CYBERTECH AWARENESS PROGRAM

CYBERSECURITY AWARENESS AND EDUCATIONAL OUT-REACH

BURLINGTON, VT

Responder

Network Reconnaissance

@cybertechvt @cybertechvt cybertechvt.com

Disclaimer/Warning

The Kali Guides provided to you by the Cyber Tech Awareness team are meant for educational purposes ONLY.

The tools covered in the Kali Guides can be used for malicious purposes, but should not be used as such.

The CyberTech Awareness team and the Leahy Center for Digital Forensics and Cybersecurity is NOT responsible any malicious activity conduced with aid from these Kali Guides.

Only use this tool on domains, addresses, files and resources that you have permission to.

Brief Summary

Responder is a tool for capturing traffic and sending data to a malicious user. It intercepts LLMNR, NBT-NS, and MDNS queries and “poisons” them with imitation replies that will send information back to the hacker when utilized.

Helpful Vocabulary

Man-in-the-middle attack:

- A cyber attack in which an attacker intercepts or alters information by positioning themselves in the middle point of two targets/communicating devices

Network Interface:

- The point of connection between a device and a network. You can run “if config” in Linux to view common interfaces such as eth0 (the ethernet interface), wlan0 (the wireless interface), and lo (the loopback interface).

IP Address:

- An Internet Protocol (IP) Address, is similar to a physical home or mailing address. All devices that are connected to the internet have a unique IP address. This allows devices to communicate and send information to specific devices using their IP address.

IP Gateway:

- A device on a network that allows for traffic to be sent from that network to other networks.

Proxy Server:

- Proxy servers sit between the client and the web server.

Reconnaissance:

- The information gathering stage of ethical hacking, where you collect data about a target system.

Helpful Vocabulary

Network Protocol:

- a universal language for communication between different devices. Each protocol has a set of rules that regulates communications and/or data processing across networks.

WPAD:

- The “Web Proxy Auto-Discovery” is a protocol that automatically detects which web proxy should be used, as well as locating cache services within a network.

IC MP:

- “Internet Control Message Protocol” is a protocol that checks for issues or errors relating to communication within the network including connectivity issues or a compromised transmission.

SMB:

- “Server Block Message” is a protocol SMB signing used to connect to or share files between devices, such as to a printer. SMB is notorious for being vulnerable to man-in-the-middle attacks.

SMB signing:

- A way of securing within an SMB protocol by “signing” a packet with a digital signature to confirm the authenticity of the packet so that the packets cannot be modified without the client knowing.

Helpful Vocabulary

DNS:

- “Domain Name System” translates domain names into IP addresses so that browsers can load internet pages. DNS servers are used to translate and resolve protocols involving hostnames and IP addresses

LLMNR:

- “Link-Local Multicast Name Resolution” is a protocol based on the DNS format that performs the same name resolution service but for local names (on the same network), or when the DNS server fails.

NBT-NS:

- “NetBIOS Name Service” is an old protocol for name resolution within a network when the DNS servers cannot

MDNS:

- “Multicast DNS” is an alternative to DNS for small networks without a local name server

RDP:

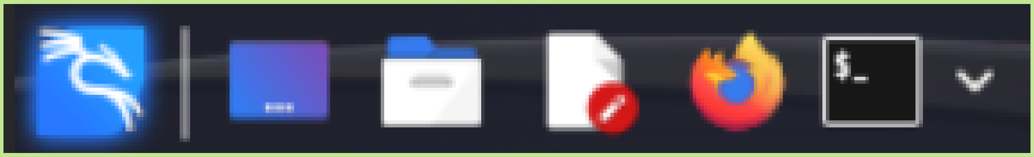
- “Remote Desktop Protocol”, a network protocol that creates secure connections between users and remote computers, servers, or virtual machines.

Hash:

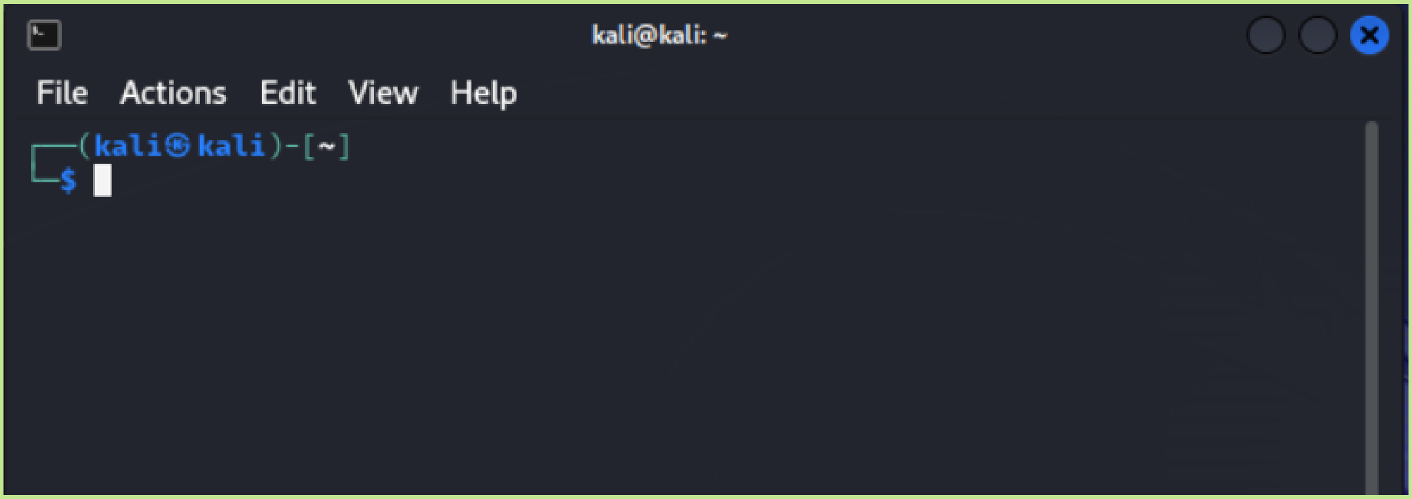
- “Hashes are an encryption method that involves a function that turns data into a unique, fixed-number string output. By design, hashes cannot be reverted back into the original data.

How to Access Responder Through the Terminal

In your taskbar, which should be located at the top left of your screen, click on the black box with white text that looks like "$_".



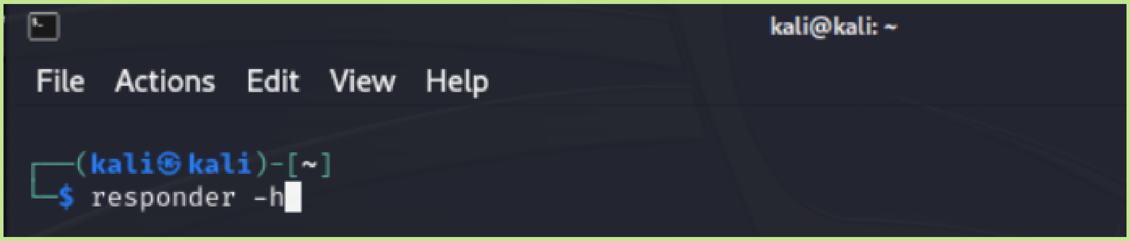
*If the black box isn't there, click on the blue dragon symbol and type "**Terminal Emulator"** into the search bar.*



```
┌──(kali㉿kali)-[~]
└─$ 
```

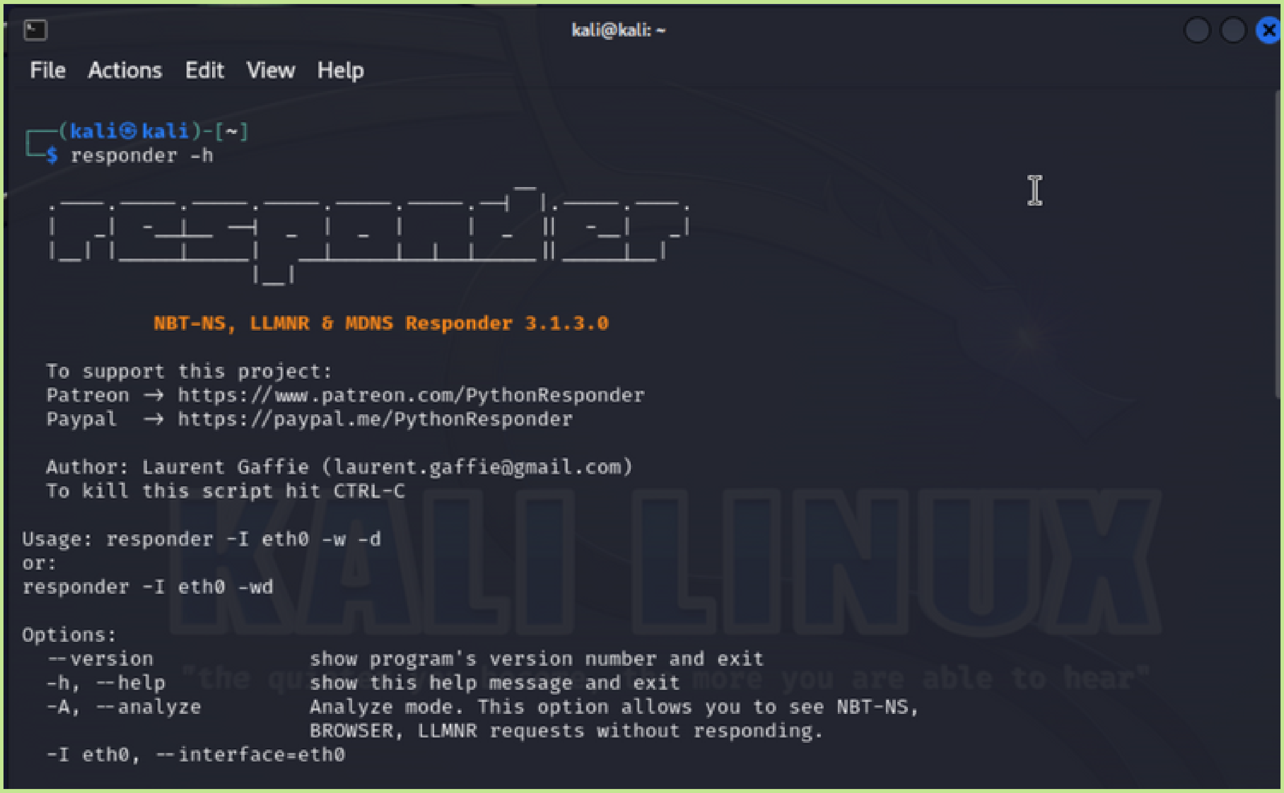
This is what the terminal looks like once it's opened. The default user is "kali@kali".

How to Find Options for the Responder tools



```
┌──(kali㉿kali)-[~]
└─$ responder -h
```

The -h command option displays "help" or "usage" options for any command that can be run in the terminal.

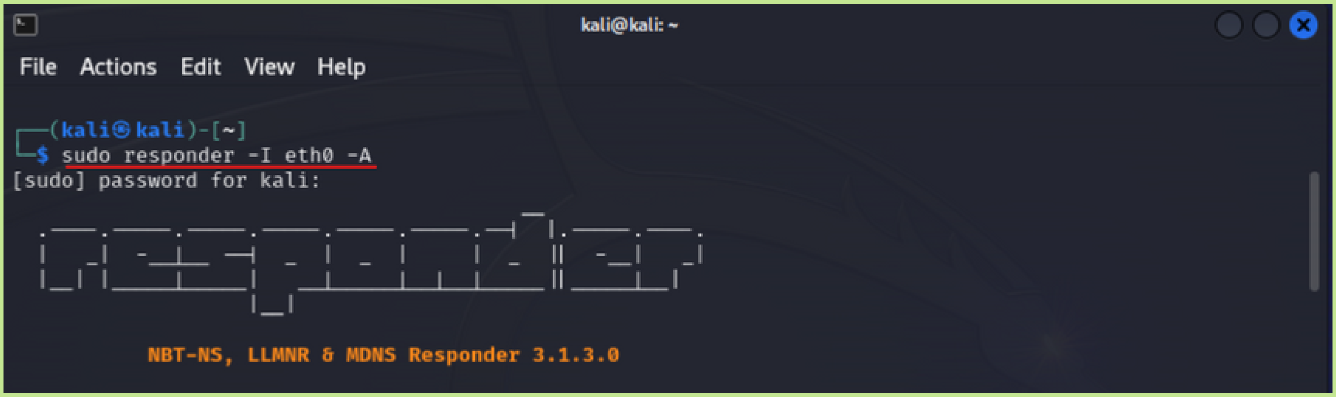


```
┌──(kali㉿kali)-[~]
└─$ responder -h
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon → https://www.patreon.com/PythonResponder
  Paypal  → https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C

Usage: responder -I eth0 -w -d
or:
responder -I eth0 -wd

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
```

Above are the help options for the "responder" tool

Example 1: responder -I eth0 -A

*****ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN*****



```
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0 -A
[sudo] password for kali:
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0
```

What is this command doing?

This command is using responder to analyze activity on a network and display those events for the user to see.

sudo

- This makes you a "root" user, which gives you access to more commands. You have to be a root user to run responder.

responder

- Tells the system that it's going to be using the **responder** tool

-I

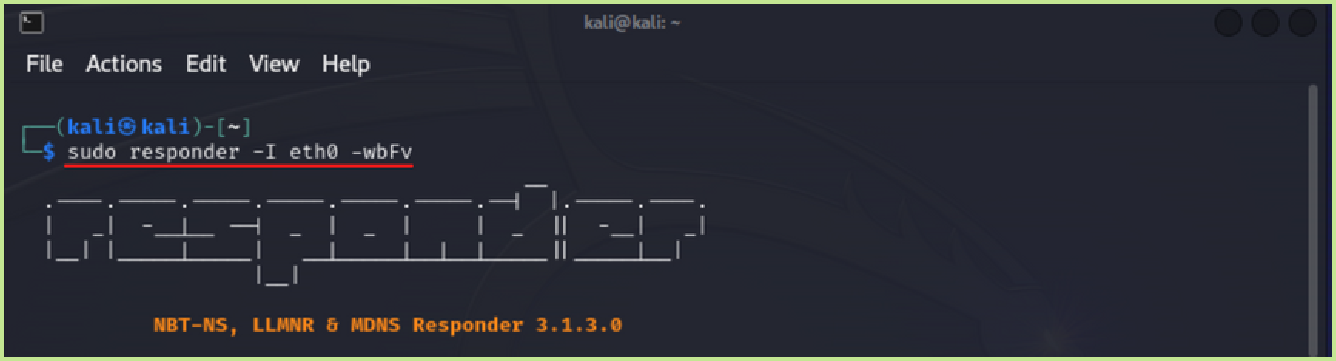
- Sets the network interface to use (in this case, eth0)

-A

- Sets the mode to analyze, which views the requests on the network without responding to them.

Example 2: responder -I eth0 -wbFv

*****ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN*****



```
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0 -wbFv
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0
```

What is this command doing?

This command is using responder to cause an authentication screen to pop up when network activity is observed. In other words, the hacker is going to capture the credentials of clients using the network. It is likely that the password is going to come back as a hash- in which case the hacker must then attempt to crack the hash.

sudo

- This makes you a "**root**" user, which gives you access to more commands. You have to be a root user to run responder.

Responder

- Tells the system that it's going to be using the **responder** tool

-w

- Starts the WPAD proxy server

-b

- sets basic HTTP authentication to be returned

-F

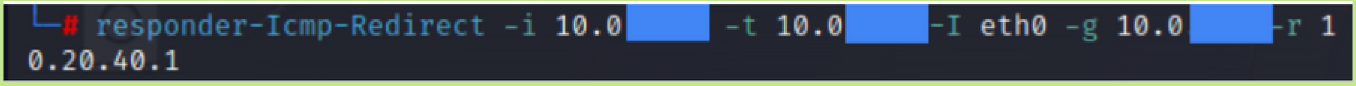
- The setting to force authentication for WPAD which causes the login prompt to appear

-v

- Setting to increase verbosity (text output for observed activity)

Example 2: responder-icmp-redirect

*****ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN*****



```
└─# responder-Icmp-Redirect -i 10.0[redacted] -t 10.0[redacted]-I eth0 -g 10.0[redacted]-r 1
0.20.40.1
```

What is this command doing?

This command is redirecting traffic from a target IP to another IP.

sudo

- This makes you a "**root**" user, which gives you access to more commands. You have to be a root user to run responder.

Responder-icmp-redirect

- Uses the ICMP redirect functionality of responder to not only display the traffic on a network, but to redirect that traffic directly to another IP.

-i

- Sets the IP address that collects the traffic

-t

- Sets the IP address of the target

-I

- Sets the network interface to use (in this case, eth0)

-g

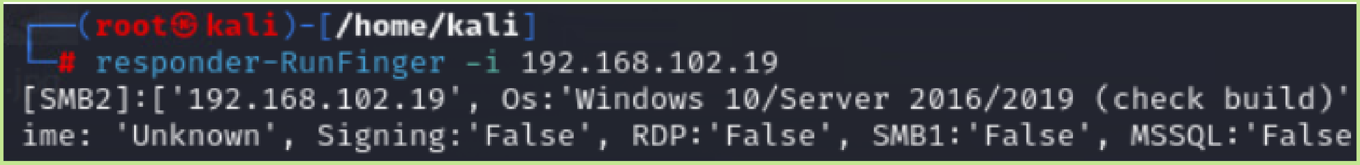
- The IP address of the original gateway

-r

- Sets the IP address of the destination target

Example 3: responder-RunFinger

*****ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN*****



```
┌──(root㉿kali)-[/home/kali]
└─# responder-RunFinger -i 192.168.102.19
[SMB2]:['192.168.102.19', Os:'Windows 10/Server 2016/2019 (check build)'
ime: 'Unknown', Signing:'False', RDP:'False', SMB1:'False', MSSQL:'False
```

What is this command doing?

This command is used to display information about machines on the network. Of maximal interest is generally if SMB signing is enabled, which helps hackers choose targets.

sudo

- This makes you a "**root**" user, which gives you access to more commands. You have to be a root user to run responder.

Responder-RunFinger

- Uses the functionality of responder that displays the OS, build, domain, bootime, signing, RDP, SMB, and MSSQL of a target

-i

- Sets the IP address that collects the traffic

Additional Resources:

Kali Linux Responder Official Webpage:
https://www.kali.org/tools/responder/

Quick Creds with Responder and Kali Linux:
https://cyberarms.wordpress.com/2018/01/12/easy-creds-with-responder-and-kali-linux/

A Detailed Guide on Responder (LLMNR Poisoning):
https://www.hackingarticles.in/a-detailed-guide-on-responder-llmnr-poisoning/

Top 100 Tools: How to use Responder in Kali Linux to Easily capture windows credentials:
https://rotnemzero.com/top-100-tools-how-to-use-responder-in-kali-linux/