iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VIII **Month of publication:** August 2022

DOI: https://doi.org/10.22214/ijraset.2022.46468

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VIII August 2022- Available at www.ijraset.com

Identifying Vulnerabilities and Reducing Cyber Risks and Attacks Using a Cyber Security Lab Environment

Gautham. K. Rajeev[1]
VJTI, Matunga, Mumbai

Abstract: ***In the present digital world where everyone is trying to digitalize their data and assets, cyber-attacks and cyber-crimes have made their presence felt much more than when compared to the previous period. During the pandemic days, the number of state sponsored and nation sponsored threat actors who pose the threat of attacking our organizational assets has increased rapidly. Organizations, especially which fall under the critical information infrastructure are becoming an increasingly common target for cyber-attacks. The rate has alarmingly gone up that the national and state government have started to give more attention and focus to cyber security and cyber-crimes. Specific bodies have been assigned by the government to notify about threats/attacks and also to suggest possible techniques to mitigate these threats/attacks. Most devices that are used in these organization are either using older versions of devices or the devices used are not properly cyber secured. This vulnerability is most often taken advantage of by the attacker when trying to access and compromise the organization. Another factor leading to cyber breaches and attacks is the limited or low competency level of employees who work in these organizations. Employees with weak cybersecurity knowledge are the main entry point for online fraud, viruses, and other threats. This creates a situation where business owners and managers should focus on teaching employees the importance of strong digital security. This report describes different techniques and tools which can be used to detect vulnerabilities or threats present in our system, the different cyber-attacks that can take place exploiting these identified vulnerabilities: How to generate an attack, How to identify an attack and How to prevent an attack. Further on, how we can create an environment, where individuals can have hands-on experience on how to detect different cyber threats or vulnerabilities present on a device which makes them confident enough to identify a cyber-attack or threat at an early stage and deploy preventive measures against it is also discussed.***
Index Terms: Cyber Security, Cyber-attacks, Cyber-risk, Cyber-threats, Vulnerability

I. INTRODUCTION

Cyber Security is an area that has gained enormous acceptance in the modern world which is very much dependent on technology. With the continuously increase in reports related to threats and attacks in the cyber world, it is important to build competencies towards cybersecurity. Private companies are becoming an increasingly common target for cybercrime, and since employees with weak cybersecurity knowledge are the main entry point for online fraud, viruses, and other threats, it makes sense that business owners and managers should focus on teaching employees the importance of strong digital security. Currently there is a great demand for trained cyber security professionals with hands-on skills. These professionals are desperately needed to defend cyberspace from threats such as hackers and malware who threaten to disrupt such services daily. Nowadays, the presence of state sponsored and nation sponsored threat actors at organizational level is alarmingly increasing. They are continuously posing a threat of attacking our system anytime because in most of the organizations, the preventive measures against the cyber-attacks or threats posed by these threat actors have not been installed or maintained properly. Also, the explosive growth of IT infrastructures, cloud systems, and Internet of Things (IoT) have resulted in complex cyber systems that are extremely difficult to secure and protect due to many factors such as their size, architecture complexity, distributed nature, heterogeneity, the large numbers of users, and diversity of services provided, just to name a few. Another factor is that, most devices that are used in critical information infrastructures are either using older versions of devices or the devices used are not properly cyber secured. This vulnerability is taken advantage of by the attacker when trying to access and attack the organization.

[1] This work was submitted for review on 25/08/2022
Gautham. K. Rajeev is with the Electronics and Telecommunication Engineering branch, Department of Electrical Engineering, VJTI, Mumbai university, Matunga, Mumbai-400019, India (e-mail: gkrajeev_m20@et.vjti.ac.in).

These challenges, coupled with a shortage of skilled cybersecurity experts and the extreme difficulty in setting up cybersecurity experimental environments, have resulted in vulnerable cyber systems with no adequate technical support.

To meet the above requirements it is necessary to detect threats, vulnerabilities and attacks as and when they happen and also to provide a training platform for professionals in the field of cyber security, an environment that is remotely placed from the normal workstation is required, where one can freely experiment and test out activities which will increase the individual competency level in detecting and preventing the cyber-attacks, vulnerabilities and threats. This journal discusses on:

1) Techniques/tools that are used in the present day for detecting the different vulnerabilities that can be present in our systems which can be utilized by threat actors or attackers for entering the organizational network
2) Different cyber-attacks that can happen due to these vulnerabilities
3) How to deploy a preventive technique against the detected attack so that in the future we can prevent the attack from happening at the first place.
4) Setting up a cyber-security lab where professionals from an organization can have hands-on training and can perform activities and tasks related to cyber security as required

II. RELATED WORK

Identification and prevention of cyber-attacks that are happening around us is an unavoidable step towards ensuring that cybersecurity is maintained around our work place.

Tihomir Latinovic et al. [1] has mentioned in his journal article that modern information technology in business requires the introduction of integrated measures for the protection of information. For this they have asked the readers to use the ISO/ IEC 27001 international standard for successful implementation of systems for information security management. Further they have explained on what information, resource and assets mean and what risk assessment is. It is necessary to determine the optimal level of safety in terms of cost-effectiveness. IEC 62443 standards were defined to secure industrial communication networks and industrial automation and control systems (IACS) through a systematic approach. Morand Fachot [2] in his article has mentioned on how we can prevent illegal or inappropriate access which in turn will provide us security. He further went on to say that IEC 62443 is all set to be adopted in more systems and sectors like energy sector, transportation systems, industrial automation etc. Riza Azmi et al. [3] in his journal of cyber policy has mentioned on what cyber security framework means and the need to group different cybersecurity frameworks together for better implementation, that various international organizations, academic institutions, corporations and different countries are trying to develop. This effort has emphasized various perspectives depending on each organization's intention, while their contents involve the same concept. In this analysis, the authors have used the document analysis method along with two cycles of coding to study these different frameworks and come to a clear picture regarding grouping the frameworks. The different actions, processes for securing cyber space were also discussed in this journal.

Julian Jang-Jaccard et al. [5] in their article have discussed about the most exploited vulnerabilities in hardware and software, the flaws in the present mitigation techniques and new attack patterns in areas like cloud computing and critical infrastructure. In the present situation, most of the cultural, social and government activities are taking place in the cyber-space. Yuchong Li et al [6] conducted a research in these areas and have discussed in their research paper the methods by which we can protect electronic data from cyber-attacks and threats, the different methods being followed to prevent cyber-attacks on these data. Further, they have investigated on challenges, weakness and strengths of different methods that they had proposed. In hardware, embedded systems are one of the most devices which are having a high risk of cyber security breach. Abdul Mohsan et al [12] has mentioned in their journal the different reasons why security breaches happen in server. They have identified twelve factors which have been influencing the embedded system's cyber security. Using these factors, a framework was developed which checks a particular server for possible vulnerable areas and helps strengthen the cyber security of embedded systems. Jae-Myeong Lee et al. [13] has found out on how a particular malware intervenes an important process that is taking place further invading the Supervisory Control and Data Acquisition (SCADA) host process using the Dynamic Link Library (DLL) Injection technique. As a preventive technique against this, an algorithm was developed which blocks DLL Injection and also shows its effectiveness in protecting the SCADA system against other real world malwares.

Making the people understand concepts related to cyber security like, what is means, how can we protect our infrastructure from cyber-attacks and threats are necessarily required for creating a better and secure cyber space. Nabin Chowdhury et al. [4] has reviewed the different methods of cyber security training required for critical infrastructure protection. The key performance indicators (KPI) for these training programs were identified by the authors to evaluate their effectiveness.

The results showed that solutions or training that provide hands-on experience, team skills development, and high level of real-life fidelity were often preferred to other options, with simulation-based solutions or trainings showing the highest amount of research and development.

Hany EL Mokadem [7] has mentioned the possible common attacks against network switches that are likely to take place. The vulnerability or weak spot that the attacker takes advantage of for carrying out these attacks were discussed and possible preventive measures against each of the identified attacks against the network switch were also explained in the article. Michal Polivka et al. [8] described about endpoint security of modems or routers. The vulnerabilities present on these devices which can be exploited by attackers to perform Denial of Service (DoS) attack were found out and how to mitigate these vulnerabilities was also explained by the authors.

A common vulnerability found in Virtual Private Networks (VPNs) was discussed by S Patton et al. [9]. A routing attack on VPN because of the identified vulnerability and the solution for protecting against the exploitation of this vulnerability was also detailed in the document. Yi Guo et al. [11] in their journal have analyzed the vulnerabilities and security threats present in inter-domain routing system.

The flows in Border Gateway Protocol (BGP) because of which most vulnerabilities arise in the inter-domain routing system was also explained. They further went on to provide solutions which addresses to improve the security of these inter-domain routing systems.

Danish Javeed et al. [14] have explained in detail in their journal about Man-In-The-Middle (MITM) attack and its types. The importance of network security and the reasons why this particular attack takes place were detailed in this journal. Some mechanisms that can be used to prevent such attacks were also discussed in this paper. The change in network performance because of various strategies used to launch MITM attack was studied by Ityas Alodat[15] in his journal. He has further researched on the types of MITM attacks that are present in wireless systems and their ways to prevent them. Silvia Bravo et al. [18] in their journal had mentioned about what a DDoS attack and the different methods used for detecting this attack. They were able to identify six aspects for analyzing the DDoS attack. They were able to detect the detection mechanism with highest accuracy for the datasets that they used. Abeer Alotaibi et al. [17] in their journal has mentioned about the different types of DDoS attacks, how to simulate this particular attack and the defense against DDoS ataacks using a tool called Slowloris tool. The two types of DDoS attacks or flooding: http with TCP connection and Ping requests were also discussed. Wael Alosaimi et al. [16] has proposed a new solution to encounter the attacks utilizing the firewall capabilities in which the firewalls will be able to control the verification process to protect the targeted system.

Hossein Abroshan et al. [20] in their paper has discussed about how the Phishing attacks have taken place during the pandemic and the co-relation of human emotions and behaviour with the success of phishing attempts during the pandemic. The phishing attack and its types where explained in detail by Jaeil Lee et al. [19].

The detailed analysis was conducted on the attack methods and observations where deduced from these analysis. The way in which a malicious system induces network vulnerability was explained by R.A Skoog et al. [10]. They further explained on how to mitigate these instabilities and the corresponding network management and control mechanisms and the same were developed and validated.

III. SYSTEM DESIGN

The paper is structured in such a way that by the end of this paper, the readers will have a general understanding regarding the following points:

1) Detecting the possible vulnerabilities likely to be present in devices in organizational industries
2) Various attacks that are likely to take place on the devices (simulating the attacks & finding out the preventive measures against these attacks)
3) Minimum Baseline Security Standard (MBSS) of devices will be available with the users so that they can use it as and when necessary.

A. Security Landscape

The general security landscape of an organization will commonly contain:

1) Application and data link layer,
2) Network and equipment layer and
3) Physical layer as mentioned in Fig 1.

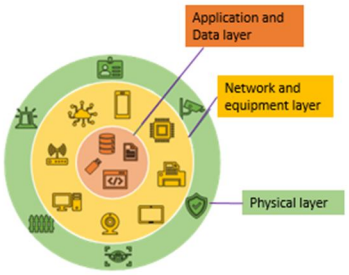


Fig. 1. Different layers in Security Landscape

The threat actors and attackers who try to gain access to the organizational network and data will attack each of these layers for trying to find a vulnerability which they can take advantage of.
Generally, the landscape of:

a) Application and data link layer contains different applications and software related to business activities while,
b) Network and equipment layer contains devices from

- Information Technology- IT (e.g. switches, routers, gateways, IP phones etc.)
- Operational Technology- OT (e.g. transformers, industrial control system, PLC, HMI etc.)
- Security cameras, access control points, sensors etc. and

c) Physical layer contains: Physical locations and physical people like:

- Power grids (Power plants, distribution centers, substations etc.)
- Personal: Every individual performing different roles in the process which can get compromised during a potential cyber-attack.

The attacks that can happen to an organization and their preventive measures can also be categorized according to the landscape as described in TABLE. 1.

Table. 1: Attacks and preventive measures for security landscape layers

Sr. No.	Security Landscape	Attacks and threats	Preventive measures against identified attacks
1	Application and Data layer	• Application misconfiguration • Sabotage attack • Data/IP theft	• Encryption of data • Role based access control
2	Network and equipment layer	• DDoS attack • Taking over server/host in network	• OS hardening • Installing firewall
3	Physical Layer	• Unauthorized entry • Phishing	• Access Control X-Ray • Biometric scanner • I-Card

The main activity that as users we need to keep note of at each layer that the attacker is most likely to perform are:

- Unauthorized access at the application and data layer
- Unauthorized modification at the network and equipment layer
- Unauthorized deletion at the physical layer

The above mentioned details related to landscape and its security is consolidated and presented as shown in the Fig 2.

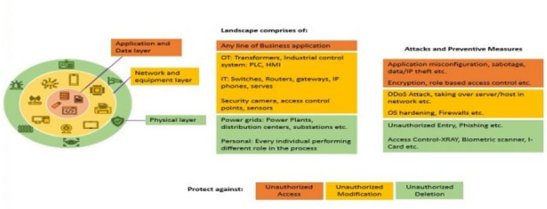


Fig. 2. Security Landscape

IV. IMPLEMENTATION

1) To start with, Operational Technology (OT) asset registers of different types of power plants like thermal, hydro was collected and analyzed. The asset register comprises of details of assets i.e. devices used in that particular plant. These details include name, version, manufacturer, area where it is installed, criticality rating, end-of-life date etc.

2) After analyzing these parameters, devices are identified that are prone to get attacked and upon which testing should be done. These identified devices include end-point devices, firewalls, switches etc. which should be cyber secure for proper and safe functioning of the plant.

3) After identification of these devices, testing is done on these devices to check for any vulnerabilities/threats found if any. Particular tools like Nessus are used for performing these vulnerability assessments and identifying the vulnerabilities present in the devices.

4) If any vulnerability is found during these conducted assessments, appropriate remedial measures should be taken to remove these identified vulnerabilities and make the system/device secure. These remedial measures should be found out from already defined standards by organizations like Centre for Internet Security (CIS) which will contain large number of guidelines from which we will have to filter out the guidelines applicable for each case.

The implementation flow is depicted as in Fig. 3.

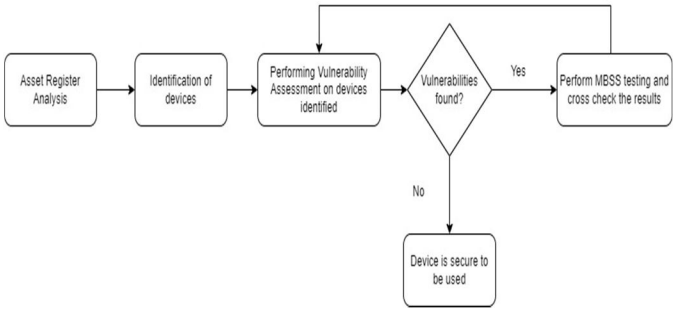


Fig. 3. Flow chart of implementation

Apart from this, we can also identify common cyber-attacks that are likely to happen on these devices and find answers to different questions like:

a) Reason to why these attack take place
b) What is the vulnerability that they take advantage of?
c) What are the preventive measures against these attacks?
d) How and where can we test and implement these attacks and preventive measures?

The network simulations for these attacks can be made using tools available like the Cisco Packet tracer or the Kali Linux from where the user will get an idea as to how these attacks take place. This will also cover the point mentioned above which is to decrease the knowledge gap of users on the field of cyber-security which in turn will help the users to prevent the attack the next time it takes place.

A cyber security lab is an environment which provides users a platform where they will be able to increase their knowledge level in cybersecurity related aspects and also test different applications which can be either developed in-house or downloaded from external source. The cyber security lab was designed in such a way that the users who are accessing the cyber lab will be able to perform the activity or testing on the required device. The structure is a mixture of physical and virtual components. Here, we can install or use a virtual simulator if it is found to satisfy the requirements of a particular physical device. For example, a network simulator can be used for creation and testing of various network architectures using different components in the network. If the same process is to be done physically, then various parameters like area, availability of the required devices, cost of procurement of the devices etc. will have to be taken into consideration. In the designed system, for starting off, we can include devices like servers, firewalls, routers, network switches, connectors and endpoint devices like computers or laptops. In these devices the users can try different configurations and settings that they are using or likely to use in their production environment, like creating a demilitarized zone and checking the traffic flow happening through them without the fear of disrupting the normal functioning of the environment.

The different attacks identified and simulated include the following:

A. Man-In-The-Middle (MITM) Attack

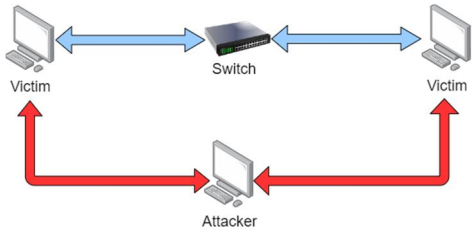


Fig. 4. Man-in-the-Middle attack

One of the common attack mechanisms used by attackers to enter and interrupt the normal communication is Man-In-The-Middle Attack. Here the attacker gets between the normal communication path of user and server and interrupts the flow as shown in Fig. 4. There are various types in which MITM can be realized like ARP spoofing, ARP poisoning, MAC spoofing. The network simulator design created for understanding about this attack is given in Fig. 5

The general steps in which MITM is realized is as follows:

1) The attacker tries to generate a connection between the existing connection of user and server by pretending that it is in the same network domain.
2) This is done by using a Service Set Identifier (SSID) that looks similar to the original SSID.
3) After the connection is established, the MAC address of common gateway at the router is accessed by the attacker and then the original mac address of threat attacker is changed to the mac address obtained.
4) After this whenever the user sends a message to server, the message will be redirected to the attacker instead of the server
5) While sending message from server to user, the MAC address of user is given to the threat actor so that server will be under the impression that it is replying or sending a message to the user while it is actually sending the message to threat actor.
6) The attacker can either passively observe the traffic flow, or it can change the message according to its need

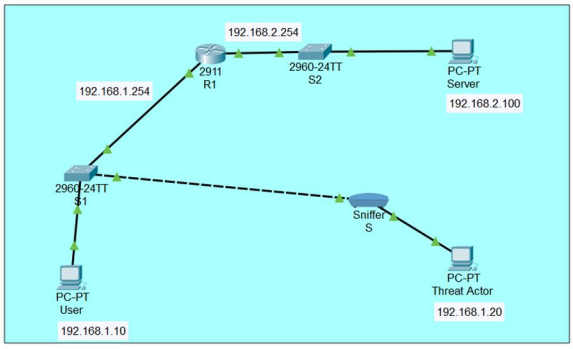


Fig. 5. Virtual Simulation of MITM

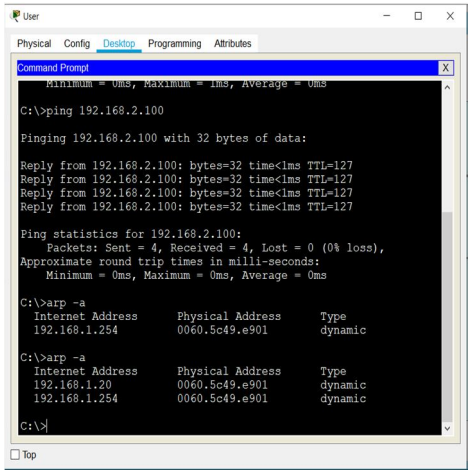


Fig. 6. Command Prompt of end-point device showing ARP spoofing

After establishing connection as mentioned in the above steps, the attacker tries to contact the end-point device by sending a ping message. On doing this the ARP table of user gets changed and the new IP of the attacker gets added along with the default gateway IP already present as shown in Fig. 6. and because both IPs are having same MAC address, the next time when the users tries to send a message to server, instead of going through the default gateway IP to the router, the communication will be diverted and will go to the attacker who can make the necessary changes and send the message to the server using the user's MAC address as mentioned before. This process continues until the either the user finds out about the attack that has taken place in the system or when the attacker has completed his requirements.

B. Phishing Attack

The type of cyber-attack called Phishing is an attack where the attackers send a communication in the form of email, message or phone call which will lure the users into giving their sensitive information. The communication message is designed and structured in such a way that it will appear to have come from a genuine source and the content in it will also seem genuine. The Phishing attack can be in the form of an email (Email Phishing), SMS message (Smishing) or in the form of a voice call (Vishing).

Users can stimulate Phishing attacks to make their respective employees or customers capable to detect possible phishing attempts that can occur to them. The procedure followed for simulating a phishing attack is as follows:

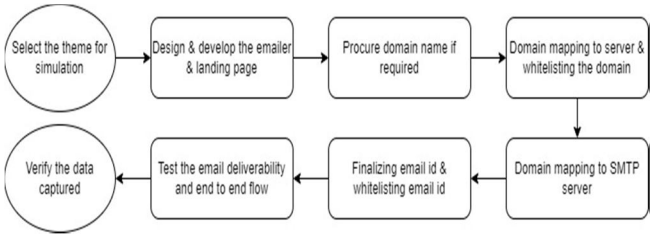


Fig. 7. Flow chart for simulating Phishing attack

After getting the report of the post phishing simulation data, the analysis is carried out by the users on the data obtained and required communication is send to the users or customers who have failed in the Phishing simulation activity.

C. Denial of Service (DoS) Attack

Another common type of attack that attackers rely on for disrupting the normal communication between user and server is Denial of Service (DoS) attack. Here, the attacker blocks the communication path between user and the server. One of the method by which this can be achieved is to continuously flood the user with Internet Control Messaging Protocol (ICMP) pings/messages. Fig. 9. shows the message used to continuously ping an endpoint device using the command "ping -t (IP address of user)". By doing so the user will continuously get message requests from the attacker for which the user will have to respond to because of which the normal communication will not be possible in this state. This ultimately causes denial of service as the server is not getting the required replies from the user.

If this same attack is done on a user system using more than one attacker system, then that type of attack is called Distributed Denial of Service (DDoS).

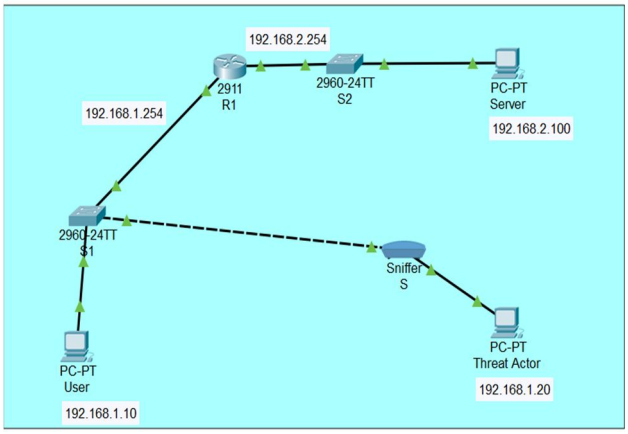


Fig. 8 Virtual simulation for Denial of Service attack

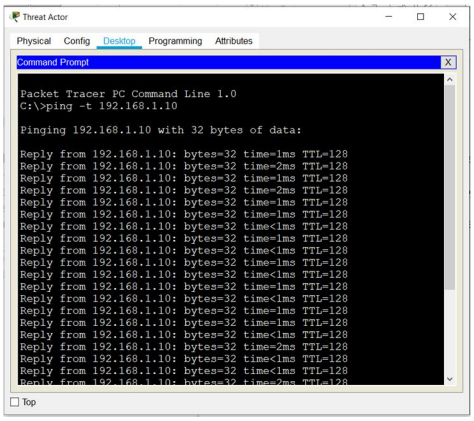


Fig. 9.View of command prompt of attacker sending continuous ping messages to user system

These attacks can be prevented if the users are well aware and well equipped against these attacks. Some of the common preventive measures that the users can implement in their workspace are:

1) Increasing awareness among users

Creating awareness among users on topics related to cyber-security may include:

a) Need to regularly update all the devices under a user's control
b) Need to conduct periodic patch management for networking devices
c) Conducting mock drills in the organizations to equip users and customers on potential cyber threats and attacks
d) Conducting webinars and seminars on Cyber security related topics

2) Minimum Baseline Security Standard (MBSS)

a) This is a standard which is in alternative words the basic/minimum security that is required to be installed and maintained in devices to ensure cyber security of these devices.
b) This is achieved by following the benchmarking provided by various organizations like Centre for Internet Security (CIS) which contains guidelines to be followed from which the applicable/required guidelines are to be selected depending upon the device/environment
c) By performing assessments or tests to detect vulnerabilities or weak-spots in the network or devices, which in other words is called vulnerability assessment, the areas to be secured can be found out. This can be done using different testing tools or applications like a tool called Nessus which is used to identify vulnerabilities in a particular device or environment.

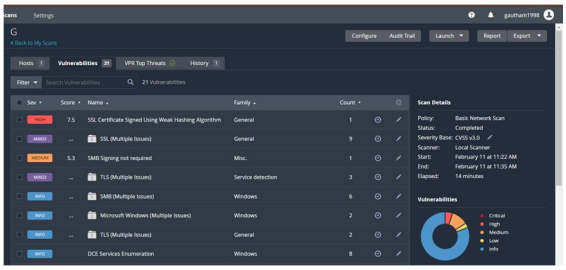


Fig. 10a). Vulnerability details found in test case

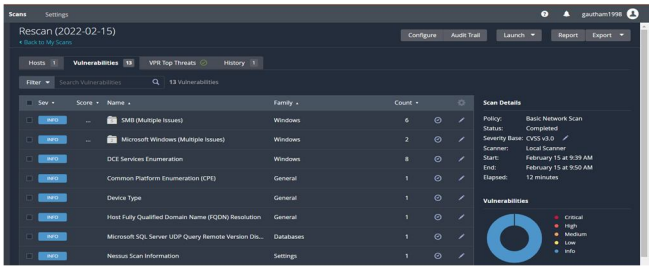


Fig. 10b). Scan showing that device is secure from vulnerabilities

An example case of vulnerability assessment which was conducted on an end-point device is given in Fig. 10. As it can be seen from the Fig 10a). , a total of 21 vulnerabilities were found upon scanning the endpoint device. Among these vulnerabilities, there will be critical, high, medium, low and also some details which can be considered as information to the user. These types are indicated using different colors in the application. In order to make this particular endpoint device cyber secure, these vulnerabilities should be mitigated. For this, the users will have to refer the global standard benchmarking and identify the required standards for each vulnerability and make sure that these standards are maintained in the device.

The rescan which was run on the endpoint device after including all the requirement standards and controls is shown in Fig 10b). In the same manner, MBSS should be ensured for all the devices identified from the asset register

3) Network Segmentation

Network segmentation is an architecture that divides a network into smaller sections or subnets. Each network segment acts as its own network, which provides security teams with increased control over the traffic that flows into their systems

This method should be installed in the power plants so as to make the entire network secure. The main advantage of this method is that, if any attack occurs in an area in the plant, only that segment of the network which contain the affected area will be affected and not the whole network. Thus the entire network system will not be affected if network segmentation is done.

Fig. 11. shows virtually how network segmentation can be performed using a simulation tool. As it is seen in the Fig 6, this can be achieved by providing different default gateway IP addresses for different areas in the plant. Here for one section, the default gateway IP is 192.168.10.1 and for the next section the default gateway IP is 192.168.20.1. By doing this there is no direct connection between the two depicted sections.

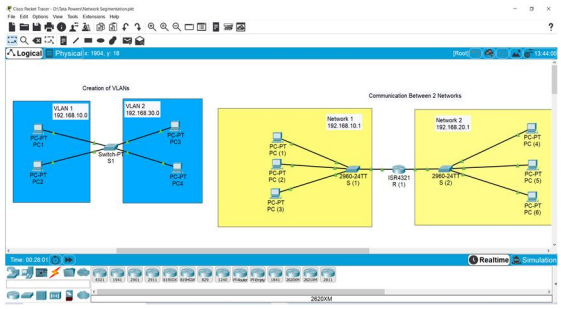


Fig. 11. Network segmentation

V. CONCLUSION

With ever-growing and ever-increasing cyber risk at both within the organization and outside the organization, because of reasons like, cyber criminals having ample time in their hands as they are sponsored by state and national bodies who identify these criminals as state sponsored or nation sponsored threat actors. Having a cyber-security lab environment where any user in an organization can freely experiment and conduct activities related to the devices they use will only increase the competency of these users on that specific domain.

The critical systems identified from the OT industries were tested for any vulnerabilities and the found vulnerabilities were removed following the guidelines of the policies. Common attacks and threats that can happen on the identified devices were researched and simulated on and the preventive measures against these were identified. Having an environment where any user can freely experiment on different aspects on the devices which they are using on a daily basis will only increase the competency of these users on that specific domain. Setting up a cyber-security lab and providing hands-on training to users and employees will increase the knowledge level/competency of these users and will in turn increase their confidence level when it comes to handing and operating on specific devices.

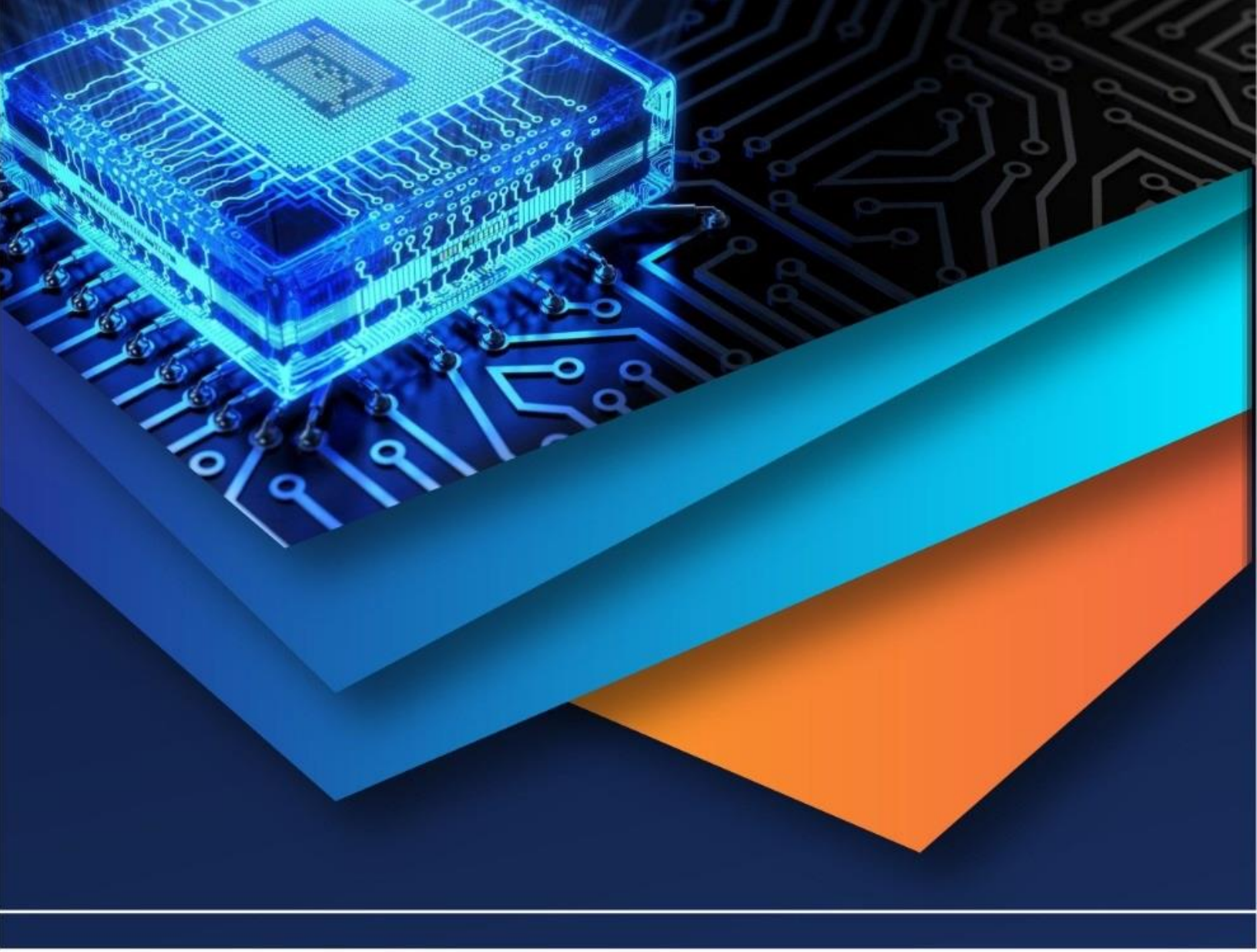
VI. FUTURE WORK

The proposed model of cyber security lab is just a representative model which is designed and operated based on the specific requirement. A similar model of this cyber security lab can be implemented in different domains other than the power domain which can be the telecommunication domain, the finance domain or any other domain where there is a need to increase the cyber security for their organization.

The concentration on using/testing only devices from the power plants can be shifted to other domains where other networks and architectures will be present that can be cyber secured. The subject cyber security is a rapidly growing and constantly developing subject because of which new attacks will emerge from the attackers and the preventive measures will have to be found out against these attacks. The different forms in which the devices can be secured can also explored.

REFERENCES

[1] Latinovic, Tihomir & Sikman, Ljilja "ISO 27001 – Information Systems Security and Economic Challenges", Journal Annals of Hunedoara . (2020).
[2] Morand Fachot. "IEC 62443 Standards – a cornerstone of industrial cyber security ", 28 July 2020
[3] Azmi, Riza & Tibben, William & Win, Khin. . "Review of cybersecurity frameworks: context and shared concepts". Journal of Cyber Policy. 3. 1-26. 10.1080/23738871.2018.1520271. (2018).
[4] Nabin Chowdhury, Vasileios Gkioulos, "Cyber security training for critical infrastructure protection:" Computer Science Review, Volume 40, 2021, 100361, ISSN 1574-0137
[5] Julian Jang-Jaccard, Surya Nepal, "A survey of emerging threats in cyber security," Journal of Computer and System Sciences 80 (2014) 973–993, Received 25 September 2012; Received in revised form 15 March 2013; Accepted 27 August 2013; Available online 10 February 2014
[6] Yuchong Li, Qinghui Liu, "A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments", Energy Reports 7 (2021) 8176–8186, Received 9 July 2021; Received in revised form 9 August 2021; Accepted 18 August 2021; Available online 3 September 2021
[7] Hany EL Mokademi "Switch attacks and countermeasures"
[8] Michal Polivka, Vaclav Oujezsky & Vladislav Skorpil, "Modem network vulnerabilities and security testing-Actual threats", 2015, 38th International Conference on Telecommunications and Signal Processing (TSP)
[9] S.Patton, D.Doss & W. Yurcik"Distributed weakness in virtual private network". Local Computer Networks. LCN 2000
[10] R.A Skoog, N.Jasinski, M.A Shayman, R.Ghahremanpour;M Kalantari, "Network management and control mechanisms to prevent maliciously induces network instability," NOMS 2002. IEEE/IFIP Network Operations and Management Symposium. 'Management Solutions for the New Communications World'(Cat. No.02CH37327)
[11] Yi Guo, Fu Miao, Liancheng Zhag & Juwei Yan, "A review on inter-domain routing system vulnerabilities and security solutions," in IEEE xplore, Wireless Communications, Networking and Mobile Computing (WiCOM 2015)
[12] Sonali Patra, N C Naveen, Omkar Prabhakar, "An automated approach for mitigating server security issues," in IEEE xplore, 2016, Recent Trends in Electronics, Information & Communication Technology (RTEICT)
[13] J. -M. Lee and S. Hong, "Keeping Host Sanity for Security of the SCADA Systems," in IEEE Access, vol. 8, pp. 62954-62968, 2020, doi: 10.1109/ACCESS.2020.2983179
[14] Danish Javeed, Umar Mohammed Badamasi, Cosmas Obiora Ndubuisi, Faiza Soomro & Muhammad Asif., "Man in the Middle Attacks: Analysis, Motivation and Prevention," International Journal of Computer Networks and Communications Security VOL. 8, NO. 7, July 2020, 52–58
[15] Iyas Alodat, "Effect of Man in the Middle attack on the network performance in various attack strategies," International Journal of Network Security & Its Applications (IJNSA) Vol.13, No.3, May 2021
[16] Wael Alosaimi, Mazin Alshamrani and Khalid Al-Begain, "Simulation-Based Study of Distributed Denial of Service attacks prevention in the cloud," in IEEE xplore, 2015, Next Generation Mobile Applications, Services and Technologies.
[17] May A Alotaibi, Asalah F Altwairqi, Abeer F Alotaibi and Sabah M Alzaharni, "DISTRIBUTED DENIAL OF SERVICE ATTACKS SIMULATION AND DEFENSE", International Journal of Advanced Research in Engineering and Technology (IJARET) Volume 11, Issue 10, October 2020, pp. 1606-1620
[18] ilvia Bravo , David Mauricio, "Systematic review of aspects of DDoS attacks detection", Indonesian Journal of Electrical Engineering and Computer Science Vol. 14, No. 1, April 2019, pp. 155~168
[19] Jaeil Lee, Yongjoon Lee, Donghwan Lee, Hyukjin Kwon, Dongkyoo Shin, "Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups", Received March 30, 2021, accepted May 25, 2021, date of publication May 31, 2021, date of current version June 10, 2021
[20] Hossein Abroshan, Jan Devos, Geert Poels, Eric Laermans, "COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic", Received August 7, 2021, accepted August 28, 2021, date of publication August 30, 2021, date of current version September 10, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY