ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Moral Hacking: A Way to Boost Data Security by Using Vulnerability Scanning Tools

Anish Kumar Anbukarsan[1], Ilampirai Nagarajan[2], K.G.S Venkatesan[3]

Dept. of C.S.E., Bharath University, Chennai, Tamil Nadu, India[1]

Dept. of C.S.E., Bharath University, Chennai, Tamil Nadu, India [2]

Associate Professor, Dept. of C.S.E., Bharath University, Chennai, India[3]

ABSTRACT: The state of security on the net is dangerous and obtaining worse. One reaction to the present state of affairs is termed as Moral Hacking that makes an attempt to extend security protection by distinguishing and fix familiar security vulnerabilities on systems in hand by different parties. As public and personal organizations migrate a lot of of their crucial functions to the net, criminals have a lot of chance and incentive to achieve access to sensitive info through the online application. therefore the necessity of protective the systems from the nuisance of hacking generated by the hackers is to push the persons WHO can punch back the ineligible attacks on our laptop systems. So, moral hacking is associate degree assessment to check associate degreed check an info technology surroundings for doable weak links and vulnerabilities. moral hacking describes the method of hacking a network in associate degree moral approach, thus with smart intentions. This paper describes what moral hacking is, what it will do, associate degree moral hacking methodology furthermore as some tools which may be used for associate degree moral hack.

KEYWORDS: Vulnerabilities, Hacker, Cracker, Moral Hacking, Weak Links, Port and Intrusion.

I. INTRODUCTION

The immense growth of web has brought several kickshaws like electronic commerce, email, quick access to immense stores of reference material etc. As, with most technological advances, there's conjointly different side: criminal hackers UN agency can on the QT steal the organization's info and transmit it to the open web. These sorts of hackers square measure known as black hat hackers [1]. So, to beat from these major problems, another class of hackers came into existence and these hackers square measure termed as moral hackers or white hat hackers. So, this paper describes moral hackers, their skills and the way they are going regarding serving to their customers and plug up security holes. moral hackers perform the hacks as security tests for his or her systems. This kind of hacking is usually legal and trustworthy. In different terms moral hacking is that the testing of resources for the betterment of technology and is focussed on securing and protective information processing systems [2].

So, just in case of laptop security, these tiger groups or moral hackers would use an equivalent tricks and techniques that hacker use however in a very legal manner and that they would neither harm the target systems nor steal data. Instead, they might appraise the target system's security and report back to the homeowners with the vulnerabilities they found and directions for the way to remedy them. moral hacking may be a means of doing a security assessment [5]. Like all different assessments Associate in Nursing moral hack may be a random sample and spending Associate in Nursing moral hack doesn't mean there are not any security problems. Associate in Nursing moral hack's results may be a elaborate report of the findings yet as a sworn statement that a hacker with bound particular an exact precise definite an explicit quantity of your time and skills is or isn't ready to with success attack a system or get access to certain data. moral hacking will be categorised as a security assessment, a form of coaching, a take a look at for the safety of Associate in Nursing data technology atmosphere . Associate in Nursing moral hack shows the risks Associate in Nursing data technology atmosphere is facing and actions will be taken to scale back bound risks or to simply accept them.

10.15680/ijircce.2015.0303194

We can simply say that moral hacking will dead match into the safety life cycle shown within the below figure.

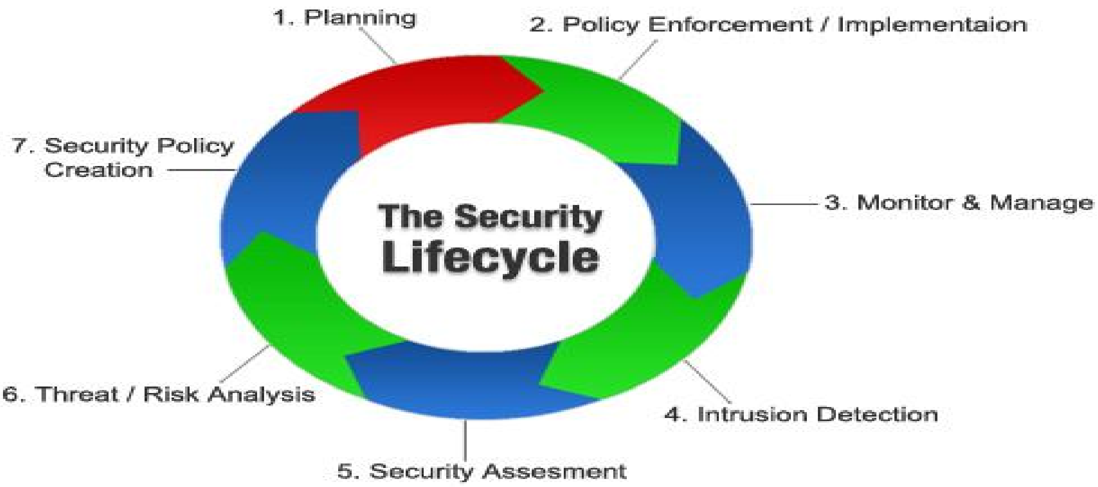

FIGURE 1: SECURITY LIFE CYCLE

II. WORKING OF AN MORAL HACKER

The operating of a moral hacker involves the beneath mentioned steps:

- Obeying the moral Hacking Commandments: each moral Hacker should follow few basic principles. If he doesn't follow, unhealthy things will happen. Most of the time these principles not needed or forgotten once coming up with or execution moral hacking tests. The results are even terribly dangerous.
- Working morally: The word ethical will be outlined as operating with high skilled morals and principles. Whether or not you're playacting moral hacking tests against your own systems or for somebody World Health Organization has employed you, everything you are doing as a Moral Hacker should be approved and should support the company's goals. No hidden agendas area unit allowed. Trustiness is that the final objective. The misuse of knowledge is totally not allowed [9].
- Respecting Privacy: Treat the knowledge you gather with complete respect. All data you acquire throughout your testing from internet application log files to clear-text passwords — should be unbroken non-public.
- Preventing failures in your systems: one among the most important mistakes is once individuals try and hack their own systems; they are available up with failures in their systems. the most reason for this can be poor coming up with. These testers haven't browse the documentation or misconceive the usage and power of the protection tools and techniques. you'll simply produce miserable conditions on your systems once testing. Running too several tests too quickly on a system causes several system lockups. several security assessment tools will management what number tests area unit performed on a system at a similar time. These tools area unit particularly handy if you would like to run the tests on production systems throughout regular business hours [11].
- Executing the plan: In moral hacking, Time and patience square measure vital. take care once you're acting your moral hacking tests.

III.MORAL HACKING METHOD

The Moral hacking method has to be planned beforehand. All technical, management and strategic problems should be thought-about. designing is vital for any quantity of take a look – from a straightforward word take a look at to any or all out penetration test on an online application. Backup off information should be ensured, otherwise the testing is also referred to as off unexpectedly if somebody claims they ne'er authorises for the tests [15]. So, a well outlined scope involves the subsequent information:

1. Specific systems to be tested.
2. Risks that square measure concerned.
3. Making ready schedule to hold take a look at and overall timeline.
4. Gather and explore information of the systems we've got before testing.
5. What's done once a serious vulnerability is discovered?
6. The precise deliverables- this includes security assessment reports and the next level report outlining the final vulnerabilities to be self-addressed, together with counter measures that ought to be enforced once choosing systems to check, begin with the foremost vital or vulnerable systems.

The overall hacking methodology consists of bound steps that square measure as follows:

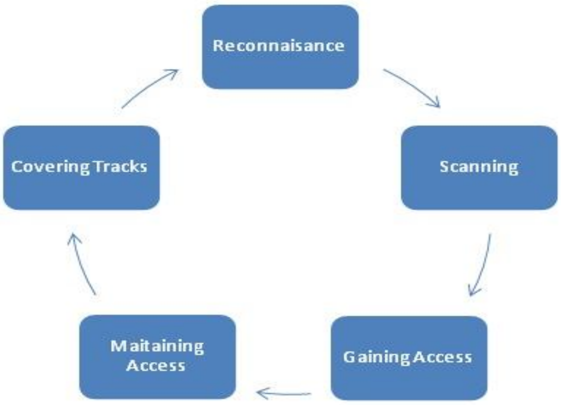

Fig. 2: PHASES OF HACKING

A.Reconnaissance:

To be able to attack a system consistently, a hacker must apprehend the maximum amount as potential concerning the target. it's necessary to urge an summary of the network and therefore the used systems. info as DNS servers, administrator contacts and scientific discipline ranges may be collected. throughout the intelligence operation part completely different reasonably tools may be used – network mapping, network and vulnerability scanning tools square measure the normally used [16]. Cheops as an example may be a superb network mapping tool that is ready to come up with networking graphs. they'll be of nice facilitate afterward throughout the attack part or to urge an summary concerning the network. A network mapping tool is extremely useful once doing an indoor moral hack. At the tip of the intelligence operation part, associate degree wrongdoer ought to have a bunch of knowledge concerning the target. With of these items of knowledge, a promising attack path may be made [19].

B. Probe and Attack :

This can be a part a pair of method as shown within the on top of fig. The probe and attack part is concerning excavation in, going nearer and obtaining a sense for the target. It’s time to do the collected, potential vulnerabilities from the intelligence operation part. Tools which might be used throughout the Probe and Attack part square measure many-sided as internet exploits; buffer overflows furthermore as brute-force may be needed. Even Trojans like NetBus may be deployed to capture keystrokes, get screenshots or begin applications and a number. The probe and attack part may be terribly time intense, particularly if brute force attack techniques square measure used or once individual items of code ought to be developed or analysed [17].

C. Listening:

This can be once more a part a pair of method i.e. scanning that may be a combination of Probe and attack and listening. being attentive to network traffic or to application knowledge will typically facilitate to attack a system or to advance deeper into a company network. Listening is very powerful as shortly mutually has management of a very important communication bottleneck. Sniffers square measure heavily used throughout the listening part. Multiple sniffers, from terribly straightforward to a lot of complexes, from console based mostly to interface driven exist for all operative systems. Some sniffers, like ettercap will even poison Arp tables to modify sniffing in switched environments and open whole new opportunities for being attentive to network traffic [18].

D. Initial Access:

This can be a part three method that isn't concerning obtaining root access, it's concerning obtaining any access to a system be it a user or root account. Once this feature is out there it's time to travel for higher access levels or new systems that square measure currently approachable through the non heritable system.

E. Advancement:

Section four i.e. Maintaining access may be a combination of Advancement and concealing method. The advancement section is perhaps the foremost inventive hard to please stage, as unlimited potentialities ar open. Sniffing network traffic could unveil bound passwords, required usernames or e-mail traffic with usable data. causation mails to directors faking some known users could facilitate in obtaining desired data or maybe access to a replacement system. most likely one conjointly needs to alter configuration files to alter or disable services or options. Last however not least, putting in new tools and useful scripts could facilitate to dig in deeper or to scan log files for additional details [21].

F. Stealth:

Some systems could also be of high price – systems that act as routers or firewalls, systems wherever a root account may be non inheritable . to own access to such systems at a later time it's necessary clean relevant log files.

G. Takeover:

Takeover may be a section five method .Once root access may be earned, the system will be thought-about won. From there on it's potential to put in any tools, do each action and begin each services on it specific machine. reckoning on the machine it will currently be potential to misuse trust relationships, produce new relationships or disable bound security checks [24].

H. Cleanup:

This might be directions within the final report on the way to take away bound trojans however most of the time this can be done by the hacker itself. Removing all traces as so much as potential is quite a obligation for the hacking craft. AN moral hack forever poses a definite risks if not properly done. A hacker might use the deployed tools or hide his attacks all told the attacks from the moral hack. He might conjointly try and attack the attackers system, so gain entry to the moral hackers system and collect all data freed from charge and already sorted and ready. getting ready AN moral hack and hold a high level of security may be a difficult task that ought to solely be done by professionals [26].

IV. SELECTION OF TOOLS IN MORAL HACKING

It is significantly essential to form certain that we have a tendency to exploitation the correct tool for moral hacking method. it's vital to grasp the non-public likewise as technical limitations. several tools specialize in specific tests, however nobody tool will take a look at for everything [28]. The additional tools you've got, the better your moral hacking efforts certify you that you're exploitation the correct tool for the task. for instance, to crack passwords, you would like a cracking tool like LC4 or Aircrack-NG. Similarly, for AN in-depth analysis of an online application, a

Web-application assessment tool (such as Whisker or WebInspect) is additional applicable than a network analyzer (such as Ethereal). There are varied characteristics for the employment of tools for moral hacking that are as follows:

1. Adequate documentation
2. Careful reports on the discovered vulnerabilities, as well as however they'll be fastened
3. Updates and support once required
4. High level reports that may be conferred to managers

These options will save the time and energy after we are writing the report. Time and patience are vital in moral hacking method. We must always use caution after we are playing the moral hacking tests [21]. It's not sensible to form certain that no hackers are on our system. Simply certify to stay everything non-public if potential. Do cipher the emails and files if potential. The list and outline of assorted tools utilized in the moral hacking method are as follows:

A.Scanning tools:

The Scanning tools quite useful within the moral hacking method. In technical detail, a scanner sends a message requesting to open a reference to a pc on a selected port. (A port is AN interface wherever completely different layers of computer code exchanges information). The pc has a possibility of ignoring the message, replying negatively to the message, or gaps a session. Ignoring the message is that the safest since if there aren't any open services it should be onerous for a cracker to see if a pc exists. Once a port scan reveals the existence of AN open service, a cracker can attack recognized vulnerabilities. Once a cracker scans all computers on a network and creates a network map showing what computers running, what in operation systems and what services are accessible, virtually any reasonably attack is feasible as well as automatic scripting program attacks and social built attacks [25]. The primary scanner was the protection administrator's tool for analysing networks – the Tempter introduced by Dan Farmer in 1995. The Tempter (Security Administrator tool for analysing networks) might analyse any system accessible over the net. However the question here is that why ought to anyone with net presence and no interest in cracking different systems find out about scanners? The solution is to be told what fruity can see in their own net presence since scanners are common attack beginning points. Fruity seek for unauthorized services like somebody running a server with identified issues, AN unauthorized server on a high port. Port scanning is done manually from one pc to be told concerning target systems or it is done mechanically by program originating from multiple computers on completely different networks to one target system over an extended amount of your time. Port scanners like different tools, have each offensive and defensive applications- what makes a port scanner smart or evil is however it's used. Actually, a port scanner is at the same time each the foremost powerful tool a moral hacker will use in protective the network of computers and therefore the most powerful tool a cracker will use to come up with attacks [29]. The table below shows a number of the scanning tools that facilitate within the moral hacking process:

Commercial Scanners	*Network Ass Cyber cop*
Sniffers	*Subterfuge, Kismet*
Network Scanners	*OpenVAS, Icinga, nSure*
War – Dialing	*iWar, WarVox*
Password Crackers	*Aircrack-NG, Brutus*
Firewall Scanners	*Firewalk*
Security and Vulnerability Scanning	*Nessus, ISS, cybercop*

Password cracking tools: Password cracking does not have to involve fancy tools, but it is a tedious process. If the target doesn't lock you out after a specific number of tries, you can spend an infinite amount of time trying every combination of alphanumeric characters. It's just a question of time and bandwidth before you break into a system [31].

There are three basic types of password cracking tests that can be automated with tools:

1. Dictionary- A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.
2. Hybrid: A common method utilized by users to change passwords is to add a number or symbol to the end. A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.
3. Brute force: The most time consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken [35].

There are some common web passwords cracking tools which are as follows:

THC Hydra	THC Hydra could be a quick network logon parole cracking tool. Once it's compared with different similar tools, it shows why it's quicker. New modules are simple to put in within the tool. You'll simply add modules and enhance the options. This tool supports varied network protocols.
Wfuzz	Wfuzz may be a net application word cracking tool that tries to crack passwords with brute forcing. It also can be accustomed realize hidden resources like directories, servlets and scripts. This tool also can determine completely different reasonably injections as well as SQL Injection, XSS Injection, LDAP Injection, etc in net applications.
RainbowCrack	RainbowCrack could be a hash cracker tool that uses a large-scale time-memory trade off method for quicker positive identification cracking than ancient brute force tools. Time-memory trade off could be a process method during which all plain text and hash pairs square measure calculated by employing a hand-picked hash formula. When computation, results square measure keep within the rainbow table. This method is incredibly time intense. But, once the table is prepared, it will crack a positive identification should quicker than brute force tools.

B.Port Scanning tools:

Port scanning is one among the foremost common intelligence activity techniques utilized by testers to find the vulnerabilities within the services listening at well-known ports. Once you have known the information processing address of a target system through foot printing, you'll be able to begin the method of port scanning: probing for holes within the system through that you – or a malicious unwelcome person – can gain access [39]. A typical system has 2^16 -1 port numbers, every with its own transmission control protocol and UDP port that may be accustomed gain access if unprotected. The foremost in style port scanner for Linux, Nmap, is additionally on the market for Windows. Nmap will scan a system in type of stealing modes, relying upon however undetectable you wish to be. Nmap will confirm lots of knowledge a couple of target, like what hosts area unit on the market, what services area unit offered and what OS is running [38].

C. Vulnerability scanning tools:

A Vulnerability scanner permits you to attach to a target system and check for such vulnerabilities as configuration errors. A well-liked vulnerability scanner is that the freely on the market open supply tool Nessus. Nessus is an especially powerful scanner that may be designed to run a range of scans. While a windows graphical face is accessible, the core Nessus product needs Linux to run. Microsoft's Baseline Security 2610endeavour could be a free Windows vulnerability scanner. MBSA are often wont to sight security configuration errors on native computers or remotely across a network. In style industrial vulnerability scanners embrace membrane Network Security Scanner, that runs on Windows, and SAINT, that runs on numerous Unix/Linux versions [40].

V. CONCLUSION

This paper self-addressed moral hacking from many views. Moral hacking appears to be a replacement buzz word though the techniques and ideas of testing security by offensive associate degree installation aren't new in the least. But, with the current poor security on the web, moral hacking is also the foremost effective thanks to plug security holes and stop intrusions. On the opposite hand moral hacking tools have conjointly been infamous tools for dotty. So, at the moment the military science objective is to remain one step before the dotty. Moral Hacking may be a tool, that if properly used, will prove helpful for understanding the weaknesses of a network and the way they could be exploited. After all, moral hacking can play a definite role within the security assessment offerings and definitely has attained its place among alternative security assessments. Last, it should be same that the moral hacker is a lecturer WHO seeks to enlighten not solely the client, however conjointly the safety business as an entire. In an endeavour to accomplish this, allow us to welcome the moral Hacker into our ranks as a partner during this quest.

VII. ACKNOWLEDGEMENT

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, HOD of Computer Science & Engineering, **Dr. K.P. Kaliyamurthie**, Bharath University, Chennai for their motivation and constant encouragement. The author would like to specially thank **Dr. A. Kumaravel, Dean School of Computing,** for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science &Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

1. J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol. 3, No. 5, pp. 3758-3763, May 2011.
2. H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.
3. Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002.
4. Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375-379, 2002.
5. B. Reto, "Ethical Hacking", in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24, 2002.
6. B. Kevin, "Hacking for dummies", 2 nd edition, 408 pages, Oct 2006.
7. D. Manthan "Hacking for beginners", 254 pages, 2010.
8. my.safaribooksonline.com/.../introduction-to-ethical-hacking-ethics-legality.
9. K.G.S. Venkatesan and M. Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 778 – 785, 2013.
10. S. Sathish Raja and K.G.S. Venkatesan, "Email spam zombies scrutinizer in email sending network Infrastructures", International journal of Scientific & Engineering Research, Vol. 4, Issue 4, PP. 366 – 373, April 2013.
11. G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE J. Sel. Areas Communication., Vol. 18, No. 3, PP. 535–547, Mar. 2000.
12. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
13. P. Indira Priya, K.G.S.Venkatesan, "Finding the K-Edge connectivity in MANET using DLTRT, International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5898 – 5904, 2014.
14. K.G.S. Venkatesan and M. Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, PP. 75 – 80, April 2013.
15. Ms. J.Praveena, K.G.S. Venkatesan, "Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.
16. K.G.S. Venkatesan. Dr. V. Khanna, "Inclusion of flow management for Automatic & dynamic route discovery system by ARS", International Journal of Advanced Research in computer science & software Engg., Vol.2, Issue 12, PP. 1 – 9, December – 2012.
17. Needhu. C, K.G.S. Venkatesan, "A System for Retrieving Information directly from online social network user Link ", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6023 – 6028, 2014.
18. K.G.S. Venkatesan, R. Resmi, R. Remya, "Anonymizimg Geographic routing for preserving location privacy using unlinkability and unobservability", International Journal of Advanced Research in computer science & software Engg., Vol. 4, Issue 3, PP. 523 – 528, March – 2014.
19. Selvakumari. P, K.G.S. Venkatesan, "Vehicular communication using Fvmr Technique", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6133 – 6139, 2014.
20. K.G.S. Venkatesan, G. Julin Leeya, G. Dayalin Leena, "Efficient colour image watermarking using factor Entrenching method", International Journal of Advanced Research in computer science & software Engg., Vol. 4, Issue 3, PP. 529 – 538, March – 2014.
21. K.G.S. Venkatesan. Kausik Mondal, Abhishek Kumar, "Enhancement of social network security by Third party application", International

Journal of Advanced Research in computer science & software Engg., Vol. 3, Issue 3, PP. 230 – 237, March – 2013.

22. Annapurna Vemparala, Venkatesan.K.G., “Routing Misbehavior detection in MANET’S using an ACK based scheme”, International Journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 261 – 268, 2013.

23. K.G.S. Venkatesan. Kishore, Mukthar Hussain, “SAT : A Security Architecture in wireless mesh networks”, International Journal of Advanced Research in computer science & software Engineering, Vol. 3, Issue 3, PP. 325 – 331, April – 2013.

24. Annapurna Vemparala, Venkatesan.K.G., “A Reputation based scheme for routing misbehavior detection in MANET”S ”, International Journal of computer science & Management Research, Vol. 2, Issue 6, June - 2013.

25. K.G.S. Venkatesan, “Planning in FARS by dynamic multipath reconfiguration system failure recovery in wireless mesh network”, International Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 8, August -2014.

26. R. Ghosh, K. Trivedi, V. Naik, and D. S. Kim, “End-to-end performability analysis for infrastructure-as-a-service cloud: An interacting stochastic models approach,” in *Dependable Computing(PRDC), 2010 IEEE 16th Pacific Rim International Symposium on*, PP. 125 –132, December – 2010.

27. K.G.S. Venkatesan, AR. Arunachalam, S. Vijayalakshmi, V. Vinotha, “Implementation of optimized cost, Load & service monitoring for grid computing”, International Journal of Innovative Research in computer & comm. Engineering, Vol. 3, Issue 2, PP. 864 – 870, February -2015.

28. R. Karthikeyan, K.G.S. Venkatesan, M.L. Ambikha, S. Asha, “Assist Autism spectrum, Data Acquisition method using Spatio-temporal Model”, International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 2, PP. 871 – 877, February -2015.

29. K.G.S. Venkatesan, B. Sundar Raj, V. Keerthiga, M. Aishwarya, “Transmission of data between sensors by devolved Recognition”, International Journal of Innovative Research in computer & comm. Engineering, Vol. 3, Issue 2, PP. 878 – 886, February -2015.

30. K.G.S. Venkatesan, N.G. Vijitha, R. Karthikeyan, “Secure data transaction in Multi cloud using Two-phase validation”, International Journal of Innovative Research in computer & comm. Engineering, Vol. 3, Issue 2, PP. 845 – 853, February -2015.

31. K.G.S. Venkatesan, “Automatic Detection and control of Malware spread in decentralized peer to peer network”, International Journal of Innovative Research in computer & comm. Engineering, Vol. 1, Issue 7, PP. 15157 – 15159, September -2013.

32. Satthish Raja, S K.G.S. Venkatesan, “Electronic Mail spam zombies purify in email connection”, International Journal of Advanced Research in Computer Science Engineering & Information Technology, Vol. 1, Issue 1, PP. 26 – 36, June – 2013.

33. K.G.S. Venkatesan. Dr. V. Khanna, S.B. Amarnath Reddy, “Providing Security for social Networks from Inference Attack”, International Journal of Computer Science Engineering & Scientific Technology, March – 2015.

34. K.G.S. Venkatesan, Dr. Kathir. Viswalingam, N.G. Vijitha, “ Associate Adaptable Transactions Information store in the cloud using Distributed storage and meta data manager”, International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 1548 – 1555, March -2015.

35. K.G.S. Venkatesan, Dr. V. Khanna, Dr. A. Chandrasekar, “Autonomous system (AS) for mesh network by using packet Transmission & Failure detection”, International Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 12, PP. 7289 - 7296, December – 2014..

36. K.G.S. Venkatesan, Dr. V. Khanna, Jay Prakash Thakur, Banbari Kumar, “Mining User profile Exploitation cluster from computer program Logs”, International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 1557 – 1561, March -2015.

37. Ms.J.Praveena, K.G.S.Venkatesan, “Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing”, International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.

38. K.G.S.Venkatesan, “Planning in FARS by dynamic multipath reconfiguration system failure recovery in wireless mesh network”, International Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 8, August -2014.

39. K.G.S. Venkatesan. Dr. V. Khanna, Dr. A. Chandrasekar, “Reduced path, Sink failures in Autonomous Network Reconfiguration System (ANRS) Techniques”, ”, International Journal of Innovative Research in computer & comm. Engineering, Vol. 3, Issue 3, PP. 2566 - 2571, March -2015.

40. Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , “Ethical Hacking ” , International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.

BIOGRAPHY

	K.G.S.Venkatesan received his B.Tech degree in Computer Science & Engineering from JNT University, Hyderabad and received his M.Tech degree in Computer Science & Engineering from Bharath University, Chennai. He is currently pursuing his Ph.D in Computer Science & Engineering at Bharath University, Chennai. He has 10 years of Teaching experience and has guided many B.Tech and M.Tech papers. He is having Membership in Indian Society of Technical Education (MISTE). He attended **HIGH IMPACT Teaching Skills** Programme conducted by WIPRO MXLA (Mission 10X Learning Approach) and also **"CLOUD INFRASTRUCTURE AND SERVICES"** conducted **by ICT Academy of TamilNadu, Government of TamilNadu,** Chennai.
	Anish Kumar Anbukarasan received the B.Tech degree in Computer Science & Engineering from the Bharath University, Chennai , in 2012. He is currently working toward the M.Tech degree in the Department Of Computer Science & Engineering at Bharath University, Chennai. His research interests include Computer Networking, Network Security and Ethical Hacking.
	Ilampirai Nagarajan received the B.Tech degree in Information Technology from the Jaya Engineering College, Thirunindravur, Anna University, Chennai, in 2008. She is currently pursuing the M.Tech degree in the Department Of Computer Science & Engineering at Bharath University, Chennai. Her research interests include Database Management Systems, Data Mining and Network Security.