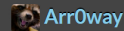




## nbtscan Cheat Sheet ∞

### CHEAT-SHEET

29 Mar 2015



**nbtscan** is a command line tool that finds exposed NETBIOS nameservers, it's a good first step for finding open shares.

### ★ Don't use the version of nbtscan that ships with KALI

Grab nbtscan from the above link and build it from source, this version tends to find more information

## Compile nbtscan on KALI

```
root@kali:~/nbtscan# wget http://www.unixwiz.net/tools/nbtscan-source-1.0.35.tgz
root@kali:~/nbtscan# tar -xvzf nbtscan-source-1.0.35.tgz
root@kali:~/nbtscan# make
root@kali:~/nbtscan# ./nbtscan
nbtscan 1.0.35 - 2008-04-08 - http://www.unixwiz.net/tools/
```

```
usage: ./nbtscan [options] target [targets...]
```

Targets are lists of IP addresses, DNS names, or address ranges. Ranges can be in /nbits notation ("192.168.12.0/24") or with a range in the last octet ("192.168.12.64-97")

## nbtscan Cheat Sheet

COMMAND	DESCRIPTION
<code>nbtscan -v</code>	Displays the nbtscan version
<code>nbtscan -f target(s)</code>	This shows the full NBT resource record responses for each machine scanned, not a one line summary, use this options when scanning a single host
<code>nbtscan -O file-name.txt target(s)</code>	Sends output to a file
<code>nbtscan -H</code>	Generate an HTTP header
<code>nbtscan -P</code>	Generate Perl hashref output, which can be loaded into an existing program for easier processing, much easier than parsing text output
<code>nbtscan -V</code>	Enable verbose mode
<code>nbtscan -n</code>	Turns off this inverse name lookup, for hanging resolution
<code>nbtscan -p PORT target(s)</code>	This allows specification of a UDP port number to be used as the source in sending a query
<code>nbtscan -i IP target(s)</code>	Include the IP address in the output

[All Blog](#)  
[Cheat Sheets](#)  
[Techniques](#)  
[Security Hardening](#)  
[WalkThroughs](#)

### CHEAT SHEETS

[Reverse Shell Cheat Sheet](#)  
[Penetration Testing Tools Cheat Sheet](#)  
[LFI Cheat Sheet](#)  
[Vi Cheat Sheet](#)  
[Systemd Cheat Sheet](#)  
[nbtscan Cheat Sheet](#)  
[Nmap Cheat Sheet](#)  
[Linux Commands Cheat Sheet](#)  
[More »](#)

### WALKTHROUGHS

[InsomniHack CTF Teaser - Smartcat2 Writeup](#)  
[InsomniHack CTF Teaser - Smartcat1 Writeup](#)  
[FristiLeaks 1.3 Walkthrough](#)  
[SickOS 1.1 - Walkthrough](#)  
[The Wall Boot2Root Walkthrough](#)  
[More »](#)

### TECHNIQUES

[SSH & Meterpreter Pivoting Techniques](#)  
[More »](#)

### SECURITY HARDENING

[Security Harden CentOS 7](#)  
[More »](#)

### /DEV/URANDOM

[MacBook - Post Install Config + Apps](#)  
[More »](#)

### OTHER BLOG

[HowTo: Kali Linux Chromium Install for Web App Pen Testing](#)  
[Jenkins RCE via Unauthenticated API](#)

nbtscan -m

include the MAC (aka "Ethernet ") addresses in the response, which is already implied by the -f option.

MacBook - Post Install  
Config + Apps  
enum4linux Cheat Sheet  
Linux Local Enumeration  
Script  
HowTo Install Quassel on  
Ubuntu  
HowTo Install KeepNote  
on OSX Mavericks

## Share this on...

[Twitter](#) [Facebook](#) [Google+](#) [Reddit](#)

## Follow Arr0way

[Twitter](#) [GitHub](#)

## Also...

## You might want to read these

CATEGORY	POST NAME
cheat-sheet	<a href="#">Reverse Shell Cheat Sheet</a>
cheat-sheet	<a href="#">Penetration Testing Tools Cheat Sheet</a>
cheat-sheet	<a href="#">LFI Cheat Sheet</a>
kali linux	<a href="#">HowTo: Kali Linux Chromium Install for Web App Pen Testing</a>
walkthroughs	<a href="#">InsomniHack CTF Teaser - Smartcat2 Writeup</a>
walkthroughs	<a href="#">InsomniHack CTF Teaser - Smartcat1 Writeup</a>
walkthroughs	<a href="#">FristiLeaks 1.3 Walkthrough</a>
walkthroughs	<a href="#">SickOS 1.1 - Walkthrough</a>
walkthroughs	<a href="#">The Wall Boot2Root Walkthrough</a>
walkthroughs	<a href="#">/dev/random: Sleepy Walkthrough CTF</a>