第3章

口令攻防

CHAPTER 3

通过本章学习，可以达到以下目标：

- 理解口令的概念，掌握口令攻防的技术及方法。
- 掌握 NTPWEdit、Hydra、Crunch 等口令攻击工具的基本使用方法。
- 从对远程暴力破解 Windows 远程桌面用户口令的防御案例中体会多层次防御方法。
- 重视对口令的管理，增强对口令攻击的防范意识。

3.1　口令攻防概念

3.1.1　口令的概念

口令是身份认证的一个组成部分，是操作系统及众多网络应用的第一道防线。口令的作用是向目标系统提供唯一标识个体身份的机制，从而保证目标系统的安全及不同用户的访问权限控制。

口令攻击是指黑客以口令为攻击目标，破解合法用户的口令或避开口令验证过程，然后冒充合法用户潜入目标系统，随心所欲地窃取、破坏和篡改目标系统的信息，直至完全控制目标系统。口令攻击是黑客实施网络攻击的最基本、最重要、最有效的方法之一。

3.1.2　口令的分类及验证方式

1. 静态口令

静态口令是指用户登录系统的口令是在注册时一次性产生的，在下一次用户修改之前的使用过程中总是固定不变的。静态口令一般存储在目标系统的数据库中，有的口令在目标系统中会以文件形式存在，如 Windows 系统的登录口令。在登录网络系统时，用户输入的用户名和口令通过网络传输给服务器，服务器将其与系统中保存的用户名和口令进行查询及匹配，检查是否一致，从而实现对用户的身份验证。

静态口令从软件设计角度最简单易行，但是由于口令在被用户修改前的静态不变特性，使得其安全性较低。此外，如果用户设计的口令过于简单，则很容易被攻击者猜测出来；如果口令过于复杂，那么用户又难以记忆口令，甚至经常忘记口令。当前互联网时代有太多的网络系统需要用户登录，一个用户需要记忆多个不同口令也不现实，因此往往会在多个系统中重复使用同一个或少数几个口令。在这种情况下，如果某用户的口令在一个系统中被攻击者破解，攻击者可能会使用口令去其他系统中“碰运气”，这无疑增加了口令被泄露的风险。

2. 动态口令

动态口令也称为一次性口令，是指根据专门的算法生成一个不可预测的随机字符组合，使得用户每次登录系统时的口令都是变化的。动态口令现在被广泛运用在网上银行、电子商务、大型门户网站等领域。例如，手机短信认证就是动态口令应用最广泛的场合之一。手机短信密码就是以手机短信形式请求包含 6 位或更多位随机数的动态口令，身份认证系统以短信形式发送随机的 6 位或 8 位密码到用户的手机上，同时将此口令存储到服务器中作为该用户的最新口令；用户在登录或交易认证时输入此动态口令进行验证。此外，短信验证要求在约定时间内完成(如 60s)，超过时间阈值后，身份认证系统会发送新的短信来等待用户验证，从而确保更高的安全性。又如，在网站登录时，除了用户名和密码登录外，还可能会加入随机变化的图片验证码，这个验证码也可以看成是一个动态口令。

动态口令应用形式还有动态口令卡、动态口令硬件等,被广泛应用在网上银行交易、高考成绩查询及志愿填报等领域。动态口令卡上有横纵坐标及对应的数字,根据服务器反馈的坐标,输入相应的数字进行验证。动态口令硬件外观如U盘,是一种内置电源、密码生成芯片和显示屏,根据专门的算法每隔一定时间自动更新动态口令的专用硬件。

动态口令不仅提高了口令安全性,而且使得用户避免了记忆复杂口令。

3.1.3 口令攻击的主要方法

1. 离线攻击

离线攻击一般是指对存储口令的文件或数据库载体直接进行攻击。破解的难度主要取决于口令的加密方式、加密算法、复杂度等。相对于在线攻击,离线攻击破解成功的可能性更大。此外,部分离线攻击是破坏或初始化口令文件。

2. 在线攻击

在线攻击一般是指通过网络访问常规的系统登录入口、模拟入口或非常规入口攻击用户口令。常规登录入口,如系统的登录窗口,通过人工输入进行口令攻击。模拟入口,如利用木马程序操控键盘和鼠标事件输入字符串来进行口令攻击,或者通过网络连接来进行口令攻击。本书后面将有案例介绍通过网络连接来破解Windows远程桌面的用户名和密码,以及通过Burp Suite工具重放攻击DVWA靶场网站的登录用户名和密码。此外,还有中间人攻击等其他非常规入口破解用户口令。

3. 弱口令攻击

弱口令主要是指两类口令,一是某些系统出厂设置的默认口令,如123456、888888、admin或空口令;二是仅包含简单数字和(或)字母组合的简单口令,如123456、a123456、5201314、1qaz2wsx、1q2w3e4r、admin123、admin、password、princess等。

4. 猜测攻击

使用口令猜测程序进行攻击。在详细了解目标对象的社会背景后,根据用户的姓名缩写、生日、身份证号后6位、所在省市缩写、单位缩写、电话号码等要素,口令猜测程序可以列举出几百种可能的口令,并在很短的时间内完成猜测攻击。

5. 字典攻击

字典是一个存储口令的列表文件。字典攻击实际上是指口令来源是字典文件,其内容为自定义的弱口令集合或通过穷举法生成的口令集合。口令既可以是明文,也可以是密文。

6. 暴力(穷举)攻击

暴力攻击是一种口令攻击方式,口令来源可以是口令字典,也可以是程序化即时生成的口令集合,其原理是对所有可能的口令集合进行穷举式的逐一测试。例如,已知口令是6位长度的数字组合,则口令集合是{000000,000001,000002,…,999999},即有10^6个字典就一

定能覆盖正确的口令，从而完成暴力攻击。理论上没有攻不破的口令，攻破只是一个时间的问题。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，则最终能破解所有的口令。

7. 生日攻击

生日攻击是一种密码学攻击手段，利用概率论中生日问题的数学原理，攻击者可找到哈希函数碰撞。生日悖论的一个结论是只要一个班里达到 23 个人，至少有两人生日日期相同的概率就大于 50%。将长度不固定的明文 C1 使用特定哈希函数，生成固定长度输出的消息摘要（哈希值）H1，那么存在一个概率能找到另一个明文 C2 对应的哈希值 H2 等同于 H1。攻击者只要找到这样的明文 C2，就可以假冒成明文 C1 的身份通过系统验证。抵御生日攻击的方法是消息摘要的长度足够长（如 128bit 以上），则哈希函数碰撞的概率就足够小。

8. 社会工程学

社会工程学是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行欺骗，从而入侵被骗者的计算机系统的一种攻击方式。后来延伸到真实社会当中，欺骗者通常以人际交往方式套取用户的秘密和口令，从而收集信息对被害人进行渗透。避免此类攻击的对策是加强用户防御意识。

3.1.4　口令攻击的防御方法

口令攻击的防御方法主要从技术角度和用户管理角度两方面考虑。

1. 技术角度

（1）口令长度尽量不少于 8 位。

（2）尽量避免使用生日、电话号码、身份证号、完整的英文单词等有意义的口令。

（3）不要使用常见弱口令，尽量使用强口令。强口令尽可能地包含多样的字符串组合，如大小写字母、数字、特殊字符的组合。

（4）系统中的口令必须使用口令的消息摘要进行存储和验证，禁止明文存储和验证。

（5）口令可使用摘要加盐机制，即系统中存储的口令摘要（哈希值）不是原始口令明文生成的摘要，而是在原始口令明文基础上附加了固定字符串或随机字符串后生成的摘要，附加的字符串又称为盐（salt），此方法可以更好地抵抗暴力攻击。

（6）系统应采用验证码、多次登录失败禁用账户等方式防止自动化攻击。

（7）有条件的系统尽量采用动态口令验证机制。

2. 用户管理角度

（1）不要将口令写到纸上或存于计算机文件中。

（2）尽量不要在不同系统上使用同一口令。

（3）为防止他人窃取口令，在输入口令时应确认无人在身边。

（4）定期改变口令，如每隔 2～6 个月要改变一次。

3.2 Windows 系统口令攻防

3.2.1 Windows 系统口令机制

SAM(Security Accounts Manager,安全账户管理器)是 Windows 操作系统的用户账户数据库,所有用户的登录名及口令等相关信息都保存在这个文件中。系统在保存 SAM 信息之前对 SAM 信息进行了压缩处理,因此,SAM 文件中的信息不可读取。此外,在系统运行期间,SAM 文件被系统锁定,也不允许复制。即使是管理员账号(account)也无法打开。SAM 数据库位于注册表 HKLM\SAM\SAM 下,受到 ACL 保护,可以使用注册表编辑器并设置适当权限查看 SAM 中的内容。SAM 数据库默认保存在 C:\Windows\System32\config 目录下的 SAM 文件中,在这个目录下还包括一个 Security 文件,是安全数据库的内容,两者有较少的关系。SAM 数据库中包括所有组和账户的信息,包括密码 Hash、账户的 SID 等。

1. Windows 系统的两种口令加密机制

Windows 系统的 SAM 文件中保存着两类口令值,一个是 LanMan 版本的散列值(LM),另一个是 NT 版本的散列值(NTLM)。

(1) LM 散列算法。

LM 散列算法处理用户口令的过程是将用户口令分成两半,每一半都是 7 个字符(不足 7 个字符的以 0x00 补齐),然后分别对这两个口令进行加密,并将加密后得到的散列值串连在一起,从而得到最终的 LM 散列值。

(2) NTLM 散列算法。

NTLM 散列值由两部分组成:一部分是通过变现 DES 算法,使用密码的大写 OEM 格式作为密钥(分成 2 个 KEY,每个 KEY 为 7 字节,用 0 补足 14 字节),通过 DESECB 方式获得一个 128 位的密钥,加密特殊字符串"KGS! @ # $ %"获得一个 16 字节长度的值;另一部分则是使用 MD4 对密码的 Unicode 形式进行加密,以此获得一个散列值。

2. Windows 系统的两种口令加密机制比较

(1) LM 安全性。

LM 算法将 14 字节的密码分为两组分别进行加密,使得两组密文可以分别破解,并且明文空间从 95^{14} 减少到 95^{7}。LM 算法不区分密码的大小写字符,使得明文空间从 95^{7} 减少到 69^{7}。LM 算法不像其他散列算法一样包含随机的初始向量,这使得用空间换取时间的字典攻击(如彩虹表)等成为可能。LM 安全性较差,Windows XP 及以前版本系统使用 LM 存储账户密码散列值。

(2) NTLM 安全性。

NTLM 算法的安全性较 LM 有所提升,这是因为其明文空间扩展到了 95^{128},采用暴力破解的时间复杂度大大增加。但是,NTLM 散列和 LM 散列一样,都没有在算法中附加随机数据的加盐机制,所以仍然会受到暴力攻击。同时,由于 NTLM 的明文空间较大,其字段

占用的空间也会呈几何级数增长，破解时间自然也较 LM 要长很多。

3.2.2　实验五：本地破解 Windows 用户口令


视频讲解

1. 实验目的

(1) 掌握使用 U 盘制作 Windows PE 系统启动盘的方法。
(2) 掌握使用 NTPWEdit 等工具破解 Windows 7 口令的原理及方法。

2. 实验任务与要求

(1) 使用 U 盘制作 Windows PE 系统启动盘。
(2) 对计算机设置开机启动顺序，并优先加载 Windows PE。
(3) 在 Windows PE 中使用 NTPWEdit 等工具破解 Windows 口令。

3. 实验原理(技术)

(1) Windows 口令 SAM 文件在当前 Windows 系统运行时是被锁定的，也不允许复制，因此需要脱机并加载其他操作系统破解。本实验无须拆卸硬盘，先制作 Windows PE 系统启动盘，并优先启动该启动盘，在 Windows PE 系统中读取并破解 SAM 文件。

(2) NTPWEdit 是一款 Windows 用户登录密码设置工具，支持破解 Windows XP/7/10，以及 Windows 2003/2008/2012 系统。NTPWEdit 破解的主要原理是在 Windows PE 环境中加载 Windows 操作系统中的 C:\Windows\System32\config\SAM 用户配置文件，对该配置文件中存储的原有用户登录密码进行删除或设置新登录密码后，再采用同样的算法加密并覆盖原有登录密码。

4. 实验仪器设备(环境条件)

(1) 攻击机。
Windows PE 和 NTPWEdit 工具。
(2) 靶机。
实体机 Windows 或虚拟机 VMware Workstation 15.5＋Windows。
(3) 空白 U 盘。

5. 实验过程

(1) 制作 Windows PE 启动盘。

使用空白 U 盘制作 Windows PE 启动盘并自带 NTPWEdit 工具，Windows PE 启动盘软件可以使用老毛桃、大白菜、深度等，制作如图 3-1 所示。

图 3-1　制作 Windows PE 启动盘

(2) 设置系统启动顺序。

首选从 U 盘启动，而非硬盘启动。例如，某主机 BIOS 中设置 U 盘(KingstonDataTraveler 3.0)为

第一启动设备并保存,如图 3-2 所示。

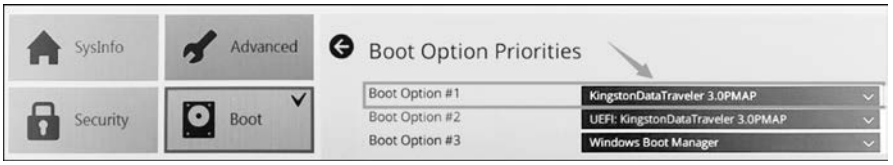


图 3-2 设置 U 盘为第一启动设备

(3) 清除原密码。

重新启动主机,从 U 盘的 Windows PE 系统启动后,找到密码清除工具 NTPWEdit 并启动。可见 SAM 文件路径被自动找到为 C:\Windows\System32\config\SAM,先单击"打开"按钮,然后左边用户列表中就显示所有的本地用户,如 Administrator、Guest 等。选中需要重置密码的用户 Administrator,再单击"更改密码"按钮,在弹出的对话框中输入两次新密码。此时,保存密码并重新启动,即可清除 SAM 文件中的旧密码并生成新密码,如图 3-3 所示。

图 3-3 使用 NTPWEdit 重置 Windows 用户密码


视频讲解

3.2.3 实验六:远程暴力破解 Windows 远程桌面用户登录密码

1. 实验目的

(1) 掌握使用 Hydra 工具远程暴力破解 Windows 远程桌面用户登录密码的方法。

(2) 掌握使用 Crunch 工具制作自定义规则的密码字典的方法。

(3) 掌握远程破解防范方法,体会口令强度的重要性。

2. 实验任务与要求

(1) 已知靶机用户名为 administrator,密码为 996,只需要对密码进行破解。因此,使用 Kali 上的 Crunch 工具制作密码字典,并了解有关命令的用法。例如,密码为 3 位数字组合,字典文件能够覆盖从 000,001,…,998,999 的字符串组合。

(2) 使用 Kali 上的 Hydra 工具,结合自制的密码字典,远程暴力破解 Windows 远程桌面用户登录密码。

3. 实验原理(技术)

(1) 远程桌面协议(Remote Desktop Protocol,RDP)是用于远程控制系统较流行的通信协议之一,适用于大多数 Windows 系统,通过提供图形用户界面,允许用户远程访问服务器或其他计算机。Windows 远程桌面连接使用 RDP 协议,默认使用 TCP 3389 端口。

(2) Hydra 是一款开源的暴力破解密码工具,在 Kali Linux 上是默认安装的,可以对多种网络服务的账号和密码进行远程暴力破解。Hydra 支持的网络服务或协议有 SMB、RDP、SSH、FTP、POP3、Telnet、MySQL 等。

(3) Crunch 是一个创建密码字典的工具,按照指定的规则生成密码字典。使用 Crunch 工具生成的密码可以输出到屏幕,保存到文件或另一个程序。密码字典强大到包含有正确的用户名和密码,是暴力破解成功的前提条件。

4. 实验仪器设备(环境条件)

(1) 攻击机。

虚拟机 VMware Workstation 15.5+Kali Linux 2021,网络连接使用 NAT 模式,IP 地址为 192.168.88.129/24。

(2) 靶机。

虚拟机+Windows 7,网络连接使用 NAT 模式,IP 地址为 192.168.88.130/24,用户名为 administrator,密码为 996。

5. 实验过程

1) 攻击前

(1) 确认靶机开启远程桌面服务。

在靶机上开启 Windows 远程桌面服务如图 3-4 所示。

图 3-4　在靶机上开启 Windows 远程桌面服务

(2) 使用 Crunch 制作口令字典文件。

在 Kali 中使用命令 crunch 3 3 1234567890 -o /usr/share/wordlists/digit3.txt,即可生成一个最短 3 位、最长 3 位且字符为全数字的 1000 个口令字典,即 000,001,…,998,999,其中包含正确的密码 996。输出的字典为/usr/share/wordlists/digit3.txt 文本文件,每个口令占一行,如图 3-5 所示。

图 3-5 使用 Crunch 制作口令字典文件

Crunch 的有关语法格式如下。

```
#crunch min-len max-len [ charset string ] [options]
```

Crunch 的几个重要参数如下。

- min-len,口令最短长度。
- max-len,口令最长长度。
- charset string,口令所选的字符集,该字符集可自定义,也可用 Crunch 自带的 charset.lst 文件,包含数字、大小写字母、特殊字符等,部分字符集如图 3-6 所示。
- -o,输出字典文件。

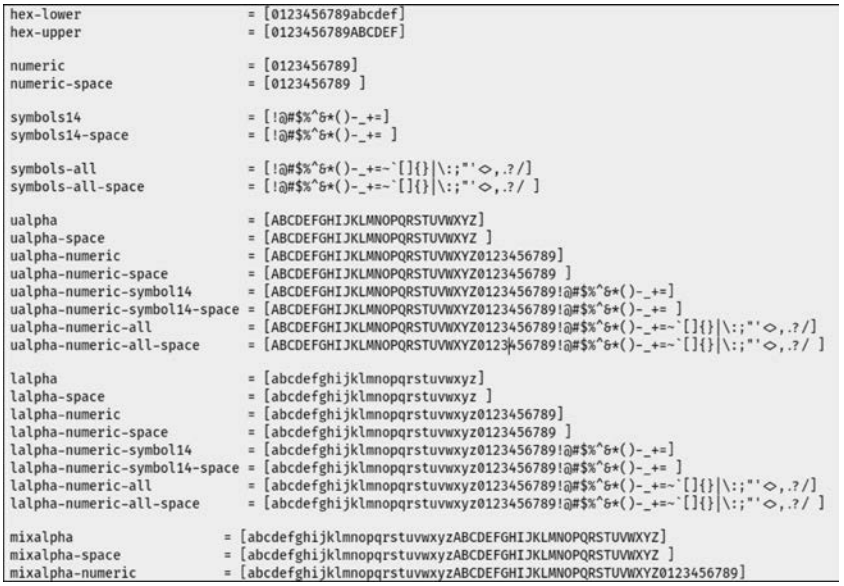
2) 攻击

(1) 使用 Hydra(命令行程序)进行暴力破解。

由于已知用户名是 administrator,因此只需要测试破解密码即可。使用命令 hydra 192.168.88.130 rdp -l administrator -P /usr/share/wordlists/digit3.txt -V,成功破解出正确密码 996,如图 3-7 所示。

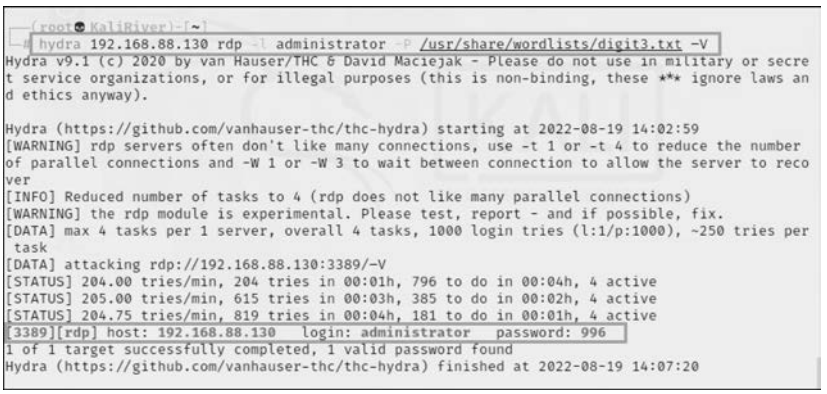
Hydra 的有关语法格式如下。

```
# hydra [[[ -l LOGIN| -L FILE] [ -p PASS| -P FILE]] | [ -C FILE]] [ -e ns]
[ -o FILE] [ -t TASKS] [ -M FILE [ -T TASKS]] [ -w TIME] [ -f] [ -s PORT] [ -S] [ -vV]
server service [OPT]
```



```
hex-lower                      = [0123456789abcdef]
hex-upper                      = [0123456789ABCDEF]

numeric                        = [0123456789]
numeric-space                  = [0123456789 ]

symbols14                      = [!@#$%^&*()-_+=]
symbols14-space                = [!@#$%^&*()-_+= ]

symbols-all                    = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
symbols-all-space              = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

ualpha                         = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
ualpha-space                   = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
ualpha-numeric                 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ualpha-numeric-space           = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
ualpha-numeric-symbol14        = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
ualpha-numeric-symbol14-space  = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+= ]
ualpha-numeric-all             = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
ualpha-numeric-all-space       = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

lalpha                         = [abcdefghijklmnopqrstuvwxyz]
lalpha-space                   = [abcdefghijklmnopqrstuvwxyz ]
lalpha-numeric                 = [abcdefghijklmnopqrstuvwxyz0123456789]
lalpha-numeric-space           = [abcdefghijklmnopqrstuvwxyz0123456789 ]
lalpha-numeric-symbol14        = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=]
lalpha-numeric-symbol14-space  = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+= ]
lalpha-numeric-all             = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
lalpha-numeric-all-space       = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

mixalpha                  = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]
mixalpha-space            = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ ]
mixalpha-numeric          = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
```

图 3-6　Crunch 自带的 charset.lst 文件部分内容



```
┌──(root💀KaliRiver)-[~]
└─# hydra 192.168.88.130 rdp -l administrator -P /usr/share/wordlists/digit3.txt -V
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secre
t service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-19 14:02:59
[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 reco
ver
[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 4 tasks per 1 server, overall 4 tasks, 1000 login tries (l:1/p:1000), ~250 tries per
 task
[DATA] attacking rdp://192.168.88.130:3389/-V
[STATUS] 204.00 tries/min, 204 tries in 00:01h, 796 to do in 00:04h, 4 active
[STATUS] 205.00 tries/min, 615 tries in 00:03h, 385 to do in 00:02h, 4 active
[STATUS] 204.75 tries/min, 819 tries in 00:04h, 181 to do in 00:01h, 4 active
[3389][rdp] host: 192.168.88.130   login: administrator   password: 996
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-19 14:07:20
```

图 3-7　使用 Hydra(命令行程序)对登录密码进行暴力破解

Hydra 的几个重要参数如下。

- server,目标 IP。
- -s < PORT >,使用非默认端口。
- -l < LOGIN >,指定特定用户名破解。
- -L < FILE >,加载用户名字典。
- -p < PASS >,指定特定密码破解。
- -P < FILE >,加载密码字典。
- -C < FILE >,使用冒号分隔格式“登录名:密码”来代替-L/-P 参数。
- -S,采用 SSL 链接。
- -o < FILE >,指定结果输出文件。
- -t < TASKS >,设置同时运行的线程数,默认为 16。
- -w < TIME >,设置最大超时时间,默认为 30s。

- -v/-V,显示详细过程。
- service,指定服务名。

例如,如果需要同时对用户名和密码进行暴力破解,可以先用 Crunch 创建一个用户名字典 user.txt,接着使用 Hydra 命令 hydra 192.168.88.130 rdp -L /usr/share/wordlists/user.txt -P /usr/share/wordlists/digit3.txt -V 进行破解。

(2) 使用 x-Hydra(图形化界面程序)进行暴力破解。

类似于 Hydra,在 x-Hydra 中也需要设置目标 IP、端口、协议类型、用户名来源、密码来源等,如图 3-8 所示。

(a) 设置目标IP、端口、协议类型　　(b) 设置用户名来源、密码来源

(c) 显示破解结果

图 3-8　使用 x-Hydra(图形化界面程序)对登录密码进行暴力破解

(3) 验证。

使用远程桌面程序连接靶机,如图 3-9 所示。

图 3-9　使用远程桌面程序连接靶机

3.2.4　实验七：对远程暴力破解 Windows 远程桌面用户口令的防御


视频讲解

1. 实验目的

(1) 掌握对远程暴力破解 Windows 远程桌面用户的防御方法。
(2) 体会口令强度的重要性。

2. 实验任务与要求

(1) 增强口令强度，并定期更换。
(2) 修改 Windows 远程桌面 RDP 默认端口。
(3) 添加安全策略，禁止 Administrator 账户远程登录，并锁定失败登录超阈值的账户。
(4) 设置 Windows 系统自带防火墙，限制远程来访 IP 地址。

3. 实验原理(技术)

(1) 暴力破解成功的一个前提条件是破解程序的口令字典强大到能覆盖正确的口令。理论上，只要口令字符串足够长和复杂，口令字典不能覆盖到该口令，就无法破解成功。即便是口令字典能覆盖该口令，由于破解时间足够长到大于口令定期更换的时间，口令破解成功也没有意义。

(2) Windows 远程桌面连接使用 RDP，默认使用 TCP 3389 端口。修改 RDP 默认端口为一个陌生端口后，NMAP 之类的扫描器可能扫描不出该端口，或者扫描出该端口后无法判断其服务类型，Hydra 之类的爆破工具也无法定位 RDP 使用的端口。

(3) 在 Windows 安全策略设置中，设置 Windows 远程桌面失败登录尝试次数的策略，防止被暴力破解。

(4) 在 Windows 系统自带防火墙，限制远程来访 IP 地址。

4. 实验仪器设备(环境条件)

(1) 攻击机。
虚拟机 VMware Workstation 15.5＋Kali Linux 2021，网络连接使用 NAT 模式。
(2) 靶机。
虚拟机＋Windows 7，网络连接使用 NAT 模式。

5. 实验过程

根据实验任务要求，完成以下 4 个任务，分别是：修改用户密码为强密码，将靶机的 RDP 默认端口 3389 修改成其他端口，添加安全策略以禁止 Administrator 账户远程登录和锁定失败登录超阈值的账户，开启防火墙以限制远程来访 IP 地址。下面依次通过实验实现以上 4 个任务。

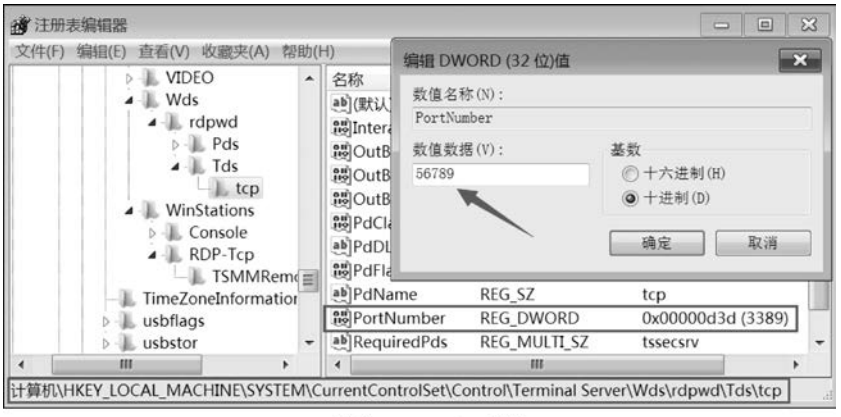
1) 修改用户密码为强密码
可将靶机中用户的密码修改为最长 14 位，同时包含大小写字母、数字和特殊字符。

2) 将靶机的 RDP 默认端口 3389 修改为其他端口

(1) 运行 cmd 命令,进入注册表编辑器,并查找如下两个路径。

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

找到两个 PortNumber 键进行编辑,均将其默认十进制端口号 3389 改为陌生端口号(如 56789),如图 3-10 所示。注意,此时需要重启靶机。



(a) 修改PortNumber键值1

(b) 修改PortNumber键值2

图 3-10 在注册表中修改 RDP 的两个 PortNumber 键值

在靶机中使用命令 netstat -ano 查看本地连接,状态是 LISTENING 的本地地址中出现 0.0.0.0:56789,如图 3-11 所示。端口修改前为 0.0.0.0:3389,可知修改完成。

注意,当 RDP 默认端口号修改后,使用远程桌面连接程序正常访问靶机时,需要在计算机名中输入“IP 地址:端口号”,如“192.168.88.130:56789”,否则不能正常连接。

(2) 使用 NMAP 扫描器试图扫描靶机 RDP 服务所用的 TCP 端口。

① 使用 NMAP 命令 nmap -sS 192.168.88.130 扫描靶机,由于 TCP 端口 56789 不是 NMAP 默认扫描的 1000 个常用端口之一,因此扫描不到 56789 端口开放。

② 使用 NMAP 命令 nmap -sS -p 1-65535 192.168.88.130 扫描靶机的所有 TCP 端

```
C:\Users\Administrator>netstat -ano

活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:4466           0.0.0.0:0              LISTENING       4068
  TCP    0.0.0.0:8908           0.0.0.0:0              LISTENING       4068
  TCP    0.0.0.0:56789          0.0.0.0:0              LISTENING       640
  TCP    127.0.0.1:61078        0.0.0.0:0              LISTENING       1560
  TCP    192.168.88.130:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.88.130:1038    106.11.40.57:80        CLOSE_WAIT      3184
  TCP    192.168.88.130:1096    106.11.43.246:80       CLOSE_WAIT      3064
```

图 3-11　在靶机中查看网络连接

口，能扫描到 56789 端口开放，但是显示该端口的 SERVICE 类型为 unknown，如图 3-12(a)所示。

③ 使用 NMAP 命令 nmap -sV -p 56789 192.168.88.130 只扫描靶机 TCP 端口 56789，但是显示该端口的 SERVICE 类型为 ssl/unknown，如图 3-12(b)所示。

```
┌──(root💀KaliRiver)-[~]
└─# nmap -sS -p 1-65535  192.168.88.130
Starting Nmap 7.91 ( https://nmap.org ) at
Nmap scan report for 192.168.88.130
Host is up (0.00066s latency).
Not shown: 65524 closed ports
PORT      STATE SERVICE
81/tcp    open  hosts2-ns
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
56789/tcp open  unknown
MAC Address: 00:0C:29:2C:70:1D (VMware)
```

(a) 显示端口类型为unknown

```
┌──(root💀KaliRiver)-[~]
└─# nmap -sV -p 56789  192.168.88.130
Starting Nmap 7.91 ( https://nmap.org ) at
Nmap scan report for 192.168.88.130
Host is up (0.00052s latency).

PORT      STATE SERVICE     VERSION
56789/tcp open  ssl/unknown
MAC Address: 00:0C:29:2C:70:1D (VMware)

Service detection performed. Please report
Nmap done: 1 IP address (1 host up) scanned
```

(b) 显示端口类型为ssl/unknown

图 3-12　使用 NMAP 扫描器扫描到 TCP56789 端口服务类型情况

将靶机的 RDP 默认端口 3389 修改为陌生端口 56789 后，避免了 NMAP 扫描器快速扫描到 3389 端口，增加了攻击者对陌生端口 56789 服务类型的判断难度。

3) 添加安全策略以禁止 Administrator 账户远程登录和锁定失败登录超阈值的账户

(1) 禁止 Administrator 账户远程登录。

当靶机上开启 Windows 远程桌面服务时，Administrator 账户是默认具有访问权的。禁止 Administrator 账户远程登录的目的有两个，一是避免攻击者直接对 Administrator 账户的密码进行暴力破解；二是锁定失败登录超阈值的账户策略仅对非 Administrator 账户有效。

在靶机中运行 gpedit.msc 组策略编辑器程序，依次选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”→“拒绝通过远程桌面服务登录”选项，双击编辑设置，添加 Administrator 用户，如图 3-13 所示。

(2) 对非 Administrator 账户设置账户锁定策略。

依次选择“计算机设置”→“Windows 设置”→“安全设置”→“账户策略”→“账户锁定策略”选项，其中有 3 项账户策略的默认设置，如图 3-14 所示。

图 3-13 禁止 Administrator 账户远程登录

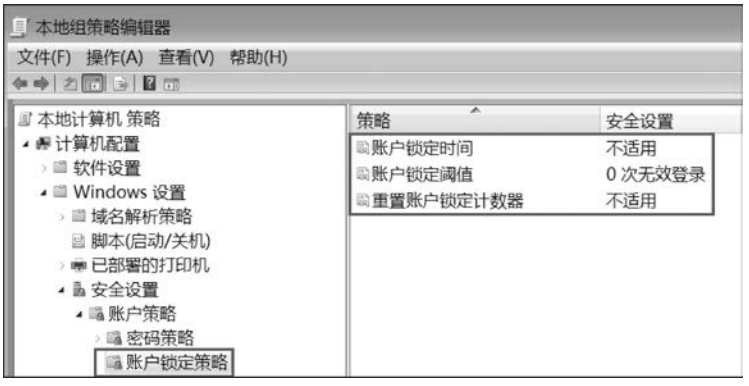


图 3-14 账户锁定策略默认设置

① 账户锁定时间：当用户错误登录次数达到账户锁定阈值后，在该时间段内会被锁定，直到自动解锁或由管理员重置。默认值是不适用。

② 账户锁定阈值：定义失败登录尝试次数的策略，将在账户锁定持续时间指定的某段时间内锁定账户。默认值是 0 次无效登录。

③ 重置账户锁定计数器：用于定义登录尝试失败后必须经过的时间段的策略，重置时间必须小于或等于账户锁定时间。默认值是不适用。

将账户锁定阈值修改为 3 次(一般为 10 次以内)无效登录，则系统提示账户锁定时间会被改为建议值 30 分钟，重置账户锁定计数器会被改为建议值 30 分钟之后，如图 3-15 所示。此时，保存设置并重启靶机。

(3) 添加新用户。

在靶机中添加一个新用户 douniwan，默认是隶属于 Users 组，必要时可以将其设置为隶属于 Administrators 组，则该用户也自动具有远程登录权限，如图 3-16 所示。

(4) 验证新用户多次错误登录并被锁定。

douniwan 用户无论是直接本地登录、远程桌面登录，还是 Hydra 远程爆破，只要密码错误次数达到 3 次，再次登录该账户都会被锁定 30 分钟。以前两种方式为例，账户被锁定时如图 3-17 所示。

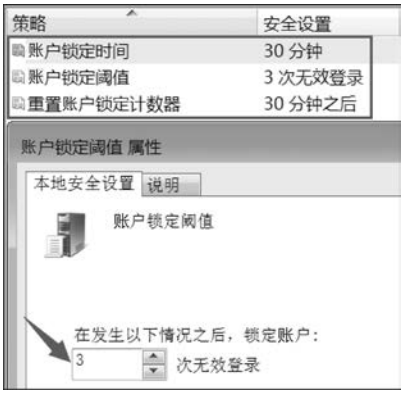


图 3-15　账户锁定策略自定义设置

图 3-16　添加新用户并设置隶属于 Administrators 组

图 3-17　账户被锁定

4）靶机开启 Windows 防火墙并限制远程来访 IP 地址

（1）在靶机中查看本地连接使用的网络类型。

在 Windows 7 中有 3 种网络类型，分别是家庭网络、工作网络和公用网络，在系统中可自行根据安全需要设置。在网络属性中，查看到靶机目前是公用网络类型，如图 3-18 所示。

图 3-18　查看靶机的网络类型

（2）在靶机中开启 Windows 防火墙。

在 Windows 防火墙中，对公用网络启用防火墙，设置程序或功能通过 Windows 防火墙，确保“远程桌面”在可通过程序的列表中被选中，网络是“公用”，如图 3-19 所示。如果“远程桌面”不在列表中，可单击“允许运行另一程序”按钮，找到远程桌面的程序文件 mstsc. exe，路径默认是 C:\Windows\System32。

（3）在靶机中添加入站规则并允许端口 56789 能被正常地远程访问。

单击 Windows 防火墙的“高级设置”菜单，再依次单击“入站规则”“新建规则”选项，选择规则类型为“端口”，如图 3-20 所示。

然后在协议和端口中选择 TCP 端口，在特定本地端口中输入 56789，并保持默认选择允许连接，如图 3-21 所示。

接着应用规则到公用网络，再将规则命名为“56789 端口入站”，如图 3-22 所示。

(a) 启用Windows防火墙　(b) 允许程序或功能通过Windows防火墙

(c) 允许运行另一程序

图 3-19　开启 Windows 防火墙并允许远程桌面程序通过

图 3-20　Windows 防火墙新建入站规则

(a) 设置TCP端口及特定本地端口　　(b) 选择允许连接

图 3-21　在 Windows 防火墙新建入站规则中设定端口号和连接操作

(a) 选择公用网络　　(b) 命名规则

图 3-22　Windows 防火墙新建入站规则作用到公用网络及命名

完成以上操作后，在实体机 Windows 中使用远程桌面程序连接到靶机，输入 IP 地址和端口号 192.168.88.130:56789，输入用户名 douniwan 和密码 996，可以正常远程登录，如图 3-23 所示。

(a) 进行远程桌面连接　　(b) 显示远程桌面连接

图 3-23　开启 Windows 防火墙时正常远程桌面连接访问

(4) 在靶机中添加入站规则并限制来访 IP 地址。

限制来访 IP 地址既可以是正常远程桌面连接的来访 IP 地址，也可以是暴力破解者的来访 IP 地址。以前者为例，已知实体机 Windows 系统 IP 地址为 192.168.2.10/24，在图 3-23 中可以正常远程桌面连接访问。此时在入站规则中，设置 56789 端口的白名单 IP 地址中不包含单个 IP192.168.2.10 或 IP 段 192.168.2.10/24，实体机就无法正常访问了。

双击图 3-22 中已创建的规则“56789 端口入站”,单击选项卡“作用域”,出现“本地 IP 地址”“远程 IP 地址”两个选项框。由于实体机 IP 地址 192.168.2.10/24 与靶机 IP 地址 192.168.88.130/24 属于不同网段,因此选择“远程 IP 地址”类型中的“下列 IP 地址”,添加一个不同网段的且允许来访的 IP 地址作为白名单,如 222.222.222.222,即可将实体机排除在外,如图 3-24 所示。

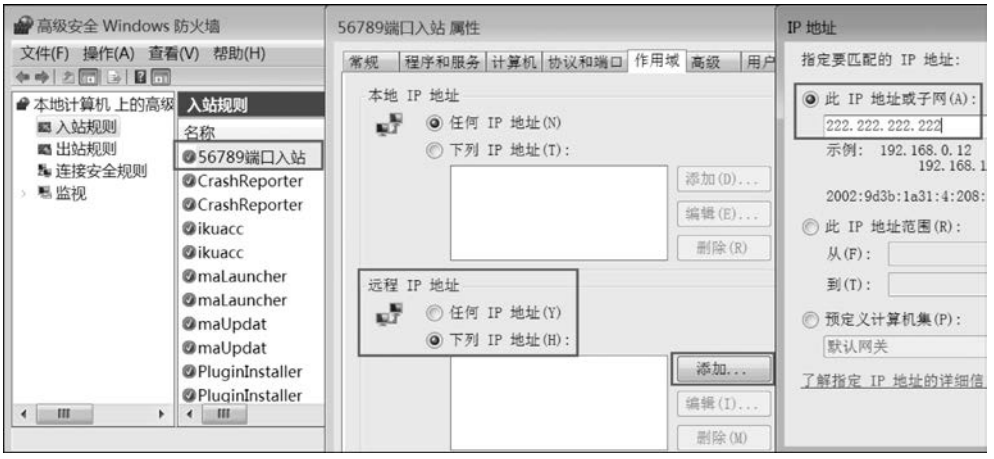


图 3-24 开启 Windows 防火墙时对远程 IP 地址开启白名单

再次从实体机 Windows 中使用远程桌面程序连接靶机,等待片刻之后一直无法切换到输入用户名和密码的界面,此时提示无法连接,如图 3-25 所示。

图 3-25 在实体机 Windows 中使用远程桌面程序无法连接靶机

继续验证对攻击机 Kali 系统限制来访,由于 Kali 系统 IP 地址 192.168.88.128/24 与靶机 IP 地址 192.168.88.130/24 属于同一网段,因此在“本地 IP 地址”中添加一个本地网段的且允许来访的 IP 地址作为白名单,如 192.168.88.88,即可将攻击机的 IP 地址排除在外,如图 3-26 所示。

再次在 Kali 系统中使用 Hydra 命令 hydra 192.168.88.130 rdp -s 56789 -l douniwan -P/usr/share/wordlists/digit3.txt -v 进行暴力破解,其中用-s 参数指定端口 56789,-l 参数指定用户名 douniwan。Hydra 命令运行结果不断提示“[ERROR] freerdp: The connection failed to establish.”,可知无法建立连接,如图 3-27 所示。

图 3-26　开启 Windows 防火墙时对本地 IP 地址开启白名单

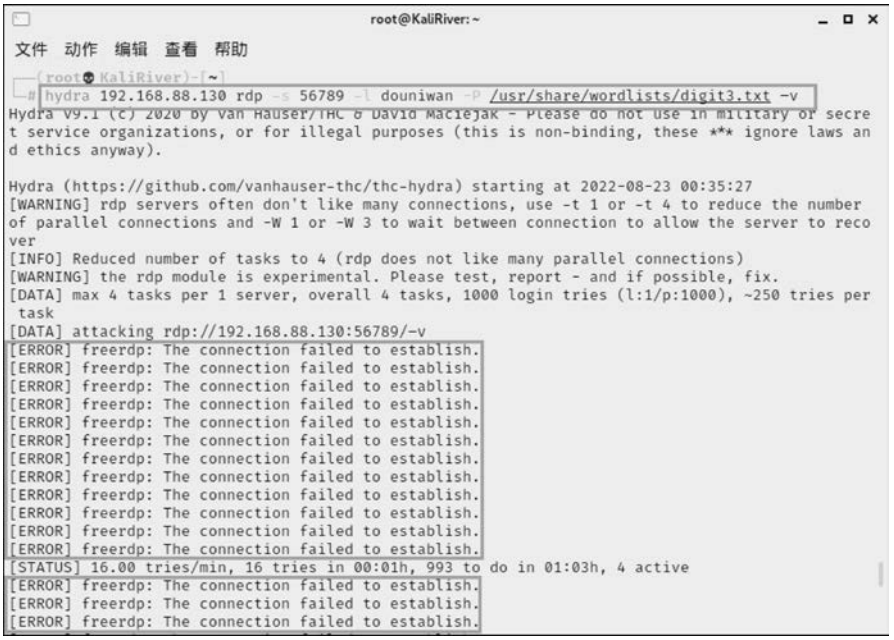


图 3-27　在攻击机 Kali 中使用 Hydra 命令无法连接靶机

(5) 思考。

① 使用安全策略锁定失败登录超阈值的账户，与通过防火墙限制远程来访 IP 地址相比较，两种方法的原理差异在哪里？哪种方法对暴力攻击的防护效果更好？

② 本实验针对远程暴力破解攻击的 4 种防御方法，如果以从外到内的防御层次来划分，4 种防御方法可以如何排序？理由是什么？

3.3　本章小结

本章介绍了有关口令的概念，包括动态口令与静态口令、口令攻击与防御的方法，并介绍了从本地及远程对 Windows 口令破解的案例。

实验五介绍了采用离线方式本地破解 Windows 用户口令,读取硬盘上的 Widnows 系统的口令 SAM 文件并重置新口令。对应的防御方法比较有限,毕竟能够离线读取硬盘文件,保护口令 SAM 文件的意义并不大。

实验六介绍了通过远程在线远程暴力破解 Windows 远程桌面用户登录密码,采用了爆破工具 Hydra 及字典工具 Crunch。暴力破解成功的一个前提是口令字典强大到能覆盖正确口令。除了 RDP 外,Hydra 还能在线爆破许多网络协议或服务。另外,Crunch 还能创建非常强大和灵活的自定义规则字典,有兴趣的读者可多研究实践。

实验七介绍了对远程暴力破解 Windows 远程桌面用户的防御的 4 种方法,其中设置强口令是最后一道防线。读者可体会到 4 种防御方法的效果及优劣各有不同。

除介绍口令的技术及实践外,本章更多的是启示读者需要从管理和人为角度去重视防御,如避免弱口令、定期更换口令、避免多个系统使用同一个口令、如何防范从社会工程学角度对口令的攻击等。


在线测试

3.4 习题

一、选择题

1.(　　)是最简单和成本最低的身份认证方式。

A. 口令　　B. 指纹识别　　C. 人脸识别　　D. 虹膜识别

2.(　　)口令是指用户登录系统的口令是在注册时一次性产生的,在下一次用户修改之前的使用过程中总是固定不变的。

A. 静态　　B. 动态　　C. Windows　　D. Linux

3.(　　)攻击一般是指对存储口令的文件或数据库载体进行攻击。

A. 离线　　B. 在线　　C. 弱口令　　D. 字典

4.(　　)攻击是指攻击者一般通过网络访问常规的系统登录入口、模拟入口或非常规入口攻击用户口令。

A. 离线　　B. 在线　　C. 弱口令　　D. 字典

5. 设置同时带有大小写字母、数字、特殊字符组合的口令是为了防止(　　)攻击。

A. 离线　　B. 在线　　C. 弱口令　　D. 字典

6.(　　)悖论的一个结论是只要一个班里超过 23 个人,那么找到同一天出生的两个人的概率就大于 1/2。

A. 组播　　B. 生日　　C. 单播　　D. 混杂

7. 8 位数字全排列是 6 位数字全排列的(　　)倍。

A. 2　　B. 10　　C. 100　　D. 1000

8. 在原始口令明文基础上附加了固定字符串或随机字符串后生成的哈希值,附加的字符串又称为(　　),此方法可以更好地抵抗对口令的暴力攻击。

A. 柴　　B. 米　　C. 油　　D. 盐

9. 登录密码在数据库中常用哈希值存储,(　　)算法的哈希值安全性最高。

A. MD5　　B. SHA-1　　C. SHA-256　　D. SHA-512

10. Windows 10 系统的口令 SAM 文件采用了(　　)散列算法。

A. LM　　B. NTLM　　C. RSA　　D. ECC

二、判断题

1. 出于安全考虑,口令修改的间隔时间应小于口令破解成功所花费的时间。　(　　)

2. 暴力(穷举)攻击的口令来源必须来自字典,不能程序自动化生成。　(　　)

3. 发生哈希函数碰撞的概率不可能为零。　(　　)

4. Windows 远程桌面连接使用 RDP。　(　　)

5. 修改了 Windows 远程桌面服务默认端口后就一定不会被扫描识别出服务。(　　)

6. 对 Windows 系统口令进行离线攻击的方法是将口令 SAM 文件中的哈希值恢复为明文。　(　　)

7. 当 Windows 系统运行时,口令 SAM 文件会被锁定,以防止被从文件层面破解。　(　　)

8. Windows 远程桌面连接服务的开启或关闭,不能通过修改注册表方式实现。　(　　)

9. 在 Windows 中,锁定失败登录次数超阈值的账户的方法是添加安全策略。　(　　)

10. 在 Windows 自带防火墙的规则中,对远程 IP 地址可使用白名单而不是黑名单。　(　　)