**A Paper Presentation**

**On**

**“ ETHICAL HACKING “**

**Submitted**

**By**

**Contact : 8096644062**

**E-mail ID : harinijoshi8@gmail.com**

**JAYAPRAKASH NARAYAN COLLEGE OF ENGINEERING**

**DHARMAPUR, MAHABOOBNAGAR**

**Ethical Hacking**

**Abstract**

During the development of the internet, computer security has become a major concern for business and governments. They want to able to take advantage of the internet for electronic commerce advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being “hacked”.

At the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home address. In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to breaking to their computer systems. This scheme is similar to having independent auditors come into an organization to verify its book keeping records.

In the case of computer security, these “tiger teams” or “ethical hackers” would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information.

**What do ethical hackers do?**

Ethical hacker’s evaluation of a system’s security seeks answers to three basic questions.

1. What can intruder see on the target systems?
2. What can an intruder do with that information?
3. Does anyone at the target notice the intruder’s attempts successes?

**Who are ethical hackers?**

Successful ethical hackers possess a variety of skills first and foremost, they must be completely trustworthy while testing the security of a client’s systems, the ethical hacker may discover information about the client that should remain secret. In many cases, this information, if publicized, could lead to real intruders breaking into the systems, possibly leading to financial losses.

During an evaluation, the ethical hacker often holds the “keys to the company”, and therefore must be trusted to exercise tight control over any information about a target that could be misused.

**Advantages**

* To catch a thief you have to think like a thief
* Help in closing the open holes in the network
* Provides security to banking and financial establishments
* Prevents website defacements

**Disadvantages**

* The ethical hacker using the knowledge they gain to do malicious hacking activities
* Allowing the company’s financial and banking details to be seen
* The possibility that the ethical hacker will send and\or place malicious code, viruses, malware and other destructive and harmful things on a computer system.

**Summary**

* Hackers are professionals when they first known but when technology advance to new stage, from day to day
* People became more interested in the cyber world
* Thus, earning the hackers a bad name by hacking into other computers to demonstrate their strength

**Conclusion**

Ethical Hacking is legal way to securing your system. Main way to that giving your system in hands of ethical hacker so that he can make your system full proof. It is a part of overall security program. System administrator should always try to find loop holes into the system and make system preventive measures.

Ethical Hacker possess same skills, mind set and tool of a hacker. Attacks are done in a non-destructive manner.