**INTRODUCTION**

**Kali Linux.**

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux was born and released on March 13th, 2013.It's a security-focused version of Linux that offers a large number of tools to seek out weaknesses and secure your network.

Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack, their previous information security testing Linux distribution.

* **More than 600 penetration testing tools included**
* OS Family - Unix like
* Working State - Active
* Platforms - x86, x86-64, armel, armhf
* Kernel Type - Monolithic kernel (Linux)
* Default UI - GNOME3
* Latest Release – 2017.2 April 25, 2017

**Penetration Testing.**

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. For example, an audit or an assessment may utilize scanning tools that provide a few hundred possible vulnerabilities on multiple systems.

A Penetration Test would attempt to attack those vulnerabilities in the same manner as a malicious hacker to verify which vulnerabilities are genuine reducing the real list of system vulnerabilities to a handful of security weaknesses.

**Different Strategies**

• Targeted testing - Testing team working together.

• External testing - Targets externally visible servers or devices.

• Internal testing - Attack behind the firewall.

• Blind testing - Simulates the actions of a real attacker

**Targeted testing** Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned on" approach because everyone can see the test being carried out.

**External testing** This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

**Internal testing** This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

**Blind testing** A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive

**Benefits of Penetration Testing**

• Intelligently manage vulnerabilities

• Avoid the cost of network downtime

• Meet regulatory requirements and avoid fines

• Preserve corporate image and customer loyalty

**Brute-force attacks**

A brute-force attack is when all possible keys are checked against encrypted data until the right key is found.

Brute-force attacks are extremely costly from a resource and time perspective because the attacker is exploiting vulnerabilities in the encryption by taking advantage of key length and simplicity of the key.

A password is often based on dictionary words meaning the total space an attacker would have to test would be all words in a matching dictionary making the guessing scope significantly smaller than a password using random characters.

Best practice to mitigate brute-force attacks is using long and complicated keys as well as timeouts after a number of attempts and other methods to add more security factors.

# Popular tools for brute-force attack.

## Aircrack-ng.

## John the Ripper.

## Ophcrack

## Hashcat

**BURP SUITE**

**Introduction to burp suite**

Burp Suite is a platform for performing penetration testing of web applications. With a suite of tools working together seamlessly, you are able to perform full-range security testing, from the initial mapping to the analysis of an application’s attack surface and vulnerabilities.

This Java-based framework is often classified as an ‘Interception Proxy,’ whereas a penetration tester configures their browser to route traffic through the proxy to capture and analyze requests to and from the web application.

A choice platform among penetration testers, Burp Suite offers users full control through a combination of advanced manual techniques and automation. The tool is written in Java and developed by PortSwigger Security. Two versions are there, Free edition and professional.

Latest version is v1.2.27 and released in 31 august 2017.

**What is Burp Suite used for?**

At a high level, Burp Suite can be used to:

* Scan for vulnerabilities
* Intercept browser traffic
* Automate custom attacks
* Perform manual testing using a variety of tools

**The tools offered as a part of Burp Suite are:**

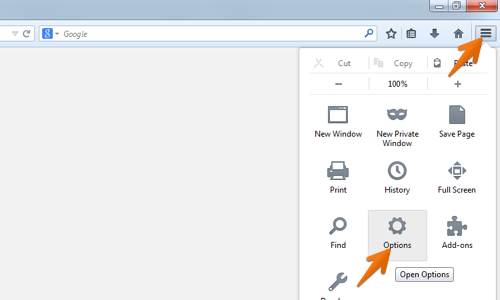
* HTTP Proxy
* Scanner
* Intruder
* Spider
* Repeater
* Decoder
* Comparer
* Extender
* Sequencer

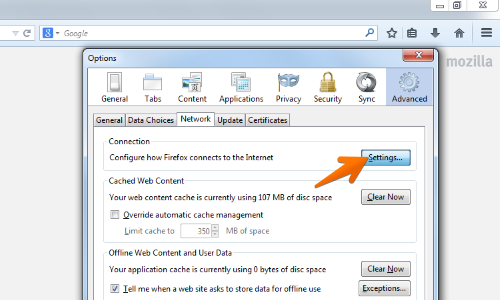
# Configuring Firefox to work with Burp Suite

We have to configure web browser with proxy and port number of burp suite.

* In Firefox, go to the Firefox Menu.
* Click on “Preferences” / "Options".
* Select the “Advanced” tab followed by the “Network” tab.
* In the “Network” tab click on the "Settings" button in the

Connection” section.





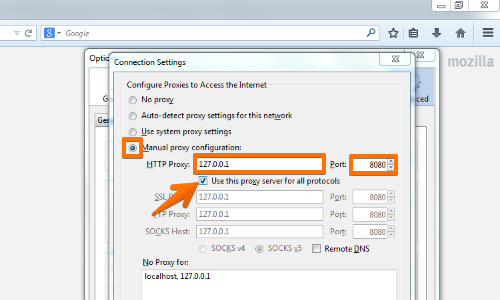
* Select the "Manual proxy configuration" option.
* Enter your Burp Proxy listener address in the "HTTP Proxy"

field (by default this is set to 127.0.0.1).

* Next enter your Burp Proxy listener port in the "Port" field

(by default, 8080).

* Make sure the "Use this proxy server for all protocols" box is checked.
* Delete anything that appears in the "No proxy for" field.
* Now click "OK" to close all of the options dialogs.

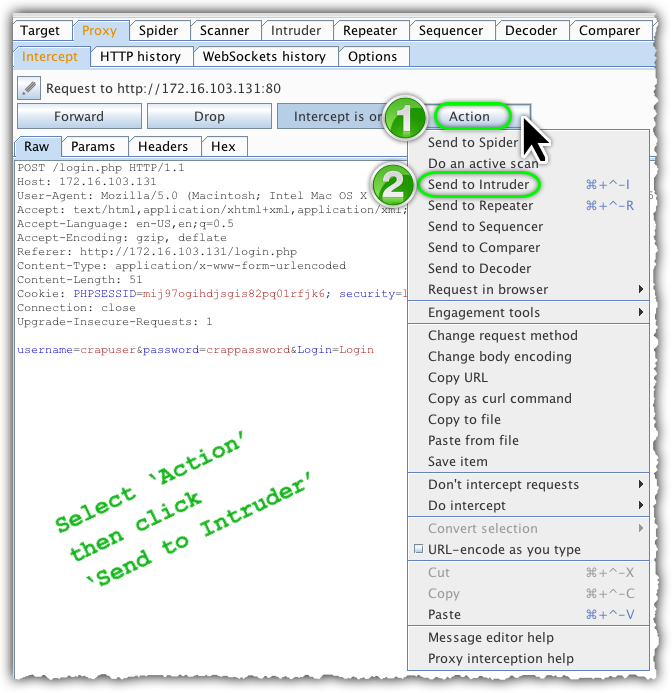


**Brute Force a Login Page.**

Select a login page.

* Put random details into the **username** and **password** fields, just to make the form submit.
* The captured request can be viewed in the Proxy "Intercept" tab.
* Right click on the request to bring up the context menu.
* Then click “Send to Intruder”.





## **Intruder**

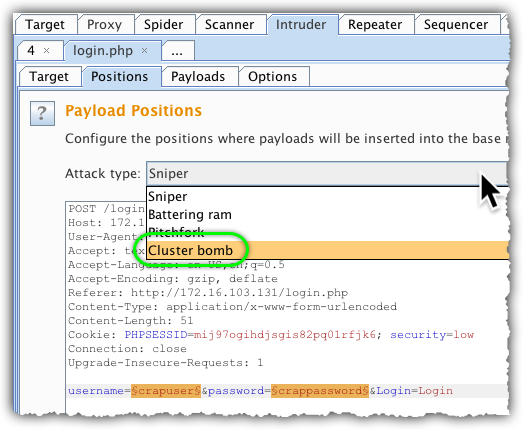
Burp Intruder is a tool for automating customized attacks against web applications. It is extremely powerful and configurable, and can be used to perform task like brute-force login page of web application. It has four panels –   target, positions, payloads and options

**Target:**This panel is used to specify the target host (the URL) and the port to use for the connection.

**Positions:**This panel is very important in automating attack strings on the target. The types of attack vectors are sniper attack, battering ram attack, pitchfork attack and cluster bomb.

* Go to the Intruder "Positions" tab.
* Change the attack to "Cluster bomb" using the "Attack type"

drop down menu.



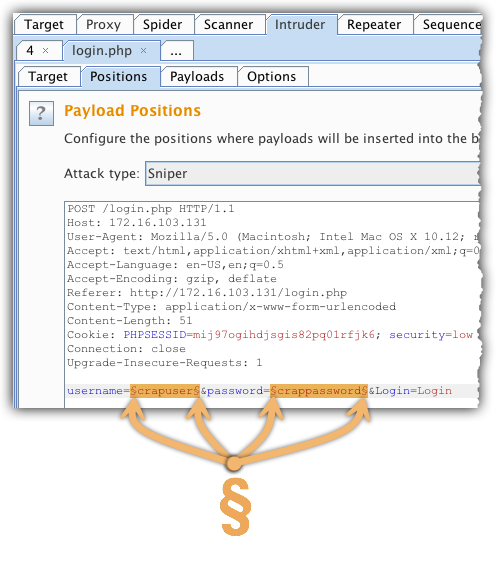
**Cluster bomb**

It starts with a specific payload to each parameter, and when all variables have been tested, will start testing with the payload from the next variable, such that all parameters get tested with all variables.

* Clear the pre-set payload positions by using the "Clear" button on the right of the request

editor..

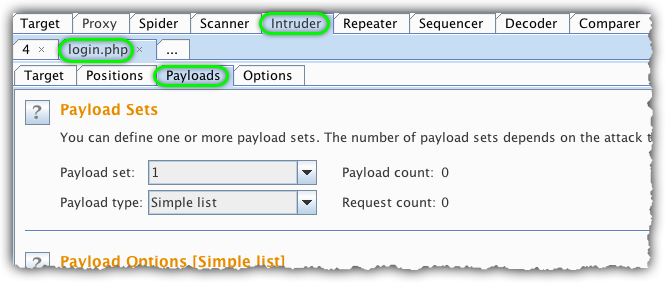
* Add the "username" and "password" parameter values as positions by highlighting them and using the "Add" button.



* Go to the "Payloads" tab.
* In the "Payload sets" settings, ensure "Payload set" is "1" and "Payload type"

is set to “Simple list”.

* In the "Payload options" settings enter some possible usernames.



* Next, in the "Payload Sets" options, change "Payload" set to "2".

In the "Payload options" settings enter some possible passwords.

  You can do this manually or using a custom list.

* Go to the "options" tab
* Select grep-match

**Grep-match**

These settings can be used to flag result items containing specified expressions in the response. For each item configured in the list, Burp will add a new results column containing a checkbox indicating whether the item was found in each response.

* Add a keyword like ‘invalid’ or ‘mismatch’

Click the "**Start attack**" button.

After clicking the **Start attack** button, a second Burp window will pop-up.  A progress bar at the bottom will tell me when it’s finished.

* When a match is found it will automatically logged in to that site.

**PREVENT BRUTE FORCE ATTACKS**

## **Captchas**

They prevent automated testing.

## **Forcing strong passwords**

Will prevent dictionary attacks.

## **Lockouts after several attempts**

Will slow down automated tests

**CONCLUSION**

Since web applications offer data access to customers, employees, and other key groups, they have become a weak link for many organizations. If a hacker gains access, they often have direct access to confidential data, meaning that web application security testing should be a high priority to businesses today.

Complete testing of a web-based system before going live can help address issues before the system is revealed to the public. An essential element of testing web application security is understanding the data moving between the browser and the server.

That is where Burp Suite comes in. This tool allows penetration testers and security analysts to ensure everything is behaving properly using a combination of manual testing and automation to ensure full visibility.

**REFERENCES**

* https://portswigger.net/burp
* https://infosecaddicts.com/burp-suite-workshop/
* https://gingsoft.com/?p=3286