Honeyssh

Anthony Vérez, Thibault Ingargiola, Guilhem Tiennot, François Moniot

Hervé Debar

Soutenance de fin de CSC3502

30/05/12

Objectifs du projet

- **But du projet : développer un honeypot ssh.**
- **Honeypot : programme volontairement sensible qui sert de « pot de miel » pour attirer les hacke**
- **Objectifs principaux :**
  - Coder un serveur SSH fonctionnel,
  - Obtenir le plus d'information sur l'attaquant

Plan de la présentation

- **Présentation de l'équipe et du projet**
  - Contraintes du projet
  - Équipe et distribution des rôles
- **Architecture du honeypot**
  - Organisation des machines
- **Organisation du code**
  - Découpage
  - Difficultés rencontrées
- **Démonstration**
- **Résultats**
  - Interprétation et conclusion

Présentation de l'équipe et du projet

- Contraintes et objectifs du projet
- Présentation de l'équipe et répartition des rôles

Présentation du projet
Contraintes

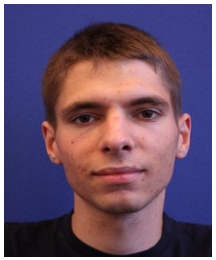
- **Un Honeypot est un piège pour hacker.**
- **Sécurité :**
  - Le honeypot doit être isolé du reste du réseau
  - L'attaquant ne doit pas pouvoir en sortir

Présentation du projet
Contraintes

- **Leurre**
  - Le honeypot doit être visible depuis l'extérieur.
  - L'attaquant doit pouvoir s'y connecter facilement.
  - Les commandes qu'il utilisera devront avoir une réponse vraisemblable.

- **Informations**
  - On doit pouvoir récupérer tout ce que fait l'attaquant.
  - Ces informations devront être stockées en dehors du honeypot.
  - On doit pouvoir différencier les attaquants.

Présentation du projet
L'équipe



Verez Anthony
- Chef de projet
- Tests
- Web
- Pare-feu

Tiennot Guilhem
- Historique bash
- Commandes
- Serveur SSH

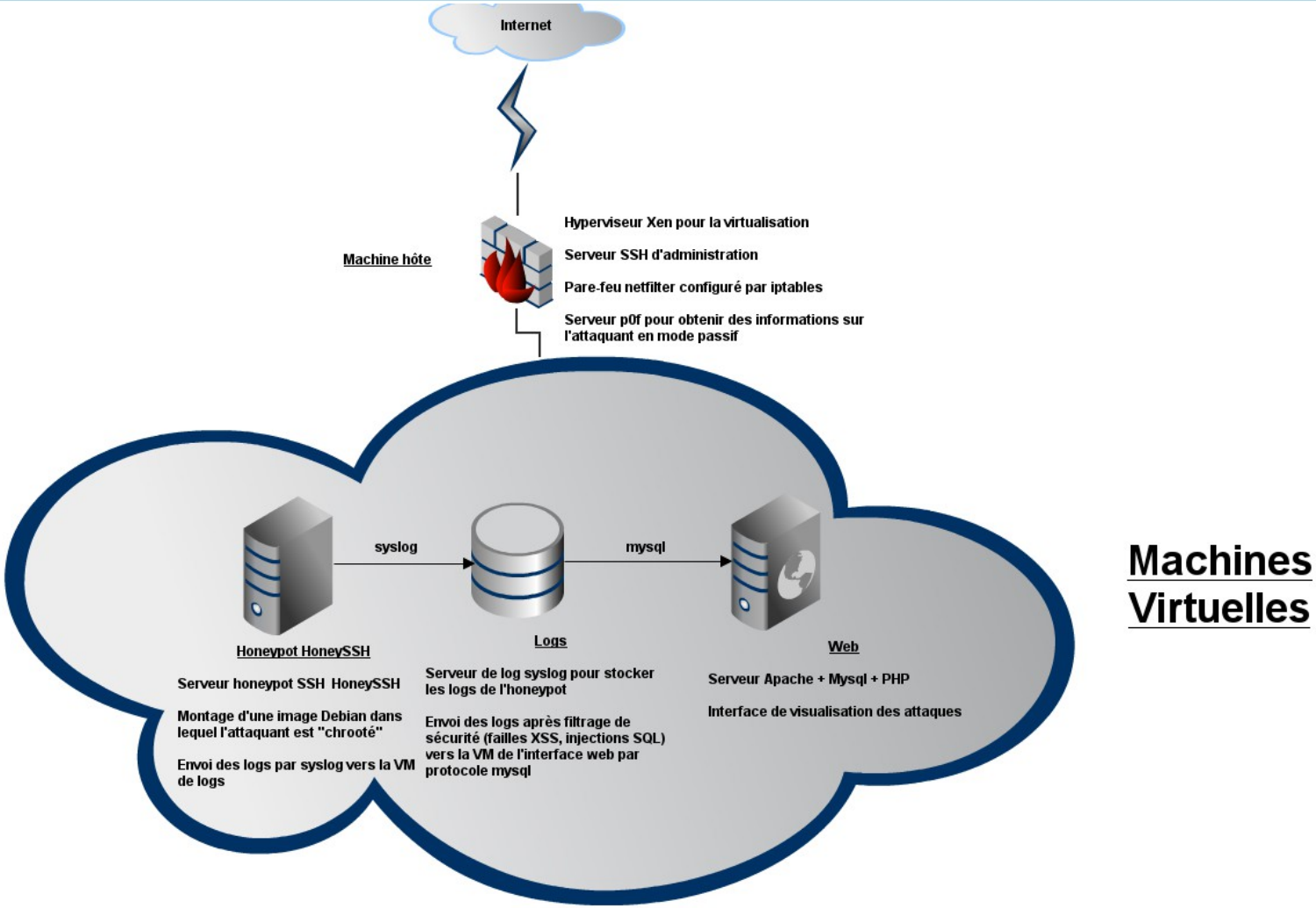
Monniot François
- Interpréteur
- Commandes
- Serveur SSH

Ingargiola Thibault
- Gestion de projet
- Commandes
- Tests

Architecture de l'honeypot

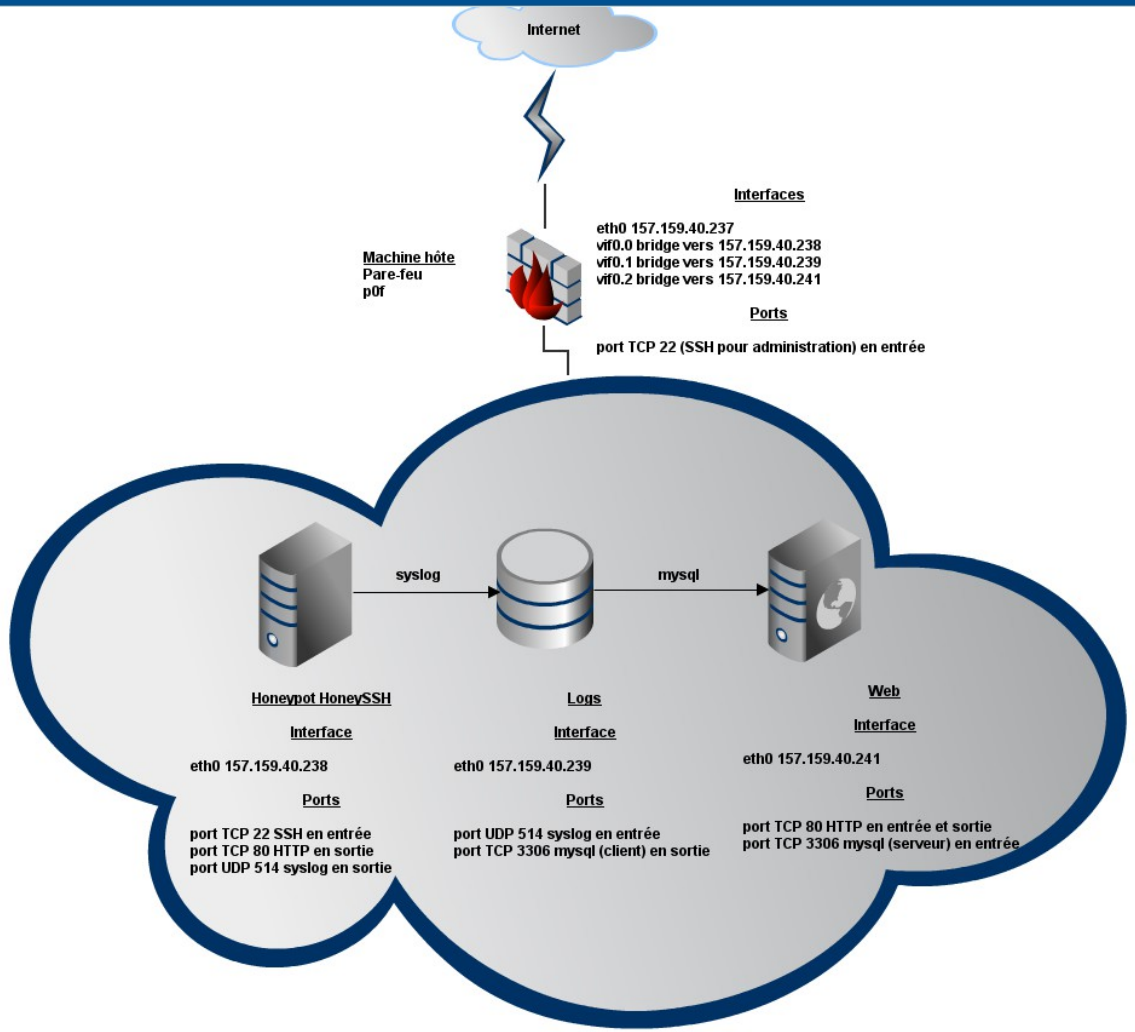
- Schéma logique
- Schéma réseau

Architecture de l'honeypot
Schéma logique



create and share your own diagrams at gliffy.com

Architecture de l'honeypot
Schéma réseau



Machines Virtuelles

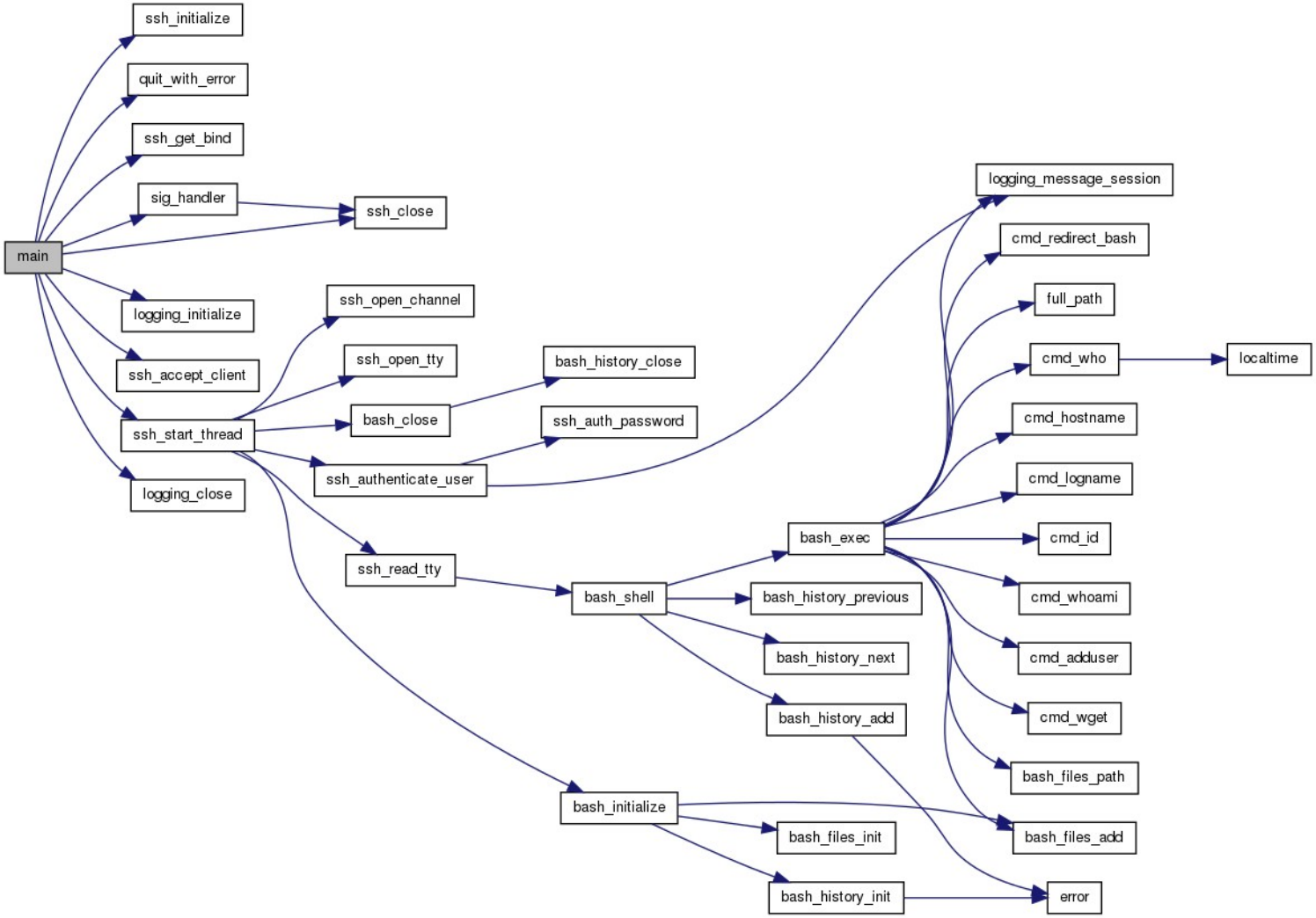
create and share your own diagrams at gliffy.com

gliffy

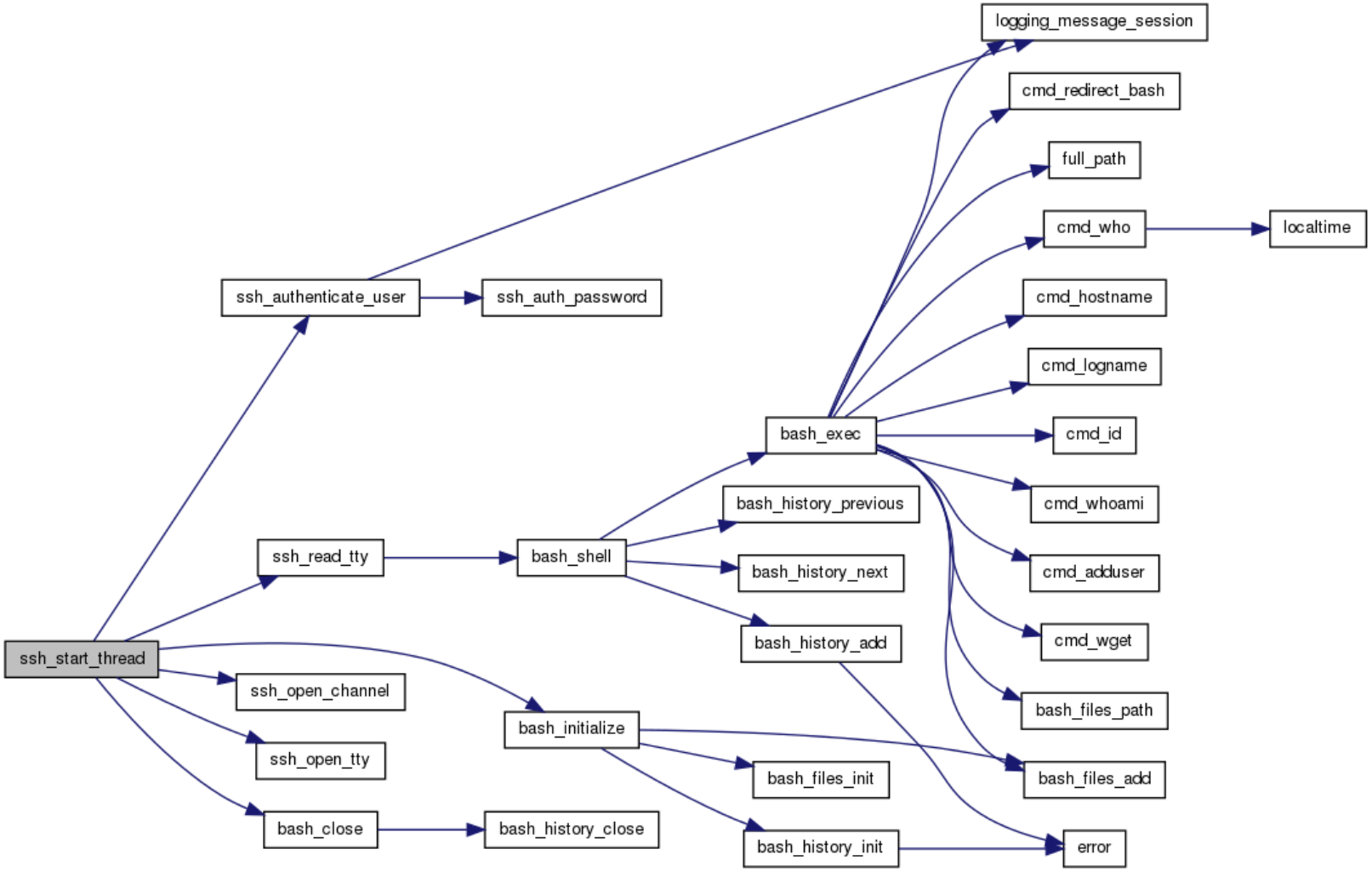
Organisation du code

- Découpage
- Difficultés rencontrées

Organisation du code
Découpage



Organisation du code
Découpage



Organisation du code
Difficultés rencontrées

- **Écriture du Bash compliquée**
  - Nombreuses fonctionnalités à implémenter
  - Variété des commandes
- **Bugs dans libssh**
  - Code d'exemple bogué
  - Impossibilité de changer la bannière
  - Peu de documentation, d'où une perte de temps supplémentaire
- **Perte de temps, car déboguage supplémentaire**

Organisation du code
P0f

- **Qu'est-ce que c'est ?**
  - Signifie « Passive OS Fingerprint »
  - Écoute les paquets TCP/IP du réseau
- **Comment ça marche ?**
  - Analyse les trames
  - Compare avec une base de donnée
- **Quels résultats ?**
  - Type de système d'exploitation
  - Client HTTP
  - Uptime et MTU
  - Et d'autres

Tests

- Unitaires
- Fonctionnels

Tests Unitaires

- Confirmer les spécifications
- Vérifier la gestion des cas particuliers
- Vérifier la non régression

- Exemple de test (égalité de chaine)

```
$ ./honeyssh_test
test_bash.c:68 expected "/root", actual: "/home"
```

Tests Unitaires

- Confirmer les spécifications
- Vérifier la gestion des cas particuliers
- Vérifier la non régression

- Exemple de test (égalité de chaine)

```
$ ./honeyssh_test
test_bash.c:68 expected "/root", actual: "/home"
```

Tests Fonctionnels

- **Vérifier que les fonctions sont bien atteintes par rapport aux attentes**
- **Chaque fonctionnalité doit être vérifiée par au moins un cas de test.**

- **Exemple :**

Sur honeyssh :

$ ssh root@<votremachine>

Sur le serveur de log :

$ tail /var/log/honeypot/honeyssh.log

May 21 22:05:39 157.159.40.238 honeyssh[2094]: 1460253435 157.159.46.34 User root AUTHENTIFIED with pass root

Démonstration

- Moment de la démonstration

Conclusion

- **Objectifs atteints :**
  - Serveur SSH fonctionnel.
  - Bash réaliste au premier abord
- **Avec plus de temps...**
  - Bash mieux finalisé
  - Tests de sécurité
  - Piéger un véritable attaquant
- **Expériences acquises :**
  - Travail en équipe
  - Architecture réseau
  - Utilisation de bibliothèques
  - Importance des tests

Questions