Linux 常用操作

1）如何创建一个用户

```
以root用户身份，执行如下操作：
useradd -m shiah
passwd shiah

将shiah添加到wheel组，wheel组具有执行sudo命令的能力
usermod -aG wheel shiah

设置新用户的SSH登录权限,编辑/etc/ssh/sshd_config文件,确保以下两行是启用的
/etc/ssh/sshd_config

查看用户的权限和信息，用id命令
id shiah
```

2）如何创建和维护vnc

1. 安装 TigerVNC 服务器

在 CentOS 中，你可以使用以下命令安装：

```
sudo yum install tigervnc-server
```

2. 添加新的 VNC 会话

要为特定用户启动一个 VNC 会话，你需要切换到该用户并运行 `vncserver` 命令。例如，为用户 `john` 启动一个 VNC 会话：

```
su - john
vncserver
```

当你首次运行 `vncserver`，它会提示你设置 VNC 密码。

3. 删除指定的 VNC 会话

每个 VNC 会话都有一个唯一的编号。例如，`:1`, `:2` 等。要删除/杀死一个 VNC 会话，你可以使用以下命令：

```
vncserver -kill :1
```

这将会杀死 `:1` 的 VNC 会话。

4. 设置分辨率

你可以在启动 VNC 服务器时指定分辨率。例如，要设置分辨率为 `1366x768`，你可以使用以下命令：

```
vncserver -geometry 1366x768
```

修改vnc分辨率: vim ~/.vnc/config（里面的geometry配置=1364x766）

5. 开启 VNC 服务

为了使 VNC 服务器在启动时自动启动，你可以使用 `systemctl` 启用并启动服务。

首先，复制 VNC 服务单元文件到 `/etc/systemd/system/`：

```
sudo cp /lib/systemd/system/vncserver@.service /etc/systemd/system/vncserver@:1.service
```

然后编辑文件 `/etc/systemd/system/vncserver@:1.service`，替换 `<USER>` 为你的用户名。

重新加载 systemd 配置。在进行配置更改后，使用以下命令重新加载 systemd 配置：

```
sudo systemctl daemon-reload
```

接下来，启动服务：

```
sudo systemctl start vncserver@:1.service
```

要在启动时自动启动 VNC 服务，执行：

```
sudo systemctl enable vncserver@:1.service
```

6. 查询 VNC 服务状态

要查询 VNC 服务的状态，你可以使用：

```
sudo systemctl status vncserver@:1.service
```

7. 修改vnc密码

```
vncpasswd
```

3）如何创建和维护RDP（远程桌面连接）

RDP (Remote Desktop Protocol) 是 Microsoft 开发的一种远程桌面协议。在 Windows 系统中，RDP 功能是内置的，允许用户从其他计算机远程访问 Windows 机器的桌面。在 Linux 和其他平台上，也有一些工具可以让你使用 RDP 连接到 Windows 机器或从 Windows 机器连接到其他系统。

以下是关于 RDP 的一些常用操作和概念：

1. 在 Windows 中使用 RDP：

1. **启用远程桌面**:
    - 打开“控制面板” > “系统和安全” > “系统” > “远程设置”。
    - 在“远程”选项卡下，选择“允许远程连接到此计算机”。
2. **使用 Remote Desktop Connection 连接**:
    - 打开“开始”菜单并搜索“Remote Desktop Connection”。
    - 在“计算机”字段中输入要连接的计算机的 IP 地址或主机名。
    - 点击“连接”，然后输入远程计算机的用户名和密码。
3. **更改 RDP 端口** (高级操作): 默认情况下，RDP 使用 3389 端口。要更改这一设置，你需要编辑 Windows 的注册表。

2. 在 Linux 中使用 RDP：

1. **连接到 Windows 机器**: `rdesktop` 和 `xfreerdp` 是两个流行的 Linux RDP 客户端。使用它们，你可以从 Linux 机器连接到 RDP 服务器（如 Windows 机器）。

   例如，使用 `rdesktop` 连接到 IP 为 `192.168.1.100` 的 Windows 机器：

   ```
   rdesktop 192.168.1.100
   ```

2. **设置 Linux 为 RDP 服务器**: `xrdp` 是一个使 Linux 机器能够接受 RDP 连接的服务器。安装和配置 `xrdp` 后，你可以从任何 RDP 客户端（如 Windows 的 Remote Desktop Connection）连接到 Linux 机器。

   安装 `xrdp`：

   ```
   sudo apt-get install xrdp   # 对于 Debian/Ubuntu
   sudo yum install xrdp       # 对于 CentOS/Red Hat
   ```

   启动 `xrdp` 服务：

   ```
   sudo systemctl start xrdp
   ```

3. **配置 `xrdp`**: `xrdp` 的主配置文件通常位于 `/etc/xrdp/xrdp.ini`。你可以编辑此文件以更改端口、安全选项等。

这些是 RDP 的一些基本操作。无论是在 Windows 还是在 Linux 中，为了确保远程桌面连接的安全性，建议采取适当的安全措施，如使用强密码、限制可访问 RDP 的 IP 地址、使用 VPN 等。

4）关于ssh登陆方式

SSH（Secure Shell）是一种用于在网络上安全传输数据的协议，通常用于远程连接到远程服务器或机器上进行管理和数据传输。下面是一些常见的 SSH 命令用法示例：

1. 连接到远程服务器

要连接到远程服务器，使用 `ssh` 命令，后面跟着目标服务器的用户名和主机名或 IP 地址。

```
ssh username@hostname_or_ip
```

例如，连接到用户名为 "myuser" 的远程服务器 "example.com"：

```
ssh myuser@example.com
```

2. 使用非默认端口

如果目标服务器使用非默认 SSH 端口（默认为 22），可以使用 `-p` 选项指定端口号。

```
ssh -p port_number username@hostname_or_ip
```

例如，如果 SSH 服务器监听在端口 2222 上：

```
ssh -p 2222 myuser@example.com
```

3. 使用X11转发

`ssh -X` 选项用于启用 X11 转发。X11 转发允许你在远程服务器上运行图形应用程序，并将其图形界面显示在本地 X 窗口系统上。这对于在远程服务器上运行图形应用程序非常有用，例如图形编辑器或图形化配置工具。

以下是使用 `ssh -X` 的示例：

```
ssh -X username@hostname_or_ip
```

4. SCP 命令

SCP（Secure Copy）用于在本地系统和远程系统之间复制文件。它使用 SSH 协议进行安全的文件传输。

将本地文件复制到远程服务器：

```
scp local_file username@hostname_or_ip:remote_path
```

从远程服务器复制文件到本地：

```
scp username@hostname_or_ip:remote_file local_path
```

例如，将本地文件 "myfile.txt" 复制到远程服务器的 "/tmp" 目录：

```
scp myfile.txt myuser@example.com:/tmp
```

5. 使用非标准端口登陆（例如7000)

1. 需要在腾讯云服务器控制面板上开放7000端口的防火墙
2. 在云服务器linux系统中开放7000端口

```
sudo firewall-cmd --list-ports
sudo firewall-cmd --add-port=7000/tcp --permanent
sudo firewall-cmd --reload
```

3. 修改ssh配置文件, 修改默认的登录端口

```
sudo vi /etc/ssh/sshd_config
修改为port 7000

sudo systemctl restart sshd
```

通过以上配置后，就可使用7000端口进行ssh登录，sftp传输等。

5）关于端口和防火墙管理

在 Linux 中，有几种流行的防火墙工具。其中最常用的是 `iptables` 和 `firewalld`。`iptables` 在各种 Linux 发行版中都存在很长时间了，而 `firewalld` 是 Red Hat 和其派生版本（如 CentOS 和 Fedora）中的较新工具，它提供了一个更为友好的接口来管理防火墙规则。

以下是关于这两个工具的基本操作：

1. iptables：

- **查询防火墙状态**:

  ```
  sudo iptables -L -n -v
  ```

  这将列出所有当前的防火墙规则。

- **清空所有规则** (谨慎操作):

  ```
  sudo iptables -F
  ```

- **允许特定端口** (例如，允许 SSH 的端口 22):

  ```
  sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
  ```

- **阻止特定 IP 地址**:

  ```
  sudo iptables -A INPUT -s 192.168.1.100 -j DROP
  ```

- **保存规则**: 在某些系统上，你可能需要使用 `iptables-save` 和 `iptables-restore` 命令或特定于发行版的方法来持久保存规则。

2. firewalld：

- **查询防火墙状态**:

```
sudo firewall-cmd --state
```

- **启动/停止/重启防火墙**:

```
sudo systemctl start firewalld
sudo systemctl stop firewalld
sudo systemctl restart firewalld
```

- **列出所有规则**:

```
sudo firewall-cmd --list-all
```

- **允许特定端口** (例如，允许 SSH 的端口 22):

```
sudo firewall-cmd --zone=public --add-port=22/tcp --permanent
sudo firewall-cmd --reload
```

- **阻止特定 IP 地址**:

```
sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source
address="192.168.1.100" drop' --permanent
sudo firewall-cmd --reload
```

- **允许特定服务** (例如，允许 http 服务):

```
sudo firewall-cmd --zone=public --add-service=http --permanent
sudo firewall-cmd --reload
```

6）服务管理（systemctl)

`systemctl` 是 `systemd` 的主要命令行工具，用于控制初始化系统的服务和其他单位。`systemd` 是许多现代 Linux 发行版（如 Fedora、CentOS 7+、Debian 8+、Ubuntu 15.04+ 等）的默认初始化系统。

以下是 `systemctl` 的一些常见用法和说明：

1. 服务管理

- **启动服务**:

```
sudo systemctl start service_name
```

- **停止服务**:

```
sudo systemctl stop service_name
```

- **重新启动服务**:

```
sudo systemctl restart service_name
```

- **重新加载服务配置** (不完全停止服务，只重新加载配置):

```
sudo systemctl reload service_name
```

- **显示服务状态**:

```
systemctl status service_name
```

- **启用服务** (使其在启动时自动运行):

```
sudo systemctl enable service_name
```

- **禁用服务** (阻止其在启动时自动运行):

```
sudo systemctl disable service_name
```

2. 系统操作

- **重启系统**:

```
sudo systemctl reboot
```

- **关机系统**:

```
sudo systemctl poweroff
```

- **挂起系统** (休眠):

```
sudo systemctl suspend
```

- **休眠并保存系统状态** (混合休眠):

```
sudo systemctl hybrid-sleep
```

- **休眠并关闭电源** (冷冻):

```
sudo systemctl hibernate
```

3. 列出和查询

- **列出所有服务**:

```
systemctl list-units --type=service
```

- **列出所有运行中的服务**:

```
systemctl list-units --type=service --state=running
```

- **检查服务是否处于活动状态**:

```
systemctl is-active service_name
```

- **检查服务是否启用**:

```
systemctl is-enabled service_name
```

- **检查服务是否失败**:

```
systemctl is-failed service_name
```

4. 其他

- **重新加载 systemd 配置** (在修改了服务文件或其他 `systemd` 配置后):

```
sudo systemctl daemon-reload
```

7) 安装软件

在 CentOS 上，软件包的管理通常使用 `yum` 或者在 CentOS 8 及更高版本中使用 `dnf`。以下是如何使用这些命令来管理软件包的方法，以 `gvim` 为例：

1. **安装软件包**:
   - 使用 `yum`：

     ```
     sudo yum install gvim
     ```

2. **查询已安装的软件包**:
   - 使用 `yum`：

     ```
     yum list installed | grep gvim
     ```

3. **删除软件包**:
   - 使用 `yum`：

     ```
     sudo yum remove gvim
     ```

4. **查询软件包信息**:
   - 使用 `yum`：

```
yum info gvim
```

5. **搜索软件包**:
    - 使用 `yum`：

```
yum search gvim
```

8) hostname(主机名/ip)

`hostname` 命令在 Linux 和其他 UNIX-like 系统中用于显示或设置系统的主机名。以下是 `hostname` 命令的一些常见用法和说明：

1. **显示当前主机名**: 直接执行 `hostname` 命令将显示当前系统的主机名。

```
hostname
```

2. **显示网络地址 (IP 地址)**:

```
hostname -i
```

这将显示主机的 IP 地址。请注意，这依赖于系统的名称解析配置。

3. **显示所有网络地址**:

```
hostname -I
```

这将显示所有配置的网络地址。

9) tar/gzip

在 Linux 中，有多种工具和命令用于文件和目录的压缩和解压缩。以下是一些最常用的命令及其用法：

1. tar

`tar` 是一个用于归档文件的工具，但它通常与其他压缩工具（如 `gzip` 或 `bzip2`）结合使用来创建压缩的归档文件。

- **打包文件或目录**:

```
tar cvf output.tar directory_or_file
```

- **打包并使用 gzip 压缩**:

```
tar czvf output.tar.gz directory_or_file
```

- **打包并使用 bzip2 压缩**:

```
tar cjvf output.tar.bz2 directory_or_file
```

- **解压 tar 归档文件**:

```
tar xvf output.tar
```

- **解压 tar.gz 归档文件**:

```
tar xzvf output.tar.gz
```

- **解压 tar.bz2 归档文件**:

```
tar xjvf output.tar.bz2
```

2. gzip & gunzip

`gzip` 是一个常用的压缩工具，而 `gunzip` 则用于解压缩。

- **压缩文件**:

```
gzip filename
```

这会创建一个 `filename.gz` 的压缩文件。

- **解压缩文件**:

```
gunzip filename.gz
```

10）id(查看权限/组群)

`id` 命令用于显示当前用户或指定用户的用户和组信息。它通常用于查看用户的 UID（用户标识符）、GID（组标识符）、附属组信息等。以下是 `id` 命令的一些常见用法：

1. 查看当前用户的信息

默认情况下，如果不提供用户名，`id` 命令将显示当前登录用户的信息。

```
id
```

示例输出：

```
uid=1000(username) gid=1000(username)
groups=1000(username),4(adm),20(dialout),24(cdrom),27(sudo),30(dip),46(plugdev),117(lpadmin),1
```

上面的输出显示了当前用户（`username`）的 UID、GID 和附属组信息。

2. 查看指定用户的信息

你可以通过提供用户名来查看指定用户的信息。

```
id username
```

示例：

```
id john
```

11）lscpu/free/df/du/uname(查看cpu，内存，硬盘，容量，操作系统)

1. `lscpu` 命令

`lscpu` 命令用于显示有关 CPU（中央处理单元）的信息。

示例：

```
lscpu
```

示例输出（部分）：

```
Architecture:        x86_64
CPU op-mode(s):      32-bit, 64-bit
CPU(s):              4
Thread(s) per core:  2
Core(s) per socket:  2
Socket(s):           1
```

2. `free -m` 命令

`free -m` 命令用于显示内存使用情况，以兆字节（MB）为单位。

示例：

```
free -m
```

示例输出：

```
              total        used        free      shared  buff/cache   available
Mem:           7887        1342        6031          78         513        6262
Swap:          2047           0        2047
```

3. `df -h` 命令

`df -h` 命令用于显示文件系统的磁盘使用情况，并以人类可读的方式显示磁盘空间。

示例：

```
df -h
```

示例输出：

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        20G  6.4G   13G  34% /
tmpfs           3.9G     0  3.9G   0% /dev/shm
/dev/sdb1        50G   20G   28G  43% /data
```

4. `du -hs` 命令

`du -hs` 命令用于查看目录的磁盘使用情况总结，以人类可读的方式显示大小。

示例：

```
du -hs /path/to/directory
```

示例输出：

```
2.1G    /path/to/directory
```

5. `du -hs *` 命令

`du -hs *` 命令用于查看当前目录中每个子目录或文件的磁盘使用情况总结。

示例：

```
du -hs *
```

示例输出：

```
2.5G    directory1
512M    directory2
25M     file1.txt
10K     file2.txt
```

6. `uname -a` 命令

`uname` 命令用于显示系统信息，包括内核名称、主机名、内核版本、操作系统类型等。`-a` 选项表示显示所有可用信息。

示例用法：

```
uname -a
```

示例输出：

```
Linux my-server 5.4.0-77-generic #86-Ubuntu SMP Thu Jun 17 02:35:03 UTC 2021 x86_64 x86_64
x86_64 GNU/Linux
```

输出的信息包括：

- `Linux`：操作系统类型。
- `my-server`：主机名。
- `5.4.0-77-generic`：内核版本。
- `#86-Ubuntu SMP Thu Jun 17 02:35:03 UTC 2021`：内核编译信息和日期。
- `x86_64 x86_64 x86_64`：CPU 架构。
- `GNU/Linux`：操作系统名称。

12）ifconfig/ip/netstat/ss/ping/wget（网络相关的命令）

Linux 提供了许多命令和工具，用于管理和配置网络设置。以下是一些常见的 Linux 网络和配置相关命令：

1. ifconfig

`ifconfig` 命令用于显示和配置网络接口的信息，如 IP 地址、子网掩码、MAC 地址等。

示例用法：

```
ifconfig
ifconfig eth0 up
ifconfig eth0 down
```

2. ip

`ip` 命令是更现代的网络配置工具，它提供了更多高级选项，用于配置网络接口、路由表和其他网络参数。

示例用法：

```
ip addr show
ip route show
```

3. netstat

`netstat` 命令用于显示网络统计信息，如网络连接、路由表、接口统计等。注意，该命令在一些 Linux 发行版中已被标记为过时。

示例用法：

```
netstat -tuln
```

4. ss

`ss` 命令是 `netstat` 的替代工具，用于显示套接字统计信息，包括网络连接和路由表。

示例用法：

```
ss -tuln
```

5. ping

`ping` 命令用于测试与远程主机的网络连通性。它发送 ICMP 回显请求并等待回复。

示例用法：

```
ping google.com
```

6. wget 和 curl

`wget` 和 `curl` 命令用于从网络上下载文件。它们可以用于获取 Web 内容、文件和资源。

示例用法：

```
wget https://example.com/file.zip
curl -O https://example.com/image.jpg
```

13）chmod/chown/chgroup

1. `chmod` 命令

`chmod` 命令用于更改文件或目录的权限。以下是一些示例用法：

示例 1: 使用数字表示法

假设你有一个文件 `example.txt`，要将其权限设置为只允许文件所有者读、写和执行，但只允许所属组和其他用户读的权限。

```
chmod 744 example.txt
```

这会将 `example.txt` 文件的权限设置为 `-rwxr--r--`。

示例 2: 使用符号表示法

假设你希望添加执行权限给文件所有者，但不更改其他权限。你可以使用符号表示法的 `+` 来添加权限。

```
chmod u+x example.txt
```

这会将 `example.txt` 文件的权限从 `-rw-r--r--` 更改为 `-rwxr--r--`，允许文件所有者执行该文件。

2. `chmod -R` 命令

`chmod -R` 命令用于递归地更改目录及其子目录中的文件和目录的权限。例如，要将某个目录及其所有内容的权限设置为特定值，可以使用 `-R` 选项。

示例: 递归更改目录权限

假设你有一个目录 `mydir`，你希望将该目录及其所有内容的权限设置为只允许文件所有者读写，但其他用户没有权限。

```
chmod -R 600 mydir
```

这会将 `mydir` 目录及其所有子目录和文件的权限设置为 `-rw-------`。

3. `chown` 命令

`chown` 命令用于更改文件或目录的所有者。以下是一些示例用法：

示例 1: 更改文件所有者

假设你有一个文件 `example.txt`，你希望将其所有者更改为新用户 `newuser`。

```
chown newuser example.txt
```

这会将 `example.txt` 文件的所有者更改为 `newuser`。

示例 2: 更改目录及其内容的所有者

假设你有一个目录 `mydir`，你希望将该目录及其所有内容的所有者更改为新用户 `newuser`。

```
chown -R newuser mydir
```

这会将 `mydir` 目录及其所有子目录和文件的所有者都更改为 `newuser`。

4. `chgrp` 命令

`chgrp` 命令用于更改文件或目录的所属组。以下是一些示例用法：

示例 1: 更改文件的所属组

假设你有一个文件 `example.txt`，你希望将其所属组更改为新组 `newgroup`。

```
chgrp newgroup example.txt
```

这会将 `example.txt` 文件的所属组更改为 `newgroup`。

示例 2: 更改目录及其内容的所属组

假设你有一个目录 `mydir`，你希望将该目录及其所有内容的所属组更改为新组 `newgroup`。

```
chgrp -R newgroup mydir
```

这会将 `mydir` 目录及其所有子目录和文件的所属组都更改为 `newgroup`。

14）关于linux端口

Linux 系统中的端口是网络通信的关键组成部分。端口用于标识不同的网络服务或进程，并且帮助将数据包路由到正确的应用程序。以下是关于 Linux 端口的详细知识：

1. 端口号

每个端口都有一个与之相关联的端口号，这是一个16位的整数，范围从0到65535。端口号分为三个范围：

- **系统端口（Well-known Ports）**：范围从0到1023。这些端口号通常用于标准服务，如 HTTP（端口号80）、HTTPS（端口号443）、SSH（端口号22）等。
- **注册端口（Registered Ports）**：范围从1024到49151。这些端口号可以由应用程序或服务注册使用，但通常不属于标准服务。
- **动态/私有端口（Dynamic/Private Ports）**：范围从49152到65535。这些端口号通常由客户端应用程序用于临时通信，例如在与服务器建立连接时。

2. 端口类型

在 Linux 中，端口可以分为两种主要类型：

- **TCP 端口**：TCP（传输控制协议）端口用于可靠的、面向连接的通信。TCP 是一种流协议，用于确保数据在传输过程中不丢失、不重复，以及按顺序传输。许多应用程序（如网页浏览器、邮件客户端等）使用 TCP 端口。
- **UDP 端口**：UDP（用户数据报协议）端口用于不可靠的、面向无连接的通信。UDP 不会确保数据的可靠传输，因此通常用于实时应用程序，如音频和视频流、DNS 查询等。

3. 端口和服务映射

每个端口通常与一个特定的网络服务或应用程序相关联。这个映射关系被记录在系统的服务配置文件中，通常位于 `/etc/services` 文件中。这个文件包含了端口号、协议类型（TCP 或 UDP）以及关联的服务或应用程序的名称。

4. 查看正在使用的端口

要查看系统上哪些端口正在使用，可以使用以下命令：

- `netstat`：这个命令可以显示系统上的网络连接、路由表和接口统计信息。例如，可以使用 `netstat -tuln` 命令来显示所有正在监听的 TCP 和 UDP 端口。
- `ss`：`ss` 命令也用于查看套接字统计信息，包括网络连接和监听端口。例如，`ss -tuln` 可以显示正在监听的 TCP 和 UDP 端口。

- `lsof`：`lsof` 命令可以列出打开的文件和套接字。通过 `lsof -i` 命令，你可以查看正在使用的网络连接和监听的端口。

5. 配置防火墙规则

Linux 防火墙可以用于控制进出系统的网络流量。你可以使用工具如 `iptables` 或 `firewalld` 来配置防火墙规则，包括允许或禁止特定端口上的通信。

- `iptables`：是一个强大的命令行工具，用于配置 Linux 内核中的防火墙规则。可以使用 `iptables` 命令来添加、删除、修改规则。
- `firewalld`：是一个更高级的防火墙管理器，它提供了更友好的界面来配置防火墙规则。它基于 `iptables`，但提供了更容易使用的抽象。

6. 端口扫描和安全性

了解端口的状态和用途对于网络安全至关重要。黑客可能会使用端口扫描工具来探测目标系统上开放的端口，以发现潜在的漏洞。因此，保护系统并限制不必要的开放端口对于维护系统的安全性至关重要。

15）nmap(端口扫描软件)

1. **Nmap：**
    - Nmap（Network Mapper）是一个强大的开源网络扫描工具，用于发现目标主机上开放的端口和服务。
    - 你可以在终端中使用以下命令来扫描网关上的开放端口：

      ```
      nmap -p- <gateway_IP>
      ```

      这将扫描所有端口（从1到65535）并显示哪些端口是开放的。
2. **Nmap的安装：**

在 Ubuntu 或 Debian 上：

在 CentOS 或 Fedora 上：

在 CentOS 或 Fedora 系统上，你可以使用 `yum` 包管理工具安装 Nmap。打开终端并运行以下命令：

```
sudo yum install nmap
```

在 Windows 上：

对于 Windows 用户，Nmap 提供了一个官方的 Windows 版本，你可以从 Nmap 官网的下载页面上获取安装程序。下载安装程序后，双击运行它并按照提示进行安装。

安装完成后，你可以在终端（命令提示符或 PowerShell）中运行 `nmap` 命令来开始使用 Nmap。

1. 扫描单个主机或 IP 地址

```
nmap <目标主机或IP>
```

示例：

```
nmap 192.168.1.1
```

2. 扫描整个子网

```
nmap <目标子网>
```

示例：

```
nmap 192.168.1.0/24
```

3. 扫描特定端口

```
nmap -p <端口号> <目标主机或IP>
```

示例：

```
nmap -p 80 192.168.1.1
```

4. 扫描一定范围的端口

```
nmap -p <起始端口号>-<结束端口号> <目标主机或IP>
```

示例：

```
nmap -p 80-100 192.168.1.1
```

5. 扫描常用端口（Top 1000）

```
nmap -F <目标主机或IP>
```

示例：

```
nmap -F 192.168.1.1
```

6. 扫描所有端口（全面扫描）

```
nmap -p- <目标主机或IP>
```

示例：

```
nmap -p- 192.168.1.1
```

7. 识别操作系统

```
nmap -O <目标主机或IP>
```

示例：

```
nmap -O 192.168.1.1
```

16）手动启动synopsys license

```
cd /opt/synopsys/lic

ls看到下面有3个文件
lmgrd  snpslmd  Synopsys.dat

手动执行
./lmgrd -c ./Synopsys.dat

执行如下命令查看服务是否启动正常
lmstat -a
```

Windows常用操作

1）win10，测试与服务器连接的端口

Test-NetConnection -Port 22 -ComputerName 114.132.51.2 Test-NetConnection -Port 3389 -ComputerName 114.132.51.2 Test-NetConnection -Port 5901 -ComputerName 114.132.51.2

2）win10，让程序开机自启动，或取消程序的开机自启动

1. 让某些程序开机自启动

```
1. 打开任务管理器。你可以按下 `Ctrl + Shift + Esc` 组合键，或者按 `Ctrl + Alt + Delete` 选择任务管理器。
2. 在任务管理器中，切换到 "启动" 选项卡。这个选项卡会列出在Windows启动时会自动运行的程序。
3. 在启动选项卡中，你将看到一个列表，显示了每个启动项的名称、制造商和状态。
4. 找到你想要开机自启动的程序。你可以通过查看"启动项"列来确定这些程序。
5. 如果某个程序的状态是 "已启用"，它将在Windows启动时自动运行。如果状态是 "已禁用"，它将被禁用。
6. 如果你想让某个程序开机自启动，只需右键单击该程序，然后选择 "启用"。
```

2. 取消某些程序的开机自启动：

```
1. 打开任务管理器，切换到 "启动" 选项卡，找到你想要取消自启动的程序。
2. 右键单击该程序，然后选择 "禁用"。
3. 这将取消该程序的开机自启动。
```