Documentation › User manual › Ruleset › Testing decoders and rules

Testing decoders and rules

The tool *ossec-logtest* allow us to test how an event is decoded and if an alert is generated.

Run the tool */var/ossec/bin/ossec-logtest* and paste the following log:

```
Mar  8 22:39:13 ip-10-0-0-10 sshd[2742]: Accepted publickey for root from 73.189.131.56 port 57516
```

```
$ /var/ossec/bin/ossec-logtest

Mar  8 22:39:13 ip-10-0-0-10 sshd[2742]: Accepted publickey for root from 73.189.131.56 port 57516

**Phase 1: Completed pre-decoding.
       full event: 'Mar  8 22:39:13 ip-10-0-0-10 sshd[2742]: Accepted publickey for root from 73.189.131.56 port 57516'
       hostname: 'ip-10-0-0-10'
       program_name: 'sshd'
       log: 'Accepted publickey for root from 73.189.131.56 port 57516'

**Phase 2: Completed decoding.
       decoder: 'sshd'
       dstuser: 'root'
       srcip: '73.189.131.56'

**Phase 3: Completed filtering (rules).
       Rule id: '5715'
       Level: '3'
       Description: 'sshd: authentication success.'
**Alert to be generated.
```

⚠ Warning

The decoder name showed in *Phase 2* will be the name of the parent decoder.

In addition, you can use the option “-v” to show more information about the rules:

```
$ /var/ossec/bin/ossec-logtest -v

Mar  8 22:39:13 ip-10-0-0-10 sshd[2742]: Accepted publickey for root from 73.189.131.56 port 57516


**Phase 1: Completed pre-decoding.
       full event: 'Mar  8 22:39:13 ip-10-0-0-10 sshd[2742]: Accepted publickey for root from 73.189.131.56
port 57516'
       hostname: 'ip-10-0-0-10'
       program_name: 'sshd'
       log: 'Accepted publickey for root from 73.189.131.56 port 57516'

**Phase 2: Completed decoding.
       decoder: 'sshd'
       dstuser: 'root'
       srcip: '73.189.131.56'

**Rule debugging:
    Trying rule: 1 - Generic template for all syslog rules.
       *Rule 1 matched.
       *Trying child rules.
    Trying rule: 600 - Active Response Messages Grouped
    Trying rule: 2100 - NFS rules grouped.
    Trying rule: 2507 - OpenLDAP group.
    Trying rule: 2550 - rshd messages grouped.
    Trying rule: 2701 - Ignoring procmail messages.
    Trying rule: 2800 - Pre-match rule for smartd.
    Trying rule: 5100 - Pre-match rule for kernel messages
    Trying rule: 5200 - Ignoring hpiod for producing useless logs.
    Trying rule: 2830 - Crontab rule group.
    Trying rule: 5300 - Initial grouping for su messages.
    Trying rule: 5905 - useradd failed.
    Trying rule: 5400 - Initial group for sudo messages
    Trying rule: 9100 - PPTPD messages grouped
    Trying rule: 9200 - Squid syslog messages grouped
    Trying rule: 2900 - Dpkg (Debian Package) log.
    Trying rule: 2930 - Yum logs.
    Trying rule: 2931 - Yum logs.
    Trying rule: 2940 - NetworkManager grouping.
    Trying rule: 2943 - nouveau driver grouping
    Trying rule: 3100 - Grouping of the sendmail rules.
    Trying rule: 3190 - Grouping of the smf-sav sendmail milter rules.
    Trying rule: 3300 - Grouping of the postfix reject rules.
    Trying rule: 3320 - Grouping of the postfix rules.
    Trying rule: 3390 - Grouping of the clamsmtpd rules.
    Trying rule: 3395 - Grouping of the postfix warning rules.
    Trying rule: 3500 - Grouping for the spamd rules
    Trying rule: 3600 - Grouping of the imapd rules.
    Trying rule: 3700 - Grouping of mailscanner rules.
    Trying rule: 3800 - Grouping of Exchange rules.
    Trying rule: 3900 - Grouping for the courier rules.
    Trying rule: 4300 - Grouping of PIX rules
    Trying rule: 4500 - Grouping for the Netscreen Firewall rules
    Trying rule: 4700 - Grouping of Cisco IOS rules.
    Trying rule: 4800 - SonicWall messages grouped.
    Trying rule: 5500 - Grouping of the pam_unix rules.
    Trying rule: 5556 - unix_chkpwd grouping.
    Trying rule: 5600 - Grouping for the telnetd rules
    Trying rule: 5700 - SSHD messages grouped.
       *Rule 5700 matched.
       *Trying child rules.
    Trying rule: 5709 - sshd: Useless SSHD message without an user/ip and context.
    Trying rule: 5711 - sshd: Useless/Duplicated SSHD message without a user/ip.
    Trying rule: 5721 - sshd: System disconnected from sshd.
    Trying rule: 5722 - sshd: ssh connection closed.
    Trying rule: 5723 - sshd: key error.
    Trying rule: 5724 - sshd: key error.
    Trying rule: 5725 - sshd: Host ungracefully disconnected.
    Trying rule: 5727 - sshd: Attempt to start sshd when something already bound to the port.
    Trying rule: 5729 - sshd: Debug message.
    Trying rule: 5732 - sshd: Possible port forwarding failure.
    Trying rule: 5733 - sshd: User entered incorrect password.
    Trying rule: 5734 - sshd: sshd could not load one or more host keys.
    Trying rule: 5735 - sshd: Failed write due to one host disappearing.
    Trying rule: 5736 - sshd: Connection reset or aborted.
    Trying rule: 5750 - sshd: could not negotiate with client.
    Trying rule: 5756 - sshd: subsystem request failed.
    Trying rule: 5707 - sshd: OpenSSH challenge-response exploit.
    Trying rule: 5701 - sshd: Possible attack on the ssh server (or version gathering).
    Trying rule: 5706 - sshd: insecure connection attempt (scan).
    Trying rule: 5713 - sshd: Corrupted bytes on SSHD.
    Trying rule: 5731 - sshd: SSH Scanning.
    Trying rule: 5747 - sshd: bad client public DH value
    Trying rule: 5748 - sshd: corrupted MAC on input
    Trying rule: 5702 - sshd: Reverse lookup error (bad ISP or attack).
    Trying rule: 5710 - sshd: Attempt to login using a non-existent user
    Trying rule: 5716 - sshd: authentication failed.
    Trying rule: 5718 - sshd: Attempt to login using a denied user.
    Trying rule: 5726 - sshd: Unknown PAM module, PAM misconfiguration.
    Trying rule: 5737 - sshd: cannot bind to configured address.
    Trying rule: 5738 - sshd: pam_loginuid could not open loginuid.
    Trying rule: 5704 - sshd: Timeout while logging in.
    Trying rule: 5717 - sshd: configuration error (moduli).
    Trying rule: 5728 - sshd: Authentication services were not able to retrieve user credentials.
    Trying rule: 5730 - sshd: SSHD is not accepting connections.
    Trying rule: 5739 - sshd: configuration error (AuthorizedKeysCommand)
    Trying rule: 5740 - sshd: connection reset by peer
    Trying rule: 5741 - sshd: connection refused
    Trying rule: 5742 - sshd: connection timed out
    Trying rule: 5743 - sshd: no route to host
    Trying rule: 5744 - sshd: port forwarding issue
    Trying rule: 5745 - sshd: transport endpoint is not connected
    Trying rule: 5746 - sshd: get_remote_port failed
    Trying rule: 5749 - sshd: bad packet length
    Trying rule: 5715 - sshd: authentication success.
       *Rule 5715 matched.
       *Trying child rules.
    Trying rule: 40101 - System user successfully logged to the system.
    Trying rule: 40112 - Multiple authentication failures followed by a success.

**Phase 3: Completed filtering (rules).
       Rule id: '5715'
       Level: '3'
       Description: 'sshd: authentication success.'
**Alert to be generated.
```