International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 4, Issue 3, March – 2020, Pages: 38-45

Building a Free Open Source Based Automated System Administration Multi-threading and Parallel Programming Performance

Dr. Sharyar Wani[1], Mourad M.H Henchiri[2]

[1]Computer Science Dept. IIUM University, Malaysia
[2]Information Systems Dept. University of Nizwa, UoN, Oman

Email: mourad@unizwa.edu.om[1], sharyarwani@iium.edu.my[2]

Abstract— *Building a system integrates the thoughts of security related issues and raises the concerns about the environment compatibility in order to provide secured environments. Administrating tasks stand behind complex dashboards and gives a view to all theoretical skills on field. Yet, limitations caused by constraints are faced, and to trespass those is a must through many different feasible ways; mainly the FOSS (Free Open Source Software) is a key for plenty of Information Technology security and also administration issues. This research covers specific outcomes to fulfill systems administration expertise along with the necessary security requirements.*

Keywords— Administrating, security, FOSS, environment;

I. INTRODUCTION

Recent years, have shown the necessity to the security over digital environments as a priority with an importance not less than building a full system with its services and modules. Here, and based on the security implemented on different scenarios over real cases[1], we reach to prove the necessity of secure programming rather than simple programming which accomplishes the requests and builds systems along with all different vulnerabilities that could be exploited with the least hacking and cracking behaviors. Thus, administration starts here, when techniques of programming are spread between the usage of built in methods, that enhances security features, and user-defined methods, which are customized and do define specific processes and services [2, 3, 4].

Adoption of Free Open Source (FOS) tools and drawing Open Source (OS) solutions architectures is not restricted to specific environments, yet, available to all environments with considering constraints; the security here stands on digitally signed third party tools whenever used [5].

On the other hand, automation of tasks has received great attention and is a vital final state when deploying policies and rules of action. In this regard, administration, is defined in this research as operating systems administration and with all services and processes. Although challenges in understanding and defining the administration tasks and the whole field, here, in this research we are able to define an administration scenario suitable for both licensed environments and free environments.

No doubt, administrating a system has been one of the most important components in the study of computer science with its variety of disciplines [3, 5], and this is a complete field of study that occupies a respected share in time and resources. Through this automated systems administration, the research team have developed and implemented the following goals:

- Drawing the best system security architecture
- Automating tasks and system threads
- Solving the issue of multi-threading and parallel processing of time loss and system's memory space allocation.

The paper is organized as follows. Section II describes a deprived and isolated environment to raise up the security to a higher level. Section III presents security and administration tools, scenario and outcomes which would explain it upon environment in Section IV. Then we summarize the paper contributions and the conclusions in Section V.

II. VIRTUAL ENVIRONMENT

The project of virtual state[6]; whether a virtual machine or complete virtual network, is famous enough to trust and deploy when trying to live the secure environment whenever in action[6]. In such scenario the security is effective to consider, yet, security has to be applied over CDN (Content Delivery Networks) which is the case of the TOR project. The TOR had played the role of the dark web because of this aspect; the private network that delivers data to its end users [7].

III. AUTOMATED ADMINISTRATION

The multi-threading and parallel programming solutions provided through this research are dedicated to specialists, whom ever are system administrators or security administrators. Defining the needed and the necessary is the main study we brought to life, thus, this group of technical knowledge required by administrators is a crucial necessity ready to receive updates and amelioration upon technological advancements[8, 9].

A system administrator has to have the deep knowledge about different work environments; licensed and free and open source. In the following table we summarize the most required utilities to be automated, with a must to mention that replicas of solutions are there; since the necessity is to be upon the system administrator choice:

Command	Description	Platform
1. dd	Disk to disk backup using dd command: dd is a powerful UNIX utility, which is used by the Linux kernel makefiles to make boot images. It can also be used to copy data.	Unix: - Debian - Bash
2. rsync	rsync command: Every sysadmin should master the usage of rsync. rsync utility is used to synchronize the files and directories from one location to another. First time, rsync replicates the whole content between the source and destination directories. Next time, rsync transfers only the changed blocks or bytes to the destination location, which makes the transfer really fast.	Unix: - Debian Bash
3. Group Policies	Sysadmin rules: If you are a sysadmin, you can't (and shouldn't) break policies and sysadmin rules.	- Valid for all
4. dmseg	Troubleshoot using dmesg: Using dmesg you can view boot up messages that displays information about the hardware devices that the kernel detects during boot process. This can be helpful during troubleshooting process.	- Unix bash - Debian based OSs
5. rpm	RPM package management: This utility explains everything we need to know about managing RPM packages on redhat based system (including CentOS).	- Unix bash - Debian based Oss
6. netstat	netstat examples: Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.,	- Windows OSs
7. apt-*	Manage packages using apt-* commands: These utility practicals solves how to manage packages using apt-get, apt-cache, apt-file and dpkg commands.	- Unix Bash - Debian based OSs
8. modprobe	Modprobe command: modprobe utility is used to add loadable modules to the Linux kernel.	- Unix Bash - Debian based OSs
9. ethtool	Ethtool: Ethtool utility is used to view and change the ethernet device parameters. This utility will help in how	- Unix Bash - Debian based OSs

	you can manipulate your ethernet NIC card.	
10. nfs	NFS mount using exportfs: This is a linux solution, `how to export a file system to a remote machine and mount it both temporarily and permanently.	- Unix Bash - Debian based OSs
11. System Center Configuration Manager	Change timezone: Use one of the methods to change the timezone on your system. Depending on your OS version or distribution.	- Valid for All
12. System Center Configuration Manager	Install phpMyAdmin: phpMyAdmin is a web-based tool written in PHP to manage the MySQL database. Apart from viewing the tables (and other db objects), you can perform lot of DBA functions through the web based interface. You can also execute any SQL query from the UI.	- Valid for All
13. System Center Configuration Manager	Install PHP5 from source: Install PHP5 from source on the questioned OS environment.	- Valid for All
14. System Center Configuration Manager	Install MySQL from source: Install MySQL from source on the questioned OS environment.	- Valid for All
15. System Center Configuration Manager	Setup squid to control internet access: Squid is a proxy caching server. We can use squid to control internet access at work.	- Valid for All
16. dd mkswap swapon	Add new swap space: Use dd, mkswap and swapon commands to add swap space. We can either use a dedicated hard drive partition to add new swap space, or create a swap file on an existing filesystem and use it as swap space.	- Unix bash - Debian based OSs
17. System Center Configuration Manager	Install and configure snort: Snort is a free lightweight network intrusion detection system for both UNIX and Windows.	- Valid for All
18. System Center Configuration Manager	Register RHEL/OEL linux to support: If we have purchased support from Oracle for your Linux, we can register to oracle support network (ULN) using up2date.	- Unix bash - Debian based OSs
19. tftpboot	tftpboot setup: We can install Linux from network using PXE by installing and configuring tftpboot server.	- Unix bash - Debian based OSs
20. System Center Configuration Manager	Delete all iptables rules: When we are starting to setup iptables, we might want to delete (flush) all the existing iptables.	- Valid for All
21. System Center Configuration Manager	Disable ping replies: Someone can flood the network with ping -f. If ping reply is disabled we can avoid this flooding.	- Valid for All
22. System Center Configuration Manager	Block ip address using fail2ban: Fail2ban is an intrusion prevention framework that scans log files for various services (SSH, FTP, SMTP, Apache, etc.) and bans the IP that makes too many password failures. It also updates iptables firewall rules to reject these ip addresses.	- Valid for All
23. dpkg	Package management using dpkg: On	- Unix bash

	debian, we can install or remove deb packages using dpkg utility.	- Debian based OSs
24. System Center Configuration Manager	Alfresco content management system: Alfresco is the best open source content management system.	- Linux - Windows
25. System Center Configuration Manager	Bugzilla bug tracking system: Bugzilla is the best open source bug tracking system.	- Linux
26. System Center Configuration Manager	Rpm, deb, dpot and msi packages: How to view and extract files from various package types used by different Linux / UNIX distributions.	- Unix bash - Debian based OSs
27. System Center Configuration Manager	Backup: using rsnapshot we can backup either a local host or remote host using rsnapshot rsync utility. rsnapshot uses the combination of rsync and hard links to maintain full-backup and incremental backups. Once we've setup and configured rsnapshot, there is absolutely no maintenance involved in it. rsnapshot will automatically take care of deleting and rotating the old backups. This utility is question to apply on your appropriate platform.	- Vaild for All
28. System Center	Create user: Create users with default configuration, create users with custom configuration, create users interactively, and creating users in bulk.	- Valid for All
29. System Center Configuration Manager	Mount and view ISO file: ISO files are typically used to distribute the operating system. Most of the linux operating systems that we download will be on ISO format. This helps to view and mount any ISO file both as regular use and as root user.	- Valid for All
30. System Center Configuration Manager	Manage password expiration and aging: Linux change command can be used to perform several practical password aging activities including how-to force users to change their password. Also, in windows, the Local Security Authority (LSA) is the environment where to set and adjust passwords.	- Valid for All
31. ifconfig	ifconfig: Interface configurator command ifconfig is used to initialize the network interface and to enable or disable the interfaces.	- Unix bash - Debian based OSs
32. ipconfig	ipconfig: Interface configurator command ipconfig is used to initialize the network interface and to enable or disable the interfaces.	- Windows based OSs
33. System Center Configuration Manager	Oracle, PostgreSQL, MySQL… db systems startup and sthudown: Every sysadmin should know some basic DBA operations.	- Valid for All
34. System Center Configuration Manager	Magic SysRq key: We can safely reboot Linux using the magic SysRq key.	- Linux

35. System Center Configuration Manager	Wakeonlan: Using Wakeonlan WOL, we can turn on the remote servers where we don't have physical access to press the power button.	- Valid for All
36. lshw	List hardware spec using lshw: ls+hw = lshw, which lists the hardware specs of the system in question.	- Unix OSs
37. Devcon.exe	List hardware spec using devcon: Device+Console = devcon, which lists the hardware specs and management of the system in question.	- Windows OSs
38. dmidecode	View hardware spec using dmidecode: dmidecode command reads the system DMI table to display hardware and BIOS information of the server. Apart from getting current configuration of the system, we can also get information about maximum supported configuration of the system using dmidecode. For example, dmidecode gives both the current RAM on the system and the maximum RAM supported by the system.	- Unix OSs
39. System Center Configuration Manager	Use the support effectively: Companies spend lot of cash on support mainly for two reasons: 1. To get help from vendors to fix critical production issues 2. To keep up-to-date with the latest version of the software and security patches released by the vendors.	- Valid for All
40. yum	Yellodog Updater Modified: installing the rpm packages in the Linux using the YUM command. There are more features available in the yum command and we can also easily manage the software repository in the Linux using the YUM command.	- Unix OSs
41. System Center Configuration Manager	Template to track your hardware assests: If we are managing more than one equipment in our organization, it is very important to document and track ALL information about the servers effectively.	- Valid for All
42. Security Enhanced Linux	Disable SELinux: If we don't understand how SELinux works and the fundamental details on how to configure it, keeping it enabled will cause lot of issues. Until we understand the implementation details of SELinux we may want to disable it to avoid some unnecessary issues.	- Linux OSs
43. SandBox utilities	SandBox utilities: security utilities for Windows. In order to install and run programs in a virtual sandbox environment.	- Windows OSs
44. Cygwin	Launch Linux clients on windows: If we are using SSH client to connect to Linux	- Windows OSs

	server from a Windows laptop, sometimes it may be necessary to launch UI application on the remote Linux server, but to display the UI on the windows laptop. Cygwin can be used to install software on Linux from Windows and launch Linux X client software on Windows.	
45. System Center Configuration Manager	IPCS: IPC allows the processes to communicate with each another. The process can also communicate by having a file accessible to both the processes. Processes can open, and read/write the file, which requires lot of I/O operation that consumes time.	- Valid for All
46. Vgcreate lvcreate lvextend	Logical Volume Manager: Using LVM we can create logical partitions that can span across one or more physical hard drives. We can create and manage LVM using vgcreate, lvcreate, and lvextend lvm2 commands.	- Unix OSs
47. tcpdump	Tcpdump: tcpdump is a network packet analyzer. tcpdump allows us to save the packets that are captured, so that we can use it for future analysis. The saved file can be viewed by the same tcpdump command. We can also use open source software like wireshark to read the tcpdump pcap files.	- Valid for All
48. fdisk	Manage partition using fdisk: Using fdisk we can create a maximum of four primary partitions, delete an existing partition, or change existing partition. Using fidsk we are allowed to create a maximum of four primary partitions, and any number of logical partitions, based on the size of the disk.	- Unix OSs
49. Virtualization	VMWare fundamentals: At some point every sysadmin should deal with virtualization. VMWare is a very popular choice to virtualize server environment.	- Valid for All
50. System Center	Rotate the logs automatically: Manging log files is an important part of sysadmin life. logrotate make it easy by allowing to setup automatically log rotation based on several configurations. Using logrotate we can also configure it to execute custom shell scripts immediately after log rotation.	- Valid for All
51. ssh	Passwordless SSH login setup: Using ssh-keygen and ssh-copy-id we can setup passwordless login to remote Linux server. ssh-keygen creates the public and private keys. ssh-copy-id copies the local-host's public key to the remote-host's authorized_keys file.	- Linux - Emulators on Windows OSs

International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 4, Issue 3, March – 2020, Pages: 38-45

IV. SECURED SYSTEM PROGRAMMING

a. Microsoft

Microsoft's platforms are very reach, and capable of providing the necessary requirement to all end users while programming and implementing and even while assistance and technical calls. Here is a stable secured solution for communicating with the Operating System. The communication purpose is to be set accordingly:

1. What processes you want achieve?
2. What security level you are testing?

The arguments used are the main secret; they are the key indicator for the routine behavior. Here, we give birth to an innovative program written in C that takes care of the communication with the operating system:

```
int main(int argc, char *argv[])
{
    if (argc != 4) {
        printf("Erroneous message\n");
        return 1;
    }
    int x = strtol(argv[1]);
    int y = strtol(argv[3]);
    if (strcmp(argv[2],"value1") == 0 )
        //
    else if (strcmp(argv[2], "value2") == 0)
        //
    else if (strcmp(argv[2], "value3") == 0)
        //
    else if (strcmp(argv[2], "value4") == 0)
        //
    printf("%d\n", z);
    return 0;
}
```

The exposure of such solution makes information assurance and computer security under control; that means a clear visibility to the system entry points.

The threading programming needs special data types and special syntax when passing parameters, here we are ameliorating the script to fulfill the efficacy and efficiency rules [8]; by creating a thread to communicate with the operating system registry, then the main to apply and execute:

Also, the following revealed solution is written in C. For both defined solutions we rectified our definition with limiting the algorithm to give the skeleton; all the empty comment indicators are to be for the end user to use, modify and implement accordingly [9].

```
DWORD WINAPI R1(LPVOID params)

{

int x1 = *((int *)params);

//

}

int main()

{

int x1 = 4, x2 = 8, x3 = 10;

HANDLE r1_thread = CreateThread(NULL, 0, R1, &x1, 0, NULL);

HANDLE r2_thread = CreateThread(NULL, 0, R2, &x2, 0, NULL);

HANDLE r3_thread = CreateThread(NULL, 0, R3, &x3, 0, NULL);

HANDLE array_of_thread[3];

array_of_thread[0] = r1_thread;

array_of_thread[1] = r2_thread;

array_of_thread[2] = r3_thread;

WaitForMultipleObjects(3, array_of_thread, TRUE, INFINITE);

CloseHandle(r1_thread);

CloseHandle(r2_thread);

CloseHandle(r3_thread);

}
```

b. Unix

Through this research we are still validating; thus, the above mentioned scenario applies here, at the Unix based environments since the complete implementation would be using C/C++ scripts and with consideration that in Unix we don't deal with registries. Linux software applications store their configuration in text-based [9]. Machine specific configs

are stored in the /etc directory tree. Thus, user specific settings are typically in the users' home directory and often in "hidden" files that start with a ".".

V. CONCLUSION

Data at rest is a hard process to analyze for the purpose of APT detection and anomalies detection. Thus, programming the operating system is defining a clear scenario for administrators and an expert path for synchronizing the processes execution which are a drawback of the benefits of the technology expertise. Since there are various constraints to implement an administration solution valid and genuine for all platforms, mastering the necessary skills is a know-all challenge. The first priority draws the requirements to the technology updates with all its secrets of the date. Then, it is no dough that the security is the next necessity in the context of information systems. And here, after all, where the activities and routines automation necessity is seen and must be implemented by administrators. And since the automation is a user routine application, then, it is a question to failure and must be implemented by the usage of the most common up to date built in routines and via smart scenarios.

REFERENCES

[1] Security Journal Nedap Security Management Issue 2014 http://www.nedapsecurity.com/sites/default / files/nedap_security_journal_2014.pdf

[2] The Proactive Factors Framework: A Key to Programming for Benefits and Evaluating forResults Journal of Park and Recreation Administration, Vol 15, Number 3, pp- 1-18

[3] Programming Evaluation Process Using Hybrid Cost Estimation Model International Journal of Software Engineering and Its Applications Vol. 8, No. 10 (2014), pp. 55-64 http://dx.doi.org/10.14257/ijseia.2014.8.10.0 6

[4] JESA The USENIX Journal of Education in System Administration Volume 1, Number 1, September 2015, www.usenix.org/jesa/0101

[5] An analysis of security issues for cloud computing Print ISSN1867-4828 Online ISSN1869- 0238

[6] Hashizume et al.; licensee Springer. 2013 Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.2011. Available: https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf Available: Google Scholar

[7] Tor, what is it good for? Political repression and the use of online anonymity- granting technologies SAGE Journals, March 31, 2016

[8] The Development and Administration of Automated Systems in Academic Libraries Information Technology and Libraries ISSN:2163-5226, Vol 1, No 1

[9] Linux Journal System Administration Special Issue 2009 Available http://www.linuxjournal.com/files/linuxjournal. com/pdf/sysadmin_09.pdf