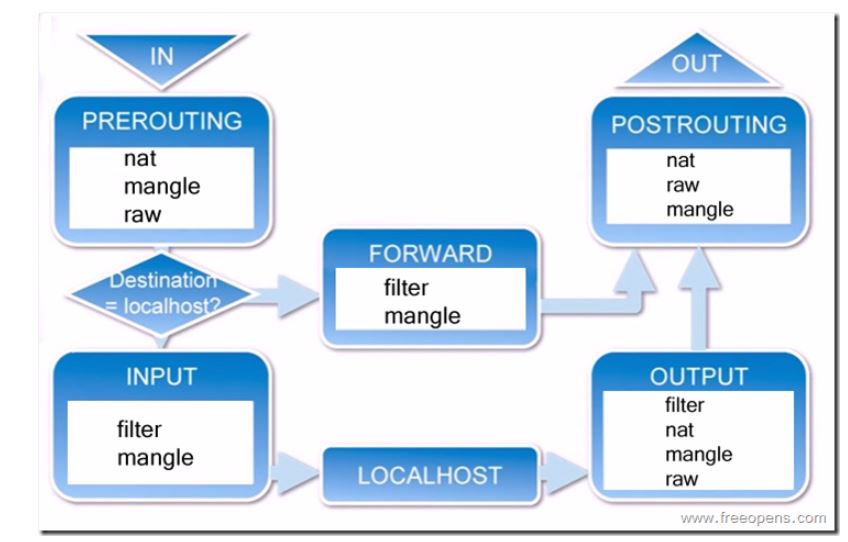
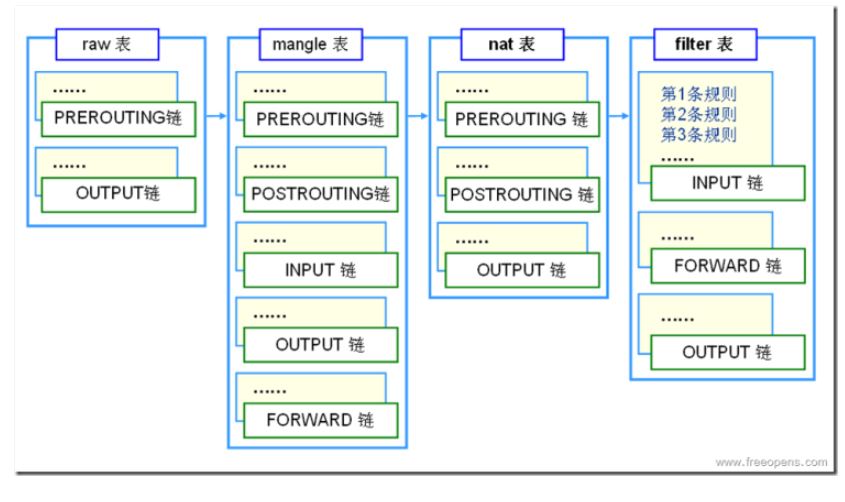
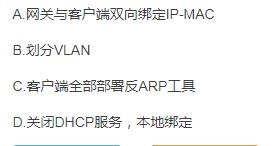
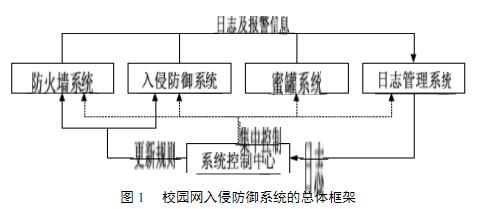
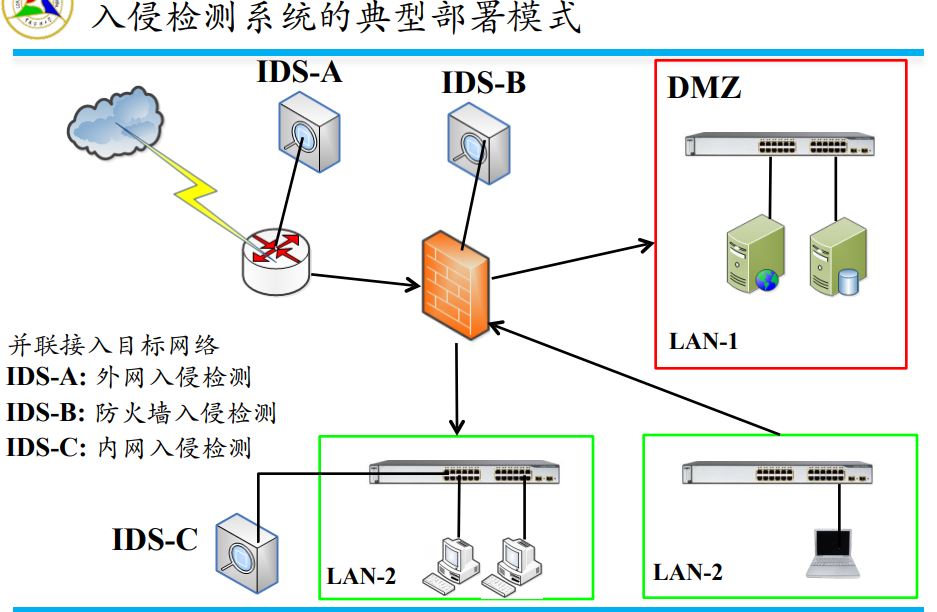
网络安全考试  
  
1、搭建攻防环境：绘图（如何联网，标记连网方式，指明IP地址）  
  
- 实验一  
  
2、网站缺陷代码：找到漏洞  
  
- git管理的应该是你 亲手 编写的代码，一个网站项目代码不要把测试文件也提交到版本仓库  
- phpinfo.php 如果是在生产环境，这个文件就会给攻击者暴露很多服务器配置信息  
- 代码里包含了你的个人密码  
  
  
  
- 存在SQL注入的代码片段  
   
    $sql="SELECT `E-mail` FROM `user` WHERE `E-mail`='$smtpemailto'";  
  
    $sql = "UPDATE `user` SET `IdetifyCode` = '$random' WHERE `user`.`E-mail` = '$smtpemailto' ";  
  
    $sql="SELECT `Title`,`Random` FROM `Documents` WHERE `UserName`='$name'";  
  
    $sql="SELECT `UserName`, `PassWordByUser`, `E-mail`,`PasswordByEmail` FROM `user` WHERE (`UserName`='$name'or `E-mail`='$email') and (`PassWordByUser`='$hash' or `PasswordByEmail`='$hash')";  
  
    $sql1="SELECT `UserName` FROM `user` WHERE (`UserName`='$name'or `E-mail`='$email')";  
  
  
- 数据库连接避免使用root用户，注意提交到git仓库中的代码不要包含真实账号密码信息  
  
  
- 避免在服务器内存中持久保存用户的明文口令，类似 心脏滴血 漏洞会直接泄漏用户的明文口令  
  
    $\_SESSION['psw']=$password  
  
> 2014年4月7日，OpenSSL发布安全公告，在OpenSSL1.0.1版本及其OpenSSL 1.0.2 Beta1中存在严重漏洞，由于未能正确检测用户输入参数的长度，攻击者可以利用该漏洞，远程读取存在漏洞版本的OpenSSL服务器内存中64K的数据，获取内存中的用户名、密码、个人相关信息以及服务器的证书等私密信息。可被用来获取敏感数据，包括会话Session、cookie、账号密码等。  
  
- 文件上传避免使用 ActiveXObject 方案，这是属于IE-only代码：兼容性问题  
  
- 注意避免直接用 key 访问关联数组的元素，要先判空，类似先检查 isset($\_POST['username']) ，再访问；  
  
3、防火墙规则，网络拓扑，阅读iptables，回答问题（INPUT、OUTPUT、FORWARD链）  
  
- iptables定义：规则（rules）其实就是网络管理员预定义的条件，规则一般的定义为“如果数据包头符合这样的条件，就这样处理这个数据包”。规则存储在内核空间的信息包过滤表中，这些规则分别指定了源地址、目的地址、传输协议（如TCP、UDP、ICMP）和服务类型（如HTTP、FTP和SMTP）等。当数据包与规则匹配时，iptables就根据规则所定义的方法来处理这些数据包，如放行（accept）、拒绝（reject）和丢弃（drop）等。配置防火墙的主要工作就是添加、修改和删除这些规则。  
  
- iptables传输数据包的过程  
  
  
    ① 当一个数据包进入网卡时，它首先进入PREROUTING链，内核根据数据包目的IP判断是否需要转送出去。   
  
    ② 如果数据包就是进入本机的，它就会沿着图向下移动，到达INPUT链。数据包到了INPUT链后，任何进程都会收到它。本机上运行的程序可以发送数据包，这些数据包会经过OUTPUT链，然后到达POSTROUTING链输出。   
  
    ③如果数据包是要转发出去的，且内核允许转发，数据包就会如图所示向右移动，经过FORWARD链，然后到达POSTROUTING链输出。  
  
  
- iptables的规则表和链：  
  
    表（tables）提供特定的功能，iptables内置了4个表，即filter表、nat表、mangle表和raw表，分别用于实现包过滤，网络地址转换、包重构(修改)和数据跟踪处理。  
  
    链（chains）是数据包传播的路径，每一条链其实就是众多规则中的一个检查清单，每一条链中可以有一条或数条规则。当一个数据包到达一个链时，iptables就会从链中第一条规则开始检查，看该数据包是否满足规则所定义的条件。如果满足，系统就会根据该条规则所定义的方法处理该数据包；否则iptables将继续检查下一条规则，如果该数据包不符合链中任一条规则，iptables就会根据该链预先定义的默认策略来处理数据包。  
  
    iptables采用“表”和“链”的分层结构。在REHL4中是三张表五个链。现在REHL5成了四张表五个链了，不过多出来的那个表用的也不太多，所以基本还是和以前一样。下面罗列一下这四张表和五个链。注意一定要明白这些表和链的关系及作用。  
  
  
  
- 规则表：  
  
    1.filter表 —— 三个链：INPUT、FORWARD、OUTPUT  
    作用：过滤数据包  内核模块：iptables\_filter.  
    2.Nat表 —— 三个链：PREROUTING、POSTROUTING、OUTPUT  
    作用：用于网络地址转换（IP、端口） 内核模块：iptable\_nat  
    3.Mangle表 —— 五个链：PREROUTING、POSTROUTING、INPUT、OUTPUT、FORWARD  
    作用：修改数据包的服务类型、TTL、并且可以配置路由实现QOS内核模块：iptable\_mangle(别看这个表这么麻烦，咱们设置策略时几乎都不会用到它)  
    4.Raw表 —— 两个链：OUTPUT、PREROUTING  
    作用：决定数据包是否被状态跟踪机制处理  内核模块：iptable\_raw  
    (这个是REHL4没有的，不过不用怕，用的不多)  
  
- 规则链：  
  
    1.INPUT——进来的数据包应用此规则链中的策略  
    2.OUTPUT——外出的数据包应用此规则链中的策略  
    3.FORWARD——转发数据包时应用此规则链中的策略  
    4.PREROUTING——对数据包作路由选择前应用此链中的规则  
    （记住！所有的数据包进来的时侯都先由这个链处理）  
    5.POSTROUTING——对数据包作路由选择后应用此链中的规则  
    （所有的数据包出来的时侯都先由这个链处理）  
  
  
- 规则表之间的优先顺序：  
  
    Raw——mangle——nat——filter  
  
- 规则链之间的优先顺序（分三种情况）：  
  
    第一种情况：入站数据流向  
  
    从外界到达防火墙的数据包，先被PREROUTING规则链处理（是否修改数据包地址等），之后会进行路由选择（判断该数据包应该发往何处），如果数据包的目标主机是防火墙本机（比如说Internet用户访问防火墙主机中的web服务器的数据包），那么内核将其传给INPUT链进行处理（决定是否允许通过等），通过以后再交给系统上层的应用程序（比如Apache服务器）进行响应。  
  
    第二种情况：转发数据流向  
  
    来自外界的数据包到达防火墙后，首先被PREROUTING规则链处理，之后会进行路由选择，如果数据包的目标地址是其它外部地址（比如局域网用户通过网关访问QQ站点的数据包），则内核将其传递给FORWARD链进行处理（是否转发或拦截），然后再交给POSTROUTING规则链（是否修改数据包的地址等）进行处理。  
  
    第三种情况：出站数据流向  
  
    防火墙本机向外部地址发送的数据包（比如在防火墙主机中测试公网DNS服务器时），首先被OUTPUT规则链处理，之后进行路由选择，然后传递给POSTROUTING规则链（是否修改数据包的地址等）进行处理。  
  
4、关键词概念-选择题  
  
5、黑客行为、黑客规则（那种说法正确/错误！！）  
  
    "黑客伦理"（hacker ethic），直到今天都被视为这方面的最佳论述：  
  
　　1. 使用计算机，不应受到任何限制。任何事情都应该亲手尝试。  
（Access to computers--and anything that might teach you something about the way the world works--should be unlimited and total. Always yield to the Hands-On Imperative!）  
  
　　2. 信息应该全部免费。  
（All information should be free.）  
  
　　3. 不信任权威，提倡去中心化。  
（Mistrust Authority--Promote Decentralization.）  
  
　　4. 判断一个人应该看他的技术能力，而不是看其他标准。  
（Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.）  
  
　　5. 你可以用计算机创造美和艺术。  
（You can create art and beauty on a computer.）  
  
　　6. 计算机使生活更美好。  
（Computers can change your life for the better.）  
  
  根据这六条"黑客伦理"，黑客价值观的核心原则可以概况成这样几点：分享（Sharing）、开放（Openness）、民主（Decentralization）、计算机的自由使用（Free access to computers）、进步（World Improvement）。  
  
  
6、CVSS 2.0和3.0的区别，局限，不足，基础评分  
  
- textbook  
  
7、IP地址不确定，匿名通信，追踪匿名通信客户端的方式  
  
\* 匿名通信方式，关系  
\* 匿名通信工具（洋葱）  
  
- 匿名通信的两种类型  
  
    匿名通信的技术大致可以分为两类：第一是转发机制（也可以叫基于重路由技术）；第二是通过广播和组播来实现匿名。   
  
    基于转发的匿名基本包括了我们常见的所有科学上网方式（比如ss，tor），其实这种机制的先祖大概是anonymizer系统。这是专门为发送者提供邮件中转的匿名系统。David Chaum 提出的 Mix-Net系统是基于转发机制的典型代表，这个系统使用了的很多实现匿名通信的技术，如：嵌套加密、数据包填充、延时、混合、缓存重排等。  
  
8、理解、认识局域网里监听方式多样：dhcp、dns、arp欺骗  
  
\* 局域网攻击手段和防御  
  
- 常见的局域网攻击类型有广播风暴、ARP欺骗攻击以及IP冲突攻击。  
  
- 局域网的缺陷   
  
    局域网一般由两层交换机或者共享式集线器组网，该类设备一般不具有基于IP地址的路由功能，故局域网内各节点间通过MAC地址（网卡物理地址）标识和通信，而MAC地址是由各个节点自行维护，这意味着我说我是谁我就是谁，这是局域网脆弱的根本因素之一。   
  
- 地址解析协议(ARP)，ARP(Address Resolution Protocol)，当内网节点间（或者是节点与网关间）需要通信时，ARP解析获得目标IP地址对应的MAC地址，通过该MAC地址完成数据包发送。ARP协议是局域网通信的基础，ARP协议是这样工作的：如主机B需要给主机A（IP为192.168.1.100)发送数据，为了知道谁是主机A，首先主机B发送一个广播包给网内所有机器“谁是192.168.1.10”，正常情况其他机器忽略该消息，仅主机A回复“俺就是192.168.1.10”，于是通信就可以开始。至于不正常情况就是本文的主题。  
  
- 域名解析系统(DNS)，互联网上的设备通过IP地址标识，全数子组成的标识不利于人类记忆和处理，域名的出现改变了这种状况，那么域名是如何对应的IP地址的呢，域名服务器（DNS服务器）就是来完成域名和IP地址的互相转换功能。DNS工作原理与ARP类似，区别是DNS通过指定的DNS服务器来查询，DNS服务器一般是安全的（实际上电信运营商等某些权威机构也经常耍流氓），问题是当明文的DNS数据包通过不安全的局域网时，会被篡改。  
  
- ARP欺骗攻击  
  
    ARP是地址转换协议（Address Resolution Protocol）的英文缩写，它是一个链路层协议，工作在OSI 模型的第二层，在本层和硬件接口间进行联系，同时对上层（网络层）提供服务。我们知道二层的以太网交换设备并不能识别32位的IP地址，它们是以48位以太网地址（就是我们常说的MAC地址）传输以太网数据包的。也就是说IP数据包在局域网内部传输时并不是靠IP地址而是靠MAC地址来识别目标的，因此IP地址与MAC地址之间就必须存在一种对应关系，而ARP协议就是用来确定这种对应关系的协议。  
      
    ARP工作时，首先请求主机会发送出一个含有所希望到达的IP地址的以太网广播数据包，然后目标IP的所有者会以一个含有IP和MAC地址对的数据包应答请求主机。这样请求主机就能获得要到达的IP地址对应的MAC地址，同时请求主机会将这个地址对放入自己的ARP表缓存起来，以节约不必要的ARP通信。ARP缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用，就会被删除。  
      
    局域网上的一台主机，如果接收到一个ARP报文，即使该报文不是该主机所发送的ARP请求的应答报文，该主机也会将ARP报文中的发送者的MAC地址和IP地址更新或加入到ARP表中。  
      
    ARP欺骗攻击就利用了这点，攻击者主动发送ARP报文，发送者的MAC地址为攻击者主机的MAC地址，发送者的IP地址为被攻击主机的IP地址。通过不断发送这些伪造的ARP报文，让局域网上所有的主机和网关ARP表，其对应的MAC地址均为攻击者的MAC地址，这样所有的网络流量都会发送给攻击者主机,ARP欺骗攻击导致了主机和网关的ARP表的不正确。  
  
- DHCP攻击：（1）DHCP服务器欺骗：客户端将自己配置为DHCP服务器分发虚假的IP地址，或直接响应DHCP请求（2）DHCP地址耗尽：客户端不断地冒充新客户机发送DHCP请求，请求服务器为自己分派IP地址，从而使服务器地址耗尽，而正常主机无法获得IP地址  
  
    DHCP工作过程：    ①首先由客户端以广播方式发出“DHCP Discover”报文来寻找网络中的DHCP服务端。  
  
                    ②当服务端接收到来自客户端的“DHCP Discover”报文后，就在自己的地址池中查找是否有可提供的IP地址。如果有，服务端就将此IP地址做上标记，并用“DHCP Offer”报文将之发送回客户端。  
  
                    ③由于网络中可能会存在多台DHCP服务端，所以客户端可能会接收到多个“DHCP Offer”报文。此时客户端只选择最先到达的“DHCP Offer”，并再次以广播方式发送“DHCP Request”报文。一方面要告知它所选择的服务端，同时也要告知其它没有被选择的服务端，这样这些服务端就可以将之前所提供的IP地址收回。  
  
                    ④被选择的服务端接收到客户端发来的“DHCP Request”报文后，首先将刚才所提供的IP地址标记为已租用，然后向客户端发送一个“DHCP Ack”确认报文，该报文中包含有IP地址的有效租约以及默认网关和DNS服务器等网络配置信息。  
  
                    当客户端收到“DHCP ACK”报文后，就成功获得了IP地址，完成了初始化过程。  
  
    DHCP攻击原理与实施  
  
                    下面搭建如图2所示的实验环境，神州数码CS6200交换机作为正常的DHCP服务端在网络中提供地址分配服务，攻击者在Kali Linux上对交换机发起DHCP攻击，使其地址池资源全部耗尽，然后攻击者再启用假冒的DHCP服务器在网络中提供地址分配服务。在假冒DHCP服务器所提供的网络配置信息中，默认网关被设置为Kali Linux的IP地址192.168.1.5（正确的默认网关应该是交换机的IP地址192.168.1.1），被攻击主机在获取了假冒DHCP服务器所提供的网络配置信息后，就会将所有的上网数据全部发送给Kali Linux。此时只要在Kali Linux上启用路由转发功能，就可以将被攻击主机的上网流量全部正常转发出去，因而并不影响其正常通信，但是其访问互联网的所有数据都可以在Kali Linux上被截取到。  
  
- 局域网DNS劫持  
  
    DNS决定的是我们的域名将解析到哪一个IP地址的记录，是基于UDP协议的一种应用层协议   
  
    这个攻击的前提是攻击者掌控了你的网关（可以是路由器，交换机，或者运营商），一般来说，在一个WLAN下面，使用ARP劫持就可以达到此效果。  
      
    你在访问一个网站的过程中,经历了如下几个阶段：   
    以访问freebuf的主页为例：  
      
    地址栏输入freebuf.com  
    访问本机的hosts文件，查找 freebuf.com 所对应的 IP，若找到，则访问该IP  
    若未找到，则进行这一步，去（远程的）DNS服务器上面找freebuf.com 的IP，访问该IP  
  
    中间人劫持就发生在第三步：由于恶意攻击者控制了你的网关，当你发送了一个查找freebuf.com的IP的请求的时候，中间人拦截住，并返回给你一个恶意网址的IP,你的浏览器就会把这个IP当做你想要访问的域名的IP!!这个IP是攻击者搭建的一个模仿了目标网站前端界面的界面，当你在该界面输入用户名密码或者付款操作的时候，就会中招。  
  
- 防范  
  
    \* dns劫持：使用SSL（HTTPS）进行登录，攻击者可以得到公钥，但是并不能够得到服务器的私钥当浏览器提示出现证书问题的时候，谨慎，再谨慎！确定你所在的网络环境是安全的，该网站是可信的再去访问。不在连接公共wifi的时候随意进行登陆操作 由于DNS劫持导向的界面的ＵＲＬ是完全正确的，因此 这类攻击一般极难分辨！   
  
    \* arp欺骗：  
    1、设置静态的MAC to IP对应表，并防止Hacker刷新静态转换表。莫把网络安全信任关系建立在IP基础上或MAC基础上，尽量将信任关系应该建立在IP+MAC上。    
    2、使用防火墙隔离非信任域对内网机器的ARP包传输。  
    3、定期使用RARP请求来检查ARP响应的真实性。  
    4、定期检查主机上的ARP缓存。  
    5、使用ARP探测工具，探测非法ARP广播数据帧。  
    6、给系统安装补丁程序。通过Windows Update安装好系统补丁程序(故只要做好对操作系统的升级与加固可以防止此类病毒感染。  
    7、给系统管理员帐户设置强密码，最好是“字母+数字+特殊符号”组合。  
    8、定时更新杀毒软件（病毒库），安装使用网络防火墙软件，可有效阻挡来自网络的攻击和病毒的入侵。盗版Windows用户若不能安装更新补丁，不妨通过使用网络防火墙等方法加强防护。  
  
    \* dhcp攻击：防范DHCP假冒攻击——在交换机上通过传统的DHCPSnooping技术就可以来防范DHCP假冒攻击。当启用了DHCP Snooping功能之后，交换机的所有端口都将无法接收DHCP Offer报文，这样假冒的DHCP服务器就无法向外分配IP地址了。防范DHCP耗尽攻击——DHCP Snooping功能只能防止假冒攻击，而无法防止耗尽攻击。这是由于耗尽攻击所采用的都是客户端正常发送的DHCPDiscover报文，因而DHCPSnooping对其无能为力。可以通过交换机的Port-Security(端口安全性)功能来防范耗尽攻击。  
  
      
9、开放式扫描，半开放式扫描，检测端口开放关闭检测手段，虚拟主机间相互通信（联网、不联网）  
  
- 端口端口一般是有下面这几种状态的  
  
     状态      详细的参数说明  
  
     Open     端口开启，数据有到达主机，有程序在端口上监控  
     Closed     端口关闭，数据有到达主机，没有程序在端口上监控  
     Filtered     数据没有到达主机，返回的结果为空，数据被防火墙或者是IDS过滤  
     UnFiltered     数据有到达主机，但是不能识别端口的当前状态  
     Open|Filtered     端口没有返回值，主要发生在UDP、IP、FIN、NULL和Xmas扫描中  
     Closed|Filtered 只发生在IP ID idle扫描  
  
- 端口扫描  
  
     1、TCP扫描（-sT） 2、SYN扫描（-sS） 3、UDP扫描（-sU）  
  
10、信息收集手段、作业（github chap0x06参考链接，解释字段含义）  
  
- 信息收集的方法可归为两类：主动式信息收集和被动式信息收集。主动式收集方法是通过直接发起与被测目标网络之间的互动来获取相关信息。例如，ICMP ping 或者 TCP 端口扫描就属于主动式信息收集手段。而被动信息收集方法，则是通过第三方服务来获取目标网络的相关信息，例如使用谷歌搜索引擎等。  
  
- chap0x06 DNS域传送漏洞及DNS信息收集实例讲解  
  
    \* 什么是dns区域传送漏洞  
  
     区域传送操作指的是一台后备服务器使用来自主服务器的数据刷新自己的zone数据库。这为运行中的DNS服务提供了一定的冗余度，其目的是为了防止主域名服务器因意外故障变得不可用时影响到全局。一般来说，DNS区域传送操作只在网络里真的有后备域名DNS服务器时才有必要执行，但许多DNS服务器却被错误地配置成只要有人发出请求，就会向对方提供一个zone数据库的拷贝。如果所提供的信息只是与连到因特网上且具备有效主机名的系统相关，那么这种错误配置不一定是坏事，尽管这使得攻击者发现潜在目标要容易得多。真正的问题发生在一个单位没有使用公用/私用DNS机制来分割外部公用DNS信息和内部私用DNS信息的时候，此时内部主机名和IP地址都暴露给了攻击者。把内部IP地址信息提供给因特网上不受信任的用户，就像是把一个单位的内部网络完整蓝图或导航图奉送给了别人。  
  
    dig axfr @nsztm1.digi.ninja zonetransfer.me  
    ; <<>DiG 9.9.5-3ubuntu0.6-Ubuntu <<>axfr @nsztm1.digi.ninja zonetransfer.me  
    ; (1 server found)  
    ;; global options: +cmd  
  
    #The information starts with the SOA record:  
  
    zonetransfer.me.7200IN  SOA nsztm1.digi.ninja. robin.digi.ninja. 2014101601 172800 900 1209600 3600  
  
    #此条目显示有关主名称服务器的信息，管理员的联系详细信息和其他关键信息，这是如何打破：  
    #nsztm1.digi.ninja。 - 主要名称服务器  
    #robin.digi.ninja。 - 负责人，这是域名负责人的电子邮件地址（换一个@）  
    #2014101601 - 域的当前序列号。这是由辅助名称服务器检查的值，以查看执行增量传输（IXFR）时是否有任何条目已更改。这个值通常是基于更改日期的某种方式  
    #172800 - 在提出更改请求之前，辅助名称服务器的时间（秒）应该等待  
    #900 - 如果主服务器无法正确刷新，应等待的重试时间（秒）  
    #1209600 - 辅助名称服务器可声称拥有权威信息的时间（秒）  
    #3600 - 这个域的最小TTL  
    #我们可以从中收集哪些安全信息？有两点我可以说是有用的，负责人字段给出一个电子邮件地址，可以用作其他攻击的一部分，从目前的序列号，如果是基于日期和定期检查，一个变化可能表明一些在公司的活动。  
  
    zonetransfer.me.300 IN  HINFO   "Casio fx-700G" "Windows XP"  
      
  
  
    #The MX records indicate where mail should be sent, these are the standard mail servers for Google indicating the company uses GMail or Google Apps to handle their email. From this you know that there is a minimum of spam and virus checking in place which helps when sending email for SE or client side attacks.  
    zonetransfer.me.7200IN  MX  0 ASPMX.L.GOOGLE.COM.  
    zonetransfer.me.7200IN  MX  10 ALT1.ASPMX.L.GOOGLE.COM.  
    zonetransfer.me.7200IN  MX  10 ALT2.ASPMX.L.GOOGLE.COM.  
    zonetransfer.me.7200IN  MX  20 ASPMX2.GOOGLEMAIL.COM.  
    zonetransfer.me.7200IN  MX  20 ASPMX3.GOOGLEMAIL.COM.  
    zonetransfer.me.7200IN  MX  20 ASPMX4.GOOGLEMAIL.COM.  
    zonetransfer.me.7200IN  MX  20 ASPMX5.GOOGLEMAIL.COM.  
  
  
    zonetransfer.me.7200IN  A   217.147.180.162  
  
    #The name servers for this domain. It is always worth checking for zone transfers on all available name servers, I've seen a number of clients with multiple servers where, for an unknown reason, a single server has zone transfer enabled. You can also look for differences in output which may leak useful information.  
    zonetransfer.me.7200IN  NS  nsztm1.digi.ninja.  
    zonetransfer.me.7200IN  NS  nsztm2.digi.ninja.  
  
  
    #SRV记录是一个服务记录，它通过显示它所运行的协议，主机和端口来识别服务。这通常用于VOIP设置以指示SIP服务器的位置，但可用于任何类型的服务。SRV记录可以显示关于目标公司正在运行的服务的一些非常有用的信息。  
    #记录分解如下：  
    #\_sip.\_tcp.zonetransfer.me - 服务的名称，包括协议名称和TCP / UDP，这里是通过TCP运行的SIP  
    #SRV中的14000 - 标准DNS值，TTL，DNS类别和类型  
    #0 - 服务的优先级，如果有多个服务，则表示首先尝试哪个服务  
    #0 - 权重，当两个服务具有相同的优先级时，表示哪个是首选  
    #5060 - 服务正在侦听的端口  
    #www.zonetransfer.me。 - 提供服务的主机  
    #\_sip.\_tcp.zonetransfer.me. 14000 IN SRV 0 0 5060 www.zonetransfer.me.  
  
    #PTR记录将IP地址映射回域名。  
    164.180.147.217.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.  
  
  
    asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.  
    asfdbbox.zonetransfer.me. 7200  IN  A   127.0.0.1  
    asfdbvolume.zonetransfer.me. 7800 INAFSDB   1 asfdbbox.zonetransfer.me.  
    canberra-office.zonetransfer.me. 7200 IN A  202.14.81.230  
    cmdexec.zonetransfer.me. 300IN  TXT "\; ls"  
    dc-office.zonetransfer.me. 7200 IN  A   143.228.181.132  
    deadbeef.zonetransfer.me. 7201  IN  AAAAdead:beaf::  
  
  
    #LOC是LOC的缩写，可以用来记录纬度/经度值。这些值以度/分/秒存储，如果您想在Google Maps中查看这些值，则需要先将其转换为小数点。  
    dr.zonetransfer.me. 300 IN  LOC 53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m  
  
  
    #TXT记录是文本信息，应始终检查有价值的信息。这里的第一个漏了一个明显与系统管理有关的人的电话号码和电子邮件地址。第二个显示该网站已经过验证可用于Google Apps帐户。第三种方法是GoDaddy用来检查申请SSL证书的人是否拥有域名的方式，如果这些信息泄漏了关于正在使用的服务或从属关系的信息，这种信息可能是有用的。  
    contact.zonetransfer.me. 2592000 IN TXT "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS changes"  
    zonetransfer.me.301 IN  TXT "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"  
    DZC.zonetransfer.me.7200IN  TXT "AbCdEfG"  
    Info.zonetransfer.me.   7200IN  TXT "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php for more information."  
  
  
    email.zonetransfer.me.  2222IN  NAPTR   1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.  
    email.zonetransfer.me.  7200IN  A   74.125.206.26  
      
    internal.zonetransfer.me. 300   IN  NS  intns1.zonetransfer.me.  
    internal.zonetransfer.me. 300   IN  NS  intns2.zonetransfer.me.  
    intns1.zonetransfer.me. 300 IN  A   167.88.42.94  
    intns2.zonetransfer.me. 300 IN  A   167.88.42.94  
    office.zonetransfer.me. 7200IN  A   4.23.39.254  
    ipv6actnow.org.zonetransfer.me. 7200 IN AAAA2001:67c:2e8:11::c100:1332  
    owa.zonetransfer.me.7200IN  A   207.46.197.32  
    robinwood.zonetransfer.me. 302  IN  TXT "Robin Wood"  
    rp.zonetransfer.me. 321 IN  RP  robin.zonetransfer.me. robinwood.zonetransfer.me.  
    sip.zonetransfer.me.3333IN  NAPTR   2 3 "P" "E2U+sip" "!^.\*$!sip:customer-service@zonetransfer.me!" .  
    sqli.zonetransfer.me.   300 IN  TXT "' or 1=1 --"  
    sshock.zonetransfer.me. 7200IN  TXT "() { :]}\; echo ShellShocked"  
    alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1  
  
  
    #The company has a test site which sits on the same server as the main web site. Test sites are often less secured than main sites so could be a better attack vector. The company also has a staging server which should also be looked at.  
    staging.zonetransfer.me. 7200   IN  CNAME   www.sydneyoperahouse.com.  
    testing.zonetransfer.me. 301IN  CNAME   www.zonetransfer.me.  
  
  
  
    vpn.zonetransfer.me.4000IN  A   174.36.59.154  
    www.zonetransfer.me.7200IN  A   217.147.180.162  
    xss.zonetransfer.me.300 IN  TXT "'><script>alert('Boo')</script>"  
    zonetransfer.me.7200IN  SOA nsztm1.digi.ninja. robin.digi.ninja. 2014101601 172800 900 1209600 3600  
    ;; Query time: 21 msec  
    ;; SERVER: 81.4.108.41#53(81.4.108.41)  
    ;; WHEN: Fri Feb 05 08:58:44 GMT 2016  
    ;; XFR size: 47 records (messages 1, bytes 1846)  
  
  
    #如何阅读以上的内容：  
    空白和www - 主要网站，总是有利于漏洞  
    vpn - 如果你能通过VPN服务器找到方法，那么你通常可以绕过任何IDS / IPS  
    owa - 通常代表Outlook Web Access，因为MX记录表明该公司正在使用Google收发邮件，所以这可能意味着他们正在下拉邮件，然后使用Exchange重新发布邮件。我也从中读到，他们可能是一家微软商店。  
    办公室，canberra\_office和dc\_office - 从这里我可以说，办公室是主要的位置，堪培拉和特区是后来建立的。与办公室相关的知识产权地理位置表明，总部位于英国。有两件事你可以从中获得，办公室往往不如数据中心更好的保护，所以可能比网络或VPN服务器更好的目标，使用这个位置信息，你可以计时你的攻击，使他们是最有效的，例如在长周末开始的星期五下班后进行攻击，防守者可能不会注意到三天的攻击。  
    我不断添加额外的条目，所以不是所有你会发现已被描述，看看周围，看看你能找到什么额外的宝石。对于奖励标志，看看你是否可以转储内部的DNS记录，所有你需要的信息都会给你。  
      
    所以，我就是这样读取信息的，那里有很多有用的东西，都是因为配置不当而泄露的。我们知道他们正在使用Google的邮件，但也可能在内部使用Exchange，我们知道他们的DR站点的位置，甚至可以通过Google街景视图获取它的照片。我们有两个电子邮件地址和系统管理员的电话号码，可以用于客户端和SE攻击。他们有一个SIP系统，我们知道作为网关的机器的IP和端口。我们有三个数据中心IP和三个来自A记录的办公室IP，它提供了六个可能的目标以及一个测试和登台服务器。我们可以假设他们已经从GoDaddy购买了SSL证书，并且正在使用Google Apps来管理他们的域名。  
  
11、whois查询：字段含义  
  
  
  
12、链路层：进入局域网，突破了外部网络连接（arp欺骗）防御者角度如何防御（地址绑定、vlan）  
  
- arp欺骗 原理： 原理简析  
    局域网内某主机运行ARP欺骗程序时，会诱骗局域网内所有主机和路由器，使上网流量必须经由该病毒主机。原来通过路由器上网的用户现在转由病毒主机，这个切换会致使用户断线。切换到病毒主机上网后，如果用户已经登录了传奇服务器，病毒主机会不断制造断线的假象，用户就得重新登录，病毒主机就可以趁机实施盗号行为。ARP欺骗木马程序发作会发送大量数据包，从而导致局域网通讯拥塞，受自身处理能力的限制，用户会感觉网速越来越慢。ARP欺骗木马程序停止运行，用户会恢复从路由器上网，该切换则会导致用户再次断网。  
  
  
- ARP攻击的局限性  
  
    ARP攻击仅能在以太网（局域网如：机房、内网、公司网络等）进行。无法对外网（互联网、非本区域内的局域网）进行攻击。  
  
- 攻击手段：  
  
1、 一般冒充欺骗  
  这是一种比较常见的攻击，通过发送伪造的ARP包来实施欺骗。根据欺骗者实施欺骗时所处的立场，可分为三种情况：冒充网关欺骗主机、冒充主机欺骗网关、冒充主机欺骗其它主机。在冒充网关欺骗中，欺骗者定时且频繁的对本网发送ARP广播，告诉所有网络成员自己就是网关，或者以网关身份伪造虚假的ARP回应报文，欺骗局域网内的其它主机，这样子网内流向外网的数据就可以被攻击者截取；冒充主机欺骗网关的过程跟冒充网关的过程相反，欺骗者总是通过虚假报文告诉网关，自己就是目标主机，从而使网关向用户发送的数据被攻击者截取；冒充主机欺骗其它主机则是同一网内设备间的欺骗，攻击者以正常用户的身份伪造虚假ARP回应报文，欺骗其它主机，结果是其它用户向该用户发送的数据全部被攻击者截获。  
2、虚构MAC地址欺骗  
  这种攻击也是攻击者以正常用户身份伪造虚假的ARP回应报文，欺骗网关。但是，和上述一般冒充欺骗不同的是，此时攻击者提供给网关的MAC地址根本不存在，不是攻击者自己的MAC地址，这样网关发给该用户的数据全部被发往一个不存在的地方。  
3、ARP泛洪  
  这是一种比较危险的攻击，攻击者伪造大量虚假源MAC和源IP信息报文，向局域网内所有主机和网关进行广播，目的就是令局域网内部的主机或网关找不到正确的通信对象，甚至直接用虚假地址信息占满网关ARP缓存空间，造成用户无法正常上网。同时网络设备CPU居高不下，缓存空间被大量占用。由于影响到了网络设备，攻击者自己上网的效率也很低，这是一种典型的损人不利己行为。  
    4、基于ARP的DoS  
    这是新出现的一种攻击方式，DoS又称拒绝服务攻击，当大量的连接请求被发送到一台主机时，由于该主机的处理能力有限，不能为正常用户提供服务，便出现拒绝服务。这个过程中如果使用ARP来隐藏自己，被攻击主机日志上就不会出现真实的IP记录。攻击的同时，也不会影响到本机。  
  
- ARP欺骗鉴定方法  
1、检查网内感染“ARP欺骗”木马病毒的计算机  
 在“命令提示符”下输入并执行“ipconfig”命令，记录网关IP地址，即“Default Gateway”对应的值，例如“192.168.18.1”。然后执行“arp -a”命令查看自己网关MAC地址，如若变成和内网一机器MAC地址相同，可据此断定内网有机器中了ARP网关欺骗型病毒。本操作前提是知道网关的正确MAC地址，可在正常上网主机上，使用“arp -a”命令查看网关MAC地址，通过对比查看网关MAC地址是否被修改。  
2、查看ARP表  
 用三层设备接入校园网的单位，网管可以检查其三层设备上的ARP表。如果有多个IP对应同一个MAC，则此MAC对应的计算机很可能中了木马病毒。可通过下连二层交换机的转发表查到此MAC对应的交换机端口，从而定位有问题的计算机。  
      
- 如何防御：  
  
    1、实现网关和终端双向绑定IP和MAC地址  
    2、设置ARP个人防火墙  
    3、通过划分VLAN和交换机端口绑定，以图防范ARP，也是常用的防范方法。做法是细致地划分VLAN，减小广播域的范围，使ARP在小范围内起作用，而不至于发生大面积影响。  
    4、网络下面给每一个用户分配一个帐号、密码，上网时必须通过PPPoE认证  
    5、实施一个免疫网络：免疫网络就是在现有的路由器、交换机、网卡、网线构成的普通交换网络基础上，加入一套安全和管理的解决方案。  
  
13、漏洞攻防：漏洞成因、代码层面什么样的会产生漏洞，如何规避-shiziyu  
  
    一、SQL注入  
  
    （1）注入产生原理  
    使用用户输入的参数拼凑SQL语句，用户对服务器端代码里的SQL语句可控，使服务器执行恶意的sql命令  
      
    http://bbs.pconline.com.cn/topic.jsp?tid=1 ' and 1=2  
      
    （2）万能密码  
    select \* from tb\_name where name = ' ' or 1=1 - - '  and  passwd = ' '  
      
      
    （3）危害  
    数据库泄露，撞库攻击，法律责任（个人信息泄露）  
      
    （4）防御方法  
    1.绑定变量：使用SqlBuilder  
      
      
    2.使用安全的存储过程  
      
    3.检查数据类型  
      
    4.使用过滤函数  
      
      
      
    二、越权操作  
      
    （1）平行越权漏洞  
    只要一个账户即可控制全站用户数据。当然这些数据仅限于存在漏洞功能对应的数据。越权漏洞的成因主要是因为开  
      
    发人员在对数据进行增、删、改、查询时对客户端请求的数据过分相信而遗漏了权限的判断。  
      
    案例分析：删除帖子时没有判断当前用户是否有权限删除该帖子，导致其他用户的帖子也被删掉了  
      
    （2）垂直越权操作漏洞  
    基于角色的权限管理，又称为“垂直权限管理”。不同角色的权限有高低之分。高权限角色访问低权限角色的资源往往  
      
    是被允许的，而低权限角色访问高权限角色的资源往往是被拒绝的。如果低权限角色获得了高权限角色的能力，那么  
      
    就发生了“越权访问”  
      
      
      
    三、跨站脚本攻击(XSS)  
      
    （1）简介  
    恶意攻击者通过某些输入点往Web页面里插入脚本代码，当用户浏览页面或执行某种操作时，就会触发嵌入的脚本代码，从而实现  
      
    恶意攻击。  
      
    （2）分类  
    1.存储型XSS(Stored XSS)  
      
    存入了数据库，再取出来时导致的xss。  
      
    2.反射型XSS(Reflected XSS)  
      
    案例：在网址url后输入xss代码，如<script>alert(1)</script>，然后访问时导致html页面加载这段代码即可达到弹框效果  
      
      
    3.DOM型XSS(DOM Based XSS)其实也是反射型的一种  
      
    严格来说该xss也属于反射型，本文的例子其实也是dom based，是指修改页面的dom对象模型，从而达成攻击，比如  
      
    页面使用了document.write\document.writeln\innerhtml等dom方法有可能引起dom based xss  
      
    案例：  
      
    http://datalib.ent.qq.com/cgi-bin/search?libid=1&keyvalue=aaaaaaa&attr=133&stype=2&tname=star\_second.shtml  
      
      
    相关代码：  
      
    if("职业1"=="职业1")  
      
    document.getElementById("titleshow").innerHTML="按职业检索：aaaaaaa";  
      
    传入的keyvalue加上xss攻击：  
      
    http://datalib.ent.qq.com/cgi-bin/search?libid=1&keyvalue=\x3Cimg\u0020src=1\u0020onerror=alert(1)  
      
    \x3e&attr=133&stype=2&tname=star\_second.shtml  
      
    经过运行后， titleshow 里的HTML就会变为 <img src=1 onerror=alert(1)> ，从而弹出1。  
      
      
      
    （3）如何防止跨站脚本攻击(XSS)  
      
    1.输出过滤  
    2.其他方法  
      
    A. HTML标签的属性必须使用引号。  
    B. 页面插入可疑flash时allowScriptAccess必须设置为never。  
    C. JSON接口返回的Content-Type为application/json。  
    D. 提供给应用调用的接口数据格式使用JSON。  
    E. 不要将可疑的数据作为HTML标签属性。  
    F. 不要将可疑的数据放到CSS属性中。  
    G. 尽可能避免多层输出。  
    H. 避免使用Javascript操作cookie。  
      
      
 四、跨站请求伪造(CSRF)  
      
    （1）简介  
    CSRF（Cross-site request forgery跨站请求伪造，也被称成为“one click attack”或者session riding，通常缩写为  
      
    CSRF或者XSRF，是一种对网站的恶意利用。  
      
    （2）发生原因  
    网站是通过cookie来识别用户的，当用户成功进行身份验证之后浏览器就会得到一个  
      
    标识其身份的cookie，只要不关闭浏览器或者退出登录，以后访问这个网站会带上这个cookie。  
      
    1.登录受信任网站A，并在本地生成Cookie。  
      
    2.如果在用户登录访问网站A的同时访问了网站B，访问者在网站A的数据就会被B使用用户cookie假冒更新。  
      
    （3）案例  
    假如某网银转账操作是以GET请求来完成：http://www.mybank.com/Transfer.php?toBankId=11&money=1000  
      
    网站B，它里面有一段HTML的代码如下：  
      
    <img src=http://www.mybank.com/Transfer.php?toBankId=11&money=1000>  
      
    当我在网银cookie有效的情况下访问了网站B，那我的网银就莫名其妙的  
      
    被转账了1000。。。  
      
    （4）防御方法  
    1.验证码与二次验  
    2.对请求的referer进行检测  
    3.添加随机token校验  
      
    五、拒绝服务  
      
    （1）CC（Challenge Collapsar）攻击  
      
    （2）防御  
    1.限制参数大小  
      
    2.sql查询性能优化  
  
14、防火墙规则：设置默认链（示例题目）  
  
15、snort规则  
  
Snort IDS（入侵检测系统）是一个强大的网络入侵检测系统。它具有实时数据流量分析和记录IP网络数据包的能力，能够进行协议分析，对网络数据包内容进行搜索/匹配。它能够检测各种不同的攻击方式，对攻击进行实时报警。此外，Snort是开源的入侵检测系统，并具有很好的扩展性和可移植性。  
  
  
16、ppt09-63页，蜜罐放哪，内网防火墙放哪  
  
  
  
校园网入侵防御系统由防火墙、NIPS和蜜罐系统三级防御体系组成。防火墙部署在内网和外网之间，监控内、外网之间的访问流量，保障内网安全。NIPS部署在防火墙之后，检测网络流量，并对攻击进行主动防御。蜜罐作为独立系统部署，一方面蜜罐是防火墙很好的补充，它能够伪装成被攻击的主机和攻击者交互，捕获黑客的入侵活动并记录日志，利用这些日志信息可以制定出新的安全策略，更新检测规则和防火墙的策略，从而起到弥补误报、漏报缺陷和完善防火墙安全策略的作用。另一方面，蜜罐吸引攻击者对真实网络的注意力，让攻击者把时间都花费在对蜜罐的攻击上，保护了真实网络的安全，减小了防火墙和未能检测到的攻击对网络造成的损失，提高了加强网络防范的效率。可见由防火墙、NIPS和蜜罐系统三级防御体系构成的校园网安全防御系统大大降低了网络攻击所造成的损失。  校园网入侵防御系统的总体框架如图1所示。整个框架由防火墙系统、NIPS、蜜罐系统、日志管理系统和系统控制中心组成。从图1中可以看到，防火墙、NIPS和蜜罐系统将各自的日志/报警信息交给日志管理系统；日志管理系统负责收集日志/报警信息并将信息交给系统控制中心处理。系统控制中心负责分析日志/报警信息，根据分析结果制定出新的安全策略并及时更新防火墙策略和NIPS的检测规则。另外，系统控制中心还负责集中控制防火墙、NIPS、蜜罐系统和日志管理系统的运行。  
  
17、识别文件类型（不只看扩展名或图标）  
  
使用WinHex软件查看硬盘或文件或内存中的原始字节内容。根据文件头判断  
  
18、电信诈骗案例：行为的正确与错误  
  
19、物理场景错误（违反信息安全管理机制）  
        锁屏、门禁...  
  


（1）离开前清空公文格，并清理工作环境中的敏感信息  
（2）将抽屉上锁，并将钥匙保存在安全的地方  
（3）当你的工作场所不在注意范围内时，安全保管你的电脑  
（4）从墙上、桌子上清除敏感信息  
（5）使用完文档后将其归档  
（6）将秘密信息安全存储  
（7）不使用磁盘和CD时，将其安全存储  
  
\* 主动：扫描  
\* 被动：嗅探   
  
从行为上来说，嗅探器是被动的获取别人的数据包，而扫描器是主动的发出某些特定的数据包（如检测对方端口是否开放，弱口令，溢出等）,然后等待目标回应从而判断对方是否开放相应的端口啊等信息。  
从应用范围说，嗅探器主要用于局域网环境，对网段的某些或者全部机器进行数据包的监听，以获取某些信息（如Mail,FTP密码）等。而扫描器没有环境的要求任何机器都可以下载使用。