IPv6 三个小Tips

最近发现家里宽带支持IPv6了，这里分享三个利用IPv6访问本地地址（内网地址）的方法。

通常来说，我们用localhost来代表本地地址`127.0.0.1`。其实在IPv6中有他自己的表示方法`ip6-localhost`：

```
$ ping6 -c 4 ip6-localhost
PING ip6-localhost(ip6-localhost) 56 data bytes
64 bytes from ip6-localhost: icmp_seq=1 ttl=64 time=0.051 ms
64 bytes from ip6-localhost: icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from ip6-localhost: icmp_seq=3 ttl=64 time=0.063 ms
64 bytes from ip6-localhost: icmp_seq=4 ttl=64 time=0.064 ms

--- ip6-localhost ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.051/0.060/0.064/0.005 ms
```

另外，大家应该都知道xip.io这个服务，可以将任何IP地址用域名的形式表示，用来测试SSRF漏洞比较方便。但xip.io只支持IPv4，IPv6下也有个类似的服务，ip6.name。

比如，我们可以通过`x.1.ip6.name`访问`::1`，也就是本地：

```
# root @
$ ping6 -c 4 x.1.ip6.name
PING x.1.ip6.name(ip6-localhost) 56 data bytes
64 bytes from ip6-localhost: icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from ip6-localhost: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from ip6-localhost: icmp_seq=3 ttl=64 time=0.051 ms
64 bytes from ip6-localhost: icmp_seq=4 ttl=64 time=0.083 ms

--- x.1.ip6.name ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3078ms
rtt min/avg/max/mdev = 0.026/0.053/0.083/0.021 ms

# root @
$ dig +short -t AAAA x.1.ip6.name
0.0.0.0.0.0.0.1.ip6.name.
::1
```

再分享一个Windows下有趣的冷知识吧。

UNC Path是Windows中访问共享资源的方法，前段时间代码审计圈子里还分享过PHP利用UNC、WebDAV来包含远程文件的方法：https://t.zsxq.com/fUjiMfY

而UNC Path是不支持冒号的，所以我们没法在UNC Path中使用IPv6地址：`\\[fe80::2]\share`。所以微软官方想了一个歪招，他们注册了一个域名`ipv6-literal.net`，然后在Windows系统中，将IPv6地址中的冒号换成横线作为`ipv6-literal.net`子域名，如`2408-8207-1850-2a60--4c8.ipv6-literal.net`。

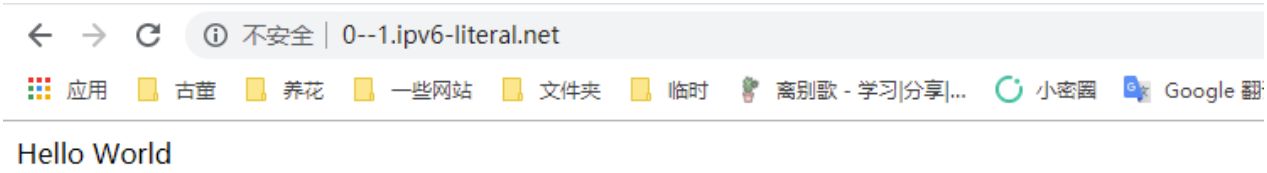
通过这个域名即可访问到对应的IPv6目标：

```
C:\Users
λ ping 2408:8207:1850:2a60::4c8

正在 Ping 2408:8207:1850:2a60::4c8 具有 32 字节的数据:
来自 2408:8207:1850:2a60::4c8 的回复: 时间=1ms
来自 2408:8207:1850:2a60::4c8 的回复: 时间=2ms
来自 2408:8207:1850:2a60::4c8 的回复: 时间=6ms
来自 2408:8207:1850:2a60::4c8 的回复: 时间=1ms

2408:8207:1850:2a60::4c8 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 6ms, 平均 = 2ms

C:\Users
λ ping 2408-8207-1850-2a60--4c8.ipv6-literal.net

正在 Ping 2408:8207:1850:2a60::4c8 具有 32 字节的数据:
来自 2408:8207:1850:2a60::4c8 的回复: 时间<1ms
来自 2408:8207:1850:2a60::4c8 的回复: 时间=4ms
来自 2408:8207:1850:2a60::4c8 的回复: 时间=1ms
来自 2408:8207:1850:2a60::4c8 的回复: 时间=1ms

2408:8207:1850:2a60::4c8 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 4ms, 平均 = 1ms
```

这就类似于微软官方推出的一个ip6.name服务。

但是，有趣的是，这里和ip6.name、xip.io有一个很大的区别，我们访问`2408-8207-1850-2a60--4c8.ipv6-literal.net`的时候，系统是不会真正发送DNS请求的，这个域名仿佛内置在Windows操作系统中，与生俱来就存在。

所以，你会发现，其实`ipv6-literal.net`这个域名微软早就已经不续费了（现在的所有者是Godaddy），但我们仍然可以直接在浏览器里通过`0--1.ipv6-literal.net`来访问到`::1`，也就是我本地：



所以在SSRF等漏洞的测试中，我们不妨利用一下上述三个URL技巧，尝试绕过一些限制。