

Sécurité informatique

Ethical Hacking

Apprendre l'attaque
pour mieux se défendre

→ Informatique technique



ε
Collection

epsilon

ACISSI

Sécurité informatique

Ethical Hacking

Apprendre l'attaque
pour mieux se défendre



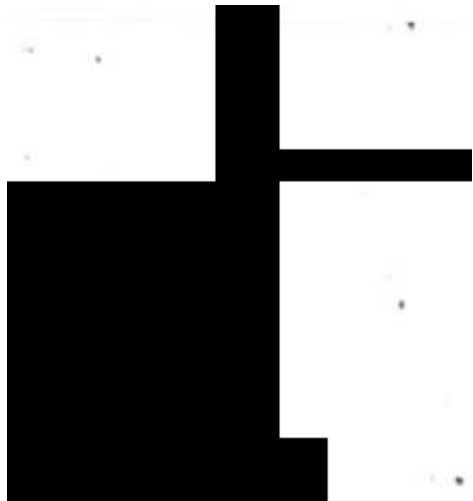
L'ÉCOLE NATIONALE DE LA SÉCURITÉ



 **epsilon**
collection

ACISSI





Sécurité

informatique

Ethical Hacking

Apprendre l'attaque

pour mieux se défendre

1

1

Toutes les marques citées ont été déposées par leur éditeur respectif.

La loi du 11 Mars 1957 n'autorisant aux termes des alinéas 2 et 3 de l'article 41,
d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective", et, d'autre part, que les analyses
et les courtes citations dans un but d'exemple et d'illustration, "toute représentation
ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de
ses ayants droit ou ayant cause, est illicite" (alinéa 1er de l'article 40).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contre-
façon sanctionnée par les articles 425 et suivants du Code Pénal.

Copyright - Editions ENI - Octobre 2009

ISBN: 978-2-7460-5105-8

Imprimé en France

Editions ENI

ZAC du Moulin Neuf

Rue Benjamin Franklin

44800 St HERBLAIN

Tél. 02.51.80.15.15

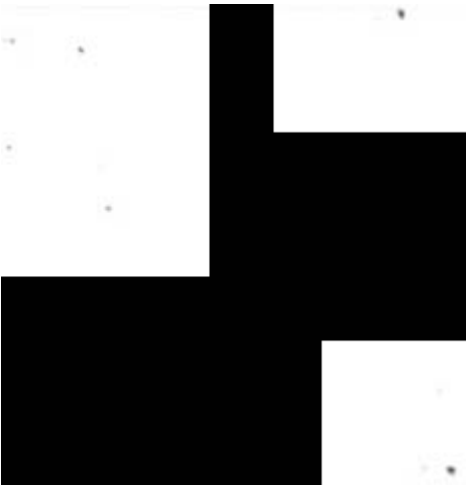
Fax. 02.51.80.15.16

e-mail : editions@ediENL.com

<http://www.editions-eni.com>

Auteurs: ACISSI

Collection Expert IT dirigée par Joëlle MUSSET



1

|

3

3

Table des matières

Chapitre 1

Introduction et définition

1. Présentation 9

.

.

.

.

.

.

1.1. L'information est partout 9

.

1.2. Connaître le système d'information pour le protéger 10

1.3. Identifier la menace 1 1

.

.

1.4. Instaurer de bonnes pratiques de sécurité 1 2

.

1.5. Auditer son système 1 3

.

.

.

2. Une nouvelle éthique de travail 1 4

2. 1. La connaissance avant toute chose 1 4

2. 1.1. Les hackers « black hats », les chapeaux noirs 15

2. 1.2. Les hackers « white hats », les chapeaux blancs 15

2.1.3. Les hackers « grey hats », les chapeaux gris 16

2. 1.4. Les « script kiddies» 1 7

2. 1.5. Les hackers universitaires ..	18
2.2. Un rapport différent au travail . .	18
2.3. La coopération comme clé de réussite ...	20

2.4. Tous des hackers !	22
-------------------------------	----

Chapitre 2

Méthodologie d'une attaque

1. Préambule	25
2. Collecte des informations	26
2. 1. Connaître sa cible	26
2.2. Google est notre ami	26
2.3. Les humains sont bavards .	29

2.4. Quelques commandes utiles .	29
----------------------------------	----

2.5. La prise d'empreinte par pile TCP/IP	30
-------------------------------------------------	----

2.6. Interroger les services lancés 3 3

.

.

3. Repérage de failles ... 36

3. 1. Consulter les failles recensées

.....

.. 36

.

.

.

.

.

.

.

.

3.2. Éliminer les failles non fondées . . 3 7

.

.



2

2

Sécurité informatique

Apprendre "attaque pour mieux se défendre

4. Intrusion dans le système .

.. .

.. .

..

..

.. 38

.

.

.

.

.

.

.

.

.

.

.

.

.

.

.

.

.

.

4. 1. Ne pas laisser de traces .

.

...

... .. 38

.

.

.

.

.

.

.

.

.

.

4.2. Extension des privilèges ..

.. .

..

..... 39

.

.

.

.

.

.

.

.

.

.

.

.

4.3. Reprise de la collecte d'informations

.. . . .

40

.

.

.

.