实验十四：使用 Nmap 进行安全检测

一、实验目的

1、了解 Namp；

2、掌握使用 Namp 对主机进行安全检测；

3、掌握使用 Namp 对 WopdPress 网站服务进行安全检测。

二、实验学时

2 学时

三、实验类型

设计性

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 操作系统，安装 Oracle VM VirtualBox 软件，安装 Mobaxerm 软件。

3、网络

本地主机与虚拟机能够访问互联网，不使用 DHCP 服务。

4、工具

无。

五、实验任务

1、完成 Nmap 的安装；

2、完成指定网络内主机的安全检测；

3、完成对 WordPress 网站服务的安全检测。

六、实验环境

1、本实验需要 VM 1 台；

2、本实验 VM 配置信息如下表所示；

虚拟机配置	操作系统配置
虚拟机名称：VM-Lab-14-Task-01-172.20.1.27 内存：1GB CPU：1 颗，1 核心	主机名：Lab-14-Task-01 IP 地址：172.20.1.27 子网掩码：255.255.255.0

虚拟磁盘：20GB 网卡：1 块，桥接	网关：172.20.1.1 DNS：8.8.8.8

3、本实验拓扑图。

无

4、本实验操作演示视频。

无

七、实验内容及步骤

1、在线方式安装 Nmap

使用 dnf 工具安装 Nmap。

```
# 使用 dnf 工具安装 Nmap  [root@Lab-14-Task-01 ~]# dnf install -y nmap
```

2、使用 Nmap 进行主机安全检测

（1）使用 Nmap 工具对 172.20.1.0/24 网络段内主机进行安全检测。

```
# 使用 Nmap 工具对 172.20.1.0/24 网络段内主机进行安全检测
[root@Lab-14-Task-01 ~]# nmap -sV -O 172.20.1.0/24

# ----------检测结果----------
# 展示 Nmap 当版本与执行操作的时间
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-12 14:51 CST

.....此处省略了部分发现的主机信息.....

# 主机(172.20.1.30)扫描的报告结果如下
Nmap scan report for bogon (172.20.1.30)
# 主机状态为开启
Host is up (0.00053s latency).
# 常用 1000 个端口中，有 980 个端口处于关闭状态
Not shown: 980 filtered tcp ports (no-response), 10 filtered tcp ports (admin-proh
ibited)
# 针对开放端口服务，查看运行版本信息
PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    closed ftp
# OpenSSHare 服务版本为 8.7，遵照开源 SSH2.0 协议
22/tcp    open   ssh         OpenSSH 8.7 (protocol 2.0)
80/tcp    closed http
9001/tcp  closed tor-orport
9002/tcp  closed dynamid
9009/tcp  closed pichat
9010/tcp  closed sdr
9011/tcp  closed d-star
```

```
9090/tcp closed zeus-admin
MAC Address: 08:00:27:78:0E:A2 (Oracle VirtualBox virtual NIC)
# 设备类型为通用设备（普通 PC 或服务器）
Device type: general purpose
# 主机操作系统名称为 Linux，版本为 5.X
Running: Linux 5.X
# 操作系统内核版本为 5
OS CPE: cpe:/o:linux:linux_kernel:5
# 主机操作系统详细名称
OS details: Linux 5.0 - 5.4
# 网络路由追踪：1 跳
Network Distance: 1 hop
# 操作系统或服务的检测结果，如有异议可在 Nmap 官网上进行提交
OS and Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
# 本次 Nmap 命令共扫描 256 地址，其中 53 个主机是处于开机运行状态，总共耗时 1343.67
秒
Nmap done: 256 IP addresses (53 hosts up) scanned in 1343.67 seconds
# --------------------检测结果--------------------
```

3、使用 Nmap 检测 WordPress 网站服务

本步骤使用 Nmap 工具对对主机 172.20.1.25 所使用的 WordPress 程序进行安全检测，实现 5 个目标：

（1）使用“http-wordpress-enum”插件检测 WordPress 是否存在主题与插件版本陈旧。

（2）使用“http-wordpress-users”插件检测 WordPress 是否存在用户名信息泄露。

（3）使用“http-wordpress-brute”插件检测 WordPress 是否存在简易密码的现象。

（4）使用“http-vuln-cve2014-8877”插件检测 WordPress 是否存在远程注入漏洞（CVE-2014-8877）。

（5）使用“http-vuln-cve2017-1001000”插件检测 WordPress 是否存在未经身份验证的内容注入漏洞（CVE-2017-1001000）。

```
# 使用 Nmap 工具对数据库服务进行扫描和安全检测，检测时使用相应脚本
[root@Lab-14-Task-01 ~]# nmap --script=http-wordpress-enum --script=http-word
press-users --script=http-wordpress-brute --script=http-vuln-cve2014-8877 --script
=http-vuln-cve2017-1001000 172.20.1.25

# --------------------检测结果--------------------
# 主机：172.20.1.29，状态为"up"，延迟为 0.00013 秒
Nmap scan report for bogon (172.20.1.25)
Host is up (0.00013s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
# SSH 服务开放
22/tcp    open  ssh
# MySQL 数据库服务开放
3306/tcp open  mysql
# HTTP 代理开放
```

```
8080/tcp open  http-proxy
# 检测到一个有效的 WordPress 登录凭证：admin:123456
| http-wordpress-brute:
|   Accounts:
|     admin:123456 - Valid credentials
|_  Statistics: Performed 9160 guesses in 600 seconds, average tps: 13.9
# 找到了一个用户名：admin。检索停止时已经达到 ID#25。可以使用 'http-wordpress-users.limit' 增加上限。
| http-wordpress-users:
| Username found: admin
|_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'
# 在前 100 个主题/插件中进行了搜索，找到了 akismet 插件
| http-wordpress-enum:
| Search limited to top 100 themes/plugins
|   plugins
|_    akismet
MAC Address: 08:00:27:CF:5E:3E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 600.47 seconds
# --------------------检测结果--------------------
```