Vishnu Institute of Technology

Vishnu Institute of Technology, the scion of Shri Vishnu Educational Society was established in 2008 and is currently the eleventh educational institution to disseminate education under the aegis of this society. Nascent that it is, it combines in its matrix the lofty idealism of its Founder Chairman the Late Padmabhushan Dr. B. V. Raju, a distinguished industrialist, philanthropist and an eminent educationalist; the experience and vigour provided by the Chairman Sri K.V. Vishnu Raju, a man of holistic vision and his team comprising dexterous administrators, reputed academicians and brilliant line of students. They constantly strive to make the institution join the ranks of prestigious technical institutions.

Campus

The Campus, sprawling over 100 acres, is located in the verdant atmosphere of Vishnupur in Bhimavaram. It is in the very vicinity of the town and is well connected by road. VISHNU also provides hostel facilities to the students who opt for a residential mode of education. The hostels are constantly updated and provide an atmosphere conducive to pursue education.

Hands on Experience

To make the instruction in VISHNU more practical-oriented, special focus is on hands on experience. The Assistive Technologies Lab run in collaboration with the University of U Mass, USA helps students to combine technology with a humanistic outlook. Gadgets for the physically challenged are designed and developed here by the students under the guidance of eminent professors both from the Institute and abroad. VISHNU aims at empowering students with technical skills and can-do entrepreneurial spirit. The IBM Software Centre of Excellence in the campus provides the students with the best of quality technical education there by increasing the skill set of each student and faculty for a great career.
Department of Information Technology

The mission of the department is to advance and enhance computer science engineering fundamentals to build the intellectual capital of students. The IT Department endeavours to be an important resource centre for the development of computing systems and applications.

The department was established in the academic year 2008-09 with an annual intake of 66. It offers 4 year B.Tech. This program affiliated to JNTU Kakinada & approved by AICTE. The department has number of well equipped Laboratories and provides excellent facilities for learning.

CONTENTS

Helm of Affairs .................
Department Activities ............
Faculty Activities ......
Placement Activities .............
Articles ......................
HELM OF AFFAIRS

Academics are a continuing process of exploration, growth and sustenance. Today information explosion has brought about many changes. New ideas are generated, new interpretations are given and new applications are invented. The equations are changing very fast both in education and at the work place. Every day brings in new demands. One has to constantly upgrade to cope with the fast emerging trends. A software professional once said “We are training people in technologies to find solutions for problems that have not yet been identified”. Moreover the roles and responsibilities of professionals are ever expanding making it imperative to move beyond the confines of the classroom and the stipulated curriculum and focus on the skills needed to cater to the needs of the society. Hence it has become imperative to all the stakeholders in education to arm themselves with the necessary knowledge, skills and attitude to keep themselves abreast of the rapid changes.

That explains everything—the Chairman’s message to the faculty to constantly update themselves with the emerging new technologies and concepts, the focus on research, paper presentations and publications, undertaking new projects, adopting new technologies for information collection and dissemination as well.

“The key to growth is the introduction of higher dimensions of consciousness into our awareness” -- Lao Tzu.

That is what the message of our Chairman does, to motivate us to action.

The stimulus has been given...

it’s time for response.
Chairman Message

I am happy to inform that the department of Information Technology of Vishnu Institute Of Technology is publishing their department news letter for the academic year 2011-2012. I Commend and appreciate the efforts taken by the staffs and students to enhance the quality of academics in the college. Vishnu Institute Of Technology moreover has the credentials and Proven strengths to initiate such an indispensable academic activity.

Message from Principal

It is my pleasure in congratulating the department of IT on the pleasant occasion of releasing the newsletter for the period 2011-2012. It is great to find a considerable number of winners and participants in co curricular and extracurricular activities which certainly prove that our staff and students are adequately equipped and possess necessary skill-sets to bring such laurels to the institution. I am sure that publishing a newsletter of this sort containing the achievements of the wards will be recognition to them and I wish them all the very best for future endeavours.

Message from HOD

Welcome and best wishes for all the Staffs and Students of the department who receive this News Letter. It has been interesting and busy year for the members of the department. And has had a number of Successful events including Guest Lecture, Workshop, National Level Conference and Symposium. I invite all the readers of this news letter to share this with your friends and contribute more items for 2014 News Letter.
Progressive Strides

The month of December witnessed a plethora of events. An AICTE sponsored staff development programme on “Recent Trends in Data Mining and Warehousing” was organized by the Department of Computer Science Engineering from 5 December to 17 December 2011. Faculty from various Engineering colleges participated in the programme. Eminent scholars were the resource persons including Prof. D.V.L.N. Somayajulu and Prof. R.B. Subramanyam of NIT Warangal, Dr.J.V.R. Murthy of JNTUK and Mr.V. Sri Kumar of Infosys.

Department Activities

VALIANT 2011 a National Level Technical Student Symposium was conducted on 29 and 30 December 2011 at VIT. 1000 papers from across the country were received out of which 200 papers were selected. Participants were from institutes of repute like IIT Kharagpur, and universities of Uttaranchal, Coimbatore and other such places. The project exhibition showcased the technical skills of the students while the creative gallery events brought to the fore their creative talents.

The inaugural was on the 29 of December and the Chief guest was Dr.K.Satya Prasad, Rector of JNTU-K. Shri P. Krishna Ganga Raju, Secretary of SVES, was the guest of honour.

Chairman Shri K.V. Vishnu Raju graced the valedictory which was on the 30 December and gave away the prizes to the toppers.

Faculty Activities

Mr. I R Krishnam Raju, Assoc. Prof, IT, has participated in Faculty Leader Ship Institute (FLI) 2012 on “Proven Strategies for Effective Teaching” conducted during 5th-7th Jan’12 conducted by University College of Engineering, Kakinada.

Foreign Languages

The second session of German Language A2 level classes was held for the III and IV B. Tech students from 9 to 13 December 2011. The results of the German A2 level course were announced and all the 18 students qualified in the examination.

Articles

----By Ruddaraju Santi.

IV-IT

IS ETHICAL HACKING ETHICAL?

I. INTRODUCTION

Understanding the true intentions of the general public is quite a
hard task these days, and it is even harder so, to understand the intentions of every single ethical hacker getting into vulnerable systems or networks. Technology is ever growing and we are encountering tools that are beneficial to the general public, but in the wrong hands can create great controversy, breaching our basic right to privacy, respect and freewill. The constant issues highlighted by the media always reporting some type of cyber crime, a study showing that nearly 90% of attacks happen on the inside [1] raising concerns of how easy it is to be working on the inside to be able to infiltrate attacks. Has ethical hacking finally come to the rescue for solving the problems or has it created new ones?

2. DISCUSSION

A. Education and training

The problem of teaching students to hack is still a very serious issue that we face today; course leaders feel that they will teach students how to improve intrusion. To understand the true intentions of students is very hard to pinpoint so the reason why ethical hacking should be used is very much a debate. Teaching a student to hack and later discover that knowledge was used to commit crimes will definitely have an impact on society as to why he was allowed to understand how to hack in the first place, but we cannot, simply, pinpoint our argument to say that it was the fault of the course leaders that allowed him to undertake the course [2]. If that were the case, then we would have major problems in other areas, such as when cars are constructed they are crash tested to fully understand areas of improvement to give users a reliable car, if companies did not test the issues, would it be the fault of the manufacturer if the car was involved in a car crash. Teaching students to hack in effect gives them a global knowledge of how to hack into computer systems with the help of University lecturers. The threat they pose is unimaginable. With the current state of mind students are in, it is
easy to imagine what kinds of threats they pose, some in the past have gone on gun sprees, killing innocent students, some starting terrorist plots and now the University helps in causing damage to networks, essentially giving students of "how to do it" directly, showing tools that can be used to do such crimes, similar to giving a burglar a crowbar to break into houses. "A problem with teaching undergraduate students using this approach is that the instructor is effectively providing them with a loaded gun". Once a student acquires new skills they may use them for good or even for bad intentions, certain policies that are not being applied at university that need to address issues for students conducting malicious acts, however these can be rectified by applying security checks on individuals which Universities do for certain courses such as ethical hacking. A criminal background check, the requirement of some sort of professional certification, and student interviews are a few measures that could potentially weed out several, if not all, students with potential malevolent intentions [5]. With an array of training courses that are available around the world it would be a difficult task to understand the reason behind their interest in the course. It could be the fact that the individual has been interested in security for a long time and that his main objective is to perfect his CV for better job Prospects and a better salary; the fact cannot be ignored that ethical hackers are highly paid individuals. To a certain extent ethical hacking is ethical. If we did not have such measures in place we would need to manually ensure that our systems are safe, so ethical hacking can ensure safety of our systems if conducted ethically.

B. Risk Management

Ethical hackers are highly paid professionals with a legitimate status and a means of access. They can minimize the risk of impact, clearly identifying benefits and flaws helping senior company
directors to understand if such activities should be undertaken. Ethical hackers could explore vulnerabilities beforehand to minimise the risk. The company could undertake penetration tests to find if they are vulnerable to attack. Finding vulnerabilities for companies not only helps the company but also minimises the risks of attacks, however ethical hackers have five days in general to perform tests, what happens if vulnerabilities are overlooked. If an ethical hacker fails to deliver results to the business and assumes the system is safe and that it has no problems, who can be liable for legal actions if a malicious hacker gets into the system? Surprisingly, a journal by IBM on ethical hacking reports, “....the client might ask “So, if I fix these things I’ll have perfect security, right?” “Unfortunately, this is not the case. People operate the client’s computers and networks, and people make mistakes. The longer it has been since the testing was performed, the less can be reliably said about the state of a client’s security. A portion of the final report includes recommendations for steps the client should continue to follow in order to reduce the impact of these mistakes in the future.”

There is little possibility of ethical hacking in work places if information is not accurate. If a company has been hacked ethically, what is the colour of the individual’s hat is it black or white? Giving special privileges to users then to return with non-accurate information as Palmer [6] describes we can ask ourselves what the differences are, as opposed to using normal security software to do the job for you. Deeper analyses showed that correctly programming systems initially would help to improve security. The main concern would be the cost to both manage and administer to provide great solutions. The idea of self-improving can be another issues, so to whom we can allow these improvements, the company or the ethical hackers to increase their knowledge and thus getting
enough information they can get hold of and then launching attacks from different parts of the world as a ethical hacking regime that would build knowledge by posing as ethical hackers and getting information to exploit. Another way to view this is, if legitimate ethical hackers who aim to remedy security issues, whether they should be allowed to access certain information and be entered into security barriers. In order to do the job we must have some leeway and be allowed to use certain tools to help them with their job, the example of Randal Schwartz, who was sentenced for only doing his job, best describes the need to use tools without any question, to identify security vulnerabilities. Ethical hackers can identify problems, but to what extent, even they would not realise a normal virus eating away at data, they may miss it or let it go since they only have a limited time to perform test, it is the hackers intent to bypass and deceive the network, the ethical hacker may be vigilant of this and compromise the network leaving it till problems arise, therefore raising the issue of “man on the inside”, so essentially ethical hackers may find it easier for hackers to infiltrate their attacks.

3. COUNTERING THE PROBLEMS

To counter problems researchers are looking towards new ways of improving ethical hacking and hacking in general from inside the company. One approach is to use models to monitor employees closely to reduce the risk of impact. One solution is to use a model approach that can seriously help in ethical hacking. Not only does this model help; it also tries to reduce the impact by identifying implications early enough to help reduce the impact of confrontation. The model depicted from [9] gives an insight to the problem and how it can be helped. To minimise risks and to further monitor the behaviour of ethical hackers and to try to eliminate the problems as and when they occur.
Not only can these models be used in the workplace they can be adopted in other fields of work such as education. Another solution could be to automate ethical hacking which causes great concerns in allowing machines take over jobs of humans, the biggest problem that lies here is that machines are prone to making mistakes and can sometimes even crash. An approach that focuses on a particular attack.

Blockage of back door leak by automatic system

4. CONCLUSIONS

To conclude the paper reports a lot of relevant information that will raise issues in the future and whether the problem needs to be handled. Technology has continued to grow at a high rate over the years and continues to do so; scholars are putting themselves in vulnerable positions by helping individuals to hack. The mind is a very powerful tool that has no control, the control will continue to grow proportionally with the desire to get knowledge of something that is impossible to achieve in its entity, but not forgotten in its entirety. Hackers will always find ways of getting into systems, whether they are doing it for good or bad.