Lab 08 – Compromise Investigation

Overview

We've talked about a great number of tools, from GUI based tools to CLI based tools to IDSs and their interfaces. A pcap file is being provided for you to investigate. Your job is to investigate and provide a write-up of what has happened on the network. You may use any of the tools we've talked about, or even some we haven't if you'd like.

To get the pcap in the IDS tools, run the following command:

```
sudo tcpreplay -ieth1 -M10 lab08.pcap
```

If no results show up you can also use (This one works best):

```
sudo so-import-pcap lab08.pcap
```

Note: Be sure you're only looking at data generated from this pcap! If you use the `tcpreplay` method the time of the packets will be shown as when the `tcpreplay` was ran, if you use `so-import-pcap` the time will be when the pcap was originally taken

Network Background

The network includes a server and desktop machine, along with supporting networking equipment. The intent was for this to be an isolated test network, but that clearly was not the case – the network may have been compromised, exposing the company to additional risk.

Deliverable

A write-up of your findings. Tell me all the details you can about what happened on the network. Was anyone compromised? How so? Include screenshots as evidence where appropriate.