

Probing the depths: assessing the efficacy of the two-tier deception-driven security model

Anazel P. Gamilla¹, Thelma D. Palaoag², Marlon A. Naagas¹

¹Faculty of Department of Information Technology, College of Engineering, Central Luzon State University, Science City of Munoz, Philippines

²Faculty of College of Information and Computer Science, University of the Cordilleras, Baguio, Philippines

Article Info

Article history:

Received Jun 12, 2024

Revised Aug 1, 2024

Accepted Aug 5, 2024

Keywords:

Cybersecurity

Cyberthreats

Deception model

Decoys

Honeypot

ABSTRACT

In the age characterized by relentless cyber threats, the need for innovative and proactive security measures has never been more important. Deception is defined as the deliberate structure of tricks, traps, and false information to mislead and discourage threats, while providing timely warning signals and useful information to defenders. The two-tier deception-driven security model's implementation focuses on applying deception security techniques to deceive potential attackers and protect network resources, with an emphasis on a proactive defense approach. The study emphasized the deployment and deep testing of the model, which aims to assess its efficacy and feasibility in real-time practice. The study shows that the two-layered approach effectively defends the network within the multiple layers using a combination of decoys, honeypots, and deceptive network segments. The deception security model effectively prevents and confuses potential threats, improving the network's overall resilience and threat defense capabilities. The findings suggest that integrating deception techniques into cybersecurity frameworks can provide a robust layer of protection against evolving cyber threats. Furthermore, this research contributes to the ongoing discourse on proactive cybersecurity strategies and offers practical insights for improving network defense mechanisms.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Anazel P. Gamilla

Department of Information Technology, Faculty of Engineering, Central Luzon State University

Science City of Munoz, Philippines

Email: apgamilla@clsu.edu.ph

1. INTRODUCTION

In a digital era where cybersecurity threats are more sophisticated than ever, traditional security measures often fall short [1], [2]. In the landscape where both persistence and threat require a continuous evolution of network security to be comprehensively improved, these older methods typically focus on passive defenses and securing the perimeter, which doesn't quite cut it anymore [3]-[5]. Once these defenses are breached, organizations find themselves drastically underprepared to stop a tacker from causing serious damage. Issues such as high false positive rates plague most current strategies, such as using machine learning for anomaly detection or deploying various types of intrusion detection systems. Furthermore, once attackers penetrate the network, these systems struggle to effectively engage or confuse them [6]. They also fail to reveal much about the attackers' tactics and motivations, which are essential for refining security strategies.

In response to these threats, the development of an imperative security model was imposed to maintain operational continuity [7], [8]. Among the emerging paradigms in cybersecurity, deception-driven

security models have gained increasing attention for their potential to enhance threat detection and mitigation capabilities [9]. By weaving in deception techniques like decoys, traps, and misinformation directly into the network fabric, this model doesn't just block attackers, it actively engages them [10]-[13]. This engagement allows for a deeper analysis of their methods and strategies, turning every attempted attack into an opportunity for insights [14]-[16].

Building on the foundational concepts of the two-tier deception-driven security model, this study seeks to further refine and enhance the deception-driven security model by introducing additional layers of deception and testing their effectiveness in a controlled environment. The goal of the study is to deploy deep testing in the created model in a controlled environment, assessing its ability to delay attacks, deceive adversaries, and gather actionable intelligence from these interactions. By building upon past research and incorporating real-world testing scenarios, this study contributes to advancing the understanding of deception-driven security paradigms and their role in modern cybersecurity frameworks [17], [18]. The investigation contributes to the ongoing discourse on deception-driven security approaches and informs cybersecurity practitioners and decision-makers about the efficacy of adopting such models, which could result in better and more adaptable security solutions.

2. METHOD

The study tests the effectiveness of a controlled testing environment using a two-layered deception architecture. A controlled testing environment was established, utilizing various penetration testing techniques to simulate real-world cyber attacks. The primary objective was to assess the model's ability to detect, divert, and gather intelligence on unauthorized access attempts.

2.1. Network architectural model

The design and implementation of the proposed two-tier deception security model cover the architectural design and the deception classification flow for the two layers of the model. Each layer intends to trap and divert an internal or external threats, allowing the defense time to investigate the perpetrator's information and determine their intentions, strategy, and intended target. Figure 1 shows the division of workflow for an intensive network defense through deception. The core layer plays a main role in controlling threats by directly implying the requirements needed before the packets go deep into the network. Layer 2 was known to directly control the flow in the internal network, which also applies the same concept to deception security. Controlling the path of the attackers by planting decoys and traps with the purpose of testing different parameters to check vulnerabilities and luring them to access decoy servers makes it more powerful to completely shift the reconnaissance as advantage. The public network (office) or server farm is designed to efficiently collect as many exposed packets as possible, using both real and fake servers.

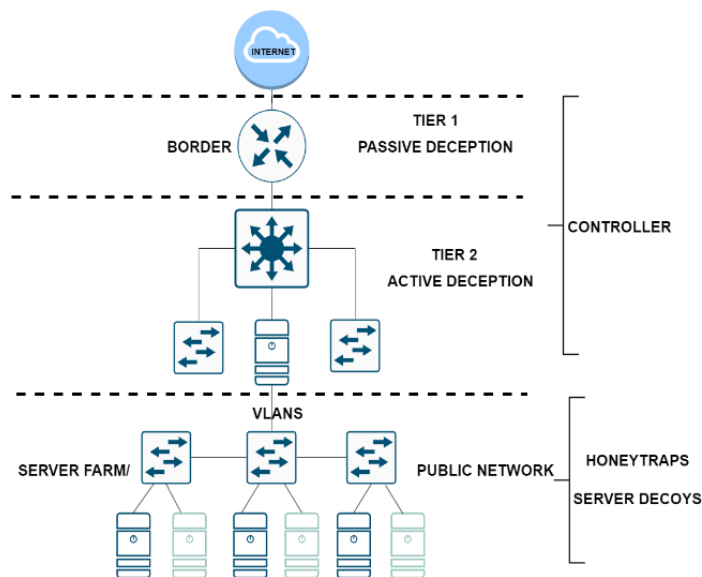


Figure 1. Tier deception security architecture

2.2. Policy and process flow

The created policy was implemented on the core layer of the network, flowing towards the lower level with a minimum amount of device resources. The false addresses and controlled process flow were added in the core’s NAT rules to manage the unwanted payloads and lured the attackers and directed them into traps and decoys while utilizing the device resources [19], [20]. The second layer of the deception model actively engages attackers by using advanced decoys and traps. These elements are designed to look like vulnerable parts of the network, drawing perpetrators in. As they interact with these decoys, it expose their method and strategies [21], [22].

2.3. Components background

The research includes an understanding of the background of critical elements such as network architecture and managed decoys and traps. The network architecture serves as the foundation for understanding the structure, protocols, and communication pathways that define the system's connectivity and functionality.

2.3.1. Network architecture for penetration testing

The procedures, including information collection, scanning, exploitation, and post-exploitation evaluation, were carried out with the utmost integrity, confidentiality, and authorization [23], [24]. After the confirmation of the effectiveness of luring the attackers in the reconnaissance phase, this test was subjected to attacks with the intent to compromise legitimate servers to deeply assess the deception security model through the used of different tools and techniques. The diagram as shown in Figure 2 represents a two-tier deception-driven security architecture designed to enhance network defenses. At the core layer, firewalls and routers serve as the primary defense and attack point for the test, controlling traffic flow and applying firewall NAT rules to test payloads. The controller manages decoys and traps, diverting malicious traffic from critical infrastructure. A vulnerability test identifies open ports and addresses, and the core layer handles initial threat engagement. The second layer distributes traps across VLANs, capturing detailed attacker behavior. The network includes a DMZ zone for isolating exposed services, adding an additional layer of protection.

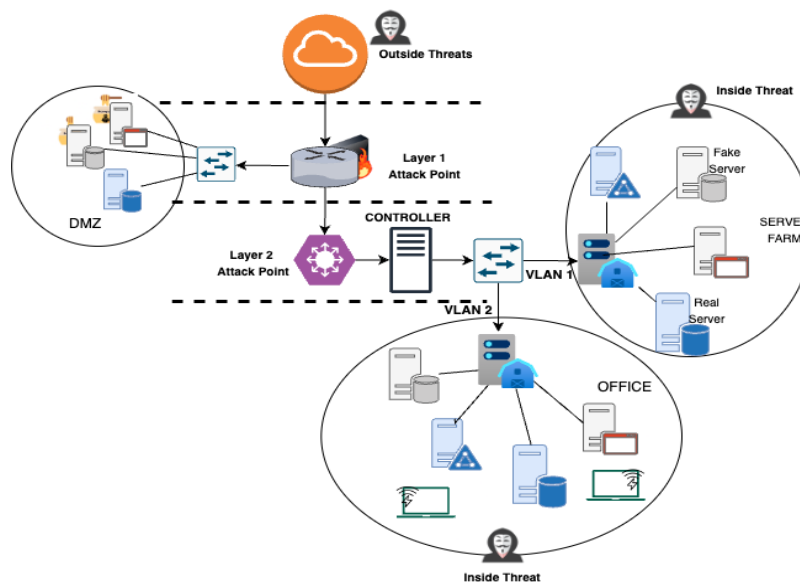


Figure 2. Test bed network diagram

2.3.2. Applied decoys and traps

In layer 1, passive deception is implemented by the core layer through the use of NAT rules. These rules generate a decoy by chaining dstnat and adding a destination address. The action is then set to log. The Figure 3 shows the sample setup of decoys that were scattered throughout the network to fully test the effectiveness of the traps. Different services were used in the penetration test, which was performed repeatedly and implemented in various perimeters, subnets, and vlans [25], [26]. This was divided based on

the deception network controller (DNC) table map to utilized and manage the distribution and effectiveness of the decoys and traps. This table helps in mapping the division of work and distributing the load effectively without burdening the resources at each layer and enhances the overall security posture [27].

Decoy Name	Services	IP Address	Apache files
DataServer	SSH - Interactive; TOMCAT;	192.168.2.251	
WebServer	APACHE;	192.168.2.250	"/usr/local/apache2/htdocs"
win10	NBNSCLIENT;	192.168.2.249	
AdminServer	FTP; SSH - Interactive; MYSQL; WEB- BASIC-AUTH;	192.168.2.248	

Figure 3. Sample list of decoys and traps

3. RESULTS AND DISCUSSION

This study looks at how a two-tier deception-driven security model can make networks more resilient against cyber threats. While past research has examined individual techniques like honeypots and decoys, it hasn't focused on how a multi-layered approach impacts overall network security. Multiple penetration tests were conducted to evaluate the efficacy of the two-tier deception-driven security model. This primarily focused on testing whether the implemented two-tier deception-driven security model could successfully block attacks through deception and utilized various techniques and tools, starting from the core layer of the network and extending to the lower levels [28], [29]. Each layer was subjected to a series of tests to determine its effectiveness in delaying and luring perpetrators to fake servers and honeypots.

Figure 4 illustrates the deep integration of the deception model within the network infrastructure. Each layer plays a crucial role in defending the network by diverting and blocking attacks, as well as providing valuable information to adjust strategies and observe attacker actions. This helps measure the efficacy and understand how the applied model works. The intended external and internal penetration attacks were both performed in the layer 1 and 2 attack points.

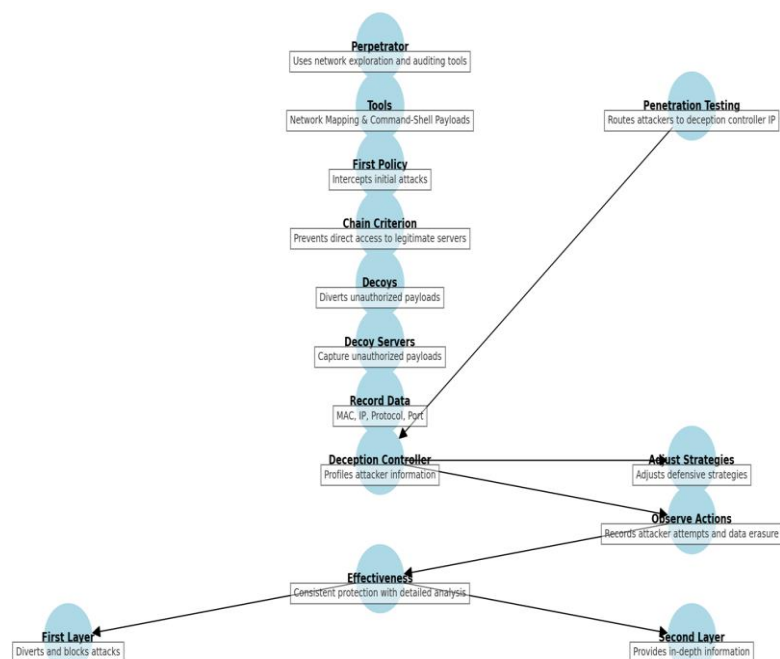


Figure 4. Deception-driven security model visual graph

3.1. Layer 1 attack point test result

The tests were conducted first in the layer 1 defenses as shown in the test bed network diagram above, focusing on the core layer's ability to detect, divert, and capture unauthorized access attempts by redirecting them from legitimate servers to decoys. Layer 1 defense resides on the border of the network with a core device that applies the policy and rules that were mentioned above. The intended perpetrator used network mapper and security auditing tools to discover and plot network hosts, services, and their associated attributes, passing them on to the core router's implemented rules.

As shown in Figure 5, the size of the payloads in the red circle indicates that the exploitation attack passes through the first policy, triggering the chain criterion and preventing the packet request from reaching a legitimate server. Instead, it is sent directly to the decoys, successfully diverting attention away from the real server. The target servers were unable to be infiltrated, as evidenced by the absence of any detected payload size as shown in the black circle in the first policy, labeled "Real Server". Furthermore, Figure 6 shows the perpetrators' exertions to infiltrate the fabricated servers in the central layer. The results obtain in the layer 1 passive deception effectively obtains information from the attackers using minimal resources.

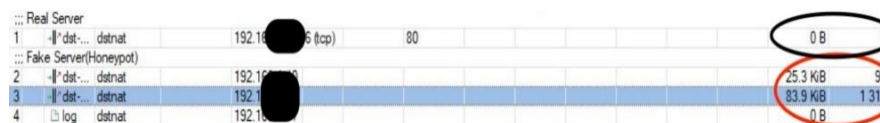


Figure 5. Penetration results in the layer 1 core packet flow

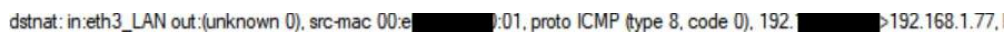


Figure 6. Core device log details of the attacks

3.2. Layer 2 attack point test result

The tests for layer 2 attack point focused on evaluating how well active deception techniques, such as strategically placed fake servers and honeypots, could capture detailed information about attacker behavior and attempts to access bait servers in the lower part of the network. The layer 2 active deception attacks were specifically targeted at strategically positioned fake servers and honeypots. The results show that it successfully records the source and destination addresses trying to access the bait server, as shown in Figure 7. Preemptive attacks effectively captured the network's MAC addresses and IP addresses, along with the protocol and port numbers, according to the captured data. The attempted attacks used SSH and remote services to check if the target IP address was accessible. This indicates that the second layer model successfully lured and captured the attempted attacks.

Another test result shown in Figure 8, reveals that the attackers were able to successfully travel to the host, or IP address, of the deception controller, waiting for an opportunity to lure them far enough to reach traps and decoys so they may collect information for an examination of a mitigation plan. This covers the specific reconnaissance attack type and the precise mechanism employed by the attackers to breach the decoy server.

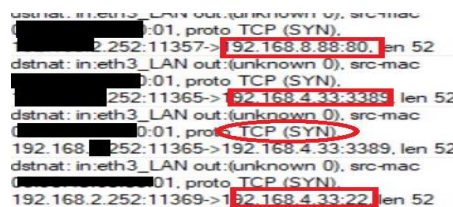


Figure 7. Server farm captured attack packets



Figure 8. Office internal penetration test results

In the last phase of testing, Figure 9 shows that it successfully captures details from the internal attacks on the decoys set by the controller. In Figure 10 illustrates how penetration testing allows attackers to access a decoy server and observe its actions and behavior. The attackers probed several directories and attempted to erase data from the server using common authentication methods. The results of the multiple tests above demonstrate the consistent success of the two-tier deception security model, which protects the network from the core layer. This model serves as a defense mode when attack payloads enter the network. The findings indicate that the attackers initially penetrated the fake servers or decoys, demonstrating the effectiveness of the packet filtering rules in luring them in.

The research findings above demonstrate the effectiveness of the two-tier deception security model in defending against malicious network access. The results reveal the perpetrators' attempts to exploit network exploration and security auditing tools. However, the applied rules successfully divert unauthorized payloads away from vital assets. By summarizing the information of source and destination addresses, including MAC addresses, IP addresses, protocol, and port numbers during preemptive attacks, the model effectively captures attempted intrusions. This illustrates the model's ability to capture details from preemptive attacks and showcases how attackers were lured to decoy servers.

```
> Frame 2: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Linux cooked capture v1
  Packet type: Unicast to another host (3)
  Link-layer address type: Ethernet (1)
  Link-layer address length: 6
  source: PcsCompu_e8:3a:cf ( [redacted] :3a:cf)
  Unused: 0201
  Protocol: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192. [redacted] 249, Dst: 192. [redacted] .250
  > User Datagram Protocol, Src Port: 137, Dst Port: 59603
  Source Port: 137
  Destination Port: 59603
```

Figure 9. Wireshark captured attack packets

DataServer	Coloc	SSH	SSH Command Execution: rm -r etc	192.168. [redacted]	192.168.2.252
DataServer	Coloc	SSH	Authentication request: Username: root and Password: admin	192.168. [redacted]	192.168.2.252
DataServer	Coloc	TCP	TCP Request: 192.168.2.252:24469 -> 192.168. [redacted] :22	192.168. [redacted]	192.168.2.252

Figure 10. Captured detailed attacks from the controller

3.3. CVSS impact assessment of preemptive attacks

The common vulnerability scoring system (CVSS) is an open framework to check the severity of common vulnerabilities, which was divided into four metric groups: base, threat, environmental, and supplementary, which all contribute to additional insight into the characteristics of a vulnerability [30]-[33]. CVSS provides a standardized and quantifiable method for evaluating the severity of vulnerabilities, which is evident in the results of our two-tier deception-driven security model. The vector string as shown in Figure 11 was derived based on the inputs from the CVSS which serve as a metric value to determine its scores.

AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H/E:F/RL:X/RC:C/CR:L/IR:L/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:L/MA:L

Figure 11. CVSS v3.1 vector

The base, temporal and environmental metrics as shown in Figures 12 ,13, and 14, reinforce the importance of maintaining alertness in network protection. The temporal score, which considers factors such as exploit maturity and remediation levels, and the environmental score, which evaluates the specific context and impact within the organization's environment, both underline the dynamic nature of threat landscapes. These scores serve as a forewarning to always be alert when it comes to protecting the network from attackers, emphasizing the need for continuous monitoring and adaptive defense strategies to mitigate evolving threats.

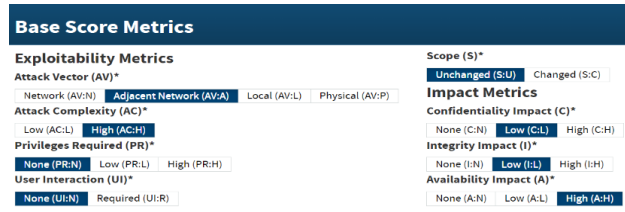


Figure 12. Based score metrics



Figure 13. Temporal score metrics

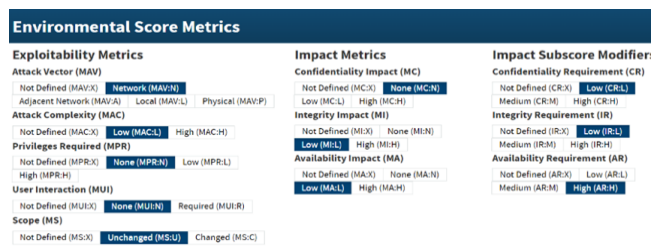


Figure 14. Environmental score metrics

The evaluation of the executed penetration attacks in Figure 15 reveals a base rating of 6.4, indicating a medium critical level. This indicates that even during the network's reconnaissance phase, there is a significant influence on the severity of vulnerabilities within the facilities. The temporal and environmental variables also gathered almost the same severity when constant changes in the environment and threat factors were considered. The overall summary of the CVSS in a controlled environment reached a severity score of 6.4, which shows that it is important to understand and continuously maintain defense against attacks, not only focusing on filtering and blocking attacks but also identifying, assessing, and mitigating risks by knowing what we are dealing with before a full-scale attack occurs.

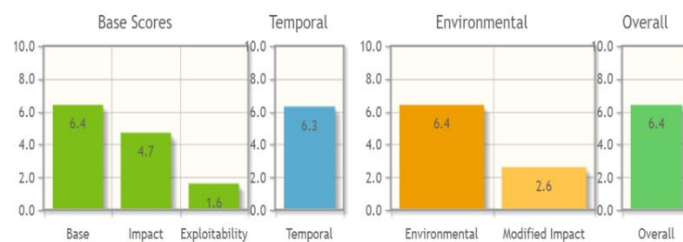


Figure 15. Summary of assessment vulnerabilities

Based on the test results above, we found that implementing the model improves network resilience against cyber threats. The data shows that this approach effectively diverts and confuses attackers, as evidenced by the increased interaction with decoy servers instead of real servers. Details and methods used by attackers were captured much more effectively with the proposed method, showing that the model can gather useful information while protecting the network's resources.

Our research demonstrated its ability to protect critical network resources and gather valuable intelligence on attacker methods. The approach not only improves the network's resilience against cyber threats but also provides a robust foundation for further research and practical applications in diverse network environments. For additional results, further studies could examine its performance in more complex and dynamic real-world network environments. Expanding the scope to include emerging and less common threats could provide a more complete understanding of the model's capabilities and resourcefulness.

4. CONCLUSION

The two-tier deception-driven security model has proven effective in enhancing network security and mitigating advanced cyber threats by integrating passive deception in the first layer to divert attackers and active deception in the second layer to engage dangers and provide defenders with crucial response time. The tests demonstrate the model's deep integration into the network infrastructure, with the first layer successfully blocking and diverting attacks while the second layer captures detailed information to refine defensive strategies. These findings indicate that diverting unauthorized payloads to decoy servers not only captures attacker details but also allows for adaptive defense strategies, creating a resilient and adaptive security environment. Implementing this model can significantly improve an organization's defense posture against cyber threats, offering valuable intelligence on attacker behavior to continuously enhance security measures. Adopting the security model is a practical and effective solution for proactive threat management, enabling organizations to better protect digital assets and ensure a more secure cyber environment for the community.

ACKNOWLEDGMENTS

The authors express their gratitude to the Central Luzon State University Information Systems Institute for granting us permission to utilize its facilities and network equipment for the execution and evaluation of our tests as part of the Deception-Driven Security research project.




REFERENCES

- [1] F. Babu, K. Sebastian, and K. Sebastian, "A review on cybersecurity threats and statistical models," *IOP Conference Series: Materials Science and Engineering*, vol. 396, p. 012029, 2018. doi:10.1088/1757-899x/396/1/012029
- [2] D. P. Möller, "Cybersecurity in digital transformation," *Advances in Information Security*, pp. 1–70, 2023. doi:10.1007/978-3-031-26845-8_1.
- [3] R. S. Dalal *et al.*, "Organizational science and cybersecurity: abundant opportunities for research at the interface," *Journal of Business and Psychology*, vol. 37, no. 1, pp. 1–29, 2021. doi:10.1007/s10869-021-09732-9.
- [4] D. Ashenden, R. Black, I. Reid, and S. Henderson, "Design thinking for cyber deception," *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2021, doi:10.24251/hicss.2021.240.
- [5] V. E. Urias, W. M. S. Stout, J. Luc-Watson, C. Grim, L. Liebrock and M. Merza, "Technologies to enable cyber deception," *2017 International Carnahan Conference on Security Technology (ICCST)*, Madrid, Spain, 2017, pp. 1-6, doi: 10.1109/CCST.2017.8167793.
- [6] F. J. Stech, K. E. Heckman, and B. E. Strom, "Integrating cyber-D&D into adversary modeling for active cyber defense," *Cyber Deception: Building the Scientific Foundation*, 2016, doi: 10.1007/978-3-319-32699-3_1.
- [7] S. Frey, "How to eliminate the prevailing ignorance and complacency around cybersecurity," in *Cybersecurity Best Practices*, M. Bartsch and S. Frey, Eds. Wiesbaden, Germany: Springer Vieweg, pp. 1-10, 2018. Doi: 10.1007/978-3-658-21655-9_1.
- [8] M. Saeed Jawad and M. Hlayel, "Intelligent cybersecurity threat management in modern information technologies systems," *Lightweight Cryptographic Techniques and Cybersecurity Approaches*, 2022. doi:10.5772/intechopen.105478
- [9] J. C. Acosta, A. Basak, C. Kiekintveld, N. Leslie and C. Kamhoua, "Cybersecurity deception experimentation system," *2020 IEEE Secure Development (SecDev)*, Atlanta, GA, USA, 2020, pp. 34-40, doi: 10.1109/SecDev45635.2020.00022.
- [10] K. J. Ferguson-Walter *et al.*, "Cyber expert feedback: experiences, expectations, and opinions about cyber deception," *Computers & Security*, vol. 130, p. 103268, 2023, doi: 10.1016/j.cose.2023.103268.
- [11] M. H. Almeshekeh and E. H. Spafford, "Cyber security deception," *Cyber Deception*, pp. 23-50, 2016.
- [12] G. Briskin *et al.*, "Design considerations for building cyber deception systems," *Cyber Deception: Building the Scientific Foundation*, pp. 69-95, 2016.
- [13] J. Happa, T. Bashford-Rogers, A. J. Van Rensburg, M. Goldsmith, and S. Creese, "Deception in network defences using unpredictability," *Digital Threats: Research and Practice*, vol. 2, no. 4, pp. 1–26, 2021. doi:10.1145/3450973.
- [14] C. Gao, Y. Wang, and X. Xiong, "A cyber deception defense method based on signal game to deal with network intrusion," *Security and Communication Networks*, vol. 2022, pp. 1–17, 2022. doi:10.1155/2022/3949292.
- [15] Attivo Networks, "Accenture/Ponemon Institute: The cost of cybercrime," *Network Security*, vol. 2019, no. 3, pp. 4-4, 2019. doi:10.1016/s1353-4858(19)30032-7.
- [16] C. S. Georgina, F. Sakinah, M. R. Fadholi, S. Yazid, and W. Syafitri, "Deception based techniques against ransomwares: a systematic review," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 3, pp. 529-553, 2023, doi: 10.52436/1.jutif.2023.4.3.886.
- [17] A. Reeves and D. Ashenden, "Understanding decision making in security operations centres: building the case for cyber deception technology," *Frontiers in Psychology*, vol. 14, 2023, doi: 10.3389/fpsyg.2023.1165705.
- [18] D. Fraunholz and H. D. Schotten, "Strategic defense and attack in deception based network security," *2018 International Conference on Information Networking (ICOIN)*, 2018. doi:10.1109/icoin.2018.8343103.




- [19] L. Zhang and V. L. L. Thing, "Three decades of deception techniques in active cyber defense-retrospect and outlook," *Computers & Security*, vol. 106, p. 102288, 2021. doi: 10.1016/j.cose.2021.102288.
- [20] D. Kusumadihardja, "Fools your enemy with MikroTik," 2016, [Online]. Available: SlideShare, <https://www.slideshare.net/zonicorb/fools-your-enemy-with-mikrotik-67235380> (accessed Feb. 15, 2024).
- [21] A. P. Gamilla, T. D. Palaoag, and M. A. Naagas, "Enhancing reconnaissance security: a 2-tier deception-driven model approach (2TDDSM)," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 34, no. 3, pp. 1999-2006, 2024. doi:10.11591/ijeecs.v34.i3.pp1999-2006.
- [22] V. Viola, "From honeypots to distributed deception platforms: theory and testing of emerging technologies for IT security," Master's thesis, Department of Communications and Computer Networks Engineering, Politecnico di Torino, Turin, Italy, 2019. Available: <https://webthesis.biblio.polito.it/13096>.
- [23] B. Patel and H. Ramadoss, "Dejavu: an open source deception framework," GitHub, 2024. [Online]. Available: <https://github.com/bhdresh/Dejavu> (accessed: Jan. 10, 2024).
- [24] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment," *NIST Special Publication*, vol. 800, p. 80, 2008, doi: 10.6028/NIST.SP.800-115.
- [25] S. P. Oriyano, "Introduction to penetration testing," *Penetration Testing Essentials*, pp. 1–13, 2017. doi: 10.1002/9781119419358.ch1
- [26] M. H. Almeshekeh and E. H. Spafford, "Cyber security deception," *Cyber Deception*, pp. 23–50, 2016. doi:10.1007/978-3-319-32699-3_2.
- [27] K. E. Heckman, F. J. Stech, R. K. Thomas, B. Schmoker, and A. W. Tsow, "Intrusions, deception, and campaigns," *Cyber Denial, Deception and Counter Deception*, pp. 31–52, 2015. doi:10.1007/978-3-319-25133-2_3.
- [28] S. Yek, "A deception based framework for the application of deceptive countermeasures in 802.11b wireless networks," thesis, Edith Cowan University, Research Online, Perth, Western Australia, Perth, Western Australia, 2003. Available: https://ro.ecu.edu.au/theses_hons/140.
- [29] C. Panek and R. Tracy, "Penetration testing tools," *CompTIA PenTest+ Practice Tests*, pp. 137–180, 2019. doi: 10.1002/9781119575931.ch4.
- [30] K. U. Sarker, F. Yunus, and A. Deraman, "Penetration taxonomy: a systematic review on the penetration process, framework, standards, tools, and scoring methods," *Sustainability*, vol. 15, no. 13, p. 10471, 2023, doi:10.3390/su151310471.
- [31] P. Mell, K. Scarfone and S. Romanosky, "The common vulnerability scoring system (CVSS) and its applicability to federal agency systems," *National Institute of Standards and Technology*, no. 7345, 2007.
- [32] A. Khazaei, M. Ghasemzadeh, and V. Derhami, "An automatic method for CVSS score prediction using vulnerabilities description," *Journal of Intelligent & Fuzzy Systems*, vol. 30, no. 1, pp. 89-96, 2016, doi: 10.3233/IFS-151733.
- [33] A. Rosli, A. M. Taib, H. Baharin, W. N. A. W. Ali and R. S. Hamid, "Enhanced risk assessment equation for IPv6 deployment," *Proceedings of the 5th International Conference on Computing and Informatics*, 2015. Available: https://www.researchgate.net/publication/281614304_Enhanced_Risk_Assessment_Equation_for_IPv6_Deployment.

BIOGRAPHIES OF AUTHORS






Anazel P. Gamilla    holds a Master's degree in Information Technology (MIT) from Tarlac State University (TSU), Philippines. An Instructor of the Information Technology Department, College of Engineering, former Chief of Management Information Systems Office at Central Luzon State University (CLSU) and a Department of Information Technology and Communications Technology (DICT-ILCDB) trainer. Her current research interests include computer networks, SDN, and cyber security. She can be contacted at email: apgamilla@clsu.edu.ph.



Dr. Thelma D. Palaoag    is the Graduate Program Coordinator of the College of Information Technology and Computer Science at the University of the Cordilleras. She is also the Director of the UC Innovation and Graduate Program Coordinator of the College of Information Technology and Computer Science Technology Transfer Office. She is passionate about writing and publishing researches in various disciplines. Her research interests focus on game-based learning, e-learning, machine learning, data analytics, intelligent systems, and artificial intelligence. Her involvement and exposure to various research projects and publication make her a notable academic researcher. She can be contacted at email: tdpalaoag@uc-bcf.edu.ph.



Dr. Marlon A. Naagas    holds a Doctorate degree in Information Technology (DIT) from the University of the Cordilleras (UC-BCF), Philippines. An Associate Professor of Information Technology Department, College of Engineering, Chief of Management Information Systems Office and Acting Dean of Admissions at Central Luzon State University (CLSU). He is a CISCO Cyber Security Scholarship Awardee, passed CCNA – CyberOps and CCCA. His current research interests include computer networks, cyber security and ethical hacking and has four research publications in the said field. He is also an active reviewer in several journals and conferences such as IEEE ICCET, ACM ICCBN, ACM ICNCT, IJECS, IRCITE. He can be contacted at email: manaagas@clsu.edu.ph.