GitHub - SpiderLabs/Responder: Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.

By Greenwolf

Archived: 2026-04-05 20:26:59 UTC

⛔ [DEPRECATED] Active at https://github.com/lgandx/Responder

LLMNR/NBT-NS/mDNS Poisoner

Author: Laurent Gaffie <laurent.gaffie@gmail.com > http://www.spiderlabs.com

Intro

Responder an LLMNR, NBT-NS and MDNS poisoner. It will answer to *specific* NBT-NS (NetBIOS Name Service) queries based on their name suffix (see: http://support.microsoft.com/kb/163409). By default, the tool will only answer to File Server Service request, which is for SMB.

The concept behind this is to target our answers, and be stealthier on the network. This also helps to ensure that we don't break legitimate NBT-NS behavior. You can set the -r option via command line if you want to answer to the Workstation Service request name suffix.

Features

- Built-in SMB Auth server.

Supports NTLMv1, NTLMv2 hashes with Extended Security NTLMSSP by default. Successfully tested from Windows 95 to Server 2012 RC, Samba and Mac OSX Lion. Clear text password is supported for NT4, and LM hashing downgrade when the --lm option is set. This functionality is enabled by default when the tool is launched.

- Built-in MSSQL Auth server.

In order to redirect SQL Authentication to this tool, you will need to set the option -r (NBT-NS queries for SQL Server lookup are using the Workstation Service name suffix) for systems older than windows Vista (LLMNR will be used for Vista and higher). This server supports NTLMv1, LMv2 hashes. This functionality was successfully tested on Windows SQL Server 2005 & 2008.

- Built-in HTTP Auth server.

In order to redirect HTTP Authentication to this tool, you will need to set the option -r for Windows version older than Vista (NBT-NS queries for HTTP server lookup are sent using the Workstation Service name suffix). For Vista and higher, LLMNR will be used. This server supports NTLMv1, NTLMv2 hashes *and* Basic Authentication. This server was successfully tested on IE 6 to IE 10, Firefox, Chrome, Safari.

Note: This module also works for WebDav NTLM authentication issued from Windows WebDav clients (WebClient). You can now send your custom files to a victim.

- Built-in HTTPS Auth server.

Same as above. The folder certs/ contains 2 default keys, including a dummy private key. This is *intentional*, the purpose is to have Responder working out of the box. A script was added in case you need to generate your own self signed key pair.

- Built-in LDAP Auth server.

In order to redirect LDAP Authentication to this tool, you will need to set the option -r for Windows version older than Vista (NBT-NS queries for HTTP server lookup are sent using the Workstation Service name suffix). For Vista and higher, LLMNR will be used. This server supports NTLMSSP hashes and Simple Authentication (clear text authentication). This server was successfully tested on Windows Support tool "ldp" and LdapAdmin.

- Built-in FTP, POP3, IMAP, SMTP Auth servers.

This modules will collect clear text credentials.

- Built-in DNS server.

This server will answer type A queries. This is really handy when it's combined with ARP spoofing.

- Built-in WPAD Proxy Server.

This module will capture all HTTP requests from anyone launching Internet Explorer on the network if they have "Auto-detect settings" enabled. This module is highly effective. You can configure your custom PAC script in Responder.conf and inject HTML into the server's responses. See Responder.conf.

- Browser Listener

This module allows to find the PDC in stealth mode.

- Fingerprinting

When the option -f is used, Responder will fingerprint every host who issued an LLMNR/NBT-NS query. All capture modules still work while in fingerprint mode.

- Icmp Redirect

  python tools/Icmp-Redirect.py

For MITM on Windows XP/2003 and earlier Domain members. This attack combined with the DNS module is pretty effective.

- Rogue DHCP

  python tools/DHCP.py

DHCP Inform Spoofing. Allows you to let the real DHCP Server issue IP addresses, and then send a DHCP Inform answer to set your IP address as a primary DNS server, and your own WPAD URL.

- Analyze mode.

This module allows you to see NBT-NS, BROWSER, LLMNR, DNS requests on the network without poisoning any responses. Also, you can map domains, MSSQL servers, workstations passively, see if ICMP Redirects attacks are plausible on your subnet.

Hashes

All hashes are printed to stdout and dumped in an unique file John Jumbo compliant, using this format:

```
(MODULE_NAME)-(HASH_TYPE)-(CLIENT_IP).txt
```

Log files are located in the "logs/" folder. Hashes will be logged and printed only once per user per hash type, unless you are using the Verbose mode (-v).

- Responder will logs all its activity to Responder-Session.log
- Analyze mode will be logged to Analyze-Session.log
- Poisoning will be logged to Poisoners-Session.log

Additionally, all captured hashed are logged into an SQLite database which you can configure in Responder.conf

Considerations

- This tool listens on several ports: UDP 137, UDP 138, UDP 53, UDP/TCP 389,TCP 1433, TCP 80, TCP 139, TCP 445, TCP 21, TCP 3141,TCP 25, TCP 110, TCP 587 and Multicast UDP 5553.
- If you run Samba on your system, stop smbd and nmbd and all other services listening on these ports.
- For Ubuntu users:

Edit this file /etc/NetworkManager/NetworkManager.conf and comment the line: `dns=dnsmasq`. Then kill dnsmasq with this command (as root): `killall dnsmasq -9`

- Any rogue server can be turned off in Responder.conf.
- This tool is not meant to work on Windows.

- For OSX, please note: Responder must be launched with an IP address for the -i flag (e.g. -i YOUR_IP_ADDR). There is no native support in OSX for custom interface binding. Using -i en1 will not work. Also to run Responder with the best experience, run the following as root:

  launchcl unload /System/Library/LaunchDaemons/com.apple.Kerberos.kdc.plist

  launchctl unload /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist

  launchctl unload /System/Library/LaunchDaemons/com.apple.smbd.plist

  launchctl unload /System/Library/LaunchDaemons/com.apple.netbiosd.plist

Usage

First of all, please take a look at Responder.conf and tweak it for your needs.

Running the tool:

Typical Usage Example:

```
./Responder.py -I eth0 -wrf
```

Options:

```
 --version             show program's version number and exit
-h, --help            show this help message and exit
-A, --analyze         Analyze mode. This option allows you to see NBT-NS,
                      BROWSER, LLMNR requests without responding.
-I eth0, --interface=eth0
                      Network interface to use
-b, --basic           Return a Basic HTTP authentication. Default: NTLM
-r, --wredir          Enable answers for netbios wredir suffix queries.
                      Answering to wredir will likely break stuff on the
                      network. Default: False
-d, --NBTNSdomain     Enable answers for netbios domain suffix queries.
                      Answering to domain suffixes will likely break stuff
                      on the network. Default: False
-f, --fingerprint     This option allows you to fingerprint a host that
                      issued an NBT-NS or LLMNR query.
-w, --wpad            Start the WPAD rogue proxy server. Default value is
                      False
-u UPSTREAM_PROXY, --upstream-proxy=UPSTREAM_PROXY
                      Upstream HTTP proxy used by the rogue WPAD Proxy for
                      outgoing requests (format: host:port)
-F, --ForceWpadAuth   Force NTLM/Basic authentication on wpad.dat file
                      retrieval. This may cause a login prompt. Default:
                      False
```

```
--lm                  Force LM hashing downgrade for Windows XP/2003 and
                      earlier. Default: False
-v, --verbose         Increase verbosity.
```

Copyright

NBT-NS/LLMNR Responder Created by Laurent Gaffie Copyright (C) 2013 Trustwave Holdings, Inc.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/

Source: https://github.com/SpiderLabs/Responder