

# NBTscan

NBTscan是一个扫描网络或域名信息的一个程序，他可以向你提供的一写列表中的每个地址或范围之中发送NetBIOS状态查询。最主要的是他可以以人类可读的形式进行输出，并且只要是响应的主机都会列出IP地址、网络基本输出系统计算机名，登入用户名、媒体访问控制地址（比如以太网）在NBTscan终端之中。

——*ribertomota*

---

## 一，前期知识

### NetBlos(Network Basic Input/Output System)

由IBM和Sytec联合开发，主要用于数十台计算机的小型局域网。系统可基于NetBlos获取计算机名称和解析响应的IP地址。以实现实时通信，在局域网内部中使用NetBlos协议可以方便的实现消息通信及资源共享。

而正是因为NetBlos他占用系统资源较小，传输效率高，所以几乎所有的局域网都是在NetBlos协议基础上工作的。

### lmhosts

lmhosts是用于进行NetBlos名解析的，将NetBlos名和IP地址进行对应。与其类似的是DNS，不过DNS是将域名、主机、IP三者对应。

## 二，帮助手册

“人类可读的服务名称”(-h) 选项不能在详细(-v)选项的情况下使用。

使用：

```
nbtscan [-v] [-d] [-e] [-l] [-t 超时] [-b 带宽] [-r] [-q] [-s 分离器] [-m 重新传输] [-f 文件名](<扫描范围>)
```

-v 详细输出。打印从每个主机收到的所有名称

-d 转储数据包。打印整包内容。

-e 以/etc/hosts格式格式化输出。

-l 以lmhosts格式格式化输出。不能与-v、-s或-h选项一起使用。

-t 时间 等待响应超时毫秒数，默认值为1000。

-b 带宽 输出节流。降低输出速度，这样它就不会占用更多的带宽。对慢速链接很有用，这样你的查询就不会被删除。

-r 使用本地端口137进行扫描。Win95 boxes仅对此做出响应。  
-q 隐藏横幅和错误消息，  
-s 分离器 脚本友好的输出。不要打印列和记录标题，用分隔符分隔字段。  
-h 为服务打印人类可读的名称。只能与-v选项一起使用。  
-m 重新传输 重传次数。默认值0。

-f 文件名称 从文件文件中获取要扫描的IP地址。-f -使NBT可以从标准输入中获取IP地址。

<scan\_range> 扫描什么。可以是单个IP，如192.168.1.1或 两种形式之一的地址范围:xxx.xxx.xxx.xxx/xx或xxx.xxx.xxx.xxx-xxx。

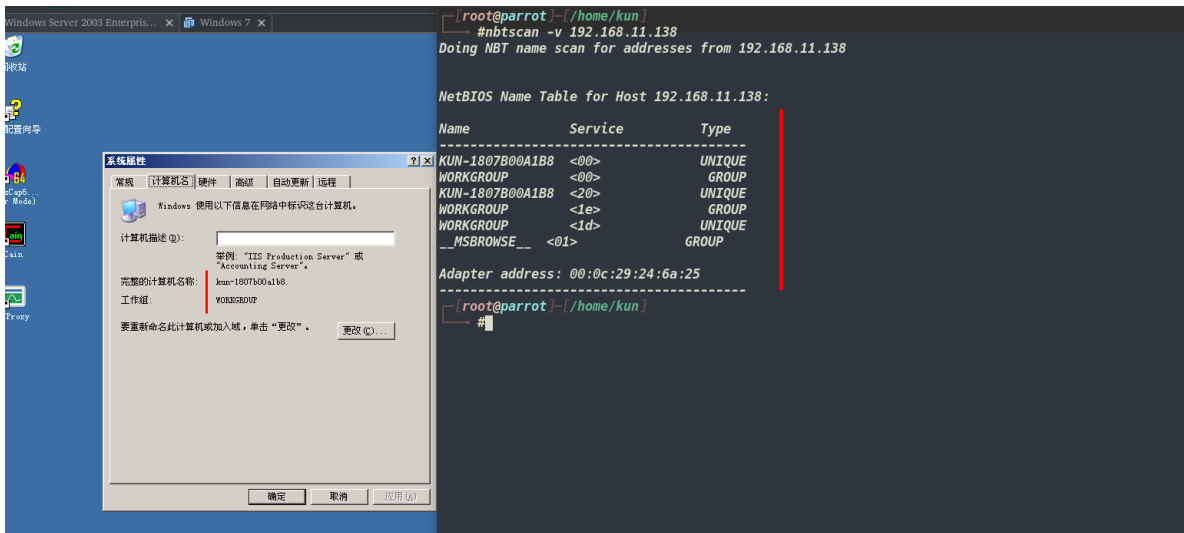
"Human-readable service names" (-h) option cannot be used without verbose (-v) option.  
Usage:  
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m retransmits] (-f filename)|(<scan\_range>)

-v	verbose output. Print all names received from each host
-d	dump packets. Print whole packet contents.
-e	Format output in /etc/hosts format.
-l	Format output in lmhosts format.
	Cannot be used with -v, -s or -h options.
-t timeout	wait timeout milliseconds for response. Default 1000.
-b bandwidth	Output throttling. Slow down output so that it uses no more than bandwidth bps. Useful on slow links, so that outgoing queries don't get dropped.
-r	use local port 137 for scans. Win95 boxes respond to this only. You need to be root to use this option on Unix.
-q	Suppress banners and error messages,
-s separator	Script-friendly output. Don't print column and record headers, separate fields with separator.
-h	Print human-readable names for services. Can only be used with -v option.
-m retransmits	Number of retransmits. Default 0.
-f filename	Take IP addresses to scan from file filename. -f - makes nbtscan take IP addresses from stdin.
<scan_range>	what to scan. Can either be single IP like 192.168.1.1 or range of addresses in one of two forms: xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.

### 三，命令实例

nbtscan -v 192.168.11.138

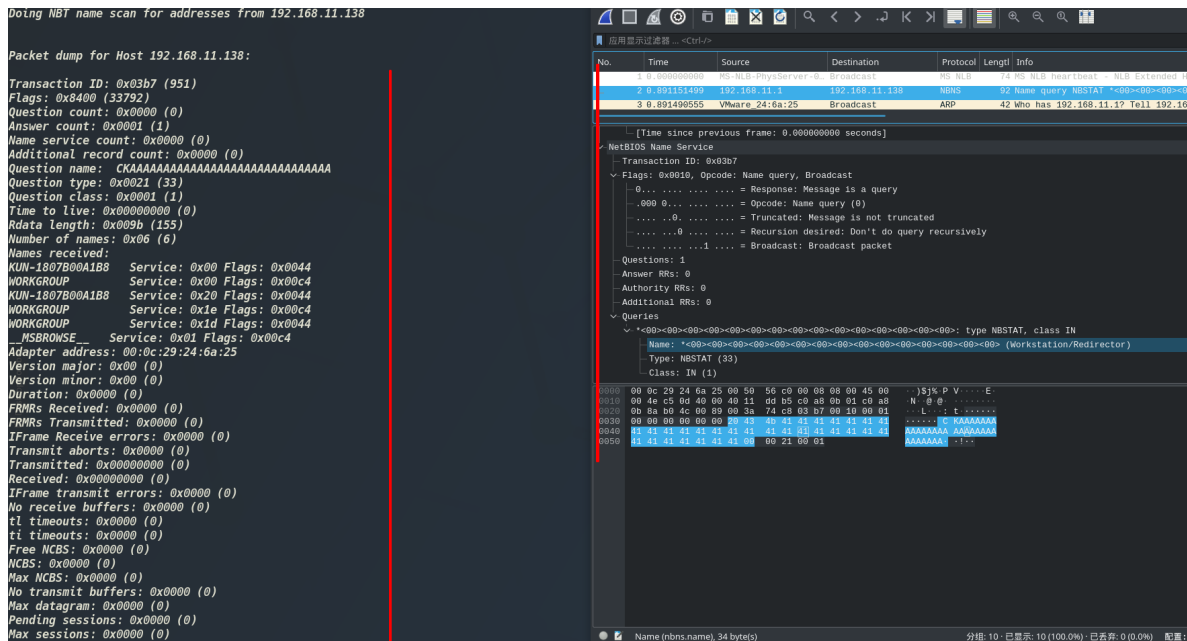
详细打印出对方主机名称及工作组信息



nbtscan -d 192.168.11.138

将数据包信息转储到NBTscan终端之中

结果包括MAC地址，从转储信息中可知对方MAC地址为：00:0c:29:24:6a:25



nbtscan -e 192.168.11.138

以IP和主机名（Eth/host）格式进行输出



Imhosts

Imhosts是用于进行NetBlos名解析的，将NetBlos名和IP地址进行对应。与其类似的是DNS，不过DNS是将域名、主机、IP三者对应。

nbtscan -l 192.168.11.138

以Imhosts格式进行输出

```
[root@parrot]# nbtscan -l 192.168.11.138
192.168.11.138 KUN-1807B00A1B8 #PRE
```

nbtscan -t 1 192.168.11.138

将响应等待值设置为1s，默认为1000s

```
[root@parrot]# nbtscan -t 1 192.168.11.138
Doing NBT name scan for addresses from 192.168.11.138

IP address      NetBIOS Name    Server  User      MAC address
-----
192.168.11.138  KUN-1807B00A1B8 <server> <unknown> 00:0c:29:24:6a:25
```

nbtscan -b 240 192.168.11.138

设置输出节流为240(调整输出的速度，降低流量输出以减少占用资源)

```
[root@parrot]# nbtscan -b 240 192.168.11.138
Doing NBT name scan for addresses from 192.168.11.138

IP address      NetBIOS Name    Server  User      MAC address
-----
192.168.11.138  KUN-1807B00A1B8 <server> <unknown> 00:0c:29:24:6a:25
```

nbtscan -t 137 192.168.11.138

使用137端口对目标进行扫描 (Win95 boxes仅对此做出响应)

```
[root@parrot]# nbtscan -t 137 192.168.11.138
Doing NBT name scan for addresses from 192.168.11.138

IP address      NetBIOS Name    Server  User      MAC address
-----
192.168.11.138  KUN-1807B00A1B8 <server> <unknown> 00:0c:29:24:6a:25
```

nbtscan -q 192.168.11.138

不输出错误信息和横幅

```
[root@parrot]# nbtscan -q 192.168.11.138
192.168.11.138 KUN-1807B00A1B8 <server> <unknown> 00:0c:29:24:6a:25
```

nbtscan -s ~~~~~ 192.168.11.138

设置分割符号

```
[root@parrot]# nbtscan -s ~~~~~ 192.168.11.138
192.168.11.138 ~~~~~KUN-1807B00A1B8~~~~~<server>~~~~~<unknown>~~~~~00:0c:29:24:6a:25
```

nbtscan -v -h 192.168.11.138

输出为更可读的信息 (需与 `-v` 一起使用)

```
#nbtscan -v -h 192.168.11.138
Doing NBT name scan for addresses from 192.168.11.138

NetBIOS Name Table for Host 192.168.11.138:

Name                Service              Type
-----
KUN-1807B00A1B8     Workstation Service
WORKGROUP           Domain Name
KUN-1807B00A1B8     File Server Service
WORKGROUP           Browser Service Elections
WORKGROUP           Master Browser
__MSBROWSE__        Master Browser

Adapter address: 00:0c:29:24:6a:25
```

nbtscan -m 2 192.168.11.138

设置数据包重传数为2，默认为0

6	11.973452899	IntelCor_c0:fb:07	Tp-LinkT_ed:2b:ae	ARP	42	192.168.0.105 is at 1c:1b:b5:c0:fb
7	13.815049902	192.168.0.1	192.168.0.255	UDP	157	1024 - 5001 Len=115
8	16.244637495	192.168.0.105	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1
9	17.245951827	192.168.0.105	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1
10	18.017718753	Tp-LinkT_ed:2b:ae	Broadcast	ARP	42	Who has 192.168.0.102? Tell 192.168.0.105
11	18.247284133	192.168.0.105	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1

nbtscan -f 201

从文件中抽取IP地址并进行枚举

```
[root@parrot]~[/home/kun]
#nbtscan -f 201
Doing NBT name scan for addresses from 201

IP address      NetBIOS Name      Server      User      MAC address
-----
192.168.11.138  KUN-1807B00A1B8   <server>    <unknown> 00:0c:29:24:6a:25

[root@parrot]~[/home/kun]
#
```

xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx 格式

nbtscan -l 192.168.11.0-192.168.11.200

在 0~200 的范围内寻找主机并以Imhosts格式输出

```
[root@parrot]~[/home/kun]
#nbtscan -l 192.168.11.0-192.168.11.200
192.168.11.0    Sendto failed: Permission denied
192.168.11.138 KUN-1807B00A1B8 #PRE
192.168.11.144 WIN-IB3UD9SBCU1 #PRE
```

xxx.xxx.xxx.xxx/xx 格式

nbtscan -l 192.168.11.0/24

扫描整个网段并以Imhosts格式进行输出

```
[root@parrot]~[/home/kun]
#nbtscan -l 192.168.11.0/24
192.168.11.0    Sendto failed: Permission denied
192.168.11.138 KUN-1807B00A1B8 #PRE
192.168.11.144 WIN-IB3UD9SBCU1 #PRE
192.168.11.255 Sendto failed: Permission denied
```