2017 年 12 月 7 日，星期四

Mutiny 模糊测试框架和 Decept 代理

作者：思科 ASIG 小组的 James Spadaro 和思科 Talos 团队的 Lilith Wyatt

假设您是一名漏洞研究人员，负责检查网络应用以识别漏洞。这项工作本身看起来不太难，但您发现了一些情况和限制：您不太了解网络应用和协议的运行信息，也没有多少时间亲自执行评估。您会怎么做？

在这些情况下，搜索和识别网络应用中的漏洞可能是一项艰巨的任务。此时，研究人员可以使用模糊测试方法，高效地测试软件并找出漏洞。然而，接下来的问题是，如何快速高效地进行模糊测试？

答案是使用 Mutiny 模糊测试框架和 Decept 代理。

MUTINY 模糊测试框架

Mutiny 模糊测试框架是一种网络模糊测试程序，通过重播网络流量执行变异型模糊测试。其目标是尽快开始网络模糊测试，尽管结果会不够彻底。

在较高级别，Mutiny 可以抽取经过准备并格式化为 .fuzzer 文件的合法流量样本（例如浏览器请求）。然后可以用这个 .fuzzer 文件运行 Mutiny，生成针对目标主机的流量，转化用户想要转化的任何数据包。您还可以扩展和配置 Mutiny，使其执行不同的行为，例如根据输入/输出更改消息，指定如何处理网络错误，以及在单独的线程中监视目标主机。

对于明文流量，Mutiny 使用起来很简单，但是它本身不支持 TLS 或其他各种网络协议。这时候便需要使用 Decept 代理。它不仅可以简化对加密流量的捕获和模糊测试，而且可以为 Mutiny 执行单步式流量捕获和处理。

DECEPT 代理

Decept 代理是一个多功能网络代理，可以将明文或通过传输层安全协议 (TLS) 保护的 TCP/UDP/DTLS/ 域套接字连接转发至另一个明文或通过 TLS 保护的套接字连接。它是 Mutiny 的一款良好配套工具，不仅可以直接生成 .fuzzer 文件，而且在对 TLS 连接进行模糊测试时尤其有用，让 Mutiny 可以与 TLS 主机通信。

Decept 代理与其他各种代理的不同之处在哪里？

- 它支持 TLS 终端、IPv6、Unix 套接字、抽象命名空间套接字、L3 协议/捕获，以及 L2 桥接和被动模式。
- 它可以执行 SSH 代理/嗅探/过滤。
- 它的设计考虑了可移植性，而且使用的全是标准 python 库。只要您想运行 Decept 代理的系统安装了 Python 2，它应该就可以运行。

Decept 代理以 Justin Seitz 所著的《Black Hat Python》中的 TCP proxy.py 为基础。

DECEPT 代理和 MUTINY 的实际运用

思科将 Mutiny 模糊测试框架和 Decept 代理视为一个有效的工具集，将其用于评估各种网络应用和设备。其中包括很多思科设备，思科根据网络模糊测试发现的缺陷和漏洞，加固了这些设备。Mutiny 模糊测试框架和 Decept 代理发挥重要作用的其他示例包括：

- CVE-2014-7815，QEMU 中的一种拒绝服务漏洞。
- TALOS-2017-0439，Tinysvcmdns 中的一种堆溢出漏洞，对 Circle with Disney 设备有影响。
- 已可靠地发布的几种 VMware 产品漏洞。

在哪里可以找到这两种工具

Talos 团队正在以开源工具的形式发布 Mutiny 模糊测试框架和 Decept 代理。这两种工具由我们积极维护，欢迎社区对其功能提出任何改进意见。请注意，这两种工具按其原样提供，没有正式支持。用户自行承担使用这两种工具的所有责任。

您可以点击下面的链接，在 GitHub 上找到 Mutiny 模糊测试框架。请注意，Mutiny 模糊测试框架有若干开发分支，希望运行稳定版本的用户应该使用其主分支。实验分支包含较新的功能，但是对于正常使用可能不够稳定。

Mutiny 模糊测试框架：
https://github.com/Cisco-Talos/mutiny-fuzzer

您可以点击以下链接，在 GitHub 上找到 Decept 代理：
https://github.com/Cisco-Talos/Decept

发布者：ALEXANDER CHIU；发布时间：13:06
标签：DECEPT 代理、模糊测试、MUTINY 模糊测试框架