# Proof of Concept Report

**Finding:** NTLMv2 Hash Capture and Password Cracking via Responder

## 1. Introduction

As part of the penetration testing engagement, an assessment was performed to identify weaknesses in authentication mechanisms within the internal network. Using **Responder** and **John the Ripper** on a Kali Linux attack host, it was demonstrated that NTLMv2 hashes could be captured and successfully cracked, exposing valid credentials.

## 2. Vulnerability Description

The attack leverages **LLMNR (Link-Local Multicast Name Resolution)** and **NBT-NS (NetBIOS Name Service)** poisoning via Responder. When a host attempts to resolve an unknown hostname, Responder can trick the target into sending authentication requests, capturing NTLMv2 hashes in the process. These hashes can then be cracked offline to recover plaintext credentials.

This vulnerability is critical because:

Attackers can obtain valid user credentials.

It allows for privilege escalation or lateral movement.

It bypasses traditional perimeter defenses since the attack is internal.

## 3. Environment & Setup

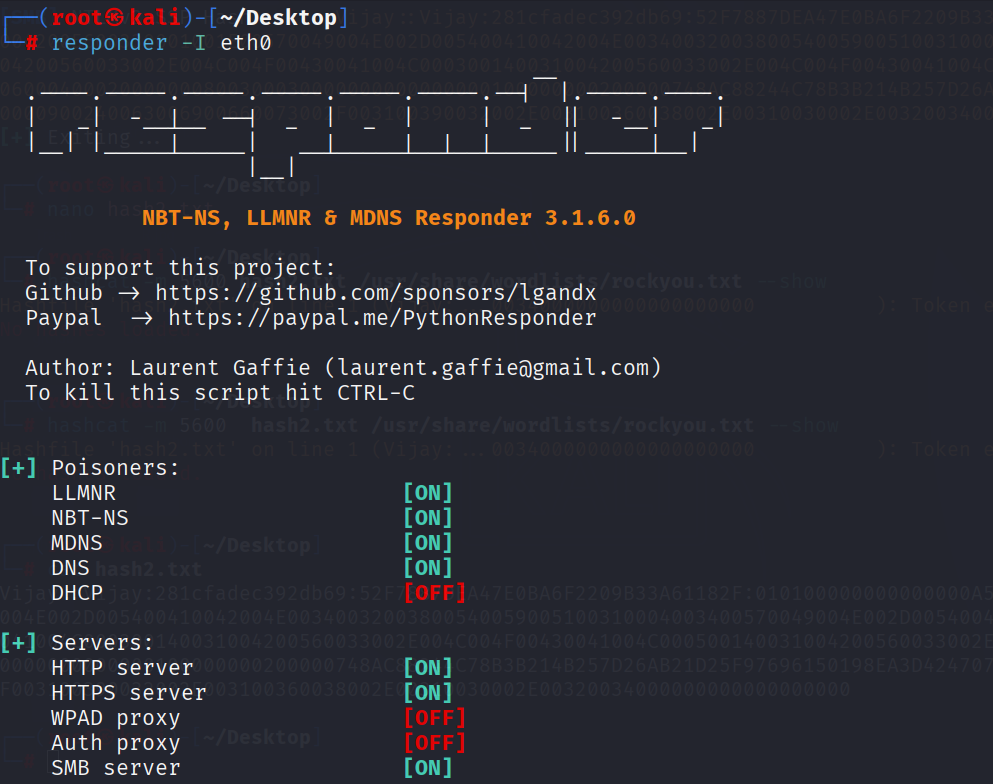
**Target:** Windows Server VM (internal network).

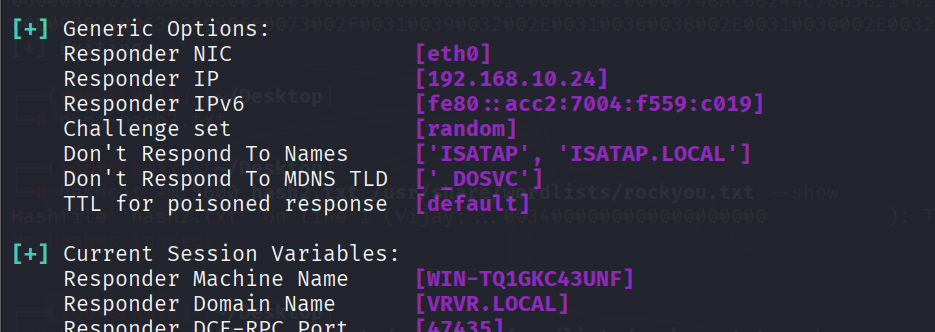
**Attacker Machine:** Kali Linux with Responder and John the Ripper.

**Network Assumptions:** Responder was deployed in the same broadcast domain as the target server.

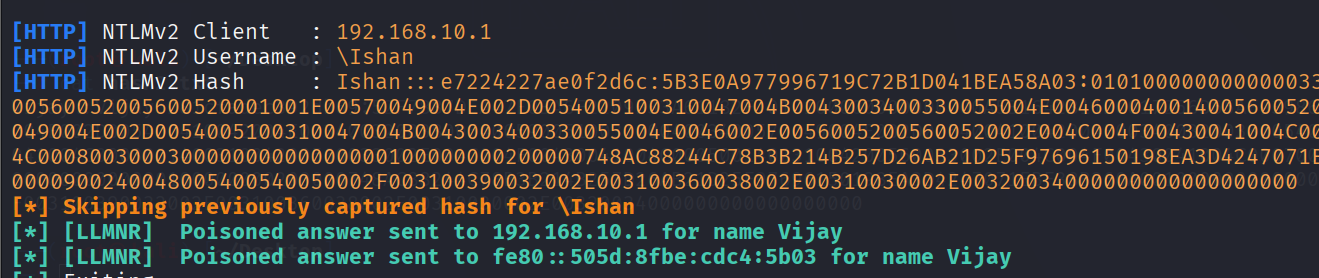
## 4. Exploitation Steps

### Step 1 – Running Responder

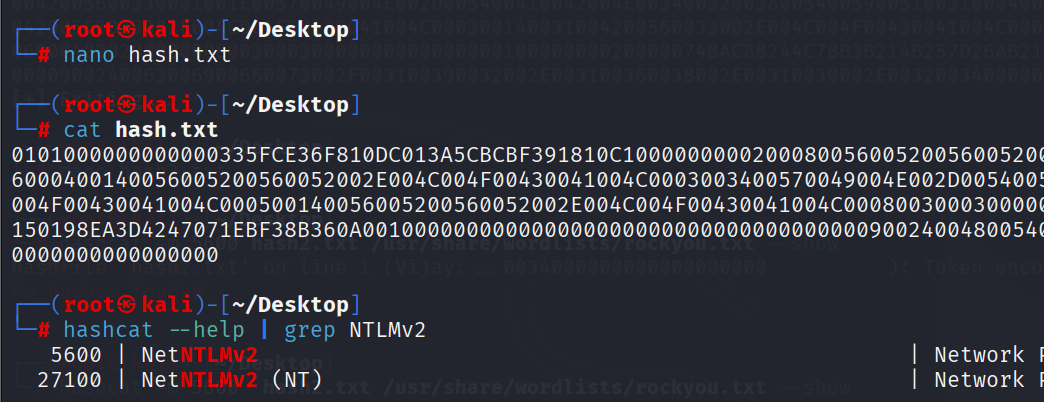
Responder was started on the Kali interface to listen for LLMNR/NBT-NS requests.  




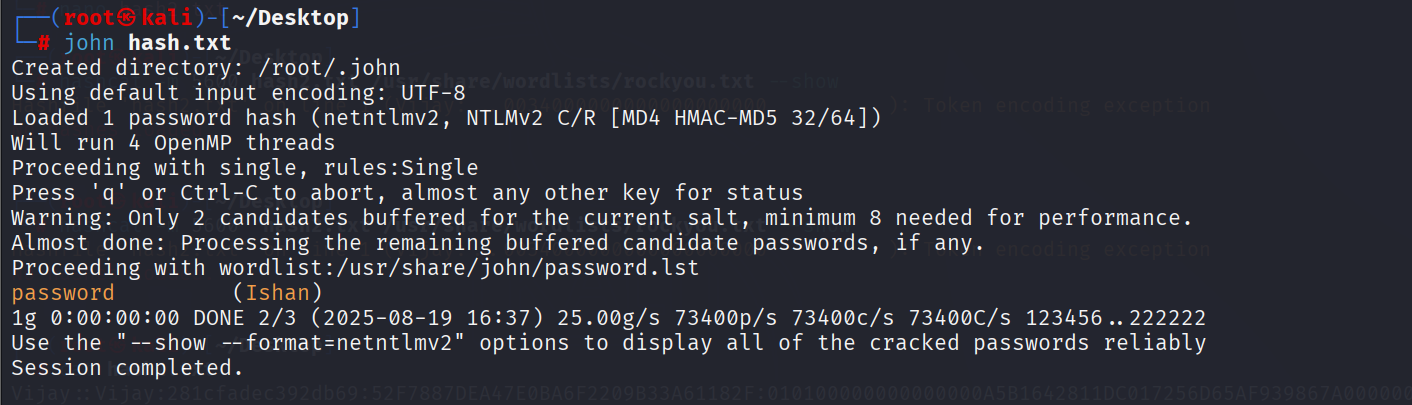
### Step 2 – Capturing NTLMv2 Hash

When the target attempted name resolution, Responder captured an NTLMv2 hash.  


### Step 3 – Preparing Hash for Cracking

The captured hash was saved into a text file (hash.txt) for password cracking.  


### Step 4 – Cracking with John the Ripper

John the Ripper successfully cracked the NTLMv2 hash, revealing the plaintext password.  


## 5. Impact

The successful recovery of valid credentials demonstrates that:

An attacker could authenticate to the server with the stolen password.

If password reuse exists, domain or enterprise-wide compromise could occur.

The organization is vulnerable to internal lateral movement attacks.

**Severity:** High / Critical

## 6. Recommendations

To mitigate this issue, the following actions are recommended:

**Disable LLMNR and NetBIOS** on all systems via Group Policy.

**Enforce strong password policies** (complexity, length, and rotation).

**Implement network monitoring** for unusual LLMNR/NBT-NS broadcasts.

**Enforce NTLM restrictions** and prefer Kerberos for authentication.

**Educate users** about phishing and password reuse risks.

## 7. Conclusion

This proof of concept demonstrates that NTLMv2 credentials can be intercepted and cracked using widely available tools. The recovered password provides an attacker with unauthorized access to sensitive systems, posing a critical security risk. Immediate mitigation is recommended to prevent exploitation in a real-world scenario.