

Some tenshi examples

Notes on pattern matching (regular expressions)

Match a single character:

- `.` matches any character
- `[abc]` matches `a`, `b` or `c` (exactly one character)
- `[0-9]` matches any digit, short for `[0123456789]`
- `[0-9a-z.]` matches 0-9 or a-z or a dot
- `\d` is another way to match any digit
- `\s` matches any white space character (space or tab)

Repeats:

- Following an item with `*` matches any number of times (zero or more)
- Following an item with `?` makes it optional (match zero or one times)
- Following an item with `+` makes it match one or more times

Position:

- `^` matches start of line
- `$` matches end of line

Grouping:

- `(...)` groups together part of a pattern, so `(...)?` makes the whole part optional
- `(xxx|yyy)` matches pattern `xxx` or `yyy`

Escaping:

- `\.` matches an actual dot
- `[.]` is another way to match an actual dot
- `\[` and `\]` match the actual characters `[` and `]`
- `\(` and `\)` match the actual characters `(` and `)`

Discarding messages

Discard messages matching particular patterns

Suppose we are not interested in the summary messages from nfcapd at all.

```
group ^nfcapd:
trash Total ignored packets
trash Ident:.*Flows:.*Packets:.*Bytes:.*Sequence Errors:.*Bad Packets
group_end
```

Another example:

```
group ^sshd:
trash ^sshd: Connection closed by.*\[preauth\]
trash ^sshd: Received disconnect from
trash ^sshd:.*from 10\.10\.0\.250
group_end
```

Discard messages from a specific host

Suppose we want to discard messages matching a particular pattern but only if they come from a particular host

```
group_host ^10\.10\.0\.254$
trash ^dhcpd:
trash ^charon:
trash ^filterlog:
trash ^check_reload_status: Reloading filter
trash ^check_reload_status: Restarting ipsec tunnels
trash ^check_reload_status: Restarting OpenVPN tunnels
trash ^check_reload_status: Syncing firewall
group_end
```

Summarising similar messages

If a pattern is match within parentheses '(...)' then it is removed, so that it may be combined with similar messages.

For example, suppose you get lots of messages like this:

```
1: sshd: Connection closed by 100.68.6.131 port 38060 [preauth]
1: sshd: Connection closed by 100.68.6.132 port 39308 [preauth]
1: sshd: Connection closed by 100.68.4.133 port 50620 [preauth]
1: sshd: Connection closed by 100.68.4.134 port 58252 [preauth]
```

and you want to combine them in a single summary line for tenshi. Try:

```
misc ^sshd: Connection closed by ([0-9.]+) port (\d+) \[preauth\]
```

Then you should get in your tenshi report:

```
4: sshd: Connection closed by port [preauth]
```