

Nessus

下载

如果想下载NESSUS，需要去官网进行下载（PS:官网有Linux kali的）

<https://www.tenable.com/downloads/nessus?loginAttempted=true>

下载完之后使用 `dpkg -i Nessus` 进行安装

如果安装正确他会给你返个

```
Unpacking Nessus Scanner Core Components...
- You can start Nessus Scanner by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner
```

正在处理用于 systemd (244-3) 的触发器 ...

```
使用 /etc/init.d/nessusd start 进行启动
Unpacking Nessus Scanner Core Components...
- You can start Nessus Scanner by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner
正在处理用于 systemd (244-3) 的触发器 ...
E:\> /etc/init.d/nessusd start
Starting Nessus : .
E:\> [Tue Mar 17 03:12:00 2020][29127.1][op=qdb_sync][name=services-udp.db][fd=7][map_sz=0][file_size=130849]: complete
Tue Mar 17 03:12:00 2020][29127.1][op=qdb_sync][name=services-tcp.db][fd=6][map_sz=0][file_size=137898]: complete
Tue Mar 17 03:12:00 2020][29127.1][op=qdb_map][name=services-udp.db][fd=-1][map_sz=38575]: complete
Tue Mar 17 03:12:00 2020][29127.1][op=qdb_map][name=services-tcp.db][fd=-1][map_sz=40899]: complete
Tue Mar 17 03:12:00 2020][29127.1][op=qdb_map][name=services-tcp.db][fd=-1][map_sz=40899]: complete
Tue Mar 17 03:12:00 2020][29127.1][op=qdb_sync][name=upgrades.db][fd=5][map_sz=0][file_size=20]: complete
Tue Mar 17 03:12:00 2020][29127.1][op=qdb_sync][name=upgrades.db][fd=5][map_sz=0][file_size=55]: complete
Tue Mar 17 03:12:01 2020][29127.1][op=qdb_sync][name=plugins-desc.db][fd=8][map_sz=0][file_size=20]: complete
Tue Mar 17 03:12:01 2020][29127.1][op=qdb_sync][name=plugins-code.db][fd=7][map_sz=0][file_size=20]: complete
Tue Mar 17 03:12:01 2020][29127.1][op=qdb_map_lowmem][name=plugins-code.db.15844291212033859932][fd=7][map_sz=0][file_size=20]: complet
Tue Mar 17 03:12:01 2020][29127.1][op=qdb_map_lowmem][name=plugins-desc.db.1584429121136401431][fd=8][map_sz=0][file_size=20]: complete
E:\>
```

你可以使用 `/etc/init.d/nessusd status` 查看启动结果

网络唤醒：

在Nessus中的Host Discovery是有一个网络唤醒功能的但是需要目标主机的mAC地址，

Wake-on-LAN

List of MAC addresses

Add File

Boot time wait (in minutes)

5

AIX Local Security Checks

AIX本地安全检查

Amazon Linux Local Security Checks

Amazon Linux本地安全检查

Backdoors

后门

Brute force attacks

蛮力攻击

CentOS Local Security Checks

CentOS本地安全检查

CGI abuses

CGI滥用

CGI abuses : XSS

CGI的弊端:XSS

CISCO

思科

Databases

数据库

Debian Local Security Checks

Debian本地安全检查

Default Unix Accounts

默认的Unix账户

Denial of Service

拒绝服务

DNS

DNS

F5 Networks Local Security Checks

F5网络本地安全检查

Fedora Local Security Checks

Fedora本地安全检查

Firewalls

防火墙

FreeBSD Local Security Checks

FreeBSD本地安全检查

FTP

FTP

Gain a shell remotely

远程获取一个shell

General

一般

Gentoo Local Security Checks

Gentoo当地安全检查

HP-UX Local Security Checks

HP-UX本地安全检查

Huawei Local Security Checks

华为本地安全检查

Junos Local Security Checks

朱诺斯当地安全检查

MacOS X Local Security Checks

MacOS X本地安全检查

Mandriva Local Security Checks

Mandriva当地安全检查

Misc.

混杂。

Netware

网络

NewStart CGSL Local Security Checks

新启动CGSL本地安全检查

Oracle Linux Local Security Checks

Oracle Linux本地安全检查

OracleVM Local Security Checks

OracleVM本地安全检查

Palo Alto Local Security Checks

帕洛阿尔托当地的安全检查

Peer-To-Peer File Sharing

点对点文件共享

PhotonOS Local Security Checks

光子本地安全检查

Policy Compliance

政策合规

Red Hat Local Security Checks

红帽当地的安全检查

RPC

RPC

SCADA

SCADA

Scientific Linux Local Security Checks

科学的Linux本地安全检查

Service detection

服务发现

Settings

设置

Slackware Local Security Checks

本地安全检查

SMTP problems

SMTP问题

SNMP

SNMP

Solaris Local Security Checks

Solaris本地安全检查

SuSE Local Security Checks

使用本地安全检查

Ubuntu Local Security Checks

Ubuntu本地安全检查

Virtuozzo Local Security Checks

Virtuozzo本地安全检查

VMware ESX Local Security Checks

VMware ESX本地安全检查

Web Servers

Web服务器

Windows

窗户

Windows : Microsoft Bulletins

Windows:微软公告

Windows : User management

Windows:用户管理

nessus 的等级划分

CVSS score	Criticality
0	Info
<4	Low
<7	Medium
<10	High
10	Critical