Linux服务器构建与运维管理

第7章：系统安全

阮晓龙

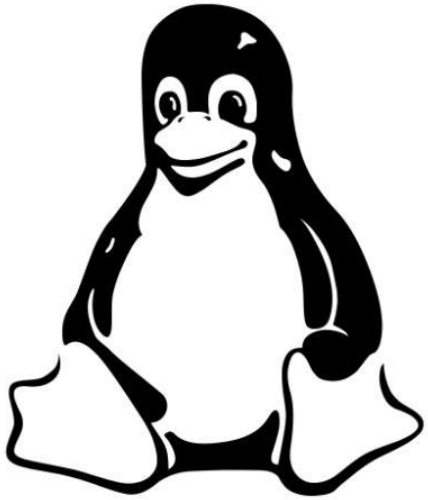
13938213680 / rxl@hactcm.edu.cn
http://linux.xg.hactcm.edu.cn
http://www.51xueweb.cn

河南中医药大学管理科学与工程学科

2018.5

提纲

- 系统安全
- SELinux
  - SELinux框架
  - SELinux文件
  - SELinux配置管理
- 防火墙
  - Linux防火墙
  - iptables
- 系统安全检测工具
  - 安全审计工具：Nmap
  - 入侵检测工具：snort、last、lastb、lastlog、history



1.系统安全

- Linux是一个开放式操作系统，许多现成的程序或工具对Linux操作系统进行管理，使得潜入Linux更容易。Linux目前存在如下安全隐患。
  - 操作系统进行文件操作时可大致分为读、写和执行三种。
    - 一些系统文件一旦可写，就可能会被任意修改。在Linux中，有许多重要文件（如/bin/login）如果被入侵者修改，那么入侵者就可以随意侵入系统。
  - 进程终止后其运行时使用的内存等资源未能重置或清空，入侵者可能通过未重置或清空资源获取信息，造成信息泄露。
  - 重要进程不受保护。Linux中有些重要进程（如VJEB服务器守护进程），并没有得到操作系统的严格保护，非常容易受到入侵者的破坏。

1.系统安全

- Linux是一个开放式操作系统，许多现成的程序或工具对Linux操作系统进行管理，使得潜入Linux更容易。Linux目前存在如下安全隐患。
  - 服务性攻击。
    - 网络中存在的服务性攻击越来越多，如众所周知的smurf攻击，如果某台服务器将大量含有虚假源地址的ICMP包发送到一个或多个服务器上，那么在一个多路广播的网络中，会导致多个服务器分别响应每一个ICMP包，使整个网络中充满广播包，导致操作系统忙于应答。
  - 扫描工具恶意攻击。
    - 扫描工具可以对系统进行扫描，检测服务器是否存在安全漏洞，尽管其本身不进行攻击，但是它可以被入侵者配置成自动攻击的脚本进行攻击，具有很高的安全隐患。

1.系统安全

- Linux内置多种安全保护机制。
  - PAM机制。
    - PAM（Pluggable Authentication Modules）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的应用程序的情况下改变本地认证方法。
  - 安全审计机制。
    - 即使运维人员在Linux中采取了各种安全措施，但还会被发现一些新的漏洞。入侵者可以在漏洞被修补之前攻破尽可能多的服务器。虽然Linux不能预测何时服务器会受到攻击，但是它可以记录入侵者的行踪。同时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进行复查提供支持。

1.系统安全

- Linux内置多种安全保护机制。
  - 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。
    - 防火墙是在被保护服务器和互联网之间，或者在其他网络之间限制访问的一种部件或一系列部件，通过配置防火墙的访问控制、审计以及抗攻击等功能，可以保障服务器自身的安全性。

2. SELinux

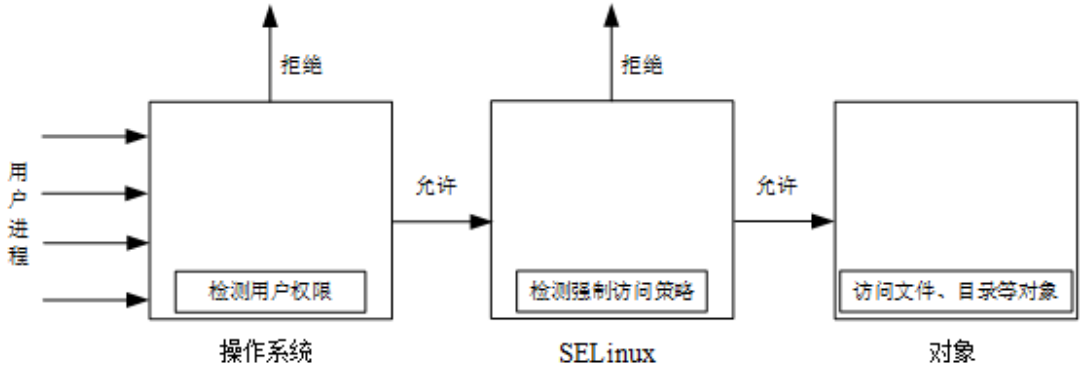
- SELinux（Security-Enhanced Linux）是基于Linux内核的强制访问控制机制的实现，是由美国国家安全局（NAS）开发的项目，旨在增强传统Linux操作系统的安全性。
- SELinux起源于1980年开始的微内核和操作系统安全的研究，这两条研究线路最后形成了分布式信任计算机（DTMach，Distribute Trusted Mach）的项目，并融合了之前研究项目的成果。
- 美国国家安全局的研究组织参加了DTMach项目，付出了巨大努力，并且继续参与了大量的后续安全微内核项目。最终引发了一个新的项目产生，即Flask，它支持更丰富的动态类型的强制机制。

2. SELinux

- 美国国家安全局认为需要通过社区推广Flask，并广泛收集使用意见。
  - 1999年夏天，美国国家安全局在Linux内核中实现Flask安全架构。
  - 2000年12月，美国国家安全局发布研究的第一个公共版本，叫做安全增强的Linux。
  - 因为是在主流的操作系统中实现的，所以SELinux开始受到Linux社区的注意，SELinux最早是在Linux 2.2.x内核中以一套内核补丁的形式发布的。
- 美国国家安全局在2001年的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。
  - SELinux可以被用来限制程序的最小执行权限，提高程序安全，从而保护程序和资料的完整性和机密性。

2. SELinux

- 目前所有2.6及以上版本的Linux内核中都集成了SELinux。
- 使用SELinux后，操作系统中的文件、目录、设备甚至端口都将作为“对象”，而用户运行的进程则被当做“主题”。
- 一个“主题”（进程）不能直接访问到任何“对象”（文件、目录、设备甚至端口），需要经过以下如图所示步骤。



2. SELinux

- 身份：
  - 在SELinux中，身份（identity）的概念不同于传统的UNIX uid（user id）。它们可以共存于一个操作系统，但却是不同的概念。
  - 在SELinux中身份是安全上下文的一部分，它会影响到哪个域可以进入。一个SELinux的身份会跟标准的UNIX登录名有很相似的文本标识，但它们是两个完全不同的概念，如运行su命令将不会改变SELinux中的身份。
- 角色：
  - 角色决定了哪些域可以使用。有关哪些域被哪些角色使用可以预先定义在策略的配置文件中。
  - 如果一个策略数据库中定义了一个角色不可以使用一个域，它将被拒绝。

2. SELinux

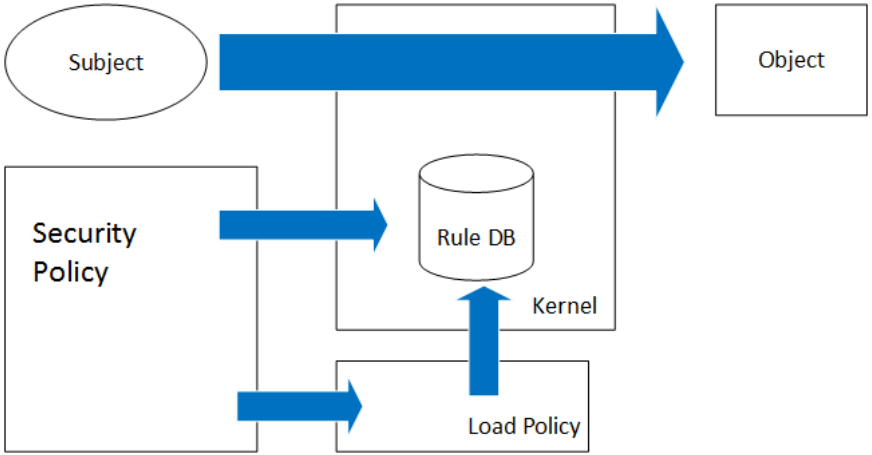
- 域：
  - 所有进程都在域中进行，域直接决定了进程的访问。
  - 域基本上是一个进程运行操作的列表，或者说它决定了一个进程可以对哪些类型进行操作。在这个系统上的任何用户，只要能够执行这个程序，就有可能获得root的权限，这存在着巨大的安全漏洞。
  - 在使用SELinux的操作系统中，如果一个正在执行的进程想要转换进入特权域中执行时，则SELinux需要检测该进程是否允许进入特权域中进行执行。
  - 常见的域类型有：sysadmi_t表示为系统管理域；user_t表示为无特权用户域； init_t表示Init进程运行域；named_t表示named进程运行域。
- 类型：
  - 类型是设定一个对象并设置该对象可以被哪些内容访问。
  - 类型的定义和域的定义基本相同，不同之处在于域是对进程的应用，而类型是分配给目录、文件和套接字的。

2. SELinux

- 策略：
  - 策略是可以设置的规则，决定了一个角色的用户可以访问什么、哪个角色可以进入哪个域和哪个域可以访问哪个类型等问题，用户可以根据想要建立系统的特点来设置相应策略。
- 安全上下文：
  - 安全上下文包括了所有事情属性的描述，包括文件、目录、进程、TCP sockets以及以上所有的内容。
  - 安全上下文同时也包含了身份、角色、域和类型等内容。在SELinux系统上可以用id命令来查看当前用户的安全上下文。
- 转换
  - 根据安全上下文来判断是否发生转换，主要有两种方式的转换：
    - 一种是当前执行了一个被限定类型的程序时会发生的进程域转换；
    - 另一种是在特殊的目录下创建文件时发生的文件类型的转换。

2. SELinux

- SELinux系统架构如图所示。
  - SELInux提供策略语言（Policy Language）供运维人员制定安全策略（Security Policy），并由核心层进行存取控制检查，同时也可加载策略（Load Policy）为SELinux提供新的策略政策，共同维护SELinux的规则数据库（Rule DB）。
  - SELinux将系统内核（Kernel）及安全策略绑在一起，从而检测一个主题（Subject）是否有权限能够访问到某一对象（Object）。



2. SELinux

- SELinux系统架构如图所示。
  - SELinux同时提供了范例策略（Example Policy），详细规划了安全策略所应有的权限，包括Server Process（如Samba Server）、Client Process（如Web Browser）等，并允许使用者利用类型强化（Type Enforce，TE）及RBAC（Role Base Access Control）方式来控制系统。
  - 通过权限的分散及强制的限制，SELinux可以有效防止rootkit及未知攻击，并且SELinux拥有较高阶的语言表示，可以分别为各分层设定安全策略，经由SELinux自动重组后，能根据所设定的策略限制存取权限。

2. SELinux

- SELinux已经作为模块集成到内核中，且默认处于开启状态。对于管理人员来说，需要关注SELinux的配置与管理。
- 配置文件目录：
  - /selinux/即为SELinux伪文件系统，它包括内核子系统最常使用的各种命令。此类型的文件系统与/proc/伪文件系统非常相似，系统管理员和用户通常不需要直接操作该部件。
  - /etc/selinux/目录是所有策略文件和主要配置文件存放的首要位置。
  - 通过cat /etc/selinux/config查看SELinux的全局配置文件。

2. SELinu

2.4 SELinux文件

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
#SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are pro
tected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22

①SELinux 模式(图 10-3 中第 6 行的 SELinux 选项)可以设置为 enforcing(强制)、permissive(宽容)或 disable(禁用)。SELinux 模式设置说明如表 10-1 所示。

表 10-1 SELinux 模式设置说明

模式	说明
enforcing	强制模式。在 enforcing 模式下，策略被完整执行，这是 SELinux 的主要模式，建议在所有要求增强 Linux 安全性的操作系统上使用
permissive	宽容模式。在 permissive 模式下，策略规则不被强制执行，只是审核遭受拒绝的消息，SELinux 不会影响系统的安全性，这个模式在调试和测试一个策略时非常有用
disabled	关闭模式。在 disabled 模式下，SELinux 内核机制是完全关闭的，设置该状态后，系统重启后模式设置才能生效

②SELinux 策略类型（图 10-3 中第 11 行的 SELINUXTYPE 选项）可以设置为 targeted 类型或 mls 类型（strict 类型）。SELinux 策略类型设置说明如表 10-2 所示。

表 10-2 SELinux 策略类型设置

类型	说明
targeted	主要对系统中的目标网络进程进行访问控制
mls（strict）	对系统中所有进程进行访问控制

targeted 为系统已经保护起来的守护进程（如 dhcpd、httpd、named、nscd、ntpd、portmap、snmpd、squid 以及 syslogd 等进程）规定了更多安全措施，mls（strict）则保护整个系统。启用 mls（strict）后，用户执行简单的命令（如 ls）都会报错，所以该策略限制太严格了，系统很难使用。因为计算机的入侵多数是来自网络的，通常选择 targeted 作为 SELinux 的策略控制类型，即提供了对目标网络守护进程的保护，又不会影响到整体系统的使用。

2. SELinux

- 查看SELinux状态：sestatu

【功能】

sestatus 命令可查看 SELinux 的运行状态、进程或文件等详细信息。

【语法】

```
# sestatus [选项]
```

【选项说明】

sestatus 命令选项及其说明如表 10-3 所示。

表 10-3 sestatus 命令选项及其说明

选项	说明
无	不需要输入其他选项。可直接查看 SELinux 状态、模式、策略类型等基本信息
-v	查看/etc/sestatus.conf 文件中的信息（文件和进程的安全上下文信息）
-b	查看一些策略的状态（开启状态或关闭状态）
-vb	可同时查看一些文件和进程的安全上下文值内容以及活动策略的值内容

2. SELinu

- 查看SELin

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
[root@Centos7Teach ~]#
```

表 10-4 SELinux 运行状态说明

状态描述	说明
SELinux status	SELinux 的运行状态，是否开启
SELinuxfs mount	SELinux 的相关文件资料挂载点
SELinux root directory	SELinux 的配置文件所在路径
Loaded policy name	SELinux 加载的策略类型名字
Current mode	SELinux 当前运行模式
Mode from config file	SELinux 配置文件中运行模式
Policy MLS status	MLS 策略状态
Policy deny_unknown status	拒绝未知策略状态
Max kernel policy version	最大内核策略版本

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 11,24 1 会话 CAP NUM

2. SELinux

- 查看SELinux状态：getenforce

【功能】

getenforce 命令可查看 SELinux 的运行模式信息。

【语法】

该命令不需要输入其他选项信息进行查看，其语法格式如下所示。

```
# getenforce
```

2. SELinu

- 查看SELin

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# getenforce
Enforcing
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 15,24 1 会话 CAP NUM

2. SELinux

- 修改SELinux状态：setenforce

【功能】

setenforce 命令可修改 SELinux 运行模式。

【语法】

```
# setenforce [选项]
```

【选项说明】

setenforce 命令的选项说明，如表 10-5 所示。

表 10-5 setenforce 命令选项

选项	说明
Enforcing	将 SELinux 的运行模式设置为强制模式
Permissive	将 SELinux 的运行模式设置为宽容模式
1	将 SELinux 的运行模式设置为强制模式，与 Enforcing 选项相同
0	将 SELinux 的运行模式设置为宽容模式，与 Permissive 选项相同

2. SELinu

- 修改SELin

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# setenforce permissive
[root@Centos7Teach ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
[root@Centos7Teach ~]# setenforce enforcing
[root@Centos7Teach ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
[root@Centos7Teach ~]# setenforce 0
[root@Centos7Teach ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
[root@Centos7Teach ~]# getenforce
Permissive
[root@Centos7Teach ~]# setenforce 1
[root@Centos7Teach ~]# getenforce
Enforcing
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 39,24 1 会话 CAP NUM

2. SELinux

- 修改SELinux状态：setenforce
  - 修改配置文件，实现SELinux的启用与禁用
    - 修改SELinux的配置文件，将配置文件中的SELINUX选项设置为“disabled”，从而关闭SELinux状态。
    - 当系统重启后，配置生效。

2. SELinux

- 修改SELinux状态：setenforce
  - 在系统启动时修改SELinux状态
    - 在系统启动前，可以通过Kernel（内核）命令行参数的方式设定，即利用Boot loader设定该参数，对常用的GRUB就可以在/etc/grub.conf中进行设定。
    - 其中主要有3种需要添加的命令，具体如下所示。

      ①selinux=0：表示为SELinux停用模式（disabled）的参数；

      ②permissive=0：表示为SELinux宽容模式（permissive）的参数；

      ③enforcing=0：表示为SELinux强制模式（enforcing）的参数。

2. SELinux

- Policy
  - 当用户要执行某一程序（例如启动Web服务器）或某一进程执行动作时，系统会依照Policy（策略）所制定的内容来检查用户或进程相对应的权限信息，如果权限符合，系统就会允许该操作的执行。
  - SELinux检查方式独立于传统的使用者权限，必须要同时符合传统的使用者权限和SELinux权限才能顺利执行相应操作。
  - SELinux需要一个合适的Policy才可以发挥效果。如果Policy太宽松会使SELinux毫无用武之地，而太严格又会让用户操作觉得碍手碍脚。
  - 通常Security Policy（安全策略）的制定工作由操作系统发行者来负责，例如RedHat、SUSE、Debian等都内置了Policy。

2. SELinux

- Policy
  - Targeted Policy是RHEL 6.0已定义好的Policy，这个Targeted Policy的用途是保护系统上的各项服务。
  - CentOS 6.0上SELinux可保护的服务有httpd（apache）、named、dhcpd、snmpd等200多个服务。
  - Targeted Policy可粗分为两种类型的属性：
    - 布尔值（boolean）
    - 文件上下文（File contexts）。

2. SELinux

- Policy
  - Targeted Policy的属性：布尔值（boolean）
    - 用来控制每个deamon（service）process“守护（服务）进程”的权限，不仅可对该进程进行整体的权限控制外（${deamonname}_disable_tran），而且还可对该进程的局部权限做控制。
    - 如httpd（apache）就有多个布尔值boolean属性，httpd_enable_cgi可控制httpd是否可以执行cgiscript；httpd_can_network_connect可控制httpd是否可以对外做网络联机等。

2. SELinux

- Policy
  - Targeted Policy的属性：文件上下文（File contexts）
    - 用来控制文件系统中每个文件及目录的SELinux权限，它可用来设定每个文件及目录的属性，可针对某个进程做严格的读写限制。
    - 简单来说，布尔值控制进程行为本身，而上下文是控制进程读写文件的权限。

2. SELinu

尔值和上下文配置

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# tree /etc/selinux/targeted/contexts/
/etc/selinux/targeted/contexts/
├── customizable_types
├── dbus_contexts
├── default_contexts
├── default_type
├── failsafe_context
├── files
│   ├── file_contexts
│   ├── file_contexts.bin
│   ├── file_contexts.homedirs
│   ├── file_contexts.homedirs.bin
│   ├── file_contexts.subs
│   ├── file_contexts.subs_dist
│   └── media
├── initrc_context
├── lxc_contexts
├── removable_context
├── securetty_types
├── sepgsql_contexts
├── snapperd_contexts
├── systemd_contexts
├── userhelper_context
├── users
│   ├── guest_u
│   ├── root
│   ├── staff_u
│   ├── sysadm_u
│   ├── unconfined_u
│   ├── user_u
│   └── xguest_u
├── virtual_domain_context
├── virtual_image_context
└── x_contexts

2 directories, 30 files
[root@Centos7Teach ~]#
```

表 10-6 Policy 部分目录架构说明

目录	说明
contexts/	存储安全上下文 contexts
modules/	多层次 policy 模块化目录
modules/active	多层次 policy 模块化目录（系统目前正式用的 policy）
modules/previous	多层次 policy 模块化目录（系统之前使用的 policy）
policy/	存放二进制的 policy 文件
modules/*/booleans	存放 policy 中每个限制的布尔值
modules/*/booleans.local	自定义 policy 的布尔值（非系统预设的布尔值可放在此路径下）
contexts/files	Domain Type 的 policy 设定文件
contexts/file/file_contests.local	管理者自定义的 policy 设置文件

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 37,24 1 会话 CAP NUM

2. SELinux

- Policy
  - 布尔值属性设定
    - 为了设定方便，SELinux中内建了许多布尔值boolean的参数，可以通过修改这些参数直接来变更一些SELinux的设定。
    - SELinux布尔值boolean属性的操作，常用的命令有getsebool（获取布尔值boolean属性的状态）和setsebool（变更布尔值boolean属性）。

2. SELinux

- getsebool

【功能】

getsebool 命令可取得目前系统上 SELinux booleans 属性的状态信息。

【语法】

```
# getsebool [选项]
```

在使用过程中可通过 getsebool 帮助命令查看选项内容，如图 10-13 所示，其可操作选项及其说明如表 10-7 所示。

```
getsebool: invalid option -- '-'
usage:  getsebool -a or getsebool boolean...
```

图 10-13 getsebool 选项

【选项说明】

getsebool 命令的选项说明，如表 10-7 所示。

表 10-7 getsebool 命令选项

选项	说明
-a	可获得所有 SELinux 配置选项的布尔值状态
boolean 名	输入某单个需要查询的 boolean 名，进行获取该 boolean 的属性状态

2. SELinu

尔值和上下文配置

Teach-CentOS 7 - root@Centos7Teach:/etc/selinux/targeted/contexts - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach contexts]# getsebool httpd_enable_cgi
httpd_enable_cgi --> on
[root@Centos7Teach contexts]# getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
auditadm_exec_content --> on
authlogin_nsswitch_use_ldap --> off
authlogin_radius --> off
authlogin_yubikey --> off
awstats_purge_apache_log_files --> off
boinc_execmem --> on
cdrecord_read_content --> off
cluster_can_network_connect --> off
cluster_manage_all_files --> off
cluster_use_execmem --> off
cobbler_anon_write --> off
cobbler_can_network_connect --> off
cobbler_use_cifs --> off
cobbler_use_nfs --> off
collectd_tcp_network_connect --> off
condor_tcp_network_connect --> off
conman_can_network --> off
container_connect_any --> off
cron_can_relabel --> off
cron_system_cronjob_use_shares --> off
cron_userdomain_transition --> on
cups_execmem --> off
cvs_read_shadow --> off
daemons_dump_core --> off
daemons_enable_cluster_mode --> off
daemons_use_tcp_wrapper --> off
daemons_use_tty --> off
dbadm_exec_content --> on
dbadm_manage_user_files --> off
dbadm_read_user_files --> off
deny_execmem --> off
deny_ptrace --> off
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,31 1 会话 CAP NUM

2. SELinux

- setsebool

【功能】

setsebool 命令可立即变更 SELinux boolean 的属性。

【语法】

```
# setsebool 【选项】
```

【选项说明】

setsebool 命令的选项说明，如表 10-8 所示。

表 10-8 setsebool 命令选项

选项		说明
-NPV		可选项，如果命令中没有该选项，只会变更目前系统 SELinux booleans 属性，并没有更新设定文件的状态，下次系统重新启动后，还会恢复到原来的属性；如果有该选项则会永久变更这个属性
boolean		需要变更的 boolean 属性名称。更改属性可单独设定一个值或者同时设定多个值，同时变更多个属性时需将属性和值之间用“=”连接
value	on 或 1	属性值。表示变更改 boolean 属性值为开启状态
	off 或 0	属性值。表示变更改 boolean 属性值为关闭状态

2. SELinu

尔值和上下文配置

Teach-CentOS 7 - root@Centos7Teach:/etc/selinux/targeted/contexts - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach contexts]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> off
[root@Centos7Teach contexts]#
[root@Centos7Teach contexts]# setsebool -P httpd_enable_homedirs 1
[root@Centos7Teach contexts]#
[root@Centos7Teach contexts]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> on
[root@Centos7Teach contexts]#
[root@Centos7Teach contexts]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 9,31 1 会话 CAP NUM

2. SELinux

- Policy
  - 上下文属性设定
    - 上下文context属性用来控制系统中每个用户、进程、文件及目录的SELinux权限，可用来设定每个user、process、文件及目录的属性，可针对某个process的某个行为做严格的读写限制。
    - 也就是说，文件可以针对某个身份（user）、某个程序（program）的某个行为开放读写权限，或做到最细致的权限调整，无须担心因程序溢位（overflow）问题，而造成的文件数据外泄或遭篡改。

2. SELinux

- Policy
  - 上下文属性设定
    - SELinux的上下文语法格式如下所示。

      USER:ROLE:TYPE[:LEVEL[:CATEGORY]]

    - 上述语法字符使用":"冒号分隔，第一个字段为用户{USER}，第二个字段为角色{ROLE},第三个字段为类型{TYPE}，第四个字段为级别{LEVEL}，第五个字段为分类{CATEGORY}。
    - 其中定义的级别{LEVEL}和分类{CATEGORY}内容只用于mls（strict）策略中，所以这两个选项为可选择的选项。

2. SELinux

- Policy
  - 上下文属性设定
    - SELinux的上下文语法格式如下所示。

      USER:ROLE:TYPE[:LEVEL[:CATEGORY]]

    - 上述语法字符使用":"冒号分隔，第一个字段为用户{USER}，第二个字段为角色{ROLE},第三个字段为类型{TYPE}，第四个字段为级别{LEVEL}，第五个字段为分类{CATEGORY}。
    - 其中定义的级别{LEVEL}和分类{CATEGORY}内容只用于mls（strict）策略中，所以这两个选项为可选择的选项。

2. SELinux

- Policy
  - 上下文属性设定：USER

用户身份是通过 SELinux 策略授权特定角色集合的账户身份，每个系统账户都通过角色映射到一个 SELinux 用户。用户身份类似 Linux 系统中的 UID，提供身份识别，用来记录身份信息。SELinux 常见的三种 user 用户身份如表 10-9 所示。

表 10-9 用户身份角色

身份	描述
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 登录后的预设

users 在 SELinux 策略类型为 targeted 的操作系统中不是很重要，但是在 SELinux 策略类型为 mls（strict）的操作系统中比较重要，所有预设 SELinux Users 都是以“_u”结尾的，root 除外。

2. SELinux

- Policy
  - 上下文属性设定：ROLE
    - SELinux部分采用基于角色的访问控制（RBAC）模型，而角色是RBAC的重要属性。SELinux账户被授予特定的角色，而角色被授予操控特定的域，角色是SELinux用户与域的媒介。
    - 在系统中不同类型的内容角色不同，具体内容角色对应关系如下所示。
      - 文件、目录和设备的角色通常是object_r。
      - 程序的角色通常是system_r。
      - 用户根据SELinux的活动策略类型不同而不同。
        - 当SELinux策略类型为targeted时，用户的角色为system_r；
        - 当SELinux策略类型为mls（strict）时，用户的角色为sysadm_r、staff_r、user_r。
        - 用户的角色，类似系统中的GID，不同角色具备不同的权限，用户可以具备多个角色，但是同一时间内只能使用一个角色。

2. SELinux

- Policy
  - 上下文属性设定：TPYE
    - SELinux类型是用来将主体（subject）和客体（object）划分为不同的组，给每个主体和系统中的客体定义了一个类型，也相当于SELinux类型定义了系统中所有进程的域以及文件的类型，为进程提供最低的权限环境。
    - 当一个类型与执行中的进程相关联时，其类型（type）也称为域（domain）。
    - SELinux类型是SELinux security context中最重要的部位，是SELinux Type Enforcement（SELinux类型强制（TE））的心脏，预设值以“_t”结尾。

2. SELinux

- Policy
  - 上下文属性设定：LEVEL
    - SELinux级别是mls（strict）策略的属性。
    - 一个mls范围是一对级别，书写格式为低级别-高级别，如果两个级别是一致的，也可以仅显示低级别，如s0-s0与s0是一样的。
    - 目前已经定义的安全等级为s0-s15，数字越高则等级越高。

2. SELinux

- Policy
  - 上下文属性设定：CATEGORY
    - SELinux分类是mls（strict）策略的属性，代表着SELinux给文件、目录、程序等内容的分类。
    - 目前已经定义的分类为c0-c1023。

2. SELinux

- Policy
  - 上下文属性查看：ls –Z / ps –Z / id -Z
    - SELinux对系统中的许多命令做了修改，通过添加一个“-Z”选项显示客体和主体的安全上下文。
    - 安全相关上下文contexts属性的操作命令较多，简单介绍几个常用命令，具体命令如下所示。
      - 查看上下文contexts属性值的命令主要有ls –Z、ps –Z和id –Z。
      - ls –Z命令主要查看文件或者目录等内容的上下文信息
      - ps –Z主要是查看进程的安全上下文信息
      - id –Z是查看目前使用者身份的安全上下文信息。

2. SE

...下文配置

Teach-CentOS 7 - root@Centos7Teach:/ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach /]# ls -Z /var/log/firewalld
-rw-r--r--. root root system_u:object_r:firewalld_var_log_t:s0 /var/log/firewalld
[root@Centos7Teach /]#
[root@Centos7Teach /]# ps -Z
LABEL                                PID TTY          TIME CMD
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 4399 pts/0 00:00:00 bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 5461 pts/0 00:00:00 ps
[root@Centos7Teach /]#
[root@Centos7Teach /]# id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@Centos7Teach /]#
[root@Centos7Teach /]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 100x40 12,24 1 会话 CAP NUM

表 10-10 文件 contexts 属性详解

结果	说明
system_u	开机过程中系统进程的预设后 SELinux 用户结果
object_r	表明该查询的内容是一个文件类型
admin_home_t	表明该文件的 SELinux 配置信息是 root 用户的个人目录
s0	表明该文件的安全级别较低

2. SELinux

- Policy
  - 上下文属性修改：chcon

【功能】

chcon 命令可以修改文件 SELinux 安全上下文。

【语法】

```
# chcon [选项] [-u SELinux 用户] [-r 角色] [-l 范围] [-t 类型] 文件
# chcon [选项] --reference=参考文件 文件
```

【选项说明】

chcon 命令选项及其说明如表 10-11 所示。

表 10-11 chcon 命令选项说明

选项	说明
-R	递归改变文件和目录的上下文
--reference	从源文件向目标文件复制安全上下文
-h	--no-dereference，影响目标链接
-u	--user=USER，设置在目标用户的安全上下文
-r	--role=ROLE，设置目标安全领域的作用
-l	--range=RANGE，设置 set role ROLE in the target security context 目标安全领域的范围
-t	--type=TYPE，在目标设定的安全上下文类型
-f	显示少量错误信息

2. SELinu

尔值和上下文配置

- Policy
  - 上下文

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach /]# cp --preserve=all /var/log/firewalld ~/
[root@Centos7Teach /]#
[root@Centos7Teach /]# cd ~
[root@Centos7Teach ~]# ls
demo.conf  samba.install.sh  vsftpd.install.sh
firewalld  samba.remove.sh   vsftpd.remove.sh
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# ls -Z firewalld
-rw-r--r--. root root system_u:object_r:firewalld_var_log_t:s0 firewalld
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# chcon -t admin_home_t firewalld
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# ls -Z firewalld
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 firewalld
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 16,24 1 会话 CAP NUM

2. SELinux

- Policy
  - 上下文属性修改：semanage

【语法】

```
# semanage 【选项】
```

【选项说明】

semanage 命令选项及其说明如表 10-12 所示。

表 10-12 semanage 命令选项说明

选项	说明
-a	--add，添加预设安全上下文
-d	--delete，删除指定的预设安全上下文
-D	--deleteall，删除所有的预设自定义上下文
-m	--modify，修改指定的预设安全上下文
-l	--list，显示预设安全上下文
-n	--noheading，不显示头部信息

2. SELinu 尔值和上下文配置

- Policy
  - 上下文

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# semanage fcontext -l
-bash: /usr/sbin/semanage: No such file or directory
[root@Centos7Teach ~]# yum install semanage
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.cqu.edu.cn
 * epel: mirrors.tongji.edu.cn
 * extras: mirrors.cqu.edu.cn
 * updates: mirrors.cqu.edu.cn
No package semanage available.
Error: Nothing to do
[root@Centos7Teach ~]# yum provides semanage
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.ustc.edu.cn
 * epel: mirrors.tongji.edu.cn
 * extras: centos.ustc.edu.cn
 * updates: centos.ustc.edu.cn
policycoreutils-python-2.5-17.1.el7.x86_64 : SELinux policy core python
                                           : utilities
Repo        : base
Matched from:
Filename    : /usr/sbin/semanage


[root@Centos7Teach ~]# yum install policycoreutils-python
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.ustc.edu.cn
 * epel: mirrors.tongji.edu.cn
 * extras: centos.ustc.edu.cn
 * updates: centos.ustc.edu.cn
Resolving Dependencies
--> Running transaction check
---> Package policycoreutils-python.x86_64 0:2.5-17.1.el7 will be installed
--> Processing Dependency: setools-libs >= 3.3.8-1 for package: policycoreutils-
python-2.5-17.1.el7.x86_64
--> Processing Dependency: libsemanage-python >= 2.5-5 for package: policycoreut
ils-python-2.5-17.1.el7.x86_64
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,21 1 会话 CAP NUM

2. SELinu

尔值和上下文配置

- Policy
  - 上下文

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
1.el7.x86_64
--> Processing Dependency: libapol.so.4(VERS_4.0)(64bit) for package: policycore
utils-python-2.5-17.1.el7.x86_64
--> Processing Dependency: checkpolicy for package: policycoreutils-python-2.5-1
7.1.el7.x86_64
--> Processing Dependency: libqpol.so.1()(64bit) for package: policycoreutils-py
thon-2.5-17.1.el7.x86_64
--> Processing Dependency: libapol.so.4()(64bit) for package: policycoreutils-py
thon-2.5-17.1.el7.x86_64
--> Running transaction check
---> Package audit-libs-python.x86_64 0:2.7.6-3.el7 will be installed
---> Package checkpolicy.x86_64 0:2.5-4.el7 will be installed
---> Package libcgroup.x86_64 0:0.41-13.el7 will be installed
---> Package libsemanage-python.x86_64 0:2.5-8.el7 will be installed
---> Package python-IPy.noarch 0:0.75-6.el7 will be installed
---> Package setools-libs.x86_64 0:3.3.8-1.1.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                  Arch        Version              Repository  Size
================================================================================
Installing:
 policycoreutils-python   x86_64      2.5-17.1.el7         base       446 k
Installing for dependencies:
 audit-libs-python        x86_64      2.7.6-3.el7          base        73 k
 checkpolicy              x86_64      2.5-4.el7            base       290 k
 libcgroup                x86_64      0.41-13.el7          base        65 k
 libsemanage-python       x86_64      2.5-8.el7            base       104 k
 python-IPy               noarch      0.75-6.el7           base        32 k
 setools-libs             x86_64      3.3.8-1.1.el7        base       612 k

Transaction Summary
================================================================================
Install  1 Package (+6 Dependent packages)

Total download size: 1.6 M
Installed size: 5.1 M
Is this ok [y/d/N]: _
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,21 1 会话 CAP NUM

2. SELinu

尔值和上下文配置

- Policy
  - 上下文

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
root                 unconfined_u         s0-s0:c0.c1023       *
system_u             system_u             s0-s0:c0.c1023       *
[root@Centos7Teach ~]# semanage module -l | tail
wine                    100     pp
wireshark               100     pp
xen                     100     pp
xguest                  100     pp
xserver                 100     pp
zabbix                  100     pp
zarafa                  100     pp
zebra                   100     pp
zoneminder              100     pp
zosremote               100     pp
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# semanage port -l | tail
zabbix_port_t                  tcp      10051
zarafa_port_t                  tcp      236, 237
zebra_port_t                   tcp      2606, 2608-2609, 2600-2604
zebra_port_t                   udp      2606, 2608-2609, 2600-2604
zented_port_t                  tcp      1229
zented_port_t                  udp      1229
zookeeper_client_port_t        tcp      2181
zookeeper_election_port_t      tcp      3888
zookeeper_leader_port_t        tcp      2888
zope_port_t                    tcp      8021
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 32,24 1 会话 CAP NUM

2. SELinux

httpd相关的SELinux安全策略

（1）布尔值

SELinux 策略是可自定义设置的，且 SELinux 针对 httpd 服务的策略非常灵活，大量的布尔值可以实现快速维护与灵活管理相关策略，实现安全快捷的访问策略维护，具体配置如下所示。

①允许 httpd 脚本或模块通过网络连接数据库，其操作命令如下所示。

```
# setsebool -P httpd_can_network_connect_db 1
```

②允许 httpd 支持 CGI 程序，其操作命令如下所示。

```
# setsebool -P httpd_enable_cgi 1
```

③允许 httpd 访问 cifs 文件系统资源，其操作命令如下所示。

```
# setsebool -P httpd_use_cifs 1
```

④允许 Apache 使用 mod_auth_pam 模块，其操作命令如下所示。

```
# setsebool -P allow_httpd_mod_auth_pam 1
```

⑤允许 httpd 访问 NFS 文件系统资源，其操作命令如下所示。

```
# setsebool -P httpd_use_nfs 1
```

⑥允许 http 守护进程发送电子邮箱，其操作命令如下所示。

```
# setsebool -P httpd_can_sendmail 1
```

⑦允许 httpd 连接网络 memcache 服务器，其操作命令如下所示。

```
# setsebool -P httpd_can_network_memcache 1
```

2. SELinux

- httpd相关的SELinux安全策略

（2）安全上下文

如果希望多个进程域（如 Apache、FTP、rsync 等）共享相同的文件，可以设置文件安全上下文为 public_content_t 或者 public_content_rw_t，这些安全上下文允许上面提到的所有服务进程域读取文件内容，如果修改为可读写，则需要 public_content_rw_t 的类型标签。

①通过添加 public_content_t 类型标签，允许 httpd 服务读取/var/httpd 目录，其操作命令如下所示。

```
# semanage fcontext -a -t public_content_t "/etc/httpd(/.*)?"
# restorecon -F -R -v /etc/httpd
```

②通过添加 public_content_rw_t 类型标签，允许 httpd 可读写/var/www 目录及子目录。注意，该设置需要开启布尔值 all_httpd_anon_write，其操作命令如下所示。

```
# semanage fcontext -a -t public_content_rw_t "/var/www(/.*)?"
# restorecon -F -R -v /var/www/html
```

具体的文件与目录资源的安全上下文描述信息对应关系如表 10-14 所示。

表 10-14 安全上下文对应关系表

文件与目录描述	安全上下文类型标签
/var/cache	httpd_cache_t
Apache 配置文件	httpd_config_t
作为 CVS 内容的文件资源	httpd_cvs_content_t
Apache 日志文件资源	httpd_log_t
httpd 代理内容资源	httpd_squid_content_t
httpd 系统资源	httpd_sys_content_t
可读写 httpd 系统资源	httpd_sys_rw_content_t

2. SELinux

- FTP相关的SELinux安全策略

（1）布尔值

①允许 ftp 读写用户家目录中的数据，其操作命令如下所示。

```
# setsebool -P ftp_home_dir 1
```

②允许本地账号登陆 ftp 可以读写文件系统中的所有文件，其操作命令如下所示。

```
# setsebool -P allow_ftpd_full_access 1
```

③允许 ftp 连接数据库，其操作命令如下所示。

```
# setsebool -P ftpd_connect_db 1
```

④允许 ftp 共享 cifs 文件系统，其操作命令如下所示。

```
# setsebool -P allow_ftpd_use_cifs
```

⑤允许 ftp 共享 NFS 文件系统，其操作命令如下所示。

```
# setsebool -P allow_ftpd_use_nfs 1
```

2. SELinux

FTP相关的SELinux安全策略

（2）安全上下文

具体的文件与目录资源的安全上下文描述信息对应关系如表 10-15 所示。

表 10-15 安全上下文对应关系表

文件与目录描述	安全上下文类型标签
/etc/目录下的 ftp 文档	ftpd_ect_t
控制 ftp 程序仅在 ftpd_t 域下运行	ftpd_exec_t
控制 ftp 程序仅在 ftpd_initre_t 域下运行	ftpd_initre_exec_t
ftp 锁数据文件	ftpd_lock_t
ftp 在/tmp 目录下生成的临时文件	ftpd_tmp_t

2. SELinux

MySQL相关的SELinux安全策略

（1）布尔值

①允许用户连接 MySQL 服务器，其操作命令如下所示。

```
# setsebool -P allow_user_mysql_connect 1
```

②允许 mysqld 服务连接所有的端口号，其操作命令如下所示。

```
# setsebool -P mysql_connect_any 1
```

（2）安全上下文

具体的文件与目录资源的安全上下文描述信息对应关系如表 10-16 所示。

表 10-16 安全上下文对应关系表

文件与目录描述	安全上下文类型标签
mysqld 数据库文件	mysqld_db_t
存储在/etc/目录下的 mysql 文件	mysqld_etc_t
控制 mysql 程序仅在 mysqld_t 域中运行	mysqld_exec_t
控制 mysql 程序仅在 mysqld_initre_t 域中运行	mysqld_initre_exec_t
控制 mysql 程序仅在 mysqld_safe_t 域中运行	mysqld_safe_exec_t
mysql 存储在/tmp 目录下的临时文件	mysqld_tmp_t
mysql 存储在/var/run 目录下的临时文件	mysqld_var_run_t

2. SELinux

MySQL相关的SELinux安全策略

（1）布尔值

①允许用户连接 MySQL 服务器，其操作命令如下所示。

```
# setsebool -P allow_user_mysql_connect 1
```

②允许 mysqld 服务连接所有的端口号，其操作命令如下所示。

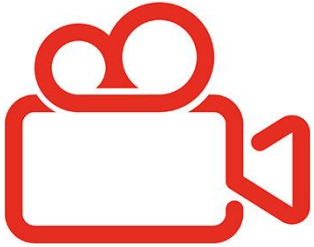
```
# setsebool -P mysql_connect_any 1
```

（2）安全上下文

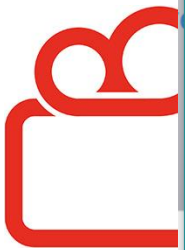
具体的文件与目录资源的安全上下文描述信息对应关系如表 10-16 所示。

表 10-16 安全上下文对应关系表

文件与目录描述	安全上下文类型标签
mysqld 数据库文件	mysqld_db_t
存储在/etc/目录下的 mysql 文件	mysqld_etc_t
控制 mysql 程序仅在 mysqld_t 域中运行	mysqld_exec_t
控制 mysql 程序仅在 mysqld_initre_t 域中运行	mysqld_initre_exec_t
控制 mysql 程序仅在 mysqld_safe_t 域中运行	mysqld_safe_exec_t
mysql 存储在/tmp 目录下的临时文件	mysqld_tmp_t
mysql 存储在/var/run 目录下的临时文件	mysqld_var_run_t



- 使用SELinux配置提升httpd安全性
  - 基于多端口发布网站的安全防护



Teach-CentOS 7 - root@Centos7Teach:/var/www/html - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach html]# ls
[root@Centos7Teach html]# systemctl stop firewalld
[root@Centos7Teach html]# systemctl start httpd
[root@Centos7Teach html]# getenforce
Enforcing
[root@Centos7Teach html]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
[root@Centos7Teach html]#
[root@Centos7Teach html]# vi /etc/httpd/
conf/           conf.modules.d/ modules/
conf.d/         logs/           run/
[root@Centos7Teach html]# vi /etc/httpd/conf
conf/           conf.d/         conf.modules.d/
[root@Centos7Teach html]# vi /etc/httpd/conf/
httpd.conf          httpd.conf.rpmsave  magic
[root@Centos7Teach html]# vi /etc/httpd/conf/httpd.conf
[root@Centos7Teach html]# systemctl restart httpd
Job for httpd.service failed because the control process exited with error code.
 See "systemctl status httpd.service" and "journalctl -xe" for details.
[root@Centos7Teach html]# systemctl status -l httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor prese
t: disabled)
   Active: failed (Result: exit-code) since Wed 2018-05-09 23:33:22 CST; 1min 12
s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 6782 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=1/FAIL
URE)
  Process: 6780 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND (code=exited, st
atus=1/FAILURE)
 Main PID: 6780 (code=exited, status=1/FAILURE)
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,27 1 会话 CAP NUM

Teach-CentOS 7 - root@Centos7Teach:/var/www/html - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor prese
t: disabled)
   Active: failed (Result: exit-code) since Wed 2018-05-09 23:33:22 CST; 1min 12
s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 6782 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=1/FAIL
URE)
  Process: 6780 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND (code=exited, st
atus=1/FAILURE)
 Main PID: 6780 (code=exited, status=1/FAILURE)

May 09 23:33:22 Centos7Teach httpd[6780]: (13)Permission denied: AH00072: make_s
ock: could not bind to address [::]:801
May 09 23:33:22 Centos7Teach httpd[6780]: (13)Permission denied: AH00072: make_s
ock: could not bind to address 0.0.0.0:801
May 09 23:33:22 Centos7Teach httpd[6780]: no listening sockets available, shutti
ng down
May 09 23:33:22 Centos7Teach httpd[6780]: AH00015: Unable to open logs
May 09 23:33:22 Centos7Teach systemd[1]: httpd.service: main process exited, cod
e=exited, status=1/FAILURE
May 09 23:33:22 Centos7Teach kill[6782]: kill: cannot find process ""
May 09 23:33:22 Centos7Teach systemd[1]: httpd.service: control process exited,
code=exited status=1
May 09 23:33:22 Centos7Teach systemd[1]: Failed to start The Apache HTTP Server.
May 09 23:33:22 Centos7Teach systemd[1]: Unit httpd.service entered failed state
.
May 09 23:33:22 Centos7Teach systemd[1]: httpd.service failed.
[root@Centos7Teach html]# semanage port -a -t http_port_t -p tcp 801
[root@Centos7Teach html]# semanage port -a -t http_port_t -p tcp 802
[root@Centos7Teach html]# systemctl restart httpd
[root@Centos7Teach html]#
[root@Centos7Teach html]# semanage port -l | grep http
http_cache_port_t              tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t              udp      3130
http_port_t                    tcp      802, 801, 80, 81, 443, 488, 8008, 8009,
8443, 9000
pegasus_http_port_t            tcp      5988
pegasus_https_port_t           tcp      5989
[root@Centos7Teach html]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,27 1 会话 CAP NUM

3.防火墙

- 防火墙是服务器安全一大重要保障系统。
- 防火墙遵循的是一种允许和阻止业务来往的网络通信安全机制，也就是提供可控的网络通信过滤服务，其主要功能如下。
  - 管理进、出网络的访问：允许运维人员定义一个中心“扼制点”来防止非法用户进入内部网络，禁止安全性较低的服务进/出网络，并抗击来自各种路线的攻击。
  - 保护网络中脆弱的服务：可过滤存在安全缺陷的网络服务来降低服务器遭受攻击的威胁。
  - 检测和报警：可方便地监视服务器的安全性，并产生告警，运维人员通过防火墙日志可以审查记录并及时响应告警，以便知道服务器是否正在遭受网络攻击。

3.防火墙

- 防火墙主要分为三类，即包过滤防火墙、应用代理防火墙以及状态检测防火墙。
  - 包过滤防火墙：
    - 包过滤防火墙是把网络层和传输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，并与预先设定的防火墙过滤规则（Filtering Rule）进行核对。一旦发现某个数据包的某个或多个部分与过滤规则匹配，则根据过滤规则进行判断该数据包是否允许通过。
    - 包过滤防火墙实现效果是较为显著的，但是却不能满足建立精细规则的要求（规则数量和防火墙性能成反比）。
    - 包过滤防火墙只能工作在网络层和传输层，并不能判断高级协议中的数据是否有害。

3.防火墙

- 防火墙主要分为三类，即包过滤防火墙、应用代理防火墙以及状态检测防火墙。
  - 应用代理防火墙：
    - 应用代理防火墙主要是通过接收来自用户的请求，调用自身的客户端模拟一个用户请求，从而连接到目标服务器，并把目标服务器返回的数据转发给用户，完成代理工作。当外界数据进入代理防火墙的客户端时，“应用协议分析”模块便根据应用层协议处理这个数据，通过预置的处理规则查询这个数据是否带有危害。
    - 应用代理防火墙不仅能根据数据层提供的信息判断数据，更能如同管理员分析服务器日志那样“看”内容辨别危害。
    - 应用代理防火墙可实现双向限制，在过滤外部网络有害数据的同时也监控内部网络的信息。

3.防火墙

- 防火墙主要分为三类，即包过滤防火墙、应用代理防火墙以及状态检测防火墙。
  - 状态检测防火墙：
    - 防火墙通过“状态检测”的模块，在不影响网络正常工作的前提下采用抽取相关数据的方法对网络通信的各个层次实行检测，并根据各种过滤规则做出安全决策。
    - 状态检测防火墙在保留了对每个数据包的头部、协议、地址、端口以及类型等信息进行分析的基础上，进一步发展了“会话过滤（Session Filtering）”功能。
    - 状态检测防火墙摆脱了传统防火墙局限于检测几个数据包头部信息的弱点，且该防火墙不必开放过多端口，进一步降低服务器因开放端口过多而带来的安全隐患。

3.防火墙

- Linux提供了一个非常优秀的防火墙工具，即Netfilter/iptables（http://www.netfilter.org）。该防火墙工具是完全免费的，并且可以在一台低配置的机器上高效运行。
  - Netfilter/iptables功能强大，使用灵活，可以对流入和流出的信息进行精细化的控制。
  - 每一个主要的Linux版本中都有不同的防火墙软件包，iptables应用程序被认为是Linux中实现包过滤功能的第4代应用程序。

3.防火墙

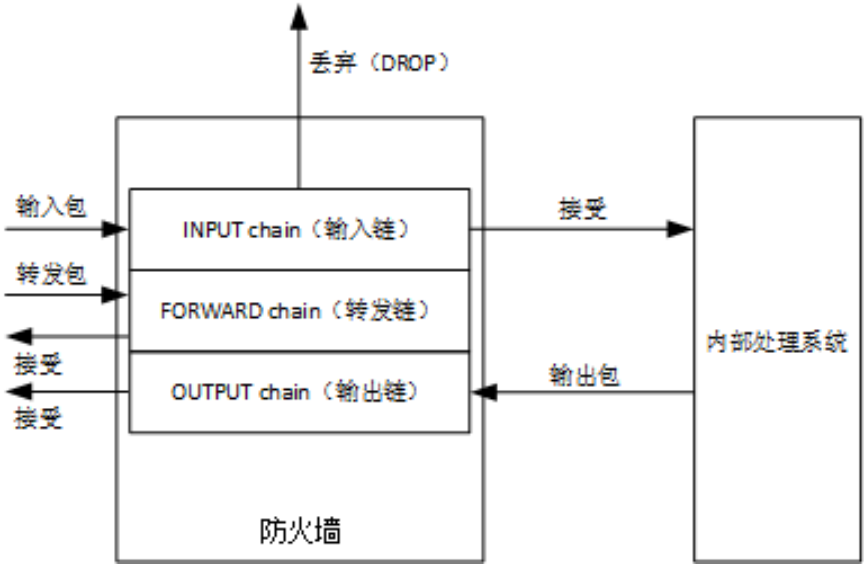
- Netfilter/iptables （IP信息包过滤系统）是一种功能强大的工具，可用于添加、编辑和删除规则。规则是在决定数据包过滤时防火墙所遵循和组成的要求，其存储在专用的数据包过滤表中，并且该表集成在Linux内核中。在过滤表中，规则被分在不同的链（chain）中。虽然Netfilter/iptables让人们觉得是个“单个实体”，但它实际上有两个组件，即Netfilter和iptables组成。
  - Netfilter组件称为“内核空间（Kernelspace）”，是内核的一部分。它由数据包过滤表组成，这些表包含内核用来控制数据包过滤处理的规则集。
  - iptables组件是一种工具，称为“用户空间（Userspace）”，它使插入、修改和删除包过滤表中的规则变得容易。通过使用用户空间可以构建自定义规则，这些规则存储在内核空间的数据包过滤表中。

3.防火墙

- 规则决定内核对来自某些源、前往某些目的地或具有某些协议类型的数据包应该如何处理。如果某个数据包与规则匹配，那么ACCEPT允许该数据包通过，DROP或REJECT来阻塞并杀死数据包。
  - 根据规则所处理的数据包的类型，可以将规则分组在链中。其中INPUT链、OUTPUT链FORWARD链这3个链是数据包过滤表中内置的默认主链。另外，还有其他可用链的类型（如PREROUTING和POSTROUTING），以及用户定义的链。
    - 如果数据包源自外界并前往系统，那么内核将其传递到内核数据包过滤表的INPUT链。
    - 如果数据包源自系统内部或系统所连接的内部网络的其他源，并且此数据包要前往另一个外部系统，那么数据包被传递到OUTPUT链。
    - 如果数据包源自外部系统并前往内部系统的数据包被传递到FORWARD链。
  - 建立规则并将其放在适当的位置之后，就可以进行数据包过滤工作了。内核空间从用户空间接管工作，当数据包到达防火墙时，内核先检查数据包的头信息，尤其是数据包的目的地，这个过程称为“路由”。

3.防火墙

- 数据包在Linux防火墙中的过滤过程如图所示。



3.防火墙

- iptables

通过使用 Netfilter/iptables 系统提供的特殊命令 iptables 建立这些规则，并将规则添加到操作系统内核空间的特定数据包过滤表内的链中，实现防火墙。添加、删除以及编辑规则的命令语法一般如下所示。

```
# iptables [选项]
```

iptables 命令的选项说明如表 10-19 所示。

表 10-19 iptables 命令选项

选项	说明
[-t tables]	规则添加的表名称
command	定义 iptables 命令要执行的操作
match	定义数据包与规则匹配所应具有的特征
target	制定与规则匹配的数据包执行什么操作

3.防火墙

- iptables：tables参数
  - [-t table]选项允许使用标准表之外的任何表，表示包含处理特定类型数据包的规则和链的数据包过滤表。有3种可用的表选项，即Filter、NAT和Mangle。该选项不是必须的，如果未指定，则Filter用作默认表。各表实现的功能如下。
  - Filter表
    - Filter表用来过滤数据包，可以在任何时候匹配包并将其过滤，根据包的内容进行DROP或ACCEPT操作。
    - Filter表主要用于数据包的过滤。

3.防火墙

- iptables：tables参数
  - [-t table]选项允许使用标准表之外的任何表，表示包含处理特定类型数据包的规则和链的数据包过滤表。有3种可用的表选项，即Filter、NAT和Mangle。该选项不是必须的，如果未指定，则Filter用作默认表。各表实现的功能如下。
  - NAT表
    - 数据包中如果包含目的IP地址，一旦内部Internet的IP地址被截获，那么内部网络资源就会被暴露并可以对其实施攻击，为了更好地提高内部网络安全性，可以采用网络地址转换技术（NAT）。
    - 防火墙中NAT表主要用于网络地址转换。

3.防火墙

- iptables：tables参数
  - [-t table]选项允许使用标准表之外的任何表，表示包含处理特定类型数据包的规则和链的数据包过滤表。有3种可用的表选项，即Filter、NAT和Mangle。该选项不是必须的，如果未指定，则Filter用作默认表。各表实现的功能如下。
  - Mangle表：
    - 主要用来修改数据包，用户可以改变不同的包及包头的内容，主要是进行TCP头部修改操作，这个表有5个内建的链，即PREROUTING、POSTROUTING、OUTPUT、INPUT和FORWARD。
      - PREROUTING：在包进入防火墙之后且路由判断之前更改数据包；
      - POSTROUTING：在所有路由判断之后更改数据包；
      - OUTPUT：在确定包的目的之前更改数据包；
      - INPUT：在包被路由到本地之后，但在用户空间的程序看到它之前更改数据包；
      - FORWARD：在确定包的转发目的地址前更改数据包

3.防火墙

- iptables：command参数
  - command是 ...tables命令要执行的操作。例... ...余规则。

表 10-20 常用命令及功能

命令名称	功能说明
-A	--append，在所选择的链末添加规则。当源地址或目的地址是以名字，而不是 IP 地址的形式出现时，并且这些名字可以解析为多个地址，则这条规则会和所有可用的地址结合
-D	--delete，从所有链中删除规则。有两种方法指定要删除的规则，一是把规则完整的写出来；二是指定规则所在链中的序号（每条链中的规则都各自从 1 被编号）
-R	--replace，在所选中的链里指定行上（每条链中的规则都各自从 1 被编号）替换规则，它的主要用处是试验不同规则。当源地址或目的地址是以名字，而不是 IP 地址的形式出现时，并且这些名字可以被解析为多个地址，则这条命令失败
-I	--insert，根据给出的规则序号向所选链中插入规则。如果序号为 1，规则会被插入链的头部，即默认序号为 1
-L	--list，显示所选链中的所有规则。如果没有指定链，则显示指定表中所有链，如果未指定任何参数，则显示默认表所有链。精确输出受其他参数的影响，如-n 和-v 等参数
-F	--flush，清空所选的链。如果没有指定链，则清空指定表中所有链，如果未指定任何参数，则清空默认表所有链
-Z	--zero，把指定链（如果未指定，则默认所有链）的所有计数器归零
-N	--new-chain，根据用户指定的名字创建新的链
-X	--delete-chain，删除指定的用户自定义链，这个链必须没有被引用。如果被引用，删除之前必须删除或者替换与之有关的规则。如果没有给出参数，这条命令将会删除默认表中所有非内建的链
-P	--policy，为链设置默认的 target（可用的是 DROP 和 ACCEPT），这个 target 称为"策略"，所以不符合规则的包被强制使用这个策略。只有内建的链才可以使用规则，但内建的链和用户自定义链都不是作为策略使用
-E	--rename-chain，对自定义的链进行重命名，原来的名字在前，新名字在后。这仅仅是改变链的名字，对整个表的结构及操作没有任何影响
-h	--help，显示帮助信息

3.防火墙

- iptables：command参数
  - command是iptables命令中的最重要组成部分，其定义iptables命令要执行的操作。例如，插入规则、将规则添加到链的末尾或删除规则。

表 10-21 部分选项及其功能

选项	可用此选项的命令	功能说明
-v，--verbose	--list、--apend、--insert、--delete 和 replace	这个选项使输出详细化，常与--list 连用。连用时，输出包括网络接口的地址、规则的选项、TOS 掩码、字节和包计数器，其中计数器是以 K、M 及 G 为单位的。如果-v 和--apend、--insert、--delete 或—replace 连用，iptables 会输出详细的信息告诉规则是如何被解释的，以及是否正确地插入等
-x，--exact	--list	使--list 输出中的计数器显示准确的数值，注意，此选项只能和—list 连用
-n，--numeric	--list	使输出中的 IP 地址和端口以数值的形式显示，而不是默认的名字，比如主机名、网络名及程序名等。注意，此选项也只能和--list 连用
--line-numbers	--list	只能和—list 连用的选项，作用是显示每条规则在相应链中的序号，这样可以知道序号
-c，--set-counters	--insert、--append 和 replace	在创建或更改规则时设置计数器
--modprobe	所有	此选项告诉 iptables 探测并装载要使用的模块。这是非常有用的一个选项，万一 modprobe 命令不在搜索路径中就要用到它。有了这个选项，在装载模块时即使有一个需要用到的模块为装载上，iptables 也知道如何搜索

3.防火墙

- iptables：match参数
  - iptables命令的可选match部分指定数据包与规则匹配所应具有的特征（如源地址和目的地址及协议），具体归为5类如下。
    - generic matches：通用匹配，适用于所有的规则；
    - TCP matches：TCP匹配，只能用于匹配TCP包；
    - UDP matches：UDP匹配，只能用于匹配UDP包；
    - ICMP matches：ICMP匹配，只能用于匹配ICMP包；
    - status matches：状态匹配，根据状态进行匹配，如所有者和访问的频率限制等。

3.防火墙

- iptables：target参数
  - 目标是由规则制定的操作，决定与规则匹配的数据包应该执行什么操作。
  - 除了允许用户定义的目标之外，还有许多可用的目标选项用于建立高级规则的目标，如LOG（记录日志）、REDIRECT（数据包重定向）、MARK（标记数据包）、MIRROR（镜像数据包）和MASQUERADE（封装数据包）等。

表 10-23 常用目标及其说明

参数	说明
ACCEPT	接受数据包，当数据包与具有 ACCEPT 目标的规则完全匹配时会被接受（允许前往目的地），并且将停止遍历链（虽然该数据包可能遍历另一个表中的其他链，并且有可能在那里被丢弃），该模板被指定为-j ACCEPT
DROP	丢弃数据包，当数据包与具有 DROP 目标的规则完全匹配时会阻塞该数据包，并且不对它做进一步处理，该目标被指定为-j DROP
REJECT	阻拦数据包，该目标的工作方式与 DROP 目标相同，但比 DROP 好。和 DROP 不同的是 REJECT 会将错误消息发回给数据包的发送方，该目标被指定为-j REJECT
RETURN	停止过滤程序，在规则中设置 RETURN 目标让与该规则匹配的数据包停止遍历包含该规则的链，如果链是 INPUT 之类的主链，则使用该链的默认策略处理数据包，它被指定为-j RETURN

3.防火墙

- iptables状态配置：
  - 安装：yum install iptables iptables-services
  - 启动：systemctl start iptables
  - 关闭：systemctl stop iptables
  - 开机自启动：systemctl enable iptables
  - 禁止自启动：systemctl disable iptables
  - 状态：systemctl status iptables

3.防火墙

3.4 iptables配置

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# systemctl is-active firewalld
active
[root@Centos7Teach ~]# systemctl is-enabled firewalld
enabled
[root@Centos7Teach ~]# iptables --version
iptables v1.4.21
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# systemctl stop firewalld
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# systemctl disable firewalld
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# systemctl is-active firewalld
unknown
[root@Centos7Teach ~]# systemctl is-enabled firewalld
disabled
[root@Centos7Teach ~]# systemctl mask firewalld
Created symlink from /etc/systemd/system/firewalld.service to /dev/null.
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# yum install -y iptables-services
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.cqu.edu.cn
 * epel: mirrors.tongji.edu.cn
 * extras: mirrors.cqu.edu.cn
 * updates: mirrors.cqu.edu.cn
Resolving Dependencies
--> Running transaction check
---> Package iptables-services.x86_64 0:1.4.21-18.3.el7_4 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch        Version                   Repository    Size
================================================================================
Installing:
 iptables-services      x86_64      1.4.21-18.3.el7_4         updates       51 k
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,24 1 会话 CAP NUM

3.防火墙

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# systemctl start iptables
[root@Centos7Teach ~]# systemctl enable iptables
Created symlink from /etc/systemd/system/basic.target.wants/iptables.service to
/usr/lib/systemd/system/iptables.service.
[root@Centos7Teach ~]# systemctl is-active iptables
active
[root@Centos7Teach ~]# systemctl is-enabled iptables
enabled
[root@Centos7Teach ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:
ssh
REJECT     all  --  anywhere             anywhere             reject-with icmp-h
ost-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere             reject-with icmp-h
ost-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 29,24 1 会话 CAP NUM

3.防火墙

- iptables规则管理：端口配置
  - 开启需要的端口，如配置TCP协议的22端口允许进出系统。

    # iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT

    # iptables -t filter -A OUTPUT -p tcp --sport 22 -j ACCEPT
  - 关闭不安全的端口，如配置不允许通过TCP协议的445端口进出系统。

    # iptables -t filter -A INPUT -p tcp --dport 445 -j DROP

    # iptables -t filter -A OUTPUT -p tcp --sport 445 -j DROP
  - 配置服务端口，如配置允许通过HTTP访问系统的80端口。

    # iptables -t filter -A INPUT -p tcp --dport http -j DROP

3.防火墙

- iptables规则管理：IP地址配置
  - 拒绝某单一IP地址，如拒绝某一单独IP地址访问系统，且系统拒绝访问该IP地址。

    # iptables -t filter -A INPUT -s xxx.xxx.xxx.xxx -j DROP

    # iptables -t filter -A OUTPUT -d xxx.xxx.xxx.xxx -j DROP
  - 拒绝某IP地址段，如拒绝某IP地址段（172.16.124.0/24）中任一地址访问系统，且系统拒绝访问该IP地址段中任一IP地址。

    # iptables -t filter -A INPUT -s xxx.xxx.xxx.xxx/x -j DROP

    # iptables -t filter -A OUTPUT -d xxx.xxx.xxx.xxx/x -j DROP

3.防火墙

- iptables规则管理：IP地址与端口结合
  - 拒绝某IP地址访问某端口，如拒绝某一单独IP地址访问系统的22端口（TCP协议）。

    # iptables -t filter -A INPUT -s xxx.xxx.xxx.xxx -p tcp --dport 22 -j DROP
  - 允许某段IP地址访问系统的服务端口，如允许某段IP地址访问系统的HTTP服务端口。

    # iptables -t filter -A INPUT -s xxx.xxx.xxx.xxx/x -p tcp --dport http -j ACCEPT

3.防火墙

- iptables规则管理：网络协议配置
  - 配置拒绝ICMP协议，如配置拒绝网络中通过PING方式发现系统地址。

```
# iptables -t filter -A INPUT -p icmp -j DROP
```

3.防火墙

- iptables规则管理：网卡接口配置
  - iptables防火墙可单独为某个网卡接口设定不同的策略规则，如不允许任何主机通过防火墙本机的eth0网卡访问系统的80端口。

```
# iptables -t filter -A INPUT -i eth0 -p tcp --dport 80 -j DROP
```

3.防火墙

- iptables规则管理：MAC地址配置
  - 拒绝某MAC地址主机的所有通信请求访问。

    # iptables -t filter -A INPUT -m mac -mac-source XX:XX:XX:XX:XX:XX -j DROP
  - 拒绝网络中某一固定IP地址且固定MAC地址的主机访问系统任意端口。

    # iptables -t filter -A INPUT -s xxx.xxx.xxx.xxx/x -m mac -mac-source XX:XX:XX:XX:XX:XX -j DROP
  - 允许网络中某一固定IP地址且固定MAC地址的主机访问系统的22号端口。

    # iptables -t filter -A INPUT -p tcp --dport 22 -s xxx.xxx.xxx.xxx/x -m mac -mac-source XX:XX:XX:XX:XX:XX -j ACCEPT

3.防火墙

- iptables规则删除：
  - 根据防火墙内容删除
  - 删除已配置的“禁止网络段IP地址进入系统”防火墙规则。

    # iptables -t filter -D INPUT -s xxx.xxx.xxx.xxx/x -j DROP

  - 根据防火墙规则顺序删除
  - iptables防火墙可根据某条链中的规则顺序进行删除，如删除filter表中INPUT链的第一条规则。

    # iptables -t filter -D INPUT 1

3.防火墙

- iptables规则修改：
  - 替换规则
  - 如filter表中INPUT链的第二条规则为“拒绝某个地址访问系统”，现将该规则替换为“拒绝除某个地址外所有主机地址访问”，其配置命令如下。

    # iptables -t filter -R INPUT 2 ! -s xxx.xxx.xxx.xxx -j REJECT

  - 修改规则
  - 如filter表中INPUT链的默认规则为“拒绝接收所有数据包”，现将该默认规则修改为“允许接收所有数据包”，其配置命令如下。

    # iptables -t filter -P INPUT ACCEPT

3.防火墙

- iptables记录规则触发的日志：
  - 在网络数据包传输过程中，需要将特殊IP地址在访问某个端口时，将其发送的所有数据包信息记录到messages日志中，以便于后续的网络分析和日志追溯。
  - 如将某个IP地址主机发送给防火墙本机“22端口”的所有数据包信息记录到messages日志。

```
# iptables -t filter -A INPUT -s xxx.xxx.xxx.xxx -p tcp --dport 22 -j LOG
```

3.防火墙

- iptables默认规则：
  - iptables防火墙在安装后，可对每条“防火墙链”设置相应的默认规则。
  - 限制所有默认输入链为丢弃规则

    # iptables -p INPUT DROP

  - 限制所有默认转发链为丢弃规则

    # iptables -p FORWARD DROP

  - 限制所有默认输出链为丢弃规则

    # iptables -p OUTPUT DROP

3.防火墙

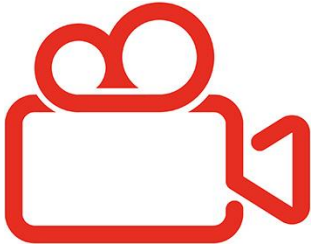
- iptables防DDoS攻击：
  - 为避免服务器中业务造成DDOS攻击后，仍被持续连接访问，可在iptables防火墙上进行访问连接数限制。
  - 如外界访问TCP 80端口，当总连接数超过100时，启动连接限制，限制每分钟最大连接数为25个。

```
# iptables -t filter -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```

3.防火墙

- iptables防SYN Flood攻击：
  - 防火墙为允许普通用户正常通过，又阻止攻击者访问网络，可以使用SYN标识来阻止那些未经授权的访问。
  - 为防止SYN Flood攻击，可对SYN连接进行连接限制。

```
# iptables -t filter -A INPUT -p tcp --syn -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```



- 基于iptables实现对httpd的安全防护
  - 配置端口80能够通过互联网访问
  - 配置端口8000仅允许内部访问
  - 配置服务器仅允许指定IP地址进行SSH管理
  - 配置网站防范DDoS攻击
  - 配置SSH操作进行日志记录

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# iptables -A INPUT -p tcp --dport 80 -m limit --limit 100/minute --limit-burst
  1000 -j ACCEPT
[root@Centos7Teach ~]# iptables -A INPUT -p tcp --dport 8000 -s 10.0.0.0/8 -j ACCEPT
[root@Centos7Teach ~]# iptables -A INPUT -p tcp --dport 8000 -s 192.168.0.0/16 -j ACCEPT
[root@Centos7Teach ~]# iptables -A INPUT -p tcp --dport 8000 -s 172.16.0.0/16 -j ACCEPT
[root@Centos7Teach ~]# iptables -A INPUT -p tcp --dport 22 -s 211.69.32.121 -j ACCEPT
[root@Centos7Teach ~]# iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "fw-22-port" --log-le
vel info
[root@Centos7Teach ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http limit: avg 100/min burst
1000
ACCEPT     tcp  --  10.0.0.0/8           anywhere             tcp dpt:irdmi
ACCEPT     tcp  --  192.168.0.0/16       anywhere             tcp dpt:irdmi
ACCEPT     tcp  --  172.16.0.0/16        anywhere             tcp dpt:irdmi
ACCEPT     tcp  --  211.69.32.121        anywhere             tcp dpt:ssh
LOG        tcp  --  anywhere             anywhere             tcp dpt:ssh LOG level info prefix "fw-
22-port"

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@Centos7Teach ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:80 limit: avg 100/min burst 10
00
ACCEPT     tcp  --  10.0.0.0/8           0.0.0.0/0            tcp dpt:8000
ACCEPT     tcp  --  192.168.0.0/16       0.0.0.0/0            tcp dpt:8000
ACCEPT     tcp  --  172.16.0.0/16        0.0.0.0/0            tcp dpt:8000
ACCEPT     tcp  --  211.69.32.121        0.0.0.0/0            tcp dpt:22
LOG        tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:22 LOG flags 0 level 6 prefix
"fw-22-port"

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 100x43 43,24 1 会话 CAP NUM

4.系统安全检测

- Nmap是一个开源免费的网络发现工具，通过该工具能够找出网络上在线主机，并测试主机上哪些端口处于监听状态，接着通过端口确定主机上运行的应用程序类型与版本信息，最后还能利用该工具侦测出操作系统的类型和版本。
- Nmap是一个功能非常强大的网络探测工具，同时它也成为网络黑客的最爱，因为Nmap所实现的这些功能正是黑客入侵网络的一个基本过程。站在安全运维角度上，只有了解黑客入侵的基本方式和过程，才能有目的、有针对性地进行服务器的安全防护。

4.系统安全检测

- Nmap是Network Mapper的缩写，由Fyodor在1997年创建，现在已经成为安全检测工具之一。
- Nmap作为一个流行的安全工具，它的主要特点有以下内容。
  - 操作灵活。Nmap支持10多种扫描方式，并支持多种目标对象扫描；
  - 支持主流操作系统。Nmap支持Windows、Linux、BSD、Solaris、AIX、Mac OS等多种平台，可移植性强；
  - 使用简单。Nmap安装与使用都较为简单，基本用法都能满足一般使用需求；
  - 自由软件。Nmap是在GPL协议下发布的，在GPL license的范围内可自由使用。

NMAP.ORG

Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

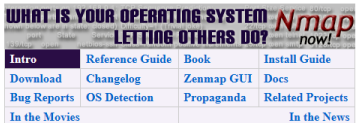
Security Lists
- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools
- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News
Advertising
About/Contact

Site Search

Sponsors:



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

News

- 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.
- **Acclaimed**: Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series. Visit the press page for further details.
- **Popular**: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

Communication

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (8 posts in 2016), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join more than 128,000 current subscribers by submitting your email address here:

Subscribe to Nmap-hackers

(or subscribe with custom options from the Nmap-hackers list info page)

We also have a development list for more hardcore members (especially programmers) who are interested in helping the project by helping with coding, testing, feature ideas, etc. New (test/beta) versions of Nmap are sometimes released here prior to general availability for QA purposes. You can subscribe at the Nmap-dev list info page.

4.系统安

全审计工具-Nmap

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# yum install nmap
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.sjtu.edu.cn
 * epel: mirrors.tongji.edu.cn
 * extras: ftp.sjtu.edu.cn
 * updates: ftp.sjtu.edu.cn
Resolving Dependencies
--> Running transaction check
---> Package nmap.x86_64 2:6.40-7.el7 will be installed
--> Processing Dependency: nmap-ncat = 2:6.40-7.el7 for package: 2:nmap-6.40-7.e
l7.x86_64
--> Running transaction check
---> Package nmap-ncat.x86_64 2:6.40-7.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package            Arch            Version                 Repository      Size
================================================================================
Installing:
 nmap               x86_64          2:6.40-7.el7            base           4.0 M
Installing for dependencies:
 nmap-ncat          x86_64          2:6.40-7.el7            base           201 k

Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 4.2 M
Installed size: 17 M
Is this ok [y/d/N]:
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 33,21 1 会话 CAP NUM

4.系统安全审计工具-Nmap

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# nmap -sn 10.10.3.201-220

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 01:57 CST
Nmap scan report for 10.10.3.201
Host is up (0.00082s latency).
MAC Address: 00:50:56:AF:5D:AF (VMware)
Nmap scan report for 10.10.3.207
Host is up (0.0013s latency).
MAC Address: 00:50:56:AF:05:31 (VMware)
Nmap scan report for 10.10.3.208
Host is up (0.0011s latency).
MAC Address: 00:50:56:AF:FA:2A (VMware)
Nmap scan report for 10.10.3.209
Host is up (0.0012s latency).
MAC Address: 00:50:56:AF:17:52 (VMware)
Nmap scan report for 10.10.3.210
Host is up (0.0011s latency).
MAC Address: 00:50:56:AF:21:C3 (VMware)
Nmap scan report for 10.10.3.212
Host is up (0.00086s latency).
MAC Address: 00:50:56:AF:33:E3 (VMware)
Nmap scan report for 10.10.3.214
Host is up (0.00037s latency).
MAC Address: 00:50:56:AF:60:CC (VMware)
Nmap scan report for 10.10.3.220
Host is up (0.00079s latency).
MAC Address: 00:50:56:AF:B8:DB (VMware)
Nmap scan report for 10.10.3.213
Host is up.
Nmap done: 20 IP addresses (9 hosts up) scanned in 0.25 seconds
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 31,24 1 会话 CAP NUM

4.系统安

全审计工具-Nmap

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# nmap -Pn 10.10.3.214

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 01:58 CST
Nmap scan report for 10.10.3.214
Host is up (0.000091s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:50:56:AF:60:CC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
[root@Centos7Teach ~]# nmap -Pn 10.10.3.212

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 01:59 CST
Nmap scan report for 10.10.3.212
Host is up (0.00057s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:50:56:AF:33:E3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 27,24 1 会话 CAP NUM

4.系统安

全审计工具-Nmap

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7 | 2 Teach-CentOS 7

```
[root@Centos7Teach ~]# nmap -sU 211.69.32.50

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 02:18 CST

[root@Centos7Teach ~]# nmap -sU -F 211.69.32.50

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 02:22 CST
Nmap scan report for 211.69.32.50
Host is up (0.00042s latency).
Not shown: 97 closed ports
PORT    STATE         SERVICE
111/udp open          rpcbind
161/udp open          snmp
631/udp open|filtered ipp

Nmap done: 1 IP address (1 host up) scanned in 98.51 seconds
[root@Centos7Teach ~]# nmap -sS -F 211.69.32.50

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 02:29 CST
Nmap scan report for 211.69.32.50
Host is up (0.00020s latency).
Not shown: 96 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 31,24 2 会话 CAP NUM

4.系统安

全审计工具-Nmap

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7 2 Teach-CentOS 7

```
[root@Centos7Teach ~]# nmap -sV 10.10.3.214

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 02:12 CST
Nmap scan report for 10.10.3.214
Host is up (0.000065s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servi
cefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=5/10%Time=5AF33A24%P=x86_64-redhat-linux-gnu%r(
SF:NULL,2A,"SSH-2\.0-OpenSSH_7\.5p1\x20Ubuntu-10ubuntu0\ 1\r\n");
MAC Address: 00:50:56:AF:60:CC (VMware)

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.29 seconds
[root@Centos7Teach ~]# nmap -sV 211.69.32.50

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 02:13 CST
Nmap scan report for 211.69.32.50
Host is up (0.00020s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3 (protocol 2.0)
80/tcp   open  http    Apache httpd
111/tcp  open  rpcbind 2-4 (RPC #100000)
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 34,24 2 会话 CAP NUM

4.系统安

全审计工具-Nmap

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7 | 2 Teach-CentOS 7

```
[root@Centos7Teach ~]# nmap -O --osscan-guess 211.69.32.50

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 02:16 CST
Nmap scan report for 211.69.32.50
Host is up (0.00030s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
8080/tcp open  http-proxy
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.9
Network Distance: 3 hops

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
[root@Centos7Teach ~]# nmap -O --osscan-guess 211.69.32.8

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-10 02:16 CST
Nmap scan report for 211.69.32.8
Host is up (0.00034s latency).
All 1000 scanned ports on 211.69.32.8 are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.89 seconds
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

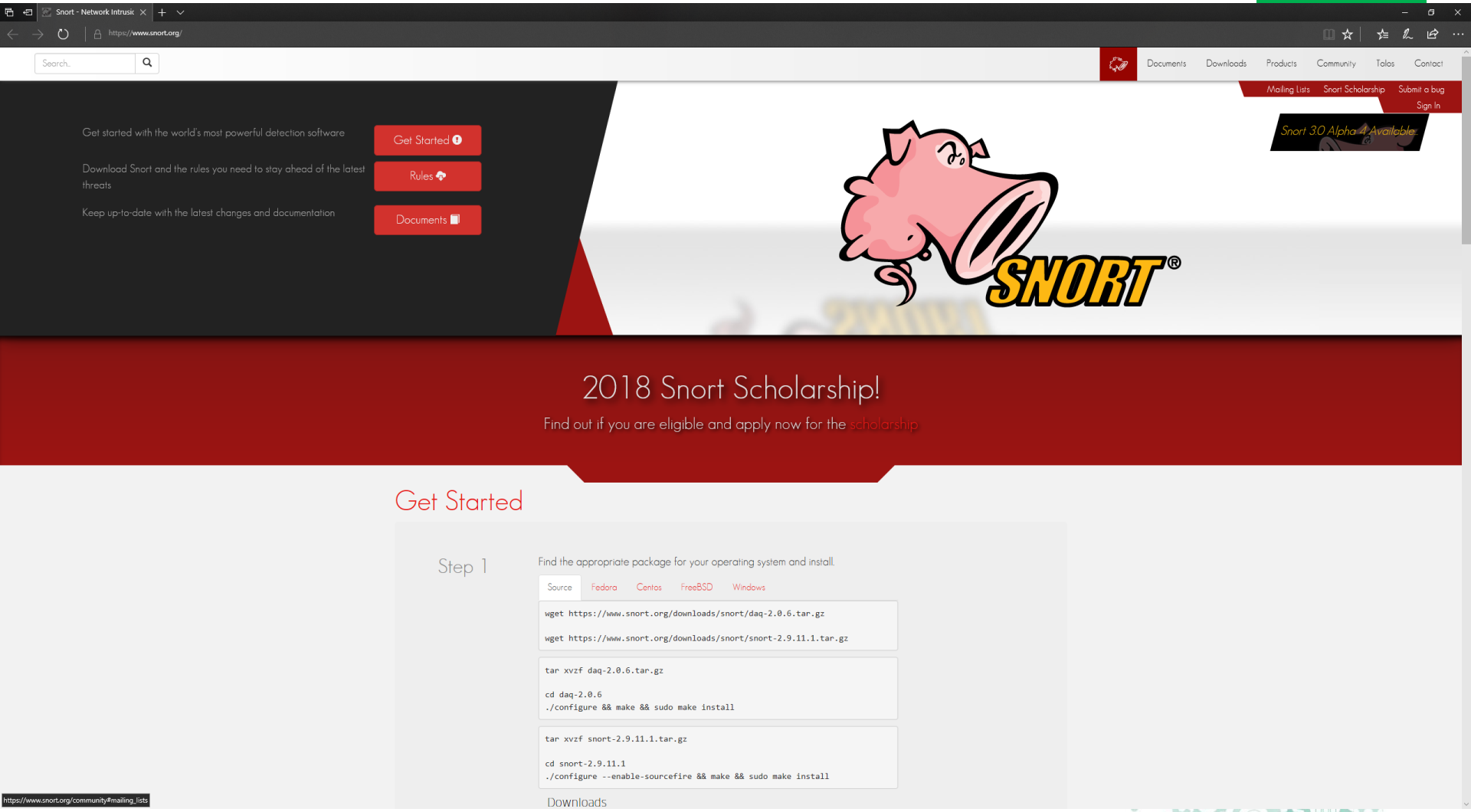
ssh://root@211.69.35.213:22 SSH2 xterm 80x40 32,24 2 会话 CAP NUM

4.系统安全检测

- Snort是一个非常优秀的入侵检测软件包，它集成了一流的技术和开源的可配置性。
- Snort实际上有几个不同的操作模式，包括嗅探器模式、数据包记录模式、入侵检测模式和内联模式，本节将介绍它的入侵检测模式。
- 当处于入侵检测模式下时，Snort通过使用其定义的许多的异常流量规则来工作，这些规则中的大部分都是通过Sourcefire（Snort的制造器）预先定义的，必要时可以自行编写规则。

4.系统安全检测

- Snort是基于事件的检测和报告进行工作的。在Snort中可通过事件处理程序对事件的报告机制进行配置，同时事件处理程序的配置也是基于阈值设置。Snort的高可配置性和阈值设置可以防止日志记录数和警报信息造成数据泛滥。
- 通常情况下希望在特定的Snort规则被触发时以某种方式通知管理员。Snort使用的输出模块可以被配置为输出到不同的位置。
  - 一个最常用的输出模块是alert_syslog模块，该模块将发送警告到本地的系统日志（syslog）中；
  - 另一个输出模块是数据库输出模块，该模块使得Snort将报警信息发送到一个SQL数据库中；
  - 除上述两种输出模块外，还有其他输出模块，关于模块的更多信息可以在Snort的文档中找到。


Snort - Network Intrusic
https://www.snort.org/
Search..
Documents
Downloads
Products
Community
Talos
Contact
Mailing Lists
Snort Scholarship
Submit a bug
Sign In
Snort 3.0 Alpha 4 Available!
Get started with the world's most powerful detection software
Get Started
Download Snort and the rules you need to stay ahead of the latest threats
Rules
Keep up-to-date with the latest changes and documentation
Documents
SNORT®
2018 Snort Scholarship!
Find out if you are eligible and apply now for the scholarship
Get Started
Step 1
Find the appropriate package for your operating system and install.
Source
Fedora
Centos
FreeBSD
Windows
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
wget https://www.snort.org/downloads/snort/snort-2.9.11.1.tar.gz
tar xvzf daq-2.0.6.tar.gz
cd daq-2.0.6
./configure && make && sudo make install
tar xvzf snort-2.9.11.1.tar.gz
cd snort-2.9.11.1
./configure --enable-sourcefire && make && sudo make install
Downloads
https://www.snort.org/community#mailing_lists

4.系统安

检测工具：Snort

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7 | 2 Teach-CentOS 7

```
[root@Centos7Teach ~]# yum install https://www.snort.org/downloads/snort/daq-2.0
.6-1.centos7.x86_64.rpm
Loaded plugins: fastestmirror
daq-2.0.6-1.centos7.x86_64.rpm                             | 147 kB     00:02
Examining /var/tmp/yum-root-Jz8jq3/daq-2.0.6-1.centos7.x86_64.rpm: daq-2.0.6-1.x
86_64
Marking /var/tmp/yum-root-Jz8jq3/daq-2.0.6-1.centos7.x86_64.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package daq.x86_64 0:2.0.6-1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package    Arch         Version         Repository                          Size
================================================================================
Installing:
 daq        x86_64       2.0.6-1         /daq-2.0.6-1.centos7.x86_64        649 k

Transaction Summary
================================================================================
Install  1 Package

Total size: 649 k
Installed size: 649 k
Is this ok [y/d/N]: _
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 27,21 2 会话 CAP NUM

4.系统安全检测

- last
  - 可用于查看系统的成功登录、关机、重启等情况。
    - 其本质就是将/var/log/wtmp文件格式化输出。
  - 命令格式：last [-adRx][-f][-n][帐号名称...][终端机编号...]
    - 参数说明：

-a 把从何处登入系统的主机名称或IP地址，显示在最后一行。

-d 将IP地址转换成主机名称。

-f <记录文件> 指定记录文件，默认是显示/var/log目录下的wtmp文件的记录，但/var/log目录下得btmp能显示的内容更丰富，可以显示远程登录，例如ssh登录 ，包括失败的登录请求。

-n <显示列数>或-<显示列数> 设置列出名单的显示列数。

-R 不显示登入系统的主机名称或IP地址。

-x 显示系统关机，重新开机，以及执行等级的改变等信息。

-I 显示特定ip登录的情况

-t 显示YYYYMMDDHHMMSS之前的信息

4.系统安

侵检测工具：last

Teach-CentOS 7 - root@Centos7Teach:/ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach /]# last -n 10
root     pts/1        10.10.0.1        Thu May 10 20:18   still logged in
root     pts/0        10.10.3.212      Thu May 10 11:48   still logged in
root     pts/2        10.10.0.1        Thu May 10 02:29 - 02:29  (00:00)
root     pts/2        10.10.0.1        Thu May 10 02:15 - 02:15  (00:00)
root     pts/2        10.10.0.1        Thu May 10 02:14 - 02:15  (00:00)
root     pts/1        10.10.0.1        Thu May 10 02:03 - 02:31  (00:27)
root     pts/0        10.10.0.1        Thu May 10 01:01 - 02:31  (01:29)
reboot   system boot  3.10.0-693.21.1. Thu May 10 00:59 - 22:29  (21:29)
root     pts/0        10.10.0.1        Wed May  9 22:30 - down   (02:29)
root     pts/0        10.10.0.1        Wed May  9 17:25 - 18:30  (01:05)

wtmp begins Sun Feb 25 22:00:53 2018
[root@Centos7Teach /]# last -n 10 -x reboot
reboot   system boot  3.10.0-693.21.1. Thu May 10 00:59 - 22:29  (21:30)
reboot   system boot  3.10.0-693.21.1. Sun May  6 22:57 - 00:59 (3+02:01)
reboot   system boot  3.10.0-693.21.1. Sun May  6 22:56 - 00:59 (3+02:02)
reboot   system boot  3.10.0-693.21.1. Wed May  2 17:28 - 22:56 (4+05:28)
reboot   system boot  3.10.0-693.21.1. Tue Apr 24 09:30 - 17:29 (8+07:58)
reboot   system boot  3.10.0-693.17.1. Wed Mar 14 11:27 - 09:33 (40+22:05)
reboot   system boot  3.10.0-693.17.1. Wed Mar 14 11:22 - 13:17 (-244+-22:-5
reboot   system boot  3.10.0-693.17.1. Wed Mar 14 11:04 - 13:17 (-244+-21:-4
reboot   system boot  3.10.0-693.17.1. Wed Mar 14 10:54 - 11:03  (00:09)
reboot   system boot  3.10.0-693.17.1. Wed Mar 14 10:49 - 10:53  (00:04)

wtmp begins Sun Feb 25 22:00:53 2018
[root@Centos7Teach /]# last -n 10 -x reboot -i 10.10.3.1
reboot   system boot  0.0.0.0          Thu May 10 00:59 - 22:30  (21:30)
reboot   system boot  0.0.0.0          Sun May  6 22:57 - 00:59 (3+02:01)
reboot   system boot  0.0.0.0          Sun May  6 22:56 - 00:59 (3+02:02)
reboot   system boot  0.0.0.0          Wed May  2 17:28 - 22:56 (4+05:28)
reboot   system boot  0.0.0.0          Tue Apr 24 09:30 - 17:29 (8+07:58)
reboot   system boot  0.0.0.0          Wed Mar 14 11:27 - 09:33 (40+22:05)
reboot   system boot  0.0.0.0          Wed Mar 14 11:22 - 13:17 (-244+-22:-5
reboot   system boot  0.0.0.0          Wed Mar 14 11:04 - 13:17 (-244+-21:-4
reboot   system boot  0.0.0.0          Wed Mar 14 10:54 - 11:03  (00:09)
reboot   system boot  0.0.0.0          Wed Mar 14 10:49 - 10:53  (00:04)

wtmp begins Sun Feb 25 22:00:53 2018
[root@Centos7Teach /]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,24 1 会话 CAP NUM

4.系统安

侵检测工具：last

Teach-CentOS 7 - root@Centos7Teach:/ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach /]# last -f /var/log/messages | head -10
0x00 PRE 0.10.0.1 DST DF PROTO=TCP SPT Wed Oct 29 09:34    gone - no logout
33:47 Ce 4600 RES=0x0 -portIN=ens32 OU Mon Oct  3 23:24    gone - no logout
10.0.1 D 6:7f:00:22:9 S=0x00 PREC=0x00 Sat May  8 21:34    gone - no logout
53 RES=0  PROTO=TCP S 2:33:47 Centos7T Tue Dec 15 06:06    gone - no logout
f:00:22: rtIN=ens32 O .10.0.1 DST=10.1 Thu Sep  5 09:55    gone - no logout
F PROTO= TOS=0x00 PRE DOW=155 RES=0x00 Wed Aug  7 06:01    gone - no logout
-portIN=  22:33:46 Ce af:76:7f:00:22:9 Mon Mar  4 11:23    gone - no logout
S=0x00 P =10.10.0.1 D  DF PROTO=TCP SP Wed Mar 22 01:09    gone - no logout
10 22:33 WINDOW=155 R  fw-22-portIN=en Sun Jan  2 16:54    gone - no logout
:00 SRC= :50:56:af:76 3 LEN=40 TOS=0x0 Mon Oct  9 04:10    gone - no logout
[root@Centos7Teach /]#
[root@Centos7Teach /]# last -n 10 -t 20180510120000
root     pts/0        10.10.3.212      Thu May 10 11:48   still logged in
root     pts/2        10.10.0.1        Thu May 10 02:29 - 02:29  (00:00)
root     pts/2        10.10.0.1        Thu May 10 02:15 - 02:15  (00:00)
root     pts/2        10.10.0.1        Thu May 10 02:14 - 02:15  (00:00)
root     pts/1        10.10.0.1        Thu May 10 02:03 - 02:31  (00:27)
root     pts/0        10.10.0.1        Thu May 10 01:01 - 02:31  (01:29)
reboot   system boot  3.10.0-693.21.1. Thu May 10 00:59 - 22:34  (21:35)
root     pts/0        10.10.0.1        Wed May  9 22:30 - down   (02:29)
root     pts/0        10.10.0.1        Wed May  9 17:25 - 18:30  (01:05)
root     pts/0        10.10.0.1        Tue May  8 22:21 - 23:24  (01:03)

wtmp begins Sun Feb 25 22:00:53 2018
[root@Centos7Teach /]#
[root@Centos7Teach /]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 27,24 1 会话 CAP NUM

4.系统安全检测

- lastb
  - 用于查看登录失败的情况。
    - 其本质就是将/var/log/btmp文件格式化输出。
  - 命令格式：lastb [-adRx][-f][-n <显示列数>][帐号名称...][终端机编号...]
    - 参数说明：

-a 把从何处登入系统的主机名称或IP地址显示在最后一行。
-d 将IP地址转换成主机名称。
-f<记录文件> 指定记录文件。
-n<显示列数>或-<显示列数> 设置列出名单的显示列数。
-R 不显示登入系统的主机名称或IP地址。
-x 显示系统关机，重新开机，以及执行等级的改变等信息。

4.系统安

侵检测工具：lastb

Teach-CentOS 7 - root@Centos7Teach:/ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach /]# lastb -n 10
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)

btmp begins Tue May  1 03:12:02 2018
[root@Centos7Teach /]# lastb -n 10 -d
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)
root     ssh:notty    10.10.0.1        Thu May 10 22:40 - 22:40  (00:00)

btmp begins Tue May  1 03:12:02 2018
[root@Centos7Teach /]# lastb root | awk '{print $3}' | sort | uniq -c | sort -nr
 303554 10.10.0.1
      1 Tue
      1 10.10.1.5
      1
[root@Centos7Teach /]#
[root@Centos7Teach /]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 33,24 1 会话 CAP NUM

4.系统安全检测

- lastlog
  - 用于查看用户上一次的登录情况。
    - 其本质就是将/var/log/lastlog文件格式化输出。
  - 命令格式：lastlog [-bChRStu]
    - 参数说明：

```
-b, --before DAYS        print only lastlog records older than DAYS
-C, --clear              clear lastlog record of an user (usable only with -u)
-h, --help               display this help message and exit
-R, --root CHROOT_DIR                directory to chroot into
-S, --set                set lastlog record to current time (usable only with -u)
-t, --time DAYS          print only lastlog records more recent than DAYS
-u, --user LOGIN         print lastlog record of the specified LOGIN
```

4.系统安

检测工具：lastlog

Teach-CentOS 7 - root@Centos7Teach:/ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach /]# lastlog -u root
Username         Port     From             Latest
root             pts/1    10.10.0.1        Thu May 10 20:18:29 +0800 2018
[root@Centos7Teach /]# lastlog -t 20180507120000
Username         Port     From             Latest
root             pts/1    10.10.0.1        Thu May 10 20:18:29 +0800 2018
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
shutdown                                   **Never logged in**
halt                                       **Never logged in**
mail                                       **Never logged in**
operator                                   **Never logged in**
games                                      **Never logged in**
ftp                                        **Never logged in**
nobody                                     **Never logged in**
systemd-network                            **Never logged in**
dbus                                       **Never logged in**
polkitd                                    **Never logged in**
postfix                                    **Never logged in**
sshd                                       **Never logged in**
rpc                                        **Never logged in**
arpwatch                                   **Never logged in**
tcpdump                                    **Never logged in**
apache                                     **Never logged in**
mysql                                      **Never logged in**
webalizer                                  **Never logged in**
rpcuser                                    **Never logged in**
[root@Centos7Teach /]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 31,24 1 会话 CAP NUM

4.系统安全检测

- history
  - 用于显示指定数目的指令命令，读取历史命令文件中的目录到历史命令缓冲区和将历史命令缓冲区中的目录写入命令文件。
    - 该命令单独使用时，仅显示历史命令，在命令行中，可以使用符号!执行指定序号的历史命令。例如，要执行第2个历史命令，则输入!2。
  - 命令格式：history [选项] [参数]
    - 参数说明：

-c	清空当前历史命令；
-a	将历史命令缓冲区中命令写入历史命令文件中
-r	将历史命令文件中的命令读入当前历史命令缓冲区
-w	将当前历史命令缓冲区命令写入历史命令文件中

4.系统安

检测工具：history

Teach-CentOS 7 - root@Centos7Teach:/ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach /]# history 10
 1129  lastlog -t 20180507120000
 1130  clear
 1131  history 10
 1132  history | awk '{print $3}' | sort | uniq -c | sort -nr
 1133  clear
 1134  history | awk '{print $3}' | sort | uniq -c | sort -nr | head 10
 1135  history | awk '{print $3}' | sort | uniq -c | sort -nr | head -n 10
 1136  history | awk '{print $3}' | sort | uniq -c | sort -nr | head -n 20
 1137  clear
 1138  history 10
[root@Centos7Teach /]# history | awk '{print $3}' | sort | uniq -c | sort -nr |
head -n 20
    225
     38 smb.conf
     36 restart
     30 install
     27 -A
     24 -p
     18 samba.install.sh
     17 remove
     16 start
     16 -n
     15 -L
     14 u
     13 -l
     12 autoremove
     12 -MN
     11 -t
     11 -sU
     11 -R
     10 stop
     10 ..
[root@Centos7Teach /]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 34,24 1 会话 CAP NUM