PLAN

INTRODUCTION

* Pourquoi la securite informatique
* Jargon
* Veille securite informatique
* Rappels TCP/IP

PREPARATION DU LAB

* NIse en place du lab

PRISE D’INFORMATIONS

* Informations publiques
* Enumeration dess machines
* Scan de ports et prise d’empreinte des services
* Prise d’empreinte des systemes

VULNERABILITES POSTES CLIENTS

* Intrusion a distance
* Intrusion Metasploit
* Vulnerabilite sur les navigateurs web
* Backdoor
* Vulnerabilites web
* Introduction
* Cartographie du site
* Les failles PHP
* Les injections SQL
* Les failles XSS
* Cross-site Request Forgery(CSRF)

VULNERABILITES RESEAUX

* Introduction
* Idle Host Scanning
* Denis de service
* Sniffing reseau
* Spoofing reseau
* Man In The Midle

VULNERABILITES APPLICATIVES

* Introduction
* Les buffers overflows
* Integer overflow
* Format String
* Introduction aux shellcodes
* Securisation
* CONTREMESURE
* Contremesure generales

LIENS UTILES

OBJECTIFS

* Tester la securite de votre reseau / application
* Comprendre et detecter les attaques sur un SI(Comprendre les scenarios d’attaque et mettre la casquette du hacker pour tester la securite du systeme)
* Deceler et mesurer la portee d’une vulnerabilite
* Corriger les vulnerabilites
* Securiser un reseau / application
* Appliquer les mesures pour lutter contre le hacking
* Comprendre le fonctionnement et le scenarion des attaques

INTRODUCTION

* Pourquoi la securite informatique
* Jargon
* Veille securite informatique
* Rappels TCP/IP

1. Pourquoi la securite informatique:

Les SI font desormais partie integrante du fonctionnement de tout organisme(Entreprise, adminitration...).

Les services assures par le SI sont de plus en plus critiques

1. L’environnement concurentiel:

Les informations detenues sont de plus en plus sensibles.

Il faut assurer leur disponibilite, leur integrite et leur confidentialite.

1. Les menaces qui pesent sur l’entreprise se multiplient:

Les risques de disfonctionnement de processuces critiques augmentent.

La maitrise et la prevention des risques sont indispensables.

1. Les obligations reglementaires et legales se generalisent:

Les responsabilites juridiques se precisent.

PREPARATION DU LAB

* NIse en place du lab

PRISE D’INFORMATIONS

* Informations publiques
* Enumeration dess machines
* Scan de ports et prise d’empreinte des services
* Prise d’empreinte des systemes

VULNERABILITES POSTES CLIENTS

* Intrusion a distance
* Intrusion Metasploit
* Vulnerabilite sur les navigateurs web
* Backdoor
* Vulnerabilites web
* Introduction
* Cartographie du site
* Les failles PHP
* Les injections SQL
* Les failles XSS
* Cross-site Request Forgery(CSRF)

VULNERABILITES RESEAUX

* Introduction
* Idle Host Scanning
* Denis de service
* Sniffing reseau
* Spoofing reseau
* Man In The Midle

VULNERABILITES APPLICATIVES

* Introduction
* Les buffers overflows
* Integer overflow
* Format String
* Introduction aux shellcodes
* Securisation
* CONTREMESURE
* Contremesure generales

LIENS UTILIES

* <https://packetstormsecurity.com>
* <http://securityfocus.com>
* <https://securitytube.net>
* <https://hackerzvoice.net>
* <https://www.xmco.fr>
* [www.zataz.com](http://www.zataz.com)
* <https://www.owasp.org>