unicornscan (version 0.4.7)

用法: unicornscan [选项`b:B:cd:De:EFG:hHi:Ij:l:L:m:M:o:p:P:q:Qr:R:s:St:T:u:Uw:W:vVzZ:' ] X.X.X.X/YY:S-E

-b, --broken-crc 设置断的 crc sums 到 [T]运输层， [N]Etwork层， 或到两个层[TN]

-B, --source-port 设置源端口?

-c, --proc-duplicates 过程重复的回答

-d, --delay-type 设置延时型 (数值；,有效的选项是1:tsc 2:gtod 3:sleep')

-D, --no-defpayload 没有默认有效负载， 只有探索已知的协议

-e, --enable-module 启用当前列为参数的模块（输出和报告）

-E, --proc-errors 处理`非公开的反应（ICMP错误，TCP RST…）

-F, --try-frags

-G, --payload-group 有效载荷组（数字）为TCP / UDP类型负载的选择（默认）

-h, --help 帮助

-H, --do-dns 在报告期解析主机名

-i, --interface 接口名字

-I, --immediate 快速方式；,立刻显示我们已经发现的东西

-j, --ignore-seq 忽视All, 复位TCP头验证序列号

-l, --logfile 写这个不是我们终端的文件

-L, --packet-timeout 等待回响的时间

-m, --mode

扫描模式，扫描是默认的TCP（SYN），U为UDP ，T为 TCP ，sf 为tcp 对于-mT你也可以指定TCP标志，就像-mTsFpU 一样

这将发送TCP SYN包（NO Syn|FIN|NO Push|URG)

-M, --module-dir 目录模块被发现在(默认是在/usr/lib/unicornscan/modules)

-o, --format 要显示的答复的格式， 查看格式规范的man page

-p, --ports 全局端口扫描，如果没有在目标选项中指定

-P, --pcap-filter 对于接收额外的PCAP筛选器字符串

-q, --covertness 从0到255的隐蔽性价值

-Q, --quiet 不要用输出到屏幕，它会去别的地方（一个数据库说…）

-r, --pps 每第二个数据包（总的，不是每台主机，当你走的更高，它得到的不准确）

-R, --repeats \*重复数据包扫描N次

-s, --source-addr \*随机数据包的源地址

-S, --no-shuffle 不要打乱端口号

-t, --ip-ttl \*设置TTL对发送的数据包为62或6或r64-128

-T, --ip-tos \*设置TOS对发送的数据包

-u, --debug debug掩码

-U, --no-openclosed 不要说打开或关闭

-w, --safefile \*把收到的数据包PCAP文件

-W, --fingerprint \*操作系统指纹 0=cisco(def) 1=openbsd 2=WindowsXP 3=p0fsendsyn 4=FreeBSD 5=nmap

6=linux 7:strangetcp

-v, --verbose verbose (each time more verbose so -vvvvv is really verbose)

-V, --version 显示版本

-z, --sniff 像sniff一样

-Z, --drone-str drone 字符串

\*: 选项与“\*”需要一个参数跟踪他们

地址范围是CIDR像 1.2.3.4/8 for all of 1.?.?.?

如果你省略 the cidr 掩码 然后/32 暗示

端口范围是1-4096 53只扫描一个端口，对所有65K，P为1-1024

例如: unicornscan -i eth1 -Ir 160 -E 192.168.1.0/24:1-4000 gateway:a