ISSN: 0974-1011
A Special Issue of International Journal Of Computer Science And Applications Vol. 13, No.1, Jan-Mar 2020

Inculcate Precise Impressions of Ethical Hacking on Teenagers

Mrs. Aarti S. Pardeshi
Assistant Professor, Dept. of Computer Science
C. K. Thakur A.C.S. College(Autonomous),
Plot No.-01, Sector-11, Khanda Colony,
New Panvel (W), Dist.-Raigad, Maharashtra,
India, Pincode-410206
pardeshi.aarti@gmail.com

Aakashsingh K. Pardeshi
Student, Dept. of Computer Science
C. K. Thakur A.C.S. College(Autonomous),
Plot No.-01, Sector-11, Khanda Colony,
New Panvel (W), Dist.-Raigad, Maharashtra,
India, Pincode-410206
aakashsingh.p@outlook.com

ABSTRACT
Techno-world bring everything at our fingertip. Business, Education, Shopping, Entertainment and even friends are available online. This leads to creation of huge data on internet and it is available 24 X 7. Freely available big data raise the concern regarding Internet security. As the commercial data and freely accessible databases are obtained through the internet, the criminals get attracted toward these data in order to access sensitive information in illegal way through web application[9]. Thus, protecting diversely classified user system from computer criminal whom are commonly referred as hacker, is a great challenge. Hacker is a computer whiz but has chosen illegal way[13]. Organizations are in search of computer experts who will work for them to protect their system or web applications. Such an expert is known as Ethical hacker[7,9]. Ethical Hacker has to face the challenge to provide security to big data which is continuously in generation mode. Data Science approach to classify and analyse this heterogeneity is must to generate decision making rules for fixing security breaches. Ethical Hacking is a process that helps in finding and fixing the vulnerabilities and deficiencies in the system morally[13]. This paper outlines the study of norms, tools and techniques used for ethical hacking in Kali Linux and generate awareness about ethical hacking amongst teenagers.

Keywords
Hackers, Ethical Hacking, OWASP TOP 10

1. INTRODUCTION
Teenagers think that hackers are extraordinarily skilled, well-informed people who can easily hack into any computer systems just by pressing some random commands and find sensitive information in short time. In movies, hackers are always shown as a teenager who is good at cracking any password, tampering the data, seek sensitive bank account details and gets appreciated for the same. In reality, a computer expert must be clear with some basic ideas like how a computer system works? and know what tools to employ to find a security weakness?[1].

Two decades ago, there was a rising popularity of computers and their high cost, access to machines was limited. Each of them was authenticated with the help of passwords or some other means of authentication. Some of the people who were not allowed to access the machines attempt to steal the password by looking from behind the shoulders or trying some incorrect passwords. The intention behind this was to run their programs or try to make changes in the original program[2].

Initially, these machine intruders were fairly good. Some of the intruders were less skilled and less concerned, they accidentally bring the system down and then they restart the machine to make the system run smoothly. Again, when they were denied to access the machine after discovering their activities, they try to bring the system down purposely. Due to this inflected machine, this became news and media picked up. Instead of using 'computer criminal', they used the term 'Hacker' to describe this intruder.

2. RELATED WORK

2.1 HACKER'S INTENTIONS:

Various available hacking tools are looking to find weaknesses in one of the following areas[10]:

- **Operating systems:** Installing operating systems with default settings raise concerns regarding potential vulnerabilities that remain unpatched.
- **Applications:** When Developers don't test the application code for vulnerabilities which leads to many programming flaws that a hacker can exploit.
- **Shrink-wrap code:** Normal Users are unaware of possible vulnerable exploits which comes with extra features of off-the-shelf programs. For example, hacker can execute vulnerable code with macros of Microsoft Word.
- **Misconfigurations:** Misconfigured Systems settings or low security settings may attract an attacker.

Following are the hacker's intentions behind any cyber-attack:

1. Passionate about computer work flow
2. Having curiosity in understanding operating system functioning
3. A Shy guy who want to become famous
4. Want to maintain rapport into dark net
5. Damage corporate reputations for taking revenge
6. Want to gain money

2.2 TYPES OF HACKERS:

A. White Hat Hackers: White Hat hackers are approved and funded person and also called as "IT Technicians". Their job is to make the industrial network safe from intruders. Sometimes they are asked to hack their services and try to find and fix the security patches in the

network. These White Hat hackers are also called as Ethical Hackers. [3,9,10]

B. Black Hat Hackers: Black Hat Hacker keeps an intention to harm the system. They break the security doors of the network or services and bring down the network and make the service unusable. Black Hat Hackers enters in the network by cracking the passwords and obtain entry to unauthorized network. They are also called "Crackers" or "Malicious Hackers". [3,9,10]

C. Grey Hat Hackers: Grey Hat Hackers have properties of both White Hat Hackers and Black Hat Hackers. Grey Hat Hackers can change the programs in the systems and then alert the industry that there are loopholes in the security and it might be hacked. [3,9,10]

D. Blue Hat Hackers: These are another form of amateur hackers much like script kiddies whose main agenda is to take revenge on anyone who makes them angry. They have no desire for learning and may use simple cyber-attacks like flooding your IP with overloaded packets which will result in DoS attacks. [4,8]

E. Green Hat Hackers: These are like script kiddies or blue hat hackers. But they have specific intentions of becoming full blown hackers. They are also known as neophytes.

F. Red Hat Hackers: They are like white hat hackers. But they do not report to hackers, instead they steal hacker's computer system information and also sometimes destroy it[8].

G. Hacktivist: These are hacker who perform hacking for a cause such as broadcasting political and social messages through social media. They raise public awareness for political and social cause[6].

H. Cyber terrorists: These types of hacker's who hack government computer or public utility infrastructure. Some of the attacks are possible on-Air traffic control towers and power stations.

2.3 HOW A SYSTEM CAN BE HACKED?

2.3.1 E-Mail Hacking or Fake E-Mail

Fraudsters hack the email account of an individual and send instructions to a commercial website or any bank acting as the customer[5,8].

2.3.2 Mobile SIM Swap

This happens when fraudster's gain customers personal information through activities like phishing(fraudulent mail), vishing (fraudulent call), social engineering, etc. By creating customers fake id, they obtain duplicate SIM cards from mobile operators and deactivate the customer's genuine SIM card. Duplicate SIM cards are then used to fraudulent transactions in the customer's (victim's) account, without his/her knowledge.

2.3.3 Brute Force attack

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. This is known as an exhaustive key search[10].

2.3.4 Keystroke Logging

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys hit by individual on a keyboard, unaware that their actions are being monitored. A keylogger can be either software or hardware.

2.3.5 Network eavesdropping

Network eavesdropping is a network layer attack that focuses on capturing small packets from the network transmitted by other computers and reading the data content in search of any type of information[15].

2.3.6 Cookie Theft

Cookie theft occurs when a third-party copies unencrypted session data and uses it to impersonate the real user. Cookie theft most often occurs when a user accesses trusted sites over an unprotected or public Wi-Fi network.

2.3.7 Bots and Botnets

A term "bot" derived from robot[6,10]. Before a decade Bots were interpreted as robot will help to avoid repeated work. But now a days the bot is also used to do cyberattack which are indirectly remotely directed by an attacker. The bot is software program which is basically going to repeat certain action. For example, Brute force attack[6] is an attack which tries all possible combinations of password to crack it. For this attack a bot can be used to try such activity with different possible dictionary attacks like wordlist, famous password and a key, pair combination of (username, password) available on darknet.[6] The cybercriminal can then use the bot (also known as a zombie computer) to launch more attacks or to bring it into a collection of controlled computers, known as a botnet[10].

2.3.7.1 Bot creation

A bot is created when the malware containing the programming to take over the computer is placed onto its target. It could be brought by a network worm that deposits its payload. It could be a virus that was launched from an infected e-mail attachment. It could be a Trojan horse disguised as a program the target user desired.

After implantation, the bot then attempts to connect with the command-and-control server (as stated above, usually an IRC server). From there, the bot herder can launch any number of attacks.

2.3.7.2 Prevention from Bot attack

With all the damage that can be done to a computer and through a computer has been turned into a malicious bot. it's important to take necessary action in regards to its prevention and it include following methods:

- Education regarding malicious bot
- Go for regular software updates and patches
- Use of antivirus software
- Use of Updated Firewall

3. What is Ethical Hacking?

Ethical hacking is also known as "Penetration Hacking" or "Intrusion Testing" or "Red Teaming"[7,13]. Ethical Hacking is defined as a practice of hacking without malicious intent. Both Malicious Hackers and Ethical Hackers are distinct from each other and play important roles in Security. According to [10,13], "Ethical hackers employ the same tools and

techniques as the intruders, but they neither damage the target systems nor steal information. Instead, they evaluate the target systems' security and report back to owners with the vulnerabilities they found and instructions for how to remedy them". [3] In today's generation of the Internet, we have many immeasurable technologies like Online Shopping, Online Banking, Commercial websites, Wikipedia, etc. For every good side, we have a bad side and that is hacking. These hackers get into the website and try to steal the information and make it open on the darknet generally identified as black hat hackers, to stop or avoid these malicious activities white hat hackers came into the picture. These white hat hackers are termed as Ethical hackers[10].

Ethical hacking is a way of hacking with good intentions. Ethical hacking can be considered as a security test of an information technology environment. [3]

3.1 Way to conduct Ethical Hacking

The following steps are a framework for performing a security audit of an organization[7,14]:

1. Discuss with the owner of the system and gather the detail information of the system and sections that are needed to be implemented during the testing.
2. Sign nondisclosure agreement (NDA) documents with the owner.
3. Unite an ethical hacking team, and prepare a pen testing schedule.
4. Conduct the pen test.
5. Prepare a brief report of analysis.
6. Handover the report to the owner.

Ethical hacker conducts a penetration testing also known as manual penetration testing[14,15]. It is possible to have automated penetration testing. Different tools are available for vulnerability assessment such as Nessus, Qualys and Web Inspect[6,10]. Nessus is the well-known vulnerability scanner, which was designed by tenable network security. It is free and is chiefly recommended for non-enterprise usage. This network-vulnerability scanner efficiently finds critical bugs on any given system. [6] There are some limitations to these automated testing such as specific task or process will be assessed, even though critical risk found, no immediate action will be taken and only assessment report will be generated. That will not be the case with manual penetration testing. Though it is time consuming but it is reliable and safe in terms of providing security to organizations system.

4. OPEN WEB APPLICATION SECURITY PROJECT (OWASP) TOP 10

It is an non-profit organization that works for the security of the websites. It maintains a prioritized based top 10 security risk lists. Priority is decided by factors like detectability, severity and exploitability. In the next sub section, there is detail explanation of these risks[6].

4.1.1 Injection

Injection flaws, such as SQL injection. In this attack unauthorized intruder tricks the SQL commands, sends the changed query and gain sensitive database information.

For example, Consider the following SQL query which accepts untrusted data

String str= "Select * from employee where eid='"+

request.getParameter("id") + "'";

In the above case, attacker can modifies the 'eid' parameter and retrieves all the records of employee relation.

http://demoexample.com/webapp/employeeView?eid= ' or '1 '=' 1

4.1.2 Broken Authentication.

Authentication and session management are frequently implemented incorrectly, allowing attackers to get access to passwords, keys, or session tokens.

4.1.3 Sensitive Data Exposure

When web applications and APIs do not maintain security for sensitive data, then there is high risk of credit card fraud, and identity theft.

4.1.4 XML External Entities (XXE)

External entities evaluated by poorly configured XML processors can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service (DoS) attacks.

4.1.5 Broken Access Control

Automated attack is possible under this type of risk, where bad guy is going to use automated system to stuff credential to guess user name and passwords and once attacker is successful in it then he can modify other users' data, change access rights, etc.

4.1.6 Security Misconfiguration

Security misconfiguration is to keep insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Here, user can follow simple principle "DON'T USE IF YOU DON'T NEED"[12].

4.1.7 Cross-Site Scripting XSS

It is also called client-side code injection. Untrusted data in a web page without sufficient validation leads to XSS flaws. In this attack, hacker executes a script in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

4.1.8 Insecure Deserialization

Insecure deserialization can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

4.1.9 Using Components with Known Vulnerabilities

Software have Components, such as libraries, frameworks, and other software modules. Many known software comes with known vulnerabilities. In this case user has advantage that he is having knowledge of flaws present in the current application.

4.1.10 Insufficient Logging & Monitoring

Logging means recording things and monitoring is one step ahead of it. Monitoring is used to analyse these log records. User should monitor warnings, error messages and so on. User should log and monitor Login Failure, Access Failure

and server-side failures. “TOO MUCH CONTENT AND TOO LITTLE CONTENT” is not good for log[11].

The strategies and policy to be taken under consideration by normal user, organizations, business entrepreneur, government and all developers who are working on sensitive data when attacker wants to hack machine are explained in Figure1.

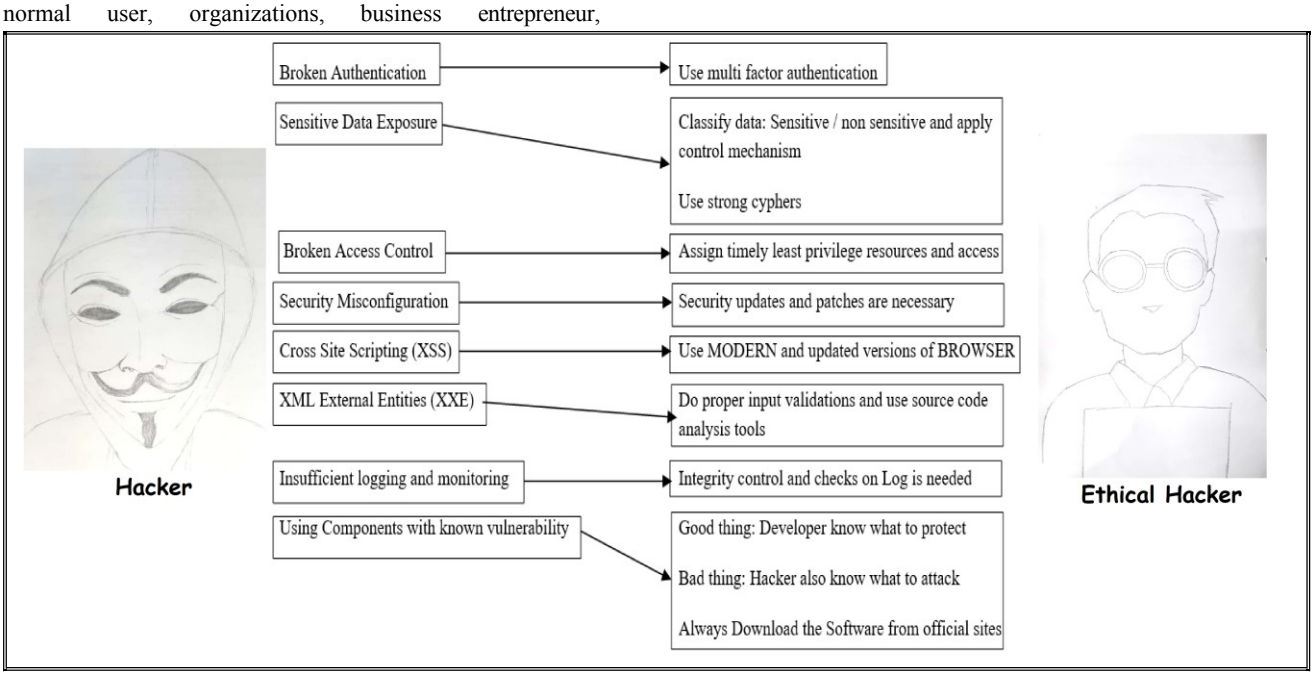

Fig 1: Possible ways with which Attacker gains access and action to be taken by ethical hacker

5. Methodology

A survey was conducted with 170 participants from various arenas such as Student, Teacher, Industry expert and an Outsider, who is not having an ethical hacking domain knowledge. 53% participants including industry expert strongly agree to the fact that ethical hacker or hacker share common property that is he has to be a computer expert.

Weka is popular tool for statistical analysis. Many machine algorithms such as Logistic regression, Decision Tree, Random Forest can be implemented on dataset of csv format. Implementation of these algorithms is explained in below section.

Logistic Regression gives accuracy of 95.88%, where 108 out of 113 instances are correctly classified for Ethical Hacking No Knowledge (EHD) and 55 out of 57 instances are correctly classified for Ethical Hacking Knowledge (EHK).

MultilayerPerceptron(MP) using 66% split gives 97.64% accuracy. Confusion matrix of Neural network based MP algorithm predicts that only four EHD class got wrongly classified.

SMO which is a binary classification support vector machine algorithm gives the accuracy of 94.11%. Random forest(RF) algortihm classifies data with 98.27% accuracy.

J48 decision tree gives 98.27% accuracy. The Fig. 2, gives proper justification. The user who think they know even tool to provide security and know method to take actions when their machine gots attacked don’t need training but the other people requires tranining to clarify ethical hacking technology. If user know one tool to provide security and have clear idea of actions needed in case of attack are the experts or having knowledge of this domain.

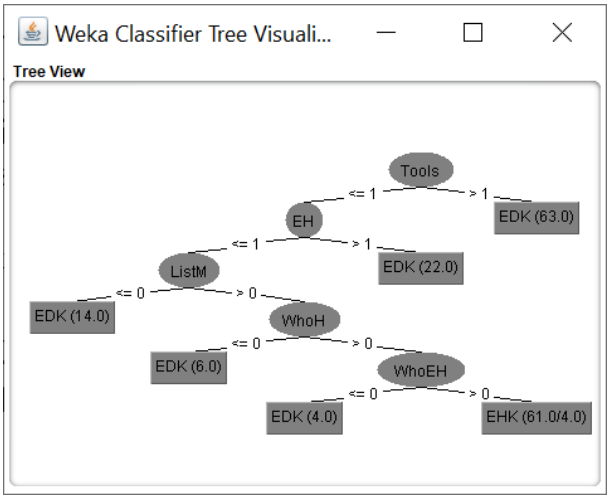

Fig. 2, J48 Decision Tree classification

So J48 and RF classifies more than 98% data correclty.

6. CONCLUSION

This paper tries to give overview of hacking and ethical hacking norms and commonly used terms. Also, an effort has been made to create awareness regarding protection and security policies to be followed by a layman. The result of analysis shows that 67% teenagers don’t know how to handle the situation when their system will get attacked. Teenagers should gain thorough knowledge of ethical hacking concepts,

instead of wasting time in learning random software to get access to other person's sensitive information. Teachers, Industry expert and T.Y. learners know tools other than Antivirus and Firewall to secure the system, as they have gained the knowledge of it.

This paper also explores one more research topic on providing security to knowingly or unknowingly created huge data.

Variations in the studied results of J48, RF and MP are because of loss of interpretation between attributes with binary values. One-word answered questions needs to be asked more elaborately.

Using Supervised learning algorithms such Decision Tree, KNN(K Nearest Neighbor), Random Forest and SVM(Support Vector Machine) answers to the following questions can be found:

- Is data being attacked is from specific type of organization?
- Is data being attacked is of specific type?
- Is organization being attacked during specific period?

Consider Section 2 as a hypothesis, the above classification can conclude on hypothesis acceptance or rejection. In future, research work will be made for comparative study and analysis of ethical hacking tools used in Windows as well as Kali Linux.

7. ACKNOWLEDGMENTS

Our thanks to the Ruturaj Patil, student who have provided hand drawn images.

8. REFERENCES

[1] Sunil K. 2018, Hacking Attacks, Methods, Techniques and Their Protection Measures, International Journal of Advance Research in Computer Science and Management. Vol(4), pp 2353-2358.

[2] Brijesh K. P., Alok S., Lovely L. B. 2015, ethical hacking (Tools, Techniques and Approaches), Conference,January 2015, DOI: 10.13140/2.1.4542.2884.

[3] Bhawana S., Ankit N., Shashikala K. 2014, Study Of Ethical Hacking, IJCST, Vol(2), pp 6-10, ISSN: 2347-8578

[4] Aamer K. (2016), Ethical Hacking for Teaching Purposes, 10.13140/RG.2.1.2028.3282

[5] Alexander P.& Eugene P. (2015). Social Learning Theory and Ethical Hacking: Student Perspectives on a Hacking Curriculum, Conference, ISECON, Vol (32)

[6] OWASP TOP 10 2017, Online: https://owasp.org/www-project-topten/OWASP_Top_- Ten_2017/Top_10-2017_A1-Injection, Copyright 2020.

[7] Jeffrey L., Walsh C.(2007), What Are Faculty Attitudes Toward Teaching Ethical Hacking and Penetration Testing?, Proceedings, Information System Security Education, pp 111-116

[8] Suriya B., Sujeeth K., Ashhar 2016, A Comprehensive Study On Ethical Hacking, IJESRT, DOI: 10.5281/zenodo.59534, pp: 214-219

[9] Marilyn L., A Closer Look at Ethical Hacking and Hackers, in East Carolina University ICTN 6865.

[10] Kimberly G. 2007, CEH Official Certified Ethical Hacker Review Guide, Wiley Publishing, 2007, ISBN: 81-265-1196-6

[11] F5 DevCentral, OWASP TOP 10 2017, Insufficient Logging & Monitoring, Online: https://www. Youtube-.com/watch?v=IFF3tkUOF5E&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD&index=10, Apr 4 2018

[12] F5 DevCentral, OWASP TOP 10 2017, Security Misconfiguration, Online: https://www.youtube.com /w-atch?v=JuGSUMtKTPU&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD&index=6, Feb 7 2018

[13] Palmer, C. C. (2001, April 13). Ethical Hacking, IBM System Journal, Vol(40), pp 769-780

[14] Susidharthaka S., Rashmi R. P. Jun 2015, Ethical Hacking, IJSRP, ISSN 2250-3153, Vol (5)

[15] Idimadakala N. Oct 2013, Ethics In Ethical Hacking, IJSER, Vol(4), pp 1593-1597