ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 196– 200 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

The Major Traits of Cyber Security: Case Study on Server Hardening

Kukatlapalli Pradeep Kumar
Dept. of Computer Science and Engineering and Information Technology
Christ University Faculty of Engineering
Bangalore-500029, India
kukatlapalli.kumar@christuniversity.in

E Soumya
Dept. of Computer Science and Engineering and Information Technology
MallaReddy Institute of Engineering and Technology
Hyderabad-500014, India
shrisowmi@gmail.com

***Abstract*— Information in and around the globe has so much to be linked up with the cyber infrastructure. This sophisticated infrastructure is said to be secure to some extent, perhaps the vulnerabilities always exists and paves way for catastrophes. The security concerns for the same has grown in recent times of internet age which led to a concept known as Cyber Security. The Cyber Security is one of the major aspects of research in the information security domain. It provides all the required security policies with ample algorithms in order to with stand attacks on the cyber infrastructure in various organizations. As most of the organizations depend on the information analytical processing for decision making, the storage areas viz., servers became the central entities of protection. This concept of server security emerged in order to safe guard the security assets in the storage environments with respect to the security fundamentals the information integrity, confidentiality and availability; is Server Hardening.**

Keywords*— *Cyber-attacks; Sever Hardening; patches; botnet; superdome; malware

I. Introduction

There are many instances in this internet world regarding the attacks happened on individual PCs and network devices viz., routers and switches. The concept of attacking a computer with unauthorised access is termed as cracking. However, documents says that a hacker is one who is more interested in learning and experimenting on computers. A phreaker is the one who breaks into telephone lines. In perceive of these attacks, there are different sections specified according to the Indian legalities in the ITA 2000 [15]. This act clearly explains the punishments for the committed cyber-crimes in and around the nation. The ITA 2000 online specifications and their descriptions are available with the department of electronics and information technology – deity; ministry of communications and information technology, government of India. Amongst the unanticipated and improvised recovery mechanisms that, information based organisations follow to secure their assets from man made threats, the server hardening is one among them. The course of augmenting the resources of the server aspects of a central computer is termed as Server Hardening. It is the unremitting process of making the server, robust and reliable in the information processing environments. Advanced security measures and metrics are well put in and installed in the server hardening process.

The figure .1 below shows the fundamental aspects of server hardening. Server hardening as mentioned, is protecting the server from different threats such as denial of service attacks, access rights violation, misconfigurations, IP sniffing etc., The corporate organisations uses different kinds of server including mainframes and virtual servers to meet their client/ customer needs on a scaled basis

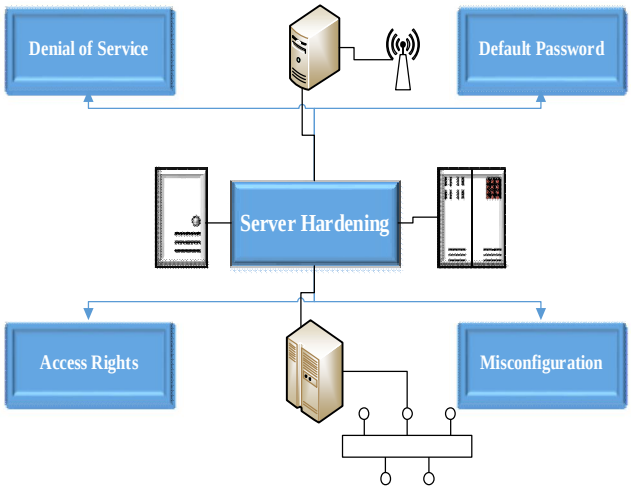

Fig. 1 The scenario Server Hardening

II. Background the Literature Survey

A. *The aspects of Cyber Security*

In the book of "The World is Flat... [2005]" Thomas Friedman calls the flattening of the technology in the current global environment as 'Triple Convergence' with respect to platform, process and people. Perhaps, resources lack in providing awareness on cyber security aspects. In light of the same bio-informatics techniques were used to forecast the attacks and crimes in the cyber infrastructure by analysing the computer infection, incursion models in human disease

ISSN 2278-3091
International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 196– 200 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

models [1]. The security metrics and measures available provides a plenty of choices which are proved to be efficient in many dynamic environments. These metrics were also customized for protecting especially the intelligent urban infrastructure systems such as Intelligent Transport Systems (ITS), Smart Grids, Cognitive Radios etc., [3].

In the regions of central Europe, Croatia, the copy right violations attracted the researchers to investigate and focus on the cybercrimes. Cluster of different groups have been examined on the awareness of intellectual property, copyright laws in the nation and the violation of copy rights both in real world and virtual world [2].

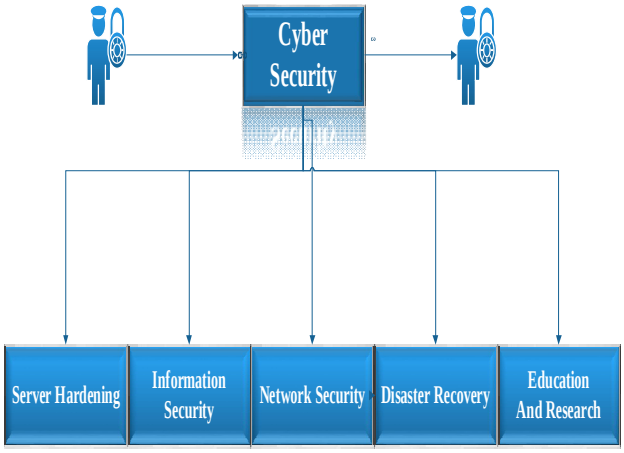

Fig. 2 The security linked with the Cyber Security

In the view towards progressing cyber security information sharing, the Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) has emerged providing a knowledge management tool for enhanced cyber information sharing and vetting of data burden sharing collaboration. The abstract level requirements have been analysed for a better CDXI concept [4]. As a part of cyber security initiative the Russian government brought in on a cyber space policy "Draft Convention on International Information Security [2011]", and the Russian military cyber proto-doctrine "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space [2011]". The political response of the Russian authorities were recorded and drafted as a case study by the researchers [5].

A survey on the cybercrimes and attacks were recently conducted by the researchers in collaboration with 'Andhra Pradesh Police Academy Hyderabad' [6]. It presented a brief descriptions on cyber criminals and crimes, types, case studies, preventive measures. The work also focused on the government agencies/ departments exclusively working on to combat cyber-crimes in India. The revolution on the protection of the cyber environments led to the theory of cyber security. Now the trend towards cyber operations does not only mean securing urban infrastructure systems, but also cyber security research and education [7]. There is a great need for collaboration among the universities on the cyber security aspects with respect to the academics and research. The cyber research teams would not only address the computer science, electrical engineering, software and hardware security, also social sciences, political science and ethics, law etc., in the years to come. The Information Technology Act-ITA, is clear with all the legalities well defined in the document released by government of India. Perhaps, awareness of the same among the common citizens in the country is still a big challenge for the government agencies. However, ambiguity among the cyber-crimes and cyber laws should be well understood and addressed for better judgments in the court of law [8]. From its inception, researchers have given the term 'security', plethora of definitions. But, the demarcation and descriptions on security were framed in terms of vulnerabilities or their absence. The security should be managed and run by pursuing a policy according to the organization's infrastructure. So the focus is, to shift from the traditional vulnerability checking to measuring the security attributes; which helps to reason security in terms of observable entities rather than conjectured, theorized causes [9].

B. The aspects of Server Hardening

In order to provide good security for the servers especially email servers, a new mechanism was developed to analyse the spam sending systems. This takes the advantage of clustering the spam based on IP addresses resolved from URLs with in spam emails rather than clustering spam according to similarities based on email contents or URLs or domain names [10]. As a part of server hardening process, an error rate named the soft error rate (SER) is calculated. The impact of the soft error is limited to the extra compute time required for correction. Collating all these factors with respect to transistors and various inner circuits' results in raw soft error rate. If the higher level layers and the bottom level layers are well protected, then this kind of protection mechanism leads to augment severs for sturdiness [11]. Providing overall security for the global internet is unmoving in some contexts and a huge challenge for the IT administrators. In pursuit of the same, researchers focused on some aspects of DNS services with respect to security. The DNS services can be secured by constantly cleansing the servers as a part of sever hardening process and also rotating the role of individual servers. This intrusion-resilient strategy contributes considerably to the total retreat of the Internet [13].

The web security hardening can be done by the deployment of reverse proxy with intrusion detection and prevention mechanisms en suiting against web attacks particularly SQL injection kind of attacks [14]. Statistical frameworks are developed for analysing honeypot arrested cyber-attack files. These frameworks are applied on the low-interaction and high-interaction sample honeypot datasets resulting in long range dependence (LRD) on honeypot-captured cyber-attacks. Such experiments led to feasible prediction of cyber-attacks in the organizations providing ample early warning time [12].

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 196– 200 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

III. Case Study I

A. Problem Scenario

The Government of India's collection of Direct and Indirect Funds were vulnerable to security treats. Torrid implements the required security measures called CA eTrust Access Control for Government of India

B. Analysis of the Case

Customer is a prime department under Government of India and processes highly sensitive financial information across its data centers distributed at different locations in India. The department is mainly responsible for matters relating to levy and collection of Direct and Indirect funds.

C. Challenges

The sheer size and type of the organization made it most vulnerable for security breaches. There was need for a high level of availability, performance density, memory scalability, and investment protection therefore they implemented Hp Superdome Servers at multiple data centers distributed over different locations in India running HP-UX 11i operating systems. The major challenges that were faced in the server infrastructure as described below:

1. Role-Based Access Control and Superuser Containment: Superuser accounts were often shared by application operators, leading to ambiguous accountability. There was no available method to restrict or delegate operators based on "who will use it".
2. No centralized enforcement administration: There were major platform security differences that existed along with lack of remote policy administration which lead to a highly decentralized system. Decentralization pointed to lack of manageability which was a big problem for the management.
3. Unrestricted Superuser: Superuser account, which have unlimited access and authority, were unrestricted making breaching a cake walk like target for hackers. Imagine one of the bad Guys in your backyard having access to your assets.
4. Inadequate auditing: Native auditing procedures were inadequate with a very low granularity level in the Operating System. Audit logs were accessible to Superusers for tampering and auditing processes could also be shut down at any time. Due to no presence of self-protecting mechanism against attacks pilferage, native logs would not be in a position to keep track of the original login and thus culprit could escape easily.
5. Consistent Cross-Platform Problems: Different platforms have different security models and for the same reason different strategies need to be used for handling the difficulties in managing various security systems which, in turn, also increase management costs.

Torrid understood the challenges faced by the customer to propose CA eTrust Access Control (AC) software that could easily mitigate the risk of different threats. eTrust AC provides capability to manage centralized access control on different servers using policy enforcement mechanism along with lots of security features. As the servers were running highly critical government applications it was not possible to put the policies into the enforced mode from day one, so initially all the policies were planned to put in the warning mode. It was a challenge in itself to provide with the accurate completion timelines to the project due to the close monitoring required for critical application and other components before enforcing the policies

D. Solutions Obtained

Torrid deployed CA's eTrust Access Control to counter the above challenges faced by the customer. Our security experts interacted with client's team to understand the basic design of the architecture, target customers, end users, and confidential assets to design eTrust Access Control framework and its policy model database (PMDB) for implementation which is used to distribute policies to clients from the servers.

There were a total of 12 superdome servers which were having a pool of 68 virtualized servers distributed over 4 locations in India. The pool of servers further comprised development, pre-production and production servers. It was a huge pool, so starting with the best and right framework was undoubtedly an essential pre-requisite.

The following steps were taken to implement the solution in the architecture:

1. Installation of eTrust Access Control server on a dedicated server.
2. As per requirements, a Master PMDB and its sub-group PMDB's were installed on the eTrust Access Control server.
3. Baseline security policies were discussed with their team and enforced on the master PMDB as these policies should be on each and every host and thereafter policies on different sub group PMDB were discussed and enforced. As there were very critical production servers, so all the policies were put in the warning mode.
4. After designing the architecture of eTrust Access Control, installation and customization of the eTrust Access Control client was done on each server and subscribed to the respective PMDB.
5. Warnings on all the servers were regularly monitored for some time, discussed with their team and then put in the restrictive mode

E. Results

After analysing the challenges, Torrid's technical expertise helped the execution of the project and the successful implementation was rolled out in the first phase itself without second iteration. All the documentation was handed over to the client and further assistance was readily available for support and solving issues.

Following benefits were reaped by the client due to the solution implementation:

1. Role-Based Access Control and Superuser Containment: By using the solution, super user privileges were fully contained and delegated. There was no back door to bypass checks and gain full

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 196– 200 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

control of the system or unauthorized access to files and services.

2. Centralized Enforcement Administration: Solution delivered a uniform level of security by bringing security up to correct level. It provided a centralized security control which allowed enterprise wide management of access enforcement and tracking with the help of Policy Model Database using a push mechanism to sequentially update the subscribers. Administrators could easily create, delete, suspend, revoke and expire user accounts centrally. They could also enforce password rules, quality, history, interval etc.
3. Data Protection: Solution helped protecting confidential and sensitive data against hackers and thefts through identity based granular access control for all files through its Host Based Intrusion Prevention feature.
4. Secure Auditing: The solution offered a very secure, scalable and reliable means to collect and report access information – It provided secure audit logs – generated locally with possibility of being collected centrally.
5. Consistent Security Policies: CA eTrust Access Control provided consistent security policy across all the HP-UX partitions

CASE STUDY II

A. Problem Scenario

Botnet owners had exploited the Windows Operating System. Microsoft equipped the systems to fight against botnets and provided permanent solutions.

B. Analysis of the Case

Botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge e.g. to send spam emails.

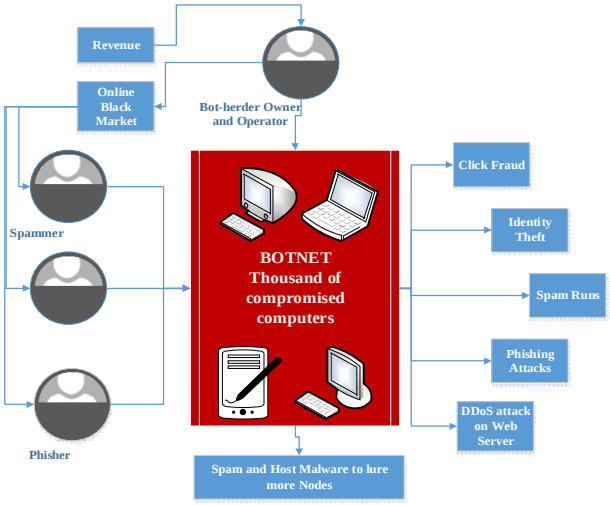

Fig. 3 The BOTNET infection through various operations

C. Solutions Obtained

In early 2011, Microsoft lawyers and U.S. marshals seized command-and-control servers for the Rustock botnet, which was housed at several web-hosting providers across the United States. Microsoft's anti-botnet actions combined with the company's numbers of vulnerability patch releases helped to clamp down on criminal activity—have turned it into a cybercrime crusader.

D. Resulting Contents

Since Microsoft was sidelined by Rustock, daily spam volume worldwide has dropped dramatically and the botnet's activity slowed to a halt.

The victories against the botnets are certainly welcome. Spam wastes the time, disk space, bandwidth, and money of everyone affected, and killing the botnets responsible for such a large proportion of spam undoubtedly benefits the Internet. But it remains an up-hill struggled for the good guys, with plenty of other botnets out there to fill our inboxes with what is at best drivel, and at worst outright dangerous!

E. Social Relevance

In the U.S., an estimated 86,000 Rustock-infected PCs in March had been reduced to some 53,000 by June 2011, a drop of 38% afterwards. Other countries saw even bigger reductions such as in India, the March 2011 tally of 322,000 infected machines plummeted by 69% to approximately 99,000 in June.

The Microsoft's Active Response for Security (MARS) team oversees the botnet effects and shared its findings about botnets with other members of the security industry. This includes taking down botnets (armies of malware-infected PCs operating secretly under the remote control of a criminal), seizing the infrastructure and domains criminals use to control them and taking the information we gain in those efforts to help better protect the Internet community and our customers.

Project MARS is a joint effort between the Microsoft Digital Crimes Unit, Microsoft Malware Protection Center, Customer Support Services and Trustworthy Computing. Recent examples of MARS include: Operation b49 (the Waledac takedown), Operation b107 (the Rustock takedown), Operation b79 (the Kelihos takedown) and Operation b71 (the Zeus disruption)

IV. Conclusion

Every server security conscious organization will have their own methods for maintaining adequate system and network security. Often you will find that server hardening consultants can bring your security efforts up a notch with their specialized expertise.

Some common server hardening techniques are to use data encryption for your communications, avoiding use of insecure protocols that send information or passwords in plain text. Minimizing the unnecessary software on the servers. The operating system is kept up to date, especially the security patches. The user accounts should have very strong passwords and passwords should be changed on a regular basis and not to

be reused again. The accounts have to be locked after too many login failures. Often these login failures are illegitimate attempts to gain access to your system. Empty passwords should not be permitted. Proper backups should be maintained and provide physical server security.

Acknowledgment

The paper is dedicated to the research and faculty fraternity working on the different heterogeneous security areas. Special thanks to our post graduate students Divya and team for working on the cases, referred in this work. Also our sincere gratitude to the Christ University Faculty of Engineering, Bangalore and MallaReddy Institute of Engineering and Technology Hyderabad, India.

References

[1] Walker, J.J. ; Jones, T. ; Blount, R. "Visualization, Modeling and Predictive Analysis of cyber security attacks against cyber infrastructure oriented systems" Technologies for Homeland Security (HST), 2011 IEEE International Conference, 2011 , Page(s): 81 – 85

[2] Vukelic, B. ; Skaron, K. "Cyber crime and violation of copyright", Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention, 2013 , Page(s): 1127 – 1130

[3] Bayuk, J.L. ; Mostashari, A., "Measuring Cyber Security in Intelligent Urban Infrastructure Systems", Emerging Technologies for a Smarter World (CEWIT), 2011 8th International Conference & Expo, 2011 , Page(s): 1 – 6

[4] Dandurand, L. ; Serrano, O.S., "Towards Improved Cyber Security Information Sharing: Requirements for a Cyber Security Data Exchange and Collaboration Infrastructure (CDXI)", Cyber Conflict (CyCon), 2013 5th International Conference, 2013 , Page(s): 1 – 16

[5] Giles, K., "Russia's Public Stance on Cyberspace Issues", Cyber Conflict (CYCON), 2012 4th International Conference, 2012 , Page(s): 1 – 13, IEEE Conference Publications

[6] Gunjan, Vinit Kumar ; Kumar, Amit ; Avdhanam, Sharda, "A Survey of Cyber Crime in India", Advanced Computing Technologies (ICACT), 2013 15th International Conference, 2013 , Page(s): 1 – 6, IEEE Conference Publications

[7] Kallberg, Jan ; Thuraisingham, Bhavani, "Towards Cyber Operations", Intelligence and Security Informatics (ISI), 2012 IEEE International Conference, 2012 , Page(s): 132 – 134

[8] Kallberg, Jan ; Thuraisingham, Bhavani, "Towards Cyber Operations", Intelligence and Security Informatics (ISI), 2012 IEEE International Conference, 2012 , Page(s): 132 – 134

[9] Abercrombie, R.K. ; Sheldon, F.T. ; Mili, A., "Validating Cyber Security Requirements: A Case Study", System Sciences (HICSS), 44th Hawaii International Conference, 2011 , Page(s): 1 – 10

[10] Jungsuk Song ; Inque, D. ; Eto, M. ; Hyung Chan Kim ; Nakao, K. "An Empirical Study of Spam : Analyzing Spam Sending Systems and MaliciousWeb Servers", Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium, 2010 , Page(s): 257 – 260

[11] Muller, K.P. ; Sanda, P.N., "Soft Error Assessments for Servers", Reliability Physics Symposium (IRPS), 2010 IEEE International Conference, 2010 , Page(s): 391 – 394

[12] Zhenxin Zhan ; Maochao Xu ; Shouhuai Xu, "Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study", Information Forensics and Security, IEEE Transactions, Volume: 8 , Issue: 11, 2013 , Page(s): 1775 – 1789, IEEE Journals & Magazines

[13] Huang, Y. ; Arsenault, D. ; Sood, A., "Securing DNS Services through System Self Cleansing and Hardware Enhancements", Availability, Reliability and Security, 2006. ARES 2006. The First International Conference, 2006, IEEE Conference Publications

[14] Huang, Y. ; Arsenault, D. ; Sood, A., "Securing DNS Services through System Self Cleansing and Hardware Enhancements", Availability, Reliability and Security, 2006. ARES 2006. The First International Conference, 2006, IEEE Conference Publications

[15] MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department) New Delhi, the 9th June, 2000/Jyaistha 19, 1922 (Saka) THE INFORMATION TECHNOLOGY ACT, 2000.