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 / sshd_rules.xml

ddpbsd Add a log message to the version rule. c076c1a · 5 years ago History

Code Blame 404 lines (343 loc) · 13.3 KB Raw

```
<!-- @(#) $Id: sshd_rules.xml,v 1.22 2010/12/19 14:50:14 ddp Exp $
  -  Official SSHD rules for OSSEC.
  -
  -  Copyright (C) 2009-2011 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
  -->


<!-- SSHD messages -->
<group name="syslog,sshd,">
  <rule id="5700" level="0" noalert="1">
    <decoded_as>sshd</decoded_as>
    <description>SSHD messages grouped.</description>
  </rule>

  <rule id="5701" level="8">
    <if_sid>5700</if_sid>
    <pcre2>Bad protocol version identification|error: Protocol major versions differ</p
    <description>Possible attack on the ssh server </description>
    <description>(or version gathering).</description>
  </rule>

  <rule id="5702" level="5">
    <if_sid>5700</if_sid>
    <pcre2>^reverse mapping.*failed - POSSIBLE BREAK</pcre2>
    <description>Reverse lookup error (bad ISP or attack).</description>
  </rule>

  <rule id="5703" level="10" frequency="4" timeframe="360">
    <if_matched_sid>5702</if_matched_sid>
    <description>Possible breakin attempt </description>
    <description>(high number of reverse lookup errors).</description>
  </rule>

  <rule id="5704" level="4">
    <if_sid>5700</if_sid>
    <pcre2>fatal: Timeout before authentication for</pcre2>
    <description>Timeout while logging in (sshd).</description>
  </rule>

  <rule id="5705" level="10" frequency="4" timeframe="360">
    <if_matched_sid>5704</if_matched_sid>
    <description>Possible scan or breakin attempt </description>
    <description>(high number of login timeouts).</description>
  </rule>

  <rule id="5706" level="6">
    <if_sid>5700</if_sid>
    <pcre2>Did not receive identification string from</pcre2>
    <description>SSH insecure connection attempt (scan).</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

```
    <description>SSH insecure connection attempt (scan).</description>
    <group>recon,</group>
  </rule>

  <rule id="5707" level="14">
    <if_sid>5700</if_sid>
    <pcre2>fatal: buffer_get_string: bad string</pcre2>
    <description>OpenSSH challenge-response exploit.</description>
    <group>exploit_attempt,</group>
  </rule>

  <rule id="5709" level="0">
    <if_sid>5700</if_sid>
    <pcre2>error: Could not get shadow information for NOUSER|</pcre2>
    <pcre2>fatal: Read from socket failed: |error: ssh_msg_send: write|</pcre2>
    <pcre2>^syslogin_perform_logout: |^pam_succeed_if\(sshd:auth\): error retrieving in
    <description>Useless SSHD message without an user/ip and context.</description>
  </rule>

  <rule id="5710" level="5">
    <if_sid>5700</if_sid>
    <pcre2>illegal user|invalid user</pcre2>
    <description>Attempt to login using a non-existent user</description>
    <group>invalid_login,authentication_failed,</group>
  </rule>

  <rule id="5711" level="0">
    <if_sid>5700</if_sid>
    <pcre2>authentication failure; logname= uid=0 euid=0 tty=ssh|</pcre2>
    <pcre2>input_userauth_request: invalid user|</pcre2>
    <pcre2>PAM: User not known to the underlying authentication module for illegal user
    <pcre2>error retrieving information about user</pcre2>
    <description>Useless/Duplicated SSHD message without a user/ip.</description>
  </rule>

  <rule id="5712" level="10" frequency="6" timeframe="120" ignore="60">
    <if_matched_sid>5710</if_matched_sid>
    <description>SSHD brute force trying to get access to </description>
    <description>the system.</description>
    <same_source_ip />
    <group>authentication_failures,</group>
  </rule>

  <rule id="5713" level="6">
    <if_sid>5700</if_sid>
    <pcre2>Corrupted check bytes on</pcre2>
    <description>Corrupted bytes on SSHD.</description>
  </rule>

  <rule id="5714" level="14" timeframe="120" frequency="1">
    <if_matched_sid>5713</if_matched_sid>
    <pcre2>Local: crc32 compensation attack</pcre2>
    <description>SSH CRC-32 Compensation attack</description>
    <info type="cve">2001-0144</info>
    <info type="link">http://www.securityfocus.com/bid/2347/info/</info>
    <group>exploit_attempt,</group>
  </rule>

  <rule id="5715" level="3">
    <if_sid>5700</if_sid>
    <pcre2>^Accepted|authenticated\.$</pcre2>
    <description>SSHD authentication success.</description>
```

```
    -->
    <rule id="5748" level="6">
      <if_sid>5700</if_sid>
      <pcre2>Corrupted MAC on input\.</pcre2>
      <description>ssh corrupted MAC on input</description>
    </rule>

    <rule id="5749" level="4">
      <if_sid>5700</if_sid>
      <pcre2>^Bad packet length</pcre2>
      <description>ssh bad packet length</description>
    </rule>

    <rule id="5750" level="0">
      <decoded_as>sshd</decoded_as>
      <if_sid>5700</if_sid>
      <pcre2>Unable to negotiate with |Unable to negotiate a key</pcre2>
      <description>sshd could not negotiate with client.</description>
    </rule>

    <rule id="5751" level="1">
      <decoded_as>sshd</decoded_as>
      <if_sid>5700</if_sid>
      <pcre2>no hostkey alg \[preauth\]</pcre2>
      <description>No hostkey alg.</description>
```

```
  </rule>

  <rule id="5752" level="2">
    <if_sid>5750</if_sid>
    <pcre2>no matching key exchange method found\.|Unable to negotiate a key exchange m
    <description>Client did not offer an acceptable key exchange method.</description>
  </rule>

  <rule id="5753" level="2">
    <if_sid>5750</if_sid>
    <pcre2>no matching cipher found\.</pcre2>
    <description>sshd could not negotiate with client, no matching cipher.</description
  </rule>

  <rule id="5754" level="1">
    <if_sid>5700</if_sid>
    <pcre2>Failed to create session: </pcre2>
    <description>sshd failed to create a session.</description>
  </rule>

  <rule id="5755" level="2">
    <if_sid>5700</if_sid>
    <pcre2>bad ownership or modes for file</pcre2>
    <description>Authentication refused due to owner/permissions of authorized_keys.</d
    <group>authentication_failed,</group>
  </rule>

  <rule id="5756" level="0">
    <if_sid>5700</if_sid>
    <pcre2> failed, subsystem not found$</pcre2>
    <description>sshd subsystem request failed.</description>
  </rule>

  <rule id="5757" level="0">
    <decoded_as>sshd</decoded_as>
    <pcre2>but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!$</pcr
    <description>Bad DNS mapping.</description>
  </rule>

  <rule id="5758" level="8">
    <decoded_as>sshd</decoded_as>
    <pcre2>^error: maximum authentication attempts exceeded </pcre2>
    <description>Maximum authentication attempts exceeded.</description>
    <group>authentication_failed,</group>
  </rule>

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

<!-- EOF -->
```