



15 - Post-Compromise Attack Strategy



POST-COMPROMISE ATTACK STRATEGY

- ✓ We have an account, now what?
- ✓ Search the quick wins
 - Kerberoasting
 - Secretsdump
 - Pass the hash / pass the password
- ✓ No quick wins? Dig deep!
 - Enumerate (Bloodhound, etc.)
 - Where does your account have access?
 - Old vulnerabilities die hard
- ✓ Think outside the box



TCM Security

It comes down to, we have an account, now what do we do?

We do not need shell in machines unless we are desperate. Rinse, and repeat.