

Université de Picardie Jules Verne

Informatique – Master CCM

INSSET – Saint-Quentin

Audit, diagnostic et tests d'intrusion

M2

v3.0

C. Drocourt

cyril.drocourt@u-picardie.fr

SOMMAIRE

Cours 1 : Informations en mode passif.....	3
Cours 2 : Scanner de Vulnérabilités Web.....	3
Cours 3 : Sécurité des applications Web.....	4
Cours 4 : Intrusion d'un réseau local.....	4
Cours 5 : Scanner réseau.....	5
Cours 6 : Outils et Framework d'exploitation.....	5
Cours 7 : Ingénierie sociale.....	5
Annexes.....	6

Cours 1 : Informations en mode passif.....	2
1 - Introduction.....	4
2 - Sites internet spécialisés.....	5
3 - Le DNS.....	10
4 - Information des moteurs de recherche.....	20
5 - Le Mail.....	32
6 - Médias sociaux.....	34

Cours 2 : Scanner de Vulnérabilités Web.....	2
1 - Introduction.....	4
2 - Nikto.....	4
3 - wapiti.....	7
4 - SkipFish.....	11
5 - Scanner de CMS.....	14
6 - OWASP.....	15
7 - W3AF.....	16

8 - OWASP ZAP.....	18
9 - Autres "scanner" de vulnérabilités.....	22

Cours 3 : Sécurité des applications Web.....2

1 - Cookies.....	4
2 - Authentification.....	7
3 - Cookie et Session.....	8
4 - Injection SQL.....	10
5 - Cross Site Scripting.....	19
6 - OWASP ZAP en Reverse Proxy.....	21

Cours 4 : Intrusion d'un réseau local.....2

1 - Introduction.....	4
2 - Détection d'informations.....	6
3 - ARP et MITM avec DSNIFF.....	11
4 - MITM avec « ettercap ».....	20

5 - Autres attaques non développées.....	21
Cours 5 : Scanner réseau.....	2
1 - Introduction.....	4
2 - NMAP.....	4
3 - Nessus/OpenVAS.....	14
Cours 6 : Outils et Framework d'exploitation.....	2
1 - Introduction.....	4
2 - John.....	5
3 - Hydra/Medusa.....	6
4 - Metasploit.....	9
5 - Armitage.....	26
Cours 7 : Ingénierie sociale.....	2
1 - Introduction.....	4

2 - Outil « SET ».....4

Annexes.....2

1 - Outils.....4

2 - Distributions Linux.....8

3 - Webographie.....9