Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 5, pp. 1439–1458
DOI : 10.47974/JIOS-1508

Empirical study on network exploitation tools and vulnerability detection tool

Kirti Sharma *
Shobha Bhatt †
Manju Khari §
Ambedkar Institute of Advanced Communication Technologies and Research (AIACTR)
Government Engineering College
Affiliated to Guru Gobind Singh Indraprastha University (GGSIU)
Geeta Colony 110031
Delhi
India

Abstract

Network security intends to shield the machine from unauthorized and conceivably destructive exercises. Network security is increasingly essential since individuals like to associate with each other all the time by means of the web. All of Personal Computers clients, representatives of expert associations, government hirelings, academicians, social specialists, students, and military people groups keep their most crucial information on web and furthermore do the cash related online exchanges. The web structure is itself with the end goal that there might be the plausibility of dangers to happen. To secure our system we should need to know which kind of security dangers may happen and how. By knowing this we may ready to discover security techniques against these dangers. This paper describes the detailed knowledge about Network exploitation tools that are used by anonymous users to exploit the network and get the credentials of the users.This provides awareness among the developers about the attack intended regarding the websites. Also, results and finding from vulnerabilities detection tools will be discussed in detail.

Subject Classification: *68M25.*

Keywords: *BeEF-XSS, DNS spoofing, Metasploit, Acunetix, Vulnerability, SQL, Information security.*

* *E-mail:* **kkirti.sharma@yahoo.com (Corrspoding Author)**
† *E-mail:* **bhattsho@gmail.com**
§ *E-mail:* **manjukhari@yahoo.com**

Introduction

Network security alludes to any exercises intended to ensure our system. In particular, these exercises secure the usability, reliability, integrity, and safety of our network and information. Powerful system security focuses on an assortment of dangers and prevents them from entering or spreading on our network. The present system comprises of huge number of open and private PC and other systems administration gadgets used to construct this system. Networks can be private, for example, inside an organization, school or extensive association or it can be available to the community. Secure Network has now turned into a need for any organization. The advancement of fast wired and remote system and web administrations have been done but since of various kinds of dangers the whole system is getting to be insecure and untrustworthy.

Network security hasn't generally been as important as it is today. The historical backdrop of network security is an account of the development of processing power, availability, and the Internet. At the point when PCs initially showed up in business, they were substantial, multi-client gadgets bolted behind the entryways of a data center. In many cases, clients didn't have terminals. They gave a demand to a PC administrator and got a report consequently. No genuine security issues here. Notwithstanding business client confinements, early PCs were once in a while joined to different PCs; and the Internet didn't exist. Open doors for anonymous access to crucial data were uncommon, and individual character data was still to a great extent kept on paper in file organizers. In the end, PCs started showing up in organizations. Obviously, administration needed these frameworks associated with the server farm frameworks. Consequently, systems showed up. Early Token Ring innovations in the long run offered approach to wireless and Ethernet connectivity giving rapid access. Add to this the present need to interface with the Internet [1], and open doors for culprits over the globe to take information or hold systems prisoner flourish.

So our propelling innovation, our need to interface with different business and open systems, and the developing necessity to gather and electronically store data require a forceful security response.To give a superior and also strong level of security [6], the goal ought to be done is the primary perspective, which is as per the following -

- Analyze the network security level.
- To break down security dangers and gives the system against it.
- Discussing part of PC framework resources in the region of security.

The viable and proficient information security designs can be created with comprehension of security issues and investigation of components that make a system powerless against assault. These days, the transfer of data in a more secure and secure path over a system has turned into a noteworthy test for the business. The assaults and the network security efforts characterize how utilizing the system security [13] devices, a superior, sound and safe system can be composed and kept up for an association/industry. This exploration centers around the issues through which network security can be managed and kept up more productively in an organization.

This paper introduced various sections. In the section named Network exploitation tools, there are several tools mentioned that are basically used by the attackers to exploit the network and the credentials of users. In the next section, the practical use of the Acunetix tool is shown. This is a vulnerability detection tool [19] that could provide the loopholes of websites to users and fix them timely. Then a brief discussion is given, post that the conclusion is given regarding the exploration and experimental study.

Related work

Network attack incorporates actions taken by computer networks to interrupt, contradict, distort or destroy the information within computers. This further compromises with the data of the valid users. The anonymous users exploit the network which allows them to breach the information security and access the crucial data of the users. To counter the exploitation, various authors stepped forward via suggesting realistic and proficient approaches.

Saravanan.et.al investigated some security ruptures in web applications that needs prompt consideration. He described some of the attacks that enable an attacker to impersonate a victim [15].

Pathak, MrunaliP.et.alpresented an analysis of the source code of the scripts used to attack the information security. The result then trained the developers and coders in the detection of faults [14].

Chavan, Savita B.et.al classified the attacks and weaknesses that can lead to the compromise of a website, its data, or its users. In that paper, web application vulnerabilities are classified based on requirement analysis, design, implementation and deployment of web application [3].

Van Goethem.et.al displayed a detailed survey on different sorts of Structured Query Dialect Injection assaults, Cross-Site Scripting Attack, vulnerabilities, and counteractive action methods [18].

Li, Xiaowei.et.al surveyed state of the art in securing web applications, with a focus on approaches that are deployed on the server-side. In particular, that survey covers the techniques which consider the threat model [12].

William G.J. Halfond. *et.al* shows another exceptionally robotized approach for securing Web applications against SQL injection [10] that has both reasonable and handy preferences over most existing systems. The authors have stated that detecting [5].

Jose Fonseca. *et.al* examined the regular web deficiencies are talked about thinking, considering different programming dialects. Keeping in mind the end goal to take care of the issue of web security vulnerabilities, the creators have examined the code fix to assemble attributes of code in charge of powerless conduct.[4].

S.Shalini. *et.al* examined the worms exploiting JavaScript XSS vulnerabilities. To counter this exploit, the creators have proposed a client-side arrangement that uses a well-ordered way to deal with secure cross-site scripting, without corrupting the perusing background [16].

Lwin KhinShar. *et.al* introduced the current ways to deal with relieve this issue basically center around successful identification of XSS vulnerabilities in the projects or counteractive action of ongoing XSS assaults [17].

Kuldeep Kumar. *et.al* proposed a technique based on the grammatical structure of a SQL injection and approval of the client input. This technique utilizes consolidated static and dynamic examination. The trials demonstrate that the proposed strategy is compelling and straightforward than different techniques [11].

These are the various approaches provided by several authors to secure the network and scan the web application with a highly adaptive vulnerability detection tool [7], [8]. In the next section, different network exploitation tools have been discussed with their experimental evaluation.

Network exploitation tools

Network breach is the process by which digital information is compromised [9]. The targets of breaching areto unshield confidentiality, destroy integrity, and weaken availability. It includes several types of tools that are used by an anonymous person to exploit the network.

1. *BeEF-XSS*

BeEF-XSS is used for exploiting the browser using a social engineering tool.The default username/password is beef. To change the username/ password, use command cd /etc/beef-xss/ vi config.yaml.

How the attack is performed:

Step 1: Run "./beef" in the terminal. The following screen will appear as shown in figure 1.

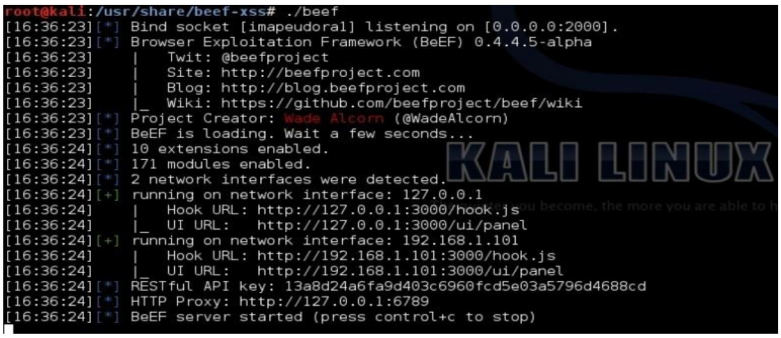

Figure 1

Terminal executing command

Step 2. The following window will appear in the browser as shown in figure 2. Type the username and password as "beef".

Figure 2

Interface to provide login details

Step 3. Click on the Online Hooked Browser to see details as shown in figure 3.

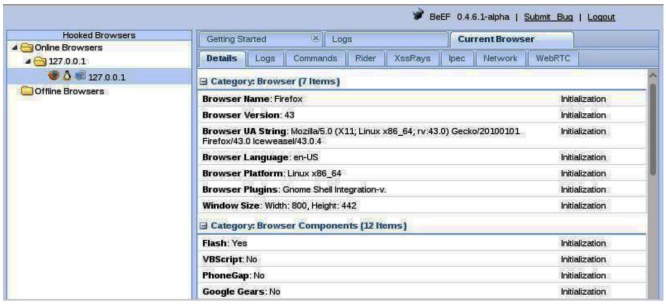

Figure 3

Category shown in current browser

Step 4. Figure 4 is a demonstration page and here typed "aslam" in the text box as shown below.

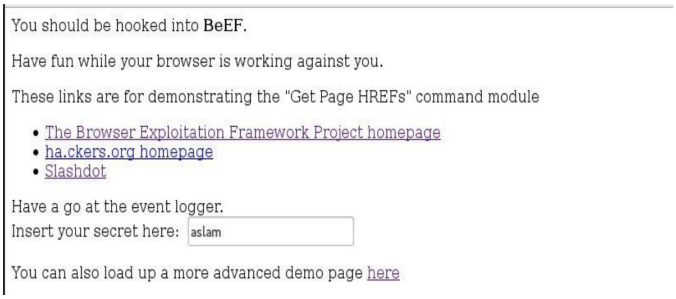

Figure 4

Demonstration page

Step 5. The typed word appears in the log tab as shown in figure 5 along with the other information about user activities.

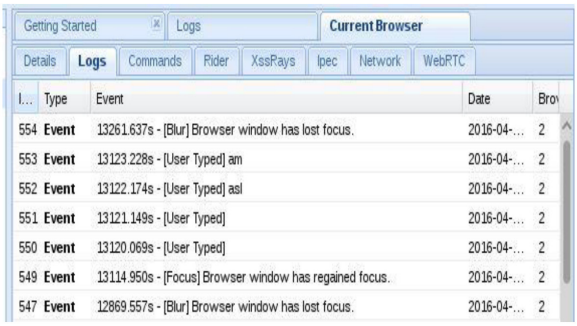

Figure 5

Typed words capturing inside log tab

Step 6. Once the browser is hooked as shown in figure 6, now perform several commands to execute on the user's machine.

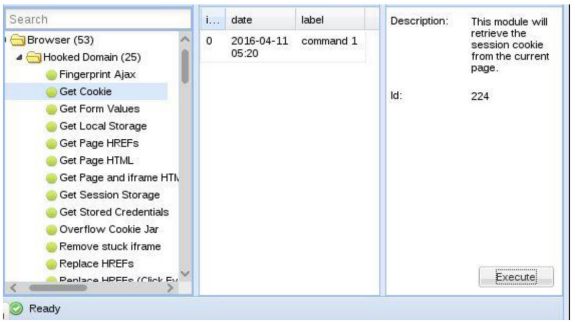

Figure 6

Hooked browser

2. *DNS-Spoofing*

If there should arise an occurrence of DNS ID caricaturing, when a name settle asks for is produced by the customer to send it to the DNS server, an ID will be created alongside the demand. The customer will acknowledge the reaction for his demand if the ID of the reaction bundle matches with the asked for packet ID. Be that as it may, along these lines of name determination isn't secured. Since any unapproved client can sniff the demand and can make a reaction bundle on the fly with a similar id and IP data contained in it isn't the normal one [2]. This sort of DNS assault is known as DNS ID Spoofing.

How the attack is performed:

Step 1. Open a terminal and locate etter.conf file as shown in figure 7 and then open the file in any editor. Set the privileges on 0 from 65334 on both group ID and user ID.

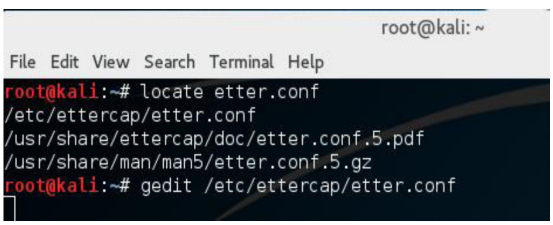

Figure 7

Locate etter.conf file

Step 2. In terminal enter "ettercap –G", this will open the graphical version of ettercap as shown in figure 8.

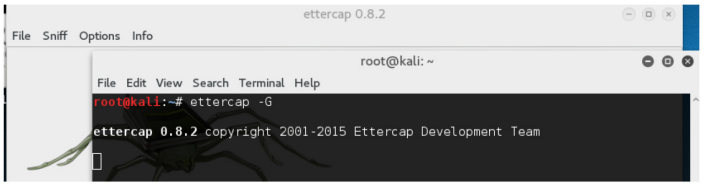

Figure 8

Command to open graphical version of ettercap

Step 3. Select unified sniff from sniff menu. Then a pop-up will appear as shown in figure 9 and ask for the Network Interface. Select eth0 if you are having LAN network connected to the system.Select wlan0 if you are having Wireless LAN connected to system.Press OK.

Figure 9

Interface of Ettercap

Step 4. To perform the attack, we must know the gateway of the network, it can be easily obtained using "route –n" as shown in figure 10. In our case the gateway is 10.40.246.1. Gateway address will be our target1 and target2 will the victim IP address.

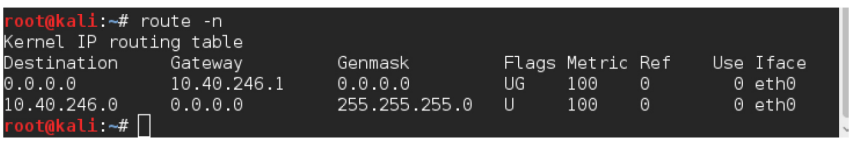

Figure 10

Command to know the gateway of network

Step 5. Press Ctrl+T to open the Target list and add as shown in figure 11. Target1: gateway address. Target2: victim address.

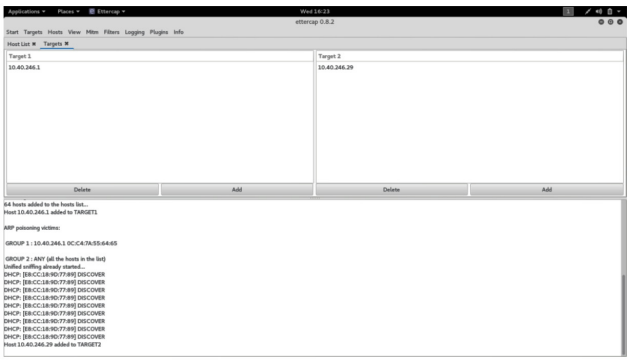

Figure 11

Target list

Step 6. Now Click on the plugin and activate dns spoof. The IP is spoofed now as shown in figure 12.

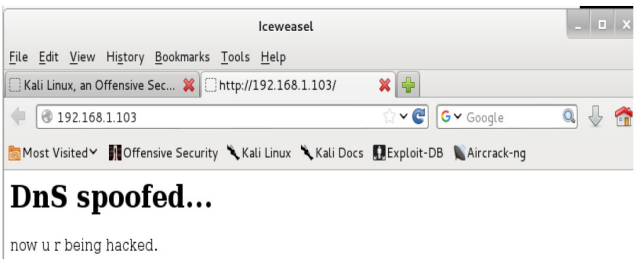

Figure 12

DNS spoofed

3. **John the Ripper**

John the Ripper is a free password breaking programming tool.

How the attack is performed:

Step 1. Open terminal and root to john password as shown in figure 13.

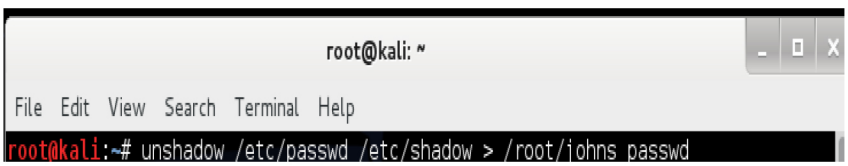

Figure 13

Command to root

Step 2. List the password file, located inside the user as shown in figure 14.

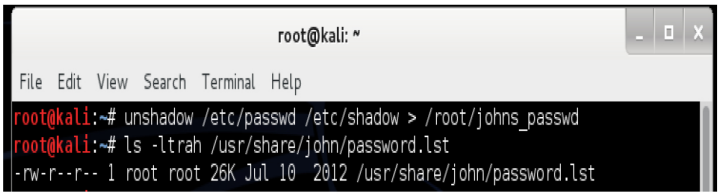

Figure 14

Locate password file list

Step 3. The created directory consists the hash of password and can be decrypted back using following command as shown in figure 15.

Figure 15

Password found

4. *Metasploit*

This is an open-source tool and used for penetration testing, IDS signature Development and exploit research. It does not require any knowledge of the software bug or exploit machine code.

How the attack is performed:

Step 1. See the files and directories in C: drive of Windows XP as shown in below figure 16.

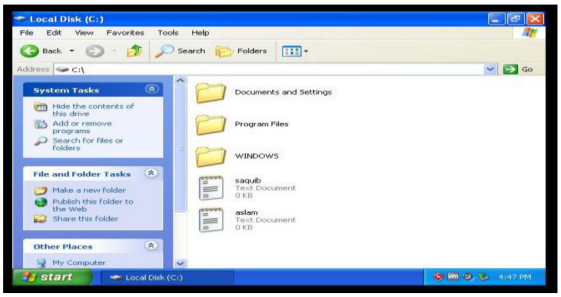

Figure 16

C-drive of windows XP

Step 2. Find the IP Address of the host machine running Windows XP as shown in figure 17.

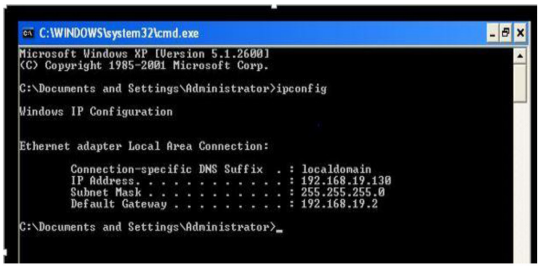

Figure 17

Observe IP address

Step 3. Run Kali Linux in Virtual Machine and Open Metasploit. The following terminal will appear as shown in figure 18.

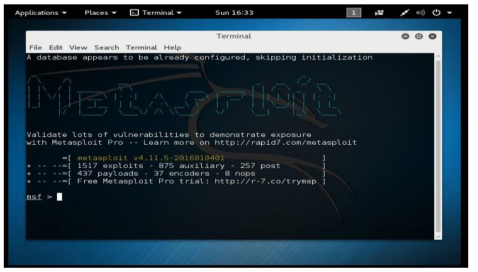

Figure 18

Opening Metasploit

Step 4. Type "search netapi" and press Enter. It will show the modules that have vulnerabilities and their rank listed against them as shown in figure 19.

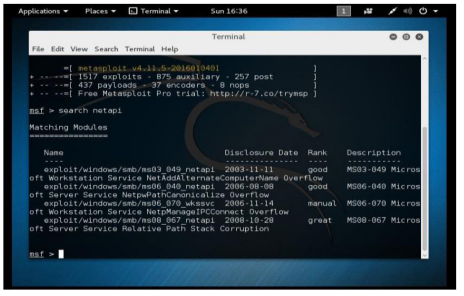

Figure 19

Modules showing vulnerabilities

Step 5. Exploit the vulnerability whose rank is Great and easy to exploit. So, Type "use [listed_vulnerability_to_exploit]". It will show the chosen vulnerability. Now, Type "show options" to see the current settings as shown in figure 20.

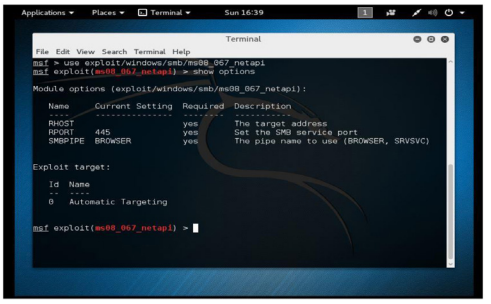

Figure 20

Choose the target to exploit

Step 6. Set the Host IP Address (Windows XP) by typing "set RHOST [IP Address]" as shown in figure 21. Also set payload by typing "set PAYLOAD windows/shell_bind_tcp".

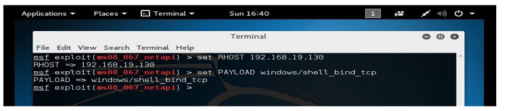

Figure 21

Set Host IP and Payload

Step 7. After that, we have to simply type "exploit" in the terminal and the attack is successful as shown in figure 22. Now, have full control access of the Host Machine (Windows XP).

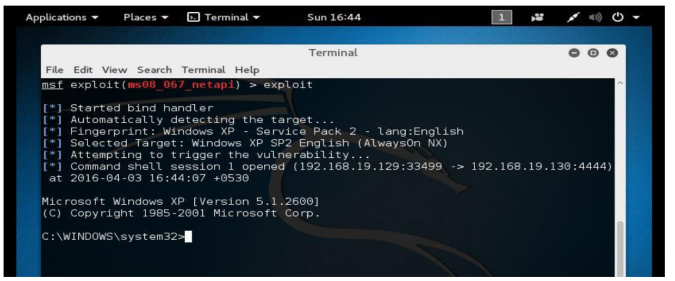

Figure 22

Command exploit and get full access

Step 8. The Attack is completed. We can access, modify, add, and delete any file and directory like the administrator as shown in figure 23.

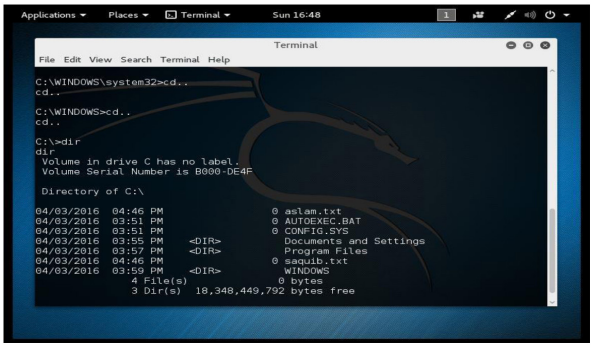

Figure 23

Accessible interface to modify, delete any director

5. SQLMAP

SQLMAP tool of Kali Linux has been used to hack a website (more specifically Database) and extract usernames and passwords.

How the attack is performed:

Step 1. Find a vulnerable website as shown in figure 24.

a. Google Dorks strings to find Vulnerable SQLMAP SQL injectable website

b. Another way is to write – php?id=

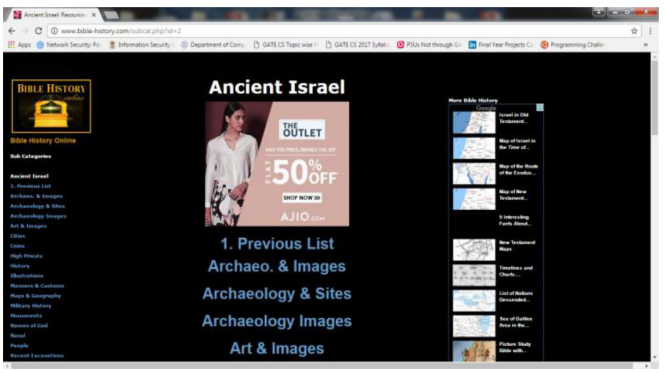

Figure 24

Search vulnerable website

Step 2. List DBMS databases using SQLMAP SQL Injection as shown in figure 25.

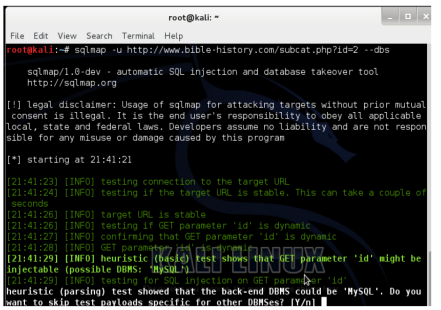

Figure 25

List databases

Step 3. Outcome of the database table as shown in figure 26.

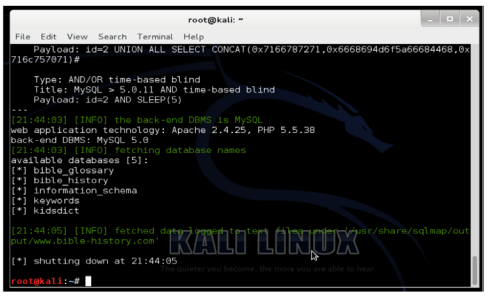

Figure 26

Table of database

Step 4. List tables of the target database using SQLMAP SQL Injection as shown in figure 27.

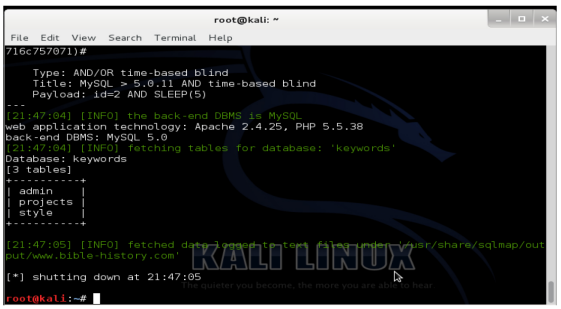

Figure 27

List of tables

Step 5. List columns on the target table of the selected database using SQLMAP SQL Injection as shown in figure 28.

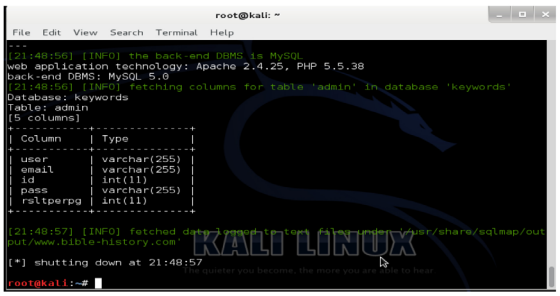

Figure 28

Getting Column names

Step 6. List usernames from target columns of the target table of the selected database using SQLMAP as shown in figure 29.

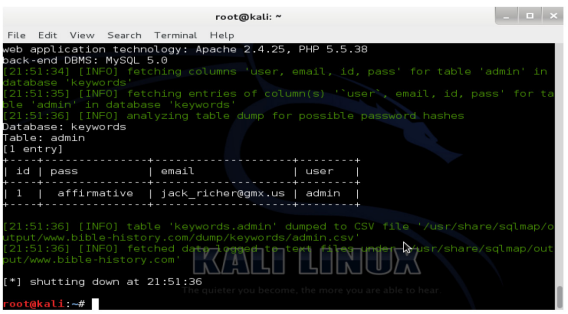

Figure 29

List of usernames

Following table 1 is showing the list of tools with their respective figures.

Table 1

Figures to be referred from annexure

S. No.	Exploitation tool	Refer figures from annexures
1.	BeEF-XSS	Figure 3, Figure 5, Figure 6
2.	DNS-Spoofing	Figure 8, Figure 9, Figure 10, Figure 11
3.	John the Ripper	Figure 13, Figure 14
4.	Metasploit	Figure 17, Figure 18, Figure 19, Figure 20, Figure 21, Figure 22
5.	SQLMAP	Figure 25, Figure 26, Figure 27, Figure 28

Network vulnerability detection tool

Vulnerability detection tools are used to detect the vulnerability of any kind of website. There are various tools available that can be used freely eg.Acunetix, Nessus, OpenVAS, Netsparker, W3af, etc. These tools are open source web application scanner.

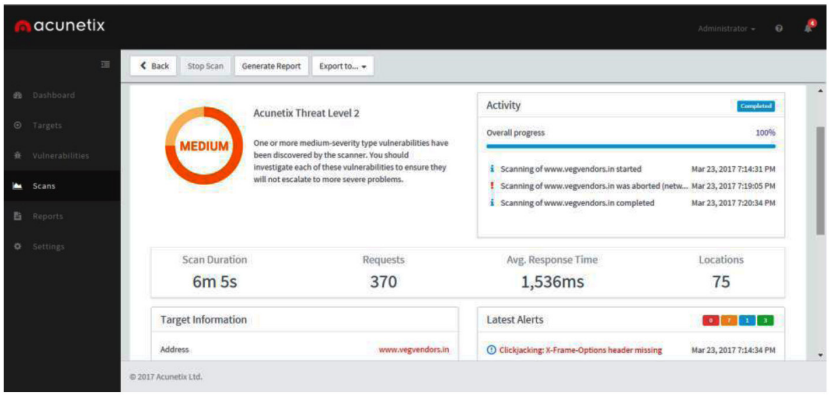

Figure 30

Four parameters in Acunetix tool

Acunetix tool is vigorously used to scan the vulnerability of the website. It is an automated scanning process, which automatically starts the scan once the target host or website is entered. It comprises various components that run the complete scanning process. It consists two phases that are crawler phase and progress phase. The website named "www.vegvendors.in" is used for vulnerability detection. This tool Acunetix shows four parameters that are shown in figure 30:

- Scan Duration
- Requests
- Average response time
- Locations

Table 2

Levels of threat

Color	Level of threat	Description
Red	High	Huge amount of risk; User cannot avoid this threat and has to find urgent solution.

Contd...

Orange	Medium	Some unavoidable vulnerabilities should not be avoided.
Blue	Low	Minimal amount of risk.
Green	None	Gives only the information about the particular vulnerability.

Also, there are levels of threats that depict different descriptions as shown in table 2. It is shown via four colors: red, orange, blue, green. Red color represents the high level of threat that means there is a huge amount of risk with the discovered vulnerabilities. User cannot avoid this threat and has to find an urgent solution. Because at any time, the system can be affected by the attack. The system is in critical stage with this kind of threat level. Orange color depicts the medium level of threat which refers that some unavoidable vulnerabilities should not be avoided. While blue color represents the low level that signifies that there is a minimal amount of risk involved with the vulnerability discovered. The user is safe with the vulnerability and can ignore the threat easily. And color green represents none threat that states it gives only the information about the particular vulnerability. There is no risk attached to this level. The system is safe with this type of threat level. Users can ignore this threat.

The screenshot in figure 31 is showing the various vulnerabilities that have been encountered by the tool Acunetix. The top orange-colored vulnerabilities are the medium level threat as per the levels of threats depicted via a color-coded scheme.

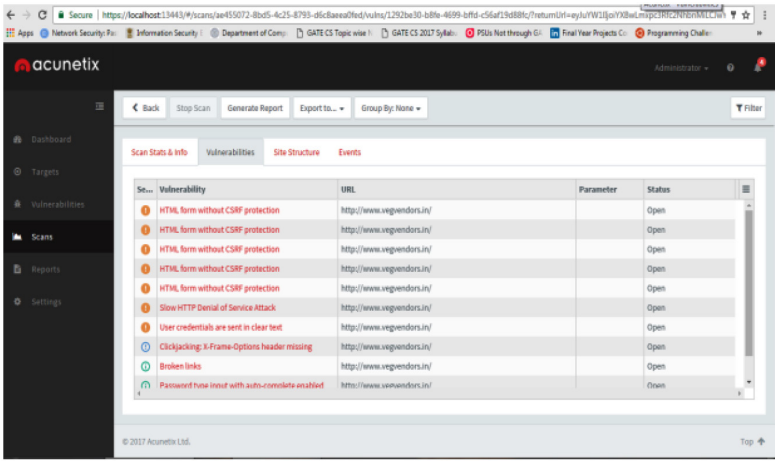

Figure 31

Acunetix showing vulnerabilities in the website

This tool scanned the target host or target website completely with the generated scan report depicting various vulnerabilities like SQL injection, Cross-site Scripting attack, etc. It alerts the developer to protect their website mainly from which of the most emergent probable attack via generating a list of vulnerabilities.

Discussion

The exploitation tool assists the attacker to exploit the information security. Attackers opt for the reconnaissance stage before commencing any attack. In that stage, they gather the complete information regarding the device and path which they follow to breach. This paper has done the experimental evaluation of various network exploitation tools like BeEF-XSS, DNS spoofing, SQLMAP, Metasploit and john the ripper. BeEF-XSS is an exploitation tool that exploits the browser using a social engineering tool. DNS spoofing is used to spoof the ID and IP data. SQLMAP tool is primarily used to get the metadata information that resides inside the database at the backend side. The attacker focuses on database name, column details, usernames list, and related subfields to inaugurate a big assault. Another exploitation tool that is Metasploit tool is used for penetration testing. This permits the attacker to get the full access onto Host machine and illegally authorize him to access, modify, delete any directory of choice. While the password cracker tool named John the Ripper handovers the password via generating the harvester file. This exploitation is resisted to some extent via approaching a high-quality vulnerability detection tool. It already detects the vulnerability and alerts the developers to fix the issue earlier before any invalid user exploits it. The Acunetix tool scanned "www.vegvendors.in" website proficiently and results various vulnerabilities. It uses the color-coded mechanism to level the threats which provide easier observation to analyze the report quickly.

Conclusion

This paper was devised to gratify the upstairs demands of the information security domain which is somehow compromised via exploiting either network or web application and spotlighted mainly the network breach tools that might be used by the anonymous users to access the crucial data that approached via gaining knowledge about intended attacks subsequently. This knowledge is the outcome of the vulnerabilities

that a particular website uphold. To prevent any system from becoming infected, the initial thing is to make the system less prone to become vulnerable to these attacks that is make the system much efficient from earlier phases. The ordinary clients are less aware of the vulnerabilities issues to their frameworks. So if framework is being hacked by an anonymous person, at that point certain bargains happen like trade-off to privacy, compromise to uprightness and accessibility. This is resisted via using efficient vulnerability detection tool which generates the report of probable threats that might harm the website in future. Listing of these vulnerabilities, allows the developers to take action at right time before bearing costly fallout.

References

[1] O. Adeyinka, "Internet attack methods and internet security technology," Modeling & Simulation, 2008. AICMS 08. *Second Asia International Conference on*, vol., no., pp. 77-82, 13-15 May (2008).

[2] J. Andress, "IPv6: the next internet protocol," Apr. (2005). [Online]. Available: www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.

[3] S. B. Chavan and B. B. Meshram, "Classification of web application vulnerabilities," *International Journal of Engineering Science and Innovative Technology* (IJESIT), vol. 2, pp. 241 (2013).

[4] J. Fonseca, M. Vieira, and H. Madeira, "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks," Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on, *IEEE* (2007).

[5] W. G. Halfond, J. Viegas, and A. Orso, "A classification of SQL-injection attacks and countermeasures," Proceedings of the IEEE International Symposium on Secure Software Engineering, vol. 1, *IEEE* (2006).

[6] "Enterprise Security Articles - Bright Hub," [Online]. Available: http://www.brighthub.com/computing/enterprise-security/articles/61557.aspx.

[7] W. Ahmad, "Network security attacks, tools, and techniques," [Online]. Available: http://www.slideshare.net/waqasahmad1995/network-securityattacks-tools-and-techniques-52207382.

[8] Vulnerability Scanning Tools, [Online]. Available: https://books.google.co.in/books?hl=en&lr=&id=RoS9BwAAQBAJ&oi=fnd&pg=

PA295&dq=vulnerability+scanning+tool&ots=K63mbzlMwa&sig=hX4RvFLF69Kvla3MYhlRqUgdDjk#v=onepage&q=vulnerability%20scanning%20tool&f=false.

[9] "Evolution of Network Security," ECPI University Blog, [Online]. Available: https://www.ecpi.edu/blog/evolution-of-network-security.

[10] R. Johari and P. Sharma, "A survey on web application vulnerabilities (SQLIA, XSS) exploitation and security engine for SQL injection," Communication Systems and Network Technologies (CSNT), 2012 International Conference on, *IEEE* (2012).

[11] K. Kumar, D. Jena, and R. Kumar, "A novel approach to detect SQL injection in web applications," *International Journal of Application or Innovation in Engineering & Management*, vol. 6, pp. 37-43 (2013).

[12] X. Li and Y. Xue, "A survey on server-side approaches to securing web applications," *ACM Computing Surveys* (CSUR), vol. 46, no. 4, pp. 54 (2014).

[13] G. A. Marin, "Network security basics," Security & Privacy, *IEEE,* vol. 3, no. 6, pp. 68-72, Nov.-Dec. (2005).

[14] M. P. Pathak, N. Kausar Khan, and T. C. Tantak, *"Novel approach to detect and prevent web attacks,"* (2016).

[15] A. Saravanan, M. S. Irfan Ahmed, and S. SathyaBama, "A survey on exposed vulnerabilities in web applications," *Asia Pacific Journal of Research*, vol. I, Issue XXXV (2016).

[16] S. Shalini and S. Usha, "Prevention of cross-site scripting attacks (XSS) on web applications in the client side," *IJCSI International Journal of Computer Science Issues*, vol. 8, no. 4 (2011).

[17] L. K. Shar and H. B. K. Tan, "Automated removal of cross site scripting vulnerabilities in web applications," *Information and Software Technology*, vol. 54, no. 5, pp. 467-478 (2012).

[18] T. Van Goethem, B. Van Dongen, W. Joosen, and F. Piessens, "Large-scale security analysis of the web: Challenges and findings," in Proc. International Conference on Trust and Trustworthy Computing, Springer International Publishing, pp. 3-21 (2014).

[19] Y. Wang and J. Yang, "Ethical hacking and network defense: Choose your best network vulnerability scanning tool," *Advanced Information Networking and Applications Workshops* (WAINA), 2017 31st International Conference on, IEEE (2017).

Receivd November, 2019