

# Debian GNU/Linux

## 安全合规之路

杨旭

Day Job: 广州市腾御安信息科技有限公司

职位: 基础架构安全运维

Night Job: HardenedLinux 社区成员

Github: [github.com/n3o4po11o/](https://github.com/n3o4po11o/)

Mail: [n3o4po11o@gmail.com](mailto:n3o4po11o@gmail.com)



**HardenedLinux**

# Why Debian ?



**debian**

- 众多的开发者
- 持续更新
- 良好的生态



**debian**

- 众多的开发者
- 持续更新
- 良好的生态



# Heartbleed



Fixing time: less than 30 mins



**debian**

- 众多的开发者
- 持续更新
- 良好的生态



# Kernel

Debian Kernel maintainers: Ben Hutchings

Linux 3.2 kernel: since 2012-01-04

Frequency(avg): 2 fix a day, 2 weeks a release





# Kernel

“If you are not using a stable/longterm kernel, your machine is insecure”

– Greg Kroah-Hartman



# Kernel

“Debian is doing a awesome job. So a non-profit organization built volunteer people is doing a better job than some largest Linux provider. That"s a shame. ”

— Greg Kroah-Hartman



# Kernel

“Base you software on Debian, or update  
your kernel on time”

– Greg Kroah–Hartman



**debian**

- 众多的开发者
- 持续更新
- 良好的生态

# Mempo

ReproducibleBuilds

**MEMPO**



**TAKE ACTION NOW**  
Oppose NSA Mass Spying!

NSA image from [eff.org](http://eff.org)

Mempo image from [debian.org](http://debian.org)

Military  
&  
Intelligence

# ASTRA LINUX

Linux 4.2 kernel

PaX kernel patch

Non-standard MAC

俄罗斯国密GOST

Military  
&  
Intelligence



CLIP

# Compliance?

## STIG ?



# STIG

Security Technical Implementation Guides (STIGs)

RHEL

# STIG



redhat®



**BIG  
BROTHER  
IS  
WATCHING**

## 严重等级

CAT I	对不合理配置的利用会直接并立即影响设备的机密性、可用性和完整性
CAT II	对不合理配置的利用可能影响设备的机密性、可用性和完整性
CAT III	存在不合理的配置会降低对设备机密性、可用性和完整性的保护



check package: package hash/screen/rsh-server/ypserv/(t)ftp

check: password quality/password mechanism/cipher (PAM/ssh/Grub)


check configuration/rules: (ssh/auditd/sysctl)

check file: owner/group owner/permission

check services: automounter/Apparmor/(r)syslog

check operation system: supported release/graphical interface

and so on...




# STIG-4-Debian

基于Bash shell 支持html模板输出 检测单元“模块化”

项目地址：<https://github.com/hardenedlinux/STIG-4-Debian>

第一版完成时间：28/06/2015 （ For Debian 8 ）

第二版完成时间：19/09/2017 （ For Debian 9 ）



# STIG for Debian 9 checking report

Date : 2017-09-21

Automatic checking

Pass count: 49

Failed count: 139

[\(Click for more details\)](#)

Rule ID	Rule Title	Severity	Status
SV-86479r2_rule	The cryptographic hash of system files and commands must match vendor values.	high	FAILED
SV-86521r1_rule	The operating system must have the screen package installed.	medium	FAILED
SV-86527r2_rule	When passwords are changed or new passwords are established, the new password must contain at least one upper-case character.	medium	FAILED
SV-86529r2_rule	When passwords are changed or new passwords are established, the new password must contain at least one lower-case character.	medium	FAILED
SV-86531r2_rule	When passwords are changed or new passwords are assigned, the new password must contain at least one numeric character.	medium	FAILED
SV-86533r1_rule	When passwords are changed or new passwords are assigned, the new password must contain at least one special character.	medium	FAILED



# Debian-GNU-Linux-Profiles

<https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles>

## **DNS**

Basic bind9 configuration for lan  
Domain based routing on openwrt

## **HA**

Using UPS with NUT

## **IDS**

Deploy Bro as an IDS

## **Storage**

Manually deploy ceph cluster step  
by step





# Debian-GNU-Linux-Profiles

<https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles>

## Harbian QA

Benchmarking PaX/Grsecurity kernel  
on Debian GNU/Linux

Syzkaller crash DEMO

Kernel QA with syzkaller and qemu

## IPSEC

Building IPSEC VPN via strongswan

## MAC/RBAC

Grsecurity RBAC system with nginx

practice





# Debian–GNU–Linux–Profiles

<https://github.com/hardenedlinux/Debian–GNU–Linux–Profiles>

## **Hardened boot**

Ways to build your own trustchain for secureboot

Debian Hardened boot

Grub for Coreboot/Grub for Secure boot

Preparation for Secure Boot on Key Management Server

Set Up Unrestricted Secure Boot On supporting machine





# Debian—GNU—Linux—Profiles


<https://github.com/hardenedlinux/Debian—GNU—Linux—Profiles>

## **SSH and Cluster**

Powerful ssh(1) options you don't know

Ways to authenticate yourself to a remote virtual machine host

Recommended way to use ssh(1) for cluster management





# Debian-GNU-Linux-Profiles

<https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles>

## **Security Operation Center**

Using Logstash/Elasticsearch/Grafana to build a small SOC(Security Operation Center) from scratch

SOC Overview






# Debian-GNU-Linux-Profiles

<https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles>

## **Unclassified**

Small-scale Enterprise KVM Deployments With Kimchi

The recommended configs of host computers and management console running Debian GNU/Linux within clusters





# Debian-GNU-Linux-Profiles

<https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles>

## **TLS**

TLS Mutual Authentication in Webdav

TLS Mutual Authentication in Gitlab

OpenConnect Server For Anyconnect Compatible Service





自由软件社区生态  
&  
立法的生态

Kernel

密码工程

Compiler

Firmware

GNU/Linux 安全体系

基于自由软件的场景化加固

ONCE, THERE WERE  
SEVEN KINGDOMS...  
C. 2 YEARS BEFORE CONQUEST

Thank to:

Pax/Grsecurity Community

Debian Community

RHEL STIG

Shawn C[a.k.a "citypw"]