# **IMPULSE 脉冲**

## **现代拒绝服务工具包**

# **方法：**

| **方法** | **目标** | **描述** |
| --- | --- | --- |
| 短信 | 电话 | 向单个目标发送大量的SMS消息和呼叫 |
| 电子邮件 | 电子邮件 | 向目标发送大量电子邮件 |
| NTP | IP：端口 | NTP放大是一种分布式拒绝服务（DDoS）攻击，在这种攻击中，攻击者利用公共可访问的网络时间协议（NTP）服务器来压倒目标用户数据报协议（UDP）流量。 |
| 同步 | IP：端口 | SYN泛洪（半开放式攻击）是一种拒绝服务（DDoS）攻击，旨在通过消耗所有可用的服务器资源来使服务器无法用于合法流量。 |
| UDP协议 | IP：端口 | UDP泛洪是一种拒绝服务攻击，其中大量用户数据报协议（UDP）数据包发送到目标服务器，目的是压倒该设备的处理和响应能力。由于UDP泛洪，保护目标服务器的防火墙也可能会用尽，从而导致对合法流量的拒绝服务。 |
| POD（死亡之屏） | 知识产权 | Ping of Death（aka PoD）是一种拒绝服务（DoS）攻击，攻击者使用简单的ping命令通过发送格式错误或过大的数据包来尝试使目标计算机或服务崩溃，不稳定或冻结。 |
| ICMP | IP：端口 | Ping泛洪，也称为ICMP泛洪，是一种常见的拒绝服务（DoS）攻击，攻击者通过用ICMP回显请求（也称为ping）压倒受害者的计算机来关闭受害者的计算机。 |
| HTTP | 网址 | HTTP Flood是一种分布式拒绝服务（DDoS）攻击，其中，攻击者操纵HTTP和POST不需要的请求以攻击Web服务器或应用程序。这些攻击通常使用互连的计算机，这些计算机已经借助Trojan Horses等恶意软件来接管。 |
| Slowloris | IP：端口 | Slowloris是一种拒绝服务攻击程序，通过打开并维护攻击者与目标之间的许多同时HTTP连接，攻击者可以使目标服务器不堪重负。 |
| 记忆快取 | IP：端口 | 内存缓存的分布式拒绝服务（DDoS）攻击是一种网络攻击，攻击者试图使目标受害者的互联网流量超载。攻击者将请求欺骗到易受攻击的UDP memcached \*服务器，然后该服务器将Internet通信量泛洪到目标受害者，从而可能淹没受害者的资源。当目标的Internet基础结构过载时，无法处理新请求，并且常规流量无法访问Internet资源，从而导致拒绝服务。 |

# **安装：**

* + 安装Python 3.8
  + 启动安装程序，单击 add python to PATH
  + 下载脉冲
  + 在Impulse目录中打开cmd或powershell
  + 运行以下命令： pip install -r requirements.txt
  + 和这个： python impulse.py --help

Linux：

* + sudo apt update
  + sudo apt install python3 python3-pip git -y
  + git clone https://github.com/LimerBoy/Impulse
  + cd Impulse/
  + pip3 install -r requirements.txt
  + python3 impulse.py --help

Termux：

* + pkg update
  + pkg install python3 python3-pip git -y
  + git clone https://github.com/LimerBoy/Impulse
  + cd Impulse/
  + pip3 install -r requirements.txt
  + python3 impulse.py --help

# **短信和电话泛洪示例：**

python3 impulse.py --method SMS --time 20 --threads 15 --target +380123456789