

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 04
**TRIỂN KHAI HỆ THỐNG GIÁM SÁT
ALIENVAULT**

Người xây dựng bài thực hành:

Th.S Cao Minh Tuấn

HÀ NỘI, 2015

MỤC LỤC

Mục lục	2
Thông tin chung về bài thực hành	3
Chuẩn bị bài thực hành	4
Đối với giảng viên	4
Đối với sinh viên	4
 CÀI ĐẶT HỆ THỐNG giám sát an ninh mạng alienvault	 5
1.1. Chuẩn bị	5
1.2. Mô hình cài đặt.....	6
1.3. Cài đặt máy chủ AlienVault.....	6
1.4. Cấu hình máy chủ AlienVault.....	9
1.4.1. Cấu hình mạng giám sát	9
1.4.2. Cấu hình bộ cảm biến OSSEC	11
1.5. Cài đặt và cấu hình OSSEC trên máy tính được giám sát	14
1.5.1. Cài đặt và cấu hình OSSEC trên máy Windows	14
1.5.2. Cài đặt và cấu hình OSSEC trên máy Linux.....	15
1.6. Quản lý AlienVault thông qua giao diện web.....	18
1.7. Thực hiện tấn công vào mật khẩu trên máy Server 2003	20
1.8. Thực hiện tấn công quét lỗ hổng đối với mã nguồn website	23

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Triển khai hệ thống giám sát AlienVault

Module: An toàn mạng máy tính

Số lượng sinh viên cùng thực hiện: 02

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
 - + Mỗi sinh viên được bố trí 01 máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 8GB, HDD 50GB
- Yêu cầu phần mềm trên máy:
 - + Hệ điều hành Windows XP, CentOS, Kali, AlienVault, Ossec agent.
 - + VMware Workstation 9.0 trở lên
- Công cụ thực hành:
 - + Máy ảo VMware: Windows XP SP3, Windows 7, Kali Linux, CentOS Linux. Trên mỗi máy ảo có ít nhất 02 phân vùng ổ cứng. Trong đó phân vùng C: chứa hệ điều hành, phân vùng D: có ít nhất 10 GB còn trống.
 - + Phần mềm máy chủ AlienVault 4.15-64bit.
 - + Phần mềm Host IDS OSSEC cho Windows và Linux.
 - + Máy ảo CentOS Linux đã cài website.
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: không
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

- Phần mềm Ossec agent 2.8

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

CÀI ĐẶT HỆ THỐNG GIÁM SÁT AN NINH MẠNG ALIENVAULT

Bài thực hành này sinh viên phải cấu hình các máy tính liên quan kết nối được với nhau trước khi cài các phần mềm.

Đối với máy chủ chạy hệ thống giám sát trung tâm AlienVault cần phải có cấu hình mạng để hiển thị thông tin giám sát.

1.1. Mô tả

Để phát hiện kịp thời các cuộc tấn công mạng, cung cấp nguồn dữ liệu khi điều tra xử lý sự cố an toàn thông tin thì hệ thống giám sát an ninh mạng là một giải pháp tối ưu.

Bộ công cụ giám sát an ninh mạng mã nguồn mở AlienVault đáp ứng được hầu hết các yêu cầu của hệ thống. Do đó nó có thể được sử dụng trong học tập và nghiên cứu.

Trong nội dung bài thực hành này ứng dụng AlienVault để thu thập và phát hiện tấn công cho máy chủ chạy hệ điều hành Windows Server và Linux web server.

1.2. Chuẩn bị

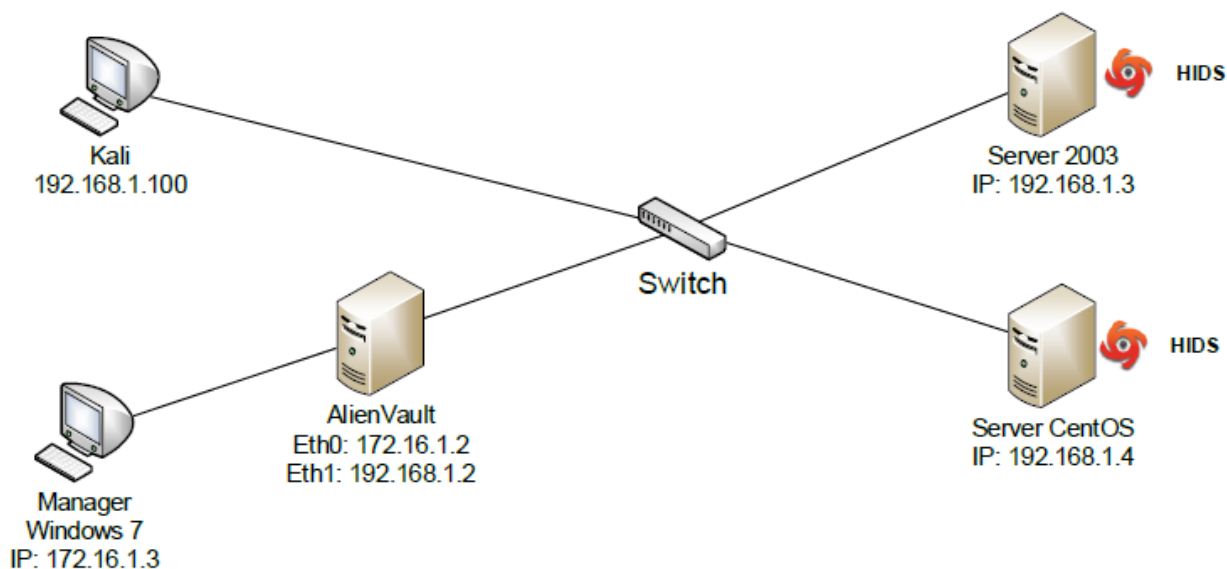
Mô hình này cần phải có 03 máy tính vật lý. Mỗi máy có chức năng như sau:

+ Máy tính 01: Tạo máy ảo có RAM > 3GB. Để chạy hệ điều hành giám sát AlienVault.

+ Máy tính 02: Tạo 02 máy ảo: Máy ảo chạy hệ điều hành Windows Server 2003 có mở cổng 3389 (Remote Desktop). Máy ảo chạy hệ điều hành Linux CentOS 6.5 có cài đặt website.

+ Máy tính 03: Chạy máy ảo Kali Linux để tấn công, và cài đặt phần mềm Acunetix trên máy XP để quét lỗ hổng website.

1.3. 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.

1.4. Cài đặt máy chủ AlienVault

Phần mềm máy chủ AlienVault đã được hãng sản xuất đóng gói thành bản ISO để cài đặt như hệ điều hành Linux.

Sau khi chèn đĩa cài đặt (file ISO) vào máy ảo, khởi động máy sẽ xuất hiện như hình sau:



Install AlienVault OSSIM 4.15.2 (64 Bit)
Install AlienVault Sensor 4.15.2 (64 Bit)

Nhấn Enter để bắt đầu cài đặt.

- Trong giao diện lựa chọn ngôn ngữ chọn English.
- Các giao diện tiếp theo chọn mặc định.
- Đến giao diện cấu hình mạng. Lựa chọn Interface mà kết nối với máy tính quản trị. Trong bài thực hành này chọn Eth0.



Configure the network

Your system has multiple network interfaces. Choose the one to use as the installation. If possible, the first connected network interface found has been selected.

Primary network interface:

eth0: Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]

eth1: Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]

- Tiếp tục cấu hình địa chỉ IP của Interface này, đây là địa chỉ IP trong mạng quản lý. Theo mô hình mạng trên nó có IP là: 172.16.1.2

Configure the network

The IP address is unique to your computer and consists of four numbers separated by periods. To use here, consult your network administrator.

IP address:

172.16.1.2

- SubnetMask: 255.255.255.0, Gateway: 172.16.1.1
- Tiếp theo nhập mật khẩu cho tài khoản quản trị root:

Note that you will not be able to see the password as you type it.

Root password:

●●●●●●

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●●●

- Các bước tiếp theo để mặc định và quá trình cài đặt bắt đầu:



Install the base system



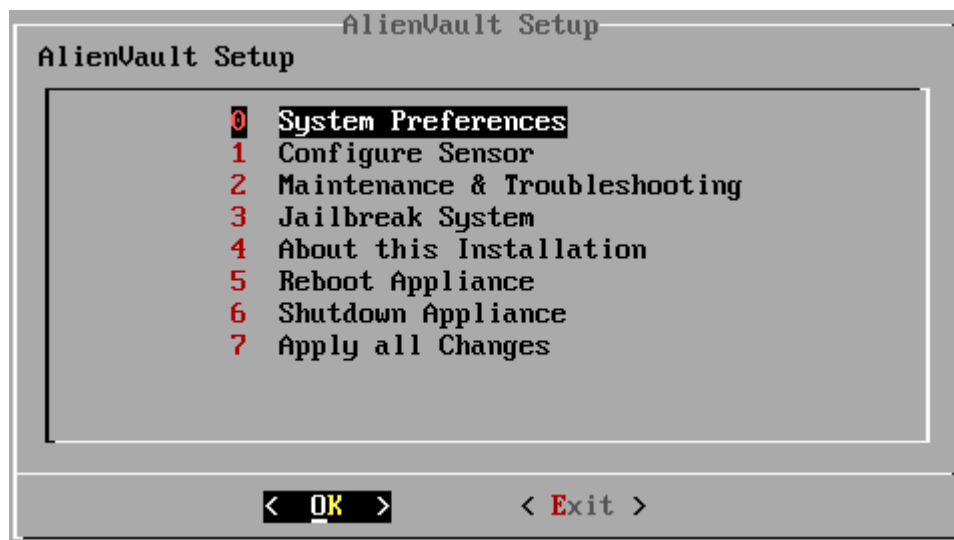
- Giao diện đăng nhập khi cài đặt xong hệ điều hành:

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

AlienVault USM 4.15.2 - x86_64 - tty1

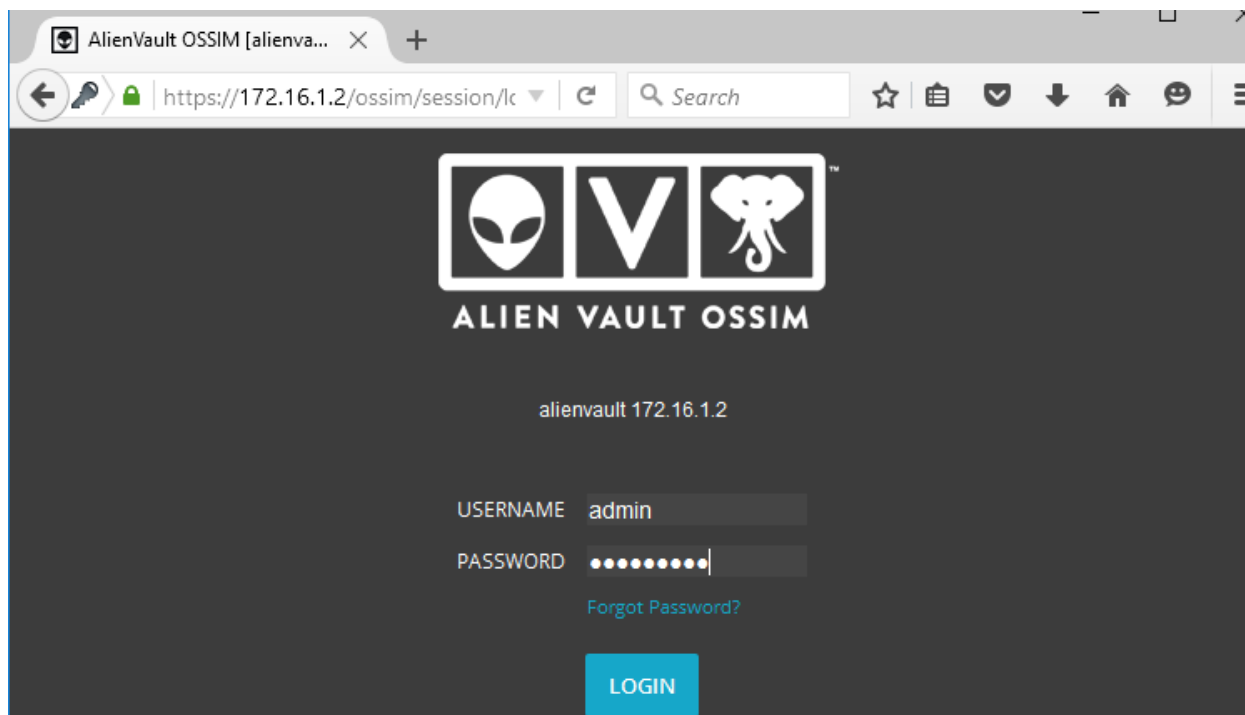
alienvault login: _

- Đăng nhập với quyền root để truy cập vào hệ thống.



Với giao diện này người quản trị có thể cấu hình các chức năng của máy theo dòng lệnh với tùy chọn số 3 (Jailbreak System).

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



1.5. Cấu hình máy chủ AlienVault

1.5.1. Cấu hình mạng giám sát

Trong mục này cần phải cấu hình giao diện mạng cho máy chủ AlienVault để nhận thông tin gửi về từ các máy trạm cài bộ cảm biến (OSSEC client).

- 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
```

```
# The primary network interface
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
    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
```

Khởi động lại cấu hình mạng:

```
alienvault:~# service networking restart
```

Kiểm tra lại cấu hình địa chỉ IP của các giao diện mạng:

```
alienvault:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9e:8f:e4
          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:1057 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1211 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:176368 (172.2 KiB)  TX bytes:1211242 (1.1 MiB)
          Interrupt:19 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0c:29:9e:8f:ee
          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:47 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:6224 (6.0 KiB)  TX bytes:0 (0.0 B)
          Interrupt:16 Base address:0x2080
```

- Kiểm tra kết nối với các máy tính Windows Server 2003 và Linux CentOS 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=2.68 ms
64 bytes from 192.168.1.3: icmp_req=2 ttl=128 time=4.91 ms
64 bytes from 192.168.1.3: icmp_req=3 ttl=128 time=4.12 ms
```

- Từ máy Windows 7 (Manager) truy cập vào máy chủ AlienVault thông qua trình duyệt web với địa chỉ đã được cấu hình trước đó:
- Cấu hình mạng cho máy Linux CentOS:

Truy cập vào máy và bật chương trình dòng lệnh.

Truy cập vào thư mục chứa giao diện mạng của máy theo lệnh sau:

```
[root@webserver ~]# ifconfig eth1 192.168.1.4/24
```

Thực hiện lệnh Ping để kiểm tra kết nối tới máy AlienVault:

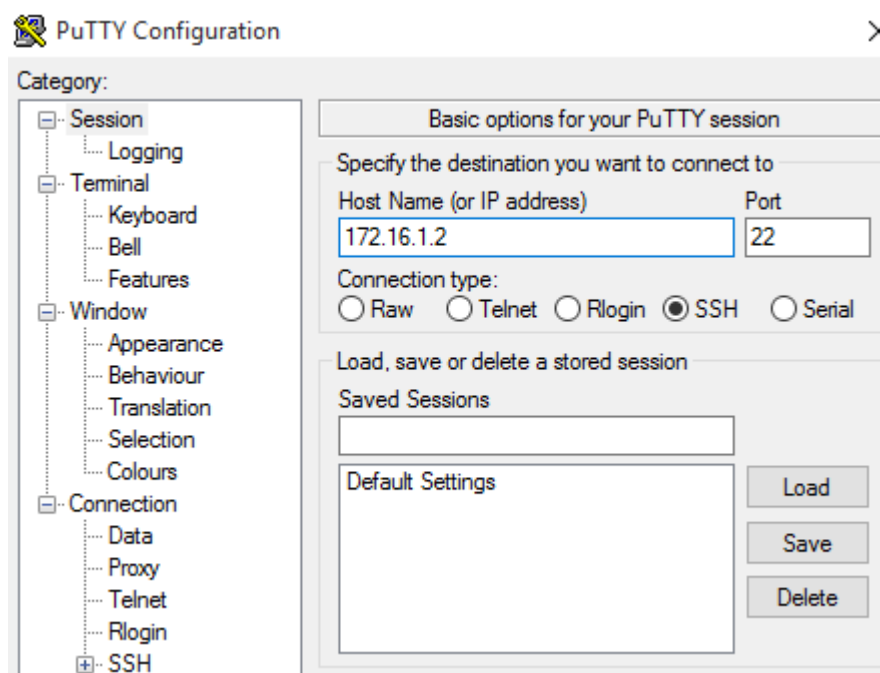
```
[root@webserver ~]# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=1.31 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=1.15 ms
```

Kết quả kết nối thành công.

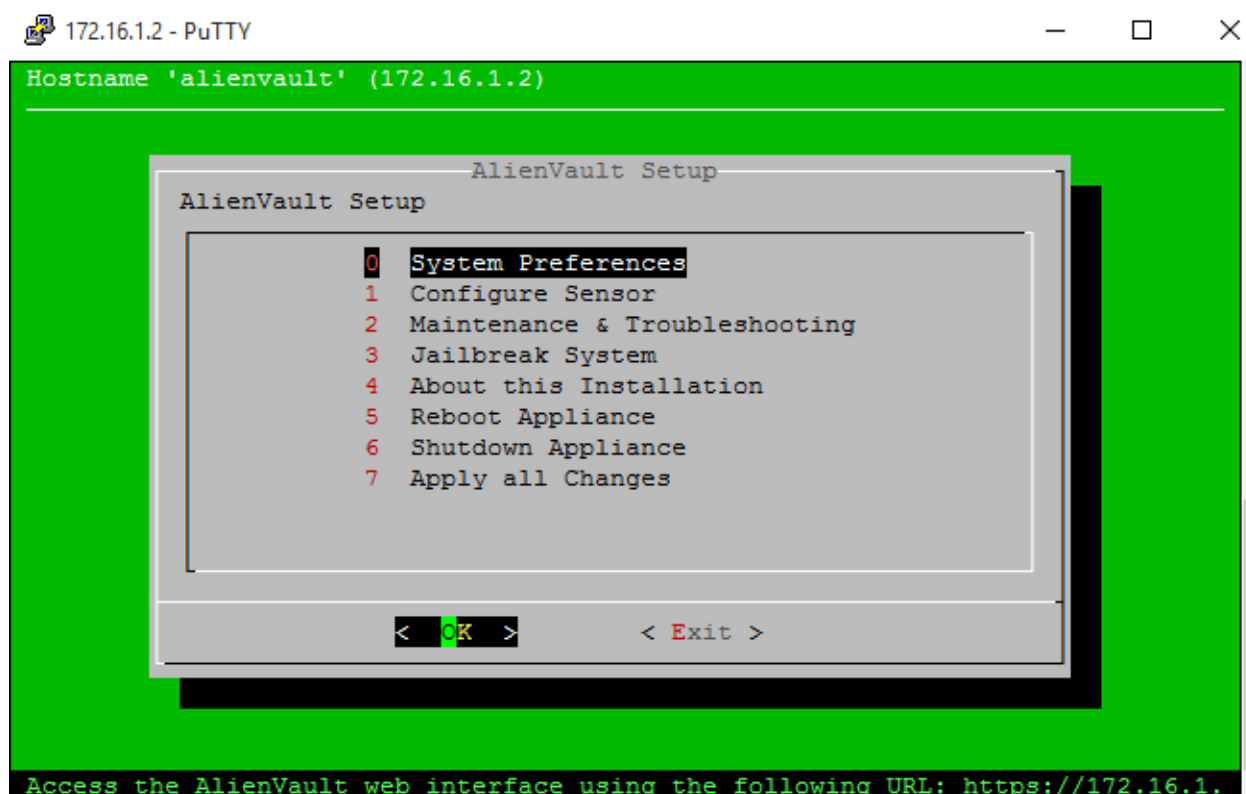
1.5.2. Cấu hình bộ cảm biến OSSEC

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 PuTTY để kết nối:



Giao diện quản trị AlienVault xuất hiện:



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

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

Giao diện quản trị OSSEC xuất hiện:

```
*****
* 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:

```
Adding a new agent (use '\q' to return to the main
menu) .

Please provide the following:
* A name for the new agent: Server2003
* The IP Address of the new agent: 192.168.1.3
* An ID for the new agent[001]:
Agent information:
ID:001
Name:Server2003
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 2003.

```
Available agents:
ID: 001, Name: Server2003, IP: 192.168.1.3
Provide the ID of the agent to extract the key (or
'\q' to quit): 001
```

```
Agent key information for '001' is:
```

```
MDAxIFNlcnZlcjIwMDMgMTkyLjE2OC4xLjMgYzQ3Yjc2NDU3YzQ2Z  
WE1MGI2MTlkNWViNDI2NTA4NWNhMmNmMDZkMDJjZWQ3ZDZmMDNkNG  
IyODhmM2RmYjExNQ==
```

Bôi đen dòng khóa và sao chép vào tệp

Windows_2003_Key_Authentication.txt:

Quay trở lại giao diện chính, thiết lập agent là máy Linux CentOS:

Chọn (A).

Nhập thông tin về tên web server và địa chỉ IP tương ứng:

```
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.
```

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

```
Available agents:
```

```
ID: 001, Name: Server2003, 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:
```

```
MDAyIHdlYnNlcnZlcjAxOTIuMTY4LjEuNCBkOTQ4YTQzNjJjMzAwNjZkZGI  
xM2ZlYzM3YjA0YTczNjg5ZjRlNDJjZDElZWQyZmJjOTY2MTcyMDUzNTZiMj  
I4
```

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

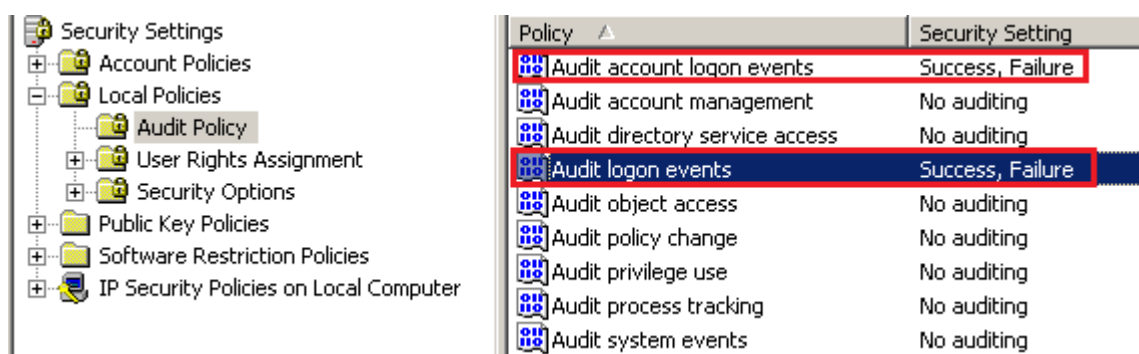
1.6.1. Cài đặt và cấu hình OSSEC trên máy Windows

Để thực hiện giám sát các hành vi tấn công tại các máy tính chạy Windows phải cài đặt công cụ phần mềm OSSEC client trên các máy đó. Khi có sự kiện xảy ra trên máy này OSSEC client sẽ gửi thông tin về máy chủ OSSEC (AlienVault) để phân tích và phát hiện hành vi tấn công.

Kích hoạt chức năng ghi lại hành động đăng nhập bằng tài khoản của Windows Server 2003 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.



Đóng cửa sổ.

Bật cửa sổ dòng lệnh DOS, nhập lệnh để hệ điều hành cập nhật chính sách mới:

```
C:\>gpupdate /force
```

```
Refreshing Policy...
```

```
User Policy Refresh has completed.
```

```
Computer Policy Refresh has completed.
```

```
To check for errors in policy processing, review the event log.
```

Tiếp theo cài đặt phần mềm Ossec agent:

Sao chép phần mềm ossec-agent-win32-2.8 vào máy Windows 2003 và cài đặt:



Nhấn Next và cài đặt theo mặc định.

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.



Chọn Save để lưu thông tin vừa nhập.

Truy cập vào Tab Manage chọn Start OSSEC để chạy dịch vụ.

1.6.2. Cài đặt và cấu hình OSSEC trên máy Linux

Truy cập vào máy webserver Linux và bật cửa sổ dòng lệnh. Chạy các lệnh sau:

```
[root@webserver ~]# yum install make gcc
[root@webserver tmp]# curl -O http://www.ossec.net/files/ossec-hids-2.8.1.tar.gz
[root@webserver tmp]# tar -zxvf ossec*
[root@webserver tmp]# cd ossec-hids-2.8.1
[root@webserver ossec-hids-2.8.1]# ./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]:
        - 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/messages
        -- /var/log/secure
        -- /var/log/maillog
        -- /var/log/httpd/error_log (apache log)
        -- /var/log/httpd/access_log (apache log)
    - 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
by visiting us online at http://www.ossec.net .
    --- Press ENTER to continue ---
```

Nhấn Enter để bắt đầu quá trình cài đặt.

Truy cập vào tiến trình quản lý ossec agent để nhập khóa xác thực đã tạo trên máy AlienVault:


```
[root@webserver ~]# cd /var/ossec/bin
[root@webserver bin]# ./manage_agents
```

Tiến trình quản lý Ossec agent xuất hiện, chọn I để nhập khóa xác thực:

```
*****
* OSSEC HIDS v2.8 Agent manager.          *
* 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):
MDAyIHdlYnNlcnZlciAxOTIuMTY4LjEuNCBkOTQ4YTQzNjJjMzAwNjZkZGI
xM2ZlYzM3YjA0YTczNjg5ZjRlNDJjZDElZWQyZmJjOTY2MTcyMDUzNTZiMj
I4

Agent information:
  ID:002
  Name:webserver
  IP Address:192.168.1.4
Confirm adding it?(y/n): y
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 CentOS: Restart lại dịch vụ và kiểm tra agent đã kết nối:

```
alienvault:~# /var/ossec/bin/ossec-control restart
alienvault:~# /var/ossec/bin/list_agents -c
webserver-192.168.1.4 is active.
Server2003-192.168.1.3 is active.
```

Xong bước này ta đã có 02 máy agent đã được thiết lập để máy chủ AlienVault giám sát sự kiện từ xa.

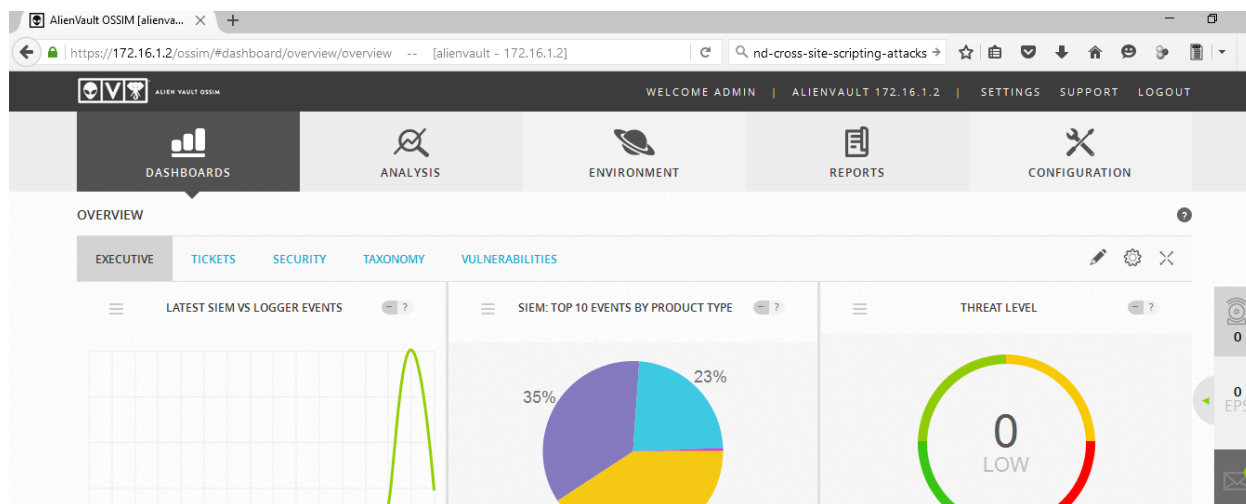
1.7. Quản lý AlienVault thông qua giao diện web

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:

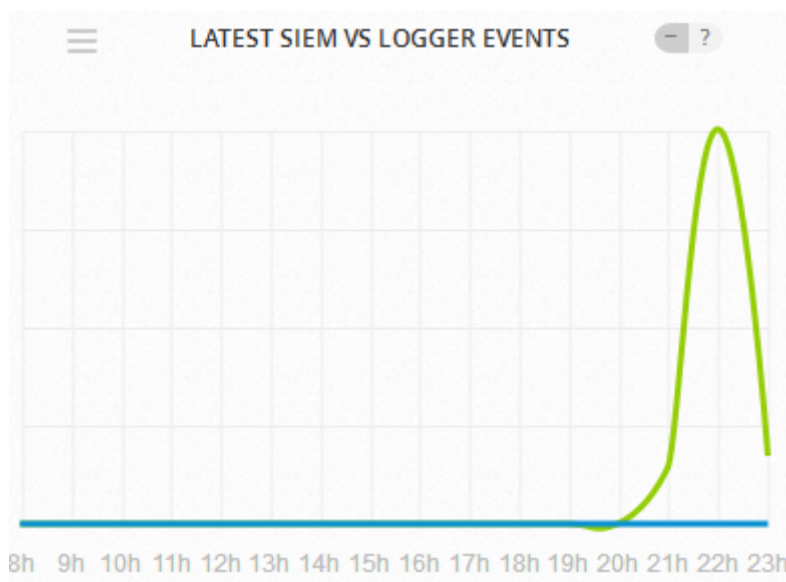
<https://172.16.1.2>

Giao diện tổng quát của AlienVault:

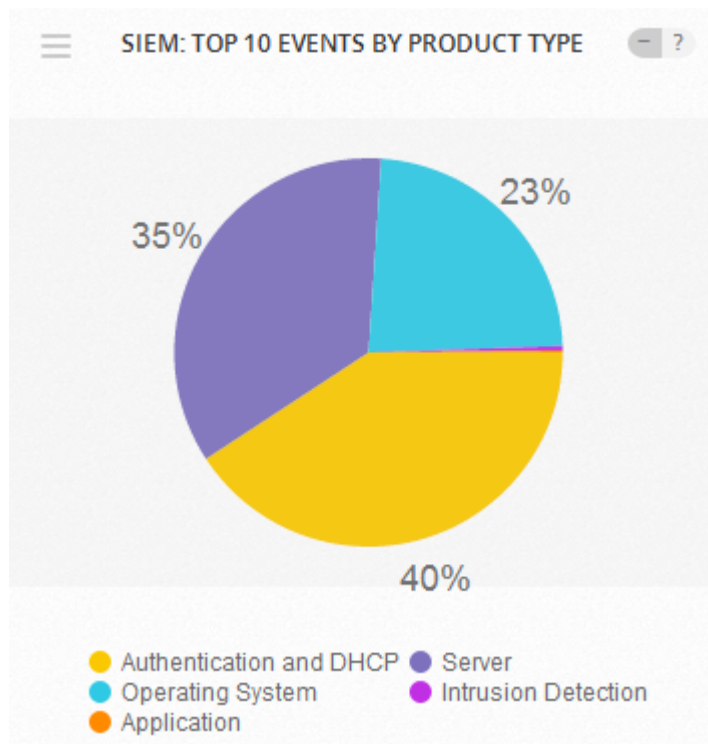


Trong giao diện của Dashboard gồm các sự kiện:

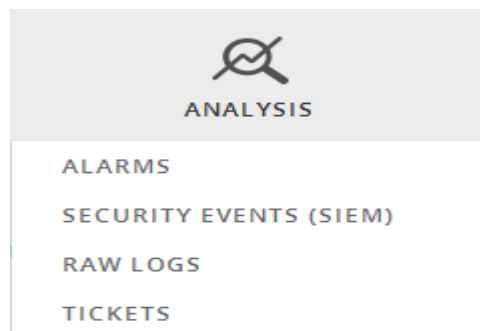
- Đồ thị thống kê về các sự kiện được ghi lại theo thời gian:



- Biểu đồ thống kê về dấu hiệu thu thập được:



- 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:

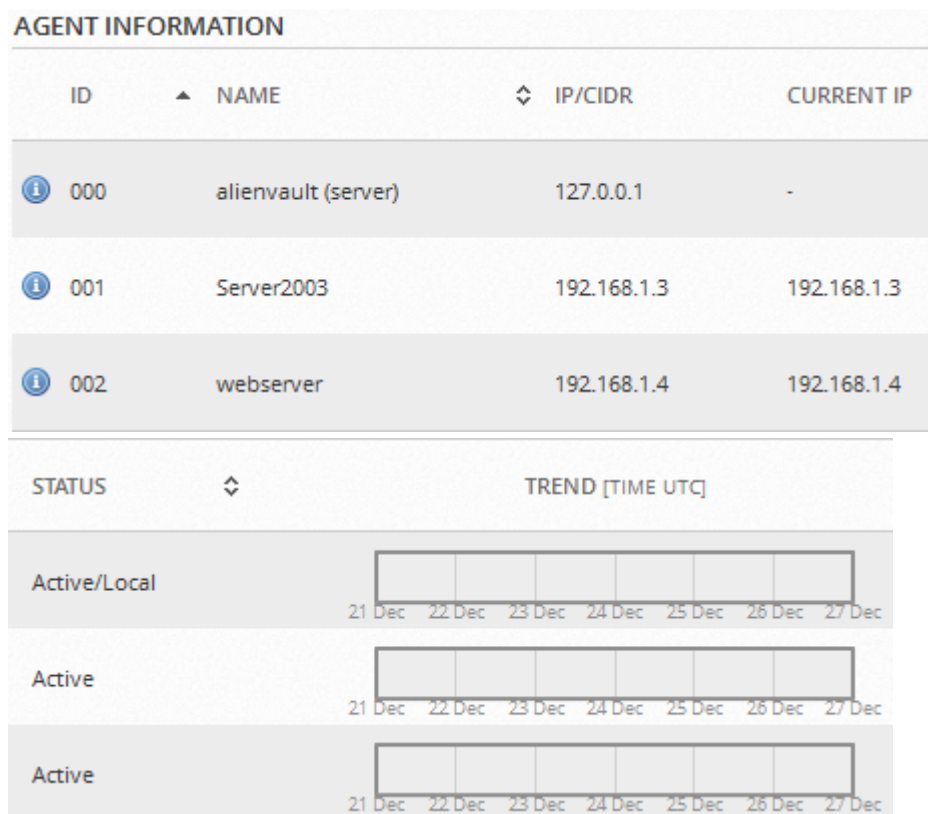
SECURITY EVENTS (SIEM)

SIEM	REAL-TIME
------	-----------

PAUSE Refreshing...

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2015-12-27 23:18:13	ossec: SSH insecure connection attempt (scan).	0	ossec-recon	alienvault	alienvault	alienvault
2015-12-27 23:18:12	SSHD: Server listening	0	ssh	alienvault	::	alienvault:22
2015-12-27 23:18:12	SSHD: Server listening	0	ssh	alienvault	0.0.0.0	alienvault:22

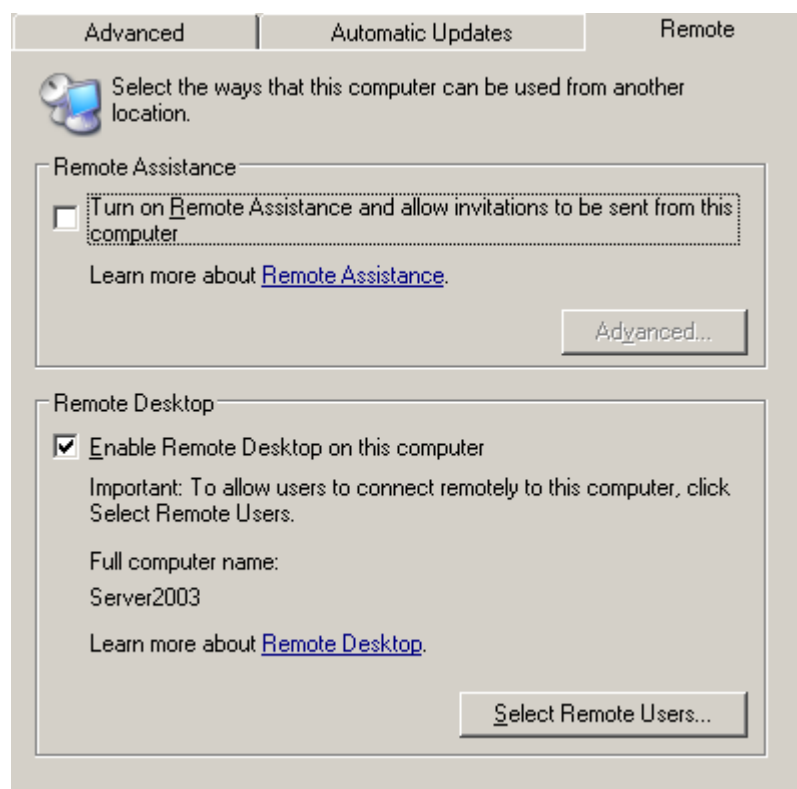
- Trong Tab Environment chọn Detection để xem các trạng thái hoạt động của các agent hiện tại:



1.8. Thực hiện tấn công vào mật khẩu trên máy Server 2003

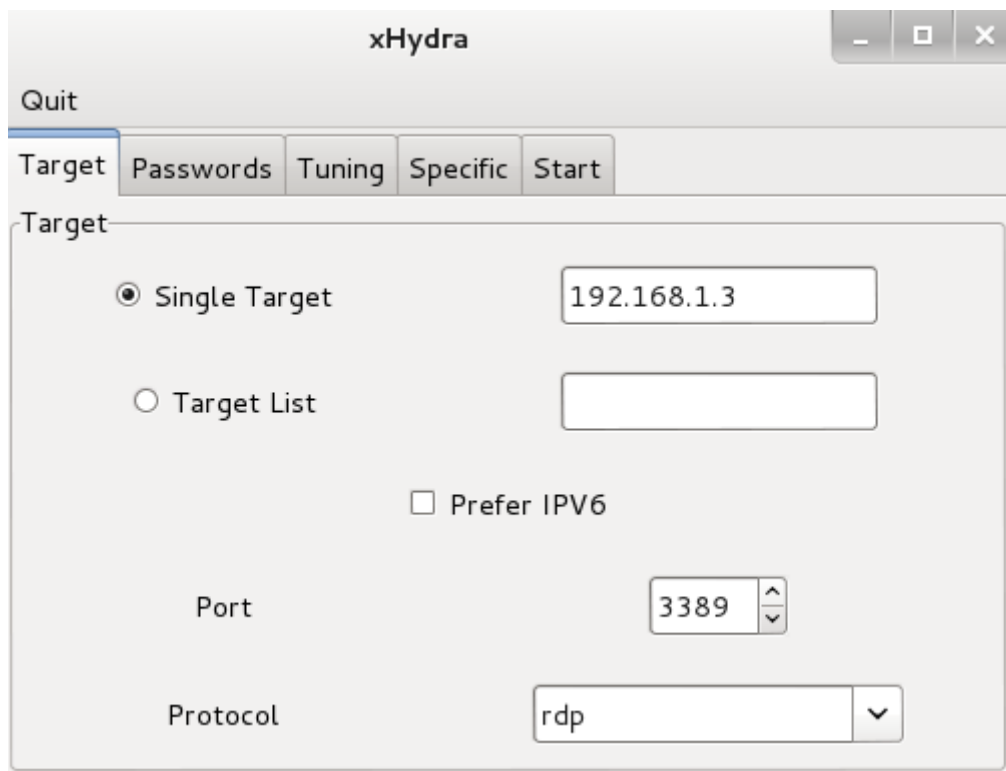
Sử dụng máy trạm Kali Linux để tấn công từ điển mật khẩu vào tài khoản Administrator trên Server 2003:

Trên máy Server 2003 bật dịch vụ truy cập từ xa Remote Desktop:



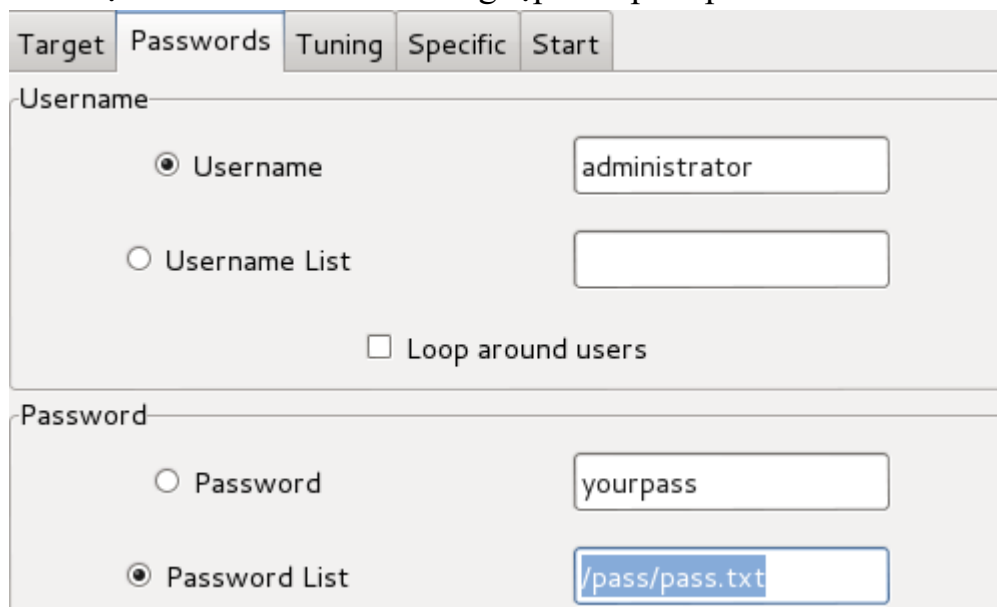
Trên máy Kali: Bật công cụ xhydra để tấn công mật khẩu bằng từ điển:

Trong Tab Target nhập địa chỉ IP của máy Server 2003, nhập cổng dịch vụ Remote Desktop là 3389, giao thức rdp:



The screenshot shows the xHydra application window with the 'Target' tab selected. The 'Single Target' radio button is chosen, and the IP address '192.168.1.3' is entered in the adjacent text field. The 'Target List' radio button is unselected. The 'Prefer IPV6' checkbox is unchecked. The 'Port' is set to '3389' in a spinner box, and the 'Protocol' is set to 'rdp' in a dropdown menu.

Trong Tab Passwords chọn tài khoản cần tấn công: Administrator
Với mật khẩu từ điển chứa trong tệp tin: /pass/pass.txt



The screenshot shows the xHydra application window with the 'Passwords' tab selected. Under the 'Username' section, the 'Username' radio button is chosen, and 'administrator' is entered in the text field. The 'Username List' radio button is unselected. The 'Loop around users' checkbox is unchecked. Under the 'Password' section, the 'Password List' radio button is chosen, and '/pass/pass.txt' is entered in the text field. The 'Password' radio button is unselected.

Chuyển sang Tab Start nhấn vào nút Start để bắt đầu tấn công:

Target	Passwords	Tuning	Specific	Start
Output				
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organ				
Hydra (http://www.thc.org/thc-hydra) starting at 2015-12-27 11:55:42				
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the numt				
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwritin				
[DATA] max 16 tasks per 1 server, overall 64 tasks, 37 login tries (l:1/p:37), ~0 tries per task				
[DATA] attacking service rdp on port 3389				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "123" - 1 of 37 [child 0]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "4235" - 2 of 37 [child 1]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "7456" - 3 of 37 [child 2]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "rgsdt3" - 4 of 37 [child 3]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "wr37h" - 5 of 37 [child 4]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "w56thgj" - 6 of 37 [child 5]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "54ysdfs" - 7 of 37 [child 6]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "vcbwery" - 8 of 37 [child 7]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "546wgsdf" - 9 of 37 [child 8]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "we5yefg" - 10 of 37 [child 9]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "vxb" - 11 of 37 [child 10]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "ywttyh" - 12 of 37 [child 11]				
[ATTEMPT] target 192.168.1.3 - login "administrator" - pass "werydhsdh" - 13 of 37 [child 12]				

Kết quả tấn công như sau:

[3389][rdp] host: 192.168.1.3 login: administrator password: 123
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
[STATUS] 165.00 tries/min, 165 tries in 00:01h, 18446744073709551488 todo in 5124095

Tấn công thành công vào tài khoản Administrator với mật khẩu 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:

2015-12-28 00:07:03	ossec: Multiple Windows Logon Failures.
2015-12-28 00:07:03	ossec: Logon Failure - Unknown user or bad password.
2015-12-28 00:07:03	ossec: Logon Failure - Unknown user or bad password.
2015-12-28 00:07:03	ossec: Logon Failure - Unknown user or bad password.

GENERATOR	SENSOR	SOURCE IP	DEST IP
-----------	--------	-----------	---------

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

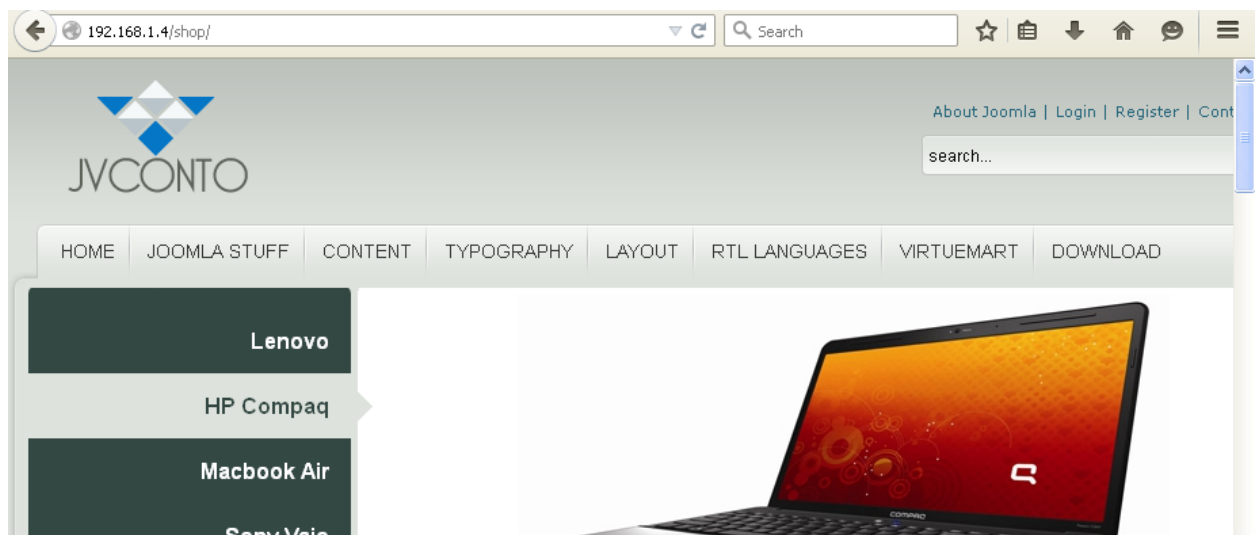
Từ sự kiện này biết được địa chỉ đích tấn công và nguồn bị tấn công.

Với dấu hiệu là rất nhiều sự kiện xác thực không thành công, vì vậy có thể kết luận máy Server 2003 đang bị tấn công vào mật khẩu.

1.9. Thực hiện tấn công quét lỗ hổng đối với mã nguồn website

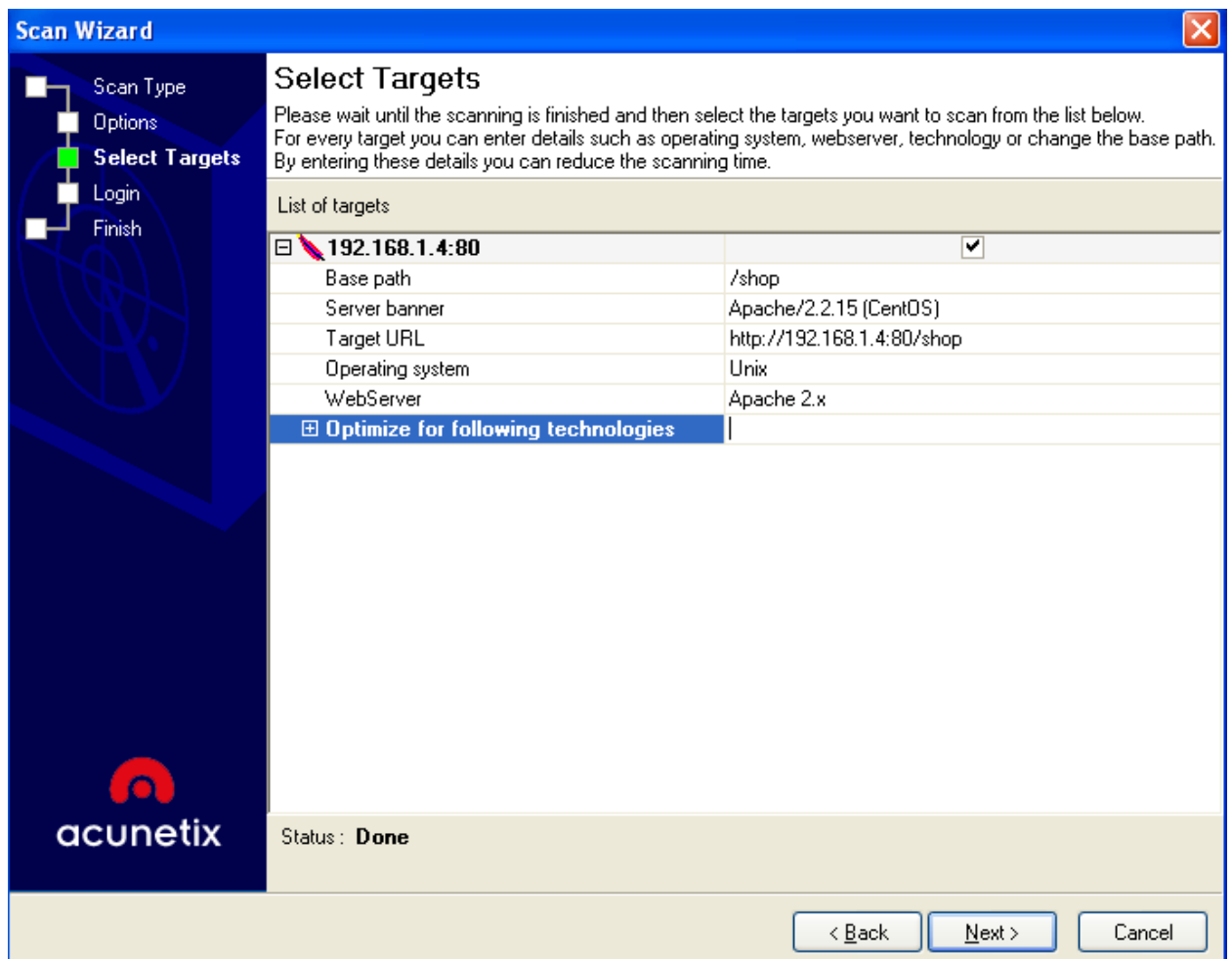
Lúc này sử dụng thêm máy ảo Windows XP để cài đặt công cụ Acunetix Web Vulnerability Scanner quét lỗ hổng website trên máy Linux CentOS.

Sử dụng trình duyệt web để truy cập thử vào trang web có trên máy chủ CentOS:



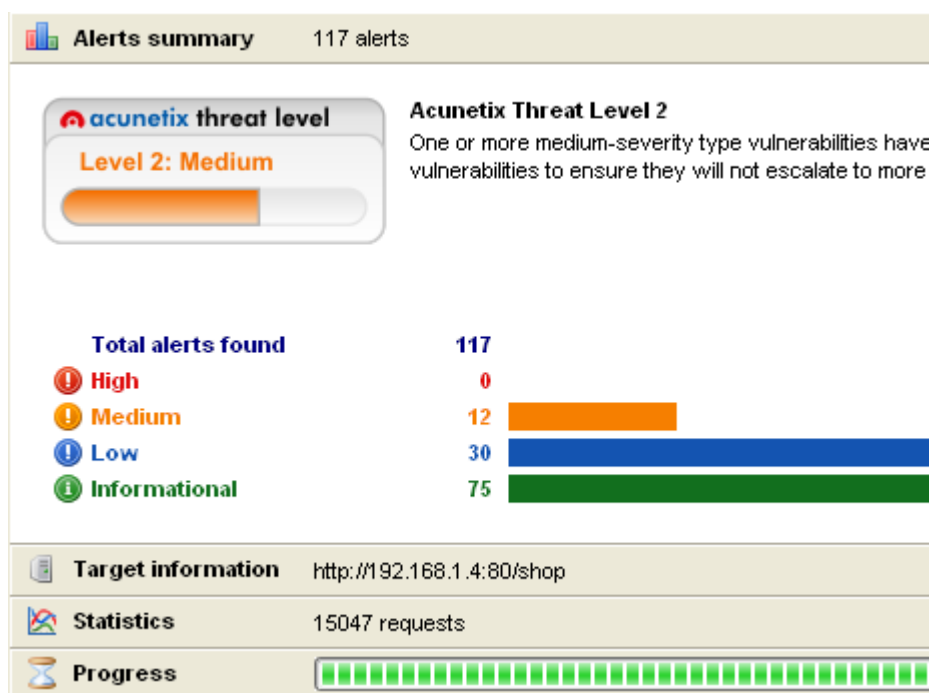
Truy cập thành công.

Cài đặt và sử dụng công cụ Acunetix Web Vulnerability Scanner để quét lỗ hổng:



Bắt đầu quá trình quét:

Scan Results	Status
Scan Thread 1 (http://192.168.1.4:80/shop)	Scanning
Web Alerts (117)	
Apache httpd Remote Denial of Serv...	
Directory Listing (11)	
Hidden form input named price was f...	
OPTIONS method is enabled (1)	
Possible sensitive directories (6)	
TRACE method is enabled (1)	
User credentials are sent in clear te...	
Broken links (1)	
Error page Web Server version discl...	
GHDB: Apache directory listing whic...	
GHDB: Possible PHP configuration fil...	
Password type input with autocompl...	
Possible internal IP address disclosur...	



Chuyển sang website quản trị của AlienVault trong trạng thái phân tích thời gian thực phát hiện các dấu hiệu:

Cùng một thời điểm và có rất nhiều request vào webserver và AlienVault hiểu các lỗi này là 400.

DATE	EVENT NAME
2015-12-28 00:23:56	ossec: Web server 400 error code.
2015-12-28 00:23:56	ossec: Web server 400 error code.
2015-12-28 00:23:56	ossec: Web server 400 error code.
2015-12-28 00:23:56	ossec: Multiple web server 400 error codes from same source ip.
2015-12-28 00:23:56	ossec: Web server 400 error code.
2015-12-28 00:23:56	ossec: Web server 400 error code.

Thông tin được lấy từ tệp tin accesslog của Apache.

Thấy được địa chỉ IP của máy tấn công và IP của máy bị tấn công.

GENERATOR	SENSOR	SOURCE IP	DEST IP
ossec-accesslog	alienvault	192.168.1.200	192.168.1.4
ossec-accesslog	alienvault	192.168.1.200	192.168.1.4
ossec-accesslog	alienvault	192.168.1.200	192.168.1.4
ossec-recon	alienvault	192.168.1.200	192.168.1.4
ossec-accesslog	alienvault	192.168.1.200	192.168.1.4
ossec-accesslog	alienvault	192.168.1.200	192.168.1.4
ossec-accesslog	alienvault	192.168.1.200	192.168.1.4

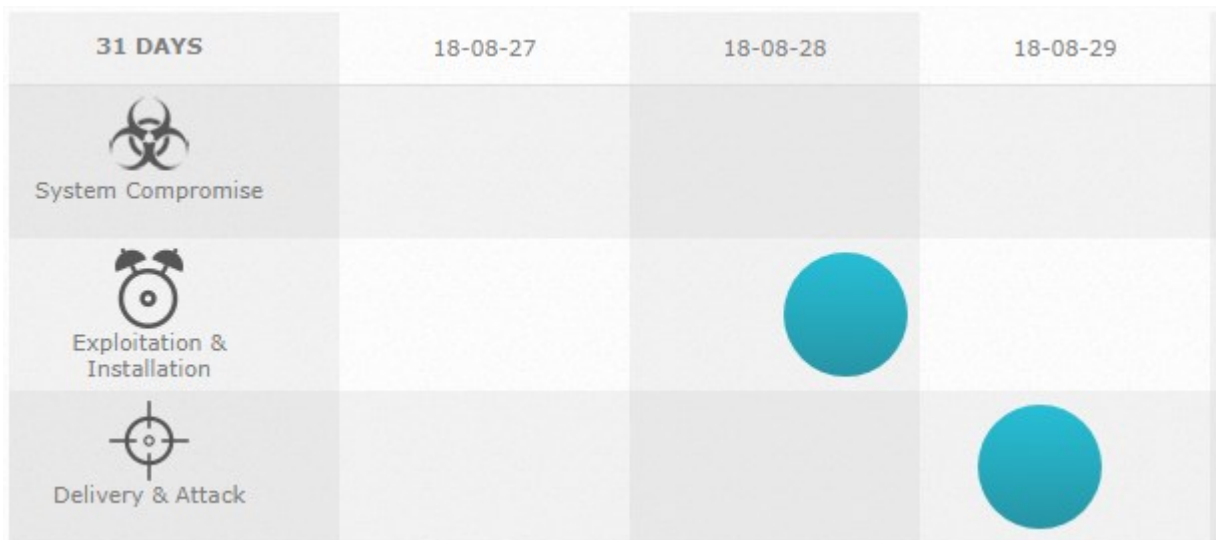
Đây là dấu hiệu của hành vi sử dụng công cụ để quét lỗ hổng website từ xa.

Tham khảo:

Phát hiện tấn công vào máy chủ web có IP 10.20.0.131

Sử dụng trình duyệt web truy cập vào website quản lý của hệ thống giám sát OSSIM.

Truy cập tới mục Analysis → Alarms



Hệ thống đã xuất hiện các cảnh báo về tấn công.

DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	ATTACK PATTERN	SOURCE	DESTINATION
2018-08-29	open	WebServer Attack - SQL Injection	Attack Pattern Detection	1		Host-10-20-0-129	Host-10-20-0-131
2018-08-28	open	WebServer Attack	XSS	1		Host-10-20-0-129	Host-10-20-0-131

Để xem chi tiết hơn về từng loại tấn công, kích chọn tấn công đó. Kết quả như hình dưới đây:

EVENTS
GROUPED
TIMELINE

SHOW TREND GRAPH
Off

DISPLAYING EVENTS 1-1 OF ABOUT 1 MATCHING YOUR SELECTION.

SIGNATURE	DATE GMT-4:00	SENSOR	SOURCE	DESTINATION
ossec: SQL injection attempt.	2018-08-29 11:22:45	alienvault	Host-10-20-0-129	Host-10-20-0-131

Hệ thống giám sát khi nhận được các sự kiện từ máy chủ web gửi về, trong các truy vấn đó có tiềm ẩn lệnh truy vấn cơ sở dữ liệu.

Truy cập chi tiết vào một sự kiện với giao diện như sau:

DATA SOURCE NAME		PRODUCT TYPE
ossec-sql_injection		Intrusion Detection

SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS
Host-10-20-0-129	0	Host-10-20-0-131

Thông tin thu được cho thấy địa chỉ IP tấn công và địa chỉ IP bị tấn công.
Định danh tấn công:

USERDATA1	USERDATA2
SQL injection attempt.	10.20.0.129 - - [29/Aug/2018:11:22:31 +0700] "GET /dvwa/vulnerabilities/sqli/?id=%25%27+and+1%3D0+union+select+null%2C+table_name+from+inf HTTP/1.1" 302 - "-" Mozilla/5.0 (Windows NT 6.1; WOW64; rv:61.0) Gecko/20100101 Firefox/61.0"

Trong đường dẫn truy cập website thấy có câu lệnh của cơ sở dữ liệu truy vấn như: Union, select, database. Kẻ tấn công đã sử dụng trình duyệt web Firefox v61.0 để truy cập.

Kết thúc bài thực hành.

Kết luận:

Như vậy sử dụng bộ công cụ giám sát an ninh mạng AlienVault giám sát được các hành vi thời gian thực tác động vào các máy chủ, máy trạm đã cài phần mềm giám sát.