

# Laboratoire : Hacking éthique et Contre-mesures

**Nom de l'étudiant :** Ismael Baby

**Date de remise :** 20-10-2025

# Laboratoire : Hacking éthique et Contre-mesures

## Laboratoire 1 : Hacking éthique et Contre-mesures

<b>ÉTAPE 1 : RECONNAISSANCE ACTIVE .....</b>	<b>3</b>
1.1 DÉCOUVERTE DES MACHINES SUR LE RÉSEAU .....	5
1.2 SCAN COMPLET DE CHAQUE CIBLE .....	6
<b>ÉTAPE 2 : IDENTIFICATION DE LA VULNÉRABILITÉ.....</b>	<b>12</b>
2.1 Metasploitable (192.168.100.20) .....	12
2.3 : OWASPBWA (192.168.100.30) .....	17
2.4 Windows XP (192.168.100.40) .....	21
2.5 :WINDOWS 7(192.168.100.50) .....	23
<b>ÉTAPE 3 : CAMPAGNE DE PHISHING :.....</b>	<b>25</b>
3.1. lancer GoPhish .....	26
3.2 CRÉATION DU PROFIL EXPÉDITEUR .....	27
3.3 CRÉATION DU MODÈLE D'EMAIL .....	28
3.4 CRÉATION DE LA PAGE DE LANDING PAGE.....	29
3.5. IMPORTATION DES CIBLES .....	30
5. LANCEMENT DE LA CAMPAGNE .....	31
<b>ÉTAPE 4 : ANALYSE DE CAPTURE RÉSEAU (.pcap) :.....</b>	<b>33</b>
4.1 :Analysez le fichier .pcap fourni à l'aide de wireshark :.....	33
4.2 :Identifiez les échanges contenant des identifiants. ....	34
4.3 :Récupérez le nom d'utilisateur et le mot de passe présents dans la.....	34
Conclusion .....	35

# Laboratoire : Hacking éthique et Contre-mesures

## Scénario de laboratoire : Mission "Red Eclipse"

### Contexte

Vous êtes engagés comme consultants en cybersécurité pour simuler une attaque ciblée contre l'infrastructure d'une entreprise fictive nommée Red Eclipse Technologies. Votre objectif est de tester la robustesse de leur réseau interne et la vigilance de leurs employés face à des menaces réalistes.

#### Étape 1 : Reconnaissance active

- Objectif : Identifier les services exposés et les configurations réseau des cibles du laboratoire.
- Instructions :
  - o Effectuez une reconnaissance active des machines cibles du laboratoire.
  - o Relevez les adresses IP, ports ouverts, services actifs et versions logiciels.
  - o Cartographiez l'environnement réseau à partir des résultats obtenus.

#### Étape 2 : Identification des vulnérabilités

- Objectif : Déetecter les failles exploitables sur les cibles identifiées.
- Instructions :
  - o Analysez les services détectés pour identifier les vulnérabilités connues.
  - o Appuyez-vous sur les résultats de la reconnaissance active pour cibler vos analyses.
  - o Documentez les vulnérabilités critiques et proposez des hypothèses d'exploitation.

#### Étape 3 : Campagne de phishing avec GoPhish

- Objectif : Tester la réactivité des utilisateurs face à une attaque par ingénierie sociale.

# Laboratoire : Hacking éthique et Contre-mesures

- Instructions :
  - o Créez une campagne de phishing avec GoPhish.
  - o Concevez un courriel et une page de capture crédibles.
  - o Lancez la campagne et analysez les résultats (clics, soumissions de données).

## **Étape 4 : Analyse de la capture réseau (.pcap)**

- Objectif : Extraire des identifiants à partir d'une capture réseau.
- Instructions :

- o Analysez le fichier .pcap fourni à l'aide d'un outil adapté.
- o Identifiez les échanges contenant des identifiants.
- o Récupérez le nom d'utilisateur et le mot de passe présents dans la capture.

### Livrables attendus

- Un rapport technique complet documentant chaque étape du laboratoire.
- Le rapport doit inclure :
  - o Les méthodes utilisées et les résultats obtenus.
  - o Des captures d'écran illustrant chaque étape.
  - o Une analyse critique des techniques employées et des recommandations

# Laboratoire : Hacking éthique et Contre-mesures

## ÉTAPE 1 : RECONNAISSANCE ACTIVE

### 1.1 DÉCOUVERTE DES MACHINES SUR LE RÉSEAU

```
(ismael_kali㉿vbox) -[~]
$ nmap -sn 192.168.100.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 20:09 ADT
Nmap scan report for 192.168.100.20
Host is up (0.00034s latency).
MAC Address: 08:00:27:BD:16:29 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.30
Host is up (0.00069s latency).
MAC Address: 08:00:27:67:2D:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.40
Host is up (0.0027s latency).
MAC Address: 08:00:27:D1:E8:0E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.50
Host is up (0.0022s latency).
MAC Address: 08:00:27:5F:85:A7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.10
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.07 seconds
```

# Laboratoire : Hacking éthique et Contre-mesures

## 1.2 SCAN COMPLET DE CHAQUE CIBLE

### 1.2.1 Scan de Metasploitable (192.168.100.20)

```
(ismael_kali㉿vbox) ~- [~]
$ nmap -sS -sV -O -A 192.168.100.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 20:13 ADT
Nmap scan report for 192.168.100.20
Host is up (0.00097s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|ftp-syst:
|  STAT:
|    FTP server status:
|      Connected to 192.168.100.10
|      Logged in as anonymous
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:c1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:72:ba:e6:1b:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dnsmasq:
|  bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     34009/udp  mountd
|   100005  1,2,3     56502/tcp   mountd
|   100006  1,3,4     37256/tcp   nlockmgr
|   100021  1,3,4     50544/udp  nlockmgr
|   100024  1         52040/udp   status
|   100024  1         55656/tcp   status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
```

```
Version: 5.8.5-1ubuntu5
Thread ID: 8
Capabilities: flags: 43564
Some Capabilities: LongColumnFlag, SupportsCompression, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, Speaks4ProtocolNew, Support4Auth
Status: Autocommit
SASL mech: SVID[TLS]TLSv1.3.1G
632/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-10-15T23:15:37+00:00; -1s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-03-17T14:07:45
900/tcp open  vnc        VNC (protocol 3.3)
vnc-info:
  Protocol version: 3.3
  Security types:
    VNC authentication (2)
000/tcp open  x11        (access denied)
667/tcp open  irc        UnrealIRCd
009/tcp open  ajp13     Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
180/tcp open  http      Apache Tomcat/Coyote JSP engine 1.1
181/tcp open  http      Apache Tomcat/1.1
|_http-favicon: Apache Tomcat/1.1
AC Address: 08:00:27:BD:16:29 (PC Systemtechnik/Oracle VirtualBox virtual NIC)
device type: general purpose
unmap: 2.6.0 - 2.6.X
5 CPE: cpe:/o:canonical:linux_kernel:2.6
5 details: Linux 2.6.9 - 2.6.33
network Distance: 1 hop
service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

os script results:
os-os-discovery:
  OS: Unix (Samba 3.0.20-Debian)
  Computer name: metasploitable
  NetBIOS computer name: metasploitable
  Domain: metasploitable.localdomain
  FQDN: metasploitable.localdomain
  System time: 2025-10-15T19:14:23-04:00
  smb-security-mode:
    account_used: <blank>
    auth_domain: <blank>
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
  smb2-time: Protocol negotiation failed (SMB2)
  _nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
  _clock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: -1s

RACEROUTE
OP RTT ADDRESS
0.97 ms 192.168.100.20

S and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 131.64 seconds
```

# Laboratoire : Hacking éthique et Contre-mesures

Ports ouverts et services :

- **21/tcp** - FTP - vsftpd 2.3.4 (Anonymous login allowed)
- **22/tcp** - SSH - OpenSSH 4.7p1
- **23/tcp** - Telnet - Linux telnetd
- **25/tcp** - SMTP - Postfix smtpd
- **53/tcp** - DNS - ISC BIND 9.4.2
- **80/tcp** - HTTP - Apache httpd 2.2.8
- **111/tcp** - RPC - rpcbind
- **139/tcp** - NetBIOS - Samba smbd 3.X-4.X
- **445/tcp** - NetBIOS - Samba smbd 3.0.20
- **512/tcp** - exec
- **513/tcp** - login
- **514/tcp** - shell
- **1099/tcp** - Java RMI
- **1524/tcp** - ingreslock? (root shell)
- **2049/tcp** - NFS
- **2121/tcp** - FTP - ProFTPD 1.3.1
- **3306/tcp** - MySQL - 5.0.51a

# Laboratoire : Hacking éthique et Contre-mesures

## Système d'exploitation : Linux 2.6.x

### 1.2.2 : Scan de OWASP BWA (192.168.100.30) :

```
[root@kali ~] -
```

```
[*] nmap -sV -O -A 192.168.100.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 20:40 ADT
Nmap scan report for 192.168.100.30
Host is up (0.0004s latency).
Not showing hosts that are up but have no ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 5.3p1 Debian JESSIE (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3024:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_ 2048:3a:94:08:3f:e8:a2:7a:b8:c1:9a:d7:5e:00:55:0c:a7 (RSA)
80/tcp    open  http       Apache httpd/2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-methods:
|   Possibly risky methods: TRACE
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap      Courier Imapd (released 2008)
|_http-server-header: IMAP4rev1:CHILONG/2.2.14
|_http-methods: HEAD,GET,POST,OPTIONS,PUT,DELETE
|_http-title: owaspbwa OWASP Broken Web Applications
443/tcp   open  ssl/http  Apache httpd/2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
|_ssl-cert: Subject: commonName=owaspbwa
|_Not valid before: 2013-01-02T21:12:38
|_Not valid after:  2025-10-15T00:00:00
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-methods:
|   Possibly risky methods: TRACE
5001/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object Java Object Serialization
8080/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache/1.1.25
|_http-methods:
|   Possibly risky methods: TRACE
|_http-title: Choose Your Path
I service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V:7.05K:7xD+10/15$Tlne=68F03DCDP=x86_64-pc-linux-gnu$R
SF-FULL,4,"xaviced@Vx86_64-pc-linux-gnu$R"
MAC: 00:0C:29:67:2D:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general-purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: Linux, CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: OWASPBWA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (<unknown>)
|_clock-skew: mean: +2s, deviation: 0s, median: -2s
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|   security_level: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

[TRACEROUTE]
```

## Système : Linux 2.6.17 - 2.6.36

### Services principaux détectés :

- Port 22/tcp - SSH - OpenSSH 5.3p1 (Accès distant)**
- Port 80/tcp - HTTP - Apache 2.2.14 (Site principal OWASP)**
- Port 139/tcp - SMB - Samba 3.X-4.X (Partages réseau)**
- Port 143/tcp - IMAP - Courier Imapd (Email)**
- Port 443/tcp - HTTPS - Apache 2.2.14 (Site sécurisé OWASP)**
- Port 445/tcp - SMB - Samba 3.X-4.X (Partages réseau)**
- Port 5001/tcp - Java - Serialization (Service Java)**
- Port 8080/tcp - HTTP - Apache Tomcat (Applications JSP)**
- Port 8081/tcp - HTTP - Jetty 6.1.25 (Applications web)**

# Laboratoire : Hacking éthique et Contre-mesures

## 1.2.3 Scan de Windows XP (192.168.100.40) :

```
(ismael_kali㉿vbox)-[~]
└─$ nmap -sS -sV -O -A 192.168.100.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 20:50 ADT
Nmap scan report for 192.168.100.40
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows XP microsoft-ds
MAC Address: 08:00:27:D1:E8:0E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp3:embedded cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:w
indows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Embedded Standard 2009, Microsoft Windows XP SP2 or SP3, or Windows Server 200
3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_nbstat: NetBIOS name: ISMAEL, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d1:e8:0e (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
|_clock-skew: mean: 1h29m57s, deviation: 2h07m16s, median: -2s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-_
|   Computer name: ismael
|   NetBIOS computer name: ISMAEL\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2025-10-15T20:50:59-03:00

TRACEROUTE
HOP RTT      ADDRESS
1  1.34 ms  192.168.100.40

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.78 seconds
└─(ismael_kali㉿vbox)-[~]
```

Système : Microsoft Windows XP SP2 ou SP3

Services principaux détectés :

- Port 135/tcp - **MSRPC** - Microsoft Windows RPC (Remote Procedure Call)
- Port 139/tcp - **NetBIOS-SSN** - Microsoft Windows netbios-ssn (Partages réseau)
- Port 445/tcp - **MICROSOFT-DS** - Windows XP microsoft-ds (Partages fichiers SMB)

Informations système :

- Nom NetBIOS : **ISMAEL**
- Computer name : **Ismael**
- Groupe de travail : **WORKGROUP**
- Signature SMB : **Désactivée (dangereux)**

# Laboratoire : Hacking éthique et Contre-mesures

- Authentification : Niveau utilisateur

## 1.2.4 : Scan de Windows 7 (192.168.100.50) :

```
(ismael_kali㉿vbox)-[~]
$ nmap -sS -sV -O -A 192.168.100.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 21:00 ADT
Nmap scan report for 192.168.100.50
Host is up (0.00052s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:5F:85:A7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: ISMAEL-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_  Message signing enabled but not required
| clock-skew: mean: 59m58s, deviation: 1h43m55s, median: -1s
| smb-os-discovery:
|_  OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|_  OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|_  Computer name: ismael-PC
|_  NetBIOS computer name: ISMAEL-PC\x00
|_  Workgroup: WORKGROUP\x00
|_  System time: 2025-10-15T21:01:40-03:00
|_ nbstat: NetBIOS name: ISMAEL-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:5f:85:a7 (PCS Systemtechnik/Oracle VirtualBox virtua
l NIC)
| smb2-time:
|   date: 2025-10-16T00:01:40
|_ start_date: 2025-10-15T22:40:33
| smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT      ADDRESS
1  0.52 ms  192.168.100.50

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.31 seconds
```

Système : Windows 7 Professional 7601 Service Pack 1

Services principaux détectés :

- Port 135/tcp - MSRPC - Microsoft Windows RPC
- Port 139/tcp - NetBIOS-SSN - Microsoft Windows netbios-ssn
- Port 445/tcp - MICROSOFT-DS - Windows 7 microsoft-ds (SMB)
- Ports 49152-49157/tcp - MSRPC - Microsoft Windows RPC (ports dynamiques)

Informations système :

- Nom NetBIOS : ISMAEL-PC

# Laboratoire : Hacking éthique et Contre-mesures

- **Groupe de travail : WORKGROUP**
- **Signature SMB : Désactivée**
- **Authentification : Niveau utilisateur avec accès guest**

## 1.2.5 : CARTOGRAPHIE DU RÉSEAU - ENVIRONNEMENT COMPLET :

### KALI LINUX (192.168.100.10)

- **Rôle : Station d'attaque principale**
- **OS : Kali Linux**
- **Fonction : Analyse et tests de pénétration**

### METASPLOITABLE (192.168.100.20)

- **OS : Linux 2.6.x (Ubuntu)**
- **Services critiques :**
  - **FTP (21) - vsftpd 2.3.4 - BACKDOOR CONNU**
  - **SSH (22) - OpenSSH 4.7p1**
  - **HTTP (80) - Apache 2.2.8**
  - **Samba (139/445) - Version vulnérable**
  - **MySQL (3306) - 5.0.51a**

### OWASP BWA (192.168.100.30)

- **OS : Linux 2.6.17-2.6.36**
- **Services critiques :**
  - **HTTP/HTTPS (80/443) - Applications web vulnérables**
  - **Tomcat (8080) - Applications JSP**
  - **Jetty (8081) - Applications web**

Samba (139/445) - Partages réseau

### WINDOWS XP (192.168.100.40)

- **OS : Windows XP SP2/SP3**
- **Services critiques :**
  - **SMB/NetBIOS (139/445) - NON SÉCURISÉ**
  - **RPC (135) - Service distant**

# Laboratoire : Hacking éthique et Contre-mesures

WINDOWS 7 (192.168.100.50)

- OS : Windows 7 Professional SP1
- Services critiques :
  - SMB/NetBIOS (139/445) - Signature désactivée
  - RPC (135 + ports dynamiques)

## ÉTAPE 2 : IDENTIFICATION DE LA VULNÉRABILITÉ

2.1 Metasploitable (192.168.100.20)

### VULNÉRABILITÉS CRITIQUES IDENTIFIÉES

#### 2.1.1. Backdoor vsftpd 2.3.4

- Port : 21/tcp + 6200/tcp
- CVE : CVE-2011-2523
- Description : Backdoor compromise dans les packages vsftpd
- Preuve : Service détecté sur le port 6200

vsftpd Compromised Source Packages Backdoor Vulnerability

9.8 (High) 99 % 192.168.100.20 6200/tcp N/A N/A

---

**Summary**  
vsftpd is prone to a backdoor vulnerability.

**Detection Result**  
Vulnerability was detected according to the Detection Method.

**Insight**  
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

**Detection Method**

Details: vsftpd Compromised Source Packages Backdoor Vulnerability OID: 1.3.6.1.4.1.25623.1.0.103185  
Version used: 2023-12-07T05:05:41Z

**Affected Software/OS**  
The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

**Impact**  
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

#### Hypothèse d'exploitation :

Avec cette backdoor, c'est super simple pour un attaquant. Il peut se connecter directement sur le port 6200 sans aucun mot de passe. En gros, c'est comme si la machine avait une porte secrète qui donne un accès direct. L'attaquant ouvre juste une connexion sur le port 6200 et il a immédiatement un shell avec les droits administrateur. C'est

# Laboratoire : Hacking éthique et Contre-mesures

littéralement la pire faille possible - ça prend 30 secondes et ça donne un contrôle total sur la machine sans avoir besoin de cracker quoi que ce soit.

## 2.1.2. Backdoor Ingreslock

- **Port : 1524/tcp**
- **CVSS : 10.0 (GVM)**
- **Description : Service ingreslock configuré comme backdoor**
- **Preuve : Port ouvert avec accès shell direct**

### Hypothèse d'exploitation :

Cette porte dérobée est encore plus simple que la précédente. Le service sur le port 1524 fournit directement un shell root dès la connexion.

En pratique, le pirate fait exactement cela :

Il ouvre une connexion vers le port 1524 .Et il obtient immédiatement un terminal avec tous les pouvoirs sur la machine.C'est comme si la machine avait laissé une session administrateur ouverte et accessible à tous les utilisateurs du réseau. Aucune compétence technique n'est requise : il suffit de se connecter et c'est tout.

Possible Backdoor: Ingreslock

10.0 (High) 99 % 192.168.100.20 1524/tcp N/A N/A

---

**Summary**  
A backdoor is installed on the remote host.

**Detection Result**  
The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)

**Detection Method**  
Details: Possible Backdoor: Ingreslock OID: 1.3.6.1.4.1.25623.1.0.103549  
Version used: 2023-07-25T05:05:58Z

**Impact**  
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected system.

**Solution**  
Solution Type: Workaround  
A whole cleanup of the infected system is recommended.

# Laboratoire : Hacking éthique et Contre-mesures

## 2.1.3. Vulnérabilité Apache Tomcat Ghostcat

- **Port : 8009/tcp (AJP Connector)**
- **CVSS : 9.8 (GVM & Nessus)**
- **CVE : CVE-2020-1938**
- **Description : Injection de requêtes AJP permettant la lecture de fichiers**

**Hypothèse d'exploitation :** Avec cette faille Ghostcat, un attaquant peut envoyer des requêtes spéciales au serveur Tomcat via le port 8009. En gros, il peut demander au serveur de lui montrer n'importe quel fichier du système. Par exemple, il pourrait lire le fichier /etc/passwd pour voir tous les utilisateurs, ou voler des fichiers de configuration qui contiennent des mots de passe. C'est super dangereux parce que sans même avoir de compte sur la machine, l'attaquant peut voler tous les fichiers sensibles. Et en plus, dans certains cas, il pourrait même réussir à exécuter du code à distance pour prendre le contrôle complet du serveur.

Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check		9.8 (High)	99 %	192.168.100.20	8009/tcp	N/A	N/A	Coordinated Universal Time
	<b>Summary</b> Apache Tomcat is prone to a remote code execution (RCE) vulnerability in the AJP connector dubbed 'Ghostcat'. <b>Detection Result</b> It was possible to read the file "/WEB-INF/web.xml" through the AJP connector. Result: AB 8\x0004 \x00088 \x00020K \x0001 \x000CContent-Type \x001ctext/html; charset=ISO-8859-1 AB\x001F\x003\x001F,<!-- Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to You under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a> Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. --> <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">							

# Laboratoire : Hacking éthique et Contre-mesures

**Description**  
A file read//inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

**Solution**  
Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

**See Also**  
<http://www.nessus.org/u?8eb6246>  
<http://www.nessus.org/u?4e287adb>  
<http://www.nessus.org/u?cb3d54>  
<https://access.redhat.com/security/cve/CVE-2020-1745>  
<https://access.redhat.com/solutions/4851251>  
<http://www.nessus.org/udd21b234>  
<http://www.nessus.org/udd772531>  
<http://www.nessus.org/u?2a01d6bf>  
<http://www.nessus.org/u?3b5af27e>  
<http://www.nessus.org/u?9dab109f>  
<http://www.nessus.org/u?5eacf70>

**Output**  
Nessus was able to exploit the issue using the following request :  

```
0x0000: 02 02 00 08 46 54 51 50 2F 31 2B 31 00 00 0F 2F      ....HTTP/1.1.../  
0x0010: 61 73 64 66 2F 78 78 78 2B 6A 73 70 00 00  and/xxxxx.jsp..  
0x0020: 09 6C 67 61 61 6C 68 6F 73 74 00 FF FF 00 09 6C  .localhost....1  
0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06  ..keep-alive....A  
0x0040: 00 0A 6B 65 70 2D 61 6C 69 76 65 00 00 0F 41  ..keep-alive....A  
0x0050: 63 61 65 70 74 2D 4C 61 6B 67 75 61 67 65 00 00  except-language..  
0x0060: 6E 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65  ..no ..-no ..-no ..  
more...
```

**Plugin Details**  
Severity: Critical  
ID: 134862  
Version: 1.54  
Type: remote  
Family: Web Servers  
Published: March 24, 2020  
Modified: October 1, 2025

**Risk Information**  
Risk Factor: High  
**CVSS v3.0 Base Score: 9.8**  
CVSS v3.0 Vector: CVSS:3.0/A:V/N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/R:C  
CVSS v3.0 Temporal Score: 9.4  
CVSS v2.0 Base Score: 7.5  
CVSS v2.0 Temporal Score: 6.5  
CVSS v2.0 Vector: CVSS:2#AV:N/AC:L/Au:N/C:P/I:P/A:P  
CVSS v2.0 Temporal Vector: CVSS:2#E:H/RL:O/R:C

**Vulnerability Information**  
CPE: cpe:/a:apache:tomcat  
Exploit Available: true  
Exploit Ease: Exploits are available  
Patch Pub Date: March 1, 2020

## 2.1.4. Vulnérabilité RCE DistCC

- Port : 3632/tcp**
- CVSS : 9.3 (GVM)**
- CVE : CVE-2004-2687**
- Description : Exécution de commandes à distance via DistCC**

**Hypothèse d'exploitation :** DistCC c'est un service qui sert normalement à compiler du code à distance, mais là il est mal configuré. Un attaquant peut envoyer des commandes au service DistCC sur le port 3632 pour lui demander d'exécuter n'importe quelle commande système. Par exemple, il pourrait lui faire lancer un shell inverse qui se connecte back à sa machine, ou exécuter des commandes pour créer un nouvel utilisateur, installer un malware, etc. En gros, au lieu de juste compiler du code, le service obéit à toutes les commandes qu'on lui donne, comme si l'attaquant était assis devant le clavier de la machine.

# Laboratoire : Hacking éthique et Contre-mesures

The screenshot shows a security analysis interface for a DistCC RCE vulnerability (CVE-2004-2687). Key details from the interface:

- Summary:** DistCC is prone to a remote code execution (RCE) vulnerability.
- Detection Result:** It was possible to execute the "id" command. Result: uid=1(daemon) gid=1(daemon)
- Insight:** DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.
- Detection Method:** Details: DistCC RCE Vulnerability (CVE-2004-2687) OID: 1.3.6.1.4.1.25623.1.0.103553 Version used: 2022-07-07T10:16:06Z
- Impact:** DistCC by default trusts its clients completely that in turn

## 2.2.5. PostgreSQL Default Credentials

- **Port :** 5432/tcp
- **CVSS :** 9.0 (GVM)
- **Description :** Authentification avec identifiants par défaut
- **Hypothèse d'exploitation :** La base de données PostgreSQL a encore les mots de passe par défaut, genre "postgres/postgres" ou des trucs comme ça.

Un attaquant peut se connecter directement à la base de données sans avoir à deviner le mot de passe. Une fois connecté, il peut :

- Lire toutes les données de la base
- Modifier ou supprimer des informations importantes
- Voler des données sensibles comme des mots de passe d'utilisateurs
- Essayer d'exécuter des commandes système via la base de données

C'est comme si la base de données était ouverte à tout le monde - pas besoin de forcer la porte, elle est déjà déverrouillée.

# Laboratoire : Hacking éthique et Contre-mesures

PostgreSQL Default Credentials (PostgreSQL Protocol)

9.0 (High) 99 % 192.168.100.20 5432/tcp N/A N/A

**Summary**  
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

**Detection Result**  
It was possible to login as user postgres with password "postgres".

**Detection Method**  
Details: PostgreSQL Default Credentials (PostgreSQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.103552  
Version used: 2024-07-19T15:39:06Z

**Solution**  
**Solution Type:** ↲ Mitigation  
Change the password as soon as possible.

## 2.3 : OWASPBWA (192.168.100.30)

### VULNÉRABILITÉS CRITIQUES IDENTIFIÉES

#### 2.3.1. Joomla Multiple Vulnerabilities (HTTP)

**Port :** 80/tcp

**CVSS :** 9.8 (GVM)

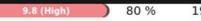
**CVE :** Multiples CVE selon les versions

**Description :** Applications Joomla avec failles de sécurité critiques sur HTTP

**Preuve :** Versions vulnérables de Joomla détectées sur le port 80

**Hypothèse d'exploitation :** Un attaquant peut exploiter ces failles pour exécuter du code à distance via le site web non chiffré.

# Laboratoire : Hacking éthique et Contre-mesures

Joomla! Core LDAP Information Disclosure Vulnerability (Nov 2017)  9.8 (High) 80 % 192.168.100.30 80/tcp N/A N/A

---

**Summary**  
Joomla is prone to an information disclosure vulnerability.

**Detection Result**

Installed version: 1.5.15  
Fixed version: 3.8.2

**Insight**  
The flaw exists due to an inadequate escaping in the LDAP authentication plugin.

**Detection Method**  
Checks if a vulnerable version is present on the target host.

Details: Joomla! Core LDAP Information Disclosure Vulnerability (Nov 2017) OID: 1.3.6.1.4.1.25623.1.0.811896

Version used: 2024-02-20T05:05:48Z

**Affected Software/OS**  
Joomla core version 1.5.0 through 3.8.1

**Impact**  
Successfully exploiting this issue allow remote attackers to disclose username and password.

## 2.3.2. Joomla Multiple Vulnerabilities (HTTPS)

**Port :** 443/tcp

**CVSS :** 9.8 (GVM)

**Description :** Applications Joomla avec failles de sécurité critiques sur HTTPS

**Preuve :** Versions vulnérables de Joomla détectées sur le port 443

**Hypothèse d'exploitation :** Même si la connexion est chiffrée avec HTTPS, le site Joomla a des failles critiques dans son code.

Un attaquant peut envoyer des requêtes malicieuses au site web pour :

- Prendre le contrôle du site en se créant un compte administrateur
- Voler la base de données qui contient tous les utilisateurs et mots de passe
- Uploader un fichier malveillant sur le serveur et l'exécuter
- Prendre le contrôle complet du serveur web

Le HTTPS protège juste la communication, mais si l'application elle-même a des failles, l'attaquant peut quand tout casser. C'est comme avoir une porte blindée mais avec une serrure pourrie.

# Laboratoire : Hacking éthique et Contre-mesures

HTTP Brute Force Logins With Default Credentials Reporting

9.8 (High)

95 %

192.168.100.30

443/tcp

N/A

N/A

**Summary**  
It was possible to login into the remote Web Application using default credentials.

**Detection Result**  
It was possible to login with the following credentials (<URL>:<User>:<Password>:<HTTP status code>)  
<https://192.168.100.30/WebGoat/attack:user:user:HTTP/1.1> 200 OK

**Insight**  
As the VT 'HTTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

**Detection Method**  
Reports default credentials detected by the VT 'HTTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041).  
Details: [HTTP Brute Force Logins With Default Credentials Reporting](#) OID: 1.3.6.1.4.1.25623.1.0.103240  
Version used: 2025-05-23T15:42:02Z

**Impact**  
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

## 2.3.3 : Failles de Chiffrement SSL/TLS

**Port :** 443/tcp

**CVSS :** 9.8 (Nessus)

**Description :** Protocoles SSLv2/SSLv3 vulnérables et chiffrements faibles

**Preuve :** Support de protocoles obsolètes détecté

**Hypothèse d'exploitation :** Même avec HTTPS, les vieux protocoles SSLv2 et SSLv3 ont des failles graves.

Un attaquant qui écoute le réseau peut :Casser le chiffrement et lire toutes les communications "protégées"Voler les identifiants de connexion qui passent sur le réseau. Se faire passer pour le site web et voler les infos des utilisateurs. Faire des attaques "man in the middle" sans que personne ne s'en rende compte. C'est comme si la connexion sécurisée avait un gros trou - le cadenas est là, mais il s'ouvre avec un trombone.

# Laboratoire : Hacking éthique et Contre-mesures

The screenshot shows the Nessus interface for the 'SSL Version 2 and 3 Protocol Detection' plugin. The status is 'CRITICAL'. The 'Description' section notes that the remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which are affected by several cryptographic flaws, including an insecure padding scheme with CBC ciphers and insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or decrypt communications. The 'Risk Information' section lists a CVSS v3.0 Base Score of 9.8. The 'Plugin Details' section provides metadata like Severity: Critical, ID: 20007, Version: 1.34, Type: remote, Family: Service detection, Published: October 12, 2005, and Modified: April 4, 2022.

## 2.3.4 :Système d'Exploitation Obsolète

**CVSS :** 10. CRITICAL (Nessus)

**Description :** Ubuntu en fin de vie sans mises à jour de sécurité

**Preuve :** Détection d'un système d'exploitation non maintenu

**Hypothèse d'exploitation :** Le système Ubuntu est trop vieux et n'est plus mis à jour. C'est comme une maison avec des fenêtres qui ne ferment plus. Un attaquant peut profiter de toutes les failles de sécurité découvertes récemment, mais qui ne seront jamais corrigées sur cette machine. Il peut : Utiliser des failles connues depuis des années. Installer des malwares sans se faire repérer. Prendre le contrôle total facilement. Rester caché très longtemps car personne ne surveille cette vieille version. C'est la cible parfaite car elle ne se défend plus du tout.

The screenshot shows the Nessus interface for the 'Canonical Ubuntu Linux SEoL (10.04.x)' plugin. The status is 'CRITICAL'. The 'Description' section states that Canonical Ubuntu Linux 10.04.x is no longer maintained by its vendor or provider, and lacks support, meaning no new security patches will be released. The 'Risk Information' section lists a CVSS v3.0 Base Score of 10.0. The 'Plugin Details' section provides metadata like Severity: Critical, ID: 201475, Version: 1.2, Type: combined, Family: General, Published: July 3, 2024, and Modified: March 26, 2022.

# Laboratoire : Hacking éthique et Contre-mesures

## 2.4 Windows XP (192.168.100.40)

### 2.4.1 : Système d'Exploitation Obsolète Windows XP

- **CVSS** : 10.0 (GVM) / CRITICAL (Nessus)
- **Description** : Windows XP en fin de vie sans mises à jour de sécurité
- **Preuve** : Détection d'un système d'exploitation non maintenu
- **Hypothèse d'exploitation** : Un attaquant peut exploiter n'importe quelle faille de sécurité connue depuis 2014, car le système ne reçoit plus de correctifs. Il peut utiliser des exploits publics comme EternalBlue ou MS08-067 pour prendre le contrôle complet sans aucune difficulté.

The screenshot shows a Nessus scan report for a host running Microsoft Windows XP. The report highlights a critical vulnerability: "Microsoft Windows XP Unsupported Installation Detection".  
Description: The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.  
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.  
Solution: Upgrade to a version of Windows that is currently supported.  
See Also: <http://www.nessus.org/u/2f80ae/f2>, <http://www.nessus.org/u/321523eb>, <https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>, <http://www.nessus.org/u/89dcab5e4>  
Output: No output recorded.  
To see debug logs, please visit individual host  
Port: 445 Hosts: 192.168.100.40  
Plugin Details:  
Severity: Critical  
ID: 73182  
Version: 1.20  
Type: combined  
Family: Windows  
Published: March 25, 2014  
Modified: September 22, 2020  
Risk Information:  
Risk Factor: Critical  
CVSS v3.0 Base Score: 10.0  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/H:H/A:H  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C  
CVSS v3.0 Temporal Score: 9.0  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Temporal Score: 7.8  
CVSS v2.0 Vector: CVSS:2.0/AV:N/AC:L/Au:N/C:C/I:C  
CVSS v2.0 Temporal Vector: CVSS:2.0/EP:R/L:O/RC:C  
Vulnerability Information:  
CPE: cpe:/o:microsoft:windows\_xp  
Exploit Available: true  
Exploit Ease: Exploits are available  
In the news: true

### 2.4.2 : Faille MS08-067 Windows SMB

- **Port** : 445/tcp
- **CVSS** : 9.8 (Nessus)
- **Description** : Vulnérabilité critique dans le service Server
- **Preuve** : Service SMB vulnérable détecté
- **Hypothèse d'exploitation** : Un attaquant envoie une requête RPC spécialement crafted au service SMB pour exécuter du code arbitraire à distance et obtenir un shell avec les priviléges SYSTEM.

# Laboratoire : Hacking éthique et Contre-mesures

**Description**  
The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.

**Solution**  
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

**See Also**  
<https://www.nessus.org/u7adf86aac>

**Output**  
No output recorded.  
To see debug logs, please visit individual host

**Port** ▾ **Hosts**  
445 /tcp /clfs 192.168.100.40

**Plugin Details**

Severity:	Critical
ID:	34477
Version:	1.53
Type:	remote
Family:	Windows
Published:	October 23, 2008
Modified:	August 5, 2020

**Risk Information**

Risk Factor:	Critical
<b>CVSS v3.0 Base Score:</b>	9.8
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector:	CVSS:3.0/E:H/RL:O/R:CC
CVSS v3.0 Temporal Score:	9.4
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Temporal Score:	8.7
CVSS v2.0 Vector:	CVSS:2#AV:N/AC:L/Au:N/C:C/I:C
CVSS v2.0 Temporal Vector:	CVSS:2#E:H/RL:O/R:CC
IAVM Severity:	I

## 2.4.3 : EternalBlue MS17-010

- Port :** 445/tcp
- CVSS :** 8.1 (Nessus)
- CVE :** CVE-2017-0144
- Description :** Vulnérabilité critique dans SMBv1
- Preuve :** Service SMBv1 activé et vulnérable
- Hypothèse d'exploitation :** Un attaquant utilise l'exploit EternalBlue pour propager un malware et prendre le contrôle de la machine, comme lors des attaques WannaCry.

**Description**  
The remote Windows host is affected by the following vulnerabilities:  
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)  
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

**Solution**  
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

**See Also**  
<http://www.nessus.org/u768fc8eff>  
<http://www.nessus.org/u7321523eb>  
<http://www.nessus.org/u0605561d0>  
<http://www.nessus.org/u7df569cf>  
<https://blogs.technet.microsoft.com/llecab/2016/09/16/stop-using-smb1/>  
<http://www.nessus.org/u7999ebf9>  
<http://www.nessus.org/u78dcab5e4>

**Plugin Details**

Severity:	High
ID:	97833
Version:	1.30
Type:	remote
Family:	Windows
Published:	March 20, 2017
Modified:	May 25, 2022

**Risk Information**

Risk Factor:	High
<b>CVSS v3.0 Base Score:</b>	8.1
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector:	CVSS:3.0/E:H/RL:O/R:CC
CVSS v3.0 Temporal Score:	7.7
CVSS v2.0 Base Score:	9.3
CVSS v2.0 Temporal Score:	8.1
CVSS v2.0 Vector:	CVSS:2#AV:N/AC:M/Au:N/C:C/I:C
CVSS v2.0 Temporal Vector:	CVSS:2#E:H/RL:O/R:CC
IAVM Severity:	I

**Vulnerability Information**

CPE:	cpe:/o:microsoft:windows
Exploit Available:	true
Exploit Ease:	Exploits are available

# Laboratoire : Hacking éthique et Contre-mesures

## 2.4.4 : Session SMB NULL Authentication

- **Port :** 445/tcp
- **CVSS :** 7.3 (Nessus)
- **Description :** Accès sans authentification aux partages SMB
- **Preuve :** Connexion anonyme possible aux partages
- **Hypothèse d'exploitation :** Un attaquant peut se connecter sans mot de passe aux partages réseau et lire/modifier/supprimer tous les fichiers accessibles.

The screenshot shows the Nessus interface with the following details:

- Vulnerabilities:** 28
- HIGH** SMB NULL Session Authentication
- Description:** The remote host is running and SMB protocol. It is possible to log into the browser or spoolss pipes using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.
- Solution:** Please contact the product vendor for recommended solutions.
- See Also:**
  - <http://www.nessus.org/u/e32d594f>
  - <http://www.nessus.org/u/9182e6b>
  - <http://www.nessus.org/u/a33fe205>
- Output:** It was possible to bind to the following pipes:
  - browserTo see debug logs, please visit individual host
- Hosts:**

Port	Hosts
445 / tcp / cifs	192.168.100.40
- Plugin Details:**
  - Severity: High
  - ID: 26920
  - Version: 1.42
  - Type: remote
  - Family: Misc.
  - Published: October 4, 2007
  - Modified: October 7, 2022
- Risk Information:**
  - Risk Factor: High
  - CVSS v3.0 Base Score: 7.3**
  - CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
  - CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/R:CC
  - CVSS v3.0 Temporal Score: 7.0
  - CVSS v2.0 Base Score: 7.5
  - CVSS v2.0 Temporal Score: 6.5
  - CVSS v2.0 Vector: CVSS2#AV:N/AC:L/A:N/C:P/I:P/A:P
  - CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:O/R:CC

## 2.5 :WINDOWS 7(192.168.100.50)

### 2.5.1 : Système Windows 7 en Fin de Support

- **Port :** général
- **CVSS :** 10.0 (GVM)
- **Description :** Windows 7 en fin de vie sans mises à jour de sécurité
- **Preuve :** Détection d'un système d'exploitation non maintenu
- **Hypothèse d'exploitation :** Un attaquant peut exploiter les failles de sécurité découvertes depuis 2020, car le système ne reçoit plus de correctifs de sécurité de Microsoft.

# Laboratoire : Hacking éthique et Contre-mesures

Operating System (OS) End of Life (EOL) Detection

10.0 (High) 80 % 192.168.100.50 general/tcp N/A N/A Fri, Oct 17, 2025 4:25 AM Coordinated Universal Time

**Summary**  
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

**Detection Result**  
The "Windows 7" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:microsoft:windows\_7::sp1  
Installed version, build or SP: sp1  
EOL date: 2020-01-14  
EOL info: <https://learn.microsoft.com/en-us/lifecycle/products/windows-7>

**Product Detection Result**  
Product cpe:/o:microsoft:windows\_7::sp1  
Method OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)  
Log View details of product detection

**Detection Method**  
Checks if an EOL version of an OS is present on the target host.

## 2.5.2 Vulnérabilités SMB Windows 7

- Port :** 445/tcp
- CVSS :** 8.8 (GVM)
- Description :** Vulnérabilités multiples dans le service SMB
- Preuve :** Service SMB vulnérable détecté
- Hypothèse d'exploitation :** Un attaquant peut exploiter des failles SMB comme EternalBlue pour exécuter du code à distance et prendre le contrôle de la machine.

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

8.8 (High) 95 % 192.168.100.50 445/tcp N/A N/A Fri, Oct 17, 2025 4:33 AM Coordinated Universal Time

**Summary**  
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

**Detection Result**  
Vulnerability was detected according to the Detection Method.

**Insight**  
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

**Detection Method**  
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)...OID: 1.3.6.1.4.1.25623.1.0.810676

Version used: 2024-07-17T05:05:38Z

**Affected Software/OS**  
- Microsoft Windows 10 x32/x64  
- Microsoft Windows Server 2012  
- Microsoft Windows Server 2016

# Laboratoire : Hacking éthique et Contre-mesures

## 2.5.3 :Services RPC Exposés

- **Port :** 135/tcp
- **CVSS :** 5.0 (GVM)
- **Description :** Services DCE/RPC et MSRPC accessibles à distance
- **Preuve :** Enumération des services RPC possible
- **Hypothèse d'exploitation :** Un attaquant peut énumérer les services RPC pour identifier des fonctionnalités vulnérables et potentiellement exécuter du code à distance.

The screenshot shows a network enumeration report for DCE/RPC and MSRPC services. The top bar includes the title 'DCE/RPC and MSRPC Services Enumeration Reporting', a progress bar at 80%, the IP address '192.168.100.50', and the port '135/tcp'. On the right, it shows the date and time: 'Fri, Oct 17, 2025 4:29 AM Coordinated Universal Time'. The main content area has a 'Summary' section stating that services can be enumerated by connecting on port 135. Below this is a 'Detection Result' section listing several services:

Port	UUID	Annotation
49152/tcp	d95afe70-a6d5-4259-822e-2c84da1ddbd0d	version 1 Endpoint: ncacn_ip_tcp:192.168.100.50[49152]
49153/tcp	06bbba54a-be05-49f9-b0a0-30f790261023	version 1 Endpoint: ncacn_ip_tcp:192.168.100.50[49153] Annotation: Security Center
49153/tcp	30adc50c-5cbc-46ce-9a0e-91914789e23c	version 1 Endpoint: ncacn_ip_tcp:192.168.100.50[49153] Annotation: NRP server endpoint
49153/tcp	3c4728c5-f0ab-448b-bdal-6ce01eb0a6d5	version 1 Endpoint: ncacn_ip_tcp:192.168.100.50[49153] Annotation: DHCP Client LRPC Endpoint

## ÉTAPE 3 : CAMPAGNE DE PHISHING :

Une campagne de phishing a été conçue à l'aide de GoPhish. Les étapes comprenaient la création du profil expéditeur, du modèle d'email, de la page de destination et l'importation des cibles avant le lancement de la campagne. Cette simulation a permis de comprendre comment les utilisateurs peuvent être incités à divulguer leurs informations d'identification

# Laboratoire : Hacking éthique et Contre-mesures

## 3.1. lancer GoPhish

```
[~] (ismael_kali㉿vbox) [-]
└─$ sudo apt update && sudo apt install -y unzip wget
Reception de : 1 http://kali.download/Kali Kali-rolling InRelease [34,0 kB]
Reception de : 2 http://kali.download/kali kali-rolling/main amd64 Packages [20,9 MB]
Reception de : 3 http://kali.download/kali kali-rolling/main amd64 Contents [1,6 MB]
Reception de : 4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Reception de : 5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [258 kB]
Reception de : 6 http://kali.download/kali kali-rolling/non-free amd64 Packages [187 kB]
Reception de : 7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [891 kB]
7 paquets à installer sur 7 en tout
480 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
unzip est déjà la version la plus récente (6.0-29).
wget est déjà la version la plus récente (1.25.0-2).
Les packages suivants sont installés mais ne sont plus nécessaires :
  amass-common      libimongocrypt0          libitheora-dec1           python3-kismet-capturerl433
  libbluray2        libipgcode349            libitheoraenc1          python3-kismet-capturerladsb
  libbison-1.0-0t64 libplacebo349            liblbdread4             python3-kismet-capturerlaml
  libbz2-1.0         libplacebo349            liblbdread4             python3-packagekit-whl
  libdata-dict-common libqt5ctct-common1.8    libtx264-104           python3-pkgconf
  libdatalog2        libqt5frame1             libveip0                python3-wheel-whl
  libgeo3s-13.1     libsigsev2              python3-bluepy          samba-ad-dc
  libgeo3s-13.1     libsigsev2              python3-bluepy          samba-ad-provision
  libgeo3s-13.1     libsigsev2              python3-bluepy          samba-dsdb-modules
  libgeo3s-13.1     libsigsev2              python3-kismetcapturebtgeiger
  libgeo3s-13.1     libtheora0               python3-kismetcapturebreakabszigbee
  libmongoc-1.0-0t64 libtheora0               Veuillez utiliser « sudo apt autoremove » pour les supprimer.

Veuillez utiliser « sudo apt autoremove » pour les supprimer.

Sommaire :
  Mise à niveau de : 0. Installation de : 0Supprimé : 0. Non mis à jour : 480

[~] (ismael_kali㉿vbox) [-]
└─$ wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip -O gophish.zip
--2025-10-18 21:35:42-- https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip
Résolution de github.com (github.com)... 140.82.113.4
Connexion à github.com (github.com)|140.82.113.4|:443... connectée.
requête HTTP transmise, en attente de la réponse... 302 Found
Emplacement : https://release-assets.githubusercontent.com/github-production-release-asset/14508450/d275c2cd-8d50-49e6-a442-fec1dd0f1a3?sp=r&ssr=https%3A%2F%2FzWnfZFc2oekhJvNjdg1vb151b91LmVcmud21uz699cy5uZXriTQ.p29RKL5jd1-1003EqYIloetTyqElrymQwQFNvAc1_Mresponse-content-disposition=attachment%3B%2ffilename%3Dgophish-v0.12.1-linux-64bit.zip&response-content-type=application%2Fzip%2B%2Ftar%2B%2Fgzip
[~] (ismael_kali㉿vbox) [-]
└─$ unzip gophish.zip && cd gophish/gophish-v0.12.1-linux-64bit
chmod +x gophish
Archive: gophish.zip
  inflating: gophish/gophish
  creating: gophish/static/js/dist/
  creating: gophish/static/js/dist/app/
  inflating: gophish/static/js/dist/app/sending_profiles.min.js
  inflating: gophish/static/js/dist/app/campaign_results.min.js
  inflating: gophish/static/js/dist/app/gophish.min.js
  inflating: gophish/static/js/dist/app/campaigns.min.js
  inflating: gophish/static/js/dist/app/autocomplete.min.js
  inflating: gophish/static/js/dist/app/settings.min.js
  inflating: gophish/static/js/dist/app/users.min.js
  inflating: gophish/static/js/dist/app/webhooks.min.js
  inflating: gophish/static/js/dist/app/dashboard.min.js
  inflating: gophish/static/js/dist/app/passwords.min.js
  inflating: gophish/static/js/dist/app/templates.min.js
  inflating: gophish/static/js/dist/app/groups.min.js
  inflating: gophish/static/js/dist/app/landing_pages.min.js
  inflating: gophish/static/js/dist/vendor/min.js
  creating: gophish/static/js/src/vendor/ckeditor/
  inflating: gophish/static/js/src/vendor/ckeditor/CHANGESEN
  creating: gophish/static/js/src/vendor/ckeditor/skins/
  creating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/
  inflating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/editor_ie.css
  inflating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/editor_gecko.css
  inflating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/icons.png
  inflating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/readme.md
  creating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/images/
  inflating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/images/refresh.png
  inflating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/images/arrow.png
  creating: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/images/hidpi/
extracting: gophish/static/js/src/vendor/ckeditor/skins/moono-lisa/images/hidpi/refresh.png
```

# Laboratoire : Hacking éthique et Contre-mesures

```
(ismael_kali㉿vbox) -[~/gophish]
$ chmod +x gophish

(ismael_kali㉿vbox) -[~/gophish]
$ sudo ./gophish

time="2025-10-18T21:40:06-03:00" level=warning msg="No contact address has been configured."
time="2025-10-18T21:40:06-03:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20220321133237
OK 20160118194630_init.sql
OK 20160131153104_0.1.2_add_event_details.sql
OK 20160211211220_0.1.2_add_ignore_cert_errors.sql
OK 20160217211342_0.1.2_create_from_col_results.sql
OK 20160225173824_0.1.2_capture_credentials.sql
OK 20160227180335_0.1.2_store-smtp-settings.sql
OK 20160317214457_0.2_redirect_url.sql
OK 20160605210903_0.2_campaign_scheduling.sql
OK 20170104220731_0.2_result_statuses.sql
OK 20170219122503_0.2.1_email_headers.sql
OK 20170827141312_0.4_utc_dates.sql
OK 20171027213457_0.4.1_maillogs.sql
OK 20171208201932_0.4.1_next_send_date.sql
OK 20180223101813_0.5.1_user_reporting.sql
OK 20180524203752_0.7.0_result_last_modified.sql
OK 20180527213648_0.7.0_store_email_request.sql
OK 20180830215615_0.7.0_send_by_date.sql
OK 20190105192341_0.8.0_rbac.sql
OK 20191104103306_0.9.0_create_webhooks.sql
OK 20200116000000_0.9.0_imap.sql
OK 20200619000000_0.11.0_password_policy.sql
OK 20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK 20200914000000_0.11.0_last_login.sql
OK 20201201000000_0.11.0_account_locked.sql
OK 20220321133237_0.4.1_envelope_sender.sql
time="2025-10-18T21:40:07-03:00" level=info msg="Please login with the username admin and the password 7d13f2e752ea70a8"
time="2025-10-18T21:40:07-03:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2025-10-18T21:40:07-03:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-10-18T21:40:07-03:00" level=info msg="Starting IMAP monitor manager"
time="2025-10-18T21:40:07-03:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-10-18T21:40:07-03:00" level=fatal msg="listen tcp 0.0.0.0:80: bind: address already in use"
```

## 3.2 CRÉATION DU PROFIL EXPÉDITEUR

### Edit Sending Profile

Name:

Support Red Eclipse

Interface Type:

SMTP

SMTP From:

support@redeclipse-tech.com

Host:

smtp.gmail.com:587

Username:

cyse387@gmail.com

Password:

\*\*\*\*\*

Ignore Certificate Errors

# Laboratoire : Hacking éthique et Contre-mesures

## 3.3 CRÉATION DU MODÈLE D'EMAIL

### Edit Template

X

Name:

Red Eclipse

 Import Email

Envelope Sender: 

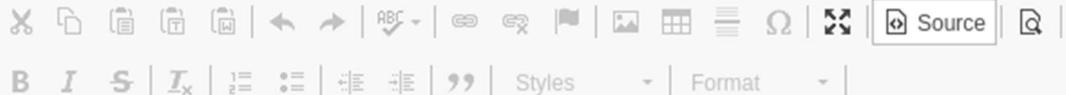
First Last <test@example.com>

Subject:

Action Requise : Vérification de sécurité de votre compte Red Eclipse

**Text**

**HTML**



```
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <style>
        body { font-family: Arial, sans-serif; color: #333; line-height: 1.6; }
        .container { max-width: 600px; margin: 0 auto; padding: 20px; }
        .header { background: #1a73e8; color: white; padding: 20px; text-align:
```

# Laboratoire : Hacking éthique et Contre-mesures

## 3.4 CRÉATION DE LA PAGE DE LANDING PAGE

### Edit Landing Page

Name:

Page de connexion Red Eclipse

**Import Site**

**HTML**

Editor toolbar:

```
<!DOCTYPE html><html><head>
<meta charset="UTF-8"/>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>
<title>Connexion - Red Eclipse Technologies</title>
<style>
    * { margin: 0; padding: 0; box-sizing: border-box; }
    body {
        font-family: 'Segoe UI', Arial, sans-serif;
```

Capture Submitted Data ?

**Cancel** **Save Page**

# Laboratoire : Hacking éthique et Contre-mesures

## 3.5. IMPORTATION DES CIBLES

### Edit Group

Name:

Employés Red Eclipse

[+ Bulk Import Users](#) [Download CSV Template](#)

First Na Last Na Email Position [+ Add](#)

Show  entries Search:

First Name	Last Name	Email	Position	
Ismael	Cyse	cyse387@gm...	Analyste	<a href="#">Delete</a>
John	Smith	john.smith@...	Directeur	<a href="#">Delete</a>
Sophie	Laurent	eibaby01@m...	Assistante	<a href="#">Delete</a>

Showing 1 to 3 of 3 entries

Previous [1](#) Next

[Close](#) [Save changes](#)

# Laboratoire : Hacking éthique et Contre-mesures

## 5. LANCEMENT DE LA CAMPAGNE

### New Campaign

Name:

Email Template:

Landing Page:

URL: [?](http://192.168.100.10)

Launch Date

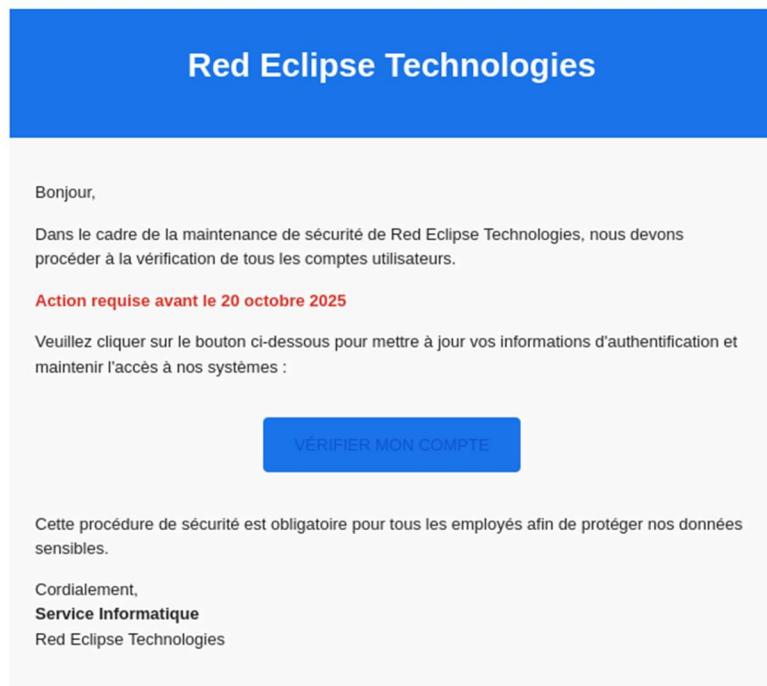
Send Emails By (Optional) [?](#)

Sending Profile:

 [Send Test Email](#)

Groups:

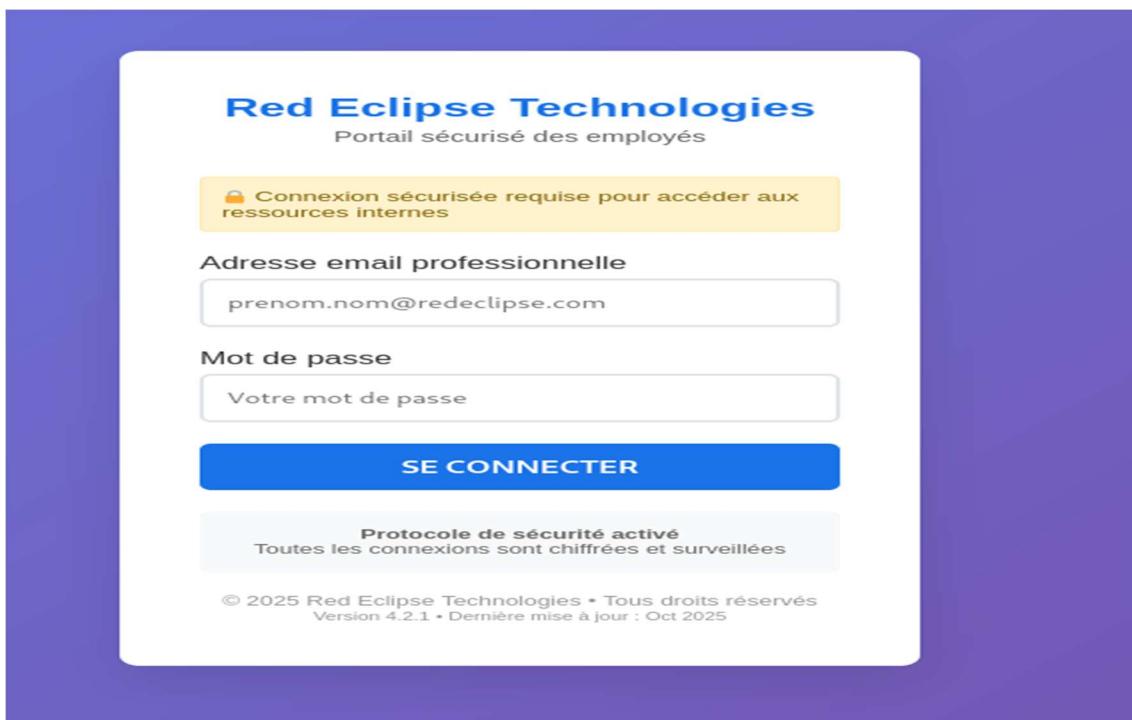
# Laboratoire : Hacking éthique et Contre-mesures



Support technique : [support@redeclipse-tech.com](mailto:support@redeclipse-tech.com)

© 2025 Red Eclipse Technologies. Tous droits réservés.

Cet email a été envoyé à tous les employés de Red Eclipse Technologies.



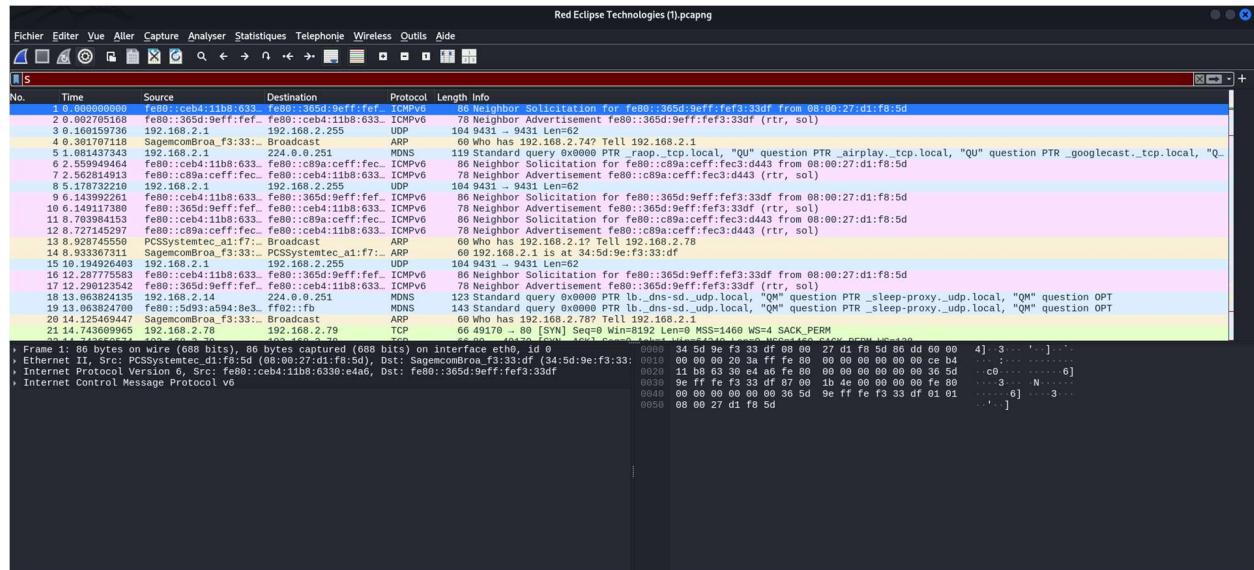
# Laboratoire : Hacking éthique et Contre-mesures

The screenshot shows the gophish application interface. On the left, a sidebar lists various sections: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (with an Admin button), Webhooks (with an Admin button), User Guide, and API Documentation. The main area features a horizontal timeline from 10:35:30 to 10:36:15. Five circular progress indicators represent different events: 'Email Sent' (4), 'Email Opened' (1), 'Clicked Link' (1), 'Submitted Data' (1), and 'Email Reported' (0). Below the timeline is a table titled 'Details' with columns: First Name, Last Name, Email, Position, Status, and Reported. The table contains five entries corresponding to the progress indicators. At the bottom, a search bar and navigation buttons for 'Previous' and 'Next' are visible.

First Name	Last Name	Email	Position	Status	Reported
Ismael	Cyse	cyse387@gmail.com	Analyste	Submitted Data	
John	Smith	john.smith@redeclipse.com	Directeur	Email Sent	
MOI	Baby	ismaelbaby2006@gmail.com	Etudiant	Email Sent	
Sophie	Laurent	eibaby01@monccn.ca	Assistante	Email Sent	

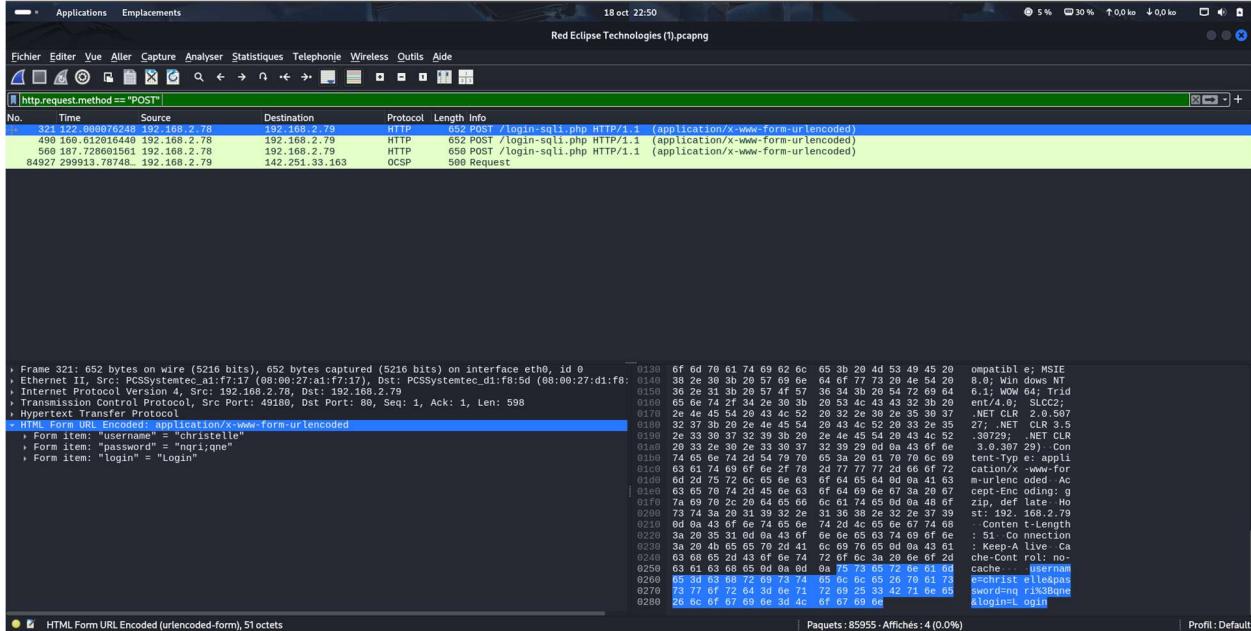
## ÉTAPE 4 : ANALYSE DE CAPTURE RÉSEAU (.pcap) :

### 4.1 : Analysez le fichier .pcap fourni à l'aide de wireshark :



# Laboratoire : Hacking éthique et Contre-mesures

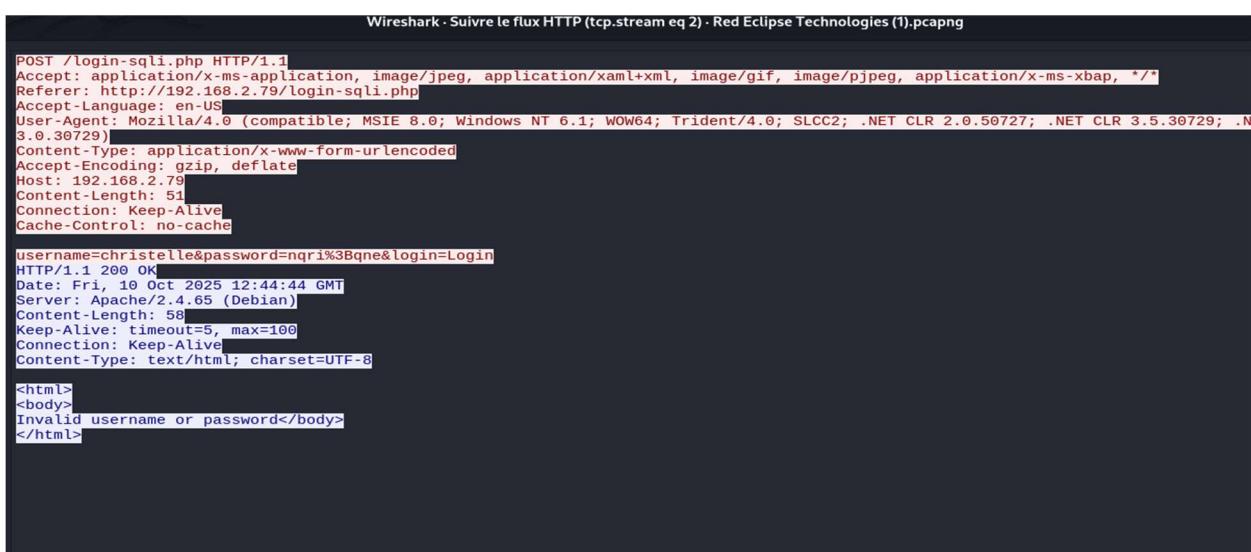
## 4.2 :Identifiez les échanges contenant des identifiants.



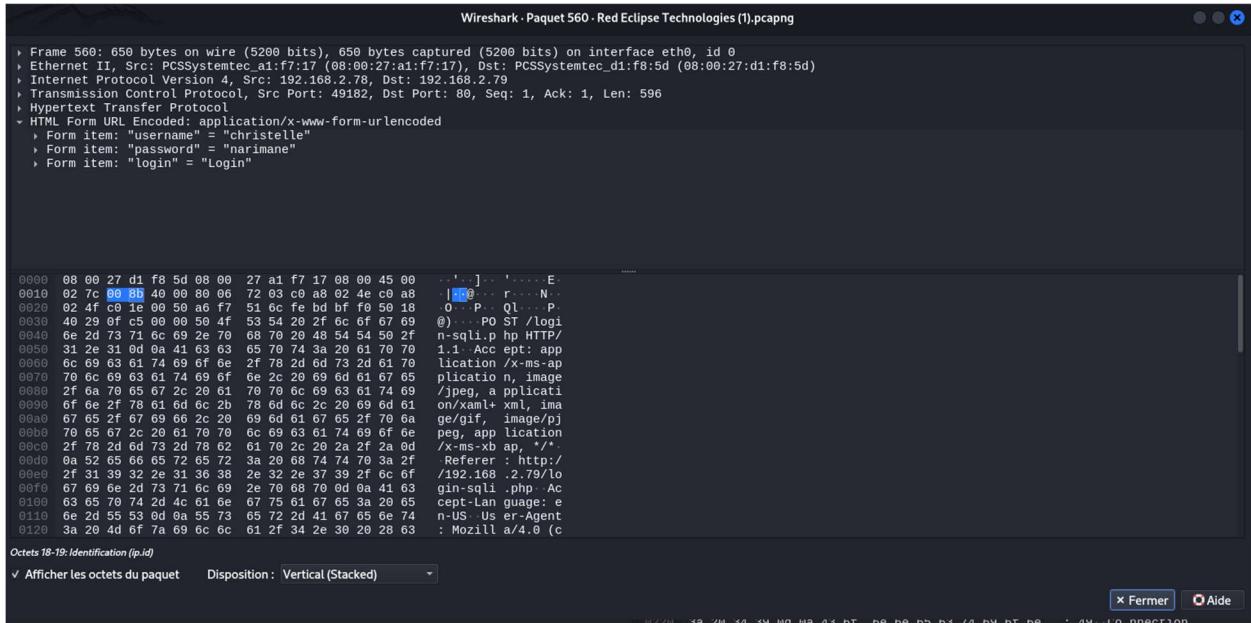
## 4.3 :Récupérez le nom d'utilisateur et le mot de passe présents dans la

Capture : L'analyse du fichier .pcap à l'aide de Wireshark a permis d'identifier plusieurs échanges contenant des identifiants en clair. Deux couples d'utilisateurs/mots de passe ont été trouvés :

- Username : christelle — Password : nqri;qne
- Username : christelle — Password : narimane



# Laboratoire : Hacking éthique et Contre-mesures



## Conclusion

Ce laboratoire m'a permis de mettre en pratique les notions fondamentales du hacking éthique, notamment la reconnaissance réseau, la détection de vulnérabilités, la sensibilisation au phishing et l'analyse de trafic. L'exercice démontre l'importance des mises à jour de sécurité, de la gestion des accès et de la vigilance des utilisateurs face aux attaques. Ces compétences sont essentielles dans tout contexte de cybersécurité professionnelle.