**1. INTRODUCTION**

* 1. **BACKGROUND**
     1. **Ethical Hacking**

Hacking is a process to bypass the security mechanisms of an information system or network. Hacking is used for the security strengthening purpose. First hacking was done at MIT, it were programming shortcuts. As every good side has a bad side, nowadays hacking is performed illegally to gain access to other system. Hacker is someone who maliciously breaks into systems for personal gain. In this world anything is hack able. But we can reduce the side effects of hacking with the help of ethical hackers. Hacking occurs due to weak securities of the system. As hacking is performed for illegal means, a new branch has been emerged ‘Ethical Hacking’. Ethical hacking is performed legally to gain access to other system to find out the security weaknesses. Ethical hacker is someone who gains access to the system with permission. He neither damages the target systems nor steals the information. He evaluates the systems security and report back to owners about the vulnerabilities found.

* + 1. **Linux**

Linux is one of a number of UNIX-like operating system variants based on the Linux kernel first written by Linus Torvalds. Linux started the true genesis of the open-source movement. Linux has evolved from being labeled as an unfriendly, unreliable operating system to a highly respected operating system that is user-friendly and capable of supporting many important applications. Linux is gaining more attention with its increasing popularity. It is favorite among the hackers.

There are a number of reasons why Linux has become the target of so many attacks. Firstly, Linux is an attractive target because it is so widely used on a large number of servers, making it a de facto backbone. Secondly, vulnerabilities are easier to find because the source code is freely available. Third, there are a large number of applications installed on Linux by default, making the system vulnerable. Unless system administrators are careful in setting policies and updating programs, security vulnerabilities can proliferate. Buffer overflows are a common cause of vulnerabilities. Some safety measures must be taken to guard the Linux operating system from being exploited due to known or unknown buffer overflows.

* + 1. **Type of Ethical Hackers**
       1. **White Hat Hacker**

A white hat hacker breaks security for non-malicious reasons, to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement.

* + - 1. **Black Hat Hacker**

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain". Black hat hackers form illegal hacking groups. Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network. Black hat hackers also are referred to as the "crackers" within the security industry and by modern programmers. Crackers keep the awareness of the vulnerabilities to themselves and do not notify the general public or manufacturer for patches to be applied. Individual freedom and accessibility is promoted over privacy and security. Once they have gained control over a system, they may apply patches or fixes to the system only to keep their reigning control.

* + 1. **Difference Between Hacker and a Cracker**

A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system. Most often, hackers are programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They may know of holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never, ever intentionally damage data. Hackers usually will hack into computers. Hackers believe in right to information. Hacking is the art of breaking into computer systems. Doesn’t matter if it's on the network or over the network it's still considered hacking.

A cracker is a person who breaks into or otherwise violates the system integrity of remote machines, with malicious intent. Crackers, having gained unauthorized access, destroy vital data, deny legitimate users service, or basically cause problems for their targets. Crackers can easily be identified because their actions are malicious. Crackers usually crack passwords. They are also the ones who crack software licenses etc. Cracking is the art of breaking software.[5]

**2. LITERATURE SURVEY**

Author Pranav s. Ambavkar and utile [1] have described WPA weaknesses . Wi-Fi device uses security authentication protocol even though they are having some weaknesses. Generally WEP (Wireless Encrypted Protocol) and WPA (Wi-Fi Protected Access) protocols are used for security purposes. It is already proved that WEP authentication protocol is a weak protocol. This paper includes the weaknesses of WPA and how to crack WPA.

WPA weaknesses such as weak passwords, WPS (Wi-Fi Protected Setup) pin recovery are included. Tools needed to exploit WPA are Blackbuntu operating system, TP Link Access point whose wireless network encrypted with a WPA passphrase, Network card that supports packet injection such as TP-Link TL-WN821N adapter with atheros chipset. WPA is cracked by using methods like Aircrack-ng against WPA, Aircrack-ng against WPA,Crack WPA/WPA2-PSK with John the Ripper,Cracking WPA Without a Dictionary (Aircrackng+ WordField),How to crack WPA/WPA2 without a dictionary using reaver.

Thus, this paper tells us that Weak passwords and WPS Pin are the main flaws in authentication. There are two types of dictionary attack aircrack-ng, johnthe-ripper if the password is weak and two types of Brute force attack wordfield and reaver if WPS PIN enabled router is in network. And we conclude that with strong passwords and by disabling WPS Pin WPA is not an easy target to hack.

Author Anil Kumar Singh [2] and utile has mentioned the security flaws of WEP. WEP is used to keep wireless connections secure from sniffing attacks. We know that it’s not very secure. It is a protocol for encrypting wirelessly transmitted packets on IEEE802.11networks. In a WEP protected network, all data packets are encrypted using the stream cipher RC4 under a common key, the root key. The root key is shared by all radio stations. A successful recovery of this Key gives an attacker full access to the network.

In this paper the security flaws of Wireless LAN by cracking 64 bit WEP key on Wi-Fi access points using Backtrack, a live Linux distribution is demonstrated. First there is an attack made on the Wi-Fi AP, making it generate packets for the cracking effort, finally cracking the WEP key successfully.

Author Muhammad Juwaini, Raed Alsaquor [3] and utilehas done a review on WEP. WEP is a wireless security protocol introduced and ratified by IEEE according to 802.11 standards. For the purpose of data broadcast encryption by telecommunication devices, RC4 (Rivest Cipher 4) stream cipher has been used as encryption engine in WEP protocol. RC4 is a stream cipher cryptographic engine used by WEP to encrypt wireless traffic. It was found by *Ron Rivest* of *RSA*1 in 1987. The main reason for RC4’s implementation in WEP is to increase its execution speed when using it in hardware.Also; its simplicity implementation over WEP makes it popular and widely used.

In WEP algorithm, a shared key used is 40-bit long with 24-bit long Initialization Vector (IV). For this initial phase, both are concatenated to 1RSA is an American computer and network security company. RSA was named after the initials of its cofounders,

Ron Rivest, Adi Shamir, and Len Adleman, after whom the RSA public key cryptography algorithm was also named produce a new 64-bit key. This new 64-bit key is used as a seed for Pseudo-Random Number Generator (PRNG). The key sequence generated by PRNG is used in the second phase, where plaintext that we want to broadcast is sent to integrity algorithm. The product of the integrity algorithm, Integrity Check Value (ICV), is compared with the previous plaintext. Afterward, key sequence generated by PRNG is sent to RC4 together with the ICV. The cipher text is generated by concatenating the IV with the product of RC4 encryption process.

It is a review paper on WEP. This paper reviews the history of WEP like how it was first cracked. It includes the weaknesses of WEP such as the short size of IV and its reuse, RC4 algorithm and easy forging of authentication messages.WEP improvements like using LSFR stream cipher and its alternatives like using WPA/WPA2 is suggested as it is not easy to crack it as WEP.

Author Ajinkya A. Farsole [4] and utile has written every basics about ethical hacking.Governments, companies, and private citizens around the world are anxious to be a part of the changing and fast growing world, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization‘s secrets to the open Internet. With these concerns and others, the ethical hacker comes into picture.

This paper encloses the epigrammatic disclosure about the. Hacking and as well the detailed role of the ethical hacking as the countermeasure to cracking in accordance with the corporate security as well as the individual refuge. This paper tries to develop the centralized idea of the ethical hacking and all its aspects as a whole.

This paper includes the history of hacking, what is hacking, a case study of an organization and its impacts, what is ethical hacking, need of hacking our own system, danger that the system faces when it is hacked, attacks like non-technical attacks,network-infrastructure attacks, operating system attacks and application attacks, process of ethical hacking, hacking tools like John the Ripper, security tools and controversy and future of ethical hacking.

**3. CRACKING 64 BIT WEP KEY**

The research was carried out to reveal WLAN Security

**Flaw:** Cracking 64 bit WEP Key.

The work was conducted at Department of Information Technology, Jagran Institute of Management, affiliated to GBT University, Uttar Pradesh. Details of materials used and the procedures employed are as follows:

One can design a scenario after understanding the theory of WEP cracking. Take the cracking software Back Track 3.0.

**Hardware Required:**

1. HCL Desktop,
2. Compaq Laptops, AP (D-Link 3200 Series Access Point)
3. Wireless card (D-Link DWA 510)

**Software Required:**

1. Operating System (Windows XP) and other application softwares.

A client is used to communicate with Access Point while User Datagram Protocol (UDP) flooding is used to send data. Another client is used to keep track of the network traffic as a hacker and listens to the WLAN. AP is linked to LAN with wires.

After booting with Back Track CD we open the console window and we find out the Wireless Network Interface Card (WNIC).

bt ~ # airmon-ng

MAC-Media Access Control address provided by the manufacturer at the time of manufacturing. It is a unique 48 bit, hexadecimal form, hardware address of WNIC. Change the MAC address of WNIC. Before changing the MAC address it should be noticed that WNIC should be down.

bt ~ # ifconfig wlan0 down

bt ~ #macchanger –mac 00:11:22:33:44:55 wlan0



**Fig3.1 showing the fake MAC address**

bt ~ #airmon-ng start wlan0

Find out the Access Point and their MAC addresses, Data, Channel, Speed in MB, Encryption, Cipher, Authentication and ESSID. We type the following command in console window.

bt ~ #airodump-ng wlan0

****

**Fig3.2 showing the MAC of AP, their Channel No. Speed, Encryption, Cipher and ESSID**

bt ~ # airodump-ng -c <channel No.> -w [pokemon] --bssid

<MAC address of the Access Point>

After execution of the above command, the output data which will be stored in the file pokemon; you can put any name of the file as you wish. This file will be offered for the WEP Crack program when we are ready to crack the WEP key. Open another shell and put down the previous command running.

Now we need to generate some fake packets to the access point to speed up the data output. Testthe access point by issuing the following command:

bt ~ #aireplay-ng -1 0 -a <MAC address of the AP> -h

<Fake MAC address of the WLAN> WLAN0

If the above command is successfully executed, then we will have to generate many packets on the target network so that we can crack the WEP Key.

bt ~ #aireplay-ng -3 -b <MAC address of the AP> -h <Fake

MAC address of the WLAN> WLAN0



**Fig3.3: showing the speed of capturing packets**

It will force the Access Point to send out a bunch of packets which we can then use to crack the WEP key.

After about capturing the 5000-10000 IVs We start cracking the WEP key by typing the following:

aireplay-ng -b <MAC address of the Access Point>

pokemon-01.cap .



**Fig3.4 showing the associated AP**

****

**Fig3.5 showing the attack with IVs**

****

**Fig3.6 showing the decrypted WEP key**

**4. CHROOTING**

# Chroot[6] a security measure in Linux that changes the root folder of a root process to one part of the system; with chrooting, the root process is restricted to one directory tree, which is called a chroot “jail”.

# If an attacker is able to successfully gain the root user privileges, then he or she will be able to do a lot of damage to the system. One way to at least limit the damage of an attack is chrooting. Chroot is a Linux security feature that enables a user to choose the directory that an application can access. This feature restricts access to the entire directory tree from unauthentic services and abuses of a process by an intruder. If the attacker is able to discover a vulnerability in a network service, he or she will be able to access the remote system and the file system. However, if the attacker is able to discover a local vulnerability, he or she will attempt to gain root access. Root has a lot of authority and many capabilities. Services running as root can be exploited to gain additional capabilities. The objective of most crackers is to gain root access on the compromised machine. Chrooting prevents this by limiting the privileges of a root process. The directory the process is limited to is known as the chroot “jail.”

# For example, assume that a program, testscript.exe, is restricted to a portion of the directory tree under /usr/local/tester. By chrooting a jail for testscript.exe, the process will be able to access files or directories within /usr/local/tester. If testscript.exe attempts to accesses the file /input.txt, it actually will access the file at /usr/local/tester/testscript/input.txt. If the administrator wants to run the program testscript.exe, he or she can chroot it before accessing it by issuing the command chroot /usr/local/tester/bin/testscript. This will first change the root to /usr/local/tester and then run the program /bin/testscript.

# 4.1 HISTORY

The chroot system call was introduced during development of Version 7 Unix in 1979, and added to BSD by Bill Joy on 18 March 1982 – 17 months before 4.2BSD was released – in order to test its installation and build system.

# 4.2 TOOL USED FOR CHROOT

# Tool: Addjailsw

# Addjailsaw is a tool that helps automate the creation of chroot jails. It copies commonly used debugging programs into the jail. It can also help in creating new users in the chroot jail. Similar programs are Cell and Zorp’s Jailer.

## 4.3 USES

A chroot environment can be used to create and host a separate virtualized copy of the software system. This can be useful for:

1. Testing and development

A test environment can be set up in the chroot for software that would otherwise be too risky to deploy on a production system.

1. Dependency control

Software can be developed, built and tested in a chroot populated only with its expected dependencies. This can prevent some kinds of linkage skew that can result from developers building projects with different sets of program libraries installed.

1. Compatibility

Legacy software or software using a different ABI (Application Binary Interface) must sometimes be run in a chroot because their supporting libraries or data files may otherwise clash in name or linkage with those of the host system.

1. Recovery

Should a system be rendered unbootable, a chroot can be used to move back into the damaged environment after bootstrapping from an alternate root file system (such as from installation media).

1. Privilege separation

Programs are allowed to carry open file descriptors (for files, pipelines and network connections) into the chroot, which can simplify jail design by making it unnecessary to leave working files inside the chroot directory. This also simplifies the common arrangement of running the potentially vulnerable parts of a privileged program in a sandbox, in order to pre-emptively contain a security breach. But chroot is not necessarily enough to contain a process with root privileges.

## 4.4 LIMITATIONS

The chroot mechanism is not intended to defend against intentional tampering by privileged (root) users. On most systems, chroot contexts do not stack properly and chrooted programs with sufficient privileges may perform a second root to break out. To mitigate the risk of this security weakness, chrooted programs should relinquish root privileges as soon as practical after chrooting, or other mechanisms – such as FreeBSD Jails - should be used instead.

At startup, programs expect to find scratch space, configuration files, device nodes and shared libraries at certain preset locations. For a chrooted program to successfully start, the chroot directory must be populated with a minimum set of the files. This can make chroot difficult to use as a general sandboxing mechanism.

Only the root user can perform a chroot. This is intended to prevent users from putting a setuid program inside a specially crafted chroot jail (for example, with a fake /etc/passwd and /etc/shadow file) that would fool it into a privilege escalation.

**5. DETAILED ANYALYSIS FOR GAINING ACCESS TO ANY ENCRYPTED WAN**

**5.1 Requirement**

1. Hacking Encrypted Wireless Network

2. Backtrack 5.0 installed hardware machine

3. System assembled with a Wi-Fi device or port

4. A Wi-Fi station

**5.2 Algorithm for proposed system**

This algorithm contains 3 basic steps-

1. Prepare a Wi-Fi device for an attack

2. Cracking WEP Encryption

3. Cracking WPA Encryption

**Step I Prepare the Wi-Fi device for an attack**

1. Start with a new terminal

2. Get access of the system in privileged mode―root‖

3. Check the status of the Wi-Fi device

4. If (Wi-Fi device = installed) Then –

a. Turn off the ―Monitor Mode‖ of W-Fi device

b. Change the mac address of the computer

c. Enable Monitor Mode of W-Fi device again

d. Prepare WI-Fi device for an attack

5. If (Wi-Fi device! = installed) Then

a. Configure a new Wi-Fi device

b. Repeat Step # 3

6. Halt with exiting the terminal

**Step II Crack WEP Encryption**

1. Log in a ―root‖ user.

2. Discover a target network to attack upon with airodump-ng.

3. Terminate the discovery once enough nereby n/w are traced

4. Capture the packets and ARPs on wireless network with airodump-ng

5. If (speed of capture is SLOW)

Use ―airoplay-ng -3 –b c‖ command.

6. If (Error = ―Waiting for becon frame‖)

Repeat from step # 4 and step # 5

7. Save the captured in a target folder

8. Decrypt the data using aircrack

9. Halt

**Step III Cracking WPA Encryption**

1. Log in a ―root‖ user.

2. Open a new terminal to check the Handshake

3. Capture the handshakes using airoplay

4. Disconnect all the clients in the network by airoplay

5. Generate a ―wordlists/wpa.txt‖

6. Brute force the password from wordlists/wpa.txt

7. If (COMPUTER DECRYPTION SUCCESSFUL)

a. Required KEY is achieved

b. Close the terminal

8. If (COMPUTER DECRYPTION SUCCESSFUL)

Repeat from step # 2 to step # 7

9. Halt

**5.3 Procedure for hacking Encrypted WAN**

1. **Preparing the Wi-Fi device for an attack**

Prepare wi-fi device for attack

Check Device Setup

Root Login

(Open Terminal1)

Go for Cracking WEP encryption

Failure

Halt this Step

(Close Terminal1)

Terminate

**Fig5.1 Preparing the Wi-Fi device for an attack**

1. Open the terminal and log in through the root user.
2. Check status of your Wi-Fi device by typing iwconfig command. We get list of all the Wi-Fi devices installed.
3. airmon-ng stop wlan0

This command disables the monitor mode of Wi-Fi device.

1. We must not use our real physical address, hence use macchanger –mac <proxy mac address>
2. Now use monitor enabling to have full control over device you want to configure by using airmon-ng start wlan0
3. **Cracking WEP Encryption**

Capture packets and ARP request

Use “airoplay –ng -3 –b c” command

Root Login

(Open Terminal2)

Yes

If (speed of capture is SLOW)

If (error waiting for Becon frame)

Discover Target Network

(Use airodumo –ng)

Yes

Terminate Discovery by Ctrl+c

No

Save packets and go for WPA Encryption crack

**Fig5.2 Cracking WEP Encryption**

1. First of all we need to select the target network to attack. Use ―airodump-ng start wlan0. This will show all the active station nereby. It also shows their mac addresses, total users, traffics etc.
2. Now hit ―Ctrl+C‖ to stop the discovery. Now,it‘s the time to capture some packets. Use followingcommand:

airodump-ng X c w <address where captured packets should be saved>

bssid <networkaddress> <devicename>

Here X is the network number enlisted in the output of the previous command. This will now capture all the data pakets.

1. Now open an new terminal and log in through root.

Use command airplay-g -3 –b <wirless bssid> -h <myFakeMacAddress> <devicename>

It is recommended to capture at least of 2000 packets.

1. **Cracking WEP Encryption**

Generate a “wordlists/wpa.txt”

Generate a “wordlists/wpa.txt”

Root Login

(Open Terminal3)

Brute force from “wordlists/wpa.txt”

Disconnect all the clients in Network

Handshake Checking (To check the ongoing communication)

No

If (DECRYPTION SUCCESSFUL)

Yes

Password Achieved

(Save and Exit)

**Fig5.3 Cracking WEP Encryption**

Let’s try to decrypt the captured date to find out the wireless network password.

1. In the other terminal press ls to enlist the data folders. Use wepcaptured 01.cap.

aircrack-ng –bssid <address o target> <path where captured data has been stored> wepcaptured 01.cap.

1. The computer now tries to decrypt the data and if successful will show the password. Now we have actually gained the access over the network.Furthermore we can manipulate as we wish.
2. For example if we want to disconnect all the clients connected, use:

airplay-ng -0 15 –a <your network device ID> <device name>

How actual handshaking is done is known on the other terminal and all the clients are being disconnected.

1. **FUTURE OF ETHICAL HACKING**

The future of the ethical hacking is huge and informative. The websites and internet networks are being secured now days in many e-businesses. As the customers are suspicious in trusting the organizations on behalf of their personal credit cards and information the organization professional are considering the future works. Recommendations also included for the future analysis of the ethical hacking. The information of the trusted customers and other users should be secured from the hackers and other attacks. The detection and prevention of the attacks of ethical hacking and its trend makes the future work efficient. The internet services and ethical hacking became an efficient problem in the security. It is very complex and risk in internet security where as ethical hacking needs the software professionals, developers, customers and administrators. Both of them need security for personal information. Ethical hacker is known as technical professional who employs the work to prevent present and future malicious from damaging and stealing the useful data and networks in computer. They make the computer network and the important information safe and secured. So they recommended with new techniques to prevent the upcoming harms for the computer network. Ethical hacking training and recommendations for the future work helps the hackers to implement the password cracking, firewalls, hacking tools, security tools and windows platform viruses with their spreading. This ethical hacking provides the business firms in achieving successful IT and developed corporate firm. It takes follows the future steps and guidelines to guarantee the security for the internet and data networks. It can benefit the firm market and protection from the ethical hackers. The launch of the denial of service dangers the internet results in fall down of the attackers.

It is always enticed to predict the future when it comes tocomputer security. Of course it‘s impossible to know for sure but it is possible to make an educated guess. They say we are in the –“the golden age of hacking” and we do not agree more. Tools for Linux are available. Hence we can hack it easily. Technology is growing strongly towards that direction. Exploiting code will slowly become more and more difficult and tools that focus on that will lose more and more of their effectiveness. Hackers will either focus on things like social engineering or gaining physical access.

1. **CONCLUSION**

The method of testing the system reliability by trying to damage is not new. From a practical standpoint the security problem will remain as long as manufacturers remain committed to current system architectures, produced without a firm requirement for security. Identification of vulnerabilities is useless without regular auditing, persistent intrusion detection, high-quality system administration practice, and computer security knowledge. A simple breakdown can expose an organization to cyber-attacks, loss of income or mind share, or even something worse. Every new technology has its advantages and its risks. Ethical hackers can only assist their clients in better understanding and identifying of their security needs, it is the responsibility of the clients who decide whether to address them or not. Using the results of penetration testing requires proper interpretation. Neither testers nor sponsors should assert that the penetration test has found all possible flaws, or that the failure to find flaws means that the system is secure. All types of testing can show only the presence of flaws and never the absence of them. The best that testers can say is that the specific flaws they looked for and failed to find aren‘t present; this can give some idea of the overall security of the system‘s design and implementation. Penetration testing is effective because it lets us consider a system as it‘s actually used, rather than as it‘s expected to be used. It‘s something to which all computer security everyone should be exposed.

1. **REFERENCES**

[1] WPA Exploitation in the World of Wireless Network

(International Journal of Advanced Research in Computer Engineering & Technology

Volume 1, Issue 4, June 2012

By Pranav S. Ambavkar, Pranit U. Patil, Dr.B.B.Meshram, and Prof. Pamu Kumar Swamy)

[2] WLAN Security Flaw: Cracking 64 bit WEP Key

(IJCSI International Journal of Computer Science Issues Vol. 7, Issue 6, November 2010

By Anil Kumar Singh, Bharat Mishra and Sandeep Singh)

[3] A Review on WEP Wireless Security Protocol

(Journal of Theoretical and Applied Information Technology 15 June 2012. Vol. 40 No.1

By Muhammad Juwaini, Raed Alsaquor, Maha Abdelhaq, OlaAlsukour)

[4] Ethical Hacking

(International Journal of Computer Applications 2010 Volume 1 – No. 10

By Ajinkya A. Farsole, Amruta G. Kashikar ,Apurva Zunzunwala)

[5] <http://www.pctools.com/security-news/crackers-and-hackers>

[6] <http://man7.org/linux/man-pages/man2/chroot.2.html>

[7] <http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPS_PIN_recovery>

[8]<https://sites.google.com/site/clickdeathsquad/Home/cds-wpacrack>

[9]<http://samiux.blogspot.in/2010/04/howto-crackwpawpa2-psk-with-john.html>

[10]<http://www.zer0trusion.com/2011/09/crackingwpa-without-dictionary.html>