Understanding NetFlow: An Introductory Guide for Incident Responders

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-11-12

Introduction to NetFlow

NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network flow. It provides valuable data about network traffic patterns, usage, and communication behaviours, making it an indispensable tool for network administrators and security professionals.

How NetFlow Works

NetFlow operates by capturing data packets at network interfaces and extracting key information such as source/destination IP addresses, port numbers, protocol types, and packet and byte counts. This data is aggregated into flows, representing a sequence of packets sharing the same attributes traversing a network path.

NetFlow Collector and nfcapd

Role of a NetFlow Collector

A NetFlow collector is responsible for receiving, storing, and processing NetFlow data sent from routers and switches. The collector provides a centralized view of

nfcapd: A NetFlow Collector Daemon

nfcapd is part of the NFDUMP suite, a set of tools to collect and process NetFlow data. It acts as a collector daemon, capturing NetFlow data sent by routers and storing it in files for analysis.

Working Mechanism of nfcapd

Capturing NetFlow Data

nfcapd captures NetFlow data sent over the network from configured devices. It listens on a specified port for incoming NetFlow exports and processes them in near real-time.

File Storage and Rotation

nfcapd stores captured data in a binary file format, typically rotated on a time basis (e.g., every 5 minutes). Each file contains a sequence of NetFlow records, ensuring efficient storage and retrieval.

The nfcapd Capture File Format

Structure of nfcapd Files

nfcapd files are binary and consist of a file header, followed by flow records. Each flow record contains detailed information about individual flows, such as timestamps, IP addresses, port numbers, and byte counts.

Benefits of the Binary Format

The binary format of nfcapd files ensures compact storage and quick access, which is crucial for handling large volumes of NetFlow data.

Analysing nfcapd Output

Tools for Analysis

The NFDUMP suite, particularly **nfdump**, is the primary tool for analysing nfcapd files. It allows for filtering, sorting, and aggregating NetFlow data.

Command Line Usage

nfdump commands typically involve specifying the nfcapd file directory and applying filters. For example:

```
```

(*note, -R is used to point to a folder or directory of files, -r is used to point to a single file*)

Example Incident Response Investigations

Identifying Command and Control (C2) Beacons

C2 beacons might be identified by analysing regular, small-sized communication patterns to suspicious IPs. For instance,

```
```

This command filters flows from a specific IP address with small byte counts and then sorts the data to identify if any external addresses are being frequently contacted.

```
root@siftworkstation:/cases/netflow/netflow# nfdump -r netflow.nfcapd -o "fmt:%sa %da" 'src ip 91.189.94.4 and bytes < 200' | sort | uniq -c | sort -n
      1      Src IP Addr      Dst IP Addr
      1 Summary: total flows: 2221, total bytes: 337592, total packets: 4442, avg bps: 0, avg pps: 0, avg bpp: 76
      1 Sys: 0.041s flows/second: 35516234.7 Wall: 0.040s flows/second: 36284938.6
      1 Time window: 2019-11-10 01:53:01 - 2020-04-30 11:06:49
      1 Total flows processed: 1463553, Blocks skipped: 0, Bytes read: 87814268
    160      91.189.94.4     192.168.2.21
    165      91.189.94.4      192.168.1.4
    167      91.189.94.4      192.168.1.5
    646      91.189.94.4      192.168.1.3
   1083      91.189.94.4     192.168.2.20
```

Example nfdump output

This can also be used to help find out which (if any) devices an external party has gained access to.

Detecting Large Data Exfiltrations

To detect potential data exfiltration, look for large and unusual data transfers. A command like the one shown here helps identify flows where more than 1GB of data was transferred.

```
root@siftworkstation:/cases/netflow/netflow# nfdump -r netflow.nfcapd 'bytes > 1000000000' -o "fmt:%ts %sap %dap %byt"
Date first seen             Src IP Addr:Port       Dst IP Addr:Port     Bytes
2020-02-05 07:46:29.631   17.253.125.203:80        192.168.1.4:43810    1.6 G
2020-02-13 14:57:06.364      192.168.1.4:3128      192.168.2.18:52250   1.6 G
2020-02-22 14:16:59.303      192.168.1.2:3262      192.168.2.50:1611    2.1 G
2020-02-22 14:32:06.200      192.168.1.2:3262      192.168.2.50:1611    2.1 G
2020-02-22 17:40:52.152        10.0.1.13:3262      192.168.2.50:1712    2.1 G
2020-02-22 17:57:14.528        10.0.1.13:3262      192.168.2.50:1712    2.1 G
2020-02-27 13:02:30.535      192.168.1.5:22        192.168.2.51:49757   2.1 G
2020-02-27 13:33:04.944      192.168.1.5:22        192.168.2.51:49757   2.1 G
2020-02-27 13:47:44.956      192.168.1.5:22        192.168.2.51:49757   2.1 G
2020-02-27 14:03:28.250      192.168.1.5:22        192.168.2.51:49757   2.1 G
2020-02-27 14:17:48.378      192.168.1.5:22        192.168.2.51:49757   2.1 G
2020-02-27 14:52:44.859      192.168.1.5:22        192.168.2.51:49757   2.1 G
2020-02-27 15:08:24.599      192.168.1.5:22        192.168.2.51:49757   2.1 G
Summary: total flows: 13, total bytes: 26.8 G, total packets: 3.0 M, avg bps: 111263, avg pps: 1, avg bpp: 8855
Time window: 2019-11-10 01:53:01 - 2020-04-30 11:06:49
Total flows processed: 1463553, Blocks skipped: 0, Bytes read: 87814268
Sys: 0.035s flows/second: 41488632.5 Wall: 0.033s flows/second: 43213446.3
```

Example nfdump output showing very large data transfers

Advanced Analysis Techniques

Time Series Analysis

For more sophisticated investigations, time series analysis of NetFlow data can reveal trends and anomalies over time, aiding in the detection of slow and stealthy attacks. It can also be very effective to look for anomalies, such as an internal host that is reaching out to an external address every few minutes (this may indicate a C2 channel).

Integration with Other Tools

Integrating NetFlow data with other security tools, like SIEMs, enhances the context and accuracy of incident response investigations.

Summary

NetFlow, with tools like nfcapd and nfdump, provides a powerful mechanism for monitoring network traffic and aiding in incident response. Through effective analysis of NetFlow data, security professionals can detect and respond to a wide range of network threats, from C2 beacons to data exfiltration attempts. As network complexities grow, mastering NetFlow analysis in incident response becomes increasingly critical.

This LinkedIn article is a very short, basic, introduction to give some ideas and remind people that this great source of information exists. If you want to learn more about how to analyse netflow data during IR properly, then have a look at the amazing SANS Institute course **FOR572 "Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response"** by Phil Hagen. You can find out more about the course at https://sans.org/for572

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858