Formation « Red Team – Sans-fil »

Réf : REDTEAM

L'apparition de nouvelles technologies permettant d'automatiser les contrôles d'accès nécessitent aujourd'hui de nouvelles techniques en plus du social engineering et des techniques de crochetage, afin de s'infiltrer dans un bâtiment de manière discrète.

Pour cela, nous avons programmer ce cours, permettant de montrer différentes attaques actuelles visant à gagner des accès physiques en s'attaquant des technologies telles que : le RFID, Bluetooth LE (avec les serrures connectées, etc.), nRF utilisés dans les claviers/souris et Sub-GHz (alarmes, portes de garage, clés voiture, etc.).

L'objectif de ce cours est montrer des techniques efficaces et rapides afin de réaliser des tests d'intrusions, mais aussi de montrer les aspects à sécuriser afin d'éviter certains scénarios à une entreprise qui pourrait être la cible de ces attaques.

Objectifs

- Evaluer et identifier les points faibles des systèmes de contrôles d'accès sans-fil
- Exploiter ces faiblesses afin de réaliser un Red Team de manière efficace
- Faire les bons choix technologiques pour une entreprise

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Auditeurs en sécurité
- Consultants en sécurité
- RSSI avec profil très technique
- Développeur de produits de sécurité employant du sans-fil
- Serruriers

Pré-requis

- Connaissances en administration Linux
- Bases en sécurité informatique
- Traiter des données sous formes binaires, hexadécimales, etc.
- Optionnellement quelques bases en sécurité hardware, qui peuvent être très complémentaires

Méthode pédagogique

- Cours magistral et rappels (environ 30%)
- Démonstrations et exercices pratiques (environ 70%)

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

RFID

- Introduction
- Outils dédiés et démonstrations
- Identification de badge LF et cas
- Attaques sur les différents badges LF (HID, EMx, etc.)
- Identification de badges HF et différents cas
- Attaques sur les badges HF courants (MIFARE Classic/Ultralight/DESFire, iClass etc.)
- Exercices sur des cas courants (tag hôtel, accès aux bâtiments, etc.)
- Les différents types de cartes « magiques » et cas d'utilisation
- Introduction à des outils plus poussés dans la recherche de vulnérabilités comme le HydraNFC

Bluetooth LE

- Introduction
- Monitorer les communications
- Outils existants
- Clonage de beacons
- Attaques Man-In-The-Middle
- Injection de trames
- Attaques sur les connexions sécurisées

nRF

- Introduction
- Analyse de la communication radio brute
- Monitoring des communications avec des outils dédiés
- Transformer un dongle de souris/clavier en implant RuberDucky à distance et en locale

Liaisons sub-GHz

- Introduction
- Identification de signal et analyse en radio-logicielle et comparaisons avec d'autres outils
- Attaque sur des communications non-sécurisées
- Analyse de communications sécurisés et défis techniques
- Attaques de communications sécurisées avec du Rolling/Hopping code
- Attaques opportunistes sur des technologies sécurisés et défauts d'implémentation

Dates de nos prochaines sessions disponibles sur la page :
https://www.hs2.fr/redteam