```
<!-- @(#) $Id: ./etc/rules/named_rules.xml, 2011/09/08 dcid Exp $

  -  Example of Named rules for OSSEC.
  -
  -  Copyright (C) 2009 Trend Micro Inc.
  -  All rights reserved.
  -
  -  This program is a free software; you can redistribute it
  -  and/or modify it under the terms of the GNU General Public
  -  License (version 2) as published by the FSF - Free Software
  -  Foundation.
  -
  -  License details: http://www.ossec.net/en/licensing.html
  -->


<group name="syslog,named,">
  <rule id="12100" level="0">
    <decoded_as>named</decoded_as>
    <description>Grouping of the named rules</description>
  </rule>

  <rule id="12101" level="12">
    <if_sid>12100</if_sid>
    <pcre2>dropping source port zero packet from</pcre2>
    <description>Invalid DNS packet. Possibility of attack.</description>
```

```
27          <group>invalid_access,</group>
28        </rule>
29
30        <rule id="12102" level="9">
31          <if_sid>12100</if_sid>
32          <pcre2>denied AXFR from</pcre2>
33          <description>Failed attempt to perform a zone transfer.</description>
34          <group>access_denied,</group>
35        </rule>
36
37        <rule id="12103" level="4">
38          <if_sid>12100</if_sid>
39          <pcre2>denied update from|unapproved update from</pcre2>
40          <description>DNS update denied. </description>
41          <description>Generally mis-configuration.</description>
42          <info type="link">http://seclists.org/incidents/2000/May/217</info>
43          <group>client_misconfig,</group>
44        </rule>
45
46        <rule id="12104" level="4">
47          <if_sid>12100</if_sid>
48          <pcre2>unable to rename log file</pcre2>
49          <description>Log permission misconfiguration in Named.</description>
50          <group>system_error,</group>
51        </rule>
52
53        <rule id="12105" level="4">
54          <if_sid>12100</if_sid>
55          <pcre2>unexpected RCODE </pcre2>
56          <description>Unexpected error while resolving domain.</description>
57        </rule>
58
59        <rule id="12106" level="4">
60          <if_sid>12100</if_sid>
61          <pcre2>refused notify from non-master</pcre2>
62          <description>DNS configuration error.</description>
63        </rule>
64
65        <rule id="12107" level="0">
66          <if_sid>12100</if_sid>
67          <pcre2>update \S+ denied</pcre2>
68          <description>DNS update using RFC2136 Dynamic protocol.</description>
69        </rule>
70
71        <rule id="12108" level="5">
72          <if_sid>12100</if_sid>
```

```
73          <pcre2>query \(cache\) denied|: query \(cache\)</pcre2>
74          <description>Query cache denied (probably config error).</description>
75          <info type="link">http://www.reedmedia.net/misc/dns/errors.html</info>
76          <group>connection_attempt,</group>
77        </rule>
78
79        <rule id="12109" level="12">
80          <if_sid>12100</if_sid>
81          <pcre2>exiting \(due to fatal error\)</pcre2>
82          <description>Named fatal error. DNS service going down.</description>
83          <group>service_availability,</group>
84        </rule>
85
86        <rule id="12110" level="8">
87          <pcre2>^zone \S+ serial number \S+ received from master </pcre2>
88          <pcre2>\S+ \S ours (\S+)</pcre2>
89          <description>Serial number from master is lower </description>
90          <description>than stored.</description>
91          <group>system_error,</group>
92        </rule>
93
94        <rule id="12111" level="8">
95          <pcre2>^transfer of \S+ from \S+ failed while receiving \S+ REFUSED</pcre2>
96          <description>Unable to perform zone transfer.</description>
97          <group>system_error,</group>
98        </rule>
99
100       <rule id="12112" level="4">
101         <pcre2>^zone \S+: expired</pcre2>
102         <description>Zone transfer error.</description>
103       </rule>
104
105       <rule id="12113" level="0">
106         <if_sid>12100</if_sid>
107         <pcre2>zone transfer deferred due to quota</pcre2>
108         <description>Zone transfer deferred.</description>
109       </rule>
110
111       <rule id="12114" level="1">
112         <if_sid>12100</if_sid>
113         <pcre2>bad owner name \(check-names\)</pcre2>
114         <description>Hostname contains characters that check-names does not like.</description>
115       </rule>
116
117       <rule id="12115" level="0">
118         <if_sid>12100</if_sid>
```

```
252       <rule id="12138" level="0">
253         <if_sid>12100</if_sid>
254         <pcre2> IN A \+</pcre2>
255         <description>Domain A record found.</description>
```

```
256       </rule>
257
258       <rule id="12139" level="3">
259         <if_sid>12100</if_sid>
260         <pcre2>client \S+: bad zone transfer request: \S+: non-authoritative zone \(NOTAUTH\)</pcre2>
261         <description>Bad zone transfer request.</description>
262       </rule>
263
264       <rule id="12140" level="2">
265         <if_sid>12100</if_sid>
266         <pcre2>refresh: failure trying master</pcre2>
267         <description>Cannot refresh a domain from the master server.</description>
268       </rule>
269
270       <rule id="12141" level="1">
271         <if_sid>12100</if_sid>
272         <pcre2>SOA record not at top of zone</pcre2>
273         <description>Origin of zone and owner name of SOA do not match.</description>
274       </rule>
275
276       <rule id="12142" level="0">
277         <if_sid>12100</if_sid>
278         <pcre2>command channel listening on</pcre2>
279         <description>named command channel is listening.</description>
280       </rule>
281
282       <rule id="12143" level="0">
283         <if_sid>12100</if_sid>
284         <pcre2>automatic empty zone</pcre2>
285         <description>named has created an automatic empty zone.</description>
286       </rule>
287
288       <rule id="12144" level="9">
289         <if_sid>12100</if_sid>
290         <pcre2>reloading configuration failed: out of memory</pcre2>
291         <description>Server does not have enough memory to reload the configuration.</description>
292       </rule>
293
294       <rule id="12145" level="1">
295         <if_sid>12100</if_sid>
296         <pcre2>zone transfer \S+ denied</pcre2>
297         <description>zone transfer denied</description>
298       </rule>
299
300       <rule id="12146" level="0">
301         <if_sid>12100</if_sid>
```

```
302         <pcre2>error sending response: host unreachable$</pcre2>
303         <description>Cannot send a DNS response.</description>
304       </rule>
305
306       <rule id="12147" level="0">
307         <if_sid>12100</if_sid>
308         <pcre2>update forwarding .+ denied$</pcre2>
309         <description>Cannot update forwarding domain.</description>
310       </rule>
311
312       <rule id="12148" level="0">
313         <if_sid>12100</if_sid>
314         <pcre2>: parsing failed$</pcre2>
315         <description>Parsing of a configuration file has failed.</description>
316       </rule>
317
318       <rule id="12149" level="10" frequency="6" timeframe="120">
319        <if_matched_sid>12108</if_matched_sid>
320        <same_source_ip />
321        <description> Multiple query (cache) failures.</description>
322        <group>connection_attempt,</group>
323     </rule>
324
325     </group> <!-- SYSLOG,NAMED -->
```