Ethical Hacking: Scope and challenges in 21st century

Ranjini Mukhopadhyay*
Department of Computer Science
St. Xavier's College(Autonomous), Kolkata, India

Asoke Nath
Department of Computer Science
St. Xavier's College(Autonomous), Kolkata, India

Abstract— Data Hacking and data manipulation from any remote server is now a very known phenomena all over the globe. Because of this problem now a days people try to store data in a computer in encrypted manner so that the hackers may not be able to decrypt the data. If the data in a server available in non-encrypted manner then a hacker can very easily get into any unknown computer and can start to attack on it. End of 20th Century and the beginning of 21st century the people were only spreading virus through internet but now the hackers are smart enough to read all data from any distant computer and can control the computer from a remote computer. Imagine a situation when a hacker get access to some bank database and start to manipulate it. The result will be all bank transactions will be closed immediately through out the globe. In the present paper the authors will primarily find the means how an user can prevent his/her computer from any attack of any hacker. Ethical hacking and also known as penetration testing or white-hat hacking involves the same tools, tricks, and techniques that hackers use. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It is part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

Keywords— data hacking, bank database, ethical hacking, white hat hackers, black hat hackers.

I. INTRODUCTION

Ethical hacking encompasses formal and methodical penetration testing, white hat hacking, and vulnerability testing. It involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a malicious attacker's viewpoint to better secure systems. Ethical hacking is part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate. Ethical hacking is the process of entering into a hacker's mindset in order to spot system vulnerabilities by performing typical hacks in a controlled environment. It helps security professionals understand how malicious users think and work, enabling administrators to defend their systems against attacks and to identify security vulnerabilities. The term 'ethical hacker' refers to security professionals who apply their hacking skills for defensive purposes. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions.

A. Types of hackers in the present world:

(i)White Hat Hackers*: Hacks for finding out the loop holes in the security system.*
(ii)Black Hat Hackers*: Hacks for illegal or malicious purposes.*
(iii)Grey Hat Hackers*: Hacks sometimes legally and sometimes not but has no malicious intentions.*

B. Ethical hacking Phases:

The Ethical hacking process needs to be planned in advance. All technical, management and strategic issues must be considered. Planning is important for any amount of testing – from a simple password test to all out penetration test on a web application. Backup of data must be ensured, otherwise the testing may be called off unexpectedly if someone claims they never authorises for the tests. So, a well defined scope involves the following information:

1. Specific systems to be tested.
2. Risks that are involved.
3. Preparing schedule to carry test and overall timeline.
4. Gather and explore knowledge of the systems we have before testing.
5. What is done when a major vulnerability is discovered?
6. The specific deliverables- this includes security assessment reports and a higher level report outlining the general vulnerabilities to be addressed, along with counter measures that should be implemented when selecting systems to test, start with the most critical or vulnerable systems.

The overall hacking methodology consists of certain steps which are as follows:

Step-1: Reconnaissance
Step-2: Scanning
Step-3: Enumeration
Step-4: Gaining Access
Step-5: Maintaining Access
Step-6: Creating Tracks

Step-1: **Reconnaissance:-**The literal meaning of the Word reconnaissance is a preliminary survey to gain the information. This is also known as foot-printing. The hacker collects information about the company which the person is going to hack. Information as DNS servers, administrator contacts and IP ranges can be collected. During the reconnaissance phase different kind of tools can be used – network mapping, network and vulnerability scanning tools etc can be commonly used. Cheops for example is a very good network mapping tool which is able to generate networking graphs. They can be of great help later on during the attack phase or to get an overview about the network. A network mapping tool is very helpful when doing an internal ethical hack.

Step-2: **Scanning**:-The hacker tries to make a blue print of the target network. The blue print includes the IP addresses of the target network which are live, the services which are running on those systems and so on. Modern port scanning uses TCP protocol to do scanning and they could even detect the operating systems running on the particular hosts.

Step-3: **Enumeration**:- Enumeration is the ability of a hacker to convince some servers to give them information that is vital to them to make an attack. By doing this the hacker aims to find what resources and shares can be found in the system, what valid user account and user groups are there in the network, what applications will be there etc.

Step-4: **Gaining Access**:- This is the actual hacking phase in which the hacker gains access to the system. The hacker will make use of all the information he collected in the pre-attacking phase. Usually the main hindrance to gaining access to a system is the passwords. In the System hacking, first the hacker will try to get in to the system.

Step-5: **Maintaining Access**:- Now the hacker is inside the system . This means that he is now in a position to upload some files and download some of them. The next aim will be to make an easier path to get in when he comes the next time. This is analogous to making a small hidden door in the building so that he can directly enter in to the building through the door easily.

Step-6: **Clearing Tracks**:- Here the hacker eliminates the physical evidence of his/her hacking the system. Whenever a hacker downloads some file or installs some software, its log will be stored in the server logs. So in order to erase the hacker uses man tools. One such tool is windows resource kit's auditpol.exe. Another tool which eliminates any physical evidence is the evidence eliminator. The Evidence Eliminator deletes all such evidences.

Some Advantages of Ethical Hacking:

1. To help in detection of crimes done through internet.
2. Provides security to banking and financial establishments.
3. It can help to detect and also to prevent cyber terrorism.
4. Everything here depends upon the trustworthiness of the ethical hacker.

Hacktivism

Hacktivism refers to 'hacking with / for a cause'. It comprises of hackers with a social or political agenda. It aims at sending across a message through their hacking activity and gaining visibility for their cause and themselves.

Ethical hackers tries to answer:

- What can the intruder see on the target system?
    - ➢ Reconnaissance and Scanning phase of hacking
- What can an intruder do with that information?
    - ➢ Gaining Access and Maintaining Access phases
- Does anyone at the target notice the intruders attempt or success?
    - ➢ Reconnaissance and Covering Tracks phases.

If hired by any organization, an ethical hacker asks the organization what it is trying to protect, against whom and what resources it is willing to expend in order to gain protection.

This document is a template. An electronic copy can be downloaded from the Journal website. For questions on paper guidelines, please contact the journal publications committee as indicated on the journal website. Information about final paper submission is available from the conference website.

II. SKILL PROFILE OF AN ETHICAL HACKER

1. Computer expert adept at technical domains.
2. In-depth knowledge about target platforms (such as windows, Unix, Linux).
3. Exemplary knowledge in networking and related hardware / software.
4. Knowledgeable about security areas and related issues – though not necessarily a security professional.

A. How do an Ethical Hacker go about it?

Any security evaluation involves three components:

1. Preparation – In this phase, a formal contract is signed that contains a non-disclosure clause as well as a legal clause to protect the ethical hacker against any prosecution that he may attract during the conduct phase. The contract also outlines infrastructure perimeter, evaluation activities, time schedules and resources available to him.
2. Conduct – In this phase, the evaluation technical report is prepared based on testing potential vulnerabilities.

3. Conclusion – In this phase, the results of the evaluation is communicated to the organization / sponsors and corrective advise / action is taken if needed.

B. Modes of Ethical Hacking

1) Remote network – This mode attempts to simulate an intruder launch an attack over the Internet.
2) Remote dial-up network - This mode attempts to simulate an intruder launching an attack against the client's modem pools.
3) Local network – This mode simulates an employee with legal access gaining unauthorized access over the local network.
4) Stolen equipment – This mode simulates theft of a critical information resource such as a laptop owned by a strategist, (taken by the client unaware of its owner and given to the ethical hacker).
5) Social engineering – This aspect attempts to check the integrity of the organization's employees.
6) Physical entry – This mode attempts to physically compromise the organization's ICT infrastructure.

III. Recent Trends in Ethical Hacking

The word hacker in the past was defined as a person who loves playing around with software or electronic systems. They wanted to discover new things on how computers operate. Today the term hacker has a different meaning altogether. It states that a hacker is "someone who maliciously breaks into systems for personal gain. Technically, these criminals are crackers (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable". (Kevin Beaver, Stuart McClure 2004, Hacking For Dummies)

"The history of hacking dates back to the 1960s when a group of people in MIT "hack the control systems of model trains to make them run faster, more effectively or differently than they were designed to". (Peter T. Leeson, Christopher J. Coyne, 2006, The Economics of Computer Hacking). Because of such activity by these individuals computer owners and supervisors took away their access to computers. As a result the hacking community came up with their own code known as the hacker ethic:

"1. Access to computers –and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!

2. All information should be free.

3. Mistrust Authority – Promote Decentralization.

4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position.

5. You can create art and beauty in a computer.

6. Computers can change your life for the better. " (Paul A Taylor, 2005,From Hackers to Hacktivists: Speed Bumps on the Global Superhighway)

The above code is still followed today and not only by hackers but by others as well.

Not all hackers today have the same level of expertise. Depending on the psychology and skills of a hacker they can be put into four groups.(M.G. Siriam, The Modus Operandi of Hacking) Old School Hackers is one group and they believe that the internet should be an open system. Script kiddies are another and they are computer novices that use tools created by professional hackers to hack systems. Most of the hackers today fit into this group. The next group is professional criminals or crackers. They break into systems for the purpose of stealing and selling information they gathered.. The final group is coders and virus writers. They are elite individuals with a very high skill in programming and operating systems that write code and use other people in charge of releasing their code to the wild.

Organizations and institutions today are under a lot of stress to protect their information from external as well as internal security threats to their computer systems. As such most of them have come up with the solution of hiring Ethical Hackers. "To catch a thief, you must think like a thief. That's the basis for ethical hacking. Knowing your enemy is absolutely critical" (Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies). In other wards Ethical hackers (white-hat hackers) are experienced security and network experts that perform an attack on a target system with permission from the owners, to find loop holes and vulnerabilities that other hackers could exploit. This process is also known has Red Teaming, Penetration Testing or Intrusion Testing. (www.networkdictionary.com) The end goal of ethical hackers is to learn system vulnerabilities so that they can be repaired for community self-interest and as a side-product also the common good of the people.(Bryan Smith, William Yurcik, David Doss, 2002, Ethical Hacking: The Security Justification)

Every Ethical hacker should follow three important rules as follows: Firstly Working Ethically. All actions performed by the ethical hacker should support the organizations goals that he works for. "Trustworthiness is the ultimate tenet. The misuse of information is absolutely forbidden." Secondly Respecting Privacy as all information that an ethical hacker gathers has to be treated with the utmost respect, "finally not crashing your systems". This is mostly due to no prior planning or having not read the documentation or even misusing the usage and power of the security tools at their disposal. (Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies)

The main attacks or methods that an ethical hackers or even hackers perform are of as follows:

Non Technical Attacks: No matter how secured an organization is in terms of software and hardware, it will always be vulnerable to security threats because security's weakest link are people or its employees.

Social engineering is a type of non technical attack where hackers "exploit the trusting nature of human beings to gain information for malicious purposes". Other attacks can be of physical nature such as stealing hardware equipment or dumpster diving.

Operating-System Attack: Hacking an operating system (OS) is a preferred method of the bad guys. OS attacks make up a large portion of hacker attacks simply because every computer has an operating system and OS(s) are susceptible to many well-known exploits.(Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies)

Distributed denial of service attacks(DDoS): This is the most popular attack used by many hackers to bring down systems. It's a type of attack that overloads the network or server with a large amount of traffic so that it crashes and renders any access to the service.

Internet Protocol (IP) spoofing: "It is a way of disguising the hacker's real identity. This method allows a hacker to gain unauthorized access to computers by sending a message to a computer with an IP address showing that the message is from a trusted host. To accomplish this, a hacker must use different tools to find an IP address of a trusted host, and then alter the packet headers so it appears that the packets are coming from the host." (Tanase 2003, IP Spoofing: An Introduction).

The process of ethical hacking contains many different steps. The first thing that is done is to formulate a plan. At this stage getting approval and authorization from the organization to perform the penetration test is extremely important. (Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies). Next the ethical hacker uses scanning tools to perform port scans to check for open ports on the system. "Once a cracker scans all computers on a network and creates a network map showing what computers are running what operating systems and what services are available, almost any kind of attack is possible" (Bryan Smith, William Yurcik, David Doss, 2002, Ethical Hacking: The Security Justification) This method is used by hackers as well but for mainly for malicious purposes. After scanning has been done the ethical hacker selects the tools that are going to be used to perform certain tests on the target system. These tools can be used for password cracking, planting backdoors, SQL injection, sniffing etc. The tests need to be carefully performed because if they are done incorrectly they could damage the system and could go unnoticed. (Bryan Smith, William Yurcik, David Doss, 2002, Ethical Hacking: The Security Justification) Finally the plan needs to be executed and the results of all the tests then need to be evaluated (Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies) Based on the results the ethical hacker tells the organization about their security vulnerabilities as well as how they can be patched to make it more secure.

A grey hat hacker is a type of hacker that has the skills and intent of a ethical hacker in most situations but uses his knowledge for less than noble purposes on occasion. Grey hat hackers typically subscribe to another form of the hacker ethic, which says it is acceptable to break into systems as long as the hacker does not commit theft or breach confidentiality. Some would argue, however that the act of breaking into a system is in itself unethical.(Red Hat, Inc, 2002) Grey hats are also a form of good hackers that usually hack into organizations systems without their permission, but then at a later stage send them information on the loop holes in their system. They also sometimes threaten to release the holes they find unless action has been taken to fix it. (Peter T. Leeson, Christopher J. Coyne, 2006, The Economics of Computer Hacking).

Nowadays ethical hacking is not only bounded in computers but it has spread its arms in the world of electronic goods such as mobile phones, ipads etc. Today we live in an age where MMS crimes and SIM card cloning has almost become a part of our daily routine. It has become extremely important for every mobile phone user to be educated and prepared for various possible known and unknown loopholes, vulnerabilities and attacks. For individuals, their mobile phones contain private photographs and personal messages, while for businessmen, their mobile phone is equivalent to their office desk containing sensitive e-mails, proposals, faxes and other intellectual property. In both cases, it has become very important to take necessary precautions to fight the malicious attackers. (Ankit Fadia, 2005, An Ethical Guide To Hacking Mobile Phones)

IV. ATTACKS USING DIFFERENT HACKING TOOLS : COUNTER MEASURES TAKEN BY AN ETHICAL HACKER

A. Pre Attack Phases

1)Footprinting one of the pre-attack phases is the blueprinting of the security profile of an organization, undertaken in a methodological manner.

Information Sources used in Footprinting

1) Who is: Who is can reveal public information of a domain that can be leveraged further.
2) ARIN (American Registry of Internet Numbers): ARIN allows search on the whois database to locate information on networks autonomous system numbers (ASNs), network-related handles and other related point of contact (POC).
3) Traceroute: Traceroute reveals the path IP packets travel between two systems by sending out consecutive UDP packets with ever-increasing Time To Lives .
4) Nslookup: Nslookup is a program to query Internet domain name servers. Displays information that can be used to diagnose Domain Name System (DNS) infrastructure.

Hacking Tool

1) Sam Spade:Sam Spade is a comprehensive network investigation tool which acts as a sleuth that finds as much public information about an IP address or DNS address.

2) NeoTrace: NeoTrace shows the traceroute output visually – map view, node view and IP view
3) VisualRoute:VisualRoute is a graphical tool that determines where and how traffic is flowing on the route between the desired destination and the user trying to access it, by providing a geographical map of the route, and the performance on each portion of that route.
4) VisualLookout:VisualLookout provides high level views as well as detailed and historical views that provide traffic information in real-time or on a historical basis.
5) eMailTrackerPro:eMailTrackerPro is the e-mail analysis tool that enables analysis of an e-mail and its headers automatically and provides graphical results.
6) Mail Tracking:Mail Tracking is a tracking service that allows the user to track when his mail was read, for how long and how many times. It also records forwards and passing of sensitive information.

2)Scanning is a method adopted by administrators and crackers to discover more about a network.

- There are various scan types - SYN, FIN, Connect, ACK, RPC, Inverse Mapping, FTP Bounce, Idle Host etc. The use of a particular scan type depends on the objective at hand.

B. Enumeration

1) NAT: The NetBIOS Auditing Tool (NAT) is designed to explore the NetBIOS file-sharing services offered by the target system.
2) Enum: Available for download from http://razor.bindview.com. Enum is a console-based Win32 information enumeration utility. Enum is also capable of rudimentary brute force dictionary attack on individual accounts.

System Hacking

A system can be hacked by cracking the password, getting access to local administrator group etc.

Hacking tool

1) KerbCrack: KerbCrack consists of two programs, kerbsniff and kerbcrack. The sniffer listens on the network and captures Windows 2000/XP Kerberos logins. The cracker can be used to find the passwords from the capture file using a bruteforce attack or a dictionary attack.
2) GetAdmin: GetAdmin.exe is a small program that adds a user to the local administrators group.
3) John the Ripper: It is a command line tool designed to crack both Unix and NT passwords. John is extremely fast and free.
4) Spector: Spector is a spy ware and it will record everything anyone does on the internet.
5) eBlaster: eBlaster lets you know EXACTLY what your surveillance targets are doing on the internet even if you are thousands of miles away.

Password Cracking Countermeasures

1. Enforce 7-12 character alpha-numeric passwords.
2. Set the password change policy to 30 days.

Spector Countermeasures

Anti Spector (www.antispector.de): This tool will detect Spector and delete them from your system.

Covering tracks

Hacking Tools

1) elsave.exe:elsave.exe utility is a simple tool for clearing the event log. The following syntax will clear the security log on the remote server 'rovil' (correct privileges are required on the remote system)
2) WinZapper: Wizapper is a tool that an attacker can use to erase event records selectively from the security log in Windows 2000.
3) Evidence Eliminator: Evidence Eliminator is an easy to use powerful and flexible data cleansing system for Windows PC.

WEB SERVER Hacking

Nature of Security Threats in a Web Server Environment are as follows:

- Bugs or Web Server Misconfiguration.
- Browser-Side or Client Side Risks.
- Sniffing
- Denial of Service Attack.

Countermeasures to web server hacking

1) cacls.exe utility: Built-in Windows 2000 utility (cacls.exe) can set access control list (ACLs) permissions globally.
2) Whisker: Whisker is an automated vulnerability scanning software which scans for the presence of exploitable files on remote Web servers.
3) Stealth HTTP Scanner: N-Stealth 5 is an impressive Web vulnerability scanner that scans over 18000 HTTP security issues.
4) WebInspect: WebInspect is an impressive Web server and application-level vulnerability scanner which scans over 1500 known attacks.
5) Shadow Security Scanner: Security scanner is designed to identify known and unknown vulnerabilities, suggest fixes to identified vulnerabilities, and report possible security holes within a network's internet, intranet and

extranet environments. Shadow Security Scanner includes vulnerability auditing modules for many systems and services.

6) IISLockdown: IISLockdown restricts anonymous access to system utilities as well as the ability to write to Web content directories.

V. Results and Discussions

A live Demo of Password Hacking

Software used: John The Ripper

Input: username and password hash generated by Username:Password Creator for HTPASSWD got from sherylcanter.com/encrypt.php

Working:The website sherylcanter.com/encrypt.php produces the hashes of username and password in two of the following forms

1.)DES-encrypted username:password entry

2.)md5-encrypted username:password entry

Using any one of this hashes produced we create a hash file. The hash file on being executed by John The Ripper gives us the password.

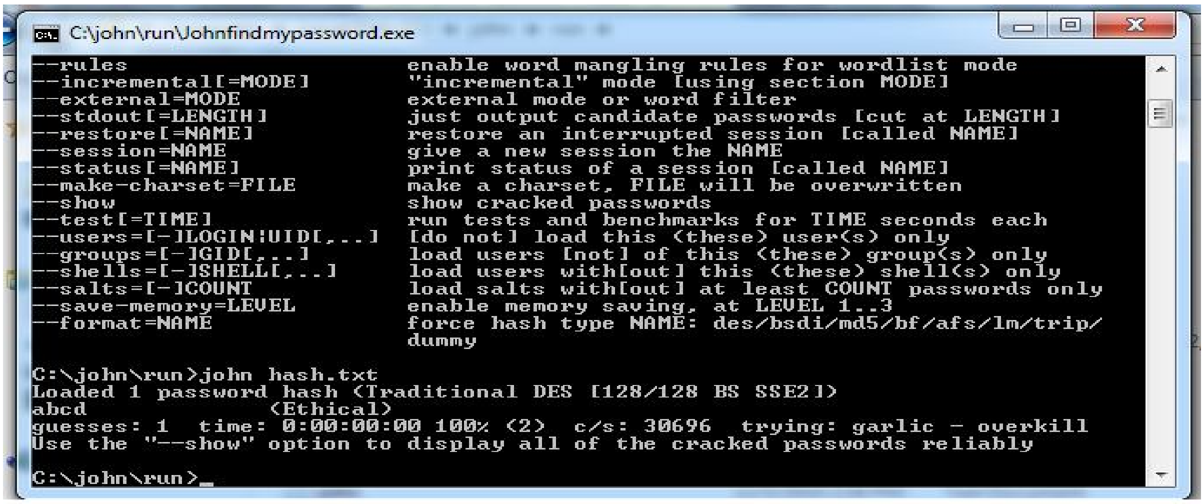
Output: Matched Password for the given username and hashed password.

Set 1

Username: Ethical

Password: abcd

Time to Break: 1 second



```
--rules                   enable word mangling rules for wordlist mode
--incremental[=MODE]      "incremental" mode [using section MODE]
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT          load salts with[out] at least COUNT passwords only
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--format=NAME             force hash type NAME: des/bsdi/md5/bf/afs/lm/trip/
                          dummy

C:\john\run>john hash.txt
Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
abcd             (Ethical)
guesses: 1  time: 0:00:00:00 100% (2)  c/s: 30696  trying: garlic - overkill
Use the "--show" option to display all of the cracked passwords reliably

C:\john\run>_
```

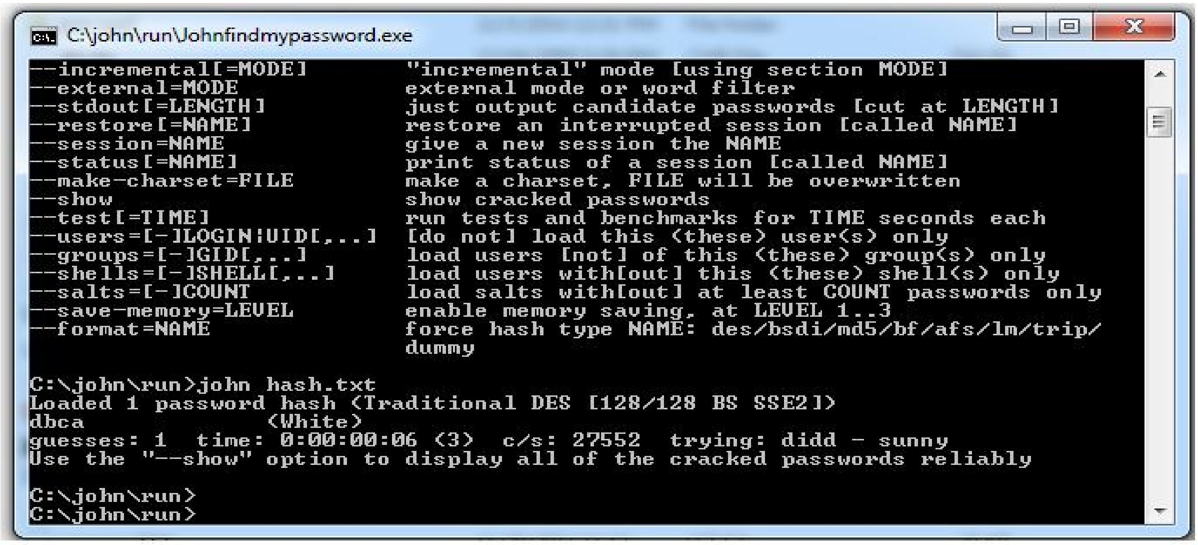
Snapshot of Set 1

Set 2

Username: White

Password: dbca

Time to Break: 6 seconds

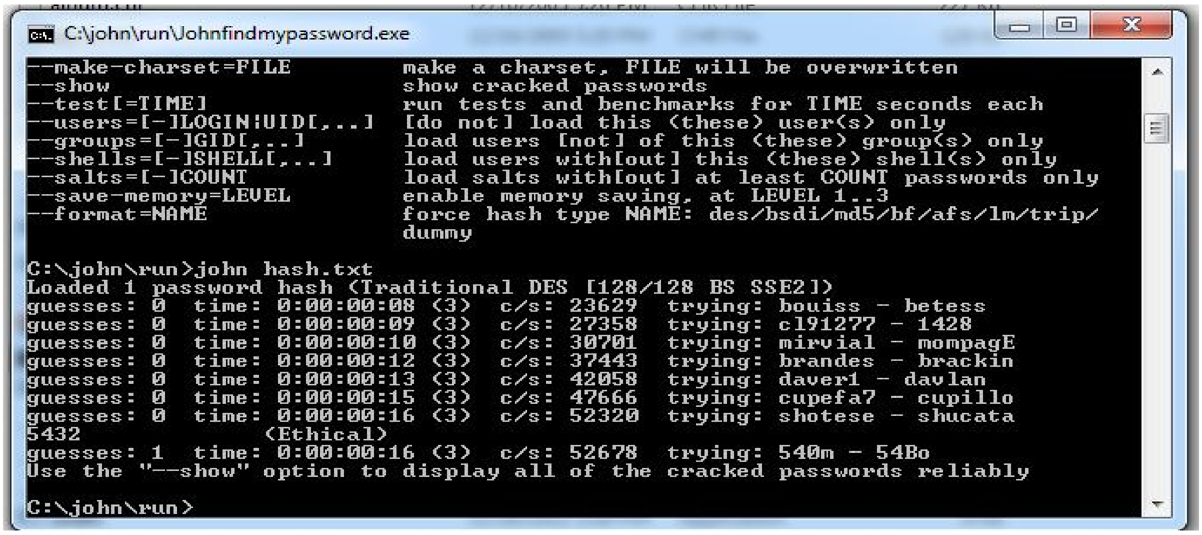


```
--incremental[=MODE]      "incremental" mode [using section MODE]
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT          load salts with[out] at least COUNT passwords only
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--format=NAME             force hash type NAME: des/bsdi/md5/bf/afs/lm/trip/
                          dummy

C:\john\run>john hash.txt
Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
dbca             (White)
guesses: 1  time: 0:00:00:06 (3)  c/s: 27552  trying: didd - sunny
Use the "--show" option to display all of the cracked passwords reliably

C:\john\run>
C:\john\run>
```

Snapshot of Set2

<u>Set 3</u>

Username: Ethical
Password: 5432
Time to Break: 16 seconds

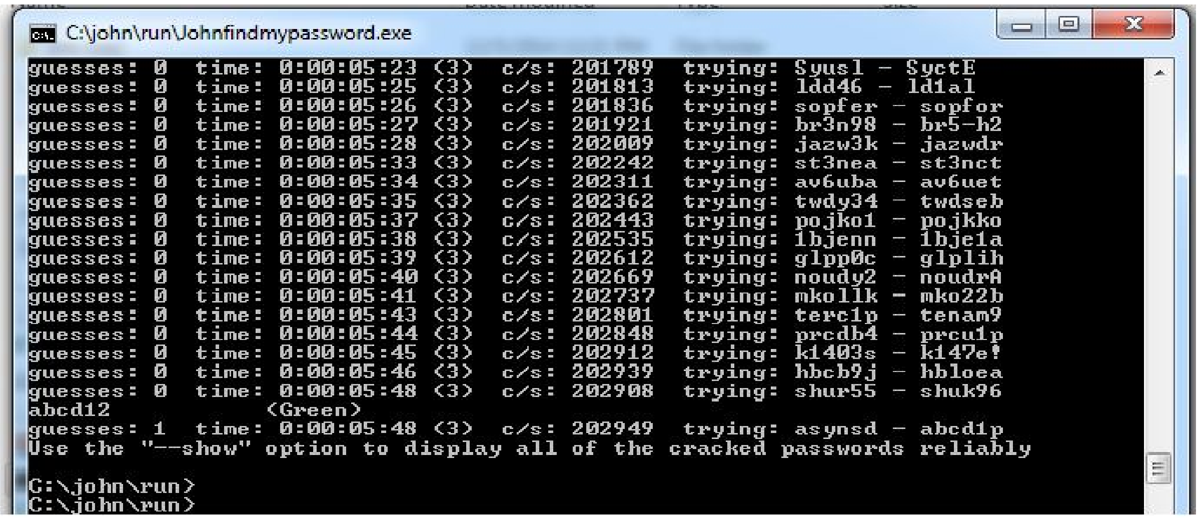


```
--make-charset=FILE        make a charset, FILE will be overwritten
--show                     show cracked passwords
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this (these) shell(s) only
--salts=[-]COUNT           load salts with[out] at least COUNT passwords only
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--format=NAME              force hash type NAME: des/bsdi/md5/bf/afs/lm/trip/
                           dummy

C:\john\run>john hash.txt
Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
guesses: 0  time: 0:00:00:08 (3)  c/s: 23629  trying: bouiss - betess
guesses: 0  time: 0:00:00:09 (3)  c/s: 27358  trying: c191277 - 1428
guesses: 0  time: 0:00:00:10 (3)  c/s: 30701  trying: mirvial - mompagE
guesses: 0  time: 0:00:00:12 (3)  c/s: 37443  trying: brandes - brackin
guesses: 0  time: 0:00:00:13 (3)  c/s: 42058  trying: daver1 - davlan
guesses: 0  time: 0:00:00:15 (3)  c/s: 47666  trying: cupefa7 - cupillo
guesses: 0  time: 0:00:00:16 (3)  c/s: 52320  trying: shotese - shucata
5432             (Ethical)
guesses: 1  time: 0:00:00:16 (3)  c/s: 52678  trying: 540m - 54Bo
Use the "--show" option to display all of the cracked passwords reliably

C:\john\run>
```

Snapshot of Set 3

<u>Set 4</u>

Username: Green
Password: abcd12
Time to Break: 5minutes 48 seconds



```
guesses: 0  time: 0:00:05:23 (3)  c/s: 201789  trying: Syusl - SyctE
guesses: 0  time: 0:00:05:25 (3)  c/s: 201813  trying: ldd46 - ld1al
guesses: 0  time: 0:00:05:26 (3)  c/s: 201836  trying: sopfer - sopfor
guesses: 0  time: 0:00:05:27 (3)  c/s: 201921  trying: br3n98 - br5-h2
guesses: 0  time: 0:00:05:28 (3)  c/s: 202009  trying: jazw3k - jazwdr
guesses: 0  time: 0:00:05:33 (3)  c/s: 202242  trying: st3nea - st3nct
guesses: 0  time: 0:00:05:34 (3)  c/s: 202311  trying: av6uba - av6uet
guesses: 0  time: 0:00:05:35 (3)  c/s: 202362  trying: twdy34 - twdseb
guesses: 0  time: 0:00:05:37 (3)  c/s: 202443  trying: pojko1 - pojkko
guesses: 0  time: 0:00:05:38 (3)  c/s: 202535  trying: 1bjenn - 1bje1a
guesses: 0  time: 0:00:05:39 (3)  c/s: 202612  trying: glpp0c - glplih
guesses: 0  time: 0:00:05:40 (3)  c/s: 202669  trying: noudy2 - noudrA
guesses: 0  time: 0:00:05:41 (3)  c/s: 202737  trying: mkollk - mko22b
guesses: 0  time: 0:00:05:43 (3)  c/s: 202801  trying: terc1p - tenam9
guesses: 0  time: 0:00:05:44 (3)  c/s: 202848  trying: prcdb4 - prcu1p
guesses: 0  time: 0:00:05:45 (3)  c/s: 202912  trying: k1403s - k147e!
guesses: 0  time: 0:00:05:46 (3)  c/s: 202939  trying: hbcb9j - hbloea
guesses: 0  time: 0:00:05:48 (3)  c/s: 202908  trying: shur55 - shuk96
abcd12           (Green)
guesses: 1  time: 0:00:05:48 (3)  c/s: 202949  trying: asynsd - abcd1p
Use the "--show" option to display all of the cracked passwords reliably

C:\john\run>
C:\john\run>
```

Snapshot of Set 4

It is very much essential to make sure that we are using the right tool for ethical hacking process. It is important to know the personal as well as the technical limitations. Many tools focus on specific tests, but no one tool can test for everything. The more tools mean it will be easy for ethical hacking. The user has to make sure that the user is using the **right tool for the task**. For example, to crack passwords, one can use a cracking tool such as LC4 or John the Ripper.

There are various characteristics for the use of tools for ethical hacking which are as follows:

1. Adequate documentation
2. Detailed reports on the discovered vulnerabilities, including how they can be fixed
3. Updates and support when needed
4. High level reports that can be presented to managers

These features can save the time and effort when we are writing the report. Time and patience are important in ethical hacking process. We should be careful when we are performing the ethical hacking tests. It is not practical to make sure that no hackers are on our system. Just make sure to keep everything private if possible. People need to encrypt the emails and files if possible.

VI. CONCLUSION

This paper addressed ethical hacking from several perspectives. Ethical hacking seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. But, with the present poor security on the internet, ethical hacking may be the most effective way to plug security holes and prevent intrusions. On the other hand ethical hacking tools have also been notorious tools for crackers. So, at present the tactical objective is to stay one step ahead of the crackers. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. After all, ethical hacking will play a certain role in the security assessment offerings and certainly has earned its place among other security assessments. In conclusion, it must be said that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole. In an effort to accomplish this, let us welcome the Ethical Hacker into our ranks as a partner in this quest.

The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time will come when all computer systems are hacked or compromised in some way. Protecting your systems from the bad guys and not just the generic vulnerabilities that everyone knows about is absolutely critical. When people know hacker tricks, he/she can see how vulnerable their systems are.

Hacking preys on weak security practices and undisclosed vulnerabilities. Firewalls, encryption, and virtual private networks (VPNs) can create a false feeling of safety. These security systems often focus on high-level vulnerabilities, such as viruses and traffic through a firewall, without affecting how hackers work. Attacking one's own systems to discover vulnerabilities is a step to making them more secure. This is the only proven method of greatly hardening one's systems from attack. If people don't identify weaknesses, it's a matter of time before the vulnerabilities are exploited.

As hackers expand their knowledge, so should people. They must think like them to protect their systems from them. Author, as the ethical hacker, must know activities hackers carry out and how to stop their efforts. We should know what to look for and how to use that information to thwart hackers' efforts.

But one should not take ethical hacking too far, though. It makes little sense to harden our systems from unlikely attacks. For instance, if a user does not have a lot of foot traffic in the office and no internal Web server running, the user may not have as much to worry about as an Internet hosting provider would have.

The Author's overall goals as an ethical hacker should be as follows:

- ➢ Hack the systems in a non-destructive fashion.
- ➢ Enumerate vulnerabilities and, if necessary, prove to upper management that vulnerabilities exist.
- ➢ Apply results to remove vulnerabilities and better secure our systems.

ACKNOWLEDGMENT

The authors are very much grateful to Prof. Shalabh Agarwal, Head, Department of Computer Science for giving us inspiration to complete this work. One of the authors AN express his sincere gratitude to Fr. Dr. John Felix Raj, Principal, St. Xavier's College(Autonomous), Kolkata for giving constant support to do research work in filed of Computer Science and Engineering.

REFERENCES

[1] Software Hacking :: Ankit Fadia, Nishant Das Patnaik
[2] An Ehtical Hacking guide to corporate Security :: Ankit Fadia
[3] An Ehtical Guide to Hacking Mobile Phones :: Ankit Fadia
[4] Hacking For Dummies :: Kevin Beaver, Stuart McClure 2004
[5] The Economics of Computer Hacking :: Peter T. Leeson, Christopher J. Coyne, 2006
[6] From Hackers to Hacktivists : Speed Bumps on the Global Superhighway ::Paul A Taylor, 2005
[7] The Modus Operandi of Hacking :: M.G. Siriam
[8] Ethical Hacking: The Security Justification :: Bryan Smith, William Yurcik, David Doss, 2002
[9] IP Spoofing: An Introduction :: Matthew Tanase 2003