ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

JUST ENOUGH ADMINISTRATION (JEA) VIA SYSINTERNALS MICROSOFT SECURED INFRASTRUCTURE

[1] Dr Mourad M.H Henchiri, [2]Mouhammed Shafakhat
[1]Information Systems Department,University of Nizwa, UoN Oman
[2]Research Department,University of Nizwa, UoN Oman

Abstract— Microsoft Windows operating systems internals are so may; even with the variety of operating systems' distributions available in the market. Beneficial, useful, and trustworthy to do all the tasks much more easy, they are making the life of Windows admins easy. All the availability are representing signed genuine and licensed utilities ready to be deployed in the search for the knowledge over the Microsoft Windows environment and they are the Just Enough Administration (JEA) utilities for all administrators. The sysinternals from Microsoft is a described as a file share that allows access to the totality of the Sysinternals utilities. Microsoft had developed this to test an alternate distribution mechanism for different Microsoft environments' utilities. Which is a prof to allow end users to download and run these tools from any Microsoft based computer connected to the Internet without having to navigate to a specific webpage, download zipped files then extract them. Even if the end users are unfamiliar with Microsoft Windows Sysinternals, Microsoft has developed a solution for their education; thus, it is highly recommended that every visitor to the website at the Microsoft technet sysinternals would absorb all the technical knowledge required before using these utilities.

Keywords— JEA, technet, sysinternals, sysmon.

I.Introduction

The development of the necessary technical skills required for all the Microsoft systems administrators is a daily endless process due to the global daily modernization of the sector. Thus, duplication of utilities on the market is a serenity sign; that gives the felling of trust towards the technology day by day. In this research our main and focal concentration is towards the clustering act of the built-in windows utilities and also the external Microsoft utilities; which are open access to all windows users online. Skills to be discussed in this paper are related to administration on the windows environments with all of the global catalogues (GC) contents. We would be describing the best experience with the most famous sysinternals utilities from Microsoft. Besides to the administration, the digital security is a main concern in such contexts. Thus, the discoveries revealed in this paper are covering:

- Sysinternals utilities administrators best friends.
- Security policies four fold approaches.
- Technical experiments of the sysmon utility to automate the systems administration activities.
- Internal security technical deployment.

We are presenting and intensifying the clarity of the view towards the security facts due to the modern malware architecture; which is presenting a more complex algorithms designs, that even the professional AV (Anti-Viruses) would have difficulty in detecting them.

II.Environment Physical Access

In modern environments[1], security tackles modern issues; thus, physical infrastructure is a crucial target to different malware. Vulnerabilities available in physical environments are numerous, yet, most of them are controlled and given measures when used[5]. Thus, physical attacks are selective, when all of them might give results, but, because of the default accounts of different physical infrastructure equipment, physical security is raised to a higher level. Vulnerabilities here, could be categorized under three groups:

1- Off-line mode access

2- Autoruns tools

3- Encryption/Decryption

The security here, pushes us to defend those scenarios; accordingly and respectively:

1- Preventing the off-line mode access, whether from the domain level or the machine level.

2- Autorun tools cannot play in modern environment by default, yet, when activated, be careful and trust investigators.

3- In Microsoft environments, data must be encrypted, in order to apply security policies

Thus, system access is an automated action mastered by all the expert administrators. Here, among the best utilities to be described first with its mode of application; the sysmon utility. Which is a sysinternal tools available from

[1]Corresponding Author

Microsoft file share resource with its official documentation. If configured well it would do exactly what administrators wish to apply in the environment. Sysmon is a background monitor that records activity to the event log for use in security incident detection and forensics, even it makes a monitoring API to the WMI (Windows Management Instrumentation) objects.

III. Administrators And Information Assurance

In the digital world, every person is secured, safe and in stable state; because nobody in the digital world care about you as you are, yet, they certainly care about your data[6]. Intruders, spies, attackers and even script kiddies care about your data. All kinds of data are available for attack and vulnerable to different kinds of attacks and data bleach, mainly[5]:

1. Injection; two main and major attacks based on the injection are analyzed, which are:

a. Steganography: the art of camouflage; hidden a complete file inside another file, file type and extension is not the matter, usually is successful. And once the injection is done, it is almost undetectable, means not to be detected, the resulting file is only seen and the one injected is hidden and to be seen only after the appropriate extraction steps.

b. Codes injection: technical analysis proves that the injection of a script inside of an executable is the best practice to spread your solutions and achieve your goals. Thus, scripts and codes are to be used clear written solutions or executable, then injected in different installing packages and setup files(might be pirated software). Once the setup or the installing package is executed the hidden and injected solution is launched silently and its process is effective.

2. impersonation Reaching roles with unauthorized permissions is an act of impersonation; raising privileges, removing authorizations, according access and editing users accounts.The scenario of impersonating an activity or a user account is successful when bad configurations are set and different access scenarios are possible which represents vulnerabilities; mainly the off line access, and also when privileges are given to non-skilled objects which by turn has access to the registry keys.

3. Phishing Which are the main prior techniques hackers and crackers think of. And they are effectively successful [7]. Social engineering is the legend of success to the phishing attacks in all scenarios. Not only the digital world I sunder attack by the phishing scenarios, but, from all network access methodologies and all networks; computer networks, mobile networks, cellular networks and even satellite networks.

Here, from the fraudulent and persistent attacks over totality of the environments that administrators can deal with is the interception of the communications; MitMs (Man in the Middle) is an exposed successful attack faced daily especially in the environment prescribed in this research; medium and large firms. Being exposed and successful is due to the weakness caused by the inevitable security policies tolerances set to make the environment active and ready to face the public usage.

This talk here is the spark of this research to define the internal security exposure [8].

When looking to the wireless communication we took the concern and we narrowed the current research deeply, and this is after a long analytical study to the access methods, which has to raise up the security level when authenticating and awarding access. This concern is vital also when designing wired infrastructures to avoid all kinds of attacks and mainly intrusions. This security takes in consideration the communication through firewalls, the secured set up of remote access and also domains configuration to avoid network based attacks like the ARP poisoning and DNS poisoning. Thus, intercepting communication is the concern of all, IT professionals, experts, technical and theoretical professors.

IV.Just Enough Administration Approach

JEA approach is a windows approach along defined within the Windows Management Framework; where its secret of creation stands behind the problem that all administrators are facing in every single environment: how to give some administrative privileges to some users but not giving them too much. As we sometimes say: have your cake and eat it too. We could observe some techniques to achieve this goal in the past but all of them were not like a solution ready to use within the modern architectures and in serious environment.

ADExplorer.exe, is a sysinternals utility that proves the high necessity to build a high secure architecture; base on the security approach. Each and every organization is set its four-fold security approach standing on the followings, with respect of the order [9]:

1. Policy set
2. Security management
3. Template and automation
4. Deployment

In a such scenario, administrators refer to the ADExplorer.exe utility to open the Active Directory when this application is installed. ADExplorer.exe is an enhanced Active Directory viewer and editor application created by Microsoft. ADExplorer.exe has the capability to access the Active Directory in the related domain without authenticity, and here is the fraudulent architecture in its essence.

With the usage and the referral to the PowerShell built in libraries it is much more enhanced the remote and local control of the environment machines. It is crucial to declare that administrators got to have the necessary technical skills to reach and extract the information in output about the data kept on a disk for a specific investigation. Digital forensics also is a matter of modern system architectures, which we present here technical algorithm to extract and investigate a hidden or deleted data from the disk in question[1].

```
$VHDPath=“C:\vhdFile.vhdx”

$disk= Mount-VHD –Path

$VHDPath Install-Module PowerForensics

Import-Module PowerForensics –Verbose

Get-ForensicFileRecord -VolumeName x: |
Where-Object {$_.Deleted}

$fr=Get-ForensicFileRecord –VolumeName x: -
Index 38 $fr | select *

$fr.Attribute

$fd=$fr.Attribute | Where-Object {$_.name –eq
‘DATA’}

$fd.DataRun

Get-ForensicVolumeBootRecord -VolumeName
x: Invoke-ForensicDD –InFile \\.\X: -Offset
(8267*4096) –BlockSize (130*4096) –Count1 –
OutFile c:\oFile
```

It is crucial to declare that you got to download the "PowerForensics" library. Here, in this context and scenario, we have information in output about the data kept on a disk for this file "oFile".

Status of the File is seen:

- Sparse
- not sparse
- where it starts; the cluster number itslength in clusters

The good news is that if it is not kept on the disk in one piece; split into multiple fragments, it is not more complicated at all but it requires more PowerShell commands which makes the process more error prone[1].

As an evaded attack, and since it is the talk of the current digital era, the ransom attack is the rich dish an unskilled administrator can afford to an attacker because of the lack of technicalities to deploy security policies set in the first approach from the four-fold approach scenarios that the organization follows.

The best description of a ransom ware is stating a real world scenario; we have followed, analyzed then concluded the results for a scientific purpose to present it in public. Here, we give the indices of the happened ransom ware attack; which it started at an incoming mail payload; a link to an audio message through the dropBox. All the criteria here proves that the attack is about to start, or in another sight, the mail receiver is on a risk of being paralyzed electronically. Till date of this research study no voice messages to be shared through the drop Box [8]. Yet, here it is a proof of that the scenario is playing the game of dominating by influence; if the mail succeeds in influencing the reader so that this attack is succeeded. The main aim of a such attack is to gain an access to the victim's device then a full control, the control based on a ransomware is the total encryption of all data available on the related storage equipment. Such attacks are tacking a deep care of conveyance; they have to be very conveying to every reader, which is the victim, in order to reach the target of the attack[1].

In this section we present the second part of the contributions of the paper; the ransomware is software that might be affecting your device as a final state of a fallacy; not trusted digital communication. In this scenario we treated the example of encrypting the Most Recently Used files (MRU):

```
Sub MostRecentAttack()

Dim E As Integer

For E = 1 To RecentFiles.Count

Selection.TypeText Text:=RecentFiles(E).Name

Selection.TypeParagraph

Next E

End Sub
```

For security purposes we presented only the browsing program used to detect the Most Recently Used files within the Microsoft environment, and written in VBA [9].

V.System Architecture

It is to consider the insider threat available at every architecture, dealing with the current domain with much more fluency than any other outsider; foreigner to the environment; reason to external attacks:

Low level designs are considered to be for the end users and centralized software deployment, and the high level designs are to be for the domain controllers and the global catalogues.

Beside of all, administrators holds their own desire to deal with GUI based environment or command based environments or even both when required.

VI. Conclusion

Security and administration research activities are updating daily, this technology we are facing nowadays is a fast paced field. Hence, in a the matter of systems administration it vital to light the security limits and evade the hackers hook, which is an aim, since the modern malware properties is a strength and success when communicating with current systems. They may impersonate identities, processes and even services without being suspected. Microsoft environment is giving birth to new technology that empowers security potential to both; users and enterprises. And from the research outcomes, the security starts from the personal knowledge and skills. It would raise the level of reconnaissance to a higher level where automated security solutions cannot achieve such reconnaissance. Modernizing the technological signature of a given corporation is the first step to face the high wave of change and the deep technical necessity to avoid been behind the market challenges and to be ready and able to prevent external intrusions. Though this security and technical issues prevention is dedicated and proper to specific measured contexts when realized, yet, it is to be valid for both platforms; genuine licensed, mainly Microsoft, and free open source. The scenario of forensics given birth in this research is the step to the cultural trust between the technical obscurity, which hides all frustrating knowledge, and the concerned users, interested by the current research outcomes.

References

[1] Software Engineering Security Modern Malware International Journal of Engineering and Information Systems (IJEAIS)Vol. 1 Issue 6, August – 2017, Pages: 197-201

[2] Best Information Security Certifications For 2017 2017 Purch http://www.tomsitpro.com/articles/ information-security-certifications,2-205.html

[3] AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011

[4] Microsoft Security Intelligence Report - Download Center Volume 16 | July through December, 2013 Available at:http://download.microsoft.com/download/7/2/b/72b5de9104f442f4a5879d08c55e0734/microsoft_security_intelligence_report_volume_16_engli sh.pdf

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

[6] Data Security and Privacy in Cloud Computing Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903

[7] Study of Ethical Hacking International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014

[8] Just Enough Administration: Windows PowerShell security controls help protect enterprise dataMicrosoft Ignite 2016 – May 2016

[9] Security+ Guide to Network Security Fundamentals© 2015, 2012, Cengage Learning

ISBN:978-1-305-09394-