ddos工具调研报告

摘要：本文主要介绍了常用的7款ddos工具，主要包括ddos工具的简介，攻击原理，使用说明以及工具的优缺点。

DDoS(Distributed Denial of Service)攻击即：分布式拒绝服务攻击，是由拒绝服务(Denial of Service)攻击发展而来的。

DoS攻击：DoS攻击以剥夺计算机和网络提供正常服务的能力为目的，使网络中的受攻击对象(主机、服务器、路由器等所有网络设备)无法提供或接受正常的服务。

最常见的DoS攻击通过向攻击目标发送大量的攻击数据包来消耗目标主机或网络的资源，这类攻击常被称为数据包洪泛攻击，例如SYN洪泛、UDP洪泛、Smurf攻击等。

DDoS攻击：攻击者利用网络上现有机器及系统的漏洞控制大量联网主机，使其成为僵尸主机。

被控制的主机叫做僵尸主机(Zombie host),由僵尸主机所形成的网络称为僵尸网络(Botnet)。

当被控制的机器达到一定数量后，攻击者通过发送指令操纵这些僵尸主机同时向目标主机或者网络发起DoS攻击，大量消耗其网络带宽和系统资源，导致该网络瘫痪无法提供正常的服务。

1.Loic

官网下载：<https://sourceforge.net/projects/loic/>

开源DDoS工具，可以轻松执行TCP、UDP和HTTP DoS攻击。它具有相当简单的GUI，用户只需知道网站的目标地址/URL以及需要执行的攻击。它通过淹没目标服务器来工作。发送tcp, udp，或http以中断服务为目标的数据包。使用Loic的攻击者产生足够的垃圾流量，从而对目标造成严重影响

使用说明：

1. 在url处输入想要测试的网站网址，也可以输入ip地址。
2. 输入完之后要点击右侧的lock on，输入的网站地址会自动填充到selected target中。
3. 下方可以调节速率，以及发送的请求类别，发送端口，以及线程等
4. 设置好之后点击开始按钮即可开始发包。



优点：具有相当简单的GUI，用户只需知道网站的目标地址/URL以及需要执行的攻击。

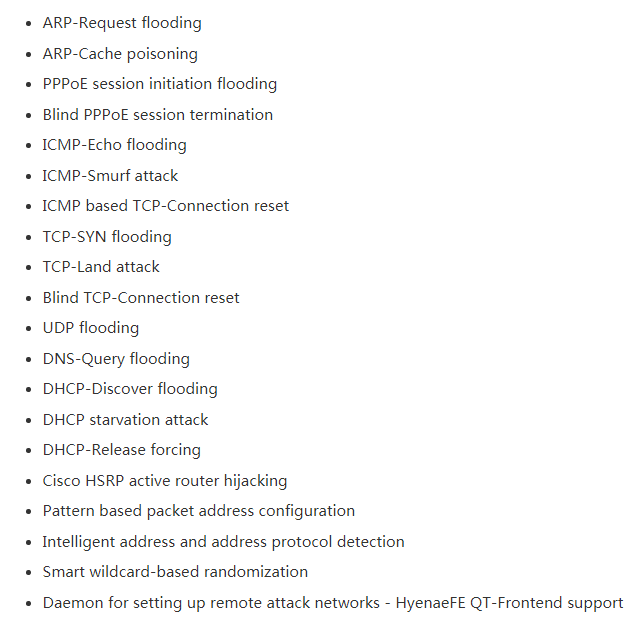
缺点：很容易找到攻击者，IP地址就暴露了。容易被IDS/IPS/AV检测到。

无法执行DDoS攻击。不能同时攻击多个目标。

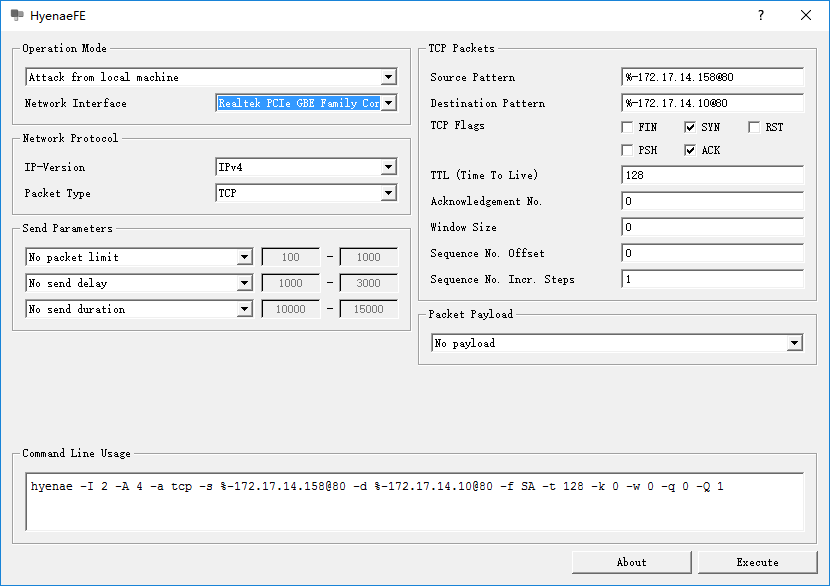
2.Hyenae

官网下载：<https://sourceforge.net/projects/hyenae/>

hyenae是在Windows平台上非常好用的一款ddos攻击工具，可以通过发送不同协议的数据包来完成绝大多数的攻击操作，可实现的攻击如下所示：



使用说明：

1. operation mode中选择网卡。
2. Network Protocol中可以选择攻击方式对应的网络协议，如SYN洪泛攻击对应传输层的TCP，IP协议可选IPv4, IPv6
3. 攻击源的IP，MAC地址以及端口号可以非常灵活的设置，按的格式书写，如图中的攻击源匹配模式MAC-IP@port，例如%-172.17.14.158@80。％代表任意，在此处代表任意的MAC地址，hyenae可以提供随机的MAC地址。172.17.14.158为伪造的攻击源IP，可以修改为任意的合法IP，80为端口号，80同时也是网络服务器的默认端口攻击目标的设置方式与攻击源一致，图的%-172.17.14.10@80
4. 针对TCP协议，给出右侧对应其的5个常见flags：FIN, SYN, RST, PSH, ACK
5. 可以随意进行单选或多选，以实现不同的攻击方式，选择不同的攻击方式，会显示相应不同的配置选项。随意的组合可以产生正常通信过程中无法出现的数据包
6. 软件下方可以设置数据包的发送速率，默认为无限速发送。

优点：可以提供绝大多数的攻击方式，有图形化界面。

缺点：由于目的MAC随机，当MAC地址首字节为奇数时，生成的数据包为广播包，此时将产生广播风暴，局域网内的所有设备都将收到大量的广播包，当速率很高时，很容易导致局域网瘫痪。

1. Ddosim

官网下载：[http://sourceforge.net/projects/ddosim/](http://sourceforge.net/projects/ddosim/" \t "https://www.freebuf.com/sectool/_blank)

DDOSIM是一种流行的DOS攻击工具。它是通过模拟控制几个僵尸主机执行DDOS攻击。所有僵尸主机创建完整的TCP连接到目标服务器。 这个工具是用c++写的,并且在Linux系统上运行。它可以使用有效的请求执行HTTP DDoS攻击。它可以使用无效请求执行DDoS攻击，可以对应用层进行攻击。

使用说明：

-d IP 目标IP地址

-p PORT 目标端口

[-k NET] 源IP来自C类网络（例如。10.4.4.0）

[-i IFNAME] 输出接口名称

[-c COUNT] 建立联系的次数

[-w DELAY] SYN数据包之间的延迟（以毫秒为单位）

[-r TYPE] 三次握手后发送的回应。 TYPE 可以是HTTP\_VALID 或HTTP\_INVALID 或 SMTP\_EHLO

[-t NRTHREADS] 发送数据包时使用的线程数（默认值1）

[-n] 不要欺骗源地址（使用本地地址）

[-v] （较慢模式）

[-h] 打印此帮助信息

使用实例：

1.从随机IP地址到www服务器建立10个TCP连接，并发送无效的HTTP请求（类似于基于DC的攻击）：

./ddosim -d 192.168.1.2 -p 80 -c 10 -r HTTP\_INVALID -i eth0

2.建立从源网络10.4.4.0到SMTP服务器的无限连接，并发送EHLO请求：

./ddosim -d 192.168.1.2 -p 25 -k 10.4.4.0 -c 0 -r SMTP\_EHLO -i eth0

3. 以更高的速度与www服务器建立无限连接，并发出HTTP有效请求：

./ddosim -d 192.168.1.2 -p 80 -c 0 -w 0 -t 10 -r HTTP\_VALID -i eth0

4. 从本地地址到POP3服务器建立无限TCP连接（不发送第7层请求）：

./ddosim -d 192.168.1.2 -p 110 -c 0 -i eth0

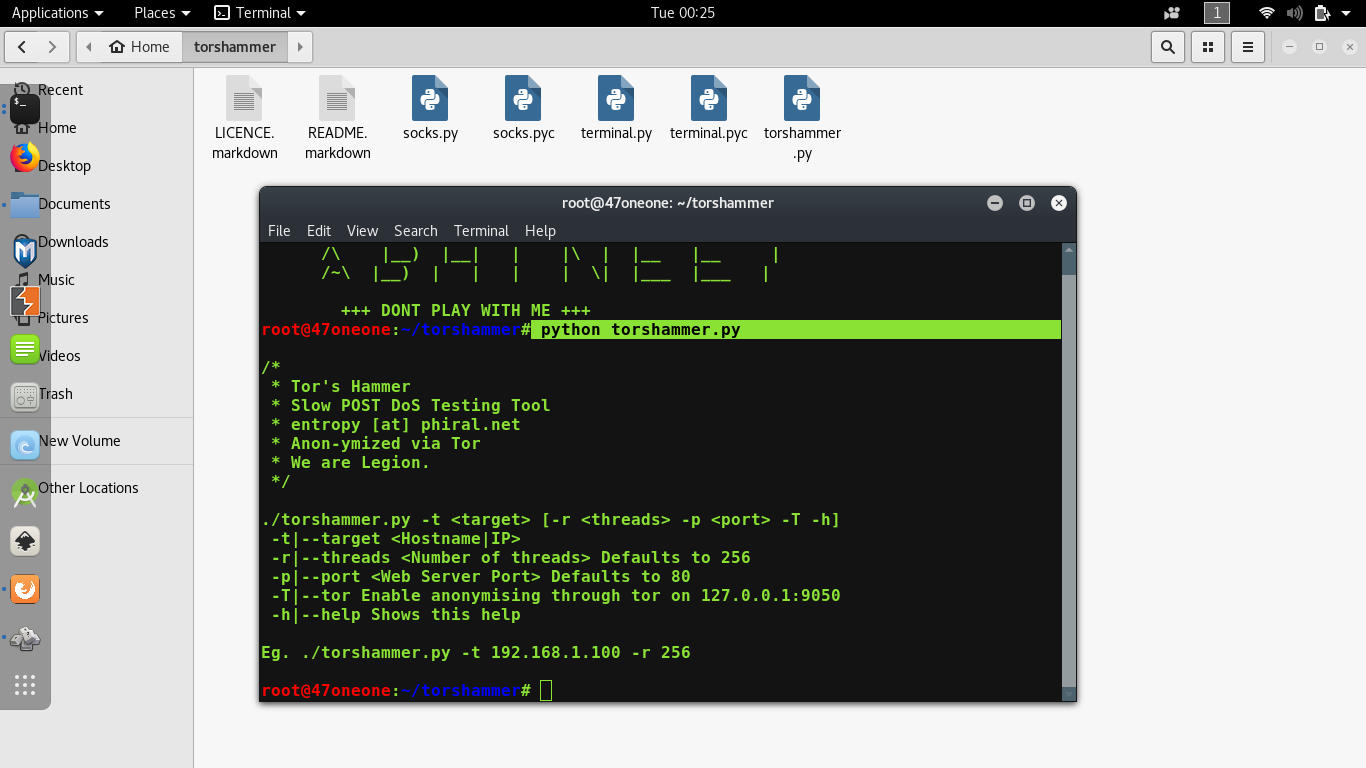
优点：模拟控制几个僵尸主机执行DDOS攻击。所有僵尸主机创建完整的TCP连接到目标服务器。

4.Tor’s Hammer

下载： [http://packetstormsecurity.com/files/98831/](http://packetstormsecurity.com/files/98831/" \t "https://www.freebuf.com/sectool/_blank)

Tor’s Hammer （最新版本为1.0）的原始版本于2011年由Packet Storm Security开发完成，是一个基于python的、可多平台运行的、主打post慢速攻击的压力测试工具，攻击原理是：首先向服务器发送一个post请求，然后缓慢的发送一系列随机内容。主打slow post功能。可使用匿名网络TOR（需安装TOR并监听于127.0.0.1:9050）发动攻击。

使用说明



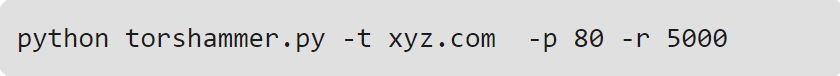
-t用于目标、某些域或IP地址。

-p为端口默认值为80。

-r是针对线程的，我们要为这个攻击运行多少线程。

-T代表tor定制攻击。

使用实例：



优点：可以使用TOR匿名网络。

缺点：慢攻攻击并不是对所有的攻击目标有效，这限制了工具的使用范围。所标称的TOR匿名网络在当前国内的网络环境下更多的是一个噱头。

5.HULK

下载：[http://packetstormsecurity.com/files/112856/HULK-Http-Unbearable-Load-King.html](http://packetstormsecurity.com/files/112856/HULK-Http-Unbearable-Load-King.html" \t "https://www.freebuf.com/sectool/_blank)

HULK是一一种Web的拒绝服务攻击工具。它能够在Web服务器上产生许多单的伪造流量， 能绕开引擎的缓存， 直接攻击服务器的资源池。HULK的特别之处在于:对于每一个请求都是独特的，能够绕开引擎的缓存直接作用于服务器的负载。

HULK使用的技术:

源代码的混淆通过 一个User Agent的已知列表，每一个HTTP请求的用户代理都是随机来自于已知列表。

引用伪装指向请求的 Referer是伪造的，要么指向主机自己，要么指向主要的已知站点。Referer 是产生请求的URL。

粘附性——使用标准的 HTTP请求去请求服务器，使用变化的keep-alive时间窗保持连接建立。

不使用缓存——是一个前提，向HTTP server 请求no-cache,一个没有在背后cache service使用的server会呈现一一个单独的页面。

URL的独特组成——为了避免缓存和其他优化工具，HULK伪造了常见的参数名称和参数值，为了单一性，他们都是根据每个请求随机生成的，使得服务器就得处理每个事件的响应。

使用方法



优点： 能绕开引擎的缓存， 直接攻击服务器的资源池。

缺点：从hulk的流量可以分析和制定适当的规则，以阻止攻击。

6.Slowloris

Slowloris也是一个慢DoS攻击脚本，就像Rudy一样。它向服务器发送HTTPGET请求，但请求尚未完成。Web服务器将等待请求完成并分配资源。与此并行的是打开这种类型的多线程，从而耗尽Web服务器的资源，属于慢速攻击。慢速攻击，目标服务器将只有那么多可用于处理并发连接的线程，每个服务器线程都将尝试在等待慢请求完成时保持活动状态，当超过服务器的最大可能连接时，会发生拒绝服务。

其基本原理是制造不完整的header。完整的http请求头结尾应该是“0d0a0d0a”，而但攻击工具只发送“0d0a”。然后以固定的时间间隔，反复发送随机的key-value键值对，迫使服务器持续等待（至超时）。最终通过不间断的并发连接耗尽系统的最大连接数直至服务端DOS。

Slowloris攻击分四个步骤进行：

1.攻击者首先通过发送多个部分HTTP请求头来打开到目标服务器的多个连接。

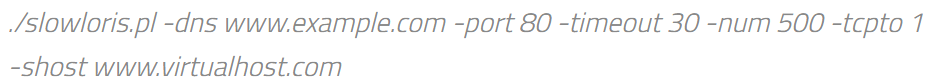
2.目标为每个传入请求打开一个线程，目的是在连接完成后关闭该线程。为了提高效率，如果连接花费的时间太长，服务器将超时异常长的连接，为下一个请求释放线程。

3.为了防止目标超时连接，攻击者定期向目标发送部分请求头，以使请求保持活动状态。本质上说，“我还在这里！我只是很慢，请等我。“

4.在等待请求终止时，目标服务器永远无法释放任何打开的部分连接。一旦使用了所有可用线程，服务器将无法响应来自常规通信量的额外请求，从而导致拒绝服务。



使用方法：



优点：方法简单。慢而低的攻击比传统的拒绝服务攻击要微妙得多，它们很难被快速发现。

缺点：只在第7层工作(基于HTTP)。慢数据可以被检测为异常流量，并可能被阻塞。没有先进的技术来调整请求。

7.R-U-DEAD-YET ?

下载: https://code.google.com/p/r-u-dead-yet/

1. U.D.Y.是拒绝服务攻击工具，它的目标是通过提交表单数据来保持Web服务器的绑定，速度慢得离谱。R.U.D.Y.被归类为低慢攻击，因为它的重点是创建几个提取出来的请求，而不是以大量快速请求压倒服务器。R.U.D.Y.软件包括一个用户友好的点击点界面，所以攻击者所需要做的就是将工具指向易受攻击的目标。

R.U.D.Y.攻击可分为以下步骤：

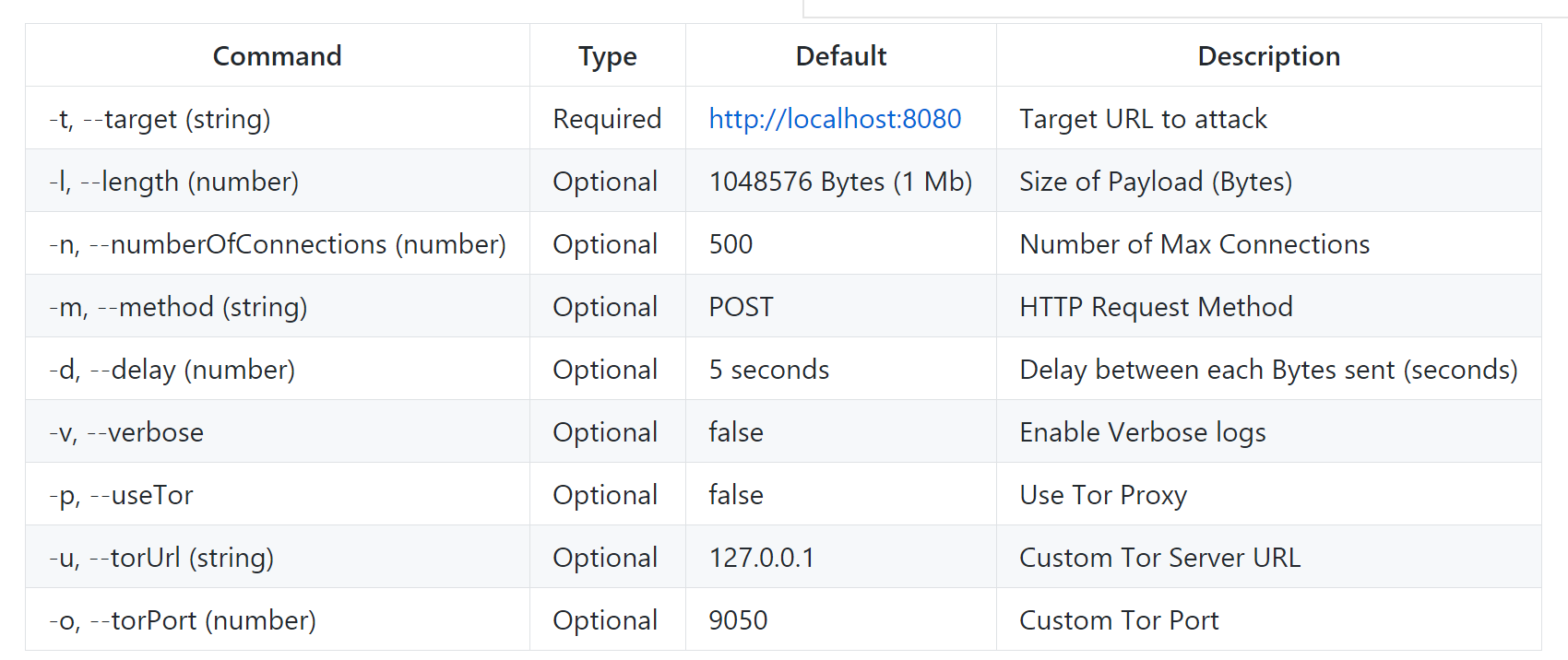
1.R.U.D.Y.工具会抓取受害者的应用程序，寻找表单字段。

2.一旦找到一个表单，该工具将创建一个http发布请求以模拟合法的表单提交。这个POST请求包含一个报头\*，它提醒服务器一段非常长的内容即将提交。

3.然后，该工具通过将表单数据分解为每个小到1字节的数据包，将提交表单数据的过程拉出来，然后将这些数据包随机地以10秒左右的间隔发送到服务器。

4.该工具继续无限期地提交数据。Web服务器将保持连接打开以接受数据包，因为攻击的行为类似于连接速度慢的提交表单数据的用户的行为。

\*HTTP报头是与任何HTTP请求或响应一起发送的键/值对，它们提供了重要信息，例如所使用的HTTP版本、内容的语言、传递的内容数量等等。

使用方法：

使用实例：

$ rudy -t "http://localhost:3000" -d 5 -n 500 --useTor --torUrl "127.0.0.1" --torPort 9051 -m "GET"

上面的命令运行RudyDDoS攻击http://localhost:3000延迟5秒，请求500次

优点：界面友好，方法简单。慢而低的攻击比传统的拒绝服务攻击要微妙得多，它们很难被快速发现。

缺点：由于攻击速度慢，所以时间很长。只在第7层工作(基于HTTP)。该网站应该有形式提交来用以攻击，以发挥作用。慢数据可以被检测为异常流量，并可能被阻塞。

其他不同ddos工具的攻击类型以及运行平台：

| **工具** | **时间** | **类型** | **运行平台** |
| --- | --- | --- | --- |
| Hping | 2004 | ICMP/UDP/SYN | Linux、Windows、Mac OS |
| Slowloris | 2007 | HTTP GET | Perl运行环境 |
| LOIC | 2009年6月 | UDP/TCP/HTTP GET | Linux、Windows、Mac OS |
| PenTBox | 2009年7月 | SYN/TCP | Linux、Windows、Mac OS |
| R.U.D.Y | 2011年1月 | HTTP POST | python运行环境 |
| HOIC | 2011年3月 | HTTP GET | Linux、Windows、Mac OS |
| THC SSL DOS | 2011年10月 | SSL renegotiation | Linux、Windows、Mac OS |
| Zarp | 2012年2月 | SYN | Linux |
| HULK | 2012年5月 | HTTP GET | python运行环境 |
| GoldenEye | 2014年2月 | HTTP GET/POST | python运行环境 |
| DAVOSET | 2014年4月 | Proxy Attacks | Perl运行环境 |
| Tor’s Hammer | 2011年 | SLOW POST | python运行环境 |
| Ddosim |  | HTTP | Linux |
| Hyenae |  | TCP/UDP/HTTP | Windows |

参考文献

<https://www.freebuf.com/articles/network/39443.html>

<http://www.yunzhan365.com/67968450.html>

<https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/>

<https://www.cloudflare.com/learning/ddos/ddos-attack-tools/r-u-dead-yet-rudy/>

<https://www.cloudflare.com/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/>

<https://blog.csdn.net/Man_In_The_Night/article/details/89014881>

<https://www.softwaretestinghelp.com/ddos-attack-tools/>

<https://github.com/sahilchaddha/rudyjs>

<https://www.greycampus.com/blog/information-security/dos-attacks-tools-and-protection>