



CASE STUDY

On-network to full directory compromise, one relay at a time

Industrial manufacturing (IT + OT) · Internal network pentest (assumed on-network)

2 Critical — layered hardening plan

Anonymised under NDA. Client and identifying details are withheld. PXL Security LTD · Sofia, Bulgaria · pxlsec.com



CASE STUDY

On-network to full directory compromise, one relay at a time

Sector	Industrial manufacturing (IT + OT)
Engagement	Internal network pentest (assumed on-network)
Outcome	2 Critical — layered hardening plan

10 hosts reached by one relay	hundreds users enumerated anonymously	multiple EOL/OT systems found
---	---	---

THE CHALLENGE

A manufacturer with a flat-ish network mixing modern Windows AD, end-of-life midrange systems and operational-technology devices wanted to know the blast radius from an on-network foothold.

HOW IT UNFOLDED

1. Poisoned name resolution (LLMNR/NBT-NS/mDNS) and captured cleartext credentials from a legacy HTTP-Basic service.
2. Found SMB signing disabled broadly and proved NTLM relay end-to-end — a relayed machine account authenticated to around ten hosts.
3. Found LDAP signing and channel binding not enforced on the domain controllers; relayed to LDAP for a full authenticated directory dump.
4. Enumerated the domain anonymously via null session — hundreds of users and the password policy — and mapped grossly excessive privileged-group membership.
5. Catalogued EOL and OT exposure (an unauthenticated AJP file read on an EOL server, cleartext protocols and SMBv1 on a legacy midrange OS, and a vulnerable OT controller line).

KEY FINDINGS

Critical	NTLM relay to LDAP (signing/channel-binding not enforced)
Critical	Unauthenticated AJP file read on an end-of-life server
High	SMB signing disabled — cross-host relay
High	Anonymous AD enumeration and excessive admin membership
High	EOL midrange OS with cleartext protocols and SMBv1

IMPACT

A chain from an unauthenticated on-network foothold to a path to full Active Directory compromise — with OT systems reachable on the same network.

OUTCOME

A layered hardening plan: enforce SMB/LDAP signing and channel binding, disable LLMNR/NBT-NS, clean up privileged groups, decommission EOL systems and segment IT from OT — with a scoped second window for delegation and AD-CS paths.

TECHNIQUES

NTLM relay · LLMNR/NBT-NS poisoning · LDAP signing · EOL systems · OT exposure

SERVICES

Active Directory & Internal Network · Penetration Testing



Work with PXL Security

Independent offensive-security testing since 2014 — penetration testing, red teaming and secure development, delivered by senior engineers with evidence for every finding and a retest to prove the fix.

Request a proposal: pxlsec.com/contact · hello@pxlsec.com

PXL Security LTD · 12 Vasil Levski Blvd., 1142 Sofia, Bulgaria · VAT BG203239331