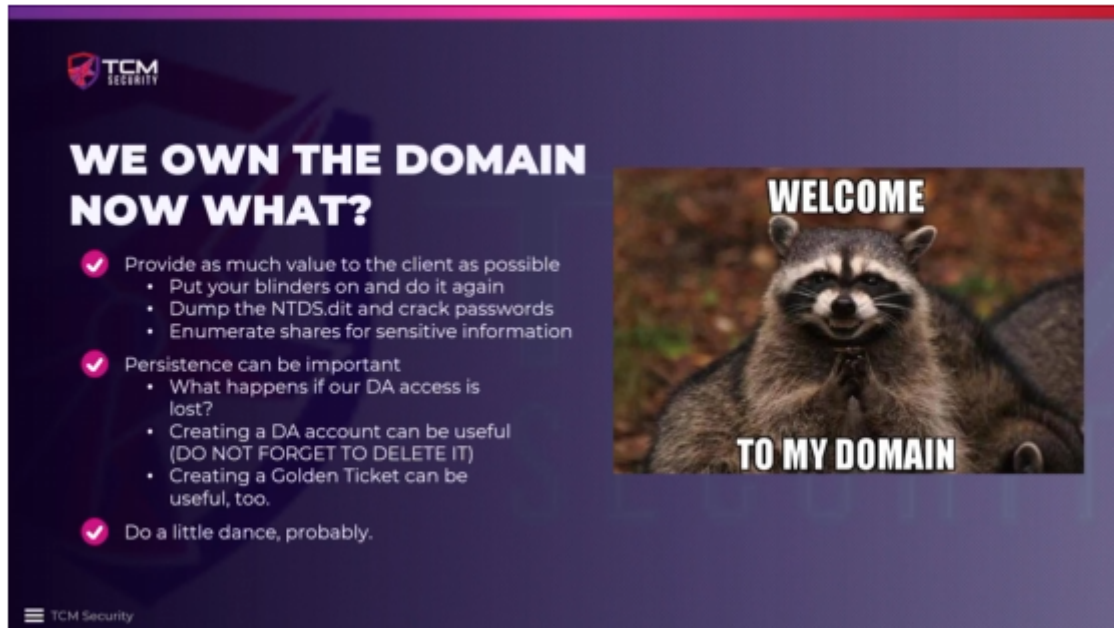


00 - Post-Domain Compromise Attack Strategy

We own the Domain, now what do we do?



TCM SECURITY

WE OWN THE DOMAIN NOW WHAT?

- ✓ Provide as much value to the client as possible
 - Put your blinders on and do it again
 - Dump the NTDS.dit and crack passwords
 - Enumerate shares for sensitive information
- ✓ Persistence can be important
 - What happens if our DA access is lost?
 - Creating a DA account can be useful (DO NOT FORGET TO DELETE IT)
 - Creating a Golden Ticket can be useful, too.
- ✓ Do a little dance, probably.

WELCOME TO MY DOMAIN

TCM Security

DA : Domain Admin. It is a very good idea to do that so we can add persistence, and this is a good test to see the organizations cybersecurity posture. They need to notice the account not too long after we create it. This would be something they needed to be alert off.

If we do create a Domain Admin account, we need to make sure to delete it before the assessment is done. Or have the client delete it, but make sure it is deleted.

As Penetration tester we are trying to give as much valuable information to our clients as possible. If we own the domain in day 1, and there are 2 weeks worth of assessments, we go back and try to find other vulnerabilities.