**扫描技术**

一个一个ping？

手工与工具相结合

主机探测与端口扫描

主机测探是指确定目标主机是否存活。

端口扫描就是寻找在线主机所开放的端口，并且在端口上所运行的服务。甚至可以进一步确定目标主机操作系统类型和更详细的信息

- 基础知识

@ 常见端口号

|  |  |  |  |
| --- | --- | --- | --- |
| 21 | FTP | 443 | HTTPS |
| 22 | SSH | 1433 | SQL Server |
| 23 | Telnet | 1521 | Oracle |
| 25 | SMTP | 3306 | MySQL |
| 80 | HTTP | 3389 | RDP |

- Nmap-扫描器之王

- 重要常用参数

|  |  |
| --- | --- |
| -sP | ping 扫描 |
| -p | 指定端口范围 |
| -sV | 服务版本探测 |
| -O（大写） | 启用操作系统探测 |
| -A | 全面扫描 |
| -oN | 保存txt |

Nmap -sP 10.1.1.1/24 扫描10.1.1.0整个网段

Nmap -p 21,23-25,3389 10.1.1.1

Nmap -p 21,23 10.1.1.1 -sV 扫描21,23的服务版本

Nmap -A 10.1.1.1 全面扫描

Nmap -O 10.1.1.1 扫描目标系统版本

Namp -p 21,23 10.1.1.1 -oN e:\result.txt

九头蛇

Hydra -l a -p 123 10.1.1.1 telnet

Hydra -l a -P e:\pass.txt 10.1.1.1 telnet

Hydra -l a -P e:\pass.txt 10.1.1.1 rdp

Hydra -l a -P e:\pass.txt 10.1.1.1 smb

Hydra -l a -P e:\pass.txt 10.1.1.1 ftp

Hydra -l a -P e:\pass.txt 10.1.1.1 ssh

Hydra -l a -P e:\pass.txt 10.1.1.1 mysql

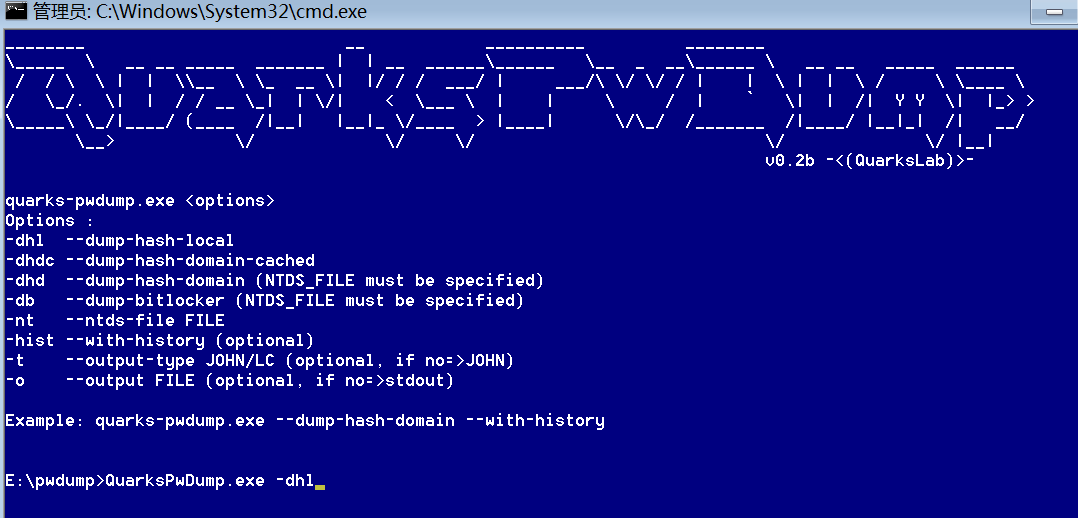
Hydra -L e:\user.txt -P e:\pass.txt 10.1.1.1 telnet

本地破解

Getpass 从内存中提取密码

本地暴力破解：

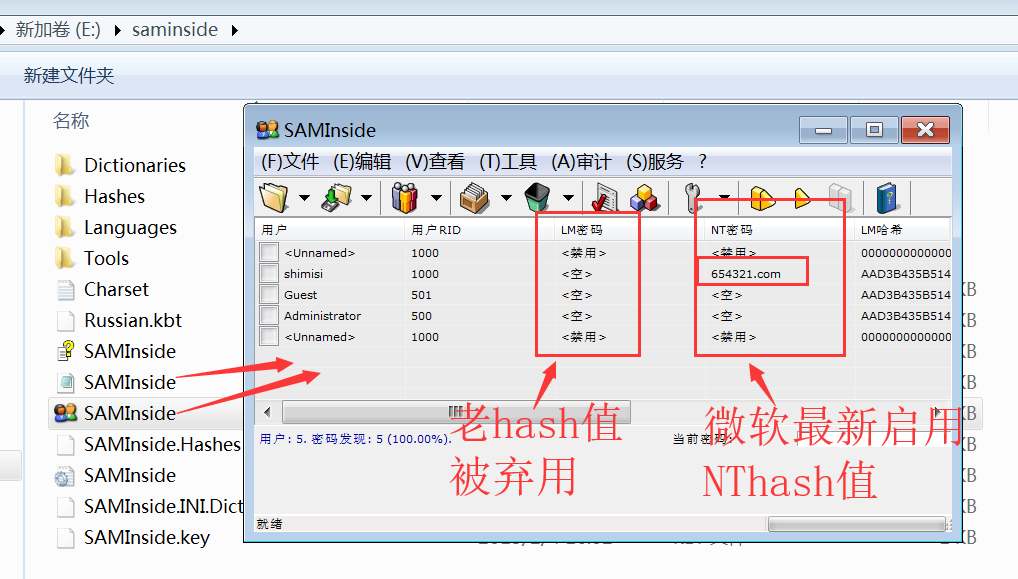
Pwdump 提取sam中的HASH值



手工将hash值存储到hash.txt中

使用saminside软件进行hash暴力破解





实验1：

在真实机上使用nmap及hydra对虚拟机2003做扫描及爆破（对FTP、telnet、rdp、smb）

实验2：

在win7或2003中虚拟机中。练习本地系统密码爆破