

Projet SERBER

Plateforme d'enseignement de la sécurité des systèmes d'information et des réseaux
Projet INSA-Lyon soutenu par le conseil régional Rhône-Alpes (2003-2005)

Samuel Galice, docteur en informatique
Présentation du 28 mai 2008



Plan

1. Présentation

- L'équipe et les intervenants
- La plateforme technique

2. Les scénarii d'usages

- Scénario attaque interne
- Scénario attaque externe
- Scénario attaque serveur Apache

3. Discussions & Conclusion

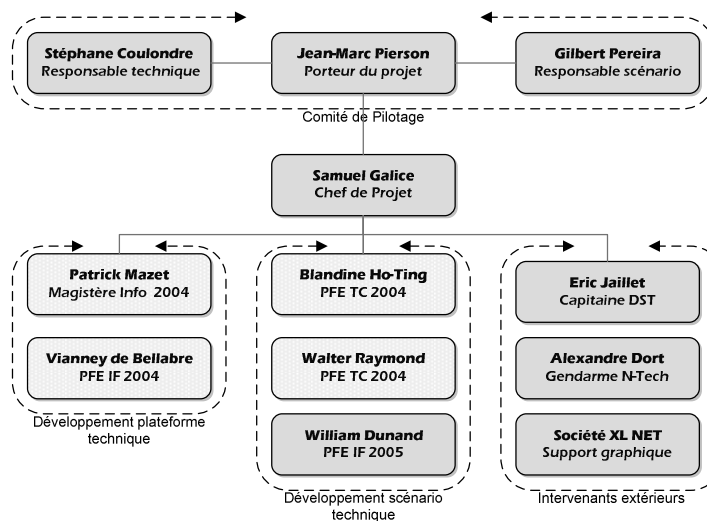
Projet SERBER

Plateforme d'enseignement de la sécurité des systèmes d'information et les réseaux

1. Présentation

- L'équipe et les intervenants
- La plateforme technique

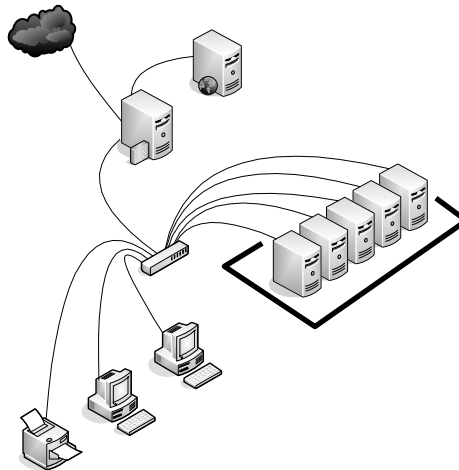
L'équipe et les intervenants



Plateforme technique :: Matériel

– 5 serveurs

- Pentium 4 560 (3,60 GHz) reliés en gigabit Ethernet dotés de 4 Go de mémoire vive, 160 Go d'espace disque dur. Graveur DVD pour sauvegarde des parties.
- Système d'exploitation Linux Mandrake
- Virtualisateur VMWare GSX 3.1



mercredi 11 juin 2008

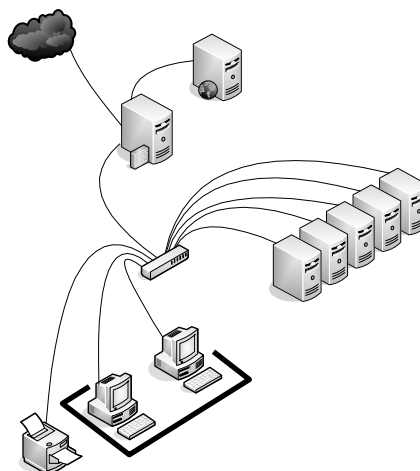
Samuel Galice

5

Plateforme technique :: Matériel

– 2 serveurs développement

- Amd Athlon 3200+ reliés en gigabit Ethernet, dotés de 2 Go de mémoire vive, 120 Go d'espace disque dur.
- Système d'exploitation Linux Debian et Mandrake



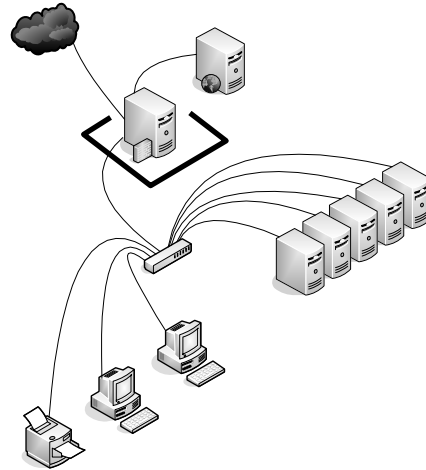
mercredi 11 juin 2008

Samuel Galice

6

Plateforme technique :: Matériel

- 1 firewall
 - Pentium II 300 Mhz
 - Système d'exploitation IPCop v1.4
 - Configuration zone rouge, jaune, vert : accès Internet de l'INSA.



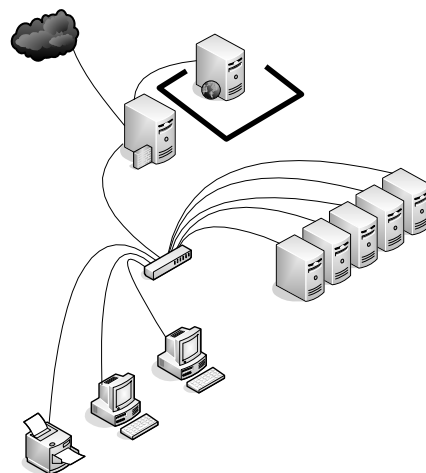
mercredi 11 juin 2008

Samuel Galice

7

Plateforme technique :: Matériel

- 1 serveur web, mail
 - Amd Duron 1200 Mhz
 - Système d'exploitation Linux Mandrake
 - Serveur Jabber pour le chat



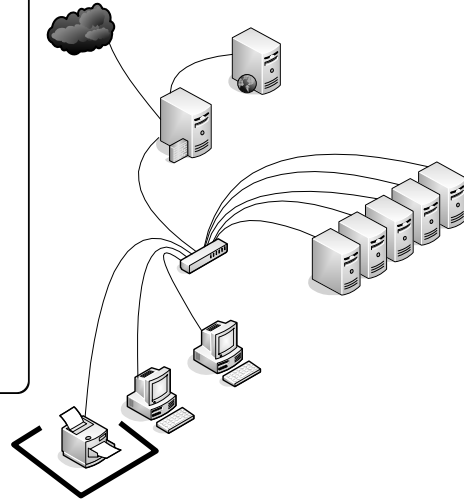
mercredi 11 juin 2008

Samuel Galice

8

Plateforme technique :: Matériel

- 1 imprimante
 - HP Laserjet Color 2550Ln



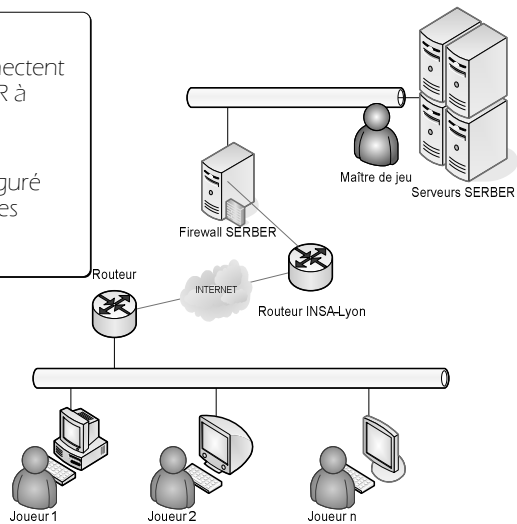
mercredi 11 juin 2008

Samuel Galice

9

Plateforme technique :: Synoptique générale

- Vue physique
 - Les joueurs se connectent aux serveurs SERBER à distance
 - Le firewall est configuré pour laisser passer les communications.



mercredi 11 juin 2008

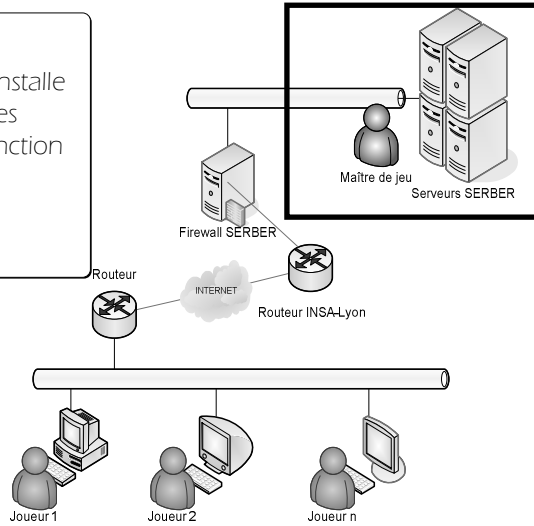
Samuel Galice

10

Plateforme technique :: Maître du jeu

– Le Maître du jeu

- Le Maître du jeu installe la partie et règle les paramètres en fonction du scénario



mercredi 11 juin 2008

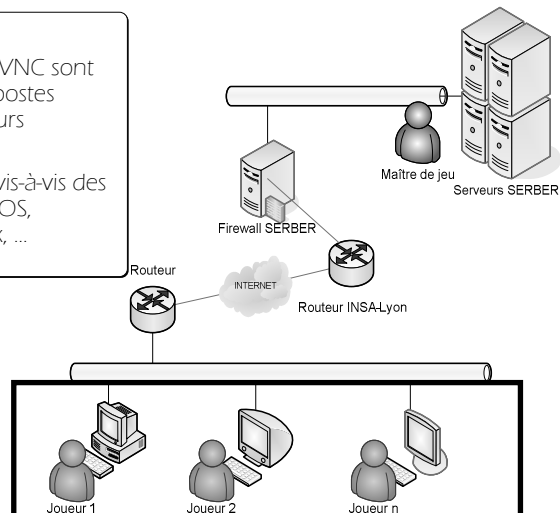
Samuel Galice

11

Plateforme technique :: Les joueurs

– Les joueurs

- Les clients TightVNC sont installés sur les postes clients des joueurs
- Indépendance vis-à-vis des machines : MacOS, Windows, Linux, ...

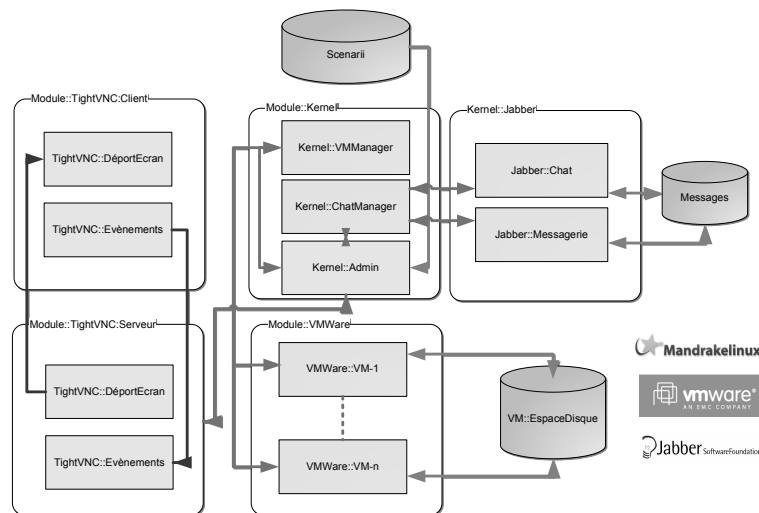


mercredi 11 juin 2008

Samuel Galice

12

Plateforme technique :: vue logique



mercredi 11 juin 2008

Samuel Galice

13

Projet SERBER

Plateforme d'enseignement de la sécurité des systèmes d'information et les réseaux

2. Les scénarii d'usages

- Scénario attaque interne
- Scénario attaque externe
- Scénario attaque serveur Apache

Scénarii d'usages

- **Plusieurs scénarii d'usages développés**
 - Attaque interne : faille LSAS sur une machine cliente sous Windows XP SP1.
 - Attaque externe : faille DCOM sur une machine cliente sous Windows XP SP0
 - Attaque serveur Apache : voir William Dunand

mercredi 11 juin 2008

Samuel Galice

15

Scénarii d'usages :: Déroulement de la partie

- **Formation initiale de 18-24 élèves ingénieurs**
 - 2 groupes de joueurs
 - 3-4 trinômes du groupe d'attaquants (pirates)
 - 3-4 trinômes du groupe des Administrateurs (victimes)
 - Chaque couple du trinôme pirate victime mène le même scénario
 - 3-4 parties en parallèle
 - Inversion des rôles un jour sur deux !!!
 - Durée de 1 à 4 jours

mercredi 11 juin 2008

Samuel Galice

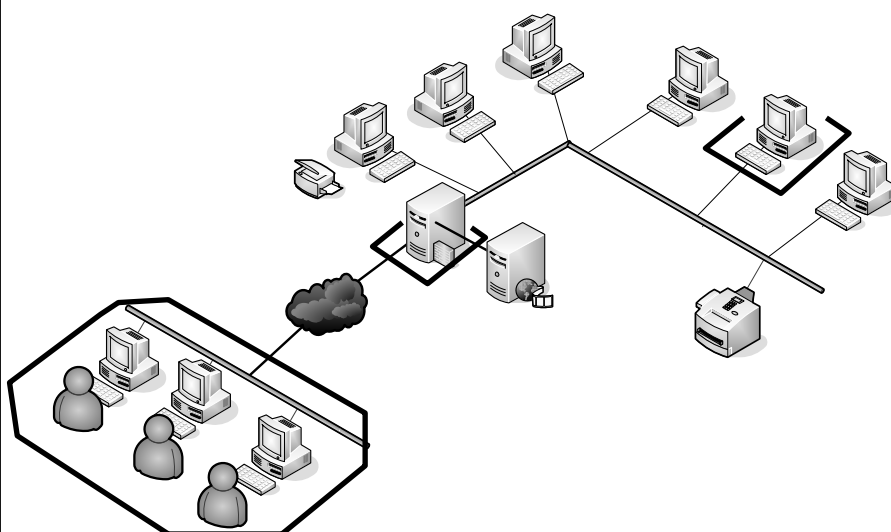
16

Projet SERBER

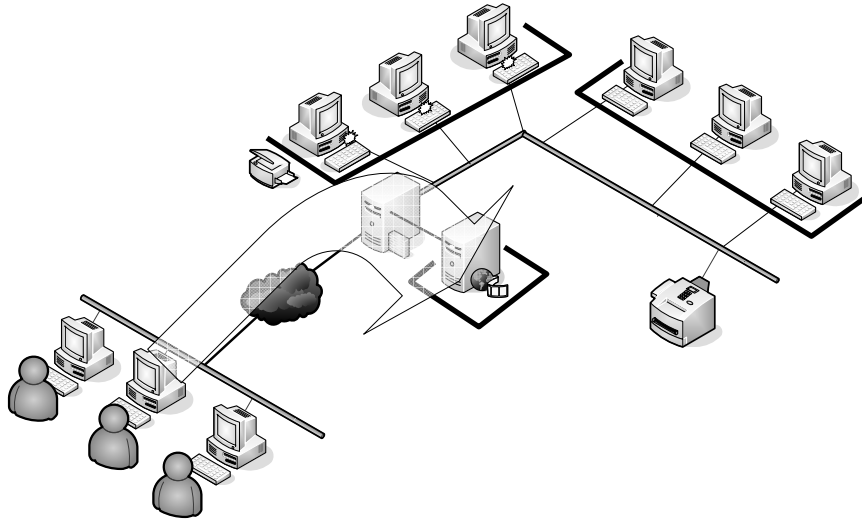
Plateforme d'enseignement de la sécurité des systèmes d'information et les réseaux

Scénario 1:: Groupe Attaquant

Scénario 1:: Groupe Attaquant



Scénario 1:: Groupe Attaquant

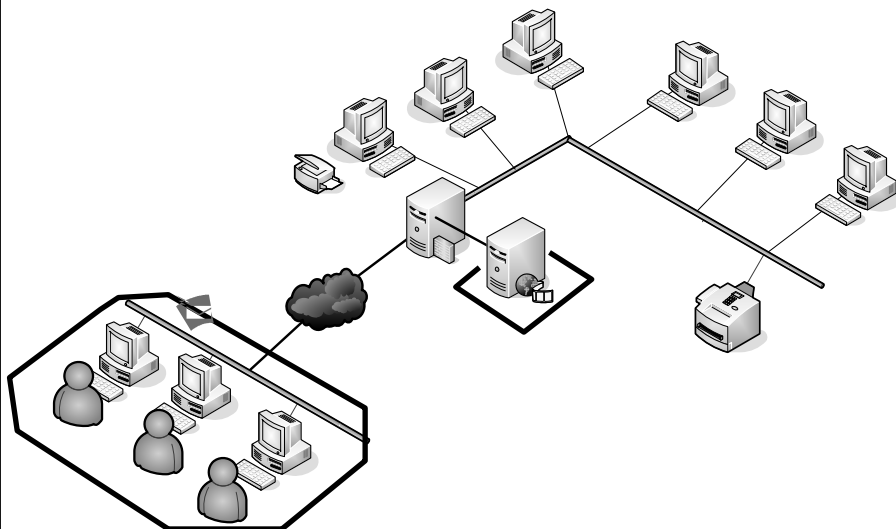


mercredi 11 juin 2008

Samuel Galice

19

Scénario 1:: Groupe Attaquant

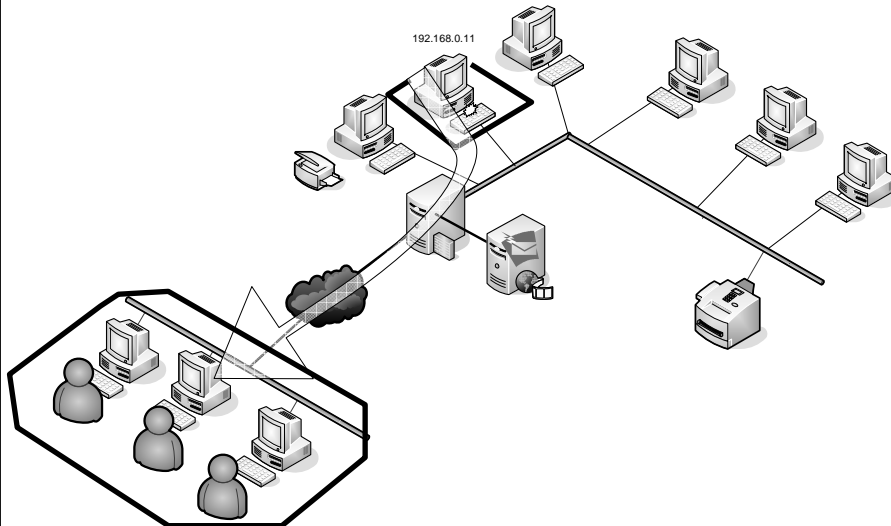


mercredi 11 juin 2008

Samuel Galice

20

Scénario 1:: Groupe Attaquant

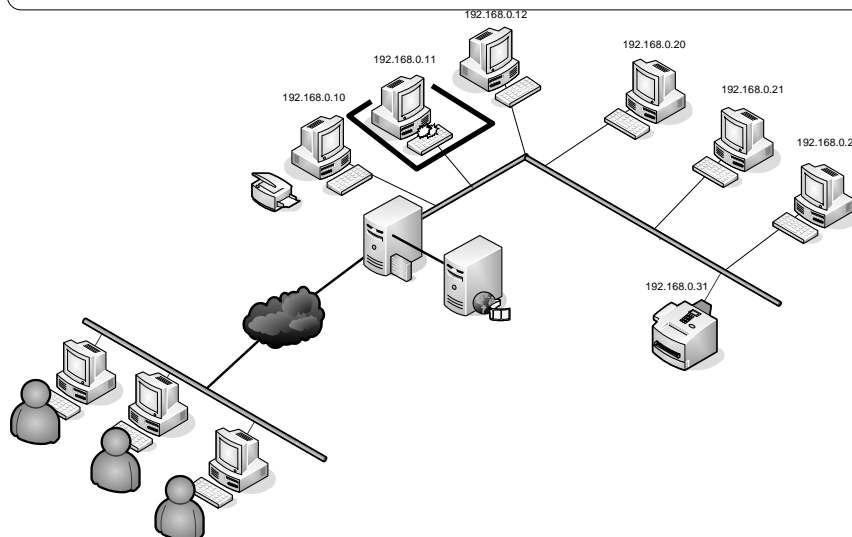


mercredi 11 juin 2008

Samuel Galice

21

Scénario 1:: Groupe Attaquant

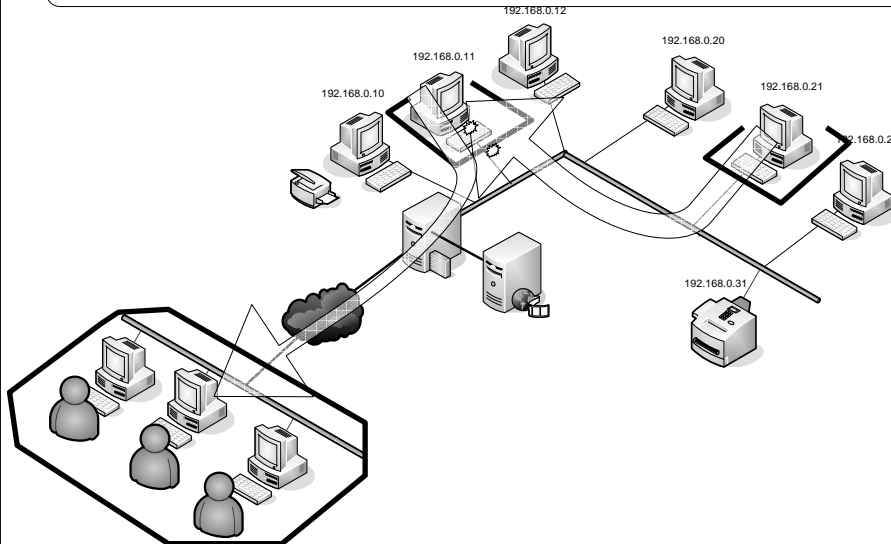


mercredi 11 juin 2008

Samuel Galice

22

Scénario 1:: Groupe Attaquant

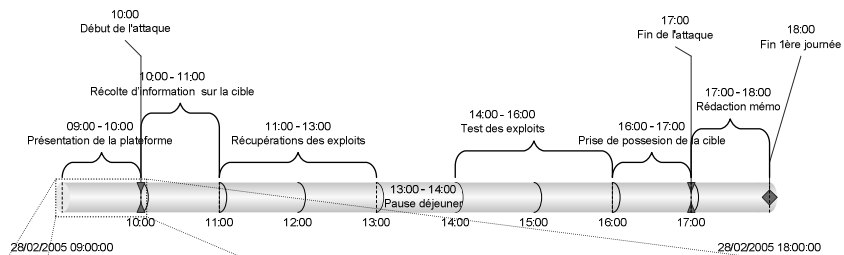


mercredi 11 juin 2008

Samuel Galice

23

Scénario 1 :: Groupe Attaque :: 1^{ère} journée



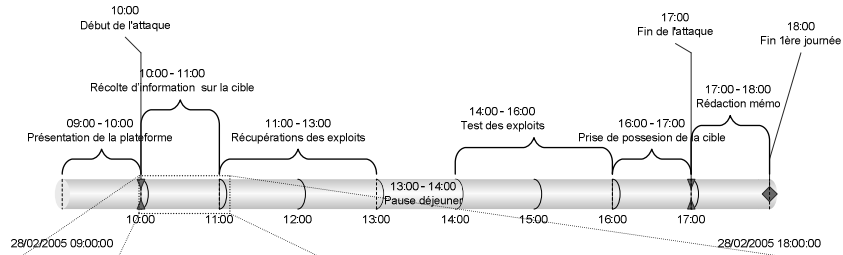
- Présentation de la plateforme
- Remise d'une documentation technique
- Remise des identifiants de connexion
- Création d'un compte Jabber personnalisé
- Assignation des objectifs
 - Une société de renseignement souhaite faire de l'espionnage industriel
 - Partie très délicate, proposition : chasse aux 'trésors'? Avec des indices?

mercredi 11 juin 2008

Samuel Galice

24

Scénario 1 :: Groupe Attaque :: 1^{ère} journée



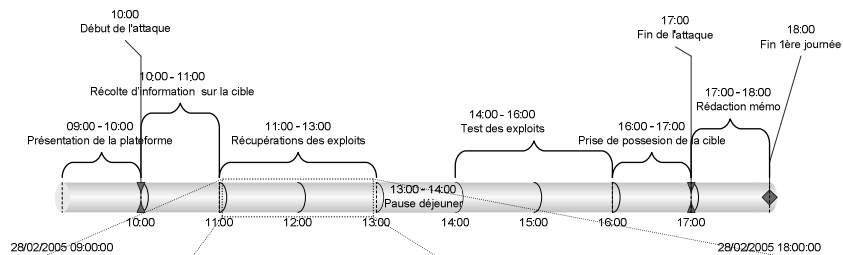
- Récupération d'informations sur le serveur WEB de l'entreprise
 - Les pirates doivent dérober un document sensible sur une machine cible dans le réseau de l'entreprise visée.
- Récupération d'information par WHOIS, ...
- Recoupement d'information sur l'organisation interne

mercredi 11 juin 2008

Samuel Galice

25

Scénario 1 :: Groupe Attaque :: 1^{ère} journée



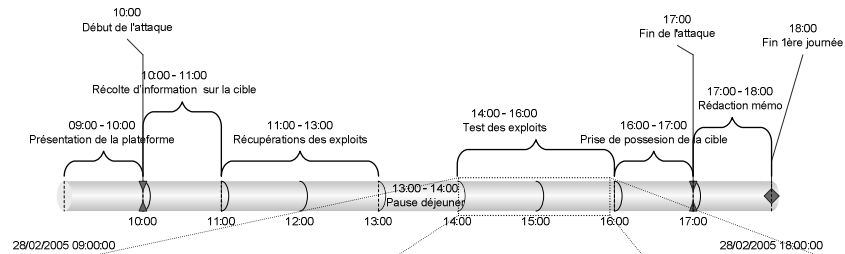
- Récupération des exploits sur le serveur WEB SERBER
 - Un document retrace les exploits et leur utilisation
- Analyse d'une attaque possible (phase guidée !!)

mercredi 11 juin 2008

Samuel Galice

26

Scénario 1 :: Groupe Attaque :: 1^{ère} journée



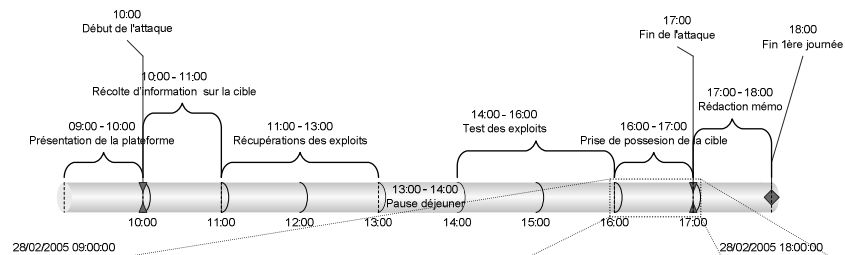
- Compilation des exploits
- Tests pour s'assurer de la validité du processus

mercredi 11 juin 2008

Samuel Galice

27

Scénario 1 :: Groupe Attaque :: 1^{ère} journée



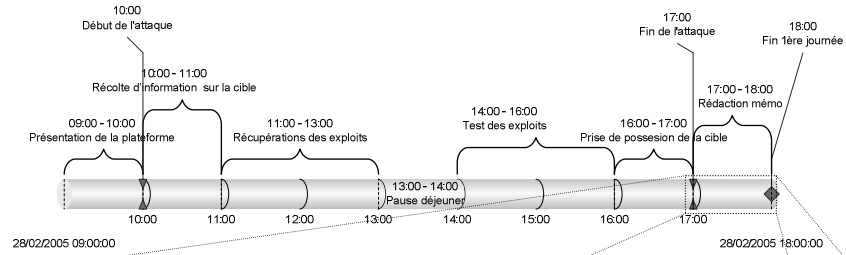
- Prise de possession de la cible
- Récupération du document recherché

mercredi 11 juin 2008

Samuel Galice

28

Scénario 1 :: Groupe Attaque :: 1^{ère} journée



- Rédaction d'un compte rendu
- Critique de la plateforme

mercredi 11 juin 2008

Samuel Galice

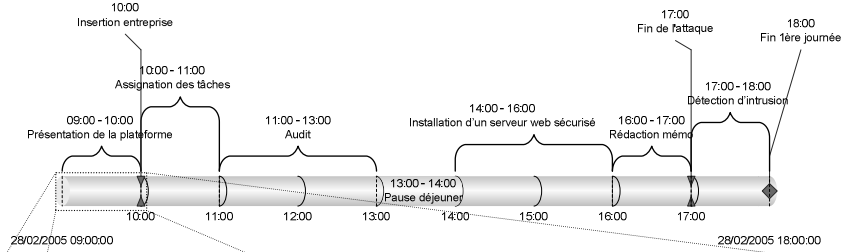
29

Projet SERBER

Plateforme d'enseignement de la sécurité des systèmes d'information et les réseaux

Scénario 1:: Groupe Admin.

Scénario 1 :: Groupe Admin. :: 1^{ère} journée



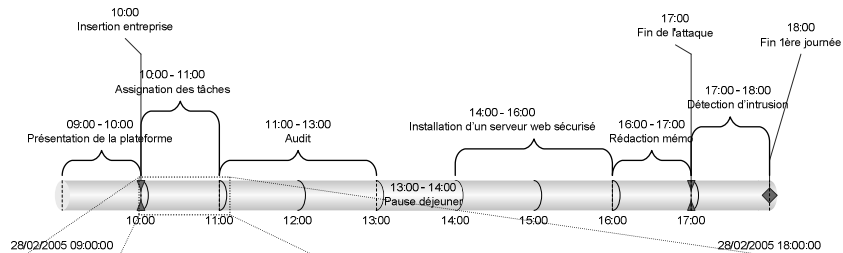
- Présentation de la plateforme
- Remise d'une documentation technique
- Remise des identifiants de connexion
- Création d'un compte Jabber personnalisé
- Assignment des objectifs

mercredi 11 juin 2008

Samuel Galice

31

Scénario 1 :: Groupe Admin. :: 1^{ère} journée



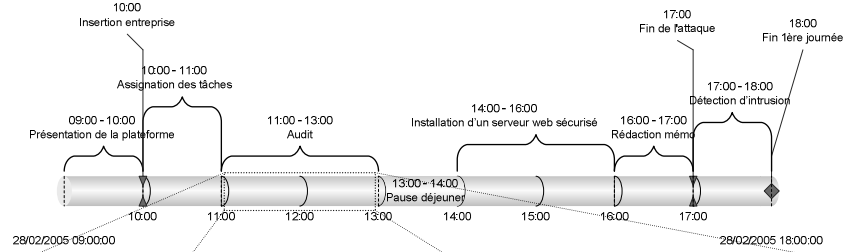
- Assignment des tâches de la journée
 - Audit des machines
 - Installation d'un serveur WEB sécurisé

mercredi 11 juin 2008

Samuel Galice

32

Scénario 1 :: Groupe Admin. :: 1^{ère} journée



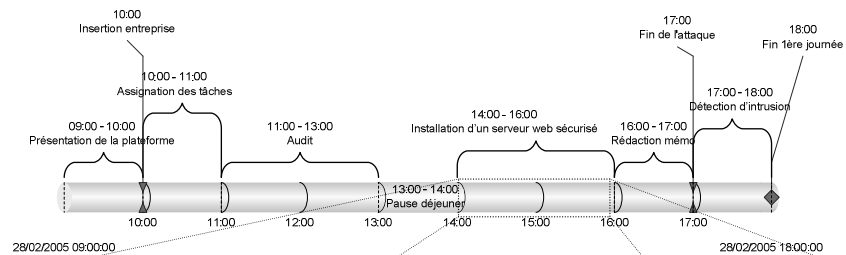
– Audit

mercredi 11 juin 2008

Samuel Galice

33

Scénario 1 :: Groupe Admin. :: 1^{ère} journée



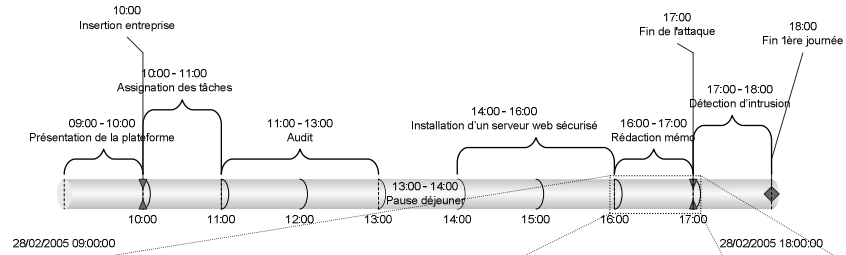
– Installation du serveur web sécurisé

mercredi 11 juin 2008

Samuel Galice

34

Scénario 1 :: Groupe Admin. :: 1^{ère} journée



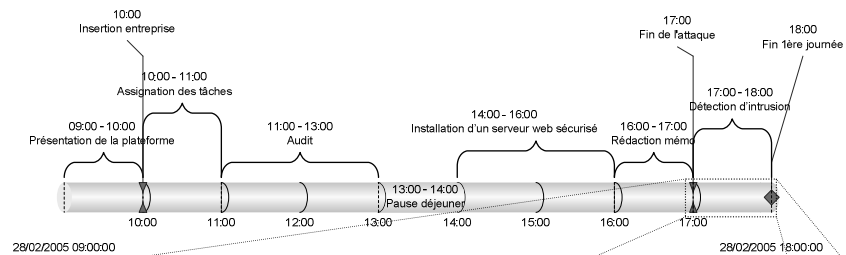
- Rédaction d'un compte rendu
- Critique de la plateforme

mercredi 11 juin 2008

Samuel Galice

35

Scénario 1 :: Groupe Admin. :: 1^{ère} journée



- Détection d'une intrusion éventuelle

mercredi 11 juin 2008

Samuel Galice

36

Projet SERBER

Plateforme d'enseignement de la sécurité des systèmes d'information et les réseaux

3. Discussions

Discussions

- **Alexandre Dort (Gendarmerie N-Tech)**
- **capitaine Eric Jaillet (DST)**
 - Nouveaux enjeux de la cybercriminalité (phishing, troyens, spywares, adwares, spoofing, ...)
 - Aspects légaux (Loi sur la confiance dans l'économie numérique – LEN -, publication de la charte numérique, ...)

Loi sur l'Économie Numérique (LEN)

- « *Art. 323-3-1.* - Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

Conclusion

<http://serber.insa-lyon.fr>