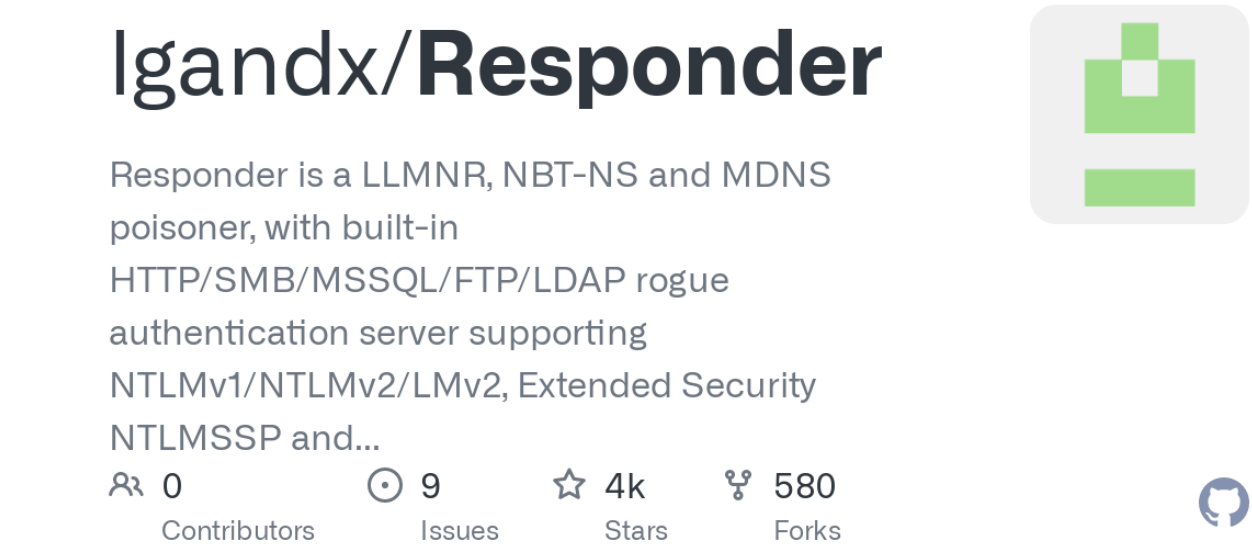
Responder/MultiRelay

github.com/lgandx/Responder

lgandx



This branch is 249 commits ahead, 2 commits behind SpiderLabs/Responder:master.

#199

IPv6/IPv4 LLMNR/NBT-NS/mDNS Poisoner and NTLMv1/2 Relay.

Author: Laurent Gaffie <laurent.gaffie@gmail.com > https://g-laurent.blogspot.com

Intro

Responder is an LLMNR, NBT-NS and MDNS poisoner.

Features

- Dual IPv6/IPv4 stack.
- Built-in SMB Auth server.

Supports NTLMv1, NTLMv2 hashes with Extended Security NTLMSSP by default. Successfully tested from Windows 95 to Server 2022, Samba and Mac OSX Lion. Clear text password is supported for NT4, and LM hashing

downgrade when the --lm option is set. If --disable-ess is set, extended session security will be disabled for NTLMv1 authentication. SMBv2 has also been implemented and is supported by default.

Built-in MSSQL Auth server.

This server supports NTLMv1, LMv2 hashes. This functionality was successfully tested on Windows SQL Server 2005, 2008, 2012, 2019.

Built-in HTTP Auth server.

This server supports NTLMv1, NTLMv2 hashes *and* Basic Authentication. This server was successfully tested on IE 6 to IE 11, Edge, 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.

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 DCE-RPC Auth server.

This server supports NTLMSSP hashes. This server was successfully tested on Windows XP to Server 2019.

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

This modules will collect clear text credentials.

Built-in DNS server.

This server will answer type SRV and 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.

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. To inject a DNS server, domain, route on all Windows version and any linux box, use -R

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 a unique John Jumbo compliant file, 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 log all its activity to Responder-Session.log
- Analyze mode will be logged to Analyzer-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, UDP 1434, TCP 80, TCP 135, TCP 139, TCP 445, TCP 21, TCP 3141,TCP 25, TCP 110, TCP 587, TCP 3128, Multicast UDP 5355 and 5353.
- 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:

  launchctl 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:

```
./Responder.py [options]
```

Typical Usage Example:

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

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, you can use 'ALL' as a
                    wildcard for all interfaces
-i 10.0.0.21, --ip=10.0.0.21
                    Local IP to use (only for OSX)
-6 2002:c0a8:f7:1:3ba8:aceb:b1a9:81ed, --
externalip6=2002:c0a8:f7:1:3ba8:aceb:b1a9:81ed
                    Poison all requests with another IPv6 address than
                    Responder's one.
-e 10.0.0.22, --externalip=10.0.0.22
                    Poison all requests with another IP address than
                    Responder's one.
-b, --basic           Return a Basic HTTP authentication. Default: NTLM
-d, --DHCP            Enable answers for DHCP broadcast requests. This
                    option will inject a WPAD server in the DHCP
response.
                    Default: False
-D, --DHCP-DNS        This option will inject a DNS server in the DHCP
                    response, otherwise a WPAD server will be added.
                    Default: False
-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
-P, --ProxyAuth       Force NTLM (transparently)/Basic (prompt)
                    authentication for the proxy. WPAD doesn't need to be
                    ON. Default: False
--lm                  Force LM hashing downgrade for Windows XP/2003 and
                    earlier. Default: False
--disable-ess         Force ESS downgrade. Default: False
-v, --verbose         Increase verbosity.
```

Donation

You can contribute to this project by donating to the following $XLM (Stellar Lumens) address:

"GCGBMO772FRLU6V4NDUKIEXEFNVSP774H2TVYQ3WWHK4TEKYUUTLUKUH"

Paypal:

https://paypal.me/PythonResponder

Patreon:

https://www.patreon.com/PythonResponder

Acknowledgments

Late Responder development has been possible because of the donations received from individuals and companies.

We would like to thanks those major sponsors:

- SecureWorks: https://www.secureworks.com/
- Synacktiv: https://www.synacktiv.com/
- Black Hills Information Security: http://www.blackhillsinfosec.com/
- TrustedSec: https://www.trustedsec.com/
- Red Siege Information Security: https://www.redsiege.com/
- Open-Sec: http://www.open-sec.com/
- And all, ALL the pentesters around the world who donated to this project.

Thank you.

Copyright

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/.