SYNACKTIV

Retex du pwn2own

FIC 2024 Box2Box

27/03/2024

whoami

SYNACKTIV

- 0xMitsurugi
- Ninja @ Synacktiv
- Pôle reverse-engineering

Plan

SYNACKTIV

- Le pwn2own, qu'est ce que c'est ?
- Pwn de routeurs
- Conclusion

Le pwn2own

Pwn2own

SYNACKTIV

- **Concours organisé par ZDI**
- **3 à 4 fois par an**
  - IOT
  - Logiciels/OS
  - Automotive
  - Scada

Pwn2own

SYNACKTIV

- **You pwn, you own**
- **Liste de produits à attaquer connue à l'avance**
  - Entre 1 et 3 mois
- **Le produit est mis à jour jusqu'au jour du concours**
- **Il faut prouver une exécution de code arbitraire**
  - Élévation de privilèges
  - Exécution de code à distance (RCE)
  - Etc…

Pwn2own

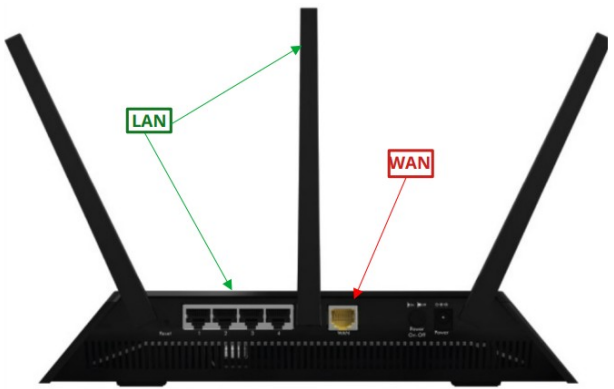
SYNACKTIV

- **Participation sur place ou à distance**
- **5 minutes pour prouver le “pwn”**
  - Généralement un shell
- **3 essais maximum**
- **En cas de victoire, on gagne :**
  - l’équipement
  - des master of pwn points
  - des $$$

- **Les vulnérabilités doivent être des 0-days**
  - Non publiques
  - Non connues de l'éditeur
- **Concours de 0-day**
  - Pas de bruteforce de mot de passe
  - Pas de man-in-the-middle de connexion d'admin
  - Pas de déni de service
  - Pas d'infoleak

Les cibles présentées ce jour

SYNACKTIV

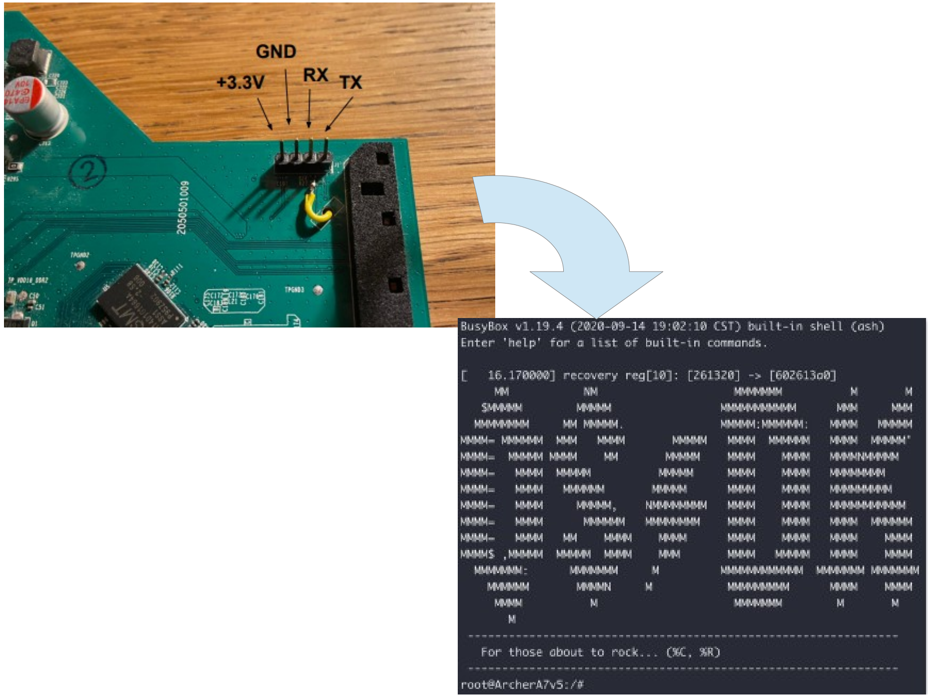


- **Routeurs SOHO**
- **Tp-link/ Cisco/ Netgear/ etc...**
- **Deux angles d'attaque**
  - LAN
  - WAN

Pwn des routeurs

TP-LINK AC1750

- **Analyse du firmware**
  - Statique via extraction
  - Dynamique via UART
- **Attaque côté LAN**
- **Plusieurs ports en écoute**
  - Webadmin
  - Dropbear
  - TdpServer ← ??



TP-LINK AC1750

SYNACKTIV

- Attaque d'un service de roaming
- Overflow dans une shared memory

TP-LINK AC1750

SYNACKTIV

- **Attaque d'un service de roaming**
- **Overflow dans une shared memory**
- **Exécution de code**
  - Une seule fois
  - Seulement 4 (!!) instructions MIPS
- **Activation d'un démon de debug**
  - Et injection de commande

Netgear R6700v3

SYNACKTIV

- **Extraction et analyse du firmware**
  - Statique
  - Dynamique via un shell de debug (merci netgear)
- **Attaque côté WAN**
- **0 port en écoute**

```
Host is up (0.00059s latency).
All 65535 scanned ports on netgear (172.16.1.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Netgear R6700v3

SYNACKTIV

- **Le routeur télécharge des bases de filtrage d'URL**
  - En HTTPS :-(
  - Mais sans vérifier le certificat :-)

Netgear R6700v3

SYNACKTIV

- **Le routeur télécharge des bases de filtrage d'URL**
  - En HTTPS :-(
  - Mais sans vérifier le certificat :-)
- **Erreur de parsing dans le fichier d'update**
  - Stack buffer overflow
  - Pas de cookie
  - ASLR partiel
- **Setup de mitm accepté par ZDI**

Netgear RAX30

SYNACKTIV

- **Firmware**
  - Statique et dynamique
- **Attaque LAN**
  - Plusieurs ports en écoute
  - Webadmin, …
- **Attaque WAN**
  - Aucun port en écoute (ou pas?)

Netgear RAX30

SYNACKTIV

- **LAN** 
  - Injection de commande fiable
- **WAN** 
  - Telnet ipv6 activé
  - Avec un mdp par défaut…

Netgear RAX30

SYNACKTIV

- **LAN** 🚀
  - Injection de commande fiable
- **WAN** 🚀
  - Telnet ipv6 activé
  - Avec un mdp par défaut…
- **Patchées la veille du concours**
- **Passer de 0-day à 0**
  - Mais fun à trouver

Conclusion

Conclusion

SYNACKTIV

- **Trouver des 0-day c'est fun \o/**
- **De nombreuses participations au pwn2own pour Synacktiv**
  - Des routeurs, caméras, Teslas, Mac OS, Windows, Linux, Virtualbox, NAS, imprimantes, enceintes, etc.. etc.. ont plié devant les ninjas
- **Trois fois master-of-pwn**
- **Last update :**
  - *pwn le 20 mars 2024 : tesla*

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com