

武汉大学国家网络安全学院

实 验 报 告

课 程 名 称: 网络安全实验

实 验 名 称: 入侵检测实验

指 导 老 师:

学 生 学 号:

学 生 姓 名:

完 成 日 期: 2022.04.18

【实验描述】

入侵检测被认为是防火墙之后的第二道安全闸门,入侵检测系统能使在入侵攻击对系统发生危害前,检测到入侵攻击,并利用报警与防护系统驱逐入侵攻击,在不影响网络性能的情况下能对网络进行监听,从而提供对内部攻击、外部攻击和误操作的实时保护,大大提高了网络的安全性。

入侵检测实验通过企业复杂网络环境的入侵检测操作实战,要求学生深刻理解入侵检测的概念、原理,进而熟悉入侵检测系统的功能,掌握常用的入侵检测技术和方法,最终具备娴熟的入侵检测能力和信息安全管理职业能力,能够胜任政府、金融、电商等企事业单位的信息安全系统设计、研究、管理等工作,并为国家网络空间安全事业做出应有的贡献。

本实验内容共包含 5 个子任务, 分别是:

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;

任务二 监视 OSSIM 服务器本地 root 用户的登录情况;

任务三 基于 SSH 的远程非法入侵检测;

任务四 监视 CentOS7 root 用户情况;

任务五 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

【实验工具】

OSSIM

OSSEC

Putty

Firefox

【实验步骤】

任务一

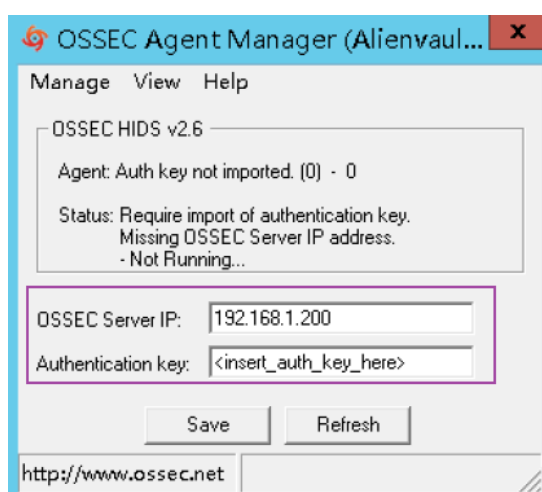
1.1 安装 OSSEC HIDS Windows Agent 工具软件

在 Windows 2012 上，安装 OSSEC 代理软件。OSSEC 安装成功后，将出现如图所示的安装成功提示窗口。单击该窗口的“Finish”按钮，关闭该窗口，即可完成 OSSEC 安装过程。



OSSEC 服务器安装于 OSSIM 系统中，且 OSSEC 服务器 IP 为 192.168.1.200，

而 Authentication key 为服务器产生的密钥，由 OSSIM 系统生成。



1.2 在 Windows 平台下安装和配置 OSSEC 代理

在 windows2012 操作系统中，使用 putty 远程登录 IP 地址为 192.168.1.200 的 OSSIM 服务器，OSSIM 服务器的用户名是 root，密码是 Simplexue123。



在 windows2012 上，使用 putty 终端启动 OSSEC 代理管理程序，创建新 OSSEC 代理，其中名称是 windows2012，代理 IP 是 192.168.1.5，即主机 Windows 2012 的 IP 地址，ID 是 005。

```
cd /var/ossec/bin
```

```
./manage_agents
```

```

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: 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.

```

然后在管理代理程序 `manage_agents` 中选择生成密钥操作，从而得到密钥。

```

*****
* 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: E

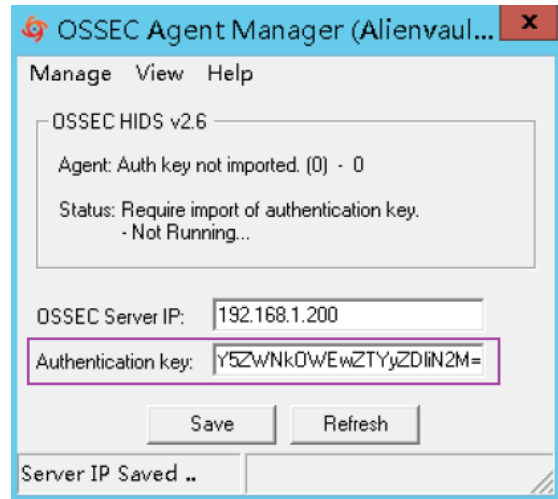
Available agents:
  ID: 001, Name: alienvault, IP: 192.168.1.200
  ID: 002, Name: windows7, IP: 192.168.1.2
  ID: 003, Name: CentOS6.5, IP: 192.168.1.4
  ID: 004, Name: windows2003, IP: 192.168.1.3
  ID: 005, Name: windows2012, IP: 192.168.1.5

Provide the ID of the agent to extract the key (or '\q' to quit): 005

Agent key information for '005' is:
MDA1IHdpbmRvd3MyMDEyIDE5Mi4xNjguMS41IDc5ZD1hM2I1NzczYmI3NGUwOWJhMDNkNzI3OGU2MjUxYjc2YmQzMjYxOGEwZlZWM3MTY5ZW5kOWEwZTYyZD1iN2M=

```

在 OSSEC AGENT 管理器窗口 Authentication key 栏里输入生成的密钥并保存。



启动新建的 OSSEC 代理，查看该代理成功运行后的运行状态信息。执行带 `-lc` 参数的 `agent_control` 程序可以列出正在运行的代理的状态信息。可以发现 windows2012 代理已经成功启动。

```
cd /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
```

1.3 在 Linux 平台下安装和配置 OSSEC 代理

登录 CentOS7 虚拟机，用户名是 root，密码是 Simplexue123。然后通过 CentOS7 使用 SSH 远程登录到 IP 地址为 192.168.1.200 的 OSSIM 服务器。

```

=====
=====
==
==
==
==
==
==
==
=====
===== http://www.alienvault.com =====
=====
== Connect to the AlienVault Web interface opening the following URL: ==
== https://192.168.1.200/ =====
=====

You have new mail.
Last login: Mon Apr 11 18:34:34 2022 from host-192-168-1-5.openstacklocal
alienvault:~# █

```

在远程登录的 192.168.1.200 终端打开 OSSEC 代理管理器程序，新建一个代理，将代理名称设为 CentOS7，代理 IP 为 192.168.1.6。操作步骤与添加 windows2012 代理时类似。

```
cd /var/ossec/bin
```

```
./manage_agents
```

```
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.

```

然后生成密钥。

```

*****
* 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: 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:
MDA2IENlbnRPUzcgMTkyLjE2OC4xLjYgMjI0YTc5YjdmOWUwMjI3ODlhYmFLMjRlNWYwOTFhZDllyZU0MWZlMzczOTBkNjFmNjI3ZDZmMjBmNDZmYjRjMg==

```

在 CentOS7 上的 manage_agents 代理管理程序中添加密钥。

```
cd /var/ossec/bin
```

```
./manage_agents
```

```
[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

* 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): MDA2IENlbnRPUzcgMTkyLjE2OC4xLjYgMjI0YTc5YjdmOWUwMjI3ODlhYmFLMjRlNWYwOTFhZDllyZU0MWZlMzczOTBkNjFmNjI3ZDZmMjBmNDZmYjRjMg==

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

Confirm adding it?(y/n): y
Added.

```

使用如下命令查看 ossec.conf 配置文件，配置文件中已包含服务器 IP 地址。

```
cat /var/ossec/etc/ossec.conf
```

```

[root@localhost bin]# cat /var/ossec/etc/ossec.conf
<ossec_config>
  <client>
    <server-ip>192.168.1.200</server-ip>
  </client>

```

使用如下命令重新启动 OSSEC 服务。


```
cd /var/ossec/bin
```

```
./ossec-control restart
```

```
[root@localhost 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...
2022/04/11 19:29:20 ossec-agentd: INFO: Using notify time: 600 and max time to reconnect: 1800
Started ossec-agentd...
2022/04/11 19:29:20 ossec-logcollector(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.conf'
: XMLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 84).
Started ossec-logcollector...
2022/04/11 19:29:20 ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.conf': X
MLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 84).
2022/04/11 19:29:20 ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.conf': X
MLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 84).
Started ossec-syscheckd...
Completed.
```

然后在服务器端查看 OSSEC 服务运行状态。

```
cd /var/ossec/bin
```

```
./agent_control -lc
```

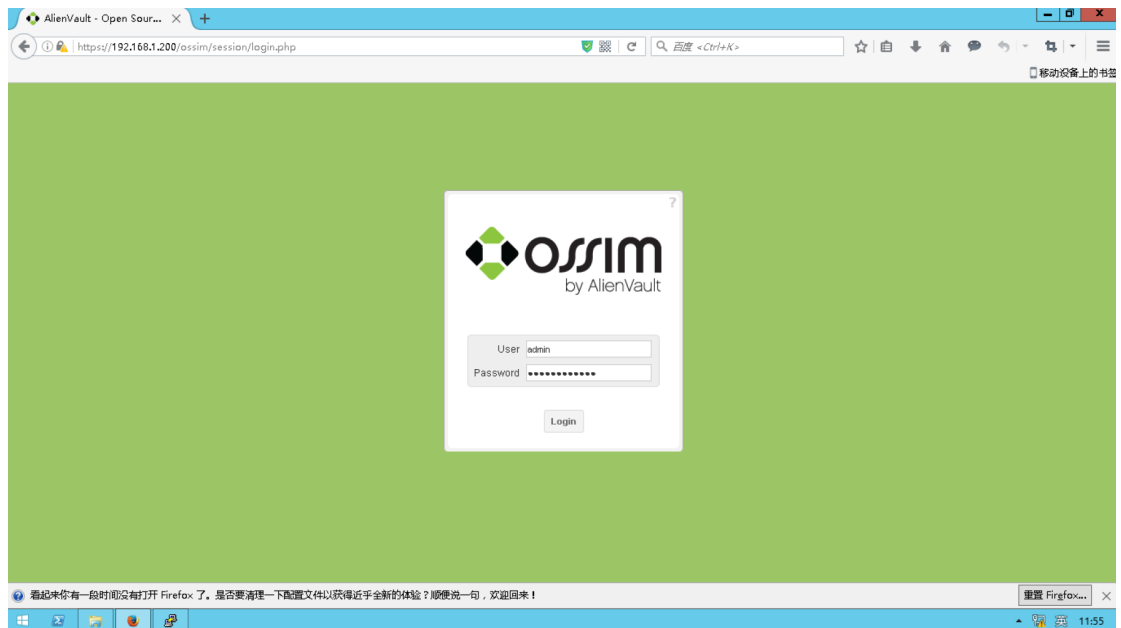
```
alienvault:/var/ossec/bin# ./agent_control -lc
```

```
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
```

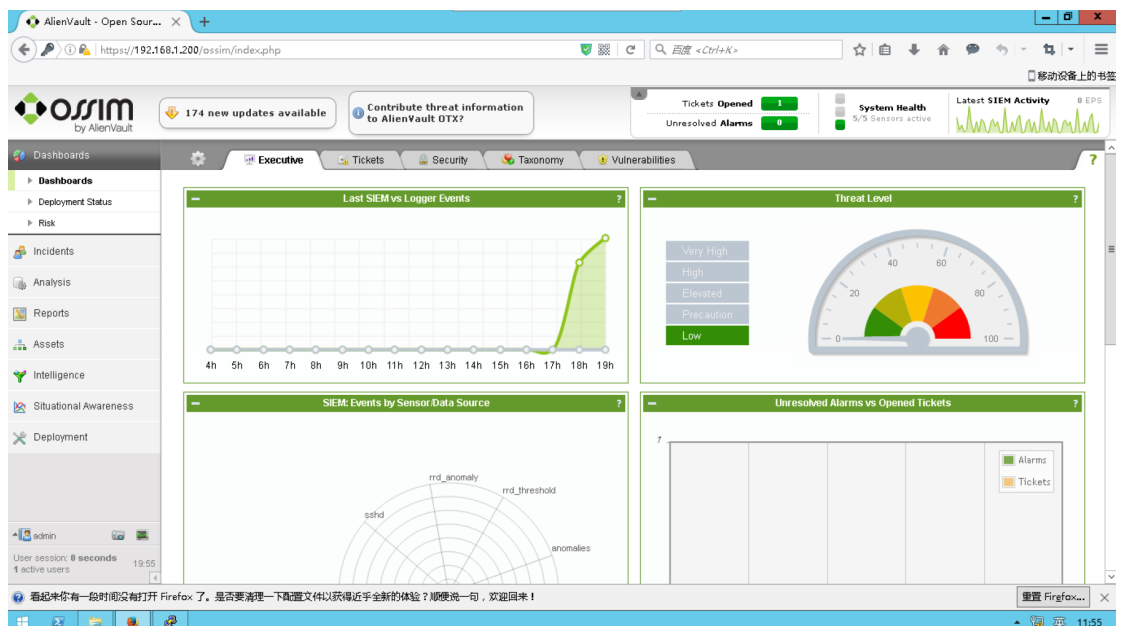
任务二

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

OSSIM 平台登录界面 URL 为 <https://192.168.1.200/ossim/session/login.php>，除此之外直接输入 <https://192.168.1.200/>也会自动跳转至登录界面。

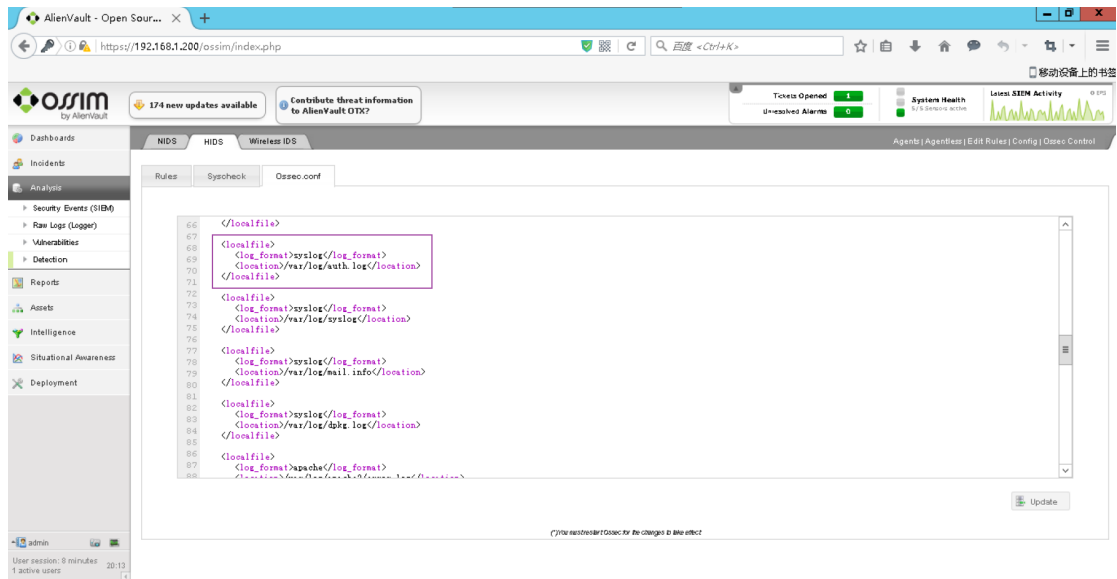


后台如图所示。



2.2 查看 ossec.conf 配置文件

在 OSSIM web 页面中，单击 Analysis---->Detection---->HIDS---->Config-->Ossec.conf，可以看到 OSSIM 集成检测平台已经默认监视了日志文件 /var/log/auth.log。



2.3 重启 OSSIM 服务器，并在命令行界面重新登录

使用如下命令重启 OSSIM 服务器。

```
cd /var/ossec/bin
```

```
./ossec-control restart
```

```
alienvault:/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.)...
2022/04/11 20:23:19 ossec-testrule: INFO: Reading local decoder file.
2022/04/11 20:23:19 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
```

实验步骤中的图形界面和命令行界面的切换登录是为了给 OSSEC 入侵检测系统提供 OSSIM 服务器的 root 用户本地登录检测信息源，以便 OSSEC 系统获取 root 用户本地登录的相关日志信息。

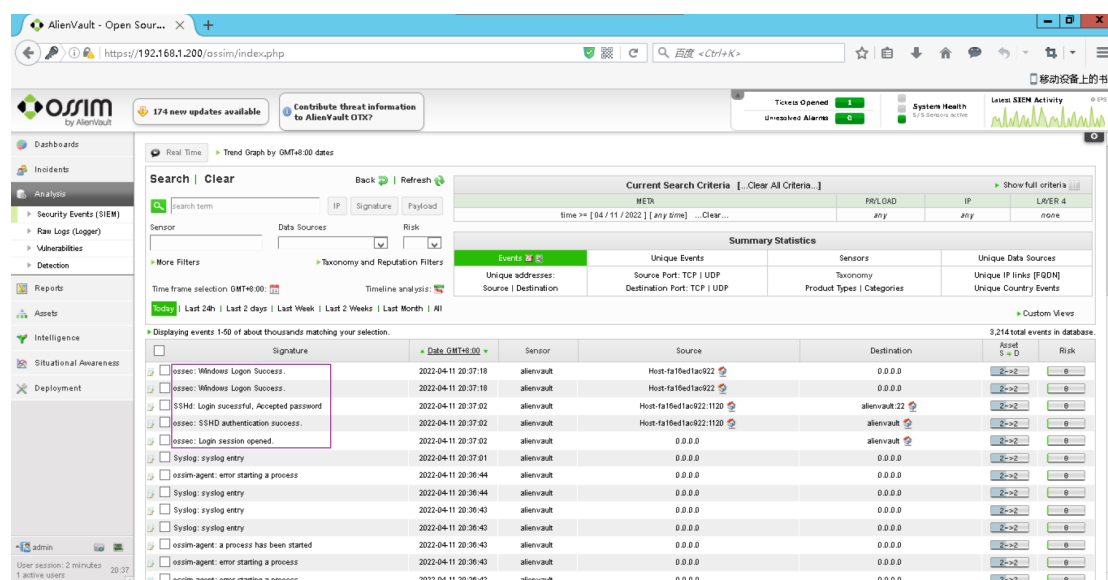
2.4 在 windows2012 上远程连接到服务器 192.168.1.200

在 Windows 2012 上使用 PuTTY 远程登录服务器 192.168.1.200。



2.5 查看安全事件日志信息

在 windows2012 的 OSSIM Web 页面上，单击 Analysis---> Security Events (SIEM)，可以看到，Security Events 页面中列出了 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，可以找到通过 putty 远程登录时相关的 SSH 登录记录报警信息。该日志信息可作为系统管理员判断本次远程登录是否为非法入侵的重要报警信息。如果 OSSIM 服务器不允许 root 用户的远程登录操作，那么 root 用户的本次远程登录操作将被视为黑客入侵行为。



2.6 数据过滤

在 OSSIM web 页面搜索框输入 ossec，回车进行 ossec 报警数据过滤。

Search | Clear

IP

Signature

Payload

Sensor

Data Sources

Risk

More Filters

Taxonomy and Reputation Filters

Time frame selection GMT+8:00

Timeline analysis

Today

Last 24h

Last 2 days

Last Week

Last 2 Weeks

Last Month

All

Current Search Criteria

Signature "ossec" ... Clear ...

time >= [04 / 11 / 2022] [any time] ... Clear ...

any

any

none

Summary Statistics

Events

Unique Events

Sensors

Unique Data Sources

Unique addresses: Source | Destination

Source Port: TCP | UDP

Destination Port: TCP | UDP

Taxonomy

Product Types | Categories

Unique IP links (FQDN)

Unique Country Events

Displaying events 1-50 of about thousands matching your selection.

3,306 total events in database.

Signature	Date GMT+8:00	Sensor	Source	Destination	Asset S = D	Risk
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:37:18	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:37:18	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0
<input type="checkbox"/> ossec: Login session opened.	2022-04-11 20:37:02	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: SSHD authentication success.	2022-04-11 20:37:02	allenvault	Host-fa16ed1ac922:1120	allenvault	2->2	0
<input type="checkbox"/> ossec: Login session closed.	2022-04-11 20:36:43	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:35:21	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0
<input type="checkbox"/> ossec: Login session opened.	2022-04-11 20:31:06	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: SSHD authentication success.	2022-04-11 20:31:06	allenvault	Host-fa16ed1ac922:1101	allenvault	2->2	0
<input type="checkbox"/> ossec: Login session closed.	2022-04-11 20:30:44	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: Ossec server started.	2022-04-11 20:23:30	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:21:17	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:21:17	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0

2.7 记录报警信息

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。

2.8 判断日志信息

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。将这次远程登录 OSSIM 服务器制造为入侵行为，如图所示，在这个时间上没有合法管理员的本地登录信息。

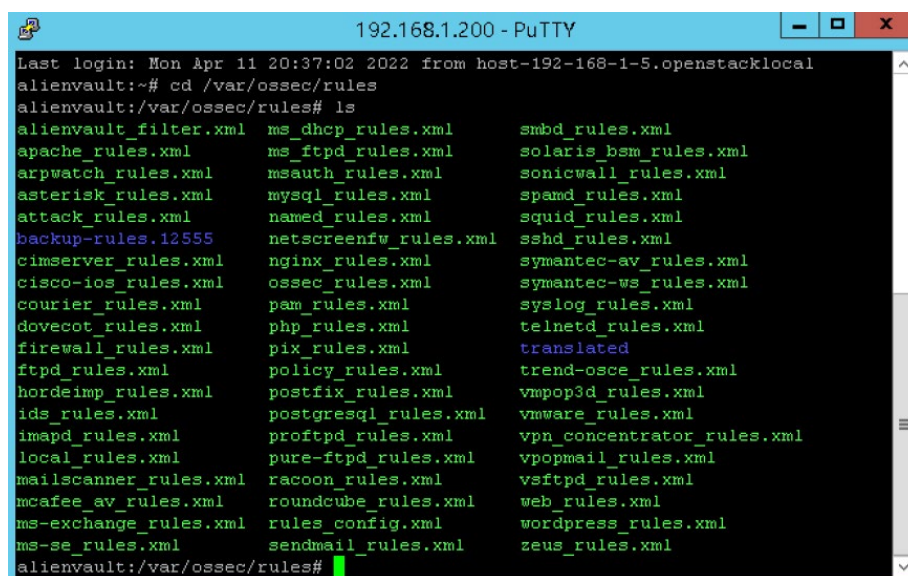
Signature	Date GMT+8:00	Sensor	Source	Destination	Asset S = D	Risk
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:37:18	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:37:18	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0
<input type="checkbox"/> ossec: Login session opened.	2022-04-11 20:37:02	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: SSHD authentication success.	2022-04-11 20:37:02	allenvault	Host-fa16ed1ac922:1120	allenvault	2->2	0
<input type="checkbox"/> ossec: Login session closed.	2022-04-11 20:36:43	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:35:21	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0
<input type="checkbox"/> ossec: Login session opened.	2022-04-11 20:31:06	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: SSHD authentication success.	2022-04-11 20:31:06	allenvault	Host-fa16ed1ac922:1101	allenvault	2->2	0
<input type="checkbox"/> ossec: Login session closed.	2022-04-11 20:30:44	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: Ossec server started.	2022-04-11 20:23:30	allenvault	0.0.0.0	allenvault	2->2	0
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:21:17	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0
<input type="checkbox"/> ossec: Windows Logon Success.	2022-04-11 20:21:17	allenvault	Host-fa16ed1ac922	0.0.0.0	2->2	0

任务三

3.1 使用 PuTTY 工具远程登录 OSSIM 服务器，并进入/var/ossec/rules 目录

使用 putty 工具远程登录 OSSIM 服务器，在打开的终端中，使用 CD 命令进

入“/var/ossec/rules”目录（该目录为 OSSEC 服务器的检测规则文件存储目录），并使用 ls 命令查看所有的 OSSEC 服务器端检测规则文件。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。

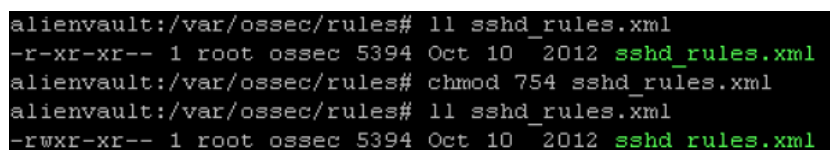


```
192.168.1.200 - PuTTY
Last login: Mon Apr 11 20:37:02 2022 from host-192-168-1-5.openstacklocal
alienvault:~# cd /var/ossec/rules
alienvault:/var/ossec/rules# ls
alienvault_filter.xml  ms_dhcp_rules.xml      smbd_rules.xml
apache_rules.xml      ms_ftp_rules.xml       solaris_bsm_rules.xml
arpwatch_rules.xml    msauth_rules.xml       sonicwall_rules.xml
asterisk_rules.xml    mysql_rules.xml        spamd_rules.xml
attack_rules.xml      named_rules.xml        squid_rules.xml
backup-rules.12555    netscreenfw_rules.xml  sshd_rules.xml
cimserver_rules.xml   nginx_rules.xml        symantec-av_rules.xml
cisco-ios_rules.xml   ossec_rules.xml        symantec-ws_rules.xml
courier_rules.xml     pam_rules.xml          syslog_rules.xml
dovecot_rules.xml     php_rules.xml          telnetd_rules.xml
firewall_rules.xml    pix_rules.xml          translated
ftpd_rules.xml        policy_rules.xml        trend-osce_rules.xml
hordeimp_rules.xml    postfix_rules.xml      vmfop3d_rules.xml
ids_rules.xml         postgresql_rules.xml    vmware_rules.xml
imapd_rules.xml       proftpd_rules.xml      vpn_concentrator_rules.xml
local_rules.xml       pure-ftp_rules.xml      vpopmail_rules.xml
mailscanner_rules.xml racoon_rules.xml        vsftpd_rules.xml
mcafee_av_rules.xml   roundcube_rules.xml    web_rules.xml
ms-exchange_rules.xml rules_config.xml        wordpress_rules.xml
ms-se_rules.xml       sendmail_rules.xml     zeus_rules.xml
alienvault:/var/ossec/rules#
```

3.2 修改 sshd_rules.xml 文件

为 sshd_rules.xml 文件添加 root 用户的写权限。

chmod 754 sshd_rules.xml



```
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# chmod 754 sshd_rules.xml
alienvault:/var/ossec/rules# ll sshd_rules.xml
-rwxr-xr-- 1 root ossec 5394 Oct 10 2012 sshd_rules.xml
```

修改 sshd_rules.xml 规则文件中的其中一条（rule id 号为 5719），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。

修改后 rule id 号为 5719 的规则如下图所示。

```
<rule id="5719" level="2" frequency="2" timeframe="30" ignore="60">
  <if_matched_sid>5718</if_matched_sid>
  <description>Multiple access attempts using a denied user.</description>
</rule>
```

3.3 重启 OSSEC 服务器

使用如下命令重新启动 ossec 服务器，以使 sshd_rules.xml 文件配置生效。

/var/ossec/bin/ossec-control restart

```
alienvault:/var/ossec/rules# /var/ossec/bin/ossec-control restart
Killing ossec-monitor ..
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.)...
2022/04/18 00:25:01 ossec-testrule: INFO: Reading local decoder file.
2022/04/18 00:25:01 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-monitor...
Completed.
You have new mail in /var/mail/root
```

3.4 尝试使用错误密码登录服务器

利用 ssh 尝试登录服务器，可以用任意错误密码尝试登录，注意至少尝试 2 次错误登录密码，操作时长 30 秒以后，才能触发自定义的报警规则。



3.5 在 ossim web 端查看报警信息

在 ossim web 端，输入 ossec 进行 ossec 报警信息筛选，可以看到 root 用户

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。

<input type="checkbox"/>	Signature	▲ Date GMT+8:00 ▼	Sensor	Source	Destination	Asset S e D	Risk
<input checked="" type="checkbox"/>	ossec: SSHD authentication failed.	2022-04-18 00:33:29	alienvaut	Host-fa16ed1ac922:1042	alienvaut	2->2	0
<input checked="" type="checkbox"/>	ossec: SSHD authentication failed.	2022-04-18 00:33:25	alienvaut	Host-fa16ed1ac922:1042	alienvaut	2->2	0
<input checked="" type="checkbox"/>	ossec: Multiple SSHD authentication failures.	2022-04-18 00:33:19	alienvaut	Host-fa16ed1ac922:1042	alienvaut	2->2	0
<input checked="" type="checkbox"/>	ossec: SSHD authentication failed.	2022-04-18 00:33:15	alienvaut	Host-fa16ed1ac922:1042	alienvaut	2->2	0
<input checked="" type="checkbox"/>	ossec: User login failed.	2022-04-18 00:33:13	alienvaut	Host-fa16ed1ac922	alienvaut	2->2	0

任务四

4.1 修改配置文件

在 OSSIM 集成检测平台上设置规则，监测 CentOS7 用户情况。在 CentOS7 终端查看代理的配置文件，可以看到 OSSIM 集成检测平台默认监控 /var/log/secure 文件。

cat /var/ossec/etc/ossec.conf

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

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

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

<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>netstat -tan |grep LISTEN |egrep -v '(127.0.0.1|::1)' | sort</command>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>last -n 5</command>
</localfile>
</ossec_config>
```

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


```

alienvault:~# /var/ossec/bin/ossec-control restart
Killing ossec-monitor ..
Killing ossec-logcollector ..
Killing ossec-remoted ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
ossec-mailed not running ..
ossec-execd not running ..
OSSEC HIDS v2.5.1 Stopped
Starting OSSEC HIDS v2.5.1 (by Trend Micro Inc.)...
2022/04/18 12:36:55 ossec-testrule: INFO: Reading local decoder file.
2022/04/18 12:36:55 ossec-mailed: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-mailed...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitor...
Completed.
You have new mail in /var/mail/root

```

4.3 使用工具模拟攻击者远程登录服务器

使用 Xshell 7 模拟攻击者远程登录服务器，用户名是 root，密码是 Simplexue123。

```

Xshell 7 (Build 0073)
Copyright (c) 2020 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
[C:\~]$

Connecting to 10.201.202.71:21083...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

Last login: Mon Apr 11 19:01:06 2022 from 10.201.83.126
ABRT has detected 1 problem(s). For more info run: abrt-cli list --since 1649674866
[root@localhost ~]#

```

4.4 添加新用户

使用如下命令在 192.168.1.200 服务器上添加新用户，密码设为 Simplexue123。

```
adduser simpleware
```

```
passwd simpleware
```

```

[root@localhost ~]# adduser simpleware
[root@localhost ~]# passwd simpleware
Changing password for user simpleware.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

```

4.5 在 OSSIM Web 页面上查看报警信息

在 OSSIM Web 页面上，进行 OSSEC 警报数据的过滤，可以看到与 CentOS7 添加新用户相关的 OSSEC 报警信息。

<input type="checkbox"/>	Signature	▲ Date GMT+8:00 ▼	Sensor	Source	Destination	Asset S = D	Risk
<input checked="" type="checkbox"/>	ossec: New user added to the system	2022-04-18 12:56:34	alienvaul	0.0.0.0	Host-fa16dedc13dc	2->2	0
<input checked="" type="checkbox"/>	ossec: New group added to the system	2022-04-18 12:56:34	alienvaul	0.0.0.0	192.168.1.6	2->2	0
<input checked="" type="checkbox"/>	ossec: Login session opened.	2022-04-18 12:56:15	alienvaul	0.0.0.0	Host-fa16dedc13dc	2->2	0
<input checked="" type="checkbox"/>	ossec: SSHD authentication success.	2022-04-18 12:56:15	alienvaul	10.201.118.79-25220	Host-fa16dedc13dc	2->2	0

4.6 获得报警信息的字段特征

在入侵检测系统中与 CentOS7 添加新用户相关的 OSSEC 报警信息的字段特征如下所示。

ossec:New user added to the system

ossec:New group added to the system

任务五

5.1 在 CentOS7 终端修改 ossec.conf 配置文件

在/var/ossec/etc/ossec.conf 配置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。

```
<localfile>
  <log_format>full_command</log_format>
  <command>netstat -tan |grep LISTEN |egrep -v '(127.0.0.1|:::1)' | sort</command>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>last -n 5</command>
</localfile>

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

5.2 重启 OSSEC 服务

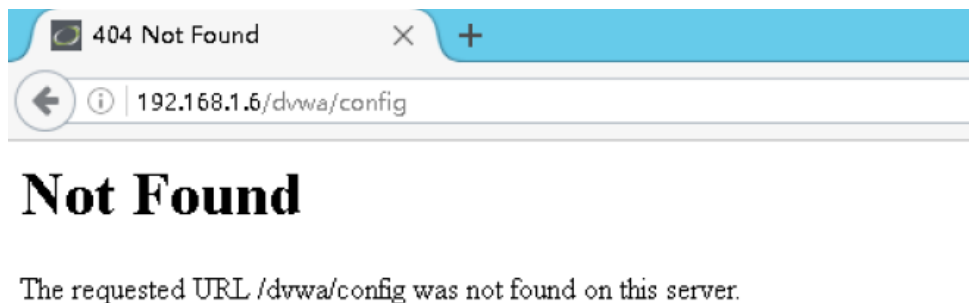
使用以下命令重新启动 OSSEC 服务。

/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...
2022/04/18 17:51:30 ossec-agentd: INFO: Using notify time: 600 and max time to reconnect: 1800
Started ossec-agentd...
2022/04/18 17:51:30 ossec-logcollector(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.conf'
: XMLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 89).
Started ossec-logcollector...
2022/04/18 17:51:30 ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.conf': X
MLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 89).
2022/04/18 17:51:30 ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.conf': X
MLERR: File '/var/ossec/etc/shared/agent.conf' not found. (line 89).
Started ossec-syscheckd...
Completed.
```

5.3 尝试访问被禁止访问的目录

在 windows2012 的火狐浏览器上访问 <http://192.168.1.6/dvwa/config>, 提示信息为 Not Found。



5.4 在 OSSIM Web 页面上查看报警信息

在 OSSIM Web 页面上, 进行 OSSEC 警报数据的过滤, 可以看到访问禁止目录时的报警信息。

<input type="checkbox"/>	Signature	Date GMT+8:00	Sensor	Source	Destination	Asset S = ID	Risk
<input type="checkbox"/>	ossec: Web server 400 error code.	2022-04-18 18:00:56	alienvault	Host-fa16ed1ac922	Host-fa16dedc13dc	2->2	0
<input type="checkbox"/>	ossec: Web server 400 error code.	2022-04-18 17:59:40	alienvault	Host-fa16ed1ac922	Host-fa16dedc13dc	2->2	0
<input type="checkbox"/>	ossec: Ossec server started.	2022-04-18 17:59:04	alienvault	0.0.0.0	alienvault	2->2	0
<input type="checkbox"/>	ossec: SSHD authentication success.	2022-04-18 17:57:44	alienvault	Host-fa16ed1ac922:1045	alienvault	2->2	0
<input type="checkbox"/>	ossec: Login session opened.	2022-04-18 17:57:44	alienvault	0.0.0.0	alienvault	2->2	0

【实验总结】