专注APT攻击与防御
https://micropoor.blogspot.com/

连载2：
在上一篇连载中讲到powershell可无缝来调.net framework。而在实战中，内网的代理尤其重要，如常见的端口转发被反病毒软件盯死。本章无图，其他同学如有环境测试，可补图。

介绍github：
https://raw.githubusercontent.com/p3nt4/Invoke-SocksProxy/master/Invoke-SocksProxy.psm1

Examples

Create a Socks 4/5 proxy on port 1234:

```
Import-Module .\Invoke-SocksProxy.psm1
Invoke-SocksProxy -bindPort 1234
```

Create a simple tcp port forward:

```
Import-Module .\Invoke-SocksProxy.psm1
Invoke-PortFwd -bindPort 33389 -destHost 127.0.0.1 -destPort 3389
```

可目前过大部分反病毒软件。

- Micropoor