Ncrack 0.5 ( http://ncrack.org )

语法: ncrack [Options] {target and service specification}

TARGET SPECIFICATION:

可以通过主机名称, IP 地址, 网络, 等.

举例: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iX <inputfilename>: Input from Nmap's -oX XML格式输出

-iN <inputfilename>: Input from Nmap's -oN Normal格式输出

-iL <inputfilename>: Input from list of hosts/networks

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude\_file>: Exclude list from file

服务规范:

可以通过目标特定的服务 <service>://target (standard) 符号或使用-将适用于所有的主机在非标准符号。

服务参数可以指定为主机特定的、特定类型的服务（- M）或全局（- G）。例如：SSH：/ / 10.0.0.10，= 10，= 30 M CL SSH：= 50克= 3000 CD EX2：Ncrack P SSH，FTP：3500,25 10.0.0.10 Scanme.nmap.org谷歌网站：80、SSL

-p <service-list>: 将适用于所有的非标准符号主机

-m <service>:<options>: 选项将被应用到这种类型的所有服务

-g <options>: 选项将被应用到全球的每一个服务

根据其选项:

ssl: 在这个服务启用SSL

path <name>: 使用HTTP（“=”模块需要转义如果使用）

定时和性能:

选择以<时间>是以秒来计算的，除非你把'小姐'（毫秒），M（分钟），或“H”（小时）的值（如30m）。

服务选项:

cl (min connection limit): 并行并行连接的最小数目

CL (max connection limit): 并行并行连接的最大数目

at (authentication tries): 每个连接的验证尝试

cd (connection delay): 在每个连接开始之间延迟<时间>

cr (connection retries): 服务连接尝试的数量上限

to (time-out): 为服务最大破解时间>，无论到目前为止的成功

-T<0-5>: 设置时间模板（更高更快）

--connection-limit <number>: 总并发连接的阈值

认证:

-U <filename>: 用户名文件

-P <filename>: 密码文件

--user <username\_list>: 逗号分隔的用户名列表

--pass <password\_list>: 逗号分隔的密码列表

--passwords-first: 迭代每个用户名密码列表。默认是相反的.

--pairwise: 选择对的用户名和密码.

OUTPUT:

-oN/-oX <file>:在正常和XML格式的输出扫描，分别到给定的文件名.

-oA <basename>:在两个主要格式输出一次

-v: 增加的详细程度（使用两次或更多更大的影响）

-d[level]: 设置或增加调试级别（高达10是有意义的）

--nsock-trace <level>: 设置 nsock 查找级别 (有效范围: 0 - 10)

--log-errors:日志错误/警告到正常格式输出文件

--append-output:附加到指定的输出文件，而不是乱码

MISC:

--resume <file>: 继续先前保存的会话

--save <file>:具有特定文件名的保存恢复文件

-f: 在找到凭据后退出破解服务

-6: 启用IPv6开裂

-sL or --list: 只列出主机和服务

--datadir <dirname>:指定自定义Ncrack数据文件的位置

--proxy <type://proxy:port>: Make connections via socks4, 4a, http.

-V: 打印版本号

-h: 打印此帮助汇总页.

支持的爆破服务:

FTP, SSH, Telnet, HTTP(S), POP3(S), SMB, RDP, VNC, SIP, Redis, PostgreSQL, MySQL

举例:

ncrack -v --user root localhost:22

ncrack -v -T5 https://192.168.0.1

ncrack -v -iX ~/nmap.xml -g CL=5,to=1h

SEE THE MAN PAGE (http://nmap.org/ncrack/man.html) FOR MORE OPTIONS AND EXAMPLES