EthACK

The Swiss Privacy Basecamp

All your databases belong to us

2016-12-12

EthACK

The Swiss Privacy Basecamp

EthACK ?

- Éthique
- État
- ACKnowledgement (reconnaissance)
- Hacking (éthique, évidemment)
- . . .

EthACK ?

- Éthique
- État
- ACKnowledgement (reconnaissance)
- Hacking (éthique, évidemment)
- . . .

Pourquoi ?

- Notre gouvernement ne s'intéresse pas (ou peu) au sujet
- Les sociétés privées nous fichent à notre insu
- Personne ne sait où sont leurs données, qui les traitent, à quoi elles servent

Pourquoi ?

- Notre gouvernement ne s'intéresse pas (ou peu) au sujet
- Les sociétés privées nous fichent à notre insu
- Personne ne sait où sont leurs données, qui les traitent, à quoi elles servent

All your databases belong to us

Cédric Jeanneret (aka @SwissTengu)

EthACK.org

12 décembre 2016

All your databases belong to us

Cédric Jeanneret (aka @SwissTengu)

EthACK.org

12 décembre 2016

Un sysadmin, c’est...

- Le mec barbu qu’on ne voit jamais ou presque
- Le mec barbu qui râle sur les développeurs
- Le mec barbu sur lequel les développeurs râlent

Un sysadmin, c’est...
- Le mec barbu qu’on ne voit jamais ou presque
- Le mec barbu qui râle sur les développeurs
- Le mec barbu sur lequel les développeurs râlent

Mais pas que ;)

- Firewall
- Updates
- configuration de services
- ... etc

Mais pas que ;)

- Firewall
- Updates
- configuration de services
- ... etc

Pwnage : surface d’attaque

- Service mal configuré
- Accès utilisateurs trop importants/mal gérés
- Application en "admin party"
- Faille de sécurité au niveau de l’application
- Faille de sécurité au niveau système/OS

Pwnage : surface d'attaque

- Service mal configuré
- Accès utilisateurs trop importants/mal gérés
- Application en "admin party"
- Faille de sécurité au niveau de l'application
- Faille de sécurité au niveau système/OS

Réduction du champ

- Application Web
- Serveur Linux
- Admin pas réveillé
- Développeur tout aussi peu réveillé

Réduction du champ
- Application Web
- Serveur Linux
- Admin pas réveillé
- Développeur tout aussi peu réveillé

Compromettre un système d’information

- Repérer les applications web installées
- Repérer les versions

1. README
2. Changelog
3. Autres fichiers courants (install, etc)

Compromettre un système d’information
- Repérer les applications web installées
- Repérer les versions

Faille détectée : exploitation

On est dans la mouise...

Faille détectée : exploitation

On est dans la mouise...

Exemple concret : phpMyAdmin

- Très souvent présent
- Bourré de failles
- Rarement mis à jour et pris en compte

Exemple concret : phpMyAdmin

- Très souvent présent
- Bourré de failles
- Rarement mis à jour et pris en compte

Dernières "features"

- CSRF
- XSS
- SQL Injection via nom de BDD
- Directory transversal (teste l'existence d'un fichier)
- MitM
- .....

Dernières "features"

- CSRF
- XSS
- SQL Injection via nom de BDD
- Directory transversal (teste l'existence d'un fichier)
- MitM
- .....

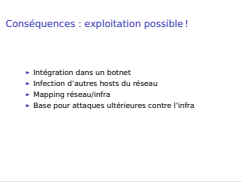
Autre exemple : Elasticsearch

- Service configuré pour écouter par défaut sur toutes les interfaces
- Aucun mécanisme de sécurité

Autre exemple : Elasticsearch
- Service configuré pour écouter par défaut sur toutes les interfaces
- Aucun mécanisme de sécurité

Conséquences : exploitation possible !

- Intégration dans un botnet
- Infection d’autres hosts du réseau
- Mapping réseau/infra
- Base pour attaques ultérieures contre l’infra



Conséquences...

- Vols de données
- Perte de clientèle
- Pertes de temps
- Blacklisting d’IPs, coupures réseau
- La fin du monde des Licornes

Conséquences...
- Vols de données
- Perte de clientèle
- Pertes de temps
- Blacklisting d’IPs, coupures réseau
- La fin du monde des Licornes

Comment éviter ?

- Communication (devops-bingo-buzz)
- Réduire la surface
- Communication (devops-bingo-buzz-bis)
- Bonnes pratiques

Comment éviter ?
- Communication (devops-bingo-buzz)
- Réduire la surface
- Communication (devops-bingo-buzz-bis)
- Bonnes pratiques

1. Quels droits, quels ports, quels services
2. Enlever les références de version, maintenir à jour, etc
3. Cycle des mises à jour
4. "Château-fort" : mauvais (l'ennemi peut aussi être à l'intérieur) ; Blacklisting : mauvais (préférer whitelisting)

Et les attaques type Déni de service ?

- "Scalabilité" de l'application
- Recherche des bottle-necks

Tests de charge et communication entre départements !

1. Note : un Déni de service peut ne pas être dû à une attaque...
2. Scalabilité : capacité de l'appli à être distribuée sur plusieurs serveurs
3. Stateless, etc, etc

Et les attaques type Déni de service ?
"Scalabilité" de l'application
Recherche des bottle-necks
Tests de charge et communication entre départements !

Questions ?

https://ethack.org/

@EthACK_org on Twitter

ethack.org on Facebook

Questions ?

https://ethack.org/

@EthACK_org on Twitter

ethack.org on Facebook

E+hACK