Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

# Penetration Testing using Linux Tools: Attacks and Defense Strategies

V. Santhi
M. Tech.
Dept. of Computer Science & Systems Engineering
Andhra University
Visakhapatnam, India

Dr K. Raja Kumar
Assistant Professor
Dept. of Computer Science & Systems Engineering
Andhra University
Visakhapatnam, India

B. L. V. Vinay Kumar
Research Scholar
Dept. of Computer Science & Systems Engineering
Andhra University
Visakhapatnam, India

***Abstract*— Penetration Testing helps you to secure a computer system, network or web applications that allows you to gain high security issues which also helps to find vulnerabilities that an attacker could exploit. This paper investigates about different penetration testing tools in kali Linux, how to deploy it and how to make use of it to perform different types of attacks which includes methodologies and also defense strategies. Technically, we performed different penetration tests with virtualized systems, tools and using private networks. The attacks that are performed were: Man in the middle attack and traffic sniffing using both terminal and by Ettercap and driftnet, Bluetooth hacking, spying a webcam. The results and implementation is discussed and summarized. This paper also gives detail methodology of how to perform these attacks.**

***Index Terms*— Ettercap, Driftnet, Nmap, kali Linux, Metasploit.**

## I. INTRODUCTION

In today's business environment, penetration testing is a critical step for the development of any IT application under secure product or system. To assess system security the most common approach is penetration testing, where it is considered as the simulation of actions performed by attackers in order to intrude an IT system. Effectiveness of penetration testing is rated depending on the skill and experience of testers. Penetration testers who follow and exercise with different tools are more effective in their use of resources. In this paper we describe different penetration tools, their usage and how they are going to penetrate the resources.

Penetration testing process is supported by automated tools that are specifically used in every distinct level of testing. Security problems vary with applications. This paper explores security weakness which causes either exposing secure data or Intrusion. Penetration testing works in 3 stages: Reconnaissance, where it searches for available information including the networking tests such as ping and finding ip address and all the penetration tools comes under this category [3]. Enumeration, it creates a picture about the configuration of the network and identifies services upon various devices like firewall, routers and web server [1]. Exploitation uses different techniques, tools to compromise the system through identified vulnerabilities. In this paper we analyzed tools like metasploit,nmap,ettercap,driftnet and worked with different commands like btscanner,echo,leafpad,ifconfig etc which are described below and how they are going to attack by injecting into the system.

The objective of this paper is to investigate different tools according to the need of research, work with it and exploiting the results successfully. User interface and report formats generated are noted and identified as shown in the results block. This paper demonstrates the basic penetration testing that is happening in real time environment over target machines by downloading intruder code from malicious websites. This paper also explains defense strategies.

## II. LITERATURE SURVEY

As we are under online. The major issue is security of transaction. To get rid of cyber crimes we need to ensure security to gateways, firewalls and systems to protect unauthorized access from disrupt services[10]. The main focus is not hacking or breaking the IT system but to provide measures to found vulnerabilities and meaningful advices where as vulnerability assessment aims to reveal potential threats in the network .Firstly, we should know about importance of the penetration tools and how the attacks are to be done either with the help of VMWare or live kali Linux [1]. It also includes attacks remote PC via IP and open ports using advanced port scanner and what are the causes of system weakness and success rate are explained in detail using charts[11].It is important to know that cyber attacks and malware are raising in this century, in many companies once systems are connected to the internet the paper focus on how they are scanned and attacked constantly using free hacking tools and inexpensive devices like key loggers and Frequency scanners[17].Penetration testing activities are undertaken to identify and exploit security weakness[6]. At first truly,you need to know what is the difference between the penetration tester and the hacker this gives detailed explanation about the roles which hacker doesn't need any permission where as the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

tester needs permission from the clients machine[7]. To perform attacks you need to know popular tools, vulnerability scanners and what is the use of penetration testing? type of tools and how they are used? What are common tools? gives the main source to implement this paper[2].TO perform all attacks the OS used is kali linux that guides how to install kali Linux ,by using guidelines the kali Linux is installed successfully with the iso image using memory card[5]. We also studied how to hack the data in the system with metasploit and by other tools that are listed and explained ,after exploiting msfconsole changed to msf which defines that it enters into exploiting stage i.e, it is ready to hack by the injected code that is running backside[11]. Live target systems or networks are probed in discovery phase, using both active probes and passive network sniffing. It is also mandatory to study how to to understand the internal network, operating system running on target systems and the services running on target system and how to analyze the threats and vulnerabilities are summarized[9]. It also understands the state of security in a system or network to find out which vulnerability is real and which one is false. We also studied about what is the difference between the penetration testing and vulnerability assessment ,how the penetration tester work in the real world ,how to compete with the real attacker[8].

## III. TOOLS AND TECHNIQUES

The main goal of this section is to demonstrate about penetration testing methodology and the brief introduction of tools used in this paper for different attacks. The methodology used for penetration testing is introduced in this section. The methodology of penetration testing is shown in Fig.3.1

It consists of four phases:

- planning
- discovery
- exploitation and
- reporting

The planning phase completely related to management approvals,agreements and documents under legal departments and their signatures.It deals with working with a customer to clearly define and document assessment objectives,scope and rules.The actual penetration testing starts from this discovery phase.It is also called as information gathering phase.Scanning and enumerating procedures are involved to gain information as much as possible about the target network including their systems and services. Such as collecting and examining key information about an application and its infrastructure.


Fig3.1 Penetration testing methodology

The third phase is exploitation phase.Basing on the discovered vulnerabilities,this phase uses different automated tools,techniques and fine-tuned manual steps to be executed in a specific way to gain the weakness of the system.Thus continuous interaction is performed between the discovery phase and exploit phase throughout the actual phase.The last phase is reporting phase.this phase gives details about all the findings and their impacts to the organization by considering both technical and management aspects.A fully detailed and well documentation is submitted to the organization inorder to inform about security risks and provides technical det ails with high level recommendations.

This section gives an overview of different penetration testing tools ,their usage,how they exploit the vulnerabilities. The tools that are introduced in this paper are listed below and Every tool is explained in detail for basic knowledge.

- Ettercap
- Driftnet
- Nmap
- Wireshark
- Metasploit

*Ettercap* supports active and passive analysis of many protocols for network and host analysis.[14] It operates in 4 modes: IP based: Packets are filtered basing on IP address of source and destination. MAC-based: Based on MAC address packets are filtered and are used for sniffing connections through gateway.ARP based: It operates in full duplex mode. Sniff the data on a switched LAN between two hosts using ARP poisoning. Public ARP based: It operates in half duplex mode. It sniffs the data on a switched LAN from a victim host to all other hosts using ARP poisoning.

It also offers some features such as HTTPS support—it supports HTTP SSL secured data even when the connection is made through proxy, character injection into an established connection—characters can be injected into a server or to client.

*Driftnet* is a fishing technique where nets hang vertically in water column without touching the bottom. They fold like loose netting, like window drapery, when a fish enters into net is snag on a fish tail and fins and wrap the fish up in nets as it struggles to escape. The same concept is applied in networks to capture the data when data transmits between the user and the attacker. Driftnet displays the images and URLs that are seen by the victim. Using Arpspoof the man in the middle attack and traffic sniffing is to be done.

*Metasploit* provides security that provides information about security vulnerabilities and helps in penetration testing and IDS signature development[4]. It is an open source Metasploit framework, a tool for both developing and executing exploit code over remote target machine. The steps included in framework for exploiting a system:

1. Choose and configure an exploit
2. Check whether the target system is susceptible to exploit
3. Choose and configure payload
4. Choose the encoding technique such that intrusion prevention system ignores the encoded payload.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

5. Execute the exploit.

The advantage of this framework is it allows the combination of any exploit with any payload. It assists the tasks of attackers, payload writers and exploits writers. It runs on both UNIX and windows. It also can be extended to use add-ons in multiple languages. To choose exploit and payload information such as operating system and installed network services about the target machine are needed. This can be done by using port scanning and Nmap.Vulnerability scanners like Nessus can detect vulnerabilities in target system. It imports vulnerabilities scan data and compare the identified vulnerabilities for accurate exploitation with existing exploit modules.

There are different Metasploit interfaces. The most popular interfaces are Metasploit Framework edition, Metasploit community edition, Metasploit Express, Metasploit pro, Armitage and Cobalt Strike. In this paper we have worked with Metasploit Framework edition. Metasploit has numerous payloads. Some of them are Command shell that runs collection scripts or arbitrary commands over the host. Meterpreter, we have worked with Meterpreter in the paper. It controls the screen of a device such as browse, upload and download files. Dynamic payloads—unique payloads are generated by anti-virus defenses.

*Wireshark* is a free and open source packet analyzer used for troubleshooting, analysis software and communications protocol. Wireshark is similar to tcpdump with graphical front-end with some integrated sorting and filtering options. Using Wireshark the user can see all traffic visible on the interface, configured addresses and broadcast/multicast traffic. Port capturing extends capture to any point in the network. To capture packets on the types of networks Wireshark uses PCap

The features of Wireshark are Data can be captured from live network or from wire or read from file of already captured packets, Network data can be browsed through GUI or terminal, Wireless connections shall be filtered. The network is traced using Libcap format supported by LIP Cap, so the captured network traces are exchanged with other applications that use the same format including tcpdump.

## IV. IMPLEMENTATION

The above section gives detailed description about all the penetration testing tools and now its time to follow procedure to implement them. Initially all tools are disabled in kali Linux by using commands you need to enable them to work. To display networks that are connected install compact-wireless in kali Linux and unzip it such that it displays all the networks that are connected and surrounded by us. Change the path and install it by using terminal. By default all the features are disabled using commands make them enable and follow.

### *A. Traffic sniffing*

#### *1) Using Wireshark*

Wireshark is the most efficient tool used for traffic sniffing. It is a network protocol analyzer for UNIX and windows used for network troubleshooting and analysis. Network capturing is also done by using terminal based (non-GUI) version called TShark. In this paper we have used wireshark, GUI interface that can see all traffic visible on the interface. Data can be captured from a live network connection through the wire or from already captured packets through read a file option.

To capture the network traffic in kali Linux install Wireshark using command Wireshark –h in the terminal. Initialize the network that you want to capture i.e., my network is eth0[16].Start and capture the data in the network you selected .Open the browser and browse for example www.google.com .The wireshark shows information like the site visited by the user , what is its length,when it is seen ,what is the ip address and the protocol version etc. as shown in the Fig 7.6 .

#### *2) Using Ettercap and Driftnet*

The network security tool called Ettercap used mainly for man in the middle attacks. It is a free and open source tool used for computer network analysis and security auditing. It is a capable of capturing passwords, traffic sniffing, intercepting traffic and eavesdropping. It works by bringing the network interface into promiscuous mode and performing ARP poisoning to target machines[14]. Use echo 1>/proc/sys/net/ipv4/ip_forward. To enable the packets to be forwarded `1` is used.The command iptables –t nat –A PREROUTING –p tcp –destination-port 80 –J REDIRECT –to-port 8080 performs routing to the destination .Initially ettercap is in inactive state let it be in active state by modifying the notepad. Type leafpad /etc/ettercap/etter.conf .Change [privs] to 0 and delete the # in iptables and save the notepad. Type ettercap –G the ettercap window is displayed. Select the network interface and scan the hosts .It displays the host list, depending on the host list add the targets[9]. The target 1 I have used is gateway and the target2 will be other network. The get the gateway address use route –n and to find the target address use nmap which list the number of victims address. Click on ARP poisoning and select sniff remote connections. Click on start sniffing .Open the other terminal and type ssltrip –l 8080 which transparently hijacks HTTP traffic on the network and demonstrates HTTPS attacks. If you want to know the URL then type urlsnarf –i <network> it displays the urls that have been watched in the network.The output is shown in the Fig 7.7.

### *B. Man in the middle attack*

#### *1) Using terminal*

Open the terminal and type ifconfig. It displays the active state networks .Use command route-n it displays the inet address of the gateway. Basing on the ipaddress search for the victim address in the network using nmap. Type nmap –sP<ipnet address> it displays the list of address in the network and makes use of one of them to perform the attack. Use ping command to check whether the ipadress is in active state and connected to the network. Perform arpspoof –i <network> –t <address1><address 2> Open the other terminal to forward the packets echo1 > /proc/sys/net/ipv4/ip_forward Open other terminal and perform arpspoofing by using the same command but change the address such as arpspoof –i <network> -t <address2><address1>.Open other terminal and type urlsnarf –i <network>.It displays the urls that are seen by the two

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

networks. Type driftnet –i <network> to see the images in the network.The output screens are shown in Fig 7.5

*2) Using ettercap and driftnet*

Follow the same procedure used in traffic sniffing then open other terminal and use driftnet –i <network>.Open the browser and browse the network[14]. IT displays all the images you have seen in the driftnet window.The output screens are shown in Fig7.4

*C. Bluetooth*

Open terminal and type hciconfig. Hciconfig configures Bluetooth devices[15] .hciX is the Bluetooth name installed in the system. Hciconfig hci0 displays the device installed in the system. Hciconfig hci0 up command opens and initialize hci device. Hciconfig prints name and basic information about all Bluetooth devices installed in the system. The hcitool scan scans all the devices nearer to the system and displays the nearer devices. With the MAC address of the device using mac address type l2ping <mac address> it automatically pings to the device .use btscanner it displays all the Bluetooth visible devices .enter the command inquiry scan, abort, quit according to your wish. It gives detailed information about the phone connected to the system Bluetooth. Sometimes it is also possible to make phone calls using phone Bluetooth connected to the system.The output results are shown in Fig 7.1

## V. DEFENSE STRATEGIES

### *A. Defense strategy for Bluetooth*

To provide security policies and standards Bluetooth enabled devices consider user responsibilities and accountability. Set the Bluetooth enabled device to invisible or hidden mode. Default PIN codes like 0000 or 1234 has to be changed. Secure and monitor the Bluetooth gateway that allows Bluetooth devices to connect to a network.

### *B. Defense strategy for Man in the middle*

Tools like XARP and ARPon are advanced address resolution protocols to prevent main in the middle attack. Implement dynamic host configuration protocol (DHCP), which prevents ARP spoofing. One of the most effective ways to use Virtual private networks (VPNs) that creates secure and encrypted tunnels while accessing organizational networks through wireless networks.

*1)Defense strategy for Traffic sniffing*

Use encrypted network protocols like IPSEC to communicate between your computer and the destination computer.It encrypts all traffic using tunnel between your computer and the trusted network like VPN. Use only applications that encrypt the communication channel like HTTPS. Encrypt files by ZIP with AES enabled before sending them over network .Using VPN technologies like anti-Arpspoof, Arpwatch, arpON, Antidote; snort can protect all your communication.

## VI. RESULTS

This section demonstrates about the implementation and the outputs of the attacks that are done which are already explained in above sections.Fig6.1 shows how the information about the mobiles with mac address are displayed.The displayed MAC address is used by attackers to ping and grab

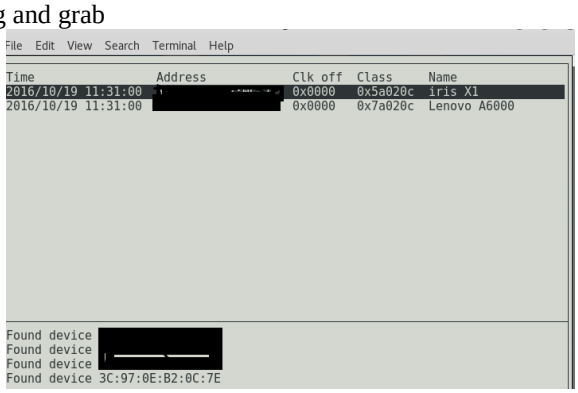


Fig 6.1 Scanned blueooth users with MAC address

the whole control over the mobile.By this it is also possible to make calls from the user mobile to the third party without the intervention of the mobile user.

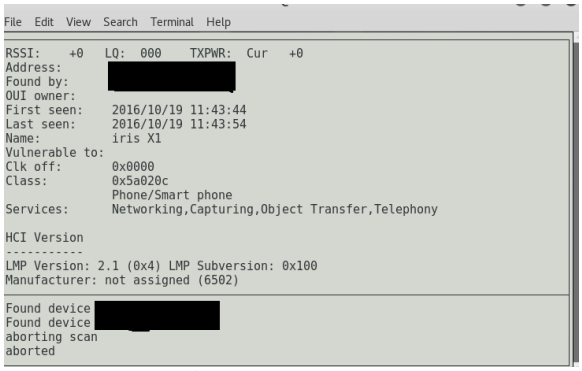


Fig 6.2 Mobile information about selected bluetooth user

Fig6.2 gives all details about the connected bluetooth user such as version,address and class details.Sometimes it is also possible to attack the phones data with such as phone storage and sd card.

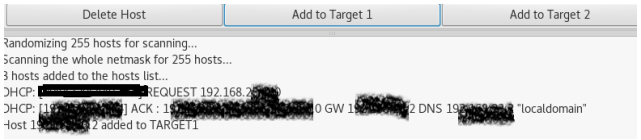


Fig 6.3 To set the targets using Ettercap

While using ettercap the hosts are scanned such that to sniff the data the target hosts are to be assigned.Add scanned hosts to target 1 and target 2 as you wish but its better to make one of the target with the gateway inet address such that the sniffed data is displayed as output which can be known .Using targets inet address man in the middle attack is also performed automatically after traffic sniffing.Fig6.4 shows how the data communication between the sender and the receiver is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

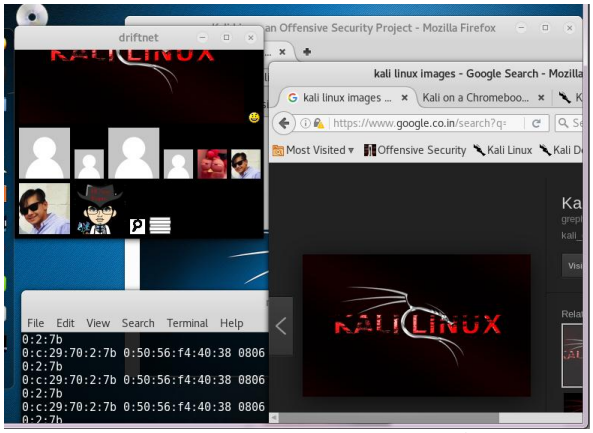


Fig 6.4 Man in the middle attack using drifnet

seen by the attacker is demonstrated.Arpspoofing is done to the both sender and receiver using commands with their ipaddress such that the driftnet displays the images that are seen by the sender/receiver.For better results,open the browser and search which automatically displays in the driftnet window. The screenshot itself shows that the data seen in the browser by the user is sniffed and seen by the attacker without knowing the actual user.

Inorder to see the URLS instead of images then urlsnarf is used such that it displays all the URLS that are requested as shown in the Fig6.5.

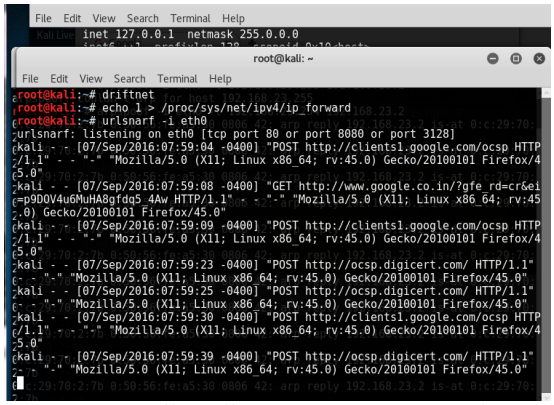


Fig 6.5 Traffic sniffing with URLs using urlsnarf

He feels that he is the only user seeing the data, no one knows about the information that he clicked but the intruder knows every click given by the user.

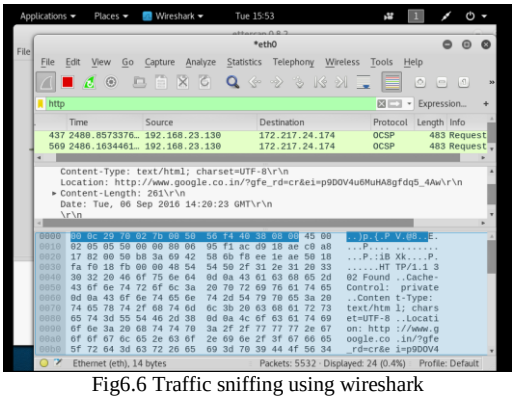


Fig6.6 Traffic sniffing using wireshark

Fig 6.6 shows how wireshark captures the network.It displays the website that have seen by victim,the date and length ofdata sent by user,ip address and protocols and it also possible to filter the interface where as the Fig 6.7 shows how Traffic sniffing is done using ettercap and driftnet.

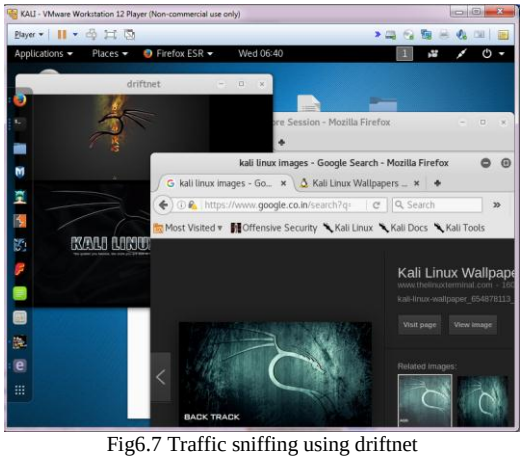


Fig6.7 Traffic sniffing using driftnet

The other case is about meterpreter Fig 6.8 illustrates that it exploits the webcam and keyscan using msfconsole.

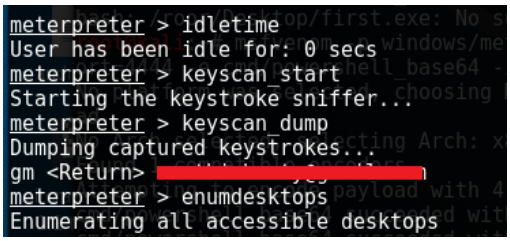


Fig 6.8 keyscan using metasploit

Meterpreter defines that the exploitation is going to be done by enabling the file in the system. For example as shown in the figure 6.6 keyscan_start defines that the file downloaded in the system need to be run or activated to perform keyscan.While running keyscan_start it scans all the keys that are typed by the user and stored. The stored keys are displayed by using command keyscan_dump .For example open the browser and click on the Gmail and login .The login details such as username and password that are stroked are displayed as a result. It is also possible to perform webcam penetration, sound recording and desktops information that are connected.

## VII. CONCLUSION

The most important factor today is IT sector should be aware of penetration testing. The computer security Now-a-days the most important factor is all about security in the e-environment. The important subject that IT administrators should be aware of is about security issues. Security is the challenging topic for regular users and also for corporate and educational institutions. So by the incidents or events that are going in the world we may judge that there is no complete security by downloading and installing antivirus programs. Now a day's there is more chance of getting hacked than getting mugged. By penetration tools had a lot of attention as it doesn't have limitation in their production. According to the individual needs Open source tools are to be modified. Now a day's every object is operated at everywhere using

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

web without considering the place and time which we concluded simply like the software is developed then in other way we should accept that not only in the software but also in hacking it is developed. Now a day's using tools cars and medical devices are hacked, in future may be there is a chance to hack data coming from satellites, weather patterns, weather forecasting and in worst cases nuclear weapons. This paper explains detailed penetration testing tools and how hacking is done between the sender and the receiver vice versa including mitigation strategies.

## REFERENCES

[1] Chiem Trieu Phong, "A study of penetration Testing Tools and Approaches" Eds. Auckland :Academic,2014
[2] Michele Fiocca "Literature study of penetration Testing" Linkopings universitet,Sweden
[3] Joseph Muniz ,Aamir Lakhani "Web Penetration Testing with Kali Linux" PACKT publishing., Open source community experience classified.
[4] Professional Information Security Training and services "Penetration testing with Kali Linux" v1.0.1,Offensive security 2014.
[5] Robert W.Beggs "Mastering Kali Linux for Advanced Penetration Testing",open source community experience classified, PACKT publishing ,BIRMINGHAM-MUMBAI 2014
[6] Konstatntinos Xynos,Iain Sutherland,Huw Read,Emlyn Everitt,Andrew J C Blyth "Penetration Testing and Vulnerability Assessments:A Professional Aproach ,International Cyber Resillence conference. 2010
[7] Stephen Nothcut,Jerry Shenk,Dave Shackleford,Tim Rosenberg,Raul Siles and Steve Mancini "Penetration Testing:Assessing your Overall Security Before Attackers Do" SANS analyst program,sponsored by CORE IMPACT June 2006.
[8] Nishant Shrestha "Security Assessment via Penetration Testing:A Network and System Administrator's Approach" university of OSLO,Department of Informatics, network and system Administration,June 4,2012.
[9] Joseph Muniz, Aamir Lakhani "Penetration Testing with Raspberry Pi" Community Experience Distilled PACKT publishing
[10] A.Bechtsoudis , N.Sklavos "Aiming at Higher Network Security Through Extensive Penetration Tests" IEEE LATIN AMERICA ,VOL 10,NO 3,APRIL,2012.
[11] Matthew Denis,Carlos Zena ,Thaier Hayajneh Computer science department "Penetration Testing:Concepts,Attack Methods and Defense strategies" 2013.
[12] Hui Liu,Zhitang Li "Methodology of network Intrusion Detection System Penetration Testing"Ninth International Conference on Web-Age Information Management Wuham,Hubei,China.
[13] Harshada Chaudri "Raspberry Pi Technology:A Review" International Journal of Innovative and Emerging Research in Engineering Volme 2,Issue 3 ,2015.
[14] Encarnacion ,Lewis. "Perform A Man in the middle attack with Kali Linux and Ettercap"
[15] Root.(2014,Auguest 17)."How to hack phones Bluetooth with kali Linux and Backtrack"
[16] Dalziel,Henry(2013,Auguest 17)"Wireshark basics:A simple concise tutorial foe beginners".
[17] Ailen G.Bacudio,Xiaohong Yaun,Bei-Tseng Bill Chu ,Monique Jones "An overview of penetration testing"International Journal of Network Security & Its Applilications(IJNSA)vol 3,No 6,November 2011.
[18] Filip Holik,Joseph Horalek "Effective penetration testing with metasploit framework and methodologies" IEEE International Symposium on Computational Intelligence and Informatics November 2014. Budapset,Hungary.