

Making \$ With COMPUTER\$

Queen City Con 0x3

John Askew & Jake Hildreth

2025-11-07

John

Hacker

Red Team Lead



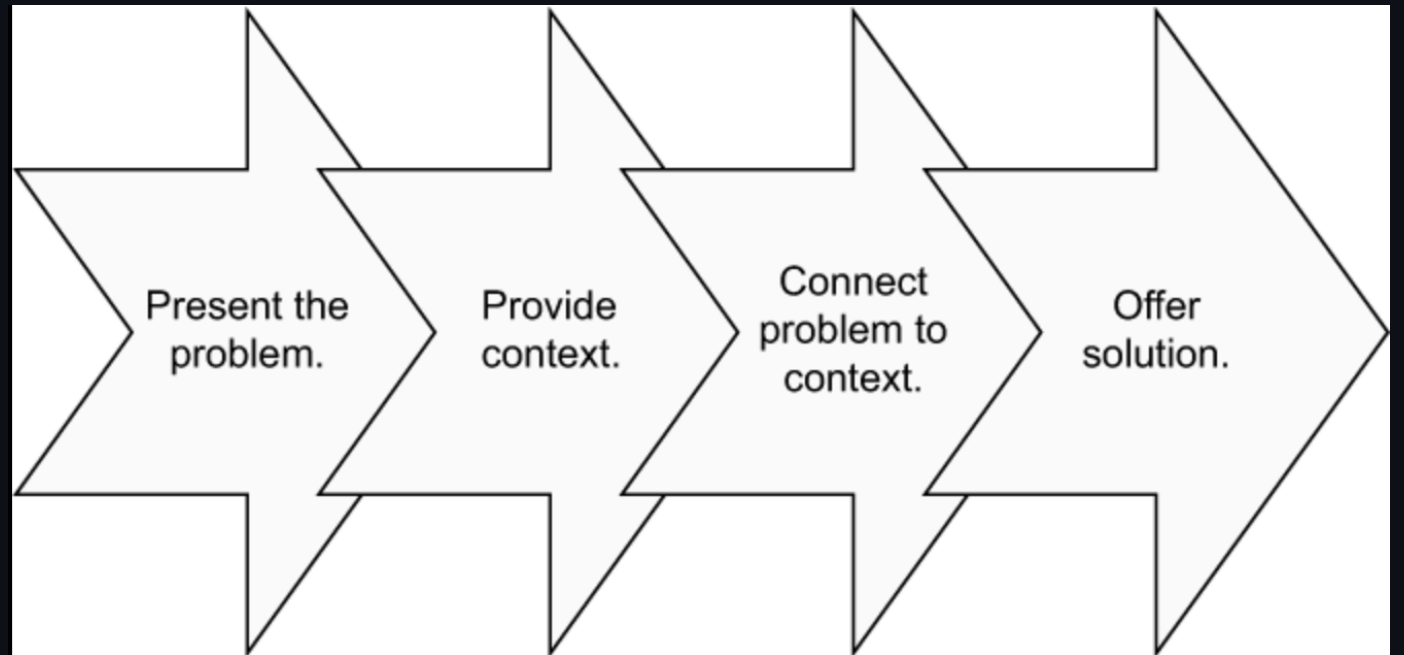
Jake

Defender
Security Consultant



Agenda

- The Problem
- Some Context
- A Demo or Two
- Some Solutions



**If a user can join a computer to your domain
they can own your Active Directory forest**

**If a user can join a computer to your domain
they can own your Active Directory forest in minutes**

The Problem

- `ms-DS-MachineAccountQuota` attribute
 - Number of computers a *regular* user can add to the domain
- Active Directory (AD) default value: 10
 - Still the default in most environments
- Made sense 25 years ago
 - But now computers are more dangerous!

Why This Matters:

What Makes Computer Accounts Special?

- Password differences:
 - Complex & 120 characters long
 - Changed automatically by AD every 30 days
- Service Principal Names (SPNs)
 - Tells others what services are available
- Note: local admin password is NOT the computer account password

The Attacker's Advantage