Overview of Linux Vulnerabilities

Shuangxia Niu
State Grid HAEPC Electric Power Research Institute
Henan, China
e-mail: sxniu_wang@163.com

Jiansong Mo
State Grid HAEPC Electric Power Research Institute
Henan EPRI GAOKE Group Co. Ltd
Henan, China
e-mail: jiansong_mo@yahoo.com.cn

Zhigang Zhang
State Grid HAEPC Electric Power Research Institute
Henan EPRI GAOKE Group Co. Ltd
Henan, China
e-mail: zhuanzhuan2325@sina.com.cn

Zhuo Lv
State Grid HAEPC Electric Power Research Institute
Henan, China
e-mail: 15838150770@126.com

***Abstract*—Various advanced key technologies can be effectively implemented on Linux cause its stability, high efficiency and open source nature. However, Linux Operating System(OS) itself and some of the services Linux-based inevitably have their vulnerability, namely Linux is not absolutely safe. This paper attempts to review and discuss the Linux vulnerabilities, which originates from Linux OS itself and some of the services shipped in Linux, with related cases presented. And Linux security enhancements, Linux OS hardening and Linux Security Modules (LSM),are systematically described and studied.**

Keywords-Linux vulnerabilities ;security measures; harden -ing; LSM

I. INTRODUCTION

Recently Linux OS is widely used from embedded systems to mainframes, supercomputers and servers, from education and science research to industry, commerce and national defense etc. Linux OS, a free and open source software collaboration: the underlying source code may be utilized, modified and distributed, by anyone under licenses such as the GNU General Public License[1], therefore advanced key technologies can be rapidly implemented on Linux. However rapid development can also cause unexpected vulnerabilities which can be abused by malicious users for their attacks. By this reason, It is necessary to understand the existing vulnerabilities and related measures in Linux. Up to now, actually, there are lots of documents which aimed at a certain type of vulnerability and related measures in Linux, but few of them had an overview.

In this paper, the Linux vulnerabilities and related security measures will be studied, reviewed and discussed systematically.

II. BACKGROUND

Let's start by taking a quick look at the volume of vulnerabilities over the last 26 years, as is shown in Figure 1 below[2][3].

This presents that the number of discovered and reported vulnerabilities in 2013 has a slight decline than 2012, but is markedly more than any year before 2005.
Surprisely, the Linux kernel was having the most CVE (Common Vulnerabilities and Exposures) vulnerabilities of all other products from 1988 to 2012,and the distribution in four mainstream LINUX version is presented, as shown in Figure 2 and 3 [2] respectively. The following data tells us a few interesting but serious things worth noting. More vulnerabilities information in 2013

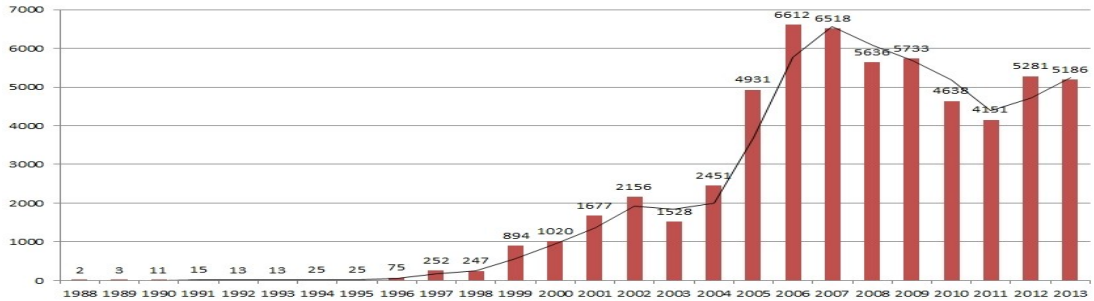

Figure 1 Vulnerabilities by year

which you may be interested in can be obtained from [3][4].

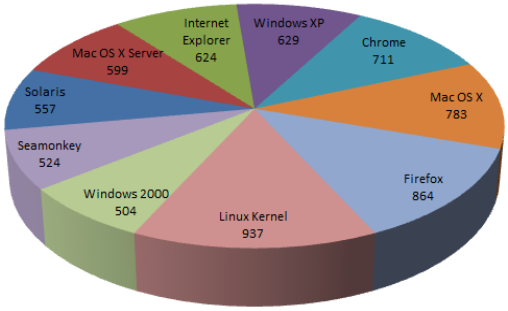

Figure 2 Top 10 products with the most reported vulnerability

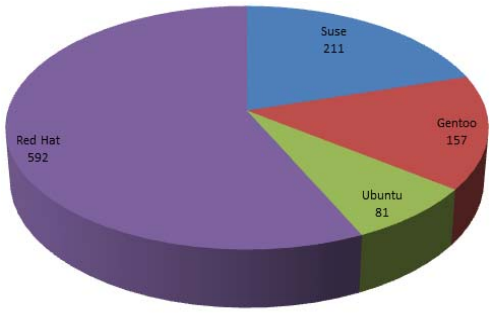

Figure 3 Vulunerabilities by Linux distribution

III. LINUX VULNERABILITIES

- **From Linux OS**

In this section, the vulnerabilities are divided into three types according to the consequences caused by exploiting these vulnerabilities.

A. *Privilege Escalation Vulnerability*

Privilege escalation, an act of exploiting a design flaw, bug or configuration oversight in software application or operating system to obtain elevated access to resources that are normally protected from user or an application. Thus an application with more privileges than intended by the system administrator or application developer can perform unauthorized actions. Various existing types of privilege escalation attack case will be described and discussed to illustrate the increasing dangers of this type of vulnerability.

Case: Security problem with *ptrace* system call

Via a PTRACE_SETREGS ptrace system call in a crafted application, race condition in the *ptrace* functionality in the Linux kernel before 3.7.5 (CVE-2013 -0871) allows local users to obtain privileges which will result in unauthorized modification, unauthorized disclosure of information and service disruption.

SSV-ID:7324[6],which was released in milw0rm.c -om,and elevated privileges to root privileges and kernel privileges from the general privileges by exploiting the special features that *ptrace* just have the function to change register when debugging the subprocess. During which the address of kernel services program anti-go to kernel space when Linux kernel calls int 0x80(%eax) while the final jump is indeed using registers %rax. Then kernel backdoor function could be executed.

Undoubtedly, there are a variety of other reasons which causes privilege escalation. Such as, integer overflow in the *do_brk* [7]function for the *brk* system call in Linux kernel 2.4.22 and earlier allows local users to obtain root privileges, and buffer overflow(CVE-2014-0049) in the *complete_ emulated_mmio* function in the Linux kernel before 3.13.6 allows guest OS users to execute arbitrary code on the host OS by leveraging a loop that triggers an invalid memory copy affecting certain cancel_work_item data. Besides, missing pointer/permission checks[8] and missing CPU-state sanitation(CVE-2014-1438) can also cause privilege escalation. And We will not discuss these reasons one by one here, actually, we can achieve more comprehens -ive cases and details of this type vulnerabilities from NVD, CVE, Security Focus, Secunia, Exploit Database, Wu Yun and Sebug, etc.

B. *Denial of Service vulnerability(DoS)*

DoS is the act of exploiting network protocol implemen -tation flaws deliberately or exhausting the attacked object's resources through brutal means directly,and the aim is to make the target computer or network can not provide normal services or access to resources, the target system to stop responding and even system services collapse.

Case: Linux kernel hash algorithm[9] vulnerability

Linux kernel hash algorithm,which is used for the Linux route catch index and fragment reassemble.When the Linux system receives a specially crafted packet from an attacker, the hash table clash will occur led to server resources are exhausted.

A same value(hash address) will be get with the operati -on of a hash algorithm for many values. To avoid address clash, these values which have same hash address are stored in the same hash slot, which makes the hash table into a singly-linked list. And the complexity of the insertion operation of this hash table soars to O(n*n) from O(n). Thus, the system will consume huge CPU resources and result in a DoS attack.

Recently, NVD released a lot of high-risk DoS vulnerab -ility in certain Linux versions. As the following two examples:

CVE-2014-2523[10], with CVSS Severity of 10 (upper limit of CVSS Severity) allows remote attackers to cause a denial of servicevia a DCCP packet that triggers a call to the (1)dccp_packet,(2)dccp_error function, or (3) dccp_ new, in the Linux kernel through 3.13.6.

CVE-2014-0100[11],with CVSS Severity of 9.3, allows remot e attackers to cause a denial of service and possibly have other unspecified impact via a large series of fragmented ICMP Echo Request packets to a system with a heavy CPU load,in the Linux kernel through 3.13.6 also.

C. IP Spoofing Vulnerability

The fault of the TCP/IP itself causes the TCP/IP stack loopholes in many operating systems, Linux is no excepti -on. IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address,aims to conceal the identity of the sender or impersonating another computing system, which exploiting a fact that there is no any check for the source IP address of IP packets and a forged source IP address from attacker can't be observed. IP address spoofing commonly as a auxiliary method of other attack, which makes the defense relying on disable specific IP lose efficacy.

An attacking client will be disguised as a trusted host and establish the application connection with the target host based on address validation. After succeeds, the attacker can place a system backdoor for unauthorized operation. Even more, the system under attack will send a large number of SYN/ACK packets to who it believes is the originator of the connection establishment sequence[12]. In this case, two systems will be damaged: the target system and the system which is really using the spoofed address in the global routing system.

Moreover, the attacker can manufacture large amounts of data requests from different bogus IP which are selected from IP segment the server can provide, and sent them to the target computer or system with real IP hiding, which will cause a denial of service. In addition, when an unreachable source address used for TCP SYN attack, the target host will attempt to reserve resources waiting for a response. Additional host resources exhausted with the forged source address on each new packet sent is repeatedly changed by the attacker[12].

To many products of Linux operating system like firewall and IDS, this vulnerability is also fatal.

Defense against IP spoofing attacks

The main defense against IP spoofing attacks is packet filtering:ingress filtering and egress filtering. Ingress filtering, the gateway to a network usually performs, tries to prevent an outside attacker spoofing the address of an internal machine, and thus indirectly combat various types of net abuse by making Internet traffic traceable to its source[12][13]. Egress filtering is just the opposite.

The opinion that designing new network protocols and services which do not rely on the IP source address for authentication is also recommended[12].

- **From services shipped in Linux**

A. Security problem with Apache

Vulnerabilities of apache such like Apache Tomcat, Apache Camel and Apache HTTP Server Vulnerabilities are commonly exposed through the web server potentially, which may cause denial of service, web site defacement, information disclosure, privilege escalation and etc.

Systems affected and Measures: All UNIX systems running Apache and many Linux and UNIX variants come with Apache installed. Don't run Apache as root and set permissions of running Apache. Ensure that you are running the latest patch level and the core OS components referenced by Apache are patched. Disable unnecessary module and the modules of your server to function should be compiled into Apache properly [14].

B. Security problem with SSH

Secure shell (SSH),a popular service for file transfers, securing logins and command execution through a network, which is greatly more secure than the ftp, telnet, and R-command programs although, there have been multiple flaws found. Most of them are minor bugs, but individual vulnerabilities are extremely dangerous which allow attackers to remotely obtain root access on a vulnerable machine. More aecurity issues are caused by the specifically misconfiguration, mismanagement of SSH, and the failure to apply patches and updates timely[14].

It is noteworthy that the openSSL"bleeding heart" 0-day vulnerability(CVE-2014-0160),which is the most serious vulnerabilities this year and exposed on April 8th, 2014,may also cause some security problem with SSH which based on open SSL.

Systems affected and Measures: Any UNIX/Linux system running Open SSH 3.3 or earlier, SSH Communica -tion Security's SSH 3.0.0 or earlier. Ensure that you are running the recent version of SSH or Open SSH. Set privilege configuration for users' environment properly. And set Fall Back To Rsh key to "No" in the SSH configuration file.SSH services provided by a host must be adequately protected[14].

C. Security problem with SYSLOG[16]

The *sysl5*ade to the latest package.

D. Security problem with TELNET

Telnet transfer all the contents of the user, including the user name and password in the form of plaintext over the Internet, which is a security risks. For example, the Linux Console on some models of the WAGO I/O System 758 has a default password for the admin and root accounts, and a default password of guest for the guest account, a default password of user for the user account, which allows attackers to gain administrative control through the Telnet service of the system leading to a loss of integrity, confidentiality, or loss of availability (CVE-2012- 4879,CVSS Severity: 10.0) [17].

Measures: Disable Telnet service, with SSH which is more secure insteading of.

E. Security problem with FTP

The WU-FTPD daemon, a FTP server, shipped with all versions of Red Hat Linux. When the user running the FTPd daemon with root privileges, the vulnerabilities of *wu-ftpd* version with Red Hat Linux 6.1 consists of MAPPING_CHDIR buffer overflow, Message File buffer overflow and SITE NEWER consumes memory, possibly remote and local intruders can execute malicious code even cause the server to consume excessive amounts of memory, preventing normal system operation[16].

In Red Hat Linux 9,the vsftpd FTP daemon is not compiled against TCP wrappers but is installed as a standalone service, which inadvertently prevents vsftpd

from restricting access as intended. Which Provides unauthorized access, allows partial integrity confidentiality, and availability violation; causes disruption of service and unauthorized disclosure of information (CVE-2003-0135).

Directory traversal vulnerability in pure-FTPd 1.0.22 and possibly other versions, which running on SUSE Linux Enterprise Server and possibly other operating systems, allows local users to overwrite arbitrary files and gain privileges via unknown vectors, when the Netware OES remote server feature is enabled(CVE-2011-3171, CVE- 2011-0988).

measures: Update of related ftp packages.

There are still many servers such as BIND,SNMP,SSL and etc, shipped in Linux which are commonly probed and attacked, Please refer to the report[14] and the paper "Linux Securities and Vulnerabilities" [16]for more details.

IV. Linux Protective Measures

Almost all of the Linux vulnerabilities published, eitherfrom Linux OS itself or from the services shipped in it,have been fixed by patching or uprating, but it is necessary to study some protective measures. Linux security enhancement methodology can be divided into two main groups based on OS hardening and on extended access control[17].

OS Hardening: A process of securing a system by reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services to decrease the potential link from the attacker to the system[18]. Measures of hardening Linux systems, which mainly involve applying a patch to the kernel; closing open network ports; and setting up firewalls, intrusion-detection/ prevention systems. Besides, hardening scripts and tools like Bastille Linux and Apache/PHP Hardener can also deactivate unneeded features in configuration files or perform other protective measures[18].Beyond all that, Linux tailoring seems to be a good idea which includes the kernel tailoring and system library tailoring.

Extended Access Control: The discretionary access control(DAC) mechanism of Linux gives users (in a certain group) the same rights, and all processes created by a user have exactly the same privileges. The acquired permissions can also be transferred to other subjects, so a flaw in one software can lead to all the users' data being compromised[19].DAC is vulnerable to bypass and tampering and enhancing the primitive access control usually requires the kernel to be adjusted to accommodate. Linux Security Modules (LSM)[20],a frame work that allows access control models to be implemented as loadab -le kernel modules, allows the Linux kernel to support a variety of computer security models while avoiding favori -tism toward any single security implementation. Modules such as AppArmor,SELinux, Smack and TOMOYO Linux are currently accepted in the official kernel [20].

V. Conclusion

In this paper, the statistics of vulnerabilities volume over the last 26 years and their distribution in different products(top10) and Linux version was presented. Then, we emphatically and systematically discusses the vulnerabilities which originate from Linux Operating Systems(OS) itself and from some of the services shipped in Linux, respectively.And two security enhancements: hardening and LSM be briefly described and discussed.

The study of various Linux vulnerabilities in this paper suggests that we still have a long way to go in secureing existing OS. Advanced technologies or products in the pursuit of greater security while always bring some new security issues inevitably. Therefore, it is necessary to understand the existing vulnerabilities and the attack principle to protect existing systems and provide more secure advanced services, and it is which we will keep tabs on.

References

[1] Linux.http://en.wikipedia.org/wiki/Linux.

[2] Younan Y. 25 Years of Vulnerabilities: 1988-2012[J],Sourcefire Crop,2013.

[3] Cisco 2014 Annual security report[J],Cisco,2014.

[4] Secunia Vulnerability Review[J],Secunia,2014.

[5] Linux kernel race condition with PTRACE_SETREGS, Openwall, 2013.http://www.openwall.com/lists/oss-security/2013/02/15/16.

[6] SSV-ID:7324.http://sebug.net/vuldb/ssvid-7324.

[7] Morton A, Starzetz P. Linux kernel do_brk function boundary condition vulnerability[J]. 2003.

[8] Chen,Haogang,et al.,Linux kernel vulnerabilities: State-of-the-art defenses and open problems.Proceedings of the Second Asia-Pacific Workshop on Systems. ACM, 2011.

[9] http://www.jb51.net/article/3507.htm.

[10] CVE-2014-2523.http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2523&cid=2.

[11] CVE-2014-0100.http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0100&cid=2.

[12] P. Ferguson,D. Senie, Network Ingress Filtering:Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC Editor, 2000.

[13] Ingress Filtering .http://en.wikipedia.org/wiki/Ingress_filtering.

[14] Vulnerabilitie In Linux Environment,Softpanorama. http:// www. softpanorama.info/Commercial_linuxes/Security/top_vulnerabilies .shtml#Introduction

[15] http://www.centos.bz/2011/07/secure-linux-apache-web-server-10 tips/.

[16] Haluk T,Seung Y. Linux Securities and Vulnerabilities,ECE 578 Project.

[17] R.Wita,Y.Teng-Amnuay.Vulnerability profile for linux.In Proceed -ings of the 19th International Conference on Advanced Informat -ion Networking and Applications,pages 953-958. IEEE, 2005.

[18] Hardening.http://en.wikipedia.org/wiki/Hardening_(computing).

[19] Nimbalkar R,Patel P,Meshram B B.Advanced Linux Security, American Journal of Engineering Research (AJER),2013.

[20] Linux Security Modules. http://en.wikipedia.org/wiki/Linux_ Security_Modules.