



TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM
KHOA CÔNG NGHỆ THÔNG TIN
Môn:

Họ Và Tên: Trần Nhật Vũ
MSSV: 2187701120
Lớp: 21DATA1

Báo Cáo Tuần 2

Câu hỏi 1:

Trả lời:

Phần 1: Cài đặt Wazuh Server

Hệ điều hành: Ubuntu 20.4

Thực hiện cập nhật hệ thống

```
sudo apt update && sudo apt upgrade -y
```

```
vu@ubuntu: ~  
vu@ubuntu:~$ sudo apt update && sudo apt upgrade -y  
[sudo] password for vu:  
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease  
Hit:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease  
Hit:3 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease  
Hit:4 http://security.ubuntu.com/ubuntu focal-security InRelease  
Hit:5 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu focal InRelease  
Hit:6 https://repo.zabbix.com/zabbix/6.3/ubuntu focal InRelease  
Reading package lists... Done
```

Cài đặt các gói phụ thuộc

```
sudo apt install vim curl apt-transport-https unzip wget libcap2-bin software-properties-  
common lsb-release gnupg2 -y
```

```
vu@ubuntu:~$ sudo apt install vim curl apt-transport-https unzip wget libcap2-bi  
n software-properties-common lsb-release gnupg2 -y  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
lsb-release is already the newest version (11.1.0ubuntu2).  
libcap2-bin is already the newest version (1:2.32-1ubuntu0.1).
```

Tải tập lệnh cài đặt Wazuh:

```
curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh
```

```
vu@ubuntu:~$  
vu@ubuntu:~$ curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh  
vu@ubuntu:~$
```

Chạy tập lệnh để tự động cài đặt Wazuh Manager, Elasticsearch, và Kibana:

```
sudo bash ./wazuh-install.sh -a -i
```

```
vu@ubuntu:~$ sudo bash ./wazuh-install.sh -a -i  
22/11/2024 08:19:09 INFO: Starting Wazuh installation assistant. Wazuh version:  
4.5.4  
22/11/2024 08:19:09 INFO: Verbose logging redirected to /var/log/wazuh-install.  
log
```

Thông tin đăng nhập:

```
User: admin
```

```
Password: eloqnuJj5*B70o?DlBtNTJAOSsvDgo7D
```

```
22/11/2024 08:44:50 INFO: You can access the web interface https://<wazuh-dashb  
oard-ip>:443  
User: admin  
Password: eloqnuJj5*B70o?DlBtNTJAOSsvDgo7D  
22/11/2024 08:44:50 INFO: Installation finished.
```

Kiểm tra ip máy Server:

```
ifconfig
```

```
22/11/2024 08:44:50 INFO: Installation finished.  
vu@ubuntu:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.24.146 netmask 255.255.255.0 broadcast 192.168.24.255  
    inet6 fe80::d985:dfef:4256:beb prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:df:aa:28 txqueuelen 1000 (Ethernet)  
    RX packets 738032 bytes 1097318680 (1.0 GB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 57083 bytes 3548108 (3.5 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Kiểm tra trạng thái các dịch vụ:

```
sudo systemctl status wazuh-manager
```

```
sudo systemctl status elasticsearch
```

```
sudo systemctl status kibana
```

```
sudo systemctl restart wazuh-manager elasticsearch kibana
```

Bật các cổng:

```
sudo ufw allow 443/tcp
```

```
sudo ufw allow 1514/tcp
```

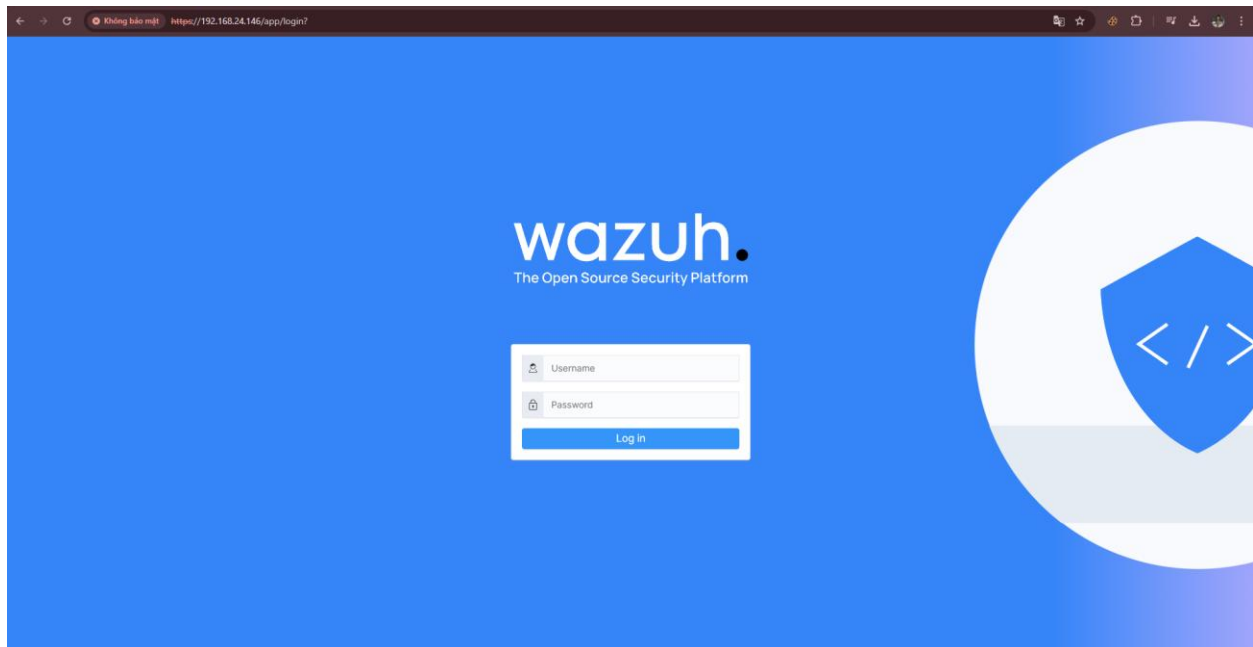
```
sudo ufw allow 1515/tcp
```

```
sudo ufw reload
```

```
vu@ubuntu:~$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
vu@ubuntu:~$ sudo ufw allow 1514/tcp
Rules updated
Rules updated (v6)
vu@ubuntu:~$ sudo ufw allow 1515/tcp
Rules updated
Rules updated (v6)
vu@ubuntu:~$ sudo ufw reload
Firewall not enabled (skipping reload)
```

Truy cập giao diện Wazuh để kiểm tra:

<https://192.168.24.146:443>



Phần 2: Cài đặt Wazuh Agent

Kali_agent







```
(root@kali)-[/home/kali]
# curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/w
azuh-agent/wazuh-agent_4.5.4-1_amd64.deb && sudo WAZUH_MANAGER='192.168.24.14
6' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Kali_Agent' dpkg -i ./wazuh-
agent.deb
Selecting previously unselected package wazuh-agent.
(Reading database ... 416391 files and directories currently installed.)
Preparing to unpack ./wazuh-agent.deb ...
Unpacking wazuh-agent (4.5.4-1) ...
Setting up wazuh-agent (4.5.4-1) ...

(root@kali)-[/home/kali]
# sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Synchronizing state of wazuh-agent.service with SysV service script with /usr
/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.servi
ce → /usr/lib/systemd/system/wazuh-agent.service.
```

Win10_Agent

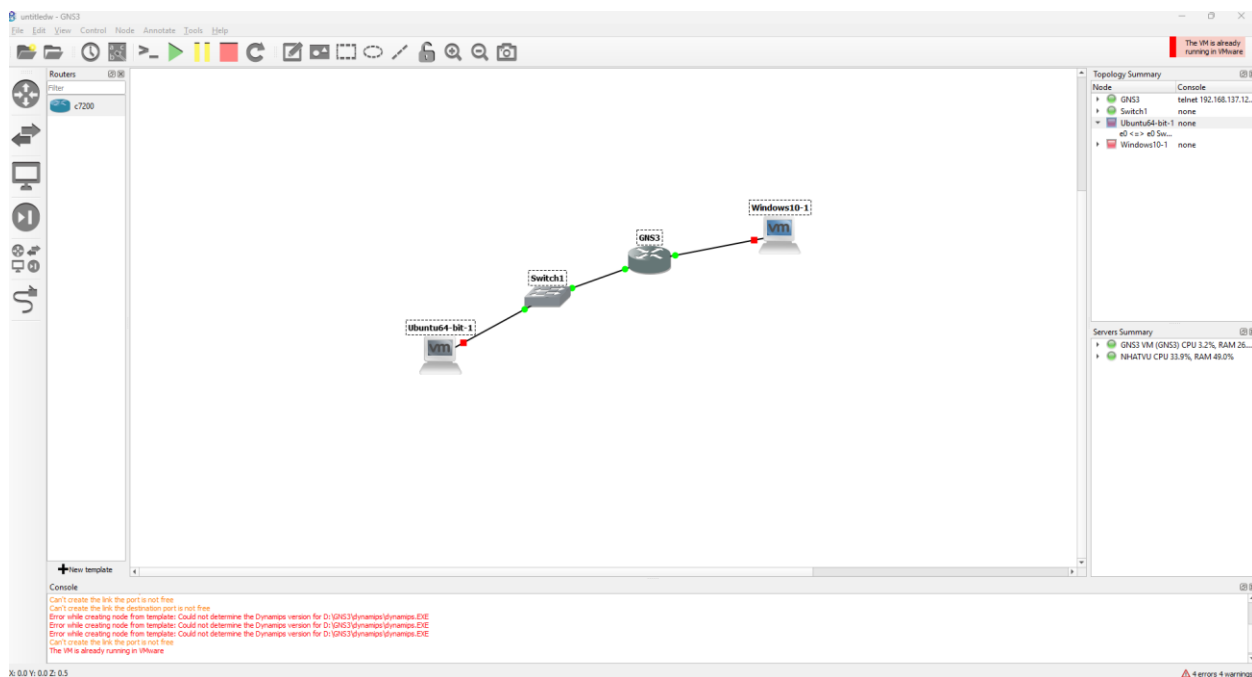
```
PS C:\Windows\system32>
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-ag
-1.msi -OutFile ${env:tmp}\wazuh-agent.msi; msixec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH
TION_SERVER='' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Win10_Agent'
PS C:\Windows\system32> NET START Wazuh
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>
```

Agents (2) ⊕ Deploy new agent 📄 Export formatted ⚙️									
ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions	
001	Kali_Agent	192.168.24.141	default	 Kali GNU/Linux 2024.4	node01	v4.5.4	●	 	
002	Win10_Agent	192.168.24.147	default	 Microsoft Windows 10 Home 10.0.19045.3803	node01	v4.5.4	●	 	

Cài gns3 và các route

Name	Date modified	Type	Size
c2600-adventerprisek9-mz.124-25d.bin	11/23/2024 9:18 PM	BIN File	29,267 KB
c3745-adventerprisek9-mz.124-25d.bin	11/23/2024 9:19 PM	BIN File	38,073 KB
c7200-adventerprisek9-mz.124-24.T5.bin	11/23/2024 9:20 PM	BIN File	44,043 KB



Phần 3: Thực nghiệm

Giám sát sự thay đổi của các file System

Ở máy Win10 thì vô phần: ossec-agent -> ossec.conf

Tiếp đến kiểm đến đoạn <syscheck> dán đoạn code directories phía dưới vào

```
<directories check_all="yes" report_changes="yes"
```

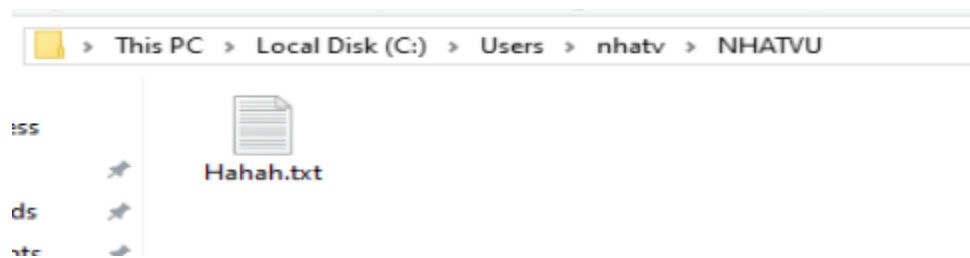
```
realtime="yes">C:\User\nhatv\NHATVU</directories>
```

```
<!-- File integrity monitoring -->
<syscheck>

<disabled>no</disabled>
<directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\nhatv\NHATVU</directories>
```

Đường dẫn C:\User\nhatv\NHATVU là nơi mình sẽ giám sát sự thay đổi của nó

Tiếp đến vào đường dẫn đó tạo một tệp bất kì



Sau đó vào Powershell chạy quyền quản trị, rồi nhập đoạn dưới để khởi động lại agent

Restart-Service -Name Wazuh

Quay trở lại dashboard server, ta thấy được có 1 alert về việc có file được thêm vào

Nov 24, 2024




@

15:02:10.865

File added to the system.

5

554

Table	JSON	Rule
@timestamp	2024-11-24T08:02:10.865Z	
   _id	1swxXZMBX2xkebcqUYlp	
agent.id	002	
agent.ip	192.168.24.147	
agent.name	Win10_Agent	
decoder.name	syscheck_new_entry	
full_log	File 'c:\users\nhatv\nhatvu\hahah.txt' added	

Trường hợp nếu file bị xóa

Nov 24, 2024	@	T1070.004	T1485	Defense Evasion, Impact	File deleted.	7	553
15:18:31.308							
Table	JSON	Rule					
@timestamp	2024-11-24T08:18:31.308Z						
_id	-sxAXZMBX2xkebcqYYiO						
agent.id	002						
agent.ip	192.168.24.147						
agent.name	Win10_Agent						
decoder.name	syscheck_deleted						
full_log	File 'c:\users\nhatv\nhatvu\hahah.txt' deleted Mode: realtime						
id	1732436311.119669						

