SIT327 - Network Forensics

Pass Task 2: Flow Record Analysis Task

Overview

This task involves utilizing Nfsdump and Argus to analyze firewall and flow records for insights into an attack incident. Begin by setting up nfsdump and Argus on your system.

Listing 1: Install Instructions

```
wget http://sourceforge.net/projects/nfdump/files/nsel/nfdump-1.5.8-NSEL/nfdump
    -1.5.8-NSEL.tar.gz/download

tar xzf download

replace .c and .h files
apt-get install bison flex
apt-get install rrdtool
apt-get install librrd-dev
apt-get install argus-client

./configure --enable-nfprofile
make
make install
```

First, obtain the modified .c and .h files. Following that, proceed with the installation of these tools using the provided commands.

At this point you should be able to view the nfsdump firewall logs. Type

```
nfdump -R cisco-asa-nfcapd/
```

Report Submission:

Submit a report containing

- A screenshot of the commands used to build the project.
- A screenshot displaying the logs