# Windows Server 2003

* Change Local admin password (start -> right click on ‘computer’ -> ‘manage’ -> ‘Local Users and Groups’ -> ‘users’ -> right click on ‘administrator’ -> ‘change password’) **OR** ( in cmd.exe “net user administrator ‘type new password here”’)
* Check for additional admin accounts/Disable Guest (start > admin tools > computer management > local users and groups > users)
* Check for updates (start -> control panel -> windows updates) **OR** ( in cmd.exe “wuapp.exe”)
* Check Time/Date
* Disable RDP (start > right click ‘my computer’ > properties > remote tab > select users)
* Antivirus (“Microsoft security essentials”)
* Configure Shadow Copies (Start > Manager your server > file server > shares > Shadow)
* Remove unnecessary roles/services (\*\*Know your server\*\*You don’t need IIS on an AD/DNS\*\* Run configuration wizard under start)
* Check disk quota
* Microsoft Security Baseline Analyzer (download and run -> will show missing issues)
* Security Config Wizard (if not installed start > Control panel > add remove programs > add windows components)
* Disable IPv6 (start -> control panel -> network and internet -> change adapter settings -> right click ‘properties’ on active NIC -> uncheck ipv6 )
* Windows Firewall Configure Start -> control panel -> windows firewall (\*\*SCW should enable it but double check\*\*Make sure unnecessary exceptions\*\*)

Click *Allow apps to communicate through Firewall* (top option on left pane)

Base Line security analyzer walks through firewall settings.

Disable LanMan (Start -> Settings -> Control Panel -> Administrative Tools -> Local Security Polic-> Expand the “Local Policies” folder and select “Security Options” beneath it. Double click “Network security: LAN Manager authentication level”.Change the setting to “Send NTLMv2 response only\refuse LM & NTLM”.)

## Reasources

http://repo.mynooblife.org/.priv8/Mag/Hackin9/CD/ebooks/windows\_server\_2003\_hardening\_checklist.pdf

# Active Directory

### 1. Installation of AD and DNS:

1. Do proper IP Configuration: Give static IP, subnet mask and Default gateway

For DNS IP, setup servers own IP or 127.0.0.1

1. Install the role ‘Active Directory Domain Services’ in the windows 2008 server.

Server manager->Roles and Features->Add role->Check ADDS role ->Install

1. Install Active Directory

* Run dcpromo.exe from “run” box or from “cmd”
* Create New Domain in New Forest
* Give desired domain name (ex: newdomain.com)
* Select Windows Server 2003 is Forest and Domain Functional level
* Check *DNS Server* in Additional Domain Controller Option
* Click Yes for DNS delegation warning
* Use default settings for Sysvol and database folders
* Restore mode admin password
* Reboot machine after installation

### 2. Creating and deleting users and Groups:

***To create a user***

1. Open Active Directory Users and Computers mmc panel (Start->Administrative Tools-ADU&C)
2. Right Click on Users-> *new user*
3. Give first/last name, login name
4. Check or uncheck relevant options below
5. User account can be disabled or enabled or unlocked from the user properties

***To delete a user:***

Right Click any user->Click delete user

***To create a group:***

1. Right Click on users (or any other folder)->new Group->give group name
2. Select Scope and Type. Most of the default options are fine

***To Create an Organizational Unit(OU):***

1. Right Click on Domain name ->New OU->Give the name
2. Users or group can be dragged and dropped to move them into a OU. Alternatively right click a user or group->move ->select destination folder/OU

***To add, delete users from a group:***

1. Right click a group-> Properties-> *members* tab
2. List of users in the group is displayed.
3. To delete a user, select user-> remove->yes->apply
4. To add a member->add->type username in new dialog box->check->ok->apply
5. User membership can also be added, removed from user properties (*member of* tab) itself in the similar manner

### 3. Configuring Group Policies

1. Open Group Policy manager: Administrative Tools->Group Policy Management
2. Navigate to group policy needed to be changed
3. Default policies can be found in Group Policy Objects folder in the tree
4. Right Click on a policy (Ex: Default domain policy)->Edit

*To create new policy:*

1. A group policy can be created at a OU level, domain level and site level
2. Right Click on Domain name or OU-> Create a GPO in this domain and link it here->Give GPO name
3. Right new GPO->Edit

*To Change Password Policy in Default Domain GP*

1. Right Click on Default domain policy ->Edit
2. Navigate to Computer Configuration->Policies->Windows Settings->Security Settings->Account Policies->Password Policies
3. Security Policies can be set at Account Policies->Local Policies->Security Options

### 4. Identifying basic AD Setup

***Things to look for in a newly created domain:***

1. Users, groups, OUs, computers in the domain:

Start->Administrative Tools->Active Directory Users and Groups

Users, Groups Computers, OUs are organized in folders in the tree

An OU may have users, groups, computers and other OUs

A Users (default) folder may have users

The *Built-in* folder has default list of groups, the *Users* folder has default created users

1. Roles installed on domain controller

Server Manager->Roles->Roles Summery Panel

1. Domain security policy, password policy
2. Member of Administrators groups

# DNS

### 5. DNS Server

***DNS server is installed along with Active Directory.***

1. To Open DNS Server mmc: Administrative Tools->DNS
2. Expand the tree by clicking on domain name, forward lookup zones, and reverse lookup zones

Usually there are two zones: one with *­\_msdsc.domain\_name* and the other with *domain\_name*

1. List of *host, NS and SOA records*  are found under the domain name folder
2. You can see zone(domain) and DNS server properties by right clicking on domain name or on DNS Server name at top of the tree respectively

### 6. Manually creating, deleting records in DNS

1. Navigate to DNS Zone (Domain name) in the tree in left panel
2. Right click on Domain name->new host/alias/MX record
3. Give IP address and host name (for a host record)
4. To *delete* a record, right click on a record->delete record

Note: When a computer is joined to domain a host record is automatically created

# DHCP

### 7. Installing DHCP Server

1. Administrative Tools->Server manager->Roles->Add New Role->DHCP

2. Click Next->Check the Server IP->Next

3. Check domain name and DNS address

4. Wins-not required

5. Create DHCP Scope-the range of IP which are to be assigned to clients

ADD-> Enter scope name, starting & ending IP, subnet mask and gateway IP

6. Leave IPv6 settings default

7. Check *Use Current Credentials* for Authorizing->Next

8. Install

DHCP Reservation :

1. In the DHCP snap-in, expand the scope for which you want to create a reservation.
2. Select and right-click **Reservations** and then click **New Reservation**.
3. In the **New Reservation** dialog box, enter the **Reservation name**, **IP address**, **MAC address**, and **Description** of the reservation.
4. Select the appropriate **Supported types**: DHCP only, BOOTP only, or Both.
5. Click **Add**.

# FTP

# Windows Tools:

1. Process hacker
2. Tcp viewer
3. Security essentials
4. Security Baseline analyzer
5. Belarc Advisor
6. Autoruns
7. Event triggers (**eventtriggers**[**.exe**] **/create** [**/s** Computer [**/u** Domain\User [**/p** Password]]] **/tr** TriggerName [**/l** [**APPLICATION**] [**SYSTEM**] [**SECURITY**] ["**DNS Server**"] [**LOG**] [DirectoryLogName] [**\***] ] {[**/eid** ID]|[**/t** {**ERROR**|**INFORMATION**|**WARNING**|**SUCCESSAUDIT**|**FAILUREAUDIT**}]|[**/so** Source]} [**/d** Description] **/tk** TaskName [**/ru** {[Domain\]User | **"System"**} [**/rp** Password]])