第四次网络安全实验报告

课程名称	入侵检测实验				
学生姓名	陈曦	学号	2020302181081	指导老师	曹越
专业	网络安全	班级	2020 级 3 班	实验时间	2023.4.16

目录

一、实验描述

【实验任务】

1. 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. 监视 OSSIM 服务器本地 root 用户的登录情况
3. 基于 SSH 的远程非法入侵检测
4. 监视 CentOS7 root 用户情况
5. 监控 Web 服务器的访问日志

【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。

【实验工具】

OSSIM
OSSEC
Putty
Firefox

【实验环境】

操作系统	IP地址	服务器角色	登录账户密码
OSSIM	192.168.1.200	OSSEC Server	用户名：root；密码：Simplexue123
CentOS7	192.168.1.6	OSSEC Agent	用户名：root；密码：Simplexue123
Windows 2012	192.168.1.5	OSSEC Agent	用户名：administrator；密码：Simplexue123

二、实验原理

1. 入侵检测与入侵检测系统的概念

入侵检测（Intrusion Detection，ID），顾名思义，是对入侵行为的检测。它通过收集和分析计算机网络或计算机系统中若干关键点的信息,检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象，以便决策者有效采取措施，以保证网络系统资源的机密性、完整性和可用性。

入侵检测系统（intrusion detection system，简称“IDS”）是一种对网络传输进行即时监视,在发现可疑传输时发出警报或者采取主动反应措施的网络安全系统。它与其他网络安全设备的不同之处便在于，IDS 是一种积极主动的安全防护技术。

2. OSSIM 与 OSSEC 简介

OSSIM 即开源安全信息管理系统(OPEN SOURCE SECURITY INFORMATION MANAGEMENT)，是一个非常流行和完整的开源安全架构体系。OSSIM 通过将开源产品进行集成，从而提供一种能够实现安全监控功能的基础平台。 它的目的是提供一种集中式、有组织的、能够更好地进行监测和显示的框架式系统。

OSSIM 明确定位为一个集成解决方案，其目标并不是要开发一个新的功能，而是利用丰富的、强大的各种程序(包括 Snort、Rrd、Nmap、 Nessus 以及 Ntop 等开源系统安全软件)。在一个保留他们原有功能和作用的开放式架构体系环境下，将他们集成起来。而 OSSIM 项目的核心工作在于负责集成和关联各种产品提供的信息，同时进行相关功能的整合。由于开源项目的优点，这些工具已经是久经考验，同时也经过全方位测试、是可靠的工具。

OSSEC 是一个运行在 OSSIM 系统中的开源的入侵检测系统，从架构上看它属于 C/S 架构，从功能上看它可以执行日志收集与分析、完整性检测、rootkit 检测、蠕虫检测、Windows 注册表和实时报警等任务。它不仅支持 OSSIM 本身，还可以在 UNIX、Linux、Mac、Windows 系统中运行。由于 OSSEC Server 端就安装在 OSSIM 系统中，并和 iptables 实现了联动功能，因此只需在客户端安装代理即可，也就是通过 OSSEC Server+Agent 方式，以实现 HIDS 系统功能。

OSSIM 系统中的 HIDS(Host-based Intrusion Detection System，简称 HIDS，即基于主机型入侵检测系统。作为计算机系统的监视器和分析器，它并不作用于外部接口，而是专注于系统内部，监视系统全部或部分的动态的行为以及整个计算机系统的状态。）通过安装在其他操作系统上的 Agent 程序来审计操作系统以及用户的活动，比如用户的登录、命令操作、软件升级、系统文件的完整性、应用程序使用资源情况等，根据主机行为特征确定是否发生入侵行为，并把警报信息发送给 OSSIM 上的 OSSEC Server。这种 HIDS 可以精确地分析入侵活动，能确定是哪一个用户或者进程对系统进行过攻击。

OSSIM 系统的工作流程为：

（1）作为整个系统的安全插件的探测器（Sensor）执行各自的任务，当发现问题时给予报警。

（2）各探测器的报警信息将被集中采集。

（3）将各个报警记录解析并存入事件数据库（EDB）。

（4）根据设置的策略（Policy）给每个事件赋予一个优先级（Priority）。

（5）对事件进行风险评估，给每个警报计算出一个风险系数。

（6）将设置了优先级的各事件发送至关联引擎，关联引擎将对事件进行关联。注意：关联引擎就是指在各入侵检测传感器（入侵检测系统、防火墙等）上报的告警事件基础上，经过关联分析形成入侵行为判定，并将关联分析结果报送控制台。

（7）对一个或多个事件进行关联分析后，关联引擎生成新的报警记录，将其也赋予优先级，并进行风险评估，存入数据库。

（8）用户监控监视器将根据每个事件产生实时的风险图。

（9）在控制面板中给出最近的关联报警记录，在底层控制台中提供全部的事件记录。

3. Putty 简介

PuTTY 是一个 Telnet、SSH、rlogin、纯 TCP 以及串行接口连接软件。较早的版本仅支持 Windows 平台，在最近的版本中开始支持各类 Unix 平台，并打算移植至 Mac OS X 上。PuTTY 为一开放源代码软件，主要由 Simon Tatham 维护，使用 MIT licence 授权。随着 Linux 在服务器端应用的普及，Linux 系统管理越来越依赖于远程。在各种远程登录工具中，Putty 是出色的工具之一。Putty 是一个免费的、Windows x86 平台下的 Telnet、SSH 和 rlogin 客户端，但是功能丝毫不逊色于商业的 Telnet 类工具。目前最新的版本为 0.68 latest release。

优点

用它来远程管理 Linux 十分好用，其主要优点如下：

完全免费;

在 Windows 9x/NT/2000 下运行的都非常好;

全面支持 SSH1 和 SSH2;

绿色软件，无需安装，下载后在桌面建一个快捷方式即可使用;

体积很小，仅 519KB(0.67 版本);

操作简单，所有的操作都在一个控制面板中实现。

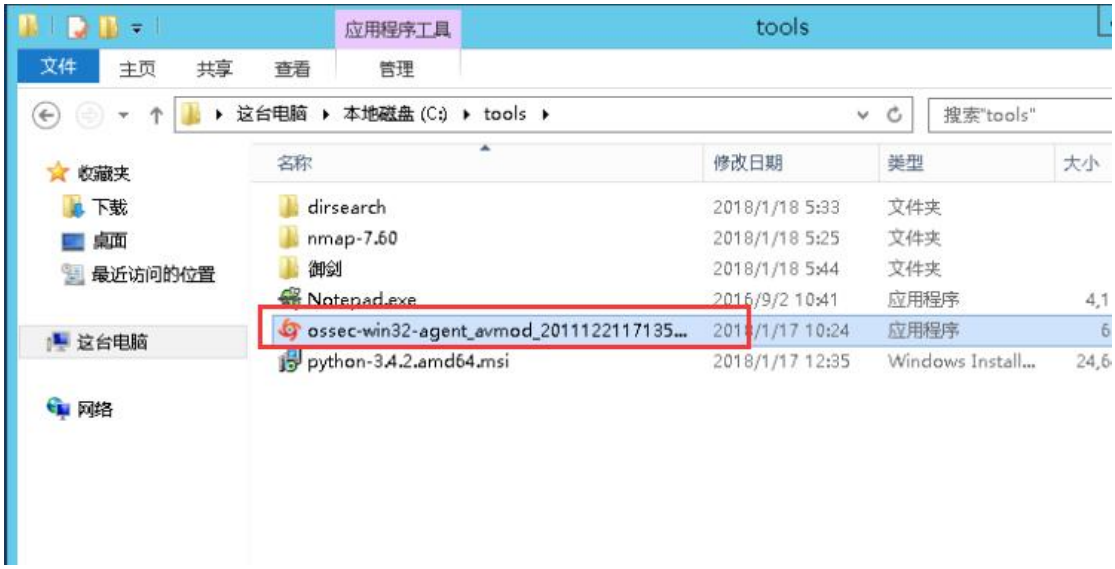
特色：PuTTY 包括了：支持 IPv6 连接。可以控制 SSH 连接时加密协定的种类。目前有 3DES、AES、Blowfish、DES（不建议使用）及 RC4。CLI 版本的 SCP 及 SFTP Client，分别叫做 pscp 与 psftp。自带 SSH Forwarding 的功能，包括 X11 Forwarding。完全模拟 xterm、VT102 及 ECMA-48 终端机的能力。支持公钥认证。

三、实验内容

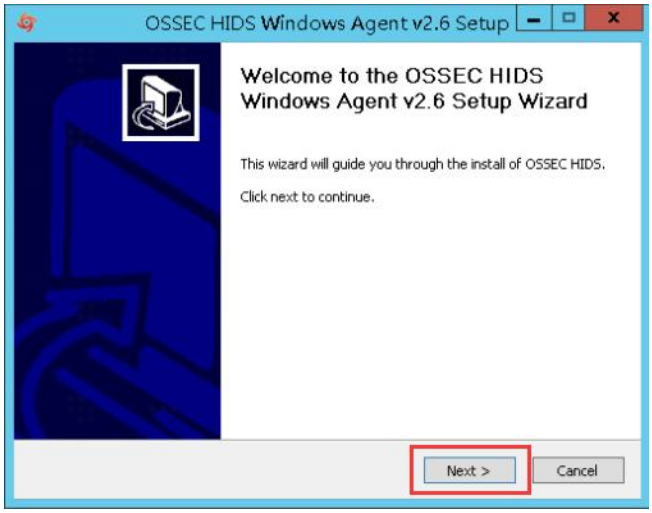
1. 在不同的操作系统环境下安装和配置 OSSEC 代理，构建入侵检测环境

【安装 OSSEC HIDS Windows Agent 工具软件】

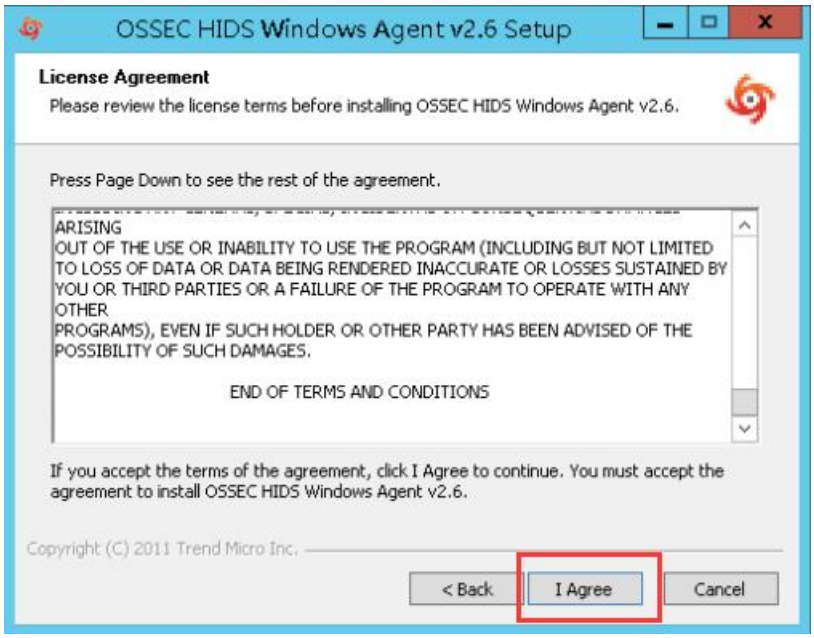
在系统 C 盘的 tools 文件夹中，我们可以找到 OSSEC 代理软件。双击软件开始安装。



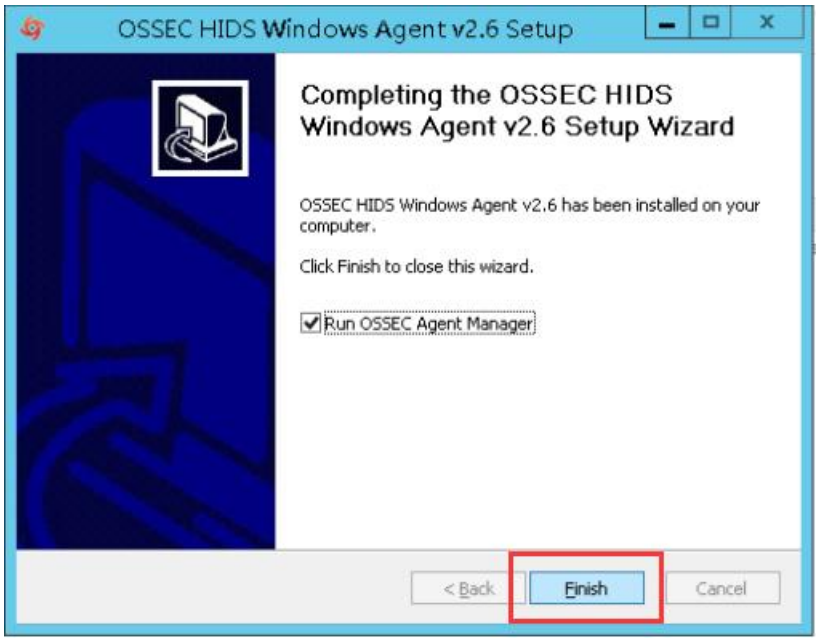
点击 Next。



选择同意协议。



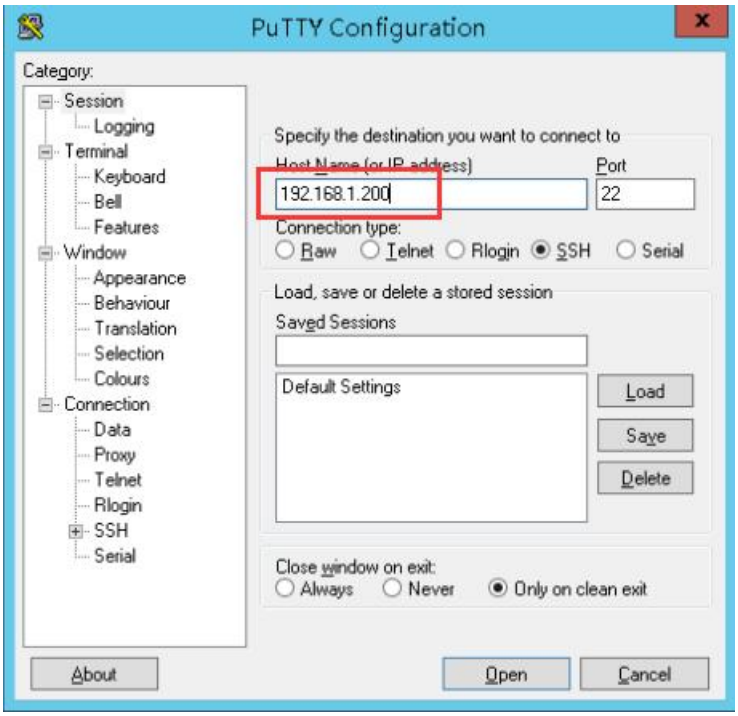
最后完成安装。



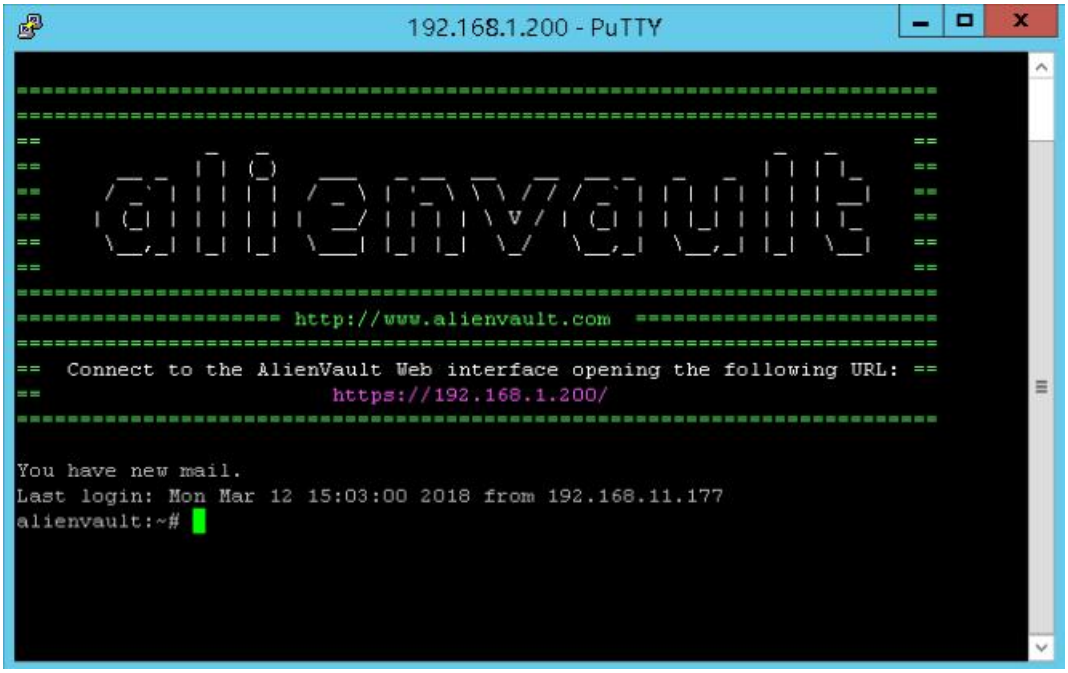
输入 OSSEC 服务 IP 为 192.168.1.200。

在桌面上找到 putty 应用程序。

将主机 IP 地址设置为 192.168.1.200。最后点击 open 开启程序。

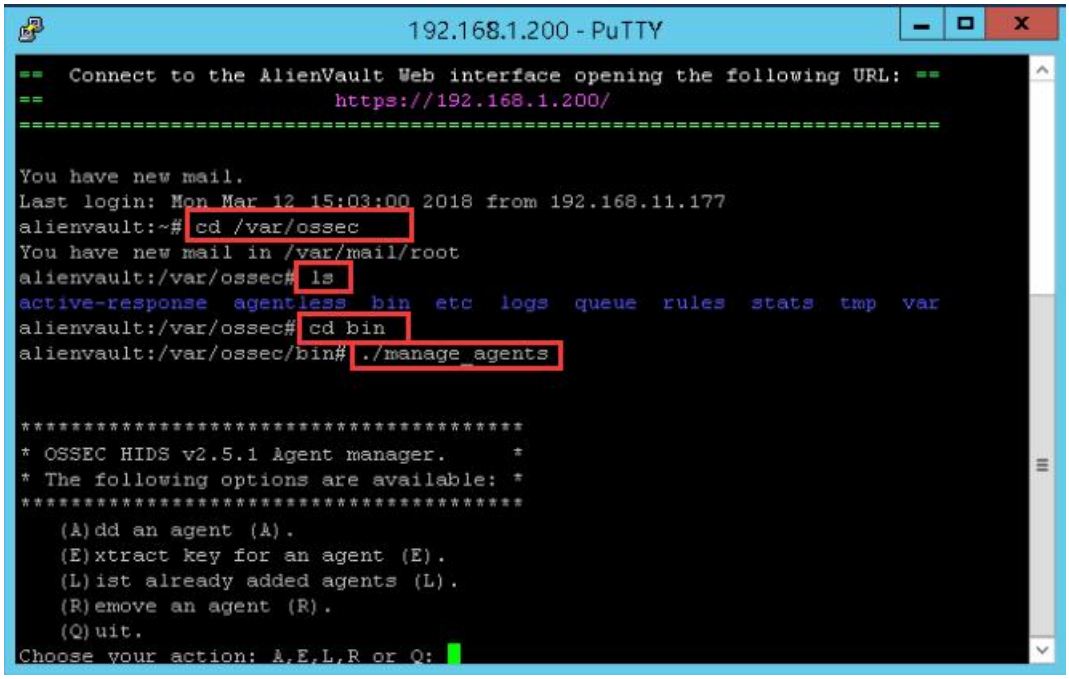


进入终端页面，输入 root 账号密码即可登陆成功。

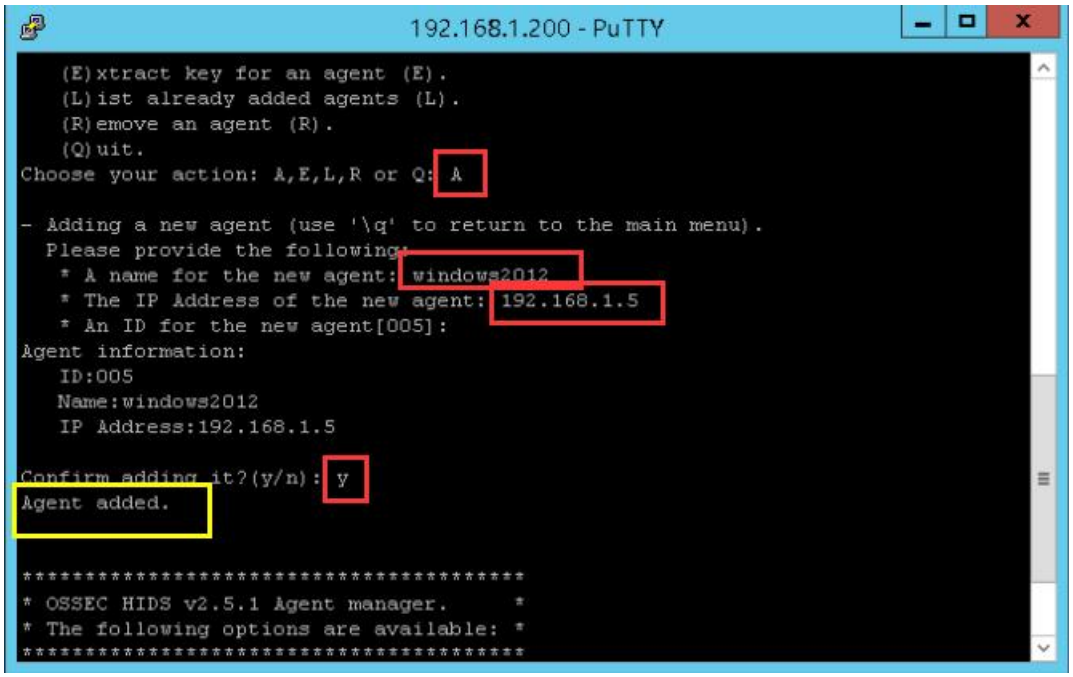


【在 Windows 平台下安装和配置 OSSEC 代理】

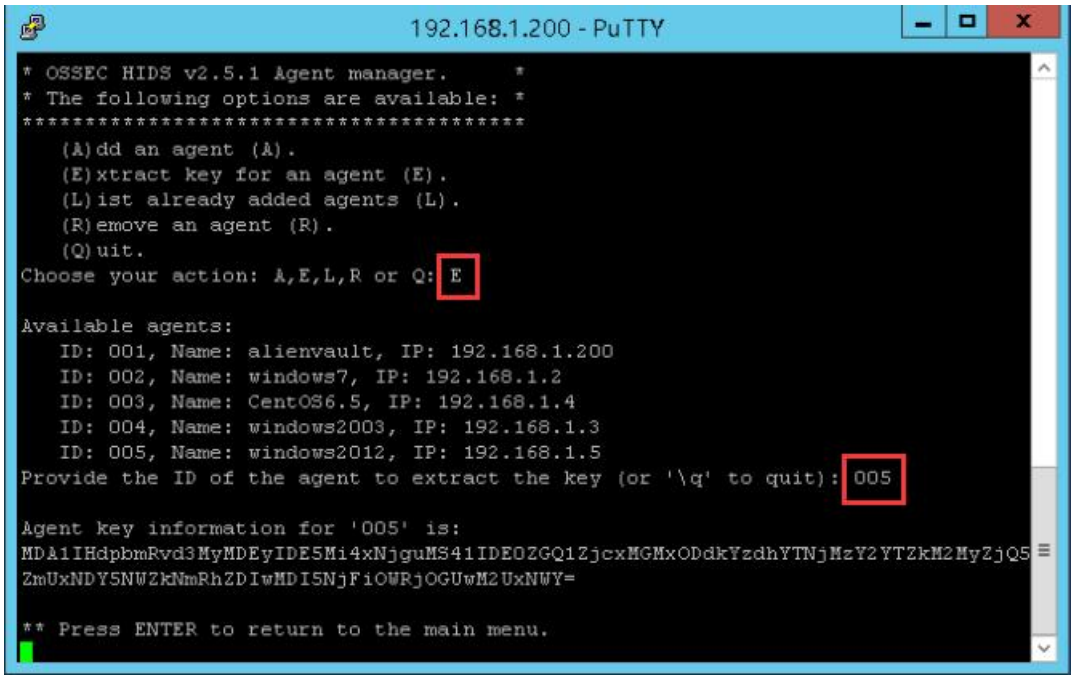
在 windows2012 上，使用 putty 终端启动 OSSEC 代理管理程序，创建新 OSSEC 代理（名称：windows2012、ID：005），生成密钥。运行 OSSEC 代理管理程序。



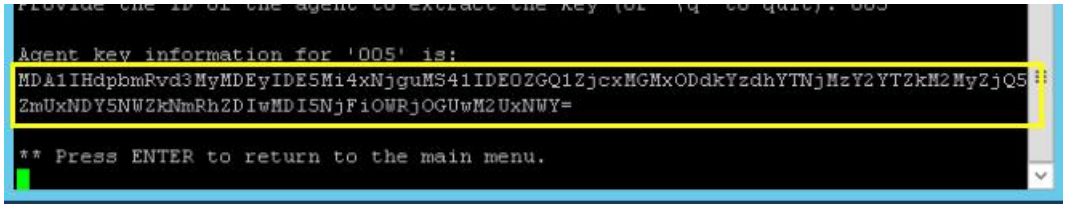
创建新的代理，选取行为为“a”表示添加，并配置相关的信息。名称为 windows2012，ID 为 005。可以看到最后代理已被添加。



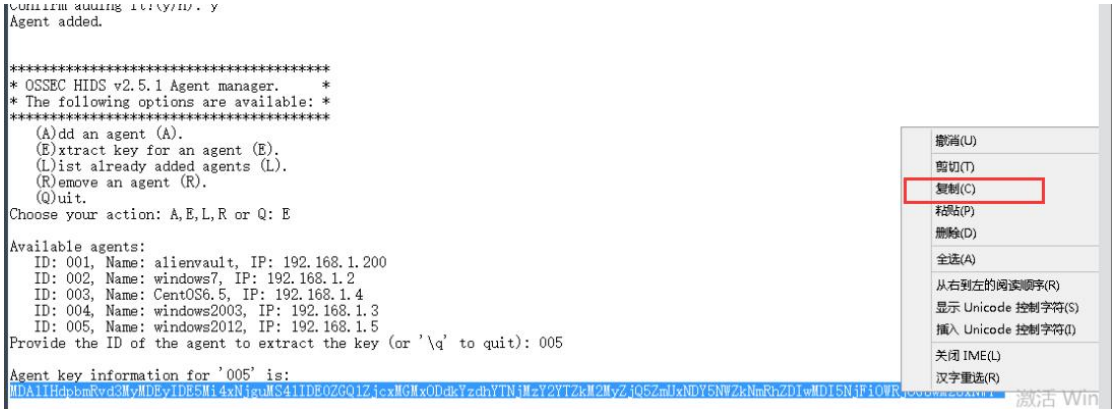
使用口令“E”来生成密钥并且保存。输入刚刚创建的 ID005。



密钥信息为：

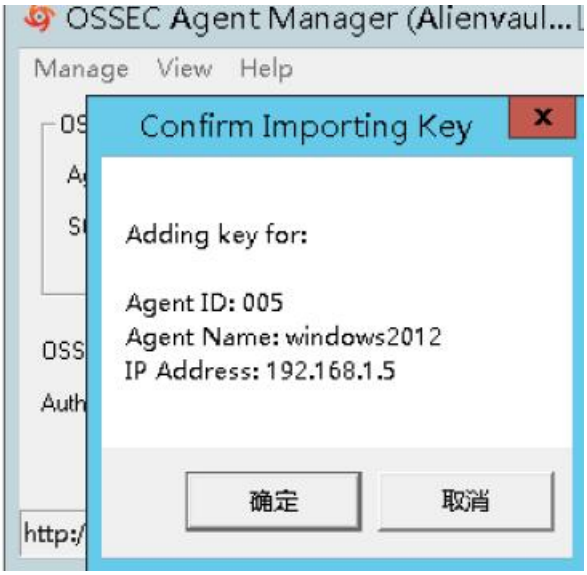


复制该密钥并把它保存在 OSSEC 客户端的密钥栏中。由于操作机不太好操控，可以将屏幕内容复制到记事本中。再进行复制。



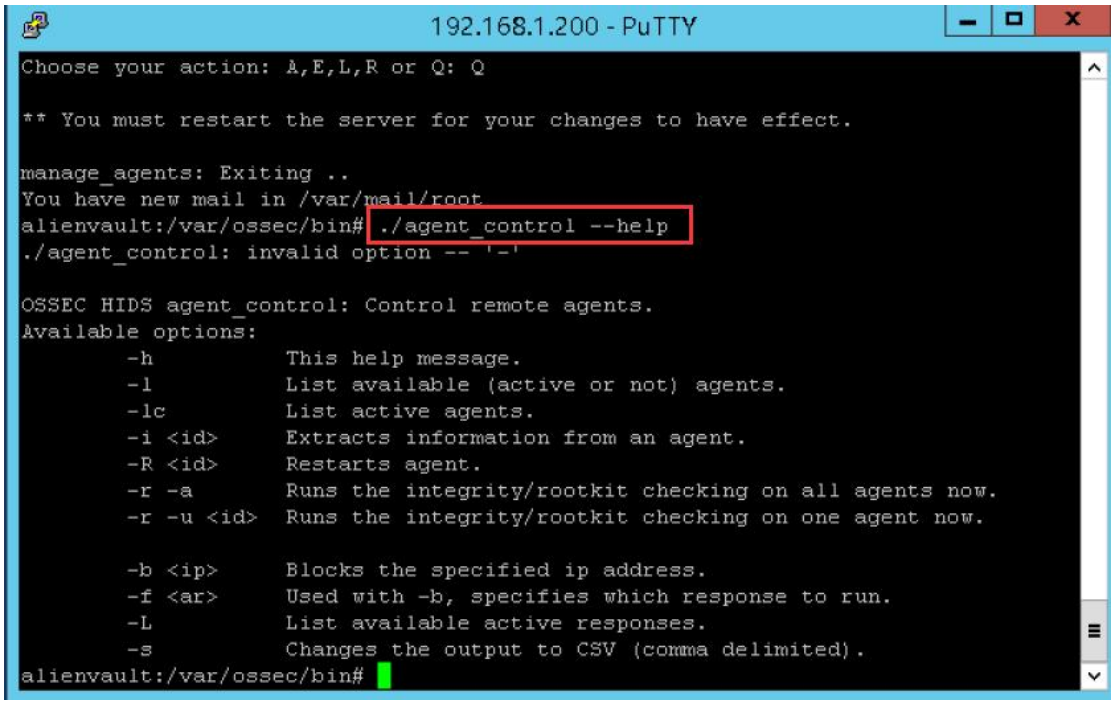
复制到 OSSEC 客户端中。

点击“save”即可保存。

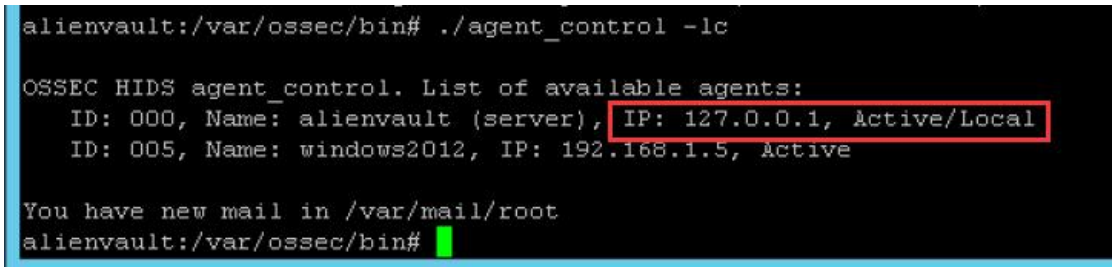


点击菜单栏的 Manage 来启动 OSSEC。

查看 agent_control 的程序帮助信息。



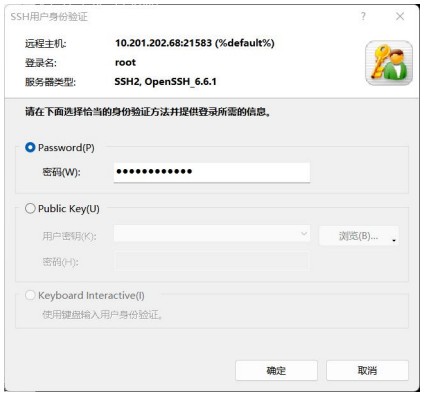
使用命令./agent_control -lc 查看代理状态，可以发现已经被激活。



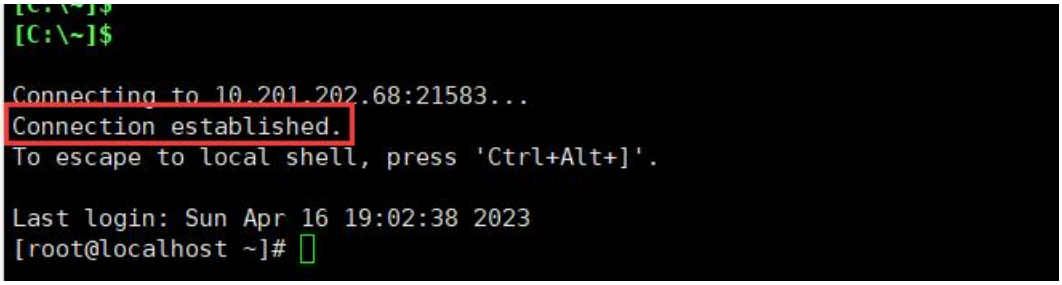
【在 Linux 平台下安装和配置 OSSEC 代理】

切换系统，使用 Xshell 连接目标机。

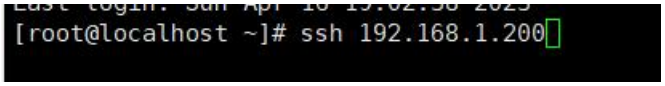
输入用户名 root 和密码。



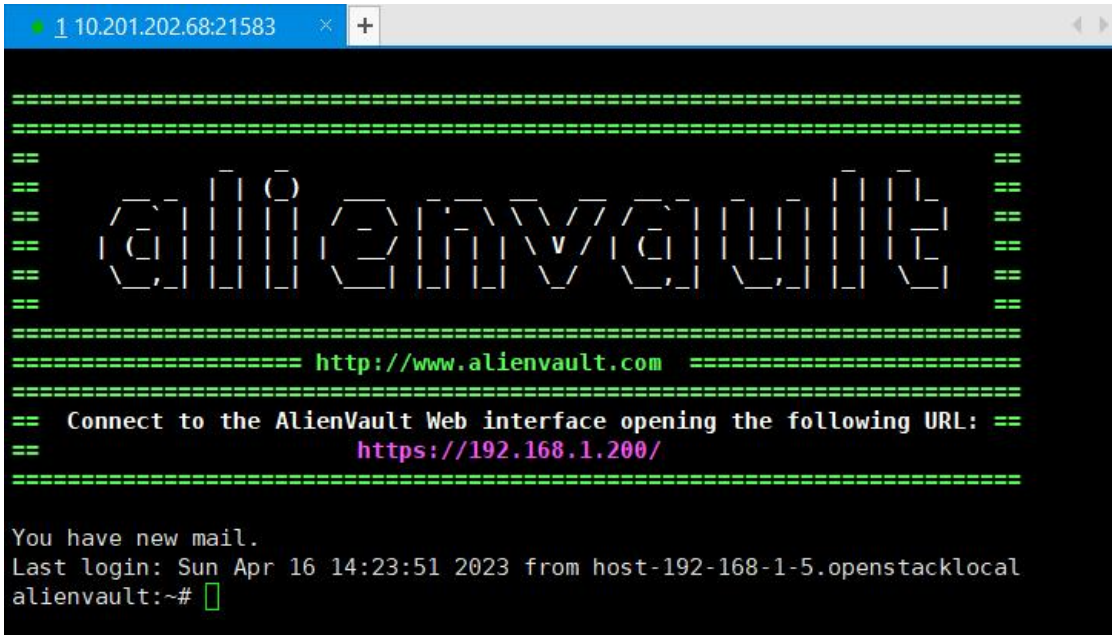
连接成功。



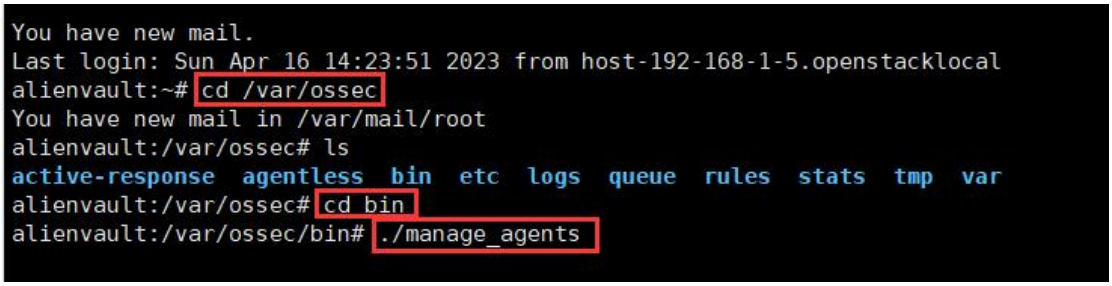
输入 ssh 192.168.1.200 来登录，并输入密码。



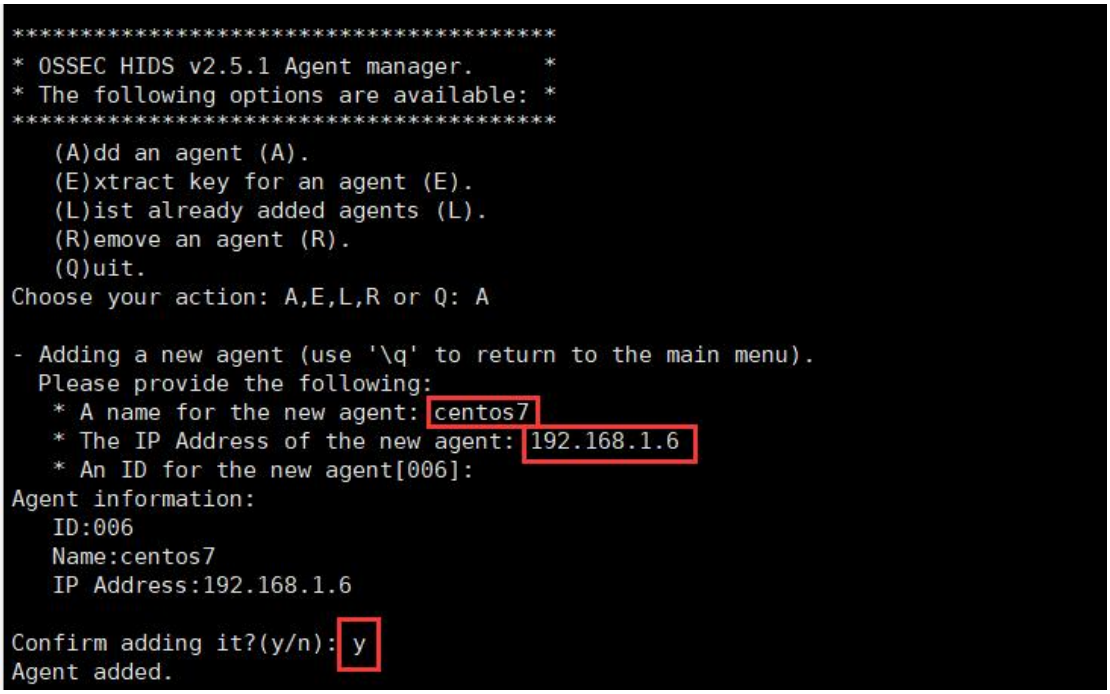
看到此页面即登录成功。



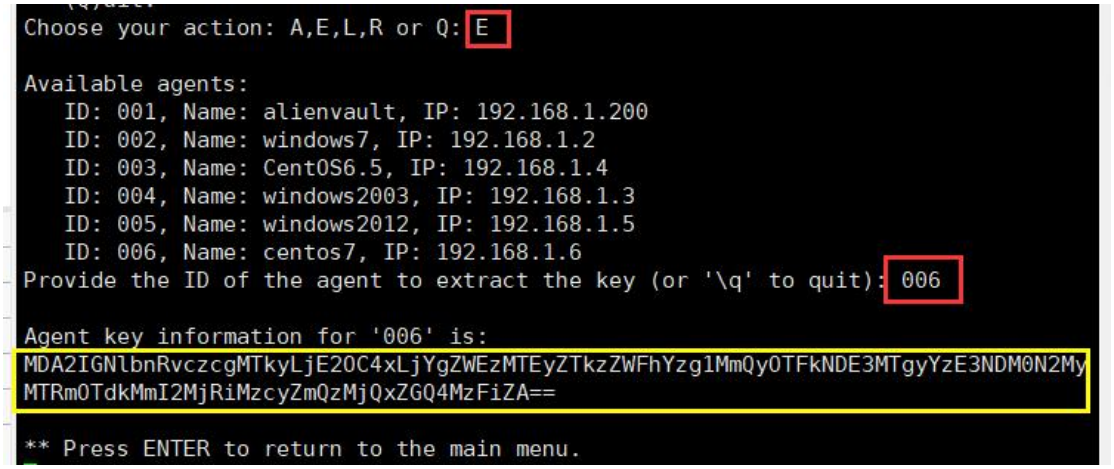
启动 OOSEC 的代理程序。



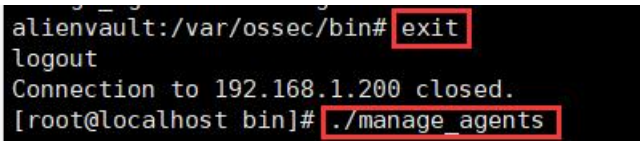
新建代理服务。代理服务添加完毕。



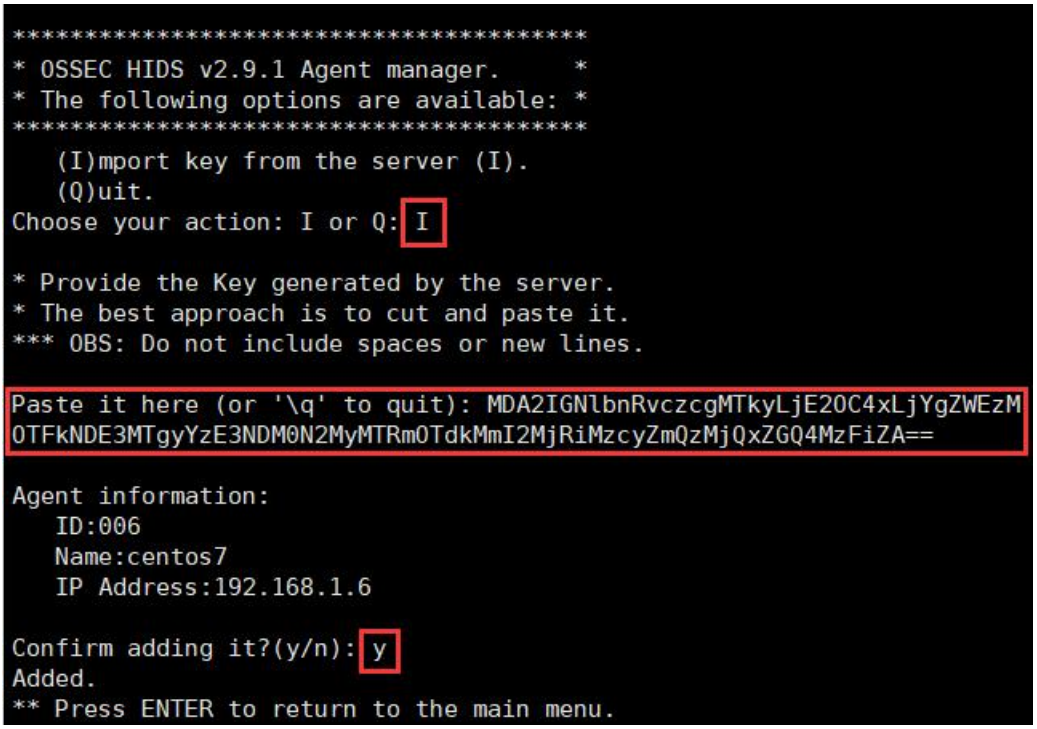
生成代理密钥。



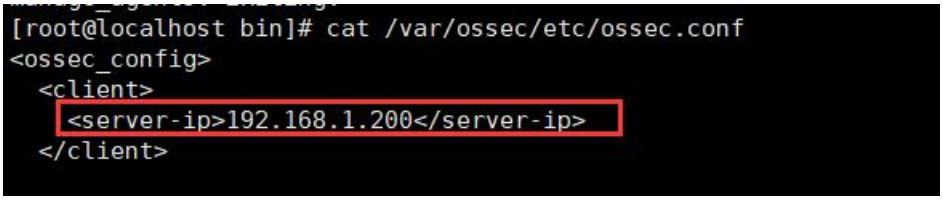
推出目前的远程连接，在本机的/var/ossec/bin 文件夹中运行程序。



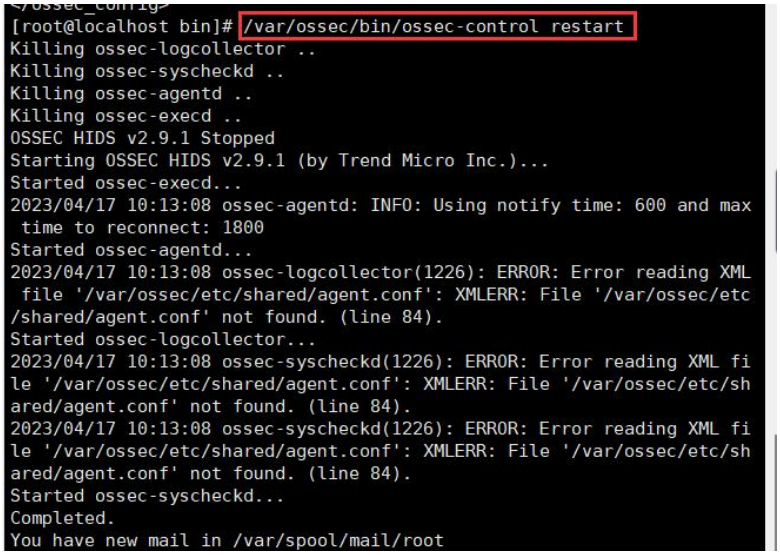
运行程序 manage_agents 并添加密钥。
MDA2IGNlbnRvczcgMTkyLjE2OC4xLjYgZWEzMTEyZTkzZWFhYzg1MmQyOTFkNDE3MTgyYzE3NDM0N2MyMTRmOTdkMmI2MjRiMzcyZmQzMjQxZGQ4MzFiZA==



使用“Q”指令退出程序。查看/var/ossec/etc/目录下的 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



重启 OSSEC 服务，查看运行状态，使用命令/var/ossec/bin/ossec-control restart。



使用命令 /var/ossec/bin/ossec-control status 查看 OSSEC 运行状态。

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

回到对 192.168.1.200 的远程连接状态。使用命令 /var/ossec/bin/agent_control -lc 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。

```
alienvault:~# cd /var/ossec/bin
alienvault:/var/ossec/bin# /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: 006, Name: centos7, IP: 192.168.1.6, Active
```

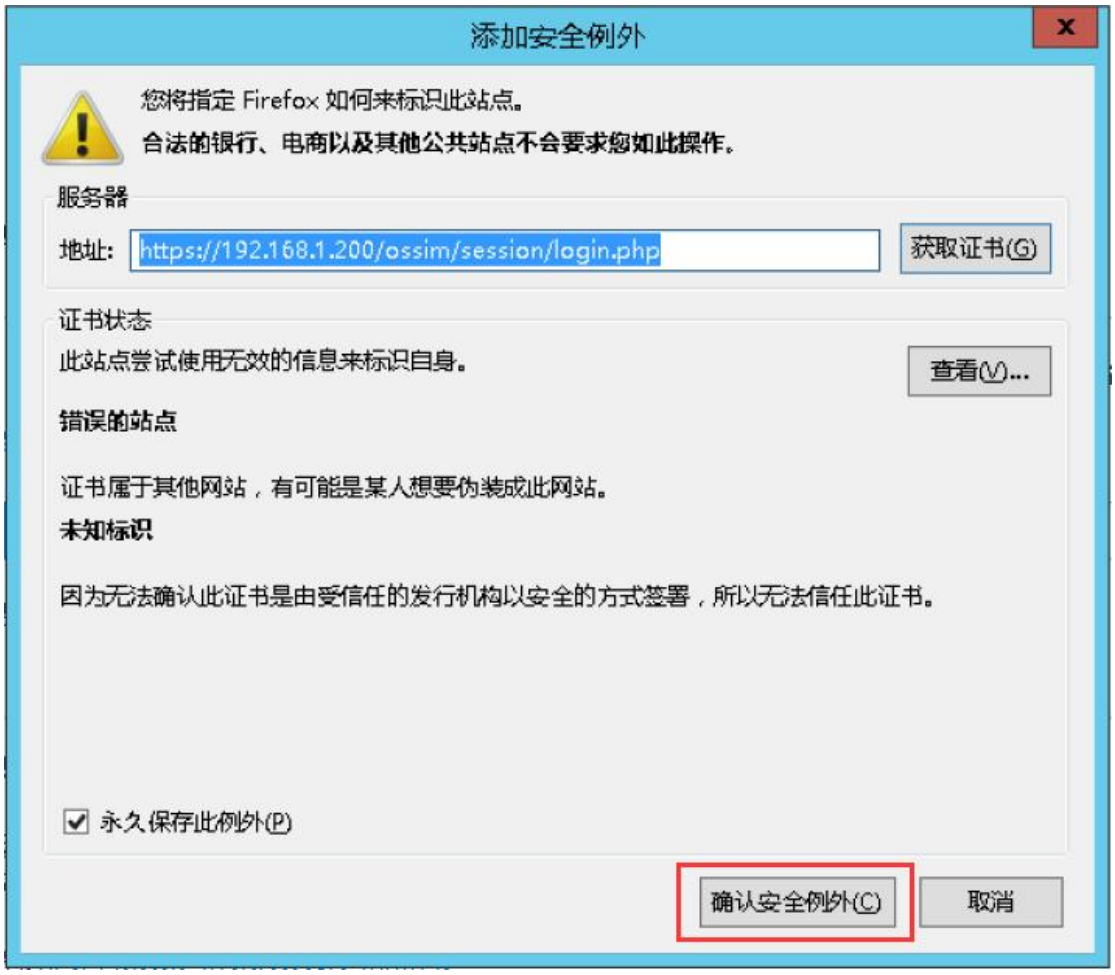
2. 监视 OSSIM 服务器本地 root 用户的登陆情况

需要在 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陆情况的重要性。

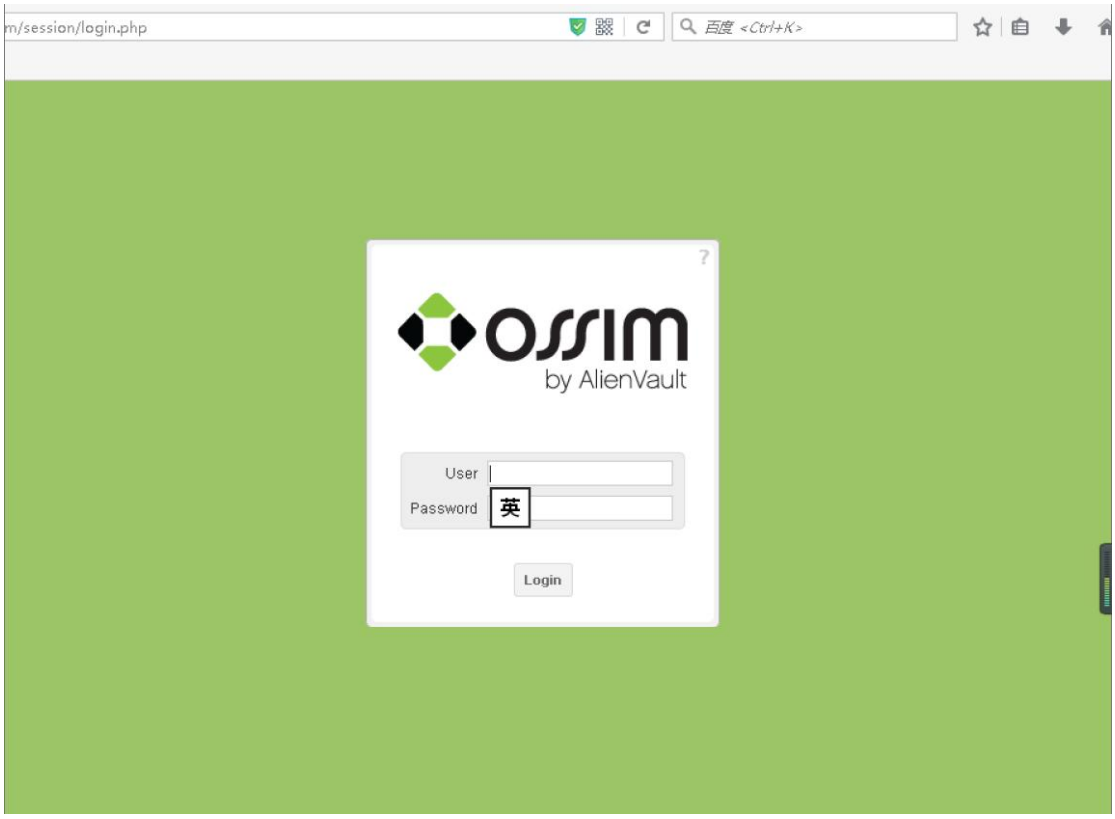
访问网址 https://192.168.1.200/ossim/session.login.php。发现火狐不能信任网站证书。

在高级-添加例外中添加例外。

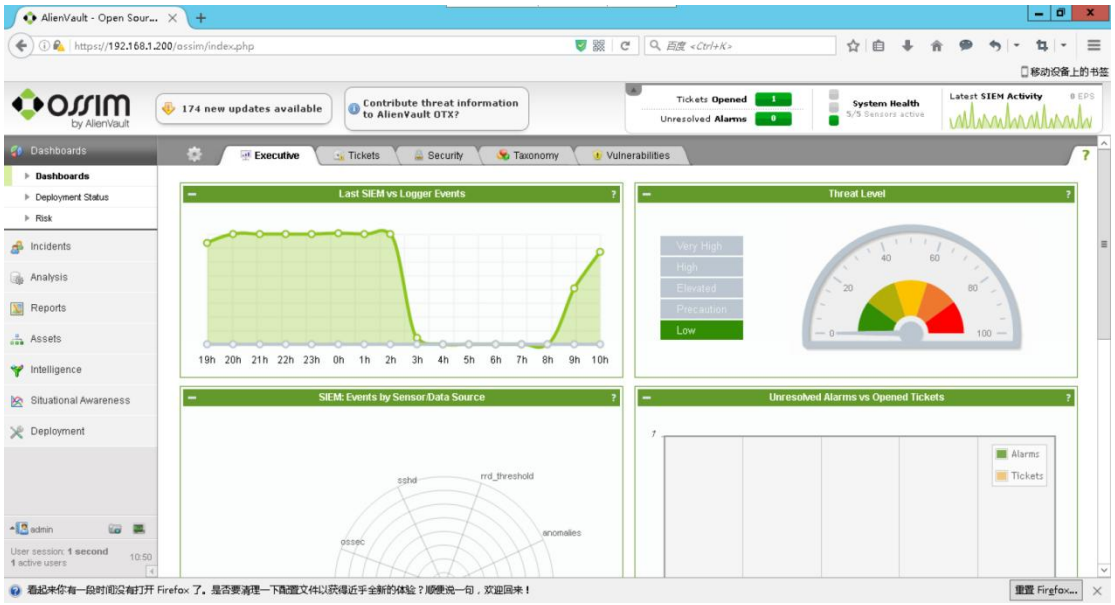
确认安全例外。



发现页面可以打开。输入用户名 admin 和密码 Simplexue123。



登录后可以查看到后台管理界面，如下图所示。



在 Analysis-Detection-HIDS-Ossec.conf 中可以查看 ossec.conf 规则配置文件。可以发现/var/log/auth.log 默认被监控，该日志主要用来记录。

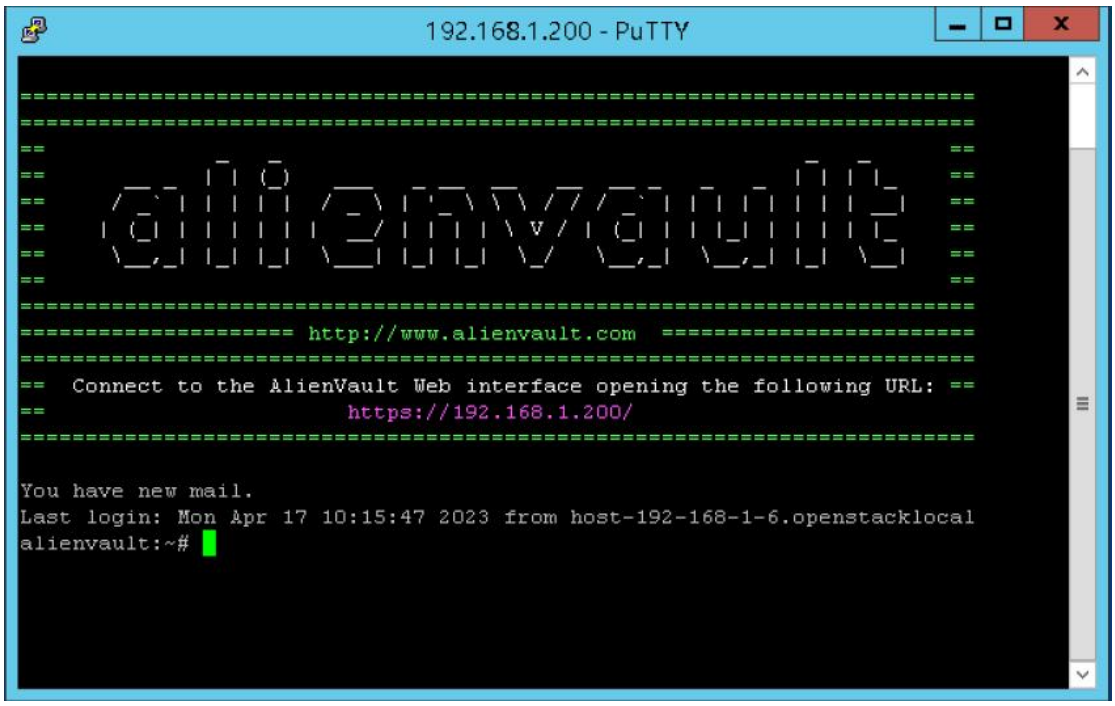
可以查看到日志。中相关配置信息。

这里使用的日志访问处理模式为 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。

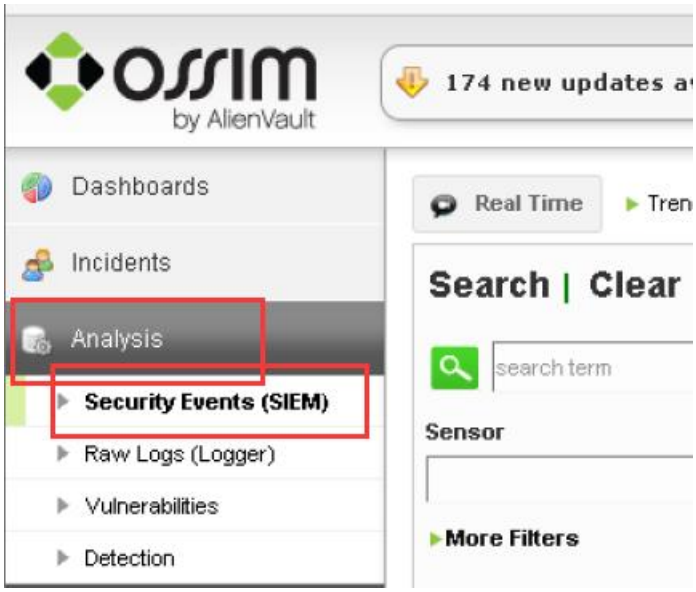
使用命令/var/ossec/bin/ossec-control restart 重启 OSSIM 服务器。

```
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-agentlessd not running ..
OSSEC HIDS v2.5.1 Stopped
Starting OSSEC HIDS v2.5.1 (by Trend Micro Inc.)...
2023/04/17 11:10:43 ossec-testrule: INFO: Reading local decoder file.
Started ossec-agentlessd...
2023/04/17 11:10:43 ossec-maild: INFO: E-Mail notification disabled. Clean E
xit.
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
```

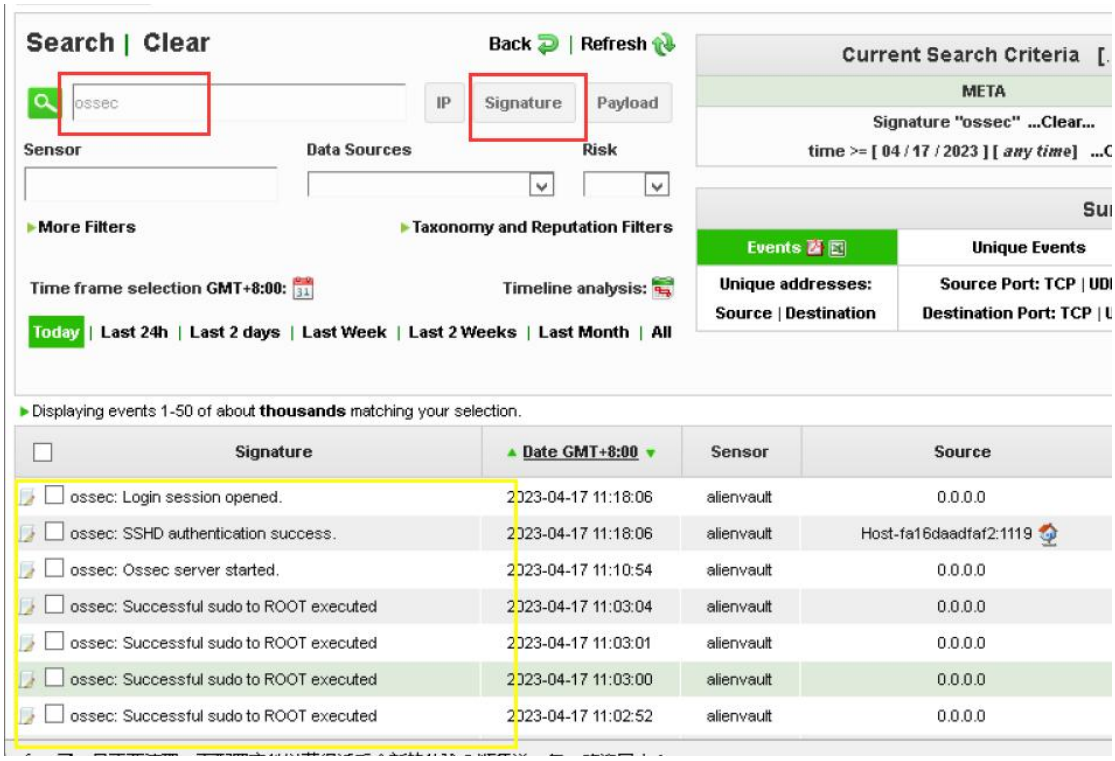
在 Windows 上使用 Putty 登录到服务器。



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安全日志信息。



在搜索框输入 ossec 过滤出 ossec 报警数据。因为 OSSEC 入侵检测系统监控了 /var/log/auth.log 文件，所以在 OSSIM 集成检测平台的 OSSIM Web 页面，除了记录 SSH 远程登录的相关安全日志信息，还会记录 OSSEC 报警信息，该报警信息可作为判断本次远程登录是否为非法入侵的重要依据



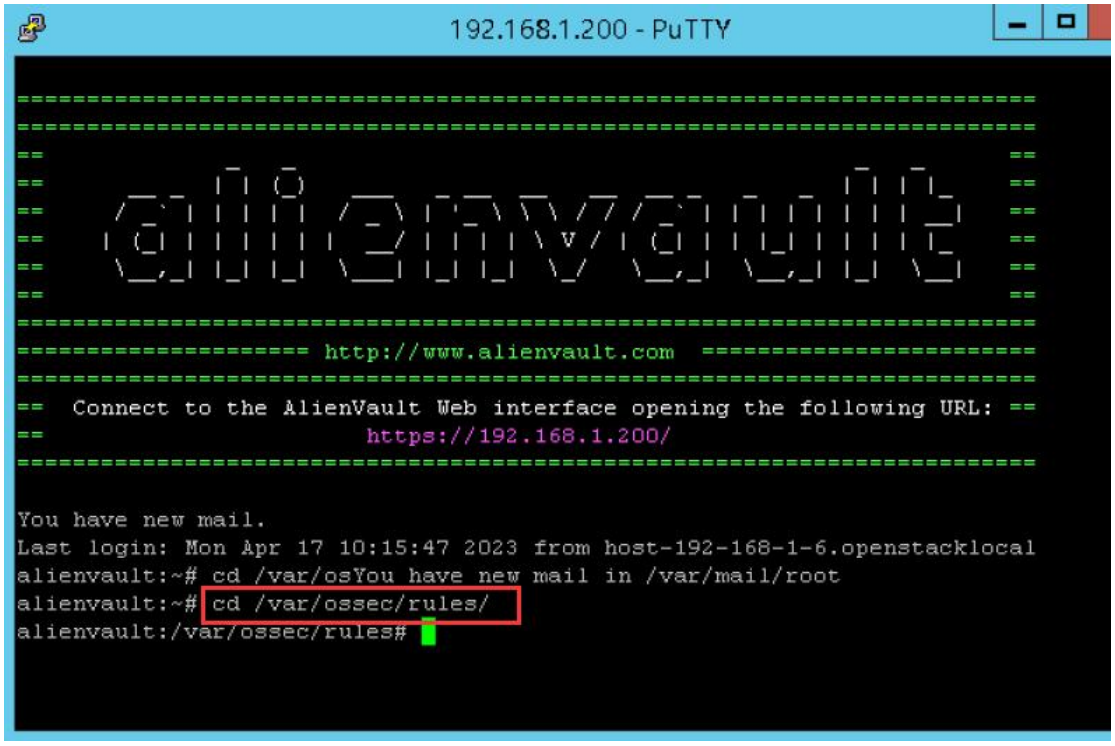
此外还可以看到本地 root 用户成功登录 OSSIM 服务器系统的日志信息。如果 root 用户的合法管理员没有在这个时间本地登录 OSSIM 服务器，那么可以断定，本次 root 用户登录操作为入侵行为可以看到身份验证成功信息如下图所示，其签名为

ossec:SSHD authentication success

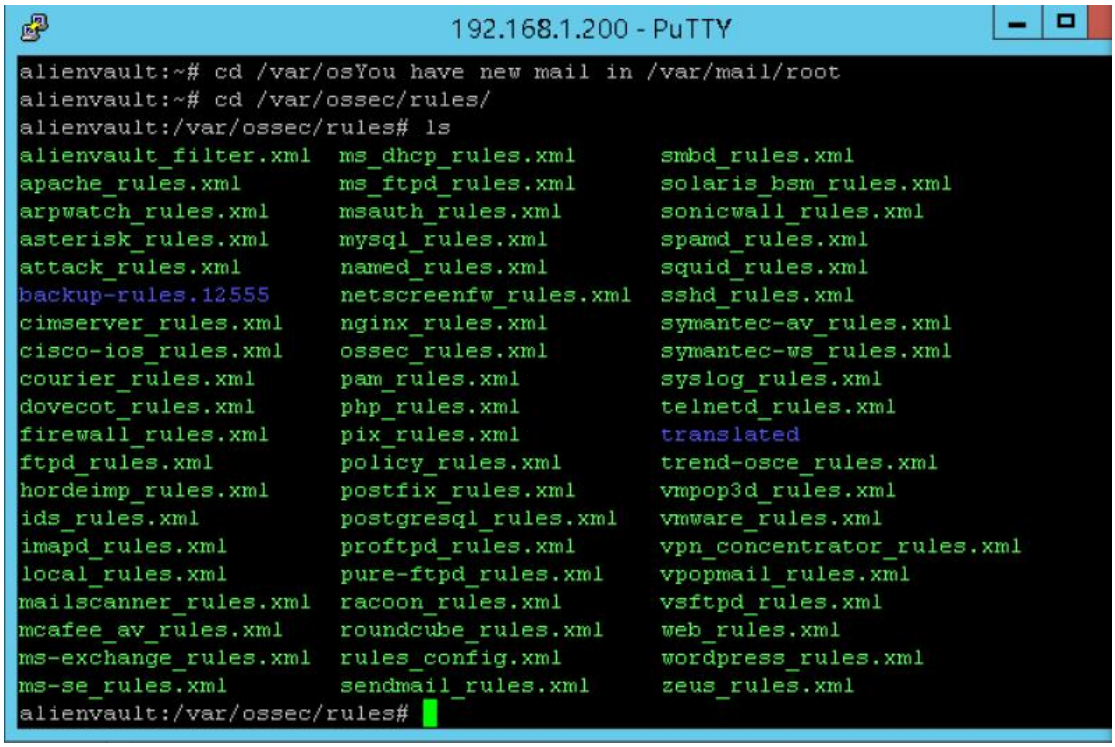
Signature	Date GMT+8:00	Sensor	Source
ossec: Login session opened.	2023-04-17 11:18:06	alienvault	0.0.0.0
ossec: SSHD authentication success.	2023-04-17 11:18:06	alienvault	Host-fa16daadfaf2:1119
ossec: Ossec server started.	2023-04-17 11:10:54	alienvault	0.0.0.0
ossec: Successful sudo to ROOT executed	2023-04-17 11:03:04	alienvault	0.0.0.0
ossec: Successful sudo to ROOT executed	2023-04-17 11:03:01	alienvault	0.0.0.0
ossec: Successful sudo to ROOT executed	2023-04-17 11:03:00	alienvault	0.0.0.0
ossec: Successful sudo to ROOT executed	2023-04-17 11:02:52	alienvault	0.0.0.0

3. 基于 SSH 的远程非法入侵检测

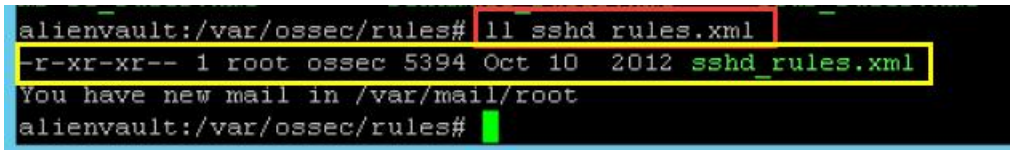
使用命令 cd /var/ossec/rules 进入规则文件夹。



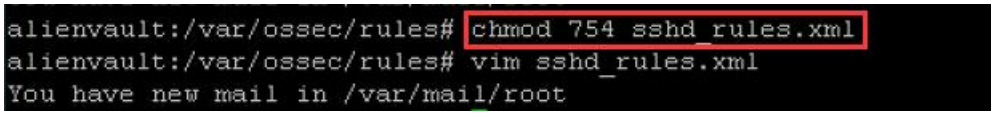
使用 ls 命令查看配置文件。可以修改这些文件的预设规则配置，来实现用户需要的自定义系统安全检测规则。其中，sshd_rules.xml 为我们本实验任务需要自定义检测规则的文件，通过自定义规则，以实现收集 root 用户远程非法登录 OSSIM 服务器的报警信息的目的，为判定、分析入侵行为和动机提供重要依据。



查看 sshd_rules.xml 文件权限，发现不具有写权限。



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：

将 level 级别设置为 2（level 级别越高，优先级就越高，与该规则对应的报警信息将更优先被 OSSIM 服务器响应和处理），告警阈值设置为 2 次。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。

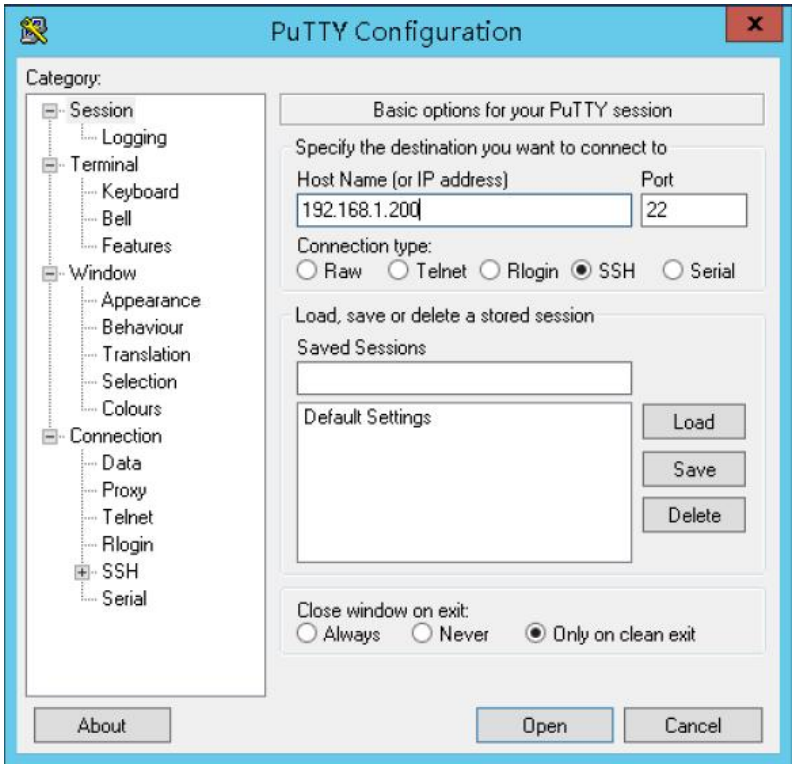
```
    <group>invalid_login,</group>
  </rule>

  <rule id="5719" level="2" frequency="6" timeframe="120" ignore="60">
    <if_matched_sid>5716</if_matched_sid>
    <description>Multiple access attempts using a denied user.</description>
  </rule>

  <rule id="5720" level="10" frequency="6">
    <if_matched_sid>5716</if_matched_sid>
-- INSERT --                                                    142,36        94%
```

重启 OSSEC 服务器，使配置文件生效。

使用命令/var/ossec/bin/ossec-control restart。

```
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-agentlessd not running ..
OSSEC HIDS v2.5.1 Stopped
Starting OSSEC HIDS v2.5.1 (by Trend Micro Inc.)...
2023/04/17 14:44:22 ossec-testrule: INFO: Reading local decoder file.
Started ossec-agentlessd...
2023/04/17 14:44:22 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.
```

再次登录 Putty。



登陆后多次输错密码并发出警报。
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。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。

Signature	Date GMT+8:00	Sensor
ossec: User missed the password more than one time	2023-04-17 14:46:12	alienvault
ossec: SSHD authentication failed.	2023-04-17 14:46:11	alienvault
ossec: SSHD authentication failed.	2023-04-17 14:46:06	alienvault
ossec: SSHD authentication failed.	2023-04-17 14:46:02	alienvault
ossec: SSHD authentication failed.	2023-04-17 14:45:57	alienvault
ossec: SSHD authentication failed.	2023-04-17 14:45:51	alienvault
ossec: SSHD authentication failed.	2023-04-17 14:45:45	alienvault
ossec: User login failed.	2023-04-17 14:45:43	alienvault
ossec: Login session closed.	2023-04-17 14:45:06	alienvault

4. 监视 CentOS7 root 用户情况

使用命令 cat /var/ossec/etc/ossec.conf | grep “var/log/secure”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。

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

自行添加文件监控内容。

```
alienvault:/var/ossec/bin# vim /var/ossec/etc/ossec.conf
```

添加文件内容为如下。

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>

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

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

再次检查发现已经被成功添加。

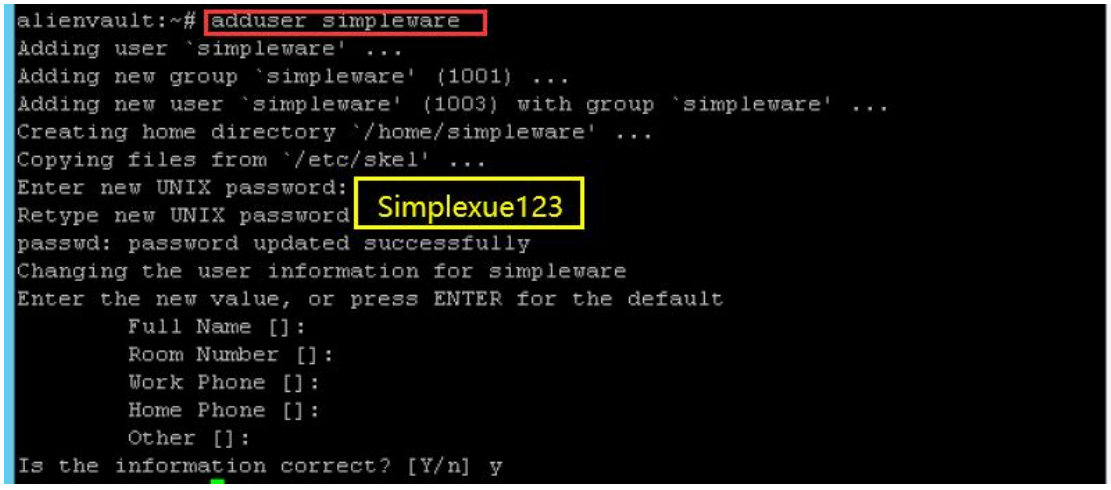
```
alienvault:/var/ossec/bin# cat /var/ossec/etc/ossec.conf | grep "/var/log/secure"
    <location>/var/log/secure</location>
alienvault:/var/ossec/bin#
```

使用命令/var/ossec/bin/ossec-control restart 重启 OSSIM 服务器。

```
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-agentlessd not running ..
OSSEC HIDS v2.5.1 Stopped
Starting OSSEC HIDS v2.5.1 (by Trend Micro Inc.)...
2023/04/17 15:02:03 ossec-testrule: INFO: Reading local decoder file.
Started ossec-agentlessd...
2023/04/17 15:02:03 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.
```

使用 Putty 登录远程服务器。

添加新用户。使用命令 adduser simpleware。密码设为 Simplexue123。



在 OSSIM web 页面上查看报警信息。

Signature	Date GMT+8:00	Sensor
ossec: Integrity checksum changed again (2nd time).	2023-04-17 15:06:16	alienvault
ossec: Integrity checksum changed again (3rd time).	2023-04-17 15:06:00	alienvault
ossec: Integrity checksum changed again (2nd time).	2023-04-17 15:05:44	alienvault
ossec: Information from the user was changed	2023-04-17 15:05:39	alienvault
ossec: New user added to the system	2023-04-17 15:05:11	alienvault
ossec: New group added to the system	2023-04-17 15:05:11	alienvault
ossec: Login session opened.	2023-04-17 15:04:10	alienvault
ossec: SSHD authentication success.	2023-04-17 15:04:10	alienvault
ossec: Ossec server started.	2023-04-17 15:02:14	alienvault

5. 监控 Web 服务器的访问日志

在 CentOS7 的终端修改 ossec.conf 文件。

```
alienvault:/var/ossec/bin# vim /var/ossec/etc/ossec.conf
```

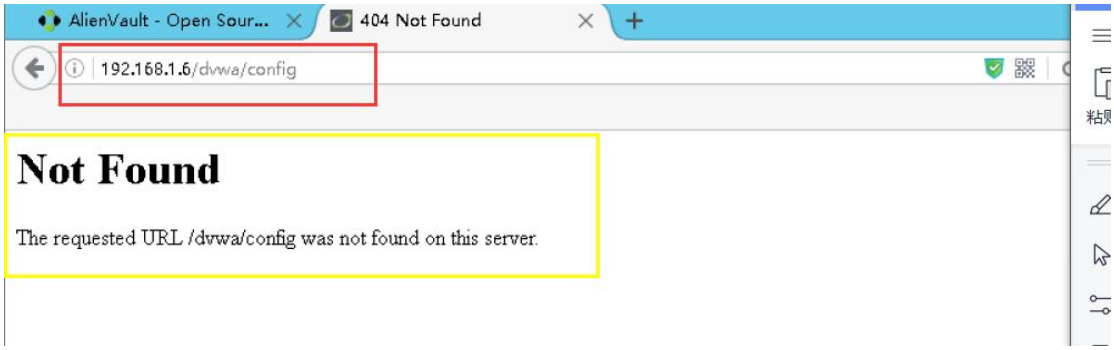
向该文件中添加如下内容，实现监控 Web 服务器的访问日志的功能。编辑完后按 esc 键退出文件编辑状态，并输入:wq 命令保存文件。

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/httpd/access_log</location>
</localfile>
```

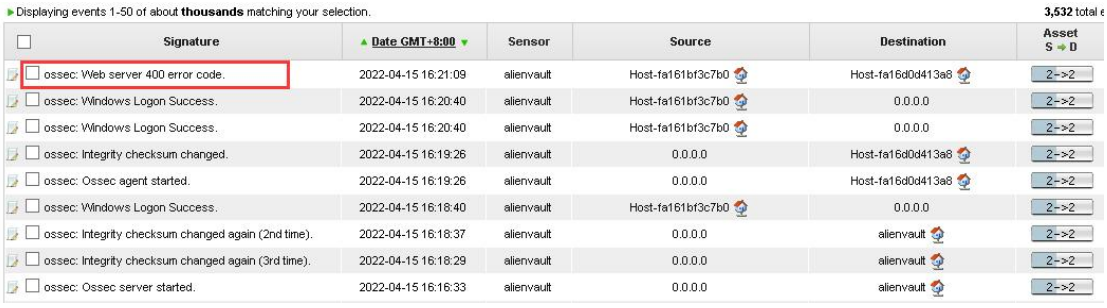
使用命令/var/ossec/bin/ossec-control restart 重启 OSSEC 服务。

```
[root@localhost bin]# vim /var/ossec/etc/ossec.conf
[root@localhost bin]# /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...
2022/04/15 16:19:25 ossec-agentd: INFO: Using notify time: 600 and max time to reconnect: 1800
Started ossec-agentd...
2022/04/15 16:19:25 ossec-logcollector(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/age
t.conf': XMLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 91).
Started ossec-logcollector...
2022/04/15 16:19:25 ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.
onf': XMLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 91).
2022/04/15 16:19:25 ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.
onf': XMLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 91).
Started ossec-syscheckd...
Completed.
```

在 Windows 上访问被禁止的网址 192.168.1.6/dvwa/config。提示信息为 Not Found。



在 OSSIM web 中查看报警信息如下。签名为 ossec:Web server 400 error code。



Displaying events 1-50 of about **thousands** matching your selection. 3,532 total e

Signature	Date GMT+8:00	Sensor	Source	Destination	Asset S → D
ossec: Web server 400 error code.	2022-04-15 16:21:09	alienvault	Host-fa161bf3c7b0	Host-fa16d0d413a8	2->2
ossec: Windows Logon Success.	2022-04-15 16:20:40	alienvault	Host-fa161bf3c7b0	0.0.0.0	2->2
ossec: Windows Logon Success.	2022-04-15 16:20:40	alienvault	Host-fa161bf3c7b0	0.0.0.0	2->2
ossec: Integrity checksum changed.	2022-04-15 16:19:26	alienvault	0.0.0.0	Host-fa16d0d413a8	2->2
ossec: Ossec agent started.	2022-04-15 16:19:26	alienvault	0.0.0.0	Host-fa16d0d413a8	2->2
ossec: Windows Logon Success.	2022-04-15 16:18:40	alienvault	Host-fa161bf3c7b0	0.0.0.0	2->2
ossec: Integrity checksum changed again (2nd time).	2022-04-15 16:18:37	alienvault	0.0.0.0	alienvault	2->2
ossec: Integrity checksum changed again (3rd time).	2022-04-15 16:18:29	alienvault	0.0.0.0	alienvault	2->2
ossec: Ossec server started.	2022-04-15 16:16:33	alienvault	0.0.0.0	alienvault	2->2

四、实验总结

本次实验我使用了两个实验环境。在使用 CentoOS7 时,我学习使用了 Xshell，一个好用的工具进行远程连接，直接解决了密钥无法复制的问题，以及有时候卡顿的问题，操作快捷简单。在实验内容上，我学习使用了工具 OSSIM，OSSEC，Putty，掌握了在不同的操作系统环境下安装和配置 OSSEC 代理，远程连接机器，了解 OSSEC 入侵检测系统的架构，功能及实现方式，根据报警信息做入侵行为分析。对入侵检测有了基本的了解，并通过实践的方式使用系统和工具检测入侵。