nbtscan Cheat Sheet ∞

CHEAT-SHEET 29 Mar 2015 Arr0way

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

All Blog
Cheat Sheets
Techniques
Security Hardening
WalkThroughs

CHEAT SHEETS

Penetration Testing Tools Cheat Sheet
LFI Cheat Sheet
Vi Cheat Sheet
Systemd Cheat Sheet
Reverse Shell Cheat Sheet
nbtscan Cheat Sheet
Nmap Cheat Sheet
Linux Commands Cheat Sheet

```
root@kali:~/nbtscan# wget http://www.unixwiz.net/tools/nbtscan-sourc
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
`nbtscan -v`	Displays the nbtscan version
`nbtscan -f target(s)`	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
`nbtscan -O file-name.txt target(s)`	Sends output to a file

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 »

`nbtscan -H`	Generate an HTTP header
`nbtscan -P`	Generate Perl hashref output, which can be loaded into an existing program for easier processing, much easier than parsing text output
`nbtscan -V`	Enable verbose mode
`nbtscan -n`	Turns off this inverse name lookup, for hanging resolution
`nbtscan -p PORT target(s)`	This allows specification of a UDP port number to be used as the source in sending a query
`nbtscan -m`	Include the MAC (aka "Ethernet") addresses in the response, which is already implied by the -f option.

Share this on...

Twitter Facebook Google+ Reddit

/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

MacBook - Post Install Config + Apps

enum4linux Cheat Sheet

Linux Local Enumeration Script

HowTo Install Quassel on Ubuntu

HowTo Install KeepNote on OSX Mavericks

Follow Arr0way

Twitter GitHub

Also...

You might want to read these

CATEGORY	POST NAME
`cheat-sheet`	Penetration Testing Tools Cheat Sheet
`cheat-sheet`	LFI Cheat Sheet
`kali linux`	HowTo: Kali Linux Chromium Install for Web App Pen Testing
`walkthroughs`	InsomniHack CTF Teaser - Smartcat2 Writeup

walkthroughs	InsomniHack CTF Teaser - Smartcat1 Writeup
walkthroughs	FristiLeaks 1.3 Walkthrough
walkthroughs	SickOS 1.1 - Walkthrough
walkthroughs	The Wall Boot2Root Walkthrough
walkthroughs	/dev/random: Sleepy Walkthrough CTF
walkthroughs	/dev/random Pipe walkthrough