



SACRED HEART UNIVERSITY

SECURED VIRTUAL NETWORK – REPOSITORY FOR HUMAN RESOURCES

NCORP

NAME: NORI ROSHAN SHARMA

ADVISOR: Greg Kyrytschenko

COURSE: CS670IC

DATE June 17, 2016



SACRED HEART UNIVERSITY

ACKNOWLEDGEMENT

The satisfaction and Elation that accompany the successful completion of any task would be incomplete without the mention of the people who motivated me to do this work. It is my great privilege to express my gratitude and respect to all the professors of cyber security and computer science department at Sacred Heart University who guided me and inspired during the course work.

First and foremost, I would express my sincere gratitude to my project advisor **Professor. Greg Kyrytchenko** for providing the necessary guidance for the completion of my project.

I wish to express my sincere thanks and love to my **PARENTS** and my dearest friend **Mr. William Miklos** who rendered enough guidance right from my first semester at Sacred Heart University. I would also like to thank my friends **Mr. Asif and Mr. Naga Ramesh** for participating in project discussions which helped me a lot to do this work successfully.

INDEX

SNO	TITLE	PAGE NO
1.1	ABSTRACT	1
1.2	PRELIMINARY INVESTIGATION PHASE	1
1.2.1	SUMMARY OF PROBLEMS AND OPPORTUNITIES	1
1.3	SYSTEM INTERFACE	1
2.0	BUSINESS RULES	2
2.1	BUSINESS RULES IN A COMPANY	2
2.2	BUSINESS RULES IN A SCHOOL	2
3.0	BUSINESS PROCESS	2
4.0	SOFTWARE & HARDWARE USED	3
5.0	DATA COLLECTED BY THE SYSTEM	3
5.1	DATA STORAGE	9
5.2	PEOPLE INVOLVED	9
5.3	FUNCTIONAL DECOMPOSITION DIAGRAM	10
5.4	USE CASE DIAGRAMS	11
6.0	ENTITY RELATIONSHIP (ER) DIAGRAM	17
7.0	DATA FLOW DIAGRAMS	18
	LEVEL 0	18
	LEVEL 1	20
	LEVEL 2	21
	LEVEL 3	25
	LEVEL 4	26
8.0	INVENTORY OF AUTHORIZED DEVICES	36
8.1	VIRTUAL MACHINES	36
8.1.1	WINDOWS SERVER 2008 R2 DATA CENTER -DOMAIN CONTROLLER	36
8.1.2	WINDOWS SERVER 2008R2 DATA CENTER – WEB SERVER, DNS SERVER	37

8.1.3	WINDOWS SERVER 2008R2 DATA CENTER – CERTIFICATE AUTHORITY	38
8.1.4	KALI LINUX – VULNERABILITY ASSESSMENTS	38
8.2	WINDOWS 8.1 – HOST MACHINE	40
9.0	DOMAIN CONTROLLER	41
9.1	ROLES CREATED IN DOMAIN CONTROLLER	41
9.2	ROLES CREATED IN CERTIFICATE AUTHORITY SERVER	42
9.3	CERTIFICATES ISSUED	42
9.3.1	DETAILS OF THE RSA PUBLIC KEY	43
9.3.2	CERTIFICATE VALIDITY	43
9.3.3	CERTIFICATE PATH	44
9.3.4	DNS ALIAS	44
9.4	DNS SERVER	44
9.5	ACTIVE DIRECTORY USERS AND COMPUTERS	46
9.5.1	ACTIVE DIRECTORY	46
9.5.2	DOMAIN CONTROLLER: DC01	47
9.6	IIS APPLICATION BINDING	48
10.0	MY MANAGEMENT CONSOLE	49
10.1	IP SECURITY POLICIES	50
10.1.1	SECURE SERVER	52
10.1.2	SECURE SERVER END RULE PROPERTIES	53
10.2	IP SECURITY POLICIES ON LOCAL COMPUTER	54
10.3	GROUP POLICY MANAGEMENT	56
10.3.1	PASSWORD AGE	56
10.3.2	ACCOUNT LOCKOUT THRESHOLD	56
10.3.3	AUDIT ACCOUNT LOGON EVENTS	56
10.3.4	AUDIT LOGON EVENTS	56
10.3.5	AUDIT SYSTEM EVENTS	57

10.3.6	DEVICES: ALLOWED TO FORMAT AND EJECT REMOVABLE MEDIA	58
10.3.7	ALL SETTINGS	58
11	VULNERABILITY ASSESSMENTS	60
12	OWASP ESAP TESTING	61
12.1	VULNERABILITY MANAGEMENT	61
12.1.1	INFORMATION GATHERING & CONDUCTING SEARCH ENGINE DISCOVERY	61
12.1.2	FINGERPRINT WEB SERVER	62
12.1.3	ENUMERATE APPLICATION ON WEBSERVER	63
12.1.4	FINGERPRINT WEB APPLICATION	63
12.1.5	TESTING IDENTITY MANAGEMENT	63
12.1.6	AUTHENTICATION TESTING	64
12.1.7	AUTHORIZATION TESTING	64
12.1.8	INPUT VALIDATION TESTING	64
12.1.9	DATABASE TESTING	64
12.1.10	CLIENT SIDE TESTING	65
13	FUTURE ENHANCEMENTS	65
14	CONCLUSION	65
	REFERENCES	66