Telnet Inspector

Telnet Inspector Overview

Type	Inspector (service)
Usage	Inspect
Instance Type	Multiton
Other Inspectors Required	`stream_tcp`
Enabled	`false`

Telnet is an application layer protocol that creates an 8-bit byte communication channel over TCP. Telnet uses a network virtual terminal to communicate between a client and a remote host. A Telnet server uses TCP port 23.

The `telnet` inspector normalizes the Telnet data buffer by detecting the Telnet command sequences and option negotiation. The `telnet` inspector eliminates the Telnet command sequences (RFC 854) from the packet. The `telnet` inspector can detect encrypted Telnet connections by examining the Telnet encryption option (RFC 2946).

Telnet Inspector Parameters

Telnt service configuration

The `binder` inspector defines the telnet `service` configuration. For more information, see the Binder Inspector Overview.

Example:

```
[
    {
        "when": {
            "service": "telnet",
            "role": any
        },
        "use": {
            "type": "telnet"
        }
    }
]
```

ayt_attack_thresh

Specifies the maximum number of consecutive Are You There (AYT) telnet commands. The `telnet` inspector detects and alerts on the number of consecutive AYT commands that exceed the `ayt_attack_thresh` value. The `ayt_attack_thresh` parameter addresses specific vulnerabilities related to BSD implementations of telnet. Specify `-1` to disable the `ayt_attack_thresh` parameter. You can enable rule 126:1 to generate events and, in an inline deployment, drop offending packets for this parameter.

Type: integer

Valid range: `-1` to `2,147,483,647 (max31)`

Default value: `-1`

encrypted_traffic

Specifies whether to detect encrypted telnet traffic. You can enable rule 126:2 to generate events and, in an inline deployment, drop offending packets for this parameter.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

normalize

Specifies whether to normalize telnet traffic. The `telnet` inspector normalizes telnet traffic by eliminating telnet escape sequences. If an enabled intrusion rule specifies a `raw` content parameter, the rule ignores the normalized telnet buffer created by the `telnet` inspector.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

Telnet Inspector Rules

Enable the `telnet` inspector to generate events and, in an inline deployment, drop offending packets.

Table 1: Telnet Inspector Rules

GID:SID	Rule Message
126:1	consecutive Telnet AYT commands beyond threshold

GID:SID	Rule Message
126:2	Telnet traffic encrypted
126:3	Telnet subnegotiation begin command without subnegotiation end

Telnet Inspector Intrusion Rule Options

The `telnet` inspector does not have any intrusion rule options.