

Informatikai biztonság alapjai

Oláh Norbert

2023.

Tartalom

1 Nessus – Fejlett szkennelés

Készíts el a fejlett szkenned

Hozz létre egy tetszőleges fejlett szkennert az alábbi célponton:

- 172.22.204.195

Laborfeladat

- Látogasson el a DVWA oldalára
<http://172.22.204.188/login.php>
Username: admin
PW: password

Készíts el a Fejlett szkenned 2.

Hozz létre egy Fejlett szkennert az alábbi beállításokkal:

- Név: DVWA, Targets: 172.22.204.188
- Állíts be Credentials fülön a Plaintext Authentication / Automatic authentication-on a login adatokat.

Készíts el az advanced szkenned

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings Credentials Plugins

BASIC ▾

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name:

Description:

Folder:

Targets:

Upload Targets [Add File](#)

Save ▾

Cancel

Készíts el az advanced szkenned

- BASIC >
- DISCOVERY >
- ASSESSMENT ▾
 - General
 - Brute Force
 - **Web Applications**
 - Windows
 - Malware
 - Databases
- REPORT >
- ADVANCED >

Web Application Settings

Scan web applications

General Settings

Use a custom User-Agent

Web Crawler

Start crawling from

Excluded pages (regex)

Maximum pages to crawl

Maximum depth to crawl

Follow dynamically generated pages

Készíts el az advanced szkenned

The screenshot displays the Nessus Settings page with the 'Settings' tab selected. The left sidebar contains a navigation menu with categories: BASIC, DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. Under ASSESSMENT, the 'Databases' sub-category is expanded, showing options for General, Brute Force, Web Applications, Windows, and Malware. The main content area is titled 'Oracle Database' and features a checked checkbox for 'Use detected SIDs'. Below this checkbox, a note states: 'If host and database credentials are specified, Nessus will attempt to authenticate to the database with SIDs detected locally.'

Settings Credentials Plugins

BASIC >

DISCOVERY >

ASSESSMENT ▾

General

Brute Force

Web Applications

Windows

Malware

▫ Databases

REPORT >

ADVANCED >

Oracle Database

Use detected SIDs

If host and database credentials are specified, Nessus will attempt to authenticate to the database with SIDs detected locally.

Készíts el az advanced szkenned

BASIC >

DISCOVERY >

ASSESSMENT ▾

General

■ Brute Force

Web Applications

Windows

Malware

Databases

REPORT >

ADVANCED >

General Settings

 Only use credentials provided by the user

Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.

Oracle Database

 Test default accounts (slow)

Hydra

 Always enable Hydra (slow)

Nessus uses Hydra to attempt brute force attacks when either this setting or the "Perform thorough tests" setting in the "Assessment / General" section is enabled.

Logins file

[Add File](#)

Passwords file

[Add File](#)

Készíts el az advanced szkenned

New Scan / Web Application Tests

[← Back to Scan Templates](#)

Settings **Credentials** Plugins

CATEGORIES Plaintext Authentication

Filter Credentials

HTTP

Authentication method: Automatic authentication

Username: admin

Password:

Global Credential Settings

Login method: POST

Re-authenticate delay (seconds): 0
The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.

Follow 30x redirections (# of levels): 0

Invert authenticated regex:

Use authenticated regex on HTTP headers:

Készíts el a webalkalmazás szkenned

Hozz létre egy Web alkalmazás szkennert az alábbi beállításokkal:

- Név: DVWA, Targets: 172.22.204.188
- Állíts be Credentials fülön a Plaintext Authentication / Automatic authentication-on a login adatokat.

Készíts el az webalkalmazás szkenned

New Scan / Web Application Tests

[← Back to Scan Templates](#)

Settings **Credentials** Plugins

CATEGORIES Plaintext Authentication

Filter Credentials

HTTP

Authentication method: Automatic authentication

Username: admin

Password:

Global Credential Settings

Login method: POST

Re-authenticate delay (seconds): 0
The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.

Follow 30x redirections (# of levels): 0

Invert authenticated regex:

Use authenticated regex on HTTP headers:

Készíts el a webalkalmazás szkenned 2


Hozz létre egy Web alkalmazás szkennert az alábbi beállításokkal:

- Név: OWASP, Targets: 172.22.204.195
- Válassz az oldalon OLD (VULNERABLE) VERSIONS OF REAL APPLICATIONS-ből egy tetszőleges alkalmazást és az Assessment fülön futasd először custom majd az ip címre a complex scan típust.

Készíts el az webalkalmazás szkenned

New Scan / Web Application Tests

[← Back to Scan Templates](#)

Settings | Credentials | Plugins 

BASIC >
DISCOVERY >
ASSESSMENT v
REPORT >
ADVANCED >

Scan Type: Scan for all web vulnerabilities (quick) v

General Settings:
Avoid potential false alarms
Enable CGI scanning

Web Applications:
Start crawling from "/"
Crawl 1000 pages (max)
Traverse 6 directories (max)
Test for known vulnerabilities in commonly used web applications
Perform each generic web app test for 5 minutes (max)

Save v | Cancel

Zárthelyi tesztfeladat

Mutassa be hogyan vizsgálná meg a www.hackthissite.org weboldalt. A feladatot Basic szkenneléssel hajtsa végre. A scan neve legyen a saját neve és válaszolja meg az alábbi kérdéseket

- Célpont IP címe
- Célpont portjai
- Válasszon egy tetszőleges sérülékenységet és szedjen össze minél több információt róla. (Térjen ki a probléma leírására, lehetséges megoldására, sérülékenységgel kapcsolatos további forrásokra). Ha nincs sérülékenység válasz egy infó típusú sérülékenységet és részletezd az adott pontot.

A szkennelés eredményéről generáljon pdf-t, amely tartalmazza az összes hibát és kapcsolódó információt. A kérdésekre a választ egy másik dokumentumba készítse el.

Thank you for your attention!