CNAM Paris – Département informatique

Les tests d'intrusion dans les réseaux Internet, l'outil Nessus

Examen probatoire

session de Mai 2004

Dongé Laurent

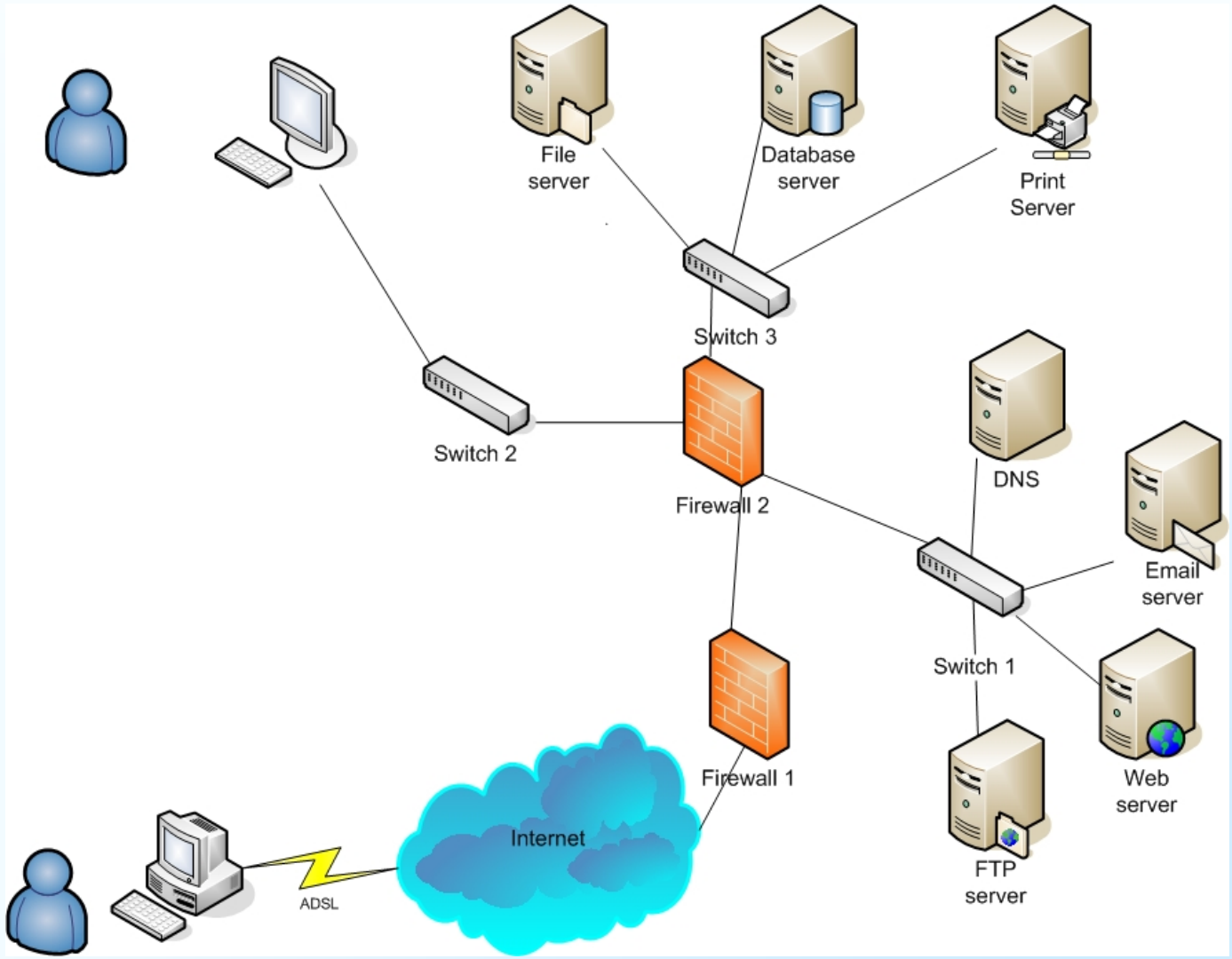
laurent_donge@yahoo.fr

Plan

- Réseaux Internet
- Tests d'intrusion
  - Démarche
  - Outils
- Nessus
- Tests d'audit réalisés
  - Scanners utilisés
  - Protocoles & Résultats
- Conclusion

Réseaux Internet

- **Réseaux Internet**
- Tests d'intrusion
  - Démarche
  - Outils
- Nessus
- Tests d'audit réalisés
  - Scanners utilisés
  - Protocoles & Résultats
- Conclusion



Tests d’intrusion

- Réseaux Internet
- **Tests d’intrusion**
  - Démarche
  - Outils
- Nessus
- Tests d’audit réalisés
  - Scanners utilisés
  - Protocoles & Résultats
- Conclusion

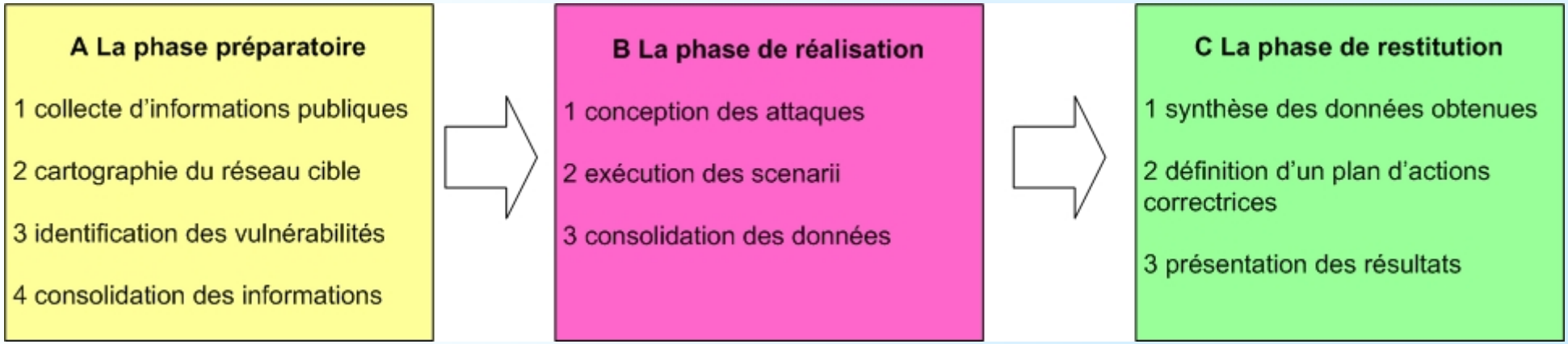
- Définition :

  une tentative autorisée de simuler les activités de pirates afin d’évaluer les failles de sécurité présentées par un système d’information
- Stratégies :
  - test interne / test externe
- Méthodes :
  - test aveugle / double aveugle / ciblé
- Types :
  - sécurité application Web
  - DoS
  - War dialing
  - ingénierie sociale …

La démarche des Tests d'intrusion

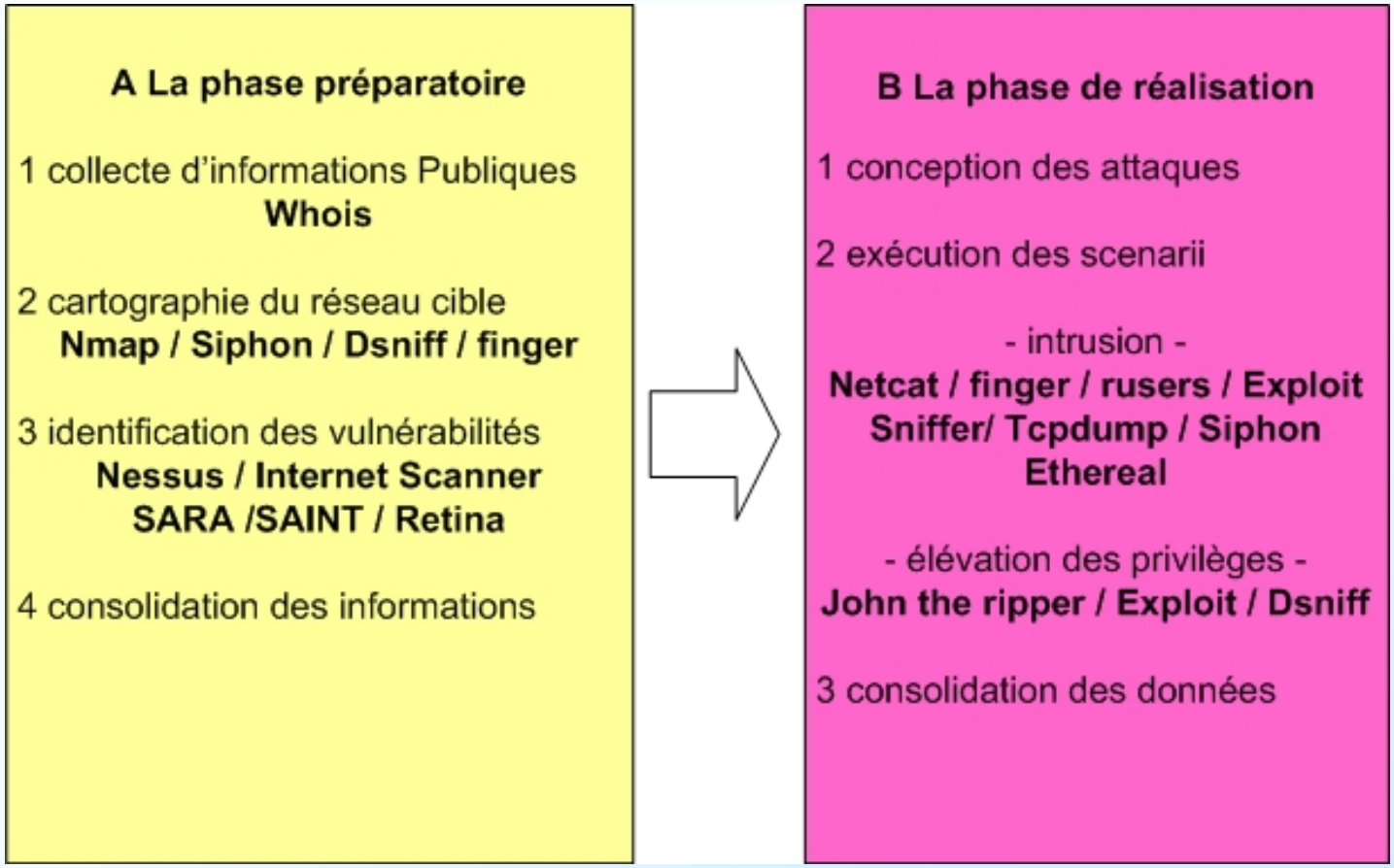
- Réseaux Internet
- **Tests d'intrusion**
  - **Démarche**
  - Outils
- Nessus
- Tests d'audit réalisés
  - Scanners utilisés
  - Protocoles & Résultats
- Conclusion

- A. Phase préparatoire
- B. Phase de réalisation
- C. Phase de restitution



Outils utilisés

- Réseaux Internet
- **Tests d'intrusion**
  - Démarche
  - **Outils**
- Nessus
- Tests d'audit réalisés
  - Scanners utilisés
  - Protocoles & Résultats
- Conclusion



Nessus (1/2)

- Réseaux Internet
- Tests d'intrusion
  - Démarche
  - Outils
- **Nessus**
- Tests d'audit réalisés
  - Scanners utilisés
  - Protocoles & Résultats
- Conclusion

- détection des services sur les différents ports en analysant les protocoles
- tests de vulnérabilités parmi 24 familles sur les services détectés
  - backdoors, CGI, CISCO, DoS , RPC, SMTP ...
- fournit :
  - une liste des vulnérabilités classées
  - des références CVE
  - des solutions

Nessus (2/2)

- Contexte
- Tests d'intrusion
  - Démarche
  - Outils
- **Nessus**
- Tests d'audit réalisés
  - Scanners utilisés
  - Protocoles & Résultats
- Conclusion

- permet de réaliser des rapports
  - HTML, LaTeX ...
- son architecture client/serveur
  - test sous forme de plug-in (NASL)
  - bases d'information
  - produits tiers : Nmap, Nitko, Hydra

Tests d'audit réalisés (1/3)

Scanners utilisés sur un réseau Ethernet

- Réseaux Internet
- Tests d'intrusion
  - Démarche
  - Outils
- Nessus
- **Tests d'audit réalisés**
  - **Scanners utilisés**
  - Protocoles & résultats
- Conclusion

Scanners	Nessus	NeWT	SAINT	Internet Scanner
Nature	Open source	Commerciale		
Plate-forme possible	Linux Unix	Windows	Linux	Windows
Pate-forme utilisée	Linux Fedora Core 1 B	Windows 2000 serveur	Linux Fedora Core 1 B	Windows 2000 serveur
Facilité d'installation	4	5	5	3

1: pas convaincant 2: passable 3: correct 4: bien 5: Excellent

Tests d'audit réalisés (2/3)

- Réseaux Internet
- Tests d'intrusion
  - Démarche
  - Outils
- Nessus
- **Tests d'audit réalisés**
  - Scanners utilisés
  - **Protocoles & résultats**
- Conclusion

- Protocole des Tests
  - audit **sans** attaques dangereuses
  - audit **avec** attaques dangereuses
  - audit **sans** puis **avec** Nmap
- Résultats
  - Nessus : détection complète, temps d'analyse correct, évolutif, ouvert
  - Positionnement de Nessus

Tests d'audit réalisés (3/3)

- Réseaux Internet
- Tests d'intrusion
  - Démarche
  - Outils
- Nessus
- **Tests d'audit réalisés**
  - Scanners utilisés
  - **Protocoles & résultats**
- Conclusion

Tableau comparatif simplifié

	Nessus	NeWT	SAINT	Internet Scanner
Détection	4	4	3	4
Temps	3	4	4	2
Rapport	3	3	4	2
Appréciation générale	4	4	3	4

1: pas convaincant 2: passable 3: correct 4: bien 5: Excellent

Conclusion

- Réseaux Internet
- Tests d'intrusion
  - Démarche
  - Outils
- Nessus
- Tests d'audit réalisés
  - Scanners utilisés
  - Protocoles & Résultats
- **Conclusion**

- L'importance de référence standardisée
- Les limites des scanners et des tests d'intrusion
- la sécurisation nécessite des outils complémentaires
- les réseaux de taille importante demandent :
  - des architectures réparties plus robustes
  - la définition de stratégies

Questions - Discussion