H4ck 1n TN

De la collecte d'informations à l'extraction

Valentin Giannini

Ceten – TELECOM Nancy

November 3, 2015

Introduction

Reconnaissance

Quesako

Pourquoi

Droit

Introduction

Reconnaissance

Collecte d'informations

HTTrack

- Clone d'un site web
- Examiner le site
- Collecte de numéros, emails, ...

Google,...

- Indexe tout et n'importe quoi
- Opérateurs *rightrow* nom:terme
  rightrow site, intitle, allintitle, inurl, filetype, cache, ...
- Exemple : inurl:admin site:telecomnancy.eu

The Harvester

Whois, Netcraft, Hosts

Whois

- Informations sur le propriétaire du domaine
- Informations de localisation

NetCraft

- Moteur de recherche
- Informations supplémentaires
  rightarrow IP, OS, versions, DNS? ...

Hosts

- Récupération d'adresse IP
  (Modèle OSI : couche 3)

DNS

DNS

- Premières cibles
- Plan du réseau
- Mal protégés/configurés

NSlookup

- Obtenir des enregistrements
- Exemple :

  $ nslookup
  > serveur X.X.X.X
  > set type=any
  > domaine.com
  Server : Y.Y.Y.Y
  Address : Y.Y.Y.Y#53

Messagerie

- Serveurs internes
- Messages d'erreurs
  rightarrow Envoie de .bat, .exe, ...

Social Engineering

En attendant une futur présentation

- Utiliser la stupidité des gens
- Utiliser l'usurpation d'identité
- Jouer un rôle avec les cibles
- Et plus encore...

Ping

Scan de ports

Script Nmap

Scans de vulnérabilités

Medusa

Metasploit

John

Wireshark

Bases

Injection

ZAP

Netcat et autres

Rootkit

Meterpreter

Comment la faire