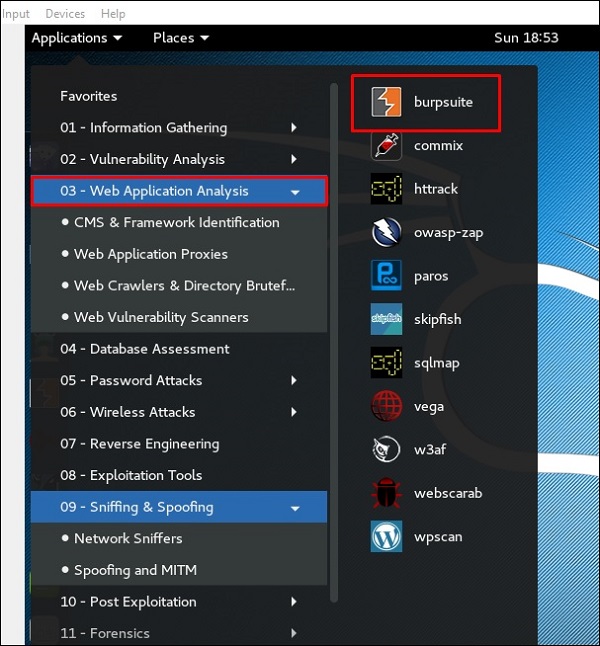
sniffing tools

The basic concept of sniffing tools is as simple as wiretapping and Kali Linux has some popular tools for this purpose. In this chapter, we will learn about the sniffing and spoofing tools available in Kali.

Burpsuite

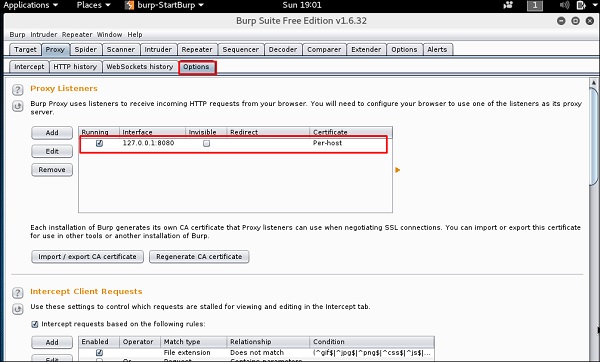
Burpsuite can be used as a sniffing tool between your browser and the webservers to find the parameters that the web application uses.

To open Burpsuite, go to Applications → Web Application Analysis → burpsuite.

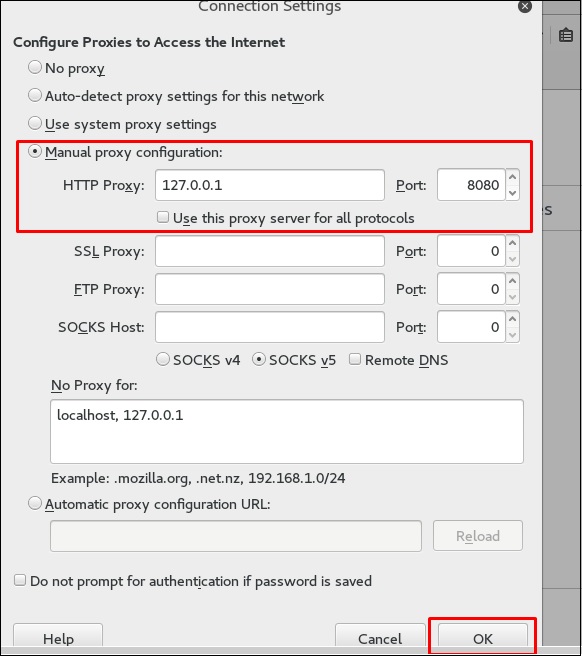


To make the setup of sniffing, we configure burpsuite to behave as a proxy. To do this, go to **Options** as shown in the following screenshot. Check the box as shown.

In this case, the proxy IP will be 127.0.0.1 with port 8080.



Then configure the browser proxy which is the IP of burpsuite machine and the port.

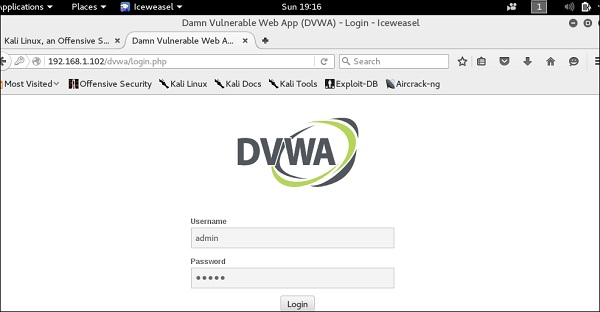


To start interception, go to Proxy → Intercept → click “Intercept is on”.

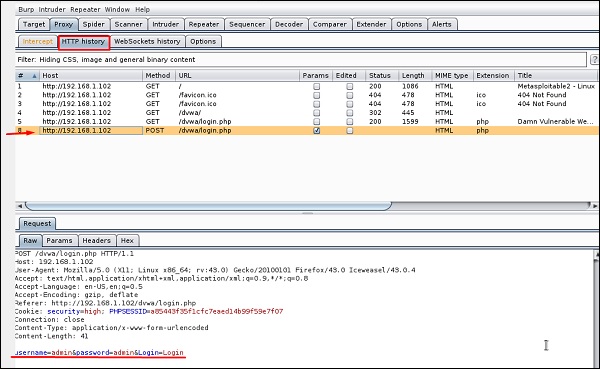
Continue to navigate on the webpage that you want to find the parameter to test for vulnerabilities.



In this case, it is metasploitable machine with IP 192.168.1.102



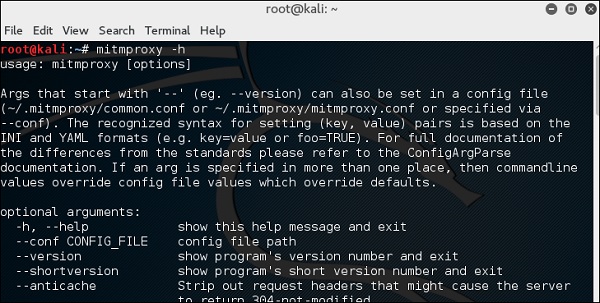
Go to “HTTP History”. In the following screenshot, the line marked in red arrow shows the last request. In Raw and the hidden parameter such as the Session ID and other parameter such as user name and password has been underlined in red.



mitmproxy

**mitmproxy** is an SSL-capable man-in-the-middle HTTP proxy. It provides a console interface that allows traffic flows to be inspected and edited on the fly.

To open it, go to the terminal and type **“mitmproxy -parameter”** and for getting help on commands, type **“mitmproxy –h”**.

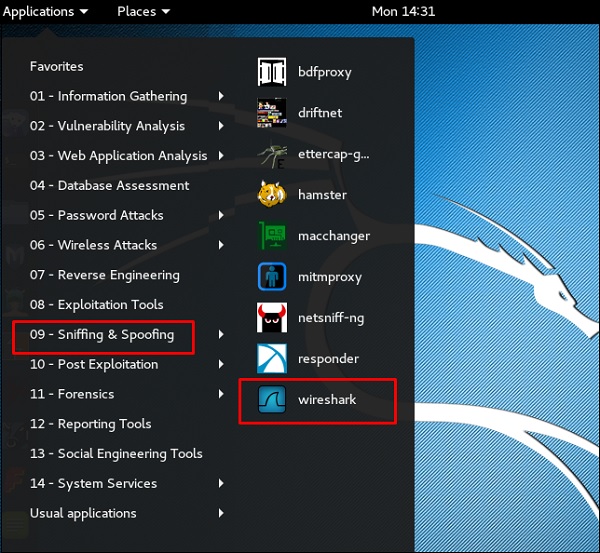


To start the mitmproxy, type **“mitmproxy –p portnumber”**. In this case, it is “mitmproxy –p 80”.

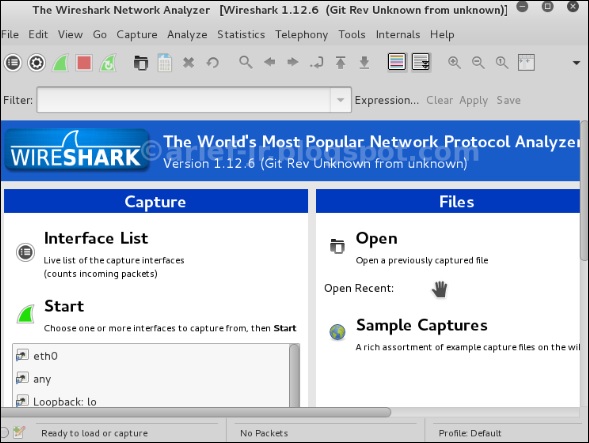
Port Number

Wireshark

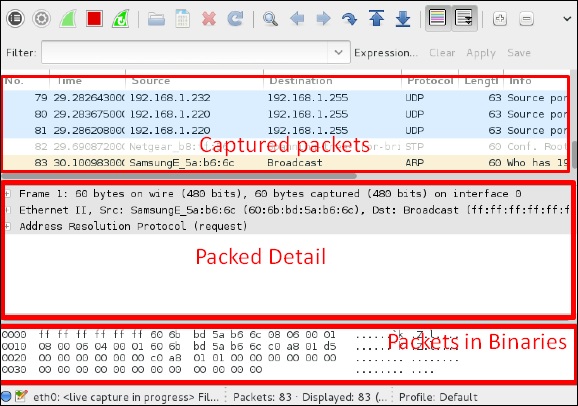
Wireshark is one of the best data packet analyzers. It analyzes deeply the packets in frame level. You can get more information on Wireshark from their official webpage: <https://www.wireshark.org/>. In Kali, it is found using the following path - Applications → Sniffing & Spoofing → wireshark.



Once you click wireshark, the following GUI opens up.



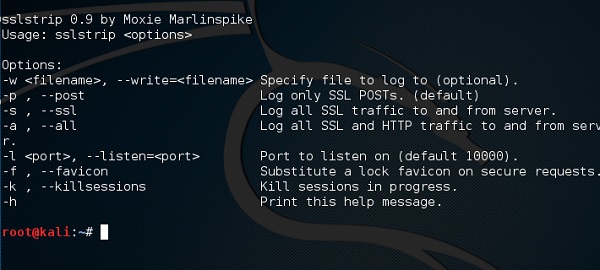
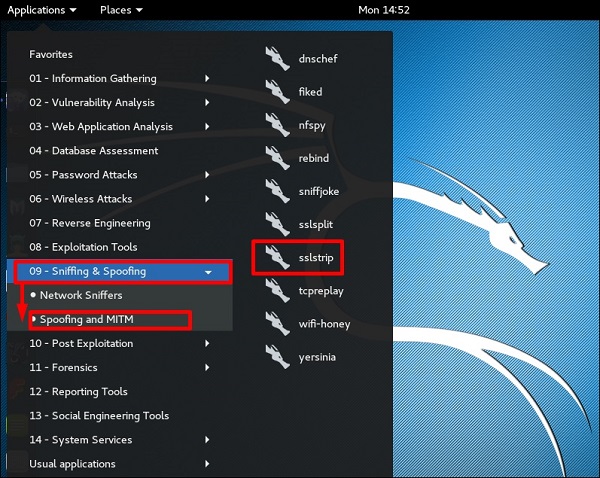
Click “Start” and the packet capturing will start as shown in the following screenshot.



sslstrip

**sslstrip** is a MITM attack that forces a victim's browser to communicate in plain-text over HTTP, and the proxies modifies the content from an HTTPS server. To do this, sslstrip is "stripping" https:// URLs and turning them into http:// URLs.

To open it, go to Applications → 09-Sniffing & Spoofing → Spoofing and MITM → sslstrip.



To set it up, write to forward all the 80 port communication to 8080.

Port Comminucation

Then, start the **sslstrip** command for the port needed.

