Linux服务器构建与运维管理

第11章：系统安全

阮晓龙

13938213680 / ruanxiaolong@hactcm.edu.cn

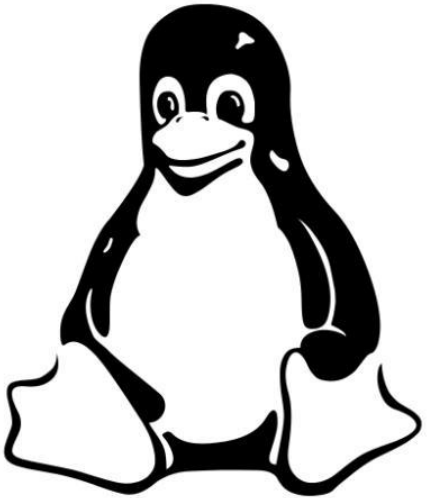
https://internet.hactcm.edu.cn
http://www.51xueweb.cn

河南中医药大学信息管理与信息系统教研室
河南中医药大学信息技术学院互联网技术教学团队
河南中医药大学医疗健康信息工程技术研究所

2022.10

提纲

- 谈谈操作系统安全
- 使用SELinux提升内核安全性
  - SELinux的工作原理、配置文件、安全策略
  - 管理SELinux
  - 案例：使用SELinux为业务提供安全保障
- 使用Firewalld提升系统安全性
  - 防火墙的工作原理、应用场景
  - 管理Firewalld
  - 案例：使用Firewalld为业务提供安全防护
- 使用Nmap实现系统安全检测
  - 安全审计与信息安全测评
  - 使用Nmap进行系统安全检测
  - 案例：对网站服务器与网站业务进行安全评估

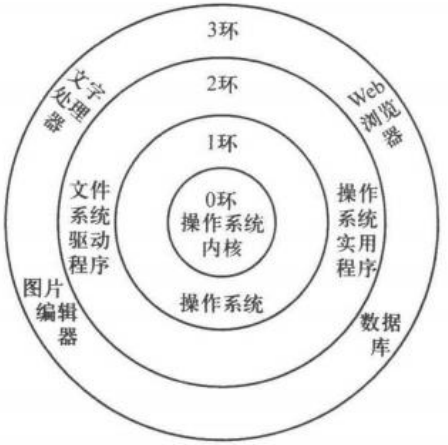


1.谈谈操作系统安全

- 系统安全是指在系统生命周期内，应用系统安全工程和系统安全管理方法，辨识系统中的隐患，采取有效的控制措施使其危险性最小，从而使系统在规定的性能、时间和成本范围内达到最佳的安全程度。
- 操作系统是信息系统的重要组成部分，操作系统的安全在整个信息系统的安全性中起到至关重要的作用，没有操作系统的安全，信息系统的安全性将犹如建在沙丘上的城堡一样没有牢固的根基。
  - 操作系统位于软件系统的底层，需要为其上运行的各类应用服务提供支持
  - 操作系统是系统资源的管理者，对所有系统软、硬件资源实施统一管理
  - 作为软硬件的接口，操作系统起到承上启下的作用，应用软件对系统资源的使用与改变都是通过操作系统来实施

1.谈谈操作系统安全

- 如果没有合理设置和防护，操作系统会成为计算机系统的薄弱点，在遭遇信息威胁时成为最脆弱的风险点。
- 为了实现安全目标：
  - 操作系统需要从用户管理、资源访问行为管理以及数据安全、网络访问安全等各个方面对系统行为进行控制，保证破坏系统安全的行为难以发生。
  - 操作系统需要对系统的所有行为进行记录，使攻击等恶意行为一旦发生就会留下痕迹，使安全管理人员有据可查。



1.谈谈操作系统安全

- 操作系统的安全风险主要分为以下3方面。
  - 硬件设备的安全风险。
    - 外部硬件设备的运行情况是否正常，硬件设备所处的环境是否长期正常稳定，在使用过程中应防止因异常关机或设备零件故障造成操作系统的无法使用。
  - 交互过程的安全风险。
    - 系统使用过程中，存在用户权限混乱、服务进程异常等安全风险。
  - 网络病毒漏洞的安全风险。
    - 当操作系统在网络中提供服务时，将会面临着服务攻击、口令破解攻击、欺骗用户攻击、网络监听攻击、端口扫描攻击、IP欺骗攻击等网络安全风险。

1.谈谈操作系统安全

- 提升操作系统安全的主要途径与方法
  - 提升物理完全
    - 安装操作系统的服务器应该放置在安装监视器、温湿度适宜的隔离房间内，确保服务器不被其他人随意接触，提升操作系统的物理安全性。
  - 删除所有测试账号、共享账号，设置合理的用户权限策略，制定复杂用户密码并定期检查等。
  - 关闭不必要的服务进程。
  - 经常更新应用程序
    - 周期性的进行操作系统补丁升级，加强系统内核安全性。
  - 严格进行防火墙规则限制。
  - 使用增强安全防护工具，定期检测操作系统的安全风险并加以修复。

1.谈谈操作系统安全

- Linux内置多种安全保护机制。
  - PAM机制
    - PAM（Pluggable Authentication Modules）机制是一套共享库，其目的是提供一个框架和一套编程接口，将认证工作由程序员交给管理员，PAM允许管理员在多种认证方法之间进行选择，它能够在不重新编译与认证相关应用程序的情况下改变本地认证方法。
  - 安全审计机制
    - 虽然Linux不能预测何时服务器会遭受攻击，但它记录入侵者行踪，记录事件信息和网络连接情况，这些信息将保存到日志列表中为后续复查提供支持。
  - 强制访问控制机制
    - 强制访问控制（MAC，Mandatory Access Control）是一种由系统管理员从全系统的角度定义和实施的访问控制机制，它通过标记系统中的主客体，强制性地限制信息的共享和流动，使不同的用户只能访问到与其相关的、指定范围的信息，从根本上防止信息泄密和访问混乱的现象。
  - 防火墙机制
    - 通过配置防火墙的访问控制、审计以及抗攻击等功能，保障服务器自身安全性。

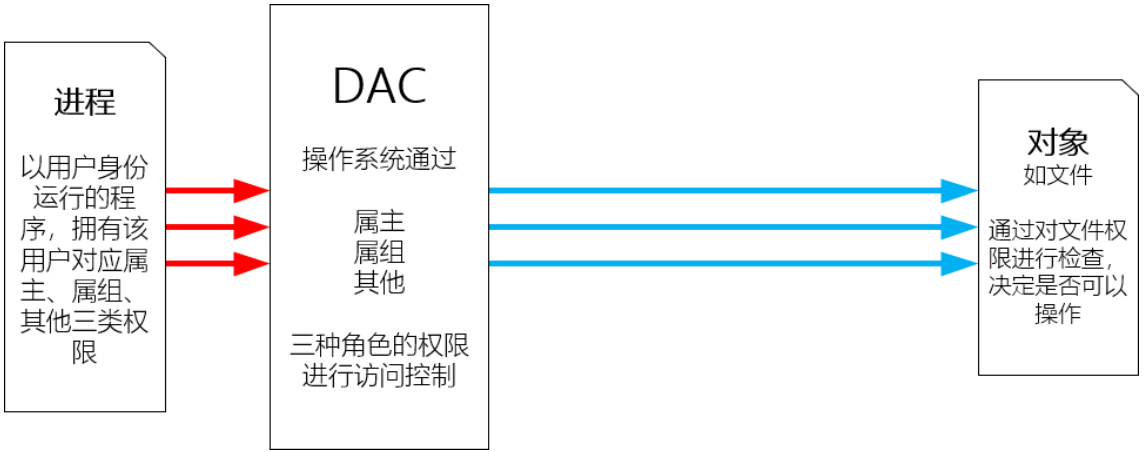
2.使用SELinux提升内核安全性

- SELinux（Security-Enhanced Linux）是基于Linux内核的强制访问控制机制的实现，旨在提升Linux操作系统内核安全性。
- Linux Kernel 2.6及以上版本均集成SELinux模块。

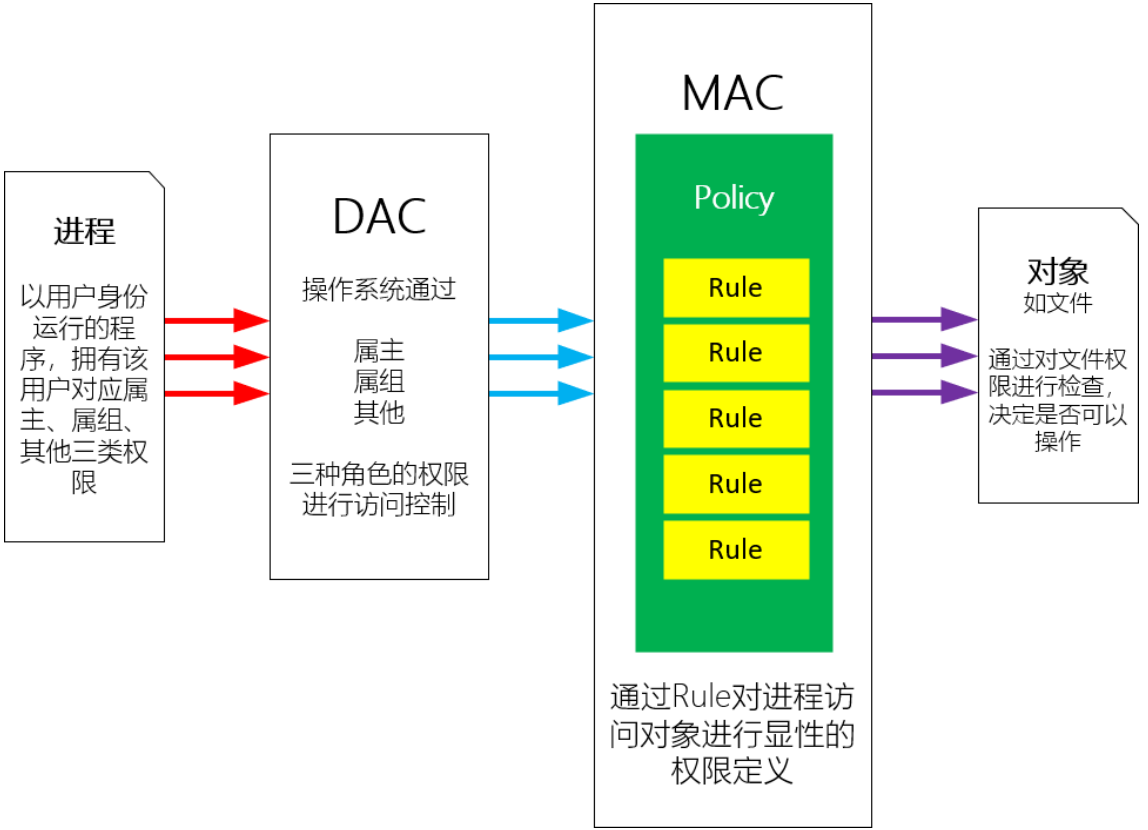
2.使用SELinux提升内核安全性

- SELinux的起源。
  - SELinux是美国国家安全局（NAS）项目，旨在增强Linux系统的安全性。
  - SELinux起源于1980年开始的微内核和操作系统安全的研究，这两个方向的研究最后形成了分布式信任计算机（DTMach，Distribute Trusted Mach）项目，融合了前期研究项目的成果。
  - 美国国家安全局参加了DTMach项目，并继续参与了后续安全微内核项目，最终产生了一个新的项目Flask，支持更丰富的动态类型的强制机制。
  - 美国国家安全局认为需要通过社区推广Flask。1999年在Linux内核中实现Flask安全架构，2000年发布第一个公共版本，叫做安全增强的Linux，并在Linux 2.2.x内核中以内核补丁形式发布。
  - 美国国家安全局在2001年Linux核心高峰会上，以普通Linux为基础架构提出了SELinux，并使用较具有弹性的MAC和Flask架构，将Linux安全等级提升至B1，同时具有资料标记与强制存取控制的功能，号称是最安全的Linux操作系统。

2.使用SELinux提升内核安全性



2.使用SELinux提升内核安全性



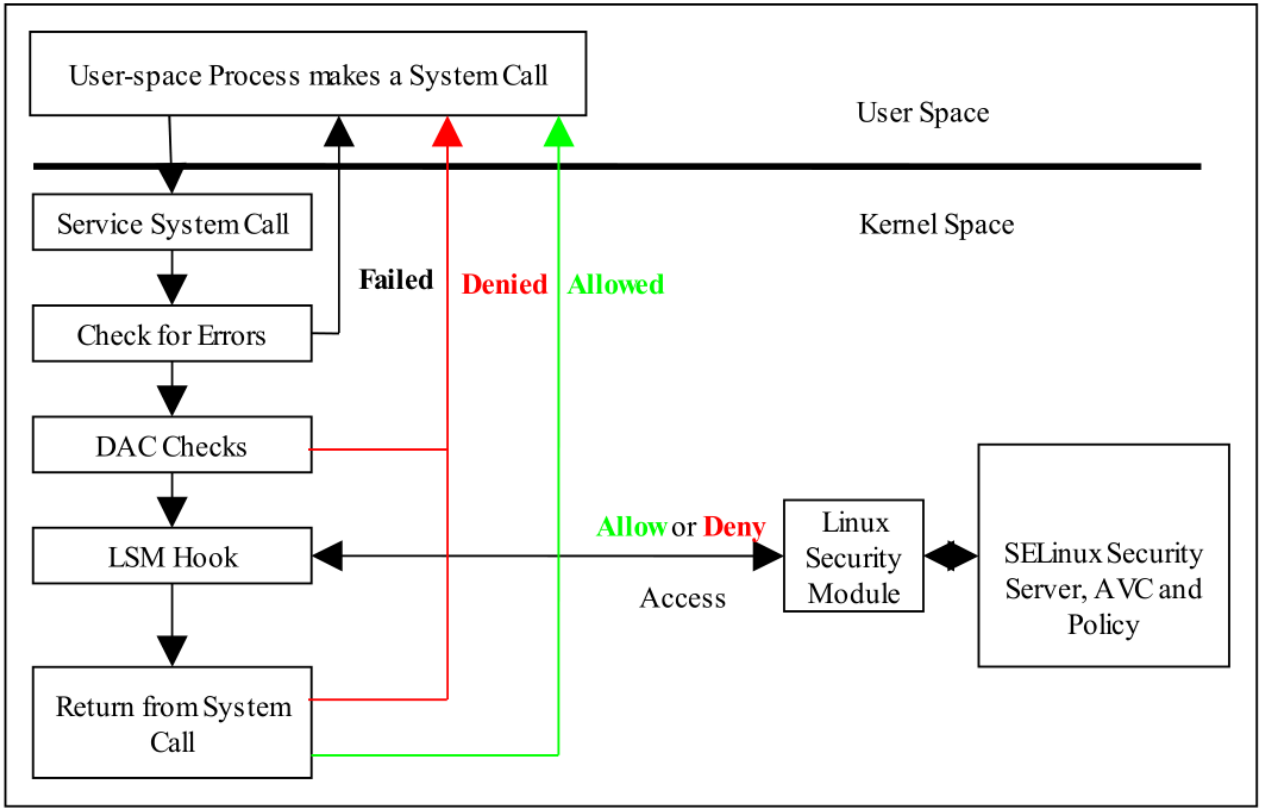


Figure 2.3: Processing a System Call - *The DAC checks are carried out first, if they pass then the Security Server is consulted for a decision.*

2.使用SELinux提升内核安全性

- SELinux的作用
  - 采用最小权限原则
  - 最大限度地减小系统中服务进程可访问的资源

按照MAC模型的定义

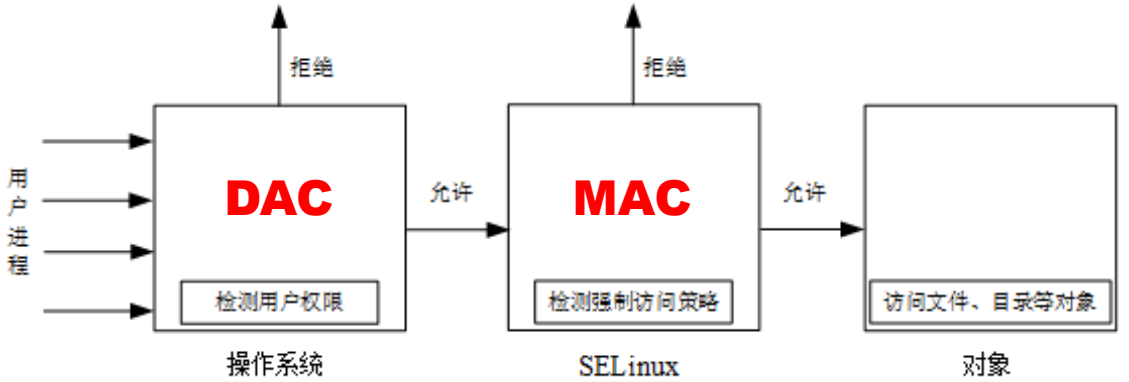
最安全的系统，就是任何人都无法做任何事情。

收放自如 进退裕如

通过精准需求调研和科学评估业务，实现网络与信息安全和业务灵活可用的平衡

2.使用SELinux提升内核安全性

- 基于SELinux安全策略的操作系统中，用户运行的进程不能直接访问到系统中的任何文件、目录、端口。
  - 首先，操作系统会检查用户权限是否允许访问（DAC控制权限）
  - 如果权限允许，继续检测SELinux的强制访问控制策略是否允许（MAC访问控制）
  - 如果策略允许，进程可访问到某对象



2.使用SELinux提升内核安全性

- SELinux provides the following benefits:
  - All processes and files are labeled. SELinux policy rules define how processes interact with files, as well as how processes interact with each other. Access is only allowed if an SELinux policy rule exists that specifically allows it.
  - Fine-grained access control. Stepping beyond traditional UNIX permissions that are controlled at user discretion and based on Linux user and group IDs, SELinux access decisions are based on all available information, such as an SELinux user, role, type, and, optionally, a security level.
  - SELinux policy is administratively-defined and enforced system-wide.

2.使用SELinux提升内核安全性

- SELinux provides the following benefits:
  - Improved mitigation for privilege escalation attacks. Processes run in domains, and are therefore separated from each other. SELinux policy rules define how processes access files and other processes. If a process is compromised, the attacker only has access to the normal functions of that process, and to files the process has been configured to have access to. For
    - example, if the Apache HTTP Server is compromised, an attacker cannot use that process to read files in user home directories, unless a specific SELinux policy rule was added or configured to allow such access.
  - SELinux can be used to enforce data confidentiality and integrity, as well as protecting processes from untrusted inputs.

2.使用SELinux提升内核安全性

- SELinux is not:
  - antivirus software
  - replacement for passwords, firewalls, and other security systems
  - all-in-one security solution

- SELinux is designed to enhance existing security solutions, not replace them. Even when running SELinux, it is important to continue to follow good security practices, such as keeping software up-todate, using hard-to-guess passwords, and firewalls.

工作模式
SELINUX

工作模式决定SELinux是否启用

- enforcing：强制模式，启用SELinux
- permissive：宽容模式，启用SELinux，但不阻止任何操作，只提出警告信息
- disabled：关闭模式，关闭SELinux

工作类型
SELINUXTYPE

工作类型指定SELinux使用的安全政策 (CentOS7/8)

- targeted：默认值，有限程序收到SELinux的保护
- minimum：targeted的简化版，仅选定程序受保护
- mls：Multi-Level Security，多级安全限制，较严格

2.使用SELinux提升内核安全性

- SELinux can run in one of three modes: enforcing, permissive, or disabled.
  - Enforcing mode is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.
  - In permissive mode, the system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development and debugging.
  - Disabled mode is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future.

2.使用SELinux提升内核安全性

- SELinux的工作模式与工作类型的配置信息记录在配置文件中。
  - SELinux的配置文件存放的位置是/etc/selinux/config
  - 查看配置文件内容：#cat /etc/selinux/config

配置文件：/etc/selinux/config

```
1.  #使用 cat 命令查看系统 SELinux 配置文件信息
2.  [root@Project-11-Task-01 ~]# cat /etc/selinux/config
3.  #以下为 SELinux 配置文件信息
4.  # This file controls the state of SELinux on the system.
5.  # SELINUX= can take one of these three values:
6.  #       enforcing - SELinux security policy is enforced.
7.  #       permissive - SELinux prints warnings instead of enforcing.
8.  #       disabled - No SELinux policy is loaded.
9.  #SELinux 运行模式为 enforcing（强制模式）
10. SELINUX=enforcing
11. # SELINUXTYPE= can take one of these three values:
12. #       targeted - Targeted processes are protected,
13. #       minimum - Modification of targeted policy. Only selected processes are protected.
14. #       mls - Multi Level Security protection.
15. #SELinux 安全策略类型为 targeted
16. SELINUXTYPE=targeted
```

2.使用SELinux提升内核安全性

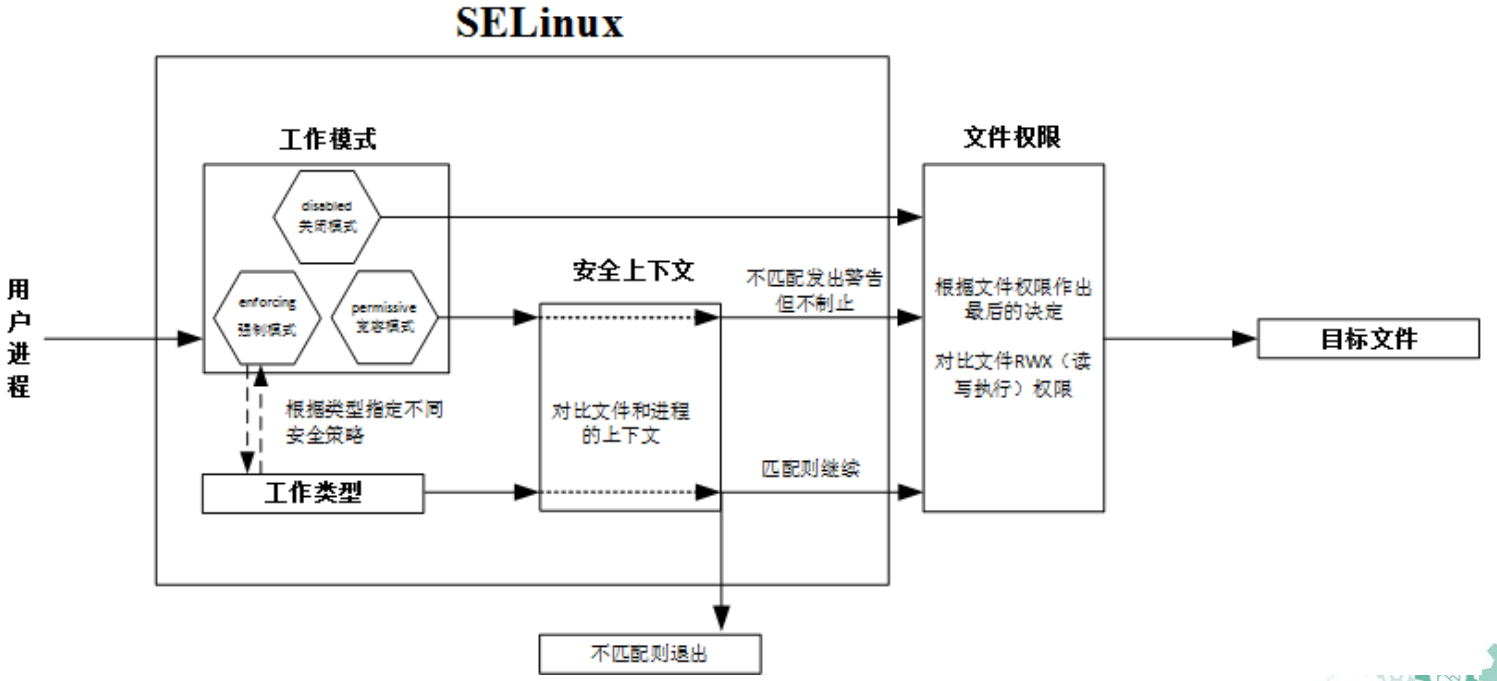
- 查看SELinux的运行状态
  - #sestatus
- 查看SELinux的工作模式
  - #getenforce
- 设置SELinux的工作模式为强制模式
  - #setenforce 1
- 设置SELinux的工作模式为宽容模式
  - #setenforce 0
- 禁用/启动SELinux
  - 修改SELinux的配置文件　　#vi /etc/selinux/config
  - 重启操作系统　　#reboot

Use the setenforce utility to change between enforcing and permissive mode.

Changes made with setenforce do not persist across reboots.

2.使用SELinux提升内核安全性

- 基于SELinux安全策略的操作系统中，用户进程访问目标文件的过程。



2.使用SELinux提升内核安全性

- Policy and Rule：政策 与 规则
  - Policy就是规则库，许多的Rule集合在一起就形成了Policy。
  - 按照MAC的定义，最佳方案就是系统上所有的程序都能够受到保护。
    - 操作系统运行的程序非常多，为所有程序撰写Policy不现实。
    - Policy的撰写难度非常高，让使用Linux操作系统的人都掌握撰写方法不可能。
    - 综合考虑安全性和易用性，只保护重要程序是最佳的选择。
  - RHEL和CentOS中内置了三种政策。
    - 提高了SELinux易用性，让SELinux能够广泛应用。
    - 保护了关键的业务和程序。
    - 操作系统使用人员不需要掌握撰写Policy和Rule的专业技能。

2.使用SELinux提升内核安全性

- SELinux的工作过程主要通过安全规则和安全上下文协同。
  - 安全规则
    - 定义主体（进程）读取对象（系统中文件、目录、端口等均可）的规则类数据库，规则中记录了哪个类型的主体使用哪个方法读取哪一个对象是允许还是拒绝，并定义了哪种行为是允许或拒绝。
  - 安全上下文（Security Context）
    - 操作系统访问控制是以关联客体和主体的访问控制属性为基础的。
    - SELinux中，访问控制属性叫做安全上下文。
    - SELinux中，所有客体（文件、进程间通讯通道、套接字、网络主机等）和主体（进程）都有与其关联的安全上下文。
    - SELinux启用后，系统中所有的资源都会进行标识，就是安全上下文。
    - SELinux通过安全上下文信息来完成访问控制。

2.使用SELinux提升内核安全性

- SELinux contexts have several fields: user, role, type, and security level.
  - The SELinux type information is perhaps the most important when it comes to the SELinux policy, as the most common policy rule which defines the allowed interactions between processes and system resources uses SELinux types and not the full SELinux context.
  - SELinux types end with _t.

user : role : type : security level [: category]

用户 : 角色 : 类型 : 安全级别 [: 分类]

2.使用SELinux提升内核安全性

安全上下文的组成元素

user : role : type : security level [: category]

用户 : 角色 : 类型 : 安全级别 [: 分类]

- user：指定登录系统的用户类型，如user_u（普通用户登录系统后的预设）、system_u（开机过程中系统进程的预设）、root（root用户登录后的预设），多数本地进程都属于自由（unconfined_u）进程。
- role：定义文件（object_r）、进程和用户（system_r）的角色，角色可以限制“type”的使用。
- type：指定数据类型，规则中定义何种进程类型访问何种文件对象目标的策略，都是基于type实现。
- security level：限制访问的需要，由规则定义的分层安全级别，每个对象均有且只有一个级别，总共分为0~15级（s0最低），目标策略默认使用等级为s0。
- category：可选字段，对于特定组织划分不同分层的分类，一个对象可以有多个分类。对于普通用户来讲，该字段可以忽略。

2.使用SELinux提升内核安全性

- Processes and files are labeled with an SELinux context that contains additional information, such as an SELinux user, role, type, and, optionally, a level.
  - When running SELinux, all of this information is used to make access control decisions.
  - SELinux provides a combination of RoleBased Access Control (RBAC), Type Enforcement (TE), and, optionally, Multi-Level Security (MLS).

- 安全上下文信息附加在用户、文件和进程中，使用-Z选项查看。
  - 查看文件的安全上下文信息：ls -Z
  - 查看进程的安全上下文信息：ps -Z
  - 查看用户的安全上下文信息：id -Z

2.使用SELinux提升内核安全性

- 配置SELinux Policy
  - SELinux is in enforcing mode, the default policy is the targeted policy.
  - Change configuration defaults, such as ports, database locations, or file-system permissions for processes.
  - The policycoreutils-python-utils package is installed.

- 配置工具
  - 配置文件安全上下文：chcon
  - 恢复文件安全上下文为默认值：restorecon
  - 查询/修改/增加/删除文件的默认SELinux类型：semanage
  - 显示SELinux规则：seinfo
  - 查询SELinux规则：sesearch

2.使用SELinux提升内核安全性

- Booleans allow parts of SELinux policy to be changed at runtime, without any knowledge of SELinux policy writing.
  - 对Security Context的修改需要一定的专业能力和丰富的经验
  - 使用Booleans可以更改安全规则的部分内容
  - 修改Booleans是SELinux管理配置的常用操作
- Booleans的管理工具
  - 列出所有Booleans：semanage boolean -l
  - 查看Boolean值：getsebool
  - 配置Boolean值：setsebool

表 11-1-8 setsebool 命令选项

选项		说明
-P		可选项，永久保存该属性值设置结果，防止系统重新启动后属性值恢复
boolean		需要设置的安全策略属性值名称。同时设置多个策略属性时需将属性和值之间用“=”号连接
value	on 或 1	属性值。表示设置策略属性值状态为开启
	off 或 0	属性值。表示设置策略属性值状态为关闭

配置
SELinux
工作模式
工作规则

修改
Security
Context

修改规则
Boolean

2.使用SELinux提升内核安全性

- 以【任务：使用Apache发布多个静态网站】 为例
- 对该任务所部署的业务进行分析和安全评估，其存在的安全风险与解决方案

序号	风险内容	安全方案
1	httpd 服务可使用任意端口发布网站	**措施：** 通过 SELinux 强制限制 httpd 服务仅允许使用 80 端口 **目标：** 即便 httpd 使用非 80 端口发布网站，且防火墙允许非 80 端口访问情况下，通过非 80 端口发布的网站依然无法被用户访问
2	httpd 服务对网站目录具有写入权限，存在通过网站攻击服务器的风险	**措施：** 通过 SELinux 将网站目录设置为只读权限 **目标：** 网站目录权限即便设置为 0777，网站目录的属主和属组设置为 apache.apache 情况下，通过网站程序对网站目录仅允许只读操作，无法通过网站程序在网站目录上修改和新增文件
3	httpd 服务发布的网站可开启目录浏览功能，存在程序与文件泄露的风险	**措施：** 通过 SELinux 配置 httpd_enable_homedirs 属性值，禁用 httpd 服务的目录浏览功能 **目标：** 即便 httpd 服务开启目录浏览功能情况下也无法生效
4	通过 httpd 服务发布的网站程序具有发送电子邮件功能，该功能存在功能被滥用，服务器成为垃圾电子邮件发送者的风险	**措施：** 通过配置 httpd_can_sendmail 属性值，禁止 httpd 服务发送电子邮件 **目标：** httpd 服务发布的网站具有电子邮件功能且配置正确，但电子邮件发送功能无法正确执行

命令指南 / 操作引导

```
#启用SELinux，且使用强制模式（enforcing）
#关键操作命令

#查看系统SELinux默认开启端口
[root@Project-03-Task-01 ~]# semanage port -l | grep -w http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
#删除TCP 81端口
[root@Project-03-Task-01 ~]# semanage port -d -t http_port_t -p tcp 81


#设置网站发布目录/var/www/html类型为httpd_sys_content_t
[root@Project-03-Task-01 ~]# semanage fcontext -R -t httpd_sys_content_t /var/www/html

#查看目录与文件的安全上下文信息
[root@Project-03-Task-01 ~]# ls -Z /var/www/html/

#禁止httpd服务允许目录浏览
[root@Project-03-Task-01 ~]# setsebool –P httpd_enable_homedirs off

#禁止httpd服务发送电子邮件
[root@Project-03-Task-01 ~]# setsebool -P httpd_can_sendmail off
```

2.使用SELinux提升内核安全性

- 以【任务：实现远程连接MySQL数据库服务器】为例
- 对该任务所部署的业务进行分析和安全评估，其存在的安全风险与解决方案

序号	风险内容	安全方案
1	mysqld 服务可连接本系统其他任意服务端口，存在系统服务间攻击访问的风险	**措施：**通过 SELinux 配置 mysql_connect_any 属性值，禁止 mysqld 服务连接访问其他业务服务 **目标：**mysqld 服务配置正确且运行正常的情况下，依然无法远程连接其他服务端口
2	通过 httpd 服务发布的网站程序可远程连接 mysqld 服务，该功能存在通过网站攻击数据库的风险	**措施：**通过 SELinux 配置 mysql_connect_http 属性值，禁止 httpd 服务能够远程连接 mysqld 服务 **目标：**即使 httpd 服务发布的网站具有连接数据库功能且配置正确，也无法成功连接数据库并进行数据查询等操作

命令指南 / 操作引导

```
#启用SELinux，且使用强制模式（enforcing）
#关键操作命令

#禁止mysqld服务连接任意服务端口
[root@Project-05-Task-01 ~]# setsebool –P mysql_connect_any off

#禁止httpd服务远程连接mysqld服务
[root@Project-05-Task-01 ~]# setsebool –P mysql_connect_http off
```

2.使用SELinux提升内核安全性

- 以【任务：通过vsftpd实现FTP服务器】为例
- 对该任务所部署的业务进行分析和安全评估，其存在的安全风险与解决方案

序号	风险内容	安全方案
1	FTP 服务允许匿名用户访问并上传文件，无法验证用户的真实性与上传文件的安全性	**措施：**通过 SELinux 配置 ftpd_anon_write 属性值，禁止匿名用户操作 **目标：**即便 FTP 服务开启允许匿名用户访问，匿名用户也无法上传文件
2	通过 httpd 服务发布的网站程序可远程连接 FTP 服务，该功能存在通过网站服务攻击 FTP 服务风险	**措施：**通过 SELinux 配置 httpd_can_connect_ftp 属性值，禁止 httpd 服务远程连接 FTP 服务 **目标：**即便 FTP 服务运行 Web 访问情况下，也无法通过网站进行 FTP 服务连接和共享数据查看
3	FTP 服务允许操作系统内用户对服务目录进行浏览与访问操作功能，无法限制和区分用户权限，存在着 FTP 服务用户权限混乱的风险	**措施：**通过 SELinux 配置 ftpd_full_access 属性值，禁止操作系统内用户对 FTP 服务目录访问 **目标：FTP** 服务目录权限即便设置为 0777，属主与属组设置为 ftp:ftp 情况下，操作系统用户仍不具有 FTP 服务目录的访问权限

命令指南 / 操作引导

```
#启用SELinux，且使用强制模式（enforcing）
#关键操作命令

#设置禁止FTP服务允许匿名用户访问
[root@Project-07-Task-01 ~]# setsebool –P ftpd_anon_write off

#设置禁止httpd服务远程连接FTP服务
[root@Project-07-Task-01 ~]# setsebool –P httpd_can_connect_ftp off

#设置禁止操作系统用户访问FTP服务目录
[root@Project-07-Task-01 ~]# setsebool -P ftpd_full_access off
```

2.使用SELinux提升内核安全性

- 以【任务：使用BIND实现域名解析服务】为例
- 对该任务所部署的业务进行分析和安全评估，其存在的安全风险与解决方案

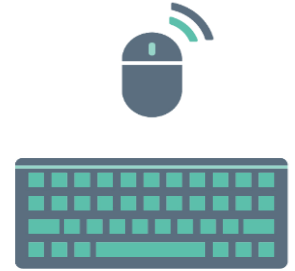
序号	风险内容	安全方案
1	域名配置文件可被系统任意服务操作修改，存在配置文件被恶意篡改的风险	**措施：**通过 SELinux 将域名配置文件设置为仅 named 服务具有操作权限 **目标：**域名配置文件权限即便设置为 0777，除 named 服务外，其他任意服务或进程均无法对配置文件进行操作修改
2	在完成主域名配置后，其配置文件仍具有可被修改操作权限，存在着运行过程中文件被修改的风险	**措施：**通过 SELinux 配置 named_write_master_zones 属性值，禁止 named 服务可对主域名配置文件进行操作 **目标：**主域名配置文件 named.conf 完成配置后，即使文件权限级别设置为 0777，named 服务配置正确且运行正常，但仍无法对该文件进行操作修改

命令指南 / 操作引导

```
#启用SELinux，且使用强制模式（enforcing）
#关键操作命令

#设置域名记录配置文件类型为named_zone_t
[root@Project-08-Task-01 ~]# semanage fcontext -t named_zone_t /var/named/*.zone

#查看域名配置文件的SELinux安全上下文信息
[root@Project-08-Task-01 named]# ls -Z /var/named/*.zone

#设置named服务对主域名named.conf配置文件具有只读权限
[root@Project-08-Task-01 ~]# setsebool –P named_write_master_zones off
```

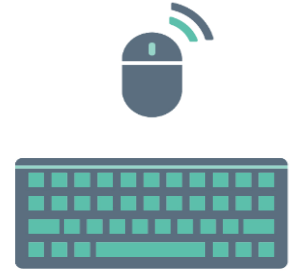
操作视频 / 现场演示

- 针对SELinux进行演示
  - 基本操作
    - SELinux工作模式和工作类型的查看与配置
    - SELinux的启用与禁用
    - SELinux配置工具的安装与基本操作
  - 案例操作
    - 使用SELinux配置非标准端口发布网站



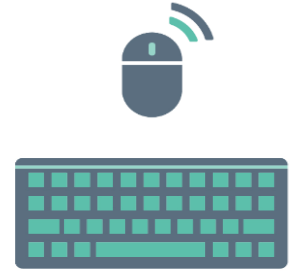
命令指南 / 操作引导

```
#使用sestatus命令，查看SELinux的运行状态信息
[root@Project-11-Task-01 ~]# sestatus

#使用systemctl list-unit-files命令，查看SELinux服务自动启动状态
#查看SELinux服务状态为static（静态），说明该服务为系统内置自动启动，不支持用户进行配置
[root@Project-11-Task-01 ~]# systemctl list-unit-files | grep selinux-autorelabel.service

#使用setenforce命令配置SELinux运行模式为宽容模式
[root@Project-11-Task-01 ~]# setenforce 0
[root@Project-11-Task-01 ~]# getenforce
[root@Project-11-Task-01 ~]# sestatus

#使用setenforce命令恢复SELinux运行模式为强制模式
[root@Project-11-Task-01 ~]# setenforce 1
[root@Project-11-Task-01 ~]# getenforce
[root@Project-11-Task-01 ~]# sestatus

#查看文件、目录、进程、用户的安全上下文信息
[root@Project-11-Task-01 ~]# ls -Z /var/www/index.html
[root@Project-11-Task-01 ~]# ls -dZ /var/www
[root@Project-11-Task-01 ~]# ps auxZ | grep httpd
[root@Project-11-Task-01 ~]# id -Z
```



命令指南 / 操作引导

```
#使用yum工具安装semanage、seinfo、sesearch工具
[root@Project-11-Task-01 ~]# yum provides semanage
[root@Project-11-Task-01 ~]# yum install policycoreutils-python-utils
[root@Project-11-Task-01 ~]# semanage --help
[root@Project-11-Task-01 ~]# semanage user -l
[root@Project-11-Task-01 ~]# semanage port -l | grep http
[root@Project-11-Task-01 ~]# semanage boolean -l | grep http
[root@Project-11-Task-01 ~]# yum provides seinfo
[root@Project-11-Task-01 ~]# yum provides sesearch
[root@Project-11-Task-01 ~]# yum install setools-console
[root@Project-11-Task-01 ~]# seinfo --help
[root@Project-11-Task-01 ~]# sesearch --help
[root@Project-11-Task-01 ~]# seinfo /var/www/index.html
[root@Project-11-Task-01 ~]# seinfo -t /var/www/index.html
[root@Project-11-Task-01 ~]# sesearch -A -t httpd_exec_t | grep httpd_t

#Booleans管理工具的使用
[root@Project-11-Task-01 ~]# getsebool -a | grep ftp
[root@Project-11-Task-01 ~]# setsebool -P tftp_anon_write 1
[root@Project-11-Task-01 ~]# getsebool -a | grep ftp
```



命令指南 / 操作引导

```
#查看SELinux的工作模式与工作规则
[root@Project-11-Task-01 ~]# sestatus
[root@Project-11-Task-01 ~]# getenforce
#安装Apache HTTP Server，并配置httpd服务
[root@Project-11-Task-01 ~]# yum install httpd
[root@Project-11-Task-01 ~]# systemctl start httpd
[root@Project-11-Task-01 ~]# systemctl enable httpd
[root@Project-11-Task-01 ~]# systemctl status httpd
#配置防火墙规则
[root@Project-11-Task-01 ~]# systemctl status firewalld
[root@Project-11-Task-01 ~]# firewall-cmd --zone=public --add-port=80/tcp --permanent
[root@Project-11-Task-01 ~]# firewall-cmd --zone=public --add-port=801/tcp --permanent
[root@Project-11-Task-01 ~]# firewall-cmd --zone=public --add-port=802/tcp --permanent
[root@Project-11-Task-01 ~]# firewall-cmd --reload
[root@Project-11-Task-01 ~]# firewall-cmd --zone=public --list-all
#创建网站Site0的默认网页
[root@Project-11-Task-01 ~]# echo "<h1>Site0。http://10.10.2.125:80</h1>" > /var/www/html/index.html
#发布网站Site0，在本地主机通过浏览器访问网站
[root@Project-11-Task-01 ~]# vi /etc/httpd/conf/httpd.conf
[root@Project-11-Task-01 ~]# systemctl reload httpd
[root@Project-11-Task-01 ~]# systemctl status httpd
#创建网站Site1的默认网页
[root@Project-11-Task-01 ~]# echo "<h1>Site1。http://10.10.2.125:801</h1>" > /var/www/site1/index.html
#创建网站Site2的默认网页
[root@Project-11-Task-01 ~]# echo "<h1>Site2。http://10.10.2.125:802</h1>" > /var/www/site2/index.html
#发布网站Site1
[root@Project-11-Task-01 ~]# vi /etc/httpd/conf.d/site1.conf
#发布网站Site2
[root@Project-11-Task-01 ~]# vi /etc/httpd/conf.d/site2.conf
[root@Project-11-Task-01 ~]# systemctl reload httpd
[root@Project-11-Task-01 ~]# systemctl status httpd
```

命令指南 / 操作引导

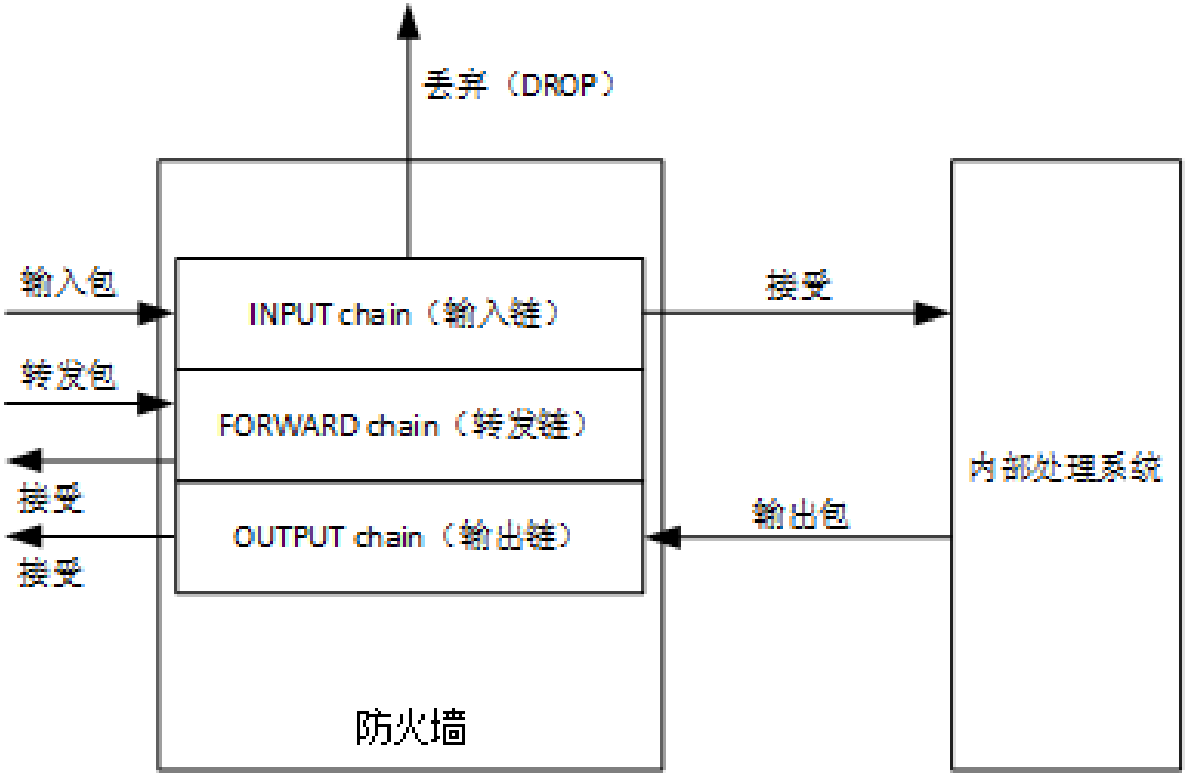
```
#查看SELinux允许http服务的端口
[root@Project-11-Task-01 ~]# semanage port -l | grep http_port_t
#增加801和802端口为允许端口
[root@Project-11-Task-01 ~]# semanage port -a -t http_port_t -p tcp 801
[root@Project-11-Task-01 ~]# semanage port -a -t http_port_t -p tcp 802
#重新启动httpd.service服务，在本地主机通过浏览器访问网站
[root@Project-11-Task-01 ~]# systemctl start httpd.service
[root@Project-11-Task-01 ~]# systemctl status httpd.service
#配置http相关的boolean值
[root@Project-11-Task-01 ~]# semanage boolean -l | grep http
[root@Project-11-Task-01 ~]# setsebool -P httpd_enable_cgi 0
[root@Project-11-Task-01 ~]# setsebool -P httpd_builtin_scripting 0
[root@Project-11-Task-01 ~]# semanage boolean -l | grep http
```

3.使用Firewalld提升系统安全性

- 防火墙是服务器安全的重要保障系统，遵循允许和业务来往的网络通信机制，提供网络通信过滤服务。
- 从保护对象上区分，防火墙可分为主机防火墙和网络防火墙。
  - 主机防火墙是部署在一台计算机系统上的软件，针对单个主机进行防护。
  - 网络防火墙是部署在两个网络之间的设备或一整套装置，针对一个网络进行防护。通常部署在网络边界以加强访问控制，其将网络划分为可信与不可信区域，对流入流出的网络流量进行过滤，实现对可信网络的防护。

3.使用Firewalld提升系统安全性

- 不管是Linux、Unix、Mac还是Windows操作系统，主机防火墙都是设置操作系统与外界网络之间的一系列软件组合。
- 主机防火墙通过检测、限制通过的数据流，尽可能地对外屏蔽操作系统的信息、结构和运行状态，有选择地接受外部网络的访问请求，进而实现提升主机安全性的目的。
- 主机防火墙工作在网络层，属于典型的包过滤防火墙。
  - 把网络层作为数据监控对象，对每个数据包的头部、协议、地址端口及类型信息进行分析。
  - 如果数据包的某个或多个部分与预先设定的防火墙规则（Filtering Rule）匹配，则按照防火墙规则进行处理，否则直接丢弃。


丢弃（DROP）
输入包
转发包
接受
接受
INPUT chain（输入链）
FORWARD chain（转发链）
OUTPUT chain（输出链）
防火墙
接受
输出包
内部处理系统

3.使用Firewalld提升系统安全性

- 防火墙虽然是重要的系统安全措施，但不能过分依赖防火墙，因为防火墙自身具有一定的局限性。
  - 防火墙可以阻断攻击，但不能消灭攻击源
  - 防火墙不能抵抗最新的未设置策略的攻击漏洞
  - 防火墙的并发连接数限制容易导致服务拥塞或溢出
  - 防火墙对针对服务器开放端口的攻击无法阻止
  - 防火墙对系统内部发起的攻击无法阻止
  - 防火墙本身也会出现问题或受到攻击
  - 防火墙无法防御病毒

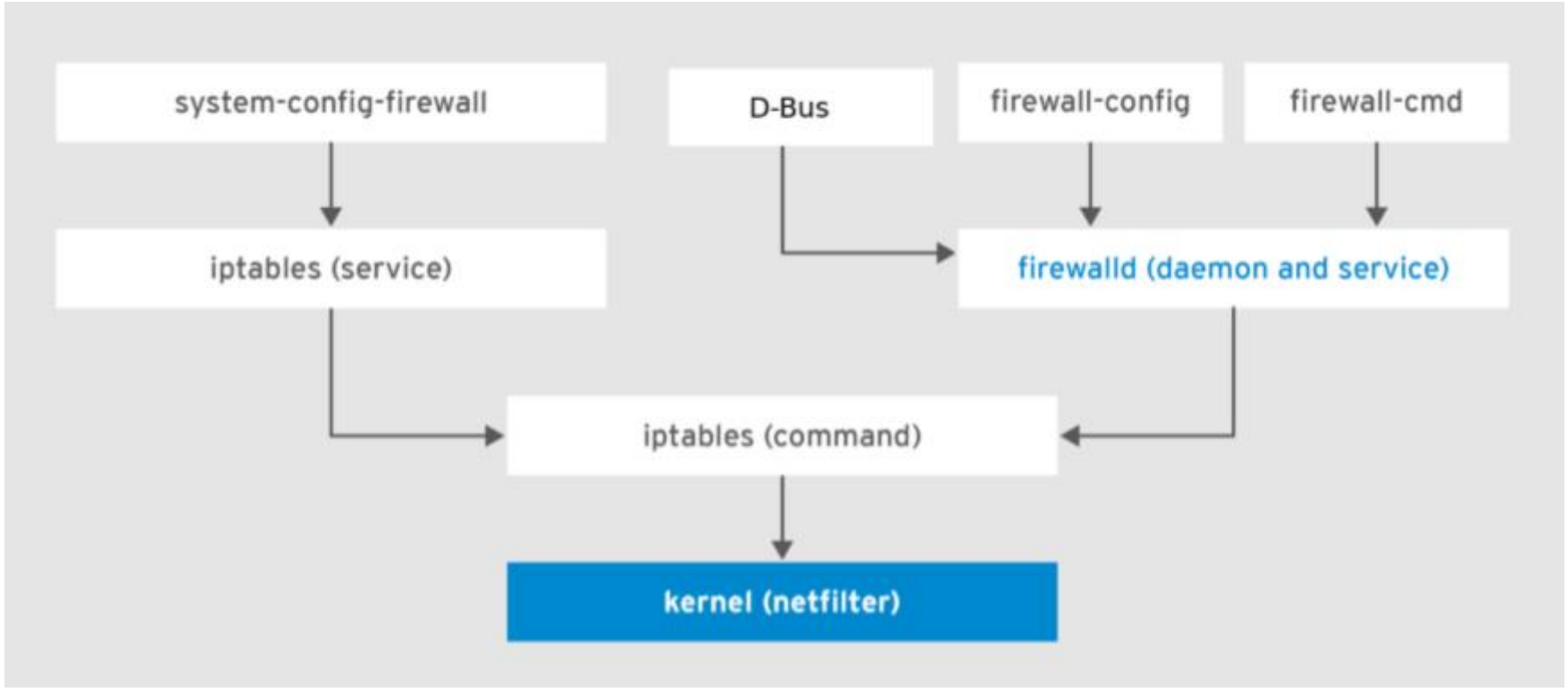
3.使用Firewalld提升系统安全性

- 在CentOS 7以前版本中，使用 iptables 防火墙。
- 在CentOS 7/8的版本中，使用 firewalld 防火墙。

- firewalld与iptables之间的异同点
  - firewalld 防火墙可以动态修改单条规则与管理规则集等，允许更新规则而不破坏现有会话和连接，而 iptables 防火墙在修改规则后必须全部会话刷新后才可以生效。
  - firewalld 防火墙使用区域和服务，而 iptables 防火墙则使用链式规则。
  - firewalld 防火墙规则默认为拒绝，而 iptables 防火墙规则默认为允许。
  - firewalld 和 iptables 本身均不具备防火墙的功能，实现的均是防火墙的管理。
  - firewalld 和 iptables 的防火墙功能是通过内核 netfilter 来实现的。

3.使用Firewalld提升系统安全性

- firewalld is a firewall service daemon that provides a dynamic customizable host-based firewall with a DBus interface.
  - Being dynamic, it enables creating, changing, and deleting the rules without the necessity to restart the firewall daemon each time the rules are changed.
- firewalld uses the concepts of zones and services, that simplify the traffic management.
  - Zones are predefined sets of rules. Network interfaces and sources can be assigned to a zone.
  - The traffic allowed depends on the network your computer is connected to and the security level this network is assigned.
  - Firewall services are predefined rules that cover all necessary settings to allow incoming traffic for a specific service and they apply within a zone.


system-config-firewall
D-Bus
firewall-config
firewall-cmd
iptables (service)
firewalld (daemon and service)
iptables (command)
kernel (netfilter)

3.使用Firewalld提升系统安全性

- 基于用户对网络中设备和通信的信任程度，防火墙将网络分割成不同的区域（Zone）。
  - 可以将一个接口归属某个区域，接口所分配的区域可以通过防火墙管理工具进行配置。
  - 一个接口只能够属于一个区域，但是一个区域内可以有多个接口。
  - 可以为不同的区域定义不同的规则集，通过更改当前使用接口对应的区域实现快速进行防火墙规则设置。
  - 当使用多个接口时，可以为每个接口设置对应不同区域，实现对不同接口进行不同的防火墙规则设置，实现更加灵活的防火墙策略配置。

区域	默认策略规则
trusted	允许所有的数据包进出。
home	拒绝外部访问。默认开启 ssh、mdns、ipp-client、amba-client 与 dhcpv6-client 服务允许对外访问
Internal	等同于 home 区域
work	拒绝外部访问。默认开启 ssh、ipp-client 与 dhcpv6-client 服务允许对外访问
public	拒绝外部访问。默认开启 ssh、dhcpv6-client 服务允许对外访问
external	拒绝外部访问。默认开启 ssh 服务允许对外访问
dmz	拒绝外部访问。默认开启 ssh 服务允许对外访问
block	拒绝外部访问
drop	拒绝外部访问

block

Any incoming network connections are rejected with an icmp-host-prohibited message for **IPv4** and icmp6-adm-prohibited for **IPv6**. Only network connections initiated from within the system are possible.

dmz

For computers in your demilitarized zone that are publicly-accessible with limited access to your internal network. Only selected incoming connections are accepted.

drop

Any incoming network packets are dropped without any notification. Only outgoing network connections are possible.

external

For use on external networks with masquerading enabled, especially for routers. You do not trust the other computers on the network to not harm your computer. Only selected incoming connections are accepted.

home

For use at home when you mostly trust the other computers on the network. Only selected incoming connections are accepted.

internal

For use on internal networks when you mostly trust the other computers on the network. Only selected incoming connections are accepted.

public

For use in public areas where you do not trust other computers on the network. Only selected incoming connections are accepted.

trusted

All network connections are accepted.

work

For use at work where you mostly trust the other computers on the network. Only selected incoming connections are accepted.

3.使用Firewalld提升系统安全性

- Listing Zones
  - To see which zones are available on your system
    - # firewall-cmd --get-zones
  - To see detailed information for all zones:
    - # firewall-cmd --list-all-zones
  - To see detailed information for a specific zone:
    - # firewall-cmd --zone=zone-name --list-all
- Changing the Default Zone
  - Display the current default zone:
    - # firewall-cmd --get-default-zone
  - Set the new default zone:
    - # firewall-cmd --set-default-zone zone-name

3.使用Firewalld提升系统安全性

- Create a new zone:
  - Create a new zone:
    - # firewall-cmd --new-zone=zone-name
  - Check if the new zone is added to your permanent settings:
    - # firewall-cmd --get-zones
  - Make the new settings persistent:
    - # firewall-cmd --runtime-to-permanent
- To set a target for a zone
  - List the information for the specific zone to see the default target:
    - # firewall-cmd --zone=zone-name --list-all
  - Set a new target in the zone:
    - # firewall-cmd --zone=zone-name --set-target=<default|ACCEPT|REJECT|DROP> --permanent

3.使用Firewalld提升系统安全性

firewall-cmd

firewall-config

yum install firewall-config

3.使用Firewalld提升系统安全性

- Firewall防火墙可以使用服务进行策略配置。
  - 服务可以是本地端口、协议、源端口、目的地址、来源地址等。
  - 使用防火墙的辅助定义模块预定义服务，可以更加灵活和简便的配置。
    - 预定于服务通过XML文件记录。
    - 预定义服务的配置文件存放位置是：/etc/firewalld/services

```
[root@Project-11-Task-01 ~]# ls -l /etc/firewalld/
总用量 8
-rw-r--r--. 1 root root 2528 11月  9 00:48 firewalld.conf
drwxr-x---. 2 root root    6 11月  9 00:48 helpers
drwxr-x---. 2 root root    6 11月  9 00:48 icmptypes
drwxr-x---. 2 root root    6 11月  9 00:48 ipsets
-rw-r--r--. 1 root root  283 11月  9 00:48 lockdown-whitelist.xml
drwxr-x---. 2 root root    6 11月  9 00:48 services
drwxr-x---. 2 root root   46 3月  21 21:52 zones
```

3.使用Firewalld提升系统安全性

- 防火墙运行时进行配置后，可以立即生效，且不需要中断当前连接。
  - 重启firewalld服务或者重启操作系统后，配置会失效，恢复为默认设置。
  - 防火墙的配置模式
    - runtime configuration：运行时配置，就是防火墙当前起效的规则
    - permanent configuration：存储的配置，就是防火墙启动时会加载的规则
  - 使规则永久生效的两种配置方式
    - 使用--runtime-to-permanent选项：将当前运行的防火墙规则永久保存
    - 使用--permanent选项：配置防火墙规则，并永久存储
    - 举例：
      - # firewall-cmd --zone=public --add-port=80/tcp --permanent
      - # firewall-cmd --runtime-to-permanent

3.使用Firewalld提升系统安全性

- Starting Firewalld
  - To start firewalld, enter the following command as root:
    - # systemctl unmask firewalld
    - # systemctl start firewalld
  - To ensure firewalld starts automatically at system start, enter the following command as root:
    - # systemctl enable firewalld

3.使用Firewalld提升系统安全性

- Stopping Firewalld
  - To stop firewalld, enter the following command as root:
    - # systemctl stop firewalld
  - To prevent firewalld from starting automatically at system start, enter the following command as root:
    - # systemctl disable firewalld
  - To make sure firewalld is not started by accessing the firewalld D-Bus interface and also if other services require firewalld, enter the following command as root:
    - # systemctl mask firewalld

3.使用Firewalld提升系统安全性

- Disabling All Traffic in Case of Emergency using CLI In an emergency situation, such as a system attack, it is possible to disable all network traffic and cut off the attacker.
  - To immediately disable networking traffic, switch panic mode on:
    - # firewall-cmd --panic-on
  - Switching off panic mode reverts the firewall to its permanent settings. To switch panic mode off:
    - # firewall-cmd --panic-off
  - To see whether panic mode is switched on or off, use:
    - # firewall-cmd --query-panic

3.使用Firewalld提升系统安全性

- Controlling Traffic with Predefined Services
  - Check that the service is not already allowed:
    - # firewall-cmd --list-services
  - List all predefined services:
    - # firewall-cmd --get-services
  - Add the service to the allowed services:
    - # firewall-cmd --add-service=<service-name>
  - Make the new settings persistent:
    - # firewall-cmd --runtime-to-permanent

3.使用Firewalld提升系统安全性

- 对防火墙日志的配置有全局日志配置和规则日志配置两部分。
- 全局日志配置是对防火墙日志规则进行配置。
  - 防火墙日志服务由系统rsyslog服务进行管理
  - 日志默认存放在/var/log/firewalld日志文件中
  - 日志文件基于日期时间自动归档。
- 规则日志配置是设置防火墙触发特定防火墙规则时记录日志的方式。

3.使用Firewalld提升系统安全性

- 全局日志配置案例：
  - 通过修改防火墙与rsyslogd配置文件，对防火墙日志字段、日志文件存放路径、日志文件分割方法等进行自定义配置。
  - 完成对防火墙全局日志的配置，实现以下3个目标。
    - 实现防火墙对单播网络通信的日志记录
    - 防火墙日志存放目录变更为/var/log/firewalldlog
    - 防火墙日志记录等级调整为所有等级的日志均记录

①使用vi工具修改防火墙的配置文件/etc/firewalld/firewalld.conf，修改后的配置文件信息如下。

配置文件：/etc/firewalld/firewalld.conf

```
1.  #firewalld.conf 配置文件内容较多，本部分仅显示与防火墙日志配置有关的内容
2.  #将 LogDenied=off 改为 LogDenied=unicast，实现对单播网络通信的日志记录
3.  LogDenied=unicast
```

操作命令+配置文件+脚本程序+结束

②使用 vi 工具修改 rsyslog 的配置文件/etc/rsyslog.conf，修改后的配置文件信息如下。

配置文件：/etc/rsyslog.conf

```
1.  #rsyslog.conf 配置文件内容较多，本部分仅显示与防火墙日志记录等级有关的内容
2.  #在配置文件中增加内容，kern.*表示为所有等级日志均可记录
3.  kern.*                                                  /var/log/firewalldlog/loginfo
```

操作命令+配置文件+脚本程序+结束

③创建防火墙日志存放的目录，重新载入配置文件，重启日志相关服务。

操作命令：

```
1.  #创建防火墙日志存放的目录
2.  [root@Project-11-Task-01 ~]# mkdir /var/log/firewalldlog
3.  #重新载入防火墙配置文件
4.  [root@Project-11-Task-01 ~]# systemctl reload firewalld
5.  #重新启动系统日志服务
6.  [root@Project-11-Task-01 ~]# systemctl restart rsyslog
```

操作命令+配置文件+脚本程序+结束

3.使用Firewalld提升系统安全性

- 规则日志设置案例：
  - 在配置防火墙规则时，可定义由该规则产生的日志的记录方式。
  - 新增一条防火墙规则并实现下述3个目标。
    - 允许本地主机（10.10.2.100）访问服务器httpd服务
    - 实现防火墙对触发规则通过的日志记录
    - 设置日志记录的频率为最多每秒3条

操作命令：

```
#根据防火墙规则要求配置
[root@Project-11-Task-01 ~]# firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=10.10.2.100 service name="http" log level=notice prefix="HTTP" limit value="3/s" accept'
success

#重新载入防火墙配置使其生效
[root@Project-11-Task-01 ~]# systemctl reload firewalld
```

操作命令+配置文件+脚本程序+结束

3.使用Firewalld提升系统安全性

- 在CentOS中，rsyslog服务的配置文件存放位置是/etc/rsyslog.conf。

表 11-2-6 日志类型内容说明

序号	日志类型	说明
1	auth	pam 产生的日志信息
2	authpriv	ssh、ftp 等登陆信息的验证日志
3	cron	时间任务相关的日志信息
4	kern	系统内核产生的日志信息
5	lpr	打印服务产生的日志信息
6	mail	邮件服务产生的日志信息
7	mark(syslog)	rsyslog 服务内部的信息
8	user	用户程序产生的日志信息
9	uucp	unix to unix 主机之间数据拷贝产生的日志信息
10	local 1-7	自定义的日志信息

3.使用Firewalld提升系统安全性

- 在CentOS中，rsyslog服务的配置文件存放位置是/etc/rsyslog.conf。

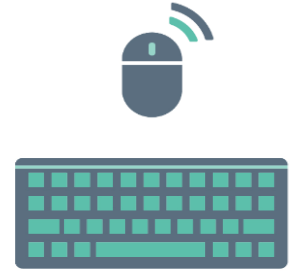
表 11-2-7 日志等级内容说明

序号	日志级别	说明
1	debug	产生调试信息，日志产生量最大
2	info	一般信息日志，最常用
3	notice	最具有重要性的普通条件信息
4	warning	警告级别
5	err	错误级别，阻止服务或模块不能正常工作产生的信息
6	crit	严重级别，阻止整个系统不能正常工作产生的信息
7	alert	需要立刻修改的信息
8	emerg	内核崩溃的重要信息
9	none	日志级别为 0，什么情况都不记录

3.使用Firewalld提升系统安全性

- 使用防火墙提升远程连接服务的安全性
  - 以【任务：通过SSH远程管理CentOS】为例，通过对防火墙规则进行设置提升远程连接服务的安全性，实现以下2个目标。
    - 允许地址范围为10.10.2.96/27内的客户端远程连接服务器，进行远程管理维护
    - 客户端远程连接服务器时，限制每分钟允许远程连接次数为5次

序号	来源地址/子网掩码	目的地址/子网掩码	协议与端口	动作	其他
1	10.10.2.96/27	10.10.2.125/32	ssh	允许	限制每分钟连接 5 次



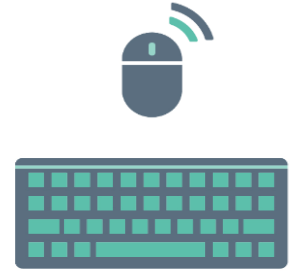
命令指南 / 操作引导

```
#使用firewall-cmd命令删除默认ssh服务规则
[root@Project-11-Task-01 ~]# firewall-cmd --permanent --remove-service=ssh
#出现success则表示规则删除成功
success

#添加指定地址能够远程访问规则
[root@Project-11-Task-01 ~]# firewall-cmd --permanent
        --add-rich-rule='rule family=ipv4 source address=10.10.2.96/27 service name=ssh limit value=5/m accept'
#出现success则表示规则添加成功
success

#重载使防火墙配置生效
[root@Project-11-Task-01 ~]# firewall-cmd --reload
success
```

3.使用Firewalld提升系统安全性

- 使用防火墙提升网站服务的安全性
  - 以【任务：使用Apache发布多个静态网站】为例，通过防火墙规则设置提升网站服务的安全性，实现以下2个目标。
    - 允许任意地址的客户端访问网站服务，并对访问网站情况进行日志记录
    - 发现某个单一客户端（10.10.2.110）一直进行攻击性访问，禁止该客户端访问

序号	来源地址/子网掩码	目的地址/子网掩码	协议与端口	动作	其他
1	0.0.0.0/0	10.10.2.125/32	TCP 80	允许	记录通过防火墙的网站访问日志
2	10.10.2.110/32	10.10.2.125/32	TCP 80	拒绝	无



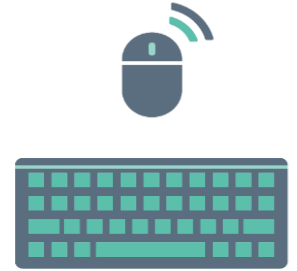
命令指南 / 操作引导

```
#使用firewall-cmd命令添加允许访问网站规则
[root@Project-11-Task-01 ~]# firewall-cmd --permanent
        --add-rich-rule='rule port port=80 protocol=tcp log level=notice prefix="HTTP" accept'
success

#添加指定主机禁止访问规则
[root@Project-11-Task-01 ~]#firewall-cmd --permanent
        --add-rich-rule='rule family=ipv4 source address=10.10.2.110 port port=80 protocol=tcp reject'
success

#重载使防火墙配置生效
[root@Project-11-Task-01 ~]# firewall-cmd --reload
success
```

3.使用Firewalld提升系统安全性

- 使用防火墙提升数据库服务的安全性
  - 以【任务：实现远程连接MariaDB数据库服务器】为例，通过对防火墙规则设置提升数据库服务的安全性，实现以下2个目标。
    - 本地客户端（10.10.2.100）能够使用MySQL WorkBench连接MariaDB数据库
    - 本地客户端（10.10.2.100）能够通过浏览器访问phpMyAdmin的管理界面，进行数据库Web化管理

序号	来源地址/子网掩码	目的地址/子网掩码	协议与端口	动作	其他
1	10.10.2.100/32	10.10.2.125/32	TCP 3306	允许	无
2	10.10.2.100/32	10.10.2.125/32	TCP 80	允许	无



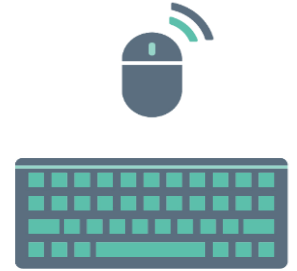
命令指南 / 操作引导

```
#使用firewall-cmd命令添加本地客户端允许远程连接数据库
[root@Project-11-Task-01 ~]# firewall-cmd --permanent
        --add-rich-rule='rule family=ipv4 source address=10.10.2.100 port port=3306 protocol=tcp accept'
success

#添加本地客户端允许访问phpMyAdmin管理界面
[root@Project-11-Task-01 ~]# firewall-cmd --permanent
        --add-rich-rule='rule family=ipv4 source address=10.10.2.100 port port=80 protocol=tcp accept'
success

#重载使防火墙配置生效
[root@Project-11-Task-01 ~]# firewall-cmd --reload
success
```

3.使用Firewalld提升系统安全性

- 使用防火墙提升文件传输服务的安全性
  - 以【任务：通过vsftpd实现FTP服务器】为例，通过对防火墙规则设置提升文件传输服务的安全性，实现以下2个目标。
    - 允许地址范围10.10.2.96/27的客户端通过主动与被动模式访问FTP服务
    - 客户端访问FTP服务时，限制每分钟连接次数为10次

序号	来源地址/子网掩码	目的地址/子网掩码	协议与端口	动作	其他
1	10.10.2.96/27	10.10.2.125/32	TCP 20-21	允许	限制每分钟连接 10 次
2	10.10.2.96/27	10.10.2.125/32	TCP 9000-9020	允许	限制每分钟连接 10 次



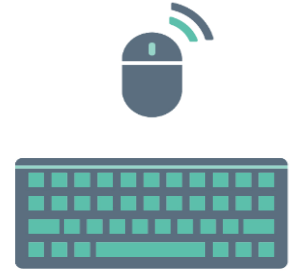
命令指南 / 操作引导

```
#使用firewall-cmd命令添加通过主动模式访问FTP服务
[root@Project-11-Task-01 ~]# firewall-cmd --permanent
        --add-rich-rule='rule family=ipv4 source address=10.10.2.96/27 port port=20-21 protocol=tcp limit value="10/m" accept'
success

#使用firewall-cmd命令添加通过被动模式访问FTP服务
[root@Project-11-Task-01 ~]# firewall-cmd --permanent
        --add-rich-rule='rule family=ipv4 source address=10.10.2.96/27 port port=9000-9020 protocol=tcp limit value="10/m" accept'
success

#重载使防火墙规则配置生效
[root@Project-11-Task-01 ~]# firewall-cmd --reload
success
```

3.使用Firewalld提升系统安全性

- 使用防火墙提升域名解析服务的安全性
  - 以【任务：使用BIND实现域名解析服务】为例，通过对防火墙规则设置提升域名解析服务的安全性，实现以下2个需求目标。
    - 允许地址范围10.10.2.96/27的客户端对DNS服务进行查询，并获取域名解析结果
    - 客户端进行DNS查询时，对域名记录解析请求行为进行日志记录

序号	来源地址/子网掩码	目的地址/子网掩码	协议与端口	动作	其他
1	10.10.2.96/27	10.10.2.125/32	UDP 53	允许	记录域名请求日志



命令指南 / 操作引导

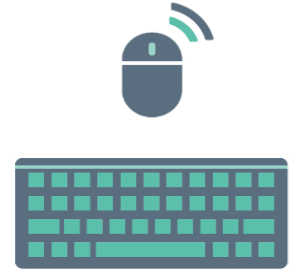
```
#使用firewall-cmd命令添加允许访问DNS服务
[root@Project-11-Task-01 ~]# firewall-cmd --permanent
        --add-rich-rule=' rule family=ipv4 source address=10.10.2.96/27 port port=53 protocol=udp log level=notice prefix="DNS" accept'
success

#重载使防火墙规则配置生效
[root@Project-11-Task-01 ~]# firewall-cmd --reload
success
```

操作视频 / 现场演示

- 针对Firewall进行演示
  - 基本操作
    - Firewall的基本管理
    - Firewall的Zone管理
    - Firewall的Log管理
    - Firewall的策略管理
  - 案例操作
    - 使用Firewall保护负载均衡业务
    - 对防火墙日志进行分析

命令指南 / 操作引导

```
#禁用firewalld
[root@Project-11-Task-01 ~]# systemctl stop firewalld
[root@Project-11-Task-01 ~]# systemctl disable firewalld
[root@Project-11-Task-01 ~]# systemctl mask firewalld
[root@Project-11-Task-01 ~]# systemctl status firewalld

#启用firewalld
[root@Project-11-Task-01 ~]# systemctl unmask firewalld
[root@Project-11-Task-01 ~]# systemctl start firewalld
[root@Project-11-Task-01 ~]# systemctl enable firewalld
[root@Project-11-Task-01 ~]# systemctl status firewalld

#使用firewalld的紧急模式
[root@Project-11-Task-01 ~]# firewall-cmd --panic-on
[root@Project-11-Task-01 ~]# firewall-cmd --query-panic
[root@Project-11-Task-01 ~]# firewall-cmd --panic-off

#查看firewalld的服务
[root@Project-11-Task-01 ~]# firewall-cmd --list-services
[root@Project-11-Task-01 ~]# firewall-cmd --get-services
```



命令指南 / 操作引导

```
#当前活跃规则永久保存到默认区域
[root@Project-11-Task-01 ~]# firewall-cmd --runtime-to-permanent

#记录所有通信的日志
[root@Project-11-Task-01 ~]# vi /etc/firewalld/firewalld.conf
[root@Project-11-Task-01 ~]# vi /etc/rsyslog.conf
[root@Project-11-Task-01 ~]# mkdir /var/log/firewalldlog
[root@Project-11-Task-01 ~]# systemctl reload firewalld
[root@Project-11-Task-01 ~]# systemctl restart rsyslog

#管理防火墙的区域
[root@Project-11-Task-01 ~]# firewall-cmd --get-zones
[root@Project-11-Task-01 ~]# firewall-cmd --list-all-zones
[root@Project-11-Task-01 ~]# firewall-cmd --zone=public --list-all

#配置防火墙的默认区域
[root@Project-11-Task-01 ~]# firewall-cmd --get-default-zone
[root@Project-11-Task-01 ~]# firewall-cmd --set-default-zone home
[root@Project-11-Task-01 ~]# firewall-cmd --get-default-zone
```

命令指南 / 操作引导

```
#配置Firewalld服务日志的存放路径
[root@Project-04-Task-01 firewalld]# vi /etc/rsyslog.conf
[root@Project-04-Task-01 firewalld]# mkdir /var/log/firewalld

#使用Rich Language进行防火墙规则配置
[root@Project-04-Task-01 firewalld]# firewall-cmd --zone=public --add-rich-rule '
rule family="ipv4"
source address="10.10.2.100/32"
port protocol="tcp"
port="80"
log prefix="[meToweb] "
level="emerg"
reject';

#查看当前zone的信息
[root@Project-04-Task-01 firewalld]# firewall-cmd --list-all

#监控防火墙拒绝的日志
[root@Project-04-Task-01 firewalld]# tail -f /var/log/firewalld/fwlog

#查看非法请求最多的IP地址
[root@Project-04-Task-01 firewalld]# cat fwlog | awk '{print $10}' | sort -n | uniq -c | head -n 20
```

4.使用Nmap实现系统安全检测

- 在网络技术高度成熟发展的今天，即便SELinux和防火墙同时使用，也无法保障操作系统无任何安全风险。
- 只有不断通过对操作系统进行安全审计评估，及时发现系统安全漏洞并进行修复，才能不断提高主机的安全性。

没有绝对的安全!

4.使用Nmap实现系统安全检测

- 安全审计是对目标主机的整体审计，主要包含以下内容与步骤。
  - 实施端口扫描与服务探测。
    - 如果目标主机处于开机状态，通过扫描与探测，可得到目标主机的端口状态（监听/关闭）、目标主机中服务程序列表和版本信息以及目标主机操作系统版本和内核信息等。
  - 以攻击渗透等方式进行模拟探测。
    - 根据获取到目标主机上的服务列表和版本信息，查询安全漏洞数据库，获取有针对性的攻击脚本，开展对目标主机系统的尝试性攻击，并记录目标主机对攻击的响应信息。
  - 对数据进行分析并产生报告。
    - 对获取的响应信息进行分析，并比对安全漏洞信息数据库，明确目标主机确实存在的安全漏洞信息，形成安全审计报告。
  - 安全风险处理。
    - 系统管理员根据安全审计报告的内容，逐项对照解决安全风险。

周期性的做! 不间断的做!

4.使用Nmap实现系统安全检测

- 主机安全扫描的常用工具

工具	功能类别	官方网站
Nmap	安全审计	https://nmap.org
Snort	网络入侵扫描	https://www.snort.org
ClamAV	病毒检测	http://www.clamav.net
Nessus	漏洞扫描	https://www.swri.org/nessus
hping	网络安全扫描	http://www.hping.org

4.使用Nmap实现系统安全检测

- 安全检测是使用工具对系统进行扫描检测，验证是否存在安全风险或漏洞，完成系统安全评估工作。
- Nmap是最常用的安全检测软件的之一，是开源软件且提供了强大的网络扫描功能，通过该工具可发现网络中在线主机、端口监听状态、主机上运行的应用程序与版本信息以及操作系统的类型和版本等。

Linux FreeBSD NetBSD OpenBSD

Nmap
http://www.insecure.org/nmap/
Prevent Security Disasters Before They Happen

Solaris IRIX BSDI SunOS

Intro	**Reference Guide**	**Book**	**Install Guide**
Download	**Changelog**	**Zenmap GUI**	**Docs**
Bug Reports	**OS Detection**	**Propaganda**	**Related Projects**
In the Movies			**In the News**

https://nmap.org

News

- Nmap 7.80 was released for DEFCON 27! [release notes | download]
- Nmap 7.70 is now available! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.60 is now available! [release notes | download]
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement/Details], [Download Site]
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes | download]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for security tools. Are you familiar with all of the 49 new tools in this edition?
- Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [Download page | Release notes]
- Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam--all in 38 minutes! (Presentation video)
- *Icons of the Web*: explore favicons for the top million web sites with our new poster and online viewer.
- We're delighted to announce the immediate, free availability of the Nmap Security Scanner version 5.00. Don't miss the top 5 improvements in Nmap 5.
- After years of effort, we are delighted to release Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning!
- We now have an active Nmap Facebook page and Twitter feed to augment the mailing lists. All of these options offer RSS feeds as well.

Introduction

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap was named "Security Product of the Year" by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

Nmap is ...

- **Flexible**: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.
- **Powerful**: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- **Portable**: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- **Easy**: While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A *targethost*". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
- **Free**: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.
- **Well Documented**: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.
- **Supported**: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines. We recommend that all users subscribe to the low-traffic nmap-hackers announcement list. You can also find Nmap on Facebook and Twitter. For real-time chat, join the #nmap channel on Freenode or EFNet.

4.使用Nmap实现系统安全检测

- Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
  - Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.
  - It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.
  - In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

4.使用Nmap实现系统安全检测

Flexible	**Powerful**	**Portable**
Easy	**Free**	**Well Documented**
Supported	**Acclaimed**	**Popular**

4.使用Nmap实现系统安全检测

- Nmap工具进行主机扫描或安全检测时，语法格式为：

nmap [选项] [对象]

- 选项：
  - 使用 “--script” 选项则说明指定检测脚本名称。
  - 未使用此选项，则默认使用“default”脚本类型，进行基本的应用服务信息收集。
- 对象：
  - 指定安全扫描与漏洞检测的主机IP地址或IP地址段。
- 安装：
  - 使用yum工具进行安装：yum install nmap

表 11-3-1 Nmap 脚本执行选项说明

选项	说明
--script	指定使用的脚本文件名称或脚本类型信息
--script-args	为脚本文件提供参数信息
--script-args-file	提供脚本执行参数文件
--script-trace	显示发送和接收到的数据信息
--script-updatedb	执行更新脚本数据库
--script-help	显示脚本帮助信息

表 11-3-2 Nmap 脚本类型与含义

类型	说明
default	默认的脚本扫描，主要是搜集各种应用服务的信息，提供基本脚本扫描能力
auth	负责处理鉴权证书（绕开鉴权）的脚本
broadcast	在局域网内探查更多服务开启状况，如 dhcp/dns/sqlserver 等服务
brute	提供暴力破解方式，针对常见的应用如 http/snmp 等
discovery	对网络进行更多的信息，如 SMB 枚举、SNMP 查询等
dos	用于进行拒绝服务攻击
exploit	利用已知的漏洞入侵系统
external	利用第三方的数据库或资源，例如进行 whois 解析
fuzzer	模糊测试的脚本，发送异常的包到目标机，探测出潜在漏洞
intrusive	入侵性的脚本，此类脚本可能引发对方的 IDS/IPS 的记录或屏蔽
malware	探测目标机是否感染了病毒、开启了后门等信息
safe	此类与 intrusive 相反，属于安全性脚本
version	负责增强服务与版本扫描（Version Detection）功能的脚本
vuln	负责检查目标机是否有常见的漏洞（Vulnerability），如是否有 MS08_067

表 11-3-3 Nmap 常用基础检测选项

选项	说明
-sn	只进行主机发现扫描，不进行端口扫描
-sU	指定使用 UDP 扫描方式扫描目标主机的 UDP 端口状况
-Pn	跳过主机发现扫描，将所有制定的主机都视为在线状态，进行端口扫描
-sL	仅列出指定的目标主机 IP，不进行主机发现扫描
-F	快速扫描模式，仅仅扫描开放率最高的前 100 个端口
--top-ports <number>	仅扫描开放率最高的 number 个端口
-PO	使用 IP 协议包探测目标主机是否在线
-sV	nmap 进行应用服务版本侦测
-O	nmap 进行操作系统版本侦测
--osscan-guess	nmap 进行操作系统类型侦测

请注意：大小写是不同的!

4.使用Nmap实现系统安全检测

- 使用Nmap进行主机检测
  - 使用Nmap工具对指定网络范围内的主机运行状态、开启的服务端口、运行软件及版本信息、操作系统信息进行检测。
  - 实现4个目标。
    - 检测网络内主机的开启状态
    - 检测开启主机的端口信息
    - 检测开启主机的业务服务信息
    - 检测开启主机的操作系统信息

命令指南 / 操作引导

```
#使用Nmap工具对10.10.2.0/24网络段内主机进行安全检测
[root@Project-11-Task-01 ~]# nmap -sV -O 10.10.2.0/24

#展示Nmap当前版本与执行操作的时间
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-26 13:44 CST

#为了排版方便此处删除了部分发现的主机信息

#主机（IP地址为10.10.2.125）扫描的报告结果如下
Nmap scan report for 10.10.2.125
Host is up (0.000014s latency).                          #主机状态为开启
Not shown: 996 closed ports                              #常用1000个端口中，有996个端口处于关闭状态
PORT     STATE SERVICE VERSION                           #针对开放端口服务，查看运行版本信息
21/tcp   open  ftp     vsftpd 3.0.3                      #FTP服务使用vsftpd软件搭建，版本为3.0.3
22/tcp   open  ssh     OpenSSH 8.0 (protocol 2.0)        #OpenSSHare服务版本为8.0，遵照开源SSH2.0协议
80/tcp   open  http    Apache httpd 2.4.37 ((centos))    #Apache版本为2.4.37，基于操作系统为CentOS
3306/tcp open  mysql   MySQL 5.5.5-10.3.17-MariaDB       #MySQL版本为5.5.5，使用的是MariaDB数据库
Device type: general purpose                             #设备类型为通用设备（普通PC或服务器）
Running: Linux 3.X                                       #主机操作系统名称为Linux，版本为3.X
OS CPE: cpe:/o:linux:linux_kernel:3                      #操作系统内核版本为3
OS details: Linux 3.7 - 3.10                             #主机操作系统详细名称
Network Distance: 0 hops                                 #网络路由追踪：0跳（直接到达）
Service Info: OS: Unix                                   #操作系统类型为Unix
#操作系统或服务的检测结果，如有异议可在Nmap官网上进行提交
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
#本次Nmap命令共扫描256地址，其中47个主机是处于开机运行状态，总共耗时4603.56秒
Nmap done: 256 IP addresses (47 hosts up) scanned in 4603.56 seconds
```

4.使用Nmap实现系统安全检测

- 使用Nmap评估域名解析服务的安全风险
  - 通过Nmap工具检测域名解析服务的安全风险。
  - 实现5个目标。
    - 使用 “dns-nsid” 插件检测DNS服务运行版本的详细信息
    - 使用 “dns-brute” 插件检测是否能够破解列出DNS服务器中“domain.com”域名下的主机记录信息
    - 使用 “dns-blacklist” 插件检测DNS服务器是否支持防止DNS反垃圾和打开Proxy黑名单等安全措施
    - 使用 “dns-random-srcport” 插件检测DNS服务器是否存在可预测的端口递归漏洞
    - 使用 “dns-random-txid” 插件检测DNS服务器是否存在可预测的TXID DNS递归漏洞

命令指南 / 操作引导

```
#根据域名解析服务器的安全检测目标进行执行检查
[root@Project-11-Task-01 ~]# nmap --script=dns-nsid
                              --script=dns-brute
                              --script=dns-blacklist
                              --script=dns-random-srcport
                              --script=dns-random-txid
                              --script-args
                              dns-brute.domain=domain.com 10.10.2.121

Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-26 19:28 CST
Pre-scan script results:
| dns-brute:                                    #破解查看domain.com域名下主机记录信息
|   DNS Brute-force hostnames:
|     ns.domain.com - 10.10.2.121
|     ns1.domain.com - 10.10.2.122
|     www.domain.com - 10.10.2.200
|_    ftp.domain.com - 10.10.2.200

Nmap scan report for ns.domain.com (10.10.3.185)
Host is up (0.00017s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
| dns-nsid:                                     #查看DNS服务运行的版本
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el8   #使用BIND工具搭建DNS服务器，BIND版本为9

MAC Address: 00:50:56:9A:DF:D9 (VMware)
Host script results:
| dns-blacklist:                                #查看DNS反垃圾邮件和Proxy黑名单解析地址等
|   SPAM
|     bl.spamcop.net - FAIL
|_    sbl.spamhaus.org - FAIL

Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

4.使用Nmap实现系统安全检测

任务1：使用Nmap实现自动化安全评估

任务2：对网站服务器与网站业务进行安全评估

4.使用Nmap实现系统安全检测

任务1：使用Nmap实现自动化安全评估

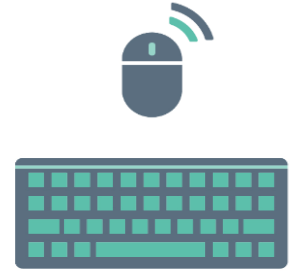
- 步骤1：安装Nmap
- 步骤2：关闭受测主机防火墙等安全措施以凸显检测效果（实验目的）
- 步骤3：安装电子邮件发送客户端工具
- 步骤4：明确安全检测的内容与计划
- 步骤5：撰写自动化安全评估的脚本程序
- 步骤6：执行并测试结果

任务总结 / 任务扩展

- 使用Nmap工具对网络内主机与域名解析服务进行安全检测，检测完成后通过电子邮件将报告发送给指定的运维管理人员。
- 以达到运维管理人员快速发现安全风险，实现运维管理与安全检测的部分自动化。
  - 本步骤通过操作系统的任务计划进行任务调度
  - 安全评估任务实现4个目标
    - 自动进行安全检测，每天00:00执行，检测结果以邮件的形式发送给运维人员
    - 对网络内主机运行状态、开启端口、运行软件版本、操作系统信息等内容进行检测
    - 实现对域名解析服务的安全性检测
    - 检测结果内容通过电子邮件发送给指定电子邮箱

操作视频 / 现场演示

- 任务1：使用Nmap实现自动化安全评估
  - 任务目标：
    - 完成Nmap的安装
    - 完成mailx的安装与配置
    - 完成安全评估脚本的撰写
    - 实现自动化安全评估并发送检测报告邮件

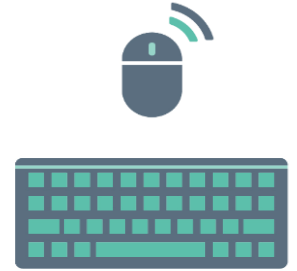


命令指南 / 操作引导

```
#安装Nmap
[root@Project-11-Task-01 ~]# yum install nmap
[root@Project-11-Task-01 ~]# nmap --version

#使用Nmap进行主机安全检测
[root@Project-11-Task-01 ~]# nmap -sV -O --osscan-guess 10.10.2.96/27

使用Nmap评估域名解析服务的安全风险
[root@Project-11-Task-01 ~]# nmap --script=dns-nsid
                              --script=dns-brute
                              --script=dns-blacklist
                              --script=dns-random-srcport
                              --script=dns-random-txid
                              --script-args
                              dns-brute.domain=hactcm.edu.cn 211.69.32.8
[root@Project-11-Task-01 ~]# nmap --script=dns-nsid
                              --script=dns-brute
                              --script=dns-blacklist
                              --script=dns-random-srcport
                              --script=dns-random-txid
                              --script-args
                              dns-brute.domain=baidu.com 10.10.2.1

#安装电子邮件发送客户端工具
[root@Project-11-Task-01 ~]# yum install -y mailx
#使用vi工具修改mailx的配置文件/etc/mail.rc，填写电子邮件发送与接收人的信息。
#配置文件：/etc/mail.rc
#mail.rc配置文件内容较多，本部分仅显示发送电子邮件配置有关的内容，
#在配置文件中增加如下内容
set from=ruanxiaolong@hactcm.edu.cn                  #设置发件人的邮箱信息
set smtp=smtp.hactcm.edu.cn                          #设置邮件服务器的地址
set smtp-auth-user=ruanxiaolong@hactcm.edu.cn        #设置发件人邮箱地址
set smtp-auth-password=********                      #设置客户端发送邮件的授权密码
set smtp-auth=login                                  #设置邮件认证方式为登录
```

命令指南 / 操作引导

```
#使用vi工具在/opt目录下创建Shell执行脚本文件，脚本内容如下。
#脚本程序：/opt/autoCheck.sh

#!/bin/bash
#清理历史报告信息
rm -rf /opt/CheckReport.txt

#定义需要检测的网络段地址
netWork="10.10.2.96/27"
#定义域名服务器地址
dnsIp="10.10.2.1"
#定义要接收邮件的运维人员邮箱，根据个人情况进行配置
userMail="****@****.***"
#获取脚本执行时的时间
time=$(date +"%Y年%m月%d日 %H:%M:%S")

#输出分隔符
echo -e "\n---------------Host CheckReport---------------\n\n" >> /opt/CheckReport.txt
#对网络段内的主机执行安全检测，并将检测结果输出到/opt/hostCheck.txt文本中
nmap -sV -O --osscan-guess $netWork >> /opt/CheckReport.txt
#输出分割符
echo -e "\n\n\n---------------DNS  CheckReport---------------\n\n" >> /opt/CheckReport.txt
#对域名解析服务进行安全检测，并将检测结果输出到/opt/dnsCheck.txt文本中
nmap --script=dns-nsid --script=dns-brute --script=dns-blacklist --script=dns-random-srcport --script=dns-random-txid --script-args dns-brute.domain=hactcm.edu.cn $dnsIp >> /opt/CheckReport.txt

#配置邮件进行发送，邮件发送主题为"安全评估报告"
echo -e '安全扫描结果详见附件。\n检测时间为：'$time | mail -s "使用Nmap进行业务安全评估的报告" -a /opt/CheckReport.txt $userMail
```



命令指南 / 操作引导

```
#添加脚本的执行权限
[root@Project-11-Task-01]# chmod +x /opt/autoCheck.sh

#手动执行脚本程序，查看能否执行成功和接收到邮件信息，完成脚本测试
[root@Project-11-Task-01]# bash /opt/autoCheck.sh

#脚本测试通过后，配置操作系统的任务计划，每天00:00执行一次
#[root@Project-11-Task-01]#echo "0 0 * * * root bash /opt/autoCheck.sh" >> /etc/crontab

#为了继续测试，暂时设定为每10分钟执行一次
[root@Project-11-Task-01]#echo "*/10 * * * * root bash /opt/autoCheck.sh " >> /etc/crontab
```

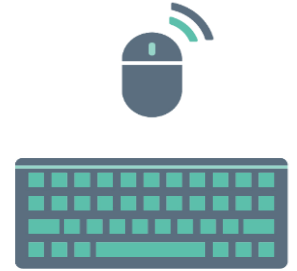
4.使用Nmap实现系统安全检测

任务2：对网站服务器与网站业务进行安全评估

- 步骤1：受测主机进行系统与业务安全配置（检测目的）
- 步骤2：检测操作系统的安全性
- 步骤3：检测网站服务的安全性
- 步骤4：检测PHP的安全性
- 步骤5：检测MariaDB的安全性
- 步骤6：检测WordPress的安全性
- 步骤7：撰写安全评估报告

操作视频 / 现场演示

- 任务2：对网站服务器与网站业务进行安全评估
  - 任务目标：
    - 完成对网站服务器和网站业务的安全评估
    - 撰写安全评估报告

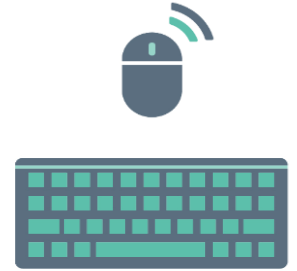


命令指南 / 操作引导

```
#网站服务器防火墙配置允许TCP 80端口访问业务
[root@Project-03-Task-03]#firewall-cmd --add-rich-rule='rule port port=80 protocol=tcp accept'
success

#开启httpd服务的版本检测与目录浏览
[root@Project-03-Task-03 ~]# vi /etc/httpd/conf/httpd.conf
#ServerTokens Prod                    #将配置文件中的ServerTokens选项进行注释

#开启php版本检测
[root@Project-03-Task-03 ~]# vi /etc/php.ini
expose_php = On                       #将expose_php = Off改为expose_php = On

#配置MySQL的远程连接
[root@Project-03-Task-03 ~]# mysql -uroot -p
Enter password:
#为了排版方便，此处删除了部分提示信息

#创建root远程连接用户
MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'centos@mariadb#123' WITH GRANT OPTION;
Query OK, 0 rows affected (0.001 sec)
#刷新用户权限
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)
#进行数据库操作退出
MariaDB [(none)]> quit

#重新载入防火墙使其配置生效
[root@Project-03-Task-03]#systemctl reload firewalld
#重载httpd服务使其配置生效
[root@Project-03-Task-03]#systemctl reload httpd
#重启mariadb服务使其配置生效
[root@Project-03-Task-03]#systemctl restart mariadb
```

命令指南 / 操作引导

```
#使用Nmap工具对网站服务器进行扫描和安全检测，使用-sV -O选项。
[root@Project-11-Task-01 ~]# nmap -sV -O 10.10.2.105

#使用Nmap工具对所部署的网站服务进行安全检测，实现下述3个目标。
#①使用"http-methods"插件检测网站服务可支持的HTTP方法类型；
#②使用"http-enum"插件检测网站服务是否存在敏感目录信息；
#③使用"http-vuln*"插件检测网站服务是否存在安全漏洞。
#使用Nmap工具对网站服务进行扫描和安全检测，检测时使用相应脚本。
[root@Project-11-Task-01 ~]# nmap --script=http-methods
                              --script=http-enum
                              --script=http-vuln*
                              10.10.2.105

#通过使用Nmap工具对PHP及扩展进行安全检测，实现下述4个目标。
#①使用"http-php-version"插件检测网站服务器中PHP版本信息；
#②使用"http-phpmyadmin-dir-traversal"插件检测易受攻击的PHP目录或文件；
#③使用"http-phpself-xss"插件检测容易受到跨站点脚本攻击的PHP文件；
#④使用"http-vuln-cve2012-1823"插件检测是否存在针对PHP-CGI模块的远程执行代码漏洞（CVE-2012-1823）。
#使用Nmap工具对PHP进行扫描和安全检测，检测时使用相应脚本。
[root@Project-11-Task-01 ~]#nmap --script=http-php-version
                             --script=http-phpmyadmin-dir-traversal
                             --script=http-phpself-xss
                             --script=http-vuln-cve2012-1823
                             10.10.2.105

#使用Nmap工具对MariaDB数据库进行安全检测，实现下述4个目标。
#①使用"mysql-info"插件检测数据库基本信息；
#②使用"mysql-empty-password"插件检测数据库是否存在空口令；
#③使用"mysql-enum"插件检测数据库中具有执行权限的用户；
#④使用"mysql-vuln*"插件检测数据库服务是否存在安全漏洞。
#使用Nmap工具对MariaDB进行扫描和安全检测，检测时使用相应脚本。
[root@Project-11-Task-01 ~]# nmap --script=mysql-info
                              --script=mysql-empty-password
                              --script=mysql-enum
                              --script=mysql-vuln*
                              10.10.2.105
```



命令指南 / 操作引导

```
#使用Nmap工具对内容网站所使用的WordPress程序进行安全检测，实现下述5个目标。
#①使用"http-wordpress-enum"插件检测WordPress是否存在主题与插件版本陈旧；
#②使用"http-wordpress-users"插件检测WordPress是否存在用户名信息泄露；
#③使用"http-wordpress-brute"插件检测WordPress是否存在简易密码的现象；
#④使用"http-vuln-cve2014-8877"插件检测WordPress是否存在远程注入漏洞（CVE-2014-8877）；
#⑤使用"http-vuln-cve2017-1001000"插件检测WordPress是否存在未经身份验证的内容注入漏洞（CVE-2017-1001000）。
#使用Nmap工具对WordPress进行扫描和安全检测，检测时使用相应脚本。
[root@Project-11-Task-01 ~]# nmap --script=http-wordpress-enum
                                  --script=http-wordpress-users
                                  --script=http-wordpress-brute
                                  --script=http-vuln-cve2014-8877
                                  --script=http-vuln-cve2017-1001000
                                  10.10.2.105

#依据Nmap对操作系统、网站服务器、PHP、MariaDB、WordPress的安全检测结果
#通过人工对安全检测内容进行整理汇总，撰写安全评估报告，
```

5.国家对信息安全的要求

- 网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法。
- 网络安全等级保护工作是对信息和信息载体按照重要性等级分级别进行保护的一种工作。
- 信息系统运营、使用单位应当选择符合国家要求的测评机构，依据《信息安全技术网络安全等级保护基本要求》等技术标准，定期对信息系统开展测评工作。

5.国家对信息安全的要求

我国关于信息安全的基本政策

政策合规

等级保护

5.国家对信息安全的要求

- 《网络安全法》明确规定信息系统运营、使用单位应当按照网络安全等级保护制度要求，履行安全保护义务，如果拒不履行，将会受到相应处罚。

第二十一条

网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

第三十八条

关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

5.国家对信息安全的要求

- 《网络安全法》明确规定信息系统运营、使用单位应当按照网络安全等级保护制度要求，履行安全保护义务，如果拒不履行，将会受到相应处罚。

第五十九条

网络运营者不履行义务的：由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行义务的：由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

5.国家对信息安全的要求

- 信息安全等级保护，是对信息和信息载体按照重要性等级分级别进行保护的一种工作，在中国、美国等很多国家都存在的一种信息安全领域的工作。
- 在中国，信息安全等级保护：
  - 广义上为涉及到该工作的标准、产品、系统、信息等均依据等级保护思想的安全工作
  - 狭义上一般指信息系统安全等级保护

5.国家对信息安全的要求

颁布时间	文件名称	文号	颁布机构	内容及意义
1994年 2月18日	《中华人民共和国计算机信息系统安全保护条例》	国务院147号令	国务院	第一次提出信息系统要实行等级保护，并确定了等级保护的职责单位。
2003年 9月7日	《国家信息化领导小组关于加强信息安全保障工作的意见》	中办国办发[2003]27号	中共中央办公厅 国务院办公厅	等级保护工作的开展必须分步骤、分阶段、有计划的实施。明确了信息安全等级保护制度的基本内容。
2004年 9月15日	《关于信息安全等级保护工作的实施意见》	公通字[2004]66号	公安部 国家保密局 国家密码管理委员会办公室（国家密码管理局） 国务院信息化工作办公室	将等级保护从计算机信息系统安全保护的一项制度提升到国家信息安全保障的一项基本制度。
2007年 6月22日	《信息安全等级保护管理办法》	公通字[2007]43号		明确了信息安全等级保护制度的基本内容、流程及工作要求，明确了信息系统运营使用单位和主管部门、监管部门在信息安全等级保护工作中的职责、任务。
2007年 7月16日	《关于开展全国重要信息系统安全等级保护定级工作的通知》	公信安[2007]861号		就定级范围、定级工作主要内容、定级工作要求等事项进行了通知。

5.国家对信息安全的要求

- 信息安全等级保护工作包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段。
  - 信息系统安全等级测评是验证信息系统是否满足相应安全保护等级的评估过程。
  - 信息安全等级保护要求不同安全等级的信息系统应具有不同的安全保护能力，
    - 一方面通过在安全技术和安全管理上选用与安全等级相适应的安全控制来实现；
    - 另一方面分布在信息系统中的安全技术和安全管理上不同的安全控制，通过连接、交互、依赖、协调、协同等相互关联关系，共同作用于信息系统的安全功能，使信息系统的整体安全功能与信息系统的结构以及安全控制间、层面间和区域间的相互关联关系密切相关。
    - 因此，信息系统安全等级测评在安全控制测评的基础上，还要包括系统整体测评。

5.国家对信息安全的要求

- 《信息安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。
- 信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。
- 信息系统的安全保护等级分为以下五级，一至五级等级逐级增高：
  - 第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。
  - 第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。国家信息安全监管部门对该级信息系统安全等级保护工作进行指导。

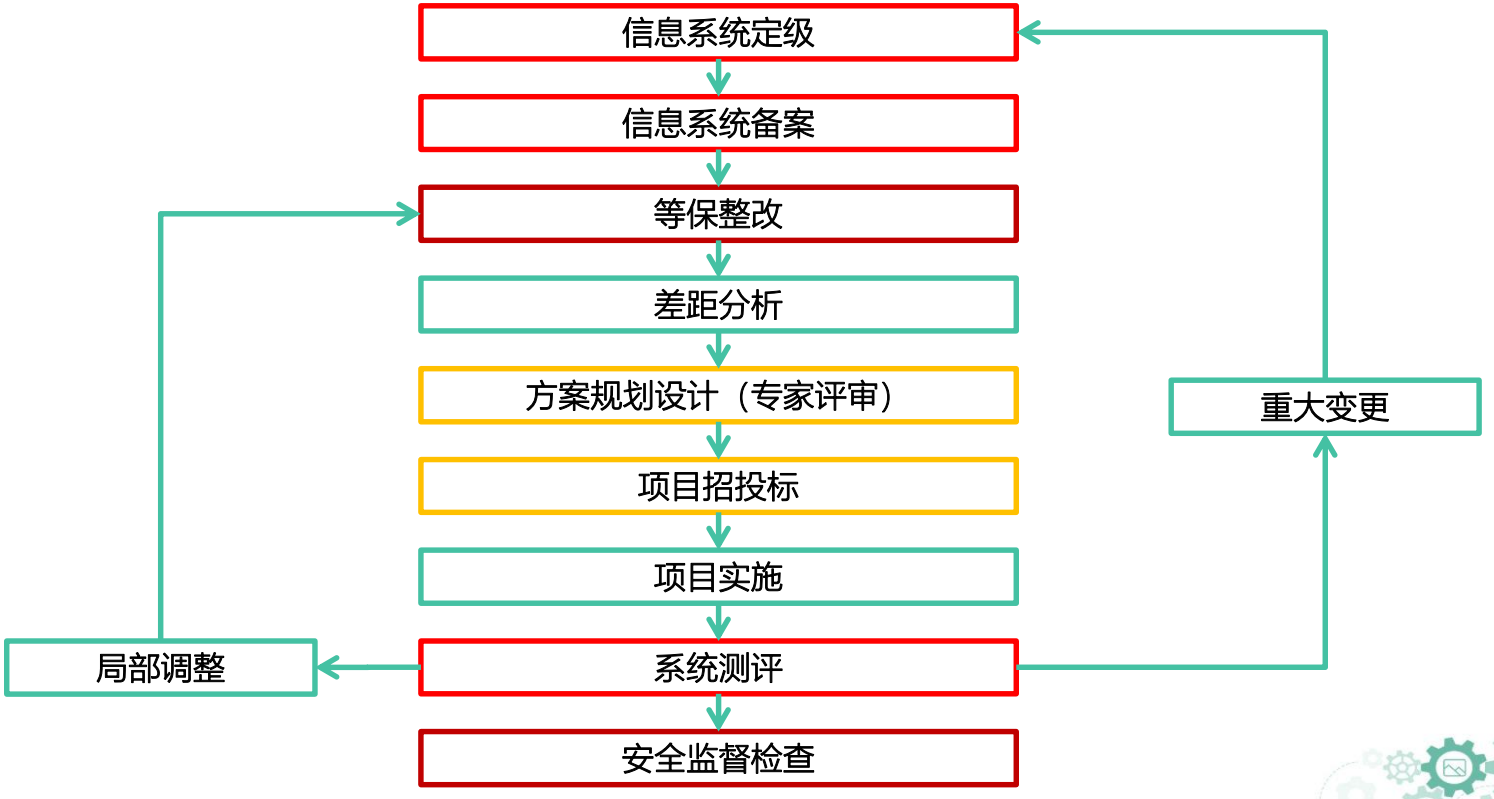
5.国家对信息安全的要求

- 《信息安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。
- 信息系统的安全保护等级分为以下五级，一至五级等级逐级增高：
  - 第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查。
  - 第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行强制监督、检查。
  - 第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查。

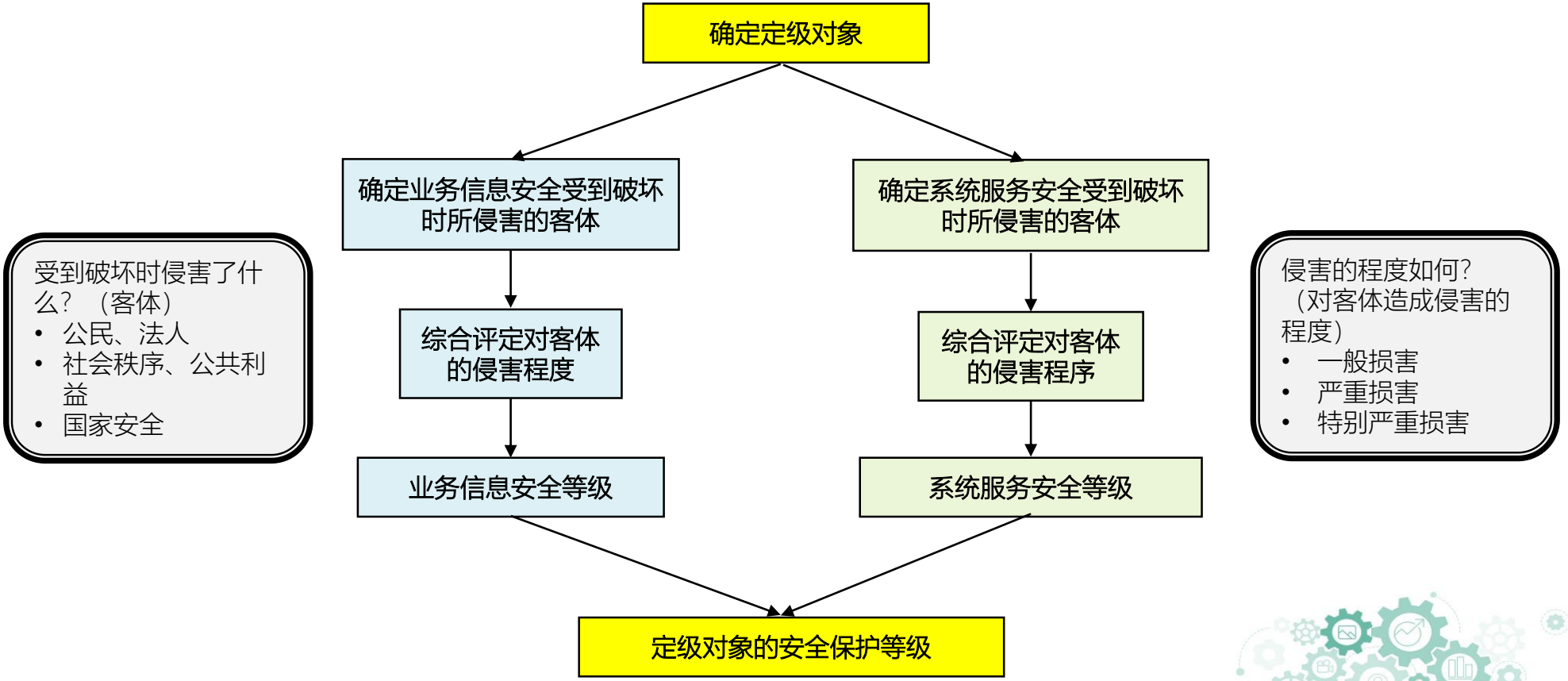
5.国家对信息安全的要求

等级	对象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法权益	一般损害	自主保护
第二级		合法权益	严重损害	指导保护
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督保护
		国家安全	损害	
第四级		社会秩序和公共利益	特别严重损害	强制保护
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专控保护

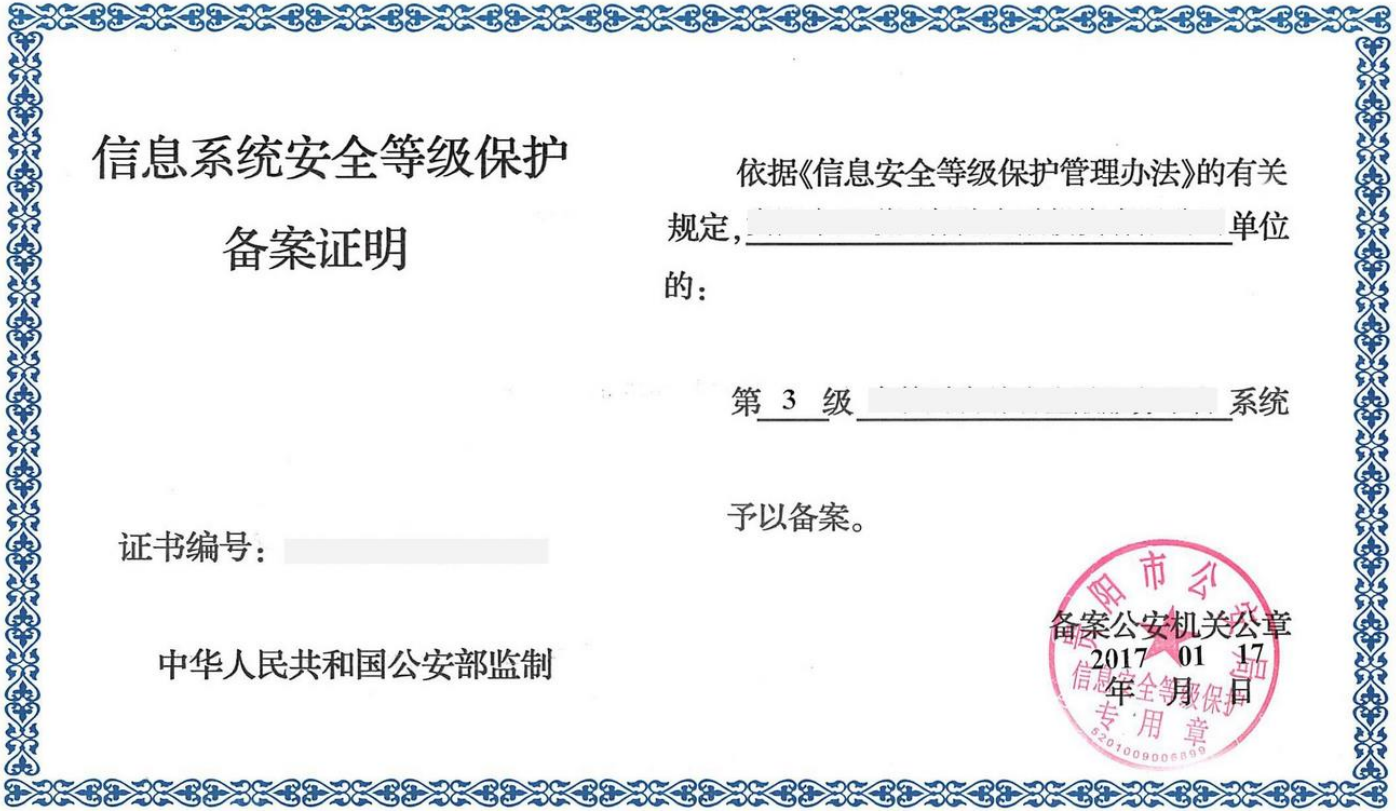
5.国家对信息安全的要求



5.国家对信息安全的要求



5.国家对信息安全的要求



信息系统安全等级保护

备案证明

依据《信息安全等级保护管理办法》的有关规定，[redacted]单位的：

第 3 级 [redacted] 系统

予以备案。

证书编号：[redacted]

中华人民共和国公安部监制

备案公安机关公章

2017 01 17

年 月 日


智能运维课程体系


棒棒堂