International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7, Issue-6, March 2019

Penetration Testing using Wireshark and Defensive Mechanisms Against MITM

V. Sahiti , Prasanth. Tilakchand, Balu. Kowshik, Pokala. Avinash, Simhadri Leela Kavya

Abstract: ***Internet Of Things(IOT) is a trending technology which is making the digital world a better platform with wide variety of applications. In this context, the security of IOT device is a major concern which has attracted many researchers and made it necessary to strengthen the IOT system from vulnerabilities from attacker's point of view. For which Penetration testing is the best technique. As the wireless technology advances, the security of the IOT devices should also advance. In this paper, Man-In-The-Middle (MITM) attack was performed using a simple Wireshark tool and the vulnerabilities were identified and different defensive mechanisms were outlined.***

Index Terms*: *Penetration testing, Wireshark, MITM , wireless devices, vulnerabilities, defensive mechanisms.

I. INTRODUCTION

IOT devices and services makes our lives easier and better in using technology and becomes a part of our daily lives. Internet of things connects different smart devices wirelessly and integrates them into a larger network. But in connecting large number of devices wirelessly there are many security threats involved which effects the potential uses of IOT. Without giving much importance to network security while designing IOT devices leads to so many vulnerabilities. Taking advantage of these vulnerabilities attackers can steal sensitive data and can monitor system activities and they can also control and damage our devices. In order to protect our devices from these attacks, we need some tools to find those vulnerabilities and make necessary defense mechanisms based on those vulnerabilities. Penetration testing is the popular method in finding vulnerabilities and some other security drawbacks in a device, network or an application. So by using penetration testing we can secure our device from different types of attacks.

Revised Manuscript Received on 30 March 2019.
***** Correspondence Author
V.Sahiti Department of ECE, KoneruLakshmaiahEducationFoundation,Vaddeswaram,Guntur-522502,AP,India
Prasanth.Tilakchand,Department.of.ECE,Koneru.Lakshmaiah.Education.Foundation,Vaddeswaram,Guntur522502,AP,India.
Avinash.Pokala,Department.of.ECE,,Koneru Lakshmaiah. Education.Foundation,Vaddeswaram,Guntur522502,AP,India.
Simhadri. Leela. Kavya,Department.of.ECE.Koneru Lakshmaiah Education Foundation, Vaddeswaram , Guntur-522502, AP, India
Balu. Kowshik, Department.of.ECE.Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur-522502, AP,India

And there are so many software tools available for penetration testing. In this paper we are using some of those tools for finding vulnerabilities and security assessment. And finally we are finding defense mechanisms and security measures that need to be implemented to protect our devices from attackers.

II. RELATED WORK

Riccardo Tomasi et.al[1], in 2011 have coined the term WSNs by introducing the concept of "Wireless Sensor Networks". At first, WSNs were essentially considered as independent frameworks however the upcoming Internet of Things(IOT) version is cultivating a deep interpretation of Wireless Sensored Networks as a section at internet. The author proposes an instrument to supporting of penetration testing at genuine Wireless sensors Networks Arrangements which depends LoWPAN, considering it as one of the most wanted building block of the IOT. It is a practical solution to tackle the IOT security on weakness of original Lo WPAN arrangements which might become easily represent the weakest security preferred link of IOT architecture. I So as to exhibit such entrance testing approaches, the commitment of this paper is an improvement of surely understood Metasploit system to help assaults focusing on IPV6 as empowered WSNs. Filip Holik et.al[2], in 2014 found that there is a requirement for a proactive way to deal with data security so as to stay away from potential security breaches. These days data security is vital since progressively increasingly secret data like restorative reports, is being secured electronically on pc structures and those structures are consistently connected with pc frameworks. For this reason the creator has quickly presents the essentials of entrance testing and demonstrates an approach to orchestrate and utilize Metasploit system while undertaking infiltration checkout. Additionally programming devices and procedures utilized in this work are likewise legitimate and relevant for SCADA frameworks. M.I.P. Salas et.al[3], in 2015 make use of blackbox method to find vulnerabilities in net administrations the utilization of infiltration testing. Web administrations artistic creations over unique associations amongst dispensed structures. This era became mainly designed to without difficulty bypass SOAP messages through firewall the use of open ports. These advantages contain various security requests like Injection strikes, phishing, Denial-of-contributions (DOS) assaults, etc. The issue to find escape clauses before they're misused urges engineers to utilize security testing like penetration trying out to deduct the ability attacks. The outcomes tells that ninety seven.1% of net services have minimum one vulnerability of those assaults Himanshu Gupta et.al[4],

in 2015 describes safety towards penetration assualts using Metasploit. The author tries to signify a framework to counter the assaults by utilizing the structures, explicitly Metasploit. It incorporates the conviction of a framework that is ready to hinder the Metasploit assualts in particular instances in any other case alert the administrator. Previous studies indicates that many IDs and antivirus are useless against Metasploit. The proposed machine make use of community monitoring application that is capable display the connection tried to the host system and provide the reply hence by using algorithm method which is used inside the device Matthew Denis et.al[5], in 2016 look into exclusive factors of penetration trying out which includes tools, assault methodologies, and defense techniques. The author carried out unique penetration by using the usage of a private networks, gadgets, and virtualized structures and tools. . The maker predominately utilized the hardware inside Kali Linux suite. The assaults performed included: phone entrance penetrated testing, hacking phones Bluetooth, guests sniffing, hacking WPA ensured wifi and hacking far of pc through IP and open ports utilizing propelled port scanner. This paper specified crucial penetration trying out assaults and discusses ability mitigation strategies. Yaroslav Stefinko et.al[6], in 2016 Infiltration testing enables associations to survey vulnerabilities proactively, using genuine world exploits, allowing them to assess the potential for their frameworks to be subverted through hacking and malware conspires in a similar way that aggressors utilize Special Operational frameworks on UNIX core ,developed scripts, utilities and applications are suggested. Pentesting is used for proactive and information structures protection. Cyber strikes have ended up being a standout amongst the best perils to the universe of business and economics. Amount of damage has been building up every day and more associations or establishments have advanced toward getting to be setbacks of ambushes or data break performed by dim hats. Hence, companies are scanning for most perfect way to deal with guarantee their structures and essential information. Most surely understood course is to test their structures by methods for penetration tests by affirmed good teams, which can proactively watch PC systems Hsiu-Chuan Huang et.al[7],in 2017 Entrance penetrated testing is a important guard against regular A web application security risks, for instance, SQL imbuement and cross-site scripting attacks. A proposed web weakness scanner thusly creates test data with combinative shirking procedures, altogether expanding test incorporation and revealing more vulnerabilities. among the most fundamental security risks to the present destinations, which are dynamic, instinctive, and network arranged, are mixture and cross-site scripting (XSS) attacks.2 An implantation strike happens when an enemy sends data to an improperly coded application that beguiles it into executing unintended headings or questions shown by the adversary. A principle driver of unapproved data get to is SQL imbuement, which incorporates sending malevolent data to change SQL request executed by web application databases. Rina Elizabeth Lopez de Jimenez et.al[8],in 2017 Without a doubt the quick development of the Web and the usage of countless and versatile applications have come to benefit everyone and change the way in which we pass on similarly as how we direct trades; It is an immediate aftereffect of this that the look at swings to be basic security endeavors to ensure the dependability and unflinching nature of information. Various associations today are concerned that web applications are the speediest or are made with the best programming improvement, anyway not a lot of pressure that have the right security. Along these lines, this article discusses the particular frameworks what's more, entrance test using unmistakable programming - based instruments to develop potential vulnerabilities a web applications

Sandhya et.al[9], in 2017 Developing innovation has made an unavoidable risk of uncover of information that is shared on the web. Wireshark apparatus empowers the moral programmer to uncover the blemishes in the framework security at the client validation level. This methodology of recognizing vulnerabilities is regarded fit as the technique engaged with this testing is fast and gives great achievement in recognizing vulnerabilities. The use of Wireshark additionally guarantees that the technique pursued is up to the required gauges. This paper talked about the need to use infiltration testing, the advantages of utilizing Wireshark for the equivalent and proceeds to delineate one technique for utilizing the apparatus to perform entrance testing. Most territories of a system are exceedingly helpless to security assaults by enemies. This paper centers around illuminating the previously mentioned issue by studying different devices accessible for infiltration testing. This additionally gives an example of fundamental entrance testing utilizing Wireshark

Chung Kuan Chen et.al[10], in 2018 Internet of Things (IoT) devices and organizations are by and by essential to practically consistently works out. Regardless, the IoT brings included solace just as, by partner an ever increasing number of things to the Web, new security dangers. Numerous applications in IoT situations, from sharp homes to changed restorative administrations, contain fragile individual information that can transform into the targets of framework assaults. Shockingly, ensuring the security of IoT objects isn't clear for three imperative reasons. In any case, the IoT's heterogeneous nature makes it frail against various sorts of strikes. Second, heavyweight security instruments are infeasible for resource constrained IoT gadgets. Third, various IoT objects are sent just once and starting there are every so often kept up or revived. We have gone through different existing work on Penetrating testing and Security threats in IOT using IEEE papers which are being summarized above this. After a good study, we come across different vulnerabilities that are there in different IOT and Wireless systems. We found one of those vulnerabilities by doing MITM attack using Wireshark and outlined some defensive mechanisms.

III. TOOLS REQUIRED FOR PENETRATION TESTING

Below mentioned are some at the different tools that are used for penetration testing and in this paper we mainly focused on Wireshark and Ettercap for performing the attack.

Wireshark: Wireshark is the open-source network protocol analyzer. It used to capture, analyze and filter packets and it has many other functions which helpful for finding vulnerabilities. It provides minute details about packet information and display them in a human readable format.

Metasploit framework: Metasploit is used for applying and executing exploit code (payload) against a victim as a remote target machine.

It also has automated process of penetration testing and we can develop our own customized tools using Metasploit framework. By using Metasploit we can do different types of penetration tests

Hping3: Hping3 is a direction line situated TCP/IP packet constructing agent/analyzer. It supports following TCP, ICMP, UDP and RAW-IP conventions. Hping3 is utilized for firewall testing, advance port examining, remote OS fingerprinting and uptime speculating and numerous others

IV. STAGES IN PENETRATION TESTING

There are different stages involved in Penetration testing technique in which every stage has its own importance.

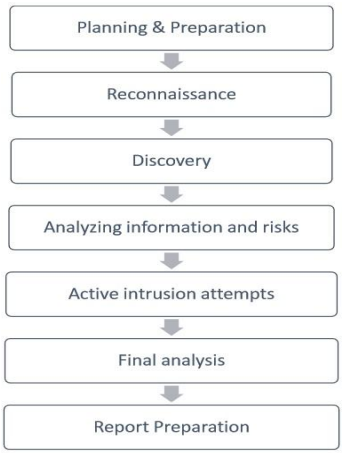

Figure 1: Penetration testing stages

Below mentioned are the different stages in penetration testing that are briefly explained one by one.

Planning and Reconnaissance:
This is the planning stage in which we define our testing goals and types of tests that we follow. Reconnaissance is intelligence gathering which involves collecting data such as network and domain names, server information and some other information.

Scanning:
Scanning involves testing the target application's response to various intrusion attempts. Scanning involves two types of analysis, one is static analysis and other is dynamic analysis.

Gaining access:
In this stage, testers try to take control of the device by using different assaults like as SQL injection, XSS(Cross site scripting) and backdoors and exploit the vulnerabilities that are uncovered by these attacks and they start gathering information after gaining access.

Maintaining access:
This stage involves maintaining our access within the exploited system as long as possible in order to gather as much as information and gaining in-depth access to repeat advanced persistent threats for remaining in the system. By this we can easily damage and steal data.

Analysis:
This is the last stage in which we analyze all the activities that tester did during testing and list the vulnerabilities that can be exploited and sensitive data that can be accessed and the time that the tester can be able to stay in the exploited system. Based on this analysis, we should take necessary security measures and protect our systems from future attacks.

V. PENETRATION TESTING METHODS

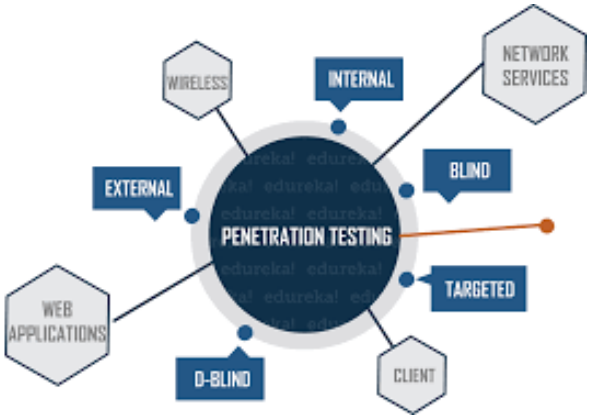

Figure 2: Different methods in Penetration testing

External testing:
External penetration tests focuses on the assets of a target which are open to the internet such as company details like web application, email and domain name servers. Finally its goal is extract valuable data by gaining access.

Internal testing:
Tester will be given access to the application's firewall and tester will perform an attack inside application firewall and steals the credentials of the application user.

Blind testing:
In blind testing, tester only knows the name of the target and this gives security personnel a real-time look into how an actual application attack would take place.

Double blind testing:
In this testing, security personnel does not know anything about the attack which performs by tester. As in the real world, security personnel does not have time to de
fense against the attack.

Targeted testing:
In targeted testing, both tester and security personnel work together to provide a real-time feedback for security team. Feedback will be given from each other's point of view.

VI. PENETRATION TEST ATTACK USING WIRESHARK

Here we are performing the Man in the middle (MITM) attack as a penetration test using Ettercap and Wireshark. A man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and is an assault where the aggressor furtively transfers and potentially modifies the correspondence between two gatherings who trust they are specifically speaking with the point is to relate the assailant's MAC address with the IP address of another host, for example, the default entryway, causing any traffic implied for that IP address to be sent to the assailant. Along these lines assailant will catch the parcels utilizing Wireshark and block the information that is being conveyed between the client and the site while Ettercap is being utilized for ARP harming. Wireshark is utilized to go into indiscriminate mode. Indiscriminate mode is the system interface mode in which NIC reports each packet that it observes.

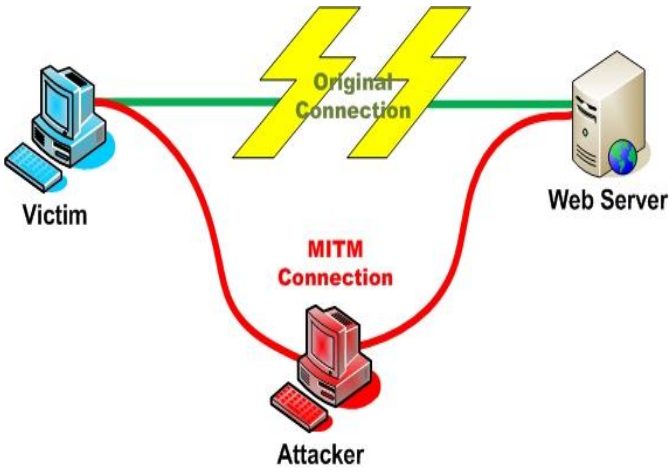

Figure 3: MITM attack model view

STEPS INVOLVED IN ATTACK

1. First, we are using Ettercap for sniffing the packets and after opening the Ettercap we started unified sniffing.

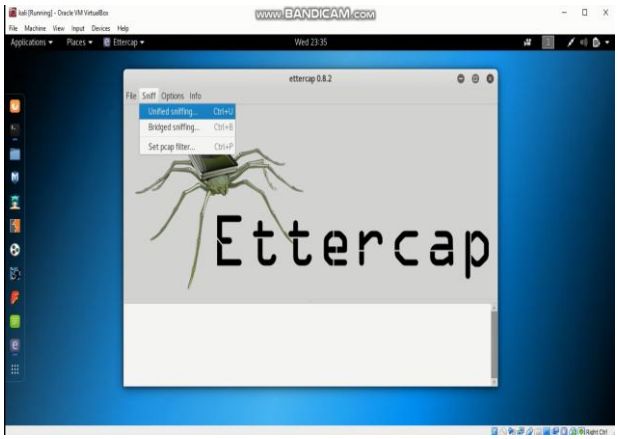

Figure 4: Starting unified sniffing

2. Next, we are scanning for hosts that are in our network in which one will be the victim and other will be the router or gateway

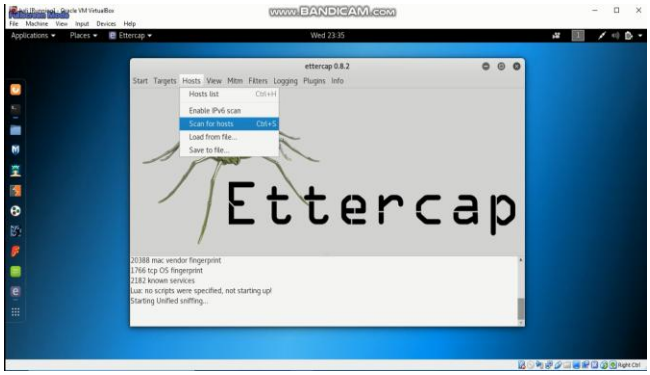

Figure 5: Scanning for hosts

3. After scanning we are adding the router's IP to target 2 and victim's IP to target 1.

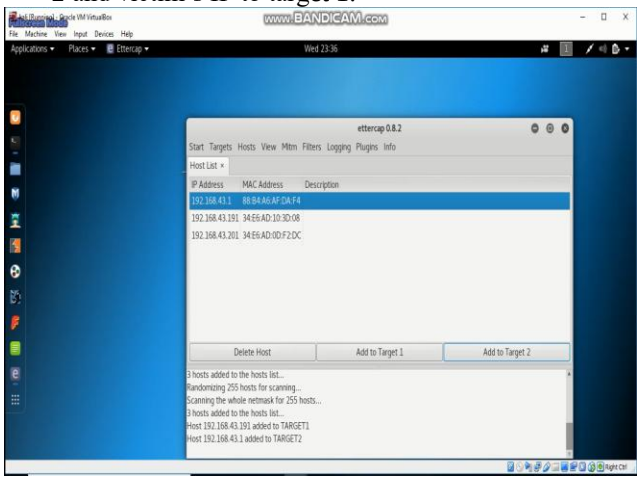

Figure 6: Adding target's IP address

4. Then we started ARP poisoning of remote connections

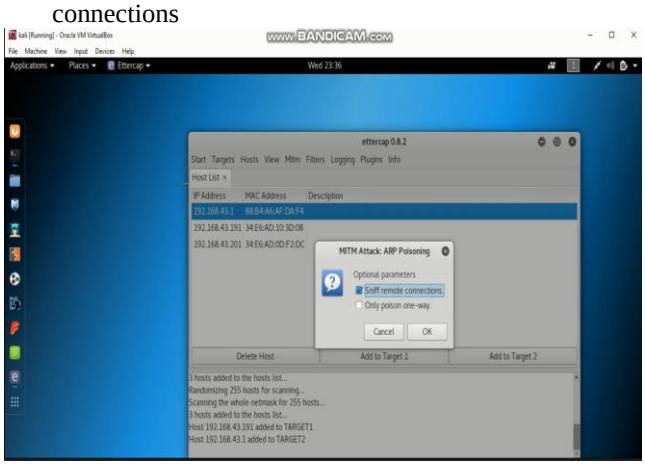

Figure 7: Starting ARP poisoning

5. Now Wireshark is used for capturing packets that are being transferred between router and victim. And we can filter packets using IP address of victim

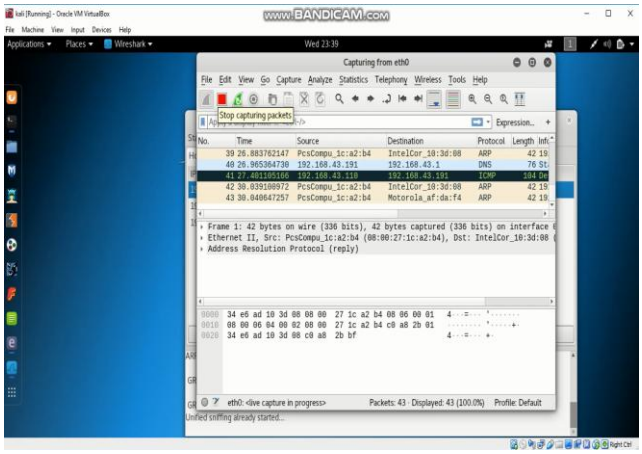

Figure 8: Capturing live packets using Wireshark

6. And whenever victim goes to a website and login into that website those packets are captured using POST request which is used to filter and capture those packets which are sent by the user to the server by request message

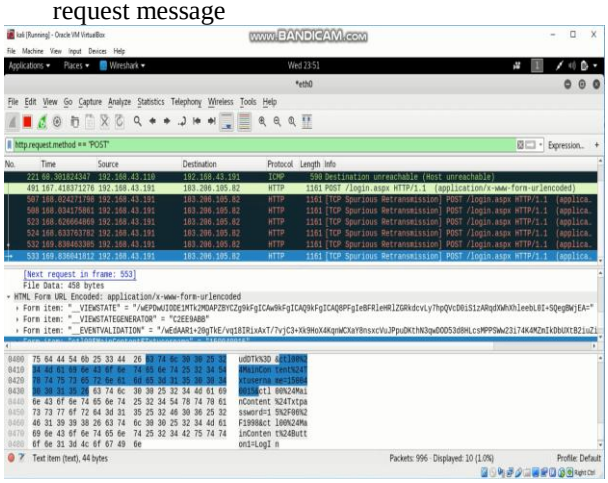

Figure 9: Searching login packets using POST request

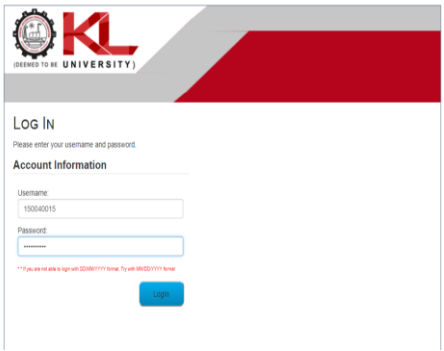

Figure 10: Logging into vulnerable website

7. After the POST request, we can see the login credentials in hexadecimal by that packet and that can be converted to plain text

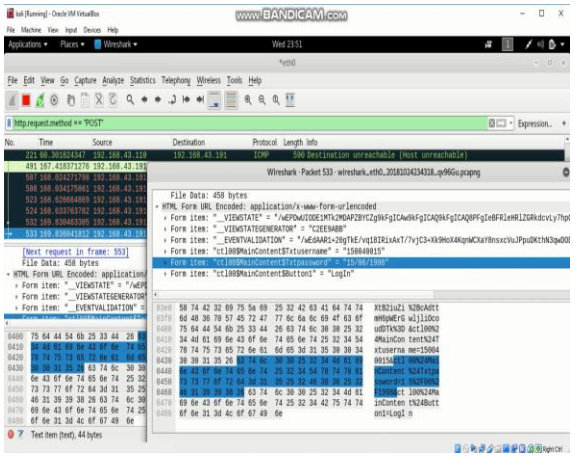

Figure 11: Captured Login credentials

VII. RESULTS AND DEFENSIVE MECHANISMS

By performing this attack, we can steal the user login credentials using Wireshark tool. From this we can conclude that the website has vulnerabilities in it.

Defensive mechanisms:

In order to protect from the attack that we did, there are the steps that need to be followed;

1.ARP Detection Software is used to verify the IP/MAC address resolution and grant them if they are authenticated and ignores unsolicited ARP reply packets. In this way it is useful in protecting the system from this attack. 2.Website should be upgraded from HTTP to HTTPS because HTTP does not require any certificates but HTTPS requires SSL certificates which provides security and cryptographic (encryption protocols) are present in HTTPS 3.Static ARP entries which are used to manually create the link between the MAC address and IP address. So, it should be used so device cannot be fooled by fake ARP requests.

VIII. CONCLUSION

IOT network security need to be enhanced in order to protect our IOT devices and applications from different vulnerabilities that are being exposed to attackers. So, to secure our devices from the attackers we should have to find the vulnerabilities in the network and application devices. For this we implemented Penetration testing technique using Wireshark by performing MITM attack and found some of the vulnerabilities that can be easily exploited by attackers and we also outlined some of the different defensive mechanisms like using ARP detection software and HTTPS connection which are useful in preventing some of those attacks.

REFERENCES

1. Riccardo Tomasi, Luca Bruno, Claudio Pastrone, Maurizio Spirito, “Meta-Exploitation of IPv6- based WSNs”,Istituto Superiore Mario Boella, Italy 2011.
2. Filip Holik, Josef Horalek, Ondrej Marik, Sona Neradova, Stanislav Zitta, “Effective penetration testing with Metasploit framework and methodologies”, University of Pardubice, 2014.

3. M. I. P. Salas, and E. Martins, “A Black-Box Approach to Detect Vulnerabilities in Web Services Using Penetration Testing”, IEEE Latin America Transactions, V0l. 13, NO. 3, March 2015.
4. Himanshu Gupta, Rohit kumar,”Protection against Penetration Attacks Using Metasploit” Amity University, Noida, India, 2015.
5. Matthew Denis, Carlos Zena, Thaier Hayajneh,” Penetration Testing: Concepts, Attack Methods, and Defense Strategies”, New York Institute of Technology Old Westbury, NY, USA,2016.
6. Yaroslav Stefinko, Andrian Piskozub, Roman Banakh,” Manual and Automated Penetration Testing”, 2016.
7. Hsiu-Chuan Huang, Zhi-Kai Zhang, Hao-Wen Cheng, and Shiuhpyng Winston Shieh,”Web Application Security:Threats,Countermeasures, and Pitfalls”,National Chiao Tung University,2017.
8. Rina Elizabeth Lopez de Jimenez, Escuela de Computacion, Itca-Fepade, Santa Tecla, EI Salvador,” Pentesting on Web Applications using Ethical Hacking”,2017.
9. S Sandhya, Sohini Purakayasta, Emil Joshua, Akash Deep,” Assessment of Website Security by Penetration Testing Using Wireshark”, RVCE, Bengaluru,2017.
10. Chung-Kuan Chen, Zhi-Kai Zhang, Shan-Hsin Lee, and Shiuhpyng shieh,”Penetration testing in the IOT age”, National Chiao Tung University,2018.

AUTHORS PROFILE

Sahiti Vankayalapati is an assistant professor currently working in the Department of Electronics and Communication Engineering in Koneru Lakshmaiah Education Foundation.Her work domain majorly covers Wireless Communications and Antennas.

Prasanth Tilakchand is currently pursuing his bachelor’s degree in Technology in the Department of Electronics and Communication Engineering at Koneru Lakshmaiah Education Foundatoin.His major field of interest is Networks and Cyber Security.

Avinash is currently pursuing his bachelor’s degree in Technology in the Department of Electronics and Communication Engineering at Koneru Lakshmaiah Education Foundatoin.His major field of interest is Networks

Simhadri Leela Kavya is currently pursuing his bachelor’s degree in Technology in the Department of Electronics and Communication Engineering at Koneru Lakshmaiah Education Foundatoin.His major field of interest is Networks

Balu Kowshik is currently pursuing his bachelor’s degree in Technology in the Department of Electronics and Communication Engineering at Koneru Lakshmaiah Education Foundatoin.His major field of interest is Networks