Task 4 Report: Network Protocol Attacks Lab

Target: HackTheBox Machine
Tool: Responder

1. Attack Simulation Log

Attack ID	Technique	Target IP	Status	Outcome
015	LLMNR/NBT-NS Poisoning & SMB Relay	10.10.10.8	Success	NTLMv2 Hash Captured

2. Technical Execution Summary

Responder was deployed on the HTB interface (`ens224`) to poison LLMNR, NBT-NS, and HTTP traffic. The target machine, during its network operations, attempted to resolve a non-existent host. Responder successfully impersonated the requested host, forcing the target to authenticate and disclose the NTLMv2 hash of a user account. The captured hash is suitable for offline cracking or relay attacks.

3. Evidence

3.1. Responder Configuration and Active Poisoning

The attacker machine was configured to listen on the HTB machine and poison all relevant protocols.
Evidence: `09__NTLMv2_Hash_Captured_HTB.png` showing Responder actively running.

3.2. Successful Hash Capture

The target machine authenticated to the attacker-controlled host, resulting in the capture of a valid NTLMv2 hash for a user account. The hash provides all necessary components for offline password cracking.

Evidence: `10_NTLMv2_Hash_Captured_HTB.png` showing the captured username and hash.

4. MitM Attack Summary

Responder poisoned LLMNR/NBT-NS on the HTB network, tricking a target into authenticating to a fake host. This resulted in the capture of a user's NTLMv2 hash, demonstrating how insecure network protocols can be exploited to harvest credentials without direct interaction with the target.

5. Remediation Recommendations

1. Disable LLMNR and NBT-NS: Group Policy can be used to disable these protocols across a domain, forcing clients to use only DNS for name resolution.
2. Enable SMB Signing: Requiring SMB signing prevents SMB relay attacks by ensuring packet integrity and authenticity.
3. Network Segmentation: Segment networks to limit the broadcast domain, reducing the scope of poisoning attacks.
4. Monitor Network Traffic: Implement IDS/IPS rules to detect and alert on anomalous LLMNR/NBT-NS traffic or repeated failed authentication attempts.