ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ETHICAL HACKING IN WINDOWS ENVIRONMENT

Navpreet Kaur*, Dr. Jaswinder Singh
* Research Scholar, Department of Computer Engineering, Punjabi University, Patiala, India.
Assistant Professor,Department of Computer Engineering, Punjabi University, Patiala, India.

DOI: 10.5281/zenodo.46485

ABSTRACT

This paper, shows by demonstration with System Penetration, how to reveal security holes by using some tools like 'Cain and Abel' and 'Wireshark' and carrying out the attacks such as cracking password, performing man in the middle attacks, sniffing user traffic etc. The tests were performed by establishing the virtual lab. The objective of the paper was to demonstrate how easily one's system can be hacked by revealing various security holes in windows-based system. The results show how simple it is to abuse a system or sniff a password if very little attention is paid to the system security and safety. Since systems can never be always safe from attacks so it is good for individuals to know about these threats and use proper security mechanisms so that they do not get exploited as discussed in this paper.

KEYWORDS: Penetration Testing, Intrusion Detection System, DNS Spoofing, ARP Poisoning

INTRODUCTION

A. Background

In today's digital arena everyone and everything is connected to the Internet. This huge web of internet connectivity has made the world a global village. Within this village whether it is a common man or businessmen or entrepreneur or an organization, each one of these are living in the cyber space world. Exploitation of computer systems and network is increasing rapidly. With a large number of hackers ready with their arsenal toolkits to attack your system, detection of the security holes is becoming so easier. This leads to all cyber citizens being at stake.

Awareness of the ongoing cyber risks has made many organizations and entrepreneurs to take appropriate steps towards cyber safety. Let it alone be full- fledged vulnerability assessment or penetration testing of the company or installation of security devices such as intrusion detection systems (IDS), firewalls, intrusion prevention systems (IPS) and so on. These organizations have funds and expertise to measure the security of their systems but the side which is bereft of these advantages is that of a common man, individual or a student. The heavily deployed machines, hardware's and software's meant for the usage of security becomes void when an individual comes into scene. Here comes the system penetration testing that comes to an aid to help minimize the losses. Penetration testing helps in revealing the security holes through which one can be compromised. No one in this world ever wants their information to be breached. So, revealing and later patching up known security holes can minimize the chances of being hacked.

B. Methodology Used

Using various penetration testing tools, a demonstration is done to show how insecure the system really is. The tools used are Cain and Abel and Wireshark. Cain and Abel is specifically developed for network administrators, penetration testers, professional IT people and everyone that wants to try a hand in ethical hacking. Common features of this tool are poisoning the ARP cache by ARP Poison Routing, various Man-in-the-middle attacks like ARP Poisoning, DNS Spoofing, and Session Hijacking so on. It also provides dictionary and brute-force attacks for common hashing algorithms, cryptanalysis attacks, password decoders etc.

Wireshark is one of the popular open source network packet analyzer specifically used by network administrators, network security engineers, developers etc. Wireshark is a great tool to troubleshoot network problems, examine security problems, debugging protocol implementations, learning network protocol internals.

THE THEORETICAL BACKGROUND

A. Meaning of Penetration Testing

With the explosive usage of internet, number of hackers increasing manifolds has set alarms for network security professionals. In order to control the malicious activities of bad guys another group of hackers called "Ethical Hackers" came into picture. Ethical Hackers are also known as white-hat hackers or pen testers. The word "Ethical" is used for these hackers because they penetrate into the system in the limits of "Ethical Standards" to disclose the vulnerabilities of the concerned system or network and take appropriate measures to patch it up.

The methodology adopted by white-hat hackers is same as that of black-hat hackers. The only difference that categorizes a hacker into one of these two categories is that of mind-set. The hacker who breaks into a system or network with the malicious intent of stealing confidential information and misusing it against the concerned person or an organization falls under the category of black-hat hackers. In contrast to this, the hacker who breaks into the system or network with the permission from authorized person in order to find the vulnerabilities of the system/network and plug-up the security holes falls under the category of white-hat hackers or pen-testers. Thus, ethical hacking is always legal and trustworthy. In other words, ethical hacking means assessment and securing of the resources with the view to protect them.

B. Need for Penetration Testing

The main purpose of penetration testing is to identify the security holes so that they can be patched before hackers exploit the system or network. Ethical hackers use their skills and apply penetration testing to discover the risks and take counter-measures for security. Penetration testing is important to understand threats for better defense and verifying the secure configurations to make informed IT decisions.

C. Types of Penetration Testing

1. Black-Box Penetration Testing

Black-box penetration testing simulates to real-world attack where no previous knowledge of the system or network to be tested is available. The criterion used in black-box testing is Information Base. The information base surrounds around the knowledge of the target organization or victim. If the level of information known to the pen-tester is zero, then it is clearly understood that black-box testing is under progress. In order to circumvent hacker, the pen-tester has to explore all the publically available information and databases, map the network, enumerate the services, detecting the Operating System and so on.

2. White-Box Penetration Testing

In White-box penetration testing, full knowledge of the system or network to be tested is available. The criterion used in this testing is same as that of black-box testing i.e. Information Base. In real world scenario this testing is conducted to circumvent hackers who have detailed knowledge of the organization's network setup such as previous employee or the external ISP who has installed security related systems. The information such as company infrastructure, network type, current security implementations, company policies and IP address/ firewalls/ IDS details are provided to the pen-tester during white-box testing.

3. Gray- Box Penetration Testing

As the name suggests, Gray-box penetration testing lies between white-box and black-box testing. In this testing, partial knowledge of the organization's infrastructure is made available to the pen-testers. This testing is conducted to circumvent the activities of gray-hat hackers. Gray-hat hackers are those people who show the traits of both white-hat and black-hat hackers. They breach into the security of an organization without any permission like black-hat hackers but after breaching they inform the concerned company of the security loopholes like white-hat hackers.

D. Penetration Testing Phases

1. Preparation Phase

The preparation phase is a mandatory step which involves pre-planning of the activities that are to be performed during penetration testing. Before the beginning of penetration testing, a number of organizational, contractual and legal issues are needed to be addressed. The penetration test to be developed should strictly stick to the requirements of the customer. For this purpose, a legal contract should be signed in by both the parties i.e. the customer and the ethical hacking team. The contract should clearly illustrate the objectives of penetration testing, sensitive information required by the ethical hacking team, Indemnification clause, Nondisclosure clause, Fees and project schedule, test methodology and reporting procedures.

2. Reconnaissance Phase

The main purpose of reconnaissance/information gathering is to explore as much information as possible about the target organization. Reconnaissance can be conducted in two ways: Passive Reconnaissance and Active

Reconnaissance. Passive reconnaissance is done behind the scenes without touching the territory of the target. Active reconnaissance trespasses the territory of the target and traces of encroachment can easily be found by network professionals. Attackers spend more time in this phase than in actual attack phase. There are a number of ways of gathering information such as Footprinting, Google hacking and Social engineering.

3. Scanning Phase

The information collected in above phase is used to scan the network. Different techniques used for scanning are Fingerprinting, Enumeration, and External Hacking etc. Fingerprinting is a means to determine the operating system of a computer in the network. It can be performed "actively" by sending specially created packets to the target system and analyzing its response or "passively" by sniffing the packets between two hosts. Narrowing down the operating system is important as it allows the hacker to exploit the vulnerabilities of the respective OS if the target is still using old, unpatched version of the operating system. Also, attempting Windows-specific attacks against UNIX hosts seems to be void. So, he needs to be doubly sure before investing his energy on performing a hack. Enumeration is a process to gather as much information as possible about the users, network resources and services. Enumeration makes a fixed active connection to the system.

4. Exploitation Phase

This is the actual hacking phase in which hacker makes use of the information discovered in above phases to attack and enter into the target network or system. This phase also known as "Owning the System". Once the hacker has gained the control of the network or system, he exploits it by performing various attacks such as password cracking, spoofing, launching man-in-the-middle attacks, hijacking and so on. In order to maintain the access for future attacks, Trojan horse, backdoors, rootkits etc. are implemented in the system.

5. Reporting Phase

Reporting phase includes winding up the results from the analysis into a readable format. As the decision making persons are not very technical, so it is important to have several sections to a report. The common format for penetration testing reports is to include Raw Output, Detailed Report and Executive Summary as its main parts. The Raw Output includes the actual output found during the penetration testing. It is too lengthy and provides too deep information. It is meant mainly for record keeping and documentation The Detailed Report includes comprehensive results of the penetration testing in technical form. It is meant for technical people such as network administrators, IT professionals. The Executive Summary is just an overview of the major findings. It does not include technical details and is meant for non-technical people who can understand in simple language.

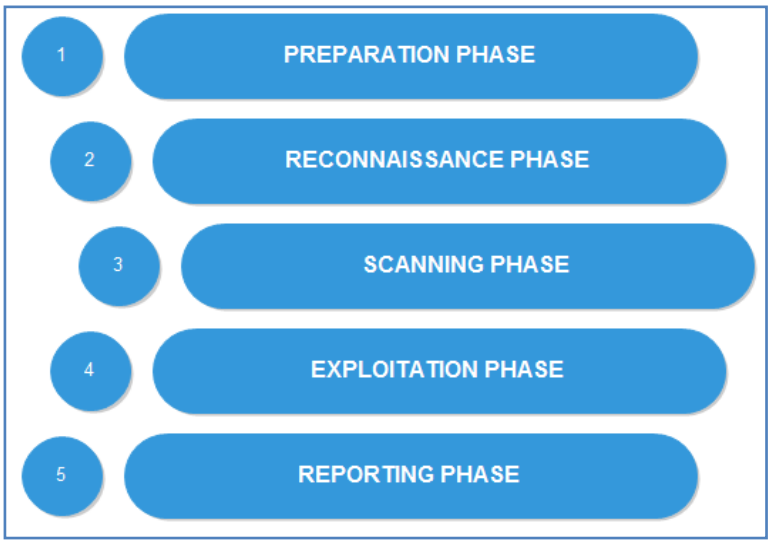
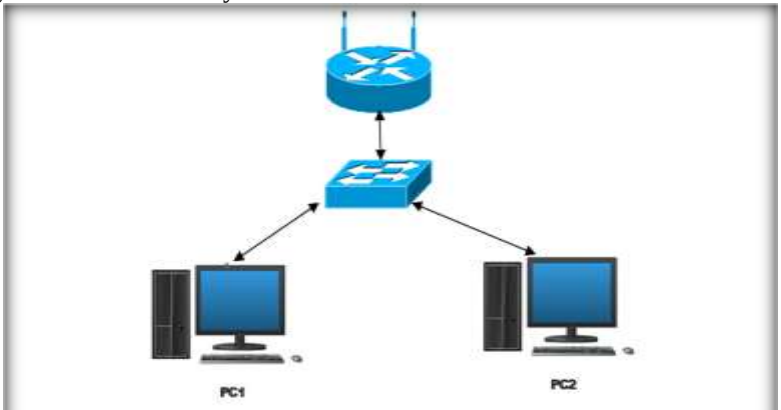


Fig. 1 Penetration Testing Phases

SYSTEM PENETRATION ATTACKS

To be able to conduct this penetration test, a virtual lab is needed to be established. We can use VMware workstation or Oracle Virtual Box for this purpose. We need two windows based systems: one the attacker system and other the victim system. The attacker system should have Cain and Abel tool installed on it.



Device (Hostname)	IP Address	Subnet Mask	Default Gateway
PC1	192.168.43.3	255.255.255.0	192.168.43.1
PC2	192.168.43.58	255.255.255.0	192.168.43.1

Fig. 2 Virtual Lab Setup

To check the IP addresses of each system open Command Prompt and Type ipconfig/all. It shows the complete TCP/IP configuration for all connectors. After checking the IP addresses, check whether the virtual setup is working or not by pinging the systems.

A. ARP Poisoning

Open Cain and Abel. Click on Configure and choose required adapter. Now, click on Sniffer Tab and an empty table will come up. In order to fill the table with entries, go to second button on toolbar and start the in-built Sniffer. Right click on the empty area and click on the plus (+) symbol on main toolbar and click ok. Mac Address Scanner Tab will appear and select the target within a particular range or all hosts in the subnet. Within few seconds a list of IP addresses, Mac addresses along with host name, OUI fingerprint etc. is obtained. After building a host list, work from the APR tab. Switch to the APR window by clicking the tab. Click on the + sign in the toolbar to add a new ARP poison routing. Choose the gateway, in the next list and in the second list IP address of victim system is shown and click ok. Activate Cain & Abel's ARP cache poisoning features by clicking yellow and black button on standard toolbar. This makes the attacker system to act as a middleman by intercepting the communication between the victims.

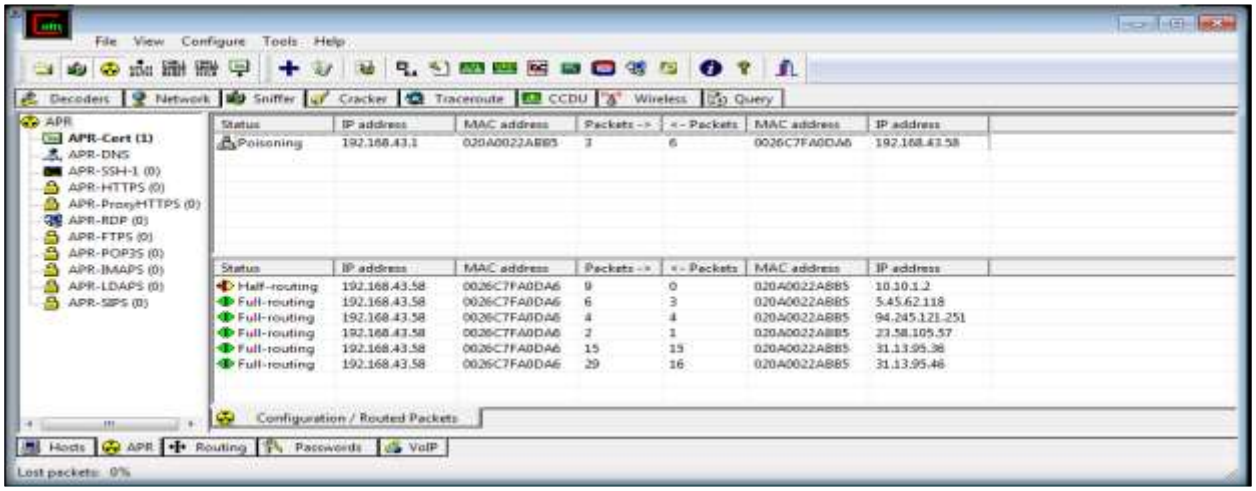


Fig. 3 ARP Poisoning

Go to victim system and open any http website requiring username and password. Fill in the credentials on that website.

B. DNS Spoofing

Open Cain and Abel. Click on Configure and choose required adapter. Now, click on Sniffer Tab and an empty table will come up. In order to fill the table with entries, go to second button on toolbar and start the in-built Sniffer. Right click on the empty area and click on the plus (+) symbol on main toolbar and click ok. Mac Address Scanner Tab will appear and select the target within a particular range or all hosts in the subnet. Within few seconds a list of IP addresses, Mac addresses along with host name, OUI fingerprint etc. is obtained. After building a host list, work from the APR tab. Switch to the APR window by clicking the tab. Click on the + sign in the toolbar to add a new ARP poison routing. Choose the gateway, in the next list and in the second list IP address of victim system is shown and click ok. Go to APR-DNS tab and again click on + sign. Web address that the attacker wants to spoof is entered, (in this case when user goes to bing.com he is diverted to google.com). Click on Resolve and type web address www.bing.com. Click ok as shown in Figure 4. Now, enable APR poisoning.

Fig. 4 DNS Spoofing

C. Sniffing Network Traffic

In order the sniff the network traffic, Wireshark tool should be installed on your system to capture the packets. Figure 5 shows the setup needed for network sniffing.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

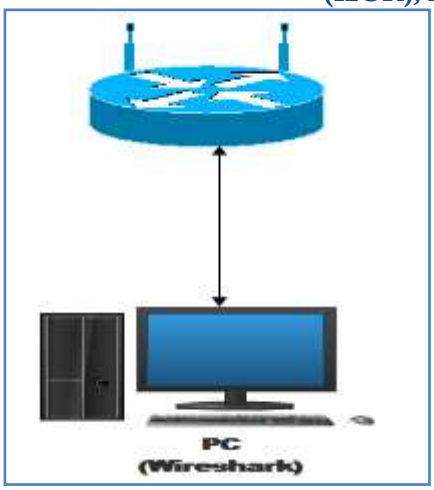


Fig. 5 Wireshark Setup

Start a Packet Capture by clicking Start. As Wireshark opens click on Interface List and select the interfaces that one wants to capture. Now, click the Start button. All the packets sent from or to one's machine are captured. Now open Web browser and go to httprecipes.com. Enter a Username as "guest" and a Password as "guest123" as shown in figure 6. In the Wireshark window, box, click Capture, Stop.

Fig.6 Input Credentials

RESULTS AND ANALYZES

A. ARP Poisoning

All the credentials filled by the user on the victim system are clearly visible to the hacker on attacker system. On the Attacker system, click on Passwords tab on the standard toolbar. Go to HTTP tab and all data is compromised as shown in figure 7.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

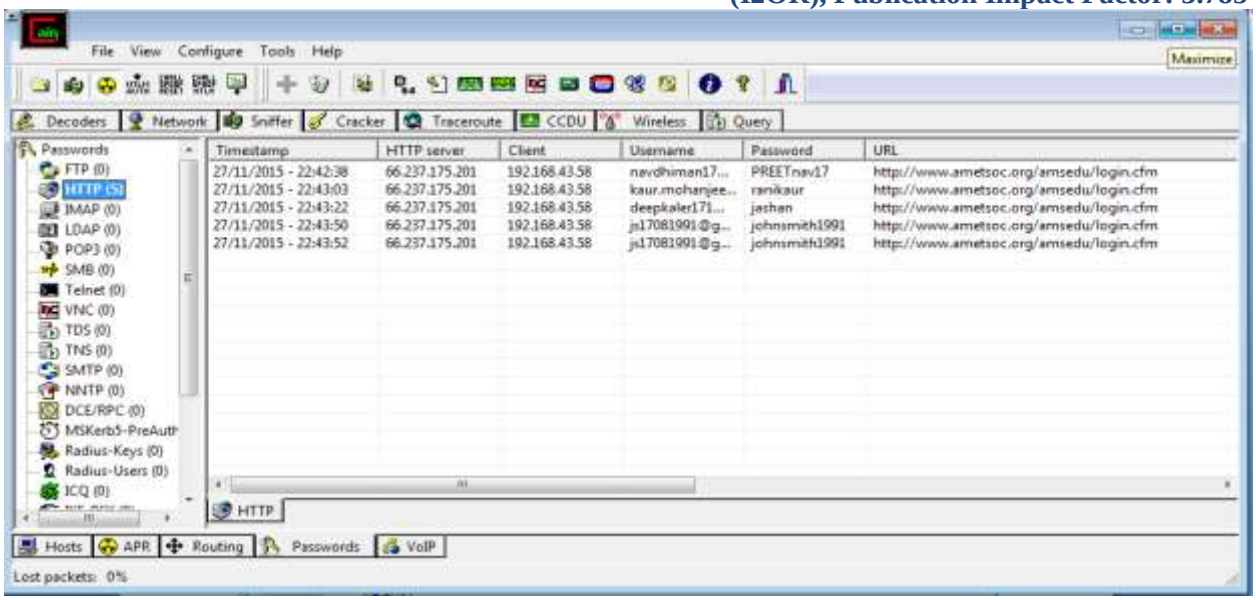


Fig. 7 Information Revealed

B. DNS Spoofing

Every time the user on victim system tries to open www.bing.com he is redirected to www.google.com.

C. Sniffing Network Traffic

In order to observe the password in Wireshark, type http in filter and click Apply. This will filter all the http packets over the network. In the upper pane of Wireshark, find "POST/1/2/forms" packet. Right click the packet and click on Follow TCP Stream. The Username and Password entered is clearly visible as shown in figure 8.

Fig. 8 Username, Password captured

D. Technical Problems

During the demonstration, there have been a lot of problems. One of the biggest problems was to download Cain and Abel on virtual machine. Since security message showing potential harmful software pops up in browser, it was very difficult to install on system. After few settings, the setup could be downloaded but again the browser blocked it. To solve this problem new rule was written by going to Control Panel -> Windows Firewall -> Advanced Settings. In Advanced settings go to Inbound Rules. Click on New Rule -> Port and click Next. Select TCP and select specific local ports and write in the field provided 450, click Next. Now select Allow the Connection, click Next. Select appropriate rule and give a name to the new rule which is created.

E. Wireshark vs. Cain and Abel

After learning the usage of Wireshark and Cain and Abel tools, following differences were drawn out:-

Table 1. Wireshark vs. Cain and Abel

Features	Wireshark	Cain and Abel
Creator	Wireshark is developed by The Wireshark Team.	Cain and Abel is developed by Massimiliano Montoro.
Interface	Wireshark is available in both GUI and CLI interface.	It is available only in GUI interface.
Software License	Freeware	GNU (General Public License)
OS	Microsoft Windows and Linux	Only on Windows platform
Main feature	It is a great tool for network analysis.	It is a great tool for ARP poisoning and password cracking.
Software vulnerabilities	It exploits software vulnerabilities.	It cannot exploit software vulnerabilities.
TCP/IP stream	It can reconstruct TCP/IP stream.	It cannot reconstruct TCP/IP stream.
Traffic Analyzes	It analyzes the whole traffic over the network with detailed information.	It cannot analyze the whole traffic. It shows only number of packets captured/sniffed.

CONCLUSION

The objective of this paper was to evaluate the system security using common techniques, to make aware how using the above mentioned simple steps, anyone can break into your system. Knowing the various ways by which intruder can enter into your system is the first step towards securing your system by covering the discovered security flaws. It was found that using tools such as Cain and Abel passwords can be easily cracked, various man in the middle attacks like ARP poisoning, DNS Spoofing can be performed with little knowledge of these tools. Other tool useful in performing penetration test was Wireshark. Proper and right usage of this tool could lead to catch handful amount of information passing over your network. Using this tool it was learnt how easily passwords and other critical information can be intercepted. From this study, it was concluded that a system can be protected by performing various penetration tests starting from the basic techniques as described above in this paper.

REFERENCES

1. R. Shanmugapriya, “A Study Of Network Security Using Penetration Testing” in IEEE Information Communication and Embedded Systems (ICICES), 2013 International Conference, DOI: 10.1109/ICICES.2013.6508375, ISSN: 978-1-4673-5786-9
2. C.C. Palmer, “Ethical Hacking,” in IBM Systems Journal, Vol 40 No 3, 2001, pp. 769-780.
3. Gurpreet K. Juneja, “Ethical Hacking: A Technique To Enhance Information Security” in International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 12, December 2013, ISSN: 2319-8753

4. Kumar Utkarsh, "System Security And Ethical Hacking" in IJREAT International Journal of Research in Engineering & Advanced Technology, Vol. 1, Issue 1, March, 2013 ISSN: 2320 – 8791
5. M. Bishop, "Polt Scanning," in Information SecurityAwareness Forum**,** Department of Information Technology, State of California, Dec. 1 2000.
6. Akanksha Bansal, Monika Agarwal, "Ethical Hacking And Social Security" in A Journal of Radix International Educational and Research Consortium RIJS, Vol. 1, Issue 11, November 2012, ISSN: 2250 – 3994
7. Pulkit Berwal, "Ethical Hacking: Need Of Modern Era" in International Journal of Engineering and Innovative Technology (IJEIT) Vol. 3, Issue 5, November 2013, ISSN: 2277-3754
8. B. Smith, W. YFcik, and D. Doss, "Ethical Hacking: The Security Justification," in Proceedings of the Ethics of Electronic Information in the 21 Cenlury Symposium (EE121). 2001
9. Aniruddha P Tekade et al., "Ethical Hacking in Linux Environment" in International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1854-1860
10. E.H**.** Spafford, **"**Are Computer Hacker Break-Ins Ethical?" in Journal of Systems Sofhvare, No 17, 1992, pp. 41 -47.
11. VMWare Software [Online] Retrieved on (2015 , Dec 10). Available: https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0