ISSN:0975-9646

Live Devices: Insider Threat to Resources

Malik Junaid Gul , Pakeeza Samin, Dr. Rabia Riaz

Department of CS & IT,
University of Azad Jammu & Kashmir
City Campus , Muzaffarabad (A.K) Pakistan

***Abstract*— Gray Hat hackers/Insider can use Live Linux distribution to get into the resources of primary/secondary installed Operating system. By using such devices and distributions they can access the critical point of an Operating system which make them able to control User/Critical files that cannot be accessed within the operating system or can accessed either by Administrator or Operating system due to windows Security policy. Here we discuss that the Insider/ Gray hat hacker, by using such device, can manipulate windows operating system registries to get desired information. These accessed file can be copied to device for further change and analysis in secure place.**

***Keywords*— Hacker, registries, critical point, Linux distributions.**

I. INTRODUCTION

With the growth of computer storage technology, both Government & Private organizations are changing their ways of storing information. Database management system made it easy to access, store and manipulate Information. But DBMS is not only the way to save information, organization like Military or other security department develops their own ways of storing data in computer with or without DBMS. This makes them able to share sensitive information in real time with security. But to do this they need software like "Army Information Technology Management" [1]. Another reason of such conversion is the decreasing rate of storage hardware [2]. But, like with old Traditional file system, Information stored in computer need security [3]. The people who commit crime of stealing information are known as "Hackers" [4].Now hacker have access to devices that are cheap and Operating system like "Linux". But Microsoft windows still dominates the market as windows7 has round about 46% user shares. This means most of the users/Organizations around the world are using MS-windows Operating system (so as a target machine we will attack on windows7).

Tools may vary on the choice of hacker or need of scenario. As hardware tool we will use USB drive and software tool will be Linux Operating system. As Linux operating system can be loaded in to USB drives [5]. Devices loaded with bootable Operating system are referred as "Live devices".

With Live-device a hacker can breach in to system. By reading line before this one, a question came into mind that "Who can get in to an organization, use Live device for hacking?" The answer for that Question is Gray hat hackers" or "Insider". Gray Hat hackers have mixed reputation they either do hacking for good or bad. Gray hat hacking can also be done with the help of insider. So often these two terms are mixed with each other but in some situation they can give different meaning. Insider have always been a threat for any organization and dealing with such attack is extremely difficult.

So, Insider with Live device can steal information. Information that is desired by hacker can vary from situation to situation. Here our target files will be "Windows registry" & System Configuration files. Hacker can replace or edit these files for further use. Files change may be visible or not visible to authenticated user. This depends on how changes are made in files. Here we will use Hashing algorithm to find the change in such files.

II. BACKGROUND

As time pass, more and more organizations are saving the Data either online with "Cloud Storage" or create a storage mechanism on their own. This mean more complex storage systems and also more loop holes. The field of Information security is dealing with it. The field of information security flourishing its self by defining more rules and regulation for cryptography, Authentication / Authorization, User access control [6] etc. As the standard changes, new type of Hacking / Information stealing evolves. To avoid data loss many companies are also checking economic aspect of Information security. Many companies, Researchers and IT decision maker are now taking interest to find the cost of Hacking or data stealing with respect to the cost of information security to balance things out [7].So with the time people are taking security issue seriously.

Companies like McAfee has keen eye on the Hacking threats and recently publish known and unknown attack list for the year 2013 in which different types of attacks are defined [9].

Hackers mainly use Linux operating system to launch attack. This is because Linux operating system provide more flexibility for programming and have more permissions with respect to Windows Operating system. So it is recommended for hacker to use Linux operating system. A recent random poll conducted on Google+ tells just how popular Ubuntu is versus other Linux desktop distributions, with over 28% of the respondents signifying their use of Ubuntu Linux distribution.

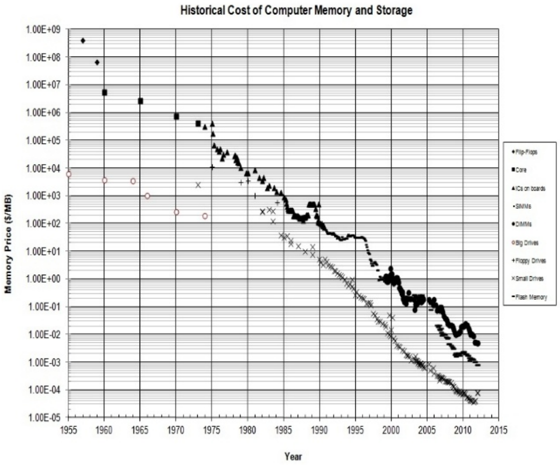
Table.I

Linux Distributions	Usage
Ubuntu	28.1%
Arch	10.2%
Mint	7.1%
Elementary OS	6.8%
Debian	5.3%
Fedora	5.2%
Other Linux distrbutions	37.3%

[10]

For our research we are using Fedora 18 [11], Wheezy Raspbain[12], Arch Linux [13], Fuduntu [14], Kali Linux [15], Damn Small Linux [16], Linux Mint [17] & Ubuntu [18].

All the above discussed Linux distribution can be installed on USB. The cause of this factor can be decreasing cost of bits on USB.[19].



[20].

As we choose Ubuntu and we also recommend Backtrack for copying the file so first we have to install it on USB drive (4GB recommended).There are many ways to create Live device but as far as procedure defined by Ubuntu official guide they use pen drive Linux software [21]. To create USB live device for Back Track (Recommended for forensic experts and hacker) use Unetbootin [22].

Now in first stage as we are attacking on registry so it is necessary to understand about Windows registry. The registry is nothing more than a central place to store all settings on the computer [23].The information that registry can store are Network setting, User passwords, Group policy, Software & Hardware configurations [24].To get this information we must know about the internal structure of windows registry that's id for which registry and how registry saves the information [25].

III. Related work

Many researchers now a days are working on windows registry. This is the most critical point of window where most important data is stored. Tanushree et al [26] said that during the past years, it is clear that Registry in Windows systems contains plenty of critical information for the forensic analysts. They claimed that the USB ports and other parts of computer which allow users to attach removable media are vulnerable of information stealing. Any user using removable media can attach that media to the system and can access registry data. They have also given the ways through which registry files are investigated and transfer of data to or from USB can be identified. The critical information located in registries is also useful for attackers. Latest research said that about 33% IT professionals claimed that they are afraid of losing their confidential data through USB devices, also 39% of IT experts are afraid of data theft by their own employees instead of outsiders. It means that insider are more risky for the organization's data. "Insider threats" are concealed to cause more financial losses then outside threats [27]. Chung-Huang Yang [28] et al used Live CD/USB to deploy their forensic system. They claimed that they can use the targeted system through live USB/CD .In their proposed system they have created a script in USB device and collected all the volatile information stored in the system. This research provide us a mile stone for our work.

IV. Methodology

In our work we have designed an attack mechanism on windows registries to prove that windows registry is the most sensitive part of the operating system and insider can access those file without leaving any trace. Almost all the configuration files of operating systems are stored in registries. We have followed the following strategy in our work.

- *Creation of Target Device:*

To attack, first we created the target system with windows 7 & Windows 8 platform. We have discussed earlier that windows registries are most critical part of OS and so they are most vulnerable too.

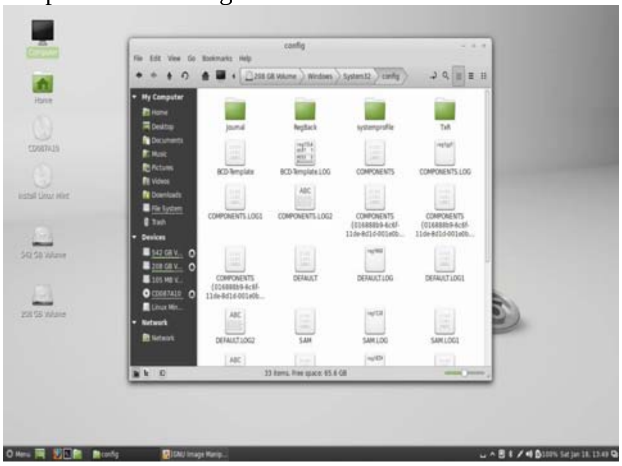
- *Creation Of LIVE USB:*

We created a USB device with live Linux distribution.

When we boot a device through USB, there will be no trace of the device in the system due to read-only nature of the medium.

- *Attack:*

To tack on registry, we have booted the victim machine (with win 7) with live USB device containing Linux distribution. Through USB we have accessed the system32/config folder, we copied that folder on USB device very conveniently and made changes to that folder. After performing attack we have checked the track record on targeted system for Our USB device and there were no such record of connected USB device. Given below is attack performed through Linux Mint.



With this technique any insider can be fatal for the organization. Insider can not only access sensitive area of windows but also to other resources containing security and other sensitive information which in future can be use illegally. But as we mentioned before there is no trace that can prove when change is made, insider can escape easily from the hands of law.

As the main part of the technique is creating live device that can easily be done at home or at secure place by the attacker. Attacker can use “Power ISO” or such other tools that support to create live devices.

Once you are in the live GUI, you can access any device attached to targeted computer but here as example we are accessing “Win reg”.

Simply copy paste the folder describe before. It is easy for attacker to analyze, expose or even handover these critical information to other hacker that can launch any further attacks.

V. Experiment & Results

As our first experiment we choose standalone computer without any client server policy enforced.

With our live devise we access registries from windows plate form one by one to check whether it is possible to copy or manipulate the file using our chosen Linux distributions.

TABLE II

Data accessed during Attack	**Linux Distributions (attacking USB)**	**Target O.S Win 7**	**Target O.S Win 8**
File acess(doc etc)	Ubuntu	Files Copied	File alteration
		yes	yes
Win Directories	Kali	yes	yes
Win Registeries	Back Track	yes	yes
	Mint	yes	yes
	Fedora	yes	yes

As from “Table II” it is clear that all the distributions successfully access the files without creating any log files for changes made.

This is because no security policy by windows was running while we are using live devices.

Then we try it on client server environment with policy.

- C: drive is not accessible for client (only admin user can open c: drive)
- Admin keep traces for client activity.
- No change can be made for pre-installed software.
- No new software can be installed without admin permission.

With above condition the results was as shown in Table III

TABLE III

Data accessed during Attack	**Linux Distributions (attacking USB)**	**Targeted O.S Win 7**	**Targeted O.S Win 8**
File acess(doc etc)	Ubuntu	Files Copied	File alteration
		yes	yes
Win Directories	Kali	yes	yes
Win Registeries	Back Track	yes	yes
	Mint	yes	yes
	Fedora	yes	yes

Now this situation made this more critical that even with the “Group policy” was enforced by the server for client machine and security policy by administrator i.e c: drive cannot be accessed by the client, potential hacker or insider still gain access to the files or folder that are restricted to the employee or client.

In this situation critical “User info” “system info” and other information that is critical for organization can be copied from the registries or Disk drive for further use. This can result in organization information revealed to public or other organizations that are looking for such information.

VI. Conclusion & Future work

Insiders are real threat to organization now a days. As programming and Operating system are getting easier more loop holes are evolving that even a beginner can use to exploit the target to get desired information. Our research shows that changes occur in windows registry, these changes can be malicious and afterwards other deadly attack can be launched. There is also a possibility that windows registry may deny changed values. But As far as forensic aspect is concerned it is hard to detect the change for whole registries. For the future we will give counter measures to prevent these registries from attackers. This will open new research direction for researchers.

Acknowledgment

Thanks to Dr. Saeed Arif Shah for his inordinate efforts. Thanks to our parents, family and friends, they were prodigious source of provision and encouragement.

References

[1] Ar25-1. “Army Information Technology”,2013, page 18-19

[2] Bureau of Labor and Statistics Producer Price Index for computer storage media. http://data.bls.gov/timeseries/pcu334112334112

[3] Merriam-Webster. “security.”Merriam-Webster Online. Accessed 04 November 2013 from

[4] www.m-w.com/dictionary/security.Merriam-Webster. “security.”Merriam-Webster Online. Accessed 04 November 2013 from http://www.merriam-webster.com/dictionary/hacker

[5] Ubuntu. “Installation From USB Stick “ Online. Accessed 05 November 2013 from https://help.ubuntu.com/community/Installation/FromUSBStick

[6] Information security principle and practice Stamp, M. 2011. Information security principle and practice. 2nd ed. A jhon willy & sons.

[7] Brecht, Matthias and Thomas Nowey (2012) "A Closer Look at Information Security Costs" WEIS 2012.

[8] O'Bryan, S. K., & CISA, C. (2006). Critical elements of information security program success. *Europe*, *26*, 4.

[9] 2013 threat prediction. McAfee Labs. Online Macafee official site.

[10] Dailyflux "Help Making the Linux Switch A Pleasure" Online. Accesses November 5, 2013 from http://www.dailyflux.com/ubuntu-tweak-making-linux-switch-pleasure/.

[11] Fedora "Fedora Project Documentation" Online. Accessed November 6, 2013 From http://docs.fedoraproject.org/en-US/index.html

[12] Wheezy Raspbain "Weezy Raspbian Documentation" Online. Accessed November 6, 2013 From http://www.raspbian.org/RaspbianDocumentation

[13] Arch Linux "Arch Linux" Online. Accessed November 6, 2013 From https://www.archlinux.org/

[14] Fuduntu "Fuduntu Linux" Online. Accessed November 6, 2013 From http://distrowatch.com/table.php?distribution=fuduntu

[15] Kali Linux "Kali Linux Documentation" Online. Accessed November 6, 2013 http://www.kali.org/official-documentation/

[16] Damn Small Linux "Damn Small Linux official" Online. Accessed November 6, 2013 http://www.damnsmalllinux.org/

[17] Linux Mint "Linux Mint Official" Online. Accessed November 6, 2013 http://www.linuxmint.com/documentation.php

[18] Ubuntu "Ubuntu Official" Online. Accessed November 6, 2013 https://help.ubuntu.com/

[19] Linux live USB "create a Linux Live USB pendrive"Online. Accessed on November 6, 2013 From http://www.linuxliveusb.com/en/help/guide

[20] USB cost per bit "Historical cost of computer memory and storage" Online. Accessed November 6,2013 From http://www.jcmit.com/MemoryDiskPriceGraph-2012Feb.jpg

[21] Ubuntu in pendrive "Install Ubuntu in USB" Online. Accessed on November 06,2013 from http://www.ubuntu.com/download/desktop/create-a-usb-stick-on-windows
http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.pdf

[22] Backtrack live USB "Installing Backtrack in USB" Online. Accessed on November 06,2013 from http://www.backtrack-linux.org/tutorials/usb-live-install

[23] Windows 7 Registry " Windows 7 Registry information for advance user" Online. Accessed on November 7,2013 from http://support.microsoft.com/kb/256986

[24] Introduction to Microsoft Windows's Registry, Robert H William III

[25] Structure of windows registry. Online. Accessed on November 07,2013 From http://msdn.microsoft.com/enus/library/windows/desktop/ms724946%28v=vs.85%29.aspx

[26] Tanushree Roy, Aruna Jain (2012). Windows Registry Forensics: An Imperative Step in Tracking Data Theft via USB Devices. International Journal of Computer Science and Information Technologies, 3(2012), 4427- 4433.

[27] Data Leakage Worldwide: The High Cost of Insider Threats: whitepaper by CISCO

[28] Fast Deployment of Computer Forensics with USBs Chung-Huang Yang et al. 2010 International Conference on Broadband, Wireless Computing, Communication and Applications