ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 10, pp. 20833-20839, October, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

A FUTURE, SCOPE, VISION AND CHALLENGES OF HACKING IN THE FIELD OF CYBER AND FORENSICS IN THE 21ST CENTURY

Lakshmi I and Sarjanaa Subramanian

Department of Computer Science, Stella Maris College, Chennai-600086
Tamil Nadu, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0810.0968

ARTICLE INFO

Article History:

Received 16th July, 2017
Received in revised form 25th August, 2017
Accepted 23rd September, 2017
Published online 28th October, 2017

Key Words:

Data hacking, bank database, ethical hacking, white hat hackers, black hat hackers

ABSTRACT

Information Hacking Furthermore information control from whatever remote server will be notwithstanding a referred to phenomena throughout those globe. Due to this issue currently a day's people attempt with store information Previously, a workstation done encrypted way thus that those hackers might not have the ability on unscramble the information. Whether the information Previously, An server accessible in non-encrypted way after that a hacker cam wood thick, as undoubtedly get under whatever obscure machine Furthermore could start should strike on it. Limit for twentieth century and the start about 21st century the individuals were just spreading infection through web At Notwithstanding those hackers are keen enough should perused all information starting with whatever inaccessible PC and cam wood control those machine from An remote workstation. Envision An circumstance At a hacker get entry will a few bank database Also begin will control it. The come about will be all bank transactions will make shut instantly for those globe. In the available paper those writers will principally Figure those implies how an client might prevent his/her workstation starting with any ambush from claiming whatever hacker. Moral hacking Furthermore otherwise called infiltration testing alternately white-hat hacking includes those same tools, tricks, Also strategies that hackers utilize. Moral hacking is performed for the target's consent. Those expectation for moral hacking may be should uncover vulnerabilities from a hacker's viewpoint thus frameworks might a chance to be superior secured. It may be and only an generally majority of the data danger administration system that considers progressing security upgrades. Moral hacking could likewise guarantee that vendors' cases something like the security from claiming their results need aid real.

INTRODUCTION

Moral hacking includes formal What's more deliberate infiltration testing, white cap hacking, What's more defencelessness testing. It includes the same tools, tricks, and strategies that hackers use, Be that as with you quit offering on that one major difference: moral hacking will be performed for those target's consent. Those expectations from claiming moral hacking may be should find vulnerabilities from a pernicious attacker's viewpoint will exceptional secure frameworks. Moral hacking is and only an Generally speaking majority of the data Hazard administration system that considers continuous security upgrades. Moral hacking might additionally guarantee that vendors' asserts regarding those security from claiming their items need aid real. Moral hacking may be the methodology for entering under a hacker's outlook so as with spot framework vulnerabilities Toward performing average hacks Previously, a controlled earth. It aides security experts comprehend how pernicious clients feel and work, empowering managers will guard their frameworks against strike and should distinguish security vulnerabilities. Those haul 'ethical hacker' alludes will security experts who apply their hacking aptitudes to protective purposes. Moral hacking depicts the procedure for hacking a organize done an moral way, Along these lines with handy intentions.

Types of hackers in the present world

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

Corresponding author:* **Lakshmi I
Department of Computer Science, Stella Maris College, Chennai-600086 Tamil Nadu, India

Ethical hacking Phases

The Ethical hacking process should be arranged ahead of time. All specialized, administration and vital issues must be considered. Arranging is imperative for any measure of testing -from a straightforward secret word test to full scale entrance test on a web application. Reinforcement of information must be guaranteed, generally the testing might be cancelled out of the blue in the event that somebody claims they never approves for the tests. Thus, a very much characterized scope includes the accompanying data:

1. Particular frameworks to be tried.
2. Dangers those are included.
3. Getting ready calendar to convey test and general timetable.
4. Accumulate and investigate learning of the frameworks we have before testing.
5. What is done when a noteworthy powerlessness is found?
6. The particular expectations this incorporates security evaluation reports and a more elevated amount report delineating the general vulnerabilities to be tended to, alongside counter measures that ought to be actualized while choosing frameworks to test, begin with the most basic or defenceless frameworks.

The general hacking system comprises of specific advances which are as per the following:

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

Step-1

Surveillance:- The exacting significance of the Word observation is a preparatory study to pick up the data. This is otherwise called foot-printing. The programmer gathers data about the organization which the individual will hack. Data as DNS servers, executive contacts and IP extents can be gathered. Amid the observation stage distinctive sort of apparatuses can be utilized-arrange mapping, system and weakness checking devices and so forth can be generally utilized. Cheops for instance is a decent system mapping device which can create organizing charts. They can be of awesome help later on amid the assault stage or to get an outline about the system. A system mapping device is exceptionally useful while doing an inside moral hack.

Step-2

Examining: - The programmer tries to influence a blue print of the objective to organize. The blue print incorporates the IP locations of the objective system which are live, the administrations which are running on those frameworks et cetera. Current port filtering utilizes TCP convention to do checking and they could even recognize the working frameworks running on the specific hosts.

Step-3

List: - Enumeration is the capacity of a programmer to persuade a few servers to give them data that is essential to them to make an assault. By doing this the programmer expects to discover what assets and offers can be found in the framework, what legitimate client record and client bunches are there in the system, what applications will be there and so forth.

Step-4

Getting entrance: - This is the real hacking stage in which the programmer accesses the framework. The programme will make utilization of all the data he gathered in the pre-assaulting stage. Typically the fundamental obstacle to accessing a framework is the passwords. In the System hacking, first the programme will endeavour to get in to the framework.

Step-5

Looking after Access:- Now the programme is inside the framework. This implies he is presently in a position to transfer a few documents and download some of them. The following point will be to make a simpler way to get in when he comes whenever. This closely resembles making a little concealed entryway in the building with the goal that he can straightforwardly enter in to the working through the entryway effortlessly.

Step-6

Clearing Tracks: - Here the programmer kills the physical confirmation of his/her hacking the framework. At whatever point a programmer downloads some record or introduces some product, its log will be put away in the server logs. So with a specific end goal to eradicate the programmer utilizes man instruments. One such instrument is windows asset unit's auditpol.exe. Another instrument which kills any physical confirmation is the proof eliminator. The Evidence Eliminator erases every such proof.

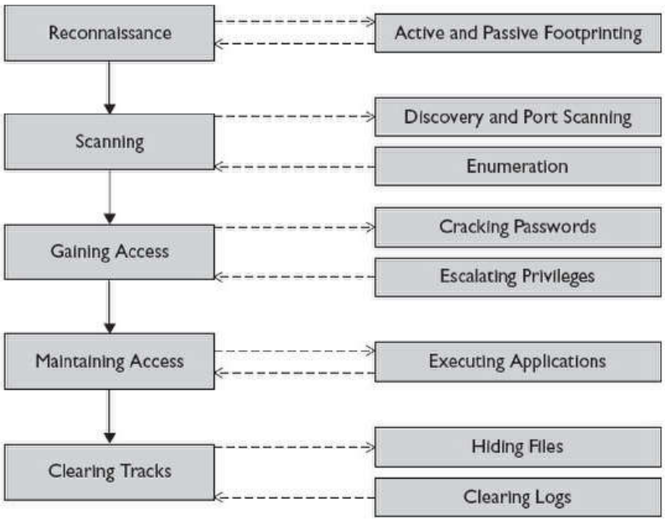


Figure 1 Phases of Ethical Hacking

A few Advantages of Ethical Hacking

1. To help in recognition of violations done through web.

2. Provides security to keeping money and monetary foundations.
3. It can recognize and furthermore to anticipate digital fear based oppression.
4. Everything here relies on the dependability of the moral programmer.

Hacktivism

Hacktivism alludes to 'hacking with/for a reason'. It contains programmers with a social or political motivation. It goes for sending over a message through their hacking action and picking up deceivability for their motivation and themselves.

A moral programmer tries to reply

- What can the interloper see on the objective framework?
    - Reconnaissance and Scanning period of hacking
- What can an interloper do with that data?
    - Gaining Access and Maintaining Access stages
- Does anybody at the objective notice the interlopers endeavour or achievement?
    - Reconnaissance and Covering Tracks stages.

In the event that enlisted by any association, a moral programmer asks the association what it is attempting to secure, against whom and what assets it will exhaust with a specific end goal to pick up insurance. This report is a layout. An electronic duplicate can be downloaded from the Journal site. For inquiries on paper rules, please contact the diary productions advisory group as showed on the diary site. Data about conclusive paper accommodation is accessible from the meeting site.

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.

How does an Ethical Hacker go about it?

Any security evaluation involves three components:

- 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.
- Conduct-In this phase, the evaluation technical report is prepared based on testing potential vulnerabilities.
- Conclusion-In this phase, the results of the evaluation is communicated to the organization / sponsors and corrective advice / action is taken if needed.

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.

Recent Trends in Ethical Hacking

The word programmer in the past was characterized as a man who cherishes playing around with programming or electronic frameworks. They needed to find new things on how PCs work. Today the term programmer has an alternate importance inside and out. It expresses that a programmer is "somebody who noxiously breaks into frameworks for individual pick up. In fact, these culprits are saltines (criminal programmers). Saltines break into (split) frameworks with malevolent aim. They are out for individual pick up: popularity, benefit, and even retribution. They change, erase, and take basic data, frequently making other individuals hopeless". (Kevin Beaver, Stuart McClure 2004, Hacking For Dummies)

"The historical backdrop of hacking goes back to the 1960s when a gathering of individuals in MIT "hack the control frameworks of model trains to influence them to run speedier, more viably or uniquely in contrast to they were intended to". (Diminish T. Leeson, Christopher J. Coyne, 2006, The Economics of Computer Hacking). On account of such action by these people PC proprietors and administrators took away their entrance to PCs. Subsequently the hacking group concocted their own code known as the programmer ethic:

1. Access to PCs-and anything which may show you something about the way the world work-ought to be boundless and add up to. Continuously respect the Hands-On Imperative!
2. All data ought to be free.
3. Mistrust Authority-Promote Decentralization.
4. Hackers ought to be judged by their hacking, not false criteria, for example, degrees, age, race or position.
5. You can make workmanship and excellence in a PC.
6. Computers can improve your life. " (Paul A Taylor, 2005,From Hackers to Hacktivists: Speed Bumps on the Global Superhighway)

The above code is still taken after today and by programmers as well as by others also. Not all programmers today have a similar level of skill. Contingent upon the brain research and aptitudes of a programmer they can be put into four groups.(M.G. Siriam, The Modus Operandi of Hacking) Old School Hackers is one gathering and they trust that the web ought to be an open framework. Content kiddies are another and they are PC tenderfoots that utilization instruments made by proficient programmers to hack frameworks. The majority of the programmers today fit into this gathering. The following gathering is proficient offenders or saltines. They break into frameworks with the end goal of taking and offering data they accumulated. The last gathering is coders and infection scholars. They are tip top people with a high expertise in programming and working frameworks that compose code and utilize other individuals responsible for discharging their code to nature.

Associations and organizations today are under a great deal of worry to shield their data from outer and inner security dangers to their PC frameworks. In that capacity the vast majority of them have thought of the arrangement of enlisting Ethical Hackers. "To get a hoodlum, you should take on a similar mindset as a cheat. That is the reason for moral hacking. Knowing your adversary is totally basic" (Kevin Beaver, Stuart McClure, 2004, hacking For Dummies). In different wards Ethical programmers (white-cap programmers) are experienced security and system specialists that play out an assault on an objective framework with authorization from the proprietors, to discover escape clauses and vulnerabilities that different programmers could abuse. This procedure is likewise known has Red Teaming, Penetration Testing or Intrusion Testing. (www.networkdictionary.com) The true objective of moral programmers is to learn framework vulnerabilities with the goal that they can be repaired for group self-premium and as a side item additionally the benefit of everyone of the people.(Bryan Smith, William Yurcik, David Doss, 2002, Ethical Hacking: The Security Justification)

Each Ethical programmer ought to take after three vital standards as takes after: Firstly Working Ethically. All activities performed by the moral programmer should bolster the association's objectives that he works for. "Reliability is a definitive fundamental. The abuse of data is totally taboo." Secondly Respecting Privacy as all data that a moral programmer accumulates must be treated with the most extreme regard, "at long last not slamming your frameworks". This is for the most part because of no earlier arranging or having not perused the documentation or notwithstanding abusing the utilization and energy of the security devices available to them. (Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies) The primary assaults or techniques that a moral programmers or even programmers perform are of as takes after:

Non Technical Attacks: No issue how secured an association is as far as programming and equipment, it will dependably be helpless against security dangers since security's weakest connection are individuals or its workers. Social designing is a sort of non specialized assault where programmers "misuse the trusting idea of individuals to pick up data for malevolent purposes". Different assaults can be of physical nature, for example, taking equipment hardware or dumpster jumping.

Working System Attack: Hacking a working framework (OS) is a favoured technique for the terrible folks. OS assaults make up an extensive bit of programmer assaults basically in light of the fact that each PC has a working framework and OS(s) are vulnerable to some outstanding exploits.(Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies)

Conveyed disavowal of administration assaults (DDoS): This is the most well known assault utilized by numerous programmers to cut down frameworks. It's a kind of assault that over-burdens the system or server with a lot of movement so it crashes and renders any entrance to the administration. Web Protocol (IP) satirizing: "It is a method for masking the programmer's genuine character. This technique enables a programmer to increase unapproved access to PCs by making an impression on a PC with an IP address demonstrating that the message is from a put stock in have. To achieve this, a programmer must utilize diverse apparatuses to discover an IP address of a put stock in host, and after that adjust the bundle headers so it gives the idea that the parcels are originating from the host." (Tanase 2003, IP Spoofing: An Introduction).

The procedure of moral hacking contains a wide range of steps. The principal thing that is done is to detail an arrangement. At this stage getting endorsement and approval from the association to play out the infiltration test is critical. (Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies). Next the moral programmer utilizes filtering devices to perform port sweeps to check for open ports on the framework. "Once a wafer filters all PCs on a system and makes a system outline what PCs are running what working frameworks and what administrations are accessible, any sort of assault is conceivable" (Bryan Smith, William Yurcik, David Doss, 2002, Ethical Hacking: The Security Justification) This strategy is utilized by programmers also yet for fundamentally for malignant purposes. In the wake of filtering has been done the moral programmer chooses the devices that will be utilized to play out specific tests on the objective framework.

These devices can be utilized for secret word splitting, planting indirect accesses, SQL infusion, sniffing and so on. The tests should be painstakingly performed on the grounds that in the event that they are done mistakenly they could harm the framework and could go unnoticed. (Bryan Smith, William Yurcik, David Doss, 2002, Ethical Hacking: The Security Justification) Finally the arrangement should be executed and the consequences of the considerable number of tests at that point should be assessed (Kevin Beaver, Stuart McClure, 2004, Hacking For Dummies) Based on the outcomes the moral programmer educates the association concerning their security vulnerabilities and also how they can be fixed to make it more secure. A dim cap programmer is a kind of programme that has what it takes and goal of a moral programmer much of the time however utilizes his insight for not as much as respectable purposes once in a while. Dim cap programmers commonly subscribe to another type of the programmer ethic, which says it is worthy to break into frameworks as long as the programmer does not submit robbery or rupture secrecy. Some would contend, however that the demonstration of softening into a framework is up itself unethical.(Red Hat, Inc, 2002) Gray caps are additionally a type of good programmers that for the most part hack into associations frameworks without their authorization, yet then at a later stage send them data on the escape clauses in their framework. They additionally once in a while debilitate to discharge the gaps they find unless move has been made to settle it. (Dwindle T. Leeson, Christopher J. Coyne, 2006, the Economics of Computer Hacking). These days moral hacking isn't just limited in PCs yet it has spread its arms in the realm of electronic products, for example, cell phones, ipads and so forth. Today we live during a time where MMS wrongdoings and SIM card cloning has nearly turned into a piece of our day by day schedule. It has turned out to be critical for each cell phone client to be instructed and arranged for different conceivable known and obscure provisos, vulnerabilities and assaults.

For people, their cell phones contain private photos and individual messages, while for representatives; their cell phone is equal to their office work area containing touchy messages, proposition, faxes and other protected innovation. In the two cases, it has turned out to be vital to play it safe to battle the malevolent aggressors. (Ankit Fadia, 2005, An Ethical Guide To Hacking Mobile Phones)

Attacks Using Different Hacking Tools: Counter Measures Taken By an Ethical Hacker

Pre Attack Phases

Foot printing 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 Foot printing

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. Visual Route: Visual Route 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. Visual Lookout: Visual Lookout 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.
7. 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.

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. Kerb Crack: Kerb Crack consists of two programs, kerb sniff and kerb crack. 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 brute force 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. Win Zapper: Win zapper 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

Natures 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 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. Web Inspect: Web Inspect 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.

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

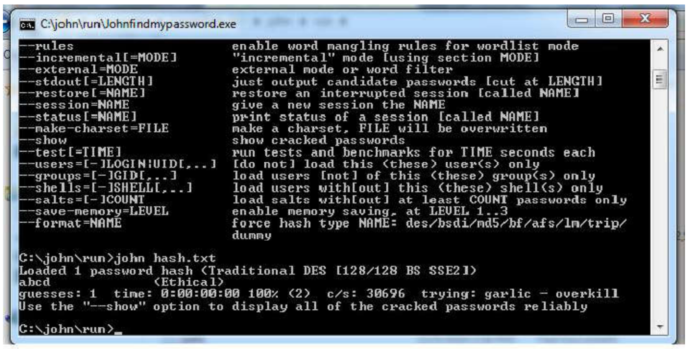
1. DES-encrypted username: password entry
2. md5-encrypted username: password entry

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
Snapshot of Set 1

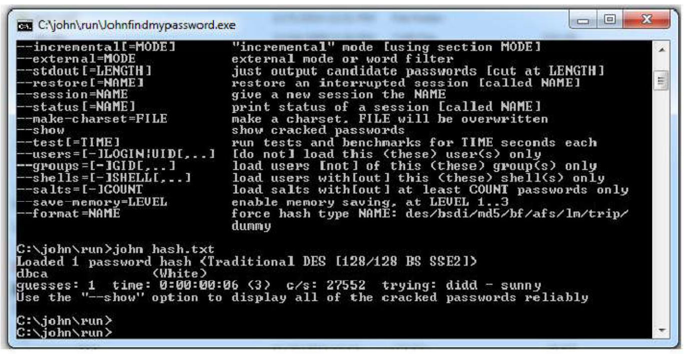


```
--rules                    enable word mangling rules for wordlist mode
--incremental[=MODE]       "incremental" mode [using section MODE]
--external=MODE            external mode or word filter
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           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>_
```

Set 2
Username: White
Password: dbca
Time to Break: 6 seconds
Snapshot of Set2

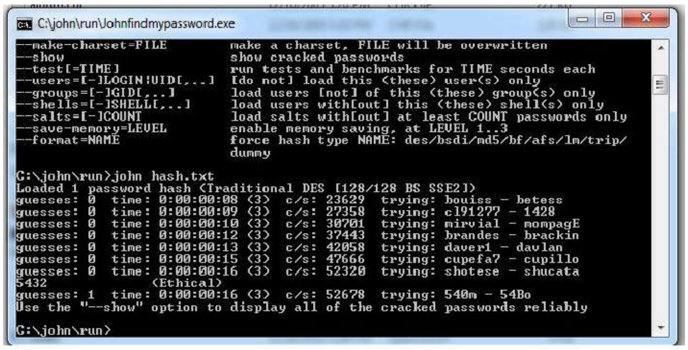


```
--incremental[=MODE]       "incremental" mode [using section MODE]
--external=MODE            external mode or word filter
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             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>
```

Set 3
Username: Ethical
Password: 5432
Time to Break: 16 seconds
Snapshot of Set 3

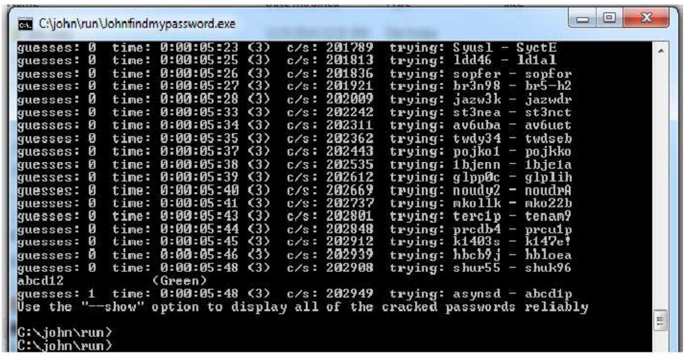


```
--make-charset=FILE        make a charset, FILE will be overwritten
--show                     show cracked passwords
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [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

G:\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: cl91277 - 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

G:\john\run>
```

Set 4
Username: Green
Password: abcd12
Time to Break: 5minutes 48 seconds
Snapshot of Set 4



```
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: 1dd46 - 1d1al
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: mkol1k - 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>
```

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.

CONCLUSION

This paper tended to moral hacking from a few perspectives. Moral hacking appears to be on be another buzz statement In spite of the systems Furthermore thoughts of trying security Eventually Tom's perusing striking a establishment aren't new in the least. But, for those exhibit poor securities on the internet, moral hacking might a chance to be the practically powerful best approach should plug security gaps also forestall intrusions. On the great holders kept all moral hacking instruments need additionally been famous instruments to wafers. So, at present those strategic goals may be with sit tight person venture ahead of the wafers. Moral Hacking is An tool, which whether legitimately utilized, could demonstrate handy for Comprehension the Shortcomings of a system what's more entryway they could make misused. Then afterward all, moral hacking will assume a sure part in the security appraisal offerings Also absolutely need earned its put "around other security appraisals. In. Conclusion, it must a chance to be said that those moral hacker is a teacher who looks for will illuminate not best the customer, as well as the security business in general. For a exert to finish this, Lesvos us welcome those moral Hacker under our ranks concerning illustration an accomplice in this mission. The theory of probability meets expectations against security. With the expanded numbers Also stretching information about hackers joined for the developing number for framework vulnerabilities Furthermore other unknowns, those run through will come At every last bit machine frameworks would hacked or compromised somehow. Securing your frameworks starting with those terrible guys and not the polar nonexclusive vulnerabilities that everybody knows around may be absolutely basic. When people realize hacker tricks, he/she cam wood perceive how defenceless their frameworks need aid.

Hacking preys ahead powerless security hones also undisclosed vulnerabilities. Firewalls, encryption, Also virtual private networks (VPNs) might make a false inclination of security. These security frameworks regularly concentrate on high-keyed vulnerabilities, for example, such that infections Furthermore movement through a firewall, without influencing how hackers fill in. Striking one's own frameworks with find vulnerabilities may be a step will settling on them a greater amount secure. This may be those just turned out system for incredibly solidifying one's frameworks starting with ambush. On people don't recognize weaknesses, it's an is concerned from claiming the long haul When those vulnerabilities are misused. As hackers grow their knowledge, thereabouts ought to individuals. They must imagine such as them will protect their frameworks from them. Author, concerning illustration the moral hacker, must recognize exercises hackers do what's more entryway on stop their exertions. We ought to realize the thing that will search for what's more entryway to utilize that majority of the data will defeat hackers' endeavours. Yet you quit offering on that one if not make moral hacking a really far, however. It makes little sense on solidify our frameworks starting with doubtful strike. For instance, though a client doesn't have a considerable measure for foot activity in the office Also no inward Web server running, the client might not need Similarly as a great part on stress around as an web facilitating supplier might need. The Author's general objectives Similarly as an moral hacker ought further bolstering be as takes after:.

- Hack those frameworks Previously, a non-destructive design.
- Identify vulnerabilities and, if necessary, substantiate on upper management that vulnerabilities exist.
- Apply effects with uproot vulnerabilities Also better secure our frameworks.

References

1. Software Hacking: Ankit Fadia, Nishant Das Patnaik
2. An Ethical Hacking guide to corporate Security: Ankit Fadia
3. An Ethical 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