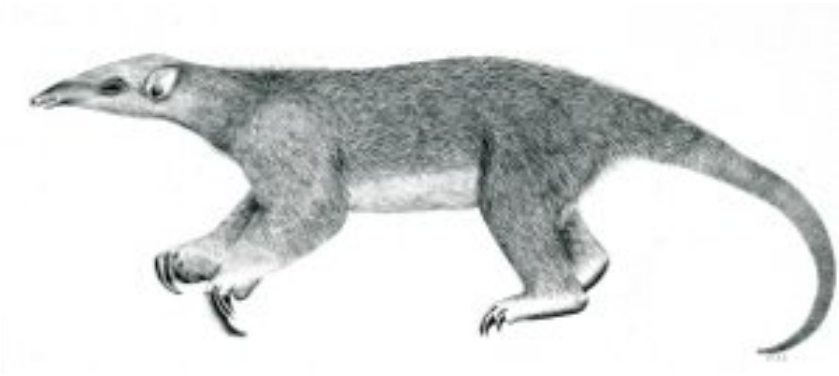
Tranalyzer2

vrrpDecode

Virtual Router Redundancy Protocol (VRRP)



Tranalyzer Development Team

Contents

1 vrrpDecode

1.1 Description

The vrrpDecode plugin analyzes Virtual Router Redundancy Protocol (VRRP) traffic.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
VRRP_NUM_VRID	5	number of unique virtual router ID to store	
VRRP_NUM_IP	25	number of unique IPs to store	
VRRP_RT	0	Whether (1) or not (0) to output routing tables	
VRRP_SUFFIX	"_vrrp.txt"	Suffix for routing tables file	VRRP_RT=1

1.3 Flow File Output

The vrrpDecode plugin outputs the following columns:

Column	Type	Description
vrrpStat	H16	Status
vrrpVer	H8	Version
vrrpType	H8	Type
vrrpVRIDCnt	U32	Virtual router ID count
vrrpVRID	RU8	Virtual router ID
vrrpMinPri	U8	Minimum priority
vrrpMaxPri	U8	Maximum priority
vrrpMinAdvInt	U8	Minimum advertisement interval [s]
vrrpMaxAdvInt	U8	Maximum advertisement interval [s]
vrrpAuthType	H8	Autentication type
vrrpAuth	SC	Authentication string
vrrpIPCnt	U32	IP address count
vrrpIP	R(IP)	IP addresses

1.3.1 vrrpStat

The vrrpStat column is to be interpreted as follows:

vrrpStat	Description
0x0001	flow is VRRP
0x0002	invalid version
0x0004	invalid type
0x0008	invalid checksum
0x0010	invalid TTL (should be 255)
0x0020	invalid destination IP (should be 224.0.0.18)

vrrpStat	Description
0x0040	invalid destination MAC (should be 00:00:5e:00:01:routerID)
0x0100	Virtual Router ID list truncated... increase VRRP_NUM_VRID
0x0200	IP list truncated... increase VRRP_NUM_IP
0x4000	Packet snapped
0x8000	Malformed packet... covert channel?

1.3.2 vrrpVer

The vrrpVer column is to be interpreted as follows:

vrrpVer	Description
0x04	VRRP v2
0x08	VRRP v3

1.3.3 vrrpType

The vrrpType column is to be interpreted as follows:

vrrpType	Description
0x01	Advertisement

1.3.4 vrrpAuthType

The vrrpAuthType column is to be interpreted as follows:

vrrpAuthType	Description
0x01	No authentication
0x02	Simple text password
0x04	IP Authentication Header

1.4 Additional Output

Non-standard output:

- PREFIX_vrrp.txt: VRRP routing tables

The routing tables contain the following columns:

Name	Description
VirtualRtrID	Virtual router ID
Priority	Priority
SkewTime[s]	Skew time (seconds)
MasterDownInterval[s]	Master down interval (seconds)
AddrCount	Number of addresses

Name	Description
Addresses	List of addresses
Version	VRRP version
Type	Message type
AdverInt[s]	Advertisement interval
AuthType	Authentication type
AuthString	Authentication string
Checksum	Stored checksum
CalcChecksum	Calculated checksum
flowIndex	Flow index

1.5 Plugin Report Output

The number of VRRP v2 and v3 packets is reported.

1.6 Post-Processing

The routing tables can be pruned by using the following command:

```
sort -u PREFIX_vrrp.txt > PREFIX_vrrp_pruned.txt
```