



Fakulti Teknologi Maklumat dan Komunikasi

Universiti Teknikal Malaysia Melaka

## Analyze Security Tools

Security Tools:

Burp Suite, Hping

Demonstration Video:

[https://youtu.be/au6R5tQV\\_aY](https://youtu.be/au6R5tQV_aY)

### **GROUP 7**

1. Muhammad Izham Bin Norhamadi (B032020039)
2. Ahmad Sha Herizam Bin Tahir (B032020009)
3. Affendy Elyas bin Azhari Sharidan (B032020024)
4. Nor Adzeezul Asrie Bin Norafandi (B031910012)
5. Muhammad Farhan Bin Mohamad Tahir (B031910105)

## Table of Contents

1.	Brief Introduction of Selected Security Tools	1
2.	Overview of Burp Suite	1
3.	Burp Suite Instruction Demo	2
4.	Advantages of Burp Suite	9
5.	Overview of Hping	10
6.	Hping Instruction Demo	10
7.	Advantages of Hping	12
8.	Conclusion	13

## 1. Brief Introduction of Selected Security Tools

In this millennium era, security is becoming a hot topic to be discussed in everyday life whether in a business environment or even in daily conversation as a security measure becomes the core of protection of any kinds of information or confidential assets. One of the security measures that needs to be paid attention to is the security tools itself since the tools will help users to implement security into their respective machines.

Now, security tools come in several types and features with specific purpose on their own to complete specific security tasks. These security tools come for a variety of purposes such as web-based application security evaluation and TCP/IP packet analyzer. Examples of security tools which are popular nowadays include Burp Suite and Hping. Both tools are handy in terms of providing such a good security environment. Burp Suite is a tool for analyzing and testing web applications and on the other hand Hping is a TCP/IP packet analyzer which specifically for network auditing and firewall testing.

## 2. Overview of Burp Suite

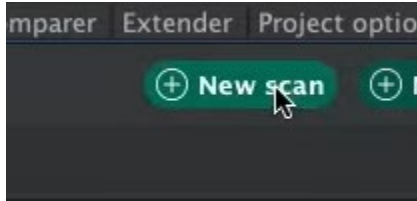


Burp Suite is a Java application for testing and analyzing web application security. It is a widely used tool to evaluate the security of web-based applications and hands-on testing. It has a robust and modular framework and packed with optional extensions that can increase web application testing efficiency. It has a user-friendly UI making it accessible for learning the basics of web security testing. Burp Suite features includes a proxy server, spider bot, automate requests and much more penetration testing tools.

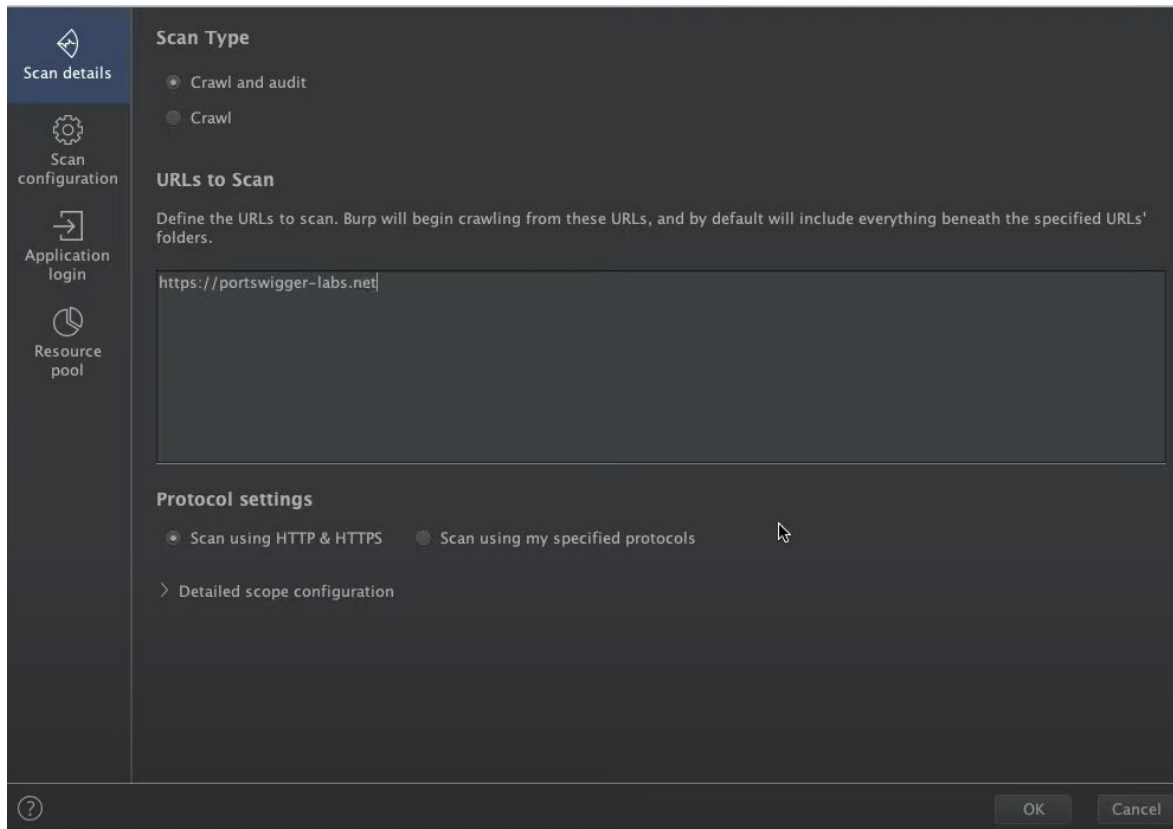
### 3. Burp Suite Instruction Demo

#### Scanning a website for vulnerabilities

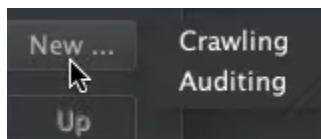
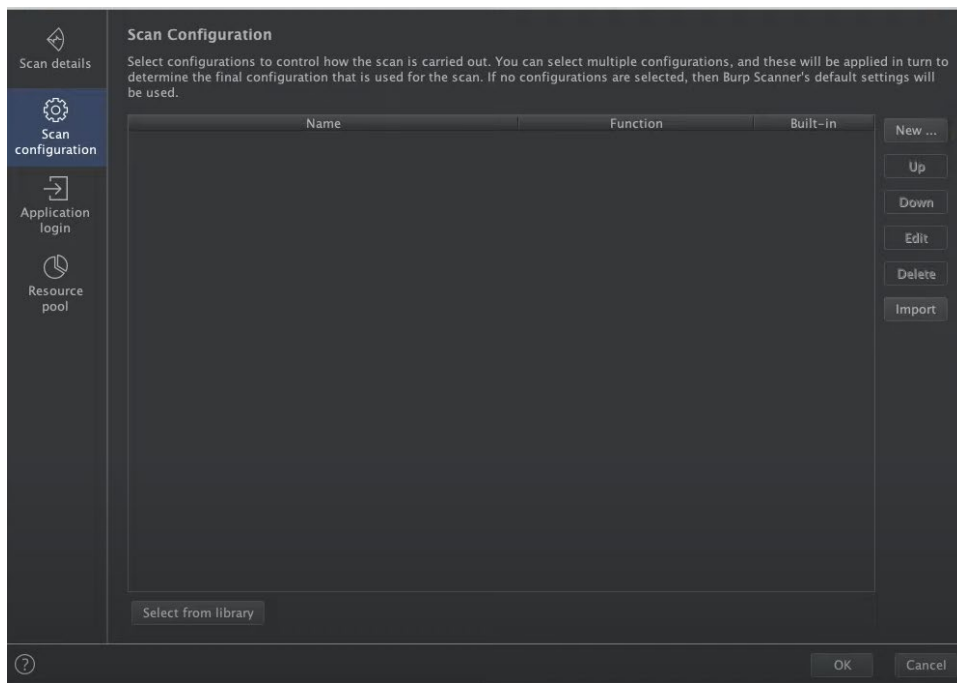
1. Click on burp dashboard and click scan



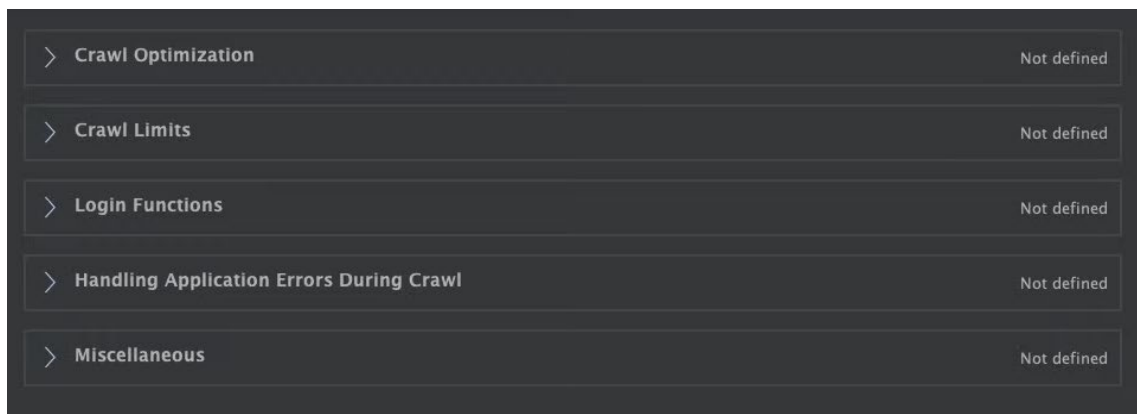
2. New scan launcher open up and then click crawler and audit, if crawler only, it will just discover the contents. Place URL that needs to scan in the text box. In protocol setting, it is recommended to stay default that is scan using HTTPS and HTTPS.



3. Next go to scan configuration, and click new and choose whether crawling or audit.



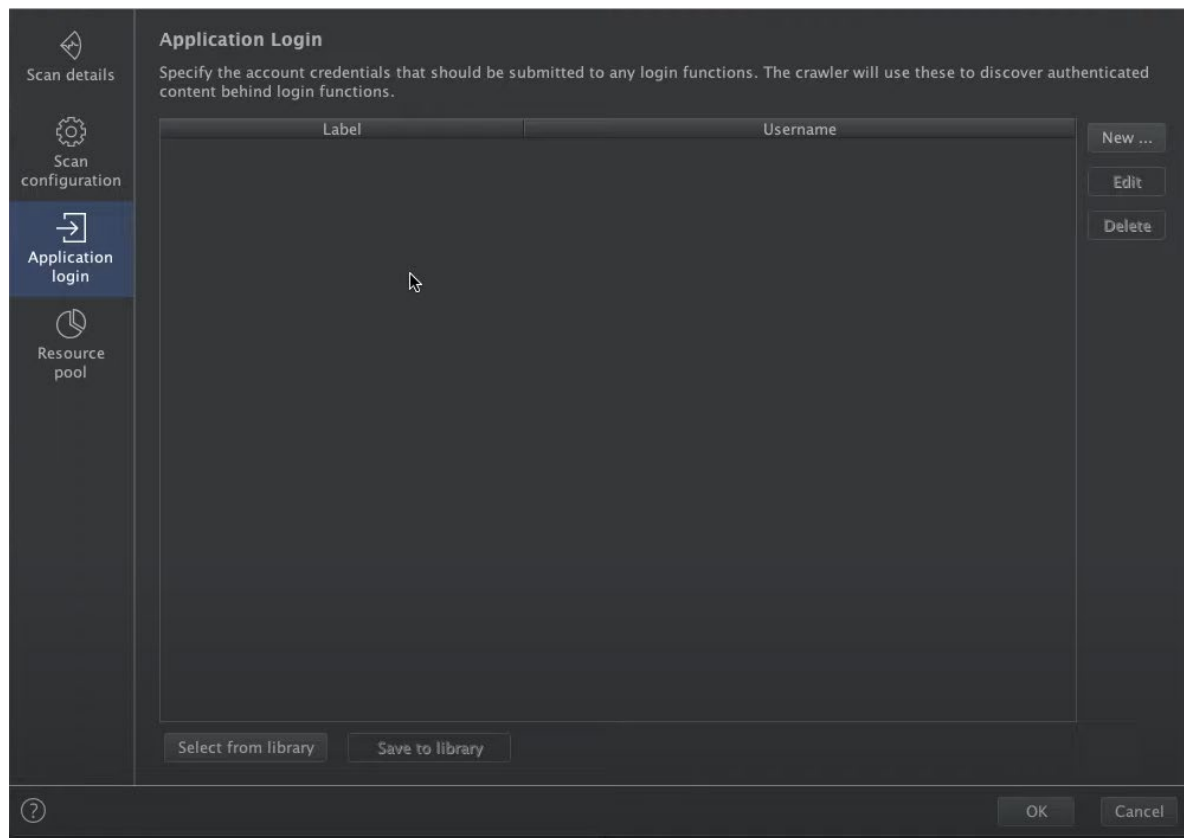
4. In crawl option there are configuration can be use such as crawl optimization, crawl limits, login functions and handling application errors during crawl.



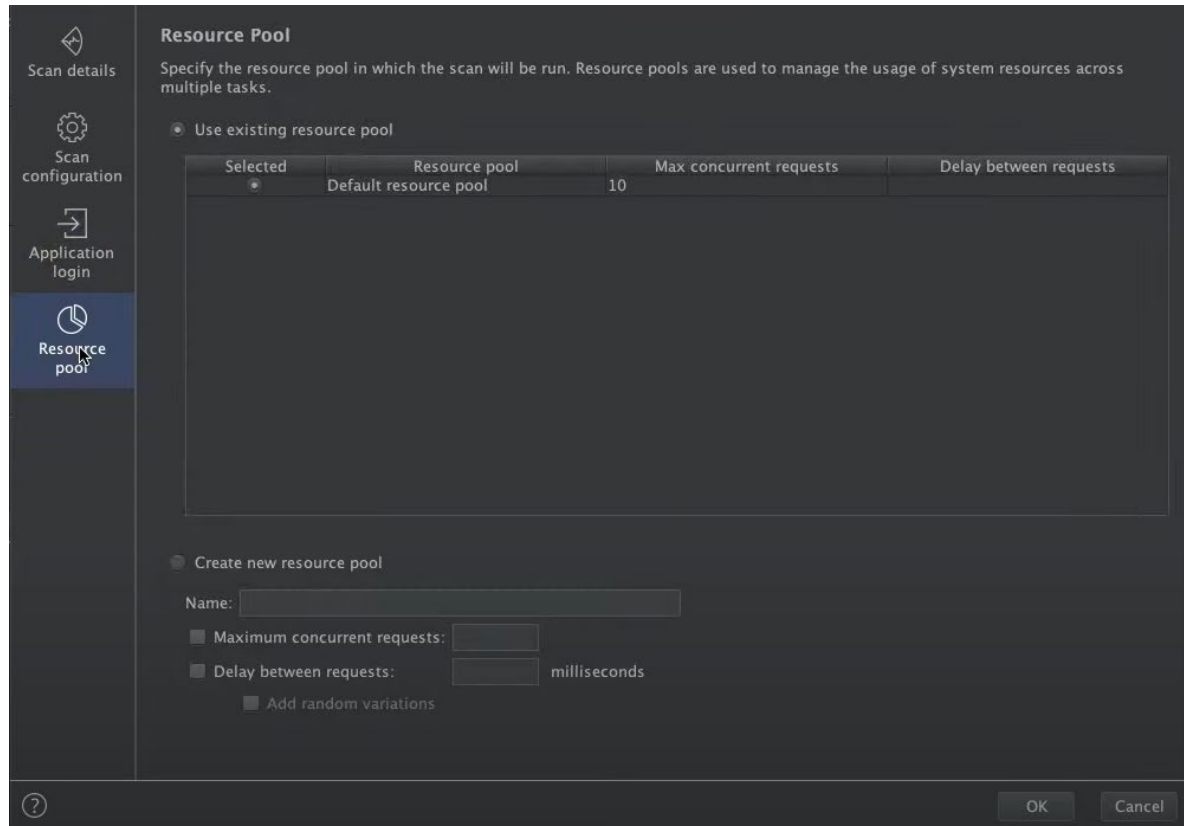
5. In crawl option there are configuration can be used such as audit optimization, issues reported, handling applications errors during audit, etc.

> Audit Optimization	Not defined
> Issues Reported	Not defined
> Handling Application Errors During Audit	Not defined
> Insertion Point Types	Not defined
> Modifying Parameter Locations	Not defined
> Ignored Insertion Points	Not defined
> Frequently Occurring Insertion Points	Not defined
> Misc Insertion Point Options	Not defined
> JavaScript Analysis	Not defined

- Next, in application login setting that can be used to specify the account credentials that should be submitted to any login functions. The crawler will use these to discover authenticated content behind login functions.



- Next, in a resource pool setting that can be used to specify the resource pool in which the scan will be run. Resource pools are used to manage the usage of system resources across multiple task.



**Resource Pool**

Specify the resource pool in which the scan will be run. Resource pools are used to manage the usage of system resources across multiple tasks.

☒ Use existing resource pool

Selected	Resource pool	Max concurrent requests	Delay between requests
<input checked="" type="radio"/>	Default resource pool	10	

☐ Create new resource pool

Name:

☐ Maximum concurrent requests:

☐ Delay between requests:  milliseconds

☐ Add random variations

OK Cancel



8. After finished setting the scanner, click ok and the scan will start

The screenshot shows the Burp Suite interface with three tasks listed at the top:

- 1. Live passive crawl from Proxy (all traffic)**: Capturing is enabled. 0 items added to site map, 0 responses processed, 0 responses queued.
- 2. Live audit from Proxy (all traffic)**: Audit checks - passive. Capturing is enabled. 0 requests (0 errors). [View details >>](#)
- 3. Crawl and audit of portswigger-labs.net**: Default configuration. Capturing is enabled. 8 requests (0 errors), 7 locations crawled. [View details >>](#)

Below the tasks is the **Event log** section with a filter set to 'Critical'. The log shows two events:

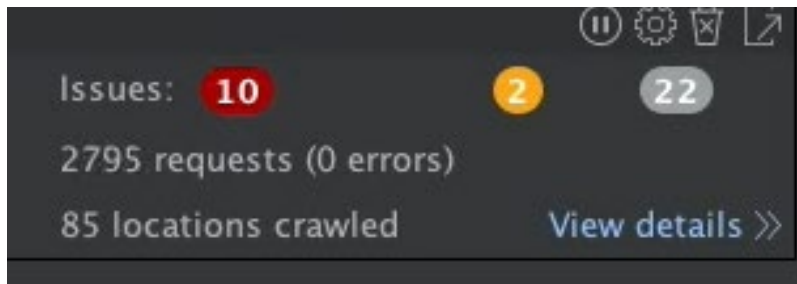
Time	Type	Source	Message
11:51:39 31 Jul 2020	Info	Task 3	Crawl started.
11:52:27 31 Jul 2020	Info	Proxy	Proxy service started on 127.0.0.1:8080

9. After scan finished, a list of issue activity show up.

The screenshot shows the 'Issue activity' tab in Burp Suite. The filter is set to 'High'. The table below lists the detected issues:

#	Task	Time	Action	Issue type	Host
34	3	11:52:17 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	https://portswigger-labs.net
33	3	11:52:17 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	http://portswigger-labs.net
32	3	11:52:14 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	https://portswigger-labs.net
31	3	11:52:14 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	http://portswigger-labs.net
30	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	https://portswigger-labs.net
29	3	11:52:13 31 Jul 2020	Issue found	Browser cross-site scripting filter disabled	https://portswigger-labs.net
28	3	11:52:13 31 Jul 2020	Issue found	Serialized object in HTTP message	https://portswigger-labs.net
27	3	11:52:13 31 Jul 2020	Issue found	Browser cross-site scripting filter disabled	http://portswigger-labs.net
26	3	11:52:13 31 Jul 2020	Issue found	Cross-domain Referer leakage	https://portswigger-labs.net
25	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	http://portswigger-labs.net
24	3	11:52:13 31 Jul 2020	Issue found	Browser cross-site scripting filter disabled	https://portswigger-labs.net
23	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	http://portswigger-labs.net
22	3	11:52:13 31 Jul 2020	Issue found	Cross-domain Referer leakage	http://portswigger-labs.net
21	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	http://portswigger-labs.net
20	3	11:52:13 31 Jul 2020	Issue found	Serialized object in HTTP message	http://portswigger-labs.net
19	3	11:52:13 31 Jul 2020	Issue found	Cross-domain script include	https://portswigger-labs.net
18	3	11:52:13 31 Jul 2020	Issue found	Directory listing	https://portswigger-labs.net
17	3	11:52:13 31 Jul 2020	Issue found	Serialized object in HTTP message	http://portswigger-labs.net
16	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	https://portswigger-labs.net
15	3	11:52:12 31 Jul 2020	Issue found	Browser cross-site scripting filter disabled	http://portswigger-labs.net

At the bottom, there is an 'Advisory' section.



10. In the content, we can see the response of the website if click any of it

Contents

Host	Method	URL	Params	Status	Length	MIME type	
https://portswigger-lab...	GET	/		200	3329	HTML	Port
https://portswigger-lab...	GET	/cors.php		200	286	HTML	
https://portswigger-lab...	GET	/cors.php/		200	286	HTML	
https://portswigger-lab...	GET	/crossdomain.xml		200	380	XML	
https://portswigger-lab...	GET	/csp/		200	1741	HTML	Inde
https://portswigger-lab...	GET	/csp/?C=D%3bO%3dA	✓	200	1741	HTML	Inde
https://portswigger-lab...	GET	/csp/?C=M%3bO%3dA	✓	200	1741	HTML	Inde
https://portswigger-lab...	GET	/csp/?C=N%3bO%3dD	✓	200	1741	HTML	Inde
https://portswigger-lab...	GET	/csp/?C=S%3bO%3dA	✓	200	1741	HTML	Inde
https://portswigger-lab...	GET	/csp/csp.php		200	332	HTML	
https://portswigger-lab...	GET	/csp/deser.html		200	560	HTML	
https://portswigger-lab...	GET	/csp/deser.html?h...		200	560	HTML	

Request Response

Raw Headers Hex

```

1 GET / HTTP/1.1
2 Host: portswigger-labs.net
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10

```

## 4. Advantage of Burp Suite

- **Have variety of features**

Burp Suite provides various kinds of features or sub-tools that can be used for a specific purpose such as manual penetration testing and configuration, automated bulk scanning as well as report generation.

- **Use local proxy**

Allow users to intercept application's traffic to discover vulnerabilities. From this interception, users can manipulate the attribute fields to find more vulnerabilities inside the application

- **Spidering Features**

The spidering is to follow all the links on a web page to discover both dynamic and static web resource of the web application. This can be done in manual or automated process and will give a flow chart representation of the workflow which can easily acquire with a click only.

- **Testing can be done manually or automatically**

Usually automated and manual tools are only available in several types of tools. However, Burp Suite is one of the tools that provide utility to perform both tasks in a single tool.

- **Have a powerful extension ready to be used**

Burp Suite has an application store called BApp Store which users can install ready-to-use extension, manage the extension, and configure the option of the extension. Users also can create their own extension and can submit to BApp Store after getting approval.

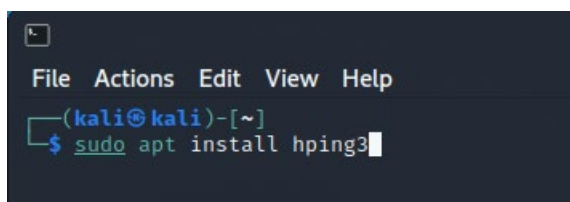
## 5. Overview of Hping



hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired by the ping (8) UNIX command, but hping is not only able to send ICMP echo requests. It supports TCP (Transmission Control Protocol), UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features. It is one of the common tools used for security auditing and testing of firewalls and networks and was used to exploit the idle scan scanning technique.

## 6. Hping Instruction Demo

1. Kali Linux comes pre-installed with hping tool, but if it isn't simply using the apt package command

A screenshot of a terminal window with a dark background. At the top, there is a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu bar, the prompt "(kali@kali)-[~]" is shown. The command "\$ sudo apt install hping3" is entered, with the cursor at the end of the line.

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install hping3
```

2. hping3 has several parameters to operate the software, you can view the list with the -help command

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hping3 -h  
usage: hping3 host [options]  
-h --help      show this help  
-v --version   show version  
-c --count     packet count  
-i --interval  wait (uX for X microseconds, for example -i u1000)  
--fast        alias for -i u10000 (10 packets for second)  
--faster      alias for -i u1000 (100 packets for second)  
--flood       sent packets as fast as possible. Don't show replies.  
-n --numeric   numeric output  
-q --quiet     quiet  
-I --interface interface name (otherwise default routing interface)  
-V --verbose   verbose mode  
-D --debug     debugging info  
-z --bind      bind ctrl+z to ttl (default to dst port)  
-Z --unbind    unbind ctrl+z  
--beep        beep for every matching packet received  
  
Mode  
default mode   TCP  
-0 --rawip     RAW IP mode  
-1 --icmp      ICMP mode  
-2 --udp       UDP mode  
-8 --scan      SCAN mode.  
Example: hping --scan 1-30,70-90 -S www.target.host  
-9 --listen    listen mode  
  
IP  
-a --spoof     spoof source address  
--rand-dest    random destination address mode. see the man.  
--rand-source  random source address mode. see the man.  
-t --ttl       ttl (default 64)  
-N --id        id (default random)  
-W --winid     use win* id byte ordering  
-r --rel       relativize id field (to estimate host traffic)  
-f --frag      split packets in more frag. (may pass weak acl)  
-x --morefrag  set more fragments flag
```

3. To start using the tool, provide the target destination IP, its port, and the desired parameter options

```
(kali@kali)-[~]  
$ sudo hping3 192.168.17.131 -p 80 -S  
HPING 192.168.17.131 (eth0 192.168.17.131): S set, 40 headers + 0 data bytes  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=7.0 ms  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=3.9 ms  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=3.9 ms  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=4.1 ms  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840 rtt=3.9 ms  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=5 win=5840 rtt=4.4 ms  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=5840 rtt=4.1 ms  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=5840 rtt=3.1 ms  
len=46 ip=192.168.17.131 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=5840 rtt=8.7 ms
```

## 7. Advantage of Hping

- **Useful for Firewall penetration testing.**

This tool can penetrate Firewall by using command available in hping to deploy such as DoS attack to see the performance of the server.

- **Can be used to check if the port is opened or filtered.**

We can analyze our port whether the host network is opened or filtered. For example, by using the command that are available in hping, if it finds a live host and an open port, it returns an RST response.

## 8. Conclusion

In conclusion, in this modern era of globalization, security tools have been popular in this digital world of security system. 'Prevention is better than cure.' This proverb really describes how security tools are all about. As modern people, evolution of security tools needs to be paid attention so that any kinds of threats that would lead to the harm of a system can be mitigated by simply having a right tool to counter specific threats.

Day by day, vulnerability and threats keep expanding and can be more harmful and harder to detect by recent security tools and software. That is why this type of tool needs to be updated regularly so that it can detect either advanced threats or new undiscovered type of vulnerabilities. Plus, we need to always keep up to date with the latest trends of threats to make sure our security tools and software are always prepared for any new type of threats.

Everyone, either a person in corporate business or even a student who studies in security field, needs to learn, and have a better understanding of the importance of security tools. Especially someone who works in web-based industries, using Burp Suite is a high recommendation since this software is extremely reliable and helpful in making sure that any web we develop or take care of always in secure conditions from any kinds of threats either physically or digitally meanwhile Hping can be handy towards individual in charge of network security auditing and firewall testing.