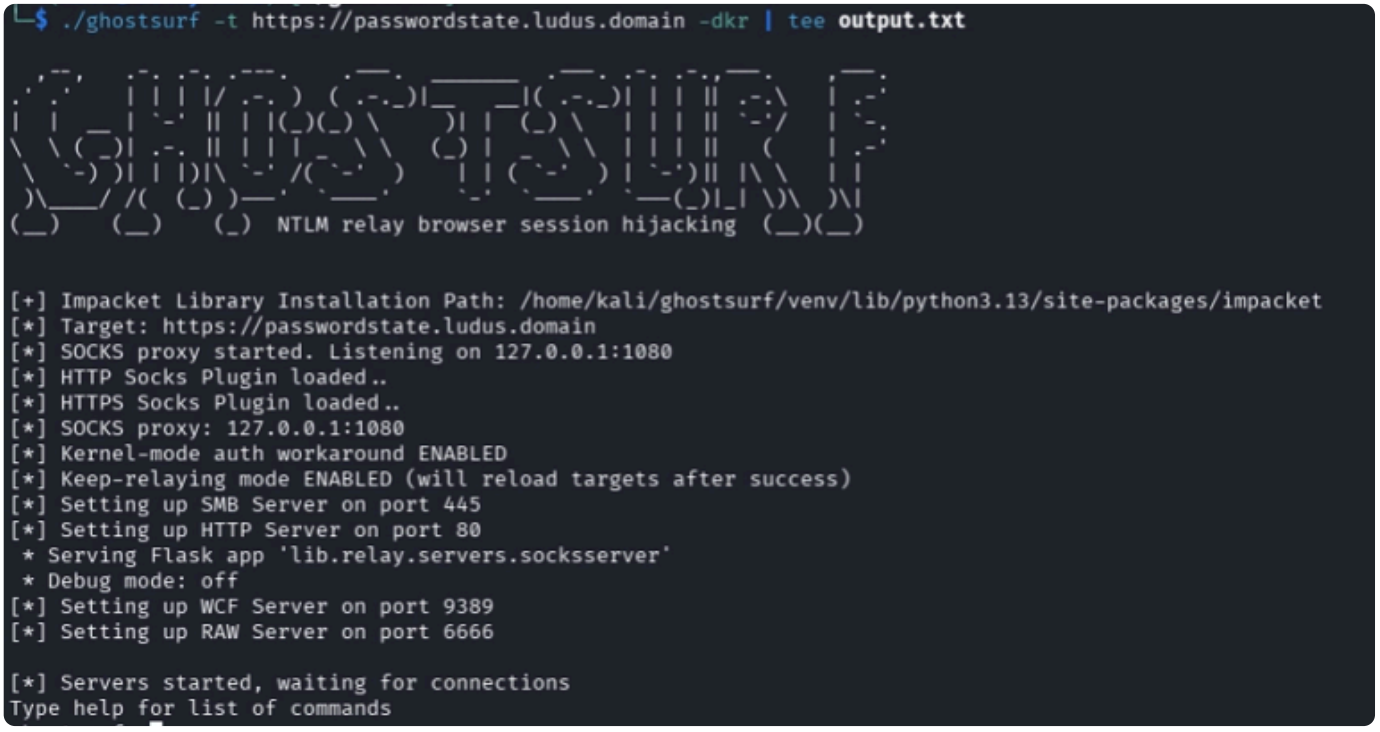
SPECTEROPS
Creators of BloodHound

SpecterOps Blog

Filters

Search Blog

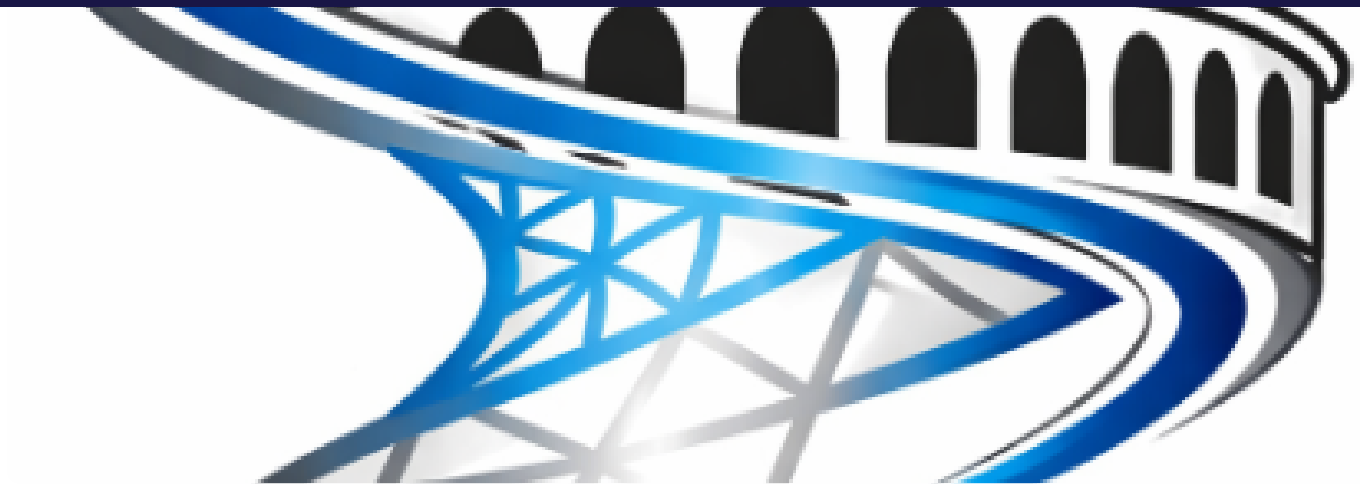


RESEARCH & TRADECRAFT

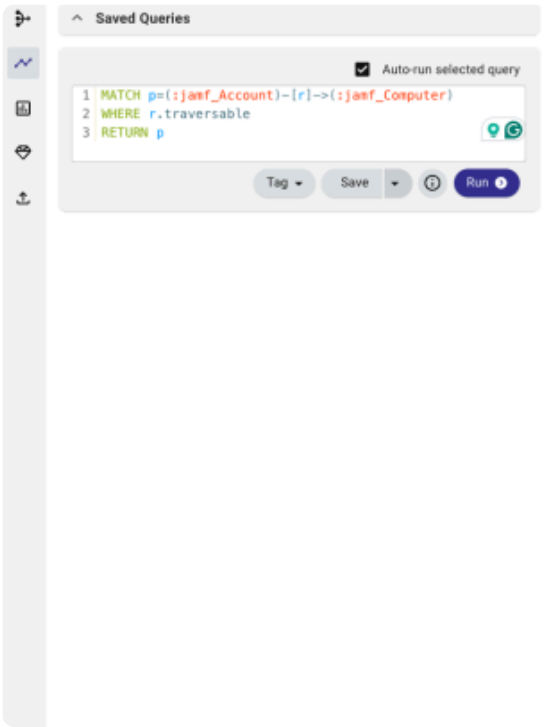
ghostsurf: From NTLM Relay to Browser Session Hijacking

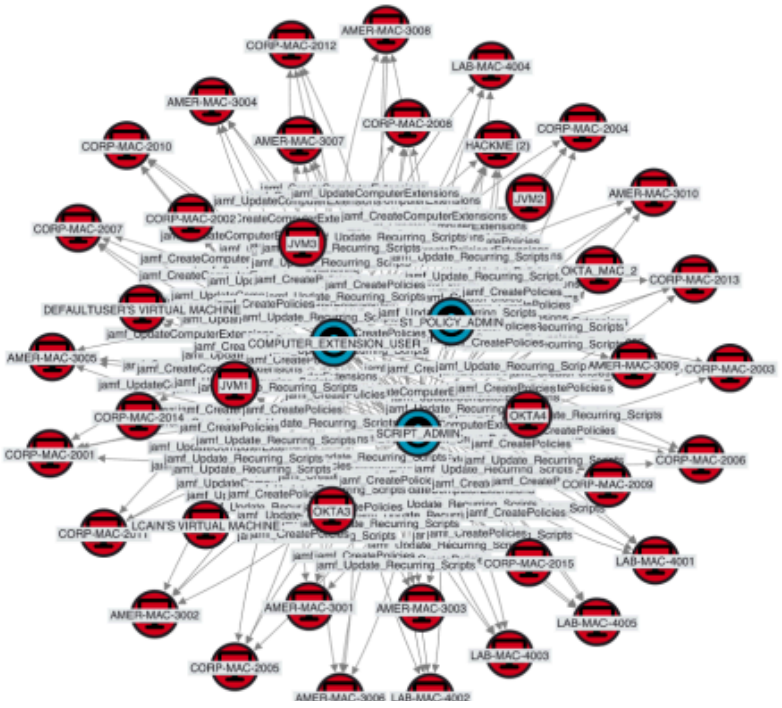
TL;DR: ntlmrelayx's SOCKS proxy works great for SMB and MSSQL but fails when you try to browse a web application...

By: Allen DeMoura 17 mins



RESEARCH & TRADECRAFT





BLOODHOUND

Expanding Attack Path Management to macOS Environments

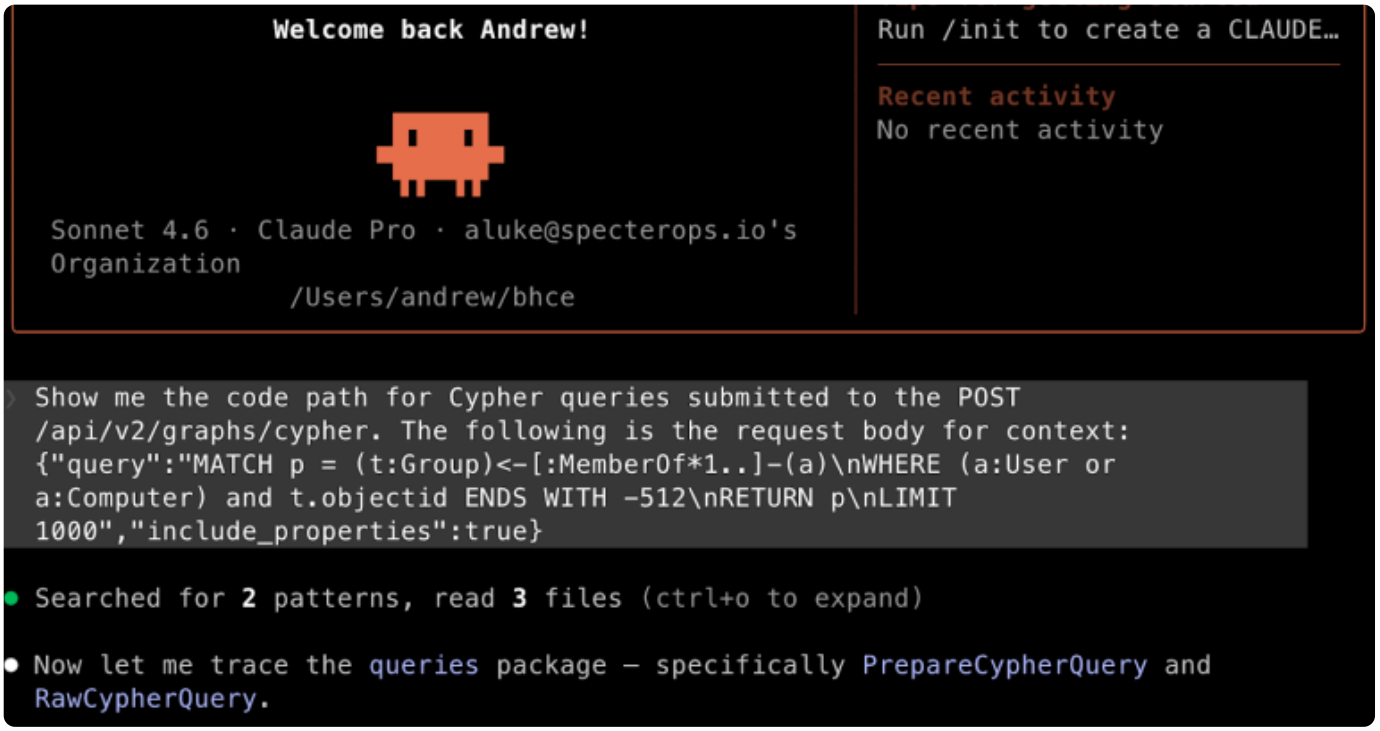
Introduction Attack path management has historically focused on identity systems like Active Directory and Entra ID. That focus made sense....

By: Jared Atkinson 11 mins

RESEARCH & TRADECRAFT

JamfHound v1.1 Update: SSO Attack Paths and Okta Additions

TL;DR : New SSO Attack Paths and Okta Edges in JamfHound: Updates have been added to the JamfHound OpenGraph collector...



RESEARCH & TRADECRAFT

Leveling Up Secure Code Reviews with Claude Code

TL;DR: Claude Code is a force multiplier when performing secure code reviews during an assessment. In this post, we discuss...

By: Andrew Luke 18 mins

RESEARCH & TRADECRAFT

Attack Paths Don't Stop at Identity Providers

Modeling Okta in BloodHound Enterprise to uncover cross-platform identity risk Introduction Identity is no longer confined to a single system....

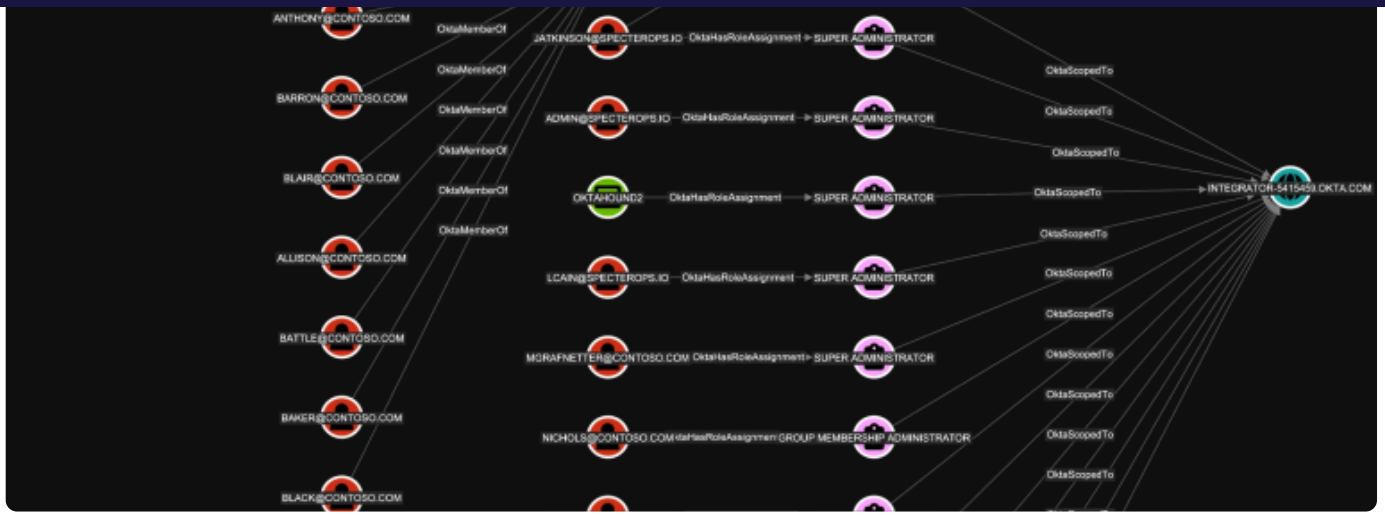
By: Jared Atkinson 10 mins

RESEARCH & TRADECRAFT

RTFM: Read The Fatal Manual – When Vendor Documentation Creates Critical Attack Paths

TL;DR: Trusted vendor documentation across 16 major technology companies were actively guiding administrators to deploy critical misconfigurations (often Active Directory...

By: Martin Sohn Christensen 55 mins



BLOODHOUND

Discovering Unexpected Okta Attack Paths with BloodHound

TL;DR: OktaHound is a new data collector for the Okta Platform that ingests information about entities and their relationships within...

By: Michael Grafnetter 15 mins