




 **ossec** / **ossec-hids** Public


 Notifications


 Fork 1k


 Star 4.5k


 **Code**


 Issues 308


 Pull requests 30

 Discussions

 Actions

 Projects

 Wiki



ossec-hids / etc / rules / sshd_rules.xml 






 **ddpbsd** Add a log message to the version rule. 

c076c1a · 5 years ago 

404 lines (343 loc) · 13.3 KB

Code

Blame

Raw   

```
1      <!-- @(#) $Id: sshd_rules.xml,v 1.22 2010/12/19 14:50:14 ddp Exp $
2      -   Official SSHD rules for OSSEC.
3      -
4      -   Copyright (C) 2009-2011 Trend Micro Inc.
5      -   All rights reserved.
6      -
7      -   This program is a free software; you can redistribute it
8      -   and/or modify it under the terms of the GNU General Public
9      -   License (version 2) as published by the FSF - Free Software
10     -   Foundation.
11     -
12     -   License details: http://www.ossec.net/en/licensing.html
13     -->
14
15
16     <!-- SSHD messages -->
17     <group name="syslog,sshd,">
18         <rule id="5700" level="0" noalert="1">
19             <decoded_as>sshd</decoded_as>
20             <description>SSHD messages grouped.</description>
21         </rule>
22
23         <rule id="5701" level="8">
24             <if_sid>5700</if_sid>
25             <pcr2>Bad protocol version identification|error: Protocol major versions differ</pcr2>
26             <description>Possible attack on the ssh server </description>
```

```
27     <description>(or version gathering).</description>
28 </rule>
29
30 <rule id="5702" level="5">
31   <if_sid>5700</if_sid>
32   <pcre2>^reverse mapping.*failed - POSSIBLE BREAK</pcre2>
33   <description>Reverse lookup error (bad ISP or attack).</description>
34 </rule>
35
36 <rule id="5703" level="10" frequency="4" timeframe="360">
37   <if_matched_sid>5702</if_matched_sid>
38   <description>Possible breakin attempt </description>
39   <description>(high number of reverse lookup errors).</description>
40 </rule>
41
42 <rule id="5704" level="4">
43   <if_sid>5700</if_sid>
44   <pcre2>fatal: Timeout before authentication for</pcre2>
45   <description>Timeout while logging in (sshd).</description>
46 </rule>
47
48 <rule id="5705" level="10" frequency="4" timeframe="360">
49   <if_matched_sid>5704</if_matched_sid>
50   <description>Possible scan or breakin attempt </description>
51   <description>(high number of login timeouts).</description>
52 </rule>
53
54 <rule id="5706" level="6">
55   <if_sid>5700</if_sid>
56   <pcre2>Did not receive identification string from</pcre2>
57   <description>SSH insecure connection attempt (scan).</description>
58   <group>recon,</group>
59 </rule>
60
61 <rule id="5707" level="14">
62   <if_sid>5700</if_sid>
63   <pcre2>fatal: buffer_get_string: bad string</pcre2>
64   <description>OpenSSH challenge-response exploit.</description>
65   <group>exploit_attempt,</group>
66 </rule>
67
68 <rule id="5709" level="0">
69   <if_sid>5700</if_sid>
70   <pcre2>error: Could not get shadow information for NOUSER|</pcre2>
71   <pcre2>fatal: Read from socket failed: |error: ssh_msg_send: write|</pcre2>
72   <pcre2>^syslogin_perform_logout: |^pam_succeed_if\(sshd:auth\): error retrieving information at
```

```
73     <description>Useless SSHD message without an user/ip and context.</description>
74 </rule>
75
76 <rule id="5710" level="5">
77     <if_sid>5700</if_sid>
78     <pcre2>illegal user|invalid user</pcre2>
79     <description>Attempt to login using a non-existent user</description>
80     <group>invalid_login,authentication_failed,</group>
81 </rule>
82
83 <rule id="5711" level="0">
84     <if_sid>5700</if_sid>
85     <pcre2>authentication failure; logname= uid=0 euid=0 tty=ssh|</pcre2>
86     <pcre2>input_userauth_request: invalid user|</pcre2>
87     <pcre2>PAM: User not known to the underlying authentication module for illegal user|</pcre2>
88     <pcre2>error retrieving information about user</pcre2>
89     <description>Useless/Duplicated SSHD message without a user/ip.</description>
90 </rule>
91
92 <rule id="5712" level="10" frequency="6" timeframe="120" ignore="60">
93     <if_matched_sid>5710</if_matched_sid>
94     <description>SSHD brute force trying to get access to </description>
95     <description>the system.</description>
96     <same_source_ip />
97     <group>authentication_failures,</group>
98 </rule>
99
100 <rule id="5713" level="6">
101     <if_sid>5700</if_sid>
102     <pcre2>Corrupted check bytes on</pcre2>
103     <description>Corrupted bytes on SSHD.</description>
104 </rule>
105
106 <rule id="5714" level="14" timeframe="120" frequency="1">
107     <if_matched_sid>5713</if_matched_sid>
108     <pcre2>Local: crc32 compensation attack</pcre2>
109     <description>SSH CRC-32 Compensation attack</description>
110     <info type="cve">2001-0144</info>
111     <info type="link">http://www.securityfocus.com/bid/2347/info</info>
112     <group>exploit_attempt,</group>
113 </rule>
114
115 <rule id="5715" level="3">
116     <if_sid>5700</if_sid>
117     <pcre2>^Accepted|authenticated\.$</pcre2>
118     <description>SSHD authentication success </description>
```

440 <description>SSH authentication success. </description>


```
331      -->
332      <rule id="5748" level="6">
333        <if_sid>5700</if_sid>
334        <pcre2>Corrupted MAC on input\.</pcre2>
335        <description>ssh corrupted MAC on input</description>
336      </rule>
337
338      <rule id="5749" level="4">
339        <if_sid>5700</if_sid>
340        <pcre2>^Bad packet length</pcre2>
341        <description>ssh bad packet length</description>
342      </rule>
343
344      <rule id="5750" level="0">
345        <decoded_as>sshd</decoded_as>
346        <if_sid>5700</if_sid>
347        <pcr2>Unable to negotiate with |Unable to negotiate a key</pcr2>
```



```
347         <pcrc2>unable to negotiate with client, unable to negotiate a key</pcrc2>
348         <description>sshd could not negotiate with client.</description>
349     </rule>
350
351     <rule id="5751" level="1">
352         <decoded_as>sshd</decoded_as>
353         <if_sid>5700</if_sid>
354         <pcrc2>no hostkey alg \[preauth\]</pcrc2>
355         <description>No hostkey alg.</description>
356     </rule>
357
358     <rule id="5752" level="2">
359         <if_sid>5750</if_sid>
360         <pcrc2>no matching key exchange method found\.|Unable to negotiate a key exchange method</pcrc2>
361         <description>Client did not offer an acceptable key exchange method.</description>
362     </rule>
363
364     <rule id="5753" level="2">
365         <if_sid>5750</if_sid>
366         <pcrc2>no matching cipher found\.</pcrc2>
367         <description>sshd could not negotiate with client, no matching cipher.</description>
368     </rule>
369
370     <rule id="5754" level="1">
371         <if_sid>5700</if_sid>
372         <pcrc2>Failed to create session: </pcrc2>
373         <description>sshd failed to create a session.</description>
374     </rule>
375
376     <rule id="5755" level="2">
377         <if_sid>5700</if_sid>
378         <pcrc2>bad ownership or modes for file</pcrc2>
379         <description>Authentication refused due to owner/permissions of authorized_keys.</description>
380         <group>authentication_failed,</group>
381     </rule>
382
383     <rule id="5756" level="0">
384         <if_sid>5700</if_sid>
385         <pcrc2> failed, subsystem not found$</pcrc2>
386         <description>sshd subsystem request failed.</description>
387     </rule>
388
389     <rule id="5757" level="0">
390         <decoded_as>sshd</decoded_as>
391         <pcrc2>but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!$</pcrc2>
392         <description>Bad DNS mapping.</description>
393     </rule>
```

```
393     </rule>
394
395     <rule id="5758" level="8">
396         <decoded_as>sshd</decoded_as>
397         <pcre2>^error: maximum authentication attempts exceeded </pcre2>
398         <description>Maximum authentication attempts exceeded.</description>
399         <group>authentication_failed,</group>
400     </rule>
401
402 </group> <!-- SYSLOG, SSHD -->
403
404 <!-- EOF -->
```