DDOS 攻击（一）

01 定义&原理

02 网络层攻击

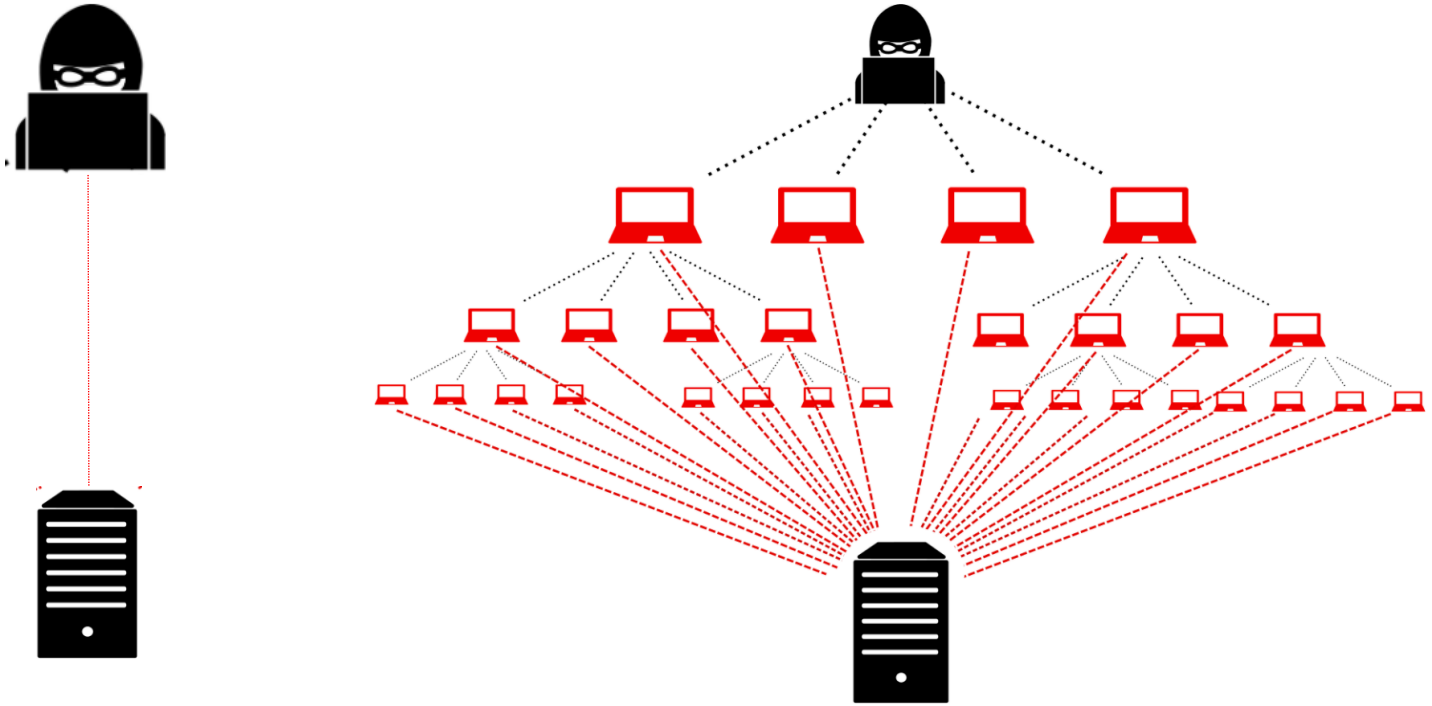
扫码试看/订阅

《Web 安全攻防实战》视频课程

01 定义&原理

定义&原理

DOS（拒绝服务）与 DDOS（分布式拒绝服务）



定义&原理

危害

大多数 DDOS 攻击的潜在有效性来自发起攻击所需的资源量与吸收或防护攻击所需的资源量之间的差异，危害在于：

- 网站瘫痪
- 无法提供正常网络服务（网络游戏）

定义&原理

OSI7 层模型 &TCP/IP4 层结构

02 网络层攻击

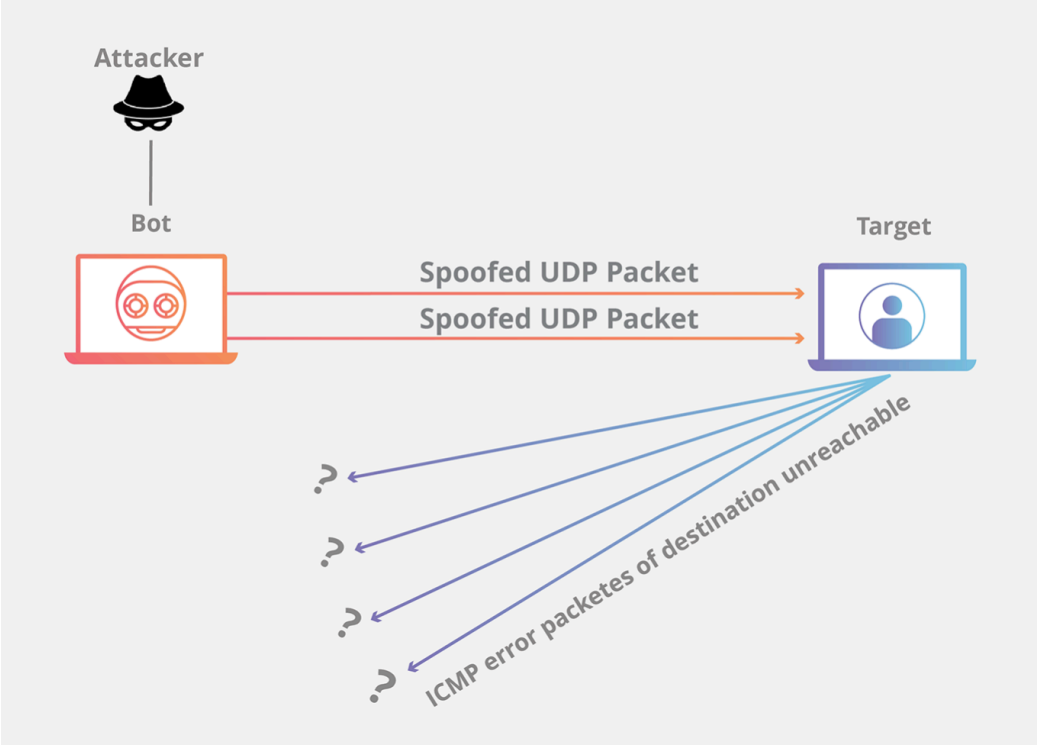
定义&原理

网络层攻击

通常通过 TCP/IP 协议簇的漏洞，对目标服务器发送大量数据流，超过设备处理能力或使网络带宽饱和，以至于网络瘫痪，典型的网络层攻击有：

- UDP 泛洪攻击：
- DNS 放大攻击：
- ICMP 泛洪攻击：
- 内存缓存 DDOS；

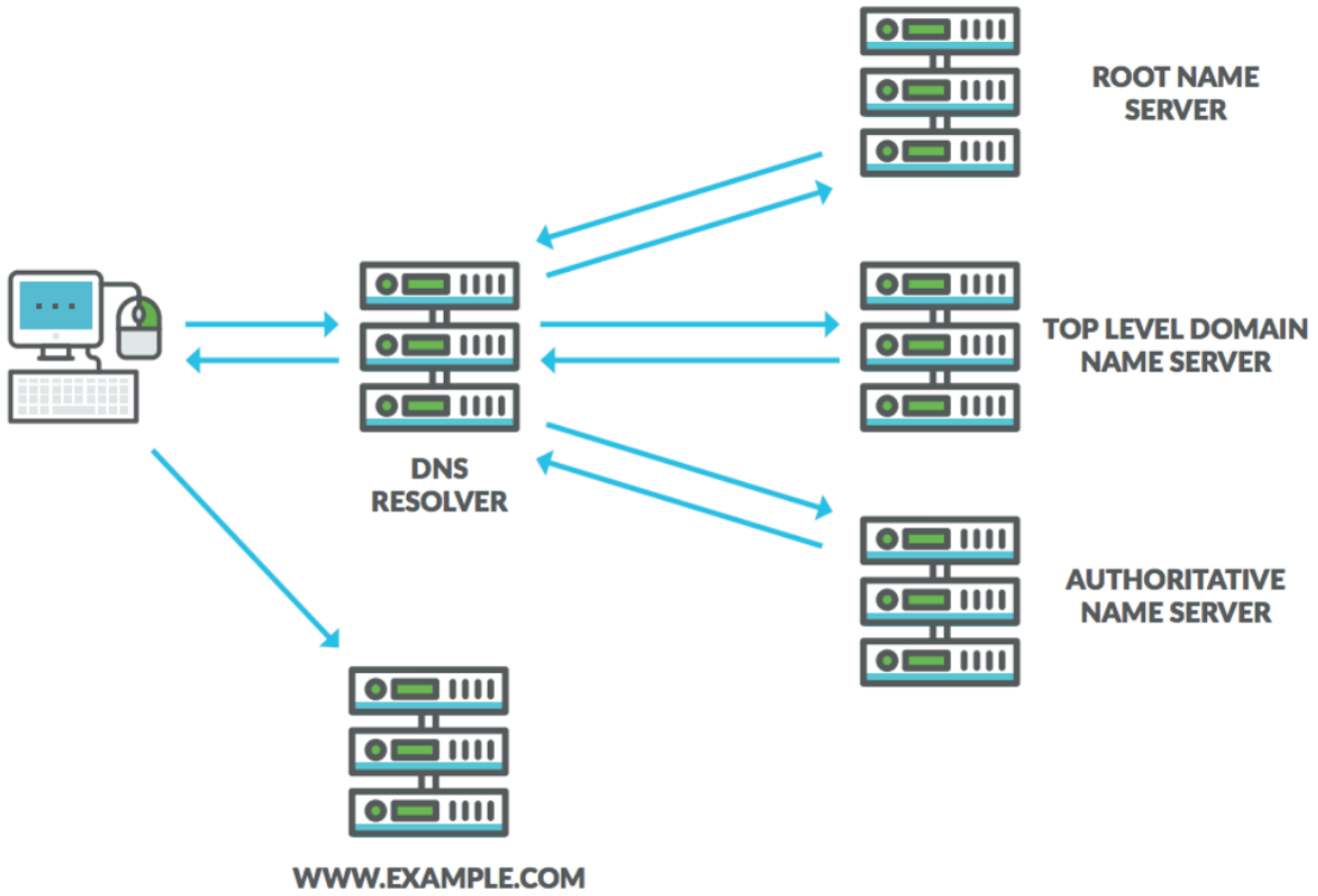
UDP 泛洪攻击



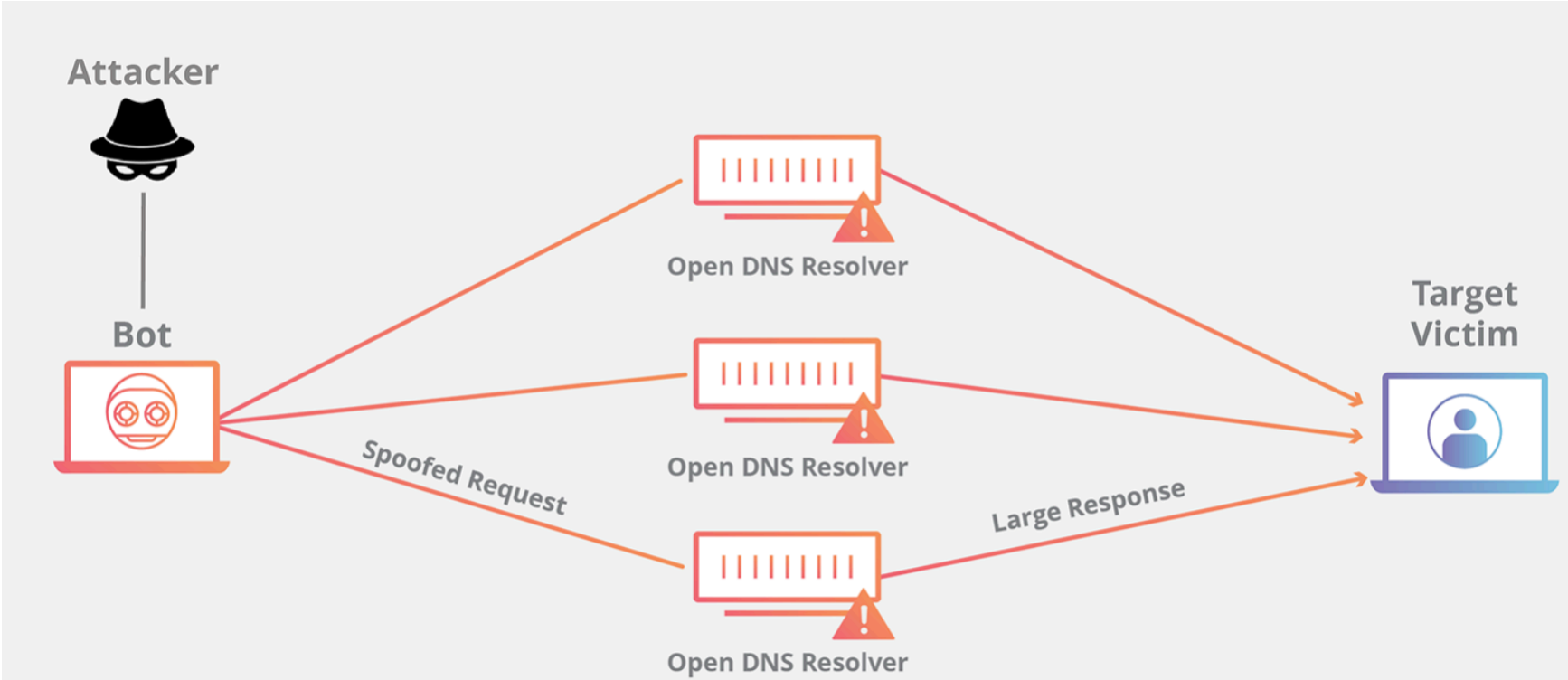
1.服务器首先检查是否有任何当前侦听指定端口请求的程序正在运行。

2.如果该端口上没有程序正在接收数据包，则服务器将以 ICMP (ping) 数据包作为响应，以告知发送方目标不可达。

DNS

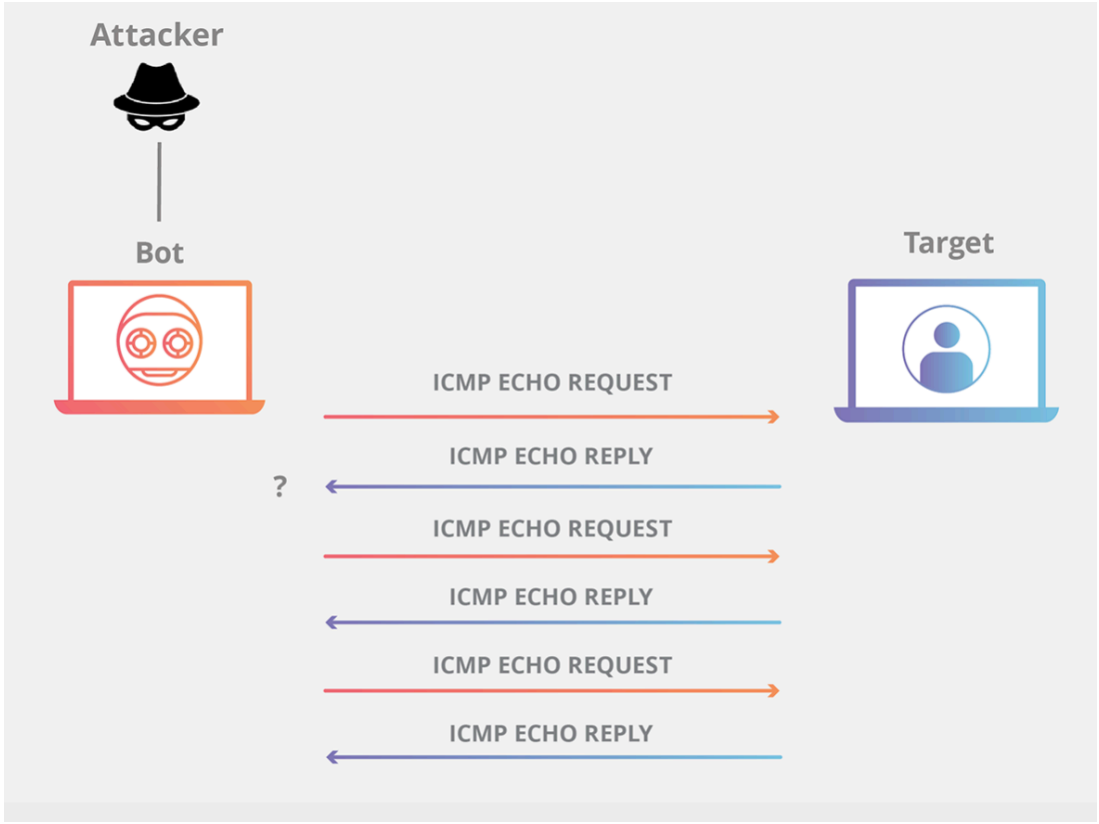

ROOT NAME SERVER
TOP LEVEL DOMAIN NAME SERVER
AUTHORITATIVE NAME SERVER
DNS RESOLVER
WWW.EXAMPLE.COM

DNS 放大攻击



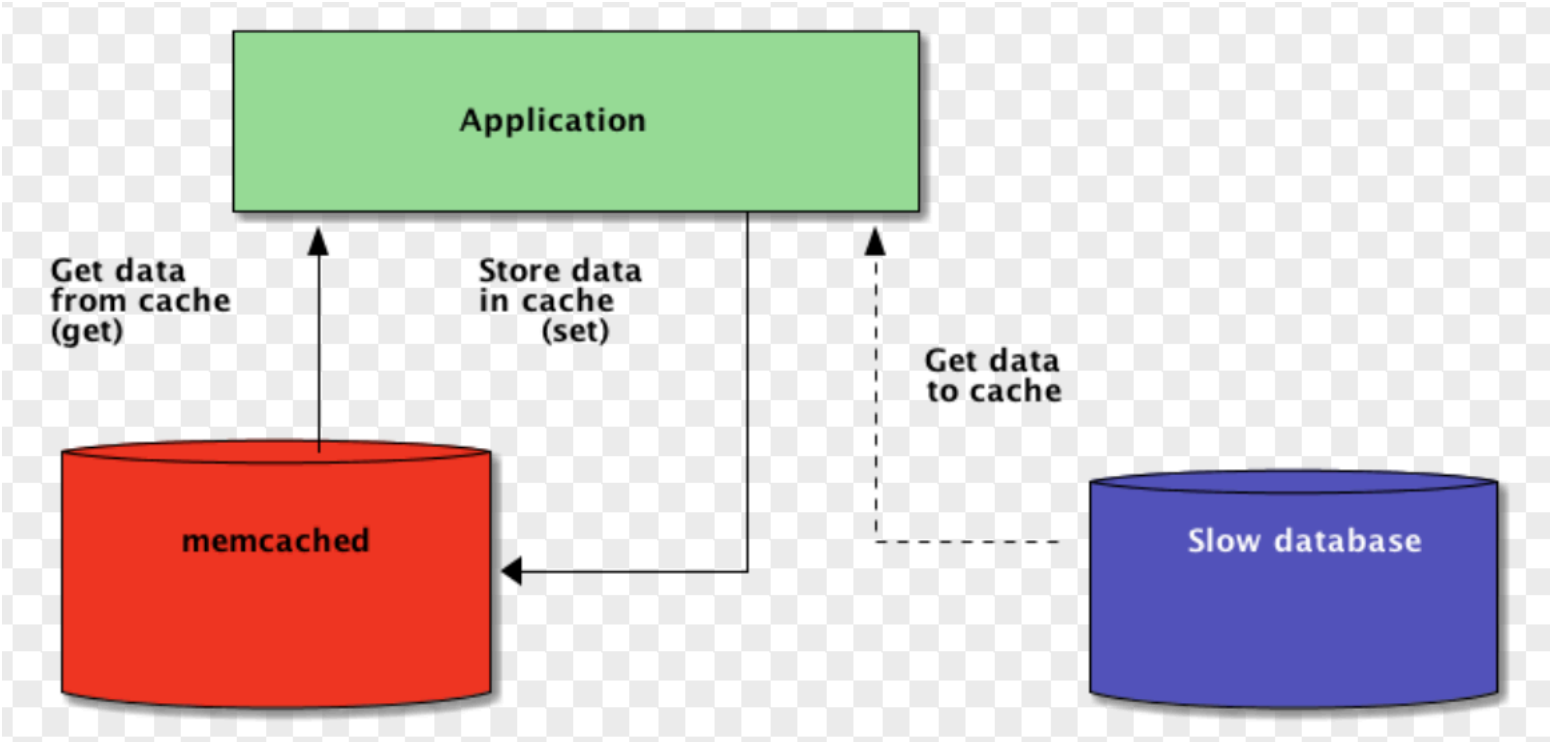
请求包较小，响应包非常大，黑客使用伪造的请求包请求 DNS 响应，IP 改为受害者 IP。DNS 服务器 向受害者发送大量的包导致而其网络则被虚假流量堵塞。

ICMP 泛洪

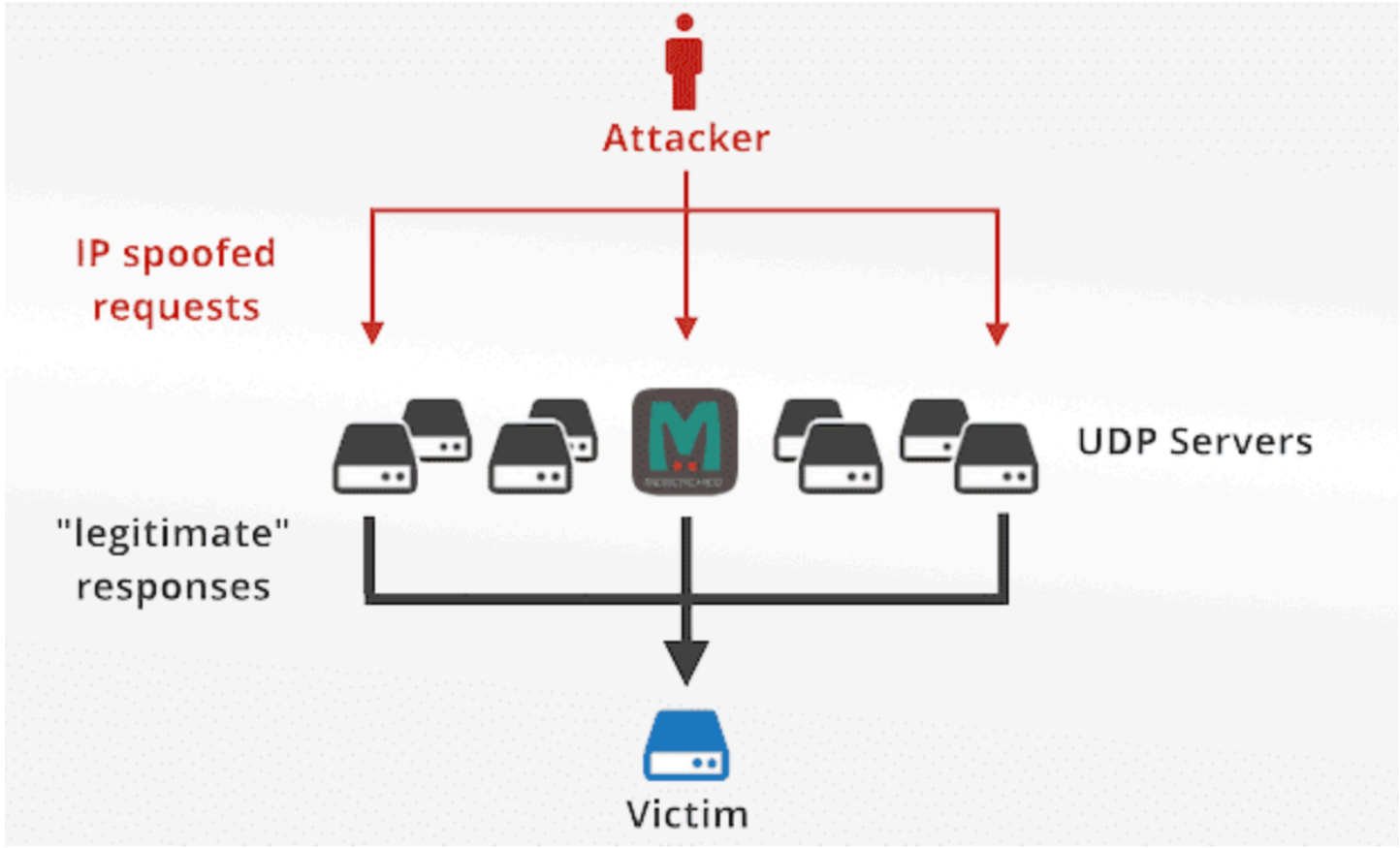


Ping 洪水的破坏效果与对目标服务器发出的请求数量成正比。

内存缓存memcached



内存缓存 DDOS



DDOS 攻击（二）

01 传输层攻击

02 应用层攻击

01 传输层攻击

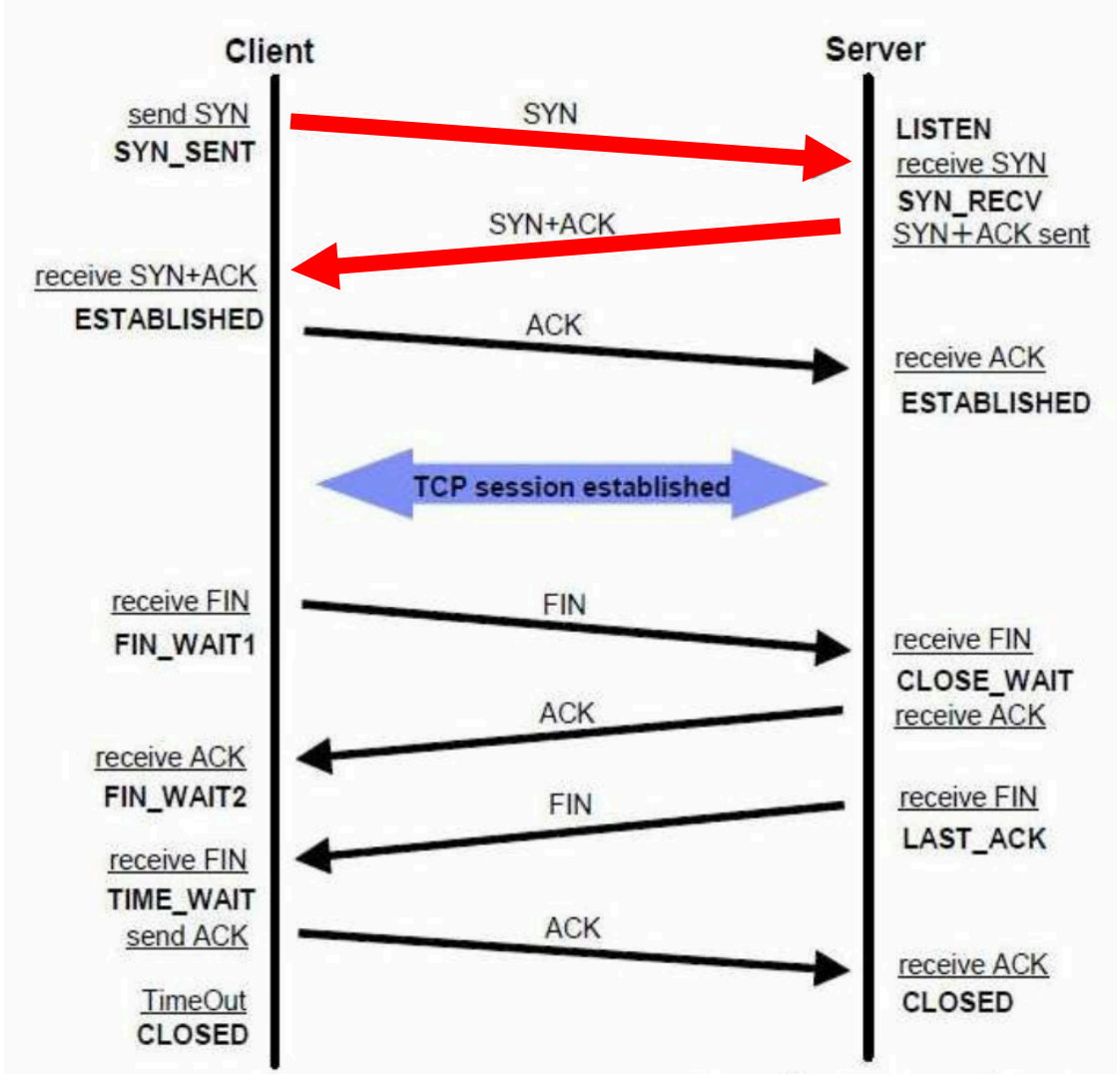
定义&原理

传输层攻击

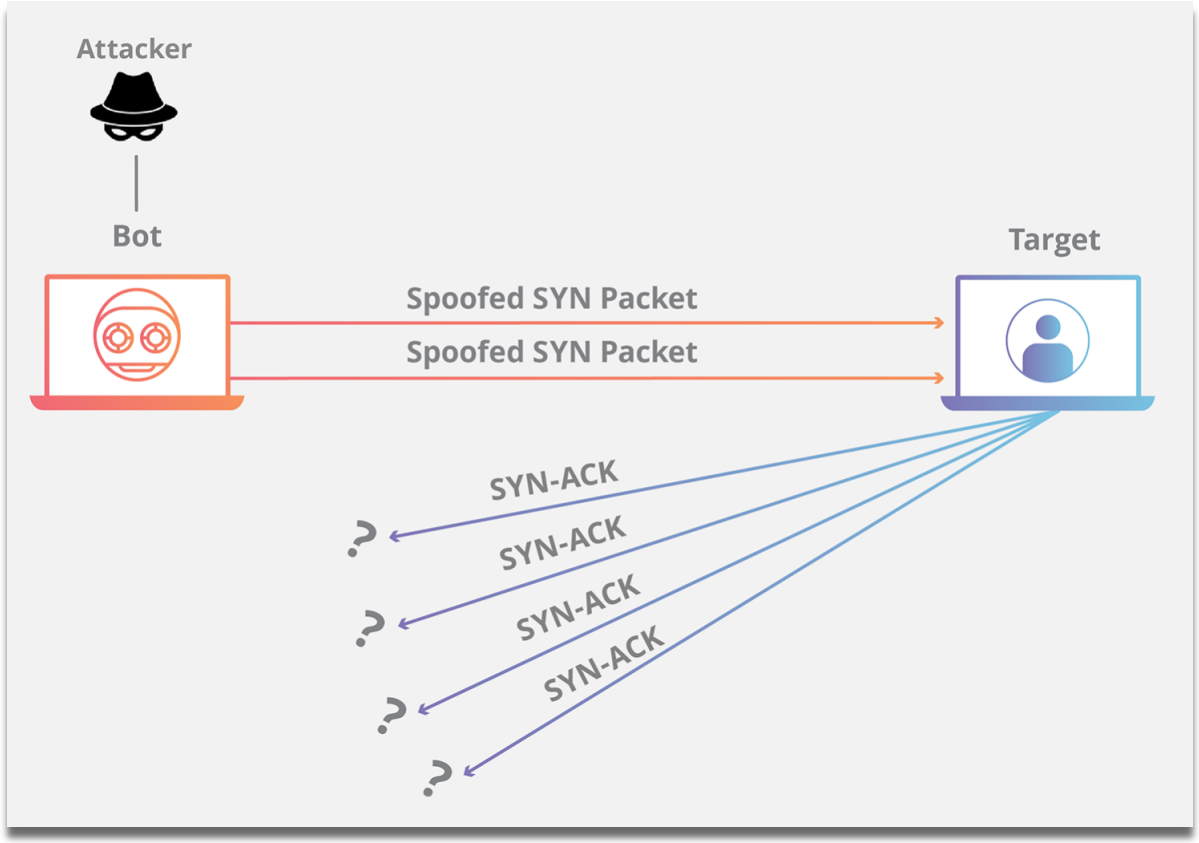
通常通过 TCP 协议的漏洞，对目标服务器发送大量数据流，使其网络带宽饱和或连接资源耗尽，以至于网络瘫痪，典型的网络层攻击有：

- SYN 泛洪攻击
- ACK 泛洪攻击

TCP 协议


Client
Server
send SYN
SYN_SENT
SYN
LISTEN
receive SYN
SYN_RECV
SYN+ACK sent
SYN+ACK
receive SYN+ACK
ESTABLISHED
ACK
receive ACK
ESTABLISHED
TCP session established
receive FIN
FIN_WAIT1
FIN
receive FIN
CLOSE_WAIT
ACK
receive ACK
receive ACK
FIN_WAIT2
FIN
receive FIN
LAST_ACK
receive FIN
TIME_WAIT
send ACK
ACK
receive ACK
CLOSED
TimeOut
CLOSED

SYN 泛洪



SYN_RECV

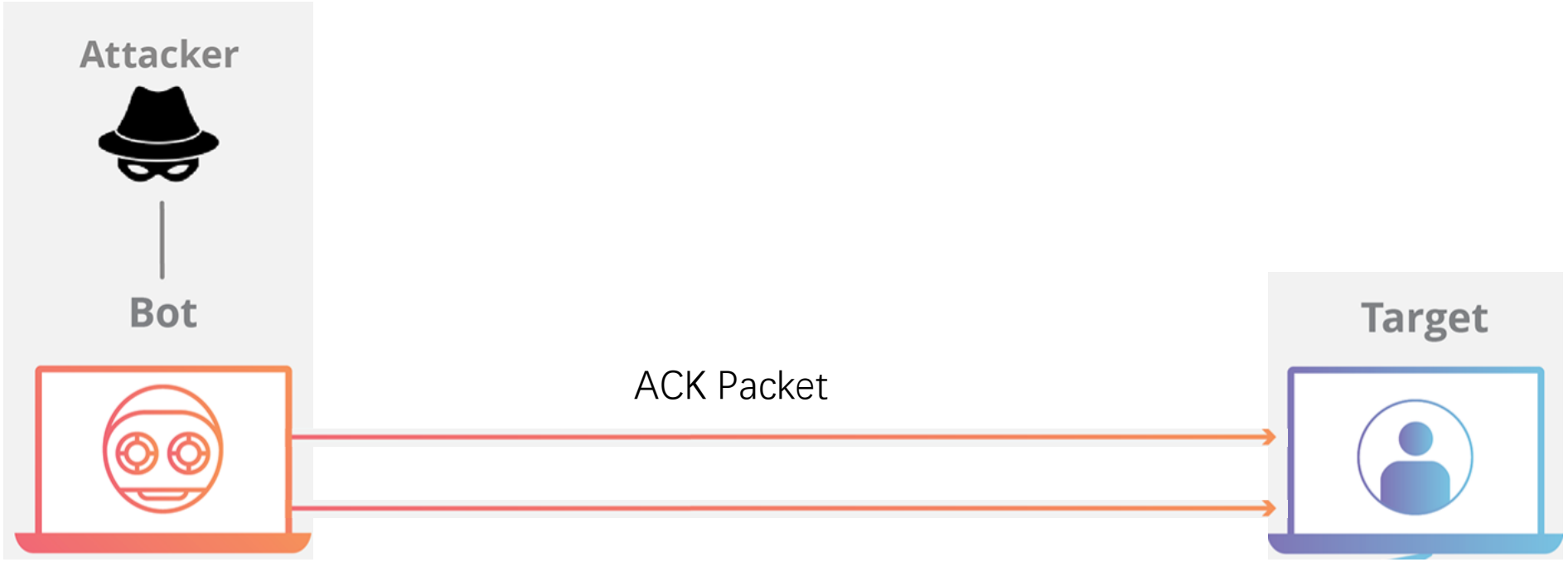
接收到了客户端的 SYN 包并且发送了 ACK 时的状态变为 SYN_RECV。再进一步接收到客户端的 ACK 就进入 ESTABLISHED 状态，但永远接受不到这个客户端 ACK 确认包。

SYN 泛洪

```
13    netstat -an|grep tcp
```

```
tcp        0      0 192.168.199.149:80      192.168.199.150:2063    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:2021    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:2028    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:2026    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1941    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:2071    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1969    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1837    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1906    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1856    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1854    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1983    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1844    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:2042    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1838    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1995    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1885    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1852    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1917    SYN_RECV    -
tcp        0      0 192.168.199.149:80      192.168.199.150:1907    SYN_RECV    -
```

ACK 泛洪



利用合法和非法 ACK 数据包看起来基本相同的特性，进行 DDOS 攻击，不易被外部安全设备拦截的特性，针对于服务器和防火墙的攻击。

02 应用层攻击

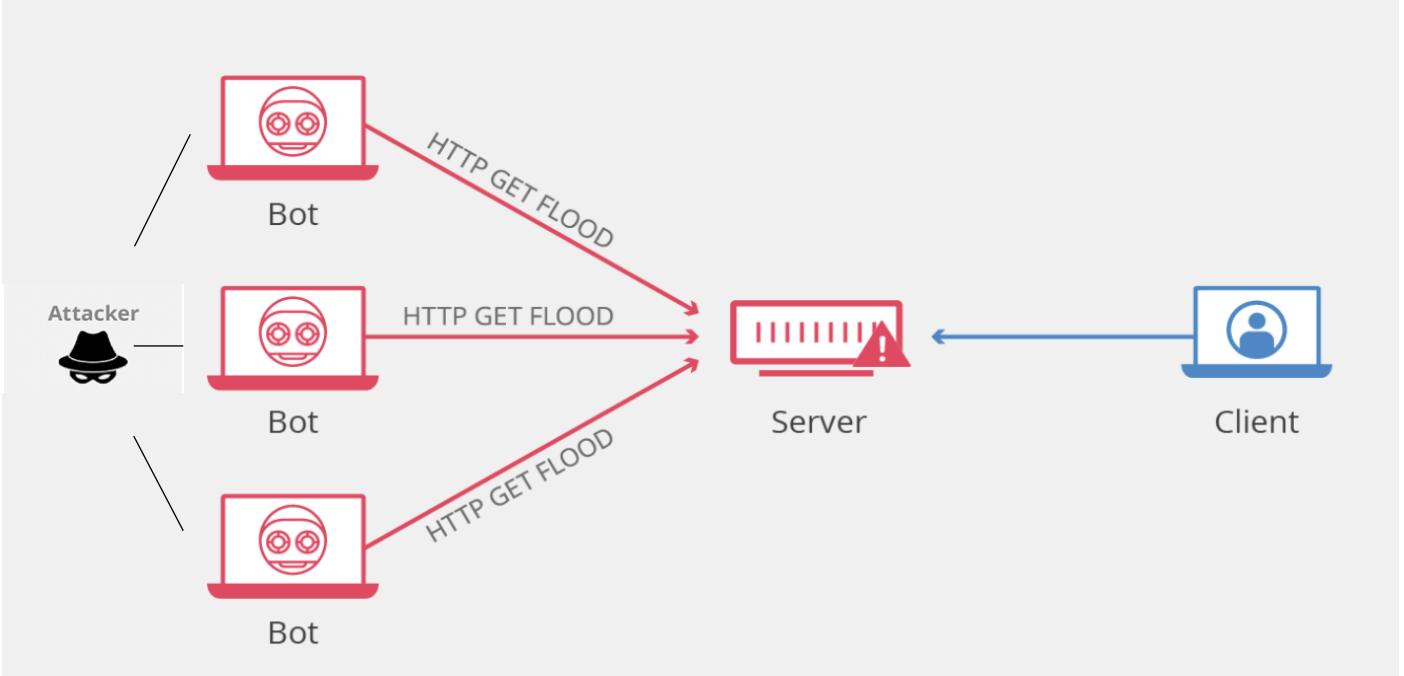
定义&原理

应用层攻击

通常通过 HTTP 协议或者容器的漏洞，对目标服务器发送少量数据流，使其连接资源耗尽，从而拒绝服务，典型的应用层攻击有：

- Slowloris 攻击：
- HTTP Post DDOS：
- HTTP 泛洪（CC 攻击）；

HTTP 泛洪（CC攻击）



黑客发送的正常的（GET POST）请求，针对于服务器需要消耗大量资源的页面，如账号登录，搜索等功能，造成服务器资源耗尽，无法响应正常连接。

Slowloris 攻击

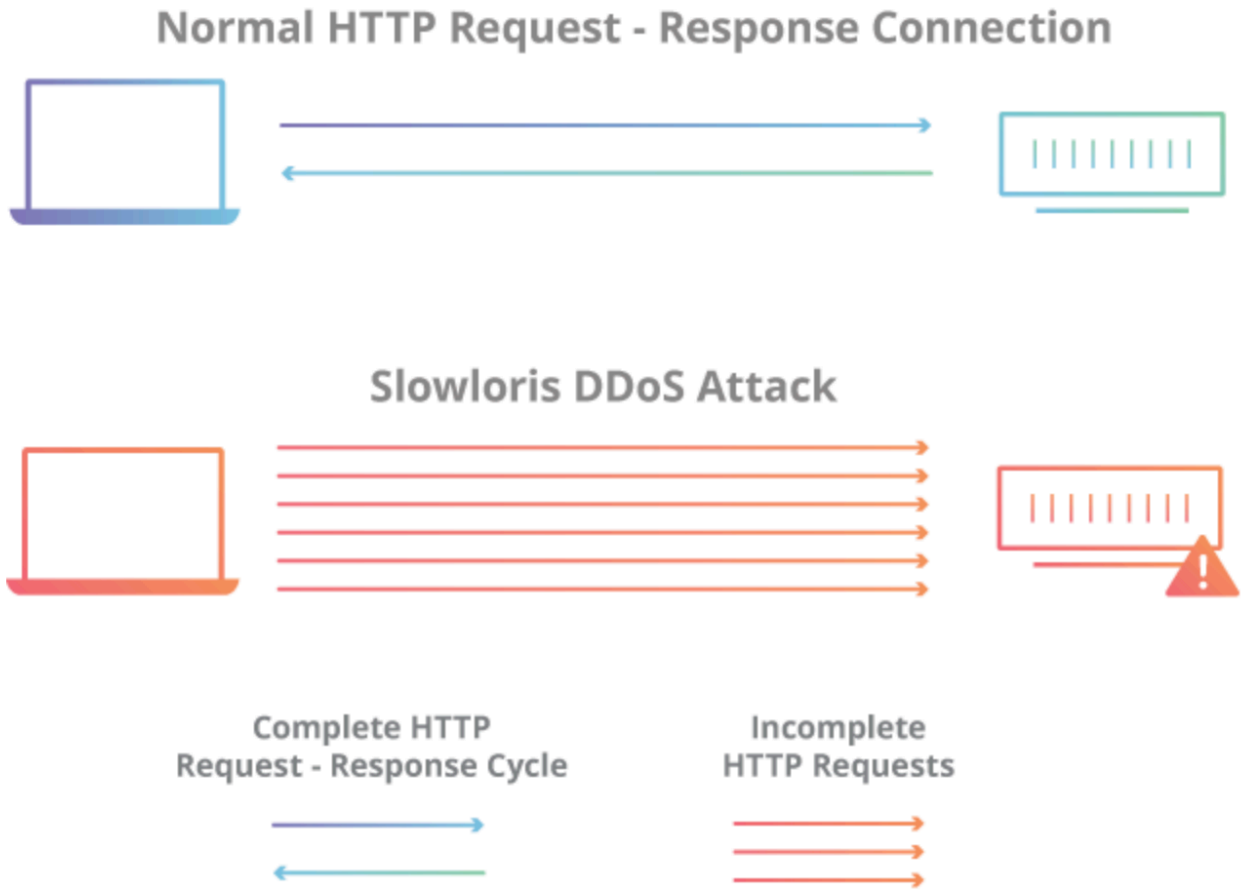
```
POST /login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/logout
Cookie: wp-settings-time-1=1600832530; donotdecodeme=eyJtb2R1bGUiOiJub2RlLXNlcmlhbGl6ZSJ9;
connect.sid=s%3ADH46gZpofreDoXsQ4kyCqYFnuoqj9ic3.bC2mPisZK8P1xigI4YZKBAF0j%2BDPhfYO2PKK0bE8Jw8
Upgrade-Insecure-Requests: 1

username=123&password=123&submit=login
```

在正常的 HTTP 包头中，是以两个 CLRF（\r\n）表示 HTTP Headers 部分结束的。

去掉一个（\r\n）表示头部未结束，客户端再发送任意头部保持连接，耗尽服务器连接数，造成拒绝服务。

Slowloris 攻击



HTTP Post DDOS

```
POST /login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/logout
Cookie: wp-settings-time-1=1600832530; donotdecodeme=eyJtb2R1bGUiOiJub2RlLXNlcmlhbGl6ZSJ9;
connect.sid=s%3ADH46gZpofreDoXsQ4kyCqYFnuoqj9ic3.bC2mPisZK8P1xigI4YZKBAF0j%2BDPhfYO2PKK0bE8Jw8
Upgrade-Insecure-Requests: 1

username=123&password=123&submit=login
```

与 Sloworis 相似，指定一个比较大的 content-length，然后以很低的速度发包，如一分钟一个字节，保持住连接。

当多台机器这样连接，耗尽服务器连接资源，造成拒绝服务。

扫码试看/订阅

《Web 安全攻防实战》视频课程