Hardening IIS

Łukasz Tomaszkiewicz
luktom@vsecure.pl
+48 604 132 518

OWASP
22 maja 2012

The OWASP Foundation
http://www.owasp.org

Aktualność systemu i jego konfiguracja

- Demo – Baseline Security Analyzer
- BSA do pobrania z:
  http://www.microsoft.com/en-us/download/details.aspx?id=7558
- Demo – Web Application Configuration Analyzer
- WACA do pobrania z:
  http://www.microsoft.com/en-us/download/details.aspx?id=573

Komponenty IIS

- Mniej komponentów = mniej miejsc w których mogą wystąpić podatności
- Dawniej: IIS Lockdown
- Obecnie: Server Manager
- Demo

Bezpieczeństwo adresów

- Moduł Request Filtering
- Demo

URLScan

- Podstawowa funkcjonalność: blokowanie nieprawidłowych URLi
- Nie zastąpi WAFa!
- Moduł Request Filtering przejął dużo funkcji od URLScan-a, ale nie wszystkie – np. ukrywanie informacji o serwerze
- Do pobrania z: http://www.microsoft.com/en-us/download/details.aspx?id=5728

Limitowanie ilości połączeń

- Moduł Dynamic IP Restrictions
- Demo

Application Pools

- Dobre praktyki
  - Pula per witryna
  - Używanie Application Pool Identity
- Application Pool Identity a uprawnienia systemu plików
- Application Pool Identity a połączenia do SQL Servera

Bezpieczeństwo systemu plików

- Dobre praktyki
  - Osobna partycja
  - Oczywiście NTFS
  - Restrykcyjne uprawnienia do plików
  - Używanie Application Pool Identity

Mocne szyfrowanie SSL/TLS

- „Magiczne” klucze:
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]
  "Enabled"=dword:00000000
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]
  "Enabled"=dword:00000000
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128]
  "Enabled"=dword:00000000
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128]
  "Enabled"=dword:00000000
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]
  "Enabled"=dword:00000000
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]
  "Enabled"=dword:00000000
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128]
  "Enabled"=dword:00000000
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server]
  "Enabled"=dword:00000000
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]
  "Enabled"=dword:00000000
- Weryfikacja używanego szyfrowania

Certyfikaty

- Problemy z self-signed certyfikatami
- Własne CA – problem?
- Demo programu XCA

Q&A

Łukasz Tomaszkiewicz
luktom@vsecure.pl