Boofuzz

Excuse the ads! We need some help to keep our site up.

List

Boofuzz

- **Boofuzz는 Network Protocol Fuzzing framework 입니다.**
- **Boofuzz는 Sully fuzzing framework의 후속 모델입니다.**
- **Boofuzz는 Sully의 중요한 요소를 모두 포함하고 있습니다.**
  - 쉽고 빠른 데이터 생성
  - 계측 - 일명 고장 탐지
  - 실패 후 대상 재설정
  - 테스트 데이터 기록
- **Boofuzz는 다음과 같이 Sully와 다른 기능도 제공합니다.**
  - 쉬운 설치
  - 임의의 통신 매체 지원
  - 시리얼 퍼징, 이더넷 및 IP 계층, UDP 브로드 캐스트를 지원
  - 테스트 데이터를 일관되고 철저하고 명확하게 기록합니다.
  - 테스트 결과 CSV로 내보내기.
  - 확장 가능한 계측 및 고장 감지

Install

Command
`pip install boofuzz`

> **Install**
>
> - http://boofuzz.readthedocs.io/en/latest/index.html#installation

API

- http://boofuzz.readthedocs.io/en/latest/index.html#api-documentation

Example

Install vsftpd.

Command

```
sudo apt-get install vsftpd
```

Run fuzz

Source code

https://raw.githubusercontent.com/jtpereyda/boofuzz-ftp/master/ftp.py

```
#!/usr/bin/env python
# Designed for use with boofuzz v0.0.1-dev3
from boofuzz import *

def main():
    session = Session(
        target=Target(
            connection=SocketConnection("127.0.0.1", 21, proto='tcp')))

    s_initialize("user")
    s_string("USER")
    s_delim(" ")
    s_string("anonymous")
    s_static("\r\n")

    s_initialize("pass")
    s_string("PASS")
    s_delim(" ")
    s_string("james")
    s_static("\r\n")

    s_initialize("stor")
    s_string("STOR")
    s_delim(" ")
    s_string("AAAA")
    s_static("\r\n")

    s_initialize("retr")
    s_string("RETR")
    s_delim(" ")
    s_string("AAAA")
    s_static("\r\n")

    session.connect(s_get("user"))
    session.connect(s_get("user"), s_get("pass"))
    session.connect(s_get("pass"), s_get("stor"))
    session.connect(s_get("pass"), s_get("retr"))

    session.fuzz()

if __name__ == "__main__":
    main()
```

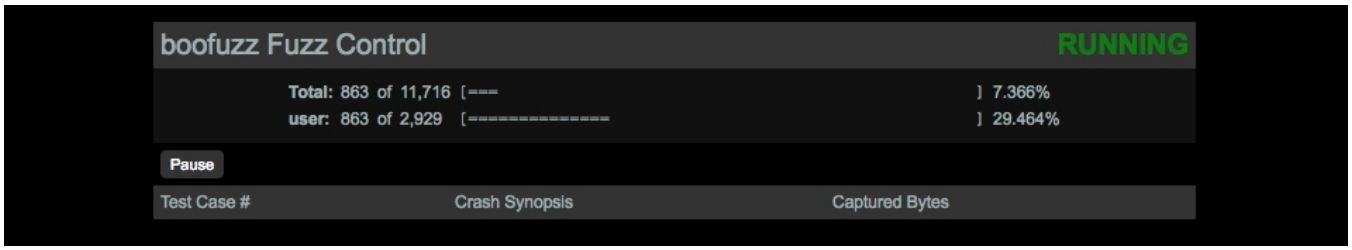
Run

Command

```
python ftp.py > fuzz-logs.txt
```

Web

http://127.0.0.1:26000/



- https://github.com/jtpereyda/boofuzz-ftp
- https://github.com/jtpereyda/boofuzz-http

Related site

- http://boofuzz.readthedocs.io/en/latest/