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 / attack_rules.xml

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

Code Blame 122 lines (98 loc) · 4.21 KB Raw

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

  -  Official "attack" correlation 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
  -->


<!-- System users. They should never log in to the system -->
<var name="SYS_USERS">^apache$|^mysql$|^www$|^nobody$|^nogroup$|^portmap$|^named$|^rpc$


<!-- Attack signatures -->
<group name="syslog,attacks,">
  <rule id="40101" level="12">
    <if_group>authentication_success</if_group>
    <user_pcre2>$SYS_USERS</user_pcre2>
    <description>System user successfully logged to the system.</description>
    <group>invalid_login,</group>
  </rule>

  <rule id="40102" level="14">
    <pcre2>^rpc\.statd\[\d+\]: gethostbyname error for [^A-Za-z0-9@_-]+</pcre2>
    <description>Buffer overflow attack on rpc.statd</description>
    <group>exploit_attempt,</group>
  </rule>

  <rule id="40103" level="14">
    <pcre2>ftpd\[\d+\]: \S+ FTP LOGIN FROM .+ 0bin0sh</pcre2>
    <description>Buffer overflow on WU-FTPD versions prior to 2.6</description>
    <group>exploit_attempt,</group>
  </rule>

  <rule id="40104" level="13">
    <pcre2>\?{21}</pcre2>
    <description>Possible buffer overflow attempt.</description>
    <group>exploit_attempt,</group>
  </rule>

  <rule id="40105" level="12">
    <pcre2>changed by \(\(null\)</pcre2>
    <description>"Null" user changed some information.</description>
    <group>exploit_attempt,</group>
  </rule>

  <rule id="40106" level="12">
    <pcre2>@{25}</pcre2>
    <description>Buffer overflow attempt (probably on yppasswd).</description>
```

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

```
    <group>exploit_attempt,</group>
  </rule>

  <rule id="40107" level="14">
    <pcre2>cachefsd: Segmentation Fault - core dumped</pcre2>
    <description>Heap overflow in the Solaris cachefsd service.</description>
    <info type='cve'>2002-0033</info>
    <group>exploit_attempt,</group>
  </rule>

  <rule id="40109" level="12">
    <pcre2>attempt to execute code on stack by</pcre2>
    <description>Stack overflow attempt or program exiting </description>
    <description>with SEGV (Solaris).</description>
    <info type="link">http://snap.nlc.dcccd.edu/reference/sysadmin/julian/ch18/389-392.
    <group>exploit_attempt,</group>
  </rule>

  <rule id="40111" level="10" frequency="10" timeframe="160">
    <if_matched_group>authentication_failed</if_matched_group>
    <description>Multiple authentication failures.</description>
    <group>authentication_failures,</group>
  </rule>

    <rule id="40112" level="12" timeframe="240">
      <if_group>authentication_success</if_group>
      <if_matched_group>authentication_failures</if_matched_group>
      <same_source_ip />
      <description>Multiple authentication failures followed </description>
      <description>by a success.</description>
    </rule>

    <rule id="40113" level="12" frequency="6" timeframe="360">
      <if_matched_group>virus</if_matched_group>
      <description>Multiple viruses detected - Possible outbreak.</description>
      <group>virus,</group>
    </rule>

  </group> <!-- SYSLOG, ATTACKS, -->



  <!-- Privilege escalation messages -->
  <group name="syslog,elevation_of_privilege,">
    <rule id="40501" level="15" timeframe="300" frequency="2">
      <if_group>adduser</if_group>
      <if_matched_group>attacks</if_matched_group>
      <description>Attacks followed by the addition </description>
      <description>of an user.</description>
    </rule>
  </group> <!-- SYSLOG, ELEVATION_OF_PRIVILEGE, -->



  <!-- Scan signatures -->
  <group name="syslog,recon,">
    <rule id="40601" level="10" frequency="10" timeframe="90" ignore="90">
      <if_matched_group>connection_attempt</if_matched_group>
      <description>Network scan from same source ip.</description>
      <same_source_ip />
      <info type="link">http://project.honeynet.org/papers/enemy2/</info>
    </rule>
  </group> <!-- SYSLOG,SCANS -->


  <!-- EOF -->
```