1.1 ABSTRACT

Identification of human resources is much important in many aspects to maintain the national and personal integrity. Designing a prototype of a secured global repository of Human resources is the main agenda of this work. Primary objective is to design a GUI web application that lists out the Businesses, employees, Universities and students. Human resources, Machines, Information, are the assets that we count in general. Final outcome of the project is a website with the security controls.

1.2 PRELIMINARY INVESTIGATION PHASE

1.2.1 Summary of Problems and Opportunities

This system is designed for companies and schools. There are many companies and schools still maintaining the employee and student profiles in paper based records.

The chances of problems with that strategy are:

More Paper usage

Less Physical Security

Time Delay

More physical work

Time, Money and Resources

This web application will be useful to register modify and delete Company, School, employee and student profiles.

1.3 SYSTEM INTERFACE

At a Company

I am creating Admin profile in this application. An administrator logs in and creates Company Profile. Later, upon verbal request by HR from the company, the Administrator collects the information and then he creates HR profile.

HR with the default username and password issued by Administrator, logs in, he / she can modify his / her profile and will have an option to Create and Manage Employee Profiles.

Employees logs in with their default username and password issued by HR logs in to see their profiles.

At a School

I am creating Admin Profile in this application. An administrator logs in and creates school profile. Later, upon verbal request by Registrar from a school, the Administrator collects the information and then he creates Registrar Profile

Registrar with his default username and password issued by Administrator, logs in, he /she can modify his /her profile and will have an option to create and manage Student profiles.

Students with the default username and password issued by Registrar logs in to view their profile.

2. BUSINESS RULES

2.1 BUSINESS RULES IN A COMPANY

Admin Creates / modifies / Deletes Company profile // affects rows in companies table in database

Admin Creates / modifies / Deletes HR Profile // affects rows in Employees table in database.

HR Creates / modifies / Deletes Employee Profiles // affects rows in Employees table in database

2.2 BUSINESS RULES IN A SCHOOL

Admin Creates / modifies / Deletes school profile // affects rows in schools table

Admin Creates / modifies / deletes Registrar profile // affects rows in employees table.

Registrar Creates / modifies / deletes student profiles // affects rows in students table.

3. BUSINESS PROCESS

The business process in NCORP for a company involves an Administrator, a HR and Employees using their personal computers to update their personal information.

The business process in NCORP for a school involves an Administrator, a Registrar and Students using their personal computers to update their personal Information

4. SOFTWARE & HARDWARE USED

VIRTUAL MACHINES

VMWARE 11.

SERVER TECHNOLOGIES

WINDOWS SERVER 2008 R2 DATACENTER (2)

OPERATING SYSTEMS

KALI LINUX, WINDOWS SERVER 2008R2

DEVELOPMENT ENVIRONMENT

VISUAL STUDIO 2012

FRONTEND & BACKEND

ASP.NET, C# .NET

DATABASE

MS SQL SERVER

DEPLOYMENT SERVER

IIS 7

5. DATA COLLECTED BY THE SYSTEM

At a Company NCORP uses

For Companies

Company ID (Assumed to be issued by state government)

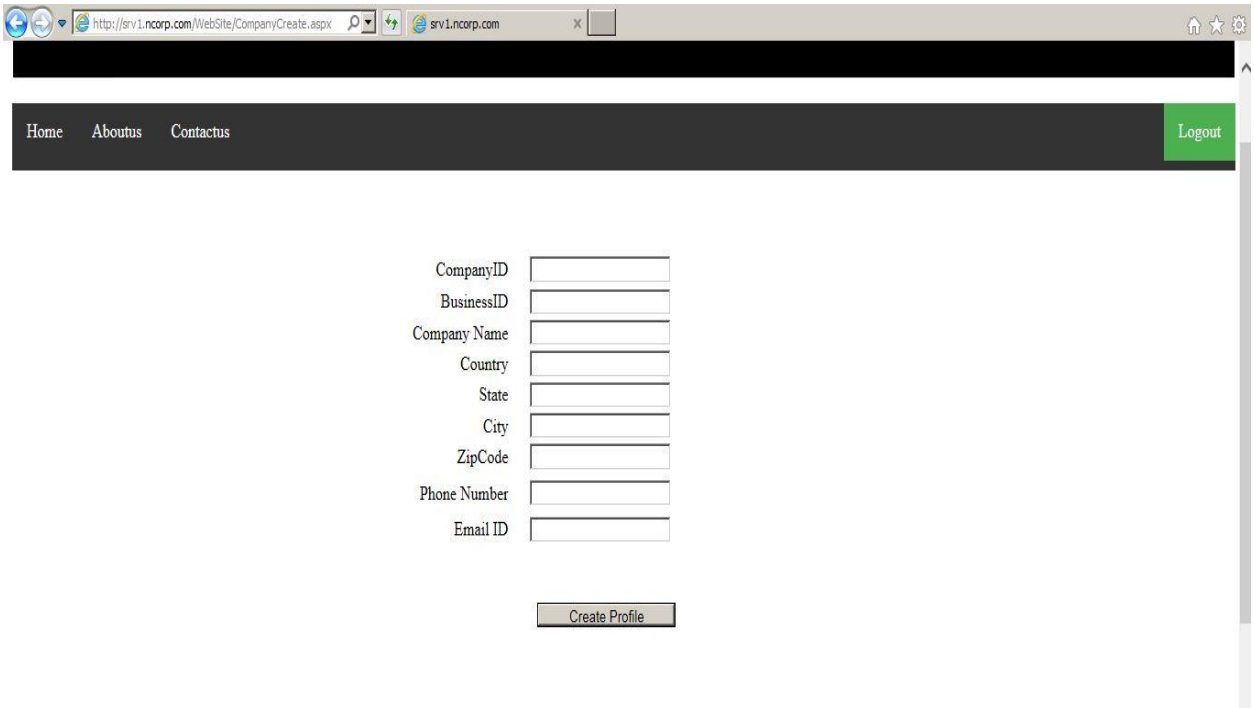
Business ID (Assumed to be issued by city labor commissioner)

Company name

Country

State City

Zip code



For Employees

Employee ID

Company ID

Company Name

Department Name

Designation

Username

Password

First name

Middle name

Password

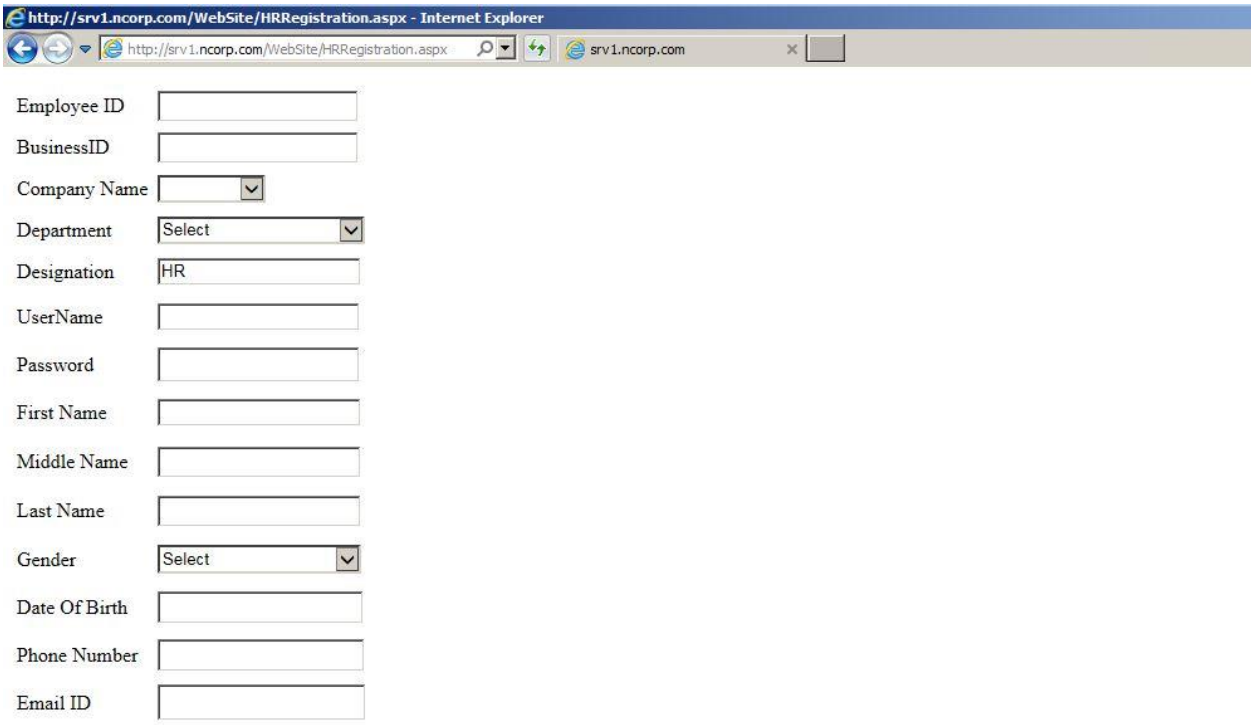
Gender

Date of Birth

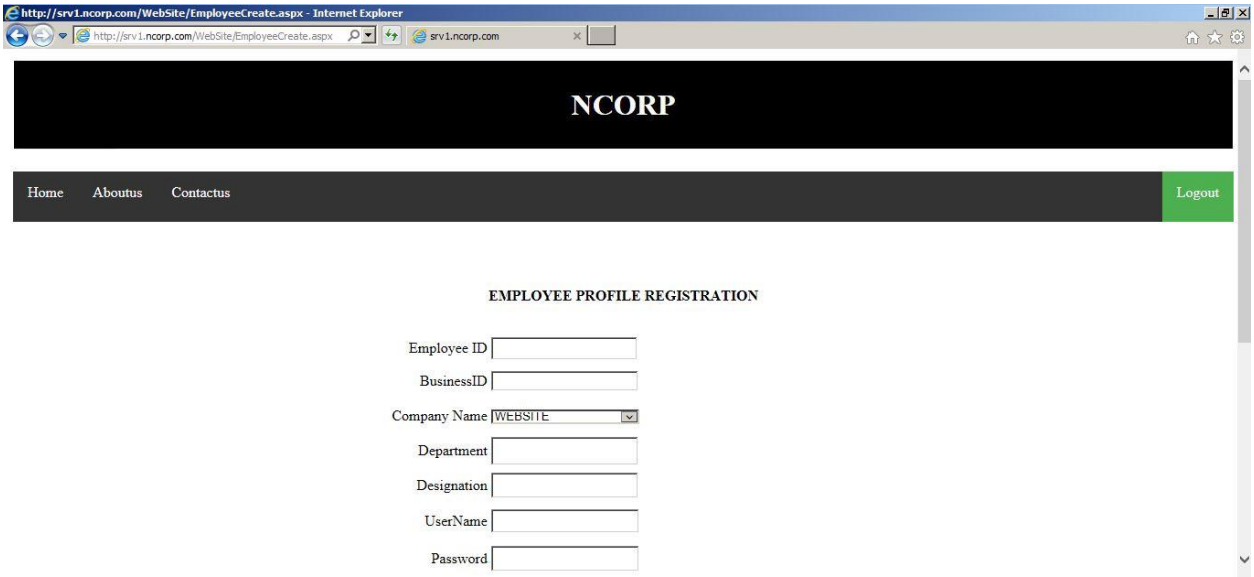
Phone Number

Email ID

HR PROFILE REGISTRATION



EMPLOYEE PROFILE REGISTRATION



At a School NCORP makes use of

<u>For Schools</u>

School ID

Business ID

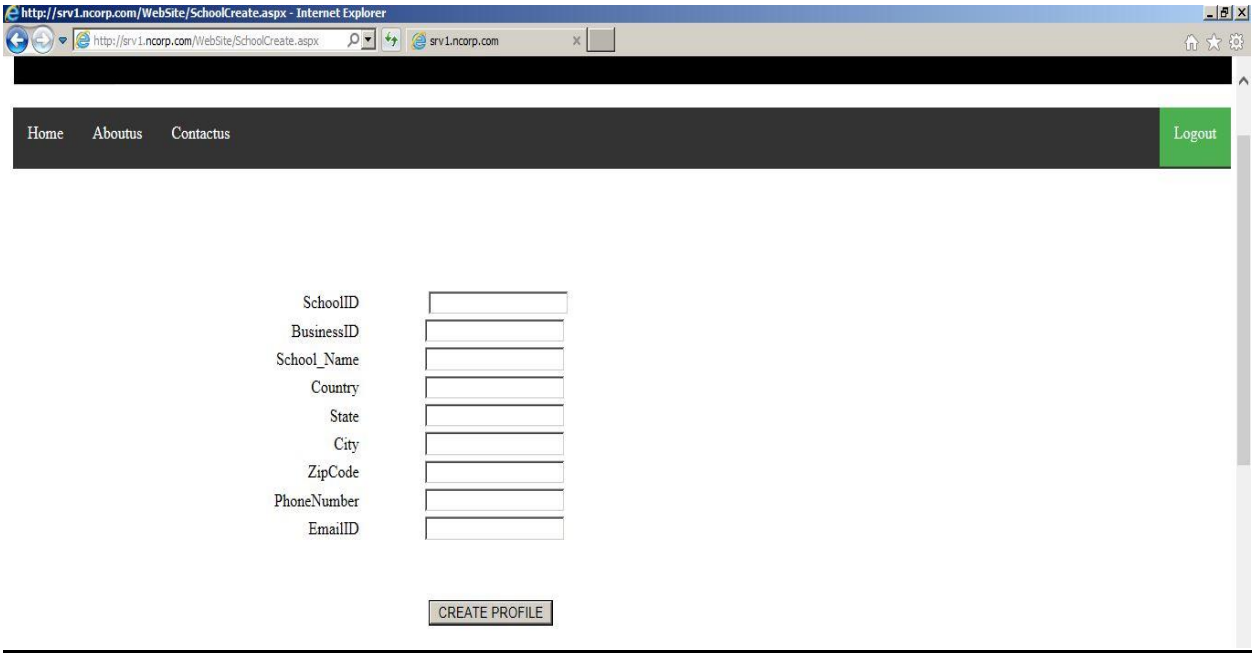
School name

Country

State

City

Zip Code



<u>For Employees / Registrar</u>

Employee ID

Business ID

School Name

Department

Designation

Username

Password

First name

Middle name

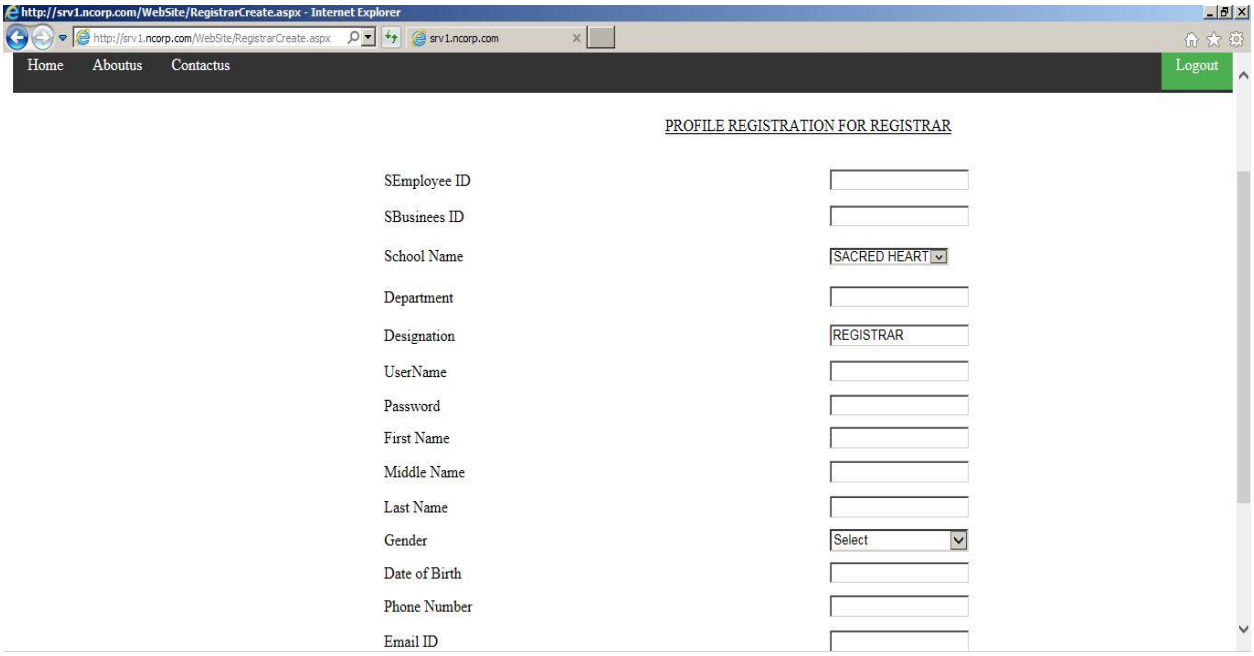
Last Name

Gender

Date of Birth

Phone Number

Email ID



<u>For Students</u>

Employee ID

School Name

Department

Username

Password

First name

Middle name

Password

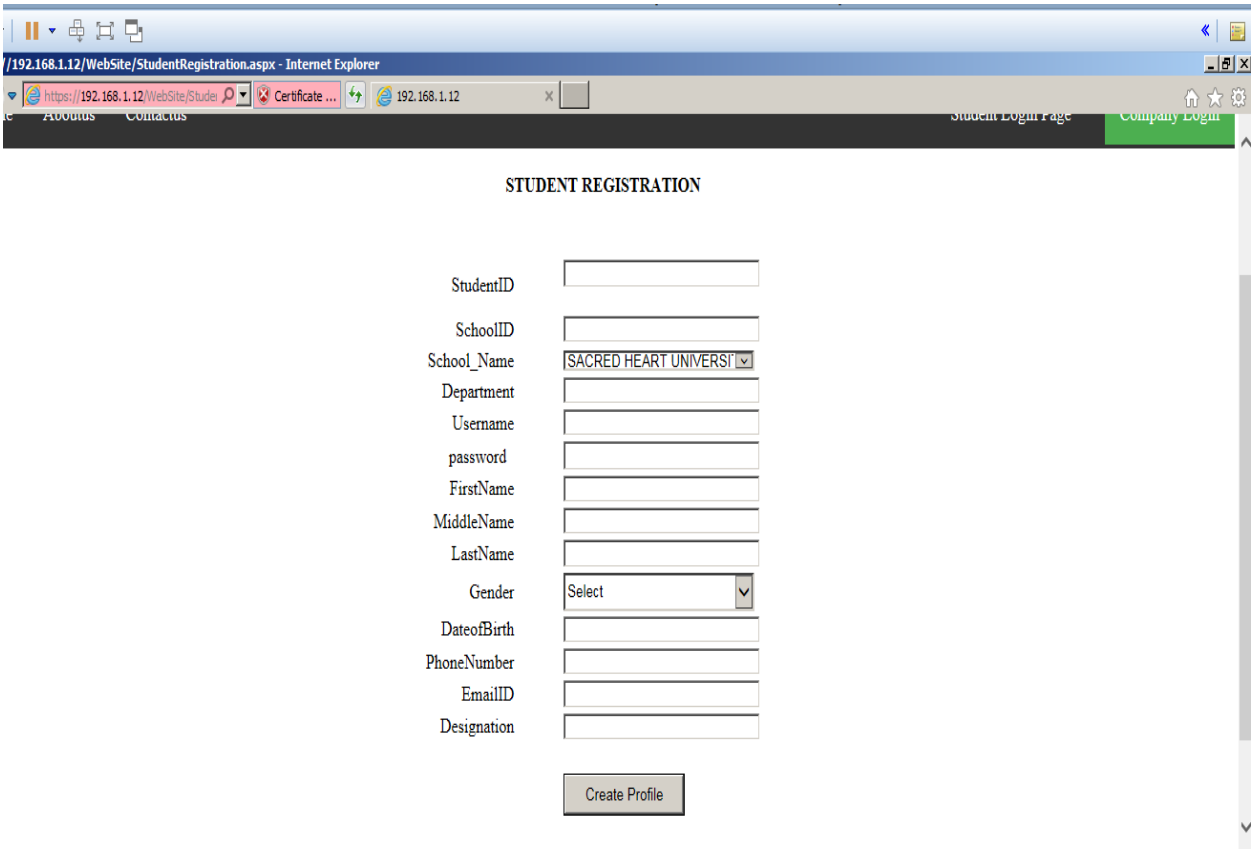
Gender

Date of Birth

Phone Number

Email ID

Designation



5.1 DATA STORAGE

The Employee and student information will be saved in the Database Servers.

5.2 PEOPLE INVOLVED

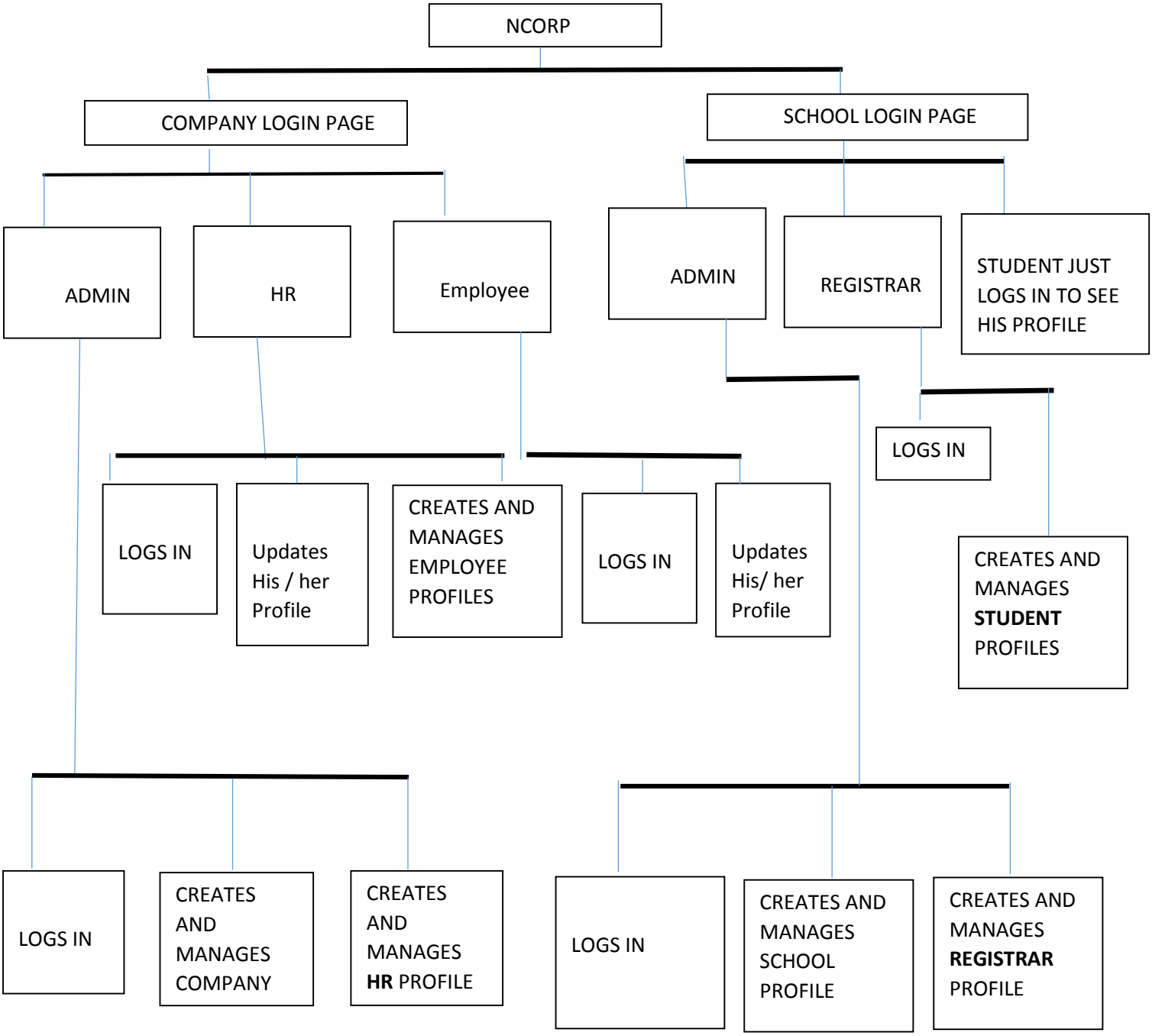
AT A COMPANY

1. ADMINISTRATOR
2. HR
3. EMPLOYEE

AT A SCHOOL

1. ADMINISTRATOR
2. REGISTRAR
3. STUDENT

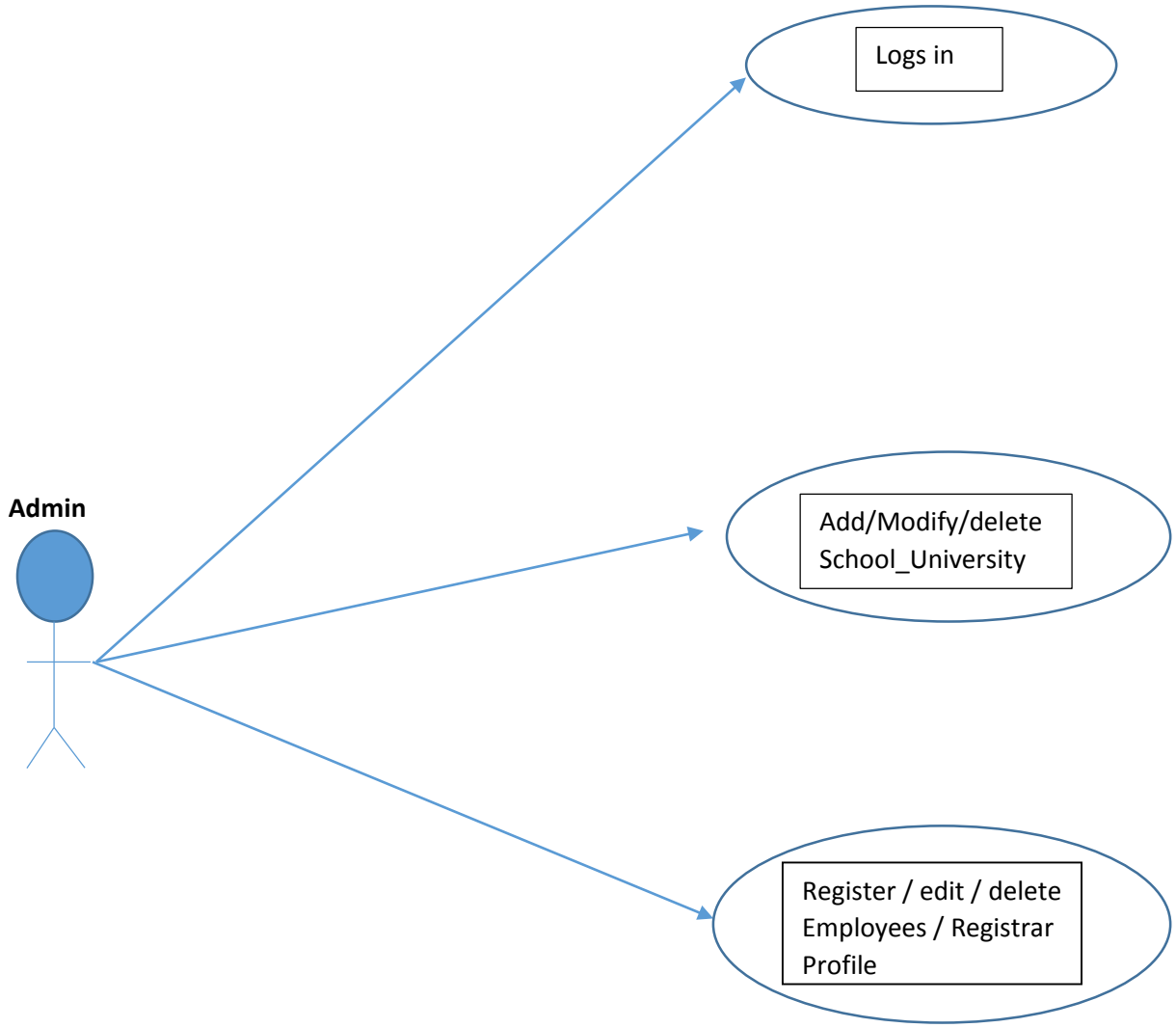
5.3 FUNCTIONAL DECOMPOSITION DIAGRAM



5.4 USE CASE DIAGRAMS

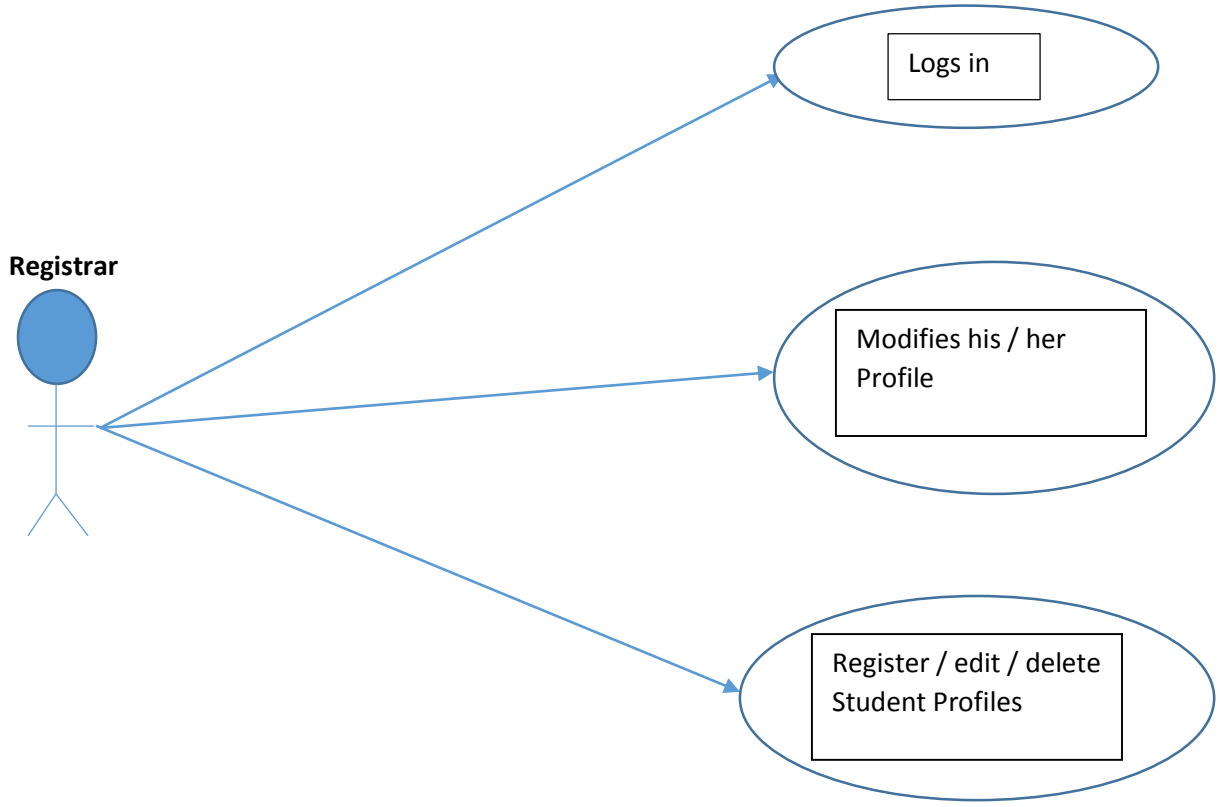
At a SCHOOL

Admin

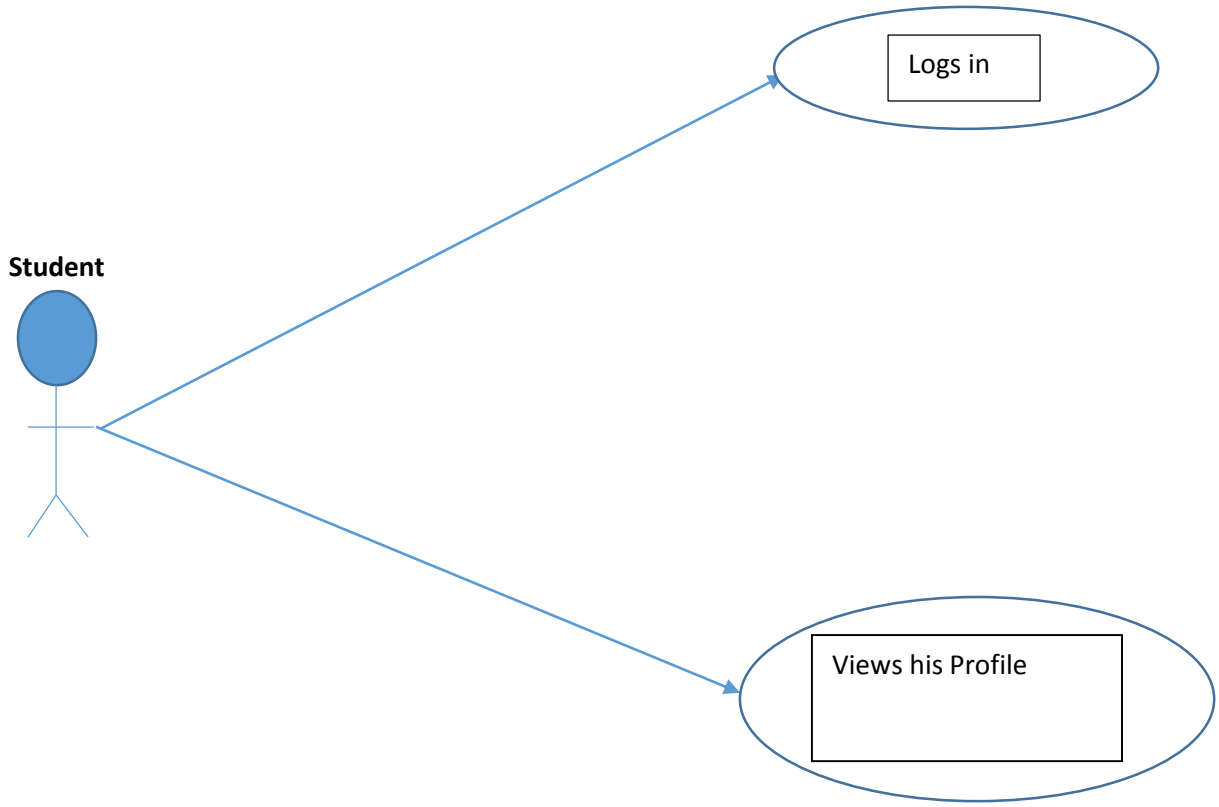


At a SCHOOL

Registrar

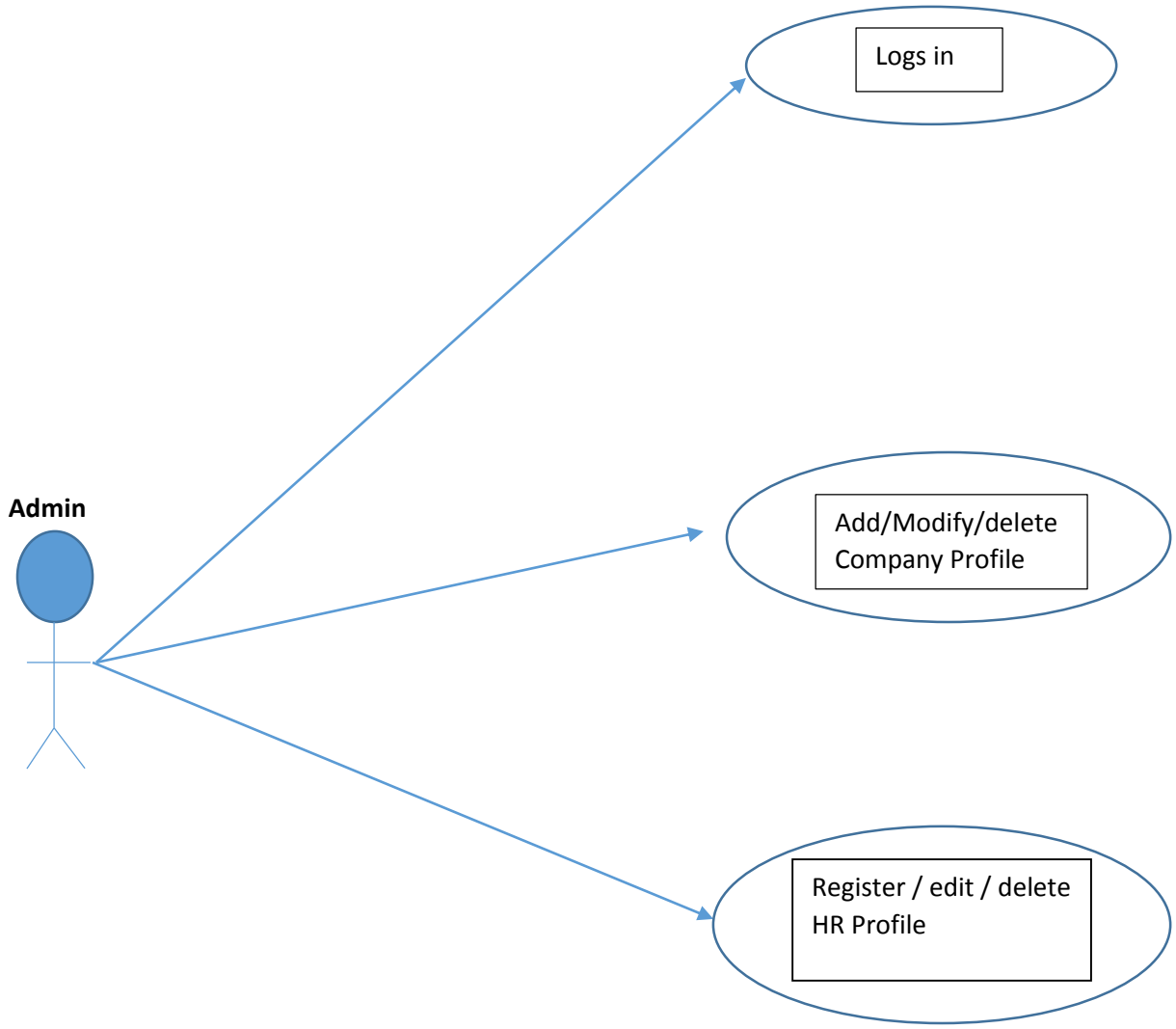


At a School



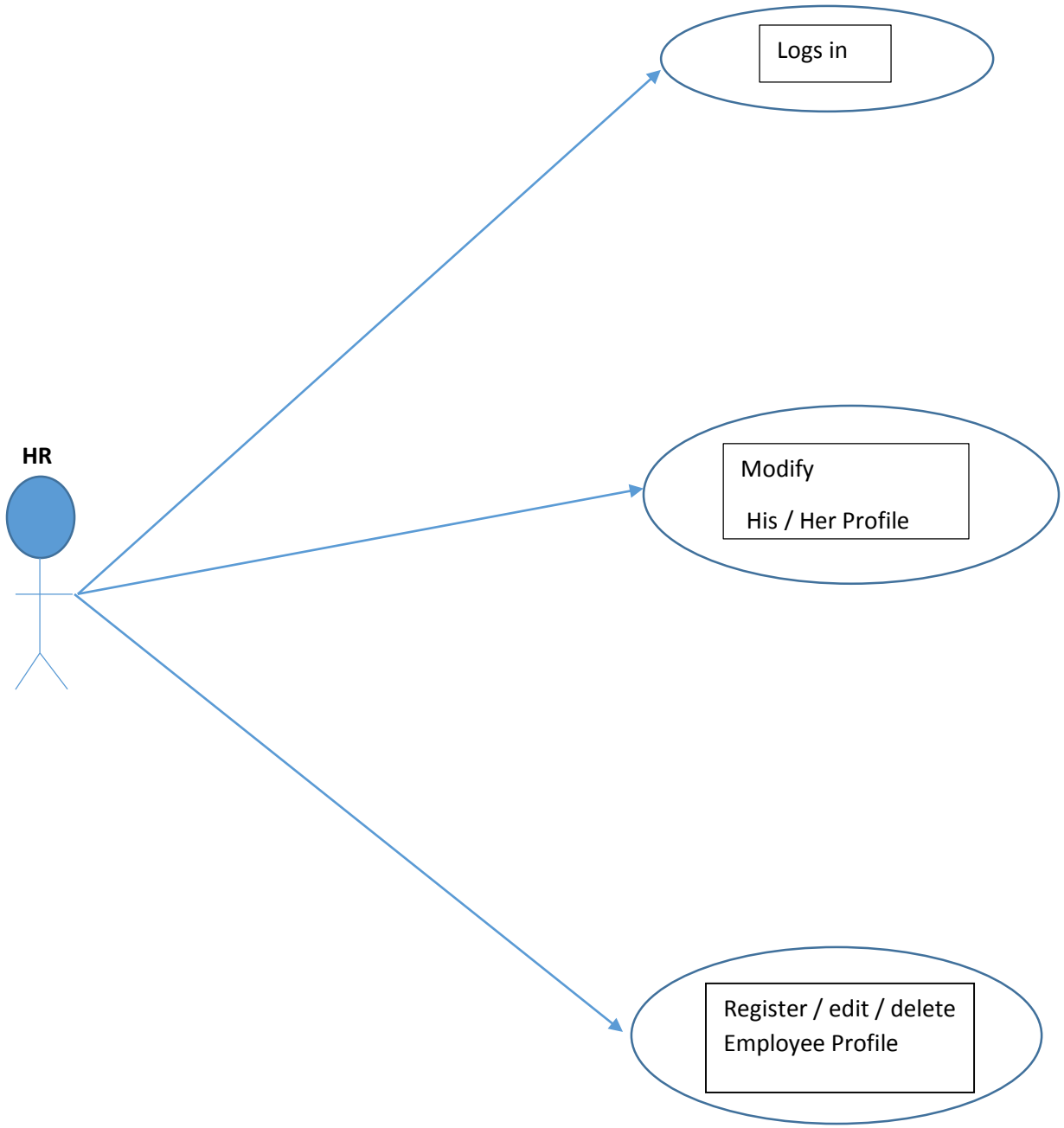
At a Company

Admin



At a Companies

HR

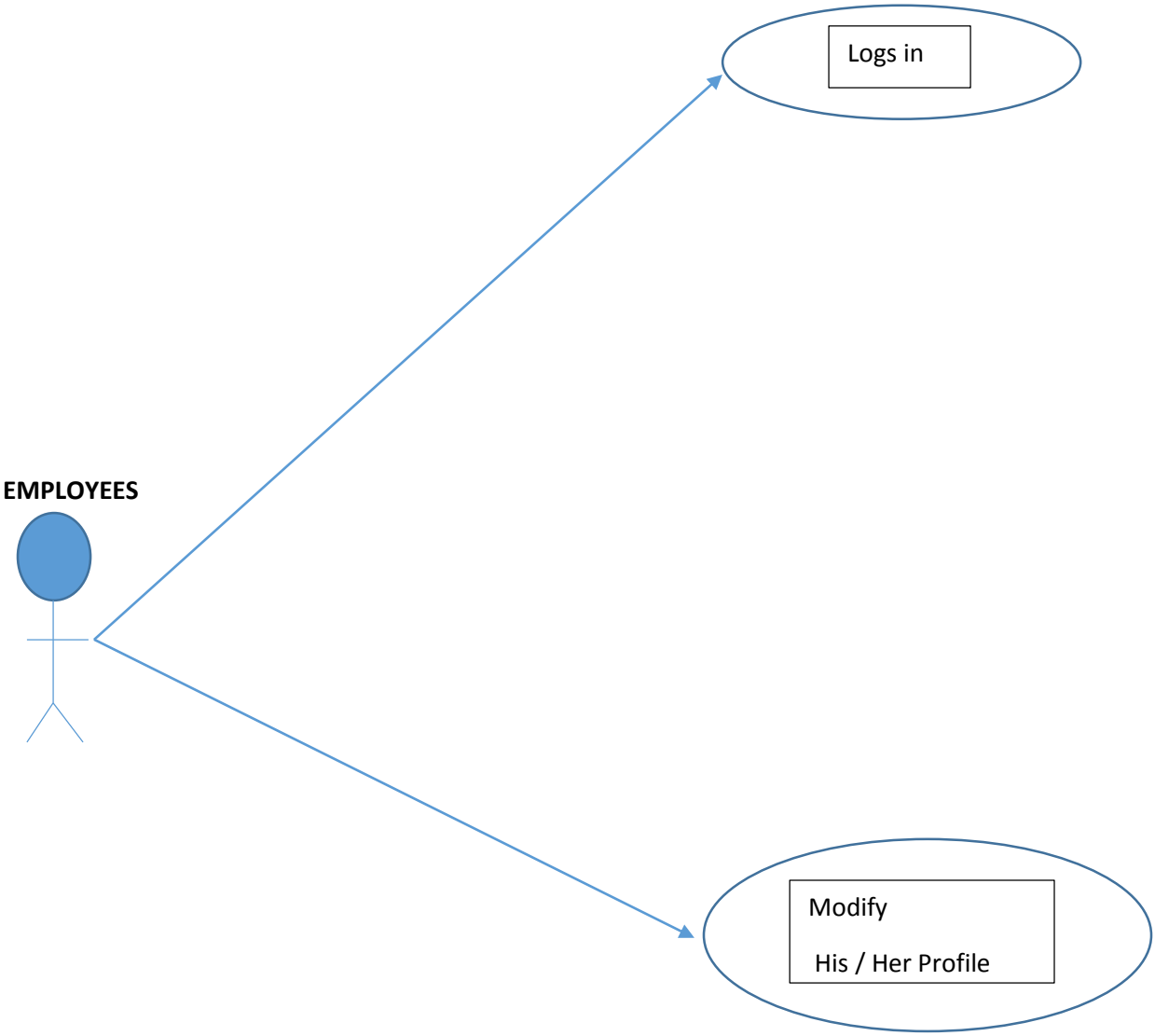


NOTE:

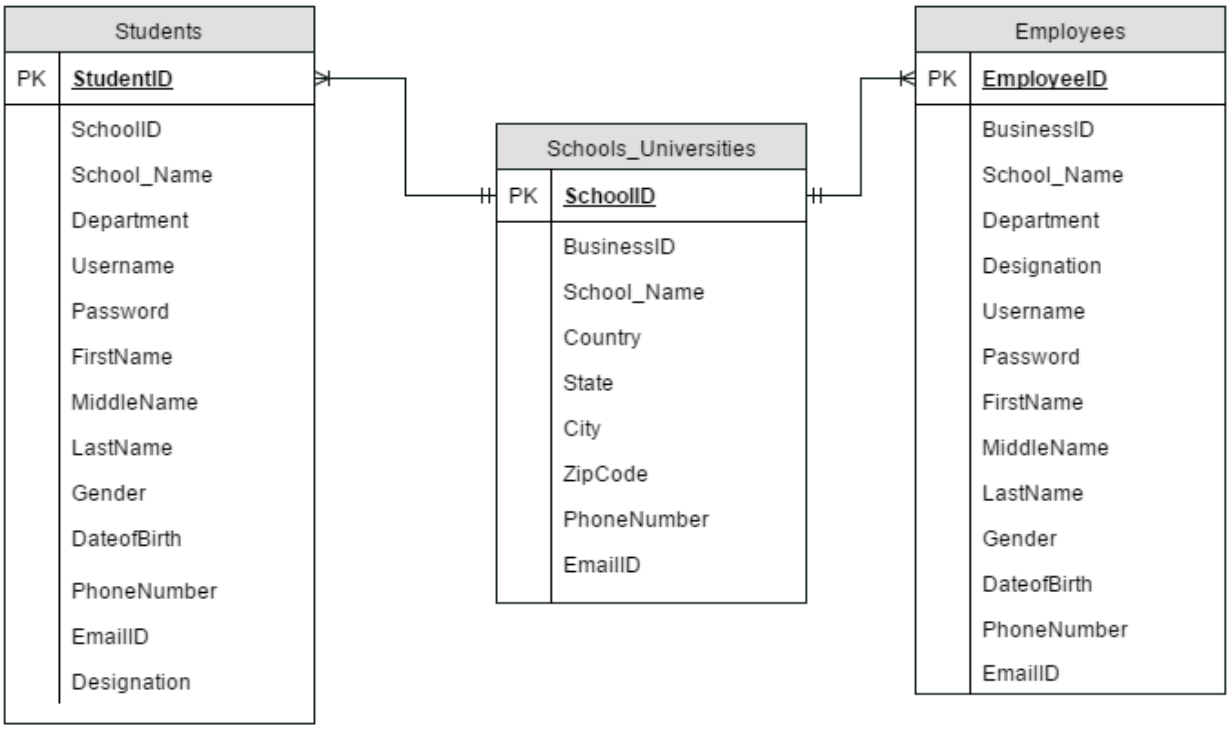
HR IS ALSO AN EMPLOYEE IN THE SAME TABLE

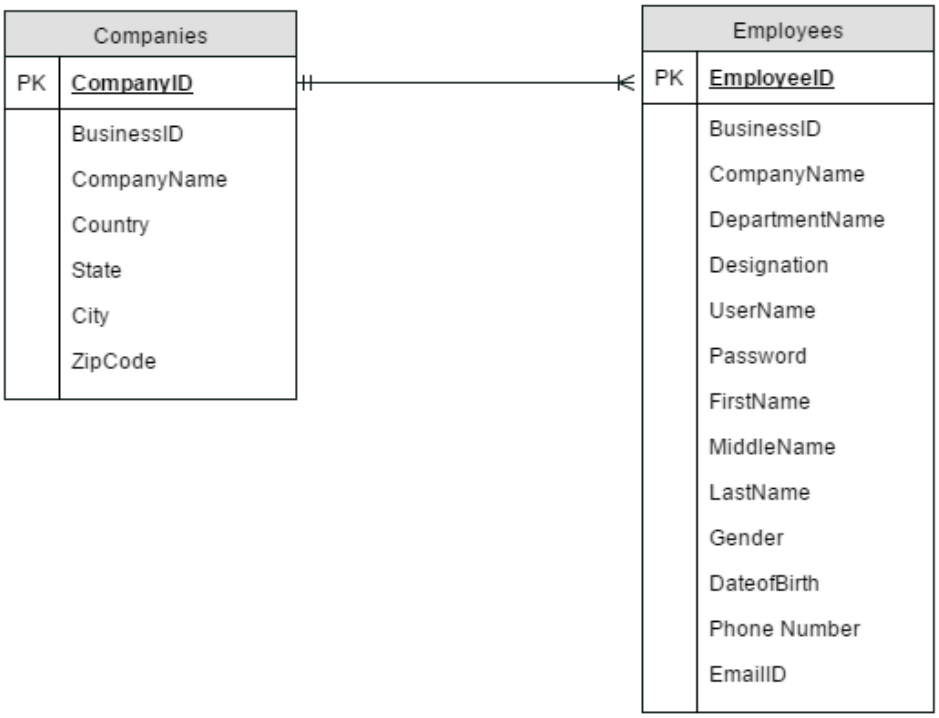
At a Company

EMPLOYEES



6. ENTITY RELATIONSHIP DIAGRAM

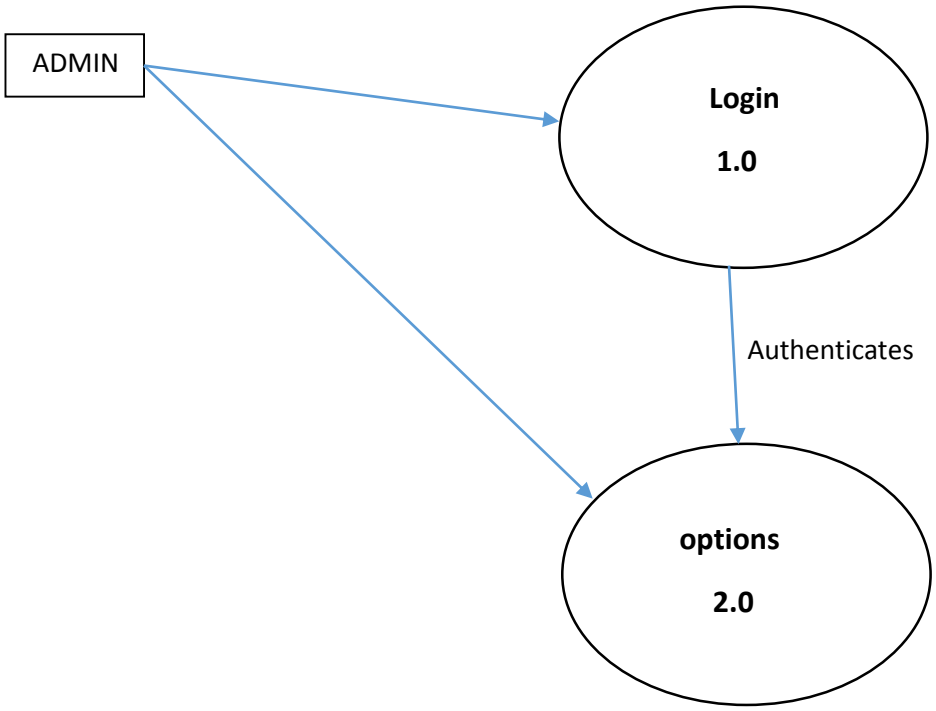


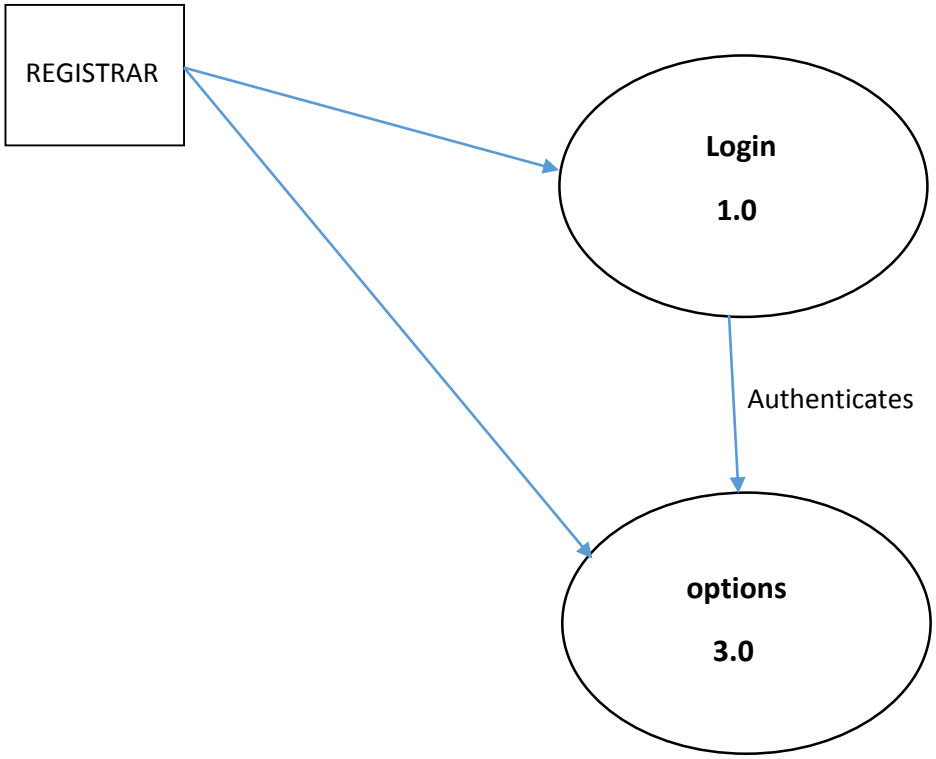


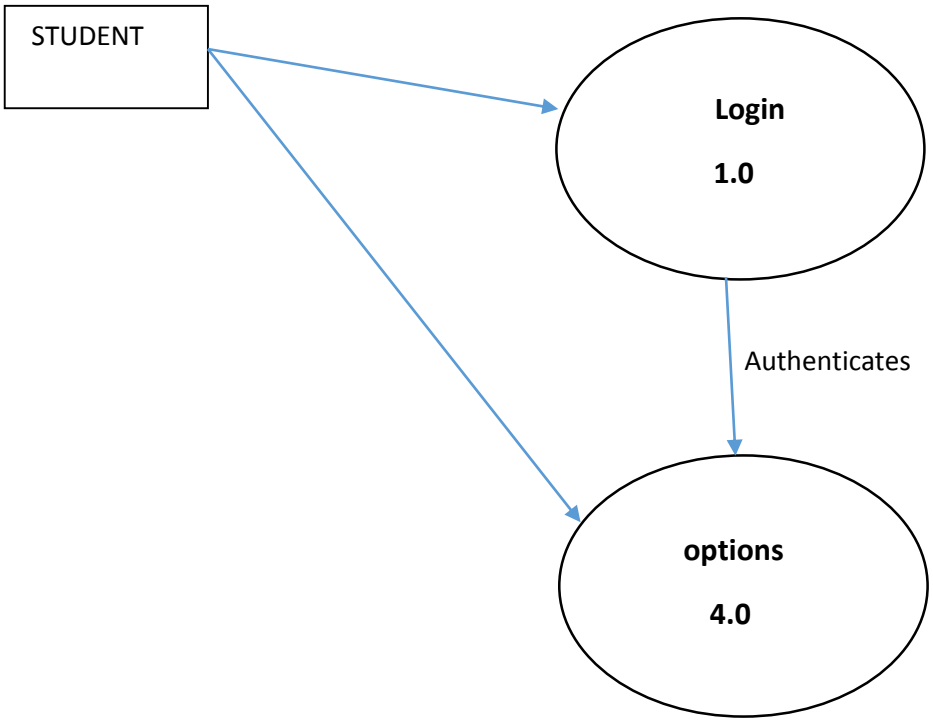
7.0 DATAFLOW DIAGRAMS

At a School

LEVEL 0

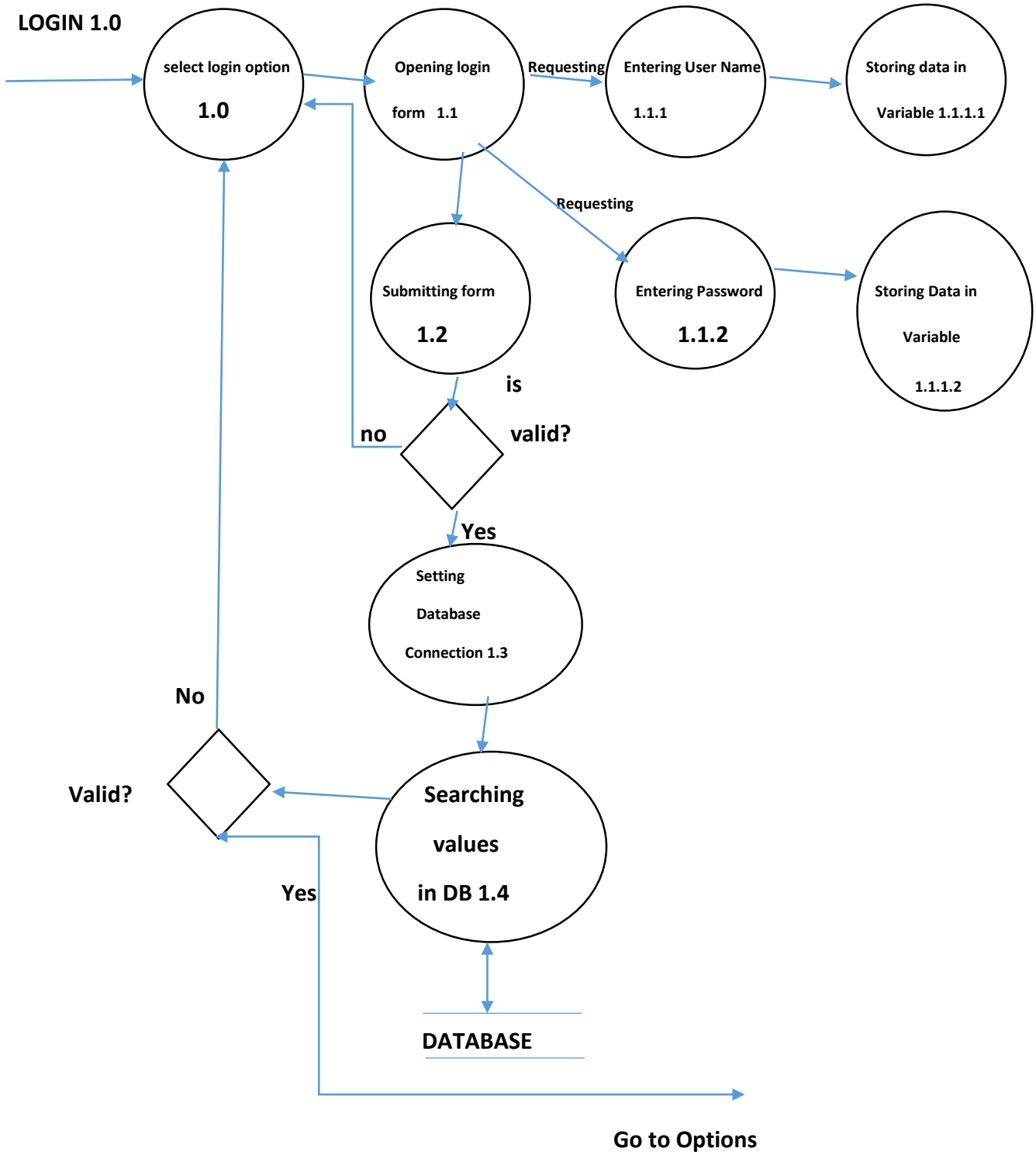





STUDENT
Login
1.0
Authenticates
options
4.0

LEVEL 1

LOGIN 1.0



LEVEL 2.0


options 2.0
Proceed to Create School 2.1
Entering School ID 2.1.1
Storing Value in Variable 2.1.1.1
Entering Business ID 2.1. 2
Storing Value in Variable 2.1.2.1
Entering School name 2.1.3
Storing Value in Variable 2.1.3.1
Entering Country. 2.1.4
Storing Value in Variable 2.1.4.1
Entering State 2.1.5
Storing value in Variable 2.1.5.1
Entering City, zipcode, EmailID, Phone Number 2.1.6
Storing Values in Variables 2.1.6.1
Submitting form
E
Setting Database Connection
Storing Values in Database
DATABASE
LOGOUT

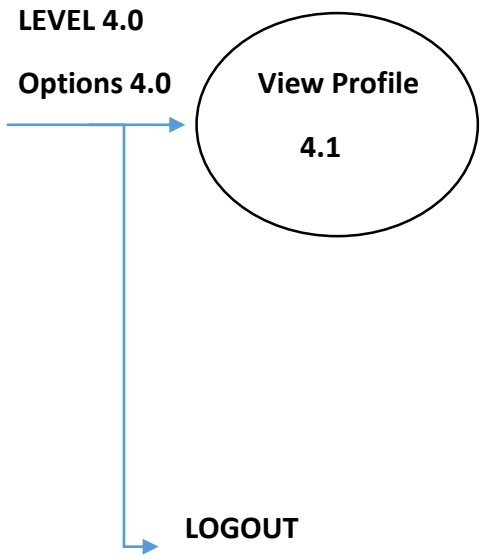

OPTIONS 2.0
Proceed to Create Registrar 2.2
Entering Employee ID 2.2.1
Storing Value in Variable 2.2.1.1
Entering Business ID 2.1. 2
Storing Value in Variable 2.1.2.1
Submitting form
Entering School name 2.1.3
Storing Value in Variable 2.1.3.1
E
Setting Database Connection
Entering Department 2.1.4
Storing Value in Variable 2.1.4.1
Entering username Passoword, 2.1.5
Storing value in Variables 2.1.5.1
Storing values In database
Entering First, Middle, LastNames, Gender 2.1.6
Storing Values in Variables 2.1.6.1
DATABASE
Entering DateofBirth Phone Email 2.1.7
Storing Values in Variables 2.1.7.1
LOGOUT


OPTIONS 2.0
Proceed to update School 2.3
Entering School ID 2.3.1
Storing Value in Variable 2.3.1.1
Entering Business ID 2.3. 2
Storing Value in Variable 2.3.2.1
Entering School name 2.3.3
Storing Value in Variable 2.3.3.1
Submitting form
Entering Country. 2.3.4
Storing Value in Variable 2.3.4.1
E
Setting Database Connection
Entering State 2.3.5
Storing value in Variable 2.3.5.1
Updating Values in Database
Entering City, zipcode, EmailID, Phone Number 2.3.6
Storing Values in Variables 2.3.6.1
DATABASE
LOGOUT


OPTIONS 2.0
Proceed to update Registrar 2.4
Entering Employee ID 2.4.1
Storing Value in Variable 2.4.1.1
Entering Business ID 2.4. 2
Storing Value in Variable 2.4.2.1
Submitting form
Entering School name 2.4.3
Storing Value in Variable 2.4.3.1
E
Setting Database Connection
Entering Department 2.4.4
Storing Value in Variable 2.4.4.1
Entering username Passoword, 2.4.5
Storing value in Variables 2.4.5.1
updating values In database
Entering First, Middle, LastNames, Gender 2.4.6
Storing Values in Variables 2.1.6.1
DATABASE
Entering DateofBirth Phone Email 2.4.7
Storing Values in Variables 2.4.7.1
LOGOUT

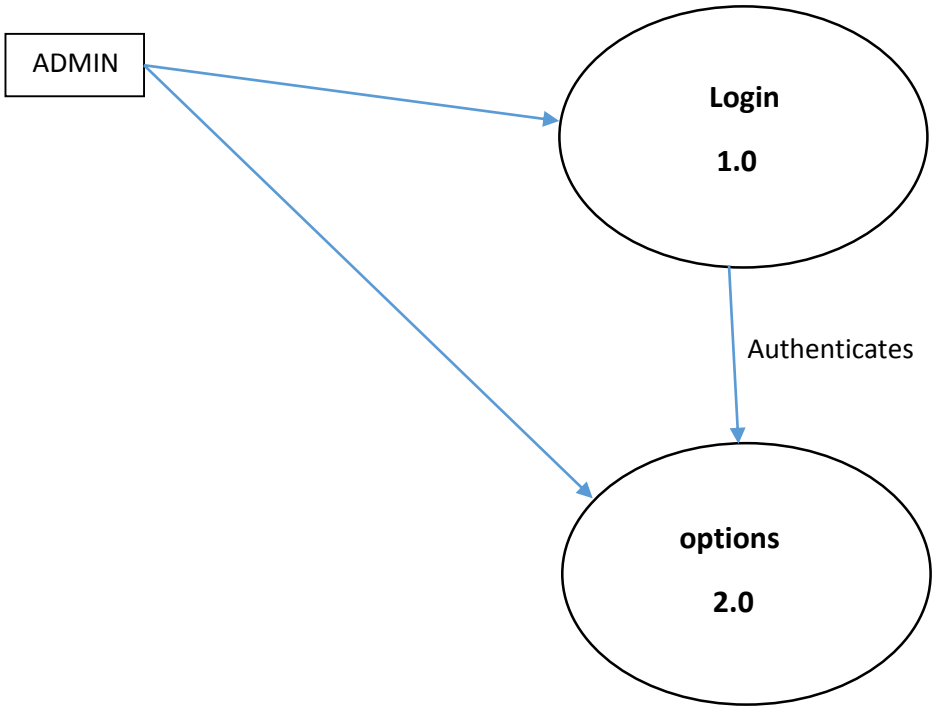
LEVEL 3.0

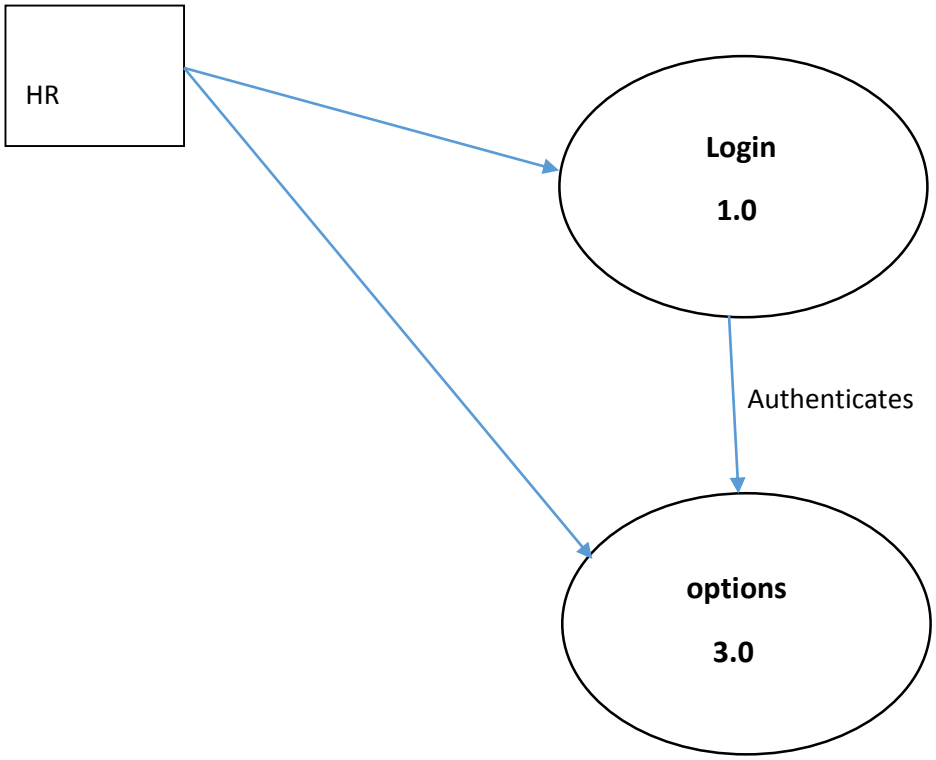

OPTIONS 3.0
Proceed to Create Student 3.1
Entering Student ID 3.1.1
Storing Value in Variable 3.1.1.1
Entering School ID 3.1. 2
Storing Value in Variable 3.1.2.1
Submitting form
Entering School name 3.1.3
Storing Value in Variable 3.1.3.1
E
Setting Database Connection
Entering Department 3.1.4
Storing Value in Variable 3.1.4.1
Entering username Passoword, 3.1.5
Storing value in Variables 3.1.5.1
Storing values In database
Entering First, Middle, LastNames, Gender 3.1.6
Storing Values in Variables 3.1.6.1
DATABASE
Entering DateofBirth Phone Email 3.1.7
Storing Values in Variables 3.1.7.1
LOGOUT

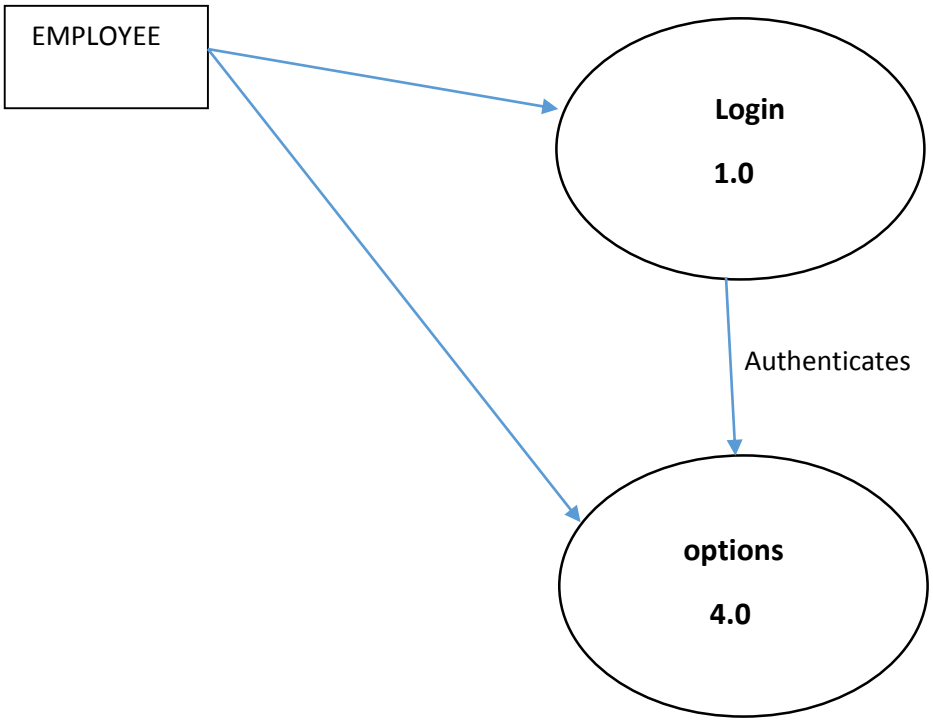

LEVEL 4.0
Options 4.0
View Profile
4.1
LOGOUT

At a Company

LEVEL 0

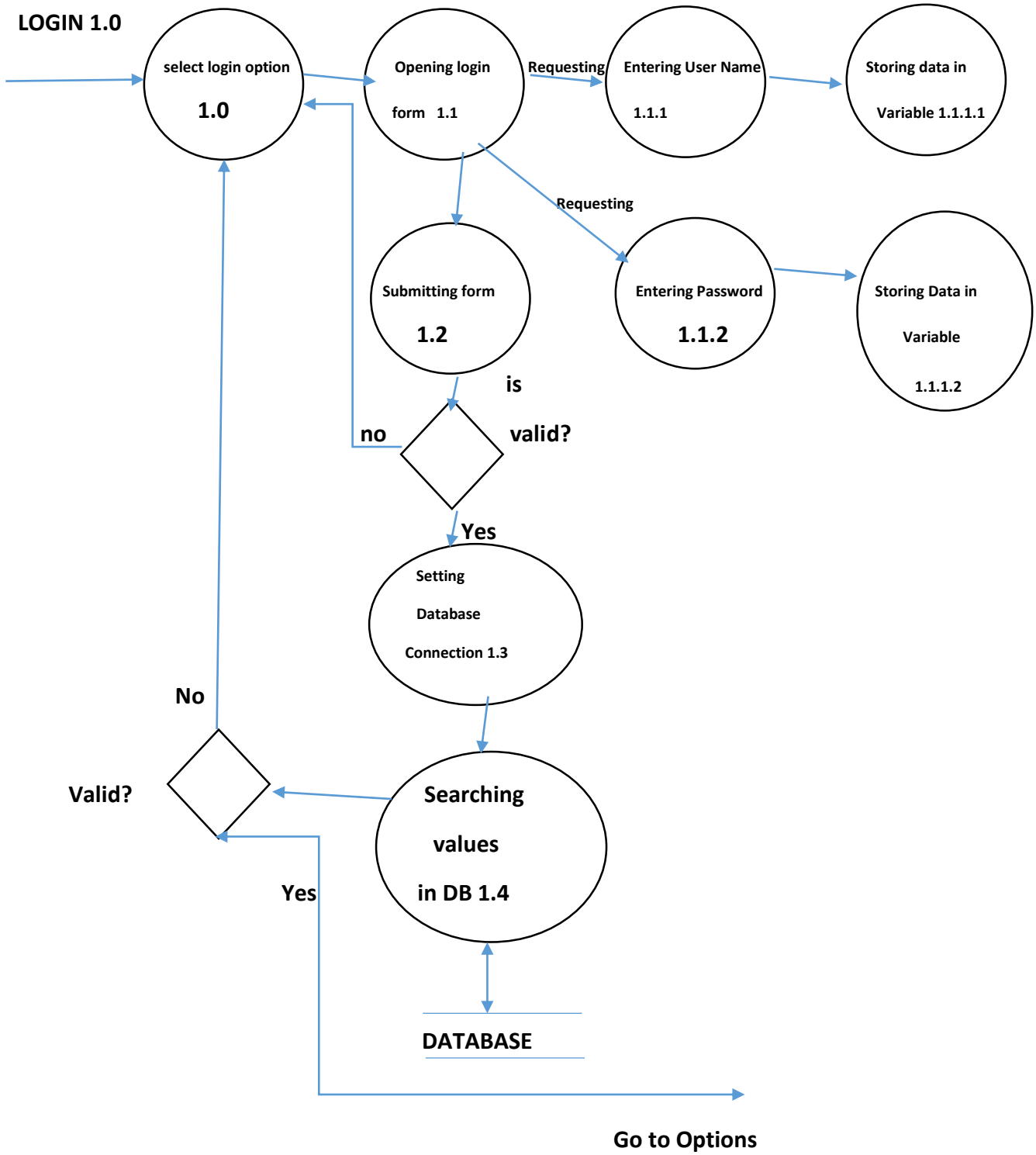





EMPLOYEE
Login
1.0
Authenticates
options
4.0

LEVEL 1

LOGIN 1.0



LEVEL 2.0


options 2.0
Proceed to Create Company 2.1
Entering Company ID 2.1.1
Storing Value in Variable 2.1.1.1
Entering Business ID 2.1. 2
Storing Value in Variable 2.1.2.1
Entering Company name 2.1.3
Storing Value in Variable 2.1.3.1
Entering Country. 2.1.4
Storing Value in Variable 2.1.4.1
Entering State 2.1.5
Storing value in Variable 2.1.5.1
Entering City, zipcode, EmailID, Phone Number 2.1.6
Storing Values in Variables 2.1.6.1
Submitting form
E
Setting Database Connection
Storing Values in Database
DATABASE
LOGOUT


OPTIONS 2.0
Proceed to Create HR 2.2
Entering Employee ID 2.2.1
Storing Value in Variable 2.2.1.1
Entering Business ID 2.1. 2
Storing Value in Variable 2.1.2.1
Submitting form
Entering Company name 2.1.3
Storing Value in Variable 2.1.3.1
E
Setting Database Connection
Entering Department Designation2.1.4
Storing Value in Variables 2.1.4.1
Entering username Passoword, 2.1.5
Storing value in Variables 2.1.5.1
Storing values In database
Entering First, Middle, LastNames, Gender 2.1.6
Storing Values in Variables 2.1.6.1
DATABASE
Entering DateofBirth Phone Email 2.1.7
Storing Values in Variables 2.1.7.1
LOGOUT


OPTIONS 2.0
Proceed to update company 2.3
Entering Company ID 2.3.1
Storing Value in Variable 2.3.1.1
Entering Business ID 2.3. 2
Storing Value in Variable 2.3.2.1
Entering Company name 2.3.3
Storing Value in Variable 2.3.3.1
Submitting form
E
Entering Country. 2.3.4
Storing Value in Variable 2.3.4.1
Setting Database Connection
Entering State 2.3.5
Storing value in Variable 2.3.5.1
Updating Values in Database
Entering City, zipcode, EmailID, Phone Number 2.3.6
Storing Values in Variables 2.3.6.1
DATABASE
LOGOUT


OPTIONS 2.0
Proceed to update HR 2.4
Entering Employee ID 2.4.1
Storing Value in Variable 2.4.1.1
Entering Business ID 2.4. 2
Storing Value in Variable 2.4.2.1
Submitting form
Entering Company name 2.4.3
Storing Value in Variable 2.4.3.1
E
Setting Database Connection
Entering Department 2.4.4
Storing Value in Variable 2.4.4.1
Entering username Password, 2.4.5
Storing value in Variables 2.4.5.1
updating values In database
Entering First, Middle, Last Name, Gender 2.4.6
Storing Values in Variables 2.1.6.1
DATABASE
Entering Date of Birth, Phone Email 2.4.7
Storing Values in Variables 2.4.7.1
LOGOUT

LEVEL 3.0


OPTIONS 3.0
Proceed to Create Employee 3.1
Entering Employee ID 3.1.1
Storing Value in Variable 3.1.1.1
Entering Company ID 3.1. 2
Storing Value in Variable 3.1.2.1
Submitting form
Entering Company name 3.1.3
Storing Value in Variable 3.1.3.1
E
Setting Database Connection
Entering Department 3.1.4
Storing Value in Variable 3.1.4.1
Entering username Password, 3.1.5
Storing value in Variables 3.1.5.1
Storing values In database
Entering First, Middle, Last Names, Gender 3.1.6
Storing Values in Variables 3.1.6.1
DATABASE
Entering Date of Birth Phone Email 3.1.7
Storing Values in Variables 3.1.7.1
LOGOUT


LEVEL 4.0
update Employee ID 2.4
Update Employee ID 2.4.1
Storing Value in Variable 2.4.1.1
Update Business ID 2.4. 2
Storing Value in Variable 2.4.2.1
Submitting form
Update Company name 2.4.3
Storing Value in Variable 2.4.3.1
E
Setting Database Connection
Update Department. 2.4.4
Storing Value in Variable 2.4.4.1
Update username Password, 2.4.5
Storing values in Variables 2.4.5.1
updating values In database
Update First, Middle, Last Name, Gender 2.4.6
Storing Values in Variables 2.1.6.1
DATABASE
Update Date of Birth, Phone Email 2.4.7
Storing Values in Variables 2.4.7.1
LOGOUT

8.INVENTORY OF AUTHORIZED DEVICES

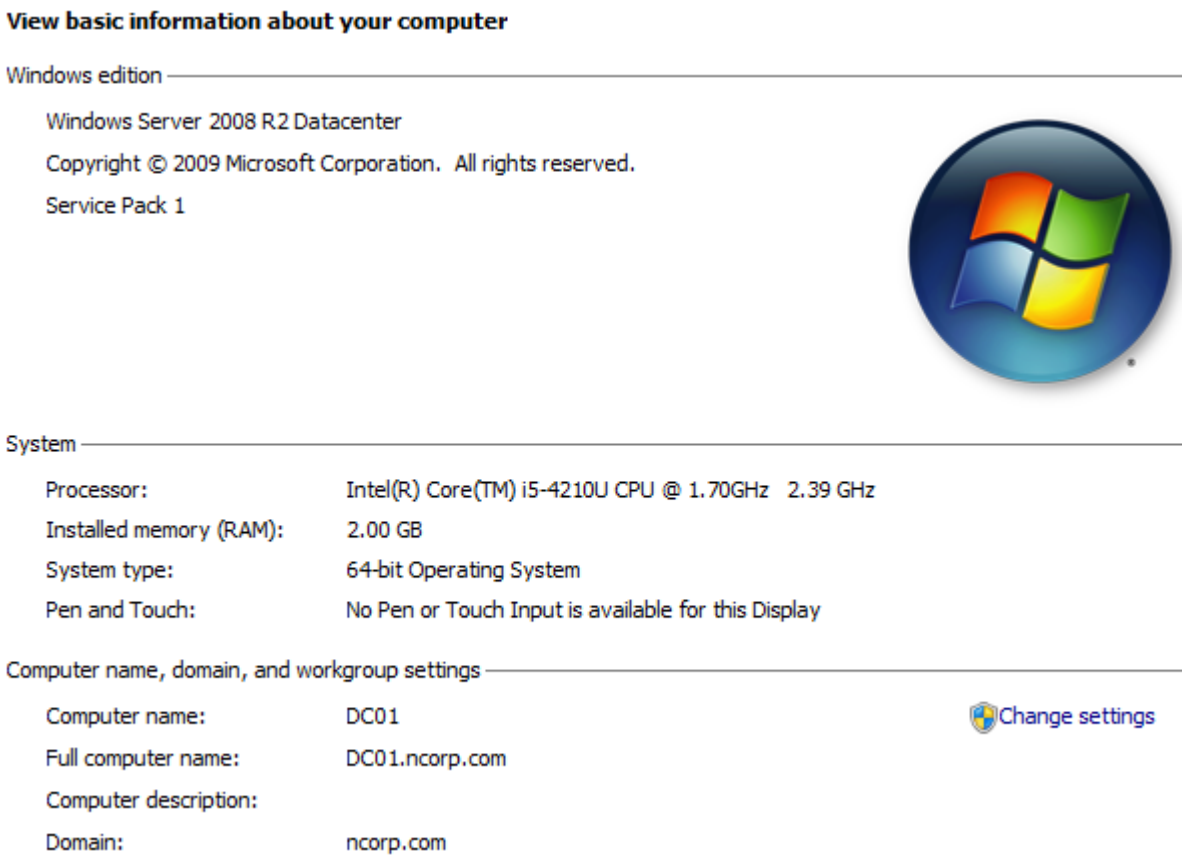
IP ADDRESS	SYSTEM TYPE	OS
192.168.1.7	VIRTUAL MACHINE FOR DOMAIN CONTROLLER	WINDOWS SERVER 2008R2 DATA CENTER
192.168.1.15	VIRTUAL MACHINE FOR CERTIFICATE AUTHORITY	WINDOWS SERVER 2008R2 DATA CENTER
192.168.1.12	VIRTUAL MACHINE FOR WEB SERVER AND APPLICATION DEVELOPMENT	WINDOWS SERVER 2008R2 DATA CENTER
192.168.1.7	VIRTUAL MACHINE FOR VULNERABILITY ASSESSMENT	KALI LINUX
	HOST MACHINE FOR ALL VIRTUAL MACHINES	WINDOWS 8.1

8.1 VIRTUAL MACHINES

INSTALLATION OF VIRTUAL MACHINES

8.1.1 WINDOWS SERVER 2008 R2 DATA CENTER -DOMAIN CONTROLLER

Configuration:



8.1.2 WINDOWS SERVER 2008R2 DATA CENTER – WEB SERVER, DNS SERVER

Configuration:

Windows edition

Windows Server 2008 R2 Enterprise

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

Processor:	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz 2.39 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	SRV1	Change settings
Full computer name:	SRV1.ncorp.com	
Computer description:		
Domain:	ncorp.com	

8.1.3 WINDOWS SERVER 2008R2 DATA CENTER – CERTIFICATE AUTHORITY

Configuration:

Windows edition

Windows Server 2008 R2 Standard
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1

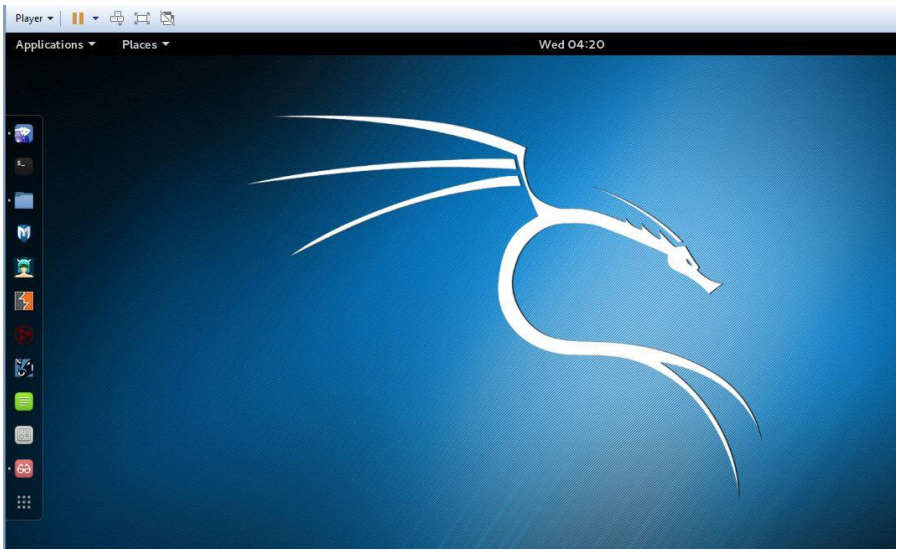
System

Processor:	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz 2.39 GHz
Installed memory (RAM):	2.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

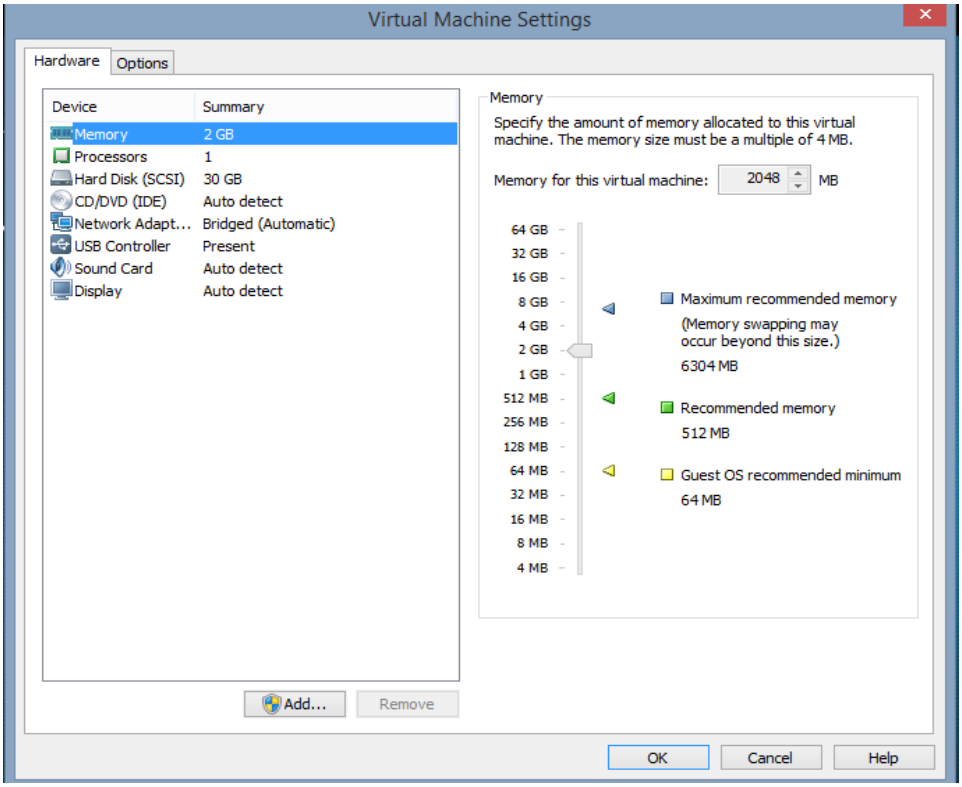
Computer name, domain, and workgroup settings

Computer name:	CA01	Change settings
Full computer name:	CA01.ncorp.com	
Computer description:		
Domain:	ncorp.com	

8.1.4 KALI LINUX – VULNERABILITY ASSESMENTS



Configuration:



8.2 WINDOWS 8.1 – HOST MACHINE WITH VIRTUAL MACHINES AND NETWORK ADAPTERS

Configuration:

View basic information about your computer

Windows edition

Windows 8.1

© 2013 Microsoft Corporation. All rights reserved.

Get more features with a new edition of Windows

System

Processor:	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz 2.40 GHz
Installed memory (RAM):	8.00 GB (7.88 GB usable)
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	Full Windows Touch Support with 10 Touch Points

Support Information

Computer name, domain, and workgroup settings

Computer name:	R0SH9N
Full computer name:	R0SH9N
Computer description:	
Workgroup:	WORKGROUP

Change settings

Windows activation

Windows is activated Read the Microsoft Software License Terms

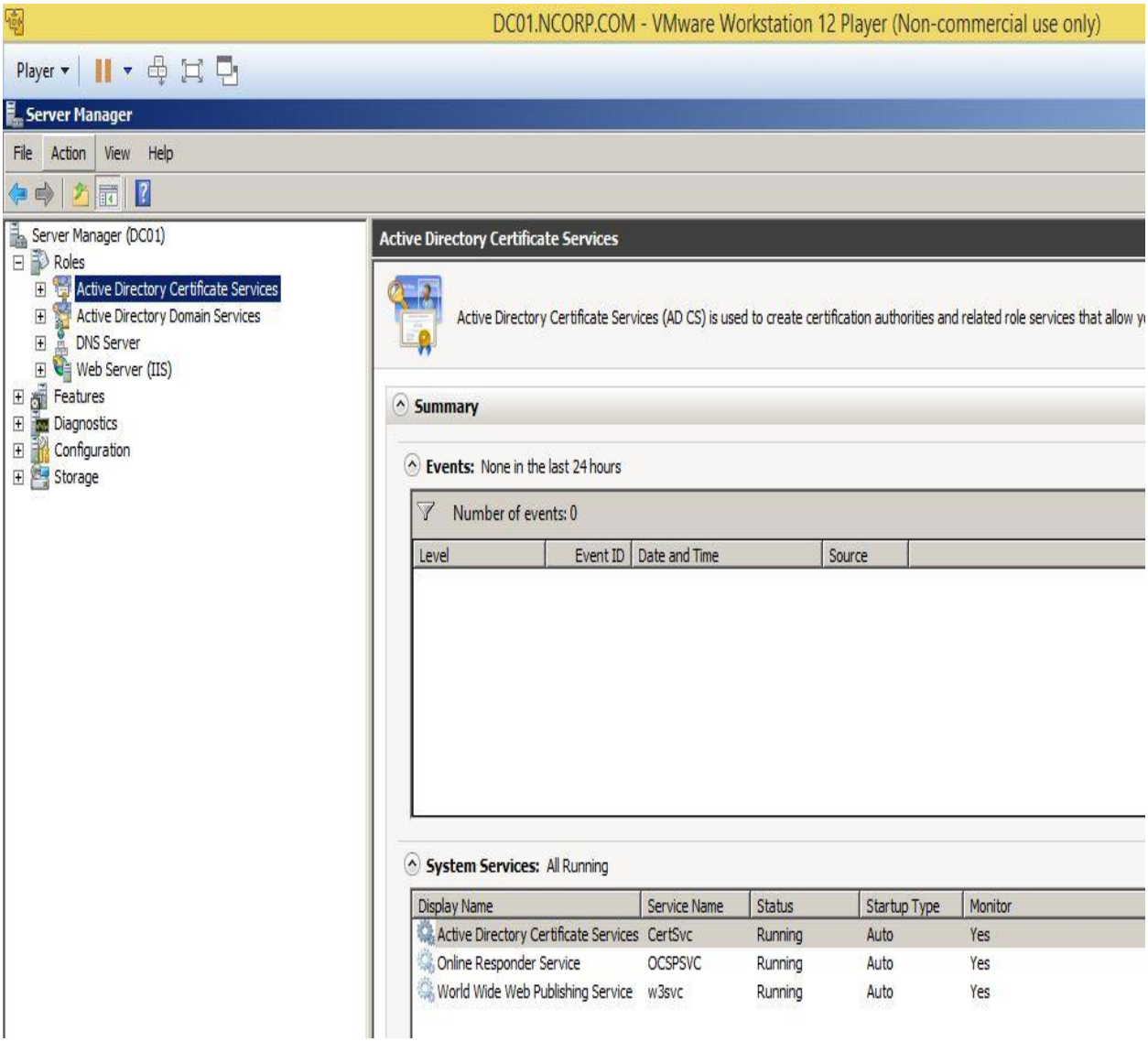
Product ID: 00258-61594-03355-AAOEM

Change product key

9.0 DOMAIN CONTROLLER

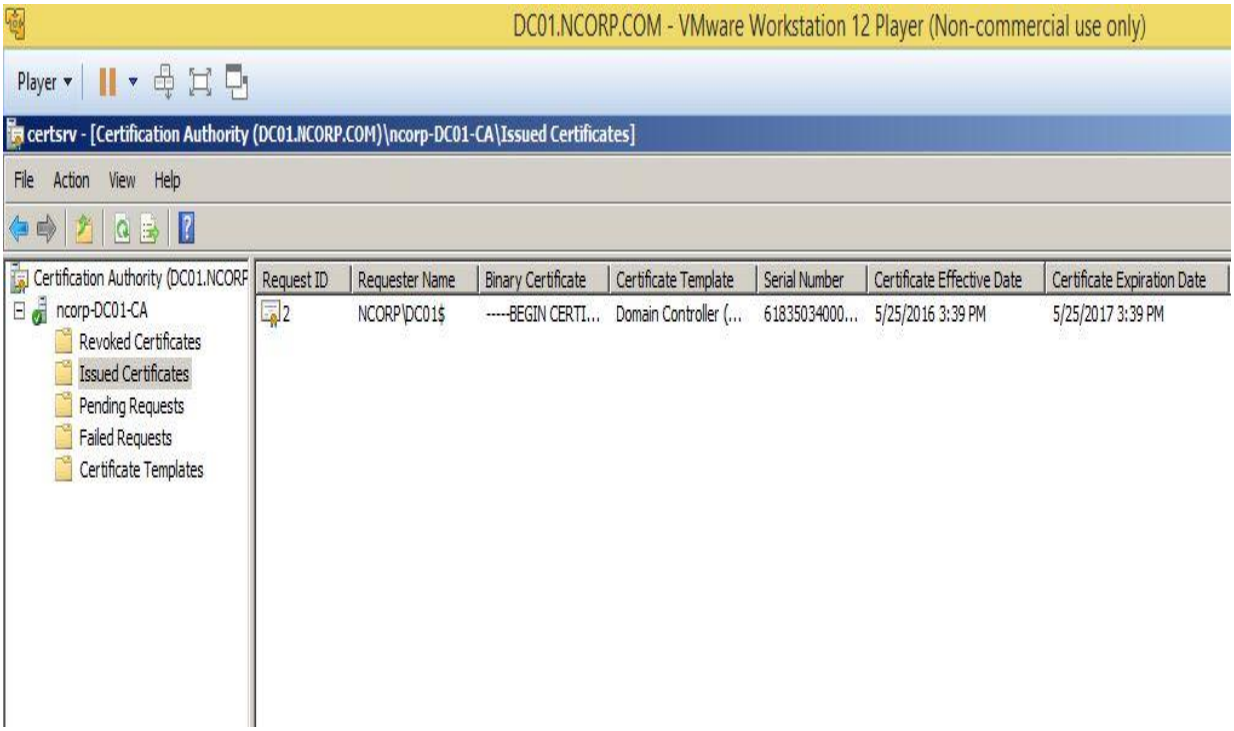
9.1 Roles Created in the Domain Controller

1) **Active Directory Certificate Service**
2) **Active Directory Domain Service**
3) **DNS Server**
4) **Web Server**

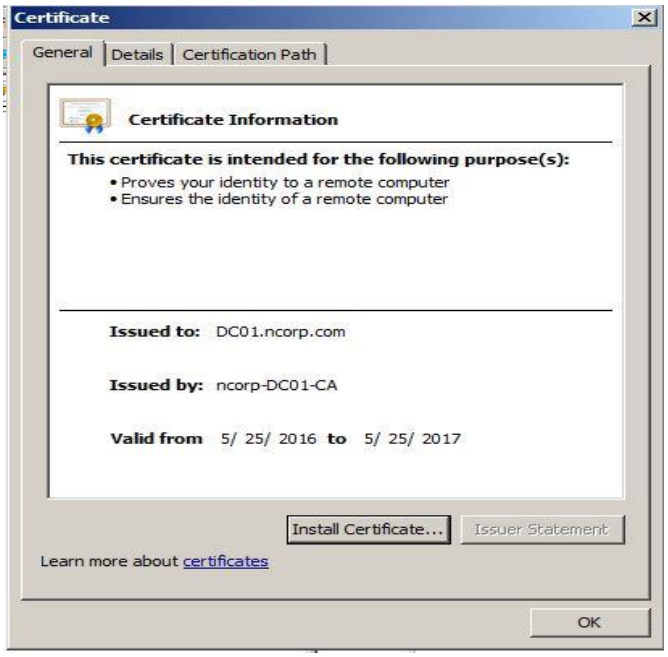


9.2 ROLES CREATED IN CERTIFICATE AUTHORITY SERVER

Active Directory Certificate Services:



9.3 Certificate Issued

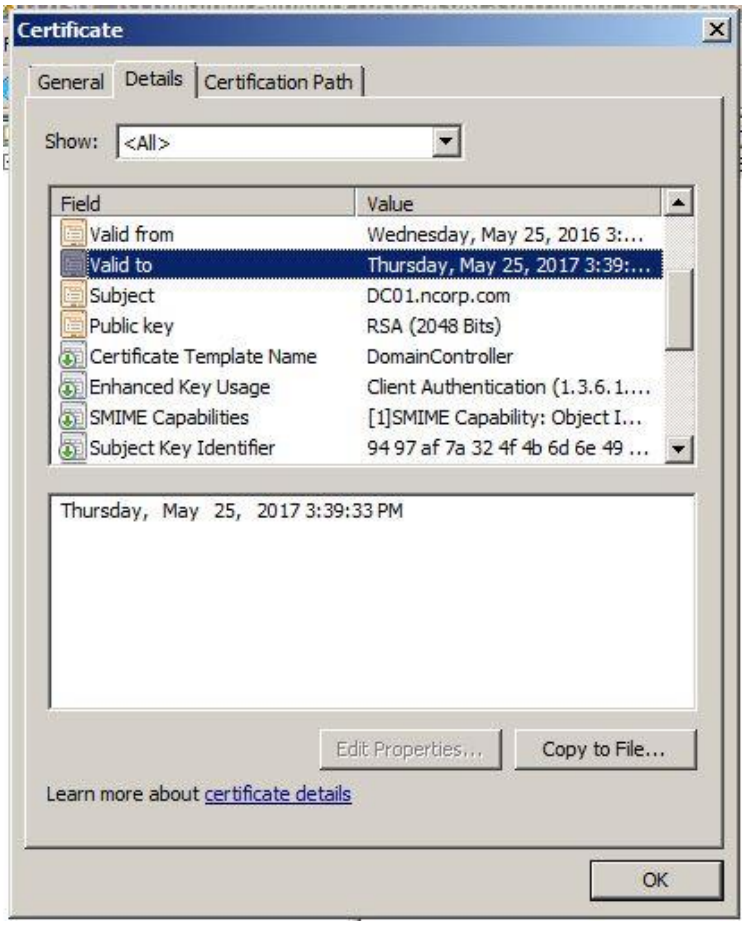


9.3.1 Details of the RSA public key :

RSA Public Key

```
30 82 01 0a 02 82 01 01 00 b1 65 4c ad 05 61 12 f3 af dd 17 5e
5c 1e 95 9d a0 4c 79 30 10 29 a2 c0 f1 05 73 65 4e d4 3e 79 83
50 46 d4 cf 59 18 47 6a bc d0 0d 69 bc 0c e7 80 0c 4d 99 78 21
18 6d ef 90 f6 a3 8a 23 e4 15 0b 97 41 68 10 75 99 bf ee 1b af
8d 0c 5c 5e 1c 3f 20 88 5f 33 ca 26 31 87 ee c6 25 40 c6 79 e8
46 f9 6c f5 93 22 fb 85 33 d5 ae 75 3f fb 27 78 01 5c b8 0d d3
02 57 b5 8c 0d c2 cc fa 90 28 d6 fb 43 67 74 46 c2 88 fb d7 e0
e3 63 ac f5 f1 e6 2c 8a 2b 66 22 90 31 9e 68 ec 05 02 26 d9 78
39 19 70 f8 81 7c d1 ce 96 4a d6 12 69 1e ce e5 0e 81 79 9e 51
99 38 27 17 6d 54 88 1c 8e 45 fb 4e a3 c9 95 f4 f1 89 72 3b 25
62 24 db 12 a6 93 5b 66 ce ed 49 8f 74 de 0a ac c2 4a 2d d2 74
99 f8 ee 5c 3c 6f df 23 f6 26 6f 70 65 27 3d 77 60 78 bc e9 0c
c5 4a a6 41 90 33 6a b6 c8 06 38 2e 55 02 03 01 00 01
```

9.3.2 Certificate Validity:



9.3.3 Certificate Path

9.3.4 DNS ALIAS

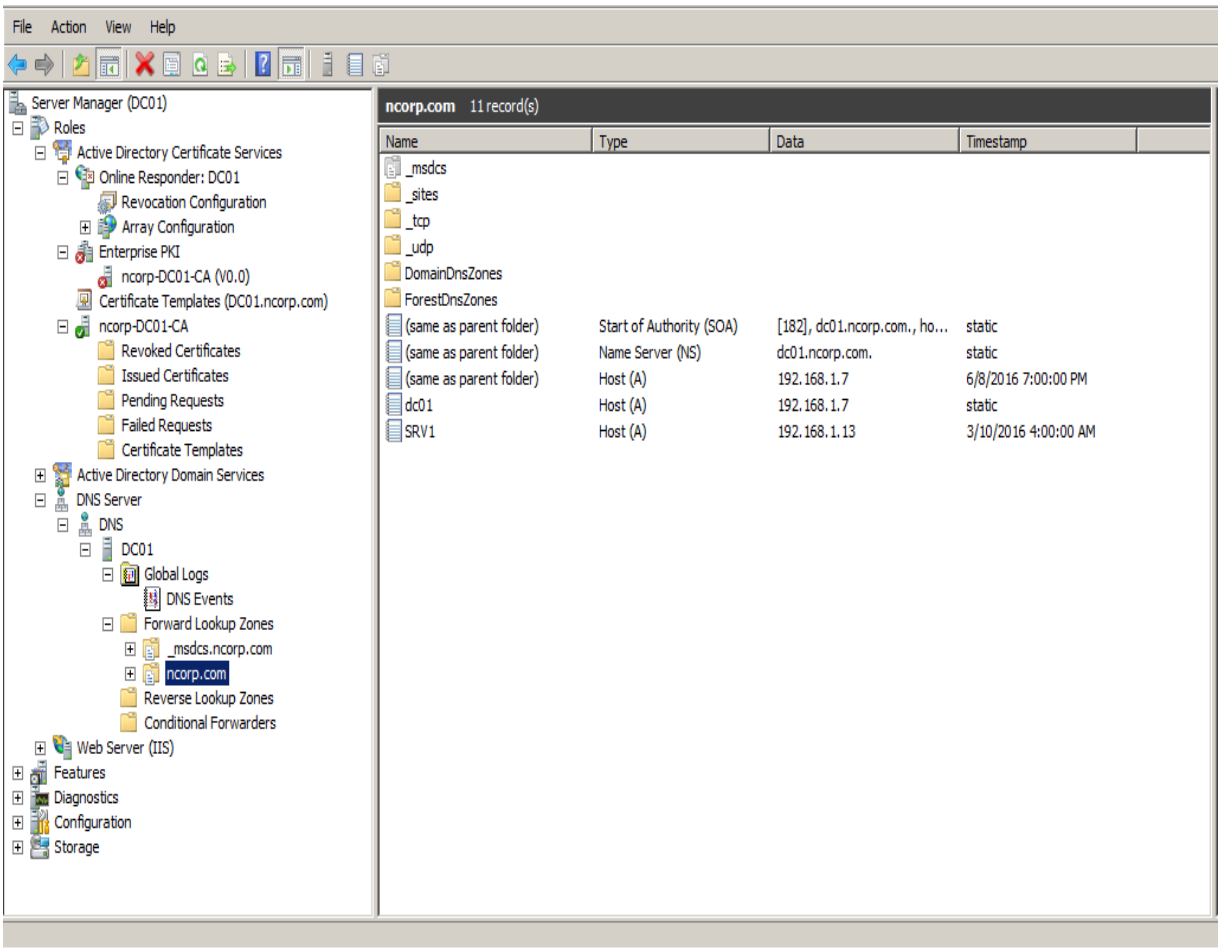
53AC411C-6124-4CB3-8804-C57C8E3304A2._msdcs.ncorp.com

9.4 DNS Server

Domain Controller Host DNS Record

SRV1 Host DNS Record created in DC01 Server pointed it to 192.168.1.13

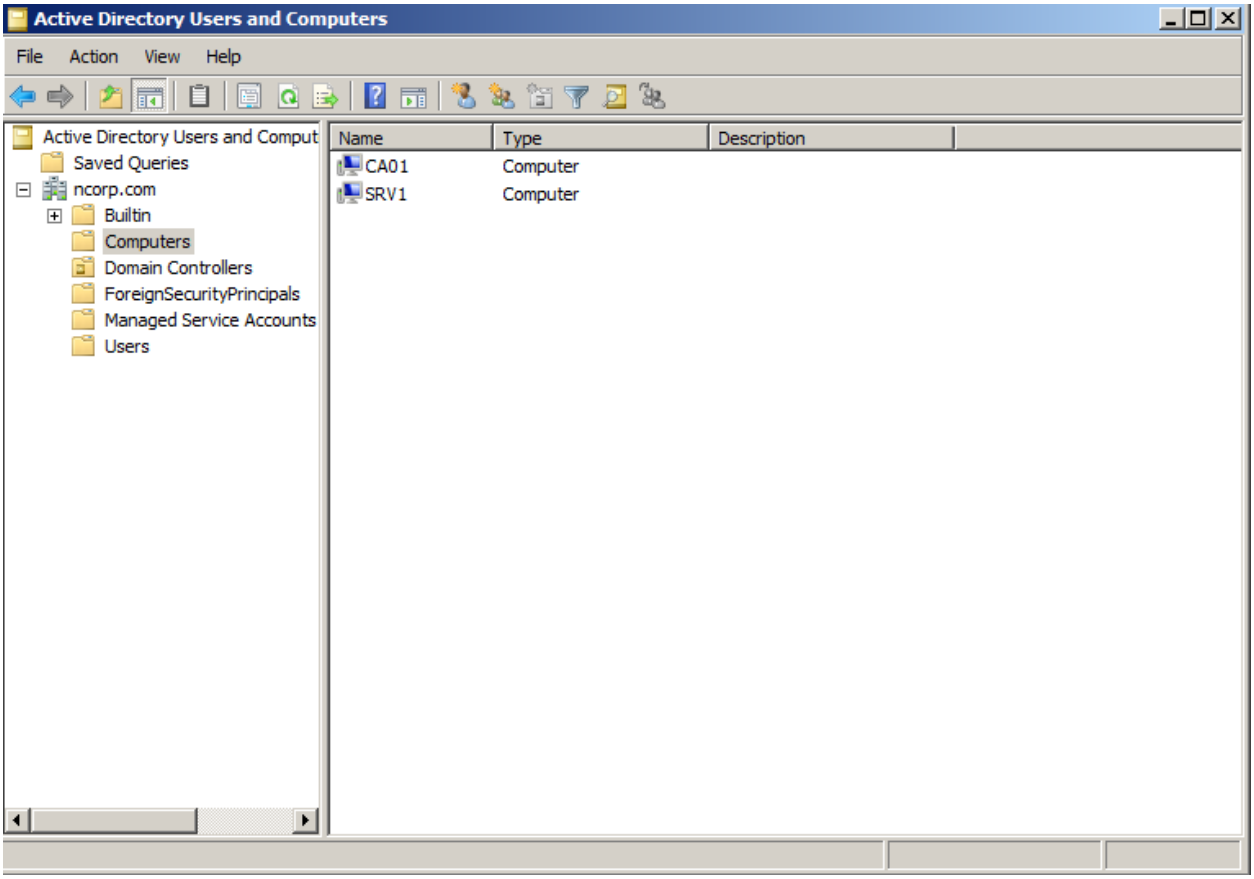
DNS linking and port binding were done in this phase.


File Action View Help
Server Manager (DC01)
Roles
Active Directory Certificate Services
Online Responder: DC01
Revocation Configuration
Array Configuration
Enterprise PKI
ncorp-DC01-CA (V0.0)
Certificate Templates (DC01.ncorp.com)
ncorp-DC01-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Active Directory Domain Services
DNS Server
DNS
DC01
Global Logs
DNS Events
Forward Lookup Zones
_msdcs.ncorp.com
ncorp.com
Reverse Lookup Zones
Conditional Forwarders
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
ncorp.com 11 record(s)
Name Type Data Timestamp
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(same as parent folder) Start of Authority (SOA) [182], dc01.ncorp.com., ho... static
(same as parent folder) Name Server (NS) dc01.ncorp.com. static
(same as parent folder) Host (A) 192.168.1.7 6/8/2016 7:00:00 PM
dc01 Host (A) 192.168.1.7 static
SRV1 Host (A) 192.168.1.13 3/10/2016 4:00:00 AM

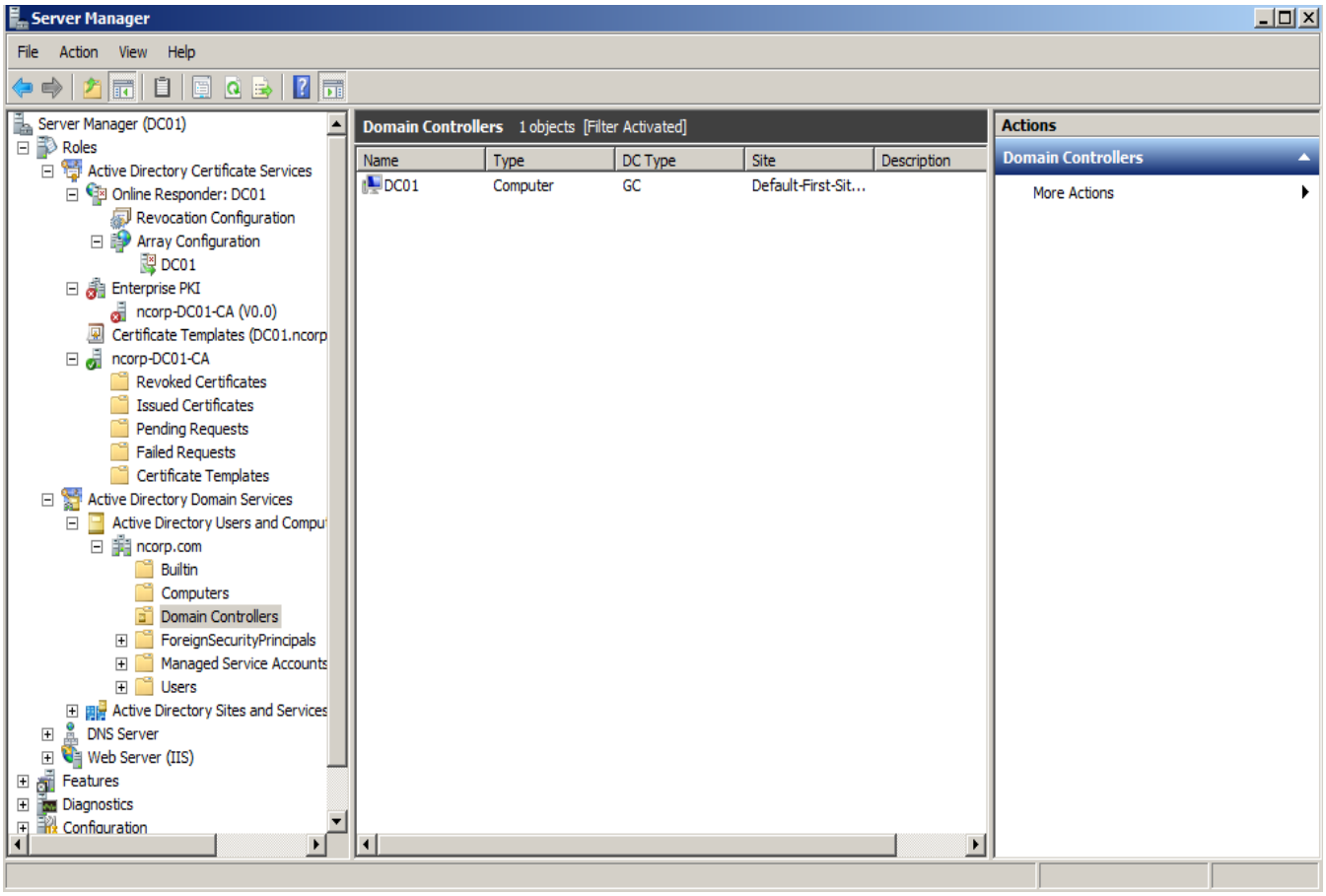
9.5 ACTIVE DIRECTORY USERS AND COMPUTERS

9.5.1 Active Directory

Users and Computers



9.5.2 Domain Controller: DC01

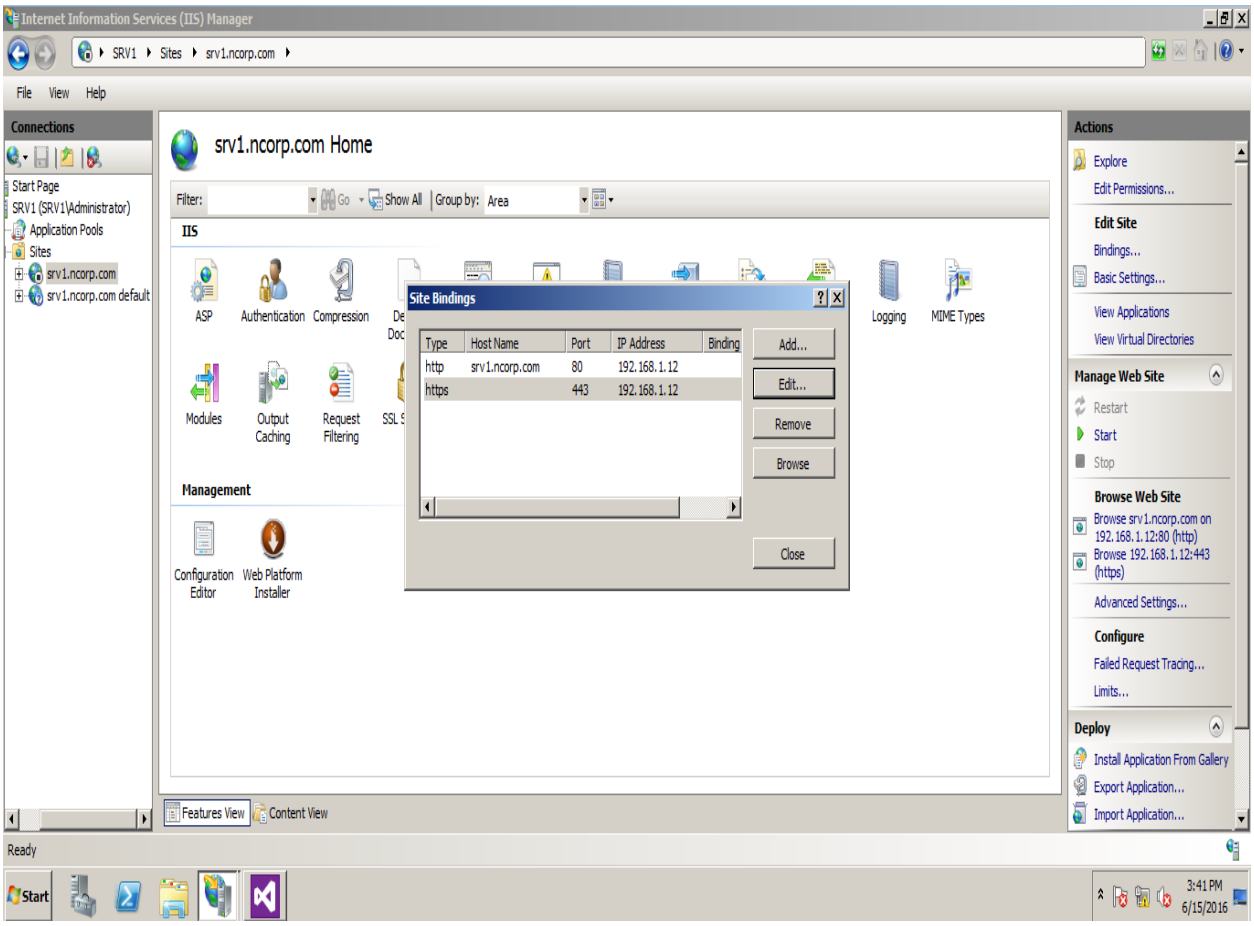


9.6 IIS APPLICATION BINDING

Binding the web application to port 80 and port 443 is done in this phase

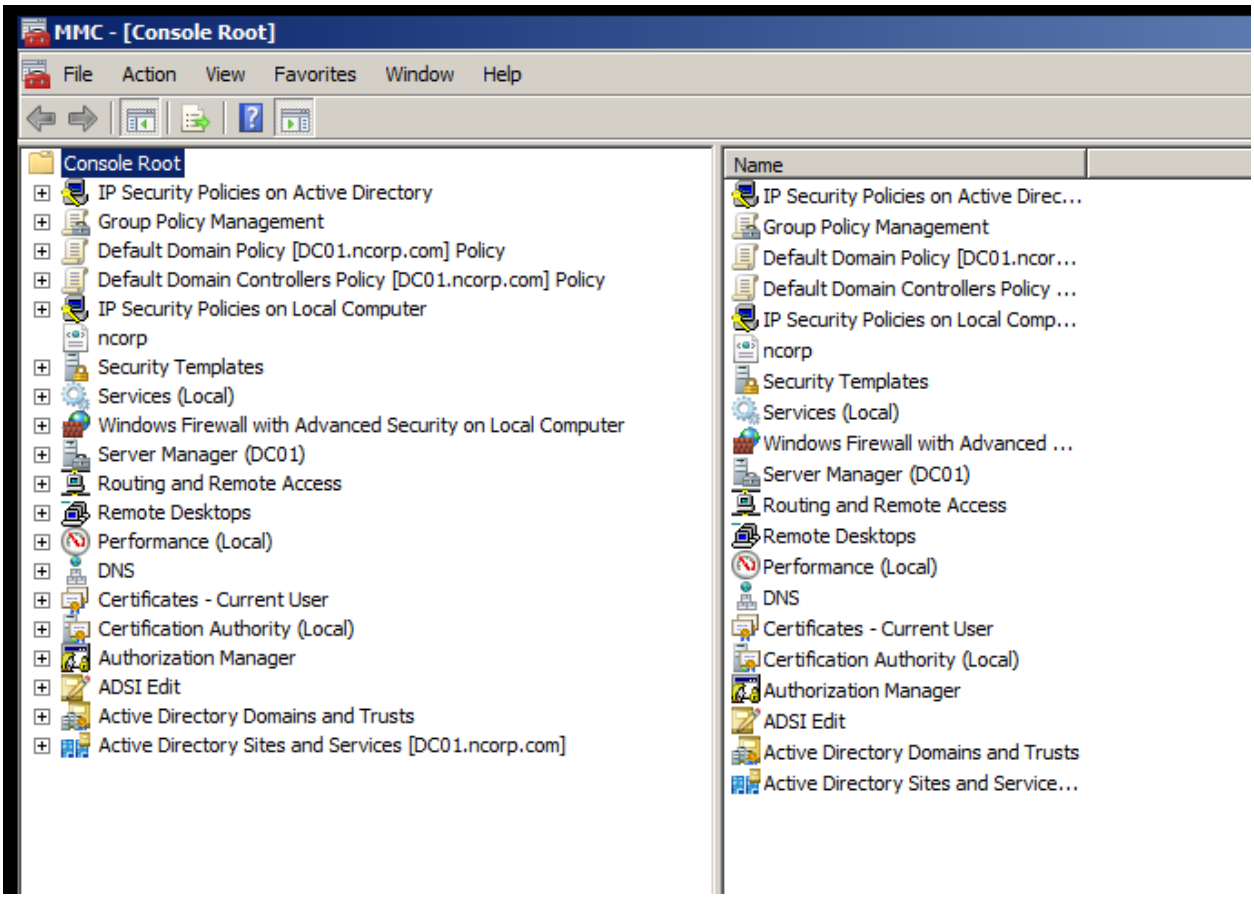
Port 80 for http website

Port 443 for https site



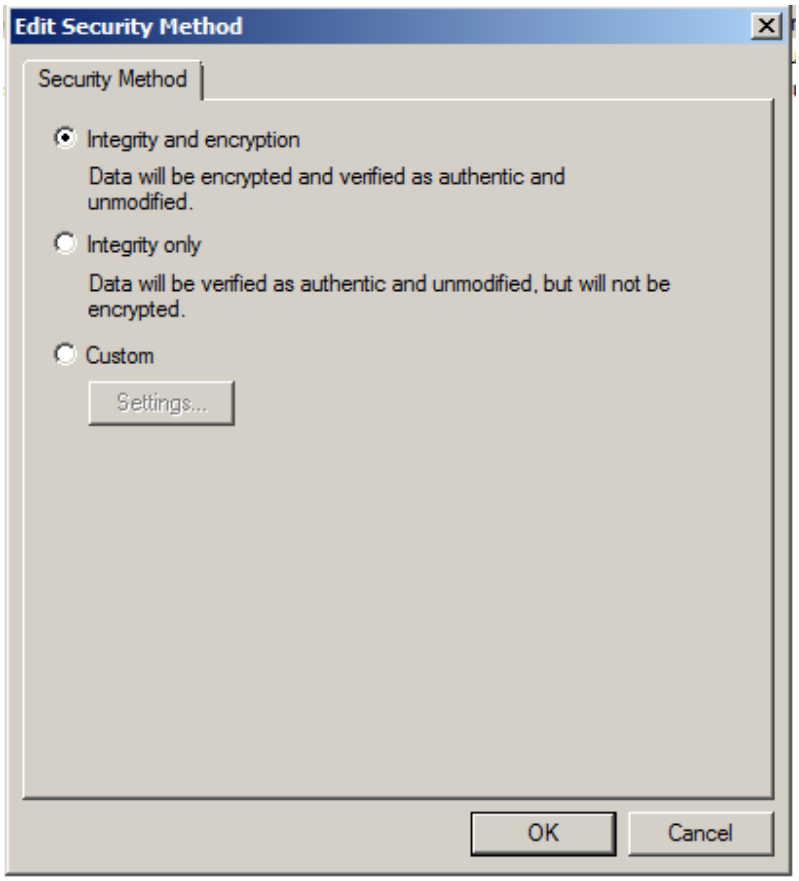
10. MY MANAGEMENT CONSOLE

I've created my management console where I can manage the set of policies and procedures in THE FQDN ncorp.com

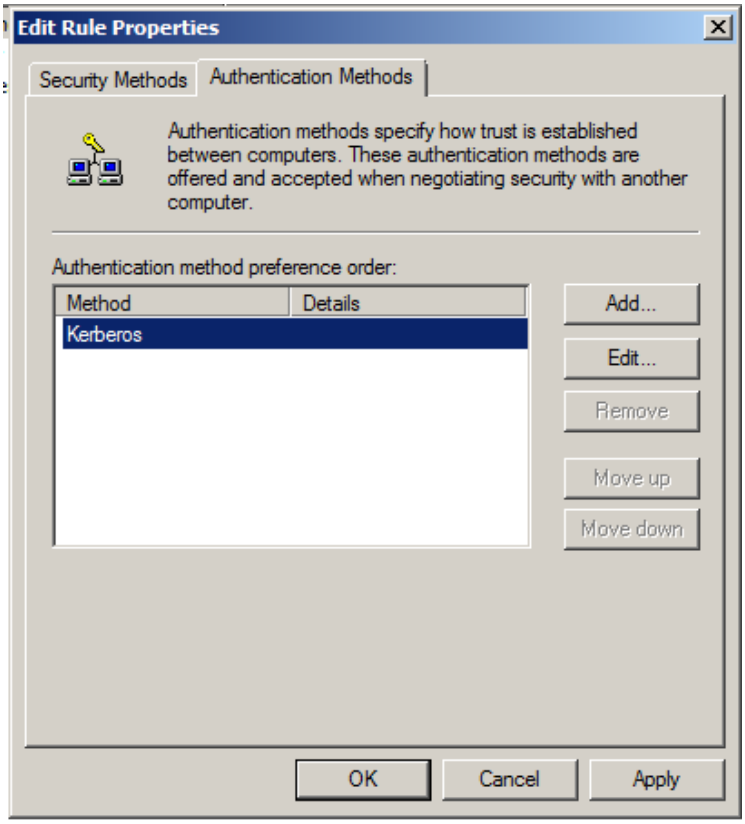


10.1 IP SECURITY POLICIES

Client Security Methods: In this process I'm choosing to encrypt the Data and making it authentic and unmodified!

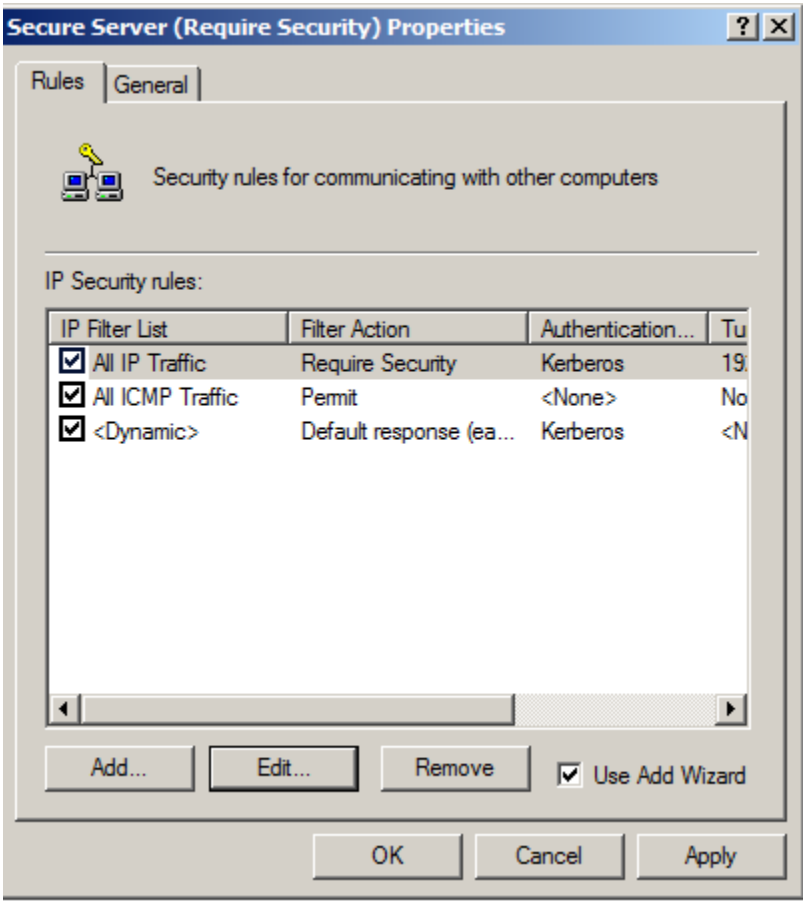


Authentication methods:

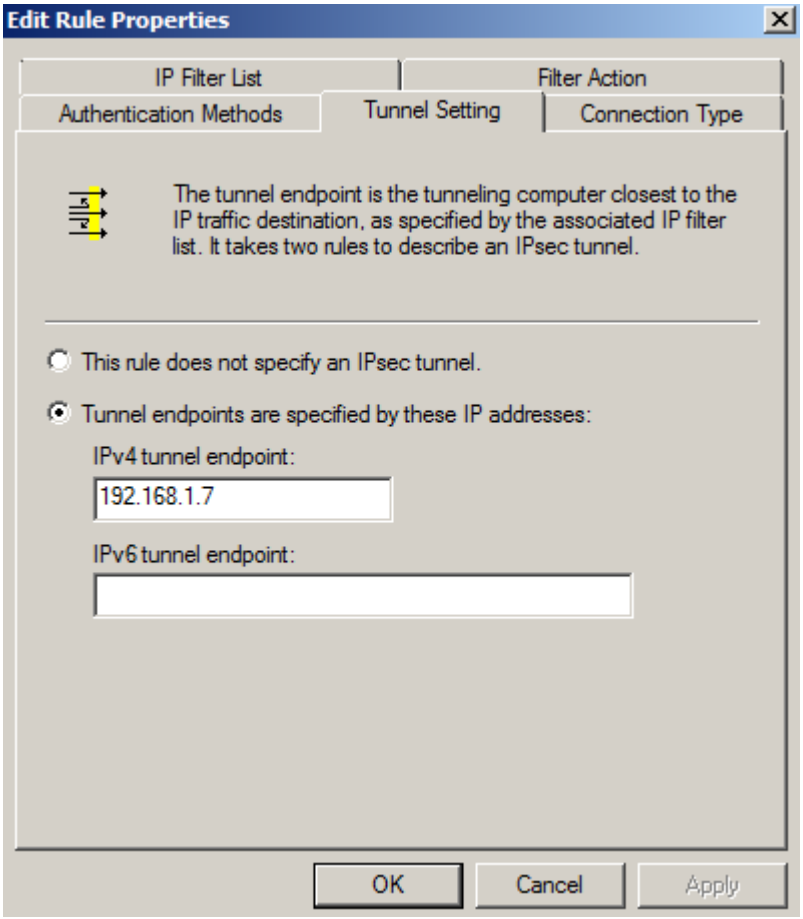


10.1.1 Secure Server

In this process, I am configuring the Kerberos authentication to the endpoint 192.168.1.12 IPSec Tunneling is done here. This IPSec tunneling is applicable to all the Network connections.

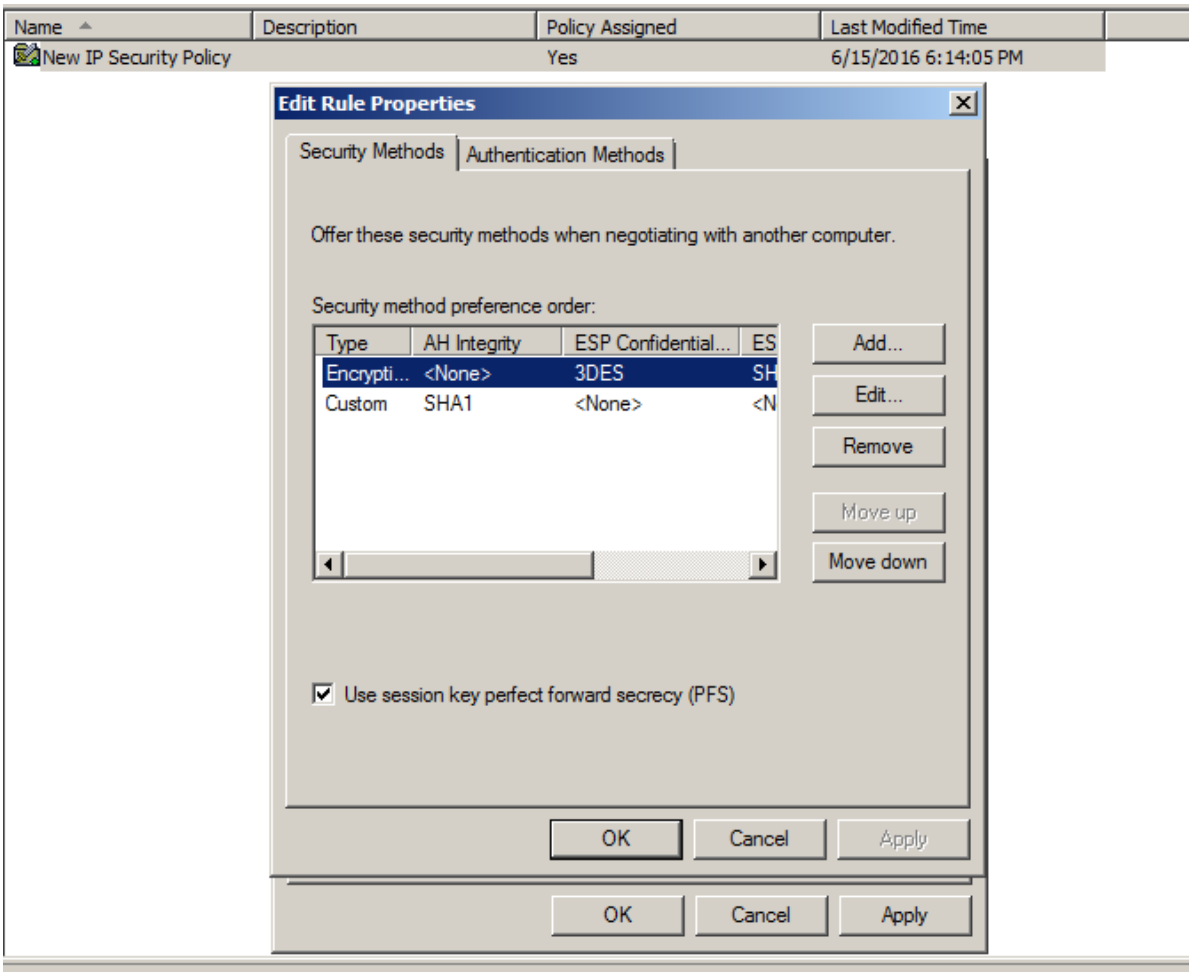


10.1.2 Secure Server End Rule Properties

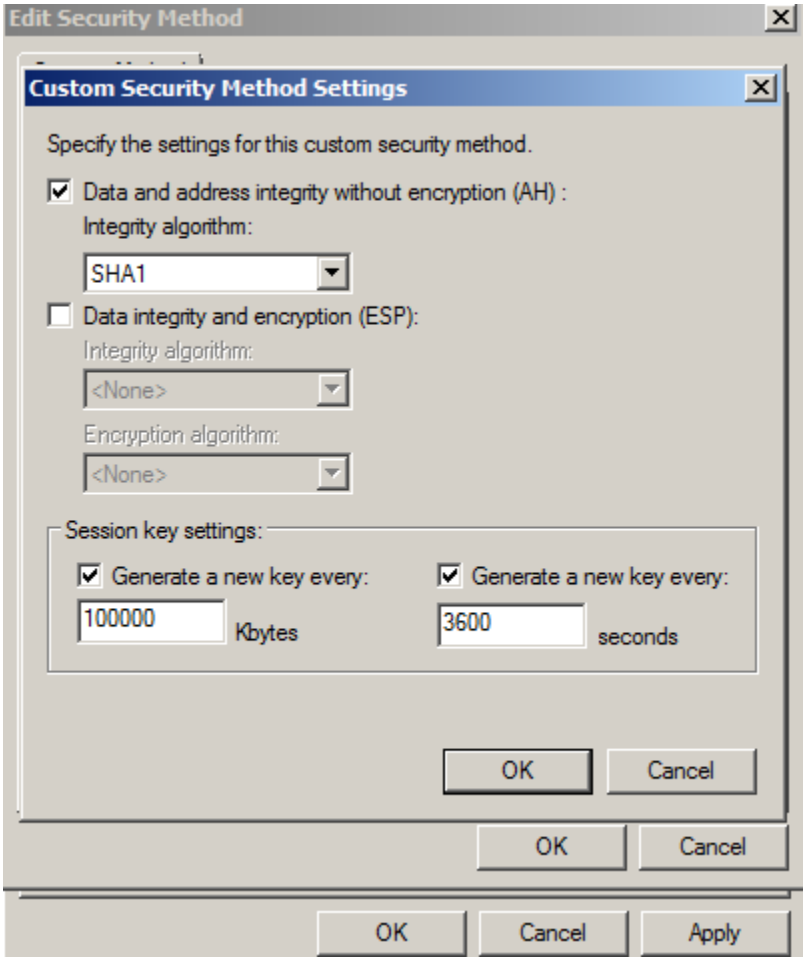


10.2 IP SECURITY POLICIES ON LOCAL COMPUTER

I've created a new IPSec policy for the local computer



I’m using SHA1 integrity algorithm to generate a new key after every 10000Kbytes and after every 3600 Seconds.



10.3 GROUP POLICY MANAGEMENT

10.3.1 Password age: I'm setting it to 30 days.

10.3.2 Account lockout threshold: Lockout duration is 2minutes for 5 invalid logon attempts. Account lockout will reset after 2 minutes.

Policy	Policy Setting
Account lockout duration	2 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	2 minutes

10.3.3 Audit Account logon Events

This security setting determines whether the OS audits each time this computer validates an account's credentials.

Account logon events are generated whenever a computer validates the credentials of an account for which it is authoritative. Domain members and non-domain-joined machines are authoritative for their local accounts; domain controllers are all authoritative for accounts in the domain. Credential validation may be in support of a local logon, or, in the case of an Active Directory domain account on a domain controller, may be in support of a logon to another computer. Credential validation is stateless so there is no corresponding logoff event for account logon events.

If this policy setting is defined, the administrator can specify whether to audit only successes, only failures, both successes and failures, or to not audit these events at all (i.e. neither successes nor failures).

10.3.4 Audit logon events

This security setting determines whether the OS audits each instance of a user attempting to log on to or to log off to this computer.

Log off events are generated whenever a logged on user account's logon session is terminated. If this policy setting is defined, the administrator can specify whether to audit only successes, only failures, both successes and failures, or to not audit these events at all (i.e. neither successes nor failures).

Default values on Client editions:

Logon: Success

Logoff: Success

Account Lockout: Success

IPsec Main Mode: No Auditing

IPsec Quick Mode: No Auditing

IPsec Extended Mode: No Auditing

Special Logon: Success

Other Logon/Logoff Events: No Auditing

Network Policy Server: Success, Failure

10.3.5 Audit system events

This security setting determines whether the OS audits any of the following events:

• Attempted system time change

• Attempted security system startup or shutdown

• Attempt to load extensible authentication components

• Loss of audited events due to auditing system failure

• Security log size exceeding a configurable warning threshold level.

If this policy setting is defined, the administrator can specify whether to audit only successes, only failures, both successes and failures, or to not audit these events at all (i.e. neither successes nor failures).

If Success auditing is enabled, an audit entry is generated each time the OS performs one of these activities successfully.

If Failure auditing is enabled, an audit entry is generated each time the OS attempts and fails to perform one of these activities.

Default:

Security State Change Success

Security System Extension No Auditing

System Integrity Success, Failure

IPsec Driver No Auditing

Other System Events Success, Failure

10.3.6 Devices: Allowed to format and eject removable media

This security setting determines who is allowed to format and eject removable NTFS media.
This capability can be given to:

Administrators

Administrators and Interactive Users

Default: This policy is not defined and only Administrators have this ability.

11. VULNERABILITY ASSESSMENTS

12.OWASP ESAPI TESTING

12.1 VULNERABILITY MANAGEMENT

MEASURES TO MANAGE WITH SOME OF THE VULNERABILITIES LISTED IN ASSESSMENTS PHASE

12.1.1 Information Gathering & Conducting Search engine discovery and Reconnaissance for information leakage

The first step a hacker does is gathering information: **Reconnaissance and foot printing** followed by scanning and enumeration gaining access, maintaining access, covering tracks.

This testing technique pursues to see what type of information is leaked out by a company and how an attack might leverage the information.

As a counterterrorism measure to defend information gathering, I am providing security by setting a **group policy to block ICMP requests** from client machines. Setting this domain policy blocks ping messages to domain controller.

Connection Security Settings

Administrative Templates

Policy definitions (ADMX files) retrieved from the local machine.

Network/Network Connections/Windows Firewall/Domain Profile

Policy	Setting	Comment
Windows Firewall: Allow ICMP exceptions	Disabled	
Windows Firewall: Allow inbound remote administration exception	Disabled	
Windows Firewall: Protect all network connections	Enabled	

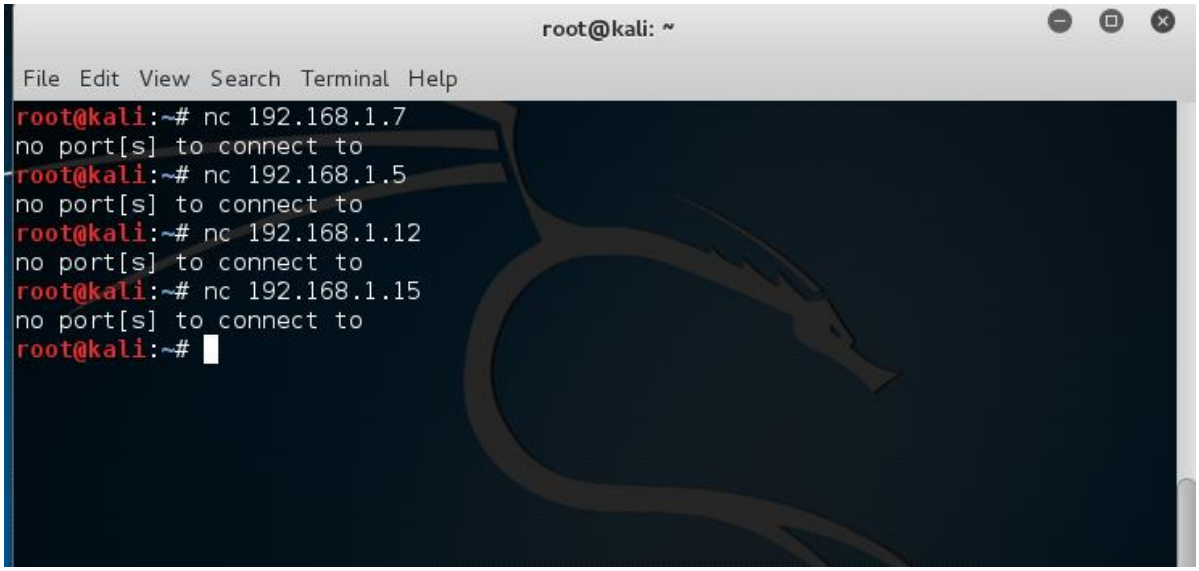
Network/Network Connections/Windows Firewall/Standard Profile

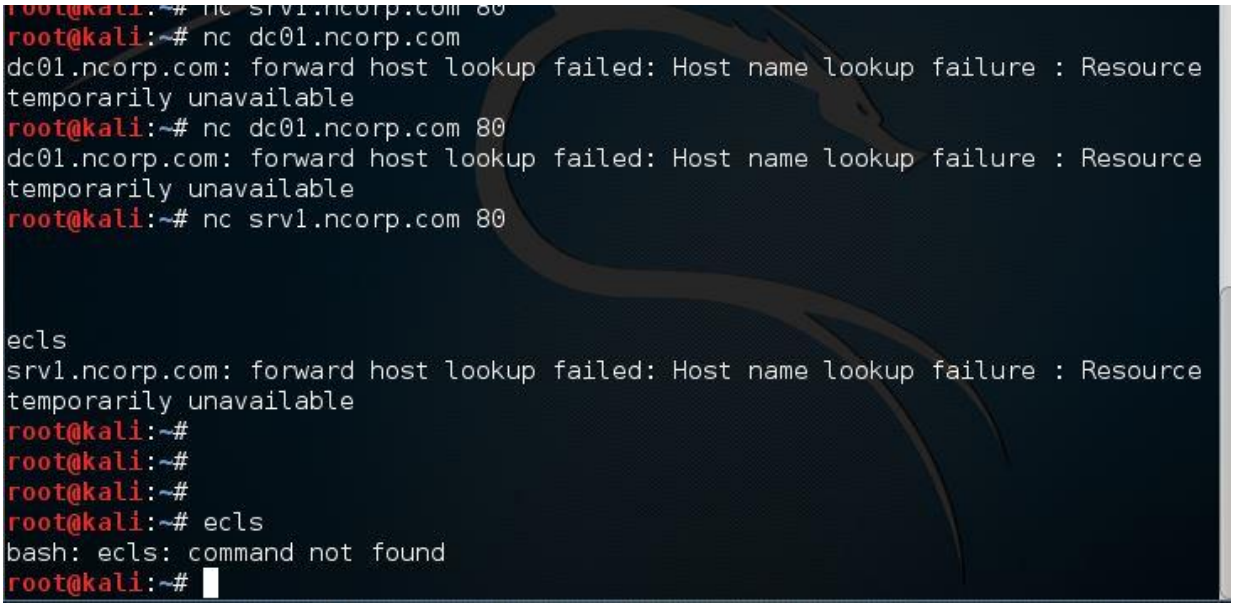
Policy	Setting	Comment
Windows Firewall: Protect all network connections	Enabled	

12.1.2 Fingerprint web server

- **Black Box testing**

From kali Linux, I tried to fingerprint the servers with: domain controller, web server, certificate authority configured. Ended up with the resultant screenshot posted below





12.1.3 Enumerate application on Webserver

As a Counterterrorism / security measure I filtered the ports & Disabled the reverse DNS lookup of 192.168.1.12,

Thus the result:

```
root@kali:~# nmap -PN -sT -sV -p0-65535 192.168.1.12

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-17 03:00 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.12
Host is up (0.0000030s latency).
All 65536 scanned ports on 192.168.1.12 are filtered

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.71 seconds
```

My security settings worked out. Enumerating the application on webserver is not possible with the current security settings.

12.1.4 Fingerprint web application:

The connection is refused due to the security settings I set in firewall i.e, to allow inbound traffic only if the connection is secured (i.e with Authentication)

```
root@kali:~# nc 192.168.1.5 443
(UNKNOWN) [192.168.1.5] 443 (https) : Connection refused
root@kali:~# nc 192.168.1.5 80
(UNKNOWN) [192.168.1.5] 80 (http) : Connection refused
root@kali:~# nc 192.168.1.5 21
(UNKNOWN) [192.168.1.5] 21 (ftp) : Connection refused
root@kali:~# nc 192.168.1.5 22
(UNKNOWN) [192.168.1.5] 22 (ssh) : Connection refused
```

12.1.5 Testing Identity Management

- ✓ **Test role definitions**

  In the web application, Admin, HR, Registrar, Employee Student roles are defined. All the tasks assigned to their roles were tested and executed.

- ✓ **Test Account provisioning process**

  The ping test from client machine to DC01 which refused to display results is one of the tests I performed to test the group policy functionality! It worked!

12.1.6 Authentication Testing

- ✓ **Login Authentication Testing**

  Example: **Test case:** In this context I'm used a test case if the username and password don't match with the user name and passwords in the Database then the application returns the label **"not a user"**

LOGIN FOR COMPANIES

UserName Admin

Password ••••

Login

not a user

12.1.7 Authorization Testing:

- ✓ Authorization testing is a concept of allowing access to resources only those who are permitted to use them. The application failed to restrict the access to some of the URLs.
- ✓ I'm still working on securing it by restricting URL access to unauthorized personnel
- ✓ Flaws with this web application: There are possibilities of Directory traversal attack!

12.1.8 Input Validation Testing:

As I intentionally didn't use validation controls, this web application is vulnerable to cross site scripting attacks (Both Client Side and Server side scripting attacks)

12.1.9 Database Testing:

Login controls, insert statement, update and delete statements that I used in the web application are the perfect examples of Database test cases. All the database queries were executed from the UI perspective.

Apart from this I did indexing(Querying) the database manually for inserting, updating and deleting the records into/from the database tables.

12.1.10 Client Side testing:

The UI & Database functionality is in a fully functional working mode.

13. FUTURE ENHANCEMENTS

To create EC2 Windows and Linux instances with Amazon web services to reduce the infrastructure and to improve application efficiency.

To redesign the Website with more security controls: Validation Controls

To Save the Web application data to Amazon DynamoDB

ESAPI Testing

To Review of Webserver metafiles for information leakage:

To Identify Application Entry points

To perform the Configuration and Deployment Management Testing

To redesign the application with sessions for Identity management for accessing the URL's

14. CONCLUSION

Security is not a state to be achieved. It's a continuous process.

REFERENCES

[1] Channel9.msdn.com

[2] www.Learnvisualstudio.net

[3] www.owasp.org