GitHub - nomex/nbnspoof: NetBIOS Name Service spoofing tool

By nomex

Archived: 2026-04-05 16:23:12 UTC

This tool was created in 2007 by Robert Wesley McGrew. You can read about the tool and the author in http://www.mcgrewsecurity.com/tools/nbnspoof/

I've made a few changes to add support to targeted spoofing.

Introduction

NBNSpoof is a tool for automatically crafting responses to NetBIOS Name Service (NBNS) name queries. When Windows machines fail to resolve domain names by DNS and WINS, they will send a broadcast NBNS query to see if the name in question matches any computer names on the local network. Crafting responses to these requests can be especially useful to an attacker in situations where the victim mis-types a domain name, or if the DNS server is unreachable.

NBNSpoof is a penetration testing tool designed to demonstrate this attack, and also serves as a useful illustration of how to develop small network security tools, as the creation of it has been documented in a short series of posts to this site.

Usage

```
nbnspoof.py [-v] -i <interface> -n <regexp> -h <ip address> -m <MAC> [-p <ip address>]

-v Verbose output of sniffed NBNS name queries, and responses sent

-i The interface you want to sniff and send on

-n A regular expression applied to each query to determine whether a
   spoofed response will be sent

-h The IP address that will be sent in spoofed responses

-p (optional) The IP address of the victim (if unset, pwn all)

-m The source MAC address for spoofed responses
```

Source: https://github.com/nomex/nbnspoof