Fall 11-17-2023

Security Datasets for Network Research

Bruce Hartpence
Rochester Institute of Technology, bhhics@rit.edu

Bill Stackpole
Rochester Institute of Technology, wrsics@rit.edu

Daryl Johnson
Rochester Institute of Technology, daryl.johnson@rit.edu

Recommended Citation
https://doi.org/10.57673/gccis-qj60

This document describes the content of the security traffic datasets included in this collection and the conditions under which the packets were collected. These datasets were assembled from 2023 onward There are periodic updates or additions to the dataset collection.

Both text and pcap (pcapng) file types can be opened with Wireshark. When referencing these datasets, please use the following DOI:

Contact info: Bruce Hartpence bhhics@rit.edu

Daryl Johnson dgjics@rit.edu

Bill Stackpole wrsics@rit.edu

Current Datasets

The datasets beginning with "intense-scan" are nmap scans of a variety of targets including a Cisco router, Kali Linux VM, Rocky Linux VM, Windows Server 2022 VM and a Windows 10 host. The scan were run using the following command: nmap -p 1-65535 -T4 -A -v

The scan files are raw meaning that they are direct captures starting prior to the scan. As a result, the capture files include additional traffic from the small network housing the hosts and VMs.

Current nmap scan pcapng files:

intense-scan-target-2651-pcapng

intense-scan-target-kali.pcapng

intense-scan-target-rocky-linux.pcapng

intense-scan-target-winsvr-2022.pcapng

intense-scan-target-windows10.pcapng

Topology

The following topology depicts that nmap scanning machine and the targets. The number at the end of the display name indicates the last octet of the IP address for that node. For example, the nmap machine is 10.140.100.66