十三、安全和匿名

Linux黑客基础–99–安全和匿名–互联网是如何出卖我们的

在互联网上如何保持匿名，不被跟踪，有以下方法

- **The Onion Network（暗网）**

“暗网”是指隐藏的网络，普通网民无法通过常规手段搜索访问，需要使用一些特定的软件、配置或者授权等才能登录。由于“暗网”具有匿名性等特点，容易滋生以网络为勾联工具的各类违法犯罪，一些年轻人深陷其中。记者在中国裁判文书网上搜索显示，涉“暗网”的案件共有21例，涉及贩卖毒品、传播色情恐怖非法信息、侵害公民个人信息等犯罪行为。 [1]

互联网是一个多层结构，“表层网”处于互联网的表层，能够通过标准搜索引擎进行访问浏览。藏在“表层网”之下的被称为“深网”。深网中的内容无法通过常规搜索引擎进行访问浏览。“暗网”通常被认为是“深网”的一个子集，显著特点是使用特殊加密技术刻意隐藏相关互联网信息。 [2]

暗网是利用加密传输、P2P对等网络、多点中继混淆等，为用户提供匿名的互联网信息访问的一类技术手段，其最突出的特点就是匿名性。 [3]

- **洋葱网络**

洋葱网络 (以下简称为 Tor) 这个名字也是十分有意思的，“洋葱”一词形象地描述了资料在其网络中传输过程的封装，而在接下来的这个章节中，我们将简单介绍一下 Tor的技术实现，以及 Tor 是怎麽使你“隐藏”在大众之中的。

- **代理服务器**

代理（英文：Proxy）也称网络代理，是一种特殊的网络服务，允许一个网络终端（一般为客户端）通过这个服务与另一个网络终端（一般为服务器）进行非直接的连接。一些网关、路由器等网络设备具备网络代理功能。一般认为代理服务有利于保障网络终端的隐私或安全，以防止攻击。

- **虚拟专用网络**

VPN(全称：Virtual Private Network)虚拟专用网络，是依靠ISP和其他的NSP，在公共网络中建立专用的数据通信的网络技术，可以为企业之间或者个人与企业之间提供安全的数据传输隧道服务。

- **私有加密的电子邮件**

Linux黑客基础–100–安全和匿名–洋葱路由系统

Tor依靠对计算机操作多次加密，通过多个网络节点（即“洋葱路由器”）选择路径，来隐藏计算机操作的来源、目的地和内容。Tor的用户是无法被追踪的，使用Tor隐匿服务的这些网站、论坛、博客也无法追踪，它们使用的是同样的流量加密系统来隐藏定位

要启用 Tor，只需从 https://www.torproject.org/安装 Tor 浏览

Linux黑客基础–101–安全和匿名–代理服务器概述

代理服务器相当于一个中间人的角色

当用户流量提交给代理服务器后，代理服务器代替用户向目标主机发送请求。

目标主机在返回流量时，也只是返回给代理服务器，并不是直接回送给用户主机，

而是有代理服务器返回给主机

通过这种方式，流量似乎来自代理，而不是原始IP地址

在代理服务器时可以使用多级代理，组成代理链

在内网的渗透测试当中代理服务器可以充当攻击的跳板（中枢）

Linux黑客基础-102-安全和匿名-proxychains介绍

代理（客户端）工具-proxychains

proxychains4 – redirect connections through proxy servers

可以通过代理服务器重定向链接

This program forces any tcp connection made by any given tcp client to follow through proxy (or proxychain). It is a kind of proxifier.

It acts like sockscap / premeo / eborder driver (intercepts TCP calls).

这个程序强制任何给定的tcp客户端建立的任何tcp连接通过代理(或代理) 链)。它是一种代理客户端程序。 它类似于sockscap / premeo / eborder驱动程序(拦截TCP调用)。

When to use it?

1）When the only way to get "outside" from your LAN is through proxy server.

当局域网仅能通过代理服务器到达外部（如互联网）

2）When you are behind restrictive firewall which filters outgoing connections to some ports.

当你处在受限的防火墙（如过滤了到达一些端口的连接）后

3）When you want to use two (or more) proxies in chain:

like: your_host <--> proxy1 <--> proxy2 <--> target_host

当你向使用多个代理时

4）When you want to "proxify" some programs with no proxy support built-in (like telnet).

当你想代理一些没有内置代理支持的程序时（如telnet）

5）When you don't want to pay for eBorder / premeo socks driver :)

Linux黑客基础-103-安全和匿名-proxychains实战

1、配置代理服务器

ccproxy-----windows平台下　　http://www.ccproxy.com/

squid ___Linux平台下常用的代理服务器

2、. Proxychains的配置

默认的配置文件：　/etc/proxychains4.conf

代理的格式

　　type　ip　port [user pass]

　　类型　代理服务器的IP地址　端口　[用户名 密码]

　　代理的类型有HTTP、SOCKS代理等

语法

proxychains4 [-f 配置文件] <程序>

【案例1】

以匿名的方式扫描目标主机

nmap -sT -Pn 主机

　　-sT　tcp的连接扫描

　　-Pn　禁用主机（假设主机是存活的）

Step01 修改/etc/proxychains4.conf

最后

socks4　　192.168.195.1 1080

```
┌──(root💀kali)-[~/桌面/work]
└─# proxychains4 nmap -sT -Pn 192.168.1.253
```

Socks是一种代理服务，可以将一端的系统连到另一端。

Socks支持多种协议，如HTTP、FTP

Socks分为Socks4和Socks5两种类型

Socks4只支持TCP协议

Socks5可以支持TCP和UDP协议，还支持各种身份验证机制

标准端口为1080

【案例2】通过代理上外网

proxychains firefox www.163.com

```
┌──(root💀kali)-[~/桌面/work]
└─# proxychains firefox www.163.com
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
```

Linux黑客基础–104–安全和匿名–proxychains三种代理模式

proxychains的代理方式有三种：

Different chaining options are supported. For instance:

- take random proxy from the list（random_chain ）

- chain proxies in exact order（strict_chain，严格的代理）

- chain proxies in dynamic order (smart exclude dead proxies from chain）dynamic_chain

strict_chain，严格的代理（默认）

所有的代理都会发挥作用，如果有一个代理不在线，则会报错

all proxies chained in the order as they appear in the list

all proxies must be online to play in chain

otherwise EINTR is returned to the app

dynamic_chain 动态的代理

我们可以设置动态链（ dynamic chaining）它通过列表中

的每个代理运行我们的流量，如果其中一个代理宕机或没有响应，则自动转到列表中的下一个代理，而不会抛出错误。如果我们不设置这个， 则其中一个失败的代理将会破坏我们整个的请求。

random_chain 随机的代理

其中 proxychain 将从列表中随机选择一组 IP地址，并使用它们创建代理链。

这意味着每次我们使用 proxychain时，代理对目标的外观都会有所不同，这使得从源跟踪我们的流量变得更加困难。

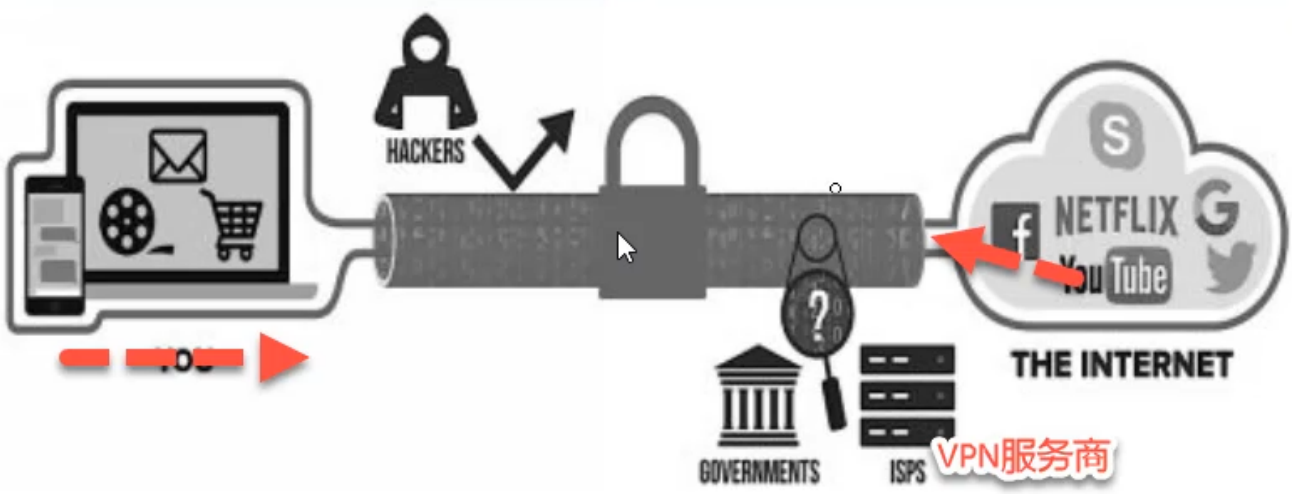
这个选项也被认为是“动态”的，因为如果一个代理关闭，它将跳到下一个代理。

同时只能设置一种。

Linux黑客基础-105-安全和匿名-VPN

什么是VPN?

全称为virtual private network （虚拟专用网络）



优势：费用低、安全可靠

从个人角度，VPN的好处：

（1）保护隐私

（2）加密流量

（3）科学上网

闪电

https://sdyun.cc/

任何人看到您的流量来自互联网VPN 设备的 IP 地址和位置，而不是您自己的。

另外，您与 VPN 设备之间的所有通信都是加密的，所以即使您的互联网服务提供商也看不到您的通信

VPN service for secure, anonymous and unrestricted internet access on all devices

VPN是一种允许您在不危及您的信息的情况下安全地访问互联网的服务

VPN协议

作用：构建在互联网上安全传送数据的隧道

（1）OpenVPN

通用的VPN协议

可以在不同类型设备工作的最安全、最流行的协议之一。它是一个开源项目

（2）IPSec

用于保护网络层的通信安全

主要用于构建企业VPN

（3）PPTP

点到点隧道协议

老的淘汰的隧道协议，操作系统通常会内置

（4）L2TP

二层隧道协议

比PPTP要安全

使用广泛

（5）WireGuard

新的VPN协议，尚在测试中

Linux黑客基础-106-安全和匿名-对邮件进行加密

Encrypted Email 加密邮件

ProtonMail 项目---瑞士

https://protonmail.com/zh-Hans/ 官网


proton.me/mail
Proton
Products
Who we are
Resources & Support
For Business
Sign in
Create a free account
Proton Mail
Overview
Security
Pricing
Bridge
Download
Support