ảo tấn công. Máy ảo tấn công sẽ được xây dựng với hệ điều hành Kali Linux, dựa trên Kali Linux Generic Cloud Image. Mặc định phiên bản Image này sẽ chỉ cài đặt một giao diện dòng lệnh cho hệ điều hành Kali Linux, không yêu cầu nhiều tài nguyên phần cứng, cần tối thiểu 12GB cho dung lượng lưu trữ. Ta tiến hành thiết lập các thông tin như sau:

- Instance name: Kali Linux
- Source: Kali Linux; Select boot source: Image; Create new Volume: No
- Flavor: m1.small (VCPUS: 1, RAM: 2GB, Total Disk: 20GB)
- Security group: Demo_Security_Group
- Networks: Demo_Network
- Key pair: Create a new key pair
 - Key Pair Name: Kali
 - Key Type: SSH Key
 - Sao chép Private Key đến tập tin Kali.pem.

Instances

Instance ID =

Filter
Launch

Displaying 2 items

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone
<input type="checkbox"/>	Kali Linux	Kali Linux	10.0.1.226, 192.168.1.223	m1.small	Kali	Shutoff	nova
<input type="checkbox"/>	Cirros	cirros-0.6. 2-x86_64-disk	10.0.1.184, 192.168.1.234	m1.micro	-	Shutoff	nova

Displaying 2 items

Hình 56: Máy ảo tấn công với hệ điều hành Kali Linux.

Tương tự, ta gắn Floating IP cho máy ảo tấn công.

Manage Floating IP Associations

IP Address *

Select the IP address you wish to associate with the selected instance or port.

Port to be associated *

Cancel
Associate

Hình 57: Thực hiện gắn Floating IP cho máy ảo tấn công.

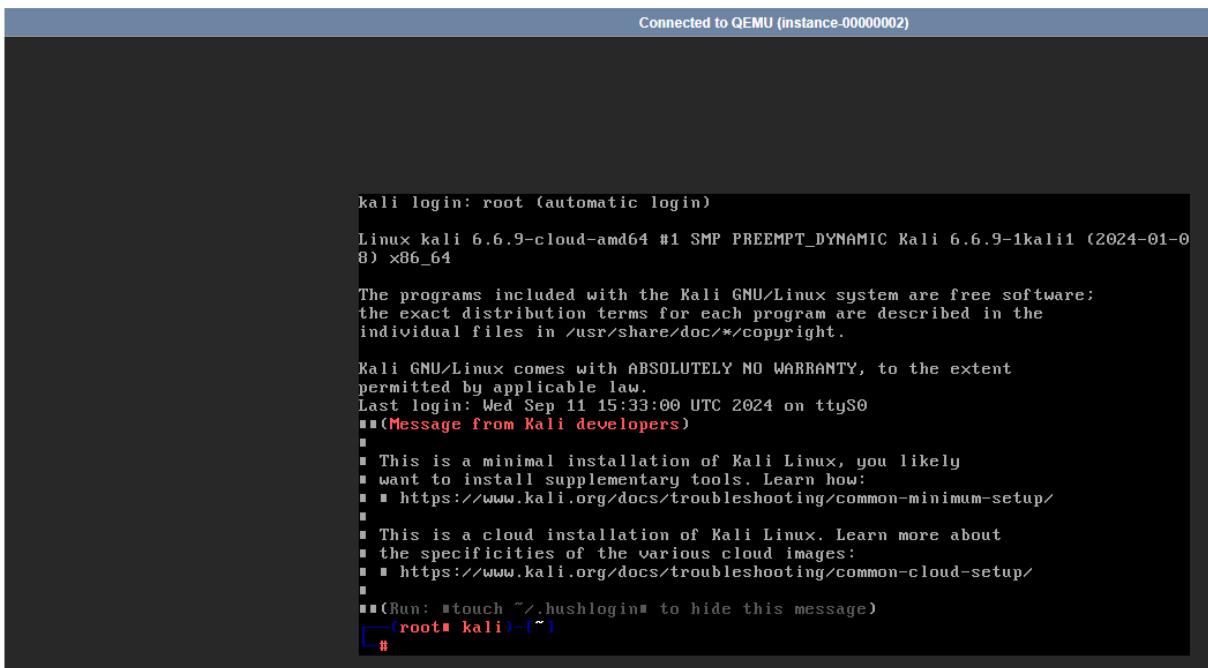
Vậy là chúng ta đã hoàn tất việc cấu hình máy ảo tấn công, ta tiến hành truy cập bảng điều khiển và kiểm tra các máy ảo có kết nối được với nhau hay không, kết nối được với Internet hay không.

Kali Linux

Overview Interfaces Log Console Action Log

Instance Console

If console is not responding to keyboard input: click the grey status bar below. [Click here to show only console](#)
To exit the fullscreen mode, click the browser's back button.



Hình 58: Bảng điều khiển máy ảo tấn công.

```
■■■(Run: touch ~/.hushlogin to hide this message)
└─[root@kali ~]#
└─# ping -c3 10.0.1.184
PING 10.0.1.184 (10.0.1.184) 56(84) bytes of data.
64 bytes from 10.0.1.184: icmp_seq=1 ttl=64 time=0.764 ms
64 bytes from 10.0.1.184: icmp_seq=2 ttl=64 time=0.488 ms
64 bytes from 10.0.1.184: icmp_seq=3 ttl=64 time=0.558 ms

--- 10.0.1.184 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.488/0.603/0.764/0.117 ms

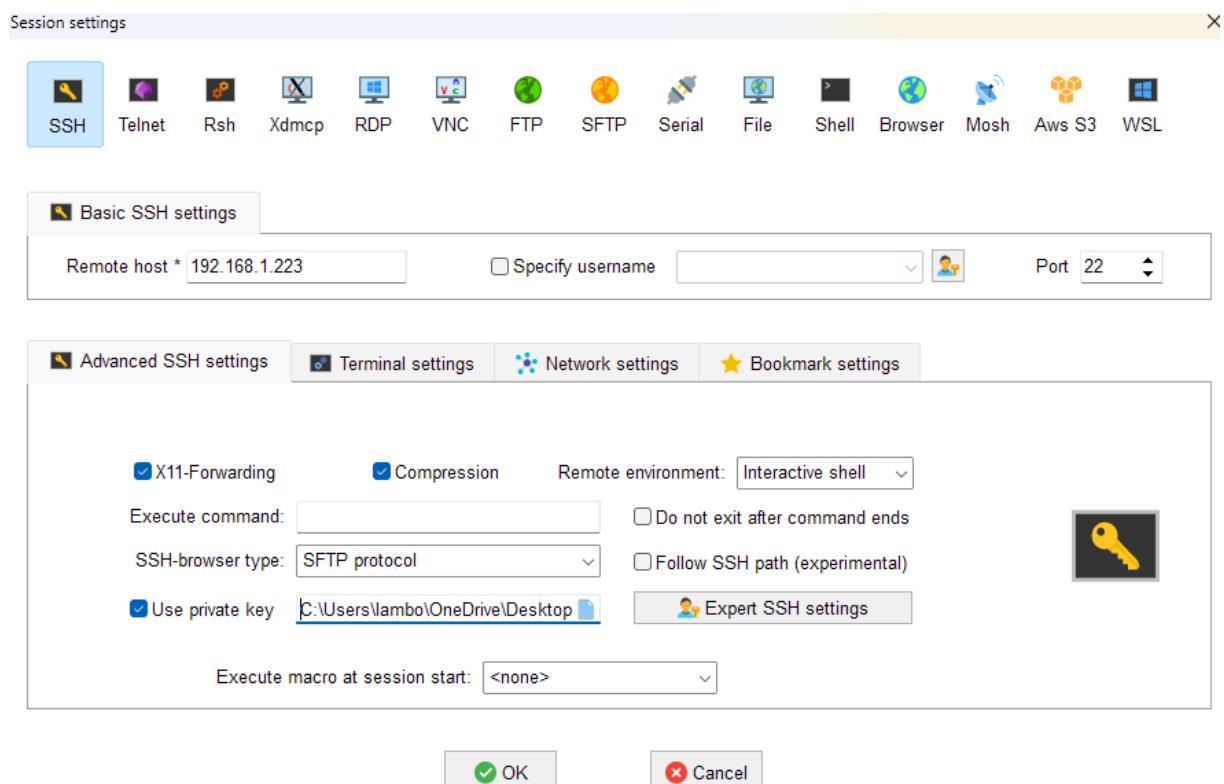
└─[root@kali ~]#
└─# ping -c3 github.com
PING github.com (20.205.243.166) 56(84) bytes of data.
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=1 ttl=111 time=34.2 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=2 ttl=111 time=35.0 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=3 ttl=111 time=34.5 ms

--- github.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 34.195/34.555/35.014/0.341 ms

└─[root@kali ~]#
└─#
```

Hình 59: Kiểm tra kết nối mạng của máy ảo tấn công.

Máy ảo tấn công này còn được cấu hình để cho phép ta truy cập từ xa thông qua dịch vụ SSH với một Key Pair được cấp phát. Ta thực hiện kết nối SSH đến máy ảo tấn công bằng tên người dùng “kali”.



Hình 60: Thiết lập kết nối SSH đến máy ảo tấn công.

```

2. 192.168.1.223
/usr/bin/xauth:  file /home/kali/.Xauthority does not exist
(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
→ https://www.kali.org/docs/troubleshooting/common-minimum-setup/

This is a cloud installation of Kali Linux. Learn more about
the specificities of the various cloud images:
→ https://www.kali.org/docs/troubleshooting/common-cloud-setup/

(Run: "touch ~/.hushlogin" to hide this message)
[(kali㉿ kali)-[~]] $ ping -c3 10.0.1.184
PING 10.0.1.184 (10.0.1.184) 56(84) bytes of data.
64 bytes from 10.0.1.184: icmp_seq=1 ttl=64 time=0.559 ms
64 bytes from 10.0.1.184: icmp_seq=2 ttl=64 time=1.62 ms
64 bytes from 10.0.1.184: icmp_seq=3 ttl=64 time=1.07 ms

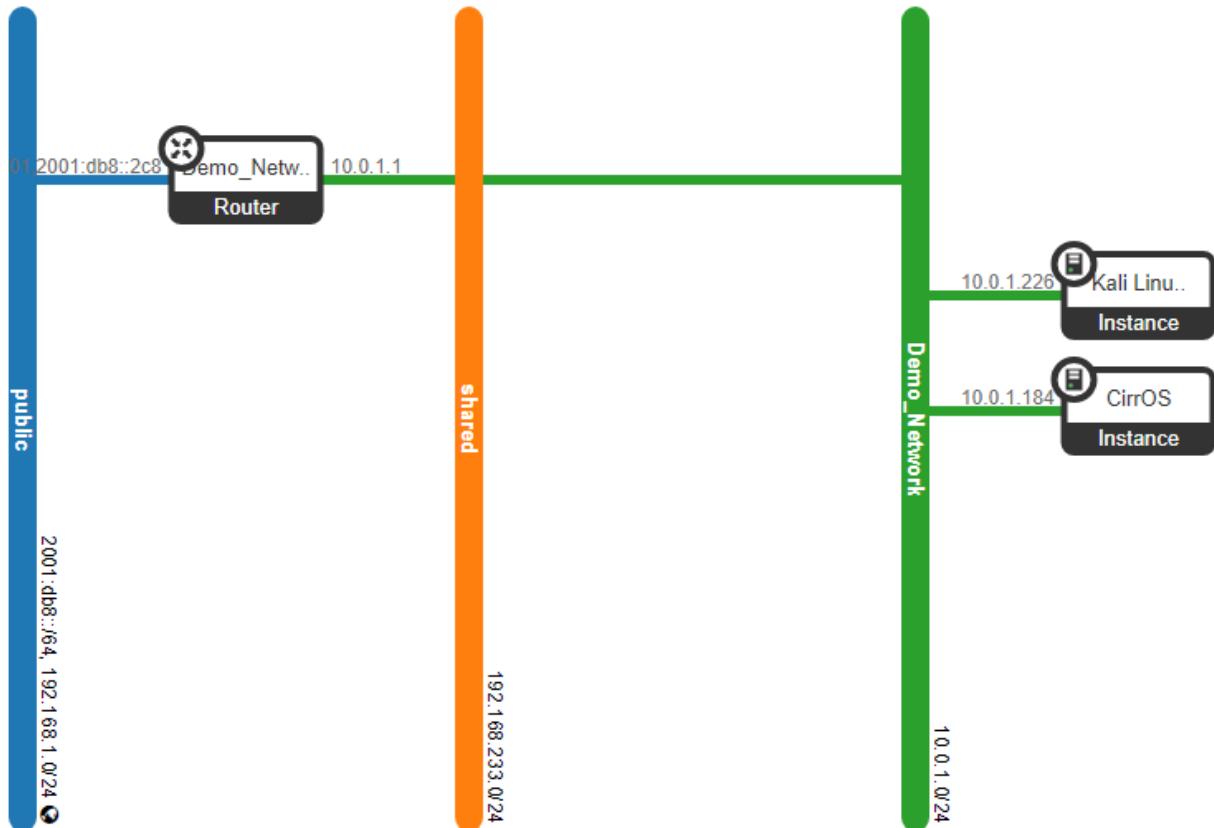
--- 10.0.1.184 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2017ms
rtt min/avg/max/mdev = 0.559/1.081/1.615/0.431 ms

[(kali㉿ kali)-[~]] $ 

```

Hình 61: Kết nối SSH đến máy ảo tấn công và kiểm tra tính năng.

Chúng ta có thể kiểm tra lại cấu trúc của bài tập thực hành ở mục Network Topology. Hình 62 thể hiện rằng ta đã xây dựng thành công một cặp máy ảo tân công - mục tiêu trên cùng một nhánh mạng riêng biệt, nhánh mạng này có thể giao tiếp với thế giới bên ngoài (bao gồm Internet) thông qua public network.



Hình 62: Cấu trúc của bài tập thực hành.

3. Xây dựng ứng dụng web

Đối với việc xây dựng ứng dụng web, nhóm sẽ sử dụng phần mềm XAMPP [29] nhằm thuận tiện cho việc cài đặt và cấu hình một máy chủ web cục bộ (localhost). Các thành phần chính được tích hợp vào XAMPP bao gồm:

- Apache: Một máy chủ web phổ biến, chịu trách nhiệm xử lý các yêu cầu HTTP và hiển thị trang web của bạn.
- MySQL: Một hệ quản trị cơ sở dữ liệu quan hệ, được sử dụng để lưu trữ dữ liệu cho các ứng dụng web.
- PHP: Một ngôn ngữ lập trình kịch bản phía máy chủ, được sử dụng rộng rãi để phát triển các ứng dụng web động.

Ứng dụng web sẽ gồm hai giao diện riêng biệt, một giao diện Admin dành cho người quản trị và một giao diện User dành cho người dùng phổ thông. Các chức năng chính của ứng dụng web:

- Đăng nhập và đăng xuất.
- Truy cập trang chủ.
- Truy cập các lớp học lý thuyết.
- Tham gia các thử thách CTF.
- Thực hành bài tập kiểm thử bảo mật.
- Truy cập trang cá nhân.
- Góp ý cho sản phẩm.
- Cài đặt.

3.1. Thiết kế giao diện ứng dụng web

Khi truy cập đến ứng dụng web, nếu không có thông tin đăng nhập đã lưu, người dùng sẽ được tự động chuyển hướng đến trang đăng nhập. Ở giao diện đăng nhập, người dùng cần phải nhập các thông tin bao gồm tài khoản và mật khẩu được cấp, cùng với tùy chọn lưu thông tin đăng nhập cho trình duyệt web hiện hành. Sau khi đăng nhập thành công, nếu tài khoản người dùng có quyền quản trị thì sẽ được chuyển hướng đến giao diện Admin, nếu tài khoản người dùng không có quyền quản trị thì sẽ được chuyển hướng đến giao diện User.



Hình 63: Giao diện đăng nhập.

Giao diện User được xây dựng nhằm phục vụ cho các người dùng có nhu cầu tiếp thu thêm kiến thức và rèn luyện các kỹ năng thuộc lĩnh vực An toàn thông tin, chủ yếu là các sinh viên Trường Đại học Cần Thơ. Trong khi đó giao diện Admin sẽ được tích hợp các tính năng thêm, sửa, xoá cho người dùng có quyền quản trị, phục vụ cho nhu cầu quản lý các tài nguyên trên ứng dụng web. Trang chủ (Home) sẽ hiển thị các thông tin liên quan đến ứng dụng web như giới thiệu chức năng, giới thiệu thành viên đài tài,...

The screenshot shows the homepage of the WORM platform. At the top, there is a navigation bar with tabs: Home (highlighted in blue), Lectures, CTF Challenges, and Labs. The title "WORM - Training with Cyberspace" is centered above a main content area. On the left, there is a graphic of a computer monitor displaying the WORM logo and the text "CTF". On the right, there is a section titled "WHAT IS CTF?" with a brief description: "CTF (Capture The Flag) is a cybersecurity competition where players solve challenges ranging from simple programming to complex server hacking. The goal is to find specific text segments, or 'flags,' hidden in various digital locations." Below this, there is another section titled "WHAT IS WORM?" with a brief description: "WORM is a cloud-based security testing practice environment project developed by a group of students from CIT." To the right of this text are three circular icons: a shield with a checkmark, the WORM logo, and a network or cloud icon.

Hình 64: Giao diện trang chủ.

Truy cập đến mục lớp học lý thuyết (Lectures), giao diện sẽ bao gồm danh sách lớp học và thanh tìm kiếm lớp học. Đối với người dùng Admin, giao diện sẽ được tích hợp thêm tính năng thêm lớp học, sửa thông tin lớp học và xoá lớp học.

The screenshot shows the "Lectures" page of the WORM platform. At the top, there is a navigation bar with tabs: Home, Lectures (highlighted in blue), CTF Challenges, and Labs. The title "Lectures" is centered above a list of course entries. The first entry is titled "One Piece" with a description: "Lorem, ipsum dolor sit amet consectetur adipisicing elit. Labore ullam, minus mollitia quidem quos quo nam commodi ipsum optio et eos ad est delectus expedita repellat quisquam vel? Beatae, provident! Lorem ipsum dolor sit amet consectetur adipisicing... [Read more](#)". Below this entry is the timestamp "2024-09-14 21:27:03" and the author "By LS". The second entry is titled "Hi Hi Hi" with a description: "Lorem, ipsum dolor sit amet consectetur adipisicing elit. Labore ullam, minus mollitia quidem quos quo nam commodi ipsum optio et eos ad est delectus expedita repellat quisquam vel? Beatae, provident! Lorem ipsum dolor sit amet consectetur adipisicing... [Read more](#)". Below this entry is the timestamp "2024-09-14 21:27:03" and the author "By LS". The third entry is titled "He He He" with a description: "Lorem, ipsum dolor sit amet consectetur adipisicing elit. Labore ullam, minus mollitia quidem quos quo nam commodi ipsum optio et eos ad est delectus expedita repellat quisquam vel? Beatae, provident! Lorem ipsum dolor sit amet consectetur adipisicing... [Read more](#)". Below this entry is the timestamp "2024-09-14 21:27:03" and the author "By LS".

Hình 65: Giao diện danh sách lớp học của User.

Lectures

New Lecture + **Search**

One Piece
Lorem, ipsum dolor sit amet consectetur adipisicing elit. Labore ullam, minus mollitia quidem quos quo nam commodi ipsum optio et eos ad est delectus expedita repellat quisquam vel? Beatae, provident! Lorem ipsum dolor sit amet consectetur adipisicing... [Read more](#)

2024-09-14 21:27:03 By LS

Hi Hi Hi
Lorem, ipsum dolor sit amet consectetur adipisicing elit. Labore ullam, minus mollitia quidem quos quo nam commodi ipsum optio et eos ad est delectus expedita repellat quisquam vel? Beatae, provident! Lorem ipsum dolor sit amet consectetur adipisicing... [Read more](#)

2024-09-14 21:27:03 By LS

He He He
Lorem, ipsum dolor sit amet consectetur adipisicing elit. Labore ullam, minus mollitia quidem quos quo nam commodi ipsum optio et eos ad est delectus expedita repellat quisquam vel? Beatae, provident! Lorem ipsum dolor sit amet consectetur adipisicing... [Read more](#)

Hình 66: Giao diện danh sách lớp học của Admin.

Add Lecture

Title:

Description:

Create New Lecture **Cancel**

Hình 67: Giao diện tạo lớp học mới của Admin.

Edit Lecture

Notice: You are editing "**One Piece**"

Title:

Description:

Lorem, ipsum dolor sit amet consectetur adipisicing elit. Labore ullam, minus mollitia quidem quos quo nam commodi ipsum optio et eos ad est delectus expedita repellat quisquam vel? Beatae, provident! Lorem ipsum dolor sit amet consectetur adipisicing elit. Eveniet, repellendus veritatis dolorum, enim esse excepturi quibusdam illo corporis deserunt cumque officiis molestias exercitationem, quis

Edit Lecture **Cancel**

Hình 68: Giao diện sửa thông tin lớp học của Admin.

Bên trong mỗi lớp học sẽ bao gồm một bảng tin với các tin tức được đăng tải từ người dùng Admin. Các tin tức sẽ đóng vai trò là các thông báo từ người đứng lớp (Admin), có thể đính kèm các bài giảng lý thuyết và tài liệu liên quan đến lĩnh vực An toàn thông tin. Phía bên phải bảng tin là một box chat, nơi các người dùng có thể trò chuyện và chia sẻ kiến thức với nhau.

The screenshot shows a user interface for a classroom session titled "One Piece". On the left, there is a "Newsfeed" section with four entries from a user named "LS" (Hung Gay). Each entry includes a timestamp (2024-09-15 10:38:31, 10:38:16, 10:38:14, 10:38:08) and a message body ("d", "dd", "ddd", and "ddd" respectively). On the right, there is a "Boxchat" window showing a conversation between "Hung Gay" and "Trương Đặng Trúc Lâm". The messages include "Hung Gay" at 2024-09-14 21:44:29 ("..."), "Trương Đặng Trúc Lâm" at 2024-09-15 10:37:44 ("aaa"), and "LS" at 2024-09-15 10:38:03 ("monkey"). A "Send message" button is visible in the chat window.

Hình 69: Giao diện bên trong lớp học của User.

The screenshot shows an administrator's interface for a classroom session titled "One Piece". On the left, there is a "Newsfeed" section with four entries from a user named "LS" (Hung Gay). Each entry includes a timestamp (2024-09-15 10:38:31, 10:38:16, 10:38:14, 10:38:08) and a message body ("d", "dd", "ddd", and "ddd" respectively). On the right, there is a "Boxchat" window showing a conversation between "Hung Gay" and "Trương Đặng Trúc Lâm". The messages include "Hung Gay" at 2024-09-14 21:44:29 ("..."), "Trương Đặng Trúc Lâm" at 2024-09-15 10:37:44 ("aaa"), and "LS" at 2024-09-15 10:38:03 ("monkey"). Below the chat window, there is an "Enter message" input field with "Submit" and "Cancel" buttons.

Hình 70: Giao diện bên trong lớp học của Admin.

Tại mục thử thách CTF (Challenges), giao diện sẽ bao gồm các thử thách CTF, một thanh tìm kiếm thử thách theo từ khoá và một bảng Category giúp người dùng tìm kiếm thử thách theo thể loại. Người dùng Admin sẽ có thêm tính năng tạo thử thách CTF mới, sau khi truy cập sẽ tiến hành nhập các thông tin cần thiết nhằm xây dựng thử thách.

The screenshot shows the 'CTF Challenges' section of a web application. At the top, there's a navigation bar with 'Home', 'Lectures', 'CTF Challenges' (which is highlighted in teal), and 'Labs'. A search bar at the top right contains the placeholder 'Search challenges...'. Below the navigation, the title 'CTF Challenges' is displayed. On the left, a sidebar titled 'Category' lists 'All Challenges', 'Reverse Engineering', 'Web Exploitation', 'Binary Exploitation', 'Forensics', and 'Cryptography'. The main area displays a grid of challenges. The first challenge in the grid is 'Red' (Forensics, Solved: 0). Other challenges include 'cc' (Reverse Engineering, Solved: 2), 'aaa' (Reverse Engineering, Solved: 1), 'mongki22' (Reverse Engineering, Solved: 1), 'monkey11' (Reverse Engineering, Solved: 0), 'sheep11' (Forensics, Solved: 0), 'cow11' (Cryptography, Solved: 0), 'dog11' (Binary Exploitation, Solved: 0), and 'mongki11' (Web Exploitation, Solved: 0). Navigation buttons at the bottom include 'First', a left arrow, a page number '1' (highlighted in blue), a right arrow, and 'Last'.

Hình 71: Giao diện các thử thách CTF của User.

This screenshot is similar to Figure 71 but shows the interface from an 'Admin' perspective. It includes an additional 'New Challenge +' button in the top right corner. The rest of the layout, including the sidebar categories and the challenge grid, is identical to the user version.

Hình 72: Giao diện các thử thách CTF của Admin.

This screenshot shows the 'New CTF Challenge' creation form. On the left, a sidebar lists the same categories as the previous screens. The main area has fields for 'Title' (with a placeholder box), 'Description' (with a large text area), 'File' (with a 'Choose File' button and note about file size), 'Key' (with a text input field), and 'Type' (with a dropdown menu set to 'Select Type'). To the right, the title 'New CTF Challenge' is displayed, along with 'Hint:' and another text input field. At the bottom right are 'Create New Challenge' and 'Cancel' buttons.

Hình 73: Giao diện tạo thử thách CTF của Admin.

Khi truy cập vào một thử thách CTF, người dùng có thể xem thêm các thông tin như mô tả và gợi ý, sau đó tải tập tin được đính kèm và tiến hành tìm flag của thử thách. Người dùng Admin sẽ được tích hợp thêm tính năng chỉnh sửa và xoá thử thách.

The screenshot shows a user interface for a CTF challenge. At the top, there is a navigation bar with links for Home, Lectures, CTF Challenges (which is the active tab), and Labs. A search bar and a 'Search' button are also present. On the left, a sidebar titled 'Category' lists various challenge types: All Challenges, Reverse Engineering, Web Exploitation, Binary Exploitation, Forensics, and Cryptography. The main content area displays a challenge titled 'mongki22' under the 'Reverse Engineering' category. It includes a 'Description' section with the text 'This is just for testing function download in Web.' and a 'Download' link. Below the description is a text input field labeled 'Enter the key...' and a 'Submit' button. To the right of the challenge title is a 'Hint' button with the text 'Open the eye'. At the bottom right of the challenge card are 'WORMS' and 'Close' buttons.

Hình 74: Giao diện bên trong thử thách của User.

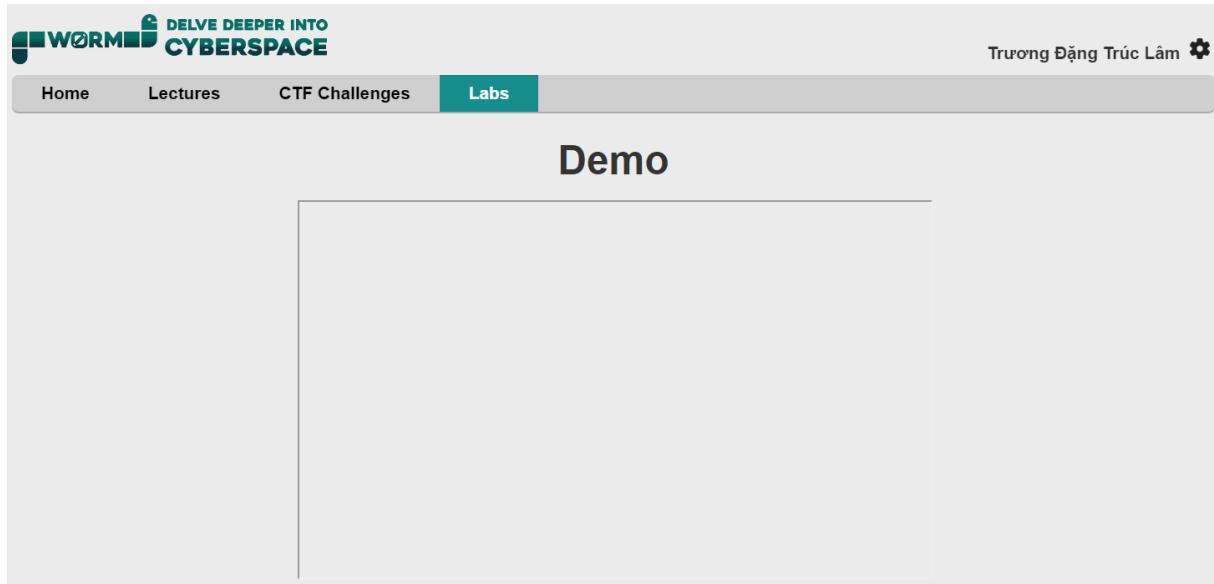
This screenshot shows the same CTF challenge 'mongki22' from the admin perspective. The layout is identical to the user interface, but the 'Edit Mode' button is visible at the bottom right of the challenge card. The 'Hint' button is replaced by a 'Show Hint' link. The 'Close' button is also present at the bottom right.

Hình 75: Giao diện bên trong thử thách của Admin.

This screenshot shows the 'Edit Mode' interface for the challenge 'mongki22'. The challenge details are displayed: Title ('mongki22'), Description ('This is just for testing function download in Web.'), and Type ('Reverse Engineering'). The 'Edit Mode' button is at the top right. The 'File' field shows 'Current File' and 'No file chosen'. The 'Key' field contains 'thekey'. At the bottom are 'Confirm', 'Cancel', and 'Delete' buttons.

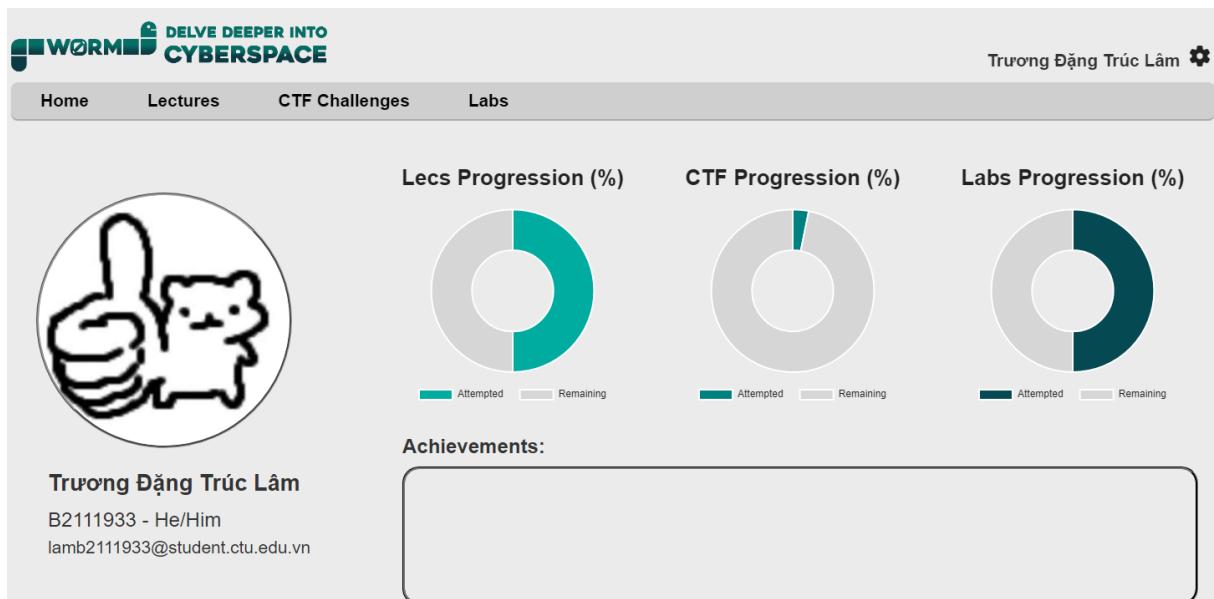
Hình 76: Giao diện chế độ chỉnh sửa thử thách của Admin.

Đối với bài thực hành kiểm thử bảo mật (Labs), do chỉ xây dựng duy nhất một bài tập thử nghiệm nên nhóm sẽ không thiết kế cơ sở dữ liệu và không phân quyền Admin cho mục này. Nhóm sẽ thiết kế một bảng điều khiển màn hình từ trang web dành cho máy ảo tấn công, tương tự như mục Console trên giao diện web (Horizon) của OpenStack.



Hình 77: Giao diện bài tập thực hành kiểm thử bảo mật.

Bên cạnh đó, nhóm còn thiết kế trang cá nhân (Profile) cho mỗi người dùng với các thông tin như họ và tên, tên tài khoản, giới tính, địa chỉ email và ảnh đại diện. Trang cá nhân còn tích hợp thư viện Chart.js [30] nhằm hiển thị tiến độ hoàn thành các nội dung dưới dạng biểu đồ.



Hình 78: Giao diện trang cá nhân của mỗi người dùng.

Để góp phần hoàn thiện ứng dụng web trong tương lai, nhóm đã thiết kế thêm tính năng đóng góp ý kiến (Comments) dành cho User, người dùng Admin khi truy cập có thể xem được những góp ý đến từ các User đã trải nghiệm ứng dụng.

The screenshot shows a comment submission form on the website. At the top, there is a logo for "WORMS DELVE DEEPER INTO CYBERSPACE". The navigation bar includes links for Home, Lectures, CTF Challenges, and Labs. A user profile for "Trương Đặng Trúc Lâm" is visible on the right. The main content area contains a placeholder text "Please give your comments to help us enhance our website". Below it, a text input field is labeled "From Trương Đặng Trúc Lâm - B2111933:" followed by a text area with a character limit of "(max 500 letters)". At the bottom of the form are two buttons: "Submit" and "Clear".

Hình 79: Giao diện dành cho User gửi đóng góp ý kiến.

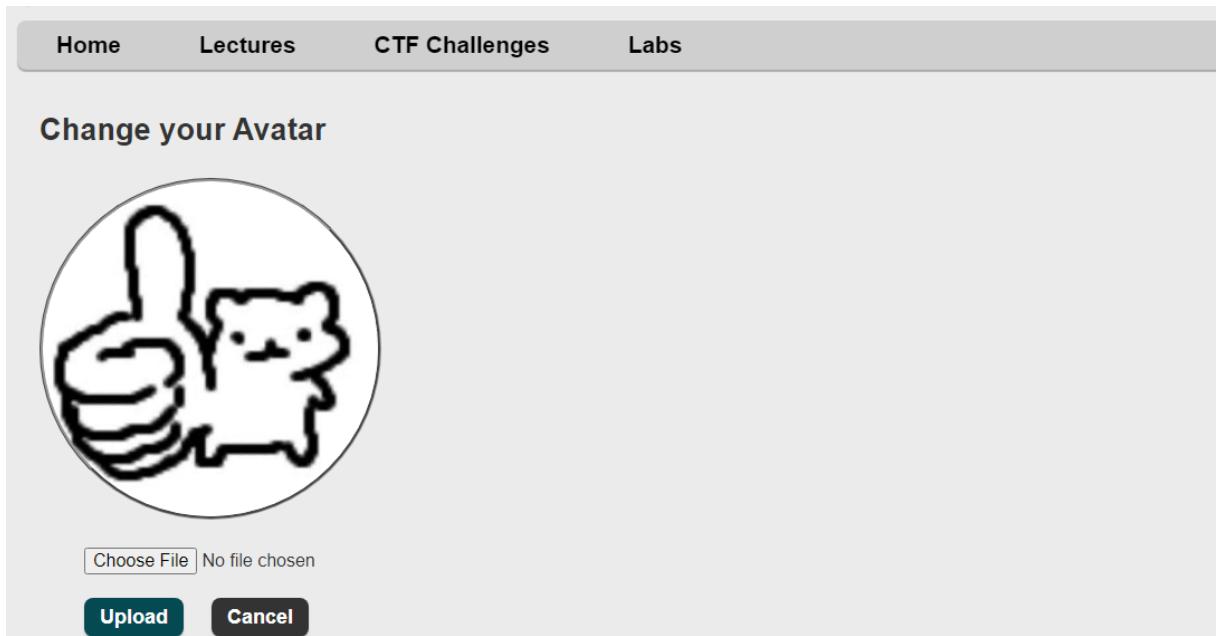
The screenshot shows a list of comments from users. The navigation bar and user profile are identical to the previous screenshot. The main content area displays several comments with their senders and timestamps. The first comment is from "mongki" at 2024-04-30 13:37:19. The second comment is from "B3333333 - LS" at 2024-04-30 13:37:19, containing a long string of characters. The third comment is from "cow" at 2024-04-30 13:37:18. The fourth comment is from "dog" at 2024-04-30 13:37:18.

Hình 80: Giao diện dành cho Admin xem các góp ý từ User.

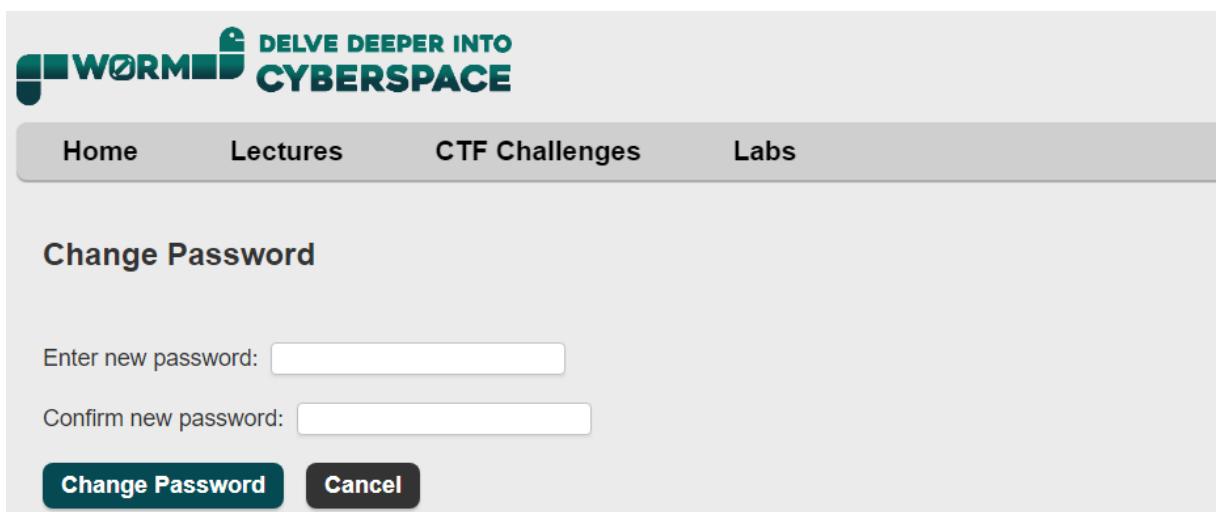
Cuối cùng là giao diện cài đặt (Settings), nơi người dùng có thể thiết lập các cài đặt cho tài khoản như cập nhật ảnh đại diện, thay đổi mật khẩu và tùy chỉnh chế độ sáng/tối.

The screenshot shows the "Settings" page. The navigation bar and user profile are consistent with the previous screenshots. On the left, there is a heading "Settings:". Below it, there are three items: "Change Avatar: [Edit](#)", "Change password: [Edit](#)", and "Switch to Dark Mode 🌙". On the right, there is a vertical menu with options: Profile, Comments, Settings (which is highlighted in blue), and Log Out. The "Settings" option in the menu has a small gear icon next to it.

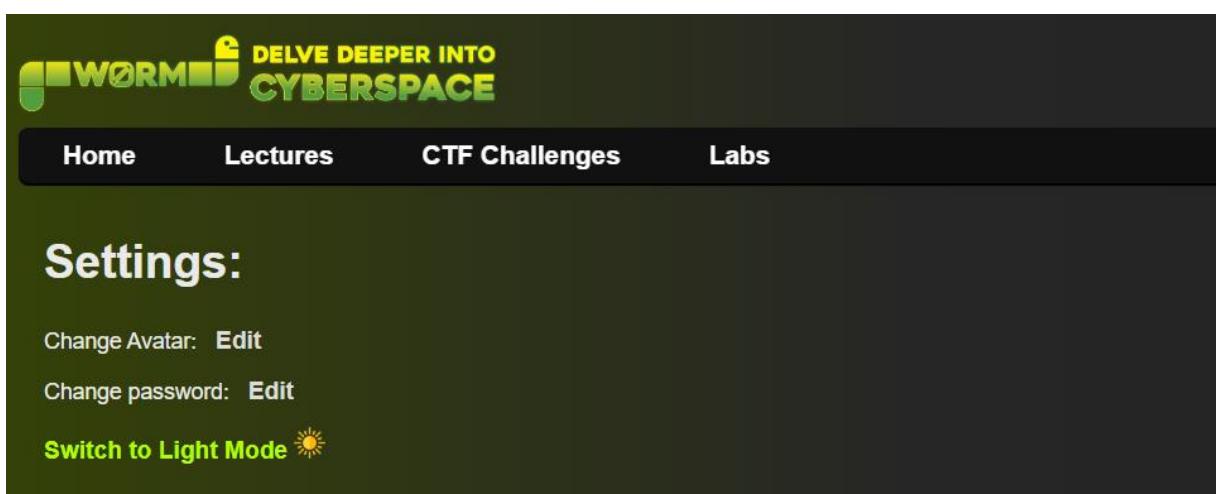
Hình 81: Giao diện cài đặt.



Hình 82: Giao diện cài đặt ảnh đại diện.



Hình 83: Giao diện đổi mật khẩu.



Hình 84: Chế độ sáng/tối.

The screenshot shows the WORM website's homepage in dark mode. At the top, there is a navigation bar with links for Home, Lectures, CTF Challenges, and Labs. The main title "WORM - Training with Cyberspace" is centered above a large image of a computer monitor displaying the WORM logo and the word "CTF". To the right of the monitor, there is a section titled "WHAT IS CTF?" with a brief description of what CTF is. Below the monitor, there is another section titled "WHAT IS WORM?" with a brief description of the project and a small icon of a shield and a cloud.

Hình 85: Trang chủ với chế độ tối.

The screenshot shows a user profile page in dark mode. It features a circular profile picture of a cat. To the right of the picture are three donut charts showing progression: "Lecs Progression (%)", "CTF Progression (%)", and "Labs Progression (%)". Each chart has two segments: "Attempted" (green) and "Remaining" (white). Below the charts is a section titled "Achievements" which contains a large empty rectangular box. On the left side of the profile area, there is a "Truong Dang Truc Lam" profile card with information: B2111933 - He/Him and lamb2111933@student.ctu.edu.vn.

Hình 86: Trang cá nhân với chế độ tối.

The screenshot shows a lecture page in dark mode. The top navigation bar includes a "Lectures" tab which is highlighted in yellow. The main content area is titled "Lectures" and contains two entries: "One Piece" and "Hi Hi Hi". Each entry has a short description, a timestamp (2024-09-14 21:27:03), and a "By LS" link at the bottom. There is also a search bar and a "Search" button at the top right of the content area.

Hình 87: Các lớp học với chế độ tối.

Hình 88: Các thử thách CTF với chế độ tối.

Hình 89: Các góp ý từ người dùng được xem với chế độ tối.

3.2. Kết nối đến bài tập kiểm thử bảo mật

Đối với bài tập kiểm thử bảo mật, ta cần thực hiện kết nối đến máy ảo tấn công được xây dựng trên nền tảng OpenStack. Nhóm nhận thấy chức năng Console trên giao diện Horizon của OpenStack đã kết nối đến các máy ảo thông qua công nghệ VNC [31].

Qua quá trình nghiên cứu và tìm kiếm các tài liệu có liên quan, nhóm lựa chọn sử dụng PHP OpenStack SDK [32]. Bộ công cụ này đóng vai trò như một lớp trung gian, giúp ứng dụng PHP giao tiếp với các API của OpenStack mà không cần phải viết các yêu cầu HTTP phức tạp. Đặc biệt PHP OpenStack SDK còn tích hợp công nghệ VNC giúp người dùng tương tác với các máy ảo trên nền tảng OpenStack, thông qua một bảng điều khiển màn hình, tương tự như chức năng Console của OpenStack Horizon.

k0ka	return unmaintained openstack versions into ci (#408)	...	✓	e32dcf1 · 5 months ago	820 Commits
.github/workflows	return unmaintained openstack versions into ci (#408)			5 months ago	
doc	fix doc links (#402)			7 months ago	
samples	add docs for volume attachment (#401)			7 months ago	
src	make swift metadata header case insensitive (#407)			6 months ago	
tests	make swift metadata header case insensitive (#407)			6 months ago	
.gitattributes	Move integration tests to phputil (#387)			8 months ago	
.gitignore	Unit test (#360)			last year	
.php-cs-fixer.dist.php	Chores (#379)			8 months ago	
.readthedocs.yaml	Restore read the docs (#371)			9 months ago	

Hình 90: Mã nguồn PHP OpenStack SDK trên GitHub.

Truy cập đến nội dung tập tin README tại kho lưu trữ PHP OpenStack SDK trên GitHub, ta có thể xem hướng dẫn cài đặt PHP OpenStack SDK cho ứng dụng web. Được biết, SDK này sử dụng curl để giao tiếp với các dịch vụ trên OpenStack và điều kiện cần thiết là phiên bản PHP phải mới hơn PHP 7.2.5. Sau khi thoả các điều kiện trên, ta cần cài đặt thư viện này với Composer [33].

Upgrade from 2.x to 3.x

Due to new `object typehint` since PHP 7.2, `Object` is a reserved keyword thus class `OpenStack\ObjectStore\v1\Models\Object` had to be renamed to `OpenStack\ObjectStore\v1\Models\StorageObject`.

This change was introduced in [#184](#).

Requirements

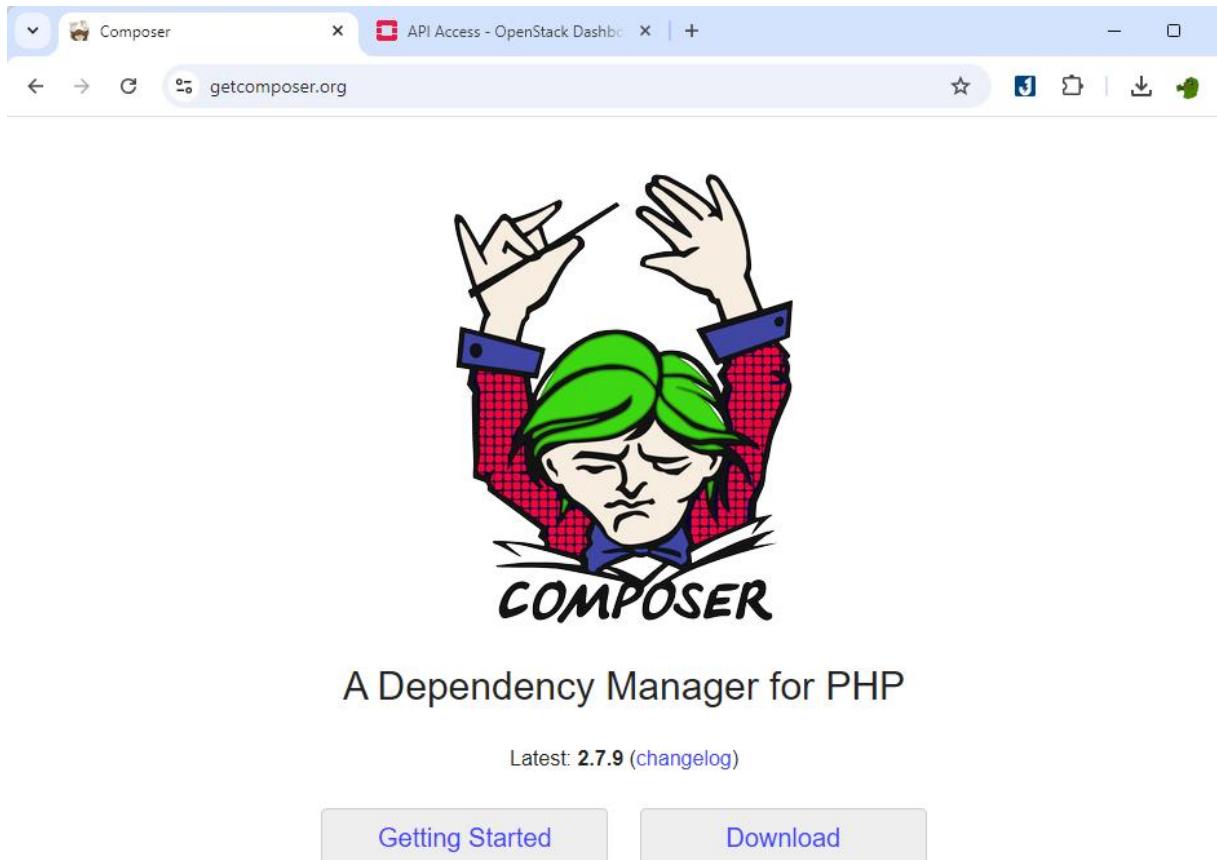
- PHP >= 7.2.5
- `ext-curl`

How to install

```
composer require php-opencloud/openstack
```

Hình 91: Tập tin README hướng dẫn cài đặt PHP OpenStack SDK.

Composer là một công cụ quản lý phụ thuộc (dependency manager) phục vụ cho việc phát triển ứng dụng PHP. Composer cho phép ta khai báo các thư viện mà dự án cần sử dụng, và khi ấy Composer sẽ tự động tải về, cài đặt và quản lý các thư viện đó. Ta có thể truy cập đến trang chủ của Composer và tiến hành cài đặt.



Hình 92: Cài đặt Composer.

Sau khi cài đặt Composer, ta truy cập đến thư mục chứa mã nguồn của ứng dụng web, mở một cửa sổ dòng lệnh và nhập vào lệnh sau:

```
$ composer require php-opencloud/openstack
```

A screenshot of a terminal window. At the top, there are tabs for 'PROBLEMS', 'OUTPUT', 'PORTS', 'DEBUG CONSOLE', 'TERMINAL' (which is underlined), 'POSTMAN CONSOLE', and 'COMMENTS'. The main area of the terminal shows a command prompt: 'PS F:\XAMPP\htdocs\W0rm>'. Below the prompt, the command 'composer require php-opencloud/openstack' is typed and highlighted with a cursor. The background of the terminal window is dark.

Hình 93: Cài đặt PHP OpenStack SDK thông qua Composer.

Sau khi cài đặt thành công, ta có thể truy cập thư mục vendor để kiểm tra các tài nguyên có trong thư viện. Ta có thể tham khảo những mã nguồn phục vụ cho việc thực hiện giao tiếp với các dịch vụ OpenStack, bao gồm tạo máy ảo, xoá máy ảo, liệt kê máy ảo, liệt kê tài khoản, cấu hình mạng,...

Name	Date modified	Type	Size
get_server_rdp_console	8/15/2024 5:44 PM	PHP Source File	1 KB
get_server_serial_console	8/15/2024 5:44 PM	PHP Source File	1 KB
get_server_spice_console	8/15/2024 5:44 PM	PHP Source File	1 KB
<input checked="" type="checkbox"/> get_server_vnc_console	8/15/2024 5:44 PM	PHP Source File	1 KB
list	8/15/2024 5:44 PM	PHP Source File	1 KB
list_security_groups	8/15/2024 5:44 PM	PHP Source File	1 KB

Hình 94: Các mã nguồn tham khảo.

Ta truy cập đến tập tin `get_server_vnc_console` và lấy mã nguồn, với mục tiêu kết nối đến máy ảo trên nền tảng OpenStack thông qua VNC Console. Ta cần tìm kiếm các thông tin cần thiết như:

- Authentication URL
- Region
- Tài khoản và mật khẩu người dùng OpenStack
- ID của Project
- IDs của các máy ảo

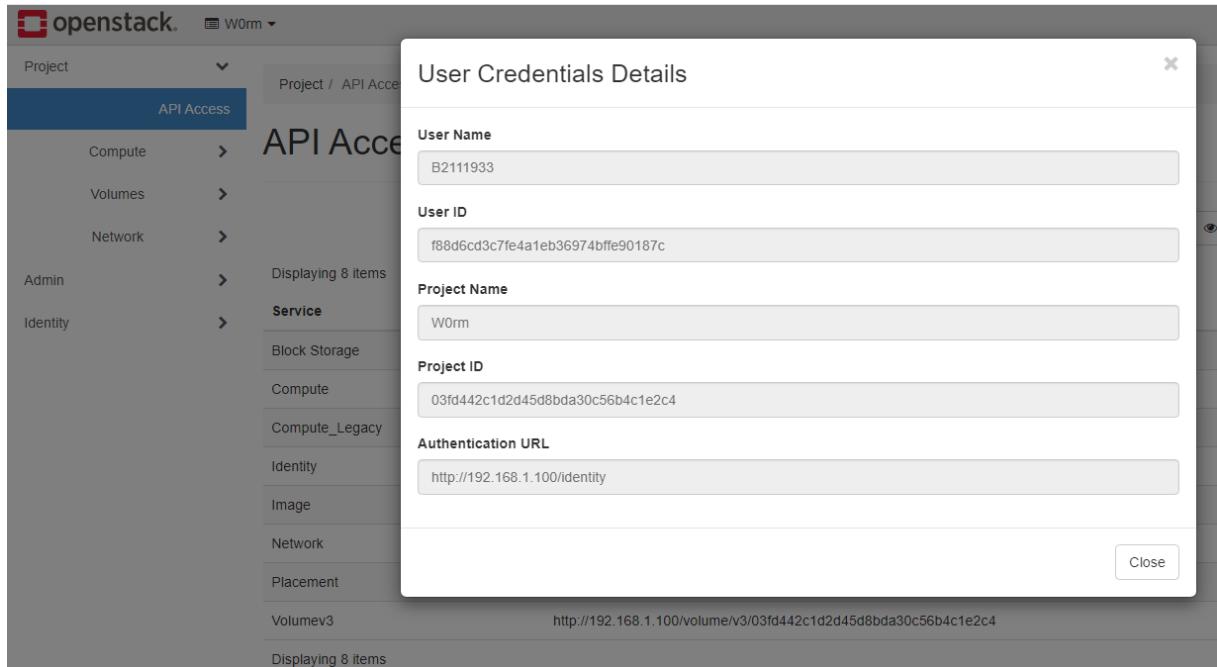
```

1 <?php
2
3 require 'vendor/autoload.php';
4
5 $openstack = new OpenStack\OpenStack([
6     'authUrl' => '{authUrl}',
7     'region' => '{region}',
8     'user' => [
9         'id' => '{userId}',
10        'password' => '{password}'
11    ],
12    'scope' => ['project' => ['id' => '{projectId}']]
13 ]);
14
15 $compute = $openstack->computeV2(['region' => '{region}']);
16
17 $server = $compute->getServer(['id' => '{serverId}']);
18
19 $console = $server->getVncConsole();

```

Hình 95: Cấu hình kết nối đến máy ảo trên OpenStack với VNC.

Ta có thể sử dụng giao diện web (Horizon) của OpenStack để tìm kiếm các thông tin trên. Trước tiên ta truy cập đến API Access và chọn View Credentials, ta sẽ có được Authentication URL và ID của Project.



Hình 96: Authentication URL kết nối đến OpenStack.

Tại các máy ảo có trong mục Instances, ta có thể xem được ID của từng máy ảo.

A screenshot of the Kali Linux instance details page. At the top, the breadcrumb navigation shows 'Project / Compute / Instances / Kali Linux'. Below it is the instance name 'Kali Linux'. There are five tabs: Overview (selected), Interfaces, Log, Console, and Action Log. Under the Overview tab, there are four data rows: 'Name' (Kali Linux), 'ID' (1e5ac608-0e84-474f-8515-4c1f28120b5d), 'Description' (-), and 'Project ID' (03fd442c1d2d45d8bda30c56b4c1e2c4).

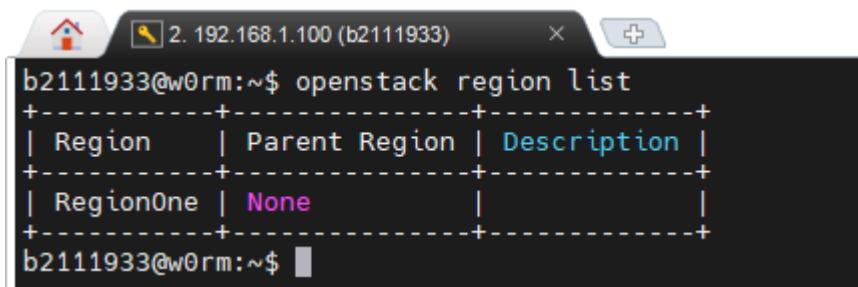
Hình 97: ID của máy ảo tấn công.

CirrOS

Overview	Interfaces	Log	Console	Action Log
Name	CirrOS			
ID	ad966429-a074-418f-a4e4-61943efd2ec0			
Description	-			
Project ID	03fd442c1d2d45d8bda30c56b4c1e2c4			

Hình 98: ID của máy ảo phòng thủ.

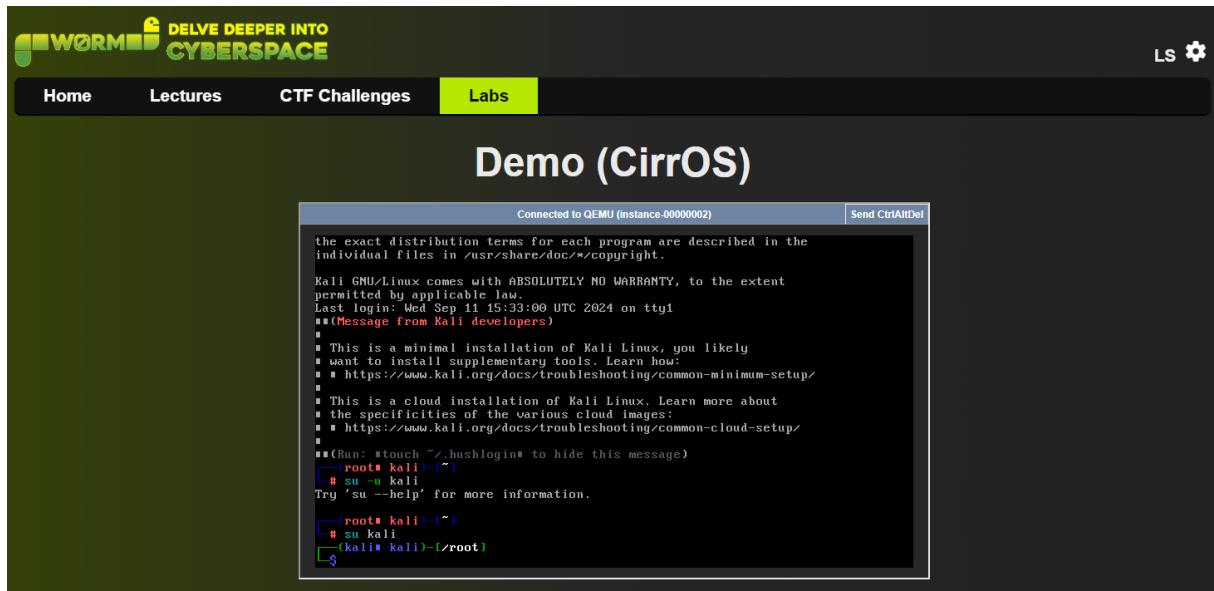
Để tìm kiếm thông tin Region, ta có thể tra khảo thông qua cửa sổ dòng lệnh.



```
b2111933@w0rm:~$ openstack region list
+-----+-----+-----+
| Region | Parent Region | Description |
+-----+-----+-----+
| RegionOne | None | |
+-----+-----+-----+
b2111933@w0rm:~$
```

Hình 99: Region của OpenStack.

Sau khi thu thập đầy đủ thông tin, ta tiến hành cấu hình kết nối dựa trên mã nguồn mẫu. Vậy là ta đã có thể thiết lập kết nối đến máy ảo tấn công trên nền tảng OpenStack từ ứng dụng web. Sau khi xây dựng trang web dành cho bài tập kiểm thử bảo mật, ta tiến hành kiểm tra kết quả.



Hình 100: Kết nối đến máy ảo tấn công từ ứng dụng web.

CHƯƠNG 5: ĐÁNH GIÁ KIỂM THỬ

1. Đánh giá kiểm thử nền tảng OpenStack

Qua thời gian nghiên cứu, nhóm nhận thấy nền tảng OpenStack được xây dựng trên Ubuntu Server hoạt động tương đối ổn định và hiệu quả. Nhờ có sự hỗ trợ của cộng đồng phát triển mạnh mẽ, các chức năng cốt lõi như quản lý máy ảo, cấu hình mạng và quản lý quyền truy cập luôn được cập nhật và nâng cấp thường xuyên, đảm bảo hoạt động trơn tru và không gặp nhiều lỗi.

Về yêu cầu tài nguyên cho phần cứng, nghiên cứu đã chứng minh rằng, ta có thể xây dựng một bài tập thực hành kiểm thử bảo mật trên nền tảng OpenStack chỉ với một chiếc máy tính cá nhân thông thường. Cấu hình yêu cầu cho máy chủ ở mục cài đặt giải pháp là không quá đáng kể (Memory: 9G, Processors: 6 CPUs, Hard Disk: 50G). Tuy nhiên, đối với cấu hình như trên, hệ thống đôi khi sẽ gặp phải tình trạng tràn Memory trong quá trình khởi động máy ảo. Tình trạng này sẽ được khắc phục nếu đề tài được thực hiện trên một máy chủ thực tế.

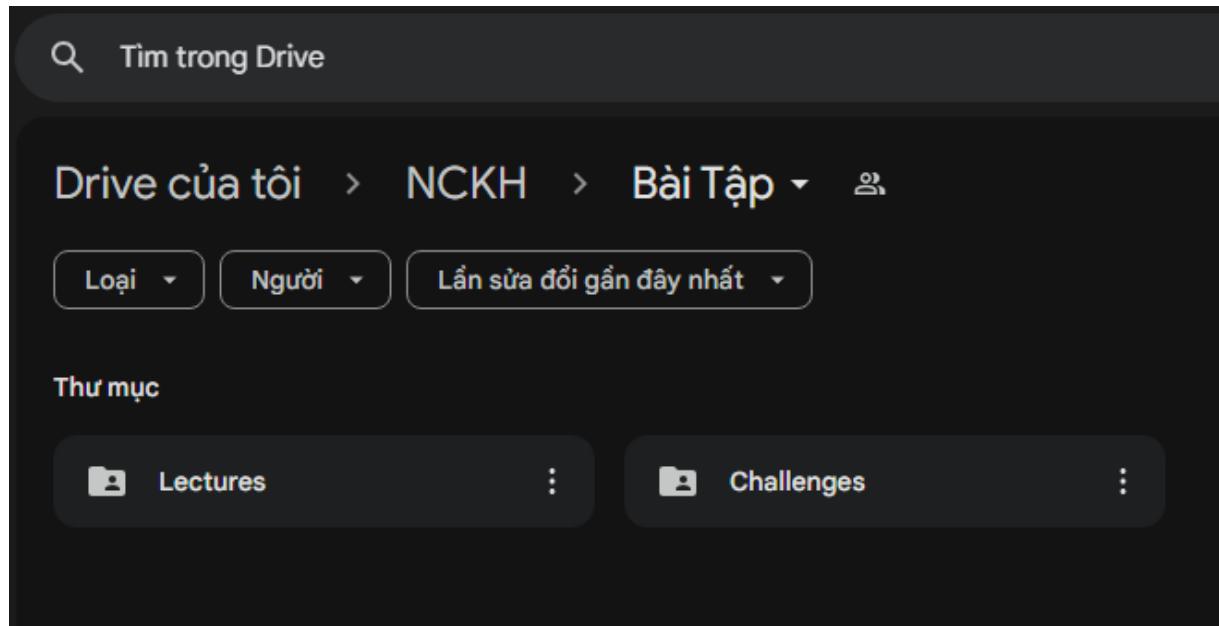
Về vấn đề truyền tải dữ liệu mạng, môi trường điện toán đám mây này sẽ được kết nối với thế giới bên ngoài thông qua nhánh mạng public. Mặc dù hoạt động trong môi trường ảo hóa, các máy ảo trên nền tảng OpenStack vẫn duy trì được tốc độ truyền tải dữ liệu ổn định, không khác biệt đáng kể so với các máy vật lý. Tuy nhiên, hiệu suất truyền tải dữ liệu có thể bị ảnh hưởng bởi nhiều yếu tố như băng thông mạng, độ trễ, jitter và mất gói tin trên mạng public.

Về tính bảo mật và an toàn của dữ liệu, OpenStack đã thiết lập một hệ thống quản lý quyền truy cập chặt chẽ thông qua việc xác thực danh tính người dùng, cấp phát token và quản lý các vai trò, quyền hạn truy cập vào các tài nguyên của hệ thống. Ngoài ra, OpenStack còn cung cấp các tính năng bảo mật khác như mã hóa dữ liệu khi lưu trữ và truyền tải, tường lửa ảo để ngăn chặn các cuộc tấn công từ bên ngoài. Nhờ đó, mỗi người dùng chỉ có thể thực hiện các thao tác được phép trên các đối tượng mà họ được phân quyền, giúp ngăn chặn các hành vi truy cập trái phép và bảo vệ dữ liệu khỏi bị rò rỉ.

Mặc dù OpenStack mang lại nhiều lợi ích, nhưng vẫn còn một số hạn chế cần được giải quyết, đặc biệt là về hiệu suất khi xử lý các tải trọng lớn và phức tạp. Việc tối ưu hóa cấu hình hệ thống và lựa chọn các công cụ phù hợp sẽ giúp khắc phục những hạn chế trên. Nghiên cứu này chỉ là bước đầu tiên trong việc khám phá tiềm năng của OpenStack. Để đánh giá toàn diện hơn về hiệu quả của nền tảng này, cần tiến hành các thử nghiệm sâu hơn trong các môi trường thực tế khác nhau.

2. Đánh giá kiểm thử ứng dụng web

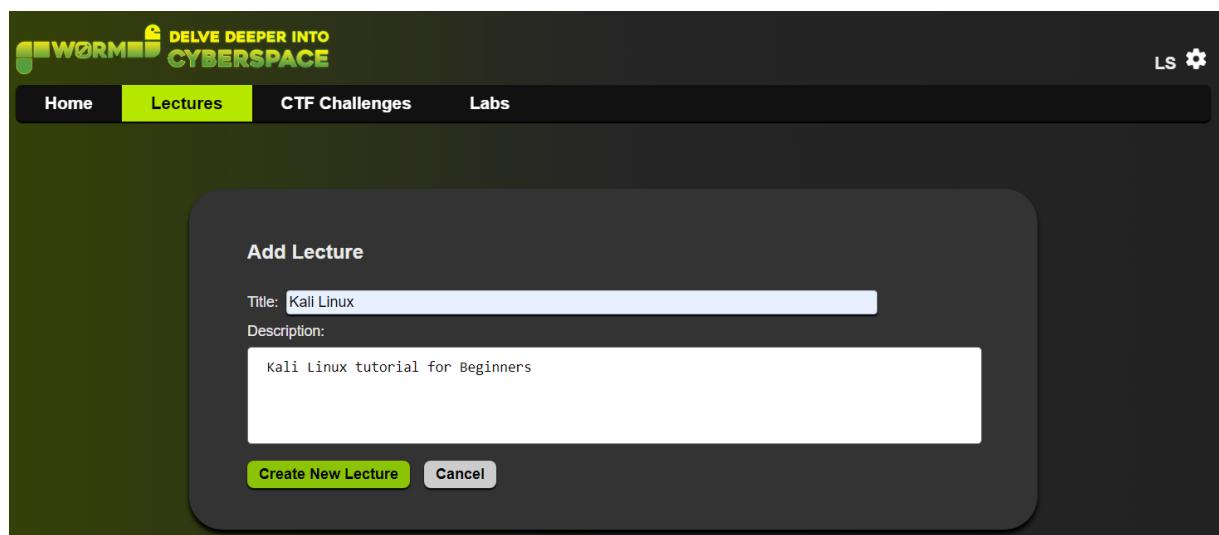
Sau khi thiết kế các giao diện web một cách tổng quát, nhóm tiến hành thực hiện việc triển khai các bài giảng lý thuyết và bài tập thực hành An toàn thông tin lên ứng dụng web. Các tài nguyên sẽ tạm thời được lưu trữ trong một thư mục Google Drive.



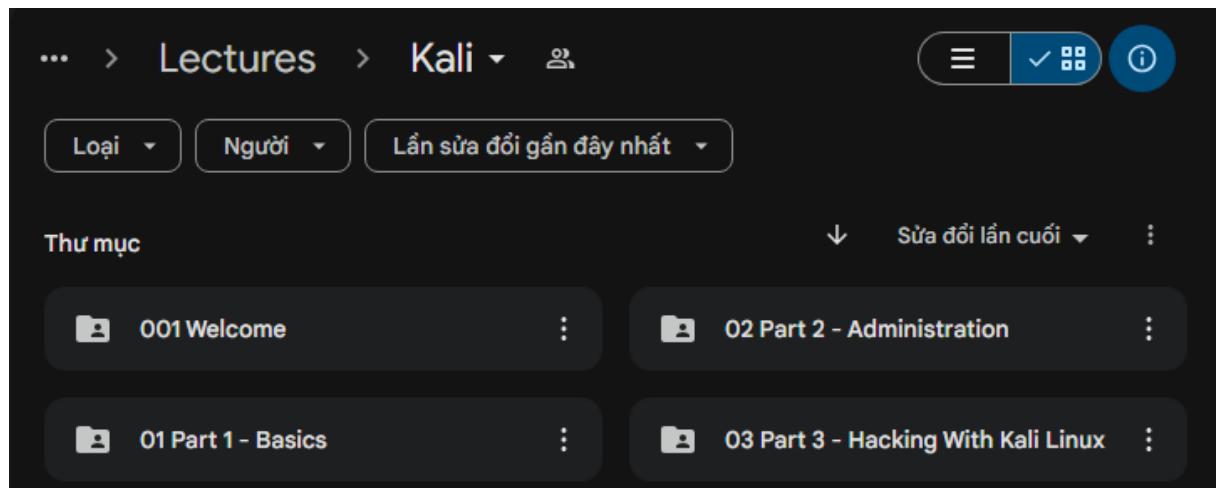
Hình 101: Thư mục lưu trữ các bài giảng và bài tập An toàn thông tin.

2.1. Đánh giá kiểm thử các lớp học lý thuyết

Người dùng quản trị (Admin) có thể tạo ra các lớp học lý thuyết và gửi tin tức đến các học viên. Nội dung trên bảng tin có thể được đính kèm các tài liệu từ bên ngoài. Trong bài nghiên cứu này, nhóm sẽ tiến hành đánh giá kiểm thử đối với việc triển khai một lớp học hướng dẫn sử dụng Kali Linux cho người mới bắt đầu.



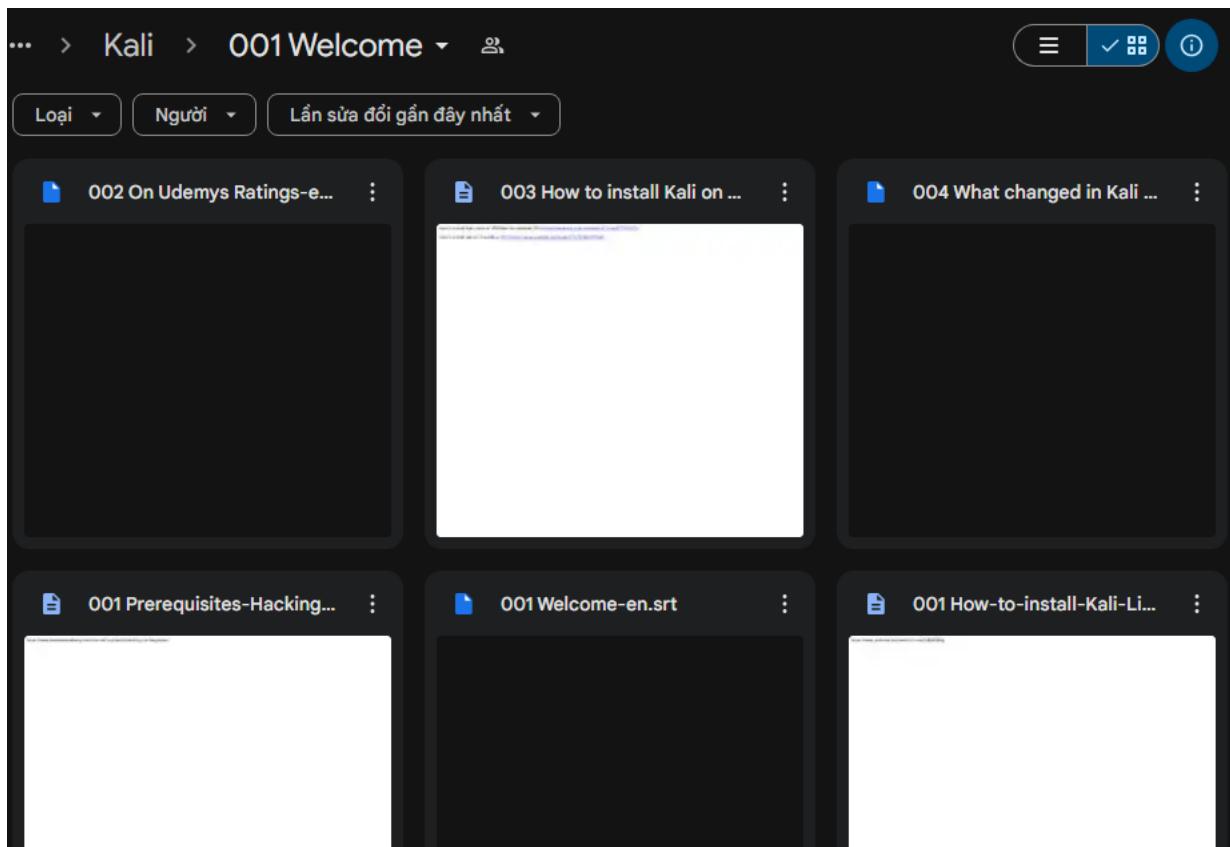
Hình 102: Tạo lớp học mới.



Hình 103: Các tài liệu liên quan đến lớp học.

Hình 104: Tạo một tin tức gửi đến lớp học

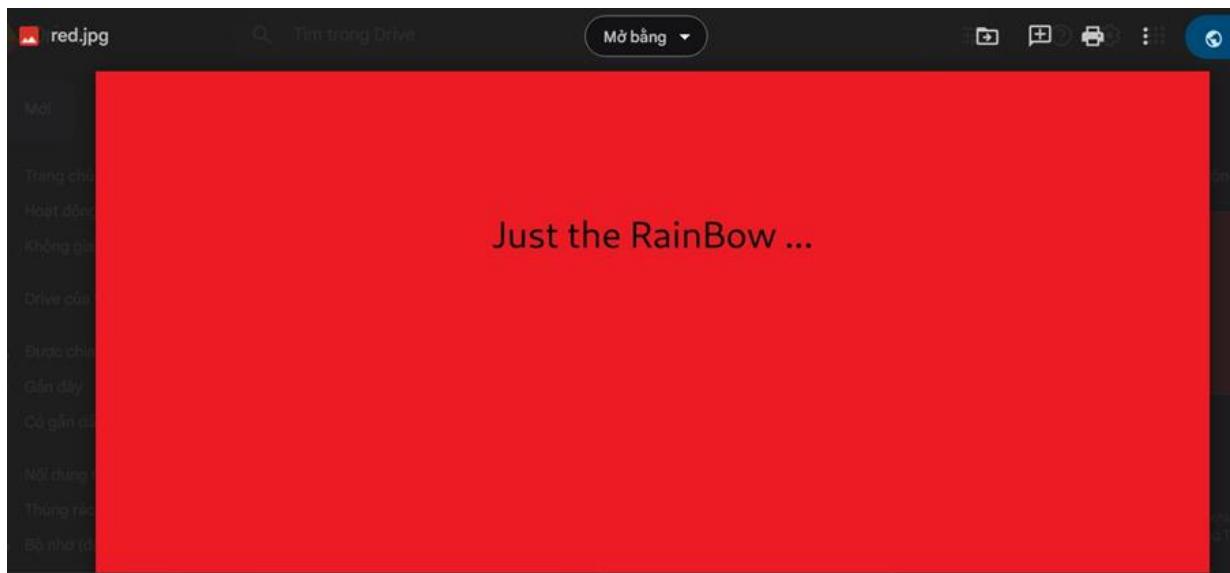
Hình 105: Bảng tin lớp học đã được cập nhật.



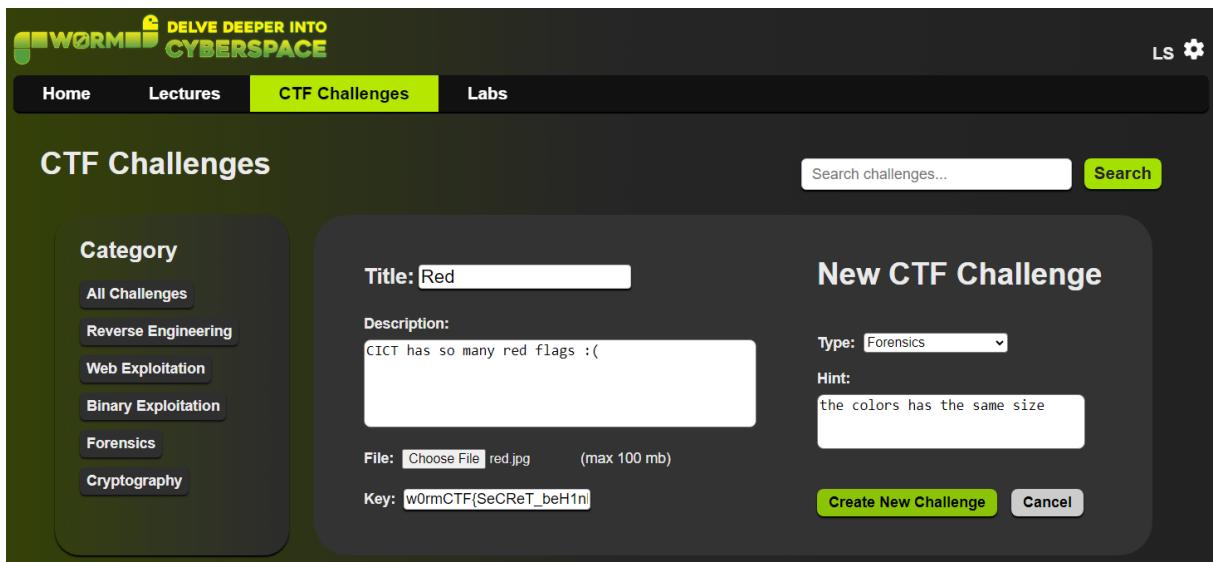
Hình 106: Sau khi truy cập đến đường liên kết.

2.2. Đánh giá kiểm thử các thử thách CTF

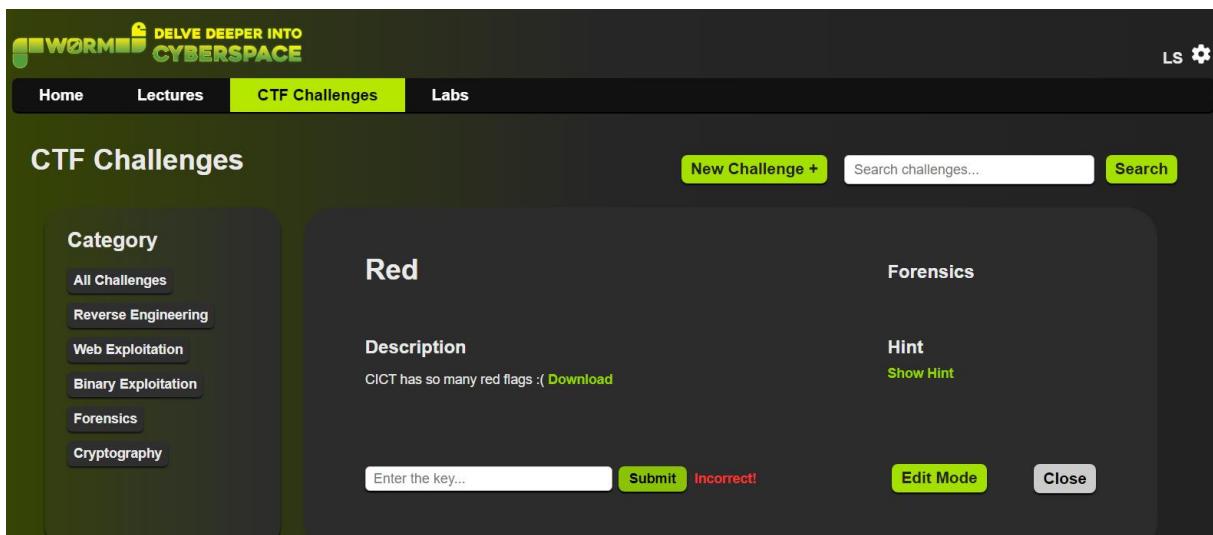
Tương tự các lớp học lý thuyết, người dùng quản trị (Admin) có thể xây dựng các thử thách CTF dành cho học viên. Nhóm sẽ trình bày việc triển khai một thử thách thuộc thể loại Forensics trong hình thức thi Jeopardy và tiến hành đánh giá kiểm thử.



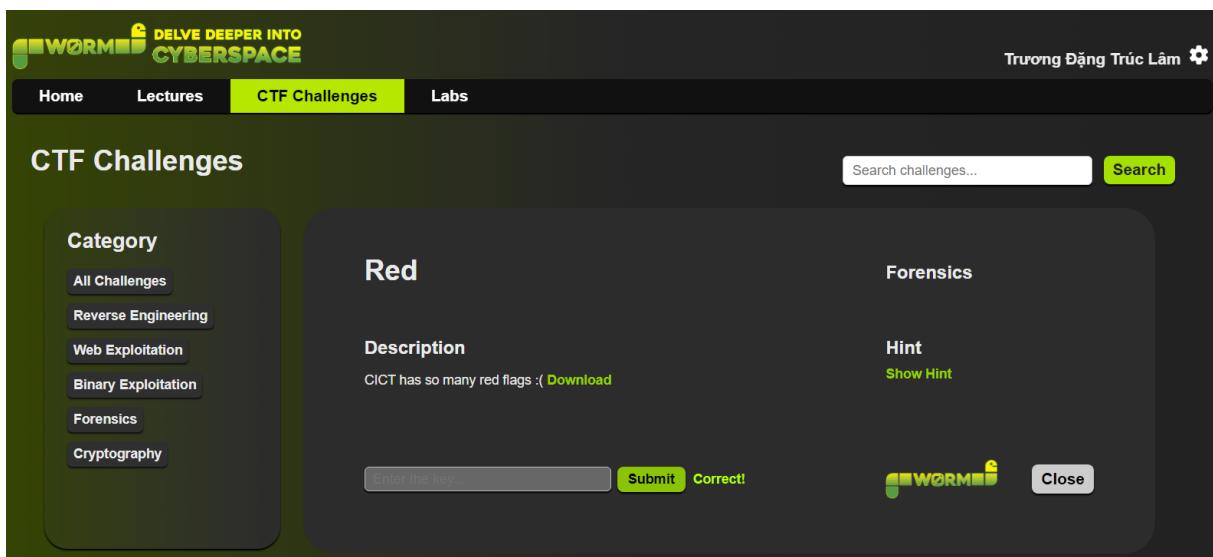
Hình 107: Tập tin chứa flag của thử thách.



Hình 108: Xây dựng thử thách CTF.



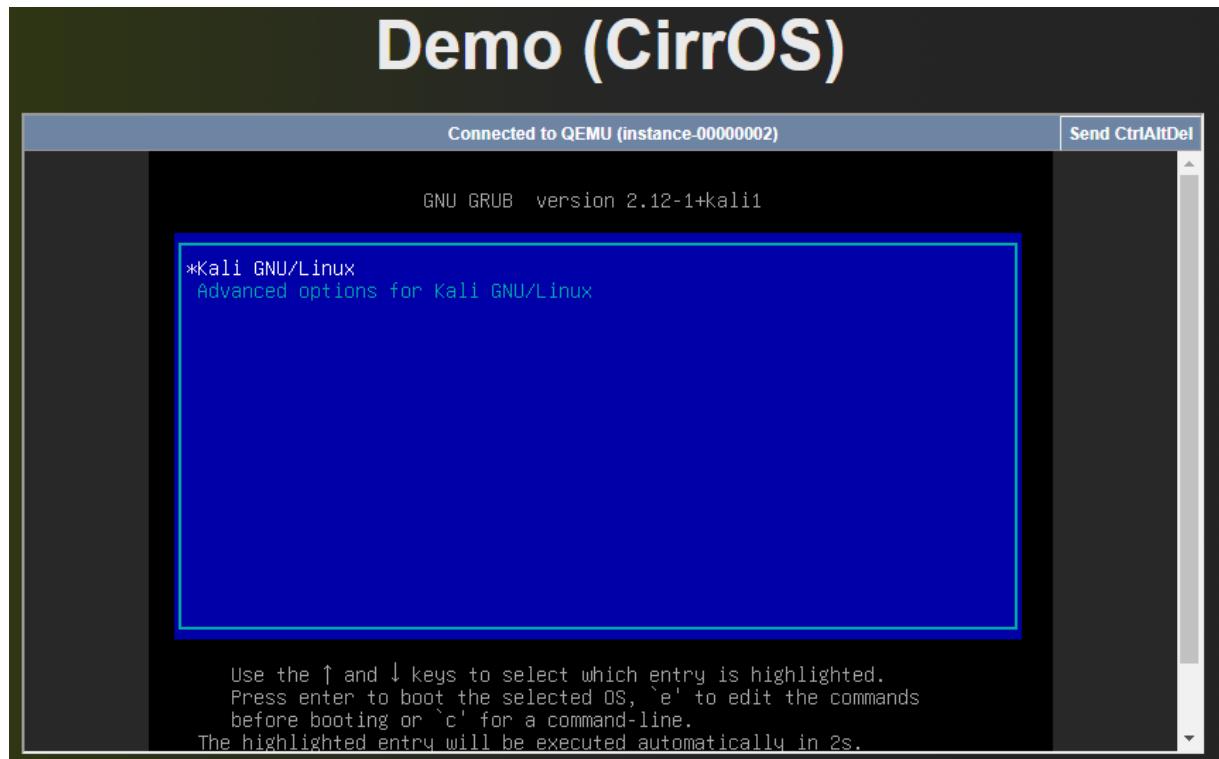
Hình 109: Thử thách CTF sau khi nhập kết quả sai.



Hình 110: Thử thách CTF sau khi nhập kết quả đúng.

2.3. Đánh giá kiểm thử bài tập kiểm thử bảo mật

Đối với bài tập thực hành kiểm thử bảo mật trên ứng dụng web, người dùng sẽ được kết nối đến màn hình của máy ảo Kali Linux thông qua một bảng điều khiển VNC. Giao thức VNC được thiết kế dựa trên ý tưởng của Remote Frame Buffer (RFB). Giao thức này chịu trách nhiệm truyền tải hình ảnh và đầu vào từ các thiết bị ngoại vi giữa máy chủ và máy khách. Nhóm sẽ tiến hành đánh giá kiểm thử bài tập thực hành trên.



Hình 111: Kết nối đến bài tập kiểm thử bảo mật từ ứng dụng web.

A screenshot of a VNC session titled "Connected to QEMU (instance-00000002)". The main window shows a terminal window with a series of messages. It starts with a message about a minimal installation of Kali Linux, followed by information about a cloud installation. Then, it shows a ping command being run to github.com. The terminal output includes the command "ping -c5 github.com", the results of five ping packets (ranging from 23.8 ms to 24.2 ms), and the final statistics: 5 packets transmitted, 5 received, 0% packet loss, time 4009ms, and rtt min/avg/max/mdev = 23.589/23.867/24.152/0.189 ms. The terminal prompt ends with a dollar sign (\$).

Hình 112: Kiểm tra kết nối mạng của bài tập từ ứng dụng web.

```

Connected to QEMU (instance-00000002) Send CtrlAltDel

└─(kali㉿kali)-[~]
$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.1 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.1 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [110 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [268 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [875 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [1 0.8 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [22.8 kB]
94% [3 Contents-amd64 store 0 B] 8996 kB/s 0s

```

Hình 113: Cập nhật các gói tin apt của máy ảo tấn công từ ứng dụng web.

```

Connected to QEMU (instance-00000002) Send CtrlAltDel

Setting up libcryptsetup12:amd64 (2:2.7.5-1) ...
Setting up libssh2-1t64:amd64 (1.11.0-7) ...
Setting up openssl (3.3.2-1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5+b1) ...
Setting up systemd-cryptsetup (256.5-1) ...
Setting up nmap (7.94+git20230807.3be01efb1+dfsg-4kali2) ...
Setcap worked! Adding configuration to environment
Processing triggers for shared-mime-info (2.4-1) ...
Processing triggers for initramfs-tools (0.142) ...
update-initramfs: Generating /boot/initrd.img-6.6.9-cloud-amd64
W: No zstd in /usr/bin:/sbin:/bin, using gzip
Processing triggers for libc-bin (2.40-2) ...
Processing triggers for dbus (1.14.10-4) ...

└─(kali㉿kali)-[~]
$ nmap --version
Nmap version 7.94SUN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.3.2 libssh2-1.11.0 libz-1.3.1 libpcre2-10.42 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

└─(kali㉿kali)-[~]
$ 

```

Hình 114: Cài đặt công cụ Nmap lên máy ảo tấn công từ ứng dụng web.

```

Connected to QEMU (instance-00000002) Send CtrlAltDel

└─(kali㉿kali)-[~]
$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc fq_codel state UP group default qlen 1000
    link/ether fa:16:3e:d7:f8:1e brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.226/24 brd 10.0.1.255 scope global dynamic eth0
        valid_lft 42118sec preferred_lft 42118sec
        inet6 fe80::f816:3eff:fed7:f81e/64 scope link proto kernel ll
            valid_lft forever preferred_lft forever

└─(kali㉿kali)-[~]
$ 

```

Hình 115: Kiểm tra cấu hình mạng của máy ảo tấn công từ ứng dụng web.

```

Nmap scan report for 10.0.1.184
Host is up (0.00088s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    closed http
443/tcp   closed https
MAC Address: FA:16:3E:D1:9C:B3 (Unknown)

Nmap scan report for 10.0.1.226
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.0.1.226 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.20 seconds

[~] $(kali㉿kali)-[~]
$ nmap -n 10.0.1.0/24

```

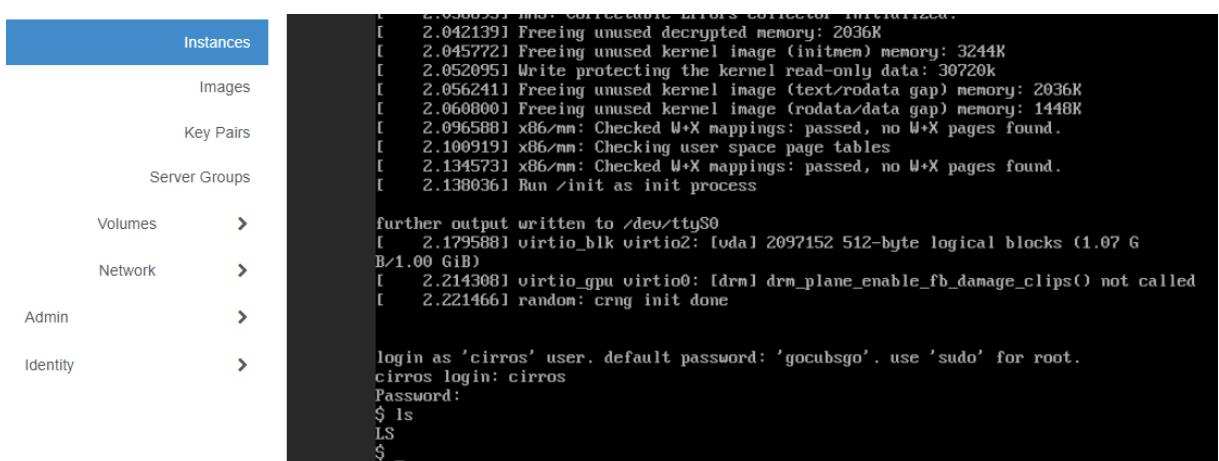
Hình 116: Quét cổng từ các máy ảo nằm trên nhánh mạng bài tập từ ứng dụng web.

```

[~] $(kali㉿kali)-[~]
$ ssh cirros@10.0.1.184
The authenticity of host '10.0.1.184 (10.0.1.184)' can't be established.
ED25519 key fingerprint is SHA256:3ZNJcMPB6rUAS2NMH7M6uiJSjhySxARoGx3L6q.jefTw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.184' (ED25519) to the list of known hosts.
cirros@10.0.1.184's password:
$ touch LS
$ ls
LS
$ _

```

Hình 117: Tiến hành tấn công vào dịch vụ SSH của máy mục tiêu từ ứng dụng web.



Hình 118: Kiểm tra tình trạng máy mục tiêu trên nền tảng OpenStack.

Nghiên cứu chứng minh rằng, với việc không tiêu tốn nhiều tài nguyên như CPU và bộ nhớ, VNC vẫn có thể hoạt động trên phần cứng có công suất thấp. Giao thức này được thiết kế đơn giản nhưng vẫn đảm bảo độ hiệu quả khi truyền tải hình ảnh màn hình hay tương tác với chuột và bàn phím. Bên cạnh đó, VNC còn có khả năng nén dữ liệu, giúp giảm thiểu băng thông cần thiết, đặc biệt hữu ích khi kết nối internet tốc độ thấp. Dù được thiết lập kết nối từ xa, bài tập thực hành vẫn mang lại trải nghiệm tương tự như việc trực tiếp sử dụng máy ảo tấn công trên môi trường OpenStack.

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

1. Kết quả đạt được

Sau 7 tháng nghiên cứu, nhóm nghiên cứu đã xây dựng thành công môi trường thực tập kiểm thử bảo mật dựa trên nền tảng điện toán đám mây OpenStack. Hệ thống đã được triển khai trên một ứng dụng web PHP, cung cấp đầy đủ các kiến thức và kỹ năng cần thiết liên quan đến lĩnh vực An toàn thông tin.

Thông qua nền tảng OpenStack, hệ thống đã cung cấp một môi trường thực tập kiểm thử bảo mật được cấu hình sẵn. Người dùng có thể truy cập ngay vào máy ảo tân công từ ứng dụng web và tiến hành thực hiện bài tập, giúp tiết kiệm thời gian và có thể tập trung vào việc rèn luyện kỹ năng thực tế.

Ứng dụng web được xây dựng và phát triển với ba chức năng chính bao gồm: các lớp học lý thuyết, các thử thách CTF và các bài tập thực hành kiểm thử bảo mật. Nhìn chung, hệ thống đã đáp ứng được các yêu cầu được đặt ra ban đầu, nhằm mang đến một môi trường học tập và rèn luyện kỹ năng An toàn thông tin một cách toàn diện.

2. Hạn chế

Về chi phí cho phần cứng, hiện tại hệ thống không đòi hỏi quá nhiều tài nguyên do được xây dựng với mục đích thử nghiệm. Tuy nhiên, nếu triển khai lên môi trường thực tế, hệ thống sẽ yêu cầu khá nhiều chi phí cho việc xây dựng và bảo trì, nhằm đáp ứng đầy đủ các yêu cầu phần cứng cho việc xây dựng nhiều cặp máy ảo.

Ứng dụng web hiện đã cung cấp tương đối đầy đủ các chức năng chính phục vụ cho việc tìm hiểu về lĩnh vực An toàn thông tin. Tuy nhiên đây vẫn là một ứng dụng web chưa hoàn chỉnh, giao diện chưa thực sự bắt mắt và còn thiếu sót nhiều chức năng so với các ứng dụng web thực tế.

3. Hướng phát triển

Trên thực tế, việc triển khai một nền tảng OpenStack hoàn chỉnh sẽ cung cấp đầy đủ các tính năng hơn so với việc cài đặt nền tảng bằng DevStack, một bộ công cụ dành cho nhà phát triển. Trong trường hợp ứng dụng được triển khai trên hệ thống máy chủ của trường học, nền tảng OpenStack sẽ phải yêu cầu một lượng tài nguyên khổng lồ, đảm bảo yêu cầu về cả số lượng lẫn chất lượng cho các bài tập thực hành kiểm thử bảo mật.

Sở hữu thiết kế giao diện đơn giản mà đặc trưng, cùng với các chức năng hoạt động tương đối ổn định, ứng dụng web có tiềm năng sẽ được phát triển thành một sản phẩm thực tế. Cụ thể, ứng dụng web sẽ cần được cải tiến một vài chỗ như: thiết kế giao diện tương thích với nhiều thiết bị khác nhau, bổ sung thêm các chức năng phụ, thiết kế cơ sở dữ liệu dành cho các bài tập kiểm thử bảo mật...để phù hợp hơn với nhu cầu sử dụng.

TÀI LIỆU THAM KHẢO

- [1] T. AnDrew Yang, Tuan Anh Nguyen. “Network Security Development Process - A Framework for Teaching Network Security Courses”, in Journal of Computing Sciences in Colleges, Volume 21, Issue 4, p. 203–209, Univ. of Houston – Clear Lake, Houston, Texas, 2006.
- [2] Malik, Saadat. Network Security: Principles and Practices. Cisco Press. 2003.
- [3] W. Yurcik and D. Doss. “Different approaches in the teaching of information systems security”, in Security, Proceedings of the Information Systems Education Conference, p. 32–33, 2001.
- [4] C. Willems and C. Meinel. “Practical Network Security Teaching in an Online Virtual Laboratory”, in Proceedings of Security and Management 2011, p. 65–71, Las Vegas, USA, 2011.
- [5] W. Luna and J. L. C. Sequera. “Collaboration in Cloud for Online Learning Environments: An Experience Applied to Laboratories” Published Online August 2015 in SciRes. www.scirp.org/journal/ce, 10.4236/ce.2015.613144
- [6] L. Xu, D. Huang, and W. T. Tsai, “V-Lab: A Cloud-based Virtual Laboratory Platform for Hands-on Networking Courses” in Proc. 17th Annu. ACM ITiCSE, 2012, pp. 256–261
- [7] J. A. González-Martínez, M. L. Bote-Lorenzo, E. Gómez-Sánchez, R. Cano-Parra, “Cloud computing and education: A state-of-the-art survey” in www.elsevier.com/locate/compedu, 2015
- [8] Hack The Box. Your Cyber Performance Center.
<https://www.hackthebox.com>.
- [9] TryHackMe. Cyber Security Training.
<https://tryhackme.com>.
- [10] pwn.college. Learn To Hack.
<https://pwn.college>.
- [11] An Introduction to Cybersecurity by SANS Institute.
- [12] An toàn thông tin [Website]. (2024, April 12). Quy I/2024:
<https://antoanthongtin.vn/an-toan-thong-tin/quy-i2024-tang-187-nghy-co-tan-cong-mang-nham-vao-cac-he-thong-cong-nghe-thong-tin-trong-yeu-109933>.

- [13] National Cybersecurity Center of Excellence (NCCOE). “Executive Summary — NIST SP 1800-25 documentation.” <https://www.nccoe.nist.gov/publication/1800-25/VoIA/index.html>
- [14] Omer Bin Tauqeer, Sadeeq Jan, Alaa Omar Khadidos, Adil Omar Khadidos, Fazal Qudus Khan, and Sana Khattak. “Analysis of Security Testing Techniques.” Intelligent Automation & Soft Computing 29, no. 01 (2021): 291-306. DOI: 10.32604/iasc.2021.017260.
- [15] Cowan, C.; Arnold, S.; Beattie, S.; Wright, C.; Viega, J. (April 2003). “[Defcon Capture the Flag: Defending vulnerable code from intense attack](#)”. Proceedings DARPA Information Survivability Conference and Exposition. Vol. 1. Pp. 120–129 vol.1. <doi:10.1109/DISCEX.2003.1194878>. ISBN 0-7695-1897-4. S2CID 18161204
- [16] Kali Linux Project. (2023). What is Kali Linux? [Website]. Retrieved from <https://www.kali.org/docs/introduction/what-is-kali-linux/>
- [17] Surarapu, P., Mahadasa, R., Vadiyala, V. R., & Baddam, P. R. (2023). An Overview of Kali Linux: Empowering Ethical Hackers with Unparalleled Features. FMDB Transactions on Sustainable Technoprise Letters
- [18] National Institute of Standards and Technology (NIST). Special Publication 800-145. <https://csrc.nist.gov/pubs/sp/800/145/final>
- [19] IBM. “What Is Virtualization?” <https://www.ibm.com/products/zvm>.
- [20] Li, Y., Li, W., & Jiang, C. (2010). A Survey of Virtual Machine System: Current Technology and Future Trends.
- [21] Olowu, Modebola, Chika Yinka-Banjo, Sanjay Misra, and Hector Florez. “A Secured Private-Cloud Computing System.” In Applied Informatics, edited by Hector Florez, 373-384. Madrid, Spain: Springer Nature Switzerland AG, 2019
- [22] OpenStack. Open Source Cloud Computing Infrastructure.
<https://www.openstack.org/>
- [23] The PHP Group. PHP Documentation.
<https://www.php.net/docs.php>
- [24] Oracle. MySQL Documentation.
https://docs.oracle.com/cd/E17952_01/
- [25] Apache. The Apache HTTP Server Project.
<https://httpd.apache.org/>

[26] OpenStack. DevStack: Automated OpenStack Installation for Developers.

<https://docs.openstack.org/devstack/latest/>

[27] Canonical Ubuntu. Ubuntu Server Documentation.

<https://ubuntu.com/server/docs>

[28] Oracle. VirtualBox Documentation.

<https://forum.virtualbox.org/wiki/Documentation>

[29] XAMPP Installers and Downloads for Apache Friends.

<https://www.apachefriends.org/docs/>

[30] A Javascript library that renders detailed SVG charts, enabling review of the data via pan, zoom, and data table actions. <https://www.chartjs.org/docs/latest/>

[31] Tribbitt, Tristan D. 1998. “Virtual Network Computing [VNC].” *ResearchGate*.

https://www.researchgate.net/publication/3419151_Virtual_Network_Computing

[32] OpenStack. OpenStack-SDK-PHP.

<https://wiki.openstack.org/wiki/OpenStack-SDK-PHP>

[33] Composer. Composer Documentation.

<https://getcomposer.org/doc/>

THUYẾT MINH ĐỀ TÀI
NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN

1. TÊN ĐỀ TÀI XÂY DỰNG MÔI TRƯỜNG THỰC TẬP KIỂM THỬ BẢO MẬT TRÊN NỀN TẢNG ĐÁM MÂY		2. MÃ SỐ THS2024-77
Lĩnh vực ưu tiên		
	1. Khoa học cơ bản	
	2. Công nghệ cao trong nông nghiệp, thủy sản và phát triển bền vững	
	3. Môi trường, tài nguyên thiên nhiên và biến đổi khí hậu	
X	4. Công nghệ, công nghệ thông tin và chuyển đổi số	
	5. Khoa học giáo dục, luật và xã hội nhân văn	
	6. Phát triển kinh tế, thị trường và nông thôn	
	7. Công nghệ sinh học và thực phẩm	
	Không thuộc 7 Lĩnh vực ưu tiên	
3. LĨNH VỰC NGHIÊN CỨU		
	Khoa học Tự nhiên	
X	Khoa học Kỹ thuật và Công nghệ	
	Khoa học Y, dược	
	Khoa học Nông nghiệp	
	Khoa học Xã hội	
	Khoa học Nhân văn	
4. LOẠI HÌNH NGHIÊN CỨU		
	Cơ bản	
X	Ứng dụng	
	Triển khai	
5. THỜI GIAN THỰC HIỆN		07 tháng
Từ tháng 4 năm 2024 đến tháng 10 năm 2024		

6. ĐƠN VỊ CỦA CHỦ NHIỆM ĐỀ TÀI

Tên đơn vị: Trường CNTT-TT

Điện thoại: 02923734713 - 02923831301

E-mail: office@cit.ctu.edu.vn

Địa chỉ: Khu 2, đường 3/2, Phường Xuân Khánh, Q. Ninh Kiều, TP. Cần Thơ, Việt Nam.

Họ và tên thủ trưởng đơn vị: Nguyễn Hữu Hòa

7. CHỦ NHIỆM ĐỀ TÀI

Họ và tên: Trương Đặng Trúc Lâm

MSSV: B2111933

Ngày tháng năm sinh: 30/01/2003

Lớp: DI21V7F3

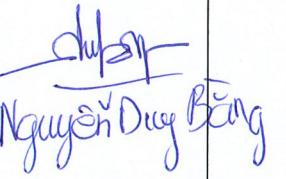
Điện thoại di động: 0907543817

Khóa: 47

E-mail: lamb2111933@student.ctu.edu.vn

8. NHỮNG THÀNH VIÊN THAM GIA NGHIÊN CỨU ĐỀ TÀI

TT	Họ và tên	MSSV, Lớp, Khóa	Nội dung nghiên cứu cụ thể được giao	Chữ ký
1	Trương Đặng Trúc Lâm	B2111933, DI21V7F3, K47	Quản lý chủ nhiệm đề tài. Tìm hiểu các nghiên cứu có liên quan đến đề tài. Cài đặt môi trường IaaS. Xây dựng và phát triển ứng dụng web. Triển khai các bài tập kiểm thử bảo mật trên ứng dụng web. Kiểm thử và đánh giá hệ thống. Viết báo cáo tổng kết đề tài.	 Truong Dang Truc Lam
2	Đặng Hoàng Hưng	B2111984, DI21V7F3, K47	Tìm hiểu các nghiên cứu có liên quan đến đề tài. Tìm hiểu và đề xuất các công nghệ sử dụng. Xây dựng và phát triển ứng dụng web.	 Đặng Hoàng Hưng

			Kiểm thử và đánh giá hệ thống. Viết báo cáo tổng kết đề tài.	
3	Lê Xuân Thành	B2111952, DI21V7F1, K47	Tìm hiểu các nghiên cứu có liên quan đến đề tài. Tìm hiểu và đề xuất các công nghệ sử dụng. Cài đặt môi trường IaaS. Xây dựng và phát triển ứng dụng web. Triển khai các bài tập kiểm thử bảo mật trên ứng dụng web. Kiểm thử và đánh giá hệ thống. Viết báo cáo tổng kết đề tài.	 Lê Xuân Thành
4	Nguyễn Duy Bằng	B2111971, DI21V7F3, K47	Tìm hiểu các nghiên cứu có liên quan đến đề tài. Tìm hiểu và đề xuất các công nghệ sử dụng. Cài đặt môi trường IaaS. Xây dựng và phát triển ứng dụng web. Triển khai các bài tập kiểm thử bảo mật trên ứng dụng web. Kiểm thử và đánh giá hệ thống. Viết báo cáo tổng kết đề tài.	 Nguyễn Duy Bằng

Cán bộ hướng dẫn sinh viên thực hiện đề tài

Họ và tên, MSVC	Đơn vị công tác và lĩnh vực chuyên môn	Nhiệm vụ	Chữ ký

TS. Thái Minh Tuấn, MSCB: 001944	Đơn vị công tác: Khoa Công nghệ Thông tin Lĩnh vực chuyên môn: Khoa học máy tính	Hướng dẫn nội dung khoa học và Hướng dẫn lập dự toán kinh phí đề tài	
-------------------------------------	---	--	---

9. ĐƠN VỊ PHỐI HỢP CHÍNH

Tên đơn vị trong và ngoài nước	Nội dung phối hợp nghiên cứu	Họ và tên người đại diện đơn vị
Không	Không	Không

10. TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU THUỘC LĨNH VỰC CỦA ĐỀ TÀI Ở TRONG VÀ NGOÀI NƯỚC

10.1. Trong nước

Đối với nhiều sinh viên, việc thiết lập môi trường thực tập kiểm thử bảo mật trên máy cá nhân sẽ gặp phải nhiều hạn chế. Xây dựng các máy ảo theo cách thủ công sẽ dẫn đến việc tiêu hao thời gian, công sức và tài nguyên. Hơn hết, để có thể thiết lập môi trường thực tập kiểm thử bảo mật, máy cá nhân của chúng ta phải có cấu hình đủ mạnh. Chính vì thế, các sinh viên có hoàn cảnh khó khăn sẽ không đáp ứng đủ điều kiện cần thiết để tự xây dựng môi trường thực tập kiểm thử bảo mật.

Trong nước hiện nay đã xây dựng và phát triển các hệ thống học tập trực tuyến. Tuy nhiên, các môi trường thực tập kiểm thử bảo mật vẫn chưa được phát triển mạnh. Điều này dẫn đến việc thiếu hụt nhân lực An toàn thông tin. Năm 2023, khoảng 13.900 vụ tấn công an ninh mạng vào các hệ thống tại Việt Nam đã diễn ra. Các mục tiêu chịu nhiều cuộc tấn công nhất trong năm qua là các cơ quan chính phủ, hệ thống ngân hàng, tổ chức tài chính, hệ thống công nghiệp và các hệ thống trọng yếu khác.

Vì vậy, để cải thiện tình trạng xuất hiện nhiều lỗ hổng trong an ninh mạng, các môi trường thực tập kiểm thử bảo mật cần được xây dựng và triển khai để cung cấp kiến thức kỹ năng thiết yếu trong lĩnh vực An toàn thông tin cho người dùng.

10.2. Ngoài nước

Đề tài xây dựng môi trường thực tập kiểm thử bảo mật là đề tài được nghiên cứu nhiều trong những năm gần đây, đặc biệt là đối với những nước đặt ra các tiêu chuẩn cao về bảo mật cho các kỹ sư lĩnh vực An toàn thông tin. Việc tiếp xúc và thực tập với môi trường An toàn thông tin từ sớm giúp cho sinh viên có cơ hội nâng cao kỹ năng. Hiện nay cũng có rất nhiều nhóm nghiên cứu đề tài này trên thế giới, các nhóm này đưa ra những phương pháp hỗ trợ sinh viên trong quá trình thực tập và làm quen với môi trường An toàn thông tin [1-6].

Bên cạnh đó, tầm ảnh hưởng của công nghệ Điện toán đám mây đang ngày một tăng và không có dấu hiệu kết thúc. Với những ưu điểm như dịch vụ nhanh chóng, tiết kiệm chi phí và thời gian, thân thiện với môi trường, đồng thời đem đến môi trường hợp tác bền vững. Chính vì thế các nhóm nghiên cứu An toàn thông tin đã chọn giải pháp xây dựng các môi trường thực tập kiểm thử bảo mật sử dụng tài nguyên trên nền tảng Điện toán đám mây [7-10].

Tài liệu tham khảo:

- [1] Lindskog, Stefan, Lindqvist, Ulf, and Jonsson, Erland (1999). IT Security Research and Education in Synergy. In Proceedings of the 1st World Conference on Information Security Education, Stockholm, Sweden.
- [2] W. Yurcik and D. Doss. "Different approaches in the teaching of information systems security", in Security, Proceedings of the Information Systems Education Conference, p. 32–33, 2001.
- [3] T. A. Yang and T. A. Nguyen, "Network security development process: A framework for teaching network security courses," J. Comput. Small Coll., vol. 21, pp. 203–209, April 2006.
- [4] C. Willems and C. Meinel. "Practical Network Security Teaching in an Online Virtual Laboratory", in Proceedings of Security and Management 2011, p. 65–71, Las Vegas, USA, 2011.
- [5] P. Li and T. Mohammed, "Integration of virtualization technology into network security laboratory," in Proc. 38th Annu. Frontiers Educ. Conf., Oct. 2008, pp. S2A-7–S2A-12.

- [6] W. Yurcik and D. Doss. "Different approaches in the teaching of information systems security", in Security, Proceedings of the Information Systems Education Conference, p. 32–33, 2001.
- [7] H. E. Schaffer, S. F. Averitt, M. I. Hoit, A. Peeler, E. D. Sills, and M. A. Vouk, "NCSU's virtual computing lab: A cloud computing solution," Computer, vol. 42, no. 7, pp. 94–97, Jul. 2009.
- [8] C. Yan, "Build a laboratory cloud for computer network education," in Proc. 6th ICCSE, Aug. 2011, pp. 1013–1018.
- [9] L. Xu, D. Huang, and W. T. Tsai, "V-Lab: A Cloud-based Virtual Laboratory Platform for Hands-on Networking Courses," in Proc. 17th Annu. ACM ITiCSE, 2012, pp. 256–261.
- [10] Illinois Security Lab, Urbana, IL, USA, "Illinois Security Lab," Apr. 2012 [Online]. Available: <http://seclab.illinois.edu/>

10.3. Danh mục các công trình đã công bố thuộc lĩnh vực của đề tài của chủ nhiệm và những thành viên tham gia nghiên cứu

- a) Của chủ nhiệm đề tài: Không
- b) Của các thành viên tham gia nghiên cứu: Không

11. TÍNH CẤP THIẾT CỦA ĐỀ TÀI

Việc tăng cường đào tạo nhân lực An toàn thông tin đang là chủ đề cấp thiết trong nước ta, đặc biệt là khu vực Đồng bằng sông Cửu Long. Hiện nay, Đại học Cần Thơ đã xây dựng và phát triển các hệ thống học tập trực tiếp như CTU E-Learning, ELSE,... nhưng vẫn chưa có môi trường thực tập kiểm thử bảo mật dành cho sinh viên.

Việc thiết lập môi trường thực tập kiểm thử bảo mật trên máy cá nhân sẽ dẫn đến việc tiêu hao thời gian, công sức và tài nguyên. Quan trọng hơn, các bạn sinh viên sẽ phải tốn rất nhiều chi phí cho máy vật lý có cấu hình đủ mạnh để có thể tự thiết lập môi trường thực tập kiểm thử bảo mật. Những trở ngại ấy sẽ mang đến nhiều thiệt thòi cho các bạn sinh viên có hoàn cảnh khó khăn.

Chính vì thế, chúng tôi đang hướng đến việc thiết kế một ứng dụng web nhằm xây dựng môi trường thực tập kiểm thử bảo mật dành cho sinh viên. Hệ thống của chúng tôi sẽ bao gồm các bài kiểm tra thực hành và thử thách dành cho sinh viên. Các thử thách bao gồm: các tập tin như ảnh, video hoặc các máy chủ được thiết kế nhằm làm mục tiêu để tấn công. Bên cạnh đó, chúng tôi sẽ tích hợp thêm các lớp học trực tuyến, các tài liệu có liên quan,...vào trang web.

12. MỤC TIÊU ĐỀ TÀI

Mục tiêu của đề tài là thiết kế và xây dựng cho sinh viên Trường Đại học Cần Thơ môi trường thực tập kiểm thử bảo mật và các kiến thức thuộc lĩnh vực An toàn thông tin, dựa trên các công nghệ Điện toán đám mây.

13. ĐỐI TƯỢNG, PHẠM VI NGHIÊN CỨU

13.1. Đối tượng nghiên cứu

Cơ sở lý thuyết An toàn thông tin và các kỹ thuật tấn công và phòng thủ trên không gian mạng. Đồng thời nghiên cứu phương pháp quy trình phát triển ứng dụng web và tích hợp tài nguyên trên đám mây phục vụ cho việc thiết kế các bài kiểm tra thực hành và thử thách.

13.2. Phạm vi nghiên cứu

Nghiên cứu sẽ tập trung vào việc thiết kế và xây dựng một môi trường thực tập kiểm thử bảo mật dành cho sinh viên. Nội dung bao gồm:

Điện toán đám mây: OpenStack (AWS, Azure, GCP,...)

Lập trình web: PHP (Node.js,...)

An toàn thông tin: các công cụ trên Kali Linux.

Thời gian thực hiện đề tài nghiên cứu: 7 tháng (04/2024 - 10/2024).

Không gian: nghiên cứu trong phạm vi Đại học Cần Thơ.

14. CÁCH TIẾP CẬN, PHƯƠNG PHÁP NGHIÊN CỨU

14.1. Cách tiếp cận

Nghiên cứu lý thuyết - thử nghiệm - ứng dụng.

14.2. Phương pháp nghiên cứu

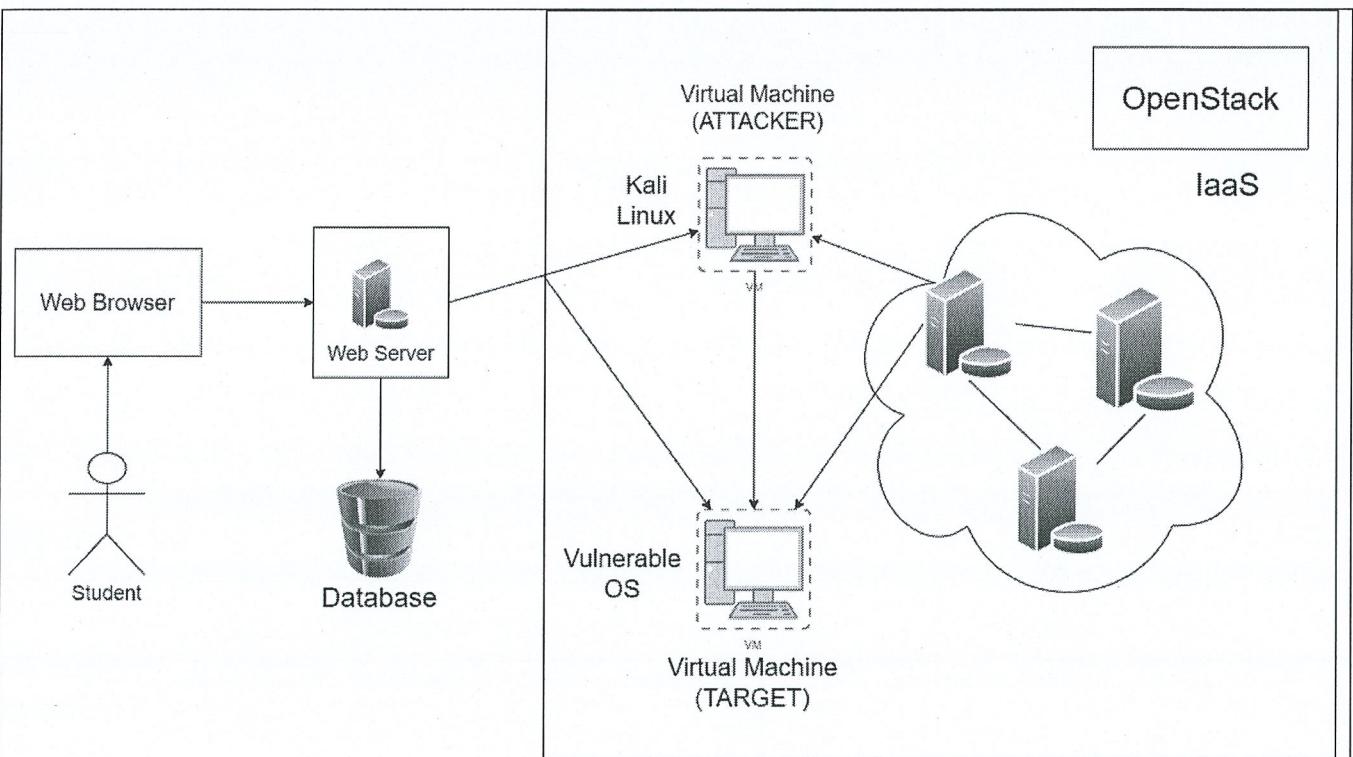
Nghiên cứu cơ sở lý thuyết An toàn thông tin: Thu thập và phân tích các tài liệu tham khảo từ các tổ chức chuyên nghiên cứu về lĩnh vực An toàn thông tin.

Xây dựng môi trường thực tập kiểm thử bảo mật: Tham khảo các môi trường thực tập kiểm thử bảo mật uy tín đã có. Từ đó thu thập, phân tích và chọn ra giải pháp xây dựng hệ thống sao cho phù hợp. Như được mô tả trong Hình 1, chúng tôi sẽ sử dụng nền tảng OpenStack để thiết lập một cơ sở hạ tầng dịch vụ cho phép xây dựng các máy ảo đóng vai trò là máy tấn công và máy mục tiêu. Bên cạnh đó chúng tôi sẽ thiết kế một giao diện web cho phép ta quản lý các bài tập thực hành và thử thách.

Kiểm thử: Tiến hành kiểm thử để đảm bảo tính ổn định và chính xác của hệ thống.

Triển khai hệ thống qua các hoạt động: Tổ chức xây dựng nội dung số gồm các bài giảng, các bài tập thực hành; tổ chức tập huấn cho giảng viên, sinh viên sử dụng hệ thống; đưa hệ thống vận hành thực tế.

Đánh giá kết quả: Kết quả của đề tài sẽ được đánh giá bằng cách so sánh với các môi trường thực tập kiểm thử bảo mật khác. Từ đó đưa ra những đánh giá về tính khả thi và hiệu quả của ứng dụng trong việc giáo dục và đào tạo.



Hình 1. Sơ đồ hệ thống

15. NỘI DUNG NGHIÊN CỨU VÀ TIẾN ĐỘ THỰC HIỆN

15.1. Nội dung nghiên cứu

Tìm hiểu các nghiên cứu có liên quan đến đề tài.

Tìm hiểu và đề xuất các công nghệ sử dụng.

Cài đặt môi trường IaaS.

Xây dựng và phát triển ứng dụng web.

Triển khai các bài tập kiểm thử bảo mật trên ứng dụng web.

Kiểm thử và đánh giá hệ thống.

Viết báo cáo tổng kết đề tài.

15.2. Tiến độ thực hiện

STT	Các nội dung, công việc thực hiện	Sản phẩm	Thời gian (bắt đầu-kết thúc)	Người thực hiện và số ngày thực hiện
1.	Tìm hiểu tài liệu nghiên cứu có liên quan đến đề tài.	Bài thuyết minh về đề tài nghiên cứu.	4/2024	Thành viên chính Nguyễn Duy Bằng (0.2 tháng); Thành viên Lê Xuân Thành (0.2 tháng);

				Thành viên Đặng Hoàng Hung (0.2 tháng); Thành viên Trương Đặng Trúc Lâm (0.2 tháng)
2.	Tìm hiểu và đề xuất các công nghệ sử dụng.	Bản trình bày về các công nghệ đề xuất sử dụng.	4/2024 - 5/2024	Thành viên chính Lê Xuân Thành (0.2 tháng); Thành viên Đặng Hoàng Hung (0.2 tháng); Thành viên Nguyễn Duy Bằng (0.2 tháng)
3.	Cài đặt môi trường IaaS.	Môi trường IaaS.	5/2024 - 6/2024	Thành viên chính Trương Đặng Trúc Lâm (1 tháng); Thành viên Lê Xuân Thành (0.6 tháng); Thành viên Nguyễn Duy Bằng (0.6 tháng)
4.	Xây dựng và phát triển ứng dụng web.	Ứng dụng web.	6/2024 - 7/2024	Thành viên chính Đặng Hoàng Hung (1.2 tháng); Thành viên Lê Xuân Thành (0.8 tháng);

				Thành viên Nguyễn Duy Bằng (0.8 tháng); Thành viên Trương Đặng Trúc Lâm (0.8 tháng)
5.	Triển khai các bài tập kiểm thử bảo mật trên ứng dụng web.	Các bài tập thực hành và thử thách.	7/2024 - 8/2024	Thành viên chính Nguyễn Duy Bằng (0.8 tháng); Thành viên Lê Xuân Thành (0.8 tháng); Thành viên Trương Đặng Trúc Lâm (0.8 tháng)
6.	Kiểm thử và đánh giá hệ thống.	Kết quả và đánh giá.	8/2024 - 9/2024	Thành viên chính Lê Xuân Thành (0.6 tháng); Thành viên Trương Đặng Trúc Lâm (0.4 tháng); Thành viên Đặng Hoàng Hưng (0.4 tháng); Thành viên Nguyễn Duy Bằng (0.4 tháng)

16. SẢN PHẨM

Số thứ tự	Tên sản phẩm	Số lượng	Yêu cầu chất lượng sản phẩm
I	Sản phẩm khoa học (Các công trình khoa học sẽ được công bố: sách, bài báo khoa học...) Không		
II	Sản phẩm đào tạo (Luận văn tốt nghiệp đại học)		

	Không		
III	Sản phẩm ứng dụng		
3.1	Website thực tập kiểm thử bảo mật	01	Môi trường thực tập kiểm thử bảo mật phải đảm bảo cung cấp đủ lượng kiến thức và kỹ năng cần thiết trong việc kiểm thử bảo mật cho người sử dụng. Bên cạnh đó, website phải có giao diện thân thiện, hiệu năng tốt, ổn định, chính xác, bền vững và tuân thủ đúng theo Luật An ninh mạng.
IV.	Sản phẩm theo quy định của Trường Đại học Cần Thơ		
4.1	Bản tin	01	Theo đúng quy định của Trường Đại học Cần Thơ.
4.2	Báo cáo tóm tắt	01	Theo đúng quy định của Trường Đại học Cần Thơ.
4.3	Video clips	01	Tối đa 02 phút. Đầy đủ thông tin trọng tâm của đề tài.

17. PHƯƠNG THỨC CHUYỂN GIAO KẾT QUẢ NGHIÊN CỨU VÀ ĐỊA CHỈ ỨNG DỤNG

17.1. Phương thức chuyển giao

Chuyển giao trực tiếp cho Trường Công nghệ thông tin và Truyền thông - Đại học Cần Thơ. Kết quả sẽ là nguồn tài liệu tham khảo cho việc giảng dạy cũng như các nghiên cứu tiếp theo.

17.2. Địa chỉ ứng dụng

Trường Công nghệ thông tin và Truyền thông, Đại học Cần Thơ.

18. TÁC ĐỘNG VÀ LỢI ÍCH MANG LẠI CỦA KẾT QUẢ NGHIÊN CỨU

18.1. Đối với lĩnh vực giáo dục và đào tạo

Là môi trường thực tập kiểm thử bảo mật phù hợp với các sinh viên có định hướng An toàn thông tin. Bên cạnh đó, giảng viên có thể sử dụng ứng dụng minh họa cho các bài giảng có liên quan.

18.2. Đối với lĩnh vực khoa học và công nghệ có liên quan

Xây dựng và phát triển môi trường thực tập kiểm thử bảo mật trên nền tảng Điện toán đám mây. Kết quả ứng dụng có thể cải tiến, phát triển cho các dự án nghiên cứu khoa học khác.

18.3. Đối với phát triển kinh tế-xã hội

Môi trường thực tập kiểm thử bảo mật cung cấp cho sinh viên kiến thức và kỹ năng An toàn thông tin cần thiết để có thể hỗ trợ tăng cường bảo mật cho các cơ quan, doanh nghiệp, tổ chức,...

18.4. Đối với tổ chức chủ trì và các cơ sở ứng dụng kết quả nghiên cứu

Hệ thống có thể tiếp tục phát triển trong tương lai với lợi ích giáo dục và đào tạo. Ngoài ra, hệ thống còn là nguồn tài liệu cho sinh viên để thực hiện các ý tưởng sáng tạo khác.

19. KINH PHÍ THỰC HIỆN ĐỀ TÀI VÀ NGUỒN KINH PHÍ

Kinh phí thực hiện đề tài: 15.000.000 đồng.

Trong đó:

Kinh phí Trường cấp: 15.000.000 đồng.

Các nguồn khác: 0 đồng.

Đơn vị tính: đồng

Stt	Khoản chi, nội dung chi	Tổng kinh phí	Nguồn kinh phí	
			Kinh phí Trường cấp	Các nguồn khác
1	Chi tiền thù lao tham gia thực hiện đề tài	11.970.000	11.970.000	0
2	Chi mua vật tư, nguyên, nhiên, vật liệu	0	0	0
3	Chi văn phòng phẩm, in ấn	305.000	305.000	0
4	Chi họp hội đồng đánh giá, nghiệm thu	2.725.000	2.725.000	0
	Tổng cộng	15.000.000	15.000.000	0

Ngày 01 tháng 4 năm 2024
CHỦ NHIỆM ĐỀ TÀI

TRƯỜNG CNTT-TT

CÁN BỘ HƯỚNG DẪN

Huỳnh Xuân Hiệp

TL. HIỆU TRƯỞNG
TRƯỜNG PHÒNG QUẢN LÝ KHOA HỌC

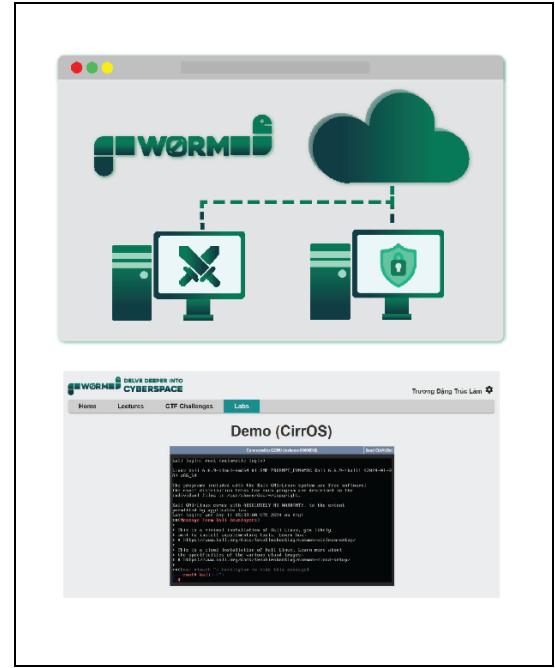


Lê Nguyễn Đoan Khôi



BẢN TIN ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN

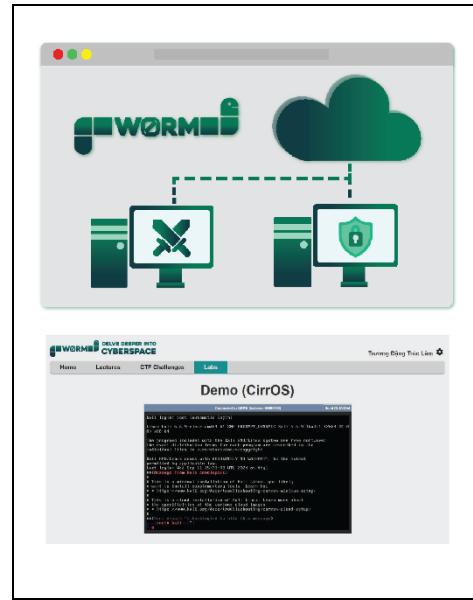
- Mã số đề tài: THS2024-77
- Tên đề tài: Xây dựng môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây
- Thời gian thực hiện: 7 tháng
- Kinh phí đã sử dụng: 15.000.000 VNĐ
- Chủ nhiệm đề tài: Trương Đặng Trúc Lâm (0907543817)
- Thành viên tham gia nghiên cứu:
 - Đặng Hoàng Hưng
 - Lê Xuân Thành
 - Nguyễn Duy Bằng
- Cán bộ hướng dẫn: Thái Minh Tuấn (minhtuan@ctu.edu.vn)
- Tính cấp thiết: Sự hạn chế của các nền tảng thực hành trực tuyến đang là rào cản lớn đối với việc đào tạo nhân lực An toàn thông tin. Sinh viên có thể gặp nhiều khó khăn trong việc tự xây dựng môi trường thực tập kiểm thử bảo mật, dẫn đến việc bất bình đẳng trong cơ hội học tập.
- Mục tiêu: Xây dựng môi trường thực tập kiểm thử bảo mật áp dụng công nghệ điện toán đám mây, đồng thời cung cấp các kiến thức thuộc lĩnh vực An toàn thông tin.
- Phương pháp nghiên cứu: Nghiên cứu cơ sở lý thuyết An toàn thông tin và xây dựng môi trường thực tập kiểm thử bảo mật.
- Nội dung nghiên cứu:
 - Cài đặt môi trường IaaS.
 - Xây dựng và phát triển ứng dụng web.
 - Triển khai các lớp học lý thuyết và bài tập thực hành An toàn thông tin.
- Kết quả đạt được: Môi trường thực tập kiểm thử bảo mật áp dụng công nghệ điện toán đám mây.
- Ý nghĩa: Sản phẩm có thể giúp sinh viên tiếp cận dễ dàng hơn trong việc thực tập kiểm thử bảo mật, góp phần thúc đẩy đào tạo nhân lực An toàn thông tin.
- Khả năng ứng dụng: Có thể phát triển thành sản phẩm hoàn chỉnh và triển khai thực tế.





SUMMARY REPORT RESEARCH PROJECT

- Project code: THS2024-77
- Project title: Building cloud-based security testing practice environment
- Project period: 7 months
- Total cost: 15.000.000 VND
- Project leader: Truong Dang Truc Lam (0907543817)
- Project members:
 - Dang Hoang Hung
 - Le Xuan Thanh
 - Nguyen Duy Bang
- Advisor: Thai Minh Tuan (minhtuan@ctu.edu.vn)
- Necessity of the project: The limitations of online practice platforms pose a significant obstacle to Cybersecurity workforce development. Students may encounter difficulties in independently constructing a secure testing environment, resulting in unequal learning opportunities.
- Objectives: Building a security testing practice environment utilizing cloud computing technology, while providing knowledge about Information Security.
- Methodology: Researching on theoretical basis of Information Security and building a practical environment for security testing.
- Project activities:
 - Setting up an IaaS environment.
 - Building a web application.
 - Implementing theoretical classes and practical exercises in Information Security
- Research results: Cloud-based security testing practice environment.
- Research new finding: This product makes it easier for students to access and practice security testing, thus advancing Information Security education.
- Application potentials: It can be developed into a complete product for deployment.





BÁO CÁO TÓM TẮT ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN

1. Thông tin chung:

- Mã số đề tài: THS2024-77
- Tên đề tài: Xây dựng môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây
- Sinh viên chủ nhiệm đề tài: Trương Đặng Trúc Lâm
- Lớp: Công nghệ thông tin CLC 03 Trưởng: CNTT-TT Năm thứ: 4 Số năm đào tạo: 4.5
- Người hướng dẫn: TS. Thái Minh Tuấn

2. Mục tiêu đề tài:

Xây dựng môi trường thực tập kiểm thử bảo mật áp dụng công nghệ điện toán đám mây, đồng thời cung cấp các kiến thức thuộc lĩnh vực An toàn thông tin.

3. Tính mới và sáng tạo:

Hệ thống sử dụng công nghệ điện toán đám mây OpenStack nhằm xây dựng môi trường Private Cloud. Ứng dụng web kết nối đến các máy ảo trên nền tảng đám mây thông qua công nghệ VNC, từ đó sinh viên có thể thực hành bài tập kiểm thử bảo mật. Nhóm nghiên cứu còn sưu tầm và sáng tạo các bài giảng và thử thách liên quan đến lĩnh vực An toàn thông tin.

4. Kết quả nghiên cứu:

Môi trường thực tập kiểm thử bảo mật áp dụng công nghệ điện toán đám mây.

5. Sản phẩm:

Môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây.

6. Công bố khoa học từ kết quả nghiên cứu của đề tài, hoặc nhận xét, đánh giá của cơ sở đã áp dụng các kết quả nghiên cứu (nếu có):

Không

7. Đóng góp về mặt kinh tế - xã hội, giáo dục và đào tạo, an ninh, quốc phòng và khả năng áp dụng của đề tài:

Sản phẩm có thể giúp sinh viên dễ dàng tiếp cận hơn trong việc thực tập kiểm thử bảo mật, góp phần thúc đẩy đào tạo nhân lực An toàn thông tin.

8. Hiệu quả, phương thức chuyển giao kết quả nghiên cứu và khả năng áp dụng:

Hiệu quả: Sản phẩm có thể giúp sinh viên dễ dàng tiếp cận hơn trong việc thực tập kiểm thử bảo mật, tiết kiệm thời gian và chi phí so với việc tự thiết lập môi trường thực hành.

Phương thức chuyển giao: Tài liệu liên quan đến môi trường thực tập kiểm thử bảo mật trên nền tảng đám mây.

Khả năng áp dụng: Có thể phát triển thành sản phẩm hoàn chỉnh và triển khai thực tế.



INFORMATION ON RESEARCH RESULTS

1. General information:

Project code: THS2024-77

Project title: Cloud-based security testing practice environment

Code number: THS2024-77

Coordinator: Truong Dang Truc Lam

Implementing institution: The College of Information and Communication Technology

Duration: from 4/2024 to 10/2024

2. Objective(s):

Building a security testing practice environment utilizing cloud computing technology, while providing knowledge about Information Security.

3. Creativeness and innovativeness:

System leverages OpenStack to establish a Private Cloud infrastructure. Web application interact with virtual machines on the cloud through VNC, providing a platform for students to conduct security testing experiments. The research team has also curated and developed educational content, including lectures and challenges, focused on Information Security.

4. Research results:

Security testing practice environment utilizing cloud computing technology.

5. Products:

Cloud-based security testing practice environment.

6. Effects, technology transfer means and applicability:

Effects: This product can help students easily access security testing practice, saving time and cost compared to setting up a practice environment themselves.

Technology transfer means: Documentation related to a cloud-based security testing practice environment.

Applicability: It can be developed into a complete product for deployment.