中国石油大学（华东）
CHINA UNIVERSITY OF PETROLEUM

《信息技术前沿讲座》课程总结报告

学生姓名：蔡园浩

学　　号：1703010329

专业班级：计算 1703

学　　院：计算机科学与技术学院

课程认识 30%	问题思考 30%	格式规范 20%	Latex 文档制作 20%	总分	评阅教师

2020 年 4 月 19 日

1 引言

1.1 信息技术前沿

2019 年中国科协会，发布信息技术领域十大热点问题。包括：自然语言理解、规模量子计算机的软件基础研究、自动驾驶车控操作系统关键技术研究及市场化应用、非正交轴系三维激光测量仪器、基于头显示增强现实系统的应用技术、完美密码学随机数的产生、复杂电磁环境卫星抗干扰新技术、全天候实时高分辨成像与识别、人工智能与生物智能的融合问题：人工生物智能的研究和应用、干涉光学成像技术。信息技术领域热点问题不断变化，为技术人员提供方向。前沿问题始终关注最新的，最热的技术，这就是“前沿”。

1.2 DoS 攻击

DoS 攻击（Denial of Service），是网络攻击中最常用的攻击，利用各种不同的 DoS 攻击方式，使计算机或网络无法为用户提供服务。现在的网络都是以服务为中心，无论使网站服务，还是聊天服务，或者 API 接口等等，都是以提供服务为基础。DoS 攻击可以说是对互联网危害最大的攻击。配合上分布式技术，出现的分布式 DoS 攻击（DDoS），危害更大。因此了解 DoS 攻击方法以及防范措施，就显得十分重要。

2 对本门课程的认识、体会

什么是信息技术前沿？正如引言中说的十大信息技术热点问题，那就是信息技术的前沿。信息技术的热点问题正是技术人员、科研人员研究前沿技术而发现的问题。本课程《信息技术前沿讲座》就是对前沿技术的探讨。可以发现十大热点技术中，有好几个问题都是关于人工智能的问题。比如“自然语言理解”、“自动驾驶车控操作系统关键技术研究及市场化应用”、“人工生物智能的研究和应用”，都是人工智能方向的问题。这也是为什么 2019 年中国科协会的主题是“人工智能”。随着深度学习的研究和应用，人工智能和机器学习被推上了信息技术浪潮的最顶端。但是前沿技术并不止人工智能一项。近年来，大数据、分布式系统、区块链、云计算等都是研究的热点。国内大力投资对新技术的研究和开发，不只是企业重视这些新技术，国家也非常重视。可以说中国把新技术看作经济发展的主要动力，正如那句话“科学技术是第一生产力”。前两年西方许多国家还在担心人工智能会对人类社会造成威胁，也就是人工智能阴谋论。担心霍金先生提出的人工智能危害人类的预言。在那时候，习近平总书记立刻提出了关于“推动我国新一代人工智能健康发展”的理论。习总书记非常看重人工智能技术对经济发展的作用，“科学技术是第一生产力”的理论永远都不过时。加上国务院印发的《新一代人工智能发展规划》[2]，正是因为国家对人工智能技术的重视，许多企业都开始投入了对人工智能的研究，阿里巴巴、华为、百度、腾讯等企业都有相应的部门来研究人工智能技术。当然国外对于信息技术的研究始终还是比较靠前的 [5]。人工智能是一个例子，代表着所有前沿技术，国家和企业对其他前沿技术的重视程度同人工智能技术一样。就比如云计算，虽然云计算技术已经早在十几年前就成为了热点技术，现在的云计算技术已经非常成熟，许多企业都有自己云计算平台。国内的阿里云、腾讯云平台对外提供云计算服务，加上近几年深度学习的超大强度的计算需求，可以说云计算技术的热度一直未降。

2.1 对人工智能发展的认识与思考

近年来，人工智能发展迅速，特别是深度学习算法兴起，将人工智能的研究推向了高潮。可以说现在成熟的人工智能算法，绝大多数都是基于神经网络。目前市面上能够用于生产的人工智能算法，也几乎是基于神经网络。深度学习算法突破了传统的算法无法超越的瓶颈，可以说连接派的人工智能目前占据了上风。

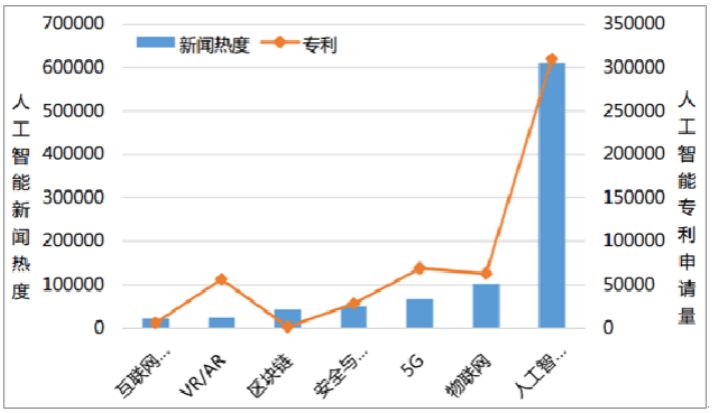


图 1: 人工智能热度及专利数

自从 2016 年 3 月 AlphaGo 以 4:0 战胜了国际围棋大师李世石后，大众对人工智能有了新的认识。以前人们以为人工智能不可能在象棋战胜人类，结果我们输了；然后人们以为人工智能不可能在围棋战胜，结果我们还是输了，而且输的很惨。2017 年 10 月，AlphaGo Zero 以 100:0 战绩战胜了 AlphaGo，AlphaGo 是利用现有的棋谱来进行学习，可以说是借鉴了人类长年来的经验，而 AlphaGo Zero 是完全的无师自通，不参考任何棋谱，由空白状态开始学习。为什么 AlphaGo Zero 能经过短时间内的训练就战胜人类 4000 年的经验，一方面是计算机的计算能力，由于高性能的计算能力，使得 AlphaGo Zero 能够迅速对战来提升自己，AlphaGo Zero 40 天能够对战 2900 万盘 [4]。这种速度是人类永远无法达到的，这也是人工智能高于人类的一项重要指标。但 AlphaGo Zero 战胜人类仅仅是因为它学得快吗？我觉得不是，和 AlphaGo Zero 对战过的棋手，都说 AlphaGo Zero 的下棋风格很诡异，让对手琢磨不透。我认为这才是 AlphaGo Zero 胜利的关键原因，人类 4000 年的经验，凭人类现在的理解能力和记忆能力以及无法有太多的提示，而 AlphaGo Zero 从零开始利用自我博弈的方式，自学围棋，可以说他已经超越了人类 4000 年来的瓶颈，所以它的下棋风格才令人琢磨不透，是因为它的方式以及超越了人类的理解范畴。

部分人（如：霍金）公开呼吁人们正式人工智能的威胁，认为人工智能的发展可能导致人类灭绝。而另一部分人（如：库克）认为人工智能能够帮助人类完成更多的事情，提高人类的生活质量。我听说过这样一个假设：如果人类创造出比人类智商更高的人工智能，那么那个人工智能可以在很短时间内创造比它自己智商更高的人工智能，如此循环，人工智能的智商会迅速提升，超过人类太多太多。这个假设听起来似乎的确细思极恐，但是现阶段的机器学习算法仅仅只是针对某个领域或某个问题的人工智能，要说达到人类的思维能力，还远远不够。所以根本无需相信人工智能会威胁人类这样的说法。

2.2 对于网络安全技术的认识与思考

网络安全不是最几年的才出现的问题，自从 1969 年美国的阿帕网开始，网络安全一直都是研究的一个方向。近几年云技术的不断发展，越来越多的数据被放在云服务器上，越来越多的计算也在云服务器上进行，而用户通过网络来访问云服务器以获得相应的服务，这使得网络安全越来越被人们重视。网络安全虽然不像其他热点问题那样热火朝天，但是网络安全确实很多技术的基础。特别像阿里云、腾讯云这样有用大量的云服务器，并对外提供云服务，一切云服务都基于网络安全这一个基础技术。可以说网络安全技术永远不过时，一直都是前沿技术。大多数的网络攻击方法都是公开的，大家都知道，但是却依然存在网络安全问题。并不是因为不断地有新的攻击方法出现，而是不断地有人把现有的攻击方法和新技术结合，就如 DoS 技术和分布式（Distributed）技术结合而成的 DDoS 攻击。甚至结合物联网技术，利用网络摄像头实现 DDoS 攻击。

随着区块链技术的完善，网络安全面临着新的问题，区块链可以再不久会成为新的网络安全问题 [8]。新技术的出现一定会带来新的安全问题，这是必然的。

3 对演讲题目的进一步的思考

3.1 DoS 攻击

DoS 攻击，英文全称 Denial of Service。是指拒绝服务攻击，也可以称作服务被拒绝。DoS 攻击广义上指任何导致被攻击的服务器不能正常提供服务的攻击方式。具体而言, DoS 攻击是指攻击网络协议实现的缺陷或通过各种手段耗尽被攻击对象的资源, 以使得被攻击计算机或网络无法提供正常的服务, 直至系统停止响应甚至崩溃的攻击方式 [7]。

3.2 历史上的 DoS 攻击事件

3.2.1 史上最大的 DoS 攻击

迄今为止最大的 DDoS 攻击发生在 2018 年 2 月。这次攻击的目标是数百万开发人员使用的流行的在线代码管理服务 GitHub。在此高峰时，此攻击以每秒 1.3 太字节（Tbps）的速率传输流量，以每秒 1.269 亿的速率发送数据包。

这是一个 memcached DDoS 攻击，因此没有涉及僵尸网络。相反，攻击者利用了一种称为 memcached 的流行数据库缓存系统的放大效应。通过使用欺骗性请求充斥 memcached 服务器，攻击者能够将其攻击放大约 50,000 倍！

幸运的是，GitHub 正在使用 DDoS 保护服务，该服务在攻击开始后的 10 分钟内自动发出警报。此警报触发了缓解过程，GitHub 才能够快速阻止攻击。最终这次世界上最大的 DDOS 攻击只持续了大约 20 分钟。

3.2.2 第二大攻击–2016 Dyn 攻击

第二大 DDoS 攻击是针对 2016 年 10 月主要 DNS 提供商 Dyn 。这次攻击造成了破坏，并造成许多主要网站的中断，包括 AirBnB，Netflix，PayPal，Visa，亚马逊，纽约时报，Reddit，

和 GitHub。这是使用名为 Mirai 的恶意软件完成的。Mirai 利用受损的物联网（IoT）设备创建僵尸网络，例如相机，智能电视，收音机，打印机甚至婴儿监视器。为了创建攻击流量，这些受损设备都被编程为向单个受害者发送请求。

幸运的是，Dyn 能够在一天内解决攻击，但攻击的动机从未被发现。黑客组织声称对此次攻击负责，因为维基解密创始人朱利安·阿桑奇在厄瓜多尔被拒绝上网，但没有证据支持这一说法。还有人怀疑这次袭击是由心怀不满的游戏玩家进行的。

3.3 DoS 攻击产生的基础

3.3.1 软件、协议的弱点

一些 DoS 攻击是由于软件、协议固有的缺陷被黑客利用产生的。软件、协议的弱点是包含在操作系统或应用程序中的与安全相关的系统缺陷，这些缺陷大多是由于程序编制的错误，源代码的副作用或程序中一些不适当的绑定所造成的。由于软件和协议几乎依赖于开发商，对于漏洞只能依赖开发商提供的补丁。及时为软件打补丁是避免收到攻击的最好办法。

但是完全避免 DoS 攻击是不可能的，因为有一些导致攻击的系统或者协议难以被弥补。所以有一些因宽带或资源过载产生瓶颈导致的 DoS 攻击，至今都还没有一个固定的解决办法 [10]。

3.3.2 系统、程序的错误配置

系统或程序的错误配置也是导致网络安全的一大隐患。很多错误配置都是因为经验不足或缺乏责任心造成的。如路由器、防火墙、交换机或其他网络设备配置不合理都会导致收到网络攻击。

3.4 常见的 DoS 攻击手段

3.4.1 SYN-flood

SYN-flood，也叫 SYN 攻击或 SYN 泛洪。Flood 就是“洪水”或“泛洪”的意思。SYN 攻击产生的原因是由于 TCP 协议的漏洞。TCP 协议是很多应用层协议的基础 [3]，在应用程的：

- HTTP 协议：超文本传输协议，用于普通浏览
- HTTPS 协议：安全超文本传输协议，身披 SSL 外衣的 HTTP 协议
- FTP 协议：文件传输协议，用于文件传输
- POP3 协议：邮局协议，收邮件使用
- SMTP 协议：简单邮件传输协议，用来发送电子邮件
- Telent 协议：远程登陆协议，通过一个终端登陆到网络
- SSH 协议：安全外壳协议，用于加密安全登陆，替代安全性差的 Telent 协议

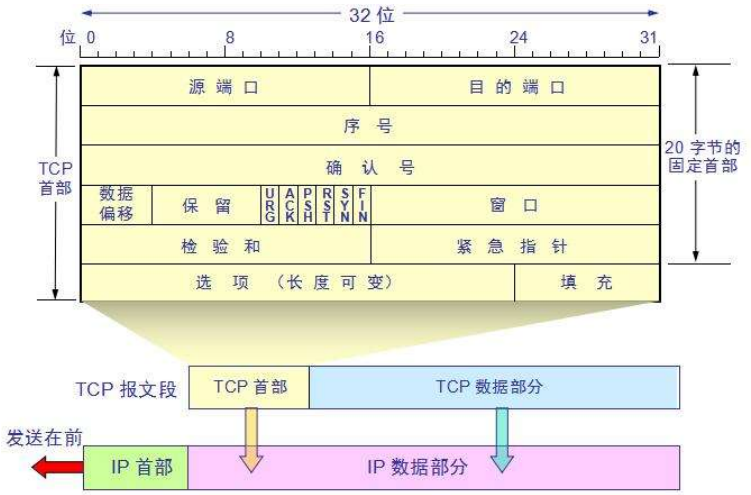


图 2: TCP 协议首部字段

这些都是基于 TCP 协议的。图 2为 TCP 协议的头部字段类型。

当两台主机要建立连接时，需要进行 TCP 协议的三次握手。如图 3所示，当发送端 S 想要和接收端 D 建立连接时，会发送三个报文，这三个报文就被称作三次握手。第一个报文包括 SYN 同步标志位，当接收端 D 接收到这个报文时，会立刻为连接分配资源，然后回复一个报文，也包括 SYN 同步标志位，以及对上一个报文的确认。最后发送端 S 再对第二个报文进行确认，连接就建立成功了。

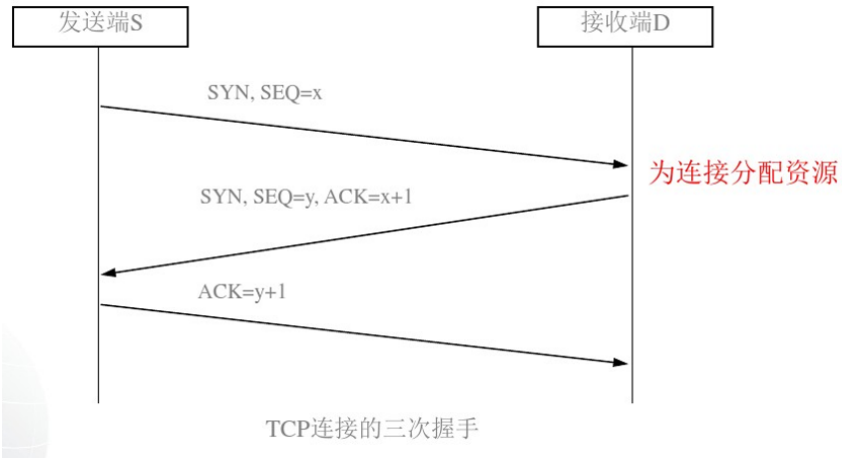


图 3: TCP 连接的三次握手

那什么是 SYN-flood 呢？SYN 攻击之所以叫这个名字，就是因为它利用了 TCP 协议中的 SYN 标志位。值得注意的是当接收端收到第一个握手报文后，就会立马为连接分配资源，这也就是 SYN 攻击利用的 TCP 协议的漏洞。如果攻击者只向被攻击之发送三次握手报文的第一个报文，即带有 SYN 标志的报文，并且是不断地发送。接收端每接收到这样一个报文，就会立刻分配资源。如果在短时间内收到大量的带有 SYN 标志的报文，就会导致被攻击者的资源迅速被消耗，以至于正常的用户想要和它建立连接时无法成功，也就无法为用户提供服务。

SYN 泛洪攻击的解决办法有两个：

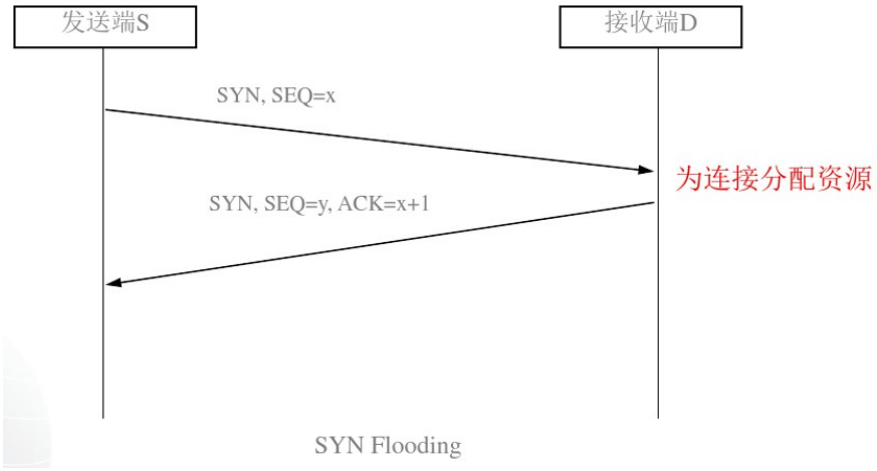


图 4: SYN 泛洪攻击

1. 缩短超时时间，可以尽快的将半连接从挤压队列中移去，而不至于消耗太多时间，浪费资源。
2. 增加挤压队列大小，可以提高某个端口连接数量，以容纳更多的半连接提高抵御 SYN 攻击的能力。

但这些办法都不是有效的解决办法，到目前为止都没有完全解决 SYN 泛洪攻击的有效办法只能说做到适当的控制。

根据 SYN 泛洪攻击的原理，我实现了一个 SYN 泛洪攻击的程序，图 5是该程序的部分代码，完整代码见附件 synflood.c。

```
    tcp->seq=random();

    int count=1;
    while(1){
        ip->ip_src.s_addr=random();
        tcp->source=random();//htons(LOCALPORT);//
        if(count%10000==0) printf("Send %d packets\n",count);
        count++;
        tcp->check=check_sum((unsigned short *)tcp,sizeof(struct tcphdr));
        sendto(sockfd,buffer,head_len,0,addr,sizeof(struct sockaddr_in));

    }
}

unsigned short check_sum(unsigned short *addr,int len){
```

图 5: SYN 攻击部分代码

使用./synflood [IP] [port] 命令运行该程序，运行效果如图 6：

为了直观的看出效果，使用 wireshark 进行抓包分析，如图 7：

我也自己编写了一个 sniffer 嗅探程序，完整代码见附件 sniffer.c。使用自己编写的嗅探程序也能清楚的看到发送的 SYN 攻击报文的详细信息，效果如图 8:

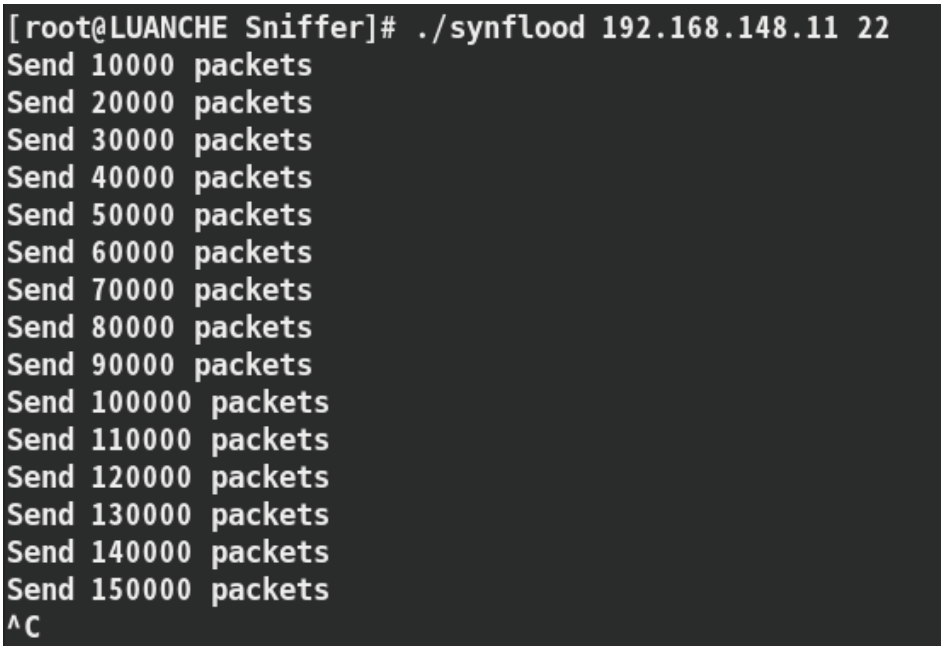


图 6: synflood 运行效果

抓包结果可以看到，源 IP 和源端口是随机生产的，大量的 SYN 攻击，主机的资源被迅速消耗。

3.4.2 Land 攻击

Land 攻击，也叫着陆攻击。Land 攻击同样是基于 TCP 一些的 SYN 标志。但是 Land 攻击与 SYN 攻击有所不同，可以说 Land 攻击是 SYN 攻击的升级版。SYN 攻击需要攻击者一直发送 SYN 攻击报文，以达到 DoS 攻击的目的，而 Land 攻击只需要发送一个报文至靶机，靶机就会瞬间瘫痪。

分析一下 Land 攻击的原理，一个正常的 TCP 三次握手报文的前两次报文如图 9所示，当两台主机想要正常建立连接，A 发送带有 SYN 标志位的报文，源 IP 地址写上自己的 IP 地址 A，目的地址写上目标 IP 地址 B。B 收到这个报文后，回复一个带有 SYN 标志的报文，源 IP 地址写上它自己的 IP 地址 B，目的地址写上刚才收到的报文中的源 IP 地址。

如果有一个攻击者发送这样一个报文，如图 10所示，这个报文带有 SYN 标志位，目的 IP 地址是 B，源 IP 地址也是 B，按照刚才的回复报文的过程，B 回复的报文就是这样，带有 SYN 标志，源 IP 地址是他自己的 IP 地址 B，目的 IP 地址是刚才收到的报文的源 IP 地址，还是 B。这个报文不会发送给别人，因为目的 IP 地址是自己，所以报文会发送给自己。前后两个报文可以发现，是完全一样的。那么就会造成一个效果：B 不断地给自己发送 SYN 报文，并且不断地分配资源。就导致自己把自己地资源消耗掉，最终造成拒绝服务。

当然 Land 攻击是由比较有效的防御办法 [1]，根据 Land 攻击的原理可以分析出，导致 Land 攻击的报文有这样的特点，就是该报文的源 IP 地址和目的 IP 地址是相同的。根据这一特点，只需要在接收到报文后分析一下该报文的源 IP 地址和目的 IP 地址是否相同，如果相同，就直接丢弃掉。这样就能避免 land 攻击。当然 SYN 攻击的防御办法对 Land 攻击也是有一定

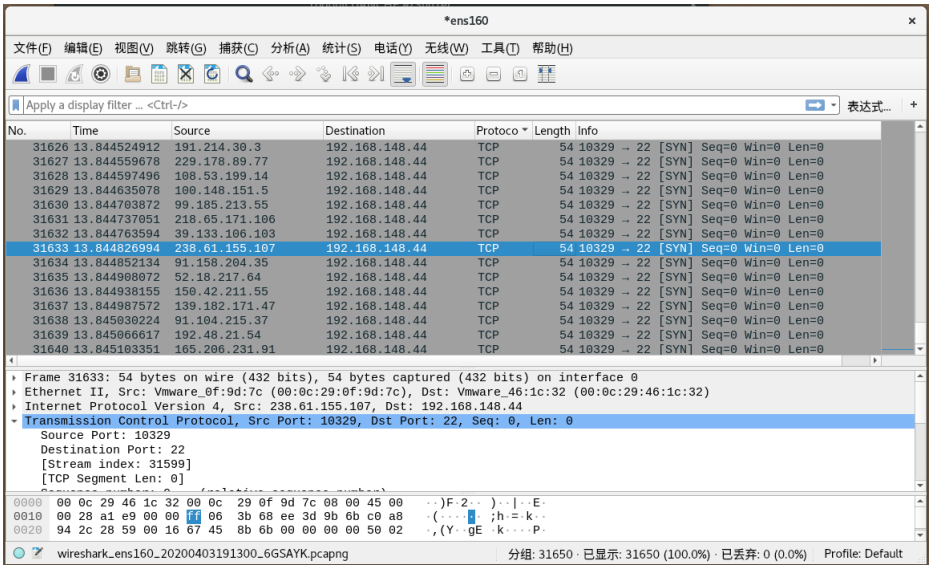


图 7: wireshark 抓包截图

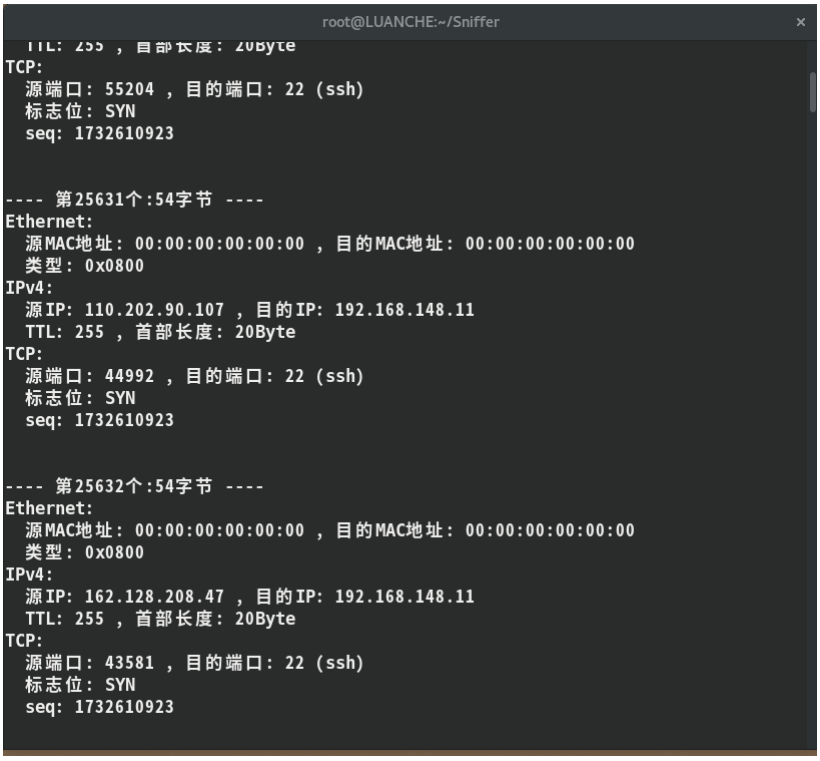


图 8: wireshark 抓包截图

的效果的。

3.4.3 IP 欺骗性攻击

IP 欺骗性攻击（IP Spoofing）起源非常早，是在 1985 年 Robert T. Morris 发表的一篇关于 TCP/IP 协议缺陷时提出的。利用 IP 欺骗进行攻击成功率并不算高，但是如果使用适当

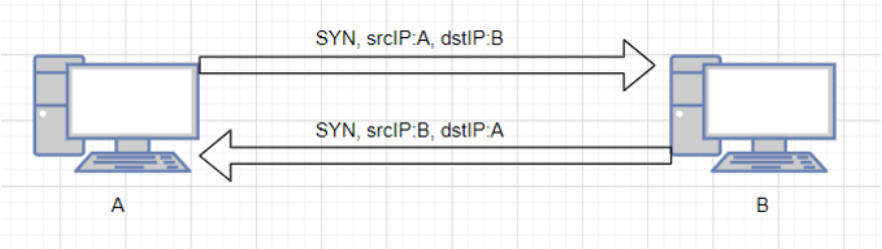


图 9: 正常 TCP 的握手包

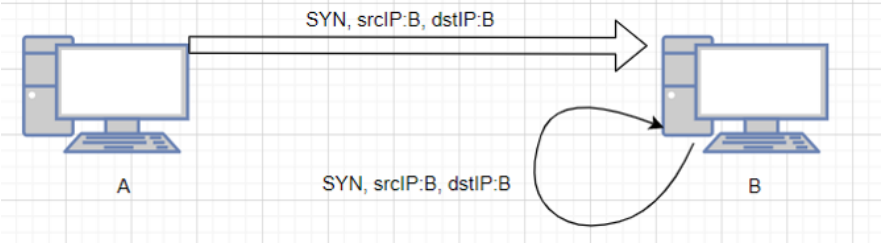


图 10: Land 攻击的 TCP 的握手包

的工具，是能够进行会话劫持的。IP 欺骗性攻击的应用有很多，比如进行拒绝服务攻击、伪造 TCP 连接、会话劫持、隐藏攻击主机地址等 [9]。

我们要探究的就是利用 IP 欺骗性攻击进行拒绝服务攻击。有一种 IP 欺骗性 DoS 攻击时利用 TCP 协议的 RST 位。假设有一个合法的用户已经和服务器建立了连接。如果攻击者利用该用户的 IP 地址，伪造一个源 IP 为该合法用户的 IP 的 TCP 报文，并且将 RST 标志位置 1。当服务器收到该报文后，会认为该用户连接有错误，需要重新建立连接，于是就会清空缓存区等待该用户重新发送建立连接的请求。但是那个合法的用户依旧会继续发送数据，但服务器并不会理会发来的数据，它只会等待新的建立连接请求。这样就造成了拒绝服务的效果。

防御 IP 欺骗性攻击的的方法很少，而且效果也并不明显。如果客户端和服务器属于内网，所有的服务请求都通过边界路由转发至内网的服务器，如图 11，就有一个比较有效的办法。通过对边界路由进行配置，禁止外网进入的数据包声明自己具有内网的 IP，如果有这样的数据包发过来，边界路由就将其过滤。以达到防御的效果。但是大多数服务器都是对外开放的，拥有一个公网 IP，而且客户端和服务器在同一个内网的的可能很小，所以这个方法也没有太多实质性的效果。

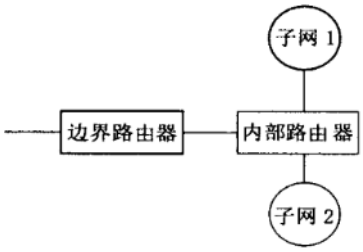


图 11: 边界路由

3.4.4 Smurf 攻击

Smurf 攻击是 DDoS 攻击中比较常见的一种，Smurf 攻击利用 ICMP 协议的漏洞，结合 IP 欺骗和 ICMP 回复，使网络为了响应 ICMP 回复请求而产生大量的数据流量，使网络造成拥塞，导致被攻击的主机无法为合法用户提供服务 [6]。我们用的 ping 命令就是基于 ICMP 协议的。

当一个攻击者想要攻击一台主机，他会向网络中的其他中间主机广播一个虚假的 ICMP 数据包，如图 12。该数据包的源 IP 地址被修改为被攻击主机的 IP 地址，当中间主机收到这些 ICMP 请求包后，根据 ICMP 协议，它们会回复同等大小的 ICMP 响应包，而这些响应包都会被发送给被攻击主机，被攻击主机在短时间内收到大量的 ICMP 响应包，导致网络资源迅速被浪费掉。以至于其他合法用户无法请求正常的服务。

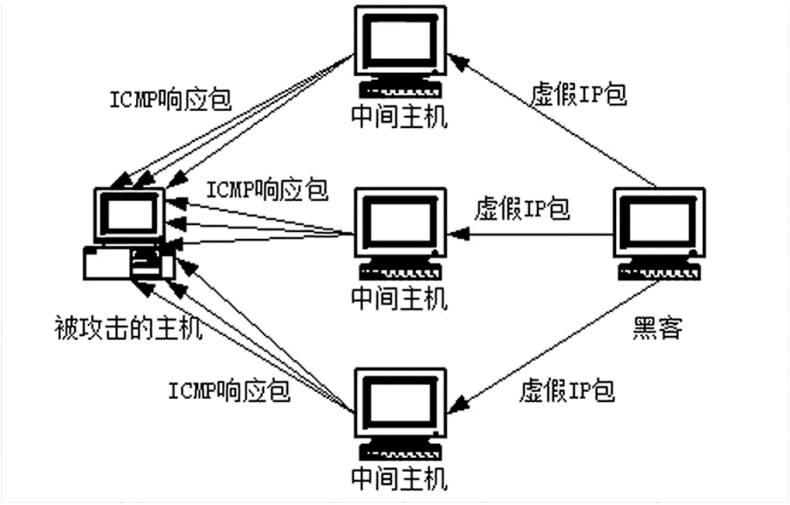


图 12: Smurf 攻击原理

根据 Smurf 攻击的攻击原理，Smurf 攻击的防御可以从攻击者、中间媒介和目标站点方面。

1. 避免站内主机成为攻击者。Smurf 攻击是利用广播包对网内主机发送 ICMP 请求报文，所以如果能对内网内数据包进行过滤，过滤类似的 ICMP 广播包，就能有效预防 Smurf 攻击。

2. 避免成为 Smurf 攻击的中间媒介。如果能避免中间主机对 Smurf 攻击的 ICMP 请求包进行相应，也能防止 Smurf 攻击。比如对网内路由器进行配置，拒绝回复带有广播地址的 ICMP 请求包，就能阻断 Smurf 攻击。

3. 防止成为 Smurf 攻击目标。目标主机可以关闭掉 ICMP 协议，从而直接过滤掉 ICMP 响应包。当时这样的办法并不是很有效，而且大部分服务器都不会关闭掉 ICMP 协议，因为 ICMP 协议对管理员有很大的作用，可以有效检测网络连通性。

3.4.5 Ping of Death

Ping of Death，也称死亡之 ping。是早期的 Windows 系统中存在的一个漏洞，但在 Windows Me 的时候已经不存在这个漏洞了。Ping of Death 是一种畸形的报文攻击，在 1996 年攻击者

开始利用这个漏洞，攻击者发现当他们一个进入使用碎片包可以将整个 IP 包的大小增加到 IP 协议允许的 65536 比特以上的时候。许多操作系统收到一个特大的 IP 包就不知道该作什么了，服务器就会被冻结、宕机或者重新启动。

实现方法也十分简单，只需要使用 ping 命令的-l 参数调整数据包的大小，超过了 65536 个字节就形成了死亡之 ping。

现在这个漏洞已经被修复，当时的各大网站为了防止被人发送大数据的 ping 包，于是将数据包压到 3000 一下，而服务器或者 dns 一般把数据包压到 10000 一下。

4 总结

DoS 攻击实现方式简单，使得 DoS 攻击成为网络攻击中十分常用的攻击方式。DoS 攻击和某些社会现象十分相似，公共资源被并不需要的人占用，而真正需要使用这些公共资源的人却无法使用。资源的合理分配，把资源分配给真正需要的人，这也是一大难题。为什么 DoS 攻击很难得到有效的防御，于社会资源相同，作为分配资源的一方，很难知道谁是真正需要资源的，谁是进行虚假请求来请求资源的。无法区分真假，使得 DoS 攻击防御变得十分困难.

虽然 DoS 攻击很早就已经出现，但是一直能算做前沿的技术。系统不断地更新，也不断地出现各种各样的漏洞，漏洞是无法避免的，也导致不断有攻击者发现新的攻击技术。也有人把早已出现的攻击方式和新的技术结合，造成更大的攻击效果，比如 DDoS 攻击。网络变得越来越重要，网络安全的重要性也永远不会过时。

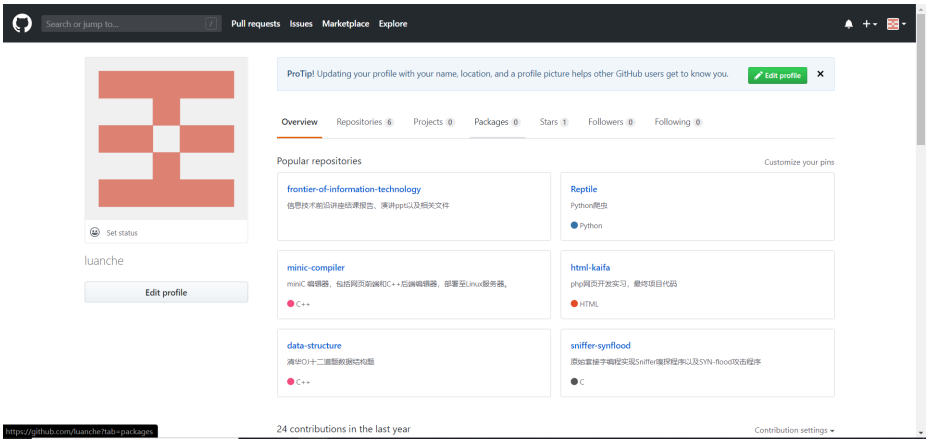
5 附录

- Github 账户

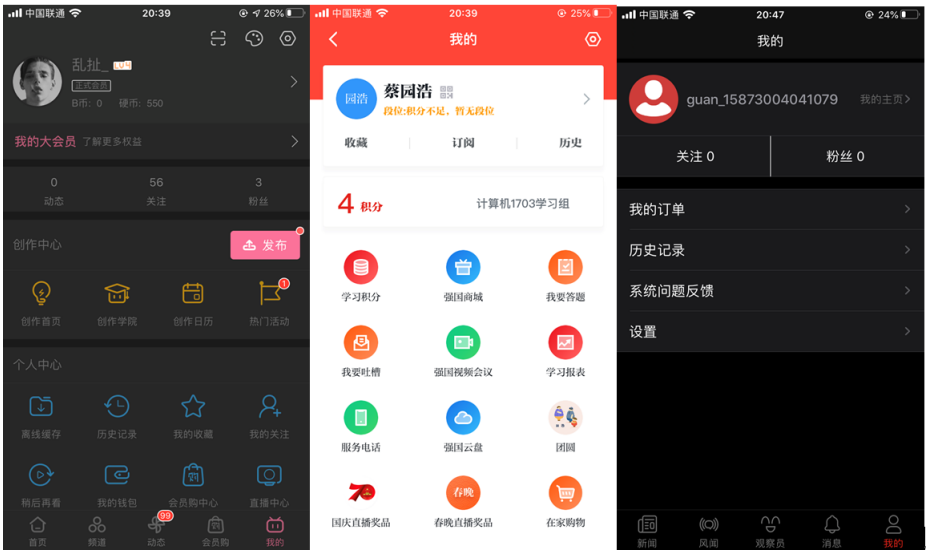
  个人网址 https://github.com/luanche

  本次课结课报告资源网址 https://github.com/luanche/frontier-of-information-technology

  主页截图

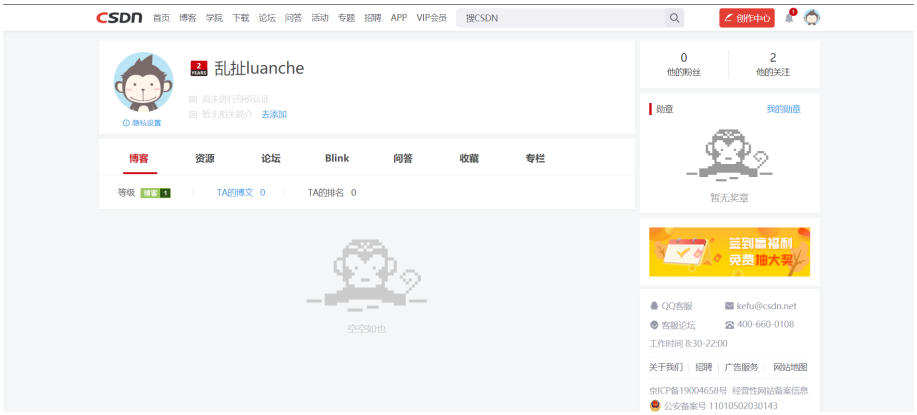


- 观察者、学习强国、哔哩哔哩 APP



- CSDN、博客园账户

  CSDN 网址 https://me.csdn.net/qq_42070757



  博客园网址 https://home.cnblogs.com/u/2013939/

- 小木虫账户

个人网址 http://muchong.com/bbs/space.php?uid=21924026

参考文献

[1] 如何全面防御黑客攻击. *互联网天地*, (9):16–17.

[2] 新一代人工智能发展规划. *科技创新与生产力*, (8):52–66, 2017.

[3] M. ALLMAN. Tcp congestion control. *RFC 2581*, 1999.

[4] Tao Tang Zhen, Kun Shao, Bin Zhao Dong, and Heng Zhu Yuan. Recent progress of deep reinforcement learning:from alphago to alphago zero. *Control Theory and Applications*, 2017.

[5] 吴金南 and 郝斌. 国外信息技术能力研究前沿探析与理论拓展. *科技进步与对策*, 29(8):155–160, 2012.

[6] 徐永红, 张琨, 杨云, and 刘凤玉. A study on smurf attack and its countermeasures *南京理工大学学报（自然科学版）*, (05):68–72.

[7] 朱良根, 张玉清, and 雷振甲. Dos 攻击及其防范. *计算机应用研究*, 21(7):82–84, 2004.

[8] 李媛媛. 区块链或将于 2025 年前成为下一个“网络安全前沿”. *互联网天地*, 000(6):60, 2017.

[9] 蒋卫华, 李伟华, and 杜君. Ip 欺骗攻击技术原理、方法、工具及对策 attack: Principles, methods,tools and countermeasures. *西北工业大学学报*, 020(004):544–548.

[10] 陈波 and 于泠. Dos 攻击原理与对策的进一步研究. *计算机工程与应用*, (10):30–33, 2001.