Hacking - Obscuring Identity

# Overview

## Why Hide Identity

There are various different reasons users might want to obsure or change their idenity while using the internet, be it to access a different region on video streaming platforms, browse hidden services anonymously using the tor service, or whistleblowing from a dangerous country where censorship is strong. While there are both morally good and bad reasons to hide identity on the internet, to keep the internet free and open it should always be considered an option to a user.

## What Identifies A User

When a user requests a resource on the internet, various identifying pieces of meta data are transferred along with the request. In order for responses to be returned to the correct user, some of this meta data must be unique and therefore identifying for the user requesting the access the resouce.

The most common piece of metadata used to identify a user is the Internet Protocol (IP) address, since this is the unique code used to route responses back to the user.

## The Challenge

To access the internet, at some point the public IP address of the user must be exposed to a gateway, otherwise receiving responses from servers would not be possible. Generally, for a third party to identify a user using IP address, they must be able to identify the public IP address the user is using, which should in turn allow them to track down the user's relative physical location. Therefore, the challenge in obscuring identity is mainly focused on hiding the public IP address of the user from a third party actively looking for it.

Since the third party looking for a user can vary widely in size, resources, and motivation to find a user. The ways to obscure identity also greatly vary in sophistication and complexity to implement, each with their own advantages, disadvantages, and effectivity of the end goal.

# Virtual Private Networks

## General

One of the most popular methods used to hide identity for the average user, create secure workplaces for businesses, and many other reasons.

## How It Works

Creates a tunnel between the user and their selected server running the same VPN software.

## How To Implement

### Create Your Own

### Buy A Service

# The Onion Router

# RDP

# Proxy Chains

## General

An expansion on the one hop VPN method, by using a chain of proxy servers to create multiple hops between the user and the destination server.

When using a single proxy between the user and destination server, it is much work for a third party with enough resource to contact the proxy server and obtain logs which identify the connecting users public IP address, therefore obtaining their identity. Even if the proxy server does not store logs, it is possible for an alert to be set which waits for when the destination server IP is accessed via the proxy server and flags the source IP addresses connecting to it.

Adding mutliple hops, ideally with proxy servers in different locations around the world, aleviates this issue since it is unlikely a third party would have enough resource or motivation to contact all the proxy servers in the chain in time to identify the connecting user before they change chain.

## Setup

A common piece of software used to proxy chain is called proxychains. Kali linux comes with the software pre-installed can be setup quite quickly, providing access to a list of proxies.

Add proxies to the proxychains.conf

sudo vim /etc/proxychains.conf

dynamic chains # chains list of proxy addresses dynamically

proxy dns # use proxy chain for dns queries

# add proxy server addresses in format: <protocol> <address> <port>

< proxy address 1 >

< proxy address 2 >

## Connect

Use the proxychains command to connect to the address using proxy:

proxychains firefox <destination-server>

## Finding Proxy Servers

### Free Server

Search google for a selection of free proxy servers, however, always assume they are insecure.

### Paid Server

Use a paid server, generally more secure, however will normally have logs and authentication requires additional setup.

The weak point is when paying for the server, ensure payment is anonymous using cryptocurrency and all connections to pay are proxied.