SWRhapsody

Tcpdump Cheat Sheet

于4月 4, 2018由**SWRhapsody**发布

在 PWK 的 lab 中遇到了 Wireshark 不方便获取链路层数据包的问题，收集一些 Tcpdump 的 cheat sheet.

列出 tcpdump 可以抓取的接口

```
1 tcpdump -D
```

对某一个接口进行监听

```
1 tcpdump -i eth0
2 tcpdump -i any
```

开启verbose

```
1 tcpdump -v
2 tcpdump -vv
3 tcpdump -vvv
```

开启verbose并同时以ASCII和Hex形式打印出每个包的数据，不包括链路层头

```
1 tcpdump -v -X
```

开启verbose并同时以ASCII和Hex形式打印出每个包的数据，包括链路层头

```
1 tcpdump -v -XX
```

让抓取时打印出来的信息更加简略些(和正常即不加 -X 选项相比)

```
1 tcpdump -q
```

限制抓取的数量

```
1 tcpdump -c 100
```

将抓取结果保存到文件

SWRhapsody

```
tcpdump -v -w capture.cap
```

在抓取时打印出 ip 和端口而不是域名

```
tcpdump -n
tcpdump -nn
```

根据目的地或来源筛选抓取的包

```
tcpdump -n dst host 192.168.1.1
tcpdump -n src host 192.168.1.1
tcpdump -n host 192.168.1.1

tcpdump -n dst net 192.168.1.0/24
tcpdump -n src net 192.168.1.0/24
tcpdump -n net 192.168.1.0/24

tcpdump -n dst port 23
tcpdump -n dst portrange 1-1023
```

限定抓取 tcp 包或 udp 的包

```
tcpdump -n tcp dst portrange 1-1023
tcpdump -n udp dst portrange 1-1023
```

多个筛选条件

```
tcpdump -n "dst host 192.168.1.1 and dst port 23"
tcpdump -n "dst host 192.168.1.1 and (dst port 80 or dst port 443)"
```

只抓特定种类的包

```
tcpdump -v icmp
tcpdump -v arp
tcpdump -v "icmp or arp"
```

参考或来源：

[1] Tcpdump usage examples：https://www.rationallyparanoid.com/articles/tcpdump.html

分类： CHEAT SHEET PENETRATION TEST

SWRhapsody

0 条评论

发表评论

名称 *

电子邮件 *

网站

在想些什么?

发表评论

近期文章

携程Apollo YAML 反序列化

CVE-2020-5410

CodeQL部分源码简读

服务器与网关的不一致

CodeQL 部分使用记录

SWRhapsody

文章归档

2020年8月

2020年6月

2020年5月

2020年3月

2020年1月

2019年12月

2019年11月

2019年8月

2019年7月

2019年5月

2019年4月

2019年1月

2018年11月

2018年10月

2018年9月

2018年4月

2018年3月

2018年2月

2018年1月

分类目录

Article Collection

Cheat Sheet

SWRhapsody

Exploit

HackTheBox

Penetration Test

Uncategorized

相关文章

PENETRATION TEST

服务器与网关的不一致

前言 一次渗透测试时遇到的，官方认为不是漏洞。 Code 遇到了大约这 阅读更多…

CHEAT SHEET

CodeQL 部分使用记录

前言 CodeQL 是一个代码分析引擎，主要原理是通过对代码进行构建并 阅读更多…

CHEAT SHEET

Wpscan

SWRhapsody

ABOUT

Hestia |由ThemeIsle开发