RITA

Real Intelligence Threat Analytics

CHEAT SHEET

This document is a quick reference guide to commonly used RITA commands and arguments. Additional RITA information and installation files can be found at: https://github.com/activecm/rita

CONFIGURATION

Command	Description
sudo nano /etc/rita/config.yaml	RITA configuration file.
rita test-config	Check the configuration file for validity.

INSTALLATION

Command	Description
sudo chmod +x ./install.sh	Make the install file executable.
sudo ./install.sh	Install RITA as well as supported versions of Zeek and MongoDB.
sudo ./install.sh --disable-zeek --disable-mongo	Install RITA only, without Zeek or MongoDB. You can use these flags individually.

IMPORTING AND ANALYZING DATA

Command	Description
mergecap -w *outfilename*.pcap *infilename1*.pcap *infilename2*.pcap	Merge multiple PCAP files into one PCAP file.
zeek -r *filename*.pcap local "Log::default_rotation_interval = 1 day"	Generate Zeek logs from a PCAP file.
rita import path/to/your/zeek_logs *datasetname*	One-off dataset import.
rita import --rolling /path/to/your/zeek_logs *datasetname*	Rolling datasets allow you to progressively analyze log data over a period of time.
/opt/zeek/logs/<date>	Default Zeek logs directory.

EXAMINING DATA

Command	Description
rita list	Print the datasets currently stored.
rita show-beacons -H *datasetname* | less -S	Print hosts which show signs of C2 software.
rita show-beacons-fqdn -H *datasetname* | less -S	Print hosts which show signs of C2 software (FQDN Analysis).
rita show-strobes -H *datasetname* | less -S	Print strobe (fast beacon) information.
rita show-long-connections -H *datasetname* | less -S	Print long connections and relevant information.
rita show-useragents -H *datasetname* | less -S	Print user agent information.
rita show-exploded-dns -H *datasetname* | less -S	Print DNS analysis. Exposes covert DNS channels.
rita show-bl-hostnames -H *datasetname* | less -S	Print blacklisted hostnames which received connections.
rita show-bl-source-ips -H *datasetname* | less -S	Print blacklisted IPs which initiated connections.
rita show-bl-dest-ips -H *datasetname* | less -S	Print blacklisted IPs which received connections.
rita html-report *datasetname*	Create an HTML report for an analyzed database.
rita delete *datasetname*	Delete database/dataset.

FILTERING RESULTS

Command	Description
rita show-beacons *datasetname* | grep -v -w -F -f exclude-beacons.txt	Place IP addresses to exclude in this text file, one per line.
rita show-strobes *datasetname* | grep -v -w -F -f exclude-strobes.txt	Place IP addresses to exclude in this text file, one per line.
rita show-long-connections *datasetname* | grep -v -w -F -f exclude-longconns.txt	Place IP addresses to exclude in this text file, one per line.
rita show-bl-hostnames *datasetname* | grep -v -w -F -f exclude-bl-hostnames.txt	Place IP addresses to exclude in this text file, one per line.
rita show-bl-source-ips *datasetname* | grep -v -w -F -f exclude-bl-source-ips.txt	Place IP addresses to exclude in this text file, one per line.
rita show-bl-dest-ips *datasetname* | grep -v -w -F -f exclude-bl-dest-ips.txt	Place IP addresses to exclude in this text file, one per line.