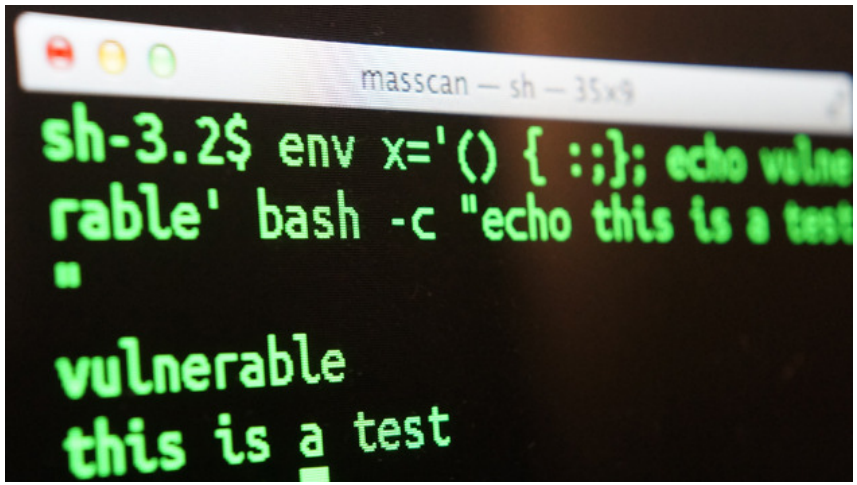
Petit apparté: ShellShock …



- Nom le plus répandu: *ShellShock*, se nomme aussi *bashdoor* et *bashbug*
- Bug de *Bash*, découvert le 12 septembre 2014!
- Divulgué le 24 septembre 2014. Grosse couverture médiatique.
- Moins de 24h après la divulgation du bug, plus de 17400 attaques sur plus de 1800 domaines provenant de 400 adresses IP (55% Chine & USA)
- En date du 30 septembre: pas moins de 1.5 millions d'attaques par jour (DDOS)
- 6 octobre: les serveurs de Yahoo sont compromis

- Les programmes qui sont en cours d'exécution possèdent leur liste de variables d'environnement.
- Quand un programme lance un autre programme, il fournit normalement la liste des variables d'environnement à ce nouveau programme.
- De façon indépendante, *Bash* maintient également une liste de variables d'environnement, et également une liste de fonctions internes.
- Puisque *Bash* opère comme un interpréteur de commande et une commande, il est possible d'exécuter *Bash* à partir de lui-même.
- Lorsque cela survient, l'instance originale de *Bash* peut exporter les variables d'environnement et les fonctions internes dans la nouvelle instance de *Bash*.
- Les définitions de fonctions sont exportées en les encodants dans des variables d'environnement dont la valeur commence avec des parenthères suivi de la définition de la fonction.

- En démarrant, la nouvelle instance de *Bash* va « scanner » ses variables d'environnement.
- Lorsqu'elle trouvera des variables dont la valeur débute par des parenthèses, elle effectuera la conversion variable → fonction interne en créant un fragment de code et en l'exécutant.
- **Problème:** Les versions de Bash affectées ne vérifient pas au préalable que ladite définition de la fonction soit dans un format valide… Créant du même coup une faille de sécurité.
- Par conséquent, quelqu'un de mal intentionné à qui on donnerait l'opportunité d'exécuter Bash et en lui donnant la chance d'entrer des valeurs arbitraires dans les variables d'environnement pourrait faire du tort au système.
- Exemple, faille de sécurité:

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

- **Problèmes**:
  - Web server : plusieurs sont basés sur Bash et exécute des Bash scritps.
  - Ssh-server: idem
  - Autres…
- **Attaques (jusqu'à maintenant…):**
  - Yahoo (DDOS)
  - Akamai technologies (DDOS)
  - United States Department of Defense (Script malveillant, balayage du contenu des serveurs)
  - Plusieurs autres

  - http://www.bbc.com/news/technology-29375636
  - https://www.youtube.com/watch?v=MyldPMn95kk