Atitt common hacker tech常见黑客技术

目录

[1. 搜集信息 嗅探技术 钓鱼网站 1](#_Toc14281)

[1.1. 建立公共wifi嗅探 1](#_Toc20239)

[1.2. Logging技术 2](#_Toc6174)

[1.3. .键盘记录 2](#_Toc21624)

[1.4. 5.窃听(被动攻击) 3](#_Toc19527)

[1.5. 屏幕定时截屏 3](#_Toc17394)

[2. 木马病毒技术 3](#_Toc20123)

[2.1. 远程控制，木马技术 3](#_Toc27856)

[2.2. 遥控技术 3](#_Toc24085)

[2.3. 发短信控制对方手机、智能电视自动打开上演午夜惊魂… 3](#_Toc21324)

[2.4. 10.诱饵和开关 3](#_Toc21124)

[2.5. 六、对任意挂马攻陷整个城市 4](#_Toc19056)

[3. 制造利用漏洞 sql注入 shell注入等漏洞 文件上传运行漏洞 4](#_Toc2912)

[4. 劫持技术 拦截器 4](#_Toc29217)

[4.1. 8.单击“杰克攻击” 4](#_Toc5661)

[4.2. 9. Cookie被盗 也称为SideJacking或Session Hijacking 5](#_Toc25247)

[4.3. 流量劫持 5](#_Toc20524)

[4.4. Url劫持 5](#_Toc22780)

[4.5. 会话劫持（Sidejacking） 5](#_Toc10774)

[5. 渗透 6](#_Toc5208)

[6. 6](#_Toc7248)

[7. 攻击技术 流量攻击 消耗资源攻击 6](#_Toc20960)

[7.1. 2.拒绝服务(DoS DDoS) 6](#_Toc9139)

[7.2. 爬虫爬取攻击 6](#_Toc1508)

# 搜集信息 嗅探技术 钓鱼网站

## 建立公共wifi嗅探

在你使用公共 Wi-Fi 时会有以下 5 种方式可能泄露你的数据：

1. 中间人攻击

2. 虚假的 Wi-Fi 连接

3. 数据包嗅探

4. 会话劫持

5. 肩部窥探。

## Logging技术

## .键盘记录

Keylogger是一个简单的软件，可将键盘的按键顺序和笔划记录到机器的日志文件中。这些日志文件甚至可能包含您的个人电子邮件ID和密码。也称为键盘捕获，它可以是软件或硬件。虽然基于软件的键盘记录器针对安装在计算机上的程序，但硬件设备面向键盘，电磁辐射，智能手机传感器等。

## ****5.窃听(被动攻击)****

与使用被动攻击的自然活动的其他攻击不同，黑客只是监视计算机系统和网络以获取一些不需要的信息。

窃听背后的动机不是要损害系统，而是要在不被识别的情况下获取一些信息。这些类型的黑客可以针对电子邮件，即时消息服务，电话，Web浏览和其他通信方法。那些沉迷于此类活动的人通常是黑帽黑客，政府机构等。

## 屏幕定时截屏

# 木马病毒技术

## 远程控制，木马技术

## 遥控技术

## 发短信控制对方手机、智能电视自动打开上演午夜惊魂…

## 10.诱饵和开****关****

黑客可以运行用户认为是真实的恶意程序。这样，在您的计算机上安装恶意程序后，黑客就可以无权访问您的计算机。

## ****六、对任意挂马攻陷整个城市****

无需入侵任何服务器，执行完全合法的操作，即可让整个城市网民访问任何网站时，都可能遭到网页挂马

## 手机远程unlock

# 制造利用漏洞 sql注入 shell注入等漏洞 文件上传运行漏洞

# 劫持技术 拦截器

## ****8.单击“杰克攻击”****

ClickJacking也有一个不同的名称，UI Redress。在这次攻击中，黑客隐藏了受害者应该点击的实际UI。这种行为在应用下载，电影流和torrent网站中非常常见。虽然他们大多使用这种技术来赚取广告费，但其他人可以使用它来窃取您的个人信息。

换句话说，在这种类型的黑客攻击中，攻击者劫持了受害者的点击，这些点击不是针对确切的页面，而是针对黑客想要的页面。它的工作原理是通过点击隐藏链接欺骗互联网用户执行不受欢迎的操作。

## ****9. Cookie被盗**** 也称为SideJacking或Session Hijacking

浏览器的cookie保留我们的个人数据，例如我们访问的不同站点的浏览历史记录，用户名和密码。一旦黑客获得了对cookie的访问权限，他甚至可以在浏览器上验证自己。执行此攻击的一种流行方法是鼓励用户的IP数据包通过攻击者的计算机。

也称为SideJacking或Session Hijacking，如果用户未在整个会话中使用SSL(https)，则此攻击很容易执行。在您输入密码和银行详细信息的网站上，对他们加密连接至关重要。

## 流量劫持

## Url劫持

## 会话****劫持（Sidejacking）****

Sidejacking 依赖于通过数据包嗅探获取信息。然而，黑客并没有追溯使用该数据，而是在现场实时使用它。更糟糕的是，它绕过了某种程度的加密！

登录详细信息通常通过加密网络发送，并使用网站持有的帐户信息进行验证。然后使用发送到你设备的 cookie 进行响应。但后者并不总是加密的——黑客可以劫持你的会话并访问你登录的任何私人帐户。

# 渗透

# 

# 攻击技术 流量攻击 消耗资源攻击

## ****2.拒绝服务(DoS DDoS)****

拒绝服务攻击是一种黑客攻击技术，通过充斥大量流量使服务器无法实时处理所有请求并最终崩溃的站点或服务器来关闭站点或服务器。这种流行的技术，攻击者使用大量请求来淹没目标计算机以淹没资源，这反过来限制了实际请求的实现。

对于DDoS攻击，黑客经常部署僵尸网络或僵尸计算机，这些计算机只能通过请求数据包充斥您的系统。随着时间的推移，随着恶意软件和黑客类型不断发展，DDoS攻击的规模不断增加

## 爬虫爬取攻击