SERVER CHECKLIST ADDITION 2016 –

Constructed by Michael Bailey (patriotdown, GMU STEM Outreach, past President)

Please attribute previous owners upon modification, but feel free to attribute yourself if you sincerely made significant modifications.

Attempt this checklist in addition to the client checklist, and also web app checklist ***if said server is a web server with a backend (i.e. not just IIS, Apache, Nginx, but additionally PHP, ASP.NET, etc).***

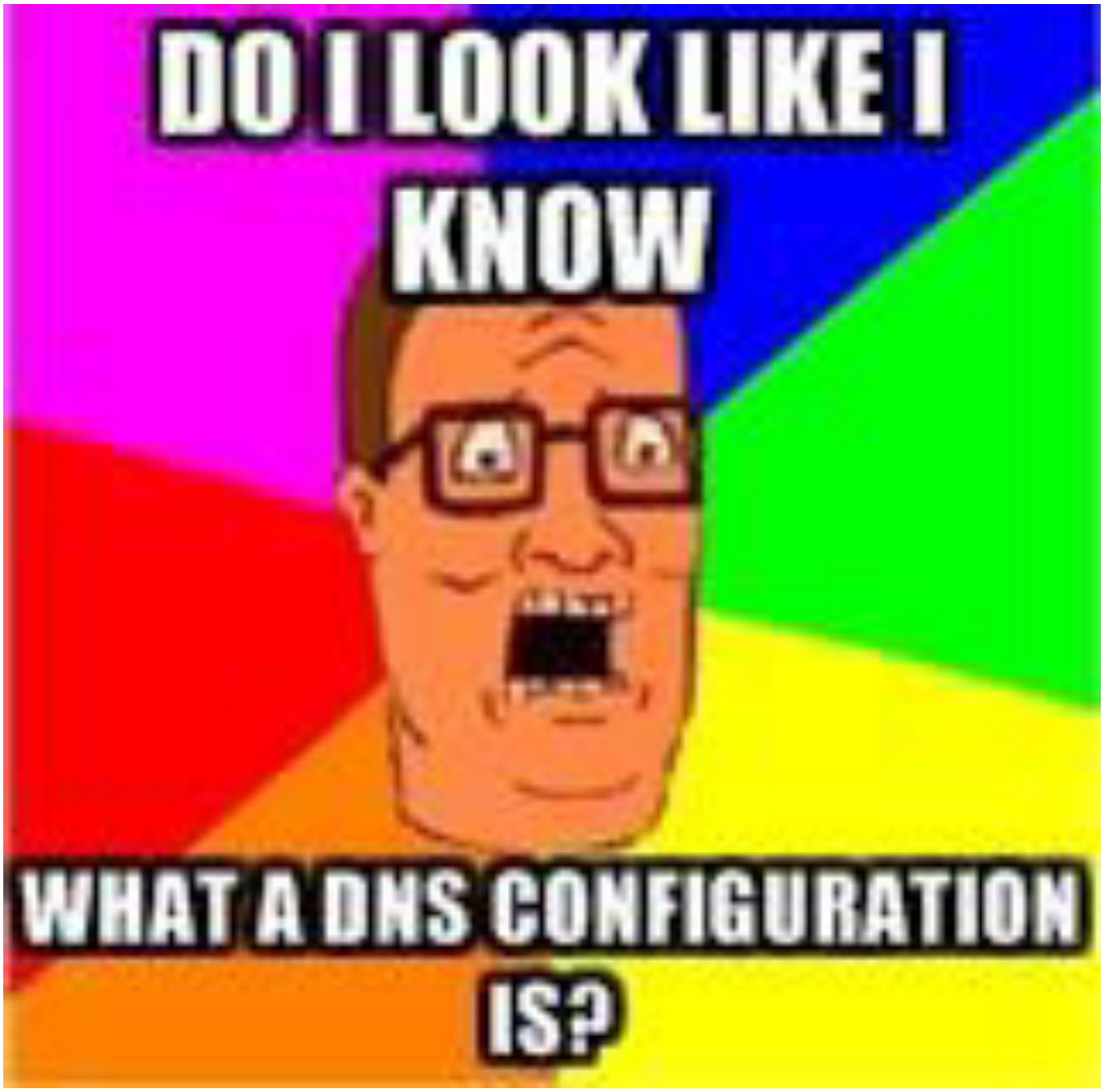


Table of Contents:

1) Opening

Please note since some Server Managers differ heavily based on user interface (i.e. 2012 looks drastically different compared to 2008), command lines will be provided as well and will be based on the Microsoft (probably TechNet) documentation. If you can't find the setting, use the command line. If you jump straight to the command line and it silently fails you may accidentally think it succeeded. **This is a reason you should run through this checklist before the round and try it out. The interface is assumed 2008R2 unless otherwise stated.**

2) IE ESC

In virtually all situations, IE ESC (Internet Explorer Enhanced Security Configuration) should be enabled. Note this basically makes it "blacklist sources by default", which makes browsing insanely difficult, so consider doing this after any internet-based activities or use your host to browse and move files over after downloading.

To change IE ESC in GUI:

Open **Server Manager**

Click "**Configure IE ESC**" (on the right side, towards the bottom under Security Information)

Set both Users and Administrators option to **On**

To change in command line:

```
REG ADD "HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A7-37EF-4b3f-8CFC-4F3A74704073}" /v IsInstalled /t REG_DWORD /d 00000001 /f
REG ADD "HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A8-37EF-4b3f-8CFC-4F3A74704073}" /v IsInstalled /t REG_DWORD /d 00000001 /f
```

Note: inconsistencies reported in 2012

3) Rogue Roles

Pay close attention to what roles are required per the readme and what roles are not. This will almost certainly be a point.

Get roles and remove roles by going to:

Open **Server Manager**

4) BPA

Microsoft Best Practices Analyzer is a not-well-known scanner on server similar to MBSA used on clients.

It sorts settings in “Compliant”, which means it’s good, “Noncompliant”, which means it may be due for a change, and “Warning” which means it’s compliant but may become noncompliant given certain conditions and time.

To access in GUI:

Open **Server Manager**

Open **Roles** and select role to analyze

Open **Summary** and open **Best Practices Analyzer**

Please note how there is a “Compliant” tab, and if it’s propagated (got stuff in it), it means a scan did take place and you aren’t firing blanks.

Command line interface seems to not reasonably be available for this.

Understand what settings mean before you see “Noncompliant” and kill the setting.

5) Configure Server Manager Remoting

To configure in GUI:

Go to **Server Manager**

Under **Server Summary** on the right, click “Configure Server Manager Remote Management”

Click on it, uncheck the box if it is checked

Command line option is: Configure-SMRemoting in Powershell, but is a pain to use.

This breaks a lot.

6) **Removal of Features**

Go to **Server Manager**

Go to **Features**

Remove anything non-mission critical (default roleless install has 0 features)

7) **Services listed**

- DNS (p. 5)
- IIS (p. 6)
- DHCP (p. 9)
- Print Services (p. 9)

8) Services to Secure

DNS:

Configure advanced settings:

Open DNS:

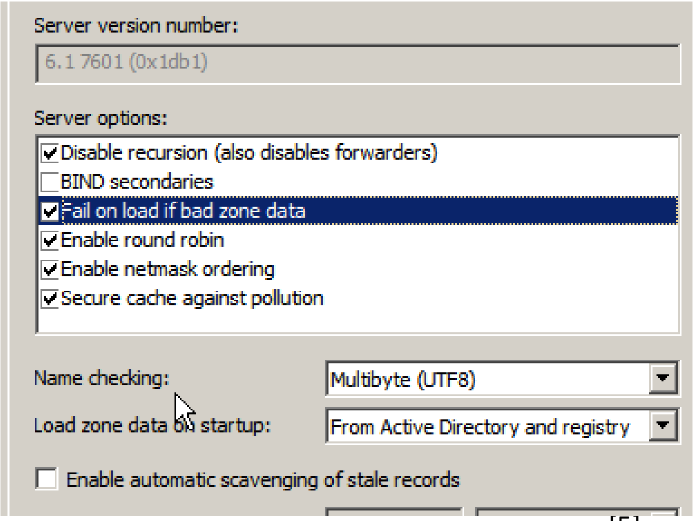
Start > All Programs > Administrative Tools > DNS

Open Configuration:

Right click on applicable DNS server (there should only be one)

Click **Properties**

Click **Advanced**



Server version number:

6.1 7601 (0x1db1)

Server options:

☑ Disable recursion (also disables forwarders)
□ BIND secondaries
☑ Fail on load if bad zone data
☑ Enable round robin
☑ Enable netmask ordering
☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

□ Enable automatic scavenging of stale records

The following should be the configuration. Should you end up with a non-functioning DNS server, the first thing to check would be "fail on load if bad zone data."

Restart may (but probably won't be) required eventually.

Open Root Hints:

Go to the **Root Hints** tab under Properties

Server FQDN's should only be a.root-servers.net. – m.root.servers.net.

IP addresses may vary, but if you must confirm them go here

(http://www.root-servers.org/)

Open Forwarders:

Go to **Forwarders**. It should be empty with the box checked saying "Use root hints…"

Open Debug Logging:

Go to **Debug Logging**. Check all of the boxes because why not?

Open Event Logging:

Go to **Event Logging.**

Select "All events"

Open Trust Anchors:

This should be empty

Open Monitoring:

Feel free to run tests

Failing to pass tests may result in scoring errors, but probably won't

IIS:

IIS has a lot of roles, and as such, you should consider removing some to limit your attack platform.

PLEASE FOR THE LOVE OF GOD FIRST VISIT AND BROWSE THE SITE IN YOUR HOST BROWSER.

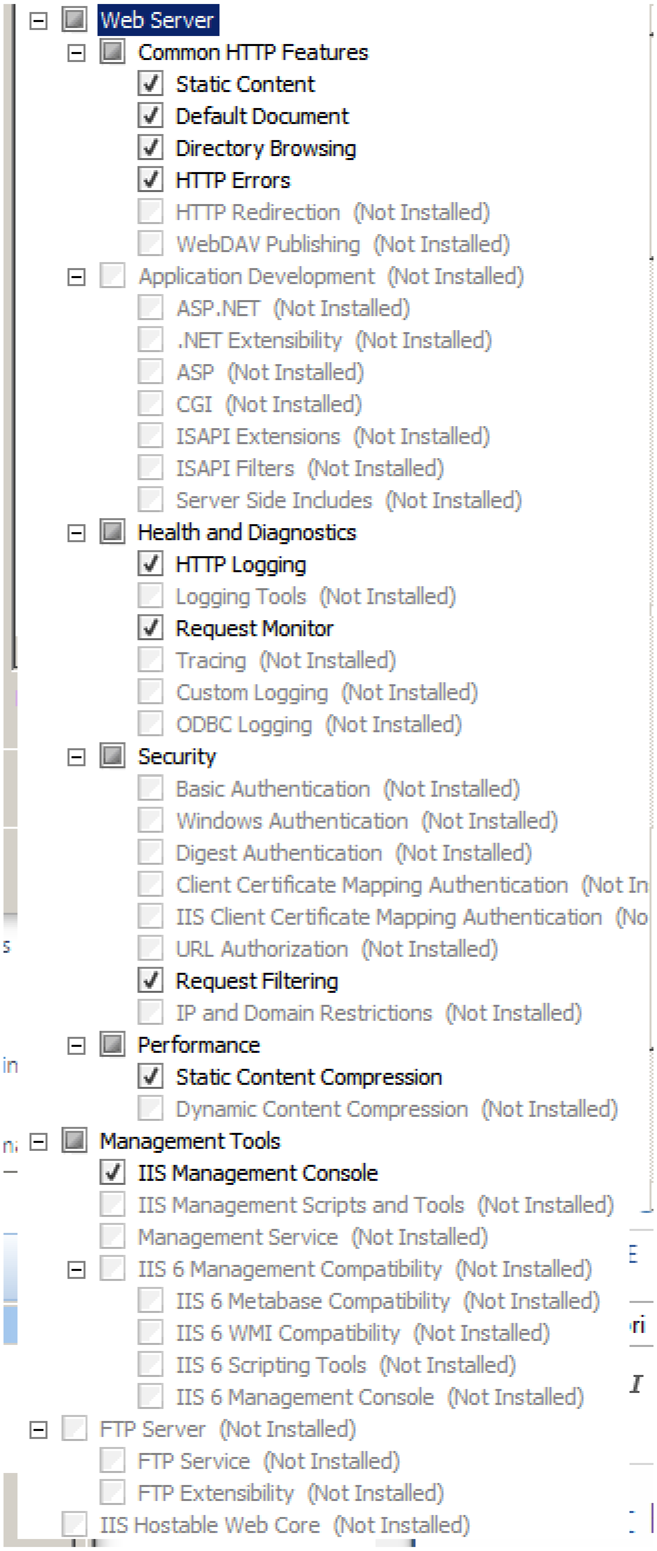
See how it handles bad requests. Try to visit pages that don't exist, for instance.

Then visit the default content folder on the server, C:\inetpub\wwwroot and see what it has other than iisstart.html and welcome.png, then open both (HTML in Notepad, image in image viewer) to see if anything is off. Delete non-critical content.

Go to **Server Manager > Roles**

Right click on **Web Server (IIS)** and select **Remove Role Services**

Confirm all role services listed are necessary and if not, clear the check box next to it’s name.



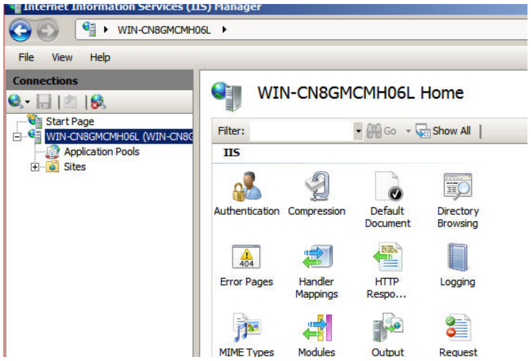
- ⊟ ▣ Web Server
  - ⊟ ▣ Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - □ HTTP Redirection (Not Installed)
    - □ WebDAV Publishing (Not Installed)
  - ⊟ □ Application Development (Not Installed)
    - □ ASP.NET (Not Installed)
    - □ .NET Extensibility (Not Installed)
    - □ ASP (Not Installed)
    - □ CGI (Not Installed)
    - □ ISAPI Extensions (Not Installed)
    - □ ISAPI Filters (Not Installed)
    - □ Server Side Includes (Not Installed)
  - ⊟ ▣ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Logging Tools (Not Installed)
    - ☑ Request Monitor
    - □ Tracing (Not Installed)
    - □ Custom Logging (Not Installed)
    - □ ODBC Logging (Not Installed)
  - ⊟ ▣ Security
    - □ Basic Authentication (Not Installed)
    - □ Windows Authentication (Not Installed)
    - □ Digest Authentication (Not Installed)
    - □ Client Certificate Mapping Authentication (Not In
    - □ IIS Client Certificate Mapping Authentication (No
    - □ URL Authorization (Not Installed)
    - ☑ Request Filtering
    - □ IP and Domain Restrictions (Not Installed)
  - ⊟ ▣ Performance
    - ☑ Static Content Compression
    - □ Dynamic Content Compression (Not Installed)
- ⊟ ▣ Management Tools
  - ☑ IIS Management Console
  - □ IIS Management Scripts and Tools (Not Installed)
  - □ Management Service (Not Installed)
  - ⊟ □ IIS 6 Management Compatibility (Not Installed)
    - □ IIS 6 Metabase Compatibility (Not Installed)
    - □ IIS 6 WMI Compatibility (Not Installed)
    - □ IIS 6 Scripting Tools (Not Installed)
    - □ IIS 6 Management Console (Not Installed)
- ⊟ □ FTP Server (Not Installed)
  - □ FTP Service (Not Installed)
  - □ FTP Extensibility (Not Installed)
- □ IIS Hostable Web Core (Not Installed)

To the left is the default selection of role services on IIS after installation. If something else is here, try to understand it’s purpose and if it can be removed. Probably the most popular ones to exploit would be ASP.NET, CGI, and FTP Server.

Open IIS Manager:

Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager

Click on the server you're managing (there should only be one and when you expand it it should have "Sites" and "Application Pools" as options) and you should be at the following page:



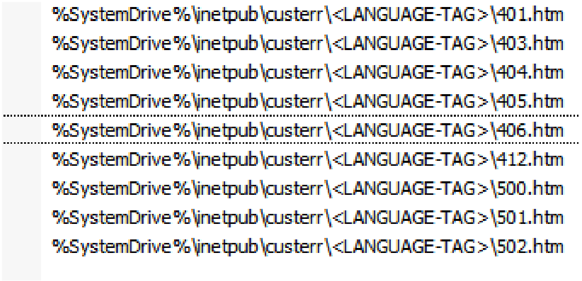
(*) Select **"Authentication"**. If possible, turn off Anonymous Authentication by highlighting it and selecting **"Disable"** on the right. ***Depending on how thoroughly and the competition SLA this may result in a reduction of points. If you are penalized in CyberPatriot for IIS going down, try re-enabled.***

Go back by reselecting the server on the left.

(*) Select **"Default Document"** and ensure "Default.htm", "Default.asp", "index.htm", "index.html", and "iisstart.htm" are the list in that order. If it's roughly that it's fine. Otherwise, remove them.

Go back by reselecting the server on the left.

(*) Select **"Error Pages"** and ensure the path looks something like this:



```
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\401.htm
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\403.htm
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\404.htm
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\405.htm
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\406.htm
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\412.htm
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\500.htm
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\501.htm
%SystemDrive%\inetpub\custerr\<LANGUAGE-TAG>\502.htm
```

If you have time, consider going through these. <LANGUAGE-TAG> is to be replaced by en-US by default.

Go to the parent folder otherwise and figure it out from there.

(*) Select **“Handler Mappings”**. By default there is only OPTIONSVerbHandler, TRACEVerbHandler, and StaticFile.

Go back by reselecting the server on the left.

(*) Select **“HTTP Request Headers.”** This should be virtually always empty. If you see anything, it’s probably pretty safe to remove it.

Go back by reselecting the server on the left.

(*) Select **“Logging”** and ensure logging is enabled (not Greyed out). If it’s greyed out select Enable on the right.

Go back by reselecting the server on the left.

(*) Select **“Modules”** and ensure all modules types are “Native”

Request Filtering, Output Caching, Server Certificates (unless HTTPS) should all be empty.

Go back by reselecting the server on the left.

(*) Select **“Shared Configuration”** and disable shared configuration by unchecking the shared configuration box

DHCP

At this time, no major role-specific security misconfigurations seem possible on Windows DHCP servers as DHCP is an unauthenticated, relatively simple protocol anyway.

DNS server too?

Dynamically update DNS A and PTR records only if requested by the DHCP clients under **Properties** on the **DNS** tab on the **DHCP server**

Print Services

The only potential flaw in a Print and Document services server in terms of the very role is the role services.

Open **Server Manager**

Roles > Right Click **Print and Document Services**

Remove unneeded services by clicking **Remove Role Services**