Journal of Engineering and Applied Sciences 12 (Special Issue 9): 8723-8729, 2017
ISSN: 1816-949X

Penetration Testing: Vulnerability Analysis in a Virtual Environment

C.V. Arjun
Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal, Karnataka, India

Abstract: Nowadays, it is common to hear about security breaches in all parts of the world, whose intensity may be big or small or it may take place in public or in private sector. Because of world wide web, all are connected. And that means systems are exposed to vulnerability. In order to reduce the risk of security breach, the application has to be rigorously tested before it can be accessed by malicious users through the internet. And here arises the role of the penetration tester to check for any vulnerabilities in the application or system. All the security testing's are done in the virtual lab which is built by using virtual box which avoids the need to buy racks of computers and other networking equipment's to perform testing. Virtual lab makes sure no testing activities reach world wide web which prevents testing activities accidentally becoming illegal activities. This is an important consideration in ethical penetration testing or pen test. The goal of penetration testing is to better protect the resources which are at the disposal. This study focuses on the vulnerability analysis phase of the penetration testing. The experiment is carried out using different tools like Nikto, Vega, Nmap and DNSenum in Kali Linux platform wherein vulnerabilities are identified and the results are displayed.

Key words: Penetration testing, vulnerability analysis, Kali Linux, virtual lab, security, phase

INTRODUCTION

Security has vital role in penetration testing to play. Penetration testing can be done in the domains like system, website and web applications, wireless networks, data storage, etc. It takes a lot of effort and persistence to secure system or web applications from attackers gaining illegal access into it (Reddy and Yalla, 2016). Attackers can be angry or dissatisfied employees from the organization or criminal groups whose aim is to perform illegal attacks (Arjun and Pooja, 2017). Penetration testing involves testing the system thoroughly, so that, to find any vulnerabilities, before it is published on the internet. Penetration testing is an important aspect of security plan as it provides a comprehensive mechanism to identify potential threats. The most important task of penetration testing is to identify vulnerabilities in the system to prevent password cracking to identify and repair vulnerabilities in the wireless networks to find weaknesses in websites and web applications to detect and neutralize malwares like viruses, worms, Trojans, etc. Penetration testing can be broadly categorized into five important activities (Cybrary, 2015).

Reconnaissance: It is also called as information gathering phase where data or information about the target is collected. The gathered information can be used to identify technology/software used, IP address of the host, name servers, subdomains along with IP address information, software configuration, load balancers, etc. Through reconnaissance, one can plan a better attack. Tools commonly used for information gathering are dnsenum, urlcrazy, WAF00F, Dmitry, maltego, etc. (Arjun and Pooja, 2017).

Vulnerability analysis: This phase is also known as scanning. Scanning uses tools to gain further intelligence on the target to do service profiling and vulnerability testing. The tools are categorized as Cisco tools, fuzzing tools and stress testing header in Kali Linux.

Gaining access: This means taking complete ownership of one or more network devices, systems, websites, applications. By which data or information about the target can be accessed, thereby, the third party device can be used to launch other attacks like reflection attacks, distributed denial of service attacks, etc.

Maintaining access: After successively compromising the target, it is very essential to maintain access to the host for further examination or penetration of the target network. Aim is to gather more information. Once access to one system is achieved, one can ultimately gain access

to all the systems that share the same subnet. Gaining information about the user activities is achieved by monitoring the keystrokes and impersonating users with captured tokens, etc.

Covering tracks: The final phase is covering tracks. Here, the attacker will take the required steps to eliminate all traces of detection. Any changes that were made, authorizations that were escalated, etc., all will be returned to a state of non-recognition by the host network's administrators (Cybrary, 2015).

MATERIALS AND METHODS

The computer system can be broadly categorized into four parts: hardware, operating system, applications and users. Hardware comprises of Central Processing Unit (CPU), memory and I/O devices. Application programs include word processes, spread sheets, compilers, browsers, etc. Application programs makes use of the service provided by the operating system and through them the hardware resources. Figure 1 depicts the abstract view of the computer system (Silberschatz *et al*., 2008).

For a hardware-level virtualized system, there will be one more layer called hypervisor on top of hardware resources. Hypervisor is responsible for providing virtual environment in the system. And upon which there will be operating system and its applications. Using hypervisor, one can have multiple operating systems and their applications hosted in the system. These are nothing but virtual machines or VMs. Hypervisor maps individual virtual machines with the hardware allocation. It is helpful in managing contention in the system (Arjun and Pooja, 2017).

An example of hardware level virtualization is Microsoft Hyper-V hypervisor which was first introduced with Windows Server 2008. Hyper-V works by the isolation of virtual machines. This is achieved by a partition. A partition is a logical unit of isolation. It is this partition where the guest operating system is hosted and executed. Normally, this kind of hypervisor setup will have one parent partition. The parent partition creates several child partitions which host the guest Oss. Figure 2 shows the Hyper-V architecture.

Similar to hardware virtualization, there is software virtualization. This can be achieved by vmware, virtual box and parallel. Parallel is a popular virtualization software tool for mac systems. It is ofetn used to achieve windows environment in the mac. Virtal box with tetsing set up is shown in Fig. 3.

Kali Linux: Kali is the latest evolution of what started out as a security testing suite called BackTrack. It runs on a wide range of hardware and is used extensively by professional security testers. Kali is a Linux distribution which includes over 300 security testing tools and some tools have their own graphical user interface for ease of use. The main Kali screen has two drop-down menu items on the top bar, applications and places and a set of quick access icons on the left. Application houses all the tools of Kali and they are arranged categorically by the header. All the tools can be broadly classified to fourteen main categories. These categories will have sub categories and tools under them. Kali supports multiple desktop screens, these are called Workspaces. Kali's internet browser is a variant to Firefox called Ice weasel. Terminal is a Bash shell. This provides a standard Linux command line. The

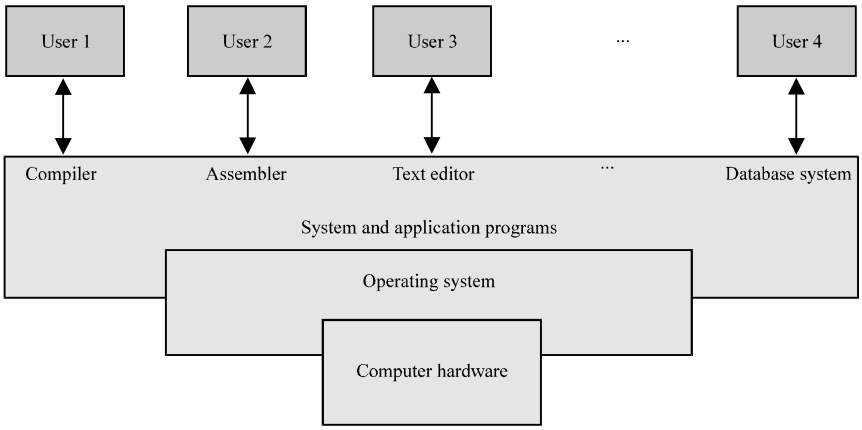

Fig. 1: Abstract view of the computer system

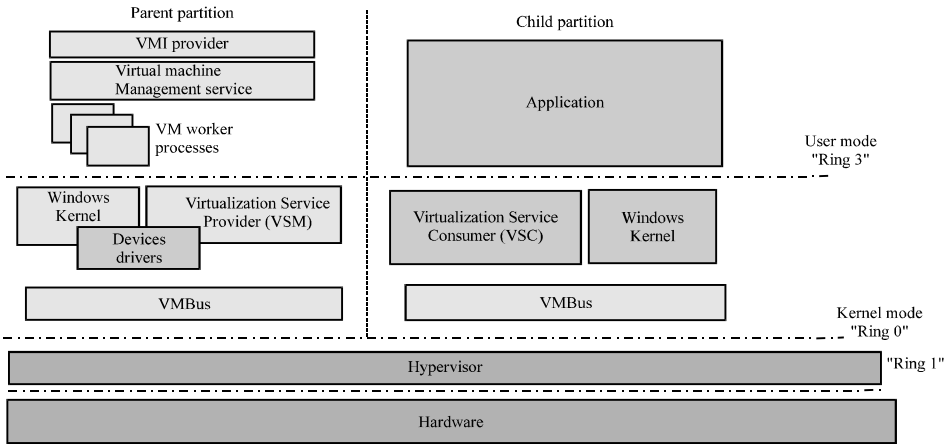

Fig. 2: Hyper-V architecture

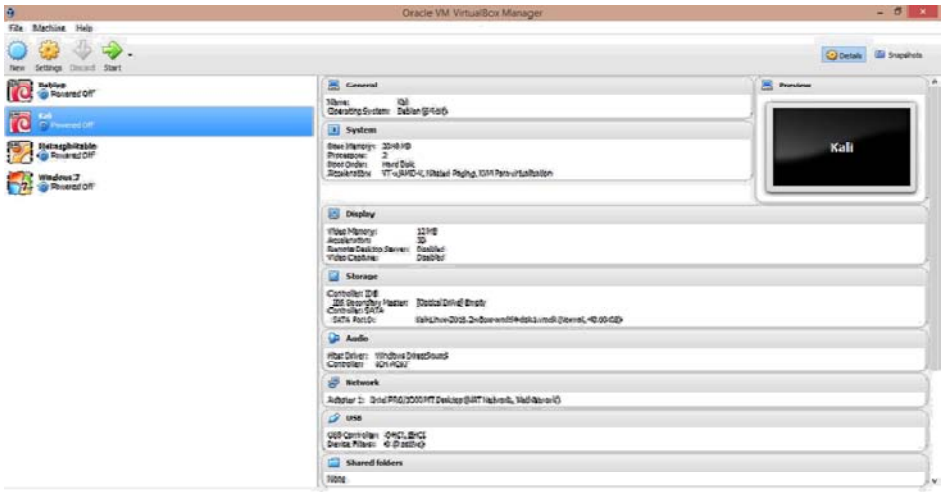

Fig. 3: Virtual environment setup

Leafpad text editor provides a similar set of functionality to Notepad or Debian's Nano. Many of the tools are shown with the Kali logo. These are command line tools which has to be opened in the terminal window and run by bash shell (Arjun and Pooja, 2017).

RESULTS AND DISCUSSION

Based on the information gathered, it becomes very easy to identify the weaknesses in the system. This helps the malicious users to launch an attack to the target, making use of the identified issues. It is duty of the penetration tester to perform vulnerability analysis phase thoroughly and fix the issues if any, before an adversary finds them. Some tools that can be used to gather and identify information are.

Nikto: Nikto is a popular open source tool. It is used as web scanners which can be used to test a website/web server to detect potentially dangerous files/programs, outdated servers and problems relating to specific servers. It gives information about installed servers and software (CIRT.net, 2017).

Vega: Vega is free and popular tool available to testify the web applications. It's an open source web scanner to test the security of a website. Vega by default runs thirteen of the injection modules (Fig. 4 and 5). Those include blind SQL text injection, XML injection checks, HTTP trace probes, URL injection checks, etc. and 23 of the response processing modules. Vega listens at port 8888. Metasploitable is used as a target for the scan test (Vega, 2014).

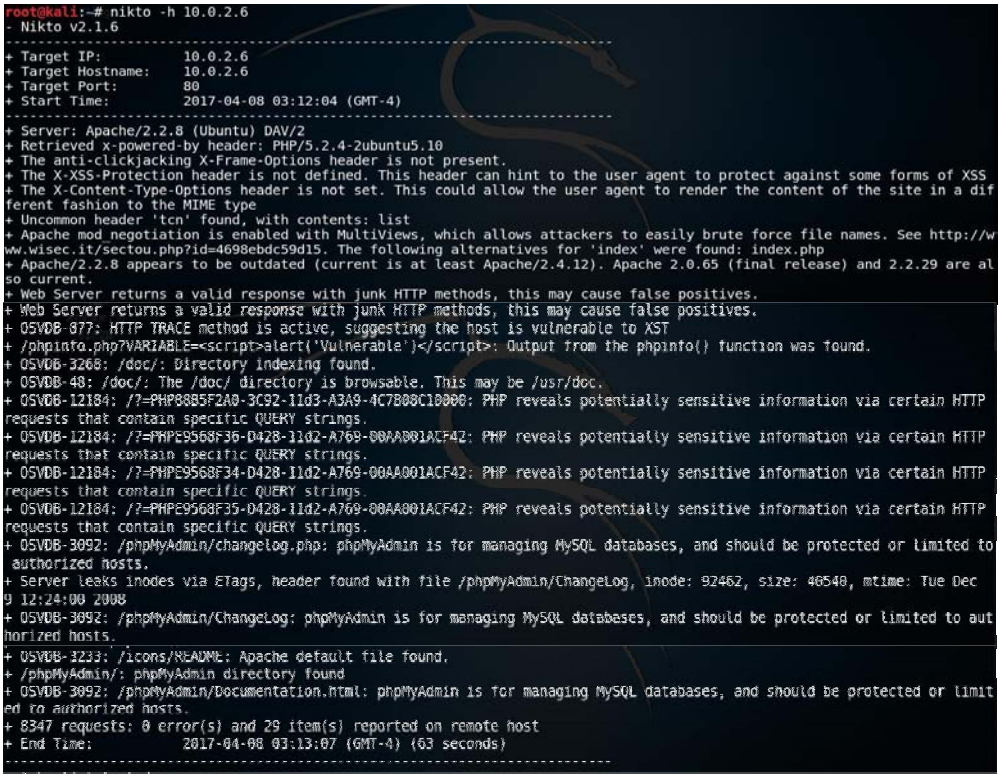

Fig. 4: Vulnerability analysis by Nikto

Nmap: Nmap is network mapper which is used mainly in network discovery and security auditing. Additionally this can also be used for tasks such as discovering the host and identifying the available services in the host, managing service upgrade schedules, service uptime, monitoring host, network inventory, etc. Nmap is a standard network administration open source tool which runs on many platforms. Full list of options can be obtained by typing Nmap-h. Its usage is Nmap [scan type(s)] [Options] {target specification}. Basic searching can be done either by making use of hostnames or its IP address which can be as: Nmap 10.0.2.6 or Nmap hostname. This gives ports detected, states of the port and its service associated. States can be open-means it is active and open for connections, closed means it will give respond to probes but most likely no services running, filtered usually means protected by firewall and unfiltered means Nmap can't determine whether it is open or closed (GitHub, Inc., 2015). Multiple targets can be scanned by specifying their hostname/IP address separated by space as namp 10.0.2.5 10.0.2.6 10.0.2.15. Here, 10.0.2.5 is the inet address of Windows 7 Virtual Machine, 10.0.2.6 is the inet address of Metasploitable and 10.0.2.15 is the inet address of Kali Linux. The entire range of IP addresses for all the targets on the network can be scanned as Nmap 10.0.2.1-24. Even the regular expression* can be used which symbolizes all for identifying the targets in the network. This can be done as namp 10.0.2* (Fig. 6 and 7).

To trace the path to the host: Nmap-traceroute hostname and to detmine the operating system O option can be used which will be Nmap-O 10.0.2.6. Service versions can be known using sV option as Nmap-sV 10.0.2.6. Aggressive scan can be performed with-A option which enables OS detection, version detection, script scanning, trace route, etc. Scan techniques can be-sS: TCP SYN, sT: TCP Connect, sA: TCP ACK, sW: TCP Window and-sM: TCP Maimon. Figure 8 makes use of -A and -sS option for performing advanced scanning.

To check the live hosts which are present in the current network or a domain-sn option is used. The option-sn comes under the category of host discovery. Sn is ping scan which can be used to disable the port scan (Fig. 8).

Dnsenum: Dnsenum (Arjun and Pooja, 2017) can also be used for identifying all the targets that are registered under a particular domain (Fig. 9). To check for the systems that are in the domain 132.181. Usage: Dnsenum [Options] "domain".

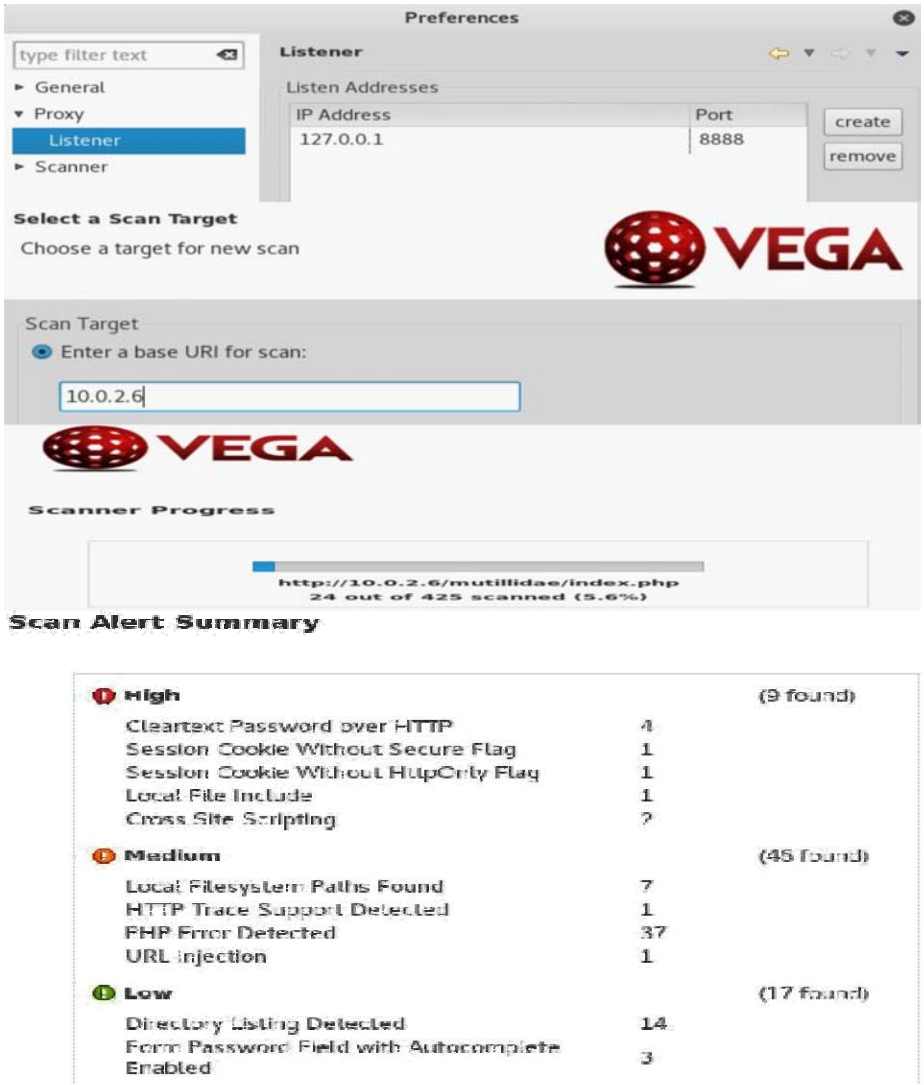

Fig. 5: Web crawling by Vega

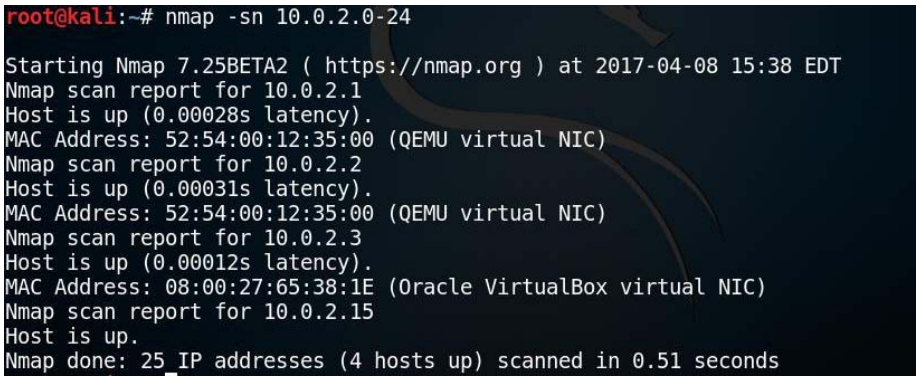

Fig. 6: Host identification by Nmap

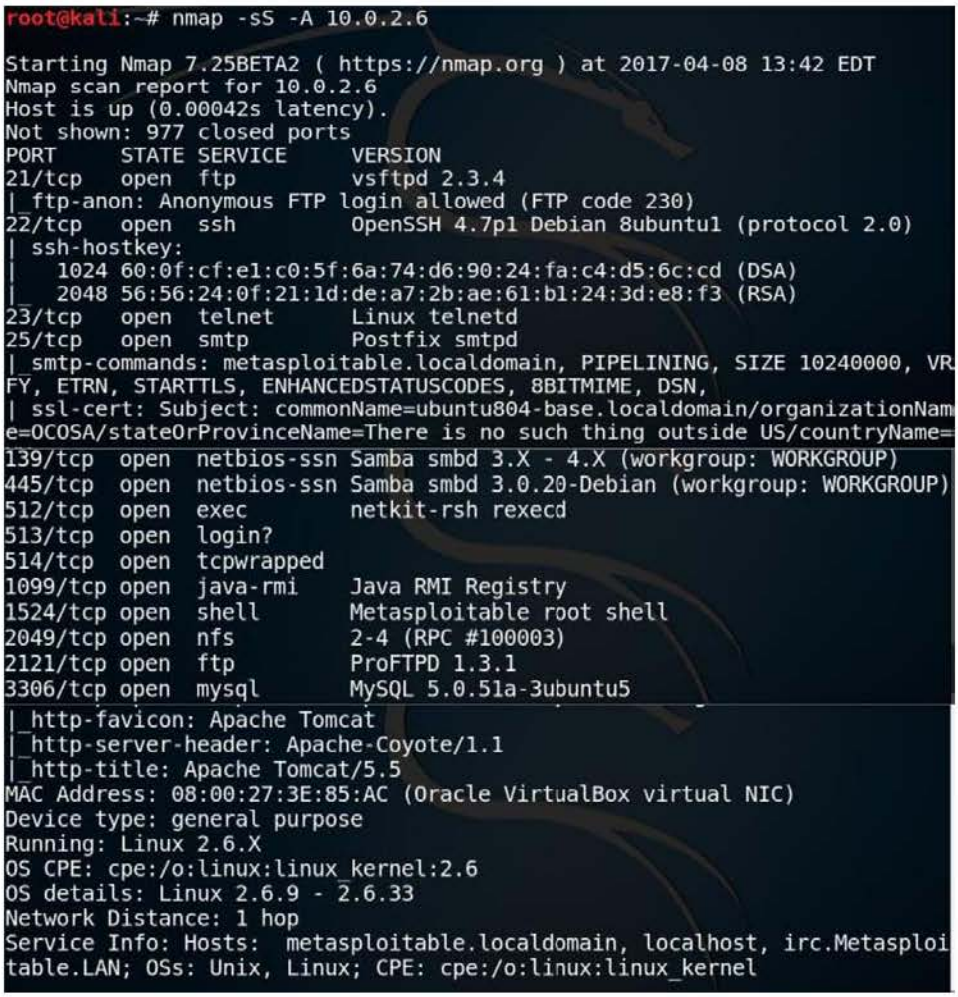

Fig. 7: Advanced TCP SYN scan using Nmap

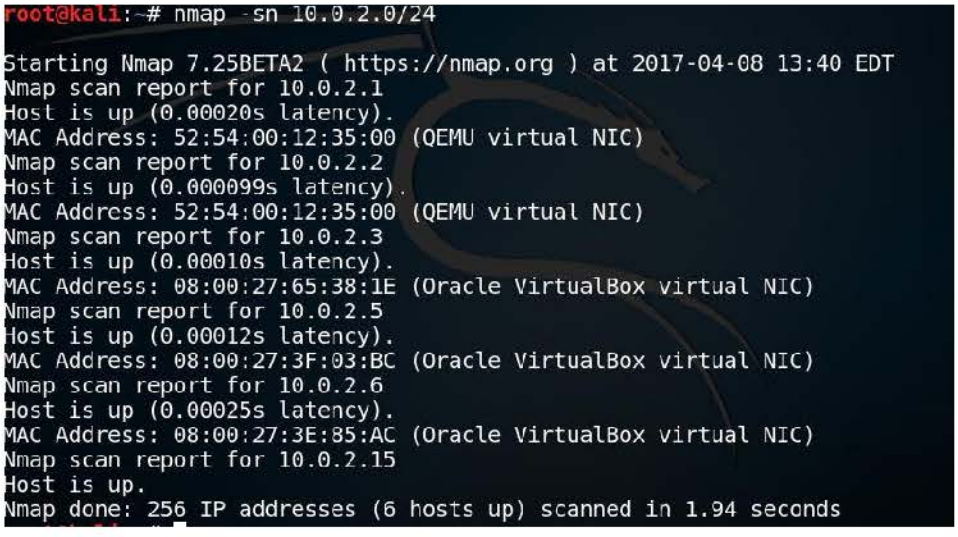

Fig. 8: Host discovery using Nmap

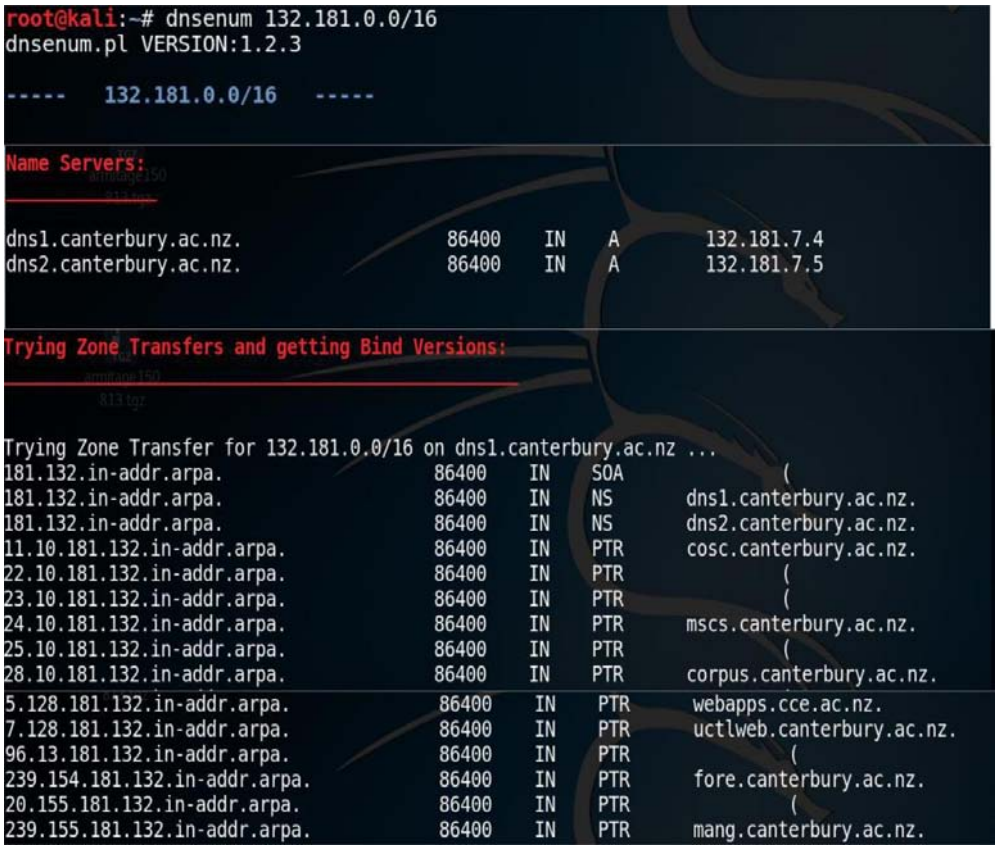

Fig. 9: Targets identification in a domain using Dnsenum

CONCLUSION

The aim of the penetration testing is to identify and fix the issues which are relating to the system, network or a web application before an adversary does. This paper discusses open source tools like Nikto, Vega, Nmap and DNSenum to identify any issues. These tools are used to identify potentially dangerous files/programs, outdated server, operating system used, problems relating to specific servers, the IP of the host, multiple targets in the network/domain, etc. Nikto and Vega can be used as a web scanner. All the tests are carried out in a virtual setup and the results are displayed.

REFERENCES

Arjun, C.V. and S. Pooja, 2017. Penetration testing: An art of information gathering in an ethical way. Proceedings of the 1st International Conference on Contemporary Issues in Science, Engineering and Management (ICCI-SEM-2017), February 18-19, 2017, Gandhi Institute for Technology, Bhubaneswar, India, pp: 119-125.

CIRT.net, 2017. Suspicion breeds confidence. CIRT.net, Chantilly, Virginia.

Cybrary, 2015. Summarizing the five phases of penetration testing. Cybrary, Greenbelt, Maryland. https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/.

GitHub, Inc., 2015. Buckyroberts/Source-code-from-tutorials. GitHub, Inc., San Francisco, California, USA. https://github.com/buckyroberts/Source-Code-from-Tutorials/blob/master/Nmap/cheatSheet.sh.

Reddy, M.R. and P. Yalla, 2016. Mathematical analysis of penetration testing and vulnerability countermeasures. Proceedings of the 2016 IEEE International Conference on Engineering and Technology (ICETECH), March 17-18, 2016, IEEE, Coimbatore, India, ISBN: 978-1-4673-9915-9, pp: 26-30.

Silberschatz, A., G.B. Peter and G. Gagne, 2008. Operating System Concepts. 8th Edn., John Wiley & Sons, Hoboken, New Jersey, USA., ISBN-13: 978-0470128725, Pages: 992.

Vega, 2014. Vega package description. Vega, Canada. https://tools.kali.org/web-applications/vega.