# AN OVERVIEW ON THE UTILIZATION OF KALI LINUX TOOLS

**B. Surya Samantha[1], M.V.Phanindra[2]**
[1]Assistant Professor Department of Information Technology, CBIT, Hyderabad, India
[2]AssistantProfessor, Kakatiya Institute of Technology and Sciences, Warangal, India

Received: Feb. 18, 2018 Accepted: March 19, 2018

**ABSTRACT** *The goal of writing this research paper is to assess the different penetration testing tools in KALI LINUX utilized for website hacking purposes. By examining these tools, we make sense of which tools are expected to distinguish the codes which make hurt websites. Websites are utilized every day by a huge piece of the total populace to convey touchy information from a man to an element with online-based nearness. In websites containing materials that are appeared after confirmation just, shapes exchange information containing client accreditations to server-side contents. Clients store their credit card details in their online records and utilize structures to purchase things online, so it is pivotal to keep the integrity, classification and accessibility of this information intact. Website hacking is an assault on a website that progressions the visual appearance and in addition substance of the website or a webpage. These are commonly crafted by system crackers, who break into a web server and supplant the hosted website with one of his own.*

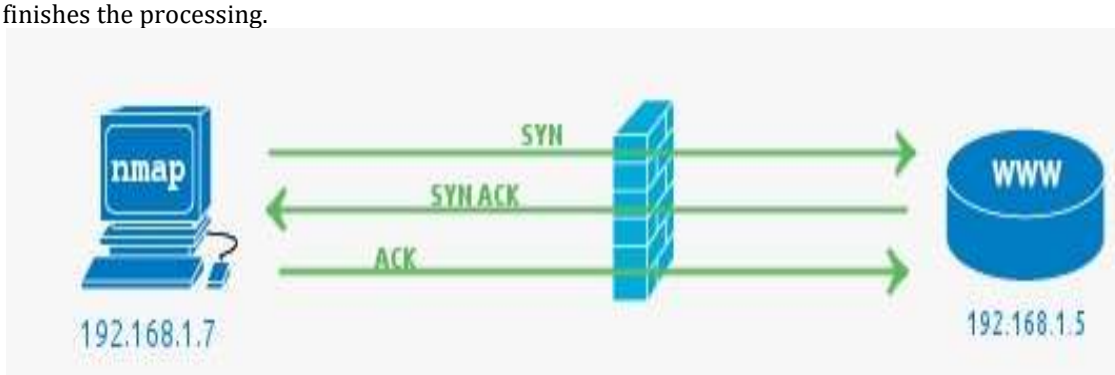
***Key Words:*** *Filtered ports, Ports scanning, hosted website, Website hacking, penetration testing tools, kali linux.*

**KALI LINUX Tools worked upon are:**

1) Zenmap:

Zenmap is a Port Scanner utilized for scanning the open, shut and sifted ports of the objective. At the point when Zenmap checks for the ports, it utilizes 3 way tcp handshake in which initially SYN flag is sent to Tcp port which has some administration joined to it, for instance HTTP(Port 80), SMTP(Port 25),SSH(Port 22), POP3(Port 110) and so on.

At that point, the server sees the SYN flag and reacts with the SYN ACK flag and Client answers it by ACK flag. This finishes the processing.




Ports scanning is fundamentally of 3 kinds of ports:

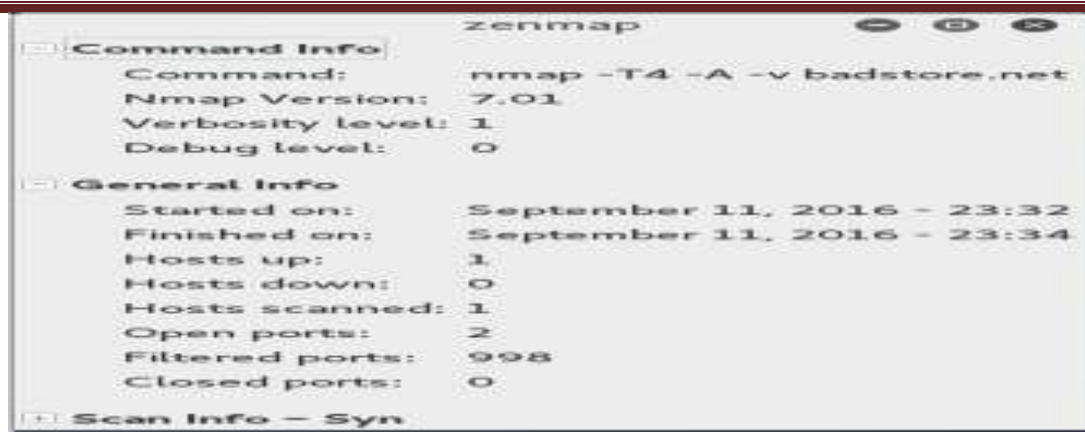
1.Filtered ports: These are the ports which are secured by the firewall itself and there isn't benefit running on these ports. These ports not reacted whenever to the nmap.

2.Closed Ports: Although no administration is running on these ports yet firewall permits to experience it to check the ports which implies firewall doesn't works for these ports.

3.Open ports: Basically these are the ports whose administrations are freely available to anybody. Anyone can perceive what administrations are running by using port scanners.

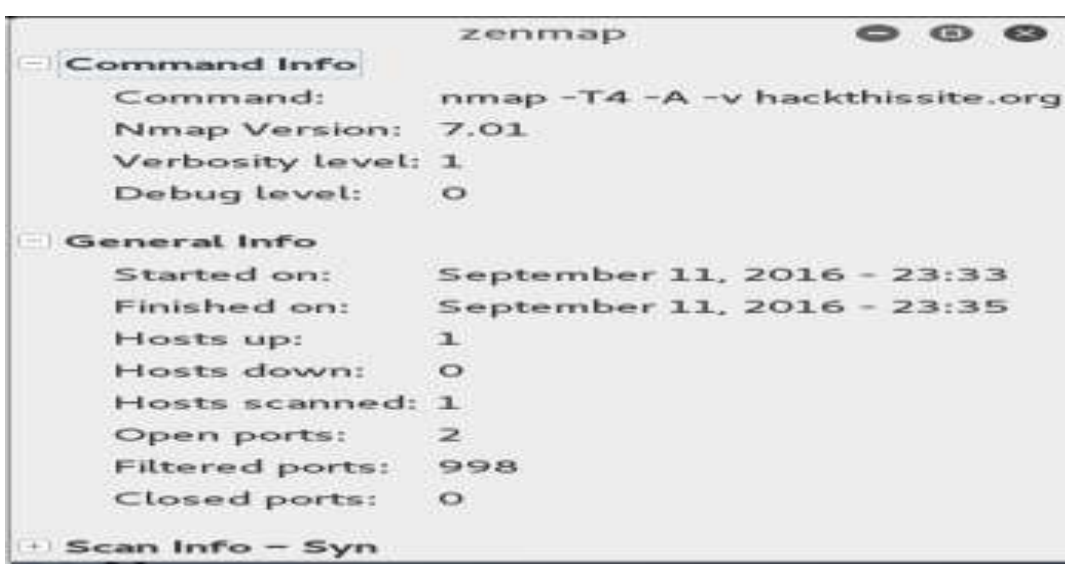
A few cases of Zenmap checks performed on websites are:

Tested site 1:

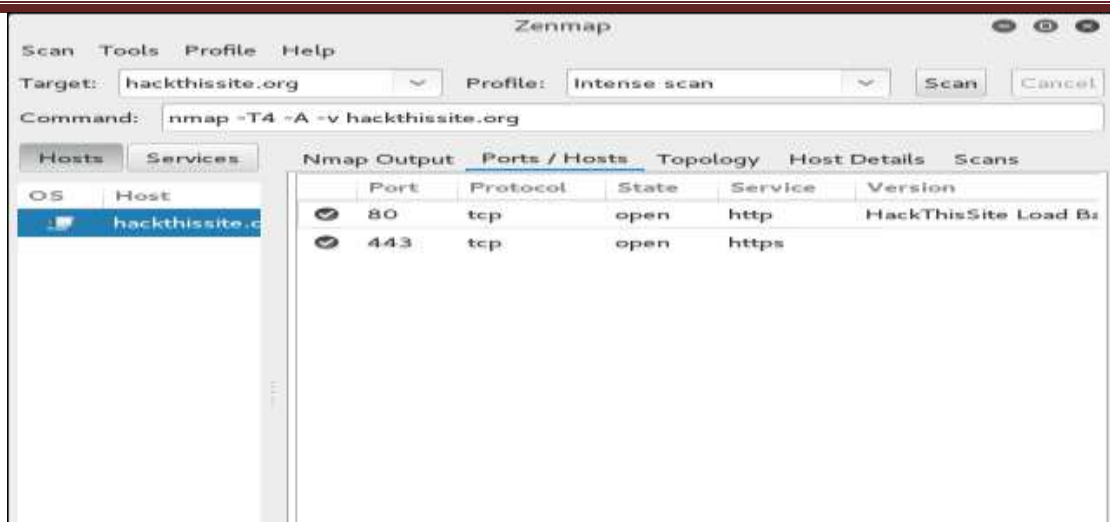



The screenshot shows that on this site 2 ports are open which are:


2) Tested site 2:




2 ports are open on this website which are:




**2) Sparta (VulnerabilityScanner):**

Sparta is a GUI application which is utilized for the penetration testing. It does scanning and examination of results give further information of systems.

It has different highlights:

1. Can import nmap comes about straightforwardly from XML records.

2. You can arrange any sort of administrations according to your need in Sparta.

3. It can likewise define some mechanized errands like what administrations to keep running on which ports.

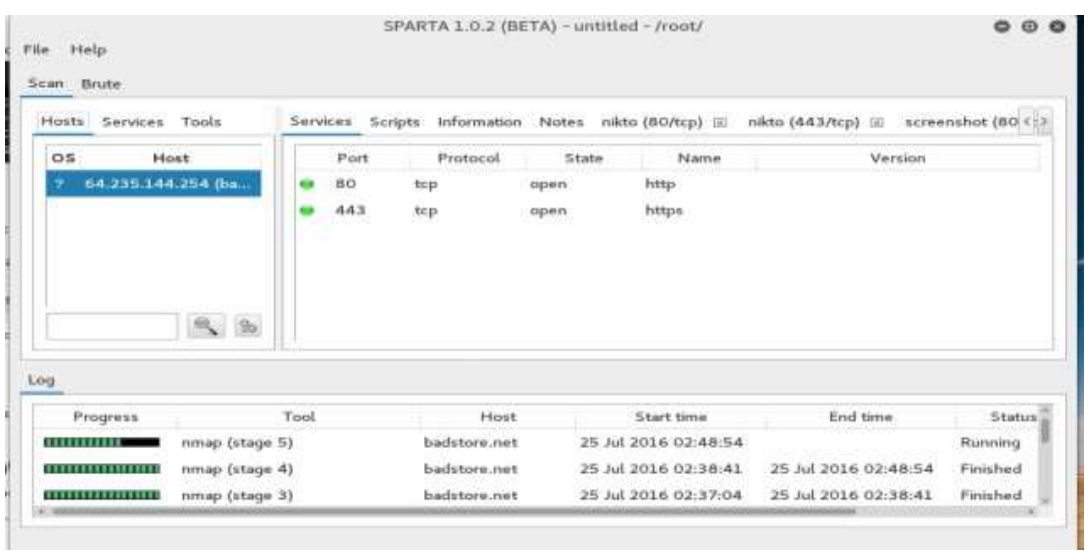
4. Passwords can be found by using its component named Hydra and are put away in internal wordlists.

5. It has likewise the capacity to recollect or stamp the systems which you have as of late worked upon.

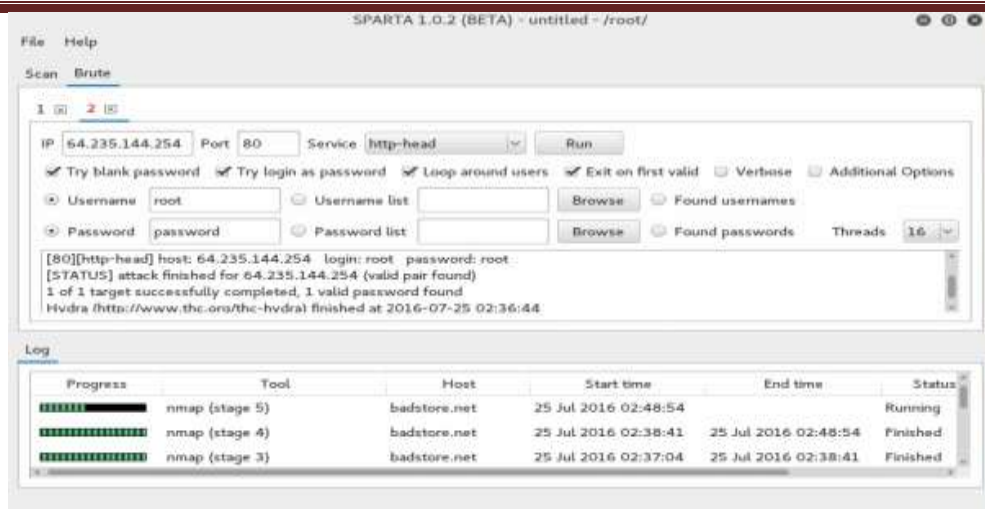
6. It has additionally the office to take screen captures whenever during the procedure.

Badstore.net (Sample vulnerablewebsite for penetration testing)

Right off the bat it examines the open ports and administrations relegated to that ports.




Secondly we perform password attack on this site using Hydra and 1 valid password found.




In Sparta, nikto vulnerability scanner is used to scan the vulnerabilities in the website.

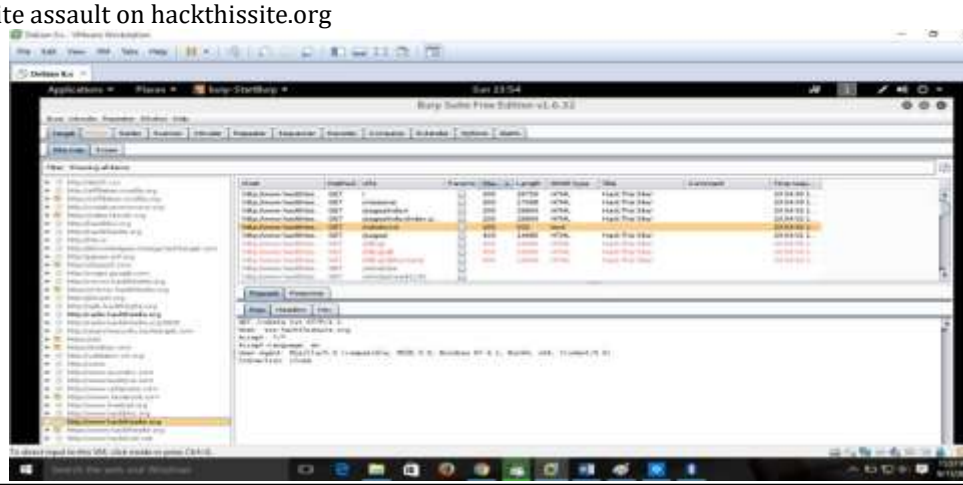

### 3) Burpsuite:

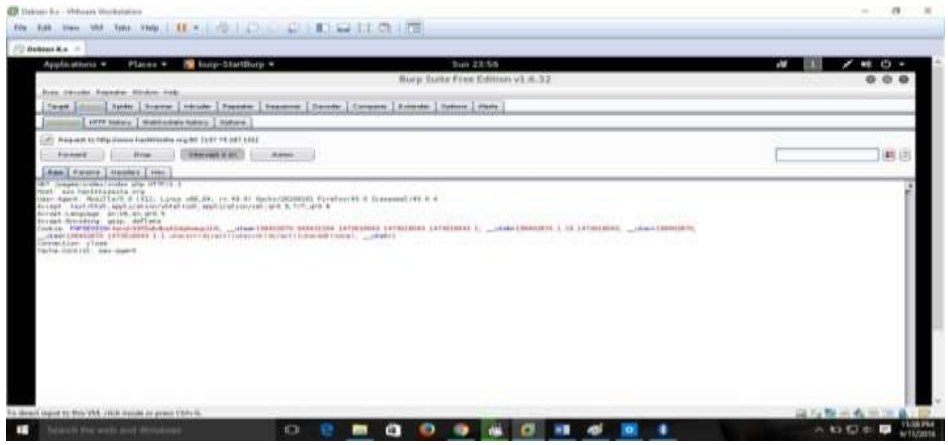
Burpsuite is a stage to test the security of web applications. It helps a great deal in security testing of web applications through its tremendous client driven interface.

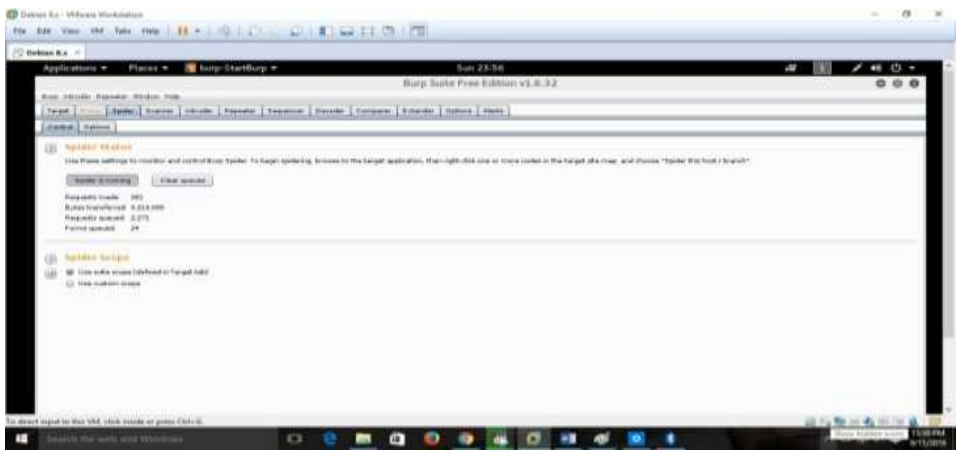
Functioning of Burpsuite:

Since burpsuite is utilized aside with the web program. As a matter of fact, burpsuite goes about as a HTTP intermediary server, from where all the http activity goes from the program must go through the burpsuite. For this initial step is to arrange the program settings according to the burp needs.

Burpsuite assault on hackthissite.org



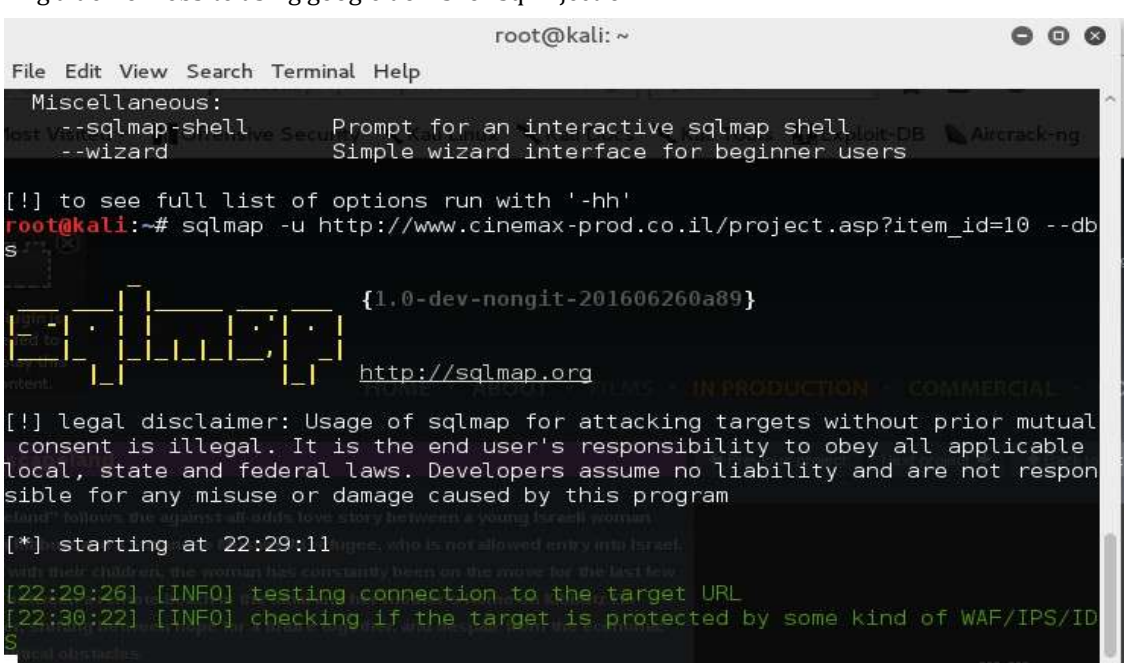




**4) Sqlmap:**

It is an apparatus utilized for sql injection method to hack websites database, in which sql articulations are added to misuse the website server. It is free based penetration testing device which has an effective discovery engine to get information and access the record system to run orders.

Checking a demo website using google dorks for sql injection:

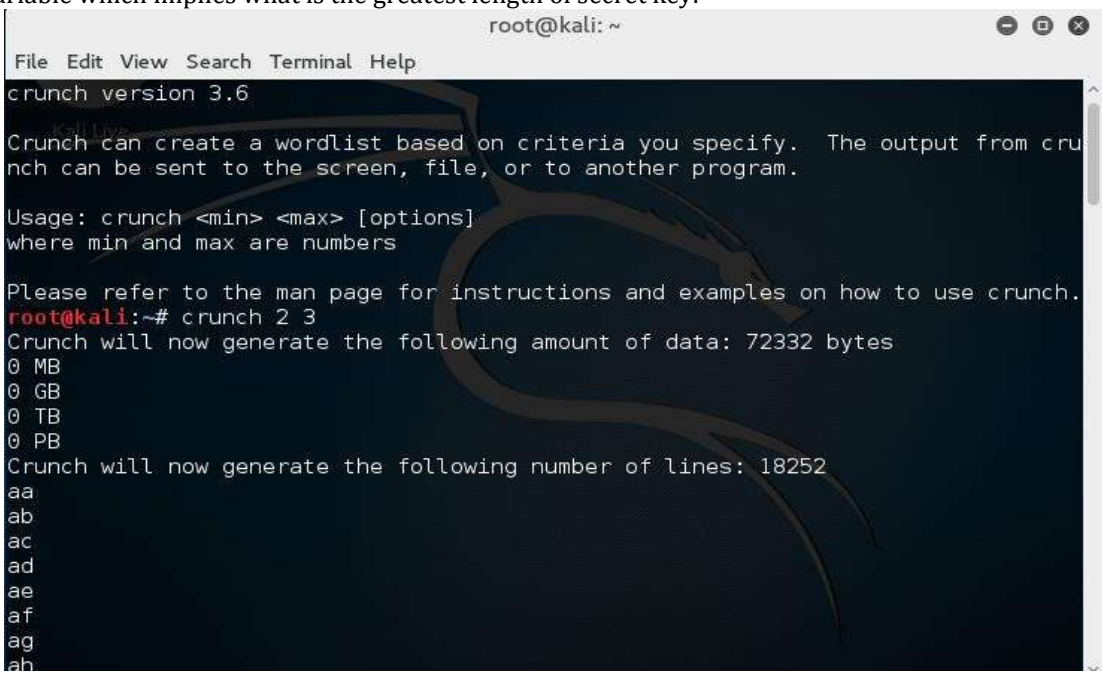


5) Crunch:

It is a watchword guessing instrument which gives us the rundown of estimated passwords depending upon how much size we give it for processing.

For instance: Crunch min max

Where min is a variable which implies what is the minimum length of secret word we are guessing for. Max is a variable which implies what is the greatest length of secret key.




**6) Cewl:**

Cewl is an instrument that is utilized for crawling the website and to gain the vast majority of the information about web pages into the profundity defined by the client. Fundamentally, it is intended to obtain the related words to a specific region which might be coordinate for passwords of the website.

Fundamentally two switches are for the most part utilized as a part of this device:

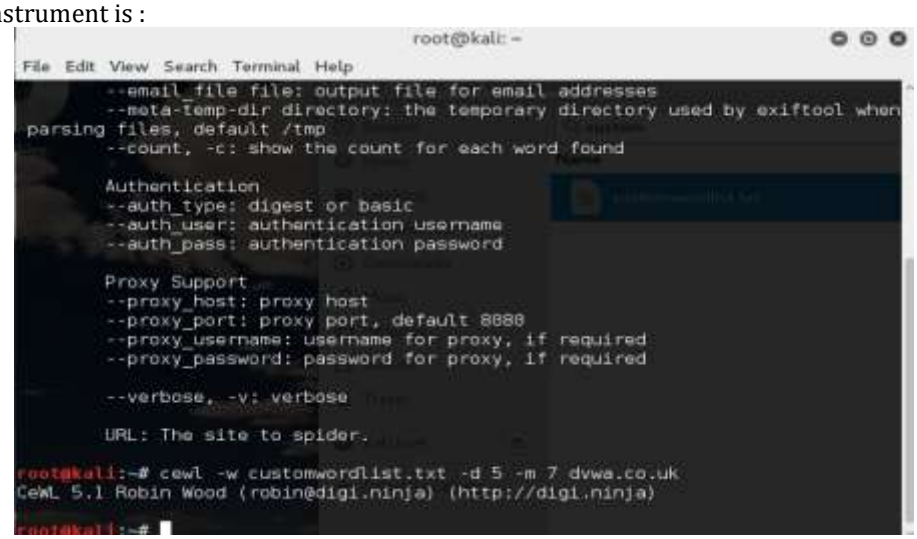
- d (profundity) and – m (Min word length)

The profundity swtich determines what number of pages top to bottom will the Cewl slithers through the website and – m determines the minimum word length that is required according to the need.

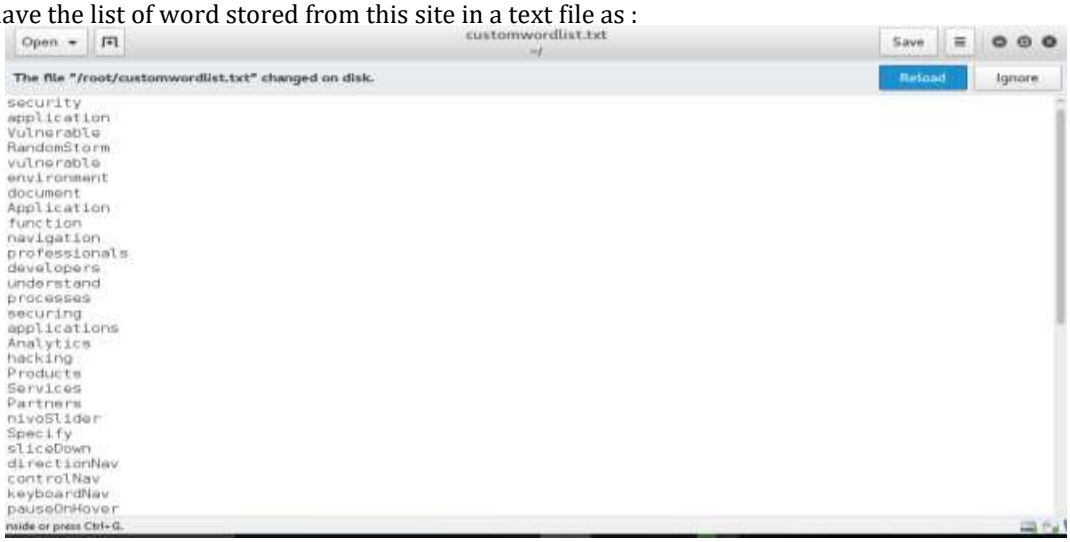
Language structure is :

Cewl – w customwordlist.txt – d 5 – m 7 <website's name>

Case of this instrument is :



Now We have the list of word stored from this site in a text file as :



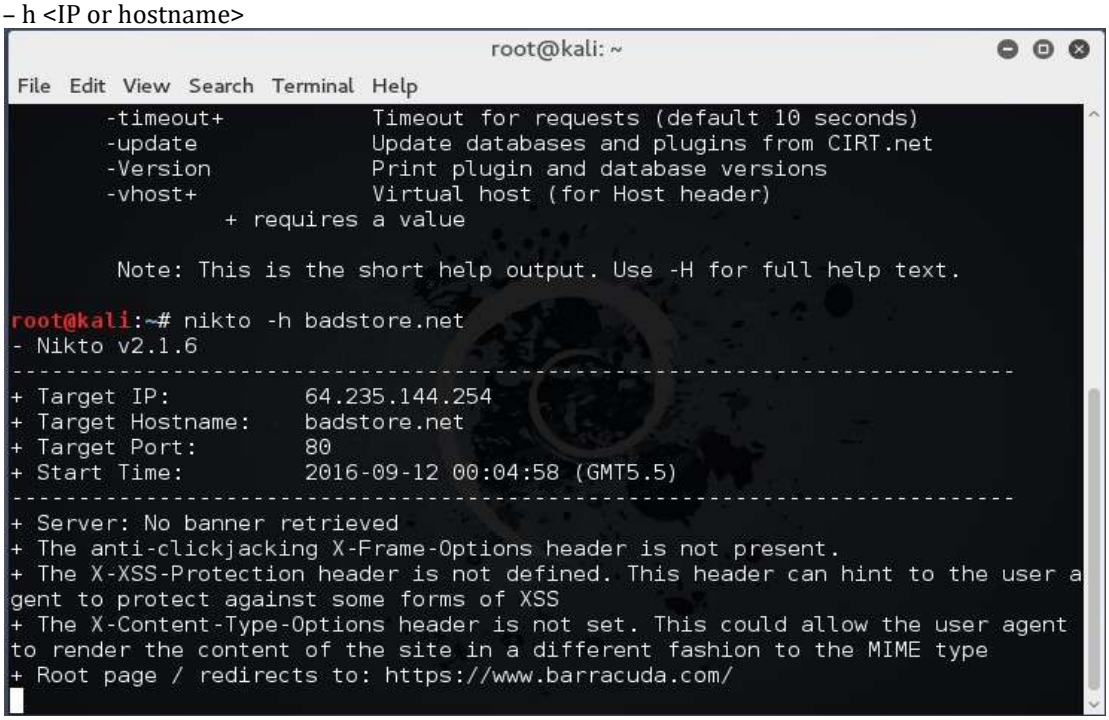

### 7) Nikto:

Nikto is a defenselessness scanner instrument which filters different kinds of vulnerabilities in the websites and on the system. It is an instrument which is utilized as observation for hacking websites.

The main shortcoming in this device is that it isn't stealthy, i.e the websites which have safety efforts can without much of a stretch recognize that you are scanning them.

Synatax of nikto :

nikto – h <IP or hostname>



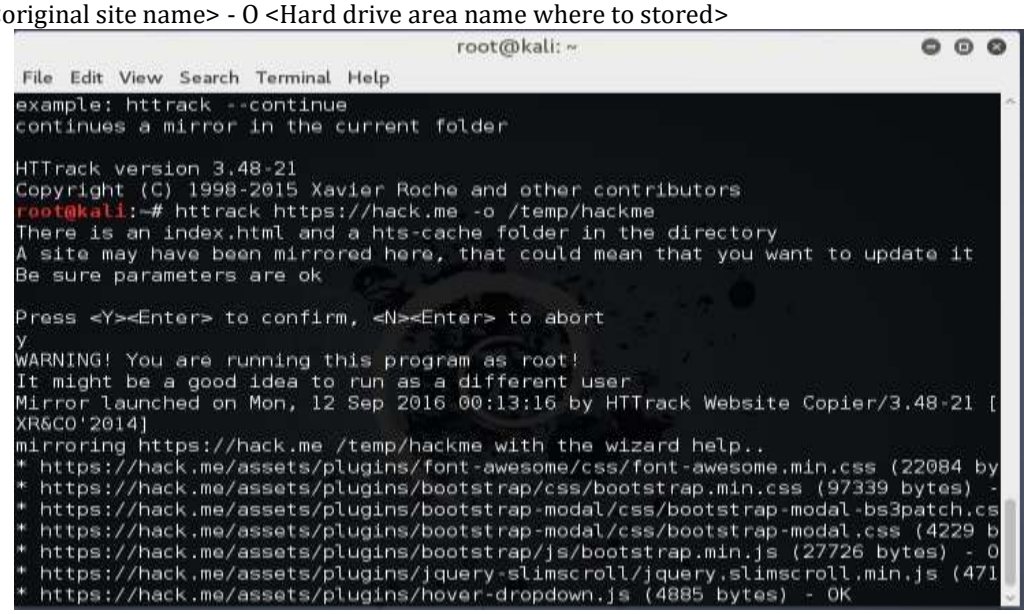

As in the screen capture, nikto instrument is utilized to find out the vulnerabilities of badstore.net website. So the yield of hardware tells that in the website X-XSS-Protection header isn't defined. And furthermore portrays the existed vulnerabilities in the website. Like hostile to clickjacking, and so forth.

### 8) Httrack:

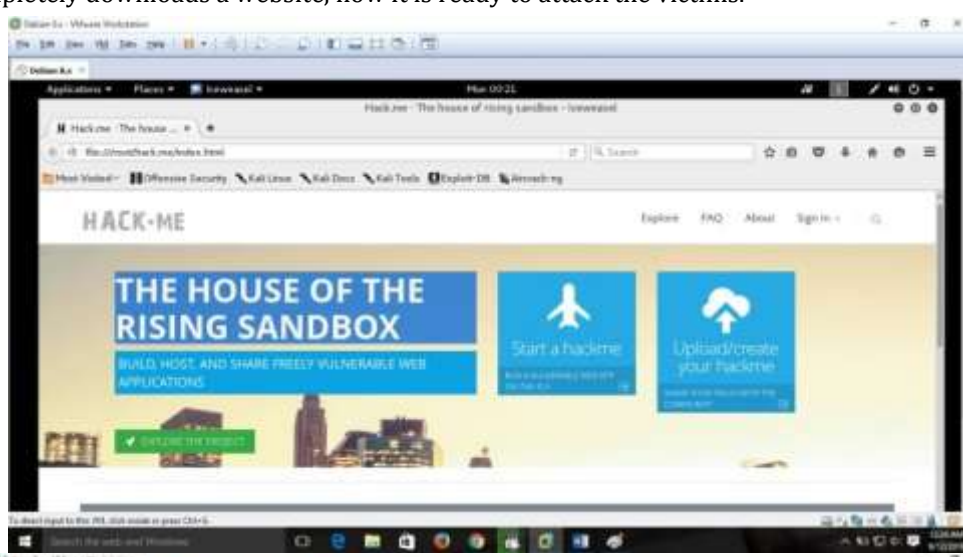
Httrack is an apparatus which is utilized to hack a client by defacing the entire website by copying every one of the substance of that website onto your hard drive. This is a device which totally downloads the full website substance which when runs gives the full photo of the original website.

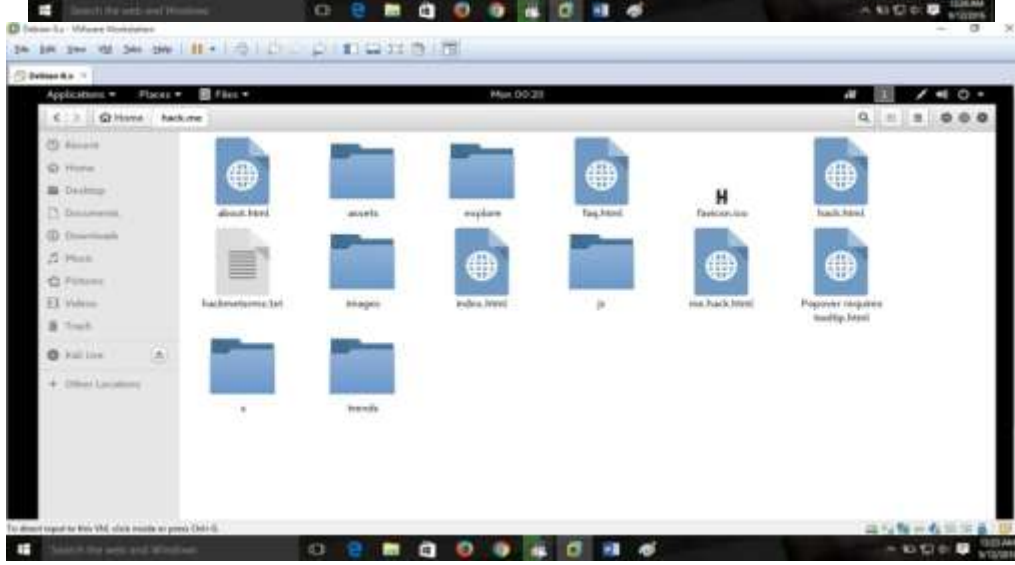
Linguistic structure:

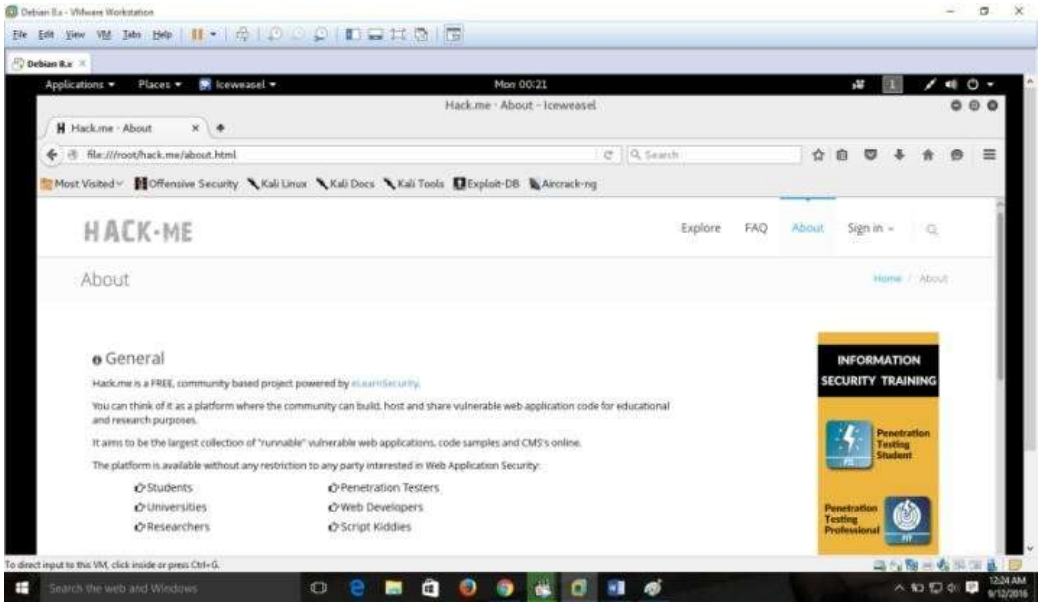
Httrack<original site name> - O <Hard drive area name where to stored>

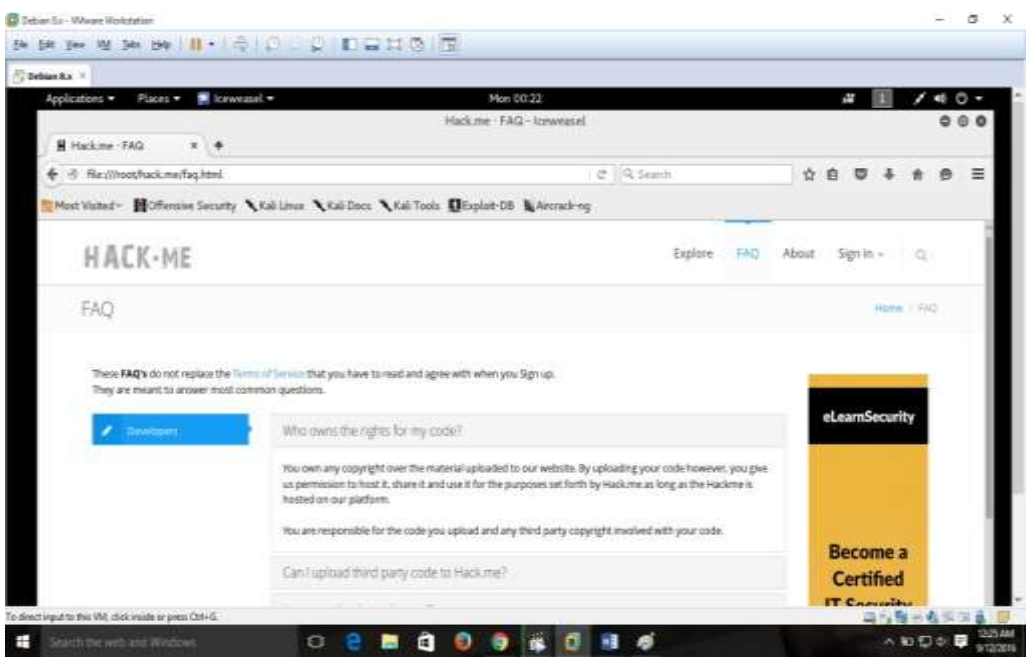



After it completely downloads a website, now it is ready to attack the victims.






**Conclusion**

Web applications are becoming prevalent and have across the board interaction medium in our day by day lives. In any case, at same point numerous vulnerabilities investigate delicate information. The distinctive web application vulnerabilities in light of the security properties that web application ought to be protected. However helplessness appraisal tools are robotized one which spares time and cash and furthermore protect the web applications from present day dangers. At the last the new propelled security assaults are continually emerging, requires the security expert to have positive security arrangement without putting tremendous number of web applications in danger. Subsequent to studying different review papers, finally it is chosen that there are such huge numbers of vulnerabilities dwell on the web servers and additionally web programs. Numerous tools are accessible online to find out these sort of vulnerabilities.The research done on penetration testing tools gives the assessment that system designer/administrator can find out what sort of vulnerabilities dwell in the system. With the goal that they can be secured from the unapproved access or assaults by aggressors.

**References**

1. Katkar Anjali S, Kulkarni Raj B, "Web helplessness recognition and security instrument". ISSN: 2231-2307, Volume 2, Issue 4, September 2012
2. Gopal R Chaudhari, Prof. Madhav V. Vaidya. "A Survey on security and vulnerabilities of web application".ISSN: 0975-9646, Vol-5(2), 2014,1856-1860
3. Mr. K.Naveen.Durai, K.Priyadharsini. "A study on security properties and web application scanner", ISSN:2320-088X, Vol-3, Issue.10,October 2014,pg.517-527.
4. SwarnaprabhaPatil, Prof. Nitin Aggarwal. "Web security assaults and injection-A study", ISSN:2278-7763,Vol-4, Issue.2,February-2015
5. KartikeyAggarwal,Dr. Sanjay Kumar Dubey. "Netwrok security: Attacks and Defense", Volume-1, Issue 3,August 2014
6. Ailin Zeng. "Discourse and research of PC arrange security",ISSN:0975-7384, Vol-6(7), pg.780-783,2014
7. Jie Shan. "Examination and research of PC organize security", ISSN:0975-7384,Vol-6(7),pg.874-877,2014

**The gem cannot be polished without friction, nor man perfected without trials.**

**~ Chinese Proverb**