running under Perl version 5.24.1.

格式: enum4linux.pl [-OPTIONS [-MORE\_OPTIONS]] [--] [PROGRAM\_ARG1 ...]

以下的单字符选项被接受：:

详细参数: -u -p -f -R -s -k -w -K

Boolean (如果没有参数): -U -M -N -S -P -G -l -L -D -d -r -v -o -h -n -a -i -P

选项可以合并在一起。 -- stops processing of options.

选项和它们之间的参数之间不需要空格。

[Now continuing due to backward compatibility and excessive paranoia.

See 'perldoc Getopt::Std' about $Getopt::Std::STANDARD\_HELP\_VERSION.]

enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)

Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar

functionality to enum.exe (formerly from www.bindview.com). Some additional

features such as RID cycling have also been added for convenience.

格式: ./enum4linux.pl [options] ip

选项 例如 (like "枚举"):

-U 得到用户列表

-M 获得机器列表

-S 得到sharelist

-P 获取密码策略信息

-G 获取组和成员列表

-d 显示更详细的数据 -U and -S

-u user 指定要使用的账户 (default "")

-p pass 指定要使用的密码(default "")

下列选项enum.exe不实施: -L, -N, -D, -f

附加选项:

-a 做所有简单的枚举 (-U -S -G -P -r -o -n -i).

这的确是如果你不提供任何其他选项。

-h 显示此帮助信息和退出

-r 枚举用户通过清除循环

-R range 排除范围枚举(默认: 500-550,1000-1050, implies -r)

-K n 继续寻找直到n个肋肋不对应的用户名。范围必须会摆脱999999点结束。对DCs有用。

-l 得到一些（有限的）通过LDAP 389 / TCP信息（DCS只）

-s file 共享名称的蛮力猜测

-k user 用户（S）存在于远程系统（默认管理员，客人krbtgt，域管理员，根，本，没有）

Used to get sid with "lookupsid known\_username"

Use commas to try several users: "-k admin,user1,user2"

-o 获取操作系统信息

-i 获取打印机信息

-w wrkg 手动指定的工作组（通常是自动的）

-n 做一个nmblookup（类似NBTSTAT）

-v Verbose. 节目全是运行命令 (net, rpcclient, etc.)

RID cycling should extract a list of users from Windows (or Samba) hosts

which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network

access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba服务器通常都可在范围3000-3050。

相关信息：你需要Samba软件包安装此脚本只是包裹rpcclient，净，nmblookup和命令。从http://labs.portcullis.co.uk/ polenum应用/ polenum /需要密码策略信息。