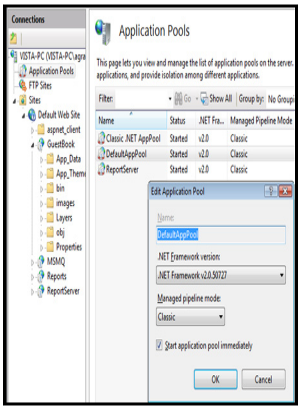
# How to cheat at IIS 7 server administration

## Syngress - Windows & Active Directory Exploitation Cheat Sheet and Command Reference :: Cas van Cooten — I ramble about security stuff, mostly



Application Pools

This page lets you view and manage the list of application pools on the server. applications, and provide isolation among different applications.

| Name | Status | .NET Fra... | Managed Pipeline Mode |
|---|---|---|---|
| Classic .NET AppPool | Started | v2.0 | Classic |
| DefaultAppPool | Started | v2.0 | Classic |
| ReportServer | Started | v2.0 | Classic |

Edit Application Pool

Name: DefaultAppPool

.NET Framework version: .NET Framework v2.0.50727

Managed pipeline mode: Classic

☑ Start application pool immediately

Filesize: 40.59 MB

Description: -

-

Hongkong -- Economic policy.
Hongkong -- Economic conditions.
Income -- Hongkong.
Christian sociology -- Catholic Church
Spanish language -- Dialects -- Bogotá
Spanish language -- Pronunciation
City planning -- Scotland -- Fife -- Maps
Pharynx.
Tongue.
Geography -- Study and teaching.
Web servers.
Microsoft Internet information server.How to cheat at IIS 7 server administration
-How to cheat at IIS 7 server administration
Notes: Includes index.
This edition was published in 2007

Tags: #Enabling #SSL #on #Windows #Server #Update #Services #(WSUS)

**DDoS monitoring: how to know you're under attack**

Another upside to these services is that if the service which the account is running becomes compromised the attacker would not have access outside of that service, unless that service account has been granted specific rights.

**Local System Account**

The Dependencies Tab The Dependencies tab displays the services that are required for the task scheduler service to run.

**Local System Account**

ProxyChains to tunnel over the target system. You are welcome for that mental image. This is because in my haste to get the SQL Server services installed on my machine I had set up the services to start up under the local service account instead of under a single domain account like my SQL Server did.

**DDoS monitoring: how to know you're under attack**

If you suspect that a particular service is stopping the system from starting properly, you may change the startup type of that service from automatic to manual. If you find that the task scheduler service has failed and you are not able to restart it, you should check the RPC service. Changing the Startup Type of a Service Troubleshooting system problems sometimes requires administrators to enable or disable a service or change its startup behavior.

**DDoS monitoring: how to know you're under attack**

Microsoft Search Service Microsoft Search Service is an external service to SQL Server that must be installed in order to perform full-text searches.

**Local System Account**

The attacker uses a centralized system that then tells these malware-infected machines to send traffic to the site. Many indexes can be in one catalog, but they must all be from the same database, because a catalog cannot span databases.

**Windows & Active Directory Exploitation Cheat Sheet and Command Reference :: Cas van Cooten — I ramble about security stuff, mostly**

With enough traffic, an attacker can eat away at your bandwidth and server resources until one or both are so inundated that they can no longer function. From a security perspective this is a pretty bad idea. You must import the certificate to all computers that will communicate with the WSUS server.

**DDoS monitoring: how to know you're under attack**

LocalAdmin -Eq True } Look for kerberoastable users Get-DomainUser -SPN select name,serviceprincipalname Look for AS-REP roastable users Get-DomainUser -PreauthNotRequired select name Look for users on which we can set UserAccountControl flags If available - disable preauth or add SPN see below Find-InterestingDomainAcl -ResolveGUIDs? Request a TGT as the target user and pass it into the current session NOTE: Make sure to clear tickets in the current session with 'klist purge' to ensure you don't have multiple active TGTs. Microsoft Search Service then executes the query and passes back the results to the query engine. The Microsoft Search Service maintains a series of files that comprise the full-text indexes in full-text catalogs.

## Related Books

- Libro de la Historia y Milagros hechos a inuocacion de nuestra Señora de Montserrat.
- The robbers
- Religion, culture, and society - a reader in the sociology of religion
- In Chancery
- Oh dear, said Tiger