

STALE NETWORK ADDRESS CONFIGURATIONS (SNAC) ATTACK

The attackers take advantage of a system or a network service that has been configured with a hard-coded IP address or fully qualified domain name (FQDN) that is no longer associated with a live host.

DETECTION

Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

Eavesarp



<https://github.com/arch4ngel/eavesarp>

<https://www.blackhillsinfosec.com/analyzing-arp-to-discover-exploit-stale-network-address-configurations>



PIVOT and ESCALATE

Created by: **BLACK HILLS** | Information Security