Démarche d’attaque et outils

GULDNER - HURIER - LACAVE - SOILIHI

Sommaire

- Démarche de groupe
- Attaques et défenses
  - de Geoffrey
  - de Médéric
  - de Valentin
  - de Mouchtali
- Conclusion

Quel démarche ?

Pas de démarche !

Mais de la collaboration:

- partage des connaissances (Redmine)
- partage des données (Redmine)
- suivi des actions (Redmine)

laissons place à l'initiative et à la créativité :)

Outils de Geoffrey

Attaques: scanners de vulnérabilité (nessus, metasploit, ikare, nmap …) + url spoofing

Défense: surveillance de la base de données et de l'espace disque (commandes du et df)

Outils de Médéric

Attaques: MITM (ettercap, wireshark), attaques web (CRSF, XSS, SQL Injection)

Défense: surveillance des journaux (logs)

Outils de Valentin

Attaques: scanners de vulnérabilités, exploitation de l'API Mediawiki

Défense: pentesting sur notre serveur

Outils de Mouchtali

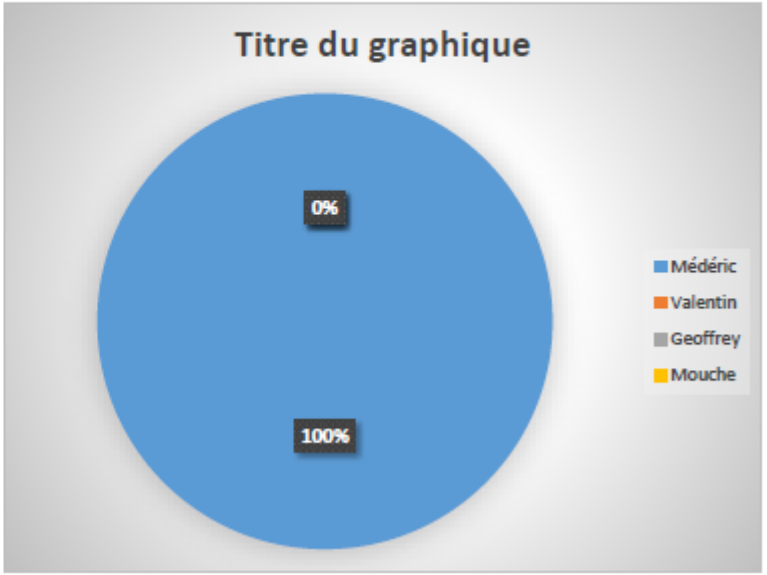
Attaques: DoS (Deny of Service)

Défense: surveillance des utilisateurs, processus, services en écoute ...

Conclusion

N° Echec	Attaquant	Effectué
EA001	Médéric	29/01/2014
EA002	Médéric	29/01/2014

Médéric	Valentin	Geoffrey	Mouche
2	0	0	0



Conclusion

- Collaboration > organisation
- Compromis attaque/défense
- Attaques variées (DoS, Web, API, …)