AmarOk

Zeste de savoir

(1/3)Retour du nsec : Introduction au badge hacking

21 décembre 2018

Table des matières

% (1/3)RETOUR DU NSEC : INTRODUCTION AU BADGE HACKING % AmarOk % 27 mai 2018

1. Introduction

Comme expliqué dans mon précédent billet (https ://zestedesavoir.com/contenus/2479/r2-pour-changer-de-gdb/), j'ai participé au NorthSec 2018 , une grosse compétition de sécurité en Amérique du Nord.

Au final, quelques épreuves valent un article, certaines où je n'ai pas les connaissances (par exemple, pour une épreuve web, il fallait réaliser du Prototype pollution attack) et quelques unes assez drôle.

Je vais donc m'attarder sur 3 challenges :

1. Pour la conférence, chaque personne possède un badge contenant le programme de la conférence, des LEDs qui clignotent, des PINS, une interface bluetooth et... 2 FLAGS (cet article).
2. On vient de recevoir 10 pdfs de 300 pages, le but est de trouver quelle page a été imprimée sur une imprimante différente des 2999 autres.
3. Un agent se trouvait dans une pièce ou une conversation top secrète a eu lieu. Il a réussi a enregistrer cette conversation, cependant comme le son de la vidéo n'est pas disponible, il faut reconstruire cette conversation à partir des vibrations du paquet de chips pris en vidéo.

Voici donc le premier article (en espérant avoir le temps d'écrire les deux suivants), avec une introduction de hacking de badges.

Note : les deux tracks des prochains articles n'ont majoritairement pas été fait par moi pour le coup (équipe de 8 et j'avais déjà fait un challenge semblable au second).

2. Recherche d'informations

La première étape, lorsqu'on commence une épreuve de ce type et de comprendre comment le badge fonctionne et où souhaite nous amener les créateurs de ce badge.

Ainsi, il faut le regarder en détails et parcourir un peu les différents menus déjà disponibles.

Voici le badge en question :

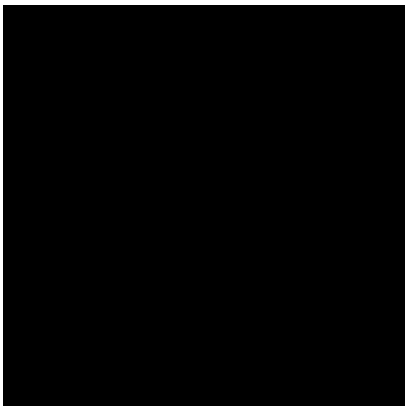

FIGURE 2. – Badge

Du coup, on peut voir qu'il y a différents menus, "Conférence schedule", "LED patterns" (basic/extra), "Settings" (LED, Turn screen off, flashlight, credits, sync key), "Battery status", "Battery warning". On remarque aussi un code en morse sur le PCB du badge ; (... .–. ..- - -. .- -.- .-.-.- –. .-) soit https ://sputnak.ga qui... nous donne la doc du badge. Bon début !

On obtient donc les circuits, la documentation des services bluetooth, les fichiers gdb. On est prêt.

3. Premiere piste, jouons avec le bluetooth

Commençons par jouer avec le bluetooth, vu qu'on à la doc. Par exemple pour changer le nom de *Cosmonaute #57* pour *AmarOk*.

D'après la documentation, il suffit d'envoyer la string vers le service *CBCA0101-BFBE-BDBC-BBBA-AFAEA* après l'avoir débloqué. Le processus complet donne :

1. Avec une application (*BleTerm* pour Android par exemple), envoyer la clé des settings vers *CBCA0102-BFBE-BDBC-BBBA-AFAEADACABAA*
2. Vérifier que le badge est prêt en lisant *CBCA0103-BFBE-BDBC-BBBA-AFAEADACABAA*
3. Envoyer le nom sur *CBCA0101-BFBE-BDBC-BBBA-AFAEADACABAA*

et c'est tout...

Le badge étant renommé, on peut maintenant commencer à cherche les flags. Pour moi à ce moment, je vois deux pistes.

1. Exploitation d'une faille bluetooth. Ça tombe bien avec des trucs comme Blueborne
2. Trouver une variable style *enable_hidden_options*. En regardant le code avec `gdb`, on peut directement la modifier et découvrir ce menu ou l'activer en envoyant du courant sur un pin par exemple. C'était le cas pour la DEFCON 24 avec Black magic probe (utilisé aussi pour ce badge)

Élément externe (vidéo) —
Consultez cet élément à l'adresse (.

---

https ://www.youtube.com/embed/mcq4ENOhuhc)[Video][]

Pour la première possibilité, je voyais un contre et un pour. Le contre, c'est qu'il me semble que le badge de l'année précédente, il s'agissait d'un exploit sur un service bluetooth. Le pour, c'est qu'un service existe (visible via `BleTerm`, mais n'est pas documenté). Après discussion, il semble que ce service était documenté et il s'agissait du changement de l'image du badge. À voir plus tard, je commence par fouiller avec `gdb`

4. La recherche du menu caché

J'ouvre donc `gdb` espérant voir quelques symboles. Pour ceci, je branche la carte `STM` en appuyant sur le boutton `DFU` et en suivant la documentation on voit très vite... un segfault mais à ma grande décéption, pas de symboles. Un peu moins de chances d'avoir un menu caché, ou plus difficile à trouver.

Du coup, back to the basics, effectuons tout de même un dump de la mémoire avec `gdb`. En recherchant sur internet on remarque très vite que la taille à dumper pour le `STM32F070F6` qu'on dumpe alors avec `gdb` avec `dump memory file début fin` avec début et fin les adresses que l'on souhaite (perso j'ai mis 0 et `0x08000000`)

Puis, on regarde ce qui se trouve dans la mémoire (avant de chercher sur internet comment faire pour se device, la commande `strings` est toujours utile (avec l'option `-e l` parfois)).

On trouve alors plein de choses intéressantes. Les strings contenant le programme, pas de strings ayant l'air de contenir un menu secret, notre pseudo, plein de caractères hexa (dont surement ceux pour déverouiller les extra led, perso j'ai juste regardé le code marqué sur le ballon géant au milieu de la pièce) et surtout :

```
 AmarOk@tars3 ▶ ~/nsec/badge ▶ strings dumpfinal| rg FLAG
NRF_ERROR_INVALID_FLAGS
FLAG-60309301fa5b4a4e990392ead6ac7b5f
FLAG-HDXudrQxavLgMGxIVDrzqLsAGdRJCQAh
FLAG-60309301fa5b4a4e990392ead6ac7b5f
```

```
FLAG-UQKhqeDkniYtZTkVIQemdYfNTqEWPDNu
FLAG-60309301fa5b4a4e990392ead6ac7b5fFLAG-UQKhqeDkniYtZTkVIQemdYfNTqEWPDNu
```

Les flags ! En tentant de soumettre, on remarque que deux fonctionnent. Nos flags sont trouvés.

Note : au début j'avais réalisé un plus petit dump contenant 2 flags. J'ai donc essayé de soumettre `FLAG-HDXudrQxavLgMGxIVDrzqLsAGdRJCQAh` puis `FLAG-md5(HDXudrQxavLgMGxIVDrzqLsAGdRJCQAh)` et `md5(FLAG-HDXudrQxavLgMGxIVDrzqLsAGdRJCQAh)` dans le doute.

5. Conclusion

Au final, un peu déçu d'avoir voulu partir trop loin avec exploit de bluetooth ou menu caché alors qu'il s'agissait d'un simple dump :D, mais ça donne l'occasion de faire un peu le tour des différentes approches pour faire des trucs rigolos avec le badge de la conférence.