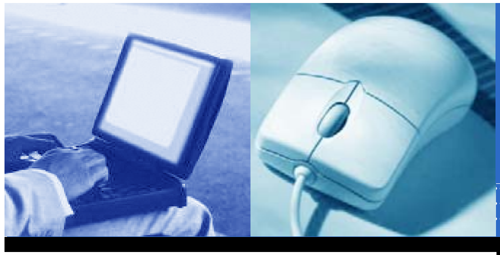
信息安全监控

人人网安全交流

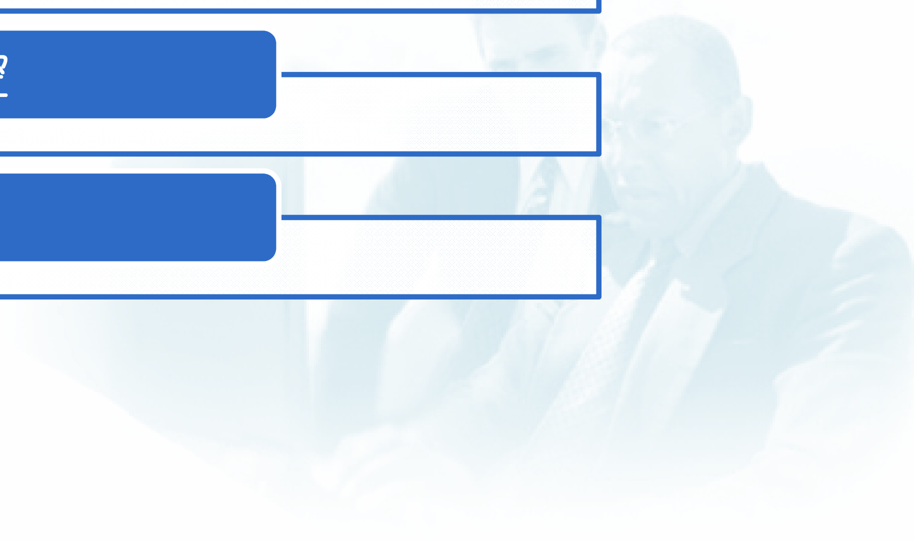
Cnbird@wanmei qQ:2010289

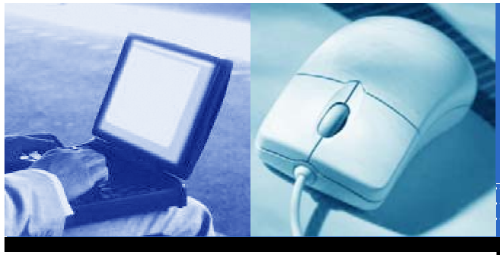
PERFECT WORLD



交流内容

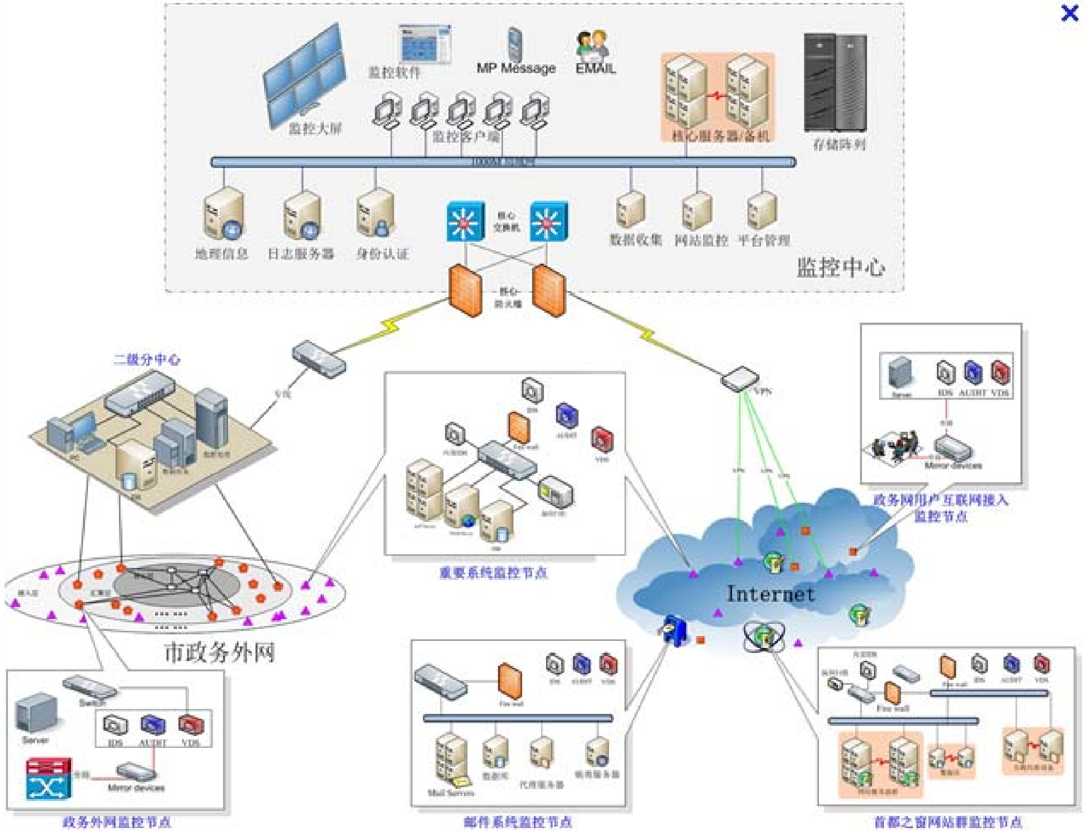
- 安全监控简介
- 文件系统监控
- 网络监控
- BASH监控
- Nagios实现高级安全监控
- OSSIM高级监控平台

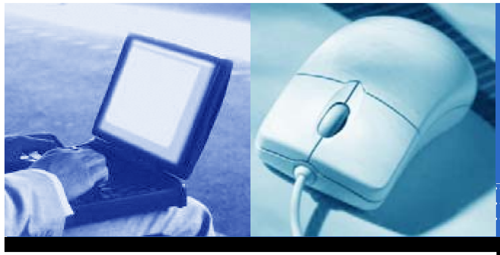




安全监控内容

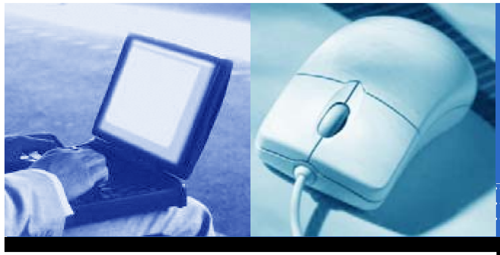
- 安全监控通过实时监控网络或主机活动，监视分析用户和系统的行为，审计系统配置和漏洞，评估敏感系统和数据的完整性，识别攻击行为，对异常行为进行统计和跟踪，识别违反安全法规的行为，使用诱骗服务器记录黑客行为等功能，使管理员有效地监视、控制和评估网络或主机系统。





文件系统监控原理

- 当文件系统监控程序运行在数据库生成模式时，会根据管理员设置的一个配置文件对指定要监控的文件进行读取，对每个文件生成相应数字签名，并将这些结果保存在自己的数据库中。除此以外，管理员还可使用MD5, MD4，CRC32，SHA等哈希函数。当怀疑系统被入侵时，可由根据先前生成的，数据库文件来做一次数字签名的对照，如果文件被替换，则与数据库内相应数字签名不匹配，这时会报告相应文件被更动，管理员会收到报警证明系统文件遭到篡改。



文件系统监控软件

- Tripwire

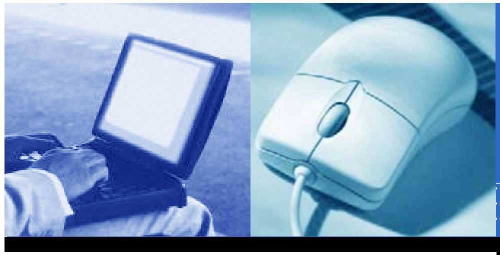
Download:http://sourceforge.net/projects/tripwire

- Aide

Download:http://aide.sourceforge.net/

- Ossec

Download:http://www.ossec.net/



文件系统监控软件实例

- Tripwire

1.源代码安装

2.rpm安装

```
rpm -ivh ftp://rpmfind.net/linux/epel/5/i386/tripwire-2.4.1.1-1.el5.i386.rpm
```

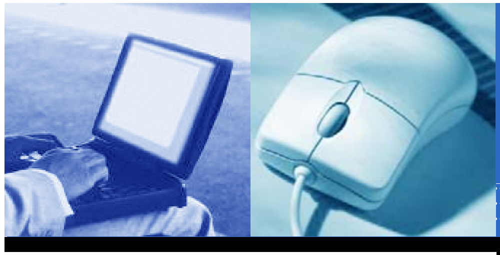
3.配置

3.1 编辑twcfg.txt修改配置

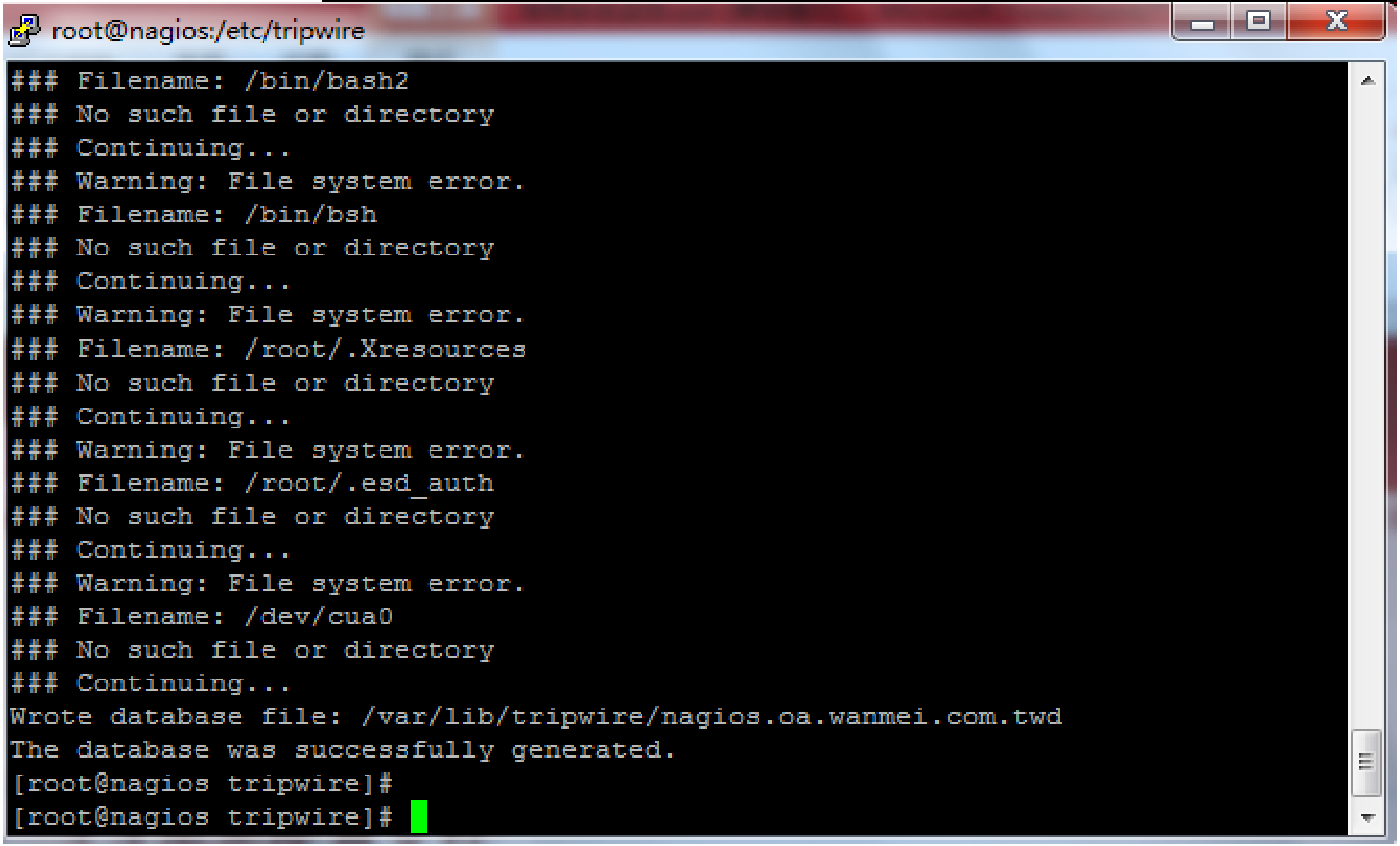
LOOSEDIRECTORYCHECKING=ture关闭监控所有的目录减少不必要的报警

3.2 生成key

```
twadmin --generate-keys --site-keyfile /etc/tripwire/site.key
twadmin --generate-keys --local-keyfile ./$HOSTNAME-local.key
```

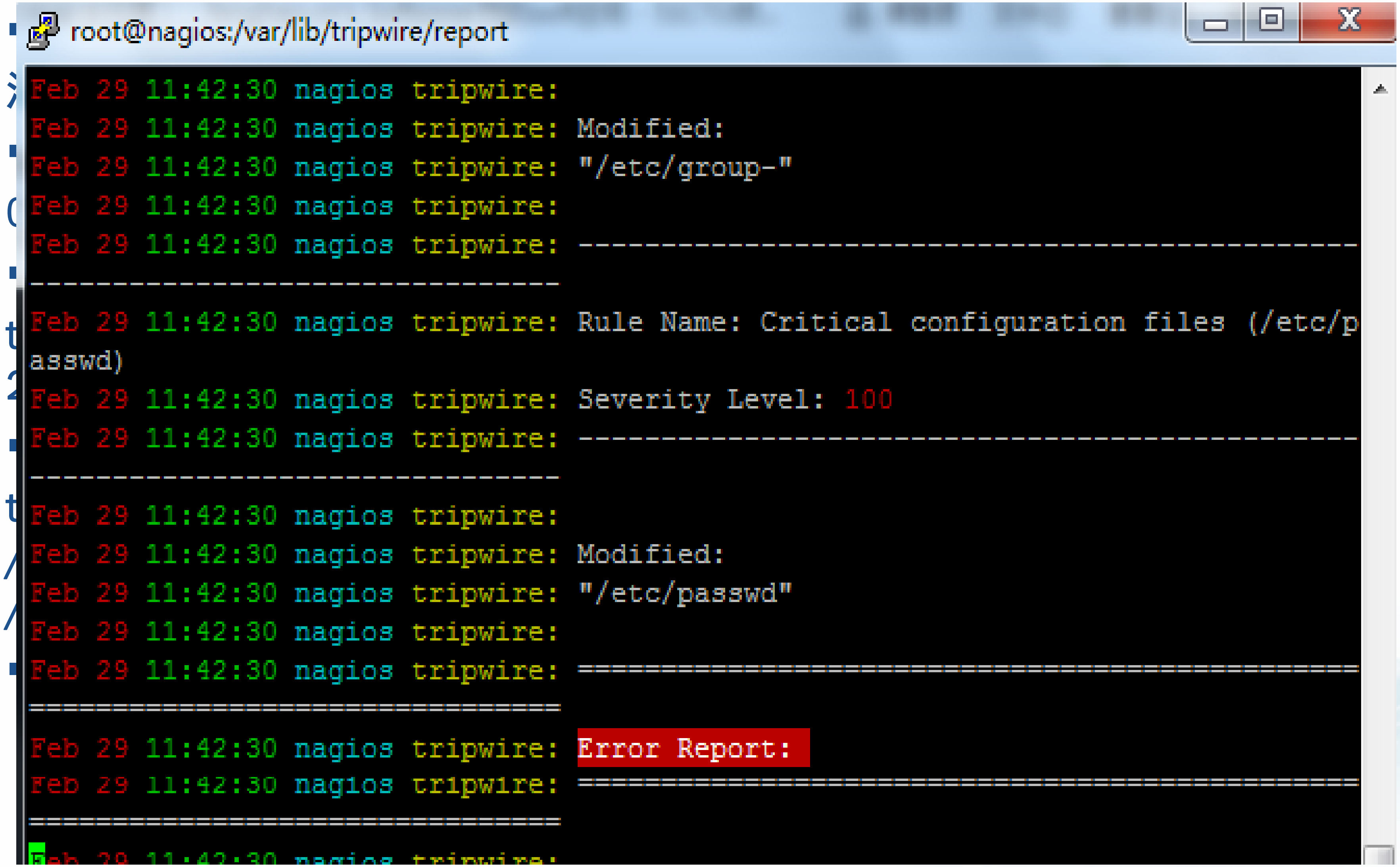


文件系统监控软件实例



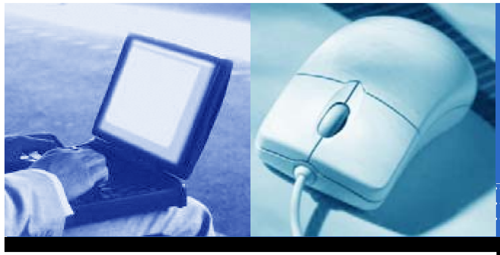
```
### Filename: /bin/bash2
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /bin/bsh
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.Xresources
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.esd_auth
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /dev/cua0
### No such file or directory
### Continuing...
Wrote database file: /var/lib/tripwire/nagios.oa.wanmei.com.twd
The database was successfully generated.
[root@nagios tripwire]#
[root@nagios tripwire]#
```

文件系统监控软件实例



root@nagios:/var/lib/tripwire/report

```
Feb 29 11:42:30 nagios tripwire:
Feb 29 11:42:30 nagios tripwire: Modified:
Feb 29 11:42:30 nagios tripwire: "/etc/group-"
Feb 29 11:42:30 nagios tripwire:
Feb 29 11:42:30 nagios tripwire: ------------------------------------------------
--------------------------------
Feb 29 11:42:30 nagios tripwire: Rule Name: Critical configuration files (/etc/p
asswd)
Feb 29 11:42:30 nagios tripwire: Severity Level: 100
Feb 29 11:42:30 nagios tripwire: ------------------------------------------------
--------------------------------
Feb 29 11:42:30 nagios tripwire:
Feb 29 11:42:30 nagios tripwire: Modified:
Feb 29 11:42:30 nagios tripwire: "/etc/passwd"
Feb 29 11:42:30 nagios tripwire:
Feb 29 11:42:30 nagios tripwire: ================================================
================================
Feb 29 11:42:30 nagios tripwire: Error Report:
Feb 29 11:42:30 nagios tripwire: ================================================
================================
Feb 29 11:42:30 nagios tripwire:
```



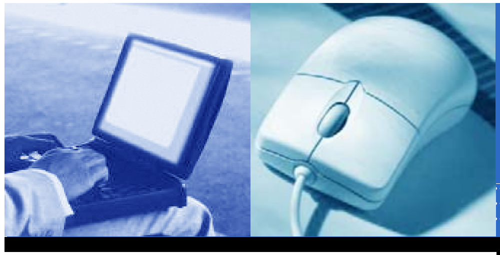
网络入侵检测监控

- Snort

Download:http://www.snort.org/

- Samhain

Download:http://la-samhna.de/samhain/



网络入侵检测实例(Snort构建属于自己的WAF)

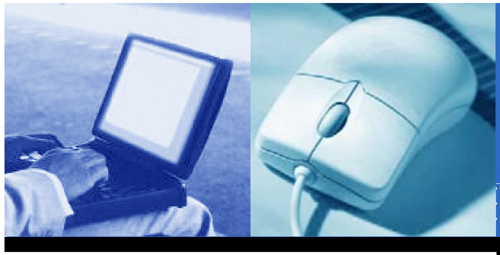
1. Snort规则简介:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-ATTACKS /bin/ps command attempt"; flow:to_server,established; uricontent:"/bin/ps"; nocase; classtype:web-application-attack; sid:1328; rev:6;)

2. 添加mod_security规则到snort(mod_security局限于apache,而snort可以全面检测各种web server)

(msg:"SQL Injection test"; flow:to_server,established;uricontent:“?";pcre:"/(\%27)|(\’)|(\-\-)|(%23)|(#)/i"; classtype:Web-application-attack; sid:9099; rev:5;)3. 我们可以自定义的WAF种类

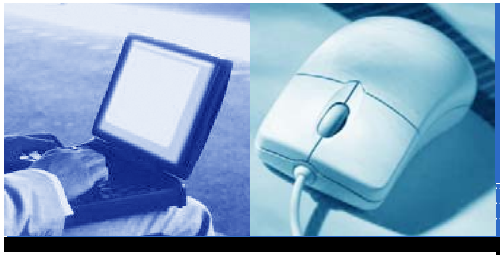
XSS,SQL INJECTION,暴力破解,请求协议检测,webshell,自动化扫描器,HPP(http参数污染攻击)等等你所有可以想到的



Bash安全监控

- 修改bash源代码进行bash记录

Microsoft Word
97 - 2003 文档



Nagios高级安全监控

- Nagios+aide

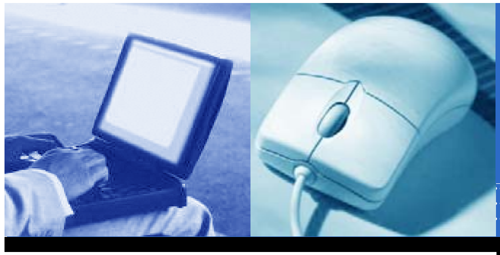
实现原理:使用aide来进行文件监控同时生成日志监控文件,我们可以使用nagios的脚本来读取aide的日志文件,提取出来感兴趣的字段然后通过nagios监控发送到报警平台。

- Nagios+snort

Download:https://www.monitoringexchange.org/inventory/Check-Plugins/Network/check_snort-

- Nagios+ossec

Download:http://kintoandar.blogspot.com/2011/01/nagios-nrpe-ossec-check.html



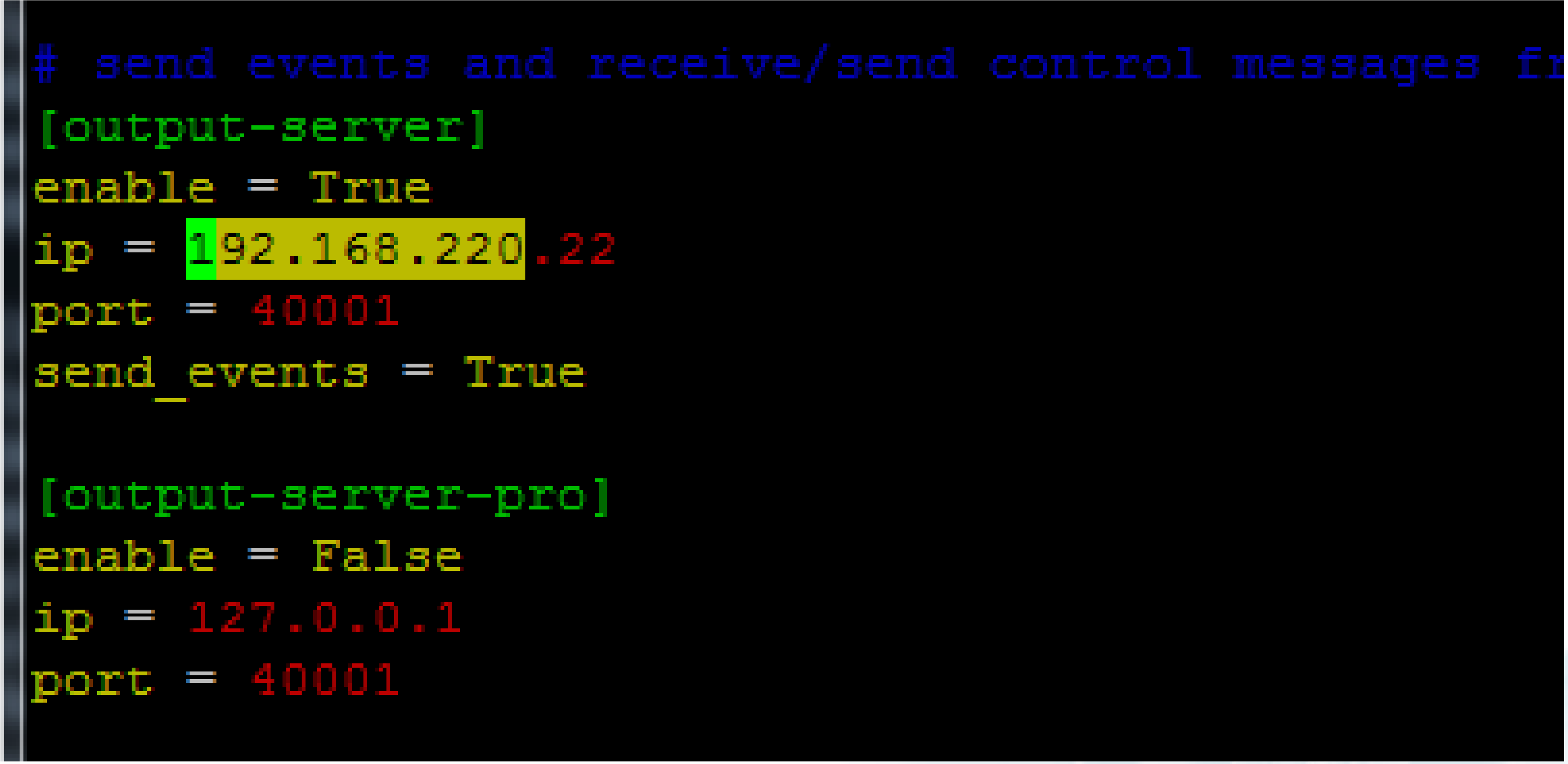
OSSIM高级安全监控平台

- OSSIM

OSSIM集成nagios,cacti,snort,nessus,ossim-agent,ossim-server

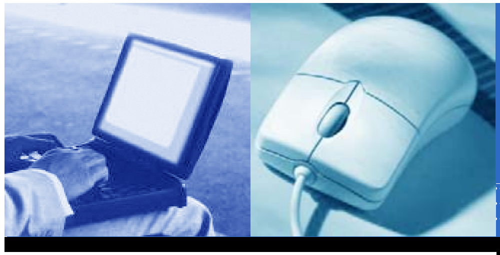
Download:http://communities.alienvault.com/community

1. 安装ossim-agent

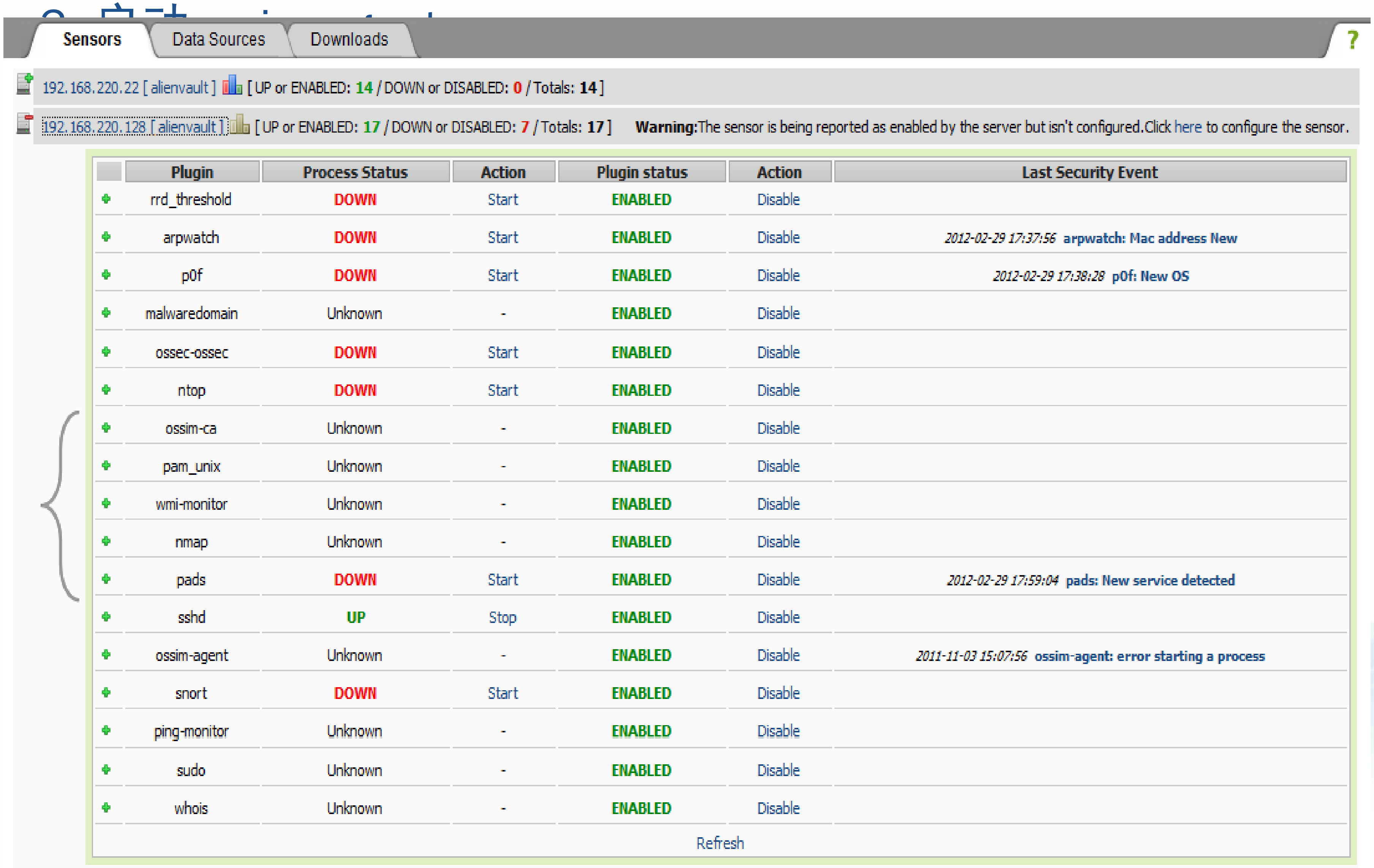


```
# send events and receive/send control messages fr
[output-server]
enable = True
ip = 192.168.220.22
port = 40001
send_events = True

[output-server-pro]
enable = False
ip = 127.0.0.1
port = 40001
```



OSSIM高级安全实践



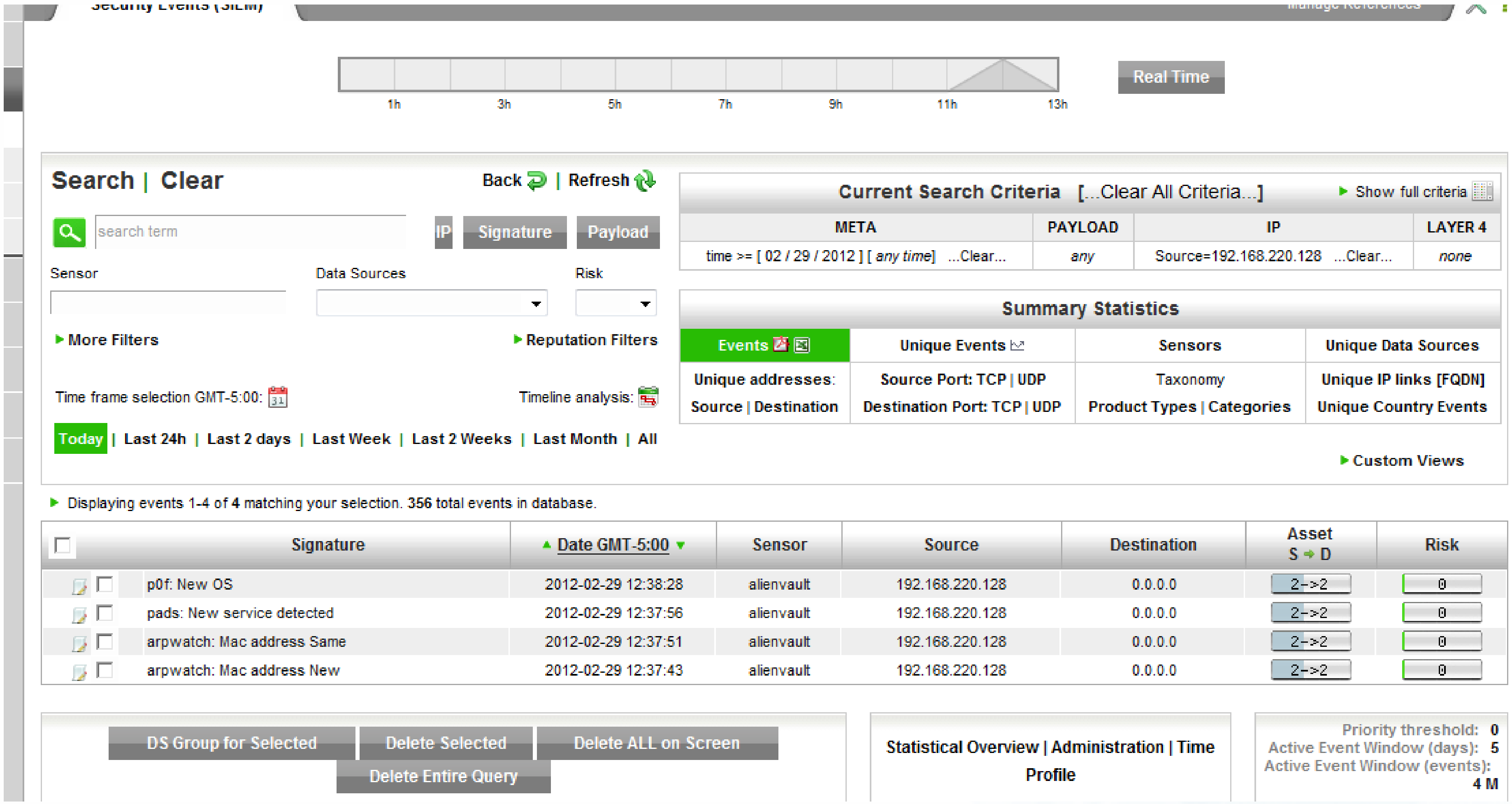
192.168.220.22 [alienvault] [UP or ENABLED: 14 / DOWN or DISABLED: 0 / Totals: 14]

192.168.220.128 [alienvault] [UP or ENABLED: 17 / DOWN or DISABLED: 7 / Totals: 17] **Warning:**The sensor is being reported as enabled by the server but isn't configured.Click here to configure the sensor.

	Plugin	Process Status	Action	Plugin status	Action	Last Security Event
✚	rrd_threshold	DOWN	Start	ENABLED	Disable	
✚	arpwatch	DOWN	Start	ENABLED	Disable	*2012-02-29 17:37:56* **arpwatch: Mac address New**
✚	p0f	DOWN	Start	ENABLED	Disable	*2012-02-29 17:38:28* **p0f: New OS**
✚	malwaredomain	Unknown	-	ENABLED	Disable	
✚	ossec-ossec	DOWN	Start	ENABLED	Disable	
✚	ntop	DOWN	Start	ENABLED	Disable	
✚	ossim-ca	Unknown	-	ENABLED	Disable	
✚	pam_unix	Unknown	-	ENABLED	Disable	
✚	wmi-monitor	Unknown	-	ENABLED	Disable	
✚	nmap	Unknown	-	ENABLED	Disable	
✚	pads	DOWN	Start	ENABLED	Disable	*2012-02-29 17:59:04* **pads: New service detected**
✚	sshd	UP	Stop	ENABLED	Disable	
✚	ossim-agent	Unknown	-	ENABLED	Disable	*2011-11-03 15:07:56* **ossim-agent: error starting a process**
✚	snort	DOWN	Start	ENABLED	Disable	
✚	ping-monitor	Unknown	-	ENABLED	Disable	
✚	sudo	Unknown	-	ENABLED	Disable	
✚	whois	Unknown	-	ENABLED	Disable	

Refresh

5.查看接收到的日志



Security Events (SIEM)

Manage References

Search | Clear   Back | Refresh

search term   IP   Signature   Payload

Sensor   Data Sources   Risk

▸ More Filters   ▸ Reputation Filters

Time frame selection GMT-5:00:   Timeline analysis:

Today | Last 24h | Last 2 days | Last Week | Last 2 Weeks | Last Month | All

Current Search Criteria [...Clear All Criteria...]   ▸ Show full criteria

META	PAYLOAD	IP	LAYER 4
time >= [02 / 29 / 2012] [*any time*] ...Clear...	*any*	Source=192.168.220.128 ...Clear...	*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

▸ Custom Views

▸ Displaying events 1-4 of **4** matching your selection. **356** total events in database.

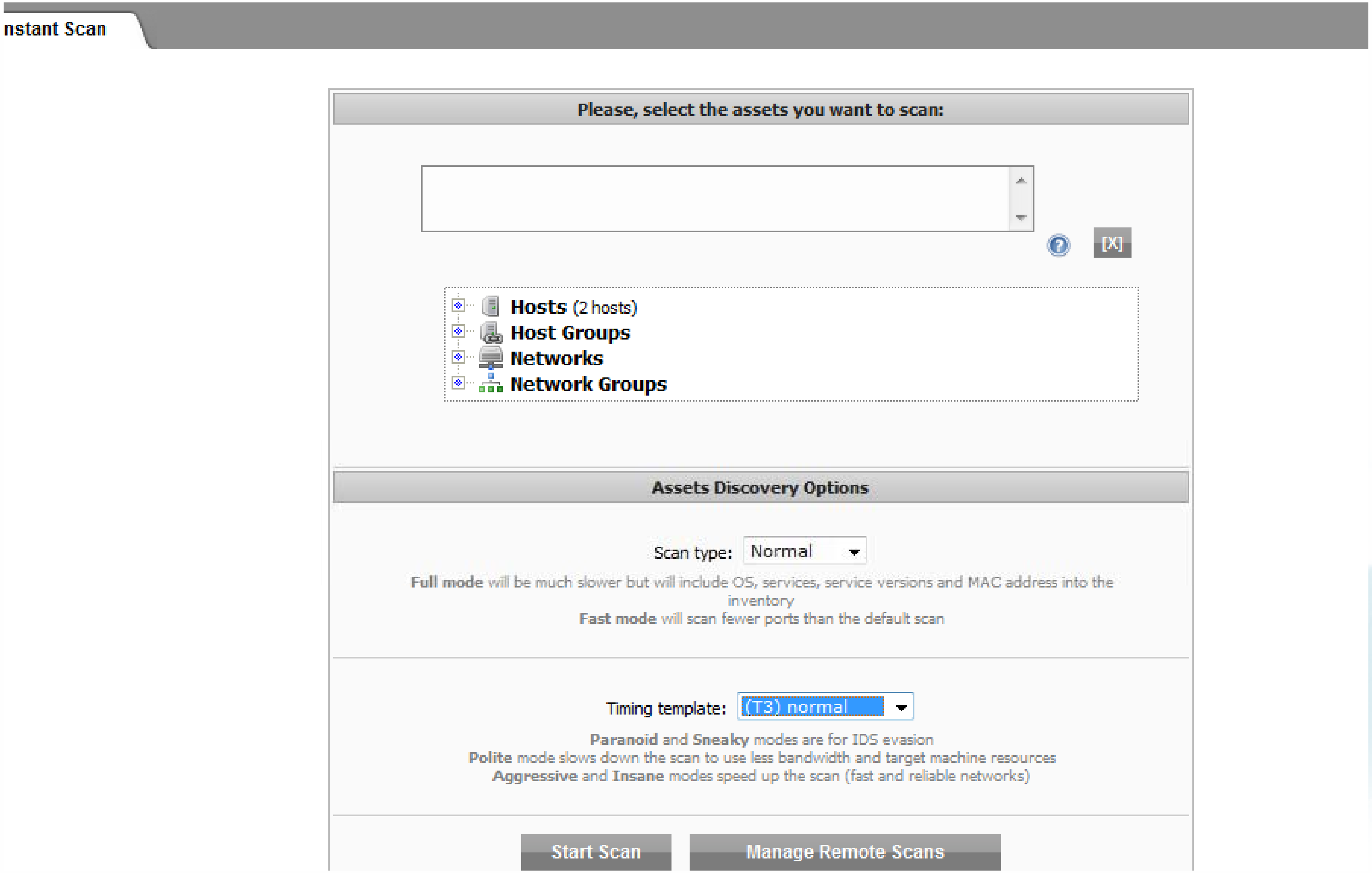
□	Signature	▲ Date GMT-5:00 ▼	Sensor	Source	Destination	Asset S ➔ D	Risk
□	p0f: New OS	2012-02-29 12:38:28	alienvault	192.168.220.128	0.0.0.0	2->2	0
□	pads: New service detected	2012-02-29 12:37:56	alienvault	192.168.220.128	0.0.0.0	2->2	0
□	arpwatch: Mac address Same	2012-02-29 12:37:51	alienvault	192.168.220.128	0.0.0.0	2->2	0
□	arpwatch: Mac address New	2012-02-29 12:37:43	alienvault	192.168.220.128	0.0.0.0	2->2	0

DS Group for Selected   Delete Selected   Delete ALL on Screen   Delete Entire Query

Statistical Overview | Administration | Time Profile

Priority threshold: 0
Active Event Window (days): 5
Active Event Window (events): 4 M

5. 资产管理



nstant Scan

Please, select the assets you want to scan:

- Hosts (2 hosts)
- Host Groups
- Networks
- Network Groups

Assets Discovery Options

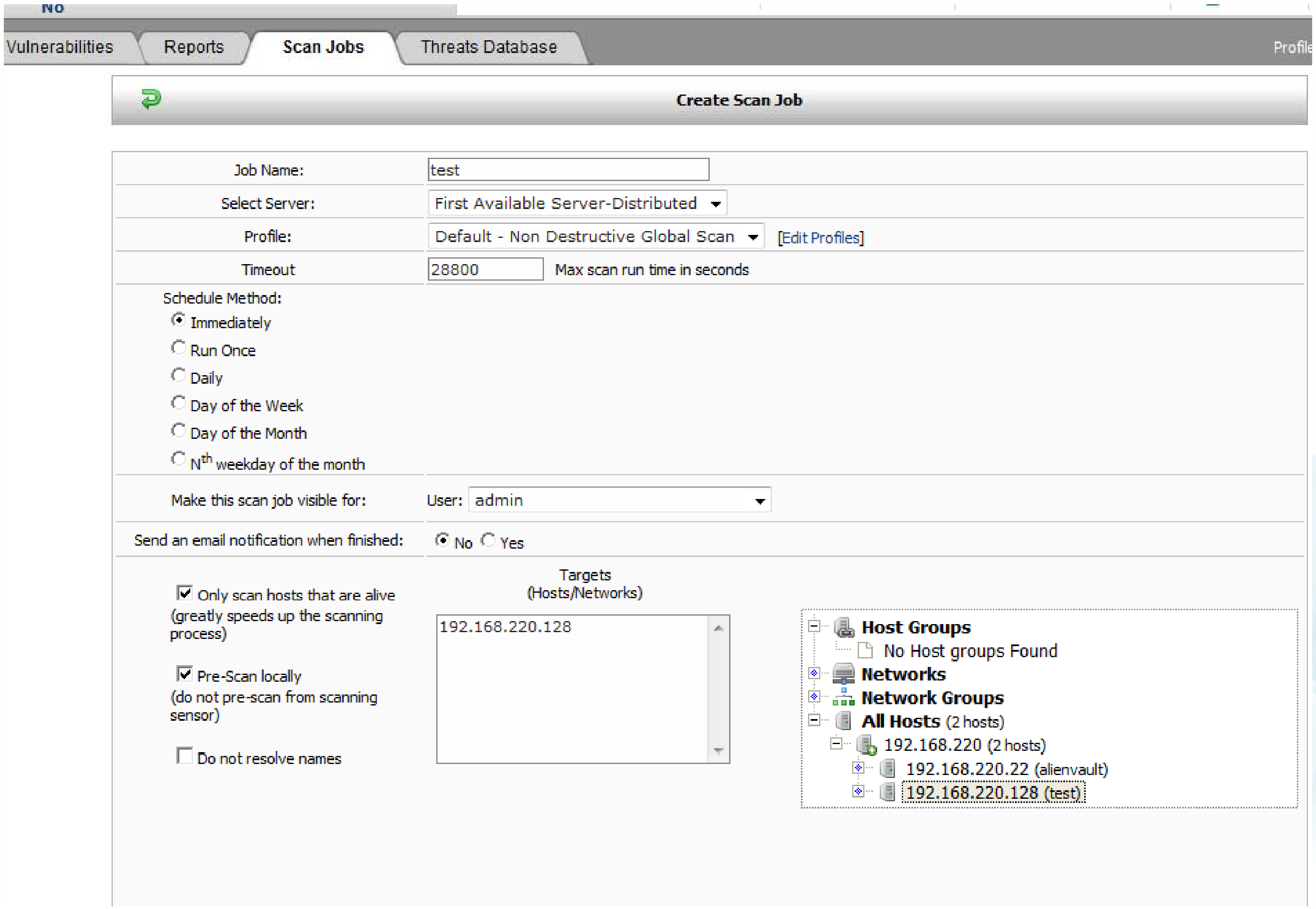
Scan type: Normal

Full mode will be much slower but will include OS, services, service versions and MAC address into the inventory
Fast mode will scan fewer ports than the default scan

Timing template: (T3) normal

Paranoid and **Sneaky** modes are for IDS evasion
Polite mode slows down the scan to use less bandwidth and target machine resources
Aggressive and **Insane** modes speed up the scan (fast and reliable networks)

6. 漏洞管理



Create Scan Job

Job Name:	test
Select Server:	First Available Server-Distributed
Profile:	Default - Non Destructive Global Scan [Edit Profiles]
Timeout	28800 Max scan run time in seconds

Schedule Method:

- ● Immediately
- ○ Run Once
- ○ Daily
- ○ Day of the Week
- ○ Day of the Month
- ○ Nth weekday of the month

Make this scan job visible for: User: admin

Send an email notification when finished: ● No ○ Yes

☑ Only scan hosts that are alive (greatly speeds up the scanning process)

☑ Pre-Scan locally (do not pre-scan from scanning sensor)

□ Do not resolve names

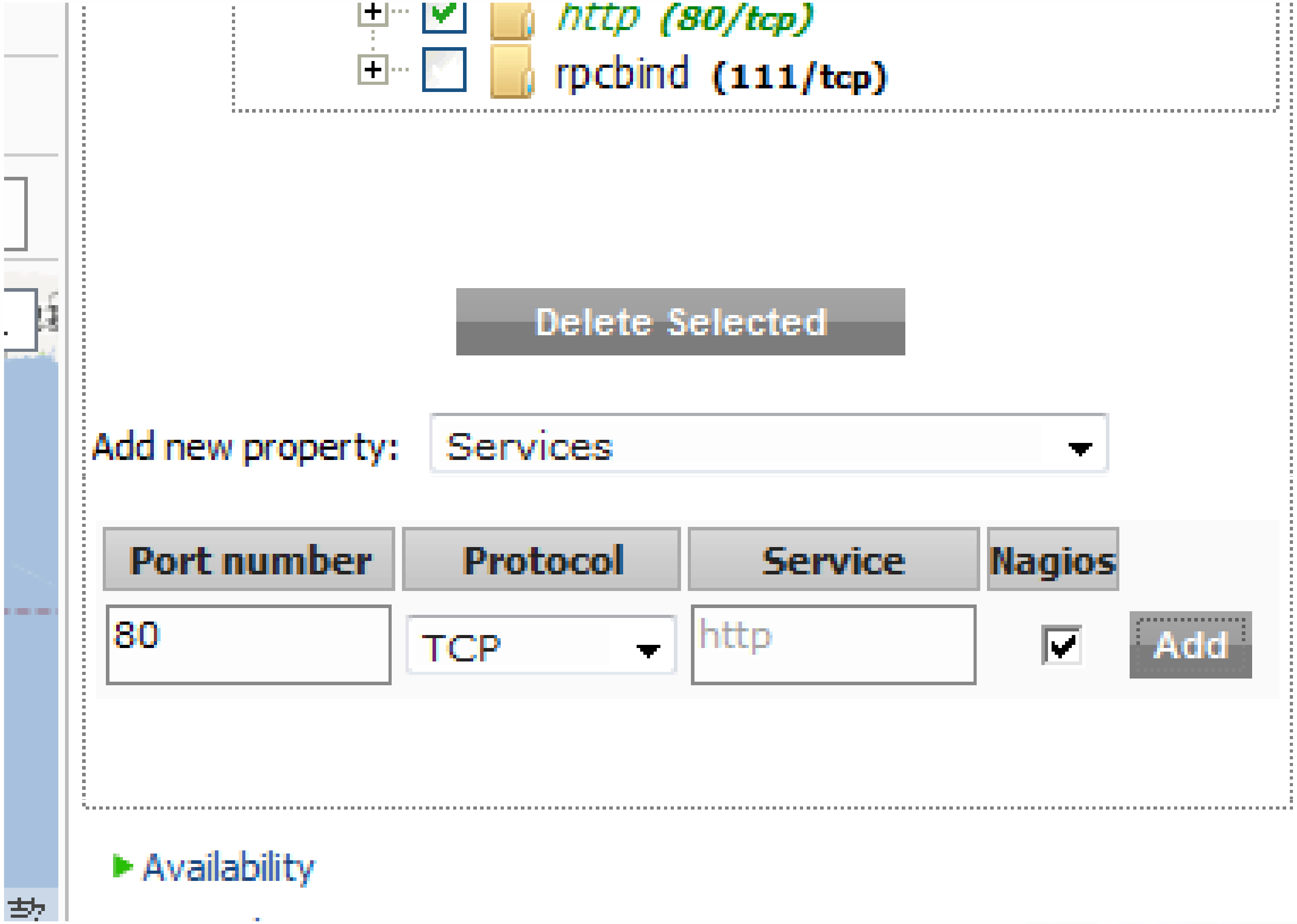
Targets (Hosts/Networks)

192.168.220.128

- Host Groups
  - No Host groups Found
- Networks
- Network Groups
- All Hosts (2 hosts)
  - 192.168.220 (2 hosts)
    - 192.168.220.22 (alienvault)
    - 192.168.220.128 (test)

OSSIM高级安全实践

7. 监控管理



☑ http (80/tcp)

□ rpcbind (111/tcp)

Add new property: Services

Port number	Protocol	Service	Nagios
80	TCP	http	☑

交流与讨论

2012-03-03