Le meilleur ami du pentester: les mots de passe

Par Martin Dubé

$ ./start.sh

- Qui suis-je?
- Les mots de passes?
- Réalité Entreprise
- Vision du Pentester
- Mitigations
- Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo Demo :)

$ whoami

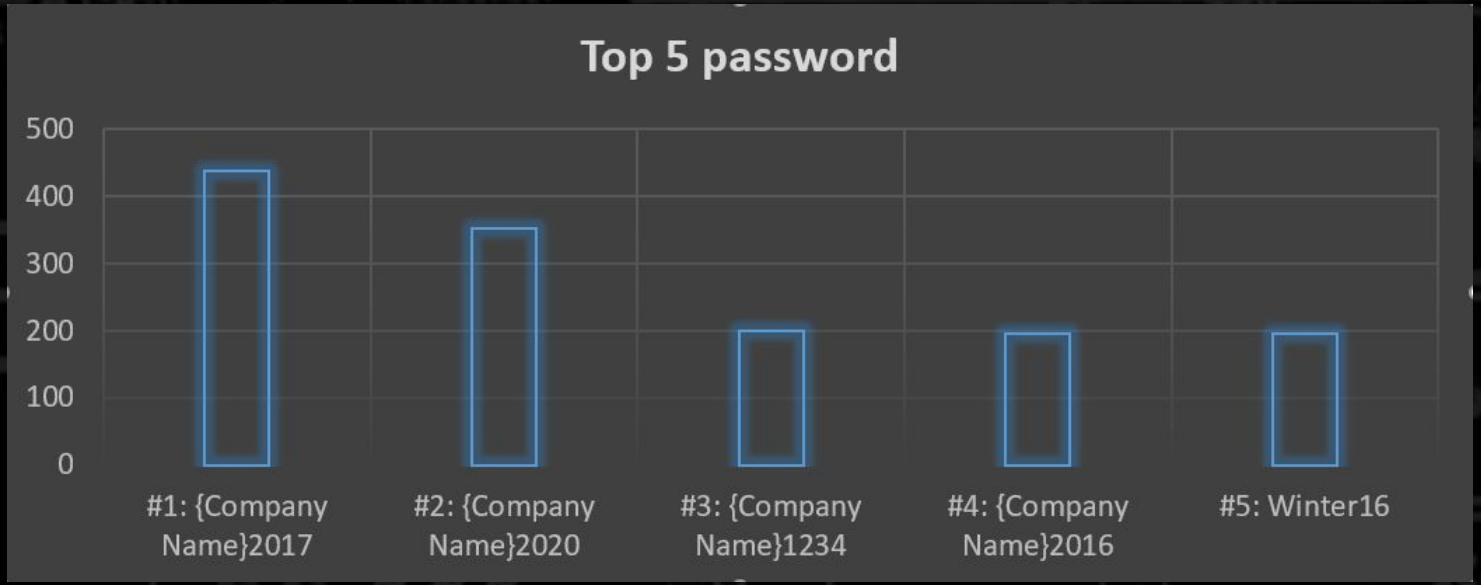
- Pentester @ GoSecure depuis 2 ans
- Co-administrateur du Hackfest de 2011 à 2015
  - Intérêt particulier pour les War Games et autre CTFs
  - Toujours impliqué dans les CTFs
- Promoteur de systèmes sécure par défaut
  - Adore OpenBSD
  - Apprenti jedi de FreeBSD
  - Haineux, parfois hostile, avec Windows
- Ninjutsu!
  - https://www.facebook.com/Bujinkan-Sannin-Dojo-108992469158396/
- Sera dû pour un Scotch après cette présentation

$ echo /etc/motd

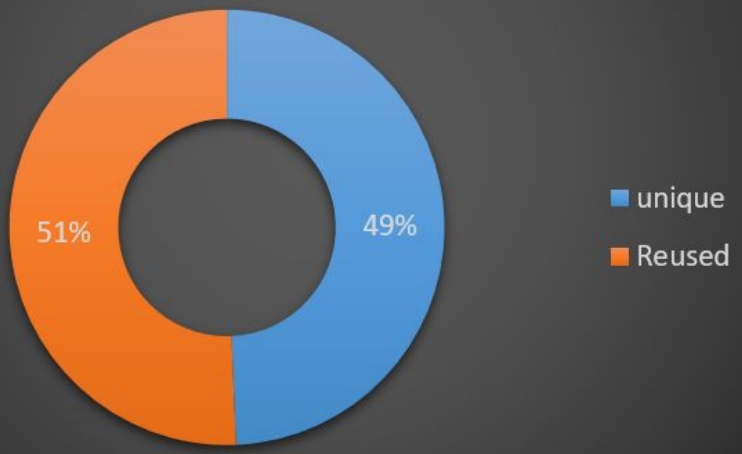
- Public Cible
  - Entreprises (surtout)
  - Actuel/Future pentester
  - Enthousiaste
- Objectif
  - Ouvrir les yeux sur l'Univers Microsoft
  - Discuter de l'importance des mots de passes forts
  - Avoir du plaisir

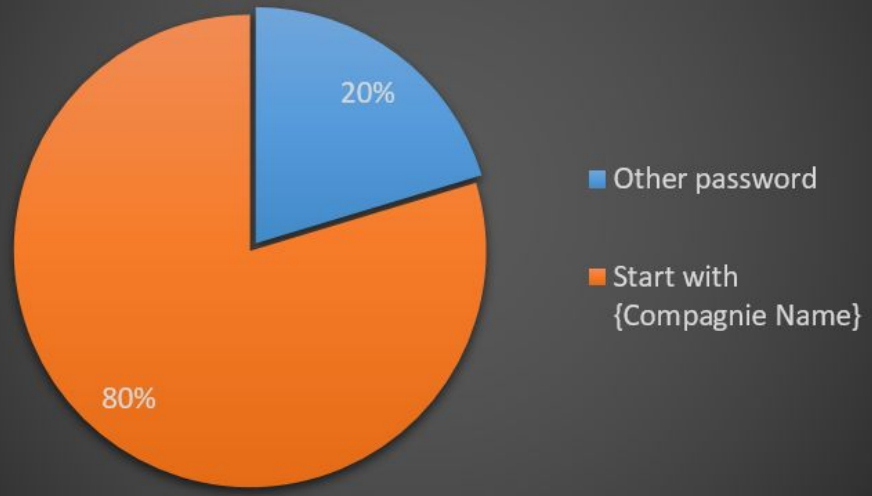
Réalité Entreprise

Réalité Entreprise

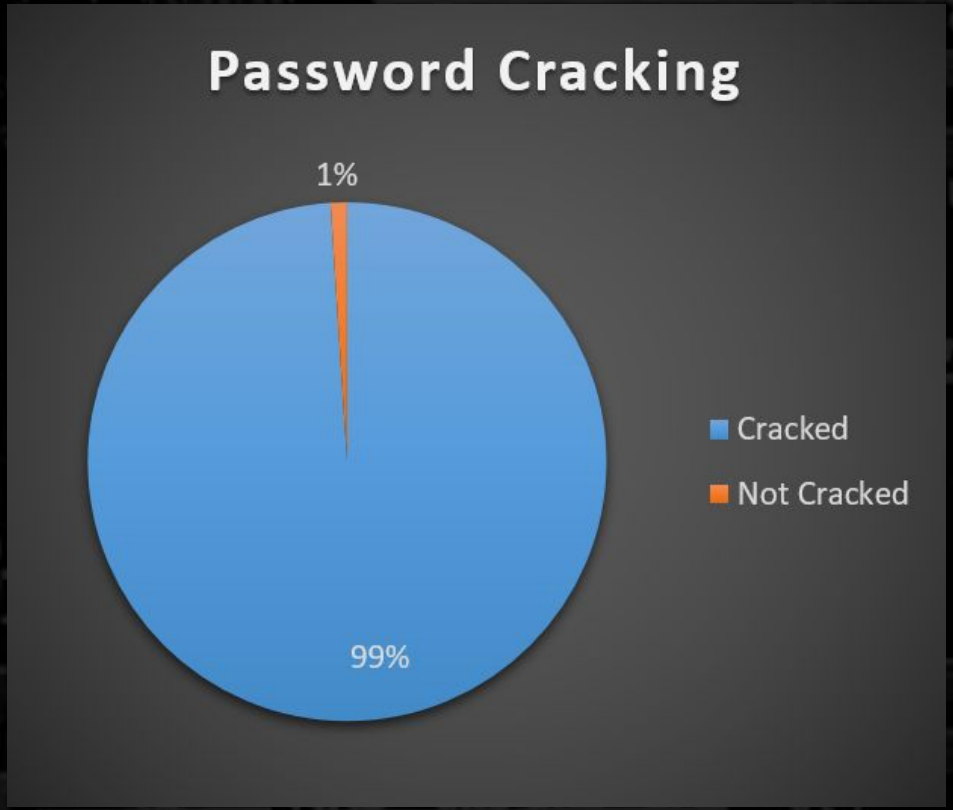


Réalité Entreprise





Réalité Entreprise



Vision du Pentester

- CVSS v3
  - Simple facteur d'authentification sur site web: 6.5 (Modéré)
    - Scope Unchanged
  - Simple facteur d'authentification sur VPN: 7.2 (Élevé)
    - Scope Changed
  - Mots de passes faibles: 7.3 à 10 (Élevé à Critique)
    - Souvent considéré Médium
  - Ségrégation inadéquate des réseaux: 5.6 (Modéré)

Mitigations

- Multiple facteurs d'authentification
- Politique de mot de passe avancée
  - Filtre de mots clés
  - Configurer une DLL de filtrage sur l'AD

La recette

- Étapes habituelles (Phase Externe)
  - Recherche de nomenclature
  - Énumération d'usager
  - Identification de mot de passes
  - Password Spray
  - Shell / VPN
- Étapes habituelles (Phase Interne)
  - NetBIOS / LLMNR
  - Kerberoast
  - Crack
  - Domain Admin

Hacking Time!


KUNG FURY