Task 1 Report: NTLM Hash Capture using Responder

Objective

The objective of this task was to capture NTLM authentication hashes by exploiting insecure name resolution protocols such as LLMNR and NBT-NS using the Responder tool within a controlled TryHackMe lab environment.

Lab Environment

Attacker Machine: Kali Linux (VPN connected via OpenVPN)
Target Machine: TryHackMe Vulnerable Host
Network Interface: tun0 (TryHackMe VPN Interface)

Tools Used

• Responder 3.2.0
• OpenVPN
• Kali Linux Terminal

Methodology

1. The Kali Linux machine was connected to the TryHackMe private network using OpenVPN.
2. The Responder configuration was verified to ensure SMB, HTTP, LLMNR, and NBT-NS services were enabled.
3. Responder was executed on the tun0 interface to listen for name resolution requests.
4. The target machine generated authentication traffic which was intercepted by Responder.
5. NTLMv2 hashes were successfully captured and stored in the Responder logs directory.

Command Used

```
sudo responder -I tun0 -dwv
```

Results

The attack was successful, and NTLMv2 authentication hashes were captured from the target system. This confirms that the target machine is vulnerable to LLMNR/NBT-NS poisoning attacks.

Conclusion

This task demonstrated how misconfigured network name resolution protocols can be abused to intercept sensitive authentication data. The successful capture of NTLM hashes highlights the importance of disabling LLMNR/NBT-NS in secure environments.