

Banner Grabbing and Firewall Detection

Let's start with **Banner grabbing**.

In simple terms, when you connect to a website, server, or any network service, it often displays a "banner" or welcome message that provides details about the software or operating system running on that system, including its name and version number. Banner grabbing involves capturing and analyzing this banner information.

- **Passive Banner grabbing using dmitry:**

```
dmitry -pb <IP OR DOMAIN>
```

- **HTTP Header grabbing with curl:**

```
curl <target IP> -v
```

Now the banner grabbing which we have performed might come under the active reconnaissance phase also. So, it is not 100% passive technique as we are connecting with the target in some way or another.

Moving on, let's perform Firewall Detection. We will use the wafwoof tool for this.

- **Firewall detection with WafW00f:**

```
wafw00f <domain>
```
