Comprehensive Design and Analysis Project

(IT 405)

Group Assessment File

Project ID: 19_20-J01

Supervisor: Mr. Amila Senarathne

Project Title:

HardnBot : Intelligent Server Hardening Software

Group Details:

Student ID	**Student Name**
IT16054400	R.M.B.B Rathnayake
IT16022416	G.G.L Anjula
IT16167742	W.M.K.M.W Wijekoon
IT16099746	Aruna S.H.G.R

Comprehensive Design and Analysis Project (IT 405)

Student Assessment File

Project ID: 19_20-J01

Student ID: IT16054400

Student Name: R.M.B.B Rathnayake

Research Domain: Information Security

Project Title:

HardnBot：Intelligent Server Hardening Software

Project Sub Title

Automated hardening against compliance issues

Individual Component Abstract

System hardening is reducing vulnerabilities in technology applications, systems, infrastructure, firmware, and other areas by applying best practices and configurations. The goal of system hardening is to eliminate potential attacks by attack vectors and minimize the system's attack surface. In order to harden a system firstly the remote connection between the system should be secure. Remote access is more commonly accomplished using a secure software solution like a VPN software.

After identifying compliance issues configuration scripts are automatically generated for classified compliance issues. In order to bring industry best practices into system configurations user interfaces are implemented to get configuration values through parameters. Parameterized values will be passed to automation scripts. These fixes are applied upon user confirmation. User interfaces including main dashboard of this system and integration of the system is handled.

Comprehensive Design and Analysis Project (IT 405)

Student Assessment File

Project ID: 19_20-J01

Student ID: IT16022416

Student Name: G.G.L Anjula

Research Domain: Information Security

Project Title:

HardnBot：Intelligent Server Hardening Software

Project Sub Title

Backup and intelligent rollback function

Individual Component Abstract

To perform good practices of hardening it is necessary to take a backup image of server before it is going to be harden. This backup is responsible for restoring files, folders, databases in order to prevent the loss of data in the event of a hardening failure, user error, disaster or accident. This will take place during the hardening process. User will receive a prompt asking about backup directory/path. As an example backup can be stored in a hard drive or a network share folder. After providing backup directory/path hardening process will take place. After hardening is done it will take some time to analyze server for detect any abnormal behavior of a server such as some applications out of services which are running on the server, high temperature of server, abnormal processing speed, etc. Inside HardnBot it has its own predefine models to detect such kind of abnormal behaviors. In case of found any abnormal behavior intelligence rollback function will automatically run and proceed to established previous status (backup) of the server.

Comprehensive Design and Analysis Project (IT 405)

Student Assessment File

Project ID: 19_20-J01

Student ID: IT16167742

Student Name: W.M.K.M.W Wijekoon

Research Domain: Information Security

Project Title:

HardnBot：Intelligent Server Hardening Software

Project Sub Title

Compliance issues classification

Individual Component Abstract

In general, all UNIX servers have default compliance issues. However, to address these issues hardening process needs to take place. Thus HardnBot's primary goal is to automate the server hardening process, to identify what compliance issues to be addressed is needed to be identified otherwise the hardening process will be not effective because it will automatically harden all useless compliances and it will take more time and server recourses to complete. To minimize the resource wastage and to manage time effectively compliance issues classification process will be introduced.

HardnBot's compliance issues classification process is going to handle with a trained machine learning model with a predefined dataset. Once the server is connected to the internal network of an organization, HardnBot will scan the sever for any compliance issues and take a list of identified compliance issues and pass those to the trained model and classify compliance issues with respect to the severity levels. Severity levels are categorized in to for main type as, Critical, High, Medium and low. After classification process, classified compliances will be used to the main hardening process. And also for the risk score prediction process this classified compliance will be used.

Comprehensive Design and Analysis Project (IT 405)

Student Assessment File

Project ID: 19_20-J01

Student ID: IT16099746

Student Name: Aruna S.H.G.R

Research Domain: Information Security

Project Title:

HardnBot : Intelligent Server Hardening Software

Project Sub Title

Risk score prediction

Individual Component Abstract

Using classified compliance issues, Overall risk score of the server is predicted. For this purpose, it is necessary to implement an algorithm to generate risk score. Using this algorithm HardnBot will predict the likelihood of Impact and probability of occurrence, to implement this algorithm, common probability functions and Bayesian methodology will be used. Potential Risk and Total asset value used to implement the Probability and impact of the risk. Using this method, the asset value to be threaten can be displayed.