MDR VULNERABILITY MANAGEMENT

Prof. Deepika Patil[1], Gaurav Sarvaiya[2], ShubhamGupta [3] Chaitali Sawant[4], Prathamesh Naik[5]
Department of Electronics and Telecommunication
[1-5]K.C. College of Engineering and Management Studies and Research
Mumbai, India
[1]deepika.patil@kccemsr.edu.in, [2]sarvaiyagaurav@kccemsr.edu.in, [3]guptashubham@kccemsr.edu.in , [4]sawantchaitali@kccemsr.edu.in, [5]naikprathamesh@kccemsr.edu.in

ABSTRACT

This paper describes how a vulnerability management (VM) process is designed & implemented within an organization. Articles and studies about VM usually focus mainly on the technology aspects of vulnerability scanning and testing. The goal of this study is to draw an attention to something that is often overlooked: a basic VM process which could be easily adapted and implemented in any part of theorganization.

It also gives ideas how to handle complexity in IT infrastructure with the increase in new trends of security... The main goal of this study is to modify traditional pattern and adopt the required-modern approach of vulnerability management. This approaches will weight achieve the good result. [1]

In the present scenario, the usage of internet is vast and is escalating day by day. Internet facilities are employed in almost every field of work and people are becoming depending on it, with the increasing dependency on the internet, concern regarding information security has been increased. Because most of the work, e-commerce, chatting, payment of the bill, etc. are work through over the internet. That is why security is most important for any web site. Basically, such security concern is high in the field of organizations, institutions, and the financial sector. This problem is greater in the field of the finance sector, this problem is greater in this field not only because the financial capital associated but also organizations and client sensitive and private data. If this data is been hacked by the attacker then attacker or unauthorized user can use this data in an unethical way. To test the security in network, web applications, the company performs penetration testing which identifies networks and web applications vulnerabilities and attackers actions. This paper is focused on network security. In this proposed research work, a framework has been built to test the vulnerabilities. This framework has the same working module as that of a financial institutions website. After penetration testing, based on the vulnerability further, a framework will be designed which will provide more security to such web sites. The developed framework can be used in several institutions, company, Organization to test the vulnerability.[2]

Keywords—Penetration Testing; Finance sector; Web Security; Vulnerability; Manual testing ; Automated testing

INTRODUCTION

As the significant use of internet and web application in the last two decades, there is a huge risk associated with unauthorized access to the confidential data and the risk of maintaining the integrity of the information. Day by day new exploitation and hacking activities are discovered. Therefore it is really necessary to identify the vulnerabilities and install the security patches for those vulnerabilities. This activity becomes the highest priority of organizations nowadays. To help organization for identifying their loopholes into the system the Vulnerability Assessment & Penetration Testing (VAPT) techniques are used. It helps to determine the reliability of the security arrangements, that they are effective against the latest cyber threats or not. This technique helps to develop a secured mechanism which is able to identify the vulnerabilities

.

The identification of the vulnerabilities into the system has become a prime issue for an organization. With the growing technology, the complexity of the systems is also being Increased so it is very difficult to identify the weakness in the complex system. To stay secure the organizations have to identify the maximum vulnerabilities and minimize the threats. To do so they have to do Vulnerability Assessment and Penetration Testing on a regular basis.

VAPT is made up of two things Vulnerability Assessment (VA) and Penetration Testing (PT), both these techniques have their own features and uniqueness. Vulnerability Assessment means to scan the system and identify the loopholes of the system and generates a report of them. Penetration Testing means it is a white box testing conducted by the organization to exploit the vulnerabilities identified in the vulnerability assessment report. There are many vulnerability scanners available in the market which can calculate the damage and threats which can be occurred due to those vulnerabilities. It can also be identified that what is the impact score of that vulnerability and what are the possible solution available for the vulnerability. VAPT techniques tests identify the flaws so that organizations can decide the priority for the mitigation process. So we can say that the combined packet of Vulnerability Assessment and Penetration Testing gives the cleared path of existing weaknesses along with the risk associated with it.[3]

This manuscript is arranged as follows, Section II describes Vulnerability Assessment in detail, includes; process, pros and cons. Section III describes Penetration Testing in detail, includes; process, pros and cons. Section IV describes the combination and comparison of VA &PT.[4]

II. VULNERABILITY ASSESSMENT

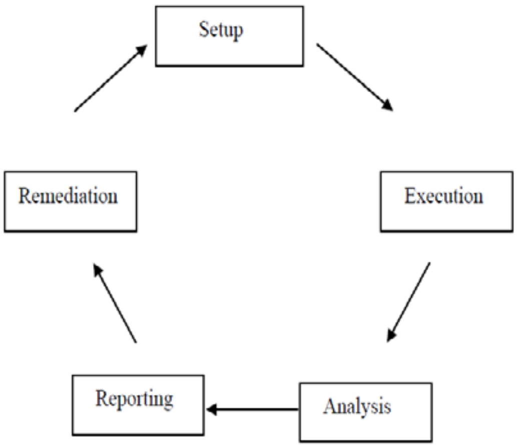


Fig: 1

A. Process of Vulnerability Assessment

Setup: Securing the permission to perform security test followed by configuring required updated tools.

Execution: Initiating scanning and testing in order to discover different vulnerabilities.

Analysis: Analyzing the scanned and tested result, classifying, defining and designating importance to the network or system resource. Identifying potential threats, developing strategy to deal with problems and applying practical solutions to reduce damages if a potential attack takesplace.

Reporting: Documenting the results and handing over the consolidated report of the analysis to the concerned authorities.

Remediation: Fixing the vulnerabilities.

B. Types of Vulnerabilities scanners

● Host Based: identifies lives host and vulnerabilities present on the target host. Host-based tools initiate intermediary software to trace the event and report it to security analyst.

● Network Based: identifies unknown services running on the ports, detect open port. This operation is carried out by network-based scanners.

● Database Based: identifies security exposure in database systems. It prevents SQL Injection by using tools and techniques.[4]

C. Pros of Vulnerability Assessment.

● Opensource tools are widelyavailable

● Scanning is automated for thousands of securitychecks

● Easy to use for regular periodicchecks

● Useful and easy layer-one remediation test[4]

D. Cons of Vulnerability Assessment.

● False positive rate is high

● Generates enormous amounts ofdata

● Easily detected byIDS

● Fails to notice latest vulnerabilities and logical attack vectors[4]

III.PENETRATIONTESTING

Process of Penetration Testing

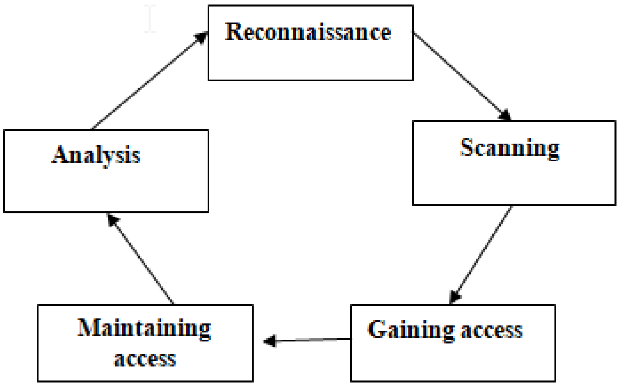


Fig: 2

1. Reconnaissance: is broadly defined as the scope and the final goal(s) of test and gathering information to completely understand thetarget.
2. Scanning: To understand the response of target to intrusion attempts, we use twomethods:

● Static analysis: an applications code is inspected to estimate its behavior while it is in progress. The complete code can be scanned in a single pass by thesetools.

● Dynamic analysis: inspection of a given code in a running state. This exhibits a real-time view into performance of an application, this is a more practical way ofscanning.

3. Gaining access: Using previous stage results, we try exploiting the uncovered vulnerabilities. Methods usedare:

● External testing: This method targets assists of the target that are visible in the internet i.e. web applications, websites and Domain Name Servers. Extracting valuable data is thegoal.

● Internal testing: This method is to simulate a condition where an insider attacks as an insider has access to the system behind the firewall. Tests can be simple phishing attack or simulate a rogueinsider.

4. Maintaining access: This step is of major importance to understand if the system is prone to advance never ending threats i.e. to achieve strong presence in the exploited system to gain in-deptaccess.
5. Analysis: Data generated is then used to configure system to secure it. Report is generated containing data of specific exploited vulnerabilities, unauthorized access to sensitive data and the amount of time testers were in the system undetected.[4]

A. Pros of PenetrationTesting

● Tests are offensive imitating realattackers

● Chain together vulnerabilities to demonstrate risks indept

● Removes all false positive (alllayers)

● Realistic evidence provided for security issue[4]

B. Cons of Penetrationtesting

● Requires time and great expertise.

● Dangerous if handled by immature pen testers causing data loss andcorruption

● Expensive and labourintensive

● Source code is exposed to thirdparty[4]

IV.PROCESS OF VULNERABILITY ASSESSMENT AND PENETRATION TESTING(VAPT)

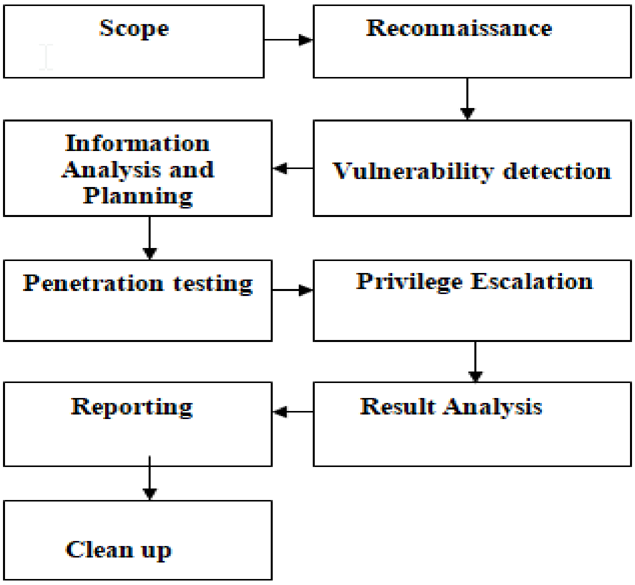
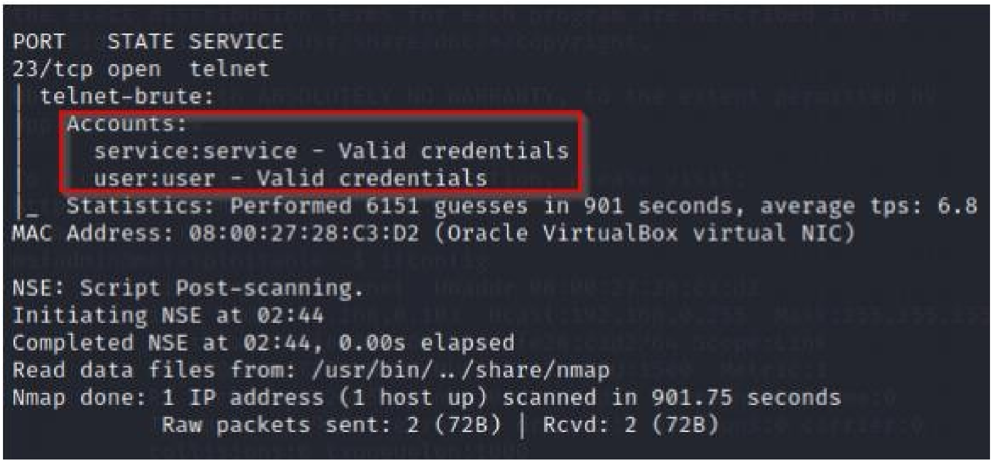


Fig: 3

1. Scope: Testers decide the scope i.e. whether the it's a Black box, Grey box or Whitebox.
2. Reconnaissance: Gathering info about network, IP andsystem.

3. Vulnerability detection: techniques (Mentioned in Section II) are used to findvulnerabilities.
4. Information Analysis and Planning: Results from VA are analyzed to plan forPT.
5. Penetration testing: Devised plan in then executed to exploit i.e. penetrate thesystem.
6. Privilege Escalation: After penetration, privilege is increased to further the reach, ease andpersistence.
7. Result Analysis: Detailed analysis of all the results of above steps aremade.
8. Reporting: Document is generated with recommendation and solutions to resolve the vulnerabilities.
9. Clean-up: in this step the system is restored to its previous state before theVAPT.[4]

Example of Penetration testing:
We performed brute forcing on the target system and found the valid credential through which an attacker can gain access and perform malicious act on the remote system.

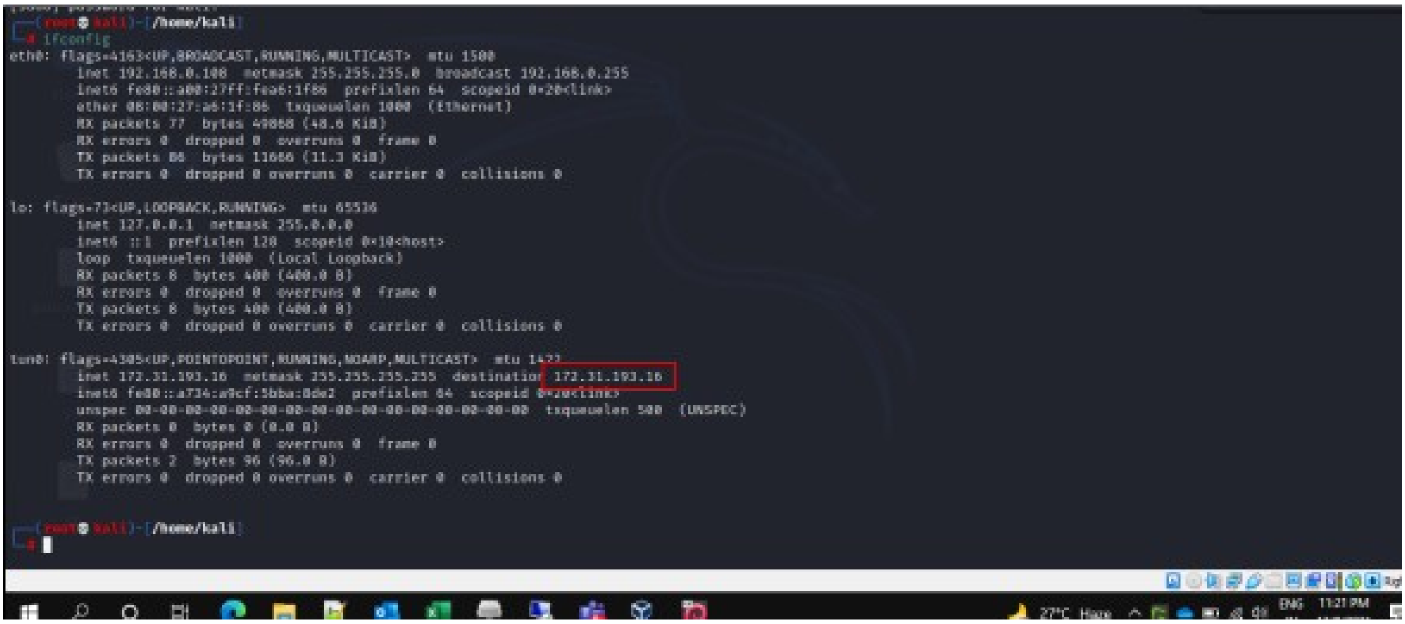


```
PORT   STATE SERVICE
23/tcp open  telnet
| telnet-brute:
|   Accounts:
|     service:service - Valid credentials
|     user:user - Valid credentials
|_  Statistics: Performed 6151 guesses in 901 seconds, average tps: 6.8
MAC Address: 08:00:27:28:C3:D2 (Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
Initiating NSE at 02:44
Completed NSE at 02:44, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 901.75 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

Example of Segmentation Testing:
The Cardholder Data Environment should be segmented from the other Non-CDE segments of the Internal network. Proper segmentation ensures that even if the system present in other internal networks is compromised, the Card Data security is intact. It was observed that the CDE segments are accessible from the Non-CDE network segment which is considered a security concern.

Step 1: Run a Host Discovery for the hosts in the CDE from a host in a Non-CDE segment.



```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.108  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fea6:1f86  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:1f:86  txqueuelen 1000  (Ethernet)
        RX packets 77  bytes 49868 (48.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86  bytes 11686 (11.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1422
        inet 172.31.193.16  netmask 255.255.255.255  destination 172.31.193.16
        inet6 fe80::a734:a9cf:5bba:8de2  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 96 (96.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kali)-[/home/kali]
└─#
```

Step 2: The following hosts/IP's are found to be live and have open ports/services when accessed from out-of-scope segments.

Conclusion :The CDE must be completely isolated from all non-CDE segments in accordance with the PCI DSS 3.2 Guidelines.

FLOWCHART OF PENETRATION AND SEGMENTATION TESTING

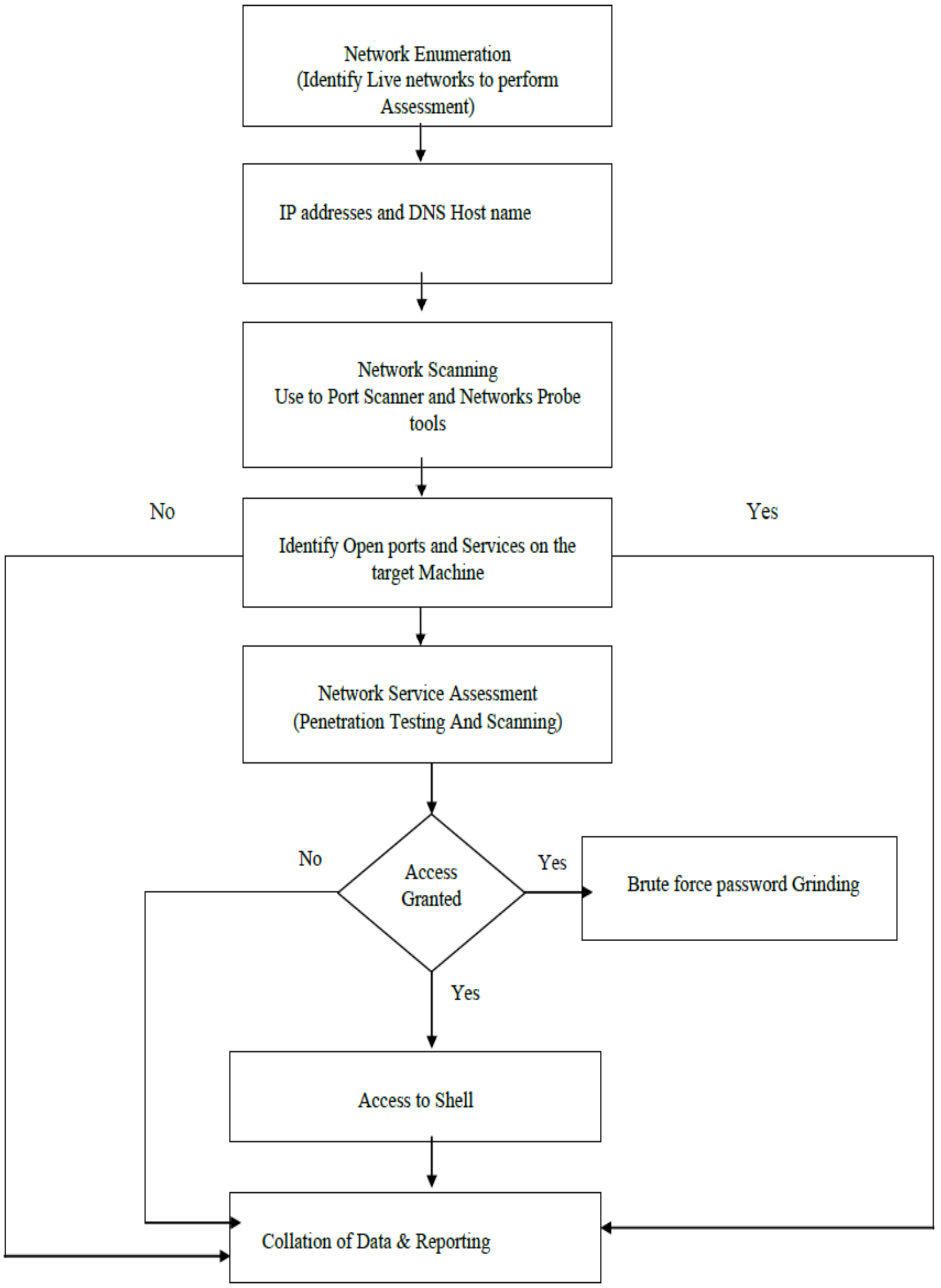

Network Enumeration
(Identify Live networks to perform Assessment)
IP addresses and DNS Host name
Network Scanning
Use to Port Scanner and Networks Probe tools
No
Yes
Identify Open ports and Services on the target Machine
Network Service Assessment
(Penetration Testing And Scanning)
No
Access Granted
Yes
Brute force password Grinding
Yes
Access to Shell
Collation of Data & Reporting

Fig: 4

TECHNOLOGY STACK

The tools implemented in order to perform, testing and scanning are as follows :

- KaliLinux
- Wireshark
- Nikto
- Nmap
- Nuclei
- Netcat
- Gobuster
- SSLscan
- TestSSL
- Open SSL
- Nessus

CONCLUSION

- ➢ MDR Vulnerability Management is a service that provides real time security, monitoring and managements across a organization.

- Without this vulnerability management process the organization is under risk and threat.
- By having a well-defined process in place, an organization can obtain a continuous view of the risk associated with the presence of security vulnerabilities in its IT systems.
- This allows management to take well-advised decisions with regards to remediating actions that could be implemented to reduce the risk
- Sufficient attention should be paid to the configuration and fine tuning of the vulnerability scanner technology.

FUTURE SCOPE

As threat landscapes evolve, vulnerability management programs are expected to integrate new automated solutions that will help organizations remain one step ahead of the hackers,managing security risks without having to sacrifice agility orspeed

REFERENCES

[1] June 2017 International Journal of Innovative Research in Computer and Communication Engineering5(6):11241-11244

[2] 2019 4th International Conference on Information Systems and Computer Networks(ISCON)
GLA University, Mathura, UP, India. Nov 21-22, 2019

[3] Proceedings of the Third International Conference on Trends in Electronics andInformatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN:978-1-5386-9439-8

[4] 978-1-7281-9393-9/20/$31.00 ©2020 IEEE 398 DOI: 10.1109/CICN.2020.72 [5] ISBN: 978-1-4799-8451-0/15/$31 2015 IEEE

[6] 978-1-5090-6231-7/17 $31.00 © 2017 IEEE DOI10.1109/WAINA.2017.39

[7] Shinde, P. S., &Ardhapurkar, S. B. (2016, February). “Cyber security analysis usingvulnerability assessment and penetration testing. In Futuristic Trends in Research and Innovation forSocial
Welfare” (Startup Conclave), World Conference on (pp. 1-5). IEEE.

[8] Goel, J. N., &Mehtre, B. M. (2015). “Vulnerability Assessment & Penetration Testing as aCyber Defense Technology”, Procedia Computer Science, 57,710-715.

[9] Shah, S. (2013). “Vulnerability assessment and penetration testing (VAPT) techniques forcyber defence”. In Nat. Conf. Adv. Comput., Netw.Secur.(IET-NCACNS)

[10] Shah, S., &Mehtre, B. M. (2014, May). “An automated approach to vulnerability assessment and penetration testing using net-nirikshak 1.0”. In 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies (pp. 707-712).IEEE.

[11] Shah, S., &Mehtre, B. M. (2015). “An overview of vulnerability assessment andpenetration testing techniques”. Journal of Computer Virology and Hacking Techniques, 11(1),27-49.