

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



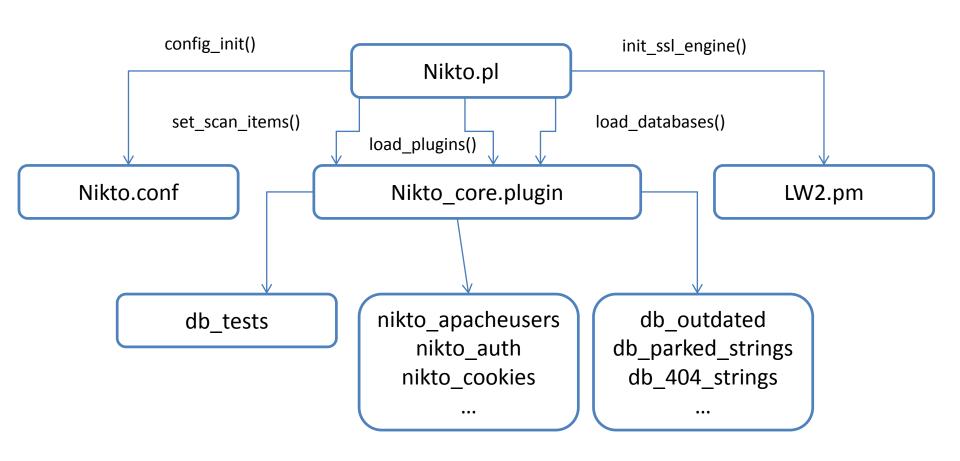
Présentation

- 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			
-D -d -F -H	onfig+ isplay+ bcheck ormat+ elp ost+	Use this config file Turn on/off display outputs check database and other key files for syntax errors save file (-o) format Extended help information target host	Pour indiquer la machine cible
_	a+	Host authentication to use, format is id.pass or id.p	
ass:realm			
-1	ist-plugins	List all available plugins	
-0	utput+	Write output to this file	
-n	ossl	Disables using SSL	
-n	0404	Disables 404 checks	
-b.	lugins+	List of plugins to run (default: ALL)	
-p	ort+	Port/to use (default 80) \//	
-r	oot+	Prepend root value to all requests, format is /direct	Pour spécifier un port par
ory			défaut le port 80
	el	Force essimode cone port ou are able to hear	delade le port oo
-T	uning+	Scan tuning	Davis contrâles la companyation
	imeout+	Timeout for requests (default 10 seconds)	Pour contrôler le scan contre une cible
	pdate	Update databases and plugins from CIRT.net	une cibie
	ersion	Print plugin and database versions	
V	OLOTOL	Traine pragati and database versions	

```
🦰 insa86.comm.ccu.edu.tw - PuTTY
insa86# nikto -h 140.123.113.1
                           www.cirt.net
  Nikto 1.32/1.19
                   140.123.113.1
  Target IP:
 Target Hostname: comm.ccu.edu.tw
                                                                              cible
  Target Port:
                   80
                  Mon Mar 1 15:11:35 2004
  Start Time:
  Server: Apache/1.3.27 (Unix)
  Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
  HTTP method 'TRACE' is typically only used for debugging. It should be dis
 Apache/1.3.27 appears to be outdated (current is at least Apache/2.0.47).
Apache 1.3.28 is still maintained and considered secure.
- Apache/1.3.27 - Windows and OS/2 version vulnerable to remote exploit. CAN
 2003-0460
 /~root - Enumeration of users is possible by requesting ~username (respond
s with Forbidden for real users, not found for non-existent users) (GET).
+ /icons/ - Directory indexing is enabled, it should only be enabled for spe
cific directories (if required). If indexing is not used all, the /icons dir
ectory should be removed. (GET)
+ /manual/images/ – Apache 2.0 directory indexing is enabled, it should only
 be enabled for specific directories (if required). Apache's manual should b
e removed and directory indexing disabled. (GET)
 / - TRACE option appears to allow XSS or credential theft. See http://www.
cgisecurity.com/whitehat-mirror/WhitePaper screem.pdf for details (TRACE)
+ / - TRACK option ('TRACE' alias) appears to allow XSS or credential that...
See http://www.cgisecurity.com/whitehat-mirror/WhitePaper screen.pdf for de
tails (TRACK)
 /doc/ - The /doc directory is browsable. This may be /usr/doc. (GET)
 /image/ - index of image directory available (GET)
 /images/ - index of image directory available (GET)
  /manual/ - Web server manual? tsk tsk. (GET)
 /webmail/ - Web based mail package installed. (GET)
 //"><img%20src=\"javascript:alert(document.domain)\"> - The IBM Web Traffi
 Express Caching Proxy is vulnerable to Cross Site Scripting (XSS). CA-2000
 02. (GET)
 /?Open - This displays a list of all databases on the server. 犵isable thi
 capability via server options. (GET)
  ont%20size=50>DEFACED<!--//-- - MyWebServer 1.0.2 is vulnerable to HTML inje
ction. Upgrade to a later version. (GET)
+ /backup/ – This might be interesting... (GET)
 /RUMI/ - INIS MIGHT DE INTERESTING... (GEI)
 2615 items checked - 15 item(s) found on remote host(s)
                  Mon Mar 1 15:11:42 2004 (7 seconds)
  End Time:
  1 host(s) tested
```

Information de base sur la machine

Information sur le serveur

Signaler certaines vulnérabilités et proposer des solutions

Rapport final

Les fichiers de configuration



- nikto.pl effectue une initialisation de Plugin: apacheusers 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.

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

##########Le composant shtml.exe de Microsoft FrontPage 2000 Ser parfois des informations sensibles

#########"000024","396","6","/_vti_bin/shtml.exe","GET","200","","","

vérifier les informations sur les requetés Les fichiers par défauts révèlent ##############causer un déni de service dans certains composants en d tels que la version du serveur

aue DOS. Incidence Pe ting a DOS evice

##########Un programme de fichier par défaut, le répertoire ou CGI qui installé par défaut avec le serveur web ou un logiciel installé a été trouvé.

########Bien qu'il n'existe aucune vulnérabilité connue ou exploit associé à cela, les fichiers par défaut révèlent souvent des informations sensibles ou contiennent d #########La présence de ces fichiers pout égoloment révélor des informations sur la version du sorgent Web, ou sustème d'exploitation.

###########Classification ############Lieu: à distance / accès rése ############Solution Exploit: Exploit pub #########Solution ###########Supprimer les fichiers du serv ##########"000034", "3233", "3", "@CGIDIRS1 ###########Les serveurs Web Apache

############ dem

############résultant en une perte o

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,

to be run, whi e d'informations. La questi du serveur Web, un attaquan

```
###########Classification
##########Lieu : à distance / accès au réseau d'impact : la perte de la confidentialité Exploit : Exploit publique
##########Solution
###########Actuellement, il n'y a pas de mises à jour ou des correctifs connus pour corriger ce problème. Il est possible de corriger
#########Solution 1: Désactiver la directive UserDir activée par défaut dans le fichier httpd.conf:
###########UserDir handicapés
```

##########Solution 2: Définissez les pages d'erreur génériques pour 403/404 messages dans le fichier httpd.co. ##########"000038","637","23","/~root/","GET","200","","","","","Allowed to browse root's home directory.",

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,