



CASE STUDY

The decade-old password behind Domain Admin

Retail bank · Red team: phishing + assumed breach

Defences validated, AD roadmap delivered

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

CASE STUDY

The decade-old password behind Domain Admin

Sector	Retail bank
Engagement	Red team: phishing + assumed breach
Outcome	Defences validated, AD roadmap delivered

0 / 2 phishing campaigns succeeded	1 path to Domain Admin found	dozens AS-REP-roastable accounts
--	--	--

THE CHALLENGE

A retail bank wanted to test its resilience to phishing, and to an attacker who has obtained a standard domain user on a virtual-desktop host.

HOW IT UNFOLDED

1. Ran two phishing campaigns — one blocked at the gateway, one delivered but ignored by well-trained staff.
2. Switched to assumed breach: a standard domain user on a virtual-desktop host.
3. Enumerated the domain with living-off-the-land native tooling only.
4. Identified a Domain Admin service account with a password unchanged for over a decade, carrying Kerberos SPNs.
5. Kerberoasted it for offline cracking; found dozens of AS-REP-roastable accounts and a stale never-expiring admin.
6. Segmentation between the virtual desktops and on-prem directory meaningfully limited further reach.

KEY FINDINGS

High	Kerberoastable Domain Admin service account, password unchanged for years
High	Dozens of accounts vulnerable to AS-REP roasting
Medium	Stale, never-expiring built-in administrator account
Positive	Phishing, awareness and segmentation controls all held

IMPACT

A single ordinary account could put a path to full-domain compromise within reach — while the bank's email controls, staff awareness and network segmentation all held as defence-in-depth.

OUTCOME

A clear privileged-account-hygiene and Kerberos-hardening roadmap, plus independent validation that the bank's phishing, awareness and segmentation controls were genuinely working.

TECHNIQUES

Phishing · Assumed breach · Living off the land · Kerberoasting · AS-REP roasting

SERVICES

Red Teaming · Active Directory & Internal Network · Social Engineering & Phishing



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