A research on criminal activity on hacking and how to prevent it by ethical hacking

Sunit Fulari

Alumni National institute of technology Goa

Abstract

Today with the development of so much of advanced technology such as fast computers, super fast internet connection connecting the entire globe, big transactions and much more to name a few. There is criminal activity being done on everywhere by the bad people such a stealing money from online transactions, changing logo of websites and completely modifying a website and apps. We need to prevent all these by employing good people who are known as ethical hackers. So our research in this paper is on ethical hacking.

Introduction:

Hacking has various forms which are two.

HACKER is A person who enjoys learning the details of computer systems and how to stretch their capability—as opposed to most users of computers, who prefer to learn only the least amount necessary. 2. One who programs passionately or who enjoys programming rather than just theorize about programming.

This was known as hacking in the prior days.

Now computers are not just available with researchers and scientists and workers it is been available with everyone so there is more risk for nonsense and criminal activity who try to exploit it. But first these activities were just simple and benign but later they turned out to be very harmful for society and people as whole. Some times people break into the computer for fun,revenge or damage and profit.

We will use ethical hacker and criminal hacker for most part of our research.

Ethical hacker:

In their search for a way to approach the problem, organization 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 break into their computer systems. This plan is similar to having self-governing auditors come into an organization to bear out its secretarial records. In the case of processor security, these “tiger teams” or “ethical hackers” would employ the same tools and technique as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems’ security and report back to the owners with the vulnerabilities they found and instructions for how to therapy them.

So who are these ethical hackers?

These early efforts provide good examples of 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 revealed. Could lead to real intruders breaking into the systems, possibly leading to financial losses.

In my previous work I have spoken about object detection using traditional methods and deep learning and machine learning which we have used slightly in this research and will use in the future.Its all common sense.

During an evaluation, the ethical hacker often holds the "key to the company," and therefore must be trusted to exercise tight control over any information about a target that could be misused. The sensitivity of the information gathered during an evaluation require that strong measures be taken to ensure the security of the systems being employed by the ethical hackers themselves: limited-access labs with physical security protection and full ceiling-to-floor walls, multiple secure Internet connections, a safe to hold paper documentation from clients, strong cryptography to protect electronic results, and isolated networks for testing.

So we all want to know what does ethical hackers do?

What can an intruder see on the target systems?

What can an intruder do with that information?

Does anyone at the target notice the intruder's at-tempts or successes?

Results:

So now that we have researched on hacking and ethical hacking in our future research we are going to invest our research on open source software which are used in this.Thanks for reading my work.

References:

[1] Palmer, C.C., 2001. Ethical hacking. *IBM Systems Journal*, *40*(3), pp.769-780.

[2] Engebretson, P., 2013. *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier.

[3] Fulari, S., 2018, May. A Survey on Motion Models Used for Object Detection in Videos. In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 348-353). IEEE.

[4] Gaitonde, J.V., Fulari, S. and Lohani, R.B., 2019, January. Application-Specific Dual-Mode Buried-Gate GaAs OPFET for Visible-Light Communication. In *Proc. International Conference on Electrical, Communication, Electronics, Instrumentation and Computing (ICECEIC)*.