

第五次实验报告

一、课程名称

网络安全实验

二、实验名称

入侵检测实验

三、实验目的

1. 掌握在不同的操作系统环境下安装和配置 OSSEC 代理。
2. 了解工具 PuTTY 的基本功能，掌握使用该工具远程连接机器的方法。
3. 通过安装 OSSEC 代理，掌握 PuTTY 工具的实验，掌握配置 OSSEC 代理的方法，了解 OSSEC 入侵检测系统的架构、功能以及实现方式，具备构建入侵检测环境的能力。
4. 掌握 OSSIM 系统的入侵检测规则设置方法，并能够根据报警信息做入侵行为分析，具备信息系统入侵检测和防范、维护系统安全的职业能力。

四、目录

| | |
|---|----|
| 第五次实验报告 | 1 |
| 一、课程名称 | 1 |
| 二、实验名称 | 1 |
| 三、实验目的 | 1 |
| 四、目录 | 1 |
| 五、实验步骤 | 2 |
| 任务一：在不同的操作系统环境下安装和配置 OSSEC 代理，构建入侵检测环境 .. | 2 |
| 任务二：监视 OSSIM 服务器本地 root 用户的登录情况 | 12 |

| | |
|--------------------------------|----|
| 任务三：基于 SSH 的远程非法入侵检测 | 18 |
| 任务四：监视 CentOS7 root 用户情况 | 21 |
| 任务五：监控 Web 服务器的访问日志 | 24 |

五、实验步骤

任务一：在不同的操作系统环境下安装和配置 OSSEC 代理，构建入侵检测环境

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容

- 在 Windows 平台下安装和配置 OSSEC 代理
- 在 Linux 平台下安装和配置 OSSEC 代理

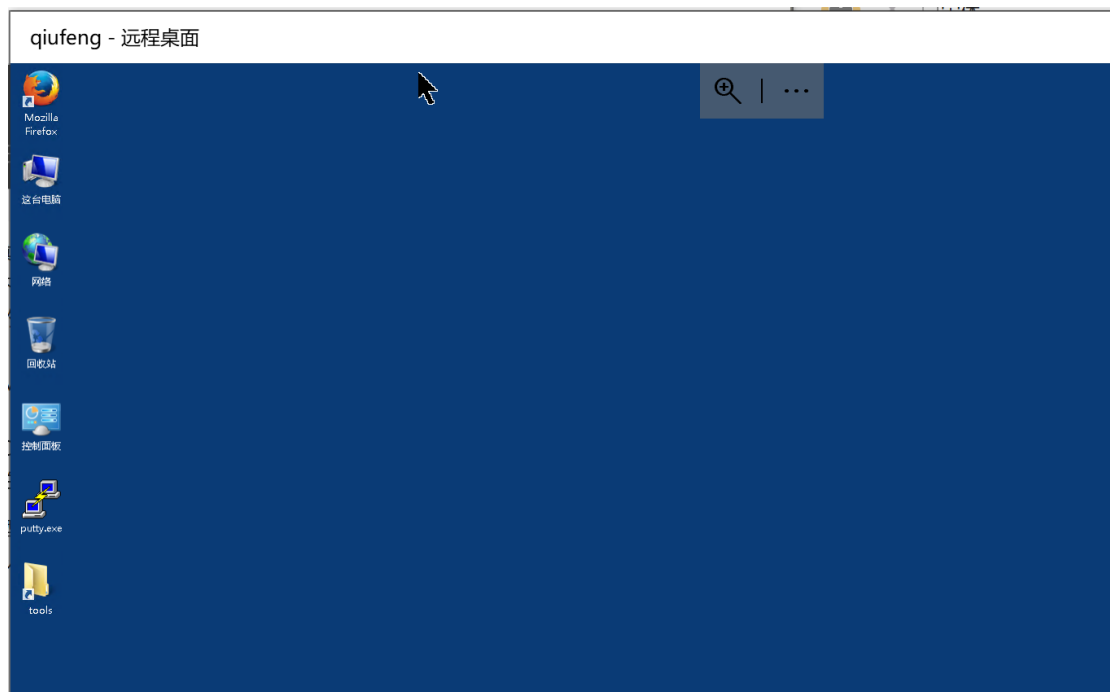
本身实验的实验目标如下

- 理解 OSSIM 开源安全信息管理的概念、功能，以及与 OSSEC 的关系及原理
- 理解 OSSEC 入侵检测系统的基本功能、C/S 模式工作原理
- 掌握在不同的操作系统平台安装并配置 OSSEC 代理的方法
- 通过安装和配置 OSSEC 代理，了解 OSSEC 入侵检测系统的架构、功能以及实现方式，具备构建入侵检测环境的能力

1.1 安装 OSSEC HIDS Windows Agent 工具软件

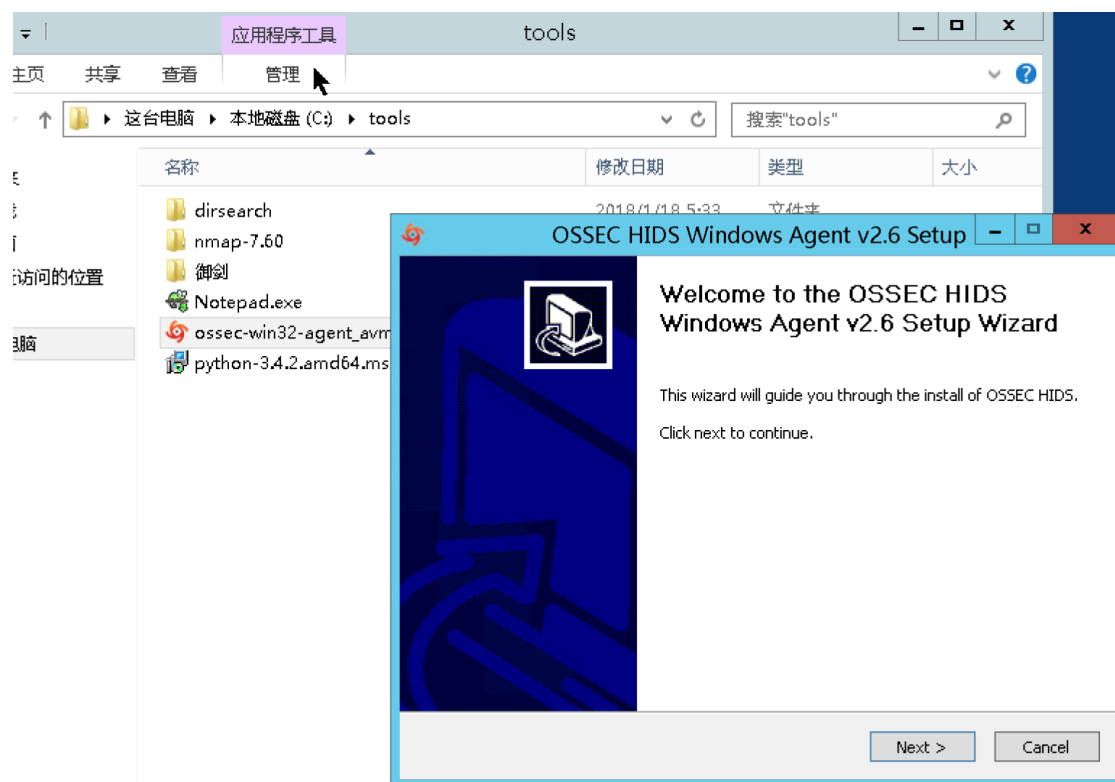
在 windows 上安装 OSSEC 代理软件

首先使用 **microsoft** 远程桌面连接 windows 2012 实验平台



远程桌面连接

在 tools 文件夹中点击安装程序进行安装



安装 OSSEC

打开 OSSEC 并进行配置 OSSEC Server IP 为 **192.168.1.200**

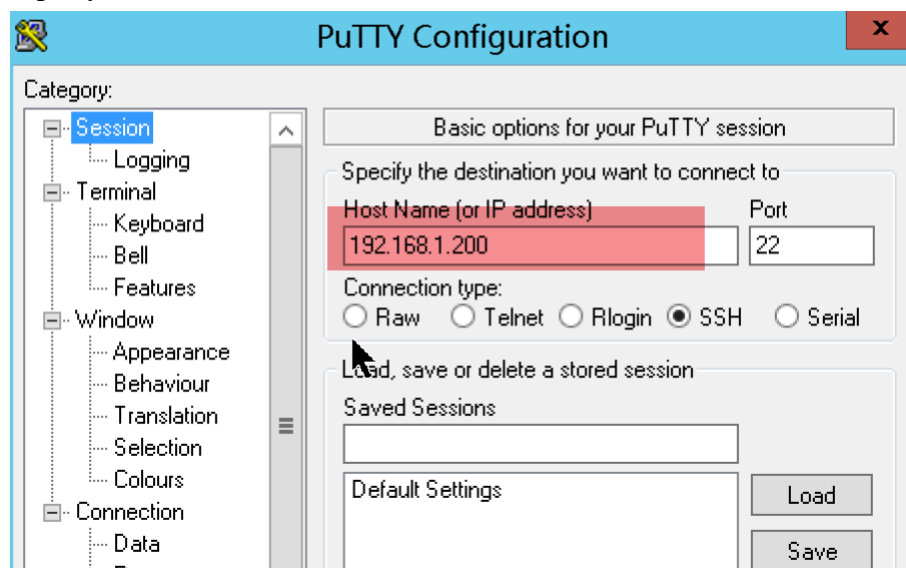


配置 OSSEC

1.2 在 Windows 平台下安装和配置 OSSEC 代理

使用 putty 远程登录 OSSIM 服务器

使用 putty 远程登录 OSSIM 服务器，注意 IP 地址为 **192.168.1.200**



配置 IP

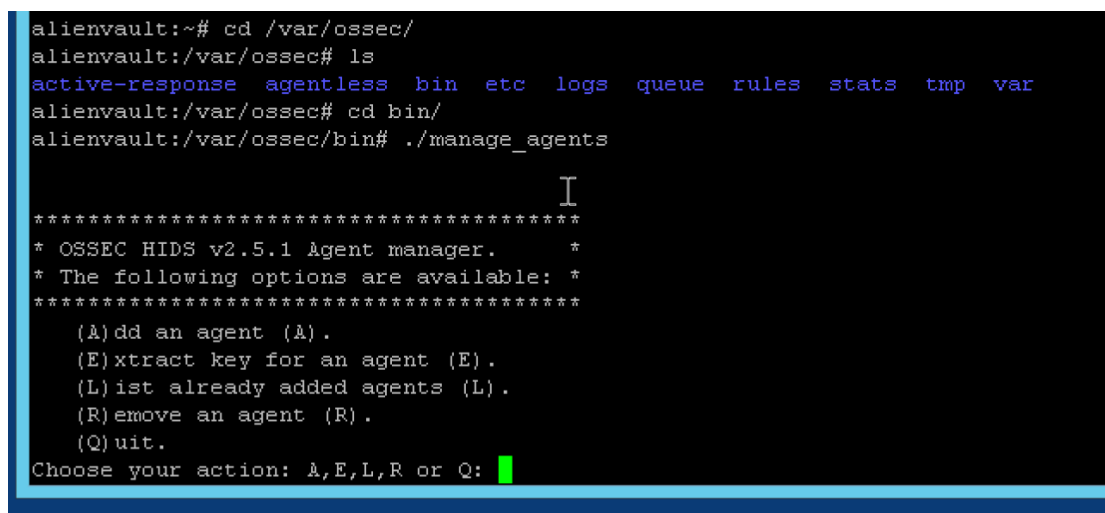
成功登录服务器



putty 登录服务器

启动 OSSEC 代理管理程序，创建新的代理

运行 OSSEC 代理管理程序



运行 OSSEC 代理管理程序

创建新的代理，并配置相关的信息

```
(Q)uit.  
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: windows2012  
  * The IP Address of the new agent: 192.168.1.5  
  * An ID for the new agent[005]:  
Agent information:  
  ID:005  
  Name:windows2012  
  IP Address:192.168.1.5  
Confirm adding it?(y/n): y  
Agent added.
```

创建代理并配置信息

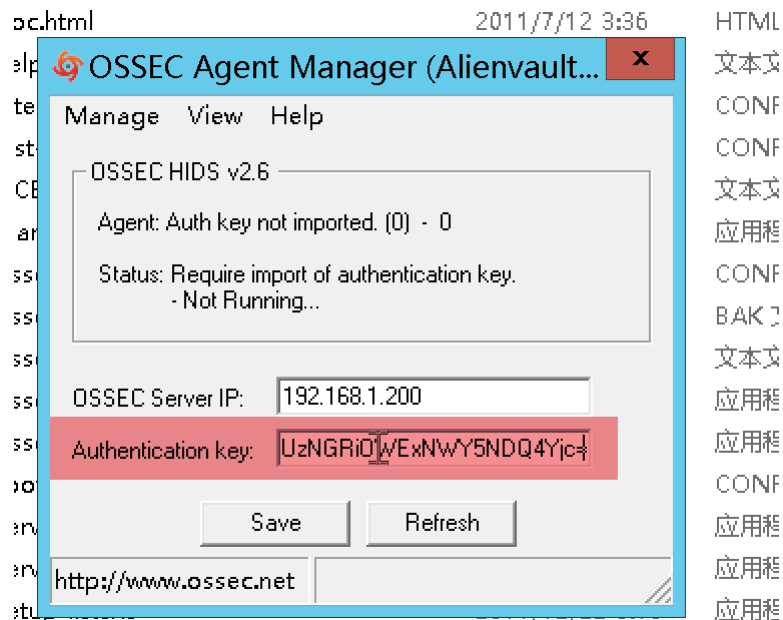
新建密钥并保存

重复运行 OSSEC 代理管理程序并为新添加的代理生成密钥

```
(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: alienvault, IP: 192.168.1.200  
  ID: 002, Name: windows7, IP: 192.168.1.2  
  ID: 003, Name: CentOS6.5, IP: 192.168.1.4  
  ID: 004, Name: windows2003, IP: 192.168.1.3  
  ID: 005, Name: windows2012, IP: 192.168.1.5  
Provide the ID of the agent to extract the key (or '\q' to quit): 005  
Agent key information for '005' is:  
MDA1IHdpbmRvd3MyMDEyIDE5Mi4xNjguMS41IDRkYjAzYjlkYTEwOWVmNTg1NGM3ODBhYWRjODBhNGVj  
NmI2ODc2NmZmMWNjZGYxZGUzNGRiOWExNWY5NDQ4Yjc=
```

生成密钥

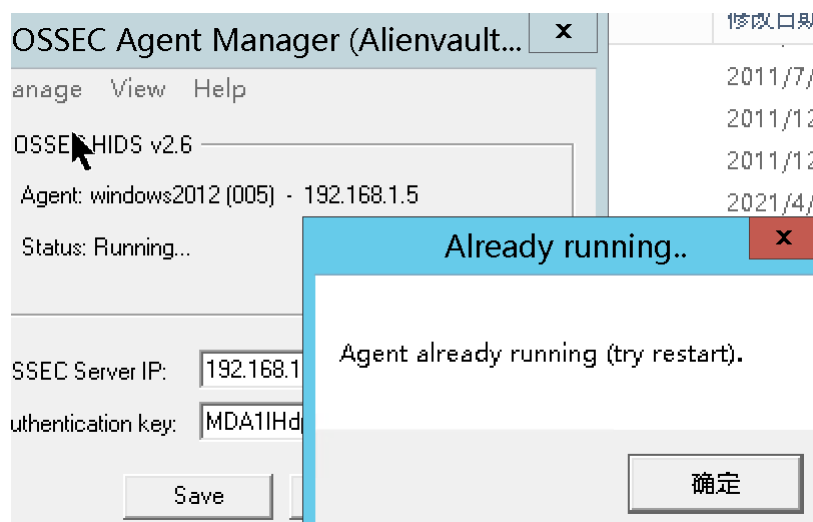
复制密钥，并将其保存在 windows 2012 上的 OSSEC 客户端程序中



保存密钥

启动 OSSEC，查看运行状态

启动 windows 中的 OSSEC 代理



启动 OSSEC

查看 agent_control 程序的帮助信息

```

alienvault:/var/ossec/bin# ./agent_control --help
./agent_control: invalid option -- '-'

OSSEC HIDS agent_control: Control remote agents.
Available options:
  -h          This help message.
  -l          List available (active or not) agents.
  -lc         List active agents.
  -i <id>     Extracts information from an agent.
  -R <id>     Restarts agent.
  -r -a       Runs the integrity/rootkit checking on all agents now.
  -r -u <id>  Runs the integrity/rootkit checking on one agent now.

  -b <ip>     Blocks the specified ip address.
  -f <ar>     Used with -b, specifies which response to run.
  -L          List available active responses.
  -s          Changes the output to CSV (comma delimited).

```

查看代理列表

agent_control 帮助信息

使用命令 `./agent_control -lc` 查看代理状态，可以发现已经被激活

```

alienvault:/var/ossec/bin# ./agent_control -lc

OSSEC HIDS agent_control. List of available agents:
  ID: 000, Name: alienvault (server), IP: 127.0.0.1, Active/Local
  ID: 005, Name: windows2012, IP: 192.168.1.5, Active

```

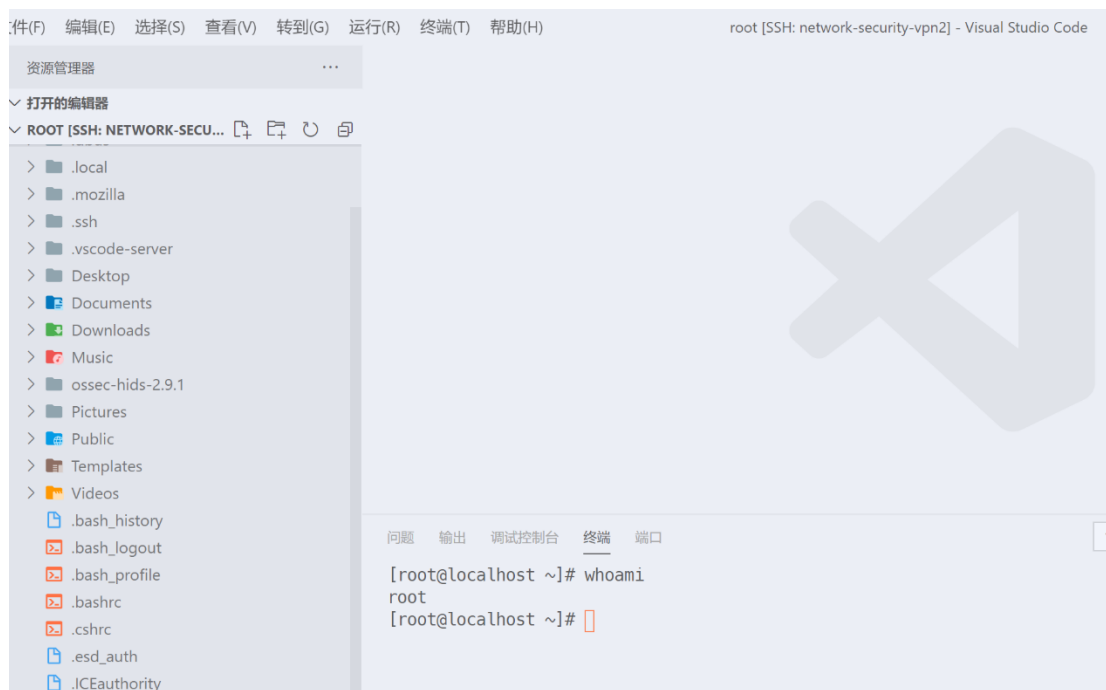
已经激活

查看代理状态

1.3 在 Linux 平台下安装和配置 OSSEC 代理

切换到 CentOS7 虚拟机并打开终端

由于可以直接通过校园网 ssh 连接 CentOS7 虚拟机，因此我们使用 `vscode remote+vcxsrv` 进行连接



连接 CentOS7

通过 CentOS7 终端 SSH 远程登录 OSSIM 服务器

使用 ssh 远程登录 OSSIM 服务器



远程登陆 OSSIM 服务器

新建代理并添加密钥

类似于上述为 **windows 2012** 新建代理的操作，我们首先生成一个代理

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

*****
* OSSEC HIDS v2.5.1 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: A

- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: CentOS7
* The IP Address of the new agent: 192.168.1.6
* An ID for the new agent[006]:
Agent information:
ID:006
Name:CentOS7
IP Address:192.168.1.6
Confirm adding it?(y/n): y
Agent added.
```

新建代理

名称

ip地址

确认添加

新建代理

并为该代理生成密钥

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

Available agents:
ID: 001, Name: alienvault, IP: 192.168.1.200
ID: 002, Name: windows7, IP: 192.168.1.2
ID: 003, Name: CentOS6.5, IP: 192.168.1.4
ID: 004, Name: windows2003, IP: 192.168.1.3
ID: 005, Name: windows2012, IP: 192.168.1.5
ID: 006, Name: CentOS7, IP: 192.168.1.6
Provide the ID of the agent to extract the key (or '\q' to quit): 006

Agent key information for '006' is:
MDA2IEN\bnRPUzcgMTkyLjE2OC4xLjYgMzJjMjUzNjNhNjJkZjdiYzc5MDU5YzAzYzE5MzJlZDRkZGQ2ZmViMjIxYmQxNGNjMmI4Y2QyZTE1OWVm
ZjFhZg==

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

为006生成密钥

生成密钥

在 **CentOS7** 上运行程序 `manage_agents` 并添加密钥

```
[root@localhost bin]# ./manage_agents

*****
* OSSEC HIDS v2.9.1 Agent manager.      *
* The following options are available: *
*****
  (I)mport key from the server (I).
  (Q)uit.
Choose your action: I or Q: I  添加密钥

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

Paste it here (or '\q' to quit): MDA2IENlbnRPUzcgMTkyLjE2OC4xLjYgMzJjMjUzNjNhNjJkZjdiYzc5MDU5YzAzYzZmViMjIxYmQxNGNjMmI4Y2QyZTE1OWVmZjFhZg==

Agent information:
  ID:006
  Name:CentOS7
  IP Address:192.168.1.6
```

添加密钥

查看 ossec.conf 配置文件

输入如下命令查看配置文件，可以发现包含服务器 IP 地址
cat /var/ossec/etc/ossec.conf

```
[root@localhost ~]# cat /var/ossec/etc/ossec.conf
<ossec_config>
  <client>                                服务器IP地址
    <server-ip>192.168.1.200</server-ip>
  </client>

  <syscheck>
    <!-- Frequency that syscheck is executed - default to every 22 hours -->
    <frequency>79200</frequency>
```

配置文件

重启 OSSEC 服务，查看运行状态

使用如下命令重启 CentOS7 的 OSSEC 服务
/var/ossec/bin/ossec-control restart

```
[root@localhost ~]# /var/ossec/bin/ossec-control restart
Killing ossec-logcollector ..
Killing ossec-syscheckd ..
Killing ossec-agentd ..
Killing ossec-execd ..
OSSEC HIDS v2.9.1 Stopped
Starting OSSEC HIDS v2.9.1 (by Trend Micro Inc.)...
Started ossec-execd...
2021/04/20 18:00:38 ossec-agentd: INFO: Using notify time: 600 and max time to reconn
Started ossec-agentd...
2021/04/20 18:00:38 ossec-logcollector(1226): ERROR: Error reading XML file '/var/oss
XMLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 84).
Started ossec-logcollector...
```

重启服务

使用如下命令查看 OSSEC 运行状态

`/var/ossec/bin/ossec-control status`

```
[root@localhost ~]# /var/ossec/bin/ossec-control status
ossec-logcollector is running...
ossec-syscheckd is running...
ossec-agentd is running...
ossec-execd is running...
```

查看运行状态

使用如下命令在服务器端查看代理的状态,可以发现 006 号代理已经被激活,状态为 **Active**

`/var/ossec/bin/agent_control -lc`

```
alienvault:/var/ossec/bin# ./agent_control -lc

OSSEC HIDS agent_control. List of available agents:
  ID: 000, Name: alienvault (server), IP: 127.0.0.1, Active/Local
  ID: 005, Name: windows2012, IP: 192.168.1.5, Active
  ID: 006, Name: CentOS7, IP: 192.168.1.6, Active
```

查看代理状态

任务二：监视 OSSIM 服务器本地 root 用户的登录情况

本实验任务在任务一完成的基础上,主要完成以下内容

- 在 OSSIM 集成检测平台上设置规则
- 使用 PuTTY 远程连接 OSSIM 服务器,模拟攻击者破解服务器的用户名和密码后登陆服务器
- 查看入侵检测系统检测到的报警信息,理解入侵检测系统对于监视用户登录情况的重要性

本实验的目标为

- 理解入侵检测的概念、原理,掌握入侵检测规则的设置方法
- 了解 PuTTY 工具的基本功能,掌握使用 PuTTY 远程登录服务器的方法
- 了解 OSSIM 集成检测平台的功能,掌握该平台报警信息的筛选与查看方法

- 熟悉 OSSEC 入侵检测系统的工作原理和常用功能，掌握 OSSEC 入侵检测系统报警信息的查看方法

2.1 在 windows2012 上使用火狐浏览器访问 OSSIM 集成监测平台 Web GUI 界面，输入用户名 admin 和密码 Simplexue123 进行登录

访问如下网址，并通过用户名 **admin** 和密码 **Simplexue123** 进行登录

<https://192.168.1.200/ossim/session/login.php>

由于 firefox 不信任其证书，因此我们需要手动添加例外



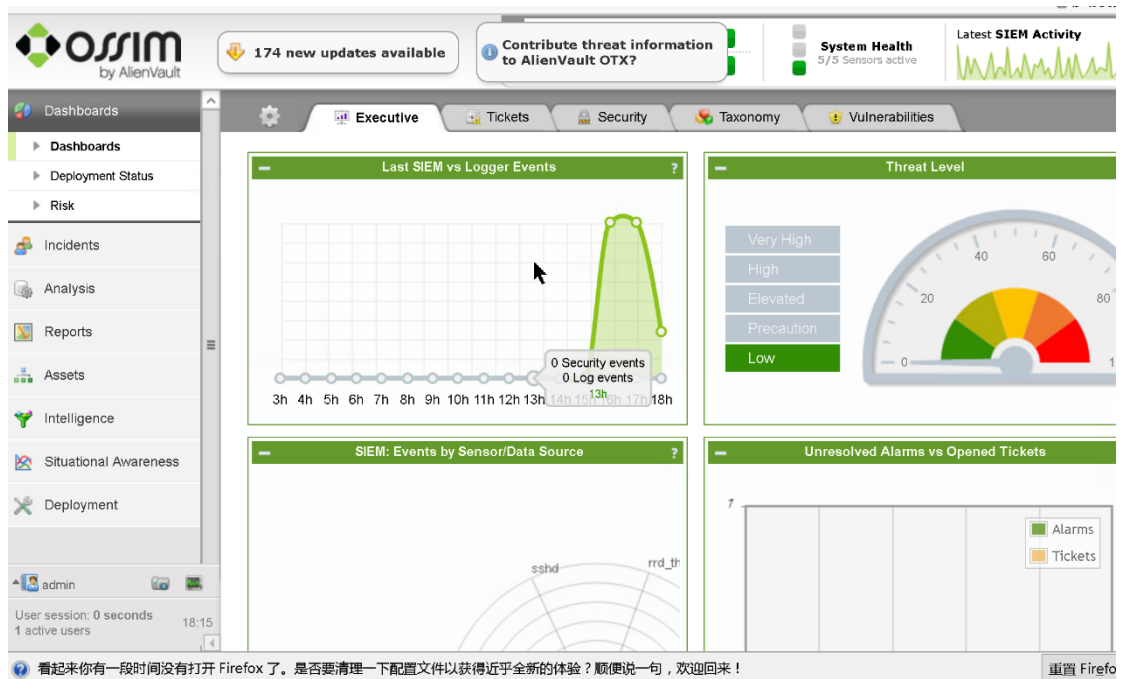
手动添加例外

使用用户名和密码登录后台管理页面



登陆后台管理页面

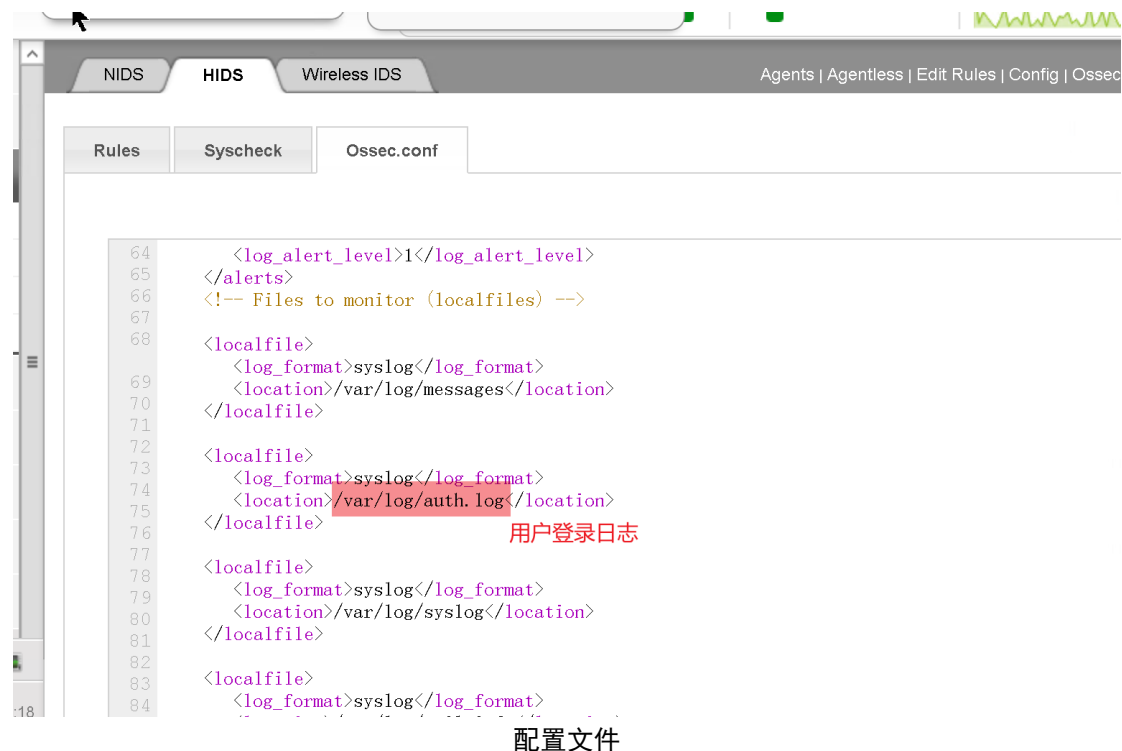
后台管理页面如下图所示



后台管理页面

2.2 查看 ossec.conf 规则配置文件

查看配置文件，可以发现 `/var/log/auth.log` 默认被监控，该日志主要用来记录用户登录的信息



这里使用的日志格式为 **syslog**，syslog 机制负责记录内核和应用程序产生的日志信息，管理员可以通过查看日志记录，来掌握系统状况。syslog 也是一种协议，广泛用于系统日志，syslog 系统日志消息可以记录在本地，也可以发送到接受 syslog 日志的服务器统一进行存储和处理，也可以解析其中的内容做相应的处理。ossec 本身对所收集日志的传输（传输给 OSSIM 服务器）也是通过 syslog 来完成。ossec 代理收集日志并传输给 OSSIM 服务器，最重要的意义是系统管理者可以根据日志进行入侵行为分析。

收集日志的作用主要包括以下几点

- 从安全方面来考虑主要是为了能够在出现问题时或出现安全问题后可以查询到日志，来追溯攻击者
- 从运维层面来说，收集系统日志对于系统管理员处理各种故障来说，可以提供很大便利性，另外可以方便运维排除故障及解决问题
- 起到备份作用，需要对日志进行安全保存，避免因为黑客入侵导致的日志丢失

2.3 重启 OSSIM 服务器并重新登录

使用如下命令重启 OSSIM 服务器

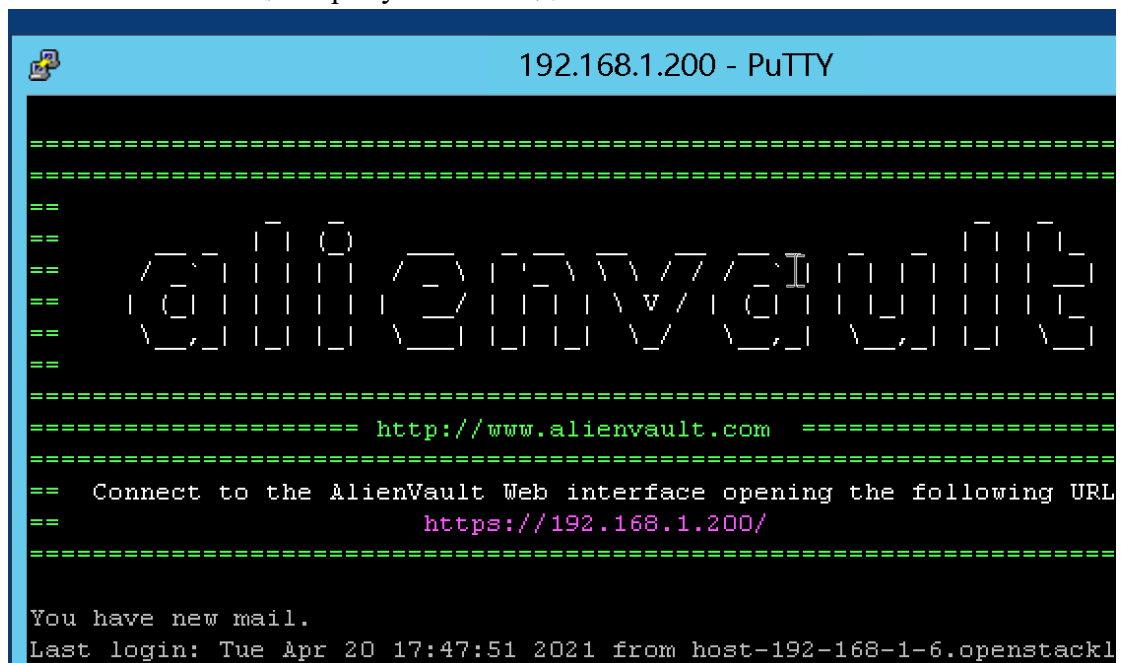
/var/ossec/bin/ossec-control restart

```
alienvault:/var/ossec/bin# /var/ossec/bin/ossec-control restart
Killing ossec-monitord ..
Killing ossec-logcollector ..
Killing ossec-remoted ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
ossec-maild not running ..
ossec-execd not running ..
OSSEC HIDS v2.5.1 Stopped
Starting OSSEC HIDS v2.5.1 (by Trend Micro Inc.)...
2021/04/20 18:26:13 ossec-testrule: INFO: Reading local decoder file.
2021/04/20 18:26:13 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
```

重启 OSSIM 服务器

2.4 在 windows 上登录服务器 192.168.1.200

在 windows 上使用 putty 登录到服务器



登录到服务器

2.5 查看安全事件

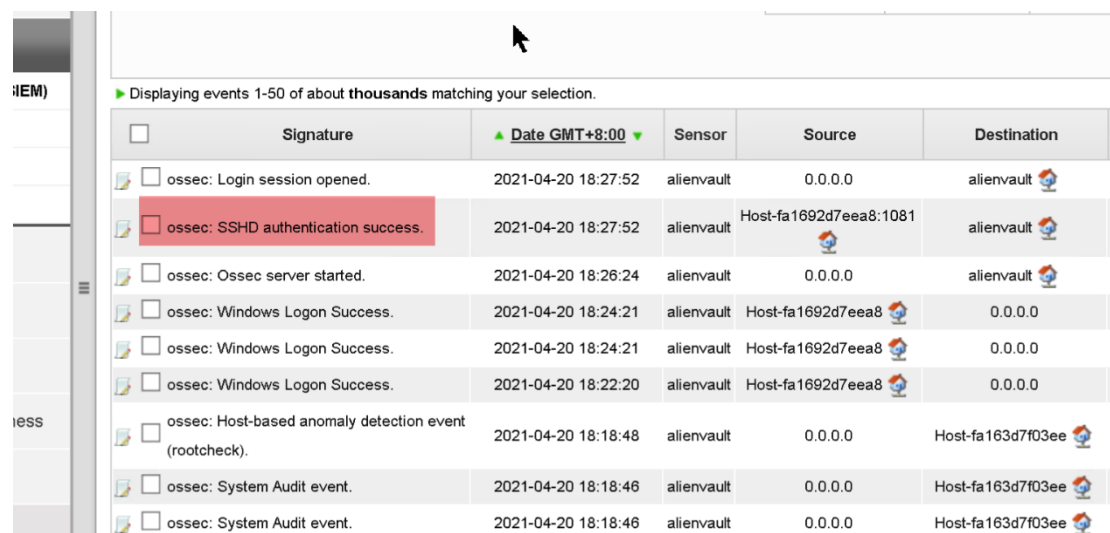
在 **Security Events** 中可以看到 OSSIM 系统预设检测规则适用范围内的所有安全事件日志信息，其中 putty 的登录信息如下

2.8 日志信息

此外还可以看到本地 root 用户成功登录 OSSIM 服务器系统的日志信息。如果 root 用户的合法管理员没有在这个时间本地登录 OSSIM 服务器，那么可以断定，本次 root 用户登录操作为入侵行为

可以看到身份验证成功信息如下图所示，其签名为(注意提交答案的时候不能有末尾的句点，并且冒号后面没有空格)

ossec:SSHD authentication success



| <input type="checkbox"/> | Signature | ▲ Date GMT+8:00 ▼ | Sensor | Source | Destination |
|-------------------------------------|--|---------------------|------------|------------------------|-------------------|
| <input type="checkbox"/> | ossec: Login session opened. | 2021-04-20 18:27:52 | alienvault | 0.0.0.0 | alienvault |
| <input checked="" type="checkbox"/> | ossec: SSHD authentication success. | 2021-04-20 18:27:52 | alienvault | Host-fa1692d7eea8:1081 | alienvault |
| <input type="checkbox"/> | ossec: Ossec server started. | 2021-04-20 18:26:24 | alienvault | 0.0.0.0 | alienvault |
| <input type="checkbox"/> | ossec: Windows Logon Success. | 2021-04-20 18:24:21 | alienvault | Host-fa1692d7eea8 | 0.0.0.0 |
| <input type="checkbox"/> | ossec: Windows Logon Success. | 2021-04-20 18:24:21 | alienvault | Host-fa1692d7eea8 | 0.0.0.0 |
| <input type="checkbox"/> | ossec: Windows Logon Success. | 2021-04-20 18:22:20 | alienvault | Host-fa1692d7eea8 | 0.0.0.0 |
| <input type="checkbox"/> | ossec: Host-based anomaly detection event (rootcheck). | 2021-04-20 18:18:48 | alienvault | 0.0.0.0 | Host-fa163d7f03ee |
| <input type="checkbox"/> | ossec: System Audit event. | 2021-04-20 18:18:46 | alienvault | 0.0.0.0 | Host-fa163d7f03ee |
| <input type="checkbox"/> | ossec: System Audit event. | 2021-04-20 18:18:46 | alienvault | 0.0.0.0 | Host-fa163d7f03ee |

身份验证成功

任务三：基于 SSH 的远程非法入侵检测

本实验在实验一的基础上完成如下内容

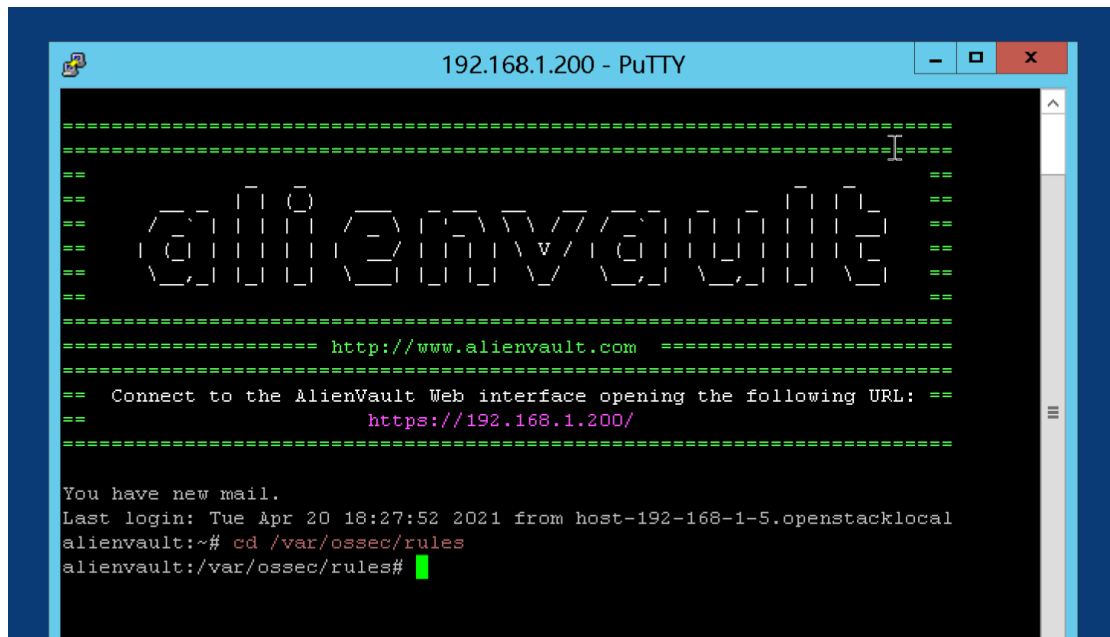
- 在 OSSIM 集成检测平台上设置 ossec 入侵检测规则
- 使用 PuTTY 远程连接 OSSIM 服务器，使用 root 用户名,多次尝试错误密码登录服务器
- 查看入侵检测系统检测到的 ossec 报警信息，理解 ossec 报警信息对于黑客入侵行为分析和防范的重要价值

本实验的实验目标如下

- 理解入侵检测的概念、原理，掌握入侵检测规则的设置方法
- 了解 PuTTY 工具的基本功能，掌握使用 PuTTY 远程登录服务器的方法
- 了解 OSSIM 集成检测平台的功能，掌握该平台报警信息的筛选与查看方法
- 熟悉 OSSEC 入侵检测系统的工作原理和常用功能，掌握 OSSEC 入侵检测系统报警信息的查看方法
- 能够根据 OSSIM 平台收集的 OSSEC 报警信息分析黑客的入侵行为，进而采取适当的入侵防范方法，维护信息系统安全
- 掌握入侵检测和防范技术，具备信息系统安全管理和入侵防范能力

3.1 使用 putty 工具远程登陆 SSIM 服务器

使用 putty 远程登录 SSIM 服务器并使用如下命令进入/var/ossec/rules 目录
`cd /var/ossec/rules`



远程登陆

使用 `ls` 命令查看配置文件



配置文件

可以修改这些文件的预设规则配置，来实现用户需要的自定义系统安全检测规则。其中，sshd_rules.xml 为我们本实验任务需要自定义检测规则的文件，通过自定义规则，以实现收集 root 用户远程非法登录 OSSIM 服务器的报警信息的目的，为判定、分析入侵行为和动机提供重要依据

3.2 修改 sshd_rules.xml 规则文件

尝试直接修改 **sshd_rules.xml** 文件，发现其不具有写权限

```
alienvault:/var/ossec/rules# ll sshd_rules.xml
-r-xr-xr-- 1 root ossec 5394 Oct 10 2012 sshd_rules.xml
alienvault:/var/ossec/rules#
```

sshd_rules.xml 权限

使用命令 **chmod 754 sshd_rules.xml** 授予其写权限

修改 **rule id** 号为 **5719** 的规则如下

```
</rule>

<rule id="5719" level="2" frequency="6" timeframe="120" ignore="60">
  <if_matched_sid>5718</if_matched_sid>
  <description>Multiple access attempts using a denied user.</description>
</rule>
```

修改规则

该规则表示：当非法用户存在 2 次以上远程登录尝试操作，且操作时间超过 30 秒，那么将触发非法远程登录尝试报警

3.3 重启 OSSEC 服务器，使配置文件生效

使用如下命令重启 OSSEC 服务器，使配置文件生效

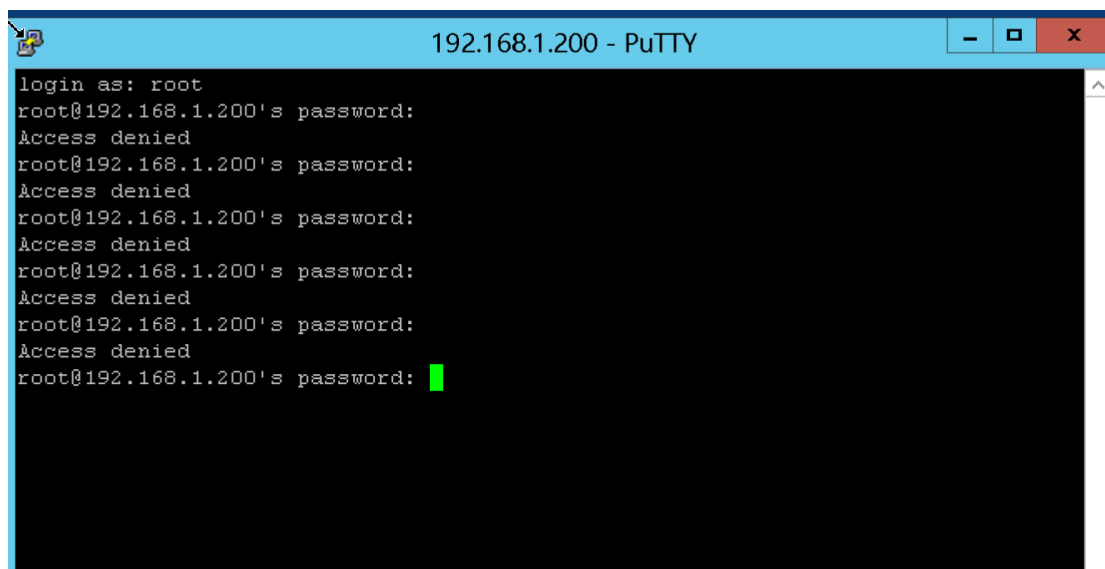
/var/ossec/bin/ossec-control restart

```
alienvault:/var/ossec/rules# sudo vim sshd_rules.xml
alienvault:/var/ossec/rules# /var/ossec/bin/ossec-control restart
Killing ossec-monitord ..
Killing ossec-logcollector ..
Killing ossec-remoted ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
ossec-maild not running ..
ossec-execd not running ..
OSSEC HIDS v2.5.1 Stopped
Starting OSSEC HIDS v2.5.1 (by Trend Micro Inc.)...
2021/04/20 18:54:28 ossec-testrule: INFO: Reading local decoder file.
2021/04/20 18:54:28 ossec-maild: INFO: E-Mail notification disabled. Clean Exit
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
You have new mail in /var/mail/root
alienvault:/var/ossec/rules#
```

重启 OSSEC 服务器

3.4 使用 ssh 登陆服务器，多次输错密码，触发警报

尝试使用 ssh 登录服务器，并且多次输错密码，尝试时间超过 30s，触发警报



多次输错密码

3.5 在 web 端查看报警信息

登录 OSSIM web 端，输入 ossec 进行 ossec 报警信息筛选，可以看到 root 用户两次使用空密码登录失败的多条报警信息，如图 3-1 所示。该信息可以作为判定黑客多次登录尝试的入侵行为重要依据

报警信息如下所示

| ▶ Displaying events 1-50 of about thousands matching your selection. 4,01 | | | | | | |
|---|------------------------------------|---------------------|------------|------------------------|-------------|------|
| <input type="checkbox"/> | Signature | ▲ Date GMT+8:00 ▼ | Sensor | Source | Destination | As S |
| <input checked="" type="checkbox"/> | ossec: SSHD authentication failed. | 2021-04-20 18:59:21 | alienvault | Host-fa1692d7eea8:1155 | alienvault | 2- |
| <input checked="" type="checkbox"/> | ossec: SSHD authentication failed. | 2021-04-20 18:59:18 | alienvault | Host-fa1692d7eea8:1155 | alienvault | 2- |
| <input checked="" type="checkbox"/> | ossec: SSHD authentication failed. | 2021-04-20 18:59:15 | alienvault | Host-fa1692d7eea8:1155 | alienvault | 2- |
| <input checked="" type="checkbox"/> | ossec: SSHD authentication failed. | 2021-04-20 18:59:11 | alienvault | Host-fa1692d7eea8:1155 | alienvault | 2- |
| <input checked="" type="checkbox"/> | ossec: SSHD authentication failed. | 2021-04-20 18:59:08 | alienvault | Host-fa1692d7eea8:1155 | alienvault | 2- |
| <input type="checkbox"/> | ossec: User login failed. | 2021-04-20 18:59:06 | alienvault | Host-fa1692d7eea8 | alienvault | 2- |

报警信息

任务四：监视 CentOS7 root 用户情况

本实验任务在实验一的基础上，主要完成以下内容

- 在 CentOS7 代理端设置规则
- 使用 PuTTY 远程连接 CentOS7，模拟攻击者破解监控的服务器的用户名和密码后登录服务器
- 查看 OSSEC 入侵检测系统检测到的报警信息，理解入侵检测系统对于

监视用户登录情况的重要性

本实验的实验目标如下

- 掌握入侵检测的概念、原理，掌握入侵检测规则的设置方法
- 熟悉 PuTTY 工具的基本功能，掌握使用 PuTTY 远程登录服务器的方法
- 熟悉 OSSIM 集成检测平台的功能，掌握该平台报警信息的筛选与查看方法
- 熟悉 OSSEC 入侵检测系统的工作原理和常用功能，掌握 OSSEC 入侵检测系统报警信息的查看方法

4.1 查看配置文件

使用如下命令在 CentOS7 终端查看代理的配置文件，可以看到 OSSIM 平台不默认监控 `/var/log/secure` 文件夹

`cat /var/ossec/etc/ossec.conf | grep "var/log/secure"`

```
alienvault:/var/ossec/bin# cat /var/ossec/etc/ossec.conf | grep "/var/log/secure"
alienvault:/var/ossec/bin#
```

要监控的文件

查看配置文件

因此我们添加该项监控规则

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/secure</location>
</localfile>
```

添加该项

再次检查发现已经成功添加

```
alienvault:/var/ossec/bin# cat /var/ossec/etc/ossec.conf | grep "/var/log/secure"
  <location>/var/log/secure</location>
alienvault:/var/ossec/bin#
```

包含该项

4.2 重启 OSSIM 服务器

使用如下命令重启 OSSIM 服务器

`/var/ossec/bin/ossec-control restart`

```

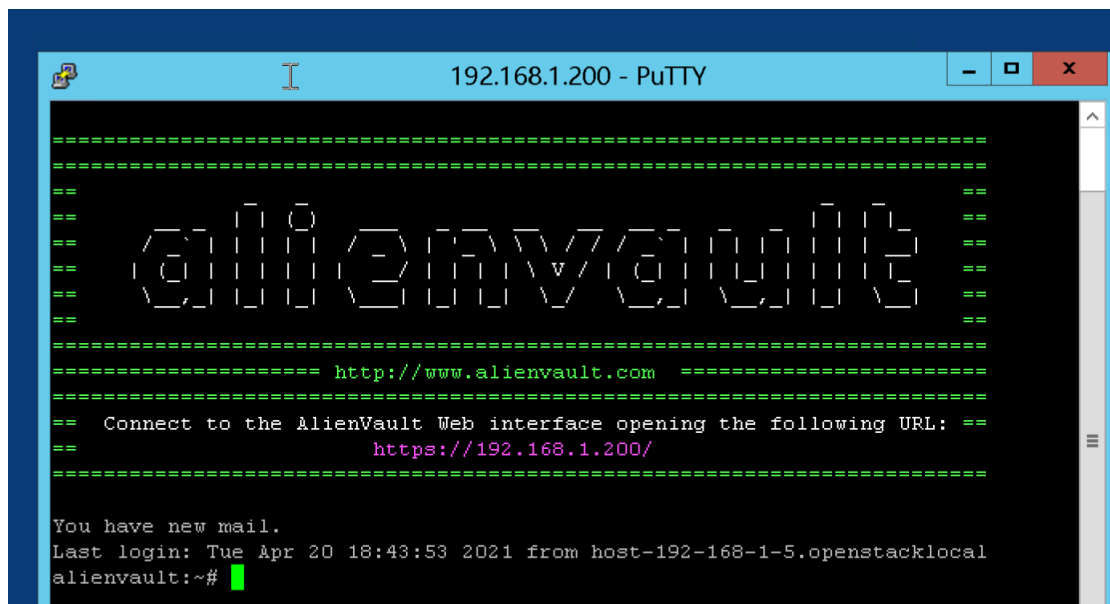
You have new mail in /var/mail/alienvault
alienvault:/var/ossec/rules# /var/ossec/bin/ossec-control restart
ossec-monitord not running ..
ossec-logcollector not running ..
ossec-remoted not running ..
ossec-syscheckd not running ..
ossec-analysisd not running ..
ossec-maild not running ..
ossec-execd not running ..
OSSEC HIDS v2.5.1 Stopped
Starting OSSEC HIDS v2.5.1 (by Trend Micro Inc.)...
2021/04/20 19:15:01 ossec-testrule: INFO: Reading local decoder file.
2021/04/20 19:15:01 ossec-maild: INFO: E-Mail notification disabled. Clean Exit
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...

```

重启服务器

4.3 使用 putty 登录远程服务器

使用 putty 登录远程服务器



登录服务器

4.4 添加新用户




















使用如下命令添加新用户 **simpleware** 并将其密码设置为 **Simplexue123**
adduser simpleware

```
alienvault:~# adduser simpleware          添加用户simpleware
Adding user `simpleware' ...
Adding new group `simpleware' (1001) ...
Adding new user `simpleware' (1003) with group `simpleware' ...
Creating home directory `/home/simpleware' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for simpleware
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
```

添加新用户

4.5 在 OSSIM web 页面上查看报警信息

在 web 页面中可以看到有添加新用户和新用户组的报警信息

| | | | | | |
|---|--|---------------------|------------|--|--|
|  | <input type="checkbox"/> ossec: Information from the user was changed | 2021-04-20 19:19:23 | alienvault | 0.0.0.0 | alienvault  |
|  | <input type="checkbox"/> ossec: Integrity checksum changed again (2nd time). | 2021-04-20 19:19:14 | alienvault | 0.0.0.0 | alienvault  |
|  | <input type="checkbox"/> ossec: Integrity checksum changed again (3rd time). | 2021-04-20 19:18:58 | alienvault | 0.0.0.0 | alienvault  |
|  | <input checked="" type="checkbox"/> ossec: New user added to the system | 2021-04-20 19:18:57 | alienvault | 0.0.0.0 | alienvault  |
|  | <input checked="" type="checkbox"/> ossec: New group added to the system | 2021-04-20 19:18:57 | alienvault | 0.0.0.0 | alienvault  |
|  | <input type="checkbox"/> ossec: Login session opened. | 2021-04-20 19:17:09 | alienvault | 0.0.0.0 | alienvault  |
|  | <input type="checkbox"/> ossec: SSHD authentication success. | 2021-04-20 19:17:09 | alienvault | Host-fa1692d7eea8:1202  | alienvault  |
|  | <input type="checkbox"/> ossec: Ossec server started. | 2021-04-20 19:15:12 | alienvault | 0.0.0.0 | alienvault  |
|  | <input type="checkbox"/> ossec: Windows Logon Success. | 2021-04-20 19:12:26 | alienvault | Host-fa1692d7eea8  | 0.0.0.0 |

报警信息

其对应的签名为如下

ossec:New user added to the system

ossec:New group added to the system

任务五：监控 Web 服务器的访问日志

本实验任务在实验一完成的基础上，主要完成以下内容

- 在 CentOS7 代理端设置监视 Web 服务器访问日志的规则。
- 访问 CentOS7 Web 服务器被禁止访问的目录。

- 查看入侵检测系统检测到的报警信息，理解入侵检测系统对于监视被禁止访问的目录的重要性。

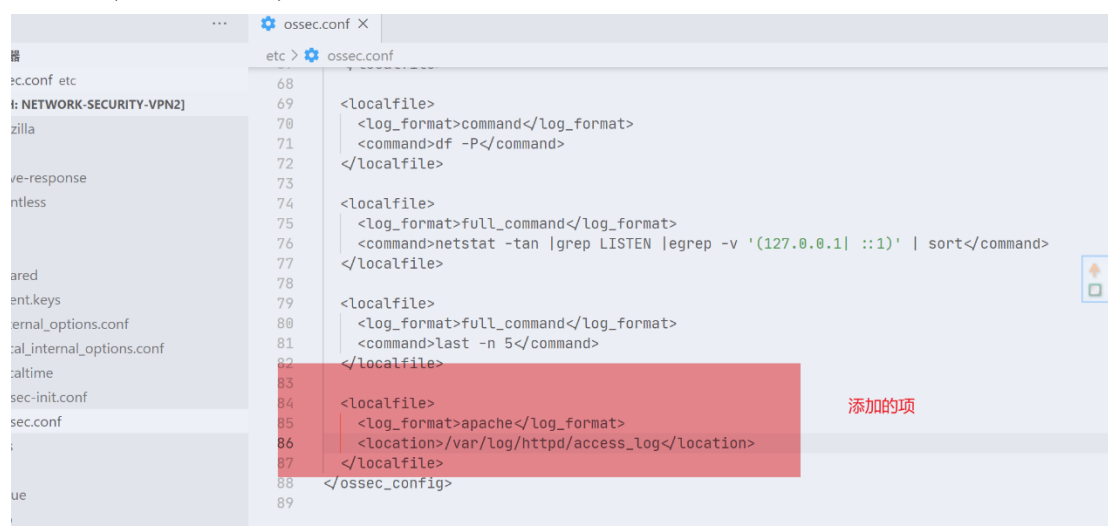
本实验的实验目标如下

- 充分理解入侵检测的概念、原理、方法和流程，掌握入侵检测规则的设置方法。
- 熟悉 OSSIM 集成检测平台的功能，掌握其报警信息的筛选与查看方法。

5.1 修改配置文件 ossec.conf

在 CentOS7 的终端修改 ossec.conf 文件。

得益于 **vscode** 强大的远程开发功能，我们可以不用 **vim**，直接对配置文件进行编辑(上面忘记了)。添加如下项



```
68 <localfile>
69 <log_format>command</log_format>
70 <command>df -P</command>
71 </localfile>
72
73
74 <localfile>
75 <log_format>full_command</log_format>
76 <command>netstat -tan |grep LISTEN |grep -v '(127.0.0.1|::1)' | sort</command>
77 </localfile>
78
79 <localfile>
80 <log_format>full_command</log_format>
81 <command>last -n 5</command>
82 </localfile>
83
84 <localfile>
85 <log_format>apache</log_format>
86 <location>/var/log/httpd/access_log</location>
87 </localfile>
88 </ossec_config>
89
```

添加如下项

5.2 重启 OSSEC 服务

在终端输入如下命令，重启 OSSEC 服务

/var/ossec/bin/ossec-control restart

```
问题 输出 调试控制台 终端 端口 1: bash

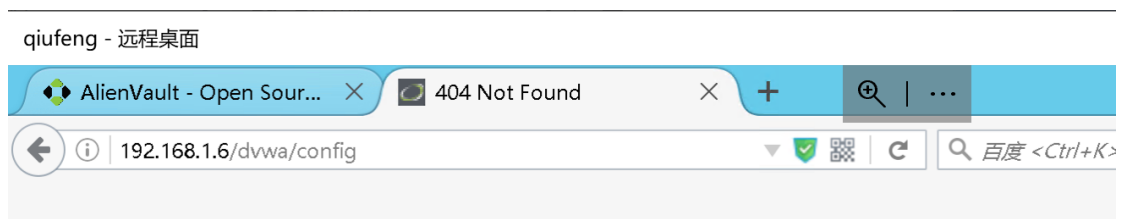
[root@localhost ossec]# /var/ossec/bin/ossec-control restart
Killing ossec-logcollector ..
Killing ossec-syscheckd ..
Killing ossec-agentd ..
Killing ossec-execd ..
OSSEC HIDS v2.9.1 Stopped
Starting OSSEC HIDS v2.9.1 (by Trend Micro Inc.)...
Started ossec-execd...
2021/04/20 19:30:04 ossec-agentd: INFO: Using notify time: 600 and max time to reconne
Started ossec-agentd...
2021/04/20 19:30:04 ossec-logcollector(1226): ERROR: Error reading XML file '/var/osse
XMLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 89).
Started ossec-logcollector...
2021/04/20 19:30:04 ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/e
ERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 89).
2021/04/20 19:30:04 ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/e
ERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 89).
Started ossec-syscheckd...
Completed
```

重启 OSSEC 服务

5.3 在 windows 上访问被禁止的目录

在 windows 2012 上访问如下地址，提示信息为 **Not Found**

<http://192.168.1.6/dvwa/config>



Not Found

The requested URL /dvwa/config was not found on this server.

访问禁止页面

在 OSSIM web 中查看报警信息

在 OSSIM web 中查看报警信息如下

