Fuzz Testing Results & Analysis

Charger Active Defense – G12

Noah Sickels, Adam Brannon, William Lochte

**Background**

Table 1: Relevant Tools & Targets

|  |  |  |
| --- | --- | --- |
| Tool | Version | Use case |
| AFLnet (AFLplusplus) | 4.21c | Network Protocol Fuzzing |
| Fuzzowski | 0.8.2 | Network Protocol Fuzzing |
| Scapy | 2.6.0 | Pcap Traffic Generation |
| Radamsa | 0.7 | Network Protocol Fuzzing |
| Randpkt | 4.4.1 | Pcap Traffic Generation |
| Peach Fuzzer | 4.3 | Network Protocol Fuzzing |
| Medusa | 2.2 | Attack Tool Target 1 |
| Masscan | 1.3.2 | Attack Tool Target 2 |

**AFLnet (AFLplusplus)**

**Fuzzowski**

**Scapy**

**Radamsa**

**Randpkt**

**Peach Fuzzer**

**Conclusion**

**References**

[1] Kali, “Kali Tools | Kali Linux Tools,” *Kali Linux*. https://www.kali.org/tools/

‌

[2] “Debian Security Tools Packaging Team / medusa · GitLab,” *GitLab*, 2018. https://salsa.debian.org/pkg-security-team/medusa (accessed Oct. 27, 2024).

‌ [3] R. D. Graham, “robertdavidgraham/masscan,” *GitHub*, Oct. 31, 2020. <https://github.com/robertdavidgraham/masscan>

[4] “Debian Security Tools Packaging Team / reaver · GitLab,” *GitLab*, 2023. https://salsa.debian.org/pkg-security-team/reaver (accessed Oct. 27, 2024).

[5] aflnet, “AFLNet: A Greybox Fuzzer for Network Protocols,” *GitHub*, Oct. 01, 2023. https://github.com/aflnet/aflnet

‌

[6] nccgroup, “GitHub - nccgroup/fuzzowski: the Network Protocol Fuzzer that we will want to use.,” *GitHub*, 2019. https://github.com/nccgroup/fuzzowski/tree/master (accessed Oct. 31, 2024).

‌

[7] “Scapy,” *GitHub*, Aug. 10, 2022. https://github.com/secdev/scapy

‌

[8] “Aki Helin / radamsa · GitLab,” *GitLab*, 2024. <https://gitlab.com/akihe/radamsa/> (accessed Oct. 27, 2024).

[9] “Wireshark Foundation / Wireshark · GitLab,” *GitLab*, 2024. https://gitlab.com/wireshark/wireshark (accessed Oct. 27, 2024).

‌

[10] “randpktdump(1),” *Wireshark.org*, 2024. <https://www.wireshark.org/docs/man->pages/randpktdump.html (accessed Oct. 27, 2024).

[11] “Files · main · GitLab.org / security-products / protocol-fuzzer-ce · GitLab,” *GitLab*, 2024. https://gitlab.com/gitlab-org/security-products/protocol-fuzzer-ce/-/tree/main?ref\_type=heads (accessed Oct. 27, 2024).

[12] “Peach Fuzzer,” *peachtech.gitlab.io*. <https://peachtech.gitlab.io/peach-fuzzer-community/>

**Appendix**

Table 2: Testbed Configuration

|  |  |  |
| --- | --- | --- |
| Component | Configuration |  |
| Hypervisor | VirtualBox | 7.1.0 |
| Virtual Machine 1 (Host) | OS | Kali Linux 2024.3 |
| Kernel Version | Linux kali 6.10.11-amd64 |
| GCC Version | 14.2.0 (Debian 14.2.0-3) |
| Network Adapter 1 | NAT |
| Network Adapter 2 | Internal Network *(intent)* |
| IP Address | 192.168.1.99 /24 |
| Miscellaneous | 16,384 MB RAM, 2 CPU cores, 80 GB HDD |
| Virtual Machine 2 (Target) | OS | Metasploitable2 |
| Kernel Version | Linux Metasploitable 2.6.24-16-server |
| GCC Version | 4.2.4 (Ubuntu 4.2.4-lubuntu4) |
| Network Adapter 1 | Internal Network *(intent)* |
| Network Adapter 2 | *Optional* |
| IP Address | 192.168.1.100 /24 |
| Miscellaneous | 2,048 MB RAM, 1 CPU core, 8 GB HDD |