IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 11, November 2024| DOI: 10.15680/IJIRCCE.2024.1211039

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Systematic Approach to Cyber Attack Modeling for Private Network Protection

Mr.Sunil J, Keerthan J, Sumanth T R

Assistant Professor, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

ABSTRACT: The world's most difficult problem is cyberattacks. Cyberattacks on digital systems and businesses are becoming more frequent these days. Infrastructure, connectivity, innovation and use of new digital technologies, and reliance on digital tactics are all changing daily. The breadth of the cyberthreat has greatly expanded. Attackers are currently developing malware programs in Python, C, C++, Java, SQL, PHP, JavaScript, Ruby, and other languages with increasing sophistication, organization, and professionalism. Cyber-attack planning is made possible by precise attack modeling techniques, which can be swiftly implemented during another active cyberattack. By extending the current model, this research seeks to develop a new cyber-attack model that will improve comprehension of the network's weaknesses. Additionally, it aids in defending the business or private network infrastructure against potential cyberattacks.The ultimate objective is to use attack modeling approaches to effectively address cyberattacks. Cybercrime has affected a lot of organizations, businesses, authorities, industries, and people these days. to carry out attacks using our approach in any environment with access to a firewall, DMZ, honeypot, and other security measures.

KEYWORDS: DMZ, Firewalls, Honeypot, Cyber Attack, Cyber Threat, Network Threat, Python, Payload, Backdoor, Network Vulnerabilities, Private Network, LAN.

I. INTRODUCTION

Our economy and civilization's infrastructures have been greatly improved, primarily by computer technology and sophisticated technological solutions [1]. According to the Symantec cybercrime report, as cyber-security grows, computer technology vulnerability rises greater harm. April 2012 [2]. As users continue to exploit computer networks, cyber-security is quickly gaining ground.

Many experts in cyber security think that malware is the tried-and-true method of introducing malevolent intent to undermine cyber defenses in cyberspace [3]. Network vulnerabilities are found by cyberattack models, which aid in defending networks against further intrusions [4]. We have the most up-to-date information on cyberattacks and security thanks to several books and publications. Following the analysis, we discovered that although security tools like firewalls, honeypots, DMZs, and antivirus software are available to stop attacks, the paradigm is insufficient for cyberattacks. The gadgets are too modern at the moment. Regretfully, the quantity of cyberattacks is quite low, and even earlier models fail to capture all the necessary characteristics of a cyberattack [5]. Therefore, we must come up with a variety of easily understood models. We will, however, put out a novel cyberattack model. With this model, we can use the internet to attack the private network. Since the target machine or server has numerous security features like a firewall, DMZ, honeypot, etc., we mostly target employees, IT specialists, and system administrators rather than the target machine directly. In order to create a cyberattack model and get beyond popular antivirus software, the study examines the current cyberattack model.

As internet services become more and more popular, this cyberattack approach may be used frequently and quickly. The study examines a variety of data regarding businesses and the industry, including the many kinds of event attacks. Numerous points, including operating system access, private network access, backdoor construction, evading the main antivirus program, etc., can be exploited by this presentation style.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This study's primary goal is to develop a model of a contemporary cyberattack that can detect network infrastructure weaknesses in any business and allow cyber security professionals to address their issues prior to being compromised and increase staff members' awareness of cyber security. A few assessments of cyberattack security and modeling methodologies are available. under the present circumstance. We've discovered that it employs many methods.

Every technique offers intriguing insights on a cyberattack [6]. According to several research, they make the cyberattack model far more effective. Nevertheless, different models cannot compromise the most recent security system. We have put forth a plan for creating cyberattacks in this work. We have developed a real-time assault model design environment.

II. LITERATURE SURVEY

The current work of the suggested model is presented in this section. Attack Graph, Attack Vector, Attack Surface, Attack Tree, and Diamond Model are a few methods for examining the cyberattack [20] – [23]. The three attack modeling approaches—Kill Chain, Diamond Model, and Attack Graph—for cyberattack modeling were described by Hamad et al. However, the drawback was that there was no real-world experiment to gather data for comprehending cyberattacks. Simeon and associates. suggested event-based systems and apps and described the circumstances behind the security flaws. Nonetheless, code analysis, encryption, and other methods are used in contemporary security solutions. However, this study has been the sole method authorized for constructing the assault model [4].

Nabi et al. presented an incident attack simulation that reused the design specification from the current application while framing the vulnerability using the Uppaal tool [24].

Wagner and associates. offered a structure that makes the system appear to interact with a potential assessment. The administrators of many network platforms were designed to simulate and evaluate certified and uncertified hardware in the defender frameworks. The agent-based simulation technique is shown by the scenarios [25].

III. CYBER ATTACKS

We outline the different types of event attacks in this section. Additionally, provide a succinct explanation of every assault that took place on the target system. The security flaws exposed based on the communication mechanism are reflected in our attacks [8].

We concentrated on local networks when creating event attacks. Organizations' information on their systems is secret, and employee data is essential to the business. In certain situations, we will start by aiming for the employees' data in order to gain access to the main system through their network. The various kinds of event attacks have been identified in the work to date:

• DNS (Domain Name Server) Spoofing: It preserves evidence of domains such as an online phone book and corresponds to IP addresses. It uses domain names to exchange IP addresses [9].
• Sniffing: This attack may involve scanning data packets and sniffing network credentials. A hacker transmits a contracted part of the information and maintains the privacy of the data. A scan can be used to decipher information that is not entirely encoded [10]. The hacker will attempt to identify and obtain credentials such as a password, email, FTP, database, etc. after gaining access to the network by spoofing [11].
• Eavesdropping: An event involving private and sensitive information may be observed by a malevolent node. It should only be accessible to the designated components [8].
• Malware is a type of malicious element that hackers may use without authorization. transferring the port forwarding variables in accordance with each strike hole Forwarding GET requests to the system is the first step in the network address translation process and revealing the specific computers that have been assembled [12].
• Collusion: Two malevolent actors may band together to take advantage of the target system's features or resources [8].
• Denial of Service (DoS) assault: This kind of assault can render a computer inoperable, preventing users from accessing the system or network [13]. It focuses on restarting the system or network and blocks the target system's massive storage [11].

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

• Ping of Death: Because the system must be able to maintain its functionality, attackers will send a massive ping packet to the target system in order to bring it down. boosting the massive ping packets [14].
• Interception: An event can be halted by a malevolent element.
It can return erroneous answers and is intended to be communicated to other items [8].
• Phishing Mail Attacks: Phishing is an email-based attack tactic used to steal login credentials and user information. In order to obtain the victim's detailed information, an attacker mostly inserts a malicious software inside emails and instant messages by pretending to be the legitimate source of the content. This assault could target all computer platforms and networks. [15] through [19].

IV. METHODOLOGY

A sophisticated new cyberattack model has been put forth by us. This model's key phenomenon is the ability to attack a private network in any system or organization that is completely unrelated to the internet, but that uses both the internet and the private network at the same time.

The goal of our strategy is to give an attacker a solid basis on which to launch an attack on a system or organization if they simultaneously use private networks and the internet. The suggested model's block diagram is shown in Figure 1 as follows.

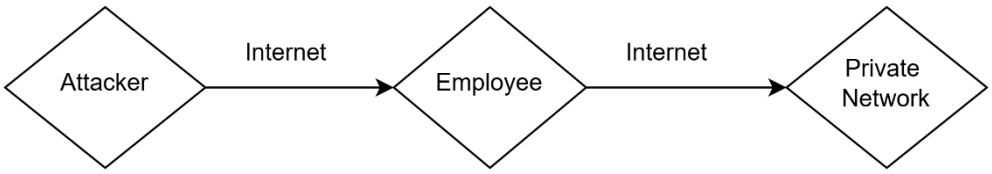

Fig 1. The Flowchart of the proposed system

The typical survey must also take into account the hazards connected to each assault as well as how an attacker could successfully exploit any vulnerabilities. The generated pseudocode in Algorithm 1 is part of our suggested attack model. Despite the highest level of security, we think our new attack model can gain access to any operating system, including iOS, Linux, Android phones, and Windows. We have already gotten past 55 antivirus products, therefore the effectiveness of our delivery strategy will determine how successful this attack is. When it comes to penetration testing, the distribution mechanism is crucial.

A. Information Gathering

The process of gathering data about servers and computer systems is called footprinting. We employed a variety of technologies, including Python, C, C++, SQL, JavaScript, PHP, Java, Ruby, and more, to obtain the victims' information. to use programming to learn more about the businesses' websites, IP addresses, domain names, DNS names, Netblocks, and social networks connected to an individual's name. First, we use the Internet to get data from company personnel. Since employees leave online traces when they access social media sites like Facebook, LinkedIn, and others, there is an additional method to learn more about them.

Algorithm 1: Cyber Attack Model
Data: Gathering Information
Result: Finally Attacked and Exploited
while Target is Not Found, do
Start Gathering Information
Target1 = Primary Target Employee
Target2 = Amied Target
Start Program to Attack = Target1 if Port
Scanning is Success then
Preparing Trojan Backdoor/Rootkit
else result → Start Scanning Another, Employee
end

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

if Sending Payload then
Bypasss Anitvirus Program
end
if Successfully Delivery Payload to Target1 then
Aimed to Target2
else Try to Delivery Payload to Target1
end
if Successfully Delivery Payload to Target2 then
Result → Attacked and Exploited
else
Result → Not Attacked
end
end

B. Target

Finding the target to enter the system is the primary motivation. We concluded that the target system is extremely protected with several security systems, such as a honeypot, DMZ, IDS & IPS, etc., after obtaining all the victim's information. Because of a private network or DMZ, we are unable to establish a direct connection to the target server. For this reason, we must split our attack procedure into two steps. Two targets were chosen: the aimed target and the primary objective. To guarantee a successful attack, target selection and attack strategy are crucial. To ensure we don't miss any targets, we devised a different strategy. A few employees' email addresses were not found. We take this action as a result. We used social media to send them a variety of links. The payload was automatically installed on the employee's machine when they clicked on those URLs.

C. Delivery

The target system can be accessed via a variety of delivery techniques. However, we have seen particular concepts and situations to target. Following that, we decided on the delivery method as, for all hackers, email is the most popular. It also depends on the type of data we have already gathered. Sending a payload or virus via email is the simplest method of distribution. No single technique can guarantee that the attack will be successful. However, it is occasionally necessary to refrain from attacking in order to obtaining the target system's basic credentials. Information-gathering techniques are common in browser-based assaults.

In such scenario, we attempt to install the malware payload on the victim's machine once the user accesses the infected webpage, which is the initial attempt to acquire the required system credentials. The victim's movement must be taken into consideration when choosing the delivery method. In this instance, we choose email delivery to infect the victim's PC with the malicious payload or backdoor. After receiving this backdoor/payload, the victim is unable to control the attacker's backdoor/payload until they execute it. We must either transmit the file again or look for an alternative distribution technique if the attacker does not run it.

D. Main Objective

We launched our assault on the main target in this step. The proliferation of computer devices on the internet gives us the ability to hack, as seen in Figure 1. To get more precise data, we employed both the sophisticated IP scanner and a second IP scanner. To find out how many IP addresses the target network is using, we scan it. We also discovered how many of the target network's ports are open or closed.

E. Backdoor Generation

To get to the main target, we must create a backdoor. Therefore, a backdoor can be built in a number of methods. Here, we developed a Python backdoor software. We have all of the Kali server's information inside that backdoor, so when a victim clicks on it, a terminal will open instantly and a reserved TCP connection will be established with the server. The victim's computer will then be completely accessible to the attacker. We can target any computer or server locally connected to the victim's computer within the private network once we have gained access to their computer or network. Our primary responsibility is to infect the computers or servers of these victims with malware.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

We frequently had to update this backdoor because the system was updated daily, but the issue is that the victim's computer permits them to update their antivirus software on a regular basis, so we can allow list malware on the victim's computer so that the malware functions properly after the antivirus update and needs to be updated right away.

F. Bypass Antivirus Program

Antiviruses are a major annoyance for attackers. Whether or not the prey system has installed antivirus software determines whether or not the attack will succeed. Nevertheless, bypass is typically the last major issue for attackers; depending on the current environment, we should try to apply all systems one at a time. There are a number of ways to avoid antivirus programs, including encoder, packer, binary editing, changing payload signatures, changing source code, and changing payload versions.

The attacker might quickly alter the malware if he managed to obtain its source code. For instance, switch the system to if-else if there is a way to change the order. No noteworthy procedure should be impacted by the code's operation. A hacker can alter a number of things, such as modifying settings, changing uppercase to lowercase, etc. perhaps changed to int TARGET=0; from int target=0; File signatures are used by antivirus software to identify malware. The pattern is distinct and only a few dozen bytes in size. It has the ability to identify viruses and, in certain situations, eliminate them. when we create backdoors that are invisible to antivirus software, albeit occasionally two or more programs are able to identify them.

To get around these programs, we have demonstrated how to use a text editor to open the backdoor and change its code. When an antivirus program examines the signature file, the backdoor code will attempt to change it. The signature file won't resemble other malicious files in appearance. If the file appears to be unique, the antivirus software will declare it to be a typical file. There is no malicious code in it. Nevertheless, we employed this strategy in our suggested approach. We searched for a typical character for text or sentences that were readable. In order to create the signature file, we changed the characters. It will enable us to get around antivirus software. To make this code appear distinct from antivirus software, we added random characters. However, we consistently maintained the same number of characters and did not add or remove any. We took great care to avoid overwriting any of the code in the process. Thus, it is saved by this altered code.

To get around the antivirus, we created a backdoor. Now, we'll use Hex Editor to open that payload or backdoor. Use HxD to open the payload/backdoor in Figure 2 [26]. We will modify the payload/backdoor using Hex Editor.
There is no guarantee that antivirus software will be able to identify it if we alter this value. In order to determine whether or not the antivirus software can identify it, we progressively alter the value. We eventually succeeded in getting past 55 antivirus programs after using this method.

G. Target Aimed

This stage gives us access to the organization's intended target. On the target machine, we installed a few apps. Consequently, certain programs transmit the data to our Kali server. We install malware right away, such as a keylogger and DDoS attack software, if we are successful in sending a payload or backdoor to the target. Disable antivirus software or include a white list payload or backdoor if at all possible.

Additionally, conduct a thorough audit of every computer as required. For example, determine the type of job this victim's computer performs and the most often used program. Then, let's call the backdoor something that sounds similar to that software. The victim is unaware that there has been computer hacking.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

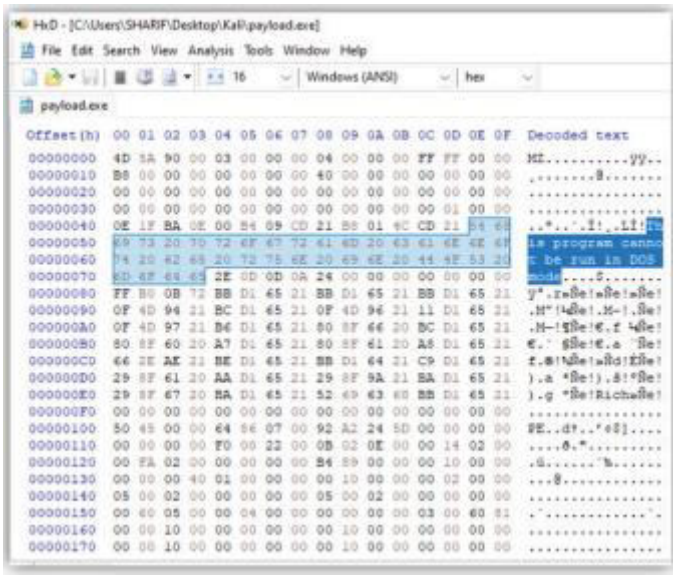

Fig 2. Bypass Antivirus Program

V. EXPERIMENTAL RESULTS

In this section, we embellish the outcome of our efforts and the proportion of incident assaults involving penetration testing of the suggested approach.

A. Setup for Experiments

This semester, we utilized five servers such as Windows 10, Ubuntu. 20.04, Windows Server 2021, CentOS 8, and Kali Linux 2021. These servers are situated in various geographic locations. We utilized the A + hosting Inc data center to perform this penetration testing.

Our servers utilize the VMware vSphere hypervisor for power. Every of our server setups is four vCPU Core Intel Xeon E5 processors, 200 GB SSD storage, and 8 GB of RAM. The kali server, along with Windows 10, Ubuntu 20.04, and Windows server 2021, is linked to a 10 Gbps network port that has a public IP address. The CentOS 8 is linked to a local IP network. The physical locations are as follows: Centos 8 and Windows 10 are located in a USA Datacenter, Windows Server 2021 is in a Singapore Datacenter, and Ubuntu 20.04 is situated in an Australia Datacenter. We employ this Kali server as the attacker's computer. Windows Server 2021 and Ubuntu 20.04 are two digital targets. It is worth noting that the virus definitions for Microsoft Windows Defender are current, and the firewall is active.

B. Contrasting

The conventional model of cyber-attacks cannot compromise any private network, computer, or server [5] [7] [10] since the private network lacks a direct connection to the internet. Nonetheless, this model may be able to breach any private network via an employee of the company. We have the ability to create differ various types of assaults utilizing this model, like Ping of Death, DNS Spoofing, Denial of Service Attack, Phishing Attempt, Interception Malicious software and network monitoring. Conversely, the classic assault The model is unable to execute the aforementioned attack due to the absence of a direct link in a private network from the web. Cybercriminals assault firms' private systems by utilizing an employee as a entrance. In general, like with any assault, it is necessary to dispatch payload .exe is a common technique but vital for any Windows System.

C. Outcomes & Discussion

This section presents the outcomes and discourse of the suggested cyber-attack framework along with the corresponding evaluation of performance-oriented attack modeling utilizing Kali Linux. Earlier, we indicated that the Kali Server has the IP 45.63.60.195 and the Windows 10 target has the IP 72.18.198.144. Ultimately, we reached the

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

intended system, as illustrated in figure 3. This image indicates that Windows 10 now provides complete computer access to the Hacker. Windows 10 and CentOS 8 are each linked to a private network. We can now target the private network computer since we already have access to it.

In our attack framework, we achieve optimal results for the attacks, including Ping of Death, DNS Spoofing, DoS Attack, Phishing Attack, Eavesdropping, Malware, and Sniffing. Our suggested model gained access to the Windows 10 operating system. The proportion of the attacks in our suggested method is displayed in Fig 3.

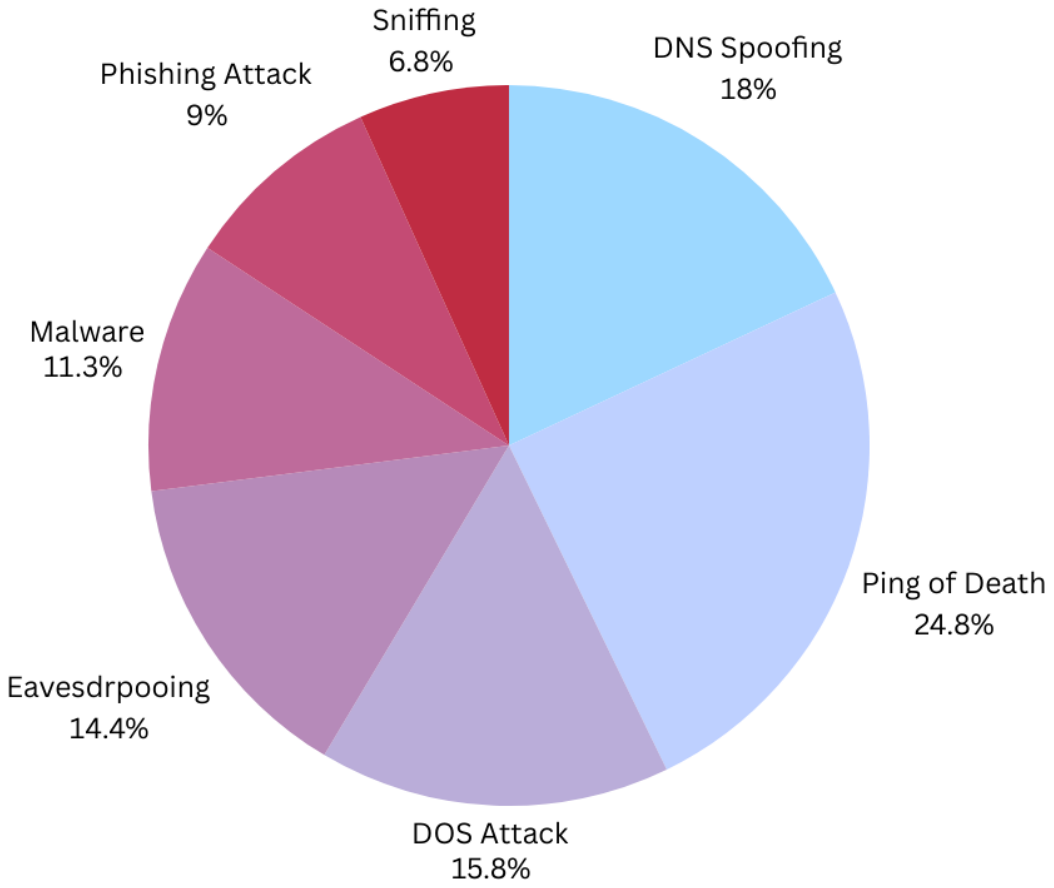

Fig 3. Event Attacks

VI. CONCLUSION

The number of cyberattacks is increasing daily. In order to gain access to the system, attackers are clever enough to produce fresh malware. Web portals and e-commerce websites are now being used by both small and large organizations. Schoolchildren are also engrossed. on a computer or the internet [27]. Therefore, we must all increase cyber awareness.

An attack method for computers and private networks was provided in this paper. Furthermore, we discovered that the private network is still vulnerable to cyberattacks using the attack model. Therefore, everyone must use caution when utilizing the internet and private networks. A private network may become the target of a cyberattack if a compromised computer is physically linked to a private network.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

[1] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 973–993, 2014.
[2] M. Fossi, G. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, J. Blackbird, M. K. Low, D. Mazurek, D. McKinney et al., "Symantec internet security threat report trends for 2010," Volume XVI, 2011.
[3] H. Ha, "Online security and consumer protection in ecommerce an australian case," in Strategic and pragmatic e-business: Implications for future business practices. IGI Global, 2012, pp. 217–243.
[4] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-attack modeling analysis techniques: An overview," in 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW). IEEE, 2016, pp. 69–76.
[5] F. Chowdhury, "Modelling cyber attacks," International Journal of Network Security & Its Applications (IJNSA) Vol, vol. 9, 2017.
[6] M. Younas, I. Awan, and J. El Haddad, 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). IEEE Computer Society, 2016.
[7] H. Al-Mohannadi, I. Awan, J. A. Hamar, A. Cullen, J. P. Disso, and L. Armitage, "Cyber threat intelligence from honeypot data using elasticsearch," 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), pp. 900–906, 2018.
[8] Y. K. Lee, D. Nam, and N. Medvidovic, "Identifying inter-component communication vulnerabilities in eventbased systems," Technical Report: USC-CSSE-17-801, Tech. Rep., 2016.
[9] N. Tripathi, M. Swarnkar, and N. Hubballi, "Dns spoofing in local networks made easy," in 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, 2017, pp. 1–6.
[10] P. Anu and S. Vimala, "A survey on sniffing attacks on computer networks," in 2017 International Conference on Intelligent Computing and Control (I2C2). IEEE, 2017, pp. 1–5.
[11] M. A. Khatun, N. Chowdhury, and M. N. Uddin, "Malicious nodes detection based on artificial neural network in iot environments," in 2019 22nd International Conference on Computer and Information Technology (ICCIT). IEEE, 2019, pp. 1–6.
[12] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016, pp. 195–200.
[13] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges," IEEE Access, vol. 4, pp. 1375–1384, 2016.
[14] E. Gelenbe and Y. Yin, "Deep learning with dense random neural networks," in International Conference on Man–Machine Interactions. Springer, 2017, pp. 3–18.
[15] M. Adil, M. A. Almaiah, A. Omar Alsayed, and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," Sensors, vol. 20, no. 8, p. 2311, 2020.
[16] A. K. Al Hwaitat, M. A. Almaiah, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, "Improved security particle swarm optimization (pso) algorithm to detect radio jamming attacks in mobile networks," Quintana, vol. 11, no. 4, pp. 614–624, 2020.
[17] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Alkhasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," International Journal of Electrical and Computer Engineering (IJECE), vol. 10, no. 6, pp. 6461–6471, 2020.
[18] A. ALMAIAH and O. ALMOMANI, "An investigation of digital forensics for shamoon attack behaviour in fog computing and threat intelligence for incident response," Journal of Theoretical and Applied Information Technology, vol. 98, no. 07, 2020.
[19] ——, "An investigator digital forensics frequencies particle swarm optimization for dectection and classification of apt attack in fog computing enviroment (idf-fpso)," Journal of Theoretical and Applied Information Technology, vol. 98, no. 07, 2020.
[20] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, and E. Weippl, "Dark clouds on the horizon: Using cloud storage as attack vector and online slack space," 2011.
[21] P. K. Manadhata and J. M. Wing, "An attack surface metric," IEEE Transactions on Software Engineering, vol. 37, no. 3, pp. 371–386, 2010.
[22] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," Center For Cyber Intelligence Analysis and Threat Research Hanover Md, Tech. Rep., 2013.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[23] C. Phillips and L. P. Swiler, "A graph-based system for networkvulnerability analysis," in Proceedings of the 1998 workshop on New security paradigms, 1998, pp. 71–79.
[24] F. Nabi, J. Yong, and X. Tao, "A novel approach for component based application logic event attack modeling." Int. J. Netw. Secur., vol. 22, no. 3, pp. 435–441, 2020.
[25] N. Wagner, R. Lippmann, M. Winterrose, J. Riordan, T. Yu, and W. W. Streilein, "Agent-based simulation for assessing network security risk due to unauthorized hardware," in Proceedings of the Symposium on Agent-Directed Simulation, 2015, pp. 18–26.
[26] M. Horz, "Hxd-freeware hex editor and disk editor," 2008. ¨
[27] P. K. Nalla, R. K. Gajavelly, J. Baumgartner, H. Mony, R. Kanzelman, and A. Ivrii, "The art of semi-formal bug hunting," in 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE, 2016, pp. 1–8.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details