TCPReplay

Analysis of options for feasibility report:

Considerations:

List of Programming Languages options as basis of our project:
-C/C++(+)
-Java(-)
-Phyton(+)
-Perl(-)

Operating System: Kali Linux (2018.2). (Taken from the Kali Linux official documentation website).

Advantages:

-Kali Linux is specifically geared to meet the requirements of professional penetration testing and security auditing. No extra layer of security needed.
-Kali Linux contains systemd hooks that disable network services by default. (No need to develop more algorithms to keep the implementation safe).
-**Custom Linux kernel:** Kali Linux uses an upstream kernel, patched for wireless injection.
-**A** *minimal* **and** *trusted* **set of repositories:** given the aims and goals of Kali Linux, maintaining the integrity of the system as a whole is absolutely key. With that goal in mind, the set of upstream software sources which Kali uses is kept to an absolute minimum. Many new Kali users are tempted to add additional repositories to their **sources.list**, but doing so runs a *very serious risk* of breaking your Kali Linux installation.

Disadvantages:

-While Kali Linux is architected to be highly customizable, don't expect to be able to add random unrelated packages and repositories that are "out of band" of the regular Kali software sources and have it Just Work. In particular, there is absolutely no support whatsoever for the apt-add-repository command, LaunchPad(repository service), or PPAs. Trying to install *Steam* on your Kali Linux desktop is an experiment that will not end well. Even getting a package as mainstream as NodeJS onto a Kali Linux installation can take a little extra effort and tinkering.
-Learning curve in relation to the number of elements of the system that ought to be learned before doing anything with the operating system.

General Consideration of the programming language that should act as a basis for the project:

In a December 2014 survey, readers of Linux Journal placed Python at the top of their list of best programming languages (30.2 percent), followed by C++ (17.8 percent), C (16.7 percent), Perl (7.1 percent), and Java (6.9 percent)

Possible Solutions:

Solution 1. Burpsuite

Elements of the Proxy:

Graphical User Interface:

GUI				
Based on our decision for what programming language should be the basis of our project.				

Network Sniffers:

Network Sniffers (Packet Analyzer)	Advantages	Disadvantages	Language	Extra
Wireshark	-Same as Tshark(3) -Scripting/ Automation is possible by using Lua scripting language.(4)	GUI Based execution. (3)	C/C++	Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.
Tshark	-Command Line Based. (3)		C/C++	

tcpdump	-You can write to PCAP files directly.(1) -All protocols are supported. (1) -Command Line Based. (2)	Limited, less filtering options are available	C	tcpcdump uses the libpcap library

Fuzzers:

Fuzzers	Advantages	Disadvantages	
AFL	Same as Tshark(3)	GUI Based execution. (3)	
Scapy	Command Line Based. (3)		

Links:
(1) https://danielmiessler.com/study/tcpdump/#protocol
(2) http://www.tcpdump.org
(3) https://www.networkcomputing.com/networking/wireshark-packet-capture-tshark-vs-dumpcap/1149900924
(4) https://www.ibm.com/developerworks/community/blogs/kevgrig/entry/wireshark_automation_with_lua_scripting?lang=en
(5) https://en.wikipedia.org/wiki/Scapy
(6) https://scapy.net
(7) https://pythonistac.wordpress.com/2017/03/09/python-network-packet-dissection-frameworks-shootout-scapy-vs-construct-vs-hachoir-vs-kaitai-struct/

Scapy	-Interface constructed to use the elements of the libpcap library. (5) -Command Line based -Extremmely Versatile (6)		Phyton	-Scapy uses the libpcap library -It can act as tcpdump

(8) http://yuba.stanford.edu/~casado/pcap/section1.html
(9) https://media.readthedocs.org/pdf/markdown222/latest/markdown222.pdf
(10) https://wiki.wireshark.org/Tools#Traffic_generators

Extra Resources:
(1) http://recursos.aldabaknocking.com/libpcapHakin9LuisMartinGarcia.pdf
(2) http://www.tcpdump.org/manpages/pcap.3pcap.html
(3) http://www.tcpdump.org/pcap.html

https://www.paessler.com/packet_sniffing
(Look for . The software or device used for capturing packet data is called *packet sniffer*, *packet analyzer, network sniffer* or simply *network analyzer*.)