Plugins

Table des matières

[1 Windows 7 2](#_Toc86304926)

[1.1 Définition 2](#_Toc86304927)

[2 Vulnerable Web Pentesting Lab 3](#_Toc86304928)

[2.1 Définition 3](#_Toc86304929)

[3 Vulnerable Credential 4](#_Toc86304930)

[3.1 Définition 4](#_Toc86304931)

[4 5](#_Toc86304932)

# Windows 7

## Définition

Faille : Server Message Block

Exploit : Envoyer des paquets malicieux au server pour propager le malware à tout le réseau ou obtenir un meterpreter sur la machine cible. Sur MSF : exploit/windows/smb/ms17\_010\_eternalblue

# Vulnerable Web Pentesting Lab

## Définition

Cette machine comprend plusieurs environnement web vulnérable pour s’entrainer au pentest web.

Liste des environnements :

* DVWA
* WebGOAT
* JuiceSHOP
* Badstore
* Wordpress

# Vulnerable Credentials

## Définition

Faille : Mots de passe et user faible (Disponible dans Rockyou)

Exploit : Bruteforce SSH (Hydra, python script, Metasploit…).

# Networking lab environnement

## Définition

2 VM communicante : L’objectif est de réaliser un attaque type Man in The Middle.

Exploit : ARPSpoofing, weak encryption…