Packet Capture Specification

James Nicholls / Clockwork Dragon group

March 10, 2013

This document provides a specification and index of the CSV files which are in use as test data for the network visualisation application NetVis.

1 File format specification

All capture files are provided to the application as CSV files with the following headers;

- `No.` Packet number
- `Time` Time elapsed since first packet (seconds)
- `Source IP` Source IPv4/6 address
- `Source HW` Source hardware (MAC) address
- `Source Port` Source Port
- `Dest IP` Destination IPv4/6 address
- `Dest HW` Destination hardware (MAC) address
- `Dest Port` Destination Port
- `Protocol` Communication protocol
- `Length` Packet length (bytes)
- `Info` Detected description of packet purpose

2 Sources

Notable external sources of packet trace (pcap) files.

- `https://www.evilfingers.com/`
  A community portal for Information Security, who publish internet security papers and keep a public archive of PCAP samples, among other resources.
- `http://www.honeynet.org/`
  The Honeynet Project is a leading international 501c3 non-profit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security.

3 Capture files

This section comprises a list of CSV files currently in use in application development and testing, as well as a short description of each.

3.1 eduroam.csv

Source: J. Nicholls
Original filename: `eduroam.pcap`
Size: 85664 packets - 16.4 MB

All traffic seen by an Ubuntu laptop with minimal running services, connected to the Eduroam network on the wlan0 interface. Approximately 85000 packets over 35 minutes.

3.2 jre-overflow.csv

Source: `https://www.evilfingers.com/`
Original filename:
`Sun_jre1.6.0_X_isInstalled.dnsResolve_Function_Overflow_PoC.pcap`
Size: 65561 packets - 14.7 MB

Proof-of-concept packet capture of a denial of service attack on JRE 1.6.0 by exploiting the DNS resolution function. A local server is flooded with 65000 packets in 11 minutes.

3.3 port-scan.csv

Source: J. Happa
Original filename: `portscan.pcap`
Size: 1818 packets - 371 kB

A port scan of a Windows Vista PC, originating from an Ubuntu PC, concluding that only port 80 (http) is open.

3.4 remote-execution.csv

Source: `http://www.honeynet.org/`
Original filename: `attack-trace.pcap_.gz`
Size: 348 packets - 53.6 kB

Packet trace of a malware attack which distributes a payload exploiting the Windows Local Security Authority (LSA) Remote Procedure Call (RPC) service of the victim host, compromising the IPC$ share. Once the share is exploited, a script is invoked, causing a connection to an FTP server named NzmxFtpd and the acquisition of an infected executable, `ssms.exe`.

3.5 skype.csv

Source: J. Nicholls
Original filename: `skype.pcap`
Size: 418 packets - 73 kB

Packets transferred during the authentication and initialisation of a Skype session. Recorded on an Ubuntu PC with minimal services running.

3.6 ssh-attack.csv

Source: `http://www.honeynet.org/`
Original filename: `hp_challenge.pcap`
Size: 5447 packets - 951.2 kB

Packet trace of an intruder gaining access to a server using a brute-force attack via SSH, before planting malware to download and execute software on the compromised host.

3.7 telnet-freebsd-exploit.csv

Source: `http://www.honeynet.org/`
Original filename: `fc.pcap`
Size: 238 packets - 35.2 kB

Demonstration of a buffer overflow exploit (CVE-2011-4862) that allows arbitrary code execution on a vulnerable FreeBSD server via telnet.

3.8 ubuntu-update.csv

Source: J. Happa
Original filename: `ubuntu-update.pcap`
Size: 497 packets - 84.6 kB

Packet trace of an Ubuntu PC communicating with a Canonical server to check for software updates. No new updates were found or downloaded.