Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

ossec / ossec-hids Public

Notifications Fork 1k Star 4.5k

Code Issues 308 Pull requests 30 Discussions Actions Projects Wiki Security Insights

Files

1ecffb1

Go to file

- active-response
- contrib
- debian_files
- doc
- etc
  - rules
    - log-entries
    - translated
    - apache_rules.xml
    - apparmor_rules.xml
    - arpwatch_rules.xml
    - asterisk_rules.xml
    - attack_rules.xml
    - cimserver_rules.xml
    - cisco-ios_rules.xml
    - clam_av_rules.xml
    - courier_rules.xml
    - dnsmasq_rules.xml
    - dovecot_rules.xml
    - dropbear_rules.xml
    - exim_rules.xml
    - firewall_rules.xml
    - firewalld_rules.xml
    - ftpd_rules.xml
    - hordeimp_rules.xml
    - ids_rules.xml
    - imapd_rules.xml
    - kesl_rules.xml
    - last_rootlogin_rules.xml
    - lighttpd_rules.xml
    - linux_usbdetect_rules.xml
    - local_rules.xml
    - mailscanner_rules.xml
    - mcafee_av_rules.xml
    - mhn_cowrie_rules.xml
    - mhn_dionaea_rules.xml

ossec-hids / etc / rules / named_rules.xml

Julien DUBOIS Updated PCRE2 rules: match_pcre2 replaced by p... d7e933e · 5 years ago History

Code Blame 325 lines (272 loc) · 10 KB Raw

```xml
<!-- @(#) $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>
    <group>invalid_access,</group>
  </rule>

  <rule id="12102" level="9">
    <if_sid>12100</if_sid>
    <pcre2>denied AXFR from</pcre2>
    <description>Failed attempt to perform a zone transfer.</description>
    <group>access_denied,</group>
  </rule>

  <rule id="12103" level="4">
    <if_sid>12100</if_sid>
    <pcre2>denied update from|unapproved update from</pcre2>
    <description>DNS update denied. </description>
    <description>Generally mis-configuration.</description>
    <info type="link">http://seclists.org/incidents/2000/May/217</info>
    <group>client_misconfig,</group>
  </rule>

  <rule id="12104" level="4">
    <if_sid>12100</if_sid>
    <pcre2>unable to rename log file</pcre2>
    <description>Log permission misconfiguration in Named.</description>
    <group>system_error,</group>
  </rule>

  <rule id="12105" level="4">
    <if_sid>12100</if_sid>
    <pcre2>unexpected RCODE </pcre2>
    <description>Unexpected error while resolving domain.</description>
  </rule>
```

- ms-exchange_rules.xml
- ms-se_rules.xml
- ms1016_usbdetect_rules.xml
- ms_dhcp_rules.xml
- ms_firewall_rules.xml
- ms_ftpd_rules.xml

```
  </rule>

  <rule id="12106" level="4">
    <if_sid>12100</if_sid>
    <pcre2>refused notify from non-master</pcre2>
    <description>DNS configuration error.</description>
  </rule>

  <rule id="12107" level="0">
    <if_sid>12100</if_sid>
    <pcre2>update \S+ denied</pcre2>
    <description>DNS update using RFC2136 Dynamic protocol.</description>
  </rule>

  <rule id="12108" level="5">
    <if_sid>12100</if_sid>
    <pcre2>query \(cache\) denied|: query \(cache\)</pcre2>
    <description>Query cache denied (probably config error).</description>
    <info type="link">http://www.reedmedia.net/misc/dns/errors.html</info>
    <group>connection_attempt,</group>
  </rule>

  <rule id="12109" level="12">
    <if_sid>12100</if_sid>
    <pcre2>exiting \(due to fatal error\)</pcre2>
    <description>Named fatal error. DNS service going down.</description>
    <group>service_availability,</group>
  </rule>

  <rule id="12110" level="8">
    <pcre2>^zone \S+ serial number \S+ received from master </pcre2>
    <pcre2>\S+ \S ours (\S+)</pcre2>
    <description>Serial number from master is lower </description>
    <description>than stored.</description>
    <group>system_error,</group>
  </rule>

  <rule id="12111" level="8">
    <pcre2>^transfer of \S+ from \S+ failed while receiving \S+ REFUSED</pcre2>
    <description>Unable to perform zone transfer.</description>
    <group>system_error,</group>
  </rule>

  <rule id="12112" level="4">
    <pcre2>^zone \S+: expired</pcre2>
    <description>Zone transfer error.</description>
  </rule>

  <rule id="12113" level="0">
    <if_sid>12100</if_sid>
    <pcre2>zone transfer deferred due to quota</pcre2>
    <description>Zone transfer deferred.</description>
  </rule>

  <rule id="12114" level="1">
    <if_sid>12100</if_sid>
    <pcre2>bad owner name \(check-names\)</pcre2>
    <description>Hostname contains characters that check-names does not like.</descript
  </rule>

  <rule id="12115" level="0">
    <if_sid>12100</if_sid>
```

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

  <rule id="12139" level="3">
    <if_sid>12100</if_sid>
    <pcre2>client \S+: bad zone transfer request: \S+: non-authoritative zone \(NOTAUTH
    <description>Bad zone transfer request.</description>
  </rule>

  <rule id="12140" level="2">
    <if_sid>12100</if_sid>
    <pcre2>refresh: failure trying master</pcre2>
    <description>Cannot refresh a domain from the master server.</description>
  </rule>

  <rule id="12141" level="1">
    <if_sid>12100</if_sid>
    <pcre2>SOA record not at top of zone</pcre2>
    <description>Origin of zone and owner name of SOA do not match.</description>
  </rule>

  <rule id="12142" level="0">
    <if_sid>12100</if_sid>
    <pcre2>command channel listening on</pcre2>
    <description>named command channel is listening.</description>
  </rule>

  <rule id="12143" level="0">
    <if_sid>12100</if_sid>
    <pcre2>automatic empty zone</pcre2>
    <description>named has created an automatic empty zone.</description>
  </rule>

  <rule id="12144" level="9">
    <if_sid>12100</if_sid>
    <pcre2>reloading configuration failed: out of memory</pcre2>
    <description>Server does not have enough memory to reload the configuration.</descr
  </rule>

  <rule id="12145" level="1">
    <if_sid>12100</if_sid>
    <pcre2>zone transfer \S+ denied</pcre2>
    <description>zone transfer denied</description>
  </rule>

  <rule id="12146" level="0">
    <if_sid>12100</if_sid>
    <pcre2>error sending response: host unreachable$</pcre2>
    <description>Cannot send a DNS response.</description>
  </rule>

  <rule id="12147" level="0">
    <if_sid>12100</if_sid>
    <pcre2>update forwarding .+ denied$</pcre2>
    <description>Cannot update forwarding domain.</description>
  </rule>

  <rule id="12148" level="0">
    <if_sid>12100</if_sid>
    <pcre2>: parsing failed$</pcre2>
    <description>Parsing of a configuration file has failed.</description>
  </rule>

  <rule id="12149" level="10" frequency="6" timeframe="120">
   <if_matched_sid>12108</if_matched_sid>
   <same_source_ip />
   <description> Multiple query (cache) failures.</description>
   <group>connection_attempt,</group>
</rule>

</group> <!-- SYSLOG,NAMED -->
```