

HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN



BÀI THỰC HÀNH SỐ 04

TRIỂN KHAI HỆ THỐNG GIÁM SÁT ALIENVAULT

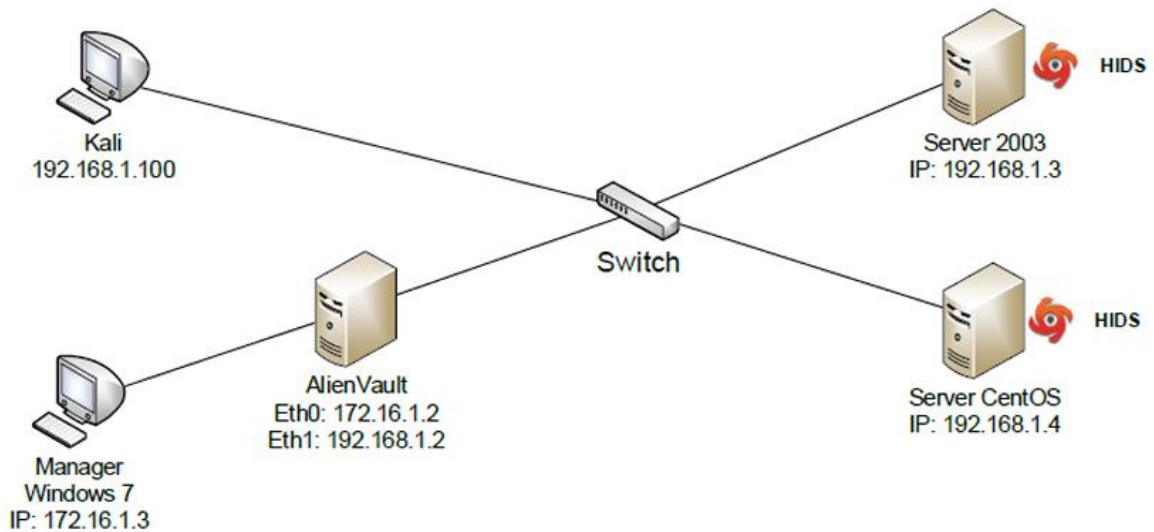
Sinh viên thực hiện: Nguyễn Hữu Văn – AT190157

Hà Nội, 2025

Mục Lục

I. Mô hình cài đặt	3
II. Cài đặt máy chủ AlienVault.....	3
III. Cấu hình máy chủ AlienVault	5
Cấu hình mạng giám sát.....	5
Cấu hình bộ cảm biến OSSEC	7
IV. Cài đặt và cấu hình OSSEC trên máy tính được giám sát.....	11
Cài đặt và cấu hình OSSEC trên máy Windows	11
Cài đặt và cấu hình OSSEC trên máy Linux.....	12
V. Quản lý AlienVault thông qua giao diện web	14
VI. Thực hiện tấn công vào mật khẩu trên máy Server 2012	16

I. Mô hình cài đặt



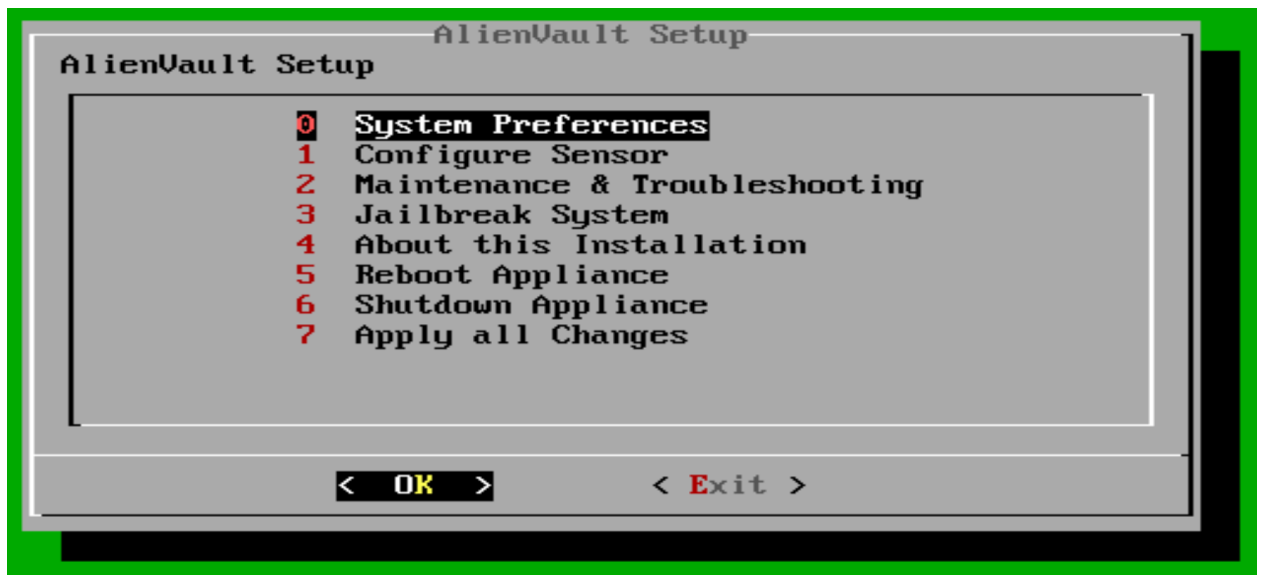
Trong mô hình trên: máy chủ chạy hệ điều hành giám sát AlienVault được kết nối vào mạng nội bộ. Và kết nối với máy vật lý Windows 7 để quản trị. Máy Kali kết nối vào cùng mạng để tấn công. Máy Server 2003 và CentOS chạy các dịch vụ Remote Desktop và web.

II. Cài đặt máy chủ AlienVault

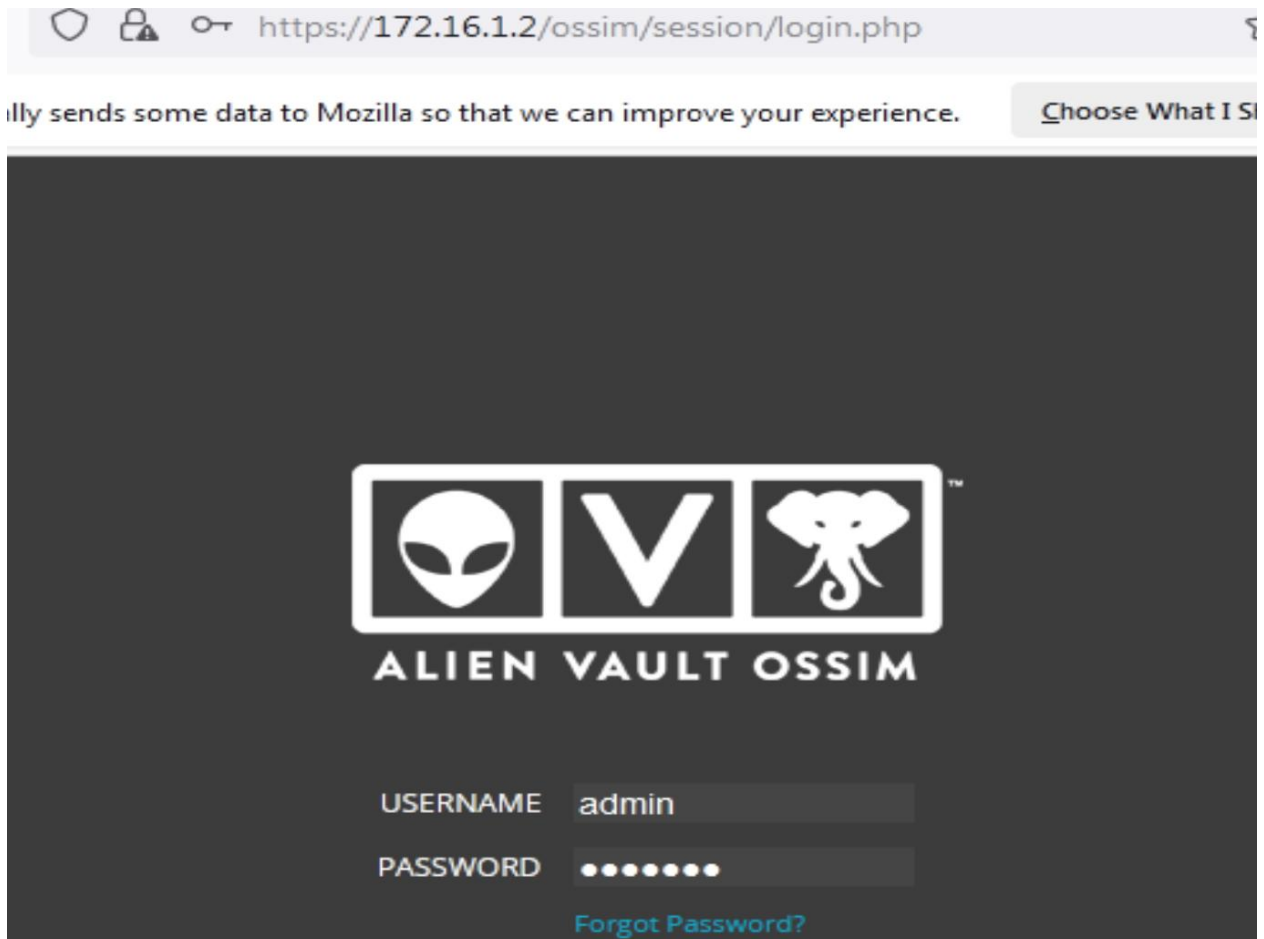
Giao diện đăng nhập khi cài đặt xong hệ điều hành AlienVault:

```
=====
===== http://www.alienvault.com =====
===== Access the AlienVault web interface using the following URL: =====
===== https://172.16.1.2/ =====

AlienVault USM 4.13 - x86_64 - tty1
alienvault login: _
```



Giao diện sau khi cài đặt thành công và truy cập bằng trình duyệt web từ máy quản lý:



III. Cấu hình máy chủ AlienVault

Cấu hình mạng giám sát

Chọn mục 3 (Jailbreak System) như hình trên để vào giao diện cấu hình mạng bằng dòng lệnh. Truy cập theo đường dẫn và điền các thông tin như sau vào giao diện mạng Eth1: alienvault:~# vi /etc/network/interfaces

```
auto eth0
iface eth0 inet static
    address 172.16.1.2
    netmask 255.255.255.0
    network 172.16.1.0
    broadcast 172.16.1.255
    gateway 172.16.1.1
    # dns-* options are implemented by the resolvconf package
    dns-nameservers 172.16.1.1
    dns-search alienvault

auto eth1
iface eth1 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
```

```
alienvault:~# service networking restart
Running /etc/init.d/networking restart is deprecated because it may
gain some interfaces ... (warning).
Reconfiguring network interfaces...Reloading Squid HTTP Proxy 3.x
files.
done.
Reloading Squid HTTP Proxy 3.x configuration files.
done.
done.
alienvault:~#
```

```

alienvault:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e6:5f:51
          inet addr:172.16.1.2  Bcast:172.16.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1090 (1.0 KiB)  TX bytes:4536 (4.4 KiB)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:e6:5f:5b
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:27595 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27595 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20384229 (19.4 MiB)  TX bytes:20384229 (19.4 MiB)

```

Kiểm tra kết nối với các máy tính Windows Server và Linux Ubuntu bằng lệnh Ping:

```

alienvault:~# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_req=1 ttl=128 time=2.55 ms
64 bytes from 192.168.1.3: icmp_req=2 ttl=128 time=0.524 ms
^C
--- 192.168.1.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.524/1.538/2.553/1.015 ms
alienvault:~# ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_req=1 ttl=64 time=2.29 ms
64 bytes from 192.168.1.4: icmp_req=2 ttl=64 time=0.513 ms
^C
--- 192.168.1.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.513/1.405/2.298/0.893 ms

```

Ping từ máy Win server và Ubuntu tới AlienVault:

```

Ping statistics for 192.168.1.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
Control-C
^C
C:\Users\Administrator>

```

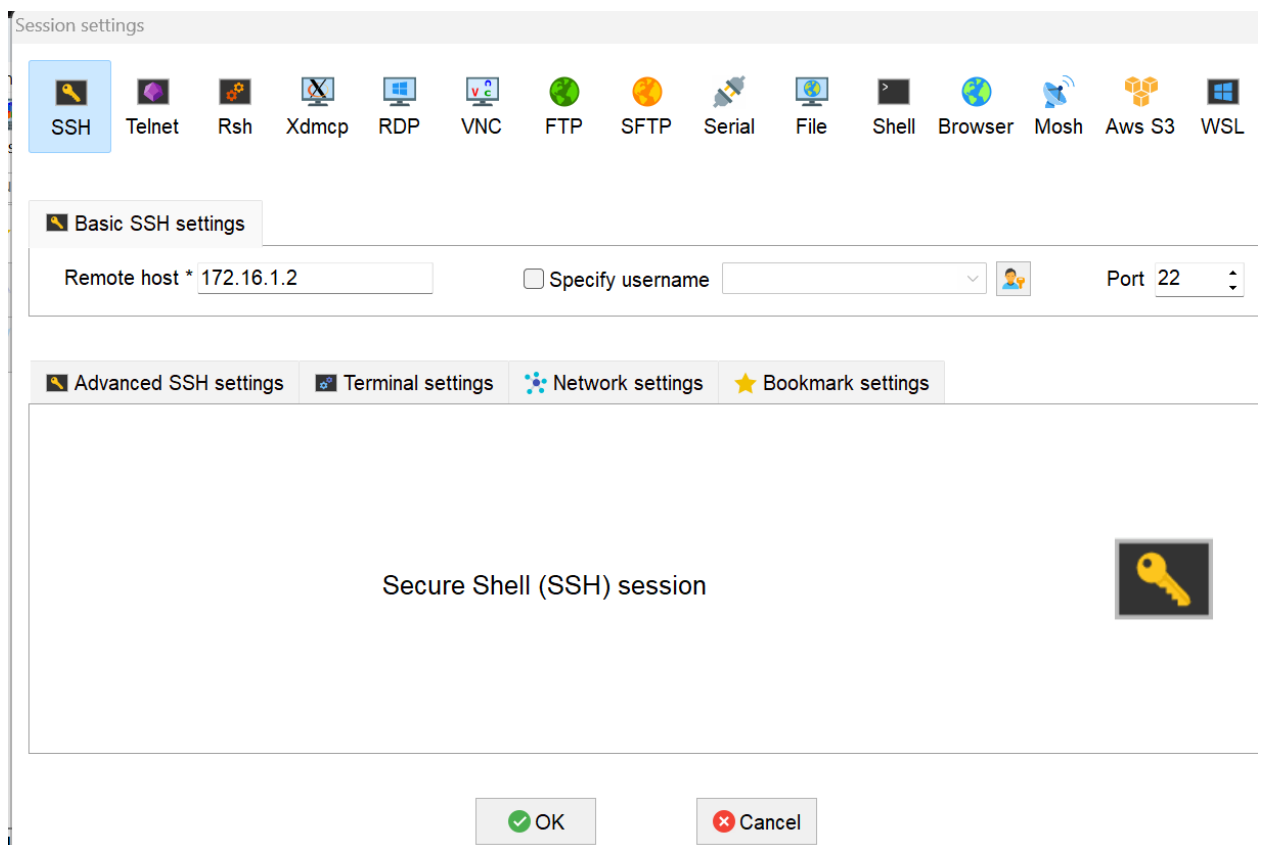
```

at190157@at190157:~/Desktop$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=1.39 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.629 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.629/1.009/1.389/0.380 ms

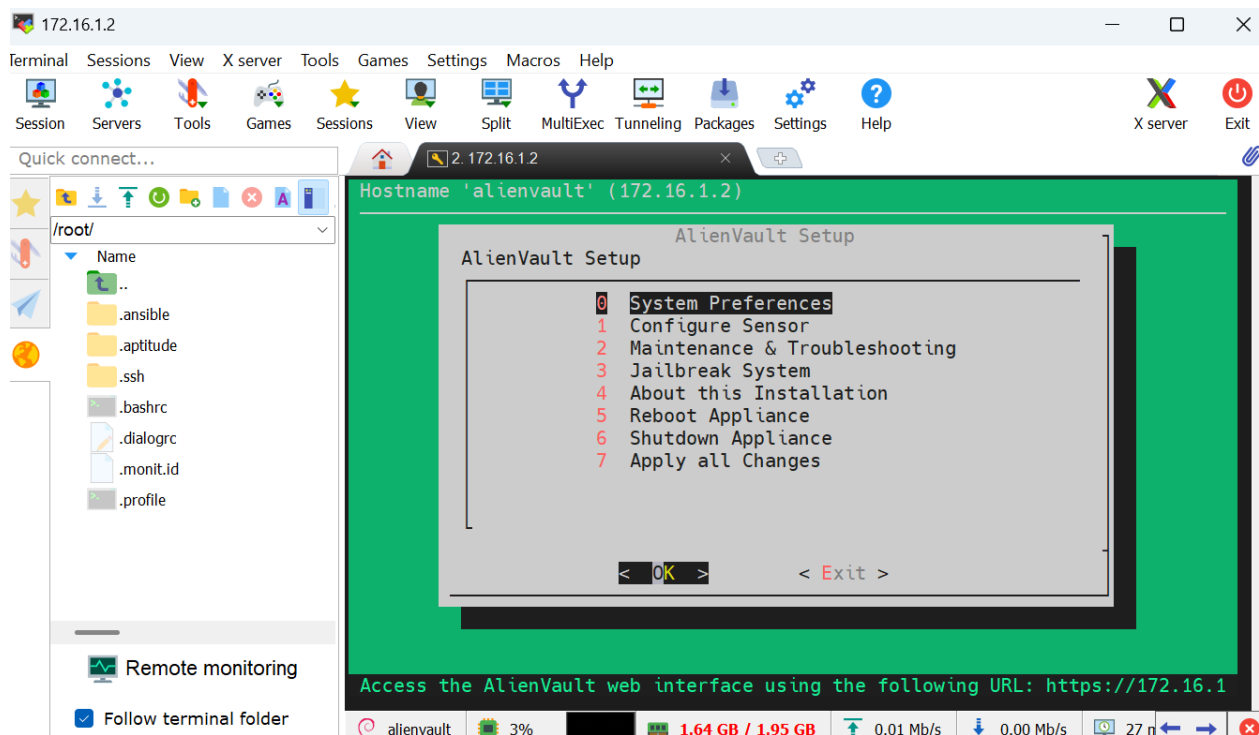
```

Cấu hình bộ cảm biến OSSEC

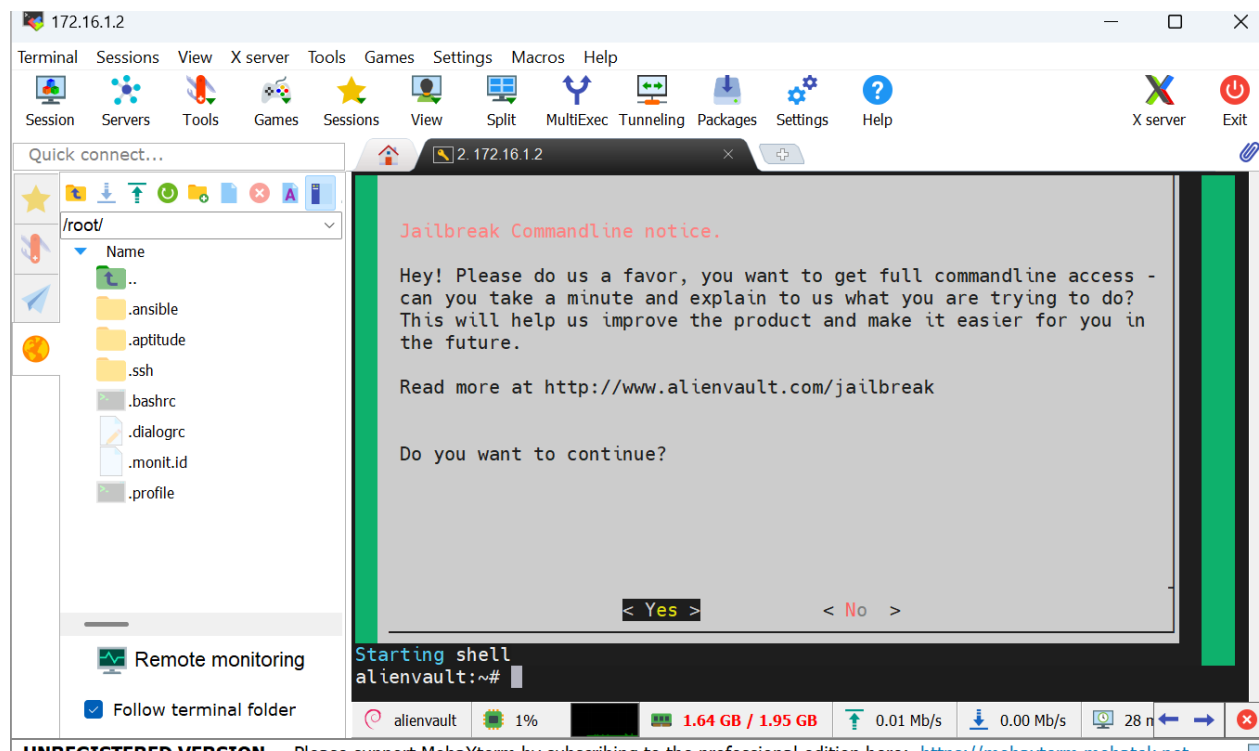
Sau khi cấu hình mạng hoàn tất, tiếp theo phải cấu hình các thông số về máy tính được giám sát bao gồm: tên máy, địa chỉ IP. Sau đó phải tạo khóa xác thực giữa máy chủ AlienVault và máy được giám sát. Để làm được điều này cần sử dụng phần mềm kết nối thông qua giao thức SSH tới AlienVault. Sử dụng MobaXterm để kết nối:



Giao diện quản trị AlienVault xuất hiện:



Chọn chức năng số 3 để vào cửa sổ dòng lệnh:




```
Starting shell
alienvault:~# cd /var/ossec/bin/
alienvault:/var/ossec/bin# ./manage_agents

*****
* OSSEC HIDS v2.8 Agent manager.      *
* The following options are available: *
*****
  (A)dd an agent (A).
  (E)xtract key for an agent (E).
  (L)ist already added agents (L).
  (R)emove an agent (R).
  (Q)uit.
Choose your action: A,E,L,R or Q: █
```

Chọn A để thêm thông tin về máy tính được giám sát:

```
  * A name for the new agent: Server2012
  * The IP Address of the new agent: 192.168.1.3
  * An ID for the new agent[001]:
Agent information:
  ID:001
  Name:Server2012
  IP Address:192.168.1.3

Confirm adding it?(y/n): y
Agent added.
```

Tiếp tục chọn E để trích xuất khóa xác thực sử dụng cho máy Windows 2012.

```
Choose your action: A,E,L,R or Q: E

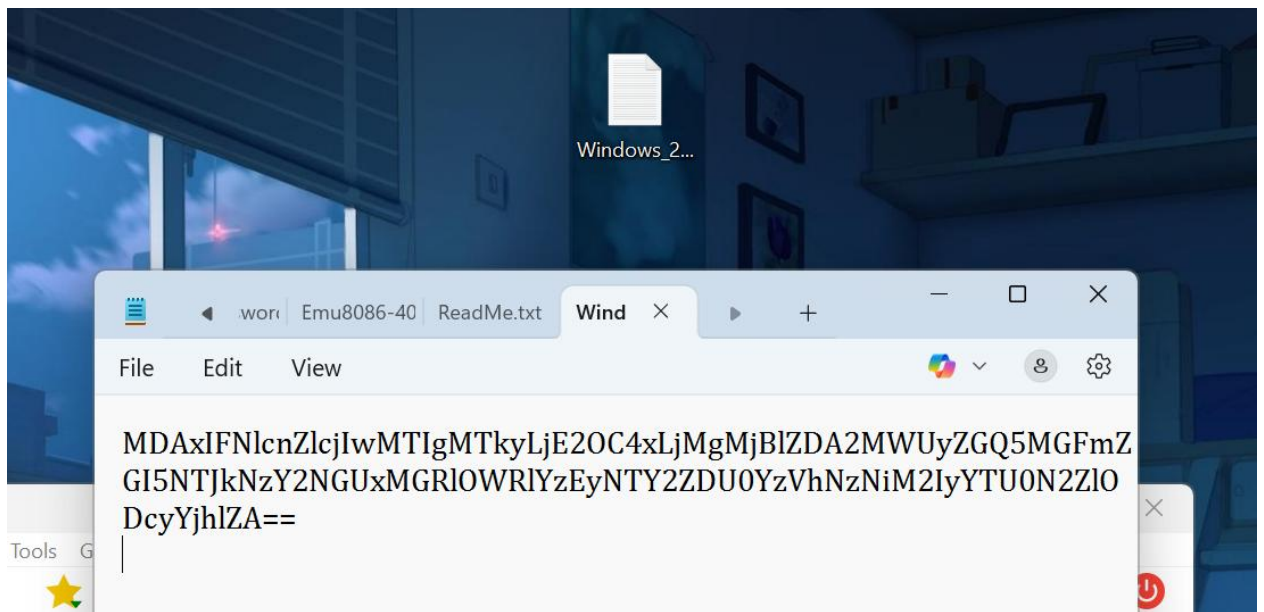
Available agents:
  ID: 001, Name: Server2012, IP: 192.168.1.3
Provide the ID of the agent to extract the key (or '\q' to quit):

** Invalid ID '' given. ID is not present.
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIFNlcnZlcjIwMTIgMTkyLjE2OC4xLjMgMjBlZDA2MWUyZGQ5MGFmZGI5NTJkNzY2NGUxMGRlOWRlYzEyNTY2ZDU0YzVhNzNiM2IyYTU0N2ZlODcyYjhlZA==

** Press ENTER to return to the main menu.
█
```

Lưu các key vào 1 file:



Tiếp tục quay lại thiết lập agent là máy linux:

```
Choose your action: A,E,L,R or Q: A
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: webserver
* The IP Address of the new agent: 192.168.1.4
* An ID for the new agent[002]:
Agent information:
ID:002
Name:webserver
IP Address:192.168.1.4

Confirm adding it?(y/n): y
Agent added.

*****
* OSSEC HIDS v2.8 Agent manager. *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
```

Tiếp tục chọn E để trích xuất khóa xác thực sử dụng cho máy Linux:

```

(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
  ID: 001, Name: Server2012, IP: 192.168.1.3
  ID: 002, Name: webserver, IP: 192.168.1.4
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIHdlYnNlcnZlciAxOTIuMTY4LjEuNCA3YWFiOGZmNzE3Y2I0ZmI1NGRlYTk3Y2E3MjA3M2E3MTV
jOWE0M2I3OGI4M2Y3YWZhMGRlNzM5Y2VmODBjNjY4

** Press ENTER to return to the main menu.

```

IV. Cài đặt và cấu hình OSSEC trên máy tính được giám sát

Cài đặt và cấu hình OSSEC trên máy Windows

Kích hoạt chức năng ghi lại hành động đăng nhập bằng tài khoản của Windows Server 2012 bằng cách: Start → Administrative Tools → Local Security Policy. Trong mục Audit Policy kích hoạt ghi lại hành động đăng nhập cả thành công và thất bại.

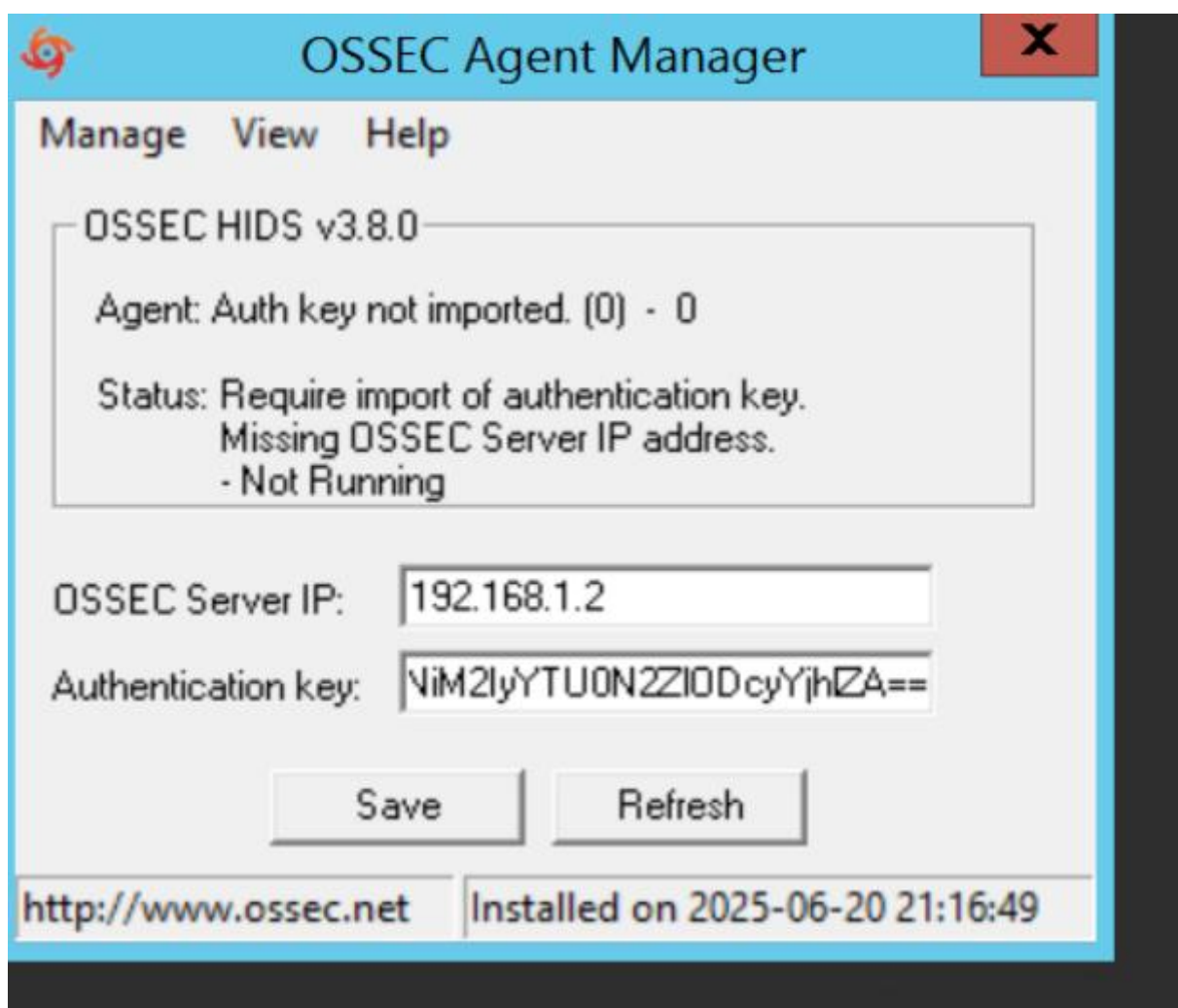
Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Tiếp theo cài đặt phần mềm Ossec agent

Sau khi cài đặt thành công nhập thông tin về máy chủ OSSEC: IP, Key Authentication đã trích xuất ở bước trên. Nhấn Save để lưu thông tin và truy cập vào Tab Manage → Start OSSEC để chạy ứng dụng.



Cài đặt và cấu hình OSSEC trên máy Linux

Vào thư mục cài OSSEC chạy lệnh `./install.sh`

Hệ thống hỏi thông tin về chế độ cài đặt của OSSEC:

```
1- What kind of installation do you want (server, agent, local, hybrid or help)?
agent

- Agent(client) installation chosen.

2- Setting up the installation environment.

- Choose where to install the OSSEC HIDS [/var/ossec]:

- Installation will be made at /var/ossec .

3- Configuring the OSSEC HIDS.

3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 192.168.1.2

- Adding Server IP 192.168.1.2

3.2- Do you want to run the integrity check daemon? (y/n) [y]:
```

```
3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 192.168.1.2

- Adding Server IP 192.168.1.2

3.2- Do you want to run the integrity check daemon? (y/n) [y]:

- Running syscheck (integrity check daemon).

3.3- Do you want to run the rootkit detection engine? (y/n) [y]:

- Running rootcheck (rootkit detection).

3.4 - Do you want to enable active response? (y/n) [y]:

3.5- Setting the configuration to analyze the following logs:
-- /var/log/auth.log
-- /var/log/syslog
-- /var/log/dpkg.log
-- /var/log/snort/alert (snort-full file)

- If you want to monitor any other file, just change
the ossec.conf and add a new localfile entry.
Any questions about the configuration can be answered
```

```
root@at190157:/home/at190157/Downloads/ossec-hids-3.8.0# cd /var/ossec/bin
root@at190157:/var/ossec/bin# ./manage_agents
```



```

* The following options are available: *
*****
(I)mport key from the server (I).
(Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAyIHdlYnNlcnZlciAxOTIuMTY4LjEuNCA3YWFiOGZmNzE
3Y2I0ZmIiNGRlYTk3Y2E3MjA3M2E3MTVjOWE0M2I3OGI4M2Y3YWVhMGRlNzMSY2VmODBjNjY4

Agent information:
  ID:002
  Name:webserver
  IP Address:192.168.1.4

Confirm adding it?(y/n): y
2025/06/20 21:50:49 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No s
uch file or directory
Added.
** Press ENTER to return to the main menu.

```

Sử dụng lệnh sau để khởi động lại dịch vụ trên cả máy chủ AlienVault và Linux:
Restart lại dịch vụ và kiểm tra agent đã kết nối:

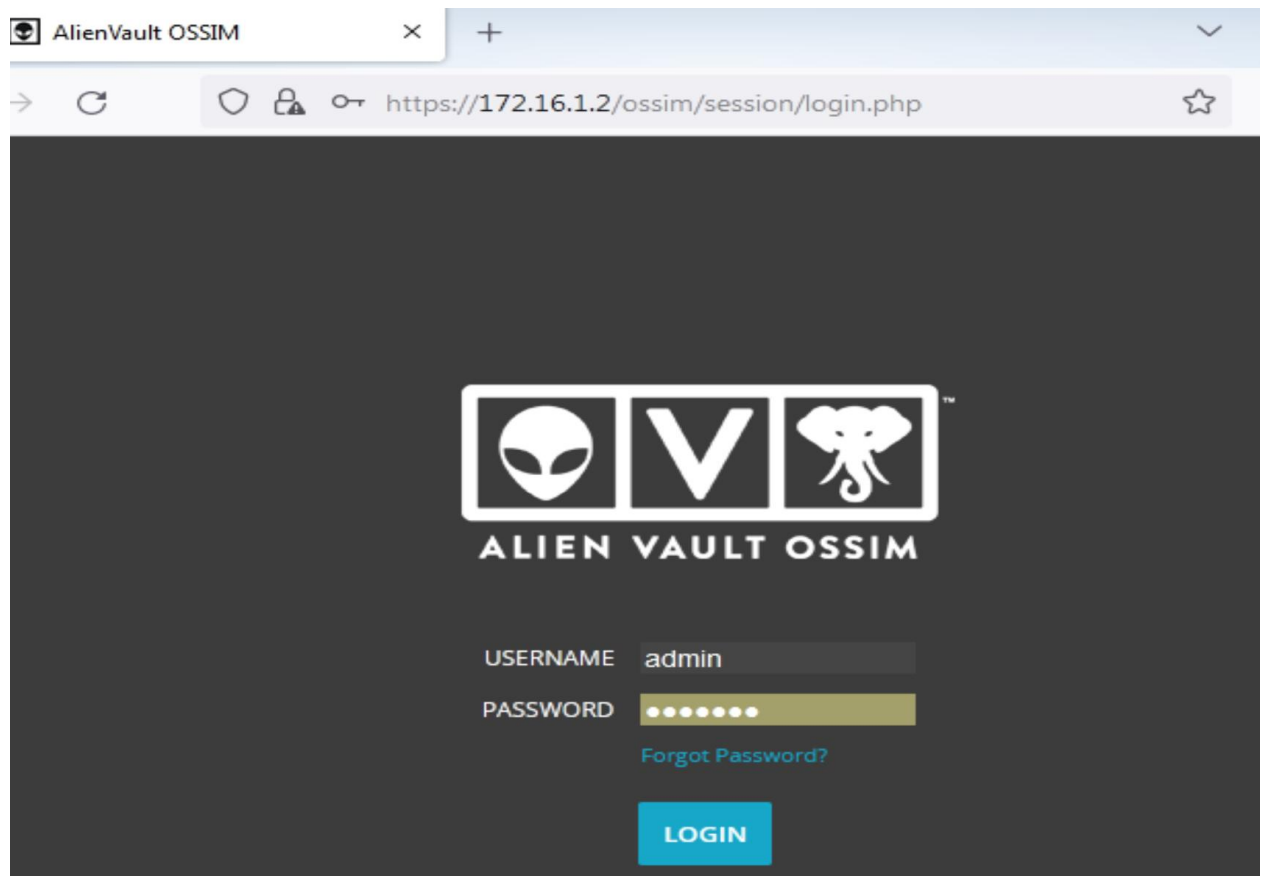
```

alienvault:/var/ossec/bin# ./list_agents -c
webserver-192.168.1.4 is active.
Server2012-192.168.1.3 is active.
alienvault:/var/ossec/bin#


```

V. Quản lý AlienVault thông qua giao diện web


Quản lý AlienVault thông qua giao diện web gồm các chức năng chính như:
Theo dõi hoạt động, giám sát hành vi, trạng thái của các agent đã kết nối. Phát
hiện các dấu hiệu tấn công. Sử dụng trình duyệt web truy cập theo địa chỉ IP:
<https://172.16.1.2>




Trong Tab phân tích, chọn chức năng phân tích sự kiện an toàn (Security events)
Chọn Real Time để theo dõi sự kiện theo thời gian thực:




DASHBOARDS



ANALYSIS



ENVIRONMENT



REPORTS

SECURITY EVENTS (SIEM)

SIEM


REAL-TIME

PAUSE

Done. [15 new rows]

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE
2025-06-20 15:04:22	ossec: Login session closed [USERNAME].	0	ossec-syslog	alienvault	172.16.1
2025-06-20 15:04:22	ossec: Login session closed [USERNAME].	0	ossec-syslog	alienvault	172.16.1
2025-06-20 15:04:22	ossec: Login session closed [USERNAME].	0	ossec-syslog	alienvault	172.16.1

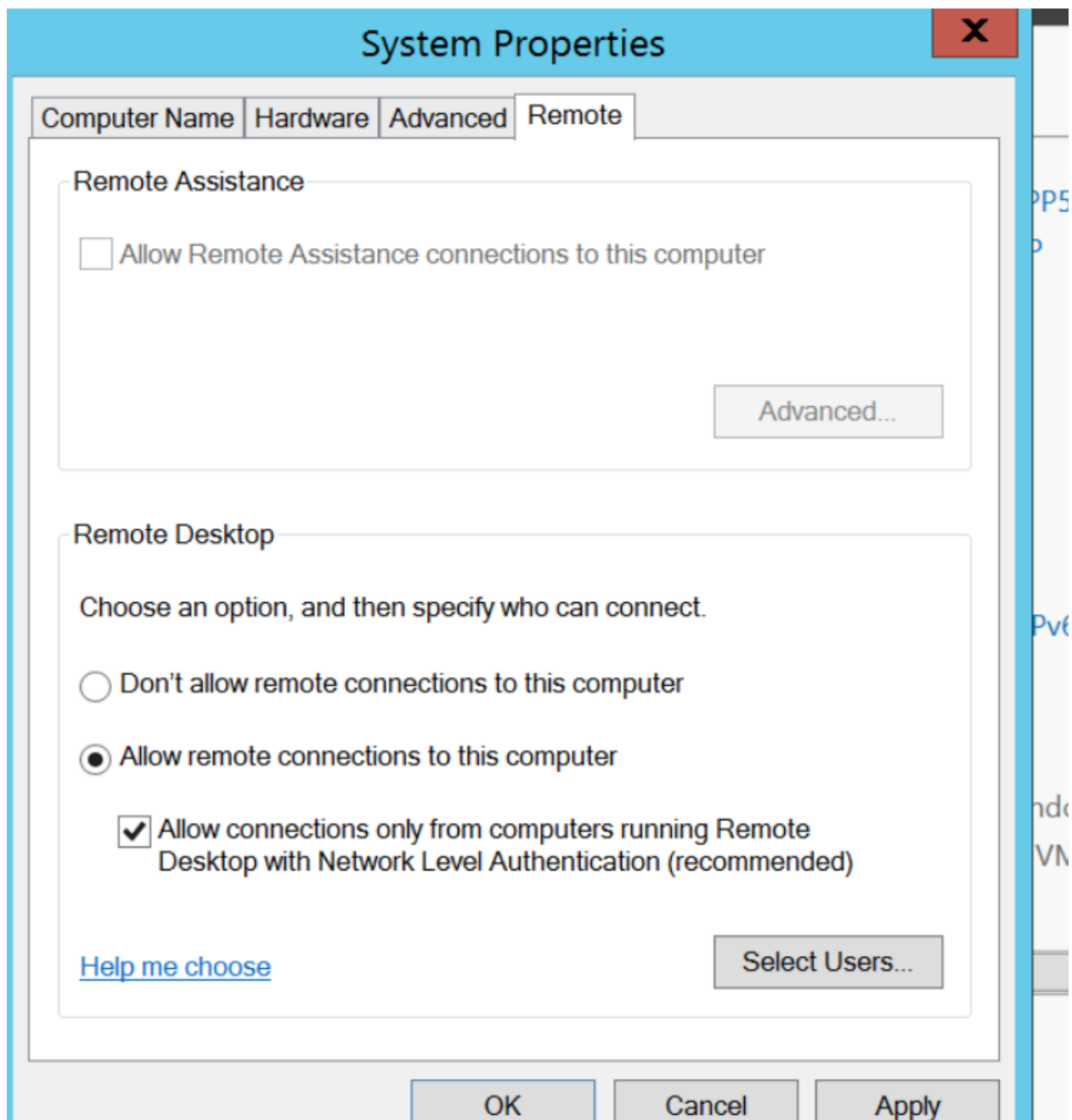
Trong Tab Environment chọn Detection để xem các trạng thái hoạt động của các agent hiện tại:



ID	NAME	IP/CIDR	CURRENT IP	CURRENT USER@DOMAIN	STATUS
000	alienvault (server)	127.0.0.1	-	-	Active/Local
001	Server2012	192.168.1.3	192.168.1.3	-	Active
002	webserver	192.168.1.4	192.168.1.4	-	Active

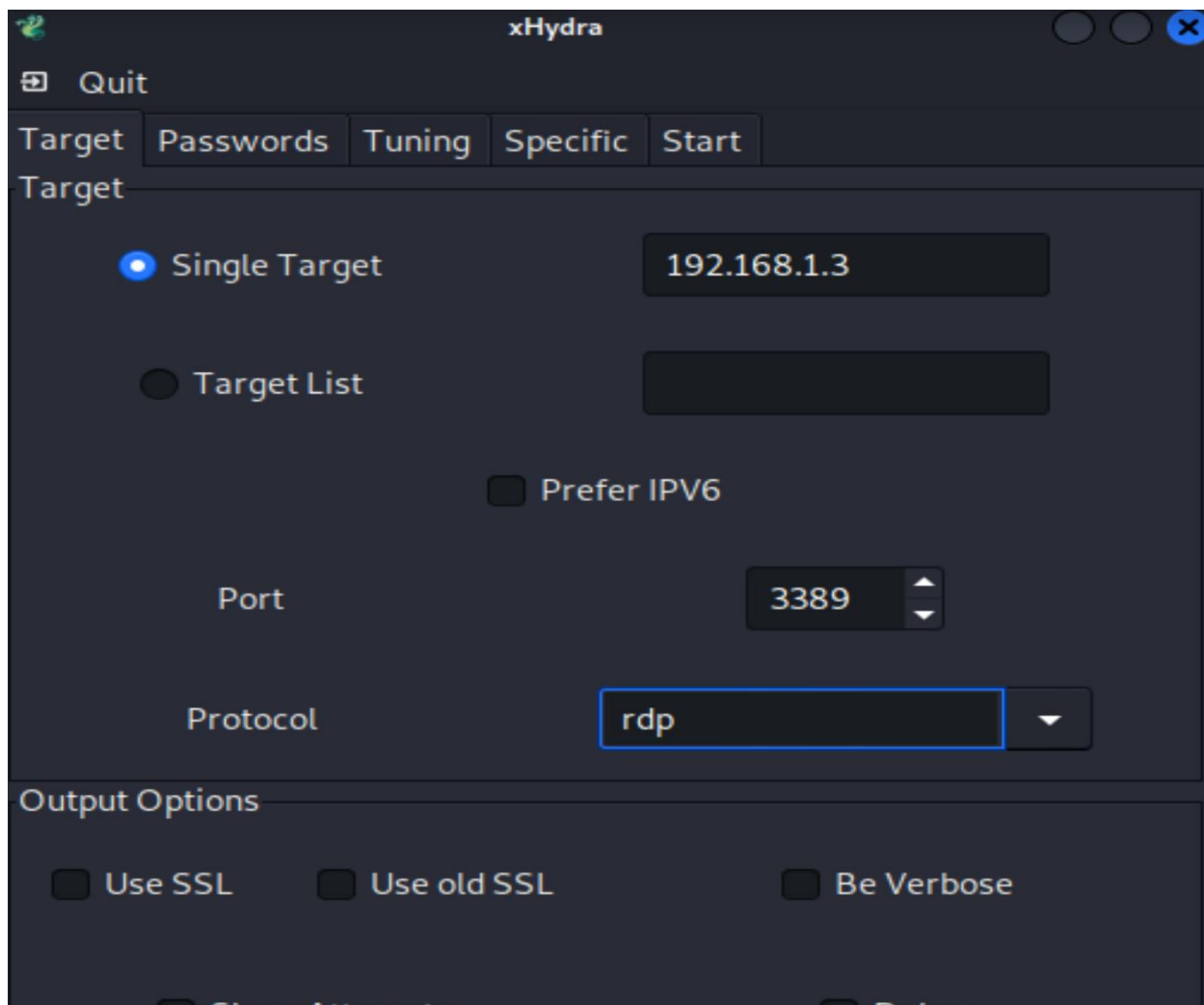
VI. Thực hiện tấn công vào mật khẩu trên máy Server 2012

Sử dụng máy trạm Kali Linux để tấn công từ điển mật khẩu vào tài khoản Administrator trên Server 2012: Trên máy Server 2012 bật dịch vụ truy cập từ xa Remote Desktop:

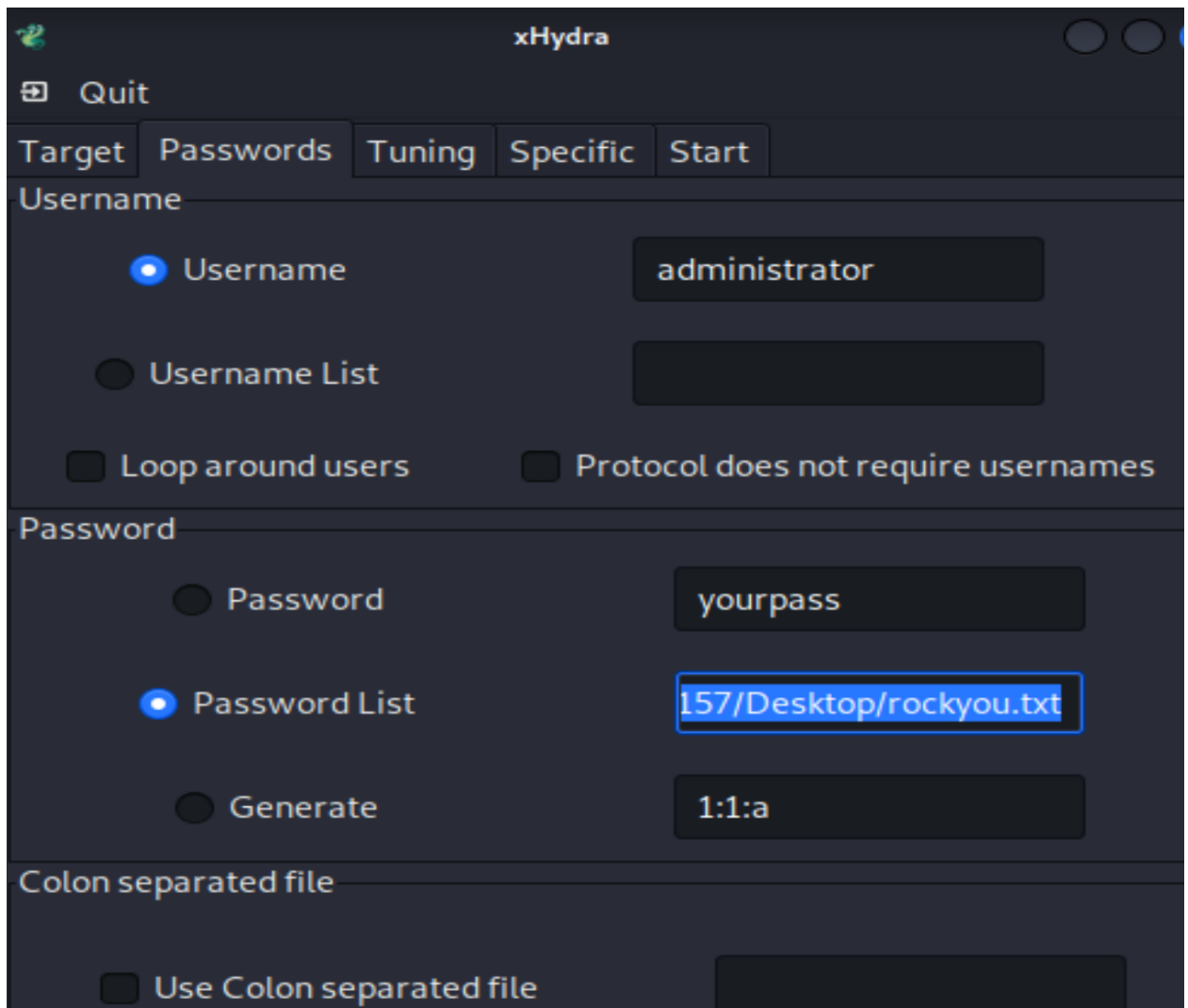


Trên máy Kali: Bật công cụ xhydra để tấn công mật khẩu bằng từ điển:

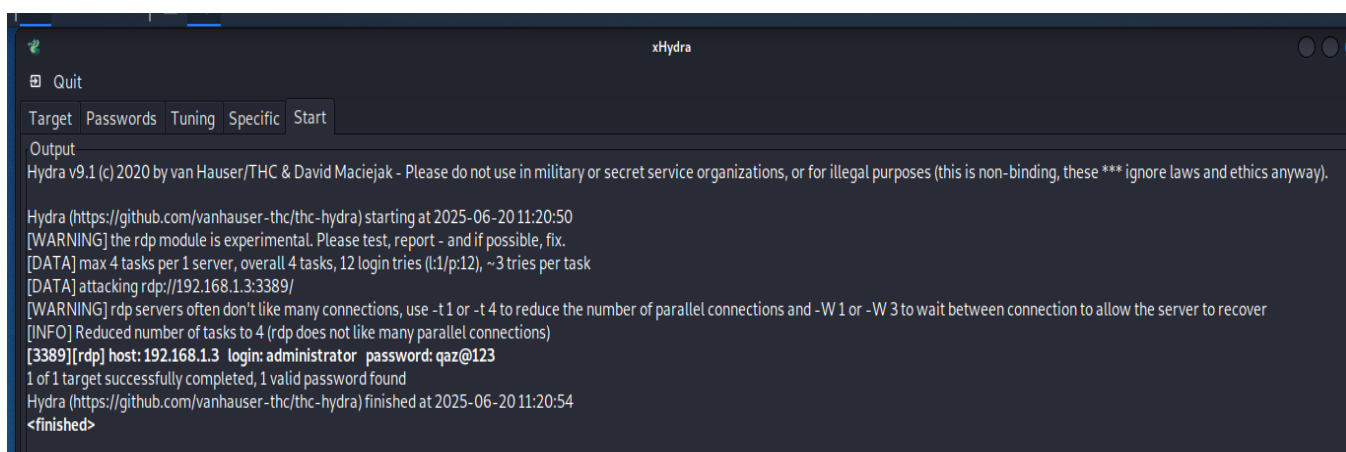
Trong Tab Target nhập địa chỉ IP của máy Server 2012, nhập cổng dịch vụ Remote Desktop là 3389, giao thức rdp:



Ở tab Passwords chọn file mật khẩu:



Tấn công thành công vào tài khoản Administrator với mật khẩu qaz@123 chứa trong từ điển:



Chuyển sang giao diện web quản trị AlienVault với chức năng giám sát thời gian thực, phát hiện sự kiện tấn công:

ossec-win_authentication_failed	alienvault	192.168.1.100:35852	192.168.1.3
ossec-win_authentication_failed	alienvault	192.168.1.100:35858	192.168.1.3
ossec-win_authentication_failed	alienvault	192.168.1.100:35850	192.168.1.3

Từ sự kiện này biết được địa chỉ đích tấn công và nguồn bị tấn công. Với dấu hiệu là rất nhiều sự kiện xác thực không thành công, vì vậy có thể kết luận máy Server 2012 đang bị tấn công vào mật khẩu