

Forum:[Hack Forums](#)

Thread: [\[Red Team Internship\] Stuck Inside an Internal Subnet Seeking Suggestions](#)

Jokinha - July 9, 2025, 3:02 pm

Hi everyone,

I'm currently doing a Red Team internship at a large company. My objective for this engagement is to: Get initial access to machines in the internal network

Escalate privileges

Ultimately reach the domain admin or the main network admin accounts.

At the moment, I'm physically connected via Ethernet to one of the internal subnets. I only have access to this segment — no routing beyond it.

Here's what I've tried so far:

ARP Spoofing (Printer <-> Workstation) + Traffic Interception Successfully intercepted traffic between a network printer and a workstation.

Captured NTLM authentication hashes and a document being sent from the printer to the computer.

The NTLM hash couldn't be cracked despite trying several methods (including Hashcat + standard/common wordlists).

Responder + ntlmrelayx.py Managed to capture NTLMv2 hashes from local systems.

Unfortunately, these were NTLMv2 hashes, which are resistant to Pass-the-Hash techniques, and cracking attempts weren't successful either.

Additionally, Responder was generating noticeable network congestion due to the NBNS/LLMNR traffic it creates. Because of that, my supervisor specifically asked me to stop using it — such disruptions aren't allowed in this environment.

Nuclei Scanning Ran Nuclei scans against some internal IPs, using both official and community templates.

Mostly found printers with default admin credentials — nothing impactful so far.

SMB Enumeration + Brute Force Attempts (nmap, smbclient, smbmap, crackmapexec) No anonymous SMB shares.

Brute-force attempts were quickly blocked after a few tries, likely due to account lockout or rate-limiting.

No valid credentials obtained so far.

Password Attacks (Hydra, Medusa, Hashcat) Still no success in cracking the captured hashes.

No valid usernames/passwords for additional brute-force attempts yet.

Vulnerability Scanning (nmap NSE scripts, OpenVAS) Scanned internal hosts for known vulnerabilities.

No critical or exploitable issues identified on exposed services within the subnet.

Current Situation: No valid credentials.

No clear lateral movement or escalation vectors available.

No foothold beyond the subnet I'm connected to.

If you've faced similar Red Team situations: What would you try next?

Any specific techniques or tools you'd recommend for lateral movement or privilege escalation in an isolated subnet like this?

Any uncommon vectors you'd suggest exploring, especially considering I have physical access to

the Ethernet network?

I appreciate any insight or advice from your experience!

DramaKing - July 9, 2025, 3:27 pm

(Jul 9, 2025 03:21 PM)MarlboroMan Wrote: [\[CITE\]](#) If you can get a payload running on the printer you can in theory use it to pivot.

Also physically connected? Why not opt for a payload trough ducky?

Also read up on double tagging (not my territory):

Physical attacks on machines would almost certainly be outside the ROE.

Jokinha - July 11, 2025, 8:13 am

(Jul 9, 2025 03:21 PM)MarlboroMan Wrote: [\[CITE\]](#) If you can get a payload running on the printer you can in theory use it to pivot.

Also physically connected? Why not opt for a payload trough ducky?

Also read up on double tagging (not my territory):

Thanks a lot for your reply and for sharing your suggestions!

Regarding the pivoting part: how would I actually leverage this printer to gain access to another machine on the same network?

My goal here is specifically to gain control of other systems through the network by identifying and exploiting potential misconfigurations or network-based vulnerabilities. I'm not looking to use physical attack methods like a USB Rubber Ducky, since that would already require physical access to the target machines, which goes beyond the scope of my current objective. I want to stick with purely network-based approaches for this task.

That said, I'll definitely look into the double tagging technique you mentioned! I'm not very familiar with it, but I'll research it and see if it's something feasible in this case.

Thanks again for the input!