www.ijaceeonline.com ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

Designing and Implementing Cyber Attack Prevention Software for Enterprise Information Security Management System

Nihat PAMUK
Associate Professor, Department of Electrical Electronics Engineering
Zonguldak Bulent Ecevit University, Turkey
Email: nihatpamuk@beun.edu.tr, nihatpamuk@gmail.com

Abstract: *Security weaknesses in information and communication systems cause these systems to be out of service or abuse, data loss, large-scale economic damage, deterioration of public order and violation of national security. The financial loss caused by cyber-attacks reaches extraordinary dimensions. It is very difficult to determine who insists and developed cyber-attacks targeting the information systems and their data. For these and similar reasons, cyber security software and cyber security hardware designed within the scope of the study aimed to ensure information security and prevent cyber-attacks. The hardware developed within the scope of the study was designed using Nano-technological computers. Open source programming technique was used in the design phase. In addition, with the integration of Nano-technology microcomputers and touch LCD screen, cyber security activities that provide ergonomic and easy use were carried out. With this cyber security software, it is aimed that especially small and medium sized enterprises and home users can benefit from the cyber security technology that they can use and manage easily.*

Keyword: *Cyber attack; Enterprise framework; Information security; Software; User-centered design*

1. INTRODUCTION

The dependence of countries on information technologies and especially the Internet is increasing day by day. Today, it is estimated that 384 billion e-mail messages are sent daily on the global network and 248 million DVDs of information are produced in one day [1-2]. YouTube servers upload 864,000 hours of video daily, Netflix users watch 22 million hours of TV or cinema a day [3]. Approximately two thirds of the world's population has an internet connection and 20% have membership in social networks. In addition, 85% of the world population uses mobile phones and 15% of them shop via mobile phones [4-5]. These values show how much the dependency on information technologies has increased.

Information technologies have created new concerns in the security aspect as well as the opportunities they provide for facilitating life. Now, in this new world, criminal acts such as theft, fraud have become possible without the need for physical contact or being in the same place with the victim. In addition, information technologies increased the communication skills of crime groups or terrorist organizations, strengthened propaganda opportunities and enabled the emergence of new fields of activity [6].

The emergence of the cyber space, both the security of users and nation states has brought many security risks for its institutions. People who attack by using cyber space can reach and leak national secrets by targeting financial institutions, attack national infrastructures and cause serious damage by causing physical damage to a kinetic attack. It is quite difficult to determine who did cyber-attacks, because attackers rarely leave traces behind them and strive to hide their own positions. In most cases, cyber attackers don't need expensive or rare tools [7]. In fact, the public's access to information technologies is easier and the role of information technologies in the operation of both public institutions and private institutions increases the security weaknesses.

In the past, the Cyber Security Control System was operated as separate networks not connected to public communication infrastructures [8-9]. However, as businesses changed to take advantage of the services and data provided by the Internet, security equipment protecting these systems decreased [10-11]. The benefits afforded by real time monitoring, peer to peer communications, multiple sessions, concurrency, maintenance and redundancy have enhanced the services provided for consumers and operators [12]. Moreover, this

Cite this paper:

Nihat PAMUK, "Designing and Implementing Cyber Attack Prevention Software for Enterprise Information Security Management System", International Journal of Advances in Computer and Electronics Engineering, Vol. 5, No. 1, pp. 1-10, January 2020.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

interconnectedness will grow with the implementation of smart grids and execution of the Internet of Things (IoT) [13-16]. Hence, the previously isolated systems have become increasingly exposed to a range of threats [17]. Information technology security often focuses on networked protection [18-19]. However, the cyber security control system recently offers IP-based communication requirements [20]. There are limits to traditional information technology security, communication security and protection of control systems. Setting these limits increases efficiency and protects the system.

The increase in economic and social critical infrastructure techniques has made societies dependent on computer networks and information technology solutions [21]. Cyber-attacks become more effective and potentially disastrous as our dependence on information technology increases. Advanced IT security systems cannot protect systems from hackers or defend against what appears to be authorized access [22]. People are easily attacked and publish high-risk attack targets for them and their social media. It is usually easy to enable computer users to infect corporate websites or mobile phones by imitating websites and by downloading and installing malicious applications and/or backdoors by clicking and tricking malicious links [23].

In the study, information security and cyber-attacks are prevented with the designed cyber security software and cyber security hardware. The purpose of the study is to enable home users to manage existing internet networks and to protect their access from the harmful effects of the internet by taking security measures in line with their needs. In addition, it is aimed to establish parental control to protect the internet and technology dependence of children between the ages of 3 and 14. Open source programming was used during the design phase. In addition, with the integration of Nanotechnology microcomputers and touch LCD screen, cyber security activities that provide ergonomic and easy use were carried out. In the last part of the study, program tests are carried out on the virtual computer lab.

2. OPERATE SYSTEM ON THE CYBER SECURITY SOFTWARE INTERFACE

Operating system studies on cyber security software interface will be completed. As a result of the performance tests carried out to realize the design module, it was decided to use the Banana Pi-R1 device. Although the device is hardware-lower than other test products, Banana Pi R2 and W2, it has been determined that it is better than other devices in software and hardware tests. For this reason, the heat tests of the device were started. The general appearance and hardware features of the Banana Pi R1 device are shown in Figure 1 [24].

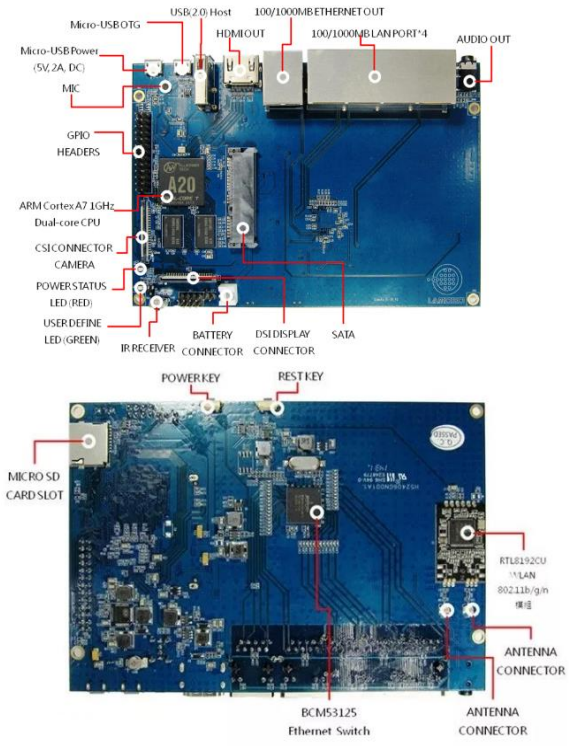

Figure 1 Banana Pi R1 overview and hardware features [24]

The BPi-R1 device supports Linux based operating systems. "Ubuntu Mate Motion 16.04" version, which is determined by the tests of the touch screen without any problems and the adjustment of the desired screen resolution to the desired scale is used. Ubuntu Mate Motion 16.04 update and package installation problems were encountered in Linux operating system. With the solution of this problem, an important step has been taken both for the operating system to have a more up-to-date structure and for the resolution of other problems encountered. Updating Ubuntu Mate Motion (Upgrade to Bionic) and package upgrades have been activated. Update process is completed by entering the "sudo do-release-upgrade" command on the terminal screen. Ubuntu Mate Bionic package updates have been made. The "sudo apt-get update", "sudo apt-get upgrade", "sudo apt dist-upgrade" structures have been updated with the list of commands and applications implemented in the Linux operating system.

"Net-Tools and DHCP Server Setup, Bind9 DNS Setup and configuration" was realized during the installation of the packages required for the interface's operation and the operation of the developed interface. In order for the Bind9 service to work integrated with the system after the necessary installations are made, the file in the /etc/systemd/system/bind9 service extension must be edited and configured. To make this arrangement, the nano text editor of Linux was used. After the package downloads and the required configura-

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

tions of these downloads, the installation of all necessary services for the interface to work successfully has been completed. It is expected that the program will be executable after all package installations for the program to run. In order for these permissions to be active, the necessary permissions are defined in the program with the help of the command shown below.

```
kuantumpi@kuantumpi-VirtualBox:~/Masaüstü/Kuantum$ sudo chmod 755 kuantum-pi-1.0.2.AppImage
```

After the operation carried out on the terminal screen, the necessary markings are made from the access rights menu on the program file, thereby giving all necessary permissions for the program to run. After all the operations done, the interface has now taken its place in the operating system as an operable extension. In the directory where the interface is located, it is provided to run terminal commands with the help of the command shown below.

```
kuantumpi@kuantumpi-VirtualBox:~/Masaüstü/Kuantum$ sudo ./kuantum-pi-1.0.2.AppImage --no-sandbox
```

It is designed to appeal directly to the end user, which includes menus such as DHCP Management, Firewall, Port Management, User Management, Device Control, Site Banning, Time Limit Setting, and Speed Limit setting. The visualization of the opening screen, which includes all the menus of the cyber security software interface, is shown in Figure 2. Using the accordion menu style, the user is provided with an overview of the menu tabs and the process of navigating between these menus is made easier. An information form for the users has been placed on the DHCP Management page, and a button has been added in the site ban section that allows users to instantly save and print the sites they visit. Management of the rules in the program interface is provided by IP tables.

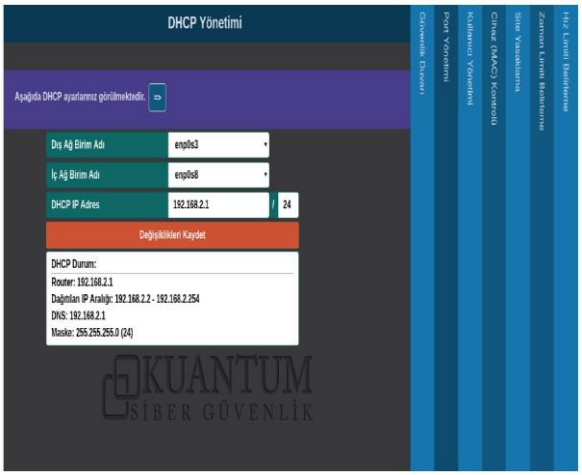

Figure 2 Screen image containing all menus of cyber security software interface

3. USING INTERFACE AND MENU TABS

In design, the interface gains functionality with the main menu button in the upper left corner. By clicking the main menu button, the left-to-right hidden menu is opened and the main headings to manage the cyber security software come in order from top to bottom. When clicking on each main title, a window opens in the middle of the screen where the relevant safety rules will be written. After the necessary settings are made and saved over the existing window, the user remains on standby on the main screen in the case when the user turns on the interface of the cyber security software by closing the relevant window. In this way, access to the opened module and ease of use are increased.

An information form for the users has been placed on the DHCP Management page, and a button has been added in the site ban section that allows users to instantly save and print the sites they visit. Buttons are added in the firewall module to allow rule priorities to be shifted up and down. The management of the rules in the program interface is provided by IP tables. IP tables is a Linux based open source firewall that uses the Net filter kernel.

3.1 DHCP Management Menu

This menu provides the user with features for selecting the range of IP addresses to be allocated to the networked devices by determining the external network unit (WAN) and the internal network unit (LAN). The Cyber Security Software interface automatically lists internal and external units, and the user selects his own internal network unit and external network unit among them. Then the IP address that will be distributed to the devices to be connected to the system is selected. It will be more convenient to select a C class IP address in the DHCP Management Menu. IPs starting in the 192-223 band are defined as C class IP in the standards. In addition, by selecting the /24 option, the capacity to distribute IP to 255 devices is determined on the specified address. The addresses assigned to the system and the choices made by the user are presented to the user after clicking the save changes button. Visuals of DHCP management menu is shown in Figure 3.

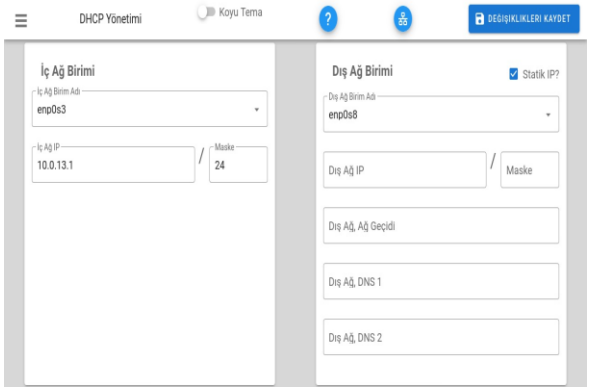

Figure 3 Visuals of DHCP management menu

3.2 Firewall Menu

Transactions made on the firewall menu are pro-

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

cessed through the code blocks in the system. By entering IP tables rule chain, all traffic rules regarding the IP of incoming requests and which port it comes from and which port to access the device in which IP can be managed from this menu. The menu, which offers options such as rejecting incoming requests, accepting and dropping directly, can also be used to add rules for which protocols can access. In addition, buttons that scroll the rules up and down have been added in order to prioritize the rules entered on the firewall. Firewall menu is shown in Figure 4.

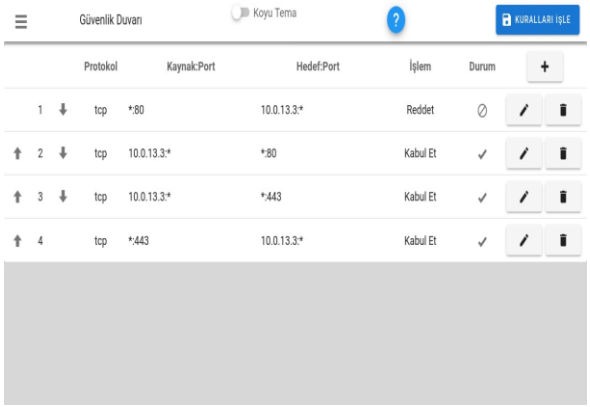

Figure 4 Firewall menu

3.3 Port Management Menu

In the menu that allows the user to add port rules to the devices registered in the system, the rules can be written by the user to determine which device will be processed for external requests and which port will be forwarded.

3.4 User Management Menu

User management menu is the section that enables user assignments to registered devices on the network. Users can be separated into groups such as manager, adult, child, guest and banned user through this section where users can add, delete and edit.

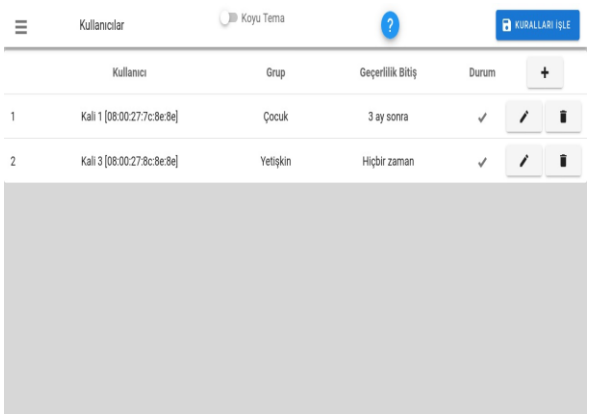

Figure 5 User management menu

It is possible to choose which users' devices will affect the operations performed within the program, then through the groups or users assigned in this section. In addition, it is possible to delete the specified user from the system at the end of the set time by entering the expiry date of the users specified in this section. User management menu is shown in Figure 5.

In order to control the traffic of the devices in the system and to create rules on the devices used in the system, the devices must first be registered with the user name in the system. Otherwise, devices will not be found in the rule operations made through other menus. After the users are added, it is provided to list the users through this menu.

3.5 Device Control Menu

The list of devices connected to the network can be accessed via the device control menu, but also can be processed by MAC filtering with the black list or white list option. Thanks to this process, when a white list is selected, access of all devices without user registration in the system can be prevented. With the device control menu, possible external or unknown connections can be prevented. User information text of the functions of the device control menu and the final version of the menu is shown in Figure 6.

Figure 6 Device control menu

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

3.6 Site Ban Menu

Through the site ban menu, only the user-based or the group of users can ban the internet sites. This feature, which operates according to the IP tables rule chain principle, prevents the IP addresses given to the devices by limiting the access of the sites with bad content. In the interface designed to reach the end user, the user can simply determine which user or which group of users cannot access which sites. At the same time, another feature on this menu increases the success of the interface. To see instantly entered sites, the tab named as sites entered on the menu can be clicked. In this way, internet traffic of devices on the network can be monitored. Site ban menu is shown in Figure 7.

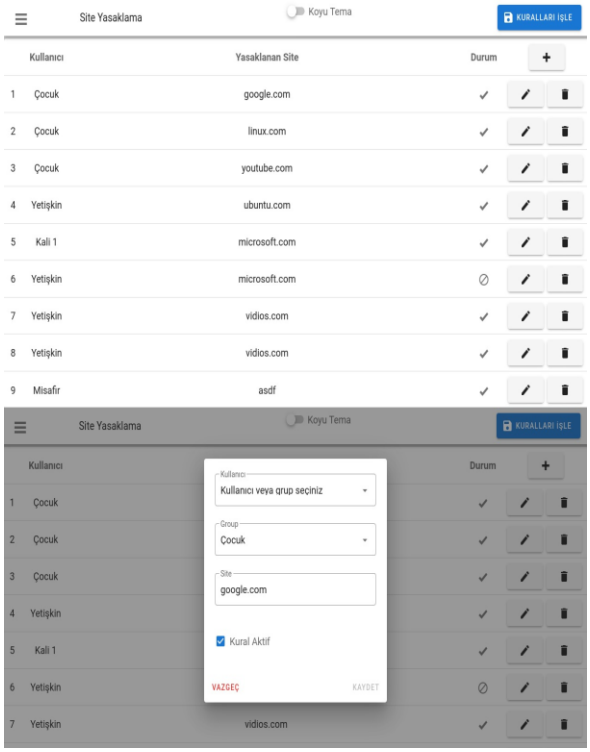

Figure 7 Site ban menu

3.7 Time Limit Setting Menu

The time limit setting menu contains definitions at which times users or user groups will stop internet access and at what times the access of these users will be activated again. Time limit setting menu is shown in Figure 8.

With this feature, the user can temporarily manage the internet access of the devices connected to the system and limit it within a time schedule according to his own request. This menu can be used especially by parents to ensure that children's internet access is restricted at certain times. A start time and an end time are specified in the feature and can be applied to a user or a group of users if desired. Thanks to this menu, the limitations made are transmitted to the user parents as a schedule.

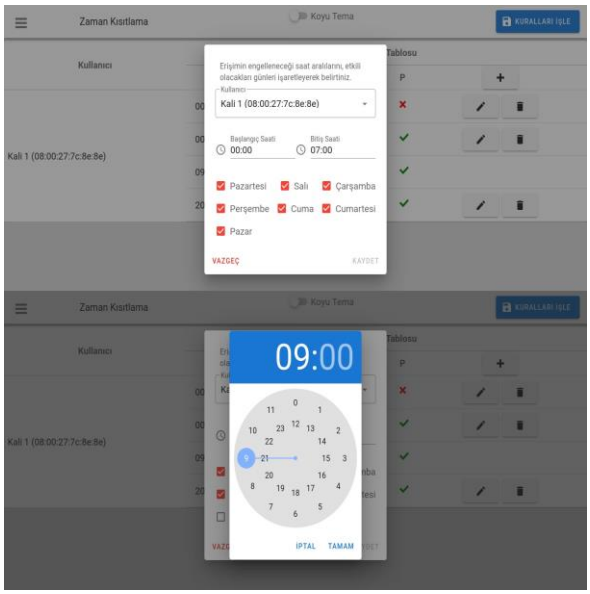

Figure 8 Time limit setting menu

3.8 Speed Limit Setting Menu

Speed limit setting menu is used to limit internet speeds of users and user groups. With this feature, the desired internet speed can be set as Mbit to the desired user. Especially, the platforms such as “youtube.com”, which are used frequently by children, use the internet speed very much and cause the internet usage efficiency of other users to decrease. Speed limit setting menu is shown in Figure 9.

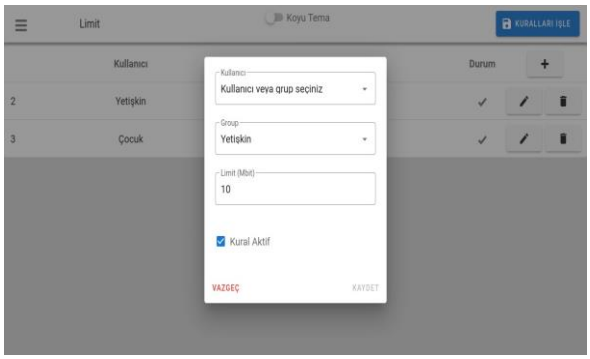

Figure 9 Speed limit setting menu

4. PROGRAM TESTS ON VIRTUAL COMPUTER LABORATORY

In order to observe that all the features described in the Interface tab can become functional, it has become necessary to perform tests for these functions. A virtual computer laboratory was established to perform the tests. The Virtual Box program suitable for the tests was selected. Virtual computers were created through the Virtual Box program and cyber security software was tested on the computer. The virtual network labor-

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

atory installed different operating systems on an existing computer through utilities, enabling them to associate these operating systems over the same network and create a test environment.

Two different operating systems were used to perform the tests. Since cyber security software will run on a Linux-based operating system, the Ubuntu distribution has been designated as the host. A virtual Windows computer was installed to test the software. After the virtual machines of these two operating systems were created in Virtual Box, configurations were made. Thanks to the configurations, the cyber security software installed on the main machine is set to receive the internet connection from the host with its NAT configuration. After the internal network is shared, Windows will use the Ubuntu operating system, where a cyber security software is installed, by identifying a virtual Ethernet card. In this case, an appropriate network laboratory was created during the test phase. NAT is selected in adapter 1 to enable the Ubuntu virtual machine to receive the Internet from NAT with the current computer. Necessary adjustments were made so that cyber security software can share networks with other virtual computers installed. Network share setting image with virtual computer is shown in Figure 10.

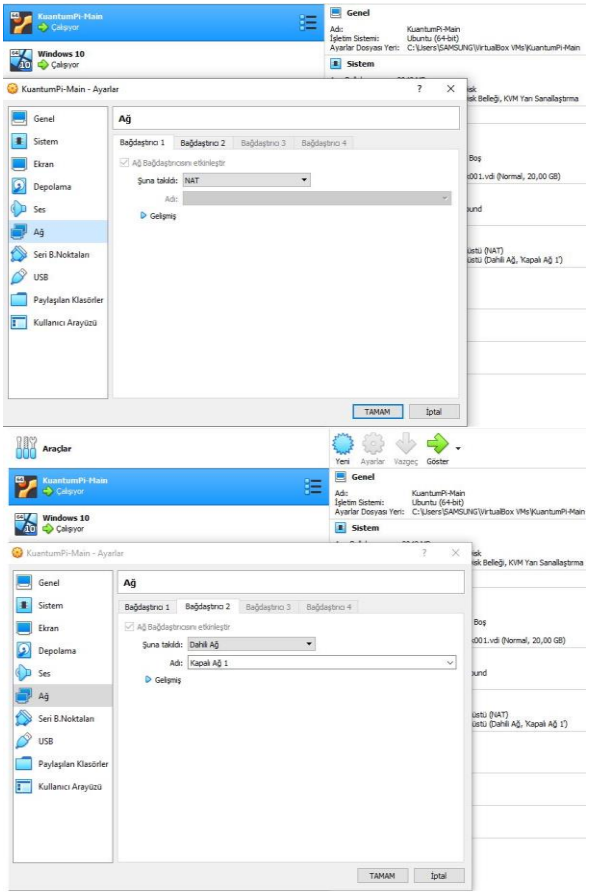

Figure 10 Network share setting image by virtual computer

In the network configuration to be made for Windows, which is determined as a second virtual computer, internet connection is not provided through the existing computer. Adjustments have been made to provide it from Ubuntu computer via a virtually created Ethernet connection. Two virtual user computers were created for testing purposes. One of them has Windows 10 operating system while the other has Windows 7 operating system.

4.1 DHCP Server Menu Tests

One of the first tests; It is the process of distribution of IP addresses to other computers through the program's DHCP server. The expectation in this test is to use the IP set on the first computer on Windows computers and provide internet access with the given IP address. It is aimed to give the second device a class C IP address through the DHCP management menu. The IP address determined within the scope of the test was 192.168.2.1. Whether the IP given to Windows computers designated as the second computer is received or not, access to the command screen (cmd) is provided from the run screen opened with the shortcut of Windows + R (run). In Windows computers, IP address querying can be learned both from the adapter settings and can be learned in more detail with the command "ipconfig" from the command line (cmd) screen. IP and external and internal network adjustments given in the program interface have been made. In Windows 7 and Windows 10 computers, IP addresses distributed from the host were successfully obtained and internet access was provided. DHCP-IP and connectivity test is shown in Figure 11.

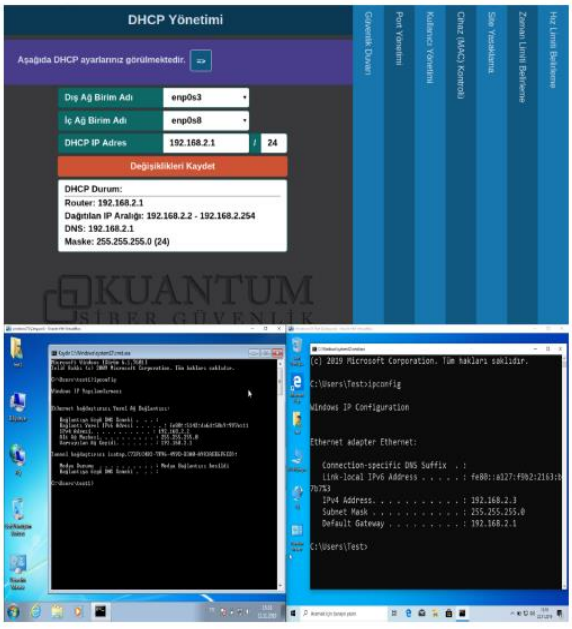

Figure 11 DHCP-IP and connectivity test

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

4.2 Device Control Tests

It was observed that the devices successfully received IP addresses during the first test phase. Tests of the interface showing the names of devices receiving IP addresses on the host computer and which IP addresses are obtained and providing device control were performed. The designed interface offers the user two filtering options: black list and white list. In addition, it is seen that the devices that have received the IP address in the first test phase have fallen to the interface screen and which IP addresses they have received. The virtual computer installed as Windows 7 received the IP address 192.168.2.2, while Windows 10 received the IP address 192.168.2.3. Through this interface, all devices connected to the local network can be seen by the user, and MAC filtering operations can be performed optionally.

4.3 User Management Menu Tests

In the program interface, devices that fall into the device control menu should be added to the interface as a user. No action can be taken on those devices without registering them as users. The area where the devices will be defined in the program is the user management menu. To be able to add devices in the menu, it is necessary to press the + symbol in the user management menu. Then, in the drop-down menu, the devices seen in the device control menu appear in the user panel. In order to move the user parameters up, the up button shown on the right should be pressed on the line with the user information. Then, the information about the user will be moved up and operations such as user name and group assignment will be done here.

4.4 Site Ban Menu Tests

The site ban menu has been created in order to prohibit other users in the system from accessing the designated sites and to prevent the devices of those users from operating on the designated sites.

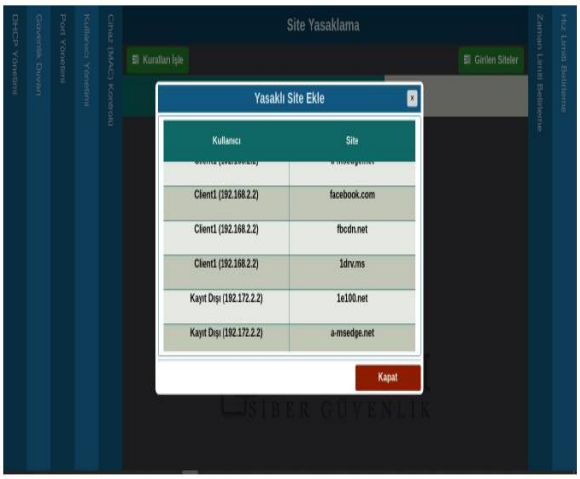

Figure 12 Site ban menu test

Using the menu, user can determine which sites users or groups of users cannot access. Cyber security software frees the user from complex rule chains and offers a simple, easy-to-use interface. In this way, the user can manage cyber security software without knowing any rule chain structure. Another process that can be done through the site ban menu is to create the site logs. With this feature, the user can see which IP address he has accessed from which site. Parents can protect their children from harmful content on the internet and track which sites they access on the internet. In addition, small and medium enterprises, institutions or organizations are required to keep the users' logging data in accordance with the obligation stipulated by the "5651" law. Therefore, the feature of saving the sites entered has gained a special importance with the "Law No. 5651". Site ban menu test is shown in Figure 12.

4.5 Speed Limit Menu Tests

Speed limit menu is a feature that can be used to limit internet speeds of users or user groups. The internet download speed required to download or process one Megabyte of data per second is 8 Megabits. It is left to the user to limit the data download speed of the devices on the system provided in the menu. Today, especially with the increase of digital broadcasting and the increase of streaming sites, internet speed has become more and more important. In particular, these sites can be optimized automatically according to internet speeds and working on a device with a fast internet infrastructure, providing a good image by working with the highest quality, may mean exploiting the speed of the internet in that infrastructure. For example, a family whose children watch videos from broadcast sites such as "youtube.com" etc. can take advantage of the internet experience without slowing down their internet speeds by taking measures to prevent all internet speeds from being used here. Speed limit menu in the Windows 10 devices with Turkey's overall average speed of 16 Mbit limitation infrastructure getirilmişk child is identified as users of Windows 7 to 9 Mbit device is designated internet speed.

4.6 Time Limit Menu Tests

The time limit menu is the menu that allows setting the time interval between which users or groups of users can access the internet. Via the menu, users can be set which days of the week and at what time intervals to access the internet. If no rules are added or adjusted in this menu, all users' internet access will be automatically adjusted 24/7. This feature is also a feature that can be used to prevent children from spending too much time on the Internet and to control their time in a more useful way by controlling their time here. In addition, this feature can be configured according to the user's own wish, that is, there is no restriction in this

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

regard. The initiative to determine the rules is left to the user. The visual that appears in the menu as a result of setting the timetable of the Windows 7 device and the Windows 10 device set in the child category is shown in Figure 13.

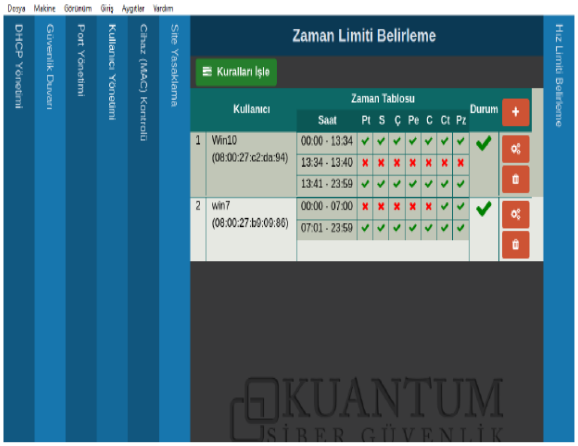

Figure 13 Time limit menu test

In Figure 13, the Internet access was interrupted between 12:00 and 7:00 on weekdays, assuming that the Windows 7 device is a child user. In the Windows 10 device for testing purposes, internet access was blocked in 13: 34-13: 40 time period and the internet connection of the device was disconnected at 13:34 and activated again at 13:40 according to the time period applied. The point to be noted in this menu is that the time zone of virtual computers is synchronized according to the system and at the right time.

4.7 Firewall and Port Management Menu Test

It is possible to do firewall and port management tests together. “Remote Desktop Protocol” must be used for test conditions to occur. After allowing 3389, which is the remote access port for the registered device through port management, this process can be performed by writing the rule on which IP device to which remote access should be directed to and which source IP will be accepted. The process steps for doing this test are given below.

Step 1: The device that requires remote access via the User Management menu must be registered to the system. Therefore, first of all, the device that will be allowed remote access is registered to the system. This procedure has to be done separately for each firewall and for the entire computer that must be authorized for port forwarding. Because there are separate computer based and user based authorizations in the firewall rule hierarchy. For this reason, the respective device must be defined in each computer and user area.

Step 2: In order to make a remote desktop for a device, a rule must be added for that device in the port management menu. TCP 3389, the remote desktop port, is set as an internal and external port. Then the Windows 7 tester is selected as the device to enable these ports. After the rule is saved, the "Process Rules" button is pressed so that the commands can be processed as possible.

Step 3: In this step, by entering the firewall menu, the rules regarding which source IP will be accepted, and the rules on which IP devices of these requests will be forwarded, are written and processed.

Step 4: After all the rules for remote access are processed and saved over the interface, the RDP software to be used for remote access can now be run and the IP of the device to be accessed remotely is entered. The device to be accessed and the RDP software are made ready.

Step 5: After entering the IP of the device to be accessed remotely from the RDP software, the software requests the user name and password to be entered for the remote desktop device. The user name and password of the device set for the test are entered.

Step 6: After the user name and password of the virtual device are entered for remote access, the session is closed on the virtual device and another open login message appears and the desktop screen of the computer accessed in the RDP software opens. The remote access test has been successfully completed.

5. CONCLUSIONS

Thanks to the software developed within the scope of the project, a significant distance has been covered in meeting the needs in this field. In the software, an effective user interface is presented with 8 different menus to ensure the cyber security of the users. In the DHCP tab, which is the welcome screen of the software, the IP addresses to be defined and distributed according to the network structure to which the device is connected are determined. Since the developed software will be located after the modem, it has undertaken the IP address distribution function. Options such as accepting, dropping and rejecting requests from different sources are presented in the firewall menu. In the port management menu, internal and external port access permissions of the devices are made adjustable by the user. In the user management tab, adding users is done. In this way, special privileges can be assigned to the users or the user can be added to previously defined groups and benefit from the permissions specially determined for that group. In this way, user management has been made more effective.

Other devices that are connected to the network other than the defined users are listed in the "Device

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 1, January 2020, pp. 1–10

(MAC) management" menu. If there are banned devices defined, when “black list” is activated, internet access will be blocked directly on these devices. Devices that have not yet been registered in the user management menu will not be affected by this action. Therefore, the necessary permissions settings must be made by adding the devices that are later included in the network to the "User Management" menu. When MAC filtering is activated with the white list, only predefined users are provided with internet access. In the site ban menu, site ban operations can be made for users or user groups. With this process, access of desired devices to the sites determined by the user can be prevented. Another important feature of the site ban menu is that the devices save the sites they enter. In the "Entered Sites" tab in this menu, you can see which IP addresses are accessed from which sites.

With the developed cyber security software, the user was also able to manage the internet access on the devices in speed and time. It is possible to determine in which time periods the defined users can access the internet with the time limit setting menu. In the speed limit menu, the internet access speeds of the devices can be limited to the limits set by the user. The software, which meets cyber security needs with all its functions, will prevent harmful content (Blue Whale and Momo), which are especially important for children, and prevent possible material and moral damages. The tests and the data obtained indicate that the developed software works with all its functions in a virtual environment. The software can provide security with easy user interaction within its interface without the need for IP tables commands. Adding rules is not directly active and is only listed on the menu. The rules written in that menu are activated by clicking the "Process Rules" button in each menu where you can add a rule. In this way, users can check these rules again when they enter a wrong or wrong rule. In addition, it has been observed that the software can perform internet control, which will be used intensely by home, small-medium enterprises, institutions and organizations.

As a result, the desktop application developed allows users to manage over the network provided that they are on the same network without going to the beginning of the current cyber security computer. The desktop application developed is possible with the installation of the "Network" package developed for Node JS. The desktop application detects the default gateway of the computer on which it is running. It sends a request to the detected gateway with SSL and is based on a coding method based on the use of the keys called SSL Public Key/Private Key, automatically to the cyber security computer detected over the network. There are two keys for SSL encoding. These keys are software encoded digitally. Only the other key can open the data that one key has locked. After creating your keys (SSL does this by default), one of the keys (private key) is defined in the software installed on the cyber security device. The other key (public key) is embedded in the desktop application codes you want to connect, so that the two keys are mutually locked together. As a result, there is no security gap between the existing desktop application and the cyber security device by using a strong encryption module.

6. ACKNOWLEDGEMENTS

The work has been developed within the framework of the project titled: Cyber Security Software, Device Design and Prototype Manufacturing: "KAR-PI". This project was supported by Kosgeb in TURKEY. I would like to thank Tuncay KARAMAN for his support in this project.

REFERENCES

[1] Chee-Wooi Ten, Govindarasu Manimaran, Chen-Ching Liu (2010), "Cybersecurity for critical infrastructures: Attack and defense modeling" *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, Vol. 40, Issue.4, pp. 853-865.

[2] Dominick J. R, (2010), "The dynamics of mass communication: Media in the digital age", *McGraw-Hill Education*, pp. 83-95.

[3] Bob Bell, Yehuda Koren, Chris Volinsky, Scalable collaborative filtering with jointly derived neighborhood interpolation weights, retrieved date:[23, June, 2019], online available at: https://www.netflixprize.com/leaderboard.html

[4] Ken Dunham, Saeed Abu Nimeh and Michael Becher, (2008), "Mobile malware attack and defense", *Syngress Media*, ISBN: 978-1-59749-298-0, pp. 159-171.

[5] Tombul F, Akdoğan H. (2016), "How do Terrorist Organizations Use Information Technologies? Understanding Cyberterrorism", *Eradicating Terrorism from the Middle East Public Administration, Governance and Globalization, Springer*, Cham, Vol 17, Chapter 6.

[6] Cardenas A, Roosta T, Taban G, Sastry S, Cyber security basic defenses and attack trends, Fujitsu Lab, retrieved date:[June, 2013], online available at: http://www.flacp.fujitsulabs.com/~cardenas/Chap4v2.pdf

[7] Hassan Takabi, James B. D. Joshi, Gail-Joon Ahn. (2010), " Security and privacy challenges in cloud computing environments" *IEEE Security & Privacy*, Vol. 8, Issue.6, pp. 24-31.

[8] Tiago Cruz, Luis Rosa, Jorge Proenca, Leandros Maglaras, Matthieu Aubigny, Leonid Lev, Jianmin Jiang, Paulo Simoes. (2016), " A Cybersecurity detection framework for supervisory control and data acquisition systems" *IEEE Transactions on Industrial Informatics*, Vol. 12, Issue.6, pp. 2236-2246.

[9] Shashikant S. Dudhagi, Mayur A. Pulse, Rohankumar V. Sable, Kishori D. Sarvade. (2017), "Banana Pi M1 single board computer" *International Research Journal of Engineering and Technology*, Vol. 4, Issue.12, pp. 602-604.

[10] Patel P. B, Choksi V. M, Jadhav S, Potdar M. B. (2016), "Smart motion detection system using Raspberry Pi" *International Journal of Applied Information Systems*, Vol.10, No.5, pp. 1723-1729.

[11] Blair, D., (2015), "Learning banana Pi: Unleash the power of Banana Pi and use it for home automation, games, and various practical applications", Packt Pu*blishing Ltd*, Switzerland.

[12] Zhu B, Joseph A, Sastry S. (2011), "A taxonomy of cyber-attacks on SCADA systems", *Proceedings of 4th International Conference on Cyber, Physical and Social Computing*, pp. 380-388.

[13] Saidur R, Poly B, (2019), "IoT based smart parking system" *International Journal of Advances in Computer and Electronics Engineering*, Vol. 4, Issue.1, pp. 11-16.

[14] Nasir M. H. M, Radzi N. A. M, Ahmad W. S. H. M. W, Abdullah F, Jamaludin M. Z. (2019), " Comparison of router testbeds: embedded system-based, software-based, and multiprotocol label switching (MPLS)" *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 15, Issue.3, pp. 1250-1256.

[15] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, (2016), "A survey on privacy preserving schemes for smart grid communications," *ArXiv*, preprint arXiv:1611.07722.

[16] Lee G. S, Thuraisingham B, (2012), "Cyber-physical systems security applied to tele-surgical robotics", *Computer Standards & Interfaces*, Vol. 34, Issue.4, pp. 225-229.

[17] Anil Lamba, Satinderjeet Singh, Balvinder Singh, Natasha Dutta, Sivakumar Sai Rela Muni. (2017), "Mitigating cyber security threats of industrial control systems (SCADA&DCS)" *International Journal for Technological Research in Engineering 3rd International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science*, pp. 31-34.

[18] Leandros A. Maglaras, Jianmin Jiang, Tiago J. Cruz. (2016), "Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems", *Journal of Information Security and Applications*, Vol. 30, Issue.1, pp. 15-26.

[19] Kirushanth S, Kuhanesan S, Thuseethan S. (2017), "Low-Cost security system using single board computer", *IUP Journal of Information Technology*, Vol. 13, Issue.3, pp. 57-61.

[20] Lech P, Włodarski P. (2017), "IoT WiFi home network stress test", *8th International Conference on Image Processing and Communications Challenges*, pp. 247-254.

[21] Julian Jang-Jaccard, Surya Nepal (2014), "A survey of emerging threats in cybersecurity" *Journal of Computer and System Sciences*, Vol. 80, Issue.5, pp. 973-993.

[22] Nabie Y. Conteh, Paul J Schmick (2016), "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks" *International Journal of Advanced Computer Research*, Vol. 6(23), pp. 31-38.

[23] Lucas M. M., Borisov, N. (2008), "Flybynight: mitigating the privacy risks of social networking" *In Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society*, pp. 1-8.

[24] Bpi, Banana Pi Open Source Project, retrieved date:[05,May, 2018], online available at: http://www.banana-pi.org/bpi-products/r1.html

Authors Biography

Nihat PAMUK, is an Associate Professor, of Department of Electrical Electronics Engineering in Zonguldak Bulent Ecevit University. He received his bachelor's degree in electrical electronics engineering department from Fırat University, Turkey, in 2005. He completed his MSc and PhD degrees all in electrical electronics engineering department from Sakarya University, Turkey in 2009 and 2012 respectively. His research interests are power system analysis, power protection systems, high voltage transmission and switch gears devices, renewable energy, smart grids and power quality.

Cite this paper:

Nihat PAMUK, "Designing and Implementing Cyber Attack Prevention Software for Enterprise Information Security Management System", International Journal of Advances in Computer and Electronics Engineering, Vol. 5, No. 1, pp. 1-10, January 2020.