Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.809 – 815

RESEARCH ARTICLE

FTP Server Hacking: Brute Force Algorithm

Savita Sharma[#1], Vikram Nandal[*2]

[1]M.Tech Student R.N. Institute of Engineering & Mgmt, MDU
Haryana (India)
savitasharma@gmail.com
[2]Asso.Prof, R.N. Institute of Engineering & Mgmt, MDU, Haryana
vikramnandal@gmail.com

Abstract:
Hacking is a serious problem. The incidences of computer hacking have increased dramatically over the years. To solve a problem first to understand how the problem occur into the system. Hacking is done by the hackers also known as the expert programmers. Hackers regard hacking as a game in which their mind is up against that of the system designers. In this paper we describe the hacking process and various hacking techniques. We mainly focus on password cracking techniques.

Keywords:
Hacker, History, Hacker Classes, Hacking Strategies, Password Cracking Techniques, Brute Force Technique, Eth ical Hacking

1. Introduction:-

As the world becomes more and more reliant on computers the computer hacking industry is greatly rising. According to Kevin Mitnick who is known as "the highest profiled computer criminal and responsible for more havoc in the computer world today [1]", he stated that as long as the technology is there it just calls to people to break into it.

According to Richard Stallman, the distinction between black and white hat hackers can be characterized as "hackers who turn new ideas toward destructive, malicious ends versus hackers who turn new ideas toward positive or, at the very least, informative ends."[2]The "Hacker Ethic," as described by Steven Levy in his book Hackers, introduces two important principles into a discussion of computer and information security: "2. all information should be free. 3. Mistrust authority - promote decentralization."[3] In 2000, hackers stole 55,000 credit card numbers from creditcards.com and 300,000 credit card numbers from CDUniverse.com. [4].In this paper we describe various hacking techniques and their impact.

2. Hacker:-

The term hacking, which is broadly, defined as intentionally accesses a computer without authorization or exceeds authorized access [5]. Although to be illegal in all uses, this is not the case as there are many shades of hacking and as such many different kinds of hackers. As with every grouping hackers come in many types and shades in which they come in. The term hacker is used in popular media to describe someone who attempts to break into computer systems [6]. This term however is not the full merit of what a hacker truly is as the purpose is just as important as the use of their skills. A skilled Hacker can be broken down into three hats, or groups depending on their motive [7]. The term hats originated from western movies, when the color of the hat was used to show if the character was a hero or villain [8]. The first group to discuss is the white hat, or true hacker. This hacker is one who has use of his or her skills to show weakness in security and inform the sever admin privately how to fix the error in their system. White hat hackers are often considered good hackers.[9] Grey hats are a mix of the two and as such walk the legal line often, but try not to cross over it. The final shade of the three colors is a black hat hacker. This form of hacker is often one with considered malicious intent [10].

3. Hacking History:-

3.1 Pre-History:-

- 1960sThe Dawn of Hacking original meaning of the word "hack" started at MIT; meant elegant, witty or inspired way of doing almost anything; hacks were programming shortcuts.

3.2 Elder Days (1970-1979):-

- 1970s: Phone Phreaks and Cap'n Crunch: One phreak, John Draper (aka "Cap'n Crunch"), discovers a toy whistle inside Cap'n Crunch cereal gives 2600-hertz signal, and can access AT&T's long-distance switching system.
- Draper builds a "blue box" used with whistle allows phreaks to make free calls.
- Steve Wozniak and Steve Jobs, future founders of Apple Computer, make and sell blue boxes. THE GOLDEN AGE (1980-1991)
- 1980: Hacker Message Boards and Groups Hacking groups form; such as Legion of Doom (US), Chaos Computer Club (Germany).
- 1983: Kids' Games Movie "War Games" introduces public to hacking.

3.3 The Great Hacker War:-

- Legion of Doom vs. Masters of Deception; online warfare; jamming phone lines.
- 1984: Hacker 'Zines Hacker magazine 2600 publication; online 'zine Phrack.

3.4 Crackdown (1986-1994):-

- 1986: Congress passes Computer Fraud and Abuse Act; crime to break into computer systems.
- 1988: The Morris Worm Robert T. Morris, Jr., launches self-replicating worm on ARPAnet.
- 1989: The Germans, the KGB and Kevin Mitnick.
- German Hackers arrested for breaking into U.S. computers; sold information to Soviet KGB.
- Hacker "The Mentor"arrested; publishes Hacker's Manifesto.
- Kevin Mitnick convicted; first person convicted under law against gaining access to interstate network for criminal purposes.
- 1993: Why Buy a Car When You Can Hack One? Radio station call-in contest; hacker-fugitive Kevin Poulsen and friends crack phone; they allegedly get two Porsches, $20,000 cash, vacation trips; Poulsen now a freelance journalist covering computer crime.
- First Def Con hacking conference in Las Vegas

3.5 Zero Tolerance (1994-1998):-

- 1995: The Mitnick Takedown: Arrested again; charged with stealing 20,000 credit card numbers.
- 1995: Russian Hackers Siphon $10 million from Citibank; Vladimir Levin, leader.

- Oct 1998 teenager hacks into Bell Atlantic phone system; disabled communication at airport disables runway lights.
- 1999 hackers attack Pentagon, MIT, FBI web sites.
- 1999: E-commerce Company attacked; blackmail threats followed by 8 million credit card numbers stolen.

4. Hacker Classes:-

4.1 Black hats-
Highly skilled, malicious, destructive "crackers"

4.2 White hats – skills used for defensive security analysts.

4.3 Gray hats – offensively and defensively; will hack for different reasons, depends on situation.

4.4 Hactivism – hacking for social and political cause.

4.5Ethical hackers – determine what attackers can gain access to, what they will do with the information, and can they be detected.

5. Hacking Strategies:-

There are several hacking techniques some of them are given below:-

5.1 Spoofing attack (Phishing):-
Phishing (password + fishing) is a form of cyber crime based on social engineering and site spoofing techniques. The name of 'phishing' is a conscious misspelling of the word 'fishing' and involves stealing confidential data from a user's computer and subsequently using the data to steal the user's money. It is unknown precisely how much phishing costs each year since impacted industries are reluctant to release figures; estimates range from US$1 billion to 2.8 billion per year [11].

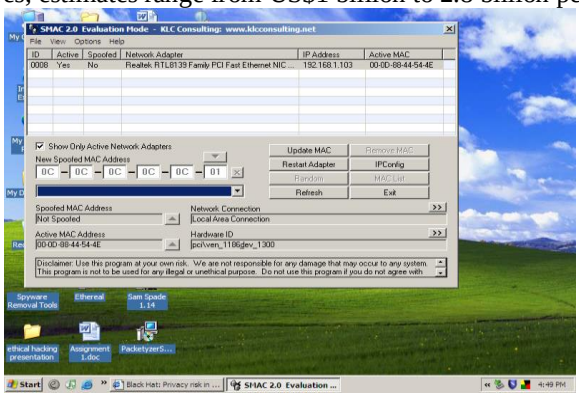

Figure1: Spoofing a MAC address Original Configuration

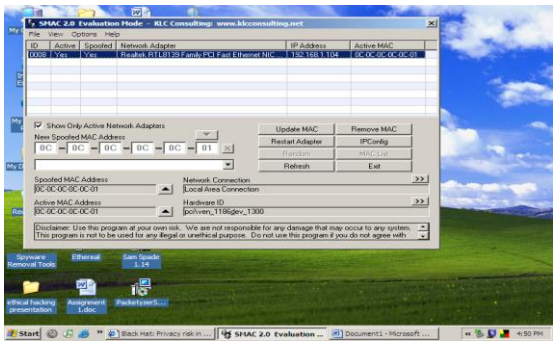

Figure 2: Spoofed Mac

5.2 Packet sniffer:-

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

5.3 Vulnerability scanner:-

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer.

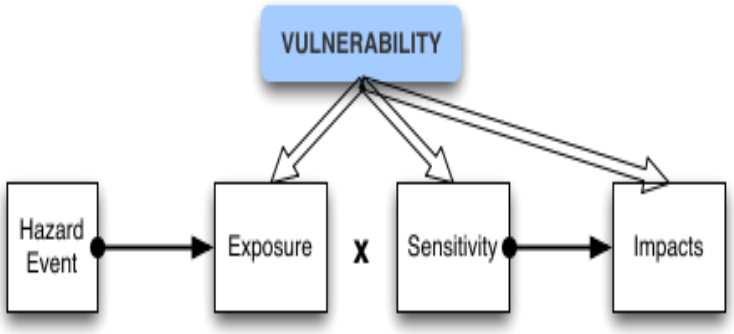

Figure 3: Vulnerability Scanner

5.4 Social Engineering:-

'Social engineering' is the term used to describe the use of psychological tricks, the manipulation of behavior often through deception, by cyber-criminals on unsuspecting users to gain 'access information'. Social Engineering is probably most succinctly described by Harl in 'People Hacking':

"…the art and science of getting people to comply with your wishes."

Social engineering plays on human nature. It may take advantage of our desire to be friendly and helpful or of our conditioned response to people of authority, or of our interest in opportunities for personal gain. Social engineering is not a new phenomenon.

Social Engineering Techniques are:-

5.4.1 Shoulder Surfing:

It means keep an eye on the individual when he types his password or pin no on the keypad. In this the victim has no knowledge that his password is being copied by another one.

5.4.2 Pretexting:-

Pretexting (adj. **pretextual**), also known in the UK as *bla ggingo*r *bohoing*, is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances[12].

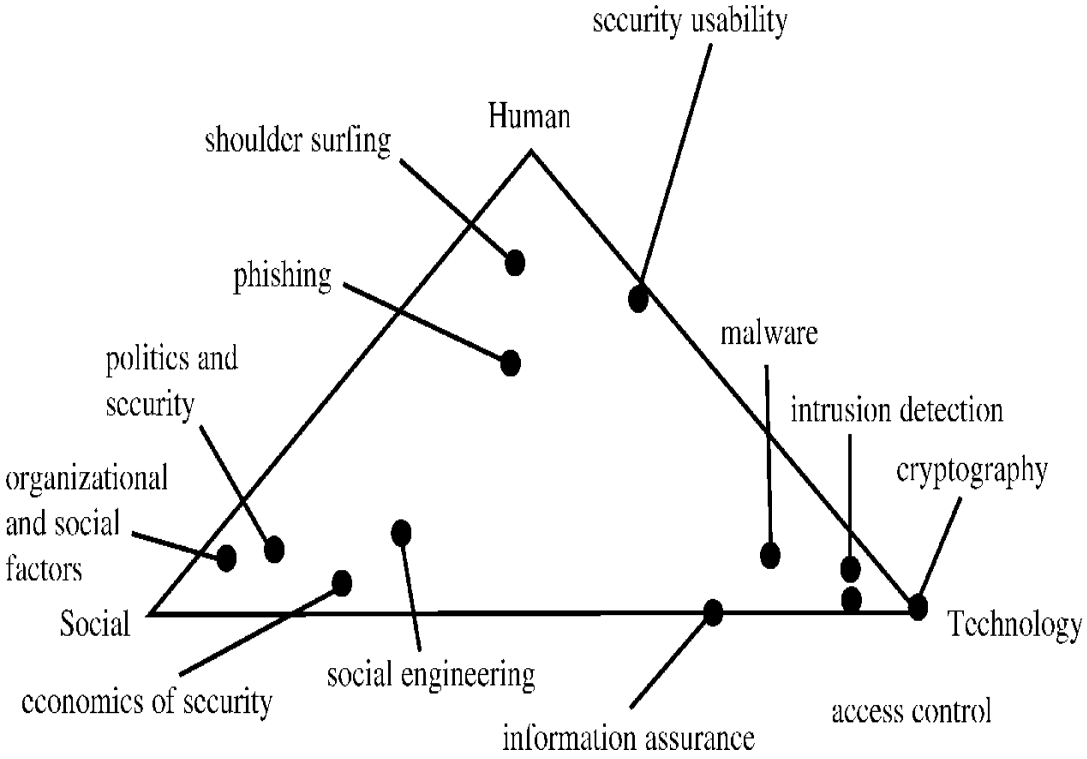

Figure 4: Social Engineering Techniques

5.4.3 Helpless user:-

In this trick an aggressor may pretend to be a user who requires assistance to gain access to the organization's systems. This is a simple process for an aggressor to carry out, particularly if he has been unable to obtain/research enough information about the organization.

5.4.4 Diversion theft:-

Diversion theft, also known as the "Corner Game"[13] or "Round the Corner Game", originated in the East End of London.

In summary, diversion theft is a "con" exercised by professional
thieves, normally against a transport or courier company. The objective is to persuade the persons responsible for a legitimate delivery that the consignment is requested else where - hence," round the e corner".

5.4.5 Forensic analysis: -

By the use of old hard disk, floppy disk and DVD/CDs etc the hacker try to find the information about the user.

6. Password Cracking:-

Human memorable passwords are an integral part of most computers security systems today. Passwords are essential to our online identity; we use them for everything from online banking.

To Facebook status updates. Therefore, accurately understanding the security that passwords provide us is highly important. Access control to information systems is often implemented via passwords; hence, attacking the passwords is one of the most straight forward attack vectors.

There are three basic types of password cracking methods that are given below:-

6.1 Dictionary-

This method is a traditional approach in which a file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.

Limitation:-

Now a day's dictionary method is not preferred because of the use of numbers in the password.

6.2 Hybrid-

Better approach rather than the dictionary method. This method is utilized by users to change passwords is to add a number or symbol to the end. Its attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.

Limitation:-

No use of symbols in the password.

6.3 Brute force-

It is better than both techniques. It uses every combination of characters, numbers and symbols and tried until the password is broken. The feasibility of brute force depends on the domain of input characters for the password and the length of the password [14].

ALGORITHM:-

a) Consider all key values like A-Z, a-z, numbers and special symbols.

b) Generate a loop.

c) Generate all the possible combinations of alphabets with numbers and symbols.

d) Start the loop for millions of times until the password is found.

e) If password is found then loop will stop and a text file is created with password details.

f) Else rearrange the keys and go to step 4.

Conclusion:-

Ethical Hacking-

A type of hacking that is deliberately installed by many organizations to find flaws in their networks to identify the flaws in the computers with security purposes.

In the preceding sections, we have discussed various hacking techniques**.** The purpose of these hacking is used to prevent the identity theft and data stealing crimes.

In order to protect the computer system from hacking, a good investment in the installation of a good firewall is effective.

References:-

1. Mitnick, K: "CSEPS Course Workbook" (2004), p. 4, Mitnick Security Publishing. A documentary based on Kevin Metnick "Freedom Downtime" was made featuring the real story of Kevin Metnick, featuring some real Hackers.
2. Free as in Freedom: Richard Stallman's Crusade for Free Software. Williams, Sam. 2002. (http://www.faifzilla.org/).
3. Hackers: heroes of the computer revolution. Levy, Steven. Anchor Press/Doubleday, 1984.
4. Associated Press, Extortionist Puts Credit Card Data on Web, CBSNEWS.COM, Dec.14, 2000, at http://www.cbsnews.com/stories/2000/12/14/archive/technology/main257200.shtml.

5. Definition of hacking: http://definitions.uslegal.com/c/computer-hacking/ .
6. Definition of a hacker: http://searchsecurity.techtarget.com/sDefinition/0, sid14_gci212220, 00.html.
7. Colors of hackers: http://www.windowsecurity.com/articles/Different-Shades-Hackers.html.
8. What is a white hat hacker?http://searchsecurity.techtarget.com/sDefinition/0, sid14_gci550882, 00.html?
9. Cyber defense exercise: http://www.nsa.gov/public_info/press_room/2010/cdx.shtml.
10. Definition of a grey hat hacker: http://searchsecurity.techtarget.com/sDefinition/0, sid14_gci555449, 00.html.
11. R. Dhamija, J.D.Tygar and M. Hearst. Why Phishing Works. In Proceedings of ACM Conference on Human Factors in Computing Systems (CHI2006), pp. 581590, April 2006.
12. The story of HP pretexting scandal with discussion is available at Davani, Faraz (14 August 2011).
13. "Train for Life", Web.archive.org. 2010.
14. Gershon Kedem and Yuriko Ishihara Brute force attack on UNIX passwords with simd computer. In Proceedings of the 8th conference on USENIX Security Symposium – Volume 8, pages 8–8, Berkeley, CA, USA, 1999 UNIX Association.

