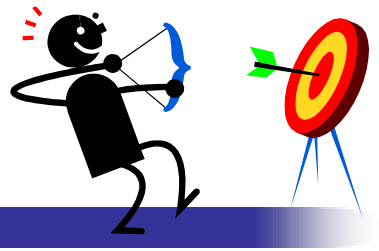

applications
vulnerabilities
web
application
attacks
security
internet
cyber
may
within
new
crimes
vulnerability
motivations
etc
developers
illegal
research
number
increasing
Cross-Site
information
computer
using
able
offline
attackers
access
including
high

NIKTO

Plan



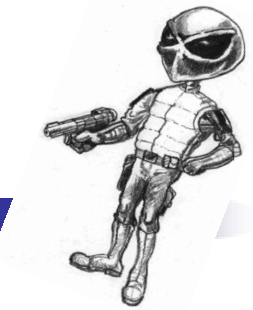
- Introduction
- Nikto
  - Présentation
  - Arboressence
  - Objectifs
  - Liste d’options
  - Les fichiers de configuration
- Démonstration
- Conclusion

Introduction

- Les outils de balayage deviennent des parties importantes dans les fonctions de tests utilisés pour trouver les erreurs dans le cycle de vie des logiciels, cependant, il y a deux approches de tests.

- La première consiste à utiliser les outils de balayages manuels qui consistent à parcourir le code source par un agent afin de détecter les vulnérabilités du site web en question, alors que la deuxième se base sur l'utilisation des outils de balayage automatisés pour détecter les vulnérabilités des serveurs utilisés.

Nikto



Présentation

- Scanner web open source,
- Permet d'auditer les serveurs web et de détecter les vulnérabilités contenues dans ces derniers.
- Effectue des vérifications pour

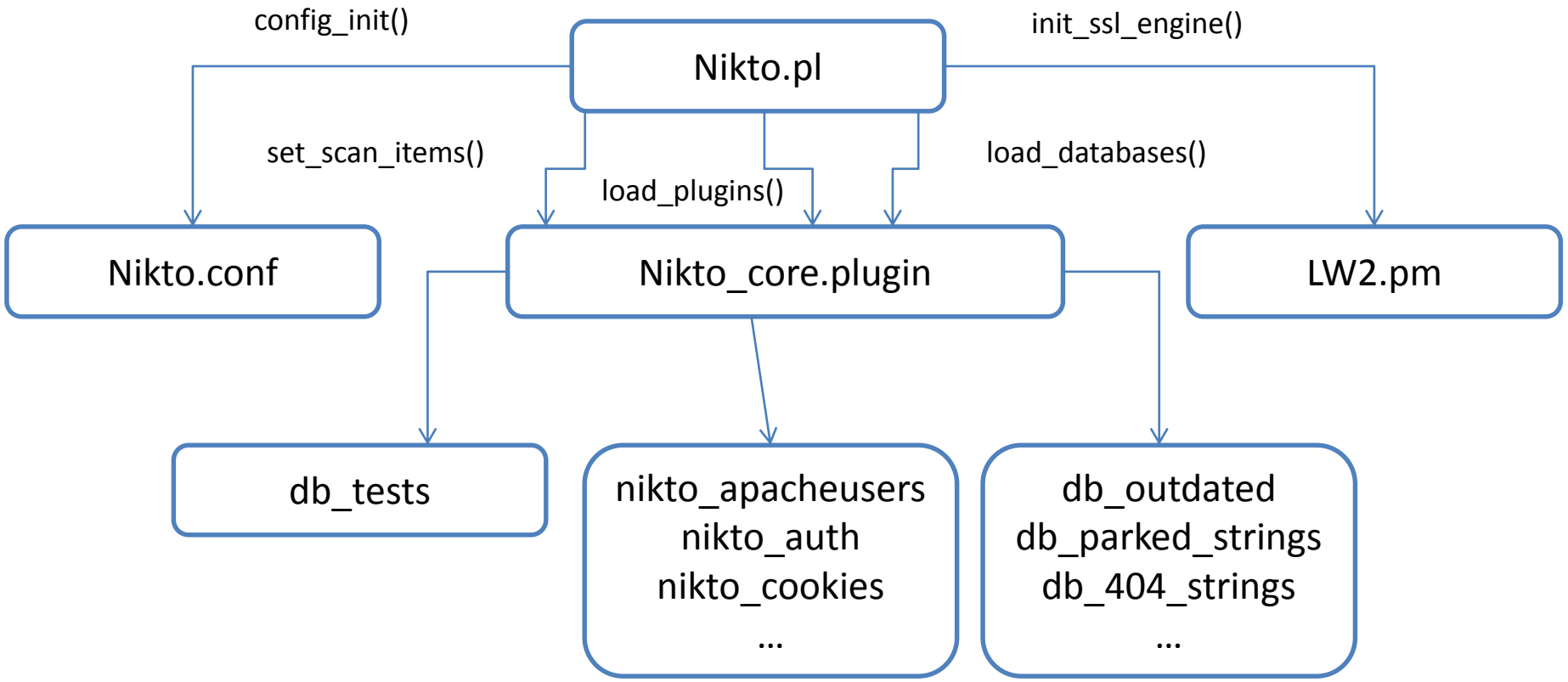
    6400 fichiers et scripts potentiellement dangereux,

    1200 versions de serveurs obsolètes,

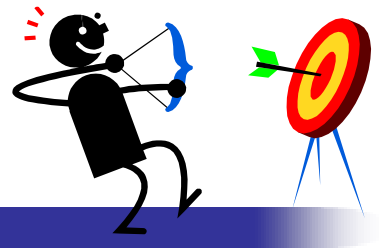
    et près de 300 problèmes spécifiques à la version sur des serveurs
- Nikto envoie des requêtes à la machine cible afin d'exploiter ses vulnérabilités,

Nikto

Arborescence



Nikto



Objectif

Nikto est conçu pour détecter :

- Les mauvaises configurations (serveurs comme logiciels)
  - Directory Traversal
  - Remote file inclusion
  - etc…
- Les fichiers et les programmes installés par défaut
- Les fichiers et les programmes mal sécurisés
- Les versions obsolètes

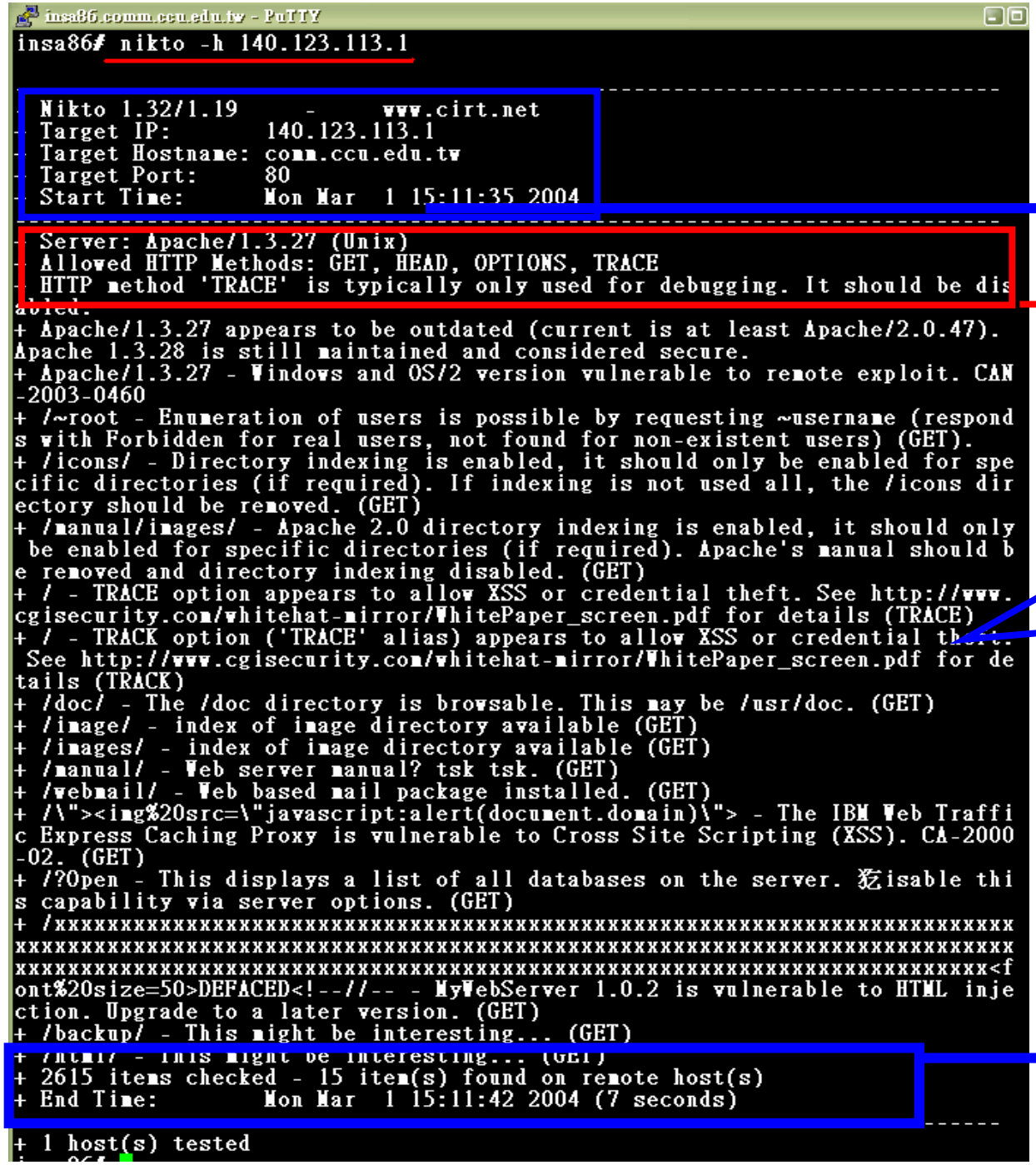
```
root@kali:~# nikto -help
Unknown option: help

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:p
ass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /direct
ory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
```

Pour indiquer la machine cible

Pour spécifier un port par défaut le port 80

Pour contrôler le scan contre une cible



Information de base sur la machine cible

Information sur le serveur

Signaler certaines vulnérabilités et proposer des solutions

Rapport final

Les fichiers de configuration

- nikto.pl effectue une initialisation de l'environnement, puis passe la main à plugins/nikto_core.plugin. C'est donc nikto_core.plugin qui s'occupe d'attaquer la cible, puis chacun des plug-ins déroulera son code afin d'analyser les informations qui lui sont demandées.
- Nikto s'appuie sur un ensemble de plug-ins, chacun dédié à un point de vulnérabilité potentielle précis. Ces plug-ins sont écrits en Perl.

```
root@kali:/usr/share/nikto# nikto -list-plugins
Plugin: apacheusers
 Apache Users - Checks whether we can enumerate usernames directly from the we
server
 Written by Javier Fernandez-Sanguinoi Pena, Copyright (C) 2008 CIRT Inc.
 Options:
  cgiwrap: User cgi-bin/cgiwrap to enumerate
  dictionary: Filename for a dictionary file of users
  enumerate: Flag to indicate whether to attempt to enumerate users
  home: Look for ~user to enumerate
  size: Maximum size of username if bruteforcing

Plugin: apache_expect_xss
 Apache Expect XSS - Checks whether the web servers has a cross-site scripting
ulnerability through the Expect: HTTP header
 Written by Sullo, Copyright (C) 2008 CIRT Inc.

Plugin: outdated
 Outdated - Checks to see whether the web server is the latest version.
 Written by Sullo, Copyright (C) 2008 CIRT Inc.
```

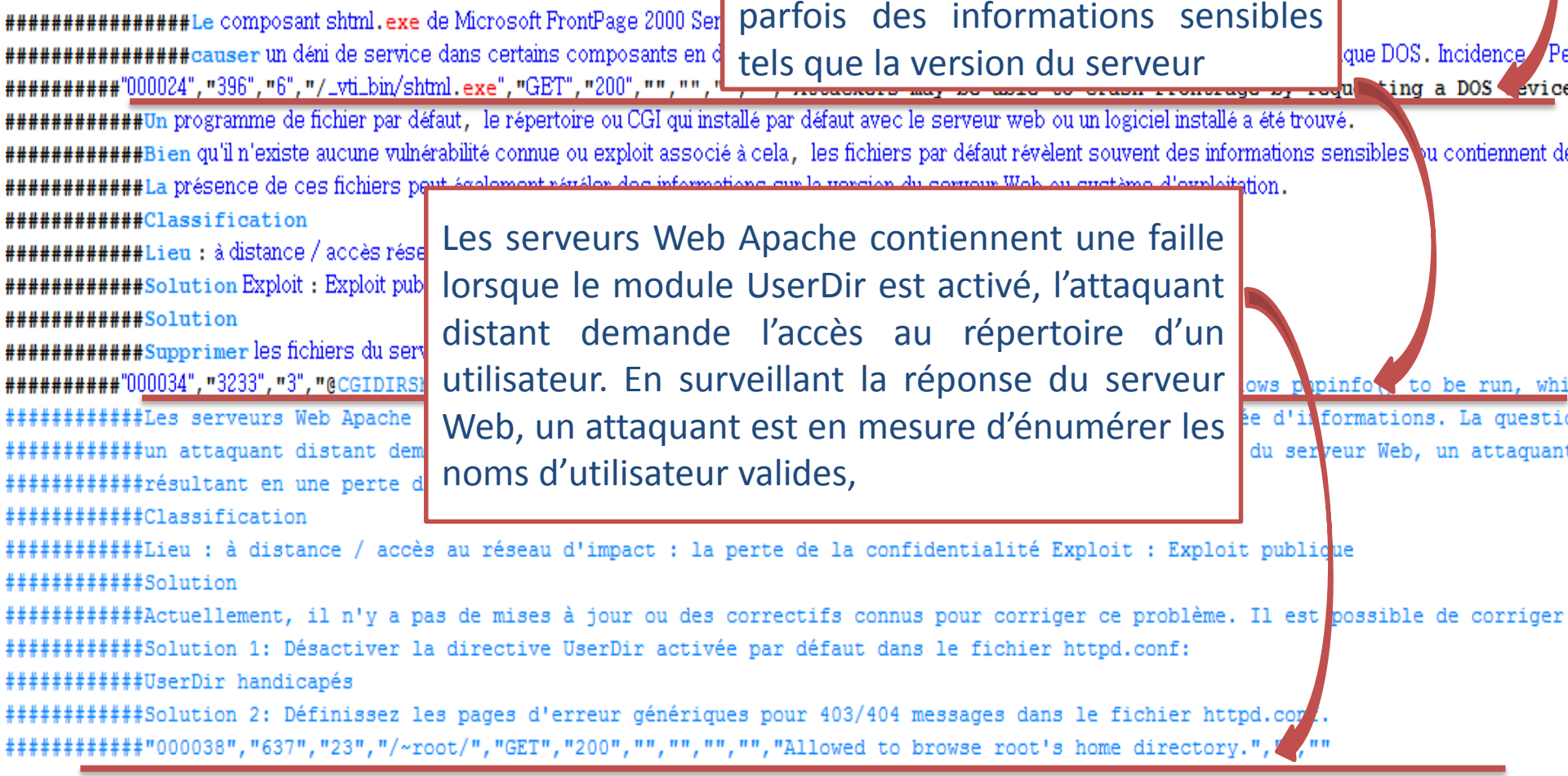
Les fichiers de configuration

Un composant de type shtml.exe permet à un attaquant de causer un DOS

- Les fichiers databases constituent la base de connaissance de l'outil Nikto, elle lui permet de vérifier les informations sur les requetés

Les fichiers par défauts révèlent parfois des informations sensibles tels que la version du serveur

Les serveurs Web Apache contiennent une faille lorsque le module UserDir est activé, l'attaquant distant demande l'accès au répertoire d'un utilisateur. En surveillant la réponse du serveur Web, un attaquant est en mesure d'énumérer les noms d'utilisateur valides,



Conclusion

- **Nikto** est un programme très pratique pour scanner les failles de sécurité de son serveur web

- Il est très important que vous analysiez votre propre site afin que vous puissiez voir ce que les attaquants peuvent voir afin d'éviter tout risque de menace,